



UNIVERSIDADE DO MINHO

DEPARTAMENTO DE INFORMÁTICA

TP4 : Redes Sem Fios (802.11)

Redes e Computadores

Grupo 56

Bruno Martins (a80410) Filipe Monteiro (a80229)
Márcio Sousa (a82400)

19 de Dezembro de 2018

Conteúdo

1	Acesso Rádio	3
1.1	Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.	3
1.2	Identifique a versão da norma IEEE 802.11 que está a ser usada.	3
1.3	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.	3
2	Scanning Passivo e Scanning Ativo	4
2.4	Selecione uma trama beacon (e.g., a trama 3XX). 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)?	4
2.5	Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura? Explícite 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.	4
2.6	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.	5
2.7	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.	5
2.8	Identifique e registre 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.	6
2.9	As tramas beacon anunciam que o AP pode suportar vários débitos de base assim como vários “extended supported rates”. Indique quais são esses débitos?	6
2.10	Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente.	6
2.11	Identifique um probing request para o qual tenha havido um probing response.	6
3	Processo de Associação	7
3.12	Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.	7
3.13	Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo	8
4	Transferência de Dados	8
4.14	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?	8
4.15	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?	9
4.16	Como interpreta a trama nº457 face à sua direccionalidade e endereçamento MAC?	9
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.)	9

4.18 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.	10
5 Conclusão	10

1 Acesso Rádio

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

Analisando a trama 356 (grupo 56), verificamos que a frequência em que está a operar a rede sem fios é de 2467MHz, no canal 12.

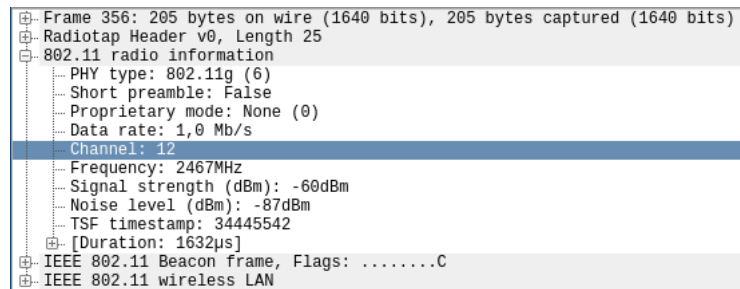


Figura 1: Informação do cabeçalho do do nível físico *radio information*

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

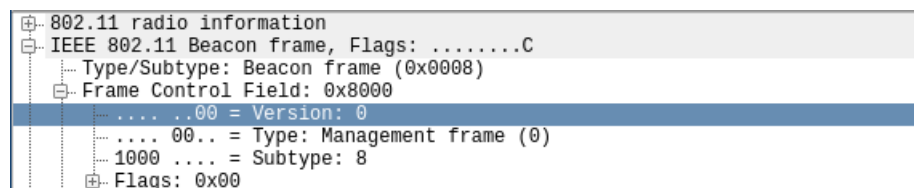


Figura 2: Versão da norma IEEE 802.11

Está a ser usada a versão 0 da norma IEEE 802.11 (*standard*).

1.3 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.

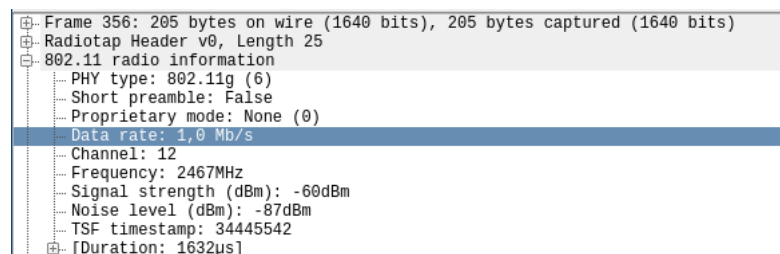


Figura 3: Débito a que foi transmitido a trama

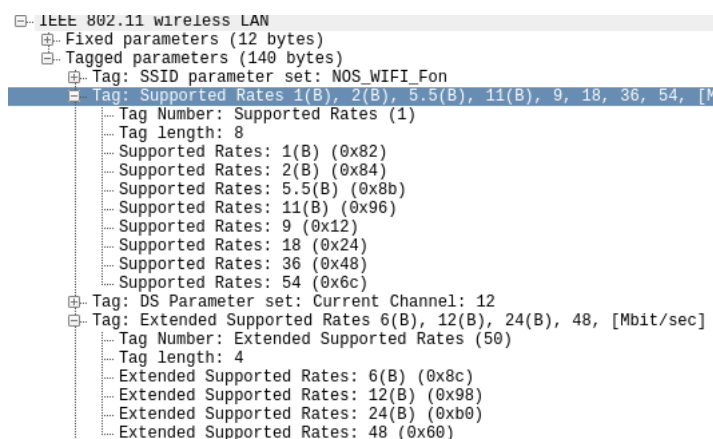


Figura 4: Vários débitos suportados pela interface

Foi enviada a um débito de 1Mb/s mas a placa de rede suportava débitos maiores pois no campo *supported rates* existem outros débitos maiores que o usado.

2 Scanning Passivo e Scanning Ativo

2.4 Selecione uma trama beacon (e.g., a trama 3XX). 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)?

Esta trama pertence ao tipo *Management Frame* (0) e ao subtipo *Beacon* (8).

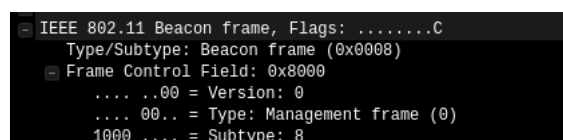


Figura 5: Parte do cabeçalho da trama Beacon

2.5 Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura? Explícite 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.

Os SSIDs são *NOS_WIFI_Fon* e *FlyingNet*. Para facilitar a procura dos SSIDs, aplicamos o filtro `wlan.fc.type_subtype == 0x0008` para filtrar apenas os *Beacon* e depois tornamos o campo SSID do cabeçalho do IEEE802.11 numa coluna, ordenando por esta.

[illegible]

Figura 6: SSIDs dos ARPs da captura

2.6 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.

Está a ser usado CRC porque a trama está a utilizar Frame Check Sequence, que é um algoritmo de Cycle Redundancy Check. Todas as tramas são recebidas corretamente pois quando se aplica o filtro no wireshark para apenas mostrar as tramas com FCS incorreto não é mostrada nenhuma.

```
Frame check sequence: 0x14cc7723 [correct]
[FCS Status: Good]
```

Figura 7: Utilização de FCS

2.7 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 de tempo entre as tramas é de 100ms. Verifica-se que numa das redes existentes (*NOS_WIFI_ZON*) não respeitava a periodicidade anunciada (valores mais baixos que o esperado).

```
[Time delta from previous captured frame: 0.100770000 seconds]
[Time delta from previous displayed frame: 0.100770000 seconds]
```

Figura 8: intervalo de tempo das tramas Beacon

- 2.8 Identifique e registre 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.

```

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

```

Figura 9: Endereços Mac das tramas Beacon

- 2.9 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 dos APs podem ser verificados nas imagens seguintes:

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

Figura 10: Débito base

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

Figura 11: Débito do “extended supported rates”

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

wlan.fc.type_subtype == 0x04 or wlan.fc.type_subtype == 0x05						
Time	Source	Destination	Protocol	Length	Info	
1390.53.746911	Apple_10:6a:f5	Broadcast	802.11	166	Probe Request, SN=2515, 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=Wi-Fi-PT-431	
2468.70.149698	ea:a4:64:7b:b9:7a	Broadcast	802.11	166	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	
2472.70.150537	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	
2477.70.152699	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	
2478.70.152878	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	
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=2346, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2698.72.180599	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	
2610.72.201570	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2565, FN=0, Flags=.....C, SSID=FlyingNet	
2617.72.202159	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	

Figura 12: Tramas de request com o filtro na parte verde

- 2.11 Identifique um probing request para o qual tenha havido um probing response.

Na primeira imagem a trama selecionada é um request, e na segunda a trama selecionada é a resposta ao request.

No.	Time	Source	Destination	Protocol	Length	Info
1589	70.140941	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2540, 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	70.149998	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	70.151789	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

```

# Frame 1380: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
# Radiotap Header v0, Length 25
# 802.11 radio information
# IEEE 802.11 Probe Request, Flags: .....C
  Type/Subtype: Probe Request (0x0004)
  Frame Control Field: 0x4080
    0000 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: Apple_10:6a:f5 (04:9a:be:10:6a:f5)
  Source address: Apple_10:6a:f5 (04:9a:be:10:6a:f5)
  BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
  .... .. 0000 = Fragment number: 0
  1001 1101 0100 .... = Sequence number: 2516
  Frame check sequence: 0xe703906b [correct]
  [FCS Status: Good]
# IEEE 802.11 wireless LAN

```

Figura 13: Probe Request

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	70.151789	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

```

# Frame 2469: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits)
# Radiotap Header v0, Length 25
# 802.11 radio information
# IEEE 802.11 Probe Response, Flags: .....C
  Type/Subtype: Probe Response (0x0005)
  Frame Control Field: 0x5000
    0000 0000 0011 0010 = Duration: 50 microseconds
  Receiver address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
  Destination address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
  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 0001 1100 .... = Sequence number: 2332
  Frame check sequence: 0xbce842e3 [correct]
  [FCS Status: Good]
# IEEE 802.11 wireless LAN

```

Figura 14: Probe response

3 Processo de Associação

3.12 Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

2463	70.041852	HitronTe_af:b1:98	Broadcast	802.11	296	8 Beacon frame, SN=3452, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2464	70.043449	HitronTe_af:b1:98	Broadcast	802.11	285	8 Beacon frame, SN=3453, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2465	70.144299	HitronTe_af:b1:98	Broadcast	802.11	296	8 Beacon frame, SN=3454, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2466	70.145895	HitronTe_af:b1:98	Broadcast	802.11	205	8 Beacon frame, SN=3455, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	4 Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431
2468	70.149998	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	4 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	5 Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2470	70.149800	HitronTe_af:b1:98	802.11	39	13 Acknowledgement, Flags=.....C	
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	5 Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2472	70.150544	HitronTe_af:b1:98	802.11	39	13 Acknowledgement, Flags=.....C	
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	5 Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2474	70.151244	HitronTe_af:b1:98	802.11	39	13 Acknowledgement, Flags=.....C	
2475	70.151789	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	5 Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2476	70.151716	HitronTe_af:b1:98	802.11	39	13 Acknowledgement, Flags=.....C	
2477	70.152089	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	5 Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2478	70.152106	HitronTe_af:b1:98	802.11	39	13 Acknowledgement, Flags=.....C	
2479	70.152570	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	5 Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2480	70.152582	HitronTe_af:b1:98	802.11	39	13 Acknowledgement, Flags=.....C	
2481	70.246616	HitronTe_af:b1:98	Broadcast	802.11	296	8 Beacon frame, SN=3455, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2482	70.248226	HitronTe_af:b1:98	Broadcast	802.11	205	8 Beacon frame, SN=3456, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2483	70.348997	HitronTe_af:b1:98	Broadcast	802.11	296	8 Beacon frame, SN=3457, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2484	70.350698	HitronTe_af:b1:98	Broadcast	802.11	285	8 Beacon frame, SN=3458, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2485	70.352671		Broadcast_04:6a:f5	802.11	39	12 Clear-to-send, Flags=.....C
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70	11 Authentication, SN=2542, FN=0, Flags=.....C
2487	70.362950	Apple_10:6a:f5	Apple_10:6a:f5 (6..	802.11	39	13 Acknowledgement, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	11 Authentication, SN=2338, FN=0, Flags=.....C
2489	70.381878	HitronTe_af:b1:98	802.11	39	13 Acknowledgement, Flags=.....C	
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175	6 Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2491	70.383873	Apple_10:6a:f5	Apple_10:6a:f5 (6..	802.11	39	13 Acknowledgement, Flags=.....C
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	1 Association Response, SN=2339, FN=0, Flags=.....C
2493	70.389352	HitronTe_af:b1:98	802.11	39	13 Acknowledgement, Flags=.....C	

Figura 15: Sequencia de frames de um processo de associação completo entre uma *Station* e uma *AP*

Da frame 2464 até á 2493 foi associado o dispositivo com MAC *Apple_10:6a:f5*. ao AP com MAC *bc:14:01:af:b1:98*.

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

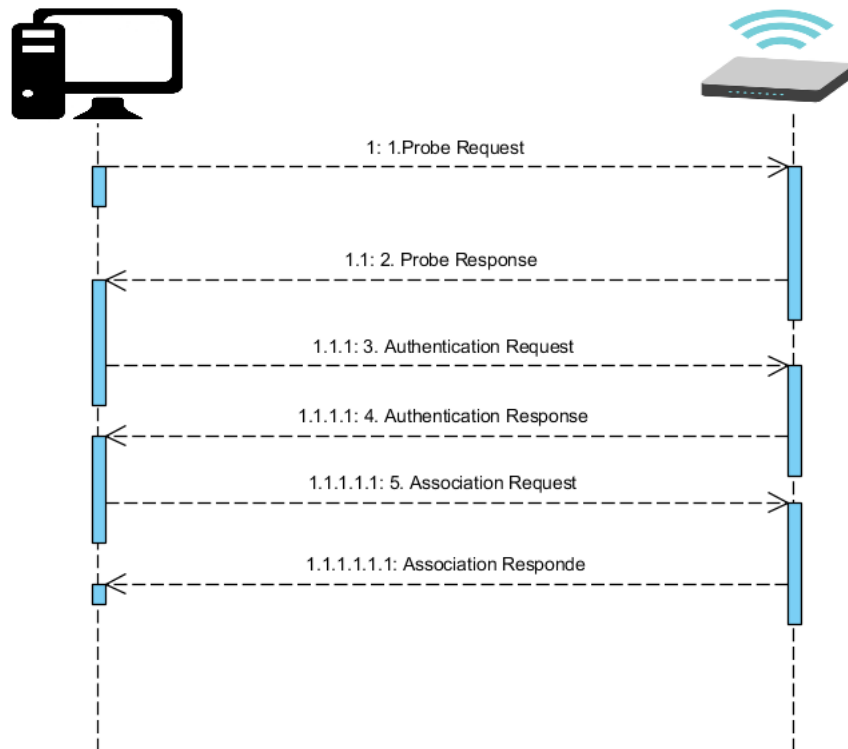


Figura 16: Diagrama com o processo de associação

4 Transferência de Dados

4.14 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?

Pode concluir-se que não é local à WLAN, pois a trama vem de um sistema de distribuição (DS) para o dispositivo *host*, através do ponto de acesso (visível na *Flag* "DS status").

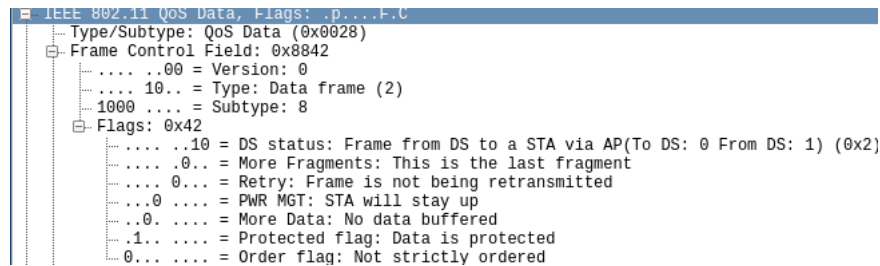


Figura 17: Campo Frame Control da trama

4.15 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 18: Vários campos com os vários endereços MAC

- MAC STA: d8:a2:5e:71:41:a1
- MAC AP: bc:14:01:af:b1:98
- MAC Router: bc:14:01:af:b1:98

Neste caso, o router para além de AP, é o ponto de ligação com o sistema de distribuição.

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

Esta trama está a ser enviada do dispositivo *host* (STA) para o sistema de distribuição através (DS) através do ponto de acesso (AP).

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.)

Os subtipos existentes nas tramas de controlo ao longo da transferência de dados são os seguintes:

- 8 - *Block Ack Request*
- 9 - *Block Ack*
- 11 - *RTS*
- 12 - *CTS*
- 13 - *ACK*

Existem porque apenas um dispositivo pode comunicar de cada vez com o AP, sendo necessário o controlo de quem está a comunicar e quando termina para outro poder começar. Numa rede Ethernet isto não é necessário pois cada dispositivo tem um domínio de colisão diferente (em IEEE802.11 o espaço é partilhado podendo haver colisão).

4.18 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.

15 0.631114	Apple_10:6a:f5 (6...	HitronTe_af:b1:98...	802.11	45	11 Request-to-send, Flags=.....C
16 0.631128		Apple_10:6a:f5 (6...	802.11	39	12 Clear-to-send, Flags=.....C

Figura 19: Exemplo de duas tramas - uma RTS e outra CTS - usadas na troca de dados entre STA e AP/Router

Verifica-se que está a ser usado RTS e CTS sendo que nas tramas apresentadas na figura, a primeira é *Station* 64:9a:be:10:6a:f5 a enviar um RTS e na seguinte o AP/Router bc:14:01:af:b1:98 envia um CTS, concedendo permissão a transferir dados.

5 Conclusão

Este trabalho incidiu no que diz respeito ao protocolo IEEE 802.11, tanto a nível do formato das suas tramas, como ao nível do endereçamento dos componentes que constituem a comunicação sem fios. Relativamente a tramas, sabemos agora que estas se dividem em três tipos, Tramas de Gestão que, tal como o seu nome diz, são as responsáveis pela gestão da comunicação entre os vários participantes da rede (*stations*, *AP* and *routers*, isto é, pelo estabelecimento e manutenção da comunicação, Tramas de Controlo que controlam o envio e receção de mensagens, e Tramas de Dados, responsáveis pela transmissão de dados. Foi abordado também como os nossos dispositivos conseguem encontrar, aceder e usar uma rede sem fios.