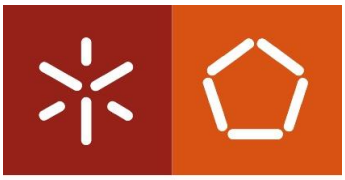


Universidade do Minho

Departamento de Informática

TP4: Redes Sem Fios (802.11)
Redes de Computadores
Grupo 45

Catarina Machado (a81047) João Vilaça (a82339)
Ricardo Milhazes Veloso (a81919)

15 de Dezembro de 2018

Conteúdo

1 Questões e Respostas

4. Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (radio information), para além dos bytes correspondentes a tramas 802.11.

Para a trama correspondente 3XX em que XX corresponde ao seu número de TurnoGrupo (e.g., 11),

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

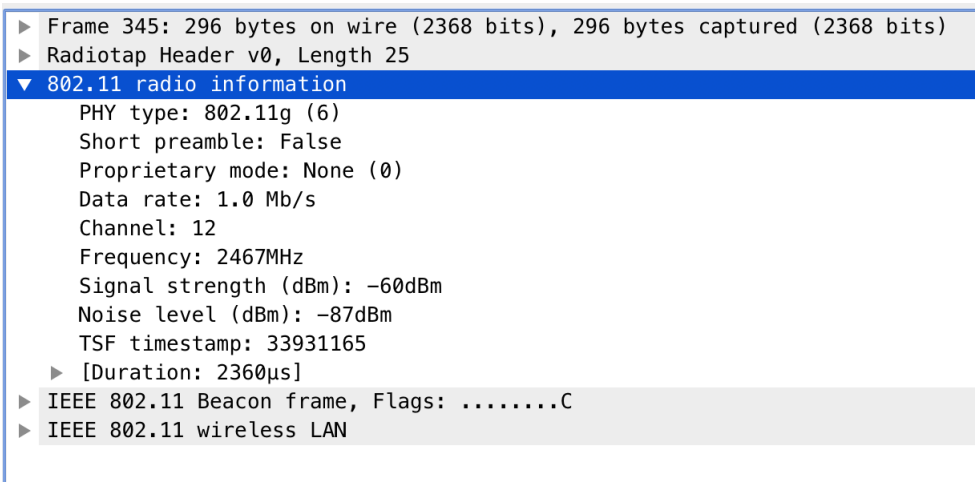


Figura 1

Frequencity: 2467MHz.
Channel: 12.

2) Identifique a versão da norma IEEE 802.11 que está a ser usada.
Tal como se pode ver na Figura 1, está a ser usada a versão 802.11g (PHY type: 802.11g).

3) Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface WiFi pode operar? Justifique
Tal como se pode ver na Figura 1:
Date rate: 1.0Mb/s
Não, o débito máximo na versão da norma IEEE 802.11g corresponde a 54Mbps. Não é utilizado este débito porque, para garantir que o beacon chega a todos os hosts, utiliza o débito mais baixo possível.

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 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)?

```
▶ Frame 345: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    ▶ 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: 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 0011 0111 .... = Sequence number: 2359
    Frame check sequence: 0x1411bc47 [correct]
    [FCS Status: Good]
▶ IEEE 802.11 wireless LAN
```

Figura 2

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	1000	Beacon

Figura 3

Pertence ao tipo Management.
Tipo: 00.
Subtipo: 1000.
Estão especificados no Frame Control Field.

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.

Construímos um filtro de visualização, onde criamos uma nova coluna com os SSIDs e filtramos com

$$wlan.addr == ff:ff:ff:ff:ff:ff$$

, em seguida abrimos a tab para análise estatística dos pedidos, Figura 3, onde estão listados os SSIDs dos APs que estão a operar na vizinhança da STA de captura.

BSSID	Channel	SSID	Percent Packe ▼	Percent Retry	Retry	Beacons	Data Pkts	Probe Reqs	Probe Resp	Auths	Deauths	Other	Protection
▶ bc:14:01:af:b1:98	12	FlyingNet	50.1	0.0	0	1256	0	0	0	0	0	0	
▶ bc:14:01:af:b1:99	12	NOS_WIFI_Fon	49.7	0.0	0	1245	0	0	0	0	0	0	
▶ 4e:0e:f5:50:50:f3		<Broadcast>	0.0	100.0	1	1	0	0	0	0	0	0	WEP
▶ 9a:87:4e:7b:5e:46		<Broadcast>	0.0	100.0	1	1	0	0	0	0	0	0	Unknown
▶ 55:0e:b7:95:b0:54		<Broadcast>	0.0	100.0	1	1	0	0	0	0	0	0	Unknown
▶ f5:4c:13:e7:32:62		<Broadcast>	0.0	0.0	0	1	0	0	0	0	0	0	WEP

Figura 4

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 o método de deteção de erros (CRC) e as tramas beacon não foram todas recebidas corretamente. A trama da Figura 5 foi recebida corretamente mas, por exemplo, a trama número 30 e 31 não foram recebidas corretamente (Figura 6 e Figura 7).

É necessário utilizar detecção de erros porque o tipo de rede local representa uma Rede Wi-Fi. As redes Wi-Fi são mais suscetíveis a erros o que implica que seja utilizado um campo que verifique se as tramas Beacon são recebidas corretamente.

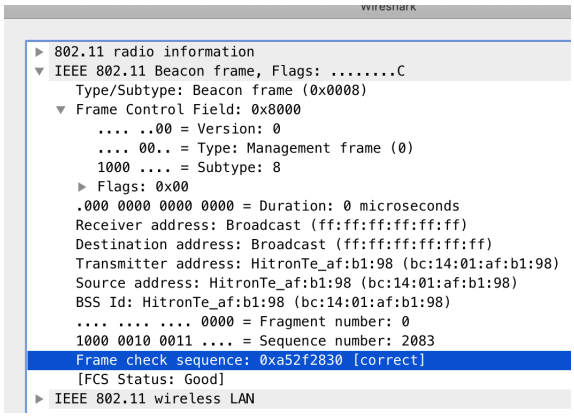


Figura 5

Figura 6

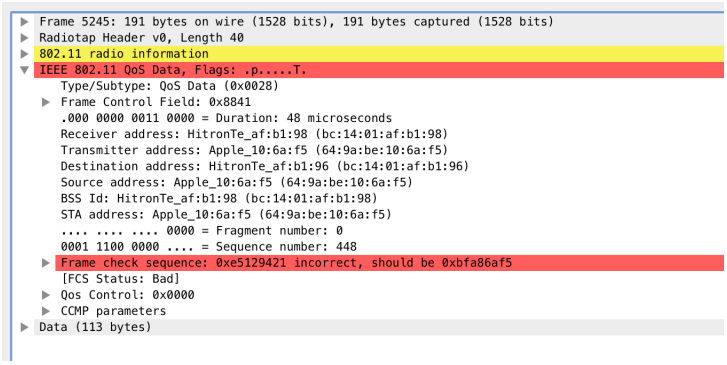


Figura 7

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 previsto entre tramas beacon consecutivas é igual a 0.1024 seg.

"Flying Net":

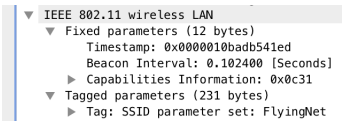


Figura 8

"NOS_WIFI_Fon":

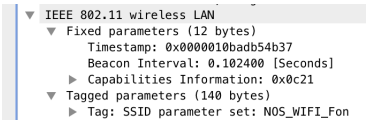


Figura 9

Como se pode verificar nas imagens seguintes (Figura 10 e Figura 11) o valor anunciado para o intervalo de tempo previsto entre tramas beacon consecutivas não se verifica. Isto pode acontecer por diversas razões nas quais se identificam, principalmente:

- A falta de precisão de um AP que pode atrasar ou acelerar este processo;
- O congestionamento da rede local utilizada;
- A distância entre os dispositivos que possuem os endereços de destino e de envio.

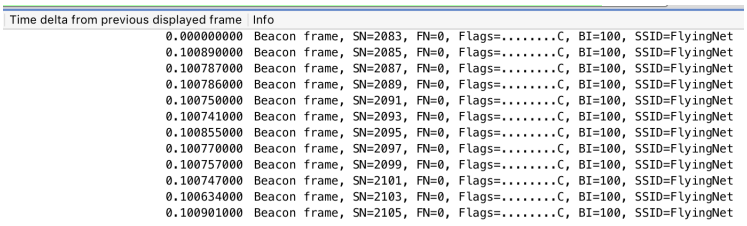


Figura 10

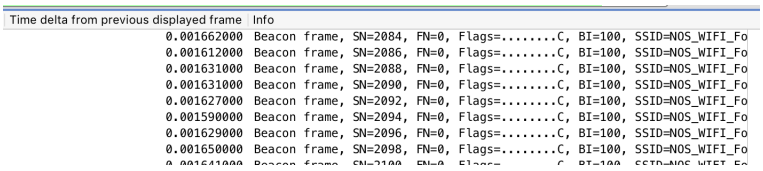


Figura 11

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.

Utilizamos um filtro:

$$wlan.sa == bc:14:01:af:b1:98 \&\& wlan.fc.subtype == 0x0008$$

(Figura 12) e depois vimos as *Conversations*. Os endereços MAC usados nas tramas beacon enviadas pelo AP encontram-se na Figura 13.

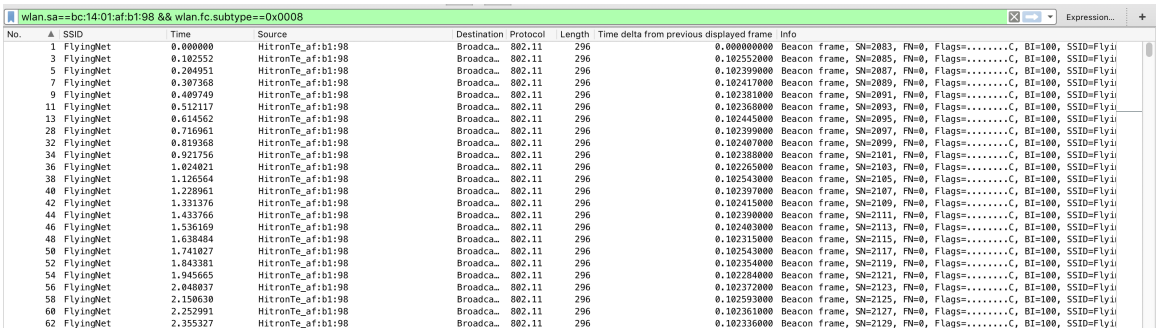


Figura 12

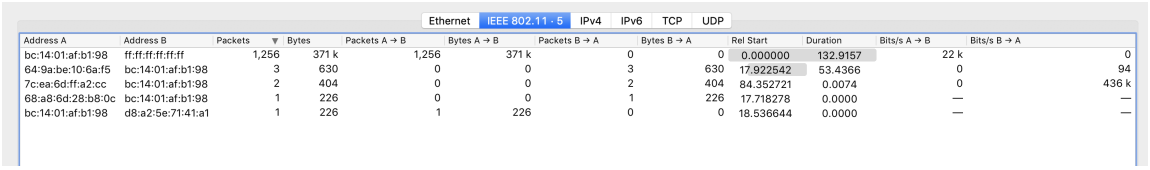


Figura 13

Aplicamos outro filtro para o segundo AP,

$$wlan.sa == bc:14:01:af:b1:99 \&\& wlan.fc.subtype == 0x0008$$

, Figura 14, e obtivemos os endereços MAC presentes na Figura 15.

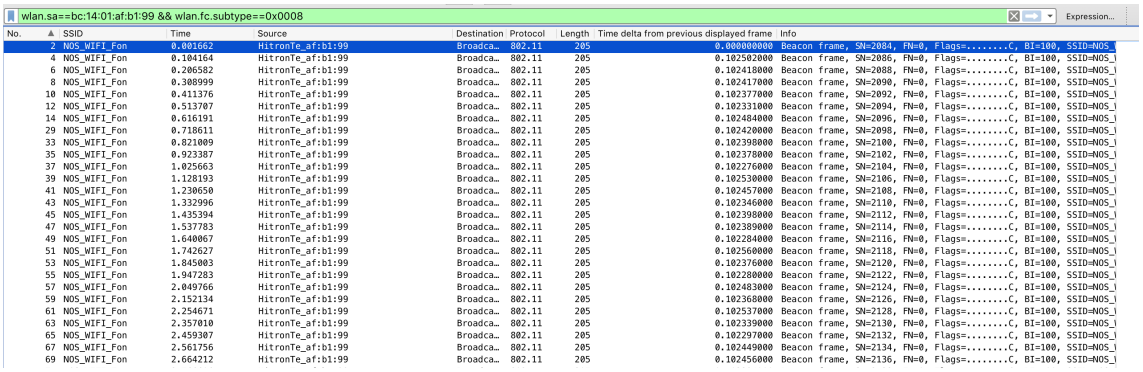


Figura 14

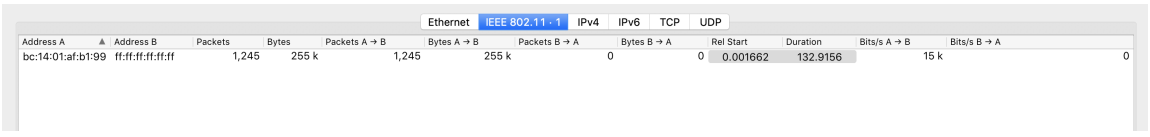


Figura 15

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?

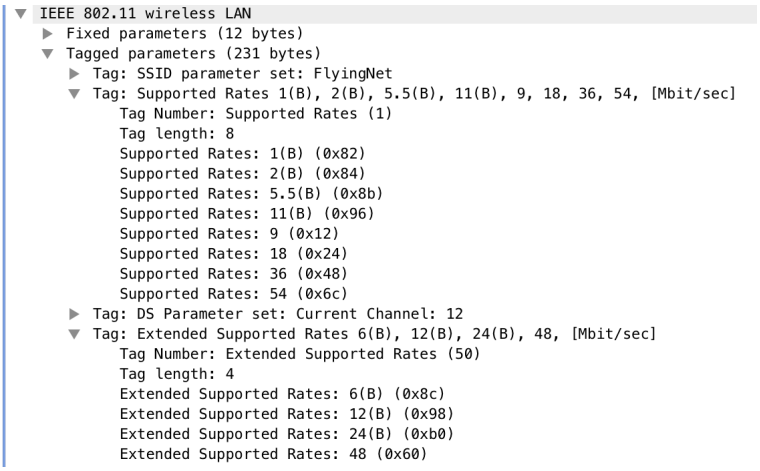


Figura 16

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 utilizado foi o seguinte:

$$wlan.fc.type == 0 \&\& (wlan.fc.subtype == 4 \parallel wlan.fc.subtype == 5)$$

.

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?

Uma vez que o endereço MAC de destino da trama é igual ao endereço MAC de origem da outra trama, significa que se trata de um probing request e probing response.

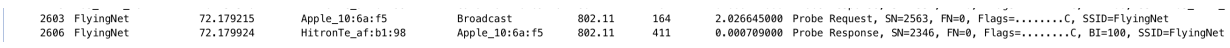


Figura 17

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.

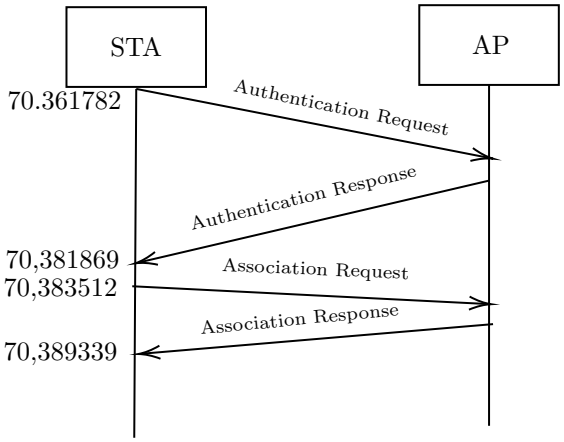
Uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação, pode ser visualizada através da Figura 18, onde também se encontra o filtro utilizado para o efeito.

wlan.fc.type==0 && (wlan.fc.type_subtype==0 || wlan.fc.type_subtype==1 || wlan.fc.type_subtype==11)

No.	SSID	Time	Source	Destination	Protocol	Length	Time delta from previ	Info
2486		70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70	0.000000000	Authentication, SN=2542, FN=0, Flags=.......C
2488		70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	0.020087000	Authentication, SN=2338, FN=0, Flags=.......C
2490	FlyingNet	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175	0.001643000	Association Request, SN=2543, FN=0, Flags=.......C, SSID=FlyingNet
2492		70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	0.005827000	Association Response, SN=2339, FN=0, Flags=.......C

Figura 18

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



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?

Tal como se pode ver através da Figura 19, os campos que especificam a direccionalidade da trama têm os seguintes valores:

TO DS: 0.

FROM DS: 1.

Assim, podemos concluir que o pacote está a entrar num ambiente wireless vindo do DS (centro de distribuição) (”Frame from DS to STA via AP”).

```
▼ IEEE 802.11 QoS Data, Flags: .p....F.C
    Type/Subtype: QoS Data (0x0028)
  ▼ Frame Control Field: 0x8842
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▼ Flags: 0x42
        .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .1.. .... = Protected flag: Data is protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0010 0100 = Duration: 36 microseconds
```

Figura 19

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?

Devido à direcionalidade da trama verificada na questão anterior e em relação ao datagrama da trama, a correspondência dos endereços MAC será a seguinte:

Address 1 = Destination;

Address 2 = BSSID;

Address 3 = Source.

Na Figura 19 pode verificar-se o valor desses endereços MAC:

```
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)
```

Figura 20

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

Na trama nº457, tal como se pode ver através da Figura 20, os campos que dizem respeito à direcionalidade da trama têm os seguintes valores:

TO DS: 1.

FROM DS: 0.

Assim, podemos concluir que o pacote está a sair do ambiente wireless, dirigindo-se para um computador na rede do centro de distribuição.

Consequentemente, em relação aos endereços MAC na frame, a correspondência será a seguinte:

Address 1 = BSSID;

Address 2 = Origem;

Address 3 = Destino.

```
▼ IEEE 802.11 QoS Data, Flags: .p.....TC
    Type/Subtype: QoS Data (0x0028)
  ▼ Frame Control Field: 0x8841
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▼ Flags: 0x41
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .1.. .... = Protected flag: Data is protected
        0... .... = Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
```

Figura 21

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 de tramas de controlo transmitidas são *acknowledgment*, como se pode ver através da figura seguinte.

```
455   18.536644   HitronTe_af:b1:98   Apple_71:41:a1     802.11   226   0.000184000  QoS Data, SN=276, FN=0, Flags=.p....F.C
456   18.536653                       HitronTe_af:b1:98… 802.11    39   0.000009000  Acknowledgement, Flags=........C
457   18.539762   Apple_71:41:a1      HitronTe_af:b1:98  802.11   178   0.003109000  QoS Data, SN=1209, FN=0, Flags=.p.....TC
458   18.540043                       Apple_71:41:a1 (d… 802.11    39   0.000281000  Acknowledgement, Flags=........C
```

Figura 22

Como a rede wi-fi é 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.

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 22, verificamos que não existem este tipo de tramas mas, por exemplo, na Figura 23, podemos observar a sua utilização.

816	30.824814	HitronTe_af:b1:98 (bc:…	Apple_10:6a:f5 (6…	802.11	45	0.000114000	Request-to-send, Flags=........C
817	30.824869		HitronTe_af:b1:98…	802.11	39	0.000055000	Clear-to-send, Flags=........C
818	30.824928	HitronTe_af:b1:96	Apple_10:6a:f5	802.11	146	0.000059000	QoS Data, SN=843, FN=0, Flags=.p....F.C
819	30.824938	Apple_10:6a:f5 (64:9a:…	HitronTe_af:b1:98…	802.11	57	0.000010000	802.11 Block Ack, Flags=........C
820	30.841236	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	0.016298000	Null function (No data), SN=2509, FN=0, Flags=...P...TC
821	30.841257		Apple_10:6a:f5 (6…	802.11	39	0.000021000	Acknowledgement, Flags=........C

Figura 23

2 Conclusão

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

Depois de finalizado o trabalho prático número 4, relativo às Redes Wireless, obtivemos mais conhecimentos sobre o funcionamento ao nível da rede das redes wi-fi.

Conceitos como, por exemplo, tipos e subtipos de tramas, STA, AP e direcionalidade de tramas foram recordados e aplicados.

O aspeto em que investimos mais tempo neste trabalho prático foi o de compreender como se filtram dados no WireShark. Para tal, foram necessárias várias pesquisas webgraficas, que nos ajudaram a encontrar os filtros que mais nos convinham para a resolução dos exercícios. Esse investimento de tempo nos filtros acabou por ser uma mais valia para nós visto que foi necessário utilizar bastantes filtros ao longo das questões.