TP4
Redes Sem Fios (802.11

Rafael Silva, José Ramos, and Luís Ferreira

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a74264,a73855,a76936}@alunos.uminho.pt

1 Desenvolvimento

1.1 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),

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

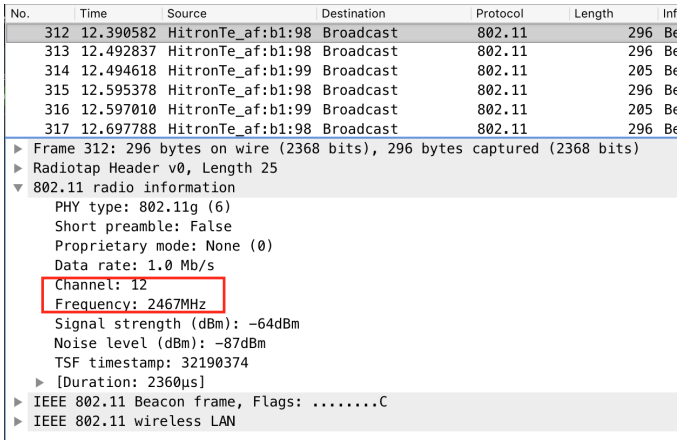

Figura 1.

Resposta: Frequência: 2467MHz e Canal : 12

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

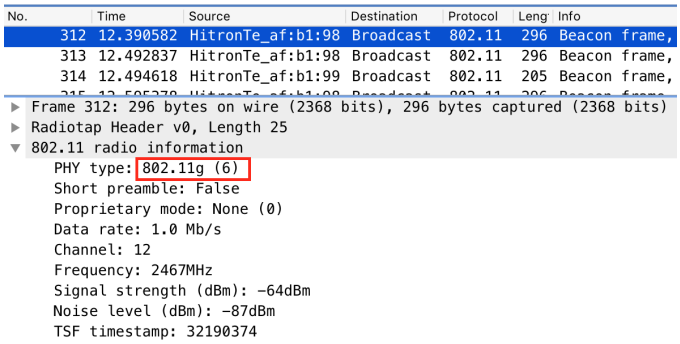

Figura 2.

Resposta: Versão Utilizada : 802.11g

Questão 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.

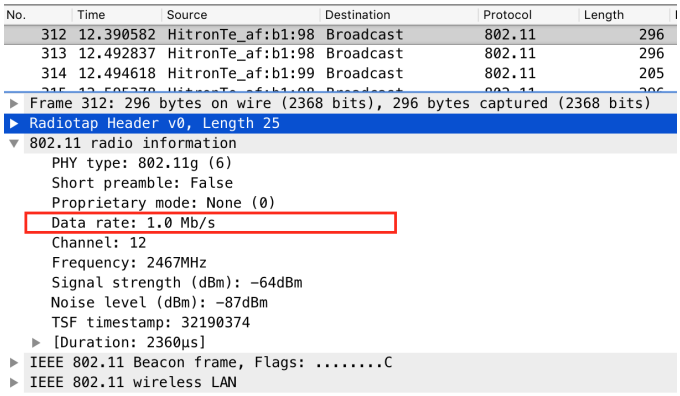

Figura 3.

Resposta: O débito a que foi enviada a trama é de 1Mb/s.
Como estamos a falar de standart 802.11g sabemos que esres podem operar até 54 Mb/s portanto não corresponde ao máximo.

1.2 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:

Questão 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)?

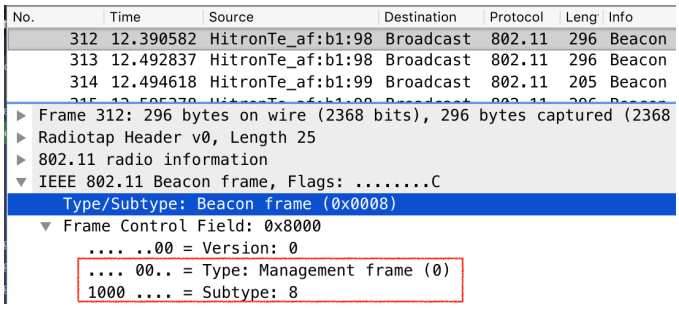

Figura 4.

Resposta: A trama pertence ao tipo (de tramas 802.11) Management, com valor de identificador de tipo 0 e subtipo 8. Todos estes dados estão especificados na Frame Control.

Questão 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.

Filtro: `(wlan.fc.type == 0 and wlan.fc.subtype == 8)`

Resposta: As SSIDs dos APs que estão a operar na rede são:

- SSID= FlyingNet;
- SSID= NOS_WIFI_Fon;

A que é capazs de proporcionar a melhor qualidade de sinal é SSID=... (ver primeira imagem).

Questão 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.

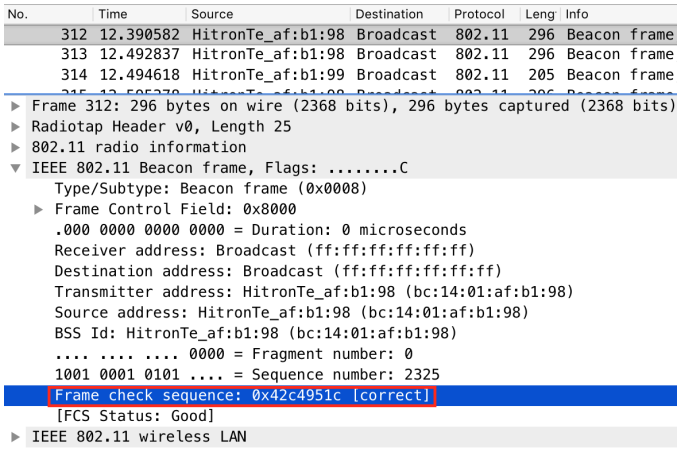

Figura 5.

Resposta: O valor de Frame check sequence (FCS) varia entre tramas sendo na maior parte delas "correct"e uma outra parte incorreto, como podemos ver na figura em baixo sendo que chegamos á conclusão que o CRC está ativo.

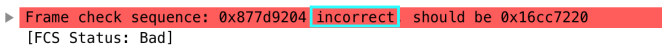

Figura 6.

Deste modo estamos a tratar de Collision Avoidance. Este é um processo usado em contraste ao Collision Detection (que sabemos ser utilizado em diferentes tipos de rede). Este ultimo não se utiliza em redes wireless pois estas não assumem que transmissão de dados entes as diferentes estações da rede de forma autónoma. No caso de utilizarmos o metodo de Collision Avoidance a estação que recebe dados verifica se o CRC é valido, e após confirmação envia uma mensagem de ACK à estação que enviou os dados.

Questão 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.

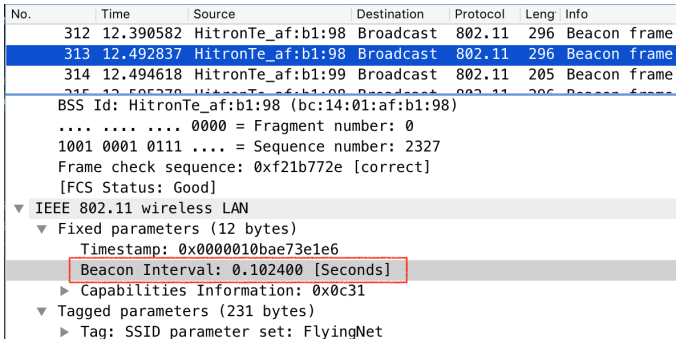

Figura 7. FlyingNet

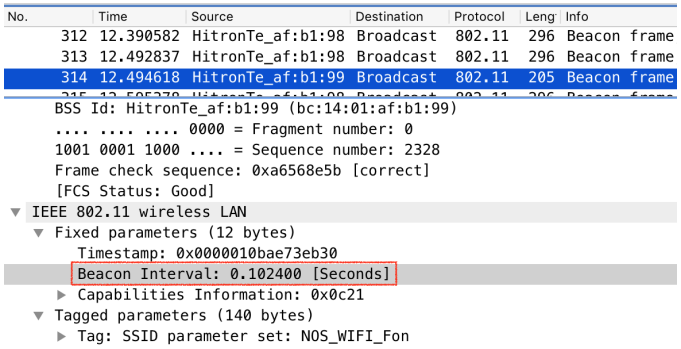

Figura 8. NOS_WIFI_Fon

Resposta: A periocidade de tramas beacon, em pratica nao se verifica, pois, a titulo de exemplo podemos ver que o intervalo de tempo entre a trama 312 e 314 = 0.104036 que é diferente do previsto 0.120400. O que acontece devido a atrasos relacionados com as caracteristicas do meio(i.e. barreiras físixas).

Questão 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.

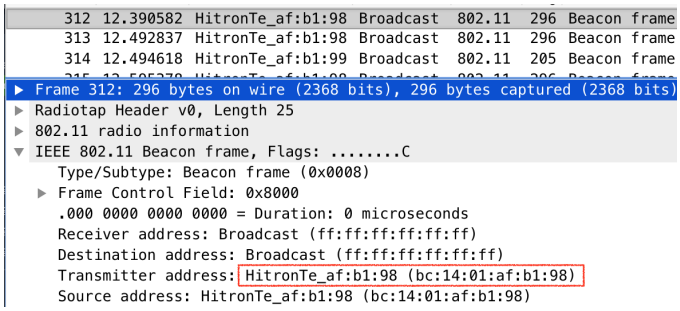

Figura 9. FlyingNet

-> FlyingNet : (bc:14:01:af:b1:98)

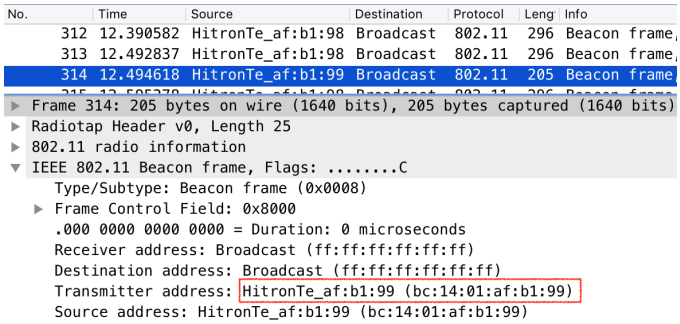

Figura 10. NOS_WIFI_Fon

-> NOS_WIFI_Fon : (bc:14:01:af:b1:99)

Questão 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?

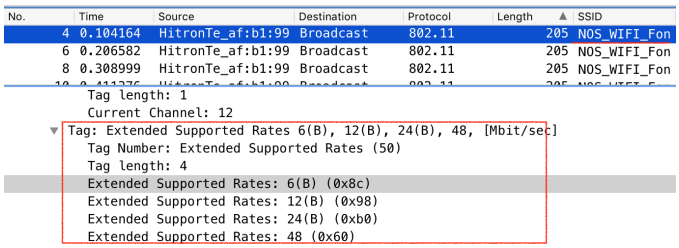

Figura 11. NOS_WIFI_Fon

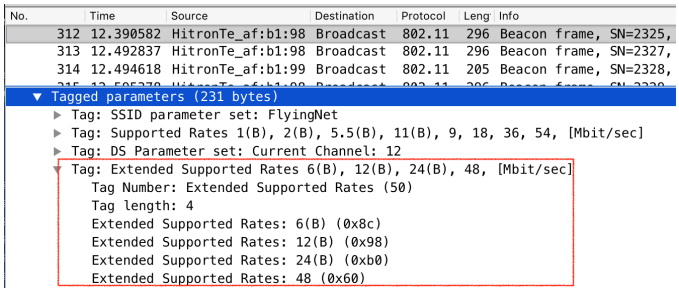

Figura 12. FlyingNet

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

Resposta: Filtro: `wlan.fc.type_subtype eq 0x04 || wlan.fc.type subtype eq 0x05.`

Uma vez que as tramas de prohibing request e prohibing response apresentam-se com 0x04 e 0x05 respetivamente.

Questão 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?

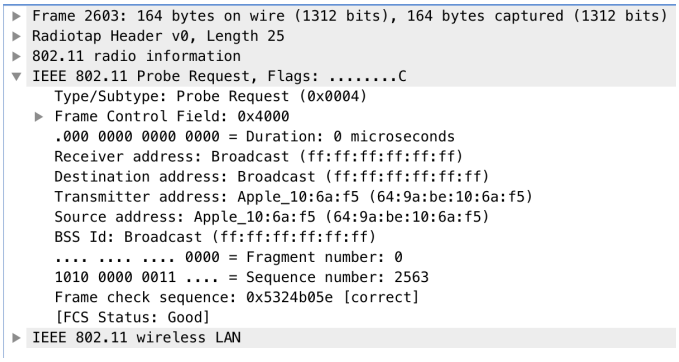

Figura 13. Trama de probing request

Resposta: O sistema que envia a trama Probe Request é o Apple-10:6a:f5, e sistema para onde a envia-a SSID: Broadcast, como resposta ao pedido de Probe Request o Broadcast envia um pedido de probe e realiza um active scan, e modo a descobrir a maquina para a qual pretende enviar informação, posteriormente esta devolve as informações relativas da STA e AP.

1.3 Processo de Associação

Questão 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.

wlan.fc.type_subtype eq 11 || wlan.fc.type_subtype eq 1 || wlan.fc.subtype eq 0

No.	Time	Source	Destination	Protocol	Length	Info
4161	80.898145	Apple_10:6a:f5	IPv6mcast_fb	802.11	199	Data, SN=2429, FN=0, Flags=.pm...F.C
4162	80.898303	Apple_10:6a:f5	IPv4mcast_fb	802.11	322	Data, SN=2430, FN=0, Flags=.pm...F.C
4163	80.898432	Apple_10:6a:f5	IPv6mcast_fb	802.11	342	Data, SN=2431, FN=0, Flags=.p....F.C
4265	81.512434	Apple_10:6a:f5	IPv6mcast_16	802.11	157	Data, SN=2433, FN=0, Flags=.p....F.C
4294	81.819682	Apple_10:6a:f5	IPv4mcast_fb	802.11	179	Data, SN=2434, FN=0, Flags=.pm...F.C
4295	81.819773	Apple_10:6a:f5	IPv6mcast_fb	802.11	199	Data, SN=2435, FN=0, Flags=.pm...F.C
4296	81.819909	Apple_10:6a:f5	IPv4mcast_fb	802.11	322	Data, SN=2436, FN=0, Flags=.pm...F.C
4297	81.820038	Apple_10:6a:f5	IPv6mcast_fb	802.11	342	Data, SN=2437, FN=0, Flags=.p....F.C
4692	83.663250	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	59	Authentication, SN=67, FN=0, 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
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
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
4894	84.584589	Apple_10:6a:f5	IPv6mcast_16	802.11	157	Data, SN=2445, FN=0, Flags=.p....F.C
5286	87.656408	Apple_10:6a:f5	IPv4mcast_fb	802.11	179	Data, SN=2450, FN=0, Flags=.pm...F.C

Figura 14. Processo de associação e autenticação entre a STA e o AP (linha 4692 até 4699)

Resposta: Filtro: `wlan.fc.type_subtype eq 11` || `wlan.fc.type_subtype eq 1` || `wlan.fc.type_subtype eq 0`. Os valores de 0, 1 e 11 correspondem às tramas association request, association response e authentication, respetivamente.

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

Resposta:

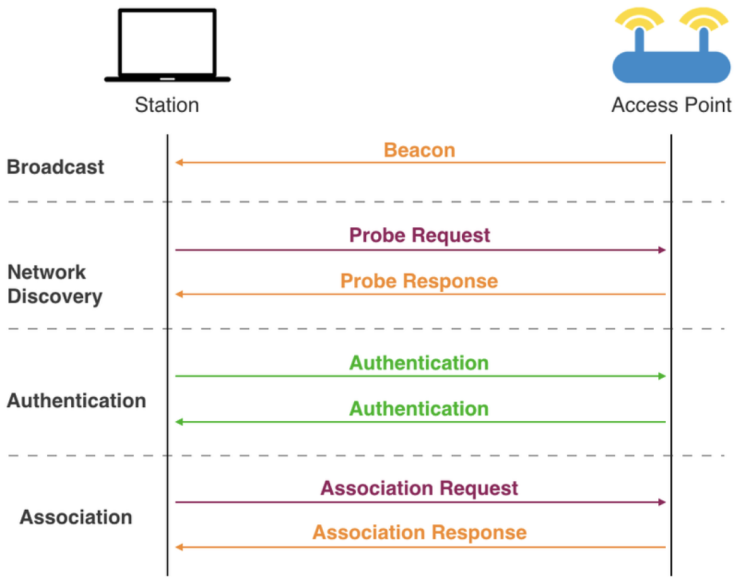

Figura 15. Troca de tramas entre um STA e um AP.

1.4 Transferência de Dados

Questão 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?

Resposta: A informação do **ToAp** e do **FromAp** está contida nos dois ultimos bits da flag **Frame Control**, portanto como os dois ultimos bites sao **1** e **0** isto quer dizer que a direção da trama é de um **STA** para um **AP**, pois o campo ToAp = 1 e o FromAp = 0. Logo não é igual a WLAN porque este requeria que o valor do DS fosse igual a 0, algo que pode-mos ver que não acontece em baixo.

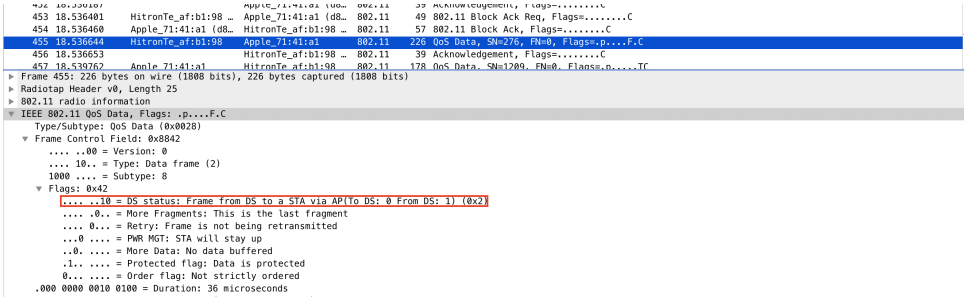

Figura 16. Analise do frame nº455

Questão 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?

Resposta: Analisando a trama de dados nº455, o endereço MAC correspondente ao host sem fios (STA) é **bc:14:01:af:b1:98**, o endereço MAC que corresponde ao AP (BSS Id) é **d8:a2:5e:71:41:a1** e o endereço MAC que diz respeito ao router de acesso ao sistema de distribuição é **bc:14:01:af:b1:98**.

```
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 17. Trama beacon com o método de correção de erros (CRC)

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

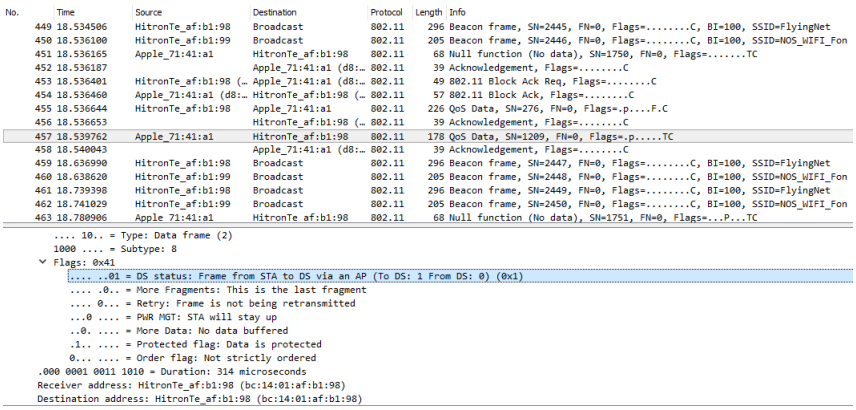

Figura 18. Trama beacon com o método de correcção de erros (CRC)

Resposta: Visto que a informação do **ToAp** e do **FromAP** está contida nos dois últimos bits da flag **Frame Control**, neste caso 0 e 1, podemos concluir que a direção da trama é de um **AP para um STA** (campo ToAp=0 e FromAp=1).
Verificamos ainda que o STA address corresponde ao endereço MAC de destino, que por sua vez este último corresponde ao router de acesso ao sistema de distribuição

Questão 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.)

Resposta: O subtipo de tramas é o ACK(acknowledgement). Serve de suporte para Collision Avoidance, algo que é necessário para redes sem fios.

Questão 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 nu´mero 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.

Resposta: O uso de tramas **Request To Send e Clear To Send** é com o principal objetivo de diminuir as colisões na rede. Quando um STA ou um AP pretende enviar dados para um Ap ou um STA respetivamente , em primeiro lugar este efetua um request e espera pelo Clear-To-Send enviado pelo destinatario. Depois de efetuar o envio, recebe um ACK (Acknowledgement) e se quiser continuar a enviar dados tem de esperar um certo tempo obtido de forma aleatória. Assim qualquer transmissor vai ter de aguardar pelo seu CTS ou pelo tempo de espera. Neste caso, é possivel ver que a direção do Request To Send é do STA para o AP e o Clear To Send tem direção do AP para o STA. Em ambos os casos, as tramas sao locais à WLAN pois o campo DS Status tem o valor 00.

```
4701 83.680434     HitronTe_af:b1:98 …  Apple_10:6a:f5 (64…  802.11     45 Request-to-send, Flags=........C
4702 83.680480                          HitronTe_af:b1:98 …  802.11     39 Clear-to-send, Flags=........C
```

Figura 19. Tramas em estudo

```
4700 83.680364                          HitronTe_af:b1:98 …  802.11     39 Acknowledgement, Flags=........C
4701 83.680434     HitronTe_af:b1:98 …  Apple_10:6a:f5 (64…  802.11     45 Request-to-send, Flags=........C
4702 83.680480                          HitronTe_af:b1:98 …  802.11     39 Clear-to-send, Flags=........C
▶ Frame 4701: 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Request-to-send, Flags: ........C
    Type/Subtype: Request-to-send (0x001b)
  ▼ Frame Control Field: 0xb400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1011 .... = Subtype: 11
    ▼ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .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
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 1010 0000 = Duration: 160 microseconds
    Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Frame check sequence: 0x11fc8d55 [correct]
    [FCS Status: Good]
```

Figura 20. Trama do tipo Request-to-Send

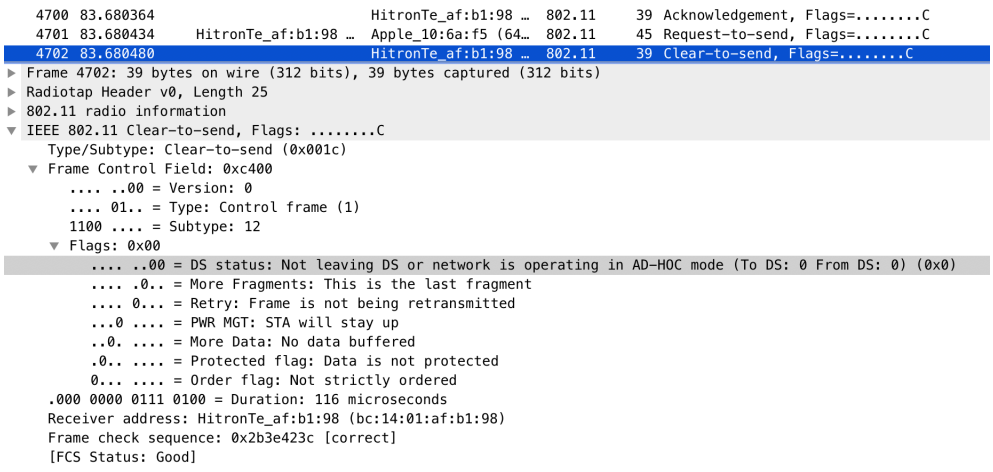

Figura 21. Trama do tipo Clear-to-Send

2 Conclusão

O trabalho prático proposto na UC para a abordagem do tema de protocolos IEEE 802.11 com recurso à ferramenta Wireshark apresentou vários assuntos pertinentes na gestão da troca e procura de informação nas Redes sem fios. Ao resolver os exercicios, analisamos a captura fornecida pelo professor(na ferramenta Wireshark), em que tivemos a oportinidade de observar e aprender sobre acesso rádio, tramas Beacon, tranferencias de dados e associaçõoes. Sobre os aspetos de acesso rádio, aprendemos os limites do espectro em que podem operar as wireless e os vários tipo de canais. Relativamente a tramas Beacon, conseguimos distinguir os varios tipos e subtipo e a sua utilização no ambito das redes sem fios. Tambémm aprendemos que o meio de propagação da inforação não é perfeito , devido ainumeras interferencias que podem ocorrer, não permitindo a periodicidade teorica destas tramas Beacon. Na Transferˆencia de Dados, avaliamos a direcionalidade e aprendemos que as tramas do tipo 802.11 do subtipo Acknowledgement são essenciais de modo a geririmos as interferências e colisões na rede. Por ultimo, aprendemos também a analisar, identificar, e procurar através de filtros no Wireshark as tramas necessarias a cada questão, evitando uma interface cheia de informação desnecessária , como por exemplo ,de forma a ver o processo de “troca” de tramas entre AP’s e STA’s.