Universidade do Minho
Licenciatura em Engenharia Informática

UC de Redes de Computadores

Ano Letivo de 2022/2023

Trabalho Prático 4 - Redes sem Fios (Wi-Fi)

Rodrigo Monteiro, Diogo Abreu, e Gustavo Barros

e-mail: {a100706,a100646,a100656}@alunos.uminho.pt

Índice

1 Acesso Rádio

Trama nº 106:

```
802.11 radio information
    PHY type: 802.11n (HT) (7)
    MCS index: 0
    Bandwidth: 20 MHz (0)
    Short GI: False
    Greenfield: True
    FEC: BEC (0)
    Data rate: 6.5 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -90 dBm
    Noise level (dBm): -93 dBm
    Signal/noise ratio (dB): 3 dB
    TSF timestamp: 929663
    .... .... .... .... .... .... .... ...1 = Last part of an A-MPDU: True
    .... .... .... .... .... .... .... ..0. = A-MPDU delimiter CRC error: False
    A-MPDU aggregate ID: 0
```

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

   A rede sem fios está a operar sobre a frequência 2412 MHz (2.4 GHz) e corresponde ao canal 1.

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

   A versão da norma é 802.11n (HT), HT significando *Higher Throughput*, que é uma extensão do *standard* 802.11, e utiliza múltiplas antenas para aumentar a velocidade de troca de dados.
   Para além disso, pode ser usada nas frequências 2.4 GHz e 5 GHz (neste caso está a ser utilizada a frequência 2.4 GHz), e foi a primeira Wi-Fi que introduziu o suporte para *Multiple-Input and Multiple-Output*.

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

   A trama escolhida, 106, foi enviada com um débito de 6.5 Mb/s, estado longe do máximo teórico de 600 Mb/s da versão 802.11n. Tal pode ter ocorrido devido a diversas razões como um valor baixo de largura de banda do canal (por exemplo, caso a largura de banda (20 MHz) esteja a ser dividida por vários dispositivos), interferências, distância e qualidade do sinal, limitações de hardware, etc.

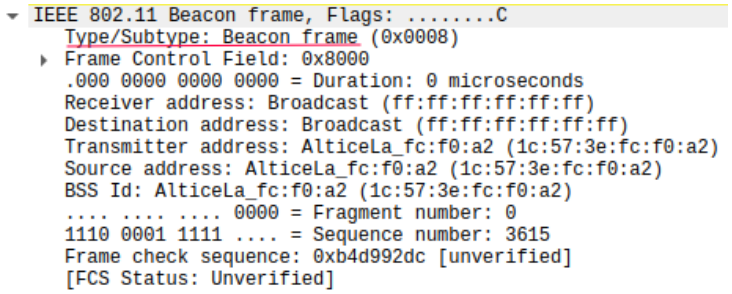
4) *Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama.*

   A força do sinal, *Signal strength*, é de -90 dBm, ou seja, a este nível a probabilidade de conexão é muito baixa.

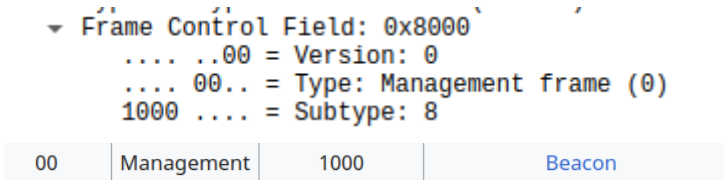
Signal strength	Expected Quality
-90dBm	Chances of connecting are very low at this level

2 *Scanning* Passivo e *Scanning* Ativo

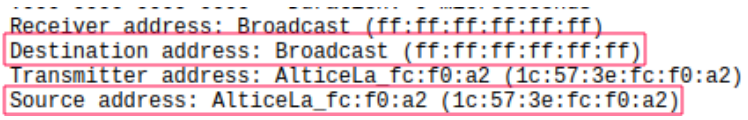
5) *Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados?*



A trama selecionada foi novamente a trama nº 106, visto que esta é uma trama beacon.
Esta possui *frame type* de "Management frame", com valor de tipo igual a 00 e subtipo 1000 (que corresponde a *beacon*). Estas informações estão especificadas no Frame Control Field no cabeçalho IEEE 802.11 beacon frame.

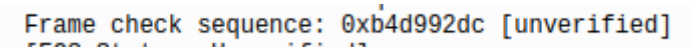


6) *Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?*



O endereço de destino é de *broadcast*, ou seja, `ff:ff:ff:ff:ff:ff`, visto que *beacon frames* são transmitidos periodicamente para "anunciar" a presença da rede *wireless*, e para sincronização dos dispositivos na rede. Receiver address é o MAC address do dispositivo que recebe a trama, e destination address é o endereço do dispositivo que tem de receber a trama, o dispositivo de destino.
O endereço de origem conclui-se que seja o AP, access point/ router (`1c:57:3e:fc:f0:a2`) — equivale ao *transmitter address* (que transmitiu) e *source address* (quem gerou).

7) *Verifique se está a ser usado o método de deteção de erros (CRC). Justifique.*

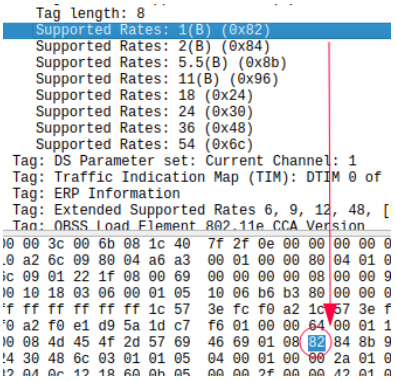


O método de deteção de erros (CRC) não está a ser utilizado devido ao facto de não ser extremamente necessário, pois *beacon frames* são transmitidos periodicamente com um tamanho fixo e estrutura padronizada, não compensando adicionar mais overhead para deteção, pois o objetivo é estes serem transmitidos com rapidez e eficiência, de modo a não influenciarem ou sobrecarregarem a rede.

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

```
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
  Tagged parameters (154 bytes)
    Tag: SSID parameter set: "MEO-WiFi"
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 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: 18 (0x24)
        Supported Rates: 24 (0x30)
        Supported Rates: 36 (0x48)
        Supported Rates: 54 (0x6c)
```

Todos os pacotes *management frames* são transmitidos usando um destes *basic rates*.



Por exemplo, o byte 82, 1000 0010 (o *basic rate* utiliza um *encoding* que coloca o primeiro bit a 1), corresponde a 1 Mb/s (000 0010 $= 02 = 1\,Mb/s$).

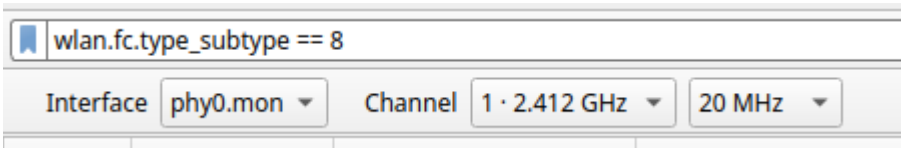
value for few of the rates:
02 = 1 Mb/s
03 = 1.5 Mb/s
04 = 2 Mb/s
05 = 2.5 Mb/s
06 = 3 Mb/s
09 = 4.5 Mb/s
11 = 5.5 Mb/s

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

```
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
      Timestamp: 2159414172377
      Beacon Interval: 0.102400 [Seconds]
    Capabilities Information: 0x1401
```

O valor é anunciado na própria trama beacon: `0.102400 seconds`. Idealmente este intervalo seria regular, no entanto, na prática, este intervalo pode variar devido por exemplo a congestionamento ou interferências na rede, apesar disso, geralmente não seria uma variação significativa.
Verificamos que a trama nº 107 também possui o mesmo intervalo de tempo, destacando-se, neste caso, precisão no valor.

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



Foi utilizado o seguinte filtro de modo a visualizar apenas os *beacon frames*.
Para listar os SSIDs foi selecionado no menu Wireless "WLAN Traffic":

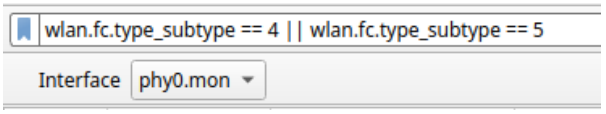
BSSID	Channel	SSID	Percent Packets	Percent Retry	Retry	Beacons	Data Pkts	Probe Reqs	Probe Resp	Auths	Deauths	Other	Protection
00:06:91:29:a9:c0	1	[redacted]	0.9	21.5	17	9	47	0	23	0	0	0	TKIP
00:06:91:29:a9:c2	1	MEO-WiFi	2.4	11.5	25	185	0	0	32	0	0	0	
00:06:91:45:be:30	1	MEO-45BE30	1.8	27.3	45	107	0	0	58	0	0	0	
00:06:91:45:be:32	1	MEO-WiFi	4.6	10.8	45	354	1	0	60	0	0	0	
00:06:91:62:40:a2	1	GV BRAGA	0.1	0.0	0	0	0	4	1	0	0	0	
00:06:91:9b:f2:a0	1	MEO-9BF2A0	2.0	1.1	2	177	0	0	2	0	0	0	
00:06:91:9b:f2:a2	1	MEO-WiFi	0.1	42.9	3	3	0	0	4	0	0	0	
00:06:91:9e:9b:b0	1	MEO-9E9BB0	8.9	1.8	14	717	62	0	19	0	0	0	CCMP
00:06:91:9e:9b:b2	1	MEO-WiFi	8.3	2.2	16	722	1	0	20	0	0	0	
00:06:91:d6:88:50	1	MEO-D68850	11.1	5.5	55	866	61	0	73	0	0	0	CCMP
00:06:91:d6:88:52	1	MEO-WiFi	8.7	5.8	45	711	1	0	65	0	0	0	
1c:57:3e:fc:f0:a0	1	MEO-FCF0A0	9.1	3.0	24	780	0	0	33	0	0	0	
1c:57:3e:fc:f0:a2	1	MEO-WiFi	9.1	4.3	35	776	1	0	43	0	0	0	
74:9b:e8:f3:9a:46	1	FlyingNet	13.6	4.2	52	893	232	0	86	2	1	11	CCMP
90:aa:c3:ee:2e:c6	1	NOS-2EC6	10.1	7.8	71	769	24	0	114	0	0	0	TKIP
b0:4e:26:a3:af:08	3	TP-LINK_AP_AF08	0.0	50.0	1	1	0	0	1	0	0	0	
cc:19:a8:d9:ed:e0	1	MEO-D9EDE0	0.0	100.0	2	0	0	2	0	0	0	0	
fc:77:7b:e7:c8:76	1	NOS-C876	8.4	0.0	0	736	2	0	18	0	0	0	CCMP
fe:d1:24:24:88:7e	1	K6000 Plus	0.1	0.0	0	6	2	0	0	1	0	1	CCMP
ff:ff:ff:ff:ff:ff	1	<Broadcast>	0.5	0.0	0	0	0	47	0	0	0	0	
ff:ff:ff:ff:ff:ff	1	IA 2 5	0.0	0.0	0	0	0	4	0	0	0	0	
ff:ff:ff:ff:ff:ff	1	Vodafone-48683C	0.0	0.0	0	0	0	3	0	0	0	0	
ff:ff:ff:ff:ff:ff		FlyingNet	0.0	0.0	0	0	0	1	0	0	0	0	
ff:ff:ff:ff:ff:ff	1	GV BRAGA	0.0	0.0	0	0	0	2	0	0	0	0	

Nota: um dos SSIDs foi censurado, pois este é um relatório *family friendly*.

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

wlan.fc.type_subtype == 4	probe requests
wlan.fc.type_subtype == 5	probe responses

(Wireshark display filters)



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

```
793 7.838631    AltoBeam_08:32:99    Broadcast            802.11    110 Probe Request,
796 7.859430    HitronTe_ee:2e:c6    AltoBeam_08:32:99    802.11    485 Probe Response,
```

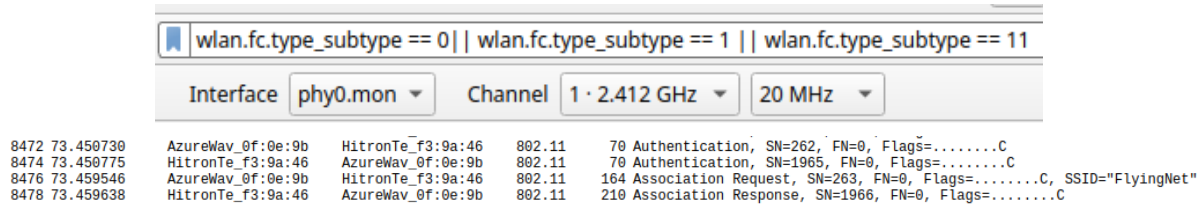
```
▾ IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  ▾ Frame Control Field: 0x4000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0100 .... = Subtype: 4
    ▸ Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
    Source address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
```

```
▾ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  ▾ Frame Control Field: 0x5000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0101 .... = Subtype: 5
    ▸ Flags: 0x00
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
    Destination address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
    Transmitter address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
    Source address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
```

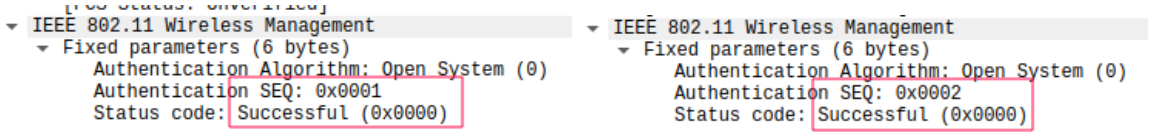
O dispositivo `AltoBeam_08:32:99` envia um *probe request* para *broadcast* para procurar pontos de acesso, APs, disponíveis, com endereço de origem `a4:ef:15:08:32:99`, MAC do dispositivo original que enviou, e com *transmitter address* também `a4:ef:15:08:32:99`, MAC do dispositivo que está a transmitir. Estas probing requests/responses são parte de um processo de "sondagem", onde os dispositivos procuram redes disponíveis antes da decisão de a qual rede efetuar conexão. Assim, o AP `HidronTe_ee:2e:c6`, com MAC address `90:aa:c3:ee:2e:c6`, envia um probe response com endereço de destino `AltoBeam_08:32:99`, MAC do destino final do *frame*, e como *receiver address* também `AltoBeam_08:32:99`, MAC do próximo destinatário imediato do *frame*.

3 Processo de Associação

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

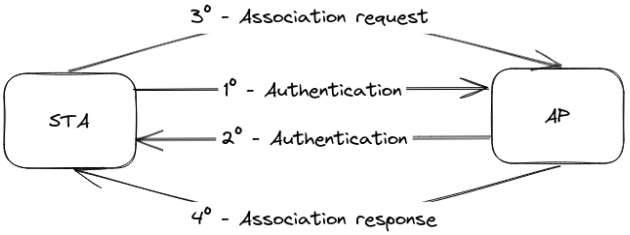


A STA envia uma trama de autenticação para o AP (fornecimento de credenciais em caso de *shared key authentication*, mas neste caso não é necessário, pois é *open system*), e de seguida o AP envia uma trama de autenticação para esse STA, aceitando ou rejeitando a autenticação — neste caso, foi aceite.



Após a autenticação bem-sucedida, a fase de associação ocorre, o que permite que o STA fique oficialmente associado ao AP e obtenha acesso aos serviços e recursos da rede (ligação lógica entre ambos). Assim, a associação permite que o AP guarde informação sobre cada dispositivo (enviadas na *association request*) para que os pacotes sejam entregues corretamente. (A *association response* inclui um *association ID*, que a STA irá utilizar).

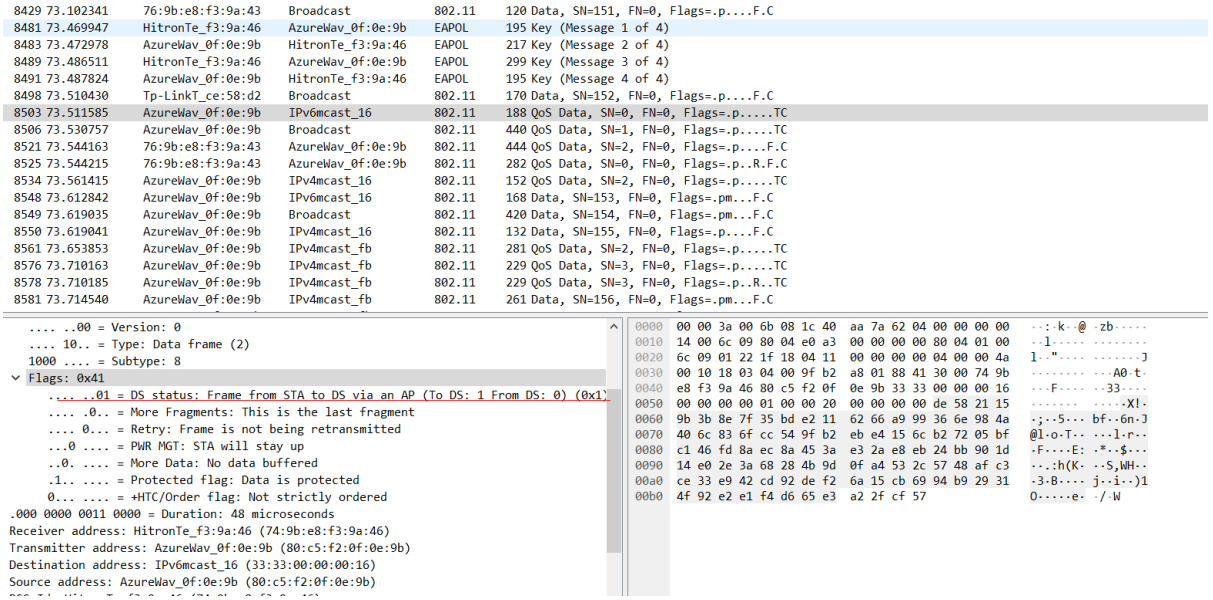
14) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.



4 Transferência de Dados

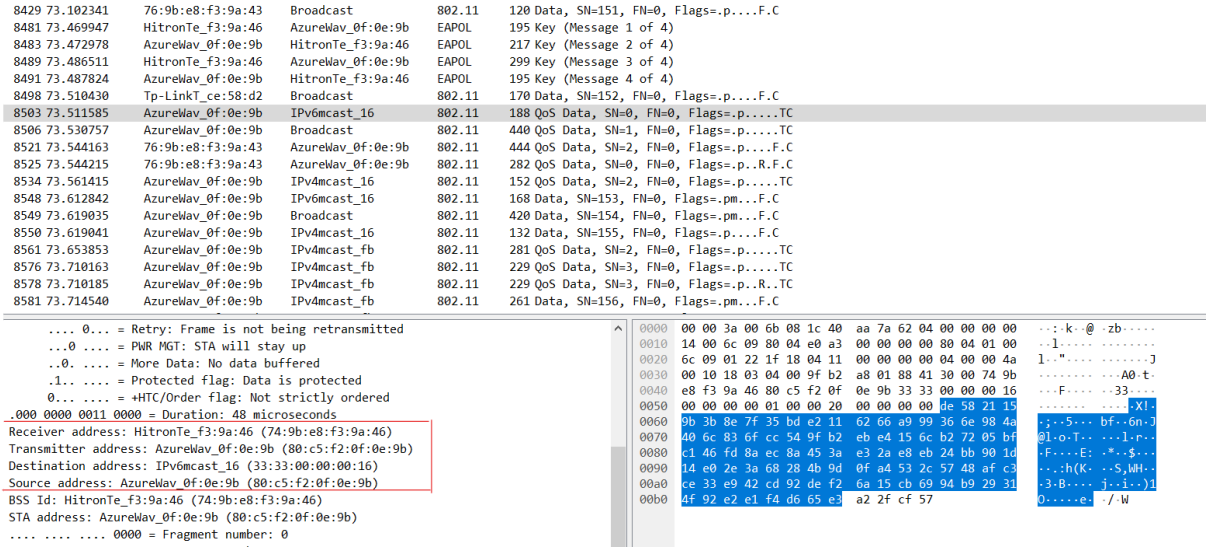
O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados.

15) *Considere a trama de dados nº 8503. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direcionalidade das tramas, o que pode concluir face à direcionalidade dessa trama, será local à WLAN?*



O ToDS apresenta o valor 1 e o fromDS 0, logo podemos concluir que a trama está direcionada de STA para o DS (passando pelo AP). Entende-se então que se trata de uma trama de saída que está a ser encaminhada para fora da WLAN.

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



Receiver: 74:9b:e8:f3:9a:46 - AP
Transmitter : 80:c5:f2:0f:0e:9b - STA
Destination: 33:33:00:00:00:16 - Router
Source: 80:c5:f2:0f:0e:9b - STA

17) *Como interpreta a trama nº8521 face à sua direcionalidade e endereçamento MAC?*

É um pacote de um sistema de distribuição para um STA. Pelos endereços MAC, podemos concluir que a fonte (Source) é o DS, o receiver e destination é o STA e o transmitter é o AP.

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

São transmitidas tramas RTS(Request to send),CTS(Clear to send) e ACK. Estas tramas são necessárias para evitar conflitos na transmissão de dados. O transmissor pede para transmitir dados, e se dado permissão (CTS), envia dados. Sem este controlo poderiam existir vários dispositivos a transmitir e sobrecarregar o AP e causar interferência nos dados uns dos outros.

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

A opção RTS/CTS está a ser utilizada visto que existem tramas com esse subtipo antes da transmissão de dados. O pacote RTS é enviado do AP para o STA, e o pacote CTS é enviado para o AP. Na imagem abaixo apresentamos um exemplo de uma transmissão de dados que não utiliza RTS/CTS.

```
8542 73.587831    PTInovac_d6:88:50 (… ce:90:6f:21:42:3a (… 802.11     68 802.11 Block Ack, Flags=........C
8543 73.590971    PTInovac_d6:88:50 (… ce:90:6f:21:42:3a (… 802.11     76 Request-to-send, Flags=........C
8544 73.591043    PTInovac_d6:88:50 (… ce:90:6f:21:42:3a (… 802.11     76 Request-to-send, Flags=........C
8545 73.594214    PTInovac_d6:88:50 (… ce:90:6f:21:42:3a (… 802.11     76 Request-to-send, Flags=........C
8546 73.603494    PTInovac_d6:88:50 (… ce:90:6f:21:42:3a (… 802.11     76 Request-to-send, Flags=........C
8547 73.612833    HitronTe_f3:9a:46    Broadcast            802.11    386 Beacon frame, SN=1703, FN=0, Flags=........C, BI=100, SSID="FlyingNet"
8548 73.612842    AzureWav_0f:0e:9b    IPv6mcast_16         802.11    168 Data, SN=153, FN=0, Flags=.pm...F.C
8549 73.619035    AzureWav_0f:0e:9b    Broadcast            802.11    420 Data, SN=154, FN=0, Flags=.pm...F.C
8550 73.619041    AzureWav_0f:0e:9b    IPv4mcast_16         802.11    132 Data, SN=155, FN=0, Flags=.p....F.C
8551 73.619045    PTInovac_d6:88:50 (… ce:90:6f:21:42:3a (… 802.11     76 Request-to-send, Flags=........C
8552 73.619048    PTInovac_d6:88:50 (… ce:90:6f:21:42:3a (… 802.11     76 Request-to-send, Flags=........C
```

5 Conclusões

Em conclusão, este trabalho proporcionou uma visão detalhada sobre o funcionamento de redes Wi-Fi, abrangendo aspectos como normas IEEE, débito das tramas, análise de tramas *beacon*, e o processo de autenticação e associação entre APs e STAs. Consideramos que estas informações são essenciais para entender o funcionamento e a comunicação em redes sem fio.