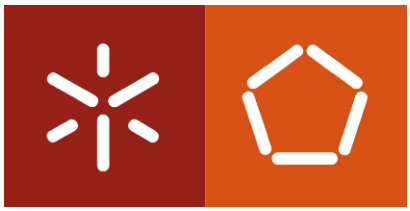

UNIVERSIDADE DO MINHO

MESTRADO INTEGRADO DE ENGENHARIA INFORMÁTICA

Redes de Computadores

TP4 - Redes Sem Fios (802.11)

Autores:

Frederico Pinto	A73639	
Pedro Silva	A78434	
Ricardo Leal	A75411	

1 de Abril de 2018

1 Introdução

Este relatório diz respeito ao quarto trabalho prático da Unidade Curricular Redes de Computadores, que se baseia nas experiências propostas no enunciado. Neste trabalho prático é abordado as redes sem fio e o respetivo protocolo IEEE 802.11. Através da análise de uma captura de uma rede WiFi foi nos possivel aprofundar conhecimentos em determinados conceitos como o acesso rádio, scanning passivo e ativo e processos de associação e transferência de dados.

2 Questões e Respostas

2.1 Acesso Rádio

1) Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.
A rede está a operar a uma frequência de 2462MHz, associada ao canal 11, como podemos ver na Figura 1.
2) Identifique a versão da norma IEEE 802.11 que está a ser usada.
Está a ser usada a versão IEEE 802.11g, Figura 1.

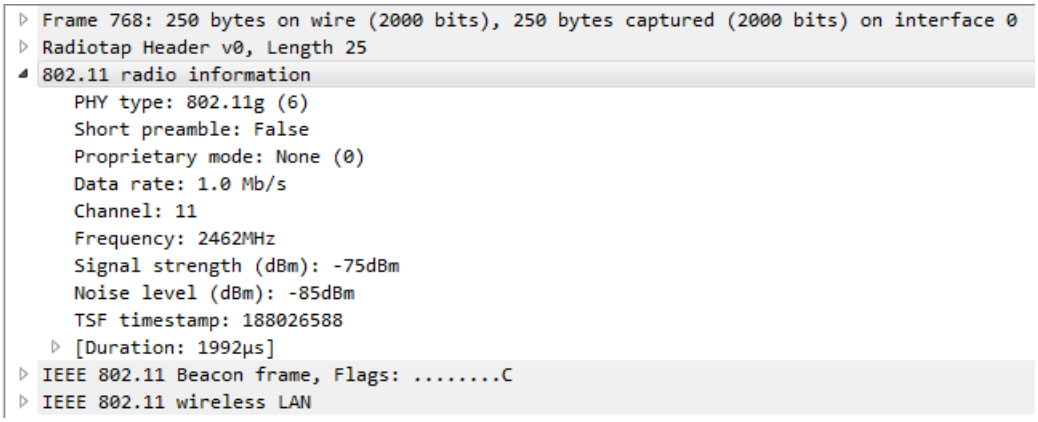

Figura 1. *Radio information* da trama 768.

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.
Podemos observar que o débito de envio corresponde a $R = 1Mb/s$, não sendo esse o máximo, visto que nesta versão da IEEE 802.11 esse valor corresponde a 54 Mb/s, estando essa informação armazenada na trama, como podemos ver na Figura 2.

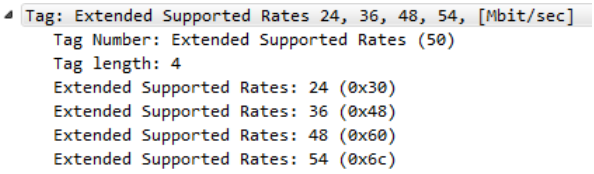

Figura 2. *Extended Supported Rates* da trama 768.

2.2 Scanning Passivo e Scanning Ativo

4) Selecione uma trama beacon (cujo número de ordem inclua o seu número de grupo). 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?
Tratamos a *beacon frame* 768, pertencente ao grupo das **Tramas de Gestão**, sendo o seu

tipo e subtipo identificados na trama com o valor 0x0008, como observamos na Figura 3, informação definida no campo *frame control* do cabeçalho da trama.

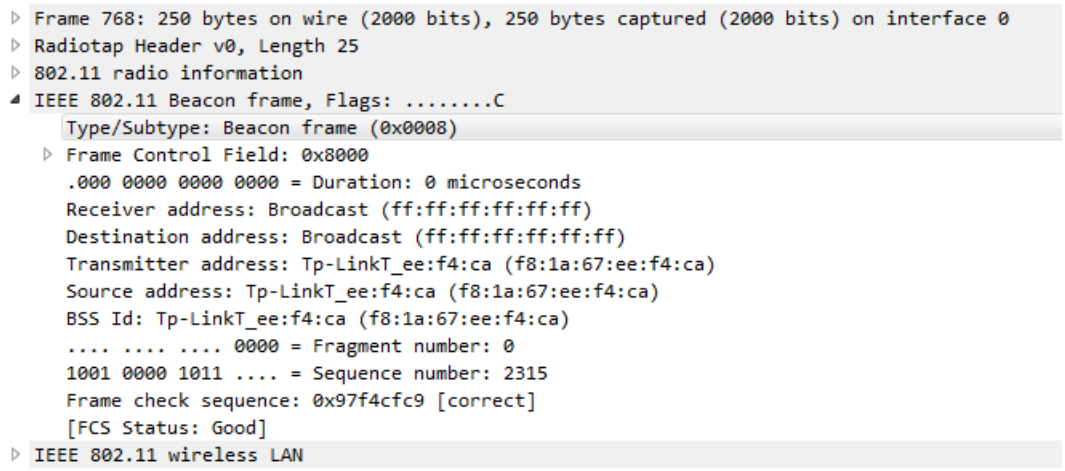

Figura 3. *Beacon frame* 768.

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.
Pela alínea anterior, sabemos que as *beacon frames* são, tais que, no campo *frame control* da trama, cujo Type/Subtype vale 0x0008, pelo que podemos definir o seguinte filtro de exibição: **wlan.fc.type_subtype == 0x8**
Podemos ver o SSID da trama como mostra a Figura 4, por exemplo. Após aplicar o filtro, verificamos que na vizinhança da trama se encontram pontos de acesso de SSID: FON_ZON_FREE_INTERNET, ZON-2770 e DDSS, Figura 5.

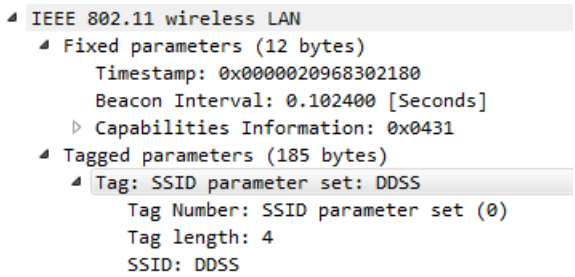

Figura 4. SSID da trama 768.

743	18.648903	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3296, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
744	18.665830	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2304, FN=0, Flags=........C, BI=100, SSID=DDSS
745	18.749515	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3297, FN=0, Flags=........C, BI=100, SSID=ZON-2770
746	18.751266	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3298, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
747	18.851850	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3299, FN=0, Flags=........C, BI=100, SSID=ZON-2770
748	18.853674	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3300, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
749	18.954256	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3301, FN=0, Flags=........C, BI=100, SSID=ZON-2770
750	18.956070	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3302, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
751	18.972658	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2307, FN=0, Flags=........C, BI=100, SSID=DDSS
752	19.056597	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3303, FN=0, Flags=........C, BI=100, SSID=ZON-2770
753	19.058447	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3304, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
754	19.158988	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3305, FN=0, Flags=........C, BI=100, SSID=ZON-2770
755	19.160930	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3306, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
756	19.261820	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3307, FN=0, Flags=........C, BI=100, SSID=ZON-2770
757	19.263634	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3308, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
758	19.364385	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3309, FN=0, Flags=........C, BI=100, SSID=ZON-2770
759	19.366267	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3310, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
760	19.466675	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3311, FN=0, Flags=........C, BI=100, SSID=ZON-2770
761	19.468683	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3312, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
762	19.569204	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3313, FN=0, Flags=........C, BI=100, SSID=ZON-2770
763	19.571053	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3314, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
764	19.671589	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3315, FN=0, Flags=........C, BI=100, SSID=ZON-2770
765	19.673422	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3316, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
766	19.774007	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3317, FN=0, Flags=........C, BI=100, SSID=ZON-2770
767	19.775923	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3318, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
768	19.791314	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2315, FN=0, Flags=........C, BI=100, SSID=DDSS
769	19.876404	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3319, FN=0, Flags=........C, BI=100, SSID=ZON-2770
770	19.878301	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3320, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
771	19.978787	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3321, FN=0, Flags=........C, BI=100, SSID=ZON-2770
772	19.980662	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3322, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
773	19.995779	Tp-LinkT_ee:f4:ca	Broadcast	802.11	250	Beacon frame, SN=2317, FN=0, Flags=........C, BI=100, SSID=DDSS
774	20.081185	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3323, FN=0, Flags=........C, BI=100, SSID=ZON-2770
775	20.083128	HitronTe_1b:27:79	Broadcast	802.11	233	Beacon frame, SN=3324, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
776	20.183633	HitronTe_1b:27:78	Broadcast	802.11	315	Beacon frame, SN=3325, FN=0, Flags=........C, BI=100, SSID=ZON-2770

Figura 5. Resultado de aplicar o filtro descrito.

6) Verifique se está a ser usado o método de detecção de erros (CRC), e se todas as tramas Beacon são recebidas corretamente. Justifique a conveniência em usar detecção de erros neste tipo de redes locais.
Pela Figura 2, constatamos que é feita a *Frame check sequence* para o código de deteção de erros. Aplicando o filtro **wlan.fc.type_subtype == 0x0008 && wlan.fcs.status == bad**, observamos que nem todas as *beacon frames* são recebidas corretamente, Figura 6. Deve ser usada deteção de erros nestas redes locais, face à considerável probabilidade de colisão, sendo CRC um método robusto de fácil implementação.

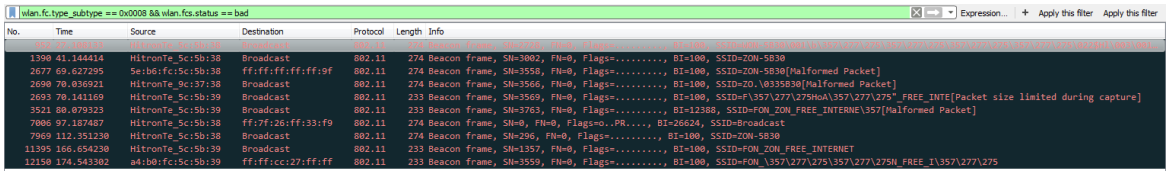

Figura 6. Resultado da aplicação do filtro descrito.

7) Para dois dos APs identificados, indique qual é o intervalo de tempo previsto entre tramas beacon consecutivas? Na prática, a periodicidade de tramas beacon é verificada? Tente explicar porquê.
Considerando os APs de SSID DDSS e ZON-2770, tomando como referência as tramas 768 e 769, respetivamente, é prevista uma periodicidade 0.1024 segundos, como podemos ver nas figuras 7 e 8. No entanto, essa periodicidade nem sempre é verificada, por exemplo, para o AP de SSID DDSS, entre as tramas consecutivas 768 e 773, obtemos:

$$\Delta_{768\rightarrow773} = 19.995779 - 19.791314 \approx 0.204465 \neq 0.1024$$

Ora, neste tipo de ligação existe uma maior vunerabilidade a interferências externas e dá-se atenuação do sinal, por exemplo, impedindo a periodicidade de ser atingida.

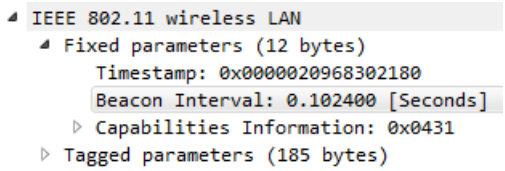

Figura 7. *Beacon interval* da trama 768.

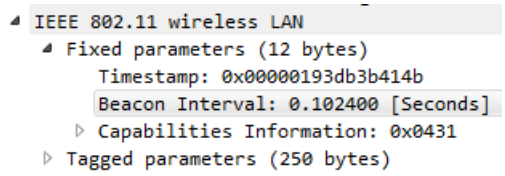

Figura 8. *Beacon interval* da trama 769.

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.
Para a trama 758 vamos ter:

Endereço do recetor - ff:ff:ff:ff:ff:ff

Endereço de destino - ff:ff:ff:ff:ff:ff

Endereço do transmissor - f8:1a:67:ee:f4:ca

Endereço de origem - f8:1a:67:ee:f4:ca

como podemos ver na Figura 2. Enquanto que para a trama 759 é considerado:

Endereço do recetor - ff:ff:ff:ff:ff:ff

Endereço de destino - ff:ff:ff:ff:ff:ff

Endereço do transmissor - bc:14:01:1b:27:78

Endereço de origem - bc:14:01:1b:27:78

pela Figura 9.

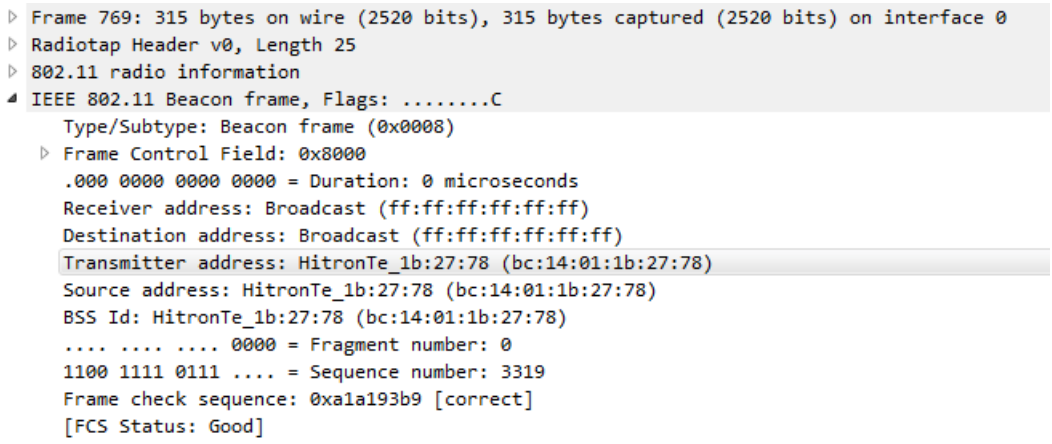

Figura 9. Informação *Beacon frame* da trama 769.

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?
Podemos constatar os débitos dos dois APs considerados nas figuras 10 e 11, respetivamente, nos campos *Supported Rates* e *Extended Supported Rates*.

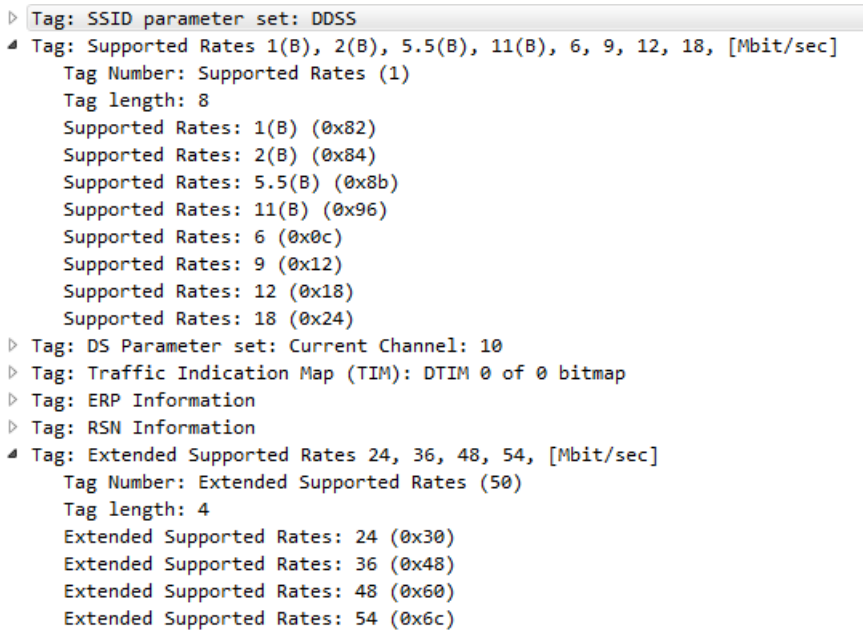

Figura 10. Débitos suportados pelo AP associado à trama 768.

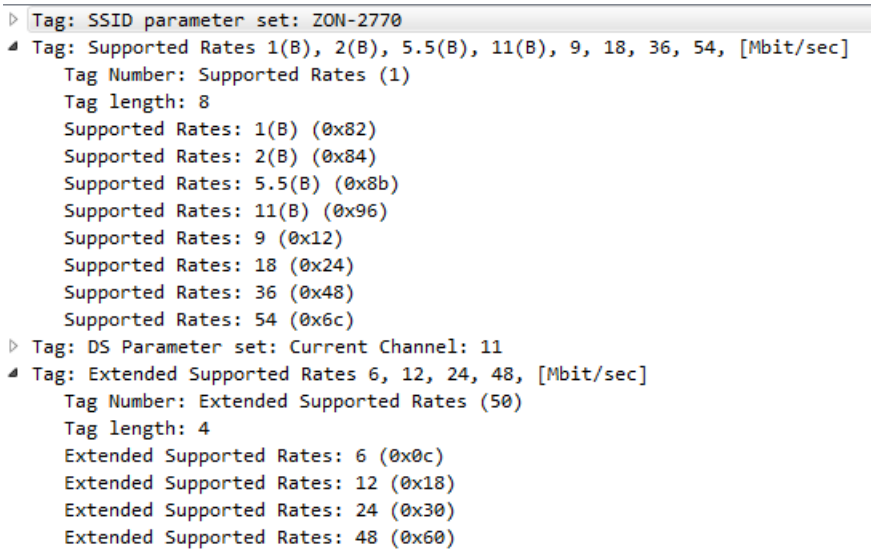

Figura 11. Débitos suportados pelo AP associado à trama 769.

10) Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request ou probing response, simultaneamente.
Consultando o anexo, verificamos que *Probe request* tem associado o valor 0x4 e *Probe response* o valor 0x5, pelo que definimos o seguinte filtro: **wlan.fc.type_subtype in {0x4 0x5}**.
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?
Tomamos como exemplo as tramas 6827 e 6828, representando *pedido de prova* e *resposta de prova*, respetivamente, destacadas nas Figuras 12 e 13. Estas tramas estão associadas a *stations*, tais que, a STA que envia o pedido a outra estação pretende obter informação sobre ela, por exemplo, para realizar *active scanning*, e a segunda envia a resposta com a informação pretendida.

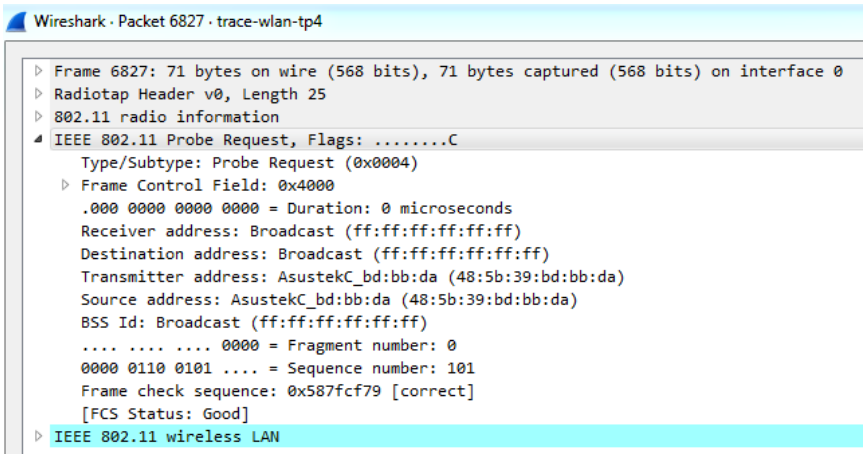

Figura 12. Exemplo de um *probe request*.

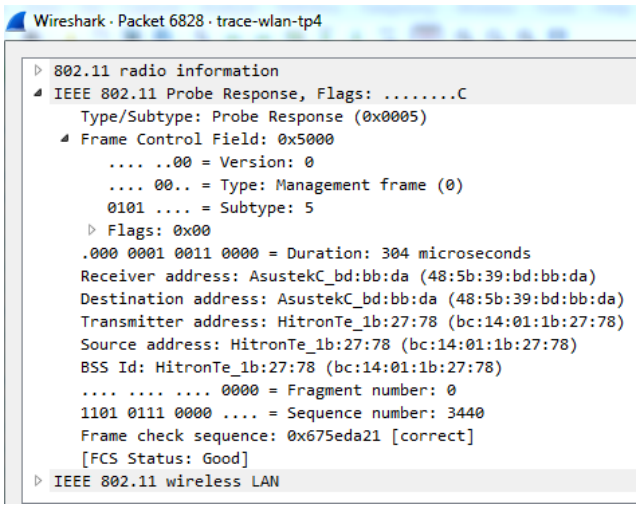

Figura 13. Exemplo de uma *probe response*.

2.3 Processo de Associação

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.
Começamos por definir um filtro para obter um subconjunto de tramas de gestão, relevantes para o processo de associação, bem como a trama de confirmação da receção, pertencente às tramas de controlo, conforme os valores destacados em anexo:
wlan.fc.type_subtype in {0x0 0x1 0x2 0x3 0xA 0xB 0xC 0x1D}
Donde obtemos, por exemplo, a seguinte sequência de tramas:

9967	136.245580	Apple_71:41:a1	HitronTe_1b:27:78	802.11	70 Authentication, SN=3346, FN=0, Flags=........C
9968	136.245910		Apple_71:41:a1 (d8:…	802.11	39 Acknowledgement, Flags=........C
9969	136.246439	HitronTe_1b:27:78	Apple_71:41:a1	802.11	59 Authentication, SN=3701, FN=0, Flags=........C
9970	136.248481	Apple_71:41:a1	HitronTe_1b:27:78	802.11	193 Association Request, SN=3347, FN=0, Flags=........C, SSID=ZON-2770
9971	136.248783		Apple_71:41:a1 (d8:…	802.11	39 Acknowledgement, Flags=........C
9972	136.255880	HitronTe_1b:27:78	Apple_71:41:a1	802.11	225 Association Response, SN=3702, FN=0, Flags=........C
9973	136.256041		HitronTe_1b:27:78 (…	802.11	39 Acknowledgement, Flags=........C

Figura 14. Exemplo do processo de associação.

13) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.
Para uma estação e um ponto de acesso, assumindo que todos os pedidos são aceites, podemos demonstrar as tramas enviadas no processo de associação entre eles da seguinte forma:

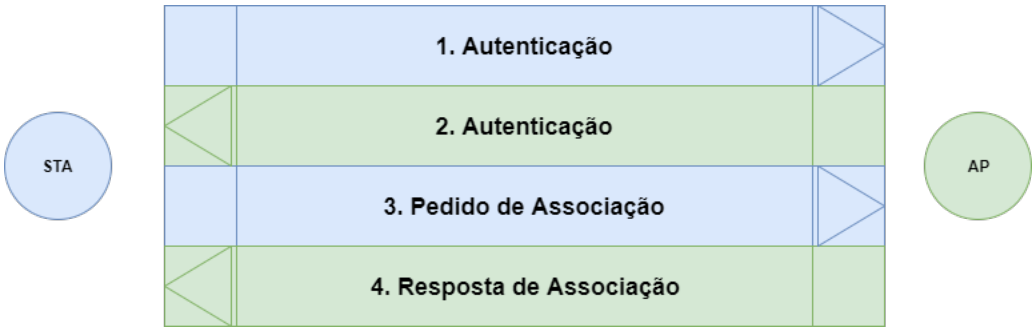

Figura 15. Ilustração do processo de associação.

onde entre essas tramas podem ser enviadas também tramas de confirmação da receção.

2.4 Transferência de Dados

14) Considere a trama de dados no1054. 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?
Pelo campo *DS status*, na Figura 16, verificamos que a direcionalidade da trama é definida, tal que, **To DS: 1** e **From DS: 0**, pelo que a trama é enviada para um sistema distribuído da rede, através do ponto de acesso, deixando de ser local à WLAN.

```
▷ Frame 1054: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
▷ Radiotap Header v0, Length 40
▷ 802.11 radio information
◢ 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 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: HitronTe 1b:27:78 (bc:14:01:1b:27:78)
```

Figura 16. *Frame Control* da trama 1054.

15) Para a trama de dados no1054, 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?
Na Figura 17 constam os endereços MAC da trama 1054, onde:

STA - a4:d1:d2:d1:fe:a8, que está associado ao endereço de origem e ao do transmissor;
AP - bc:14:01:1b:27:78, identificando o endereço do recetor;
Router - bc:14:01:1b:27:76, que define o endereço de destino.

```
Receiver address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
Destination address: HitronTe_1b:27:76 (bc:14:01:1b:27:76)
Transmitter address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
Source address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
BSS Id: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
STA address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
```

Figura 17. Endereços MAC da trama 1054.

16) Como interpreta a trama no1060 face à sua direccionalidade e endereçamento MAC?

Podemos observar no campo *DS status*, representado na Figura 18, que a direcionalidade da trama 1060 é definida por **To DS: 0** e **From DS: 1**, o que nos indica que a trama vem de um sistema distribuído para a rede sem fios, até uma STA, através do ponto de acesso. Isso pode ser verificado através dos endereços MAC desta trama, que estão associados aos sistemas já analisados na alínea anterior, onde nesta trama o endereço da STA corresponde ao recetor/destino, o do AP ao transmissor e o *router* a origem, como seria de esperar.

```
▲ 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 1100 1010 = Duration: 202 microseconds
Receiver address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
Destination address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
Transmitter address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
Source address: HitronTe_1b:27:76 (bc:14:01:1b:27:76)
BSS Id: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
STA address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
```

Figura 18. Conteúdo da *Frame Control* da trama 1060.

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.)

As tramas de confirmação de receção, responsáveis pela deteção de erros nas tramas de dados recebidas, sendo enviadas para a STA de origem por forma a informar que não foram identificados erros nessas tramas. Ora, face à natureza deste tipo de ligação, a sua maior suscetibilidade a interferências externas, comparativamente com redes Ethernet, bem como a inexistência de mecanismos de correção de erros, mas que existem nas redes *wired*, faz com que seja necessário vigiar constantemente a integridade dos dados transmitidos, usando tramas *ACK* para atingir esse objetivo.

```
1052 31.139152     Apple_d1:fe:a8 (a4:… HitronTe_1b:27:78 (… 802.11     45 Request-to-send, Flags=........C
1053 31.139166                          Apple_d1:fe:a8 (a4:… 802.11     39 Clear-to-send, Flags=........C
1054 31.139171     Apple_d1:fe:a8       HitronTe_1b:27:76    802.11    122 QoS Data, SN=4006, FN=0, Flags=.p.....TC
1055 31.139280     HitronTe_1b:27:78 (… Apple_d1:fe:a8 (a4:… 802.11     57 802.11 Block Ack, Flags=........C
1056 31.139774     HitronTe_1b:27:78 (… Apple_d1:fe:a8 (a4:… 802.11     49 802.11 Block Ack Req, Flags=........C
1057 31.140244     Apple_d1:fe:a8 (a4:… HitronTe_1b:27:78 (… 802.11     57 802.11 Block Ack, Flags=........C
1058 31.140255     Apple_d1:fe:a8       HitronTe_1b:27:78    802.11     68 Null function (No data), SN=1106, FN=0, Flags=....R..TC
1059 31.140315                          Apple_d1:fe:a8 (a4:… 802.11     39 Acknowledgement, Flags=........C
1060 31.141446     HitronTe_1b:27:76    Apple_d1:fe:a8       802.11    125 QoS Data, SN=1753, FN=0, Flags=.p....F.C
1061 31.146301     HitronTe_1b:27:78    Broadcast            802.11    315 Beacon frame, SN=3539, FN=0, Flags=........C, BI=100, SSID=ZON-2770
1062 31.148111     HitronTe_1b:27:79    Broadcast            802.11    233 Beacon frame, SN=3540, FN=0, Flags=........C, BI=100, SSID=FON_ZON_FREE_INTERNET
1063 31.159660     Apple_d1:fe:a8       HitronTe_1b:27:78    802.11     68 Null function (No data), SN=1107, FN=0, Flags=...P...TC
1064 31.159680                          Apple_d1:fe:a8 (a4:… 802.11     39 Acknowledgement, Flags=........C
```

Figura 19. Tráfego na vizinhança da trama 1054.

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.

Constatamos que está a ser usada a opção RTS/CTS, como mostra a Figura 19, onde as tramas RTS e CTS correspondem às *frames* 1052 e 1053, respetivamente. Podemos observar nas figuras 20 e 21, que a direcionalidade de ambas as tramas é definida, tal que, **To DS: 0** e **From DS: 0**, indicando que a comunicação é feita entre STAs e APs. Ora, uma estação envia a trama RTS para outras STAs, por forma a "reservar"o canal antes de começar a enviar os dados, obtendo resposta CTS dessas estações, indicando que pode iniciar a tranmissão.

```
▾ 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 0101 0110 = Duration: 86 microseconds
    Receiver address: HitronTe_1b:27:78 (bc:14:01:1b:27:78)
    Transmitter address: Apple_d1:fe:a8 (a4:d1:d2:d1:fe:a8)
    Frame check sequence: 0xac3202be [correct]
    [FCS Status: Good]
```

Figura 20. Exemplo de trama *Request-to-Send*.

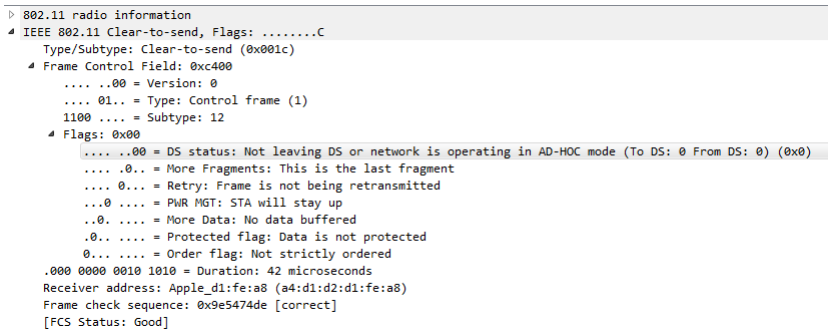

Figura 21. Exemplo de trama *Clear-to-Send*.

3 Conclusão

Este trabalho visou praticar e expandir o conhecimento adquirido acerca do protocolo IEEE 802.11 e seu funcionamento. Foi feito um estudo aprofundado sobre o diferente tipo de tramas : Management Frames, Control Frames, Data Frames e seus respectivos subtipos. Devido á dificuldado em obter boas capturas para análise neste protocolo, foi disponiblizada uma pelo professor. Inicialmente foi feita uma pequena análise das informações do nível físico de uma trama dada (frequência do espetro, versão da norma,...), bem como os bytes que dizem respeito às tramas 802.11. Expandiu-se a área de estudo com a investigação do scanning passivo e ativo que permitem que uma estação possa optar por um AP que lhe seja mais favorável. Relativamente ao scanning passivo, que é realizado através do envio periódico de tramas de subtipo Beacon a todas as estações da rede, possibilita ao AP anunciar a sua presença e transmitir diferentes e variadas informações sobre si.O scanning ativo envolve os subtipos de tramas Probe Request e Probe Response. As tramas de Probing request são utilizadas de modo a obter informações sobre as estações que estão no seu alcance rádio, enquanto que as tramas de Probing response são uma resposta por partes das estações que receberam a trama de Probe Request e que contêm todas as informações e dados sobre a própria estação que envia a trama (Probe Response). Foi estudado um processo de associação de um host e um ponto de acesso (AP), que antes do envio de dados se inicia através do envio de uma trama Association Request do host para o AP e uma Association Response como resposta do AP. Na parte final estuda-se o processo de transferência de dados e os protocolos inerentes. Este estudo permitiu-nos expandir os conhecimento da Unidade Curricular.