

Relatório Trabalho Prático nº4

João Pimentel (a80874) Rodolfo Silva (a81716) Pedro Gonçalves (a82313)

Dezembro 2018

Universidade do Minho
Mestrado Integrado em Engenharia Informática
Redes de Computadores
Grupo 64

Conteúdo

1	Questões e Respostas	3
1.1	Acesso Rádio	3
1.2	Scanning Passivo e Scanning Ativo	4
1.3	Processo de Associação	10
1.4	Transferência de Dados	11
2	Conclusões	14

1 Questões e Respostas

1.1 Acesso Rádio

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

Esta rede sem fios opera na frequência $2467MHz$, e corresponde ao canal 12, como é possível observar na Figura 1.

The screenshot shows a portion of a Wireshark capture. A specific frame's details pane is open, showing the following information under the section "802.11 radio information":

- PHY type: 802.11g (6)
- Short preamble: False
- Proprietary mode: None (0)
- Data rate: 1.0 Mb/s
- Channel: 12
- Frequency: 2467MHz
- Signal strength (dBm): -66dBm
- Noise level (dBm): -87dBm
- TSF timestamp: 34955163
- [Duration: 2360μs]

Figura 1 - 802.11 Radio Information da trama 364 da captura.

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

A norma IEEE 802.11 que está a ser utilizada é a $802.11g$, como se pode observar na Figura 1, no campo *PHY type*.

- 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.

O débito de envio da trama escolhida foi de $1.0MB/s$, como se pode verificar no campo *Data Rate* da Figura 1. Este débito de envio não corresponde ao débito máximo suportado pela interface *WIFI*, pois o máximo suportado por esta é $54Mb/s$.

1.2 Scanning Passivo e Scanning Ativo

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?

O tipo desta trama é *Management* e o seu subtipo é *Beacon* ($0x0008$). Como se pode ver no campo *Frame Control Field*, na Figura 2, o identificador de tipo é 00_2 e de subtipo é 1000_2 .

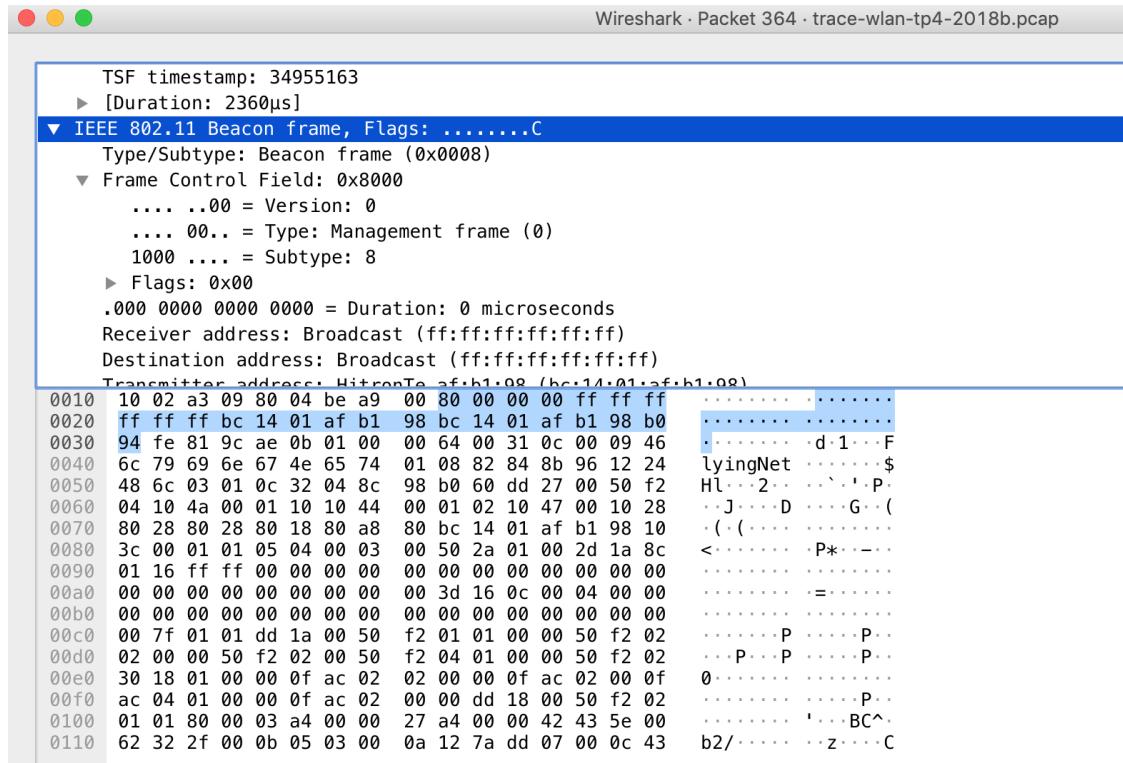


Figura 2 - IEEE 802.11 Beacon frame da trama 364 da captura.

5. Liste todos os SSIDs dos APs (*Acess 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).

Os *SSIDs* dos *APs* que estão a operar na vizinhança da *STA* são *FlyingNet* e *NOS_WIFI_Fon*, sendo que esta informação foi obtida o filtro *wlan*, como se pode observar na Figura 3, para se observar apenas as tramas *Beacon*. Foi necessário percorrer os a captura para confirmar a existência de apenas estes dois *SSIDs*.

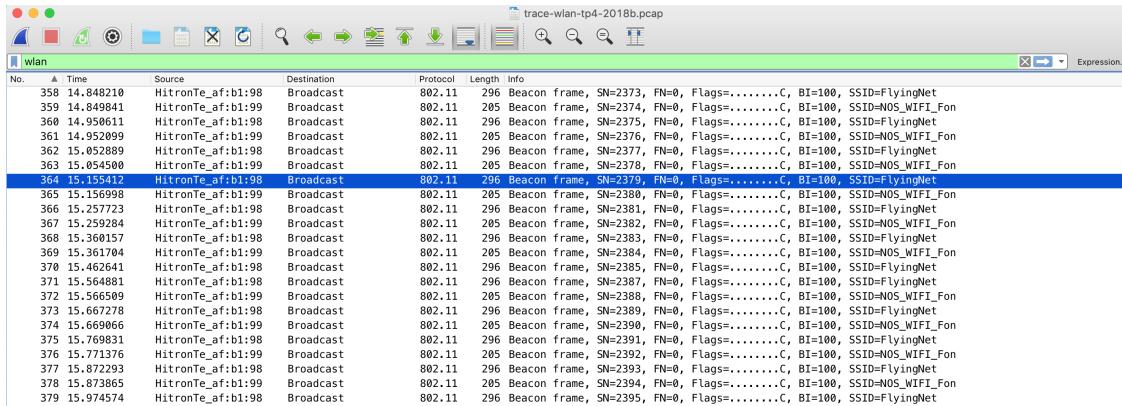


Figura 3 - Filtro *wlan* aplicado à captura.

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 utilizado *CRC* pois o *FCS* está ativo, como se observa na Figura 4. Como se trata de uma rede *Wireless* a deteção de erros é feita, visto que os pacotes são mais suscetíveis a erros.

Estes erros podem ir desde interferências causadas por um co-canal ou por uma outra fonte, até demasiada energia no *AP*.

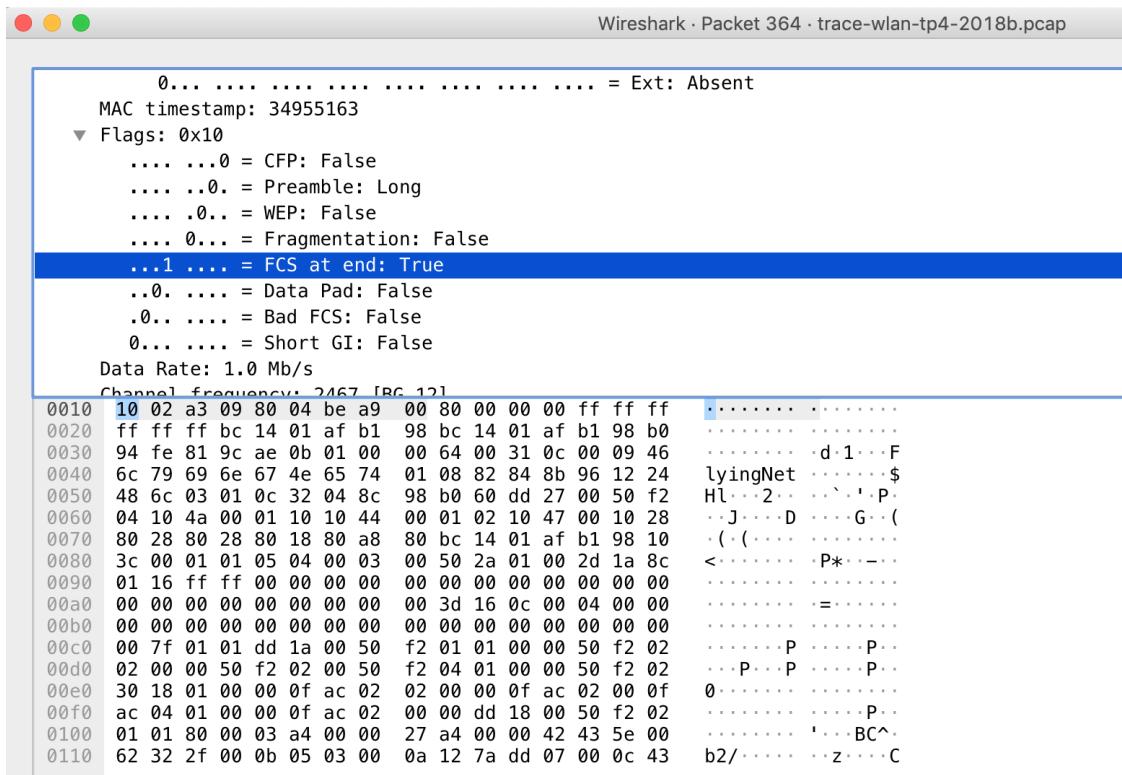


Figura 4 - *Flags* da trama 364 da captura.

Como se vê na Figura 5, existem tramas que não são recebidas corretamente.

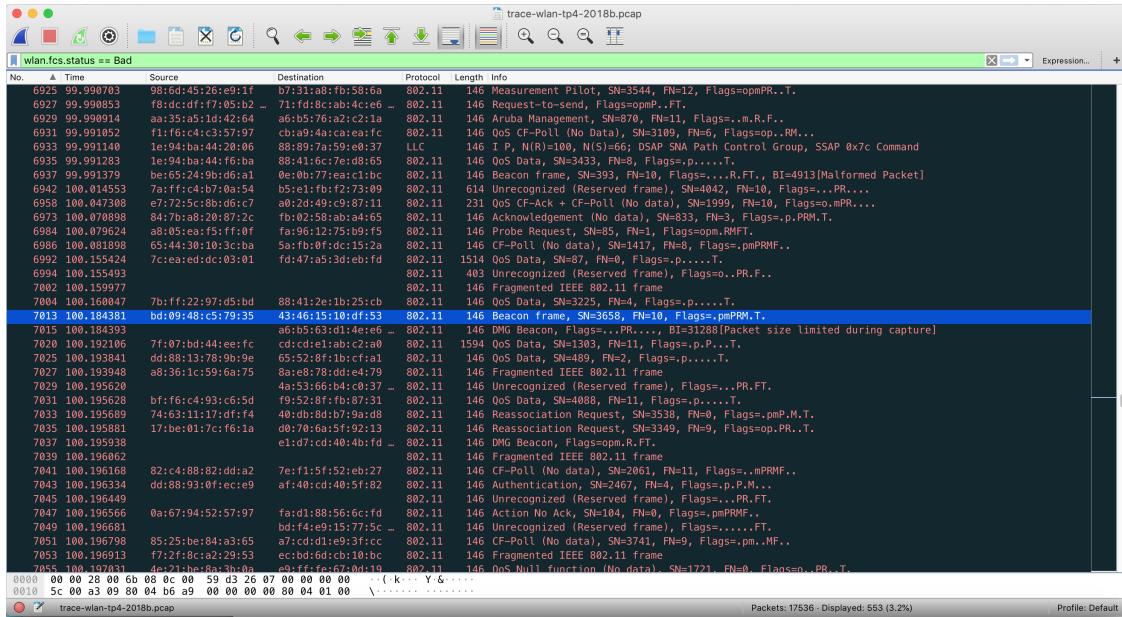


Figura 5 - Aplicação do filtro para ver tramas com *Bad FCS*.

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 consecutivas é 0.102400 segundos, como se vê no parâmetro *Beacon Interval*, na Figura 6. Na prática, a periodicidade das tramas *Beacon*, com igual *SSID* é verificada, devido ao facto de este parâmetro ser um valor pré-definido, normalmente 100 ms, que serve, entre outros, para sincronizar os aparelhos ligados a um determinado *AP*.

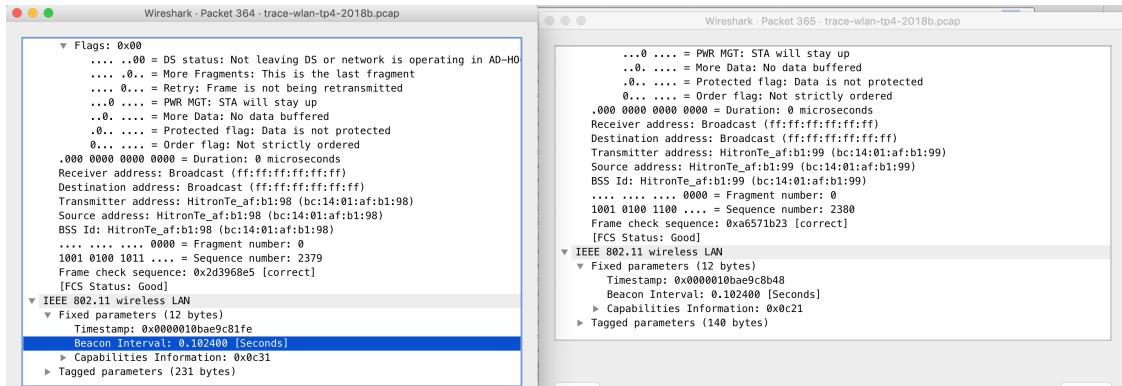


Figura 6 - *Beacon Interval*.

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.

Os endereços *source* são *bc:14:01:af:b1:98* e *bc:14:01:af:b1:99*. O de destino é *broadcast*, ou seja, *ff:ff:ff:ff:ff:ff*, como se vê na Figura 7.

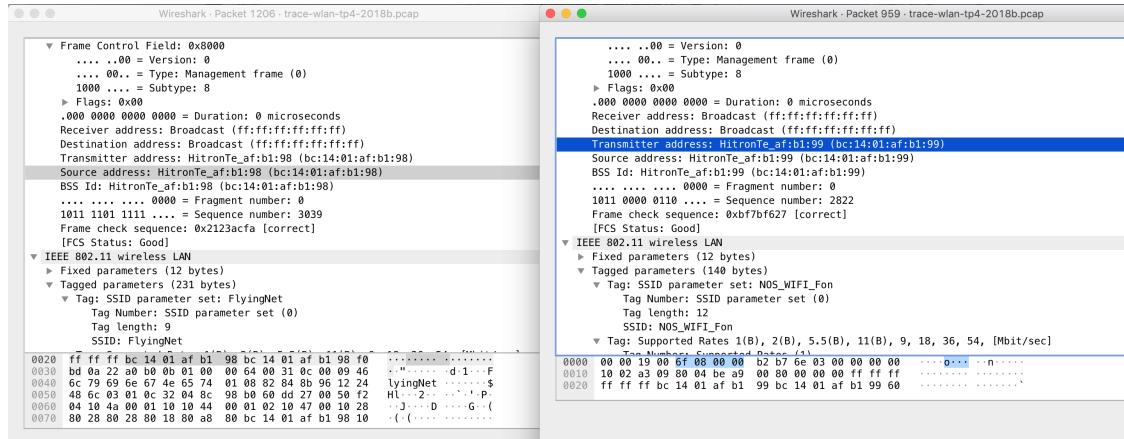


Figura 7 - Endereços *MAC* usados nas tramas *Beacon* enviada pelos *APs*.

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?

Como se pode verificar na Figura 8, no campo *Supported Rates*, são suportados os seguintes débitos:

1. 1 Mbps(11b)
2. 2 Mbps(11b)
3. 5.5 Mbps(11b)
4. 11Mbps (11b)
5. 9Mbps(11g)
6. 18Mbps(11g)
7. 36Mbps(11g)
8. 54Mbps(11g)

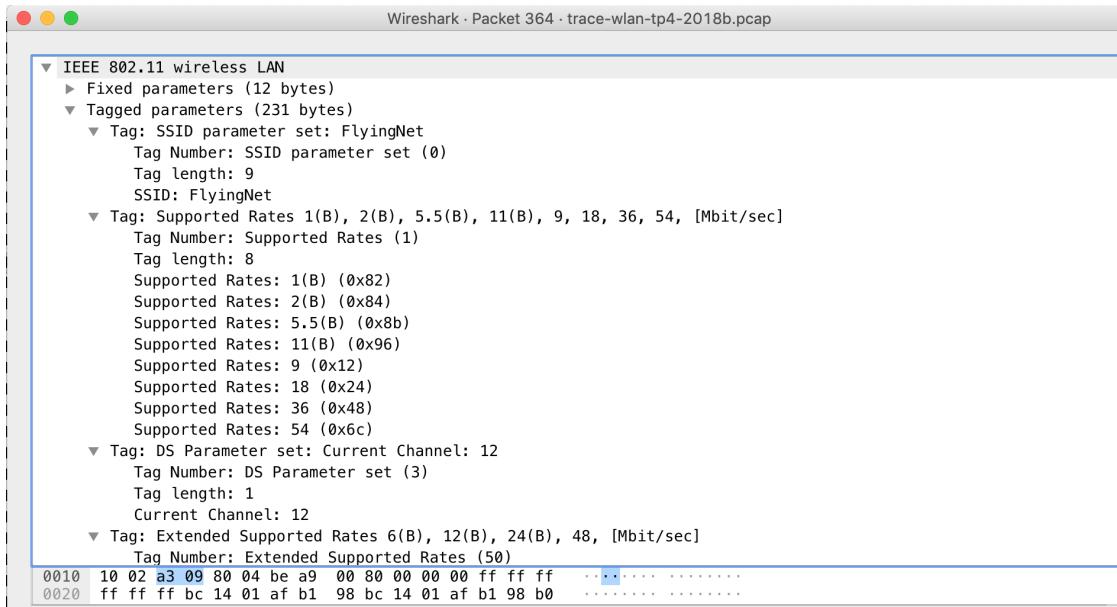


Figura 8 - Débitos de base suportados pelo AP.

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

Como se vê na Figura 9, foi aplicado o filtro wlan.fc.type_subtype eq 4 || wlan.fc.type_subtype eq 5.

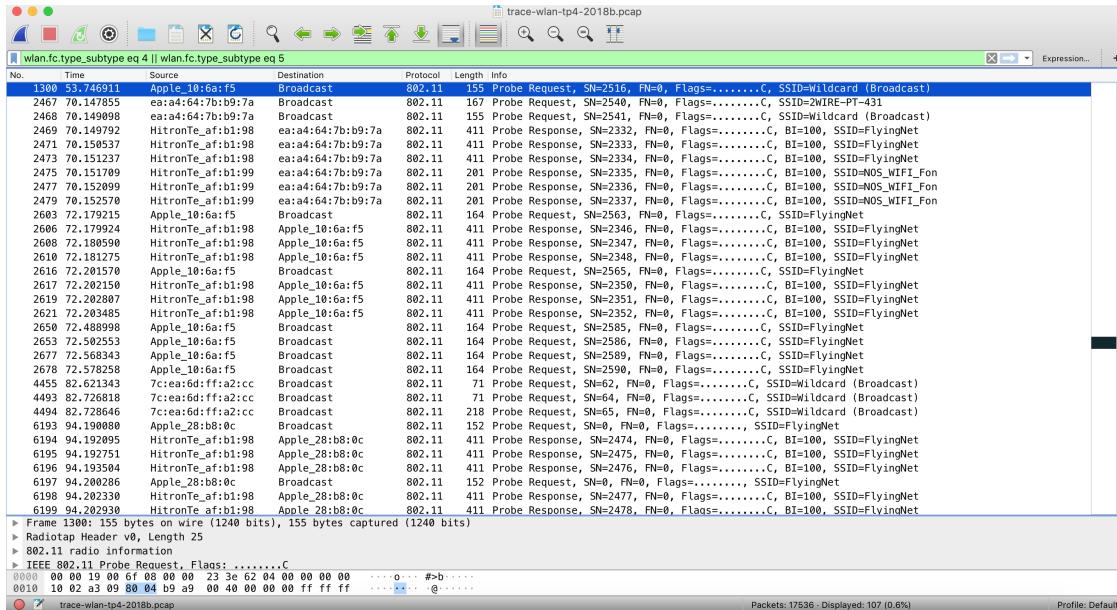


Figura 9 - Tramas probing request ou probing response

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

As tramas são endereçadas respetivamente ao *Access Point* e à *Station*. Servem forma da *Station* pedir informação sobre as redes disponíveis na sua proximidade.

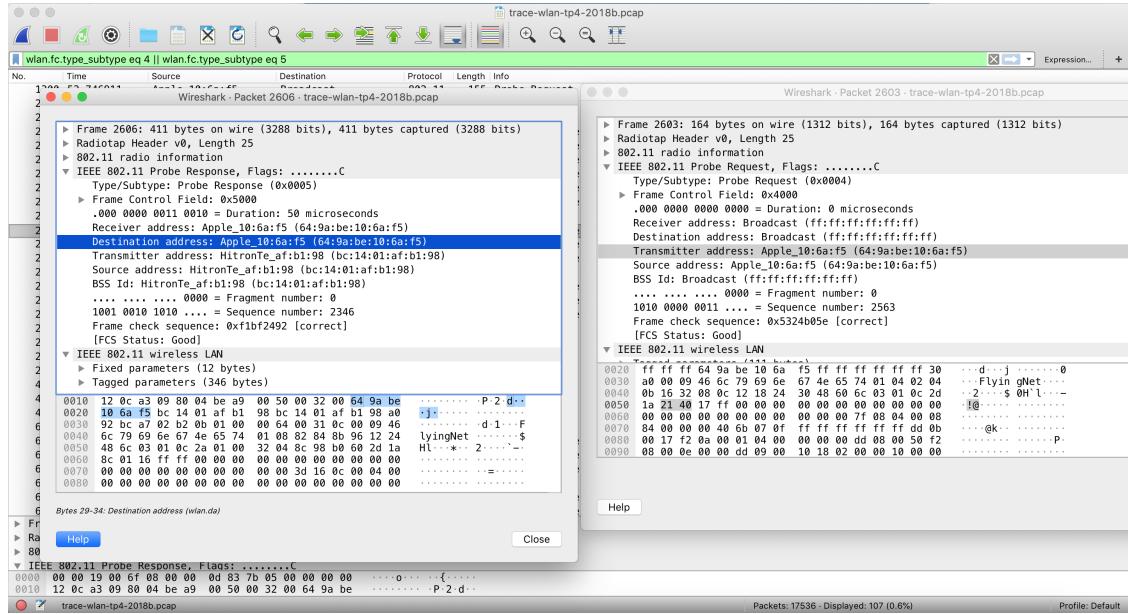


Figura 10 - *Probing request* e *Probing response*.

1.3 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.

2486 70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70 Authentication, SN=2542, FN=0, Flags=.....C	70.361
2487 70.362050		Apple_10:6a:f5 (64:..	802.11	39 Acknowledgement, Flags=.....C	70.362
2488 70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59 Authentication, SN=2338, FN=0, Flags=.....C	70.381
2489 70.381878		HitronTe_af:b1:98 (...	802.11	39 Acknowledgement, Flags=.....C	70.381
2490 70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175 Association Request, SN=2543, FN=0, Flags=.....C..	70.383
2491 70.383873		Apple_10:6a:f5 (64:..	802.11	39 Acknowledgement, Flags=.....C	70.383
2492 70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225 Association Response, SN=2339, FN=0, Flags=.....C	70.389
2493 70.389352		HitronTe_af:b1:98 (...	802.11	39 Acknowledgement, Flags=.....C	70.389

Figura 11 - Processo de associação.

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

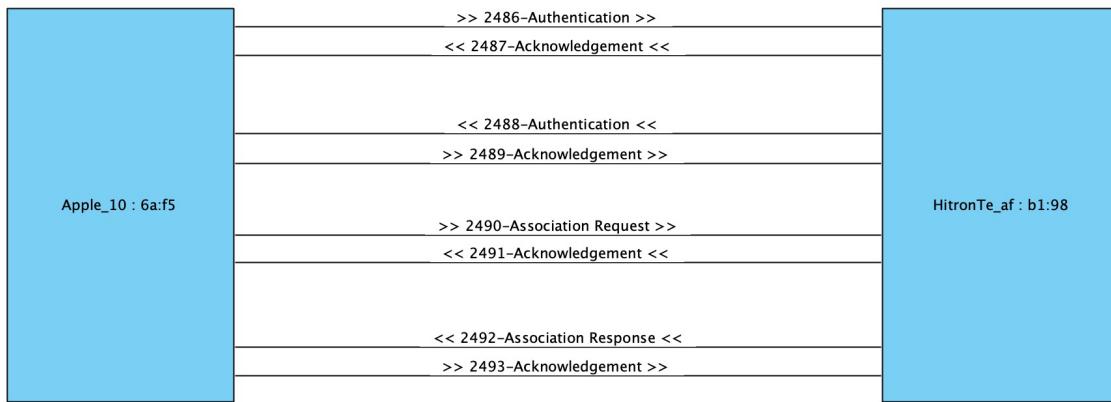


Figura 12 - Diagrama ilustrativo de todas as tramas trocadas no processo.

1.4 Transferência de Dados

14. Considere a trama de dados nº818. 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?

A trama está a entrar num ambiente *wireless*, vinda do à *DS*. A Figura 13 mostra isso mesmo, no parâmetro *DS Status*, possuindo o valor 10_2 . Sendo assim, a direccionalidade local WLAN.

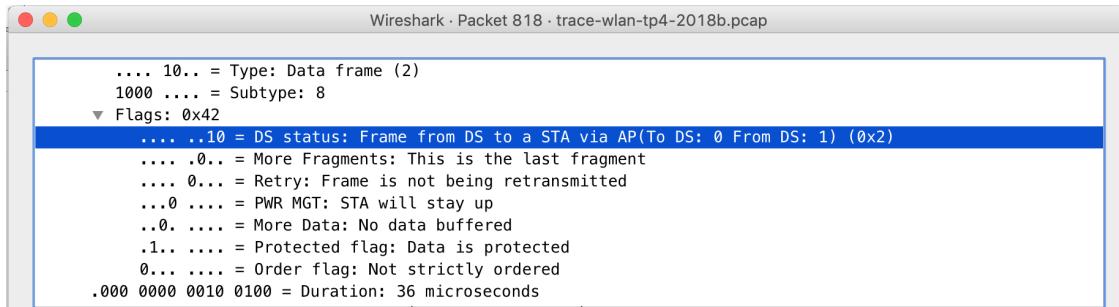


Figura 13 - *Flags* da trama 818.

15. Para a trama de dados nº818, 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.

Como se vê na Figura 14, têm-se os seguintes endereços:

ROUTER - Source address: HitronTe_af:b1:96 (bc:14:01:af:b1:96)

AP - BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)

STA - STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)

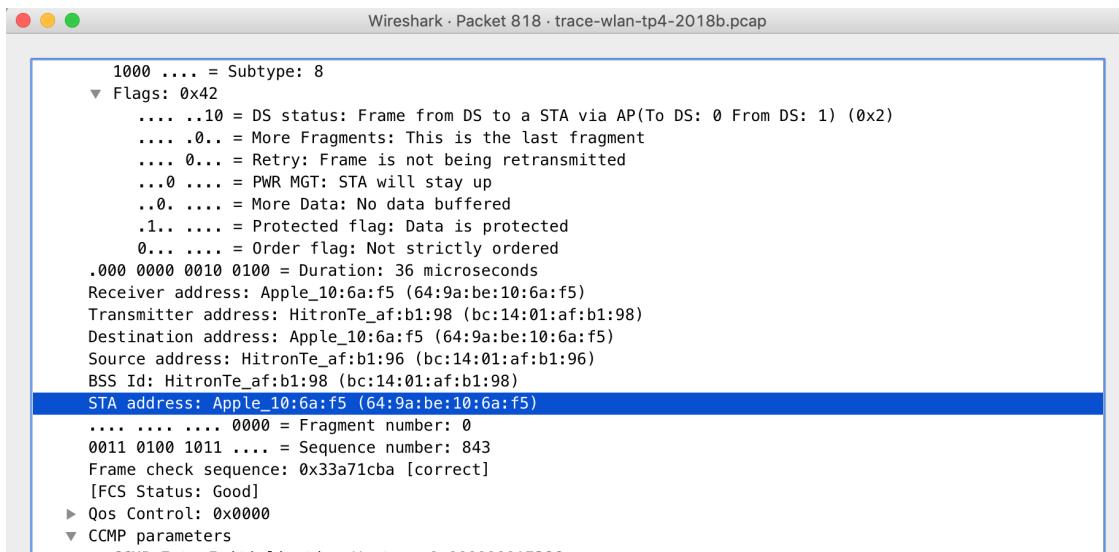


Figura 14 - Endereços presentes na trama 818.

16. Como interpreta a trama nº1434 face à sua direccionalidade e endereçamento MAC?

Tendo em conta que, como se vê na Figura 15, a flag *DS Status*, na trama, possuir o valor 01_2 , o endereço de destino ser o *bc:14:01:af:b1:96* e o de fonte ser o *64:9a:be:10:6a:f5*, a direccionalidade da trama é da *STA* para o *DS*.

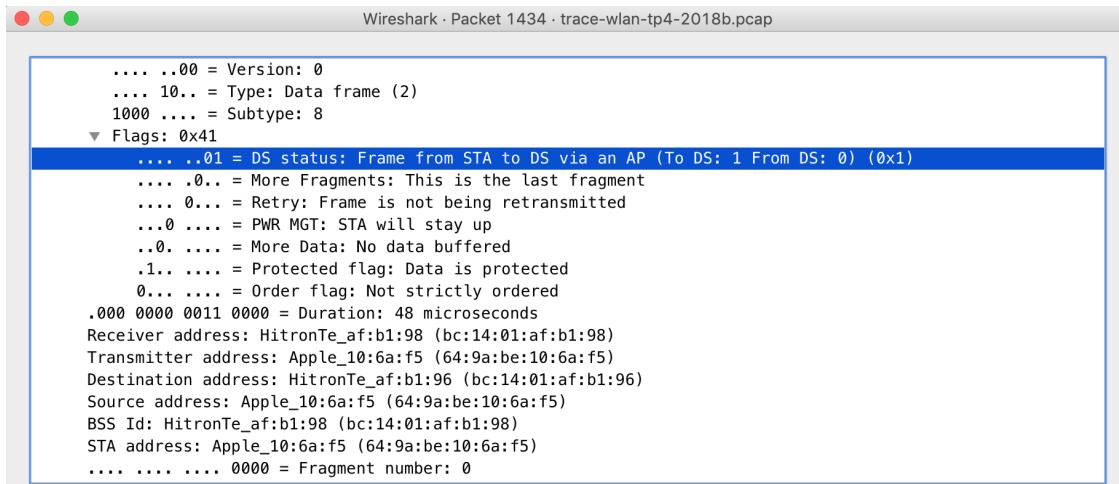


Figura 15 - Endereços presentes na trama 1434.

17. Que subtípico 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).

Como se vê na Figura 16, os subtípitos de tramas de controlo que são transmitidas ao longo da transferência de dados em análise são *Request-to-send*, *Clear-to-send* e *802.11 Block-Ack*.

RTS/CTS é um mecanismo que ajuda a prevenir a ocorrência de colisões. Sempre que uma *station* quer enviar uma trama, deve ocorrer uma troca *RTS/CTS* antes de qualquer troca de dados.

Já *Block-Ack* é usado para reconhecer uma bloco de uma trama de dados *QoS*, em vez de reconhecer cada trama unicast de forma independente.

Assim, devido à enorme propriedade de colisões numa rede *Wireless*, contrariamente a uma rede *Ethernet*, o uso destas tramas de controlo permite uma maior garantia da falta de corrupção dos dados em transferência.

1432 57.406630	Apple_10:6a:f5 (64...	HitronTe_af:b1:98 ...	802.11	45 Request-to-send, Flags=.....C
1433 57.406638		Apple_10:6a:f5 (64...	802.11	39 Clear-to-send, Flags=.....C
1434 57.406641	Apple_10:6a:f5	HitronTe_af:b1:96	802.11	158 QoS Data, SN=3691, FN=0, Flags=..p....TC
1435 57.406730	HitronTe_af:b1:98 ...	Apple_10:6a:f5 (64...	802.11	57 802.11 Block Ack, Flags=.....C

Figura 16 - Transferência de dados relativa à trama 1434.

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 se 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.

Para o exemplo mencionado acima, é utilizada a opção *RTS/CTS*, visível na Figura 17, permitindo uma redução no número de colisões. A direccionalidade das tramas *RTS* é da *Station* para o *AP*. Já a das *CTS* é do *AP* para a *Station*.

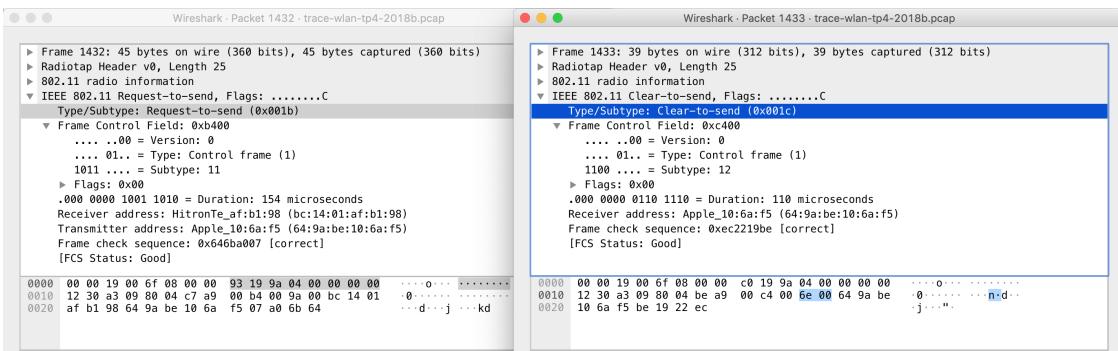


Figura 17 - Tramas *RTS* e *CTS* envolvidas na transferência de dados relativa à trama 1434.

2 Conclusões

O desenvolvimento deste projeto permitiu um aumento no conhecimento relativamente a redes *Wireless*, nomeadamente a forma como são enviadas tramas entre os vários componentes destas redes, como são tratadas colisões, entre outros aspetos.

Tendo em conta que, hoje em dia, quase todos os dispositivos possuem uma forma de se ligar à rede, sem a utilização de fios, um conhecimento forte sobre estas é uma mais valia.

Em suma, este projeto permitiu solidificar a matéria lecionada até ao momento, no que toca a redes *Wireless*, tendo sido proveitoso para a realização de qualquer trabalho futuro relativo a este tipo de redes.