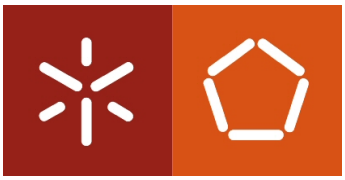


Universidade do Minho

Departamento de Informática

Relatório de Redes de Computadores
Grupo 3

Inês Alves (A81368) João Lopes (A80397)
Sofia Teixeira (a80624)

16 de Dezembro de 2018

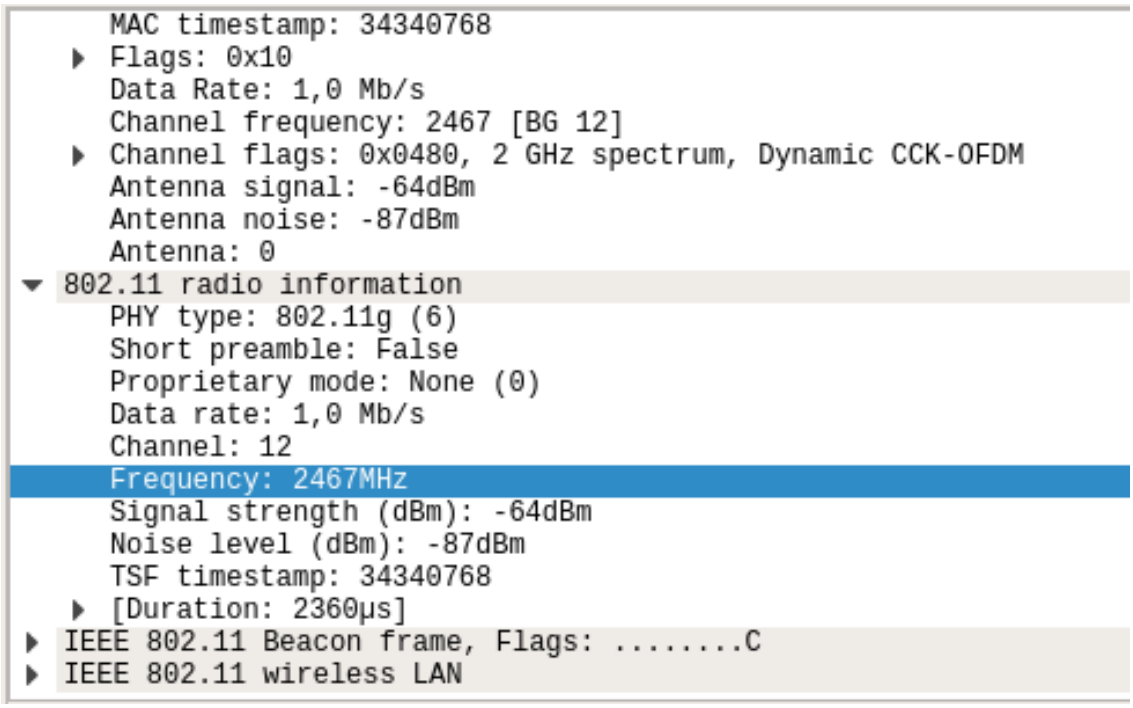
Conteúdo

1 Questões e Respostas

1.1 Pergunta 4: Acesso Rádio

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

Visto que estamos a operar na norma IEEE 802.11g, a sua frequência tem que estar entre 2400MHz e 2485000 MHz. O espectro está a operar a uma frequência de 2467MHz, estando este valor dentro do intervalo esperado e correspondendo ao canal 12.

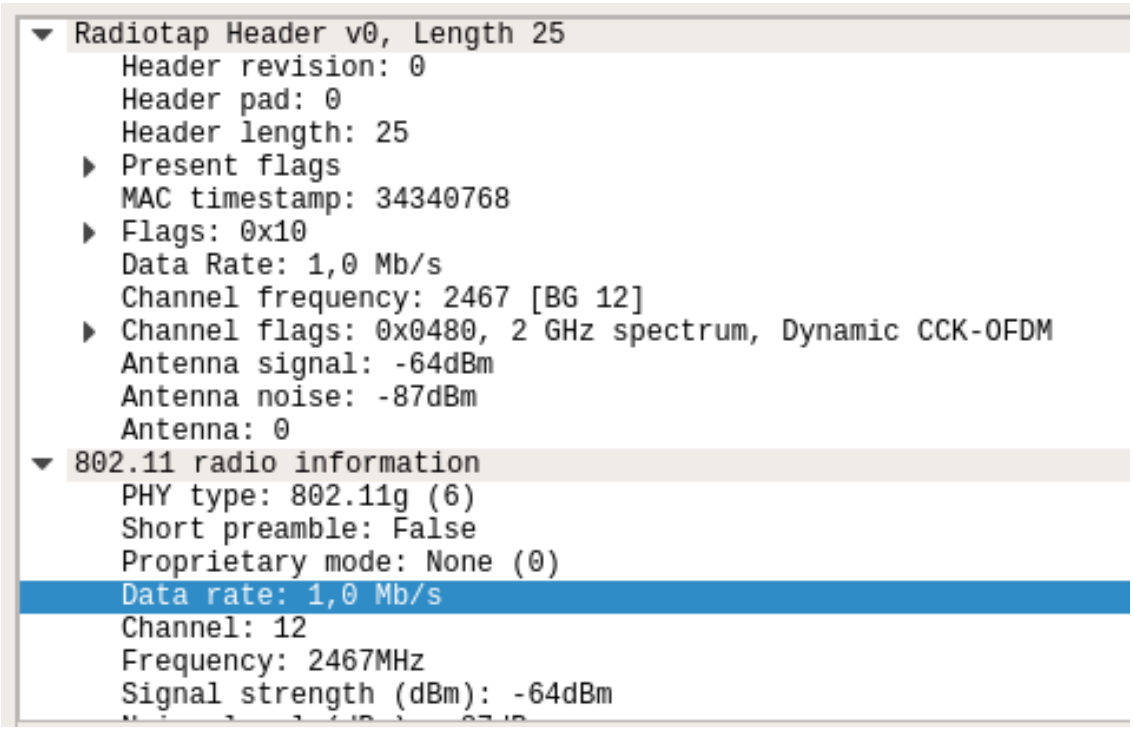


2. Identifique a versão da norma IEEE 802.11 que está a ser usada.

Está a ser usada a versão 802.11g, como já foi referido na alínea anterior.

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

A trama escolhida foi enviada com um débito de 1.0 Mbps. Este débito não corresponde ao débito máximo a que a interface WiFi pode operar, uma vez que o débito máximo desta é de 54Mbps, já que estamos a operar na norma IEEE 802.11g.

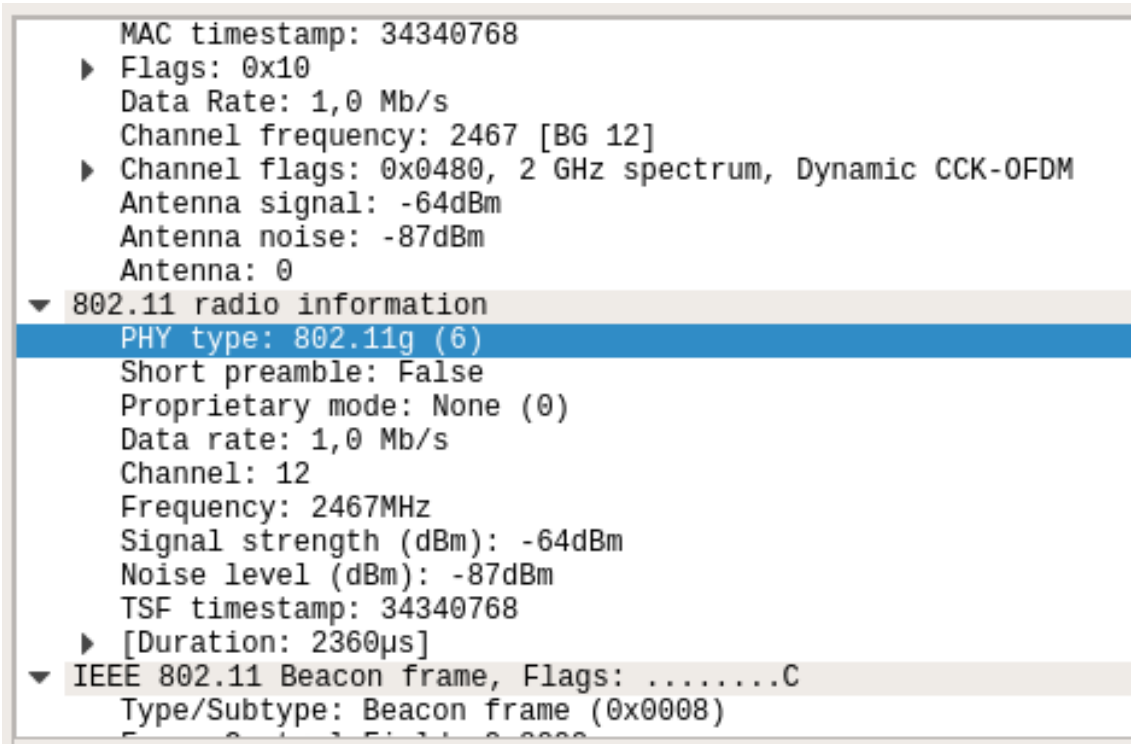

Radiotap Header v0, Length 25
Header revision: 0
Header pad: 0
Header length: 25
Present flags
MAC timestamp: 34340768
Flags: 0x10
Data Rate: 1,0 Mb/s
Channel frequency: 2467 [BG 12]
Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
Antenna signal: -64dBm
Antenna noise: -87dBm
Antenna: 0
802.11 radio information
PHY type: 802.11g (6)
Short preamble: False
Proprietary mode: None (0)
Data rate: 1,0 Mb/s
Channel: 12
Frequency: 2467MHz
Signal strength (dBm): -64dBm

1.2 Pergunta 5: Scanning Passivo e Scanning Ativo

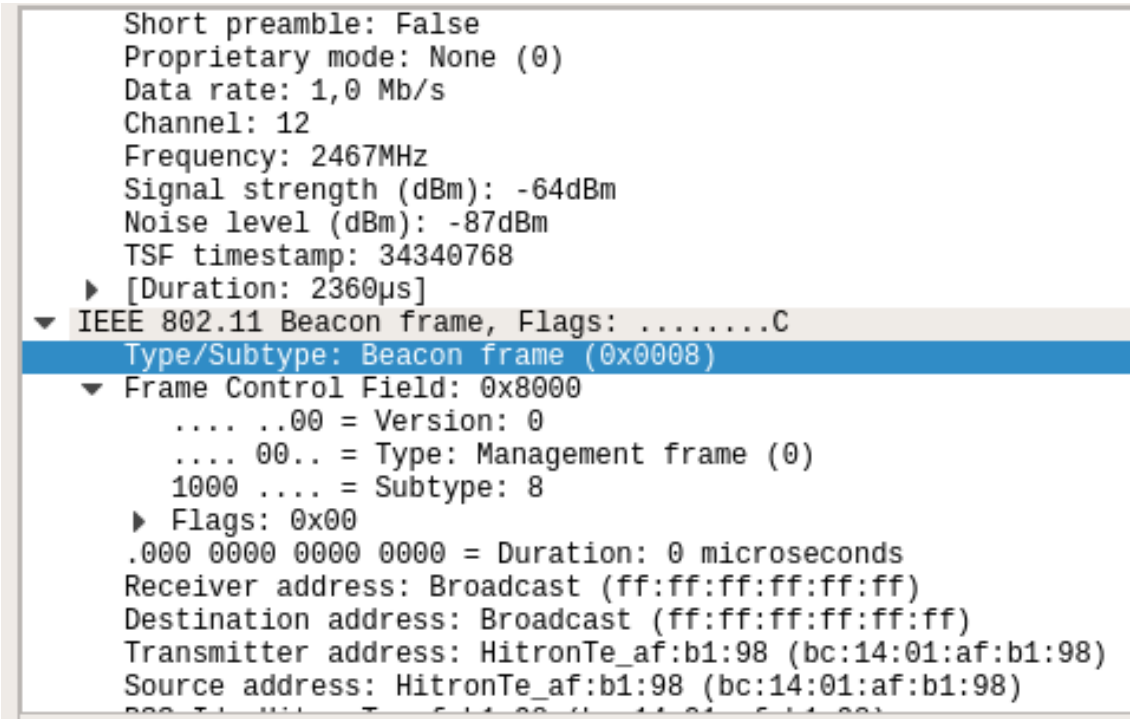
As tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (WiFi). Para a captura de tramas disponibilizada, responda às seguintes questões:

4. Selecione uma trama beacon (e.g., a trama 353). 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)?

Como já foi referido em alíneas anteriores, esta trama pertence ao tipo 802.11g.



O tipo e o subtipo dos seus identificadores estão apresentados na figura seguinte, onde podemos verificar que se trata de uma trama de gestão (Management frame), sendo este o tipo da trama. Já o subtipo tem como valor de identificação 8. Estas informações encontram-se específicadas no campo *Frame Control*, tendo este campo os 2 campos referidos: *type* e *subtype*.

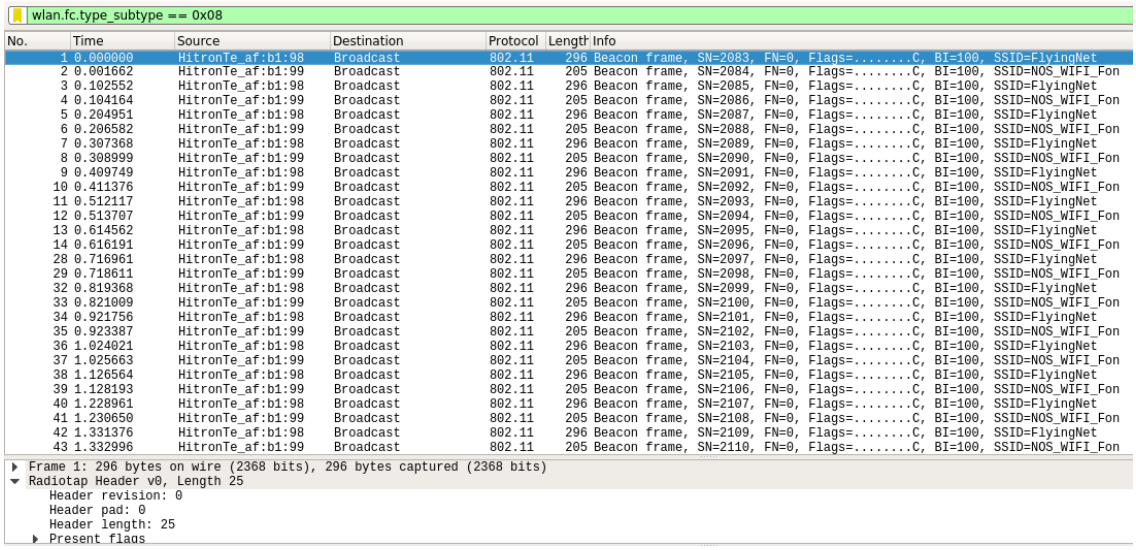


5. Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura. Explicite o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida.

Para listar todos os SSIDs dos APs (*Access Points*) começamos por aplicar o seguinte filtro: wlan.fc.type_subtype==0x08

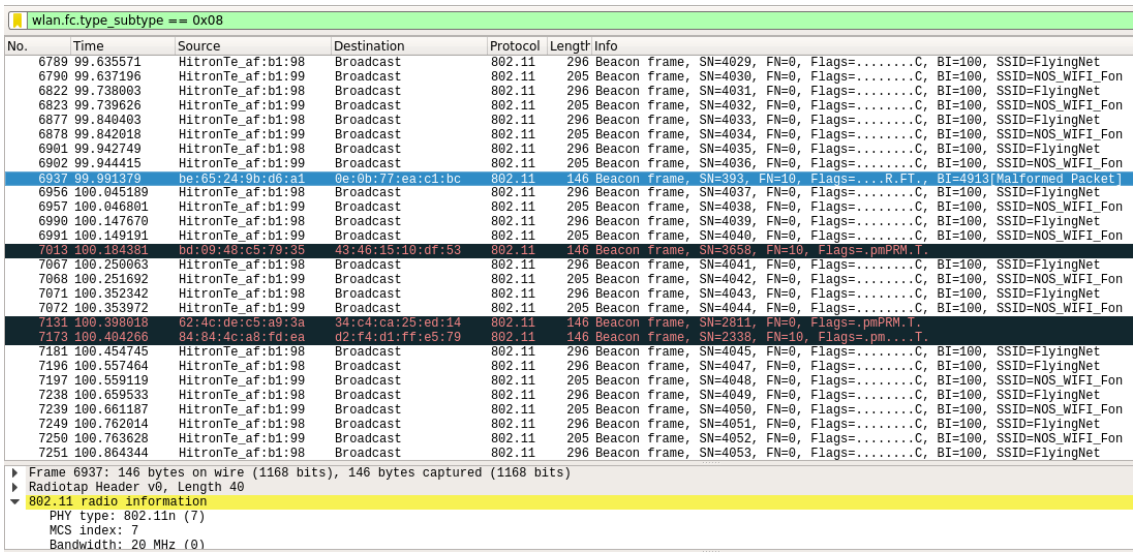
Este filtro faz com que sejam apresentadas somente tramas *Beacon*. A partir do resultado deste filtro podemos verificar 2 APs a operar na vizinhança da STA de captura:

1. FlyingNet
2. NOS_WIFI_Fon

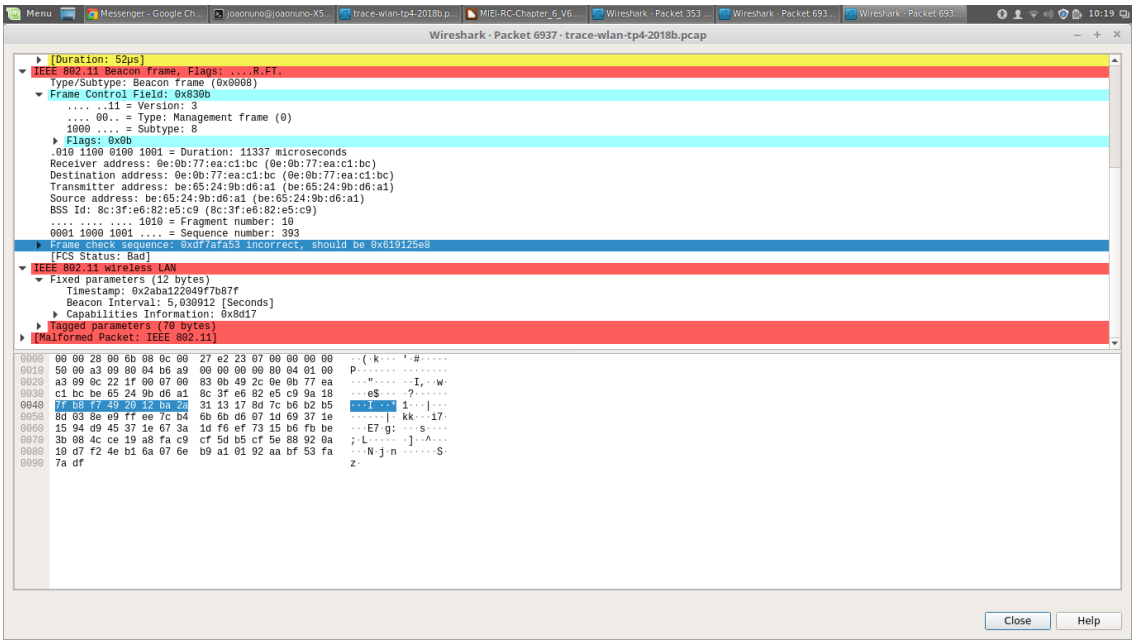


6. Verifique se está a ser usado o método de detecção de erros (CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique o porquê de usar detecção de erros neste tipo de redes locais.

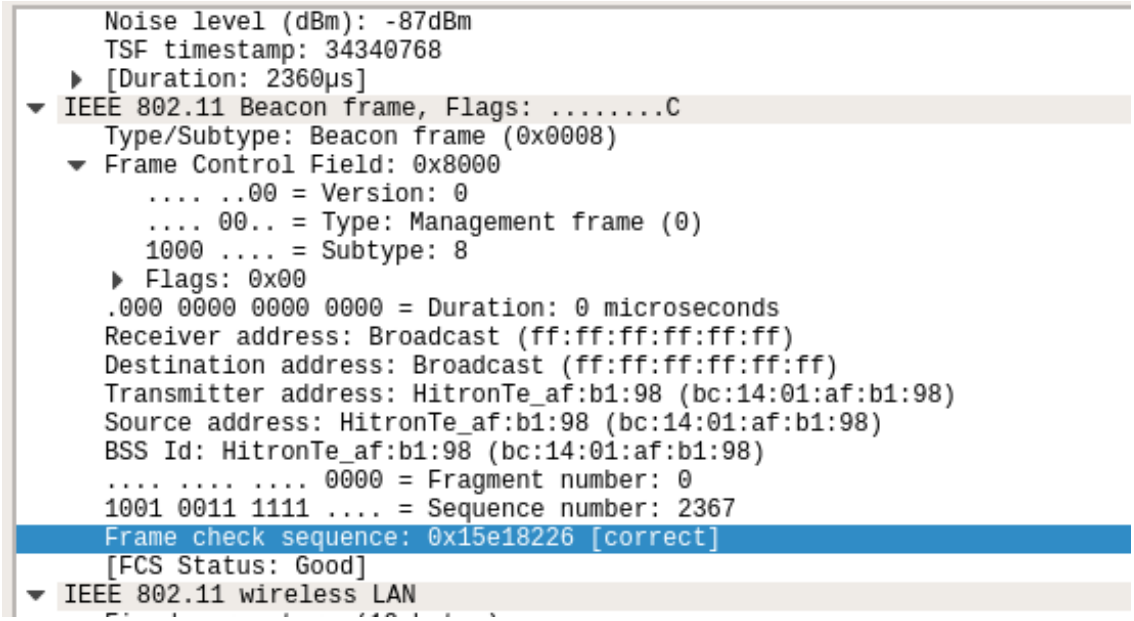
A partir das imagens seguintes podemos concluir que está a ser usado o método de deteção de erros (CRC), uma vez que está presente o campo *Frame Check Sequence*. De notar que a utilização de métodos de deteção de erros é improtante neste tipo de redes, uma vez que é mais frequente a ocorrência de colisões nestas.



Na imagem apresentada abaixo vemos que ocorreram erros na trama, já que o valor do campo *Frame Check Sequence* apresenta um valor incorreto, apresentando ainda o valor que o campo deveria ter em substituição do valor incorreto.



Por outro lado, na seguinte imagem conseguimos perceber que o campo *Frame Check Sequence* foi utilizado, mas não foi detetado nenhum erro.



Posto isto, concluimos facilmente que nem todas as tramas *Beacon* são recebidas corretamente.

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

O intervalo previsto entre tramas consecutivas é de 0.102400 segundos, tal como se pode verificar a seguir:

```
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 0x0000010bae9321fb
      Beacon Interval: 0,102400 [Seconds]
```

Na prática, a periodicidade de tramas *beacon*, apesar de apresentar um valor bastante próximo, não é verificada.

Através da figura seguinte podemos verificar que o intervalo entre 2 tramas *beacon* consecutivas (neste caso, 353 e 355), é dado por: 14.643405 - 14.540874 = 0.102531 segundos, sendo um valor mais pequeno do que o previsto.

wlan.fc.type_subtype == 0x08

No.	Time	Source	Destination	Protocol	Length	Info
340	13.825838	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2354, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
341	13.926596	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2355, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
342	13.928225	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2356, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
343	14.028868	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2357, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
344	14.030499	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2358, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
345	14.131398	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2359, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
346	14.133029	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2360, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
347	14.233824	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2361, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
348	14.235456	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2362, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
349	14.336138	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2363, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
350	14.337754	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2364, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
351	14.438603	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2365, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
352	14.440234	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2366, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
353	14.540874	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2367, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
354	14.542494	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2368, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
355	14.643405	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2369, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
356	14.645055	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2370, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
357	14.745813	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2371, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
358	14.848210	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2373, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
359	14.849841	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2374, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
360	14.950611	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2375, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
361	14.952099	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2376, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
362	15.052889	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2377, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
363	15.054500	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2378, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
364	15.155412	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2379, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
365	15.156998	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2380, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
366	15.257723	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2381, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
367	15.259284	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2382, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

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

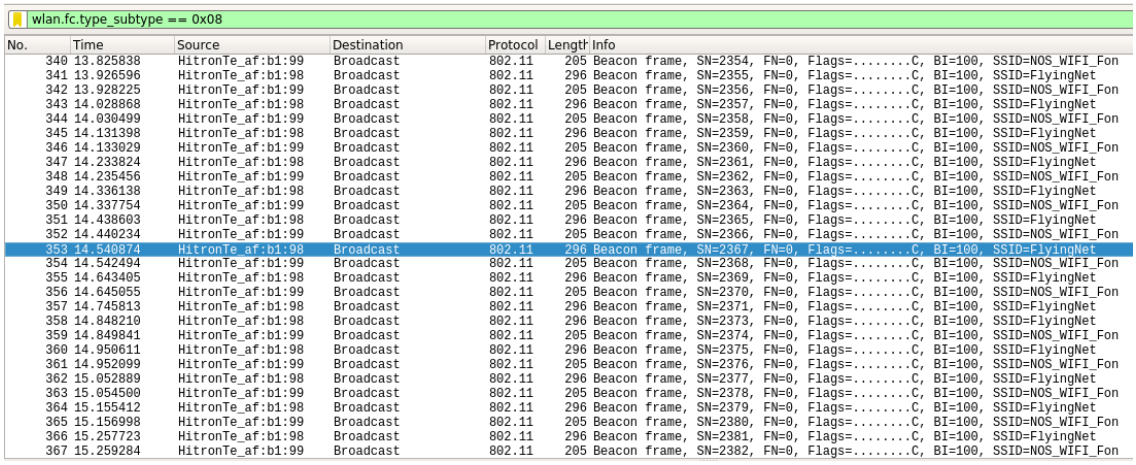
As tramas 353 e 354 têm nos campos *Receiver Address* e *Destination Adress* o endereço MAC ff:ff:ff:ff:ff:ff (*Broadcast*).

No entanto, no que toca aos campos *Transmitter Address* e *Source Address* os valores já não são iguais em ambas as tramas.

Na trama 353 estes campos possuem o valor bc:14:01:af:b1:98, correspondendo à STA HitronTe_af:b1:98, como podemos verificar na imagem abaixo.

```
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
```

Já quanto à trama 354 os campos referidos têm o valor bc:14:01:af:b1:99, correspondendo, analogamente, à STA HitronTe_af:b1:99.

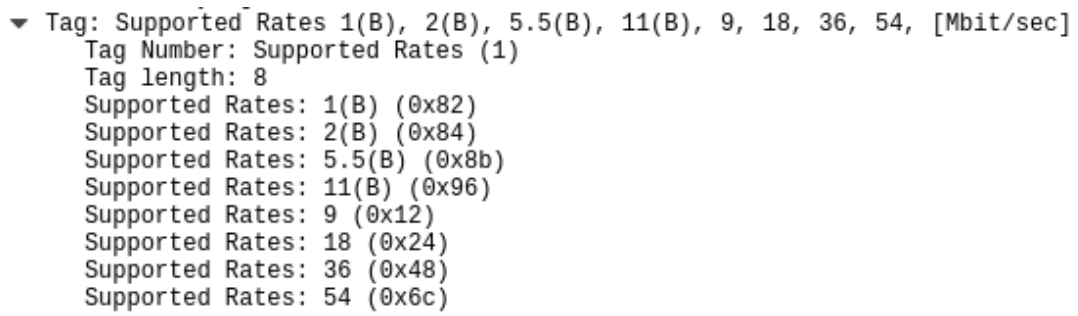


wlan.fc.type_subtype == 0x08

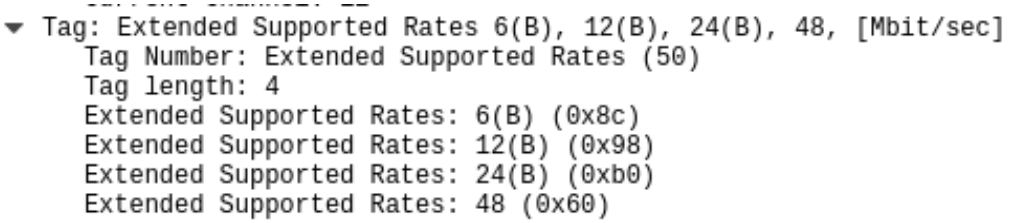
No.	Time	Source	Destination	Protocol	Length	Info
340	13.825838	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2354, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
341	13.926596	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2355, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
342	13.928225	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2356, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
343	14.028868	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2357, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
344	14.030499	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2358, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
345	14.131398	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2359, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
346	14.133029	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2360, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
347	14.233824	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2361, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
348	14.235456	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2362, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
349	14.336138	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2363, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
350	14.337754	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2364, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
351	14.438603	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2365, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
352	14.440234	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2366, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
353	14.540874	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2367, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
354	14.542494	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2368, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
355	14.643405	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2369, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
356	14.645055	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2370, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
357	14.745813	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2371, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
358	14.848210	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2373, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
359	14.849841	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2374, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
360	14.950611	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2375, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
361	14.952099	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2376, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
362	15.052889	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2377, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
363	15.054500	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2378, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
364	15.155412	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2379, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
365	15.156998	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2380, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
366	15.257723	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2381, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
367	15.259284	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2382, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon

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

Os débitos de base suportados pelo AP são: 1, 2, 5.5, 11, 9, 18, 36 e 54 Mbps. Já quanto os *extended supported rates* são suportados: 6, 12, 24 e 48 Mbps, como podemos verificar nas figuras seguintes:



```
▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
    Supported Rates: 9 (0x12)
    Supported Rates: 18 (0x24)
    Supported Rates: 36 (0x48)
    Supported Rates: 54 (0x6c)
```



```
▼ Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 4
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 12(B) (0x98)
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 48 (0x60)
```

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

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

O filtro *Wireshark* que nos permitiu visualizar todas as tramas *probing request* ou *probing response*, simultaneamente foi o seguinte:

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?

Temos um exemplo de um probing request para o qual houve um probing response nas tramas 2468 e 2469, correspondendo, respetivamente, ao *probe request* e ao *probe response*.

Um *wireless host* envia uma trama *probe request* a todos os APs que se encontrem ao alcance deste host. Os APs respondem a esta trama com uma trama *probe response* e o *wireless host* pode, então, escolher a que AP se associará, entre aqueles que enviaram uma trama *probe response*. Depois de escolher o AP com o qual o *host* se vai associar, este envia uma *association request frame* ao AP escolhido e este AP responde com uma *association response frame*.

De notar que esta segunda concordância entre pedido/resposta é importante, uma vez que um AP que responda a uma *probe response frame* inicial não sabe a que AP de resposta o *host* escolherá associar-se.

Uma vez associado a um AP, o *host* vai querer ingressar na sub-rede à qual o AP pertence.

wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5

No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=........C, SSID=2WIRE-PT-431
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
2469	70.149792	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0, Flags=........C, BI=100, SSID=FlyingNet
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, Flags=........C, BI=100, SSID=FlyingNet
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=........C, BI=100, SSID=FlyingNet
2475	70.151709	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_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	72.180590	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	94.190080	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

1.3 Pergunta 6: Processo de Associação

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

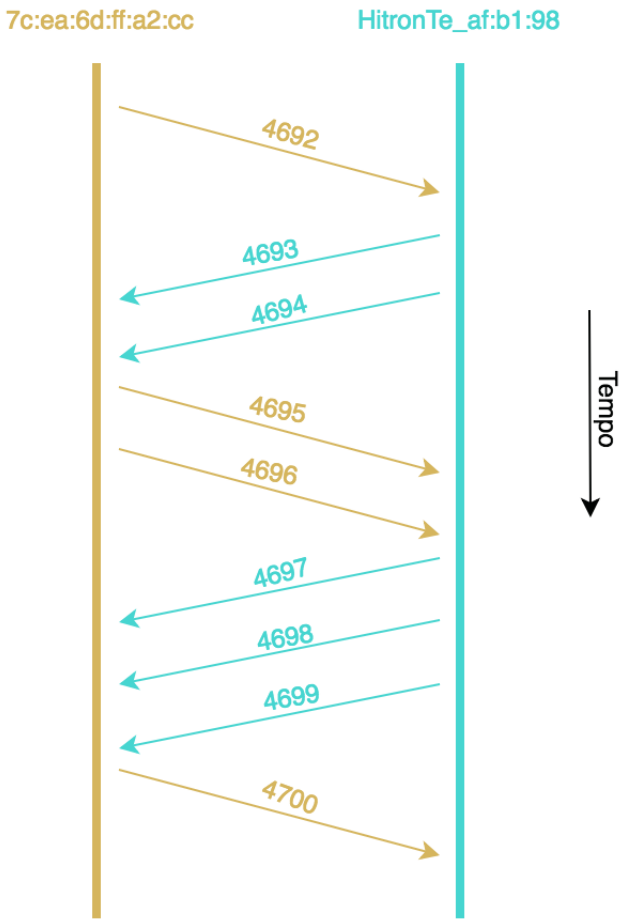
De seguida, é possível observar a nossa seleção de uma sequência correspondentes a um processo de associação completo entre a STA e o AP:

```
4692 83.663250     7c:ea:6d:ff:a2:cc    HitronTe_af:b1:98    802.11      59 Authentication, SN=67, FN=0, Flags=........C
4693 83.663574                          7c:ea:6d:ff:a2:cc (… 802.11      39 Acknowledgement, Flags=........C
4694 83.663681     HitronTe_af:b1:98    7c:ea:6d:ff:a2:cc    802.11      59 Authentication, SN=2439, FN=0, Flags=........C
4695 83.663750                          HitronTe_af:b1:98 (… 802.11      39 Acknowledgement, Flags=........C
4696 83.665976     7c:ea:6d:ff:a2:cc    HitronTe_af:b1:98    802.11     153 Association Request, SN=68, FN=0, Flags=........C, SSID=FlyingNet
4697 83.666176                          7c:ea:6d:ff:a2:cc (… 802.11      39 Acknowledgement, Flags=........C
4698 83.678873     HitronTe_af:b1:98    7c:ea:6d:ff:a2:cc    802.11     225 Association Response, SN=2440, FN=0, Flags=........C
4699 83.680045     HitronTe_af:b1:98    7c:ea:6d:ff:a2:cc    802.11     225 Association Response, SN=2440, FN=0, Flags=....R...C
4700 83.680364                          HitronTe_af:b1:98 (… 802.11      39 Acknowledgement, Flags=........C
```

Vejamos a sequência mais detalhadamente:

- 1.º: É feita a autenticação da STA
- 2.º: AP aceita a autenticação da STA
- 3.º: Autenticação do AP
- 4.º: Trama ACK enviada pela STA
- 5.º: STA faz *association request* ao AP
- 6.º: AP envia trama ACK
- 7.º: AP envia *association response*
- 8.º: Como a trama continha erros, a STA não recebeu a trama ACK num determinado intervalo de tempo. Assim, o AP envia novamente um *association response*. (A trama é reenviada)
- 9.º: STA envia trama ACK

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

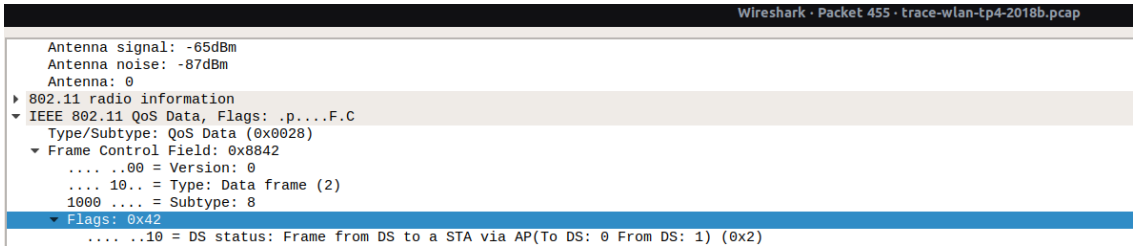


1.4 Pergunta 7: Transferência de Dados

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

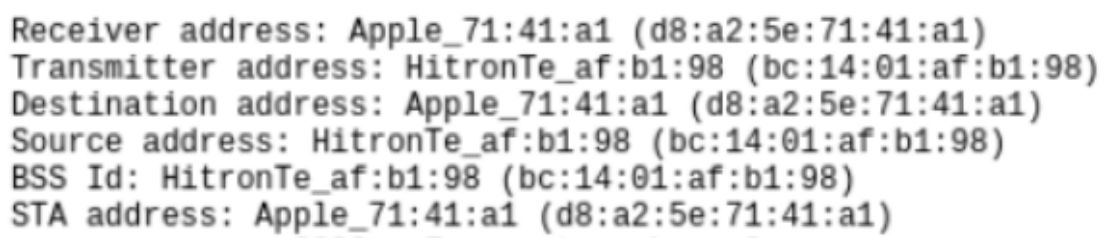
14. Considere a trama de dados nº455. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?

A flag *To DS* tem valor 0 e a flag *From DS* tem valor 1, indicando que a trama recebida veio do sistema de distribuição, logo não é local à WLAN.



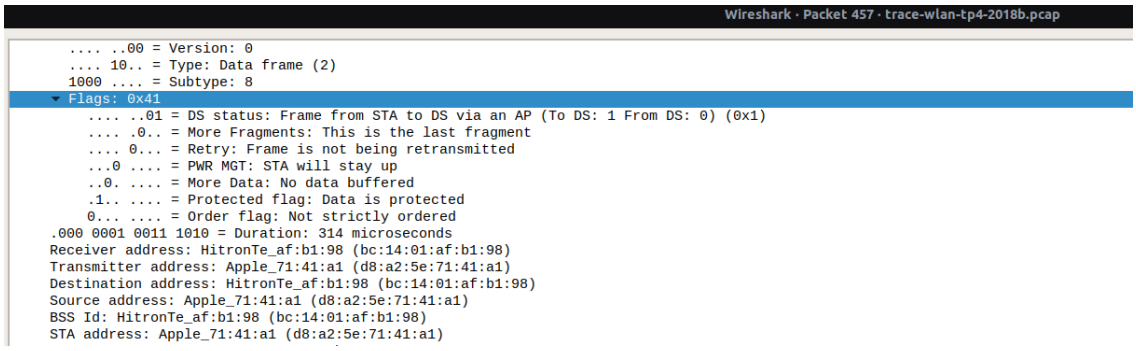
15. Para a trama de dados nº455, transcreva os endereços MAC em uso, identificando qual o endereço MAC correspondente ao host sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição?

Como podemos observar na seguinte figura, o endereço MAC correspondente ao *wireless host* é Apple_71:41:a1, ao AP é HitronTe_af:b1:98 e ao router de acesso ao sistema de distribuição é HitronTe_af:b1:98.



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

A trama 457 tem a flag *To DS* com valor 1 e a flags *From DS* com valor 0, significando que a trama está a ser transmitida para fora da rede local.



Quanto ao endereço MAC, podemos concluir que o AP corresponde ao *receiver adress*, a STA corresponde *transmitter adress* e o *router* corresponde ao *destination adress*.

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.)

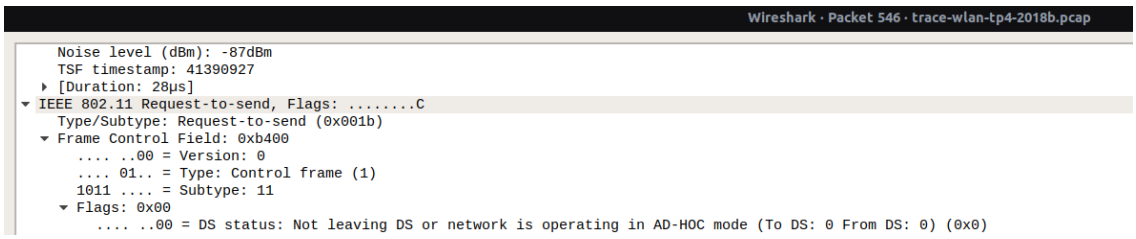
Ao longo da transferência de dados acima mencionada é transmitida uma trama Acknowledgement.

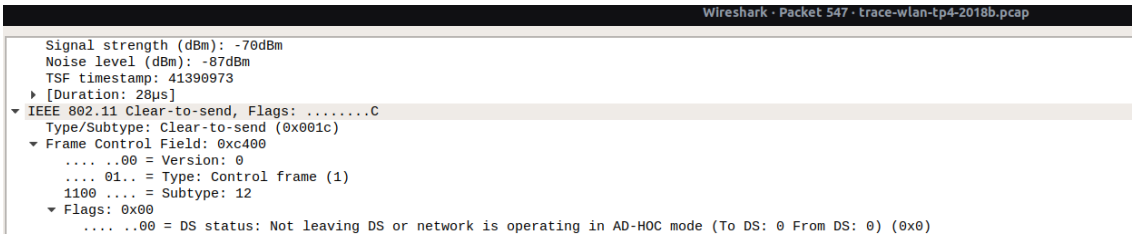
Tal como já foi referido neste relatório, uma rede *wireless* possui uma probabilidade muito maior de ocorrência de erros quando comparada a uma rede com fios. Posto isto, a utilização de tramas Acknowledgement é importante para detetar se há ou não erros na transferência de dados. Uma STA, após receber uma trama, quando não se verificam erros, envia a quem a transmitiu uma trama *acknowledgement*. Caso isto não aconteça durante um certo intervalo de tempo, ou seja, caso se verifique a ocorrência de erros na trama, esta é reenviada. Assim, quando ocorre um erro, é a partir da resposta da trama *acknowledgement* que é decidido se a trama é ou não reenviada.

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.

A opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN está a ser usada. As tramas 546 e 547 correspondem, respetivamente, a um *request-to-send*(RTS) e a um *clear-to-send*(CTS).

Como tanto a flag *To DS* como a flag *From DS* têm valor 0, é seguro dizermos que as redes estã a operar localmente.





Os sistemas envolvidos são HitronTe_af:b1:98 e Apple_10:6a:f5.

Neste exemplo, a STA (HitronTe_af:b1:98) envia um RTS para o AP (Apple_10:6a:f5) e este depois envia um CTS para a STA.

```
546 21.588982     HitronTe_af:b1:98 (… Apple_10:6a:f5 (64:… 802.11     45 Request-to-send, Flags=........C
547 21.588987                          HitronTe_af:b1:98 (… 802.11     39 Clear-to-send, Flags=........C
```

2 Conclusão

Com este projeto foi-nos possível aprofundar os nosso conhecimento sobre redes *wireless*. Para além disso, vimos ainda com mais detalhe o protocolo IEEE 802.11.

Pudemos ainda aprender que existem diversos tipos de tramas, tendo as tramas de controlo um papel fundamental na deteção de erros destas redes, uma vez que estas são muito mais propícias à ocorrência de colisões e erros quando comparadas a redes com fios.