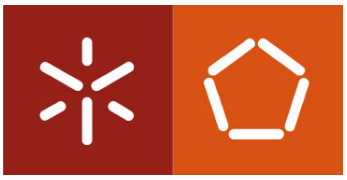


Universidade do Minho

Departamento de Informática

Redes de Computadores

Trabalho 4

Simão Brito (A89482)
António Silva (A89558)
José Martins (A90122)

1 de fevereiro de 2021

Simão Brito A89482

António Silva A89558

José Martins A90122

Conteúdo

Acesso Rádio

1.1 Para a trama correspondente 3XX em que XX corresponde ao seu número de TurnoGrupo

No.	Time	Source	Destination	Protocol	Length	Info
320	12.801833	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2334, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
321	12.902583	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2335, FN=0, Flags=........C, BI=100, SSID=FlyingNet
322	12.904212	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2336, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
323	13.005001	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2337, FN=0, Flags=........C, BI=100, SSID=FlyingNet
324	13.006518	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2338, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
325	13.107409	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2339, FN=0, Flags=........C, BI=100, SSID=FlyingNet
326	13.109035	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2340, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
327	13.209790	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2341, FN=0, Flags=........C, BI=100, SSID=FlyingNet
328	13.211424	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2342, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
329	13.312189	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2343, FN=0, Flags=........C, BI=100, SSID=FlyingNet
330	13.313819	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2344, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
331	13.414588	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2345, FN=0, Flags=........C, BI=100, SSID=FlyingNet
332	13.416217	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2346, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
333	13.516879	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2347, FN=0, Flags=........C, BI=100, SSID=FlyingNet
334	13.518509	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2348, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
335	13.619286	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2349, FN=0, Flags=........C, BI=100, SSID=FlyingNet

Figura 1.1: Trama correspondente ao número de grupo (325)

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

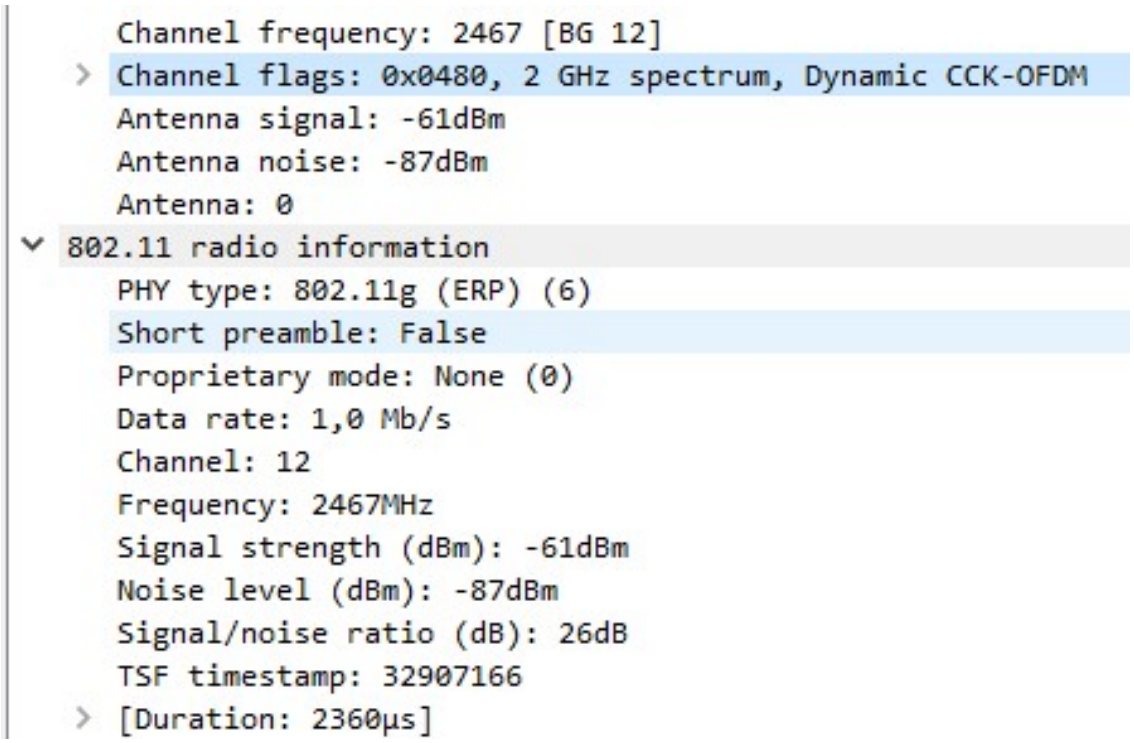


Figura 1.2

Como se pode observar na fig acima a rede sem fios está a operar numa frequência de espetro de 2467 MHz. Essa frequência corresponde ao canal 12.

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

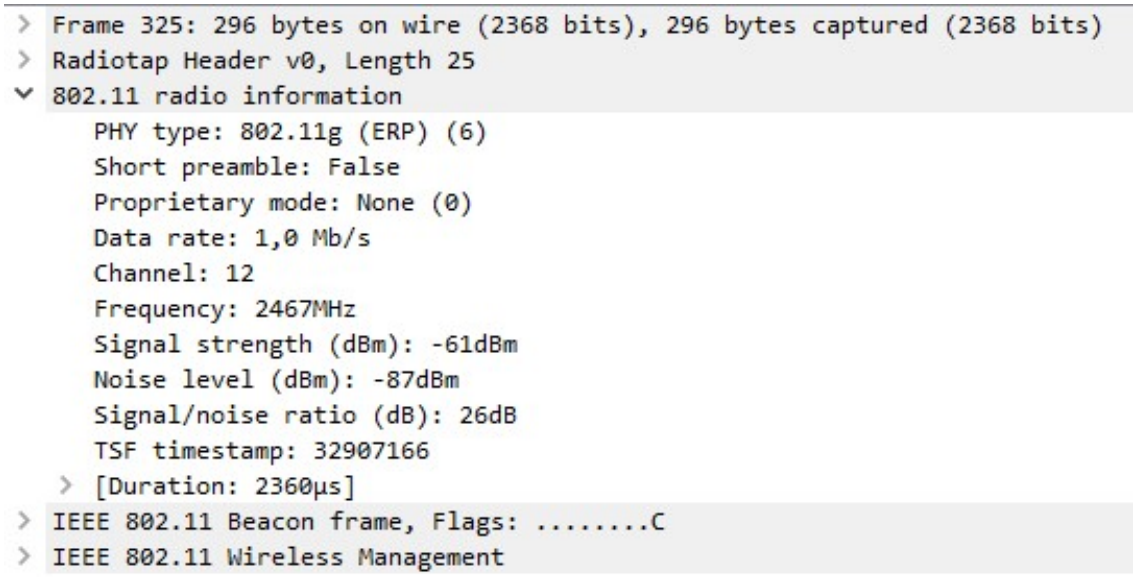


Figura 1.3

A versão da norma IEEE 802.11 que está a ser usada é "802.11g (ERP) (6)".

1.4 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.

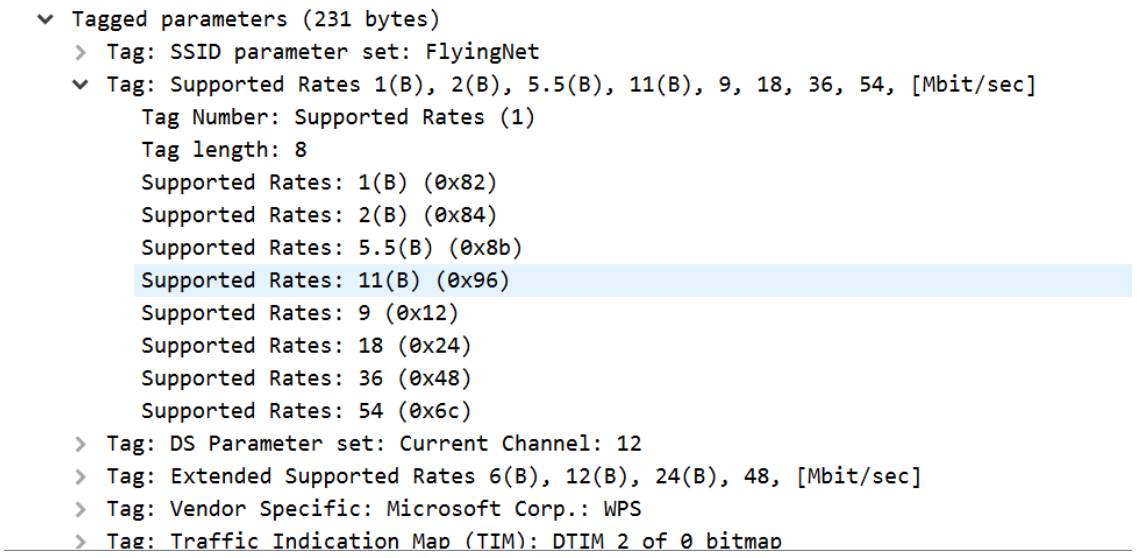


Figura 1.4: Análise do débito máximo

Através da análise da Figura 1.3, podemos concluir que a trama escolhida foi enviada a 1,0 Mb/s. Este valor de débito não corresponde ao débito máximo a que a interface WiFi pode operar, uma vez que, analisando a Figura 1.4 podemos ver que esse débito máximo é de 54 Mb/s.

Scanning Passivo e Scanning Ativo

2.1 4) Selecione uma trama beacon (e.g., trama 10XX). Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

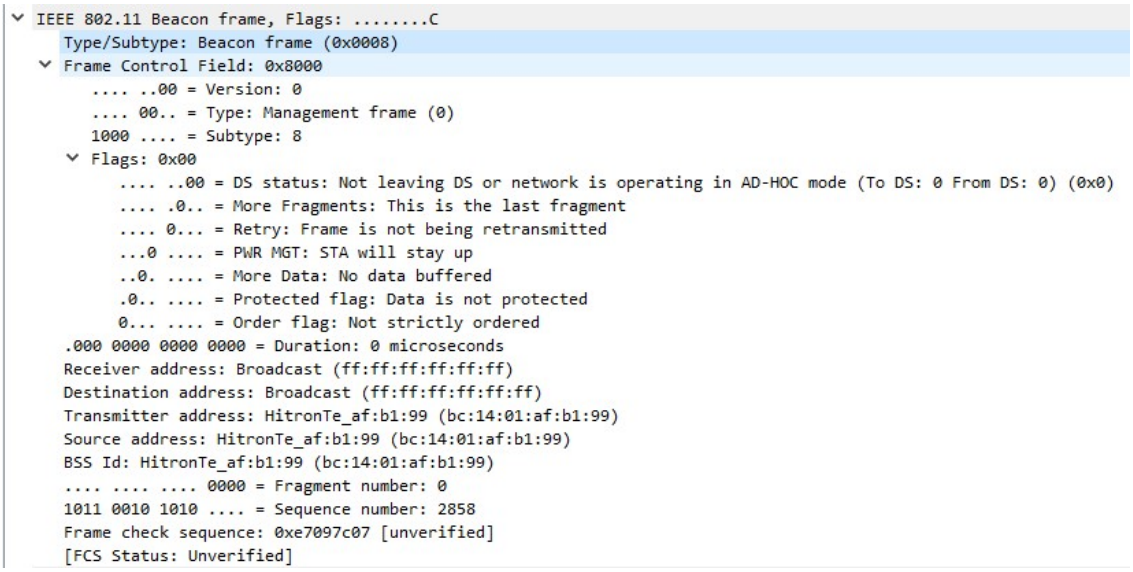


Figura 2.1: Cabeçalho de trama beacon

Como se pode verificar na Fig 2.1, a trama beacon selecionada pertence ao tipo Management. O valor do seu tipo é de 0x00 e o valor do seu subtipo (8) é 1000. Tudo esta informação está especificada na Frame Control Field do cabeçalho da trama.

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

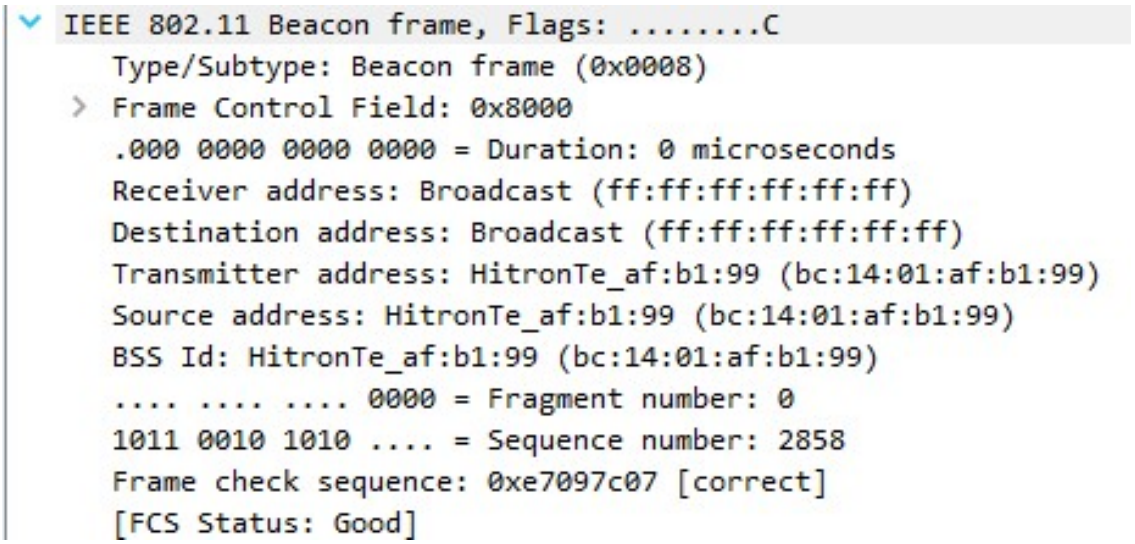


Figura 2.2: Análise de endereços MAC

Através da análise do cabeçalho da trama selecionada podemos identificar os seguintes endereços MAC em utilização:

Receiver address: (ff:ff:ff:ff:ff:ff)
Destination address: (ff:ff:ff:ff:ff:ff)
Transmitter address: (bc:14:01:af:b1:99)
Source address: (bc:14:01:af:b1:99)

Podemos concluir que as tramas estão a ser transferidas do router de acesso da rede local para um endereço de broadcast, ou seja para todos os hosts que estão ligados a esse router.

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

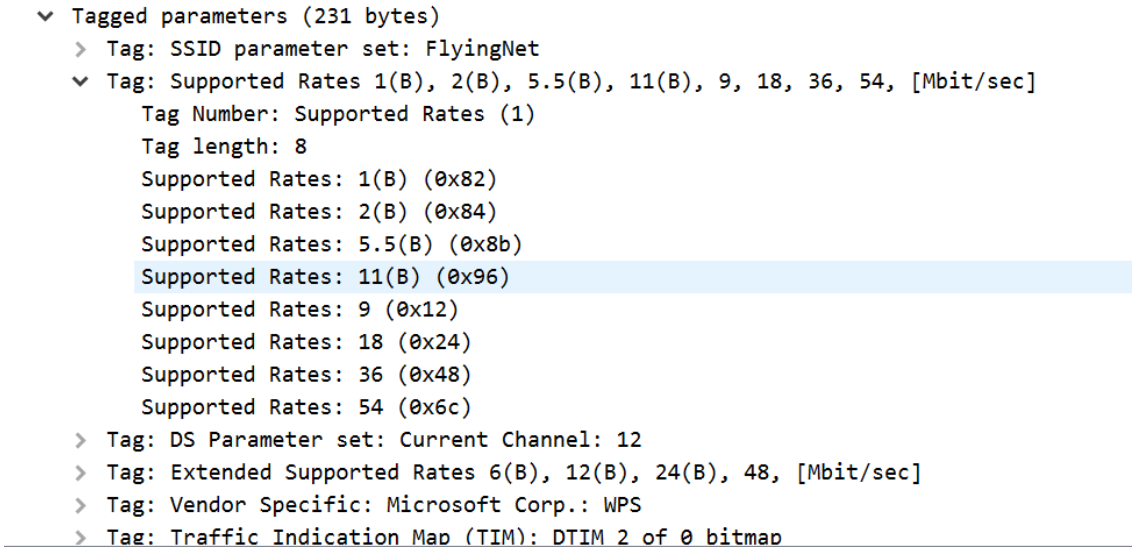


Figura 2.3: Análise de débitos de base

Os débitos de base são: 1(B) , 2(B), 5.5(B), 11(B), 9, 18, 36 e 54 [Mbit/sec].

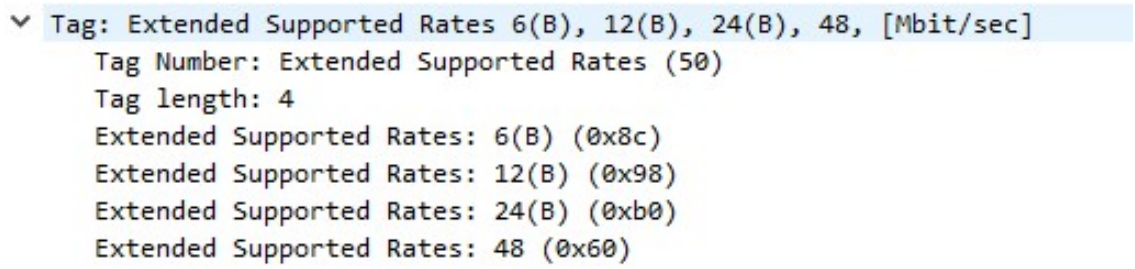


Figura 2.4: Análise de débitos adicionais

Os débitos adicionais são: 6(B) , 12(B), 24(B), 48 [Mbit/sec].

2.4 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.

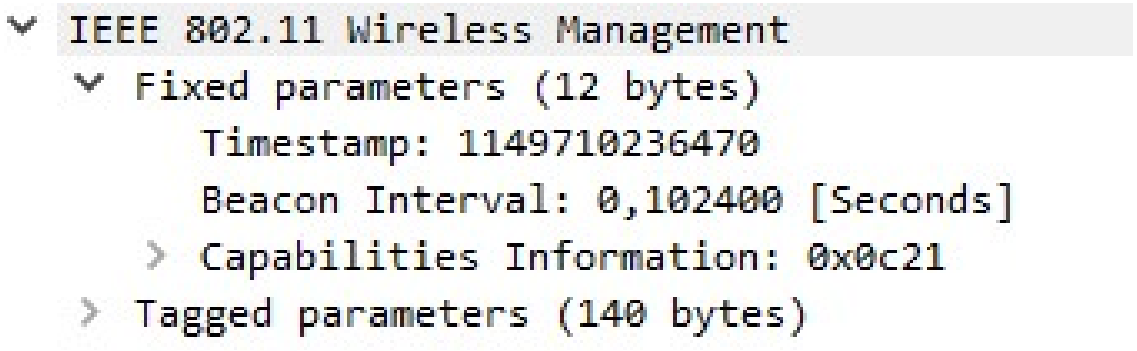


Figura 2.5: Intervalo de tempo previsto entre tramas beacon

O intervalo de tempo entre tramas beacon é de 0,102400 segundos, tal como se pode ver na figura acima.

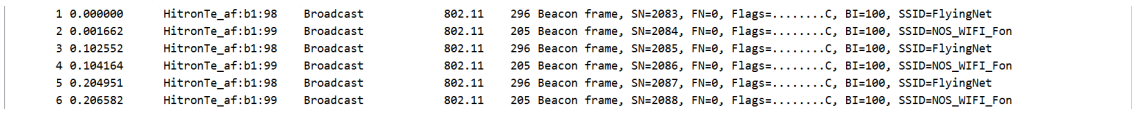


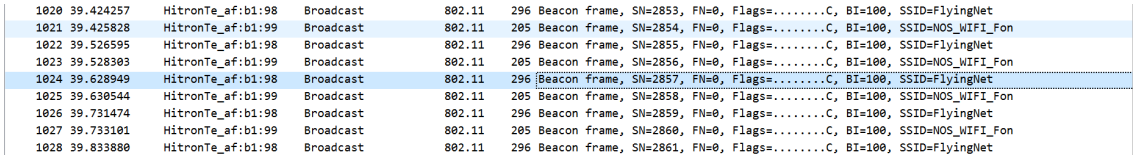
Figura 2.6: Tempos de tramas beacon

Através da análise dos tempos das tramas 1,2,3,4 podemos concluir o seguinte:

O intervalo de tempo, na prática, entre as tramas 1 e 3 que têm o mesmo SSID é de 0.102552 (0.102552 - 0.000000 = 0.102552), que é um valor muito aproximado do esperado. O intervalo de tempo, na prática entre as tramas 2 e 4 que têm o mesmo SSID é de 0.102502 (0.104164 - 0.001662 = 0.102552), que também é um valor muito aproximado do esperado.

Como se pode verificar o valor anunciado para o intervalo de tempo previsto entre tramas beacon verifica-se, pois atinge valores muito aproximados. Nâo é no entanto o valor esperado exato (e sim muito aproximado), o que pode ser justificado pelo possível congestionamento da rede.

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

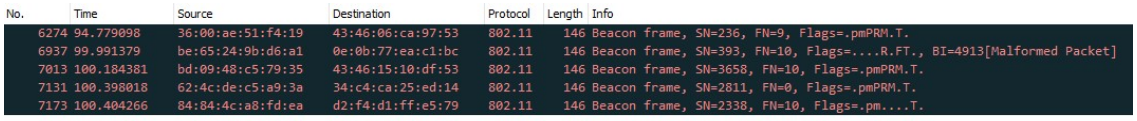


1020	39.424257	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2853, FN=0, Flags=........C, BI=100, SSID=FlyingNet
1021	39.425828	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
1022	39.526595	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID=FlyingNet
1023	39.528303	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
1024	39.628949	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID=FlyingNet
1025	39.630544	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2858, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
1026	39.731474	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2859, FN=0, Flags=........C, BI=100, SSID=FlyingNet
1027	39.733101	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
1028	39.833880	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID=FlyingNet

Figura 2.7

Na Fig 2.7 (acima) podemos identificar dois SSIDs: FlyingNet, NOS-WIFI-FON. Através da utilização de um filtro conseguimos apenas identificar estes dois SSIDs.

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



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.FT., BI=4913[Malformed Packet]
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.

Figura 2.8: Resultado da aplicação do filtro

Através da imagem anterior, conseguimos verificar que em 5 tramas ocorreu erros. Usa-se deteção de erros, dado que as redes sem fios são suscetiveis a interferências de ondas devido ao metodo de propogação de ondas, altamento povoado.

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

Utilizou-se o filtro:

```
wlan.fc.type_subtype == 0x04 || wlan.fc.type_subtype == 0x05
```

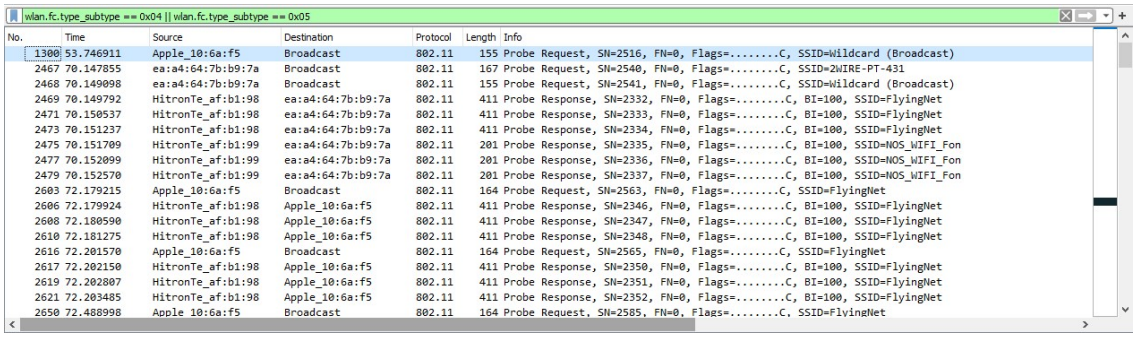


Figura 2.9: Resultado da aplicação do filtro

2.8 11) Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

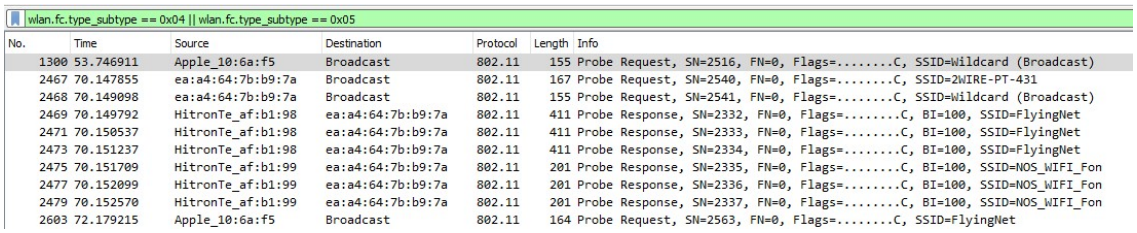


Figura 2.10: Probing request e respetivo probing response

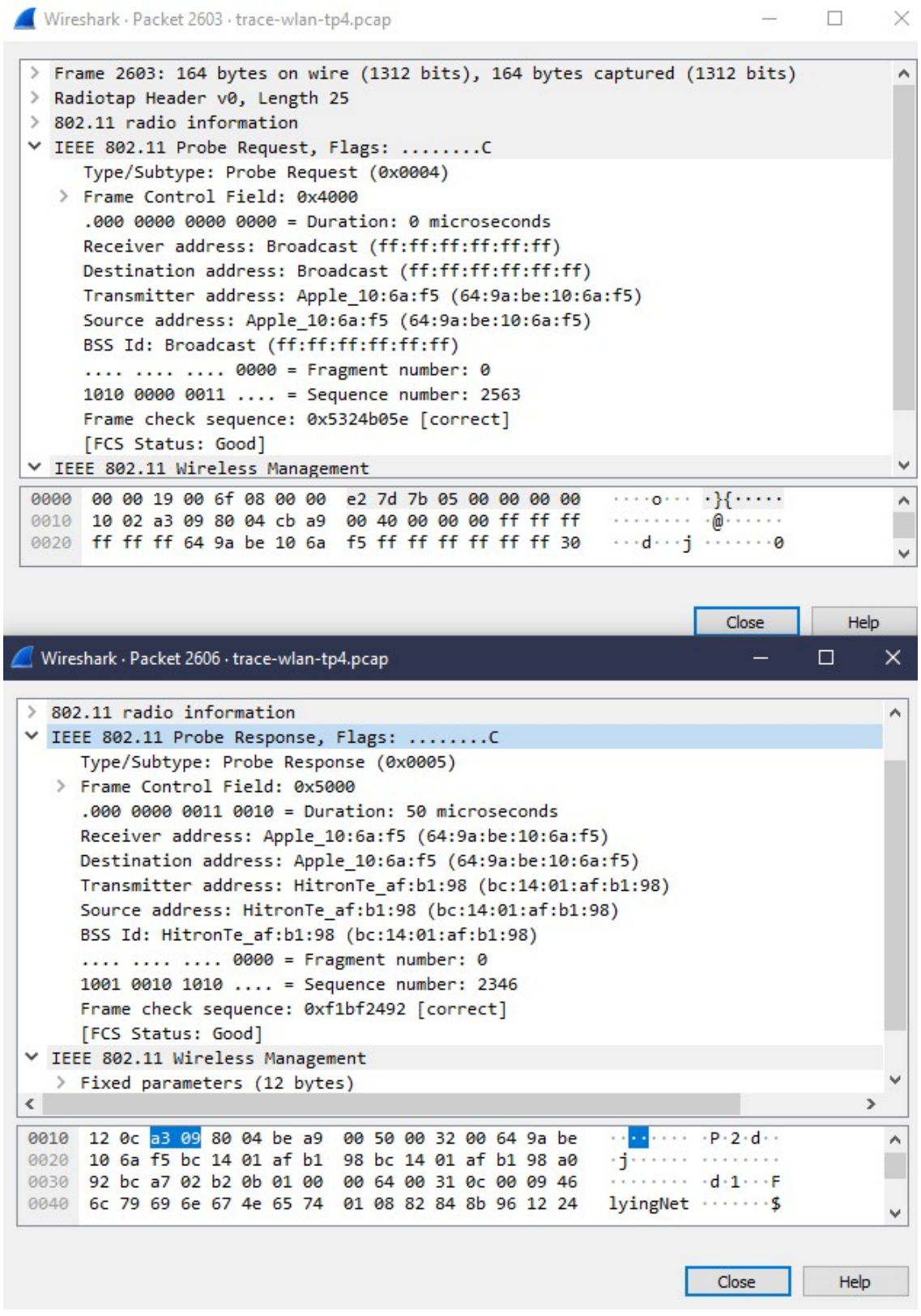


Figura 2.11: Sistemas endereçados a ambas as tramas

Uma *frame probe request* é enviada por um host para todos os AP's na sua vizinhança e estes respondem com um *trama probe response*. O host escolhe o AP a que se quer associar. Após escolher a qual se pretende associar, o host envia uma *frame association request* para o AP selecionado, sendo que este responde com uma *frame association response*.

Processo de Associação

3.1 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.

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

Figura 3.1: Sequência de tramas

Esta sequência de tramas corresponde a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação:

- Autenticação da STA;
- AP aceita autenticação da STA;
- Autenticação do AP;
- Trama ACK enviada pela STA;
- STA faz association request ao AP;
- Trama ACK enviada pelo AP;
- AP envia association response;
- Como a trama continha erros, a STA não recebeu a trama num determinado intervalo de tempo. Logo, o AP envia uma association response novamente (reenvia a trama).
- STA envia trama ACK;

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

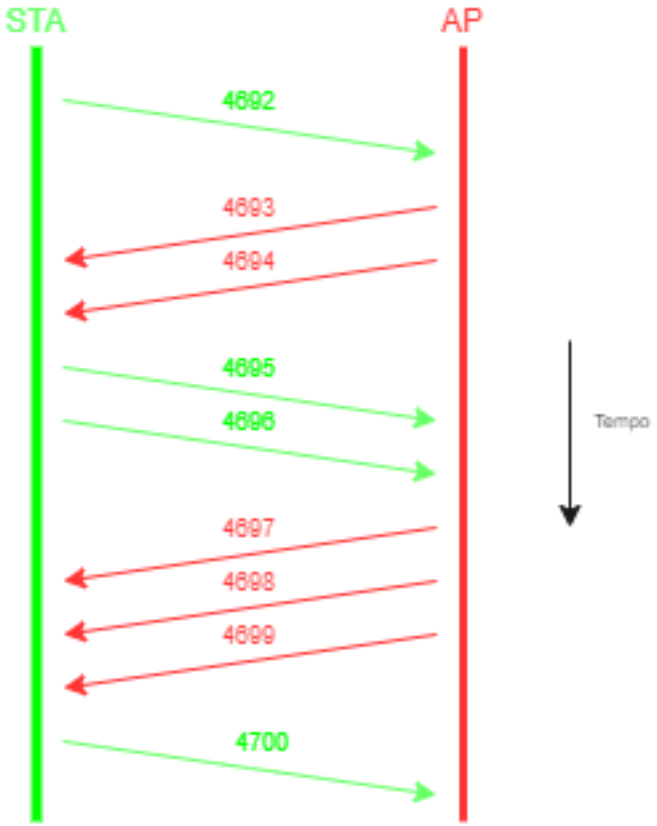


Figura 3.2: Diagrama

Transferência de Dados

4.1 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?

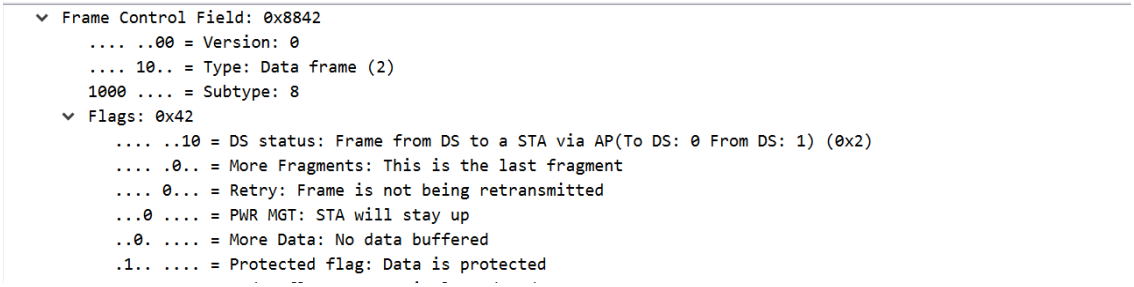


Figura 4.1: Campo Frame Control da trama nº455

Através da imagem acima e observando as flags, podemos concluir que a direcionalidade das tramas é de do sistema de distribuição para a STA, pois temos o campo To DS a 0 e o campo From DS a 1, logo é não é local à WLAN(rede local).

4.2 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?

```
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)
```

Figura 4.2: Endereços da trama nº455

Endereços MAC correspondentes ao:
- STA - d8:a2:5e:71:41:a1
- AP - bc:14:01:af:b1:98
- Router de acesso - bc:14:01:af:b1:98

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

```
Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Transmitter address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
```

Figura 4.3

```
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
```

Figura 4.4

Observando as imagens podemos identificar que o endereço de destino é bc:14:01:af:b1:98 que corresponde ao router da rede local e o endereço de origem é d8:a2:5e:71:41:a1 que corresponde ao endreço MAC da STA. Observamos também através das flags que temos To DS a 1 e o From DS a 0. Isto significa que as tramas estão a ser transmitidas da STA para fora da rede local, através do AP.

4.4 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.)

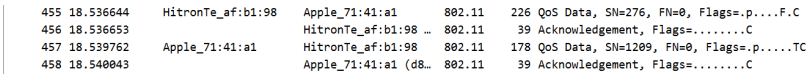


Figura 4.5: Tramas de controlo envolvidas na transferência de dados mencionada

Os subtipos de tramas de controlo transmitidas são acknowledgment, como pode ser visto através da figura. Uma vez que a rede wi-fi è mais suscetível a falhas, então são enviadas tramas de controlo com o objetivo de enviarem uma confirmação dizendo que as tramas enviadas foram corretamente recebidas.

4.5 18) O uso de tramas Request To Send e Clear To Send, apesar de opcional, é comum para efetuar "pré-reserva"do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/-Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos.

No caso do exemplo anterior, Figura 4.5, verificamos que não existem este tipo de tramas. No entanto decidimos apresentar um exemplo onde podemos observar a sua utilização.

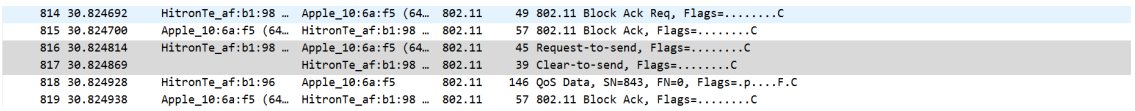


Figura 4.6: Tramas Request To Send e ClearTo Send

Conclusão

Este trabalho prático serviu mais uma vez de complemento às aulas teóricas e ajudou a consolidar a matéria lecionada nas mesmas.

Depois de finalizado o TP4, relativo às Redes Wireless, obtivemos mais conhecimentos sobre o funcionamento das redes wi-fi(802.11).

Tivemos a opurtunidade de rever e aplicar conceitos como, por exemplo, tipos e subtipos de tramas, STA, AP e direcionalidade de tramas.

Conseguimos também adquirir conhecimentos face ao uso de alguns filtros no WireShark.

Em suma, foi mais um trabalho importante no que toca a rever e aplicar conceitos das aulas teóricas e para nos ambientarmos melhor com esta disciplina de Redes de Computadores.