Trabalho Prático 4: Redes sem fios (Wi-Fi)

Alexandra Santos, Inês Ferreira e Joana Branco
Universidade do Minho, Departamento de Informática
email: {a94523, a97372, a96584}@alunos.uminho.pt

Acesso rádio

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (radiotap header, radio information), para além dos bytes correspondentes a tramas 802.11. Selecione a trama de ordem 16 correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

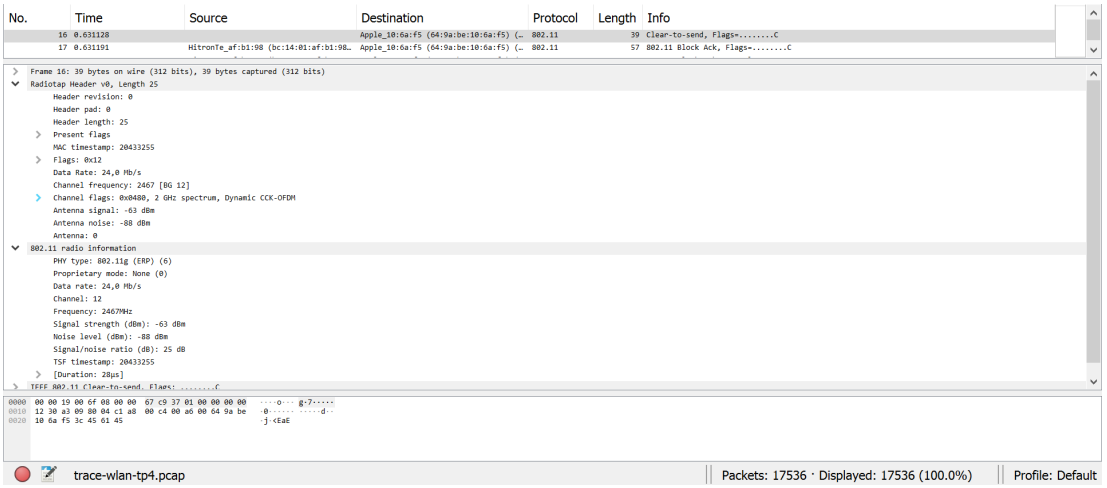


Figura 1: Trama 802.11

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

   R: Tal como podemos observar na figura 1, a rede sem fios opera no canal 12, com uma frequência de 2467 MHz.

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

   R: Na figura 1 podemos observar que a versão utilizada é a 802.11g. Esta informação encontra-se no campo PHY type.

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.

   R: A trama escolhida foi enviada com um débito de 24.0 Mb/s. Este valor por sua vez não corresponde ao débito máximo da versão 802.11g, uma vez que o valor da mesma é 54 Mbps.

Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando XX o seu nº de grupo, responda às seguintes questões:

4. Selecione a trama beacon de ordem (260 + XX). 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)?

   R: De acordo com o campo *Type/Subtype* podemos afirmar de que se trata de uma trama do tipo *Management* (00) e de subtipo *Beacon* (08). Isto pode ser verificado através do valor indicado, 0x0008, no mesmo campo mencionado anteriormente. Assim sendo, a trama é uma *Beacon frame.*

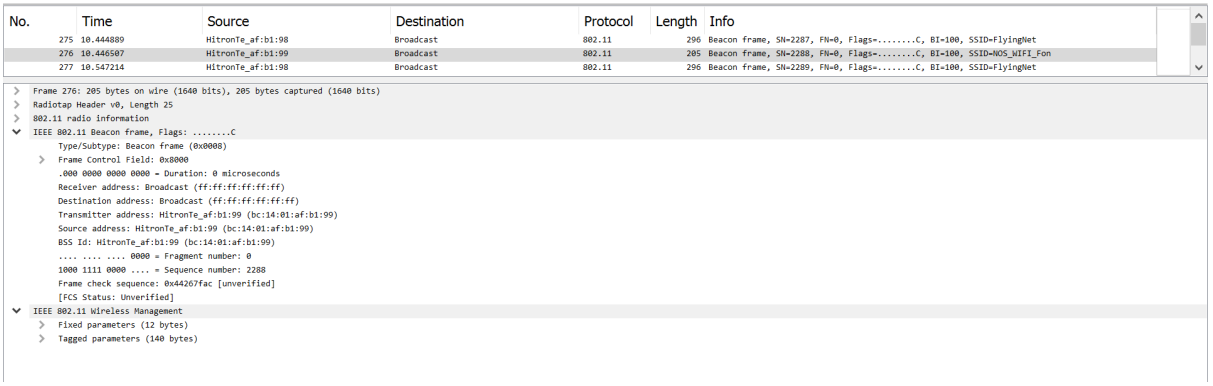


Figura 2: *Beacon frame* relativa ao nosso grupo

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

   R: Na figura 2 podemos observar os endereços MAC em uso:
   D*estination address:* ff:ff:ff:ff:ff:ff
   Transmitter address: bc:14:01:af:b1:99
   Source address: bc:14:01:af:b1:99
   Receiver address: ff:ff:ff:ff:ff:ff

   Como o *destination address* é o mesmo que o *receiver address* e estes são do tipo *broadcast* podemos concluir que a trama pode ser captada por qualquer dispositivo.

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

   R: Os débitos de base que são suportados pelo AP são (*Supported Rates)*:

   → 1 Mb/s
   → 2 Mb/s

→ 5.5 Mb/s
→ 11 Mb/s
→ 9 Mb/s
→ 18 Mb/s
→ 36 Mb/s
→ 54 Mb/s

E os débitos adicionais (*Extended Supported Rates*) são:
→ 6 Mb/s
→ 12 Mb/s
→ 24 Mb/s
→ 48 Mb/s

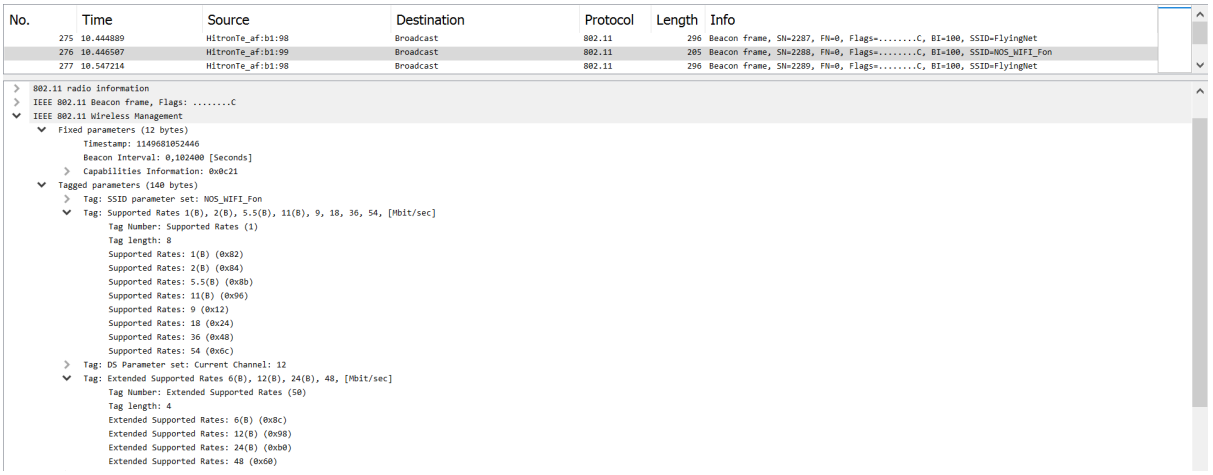


Figura 3: Débitos suportados pelo AP

7. 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.

   R: Na figura 3 verifica-se que o intervalo de tempo entre tramas consecutivas é igual a 0,102400 segundos (*Beacon Interval*). Mas visto que às vezes a AP pode não estar disponível para outra trama, vai haver tempo de espera que vai fazer com que este valor indicado de tempo não seja muito preciso.

8. 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).

   R: Os SSIDs existentes nesta captura são *NOS_WIFI_Fon* e *FlyingNet*. Esta informação foi obtida através da observação do campo *Info* na *Beacon Frame* número 276 e, sendo apenas observados estes dois SSIDs referidos, é garantido que são os únicos que existem neste exercício.

9. Verifique se está a ser usado o método de deteção de erros (CRC).
   Sugestão: Use o filtro: (wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad) Que conclui? Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

   R: Aplicando o filtro *(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)* observamos que não é visível nenhuma informação, ver figura 4.

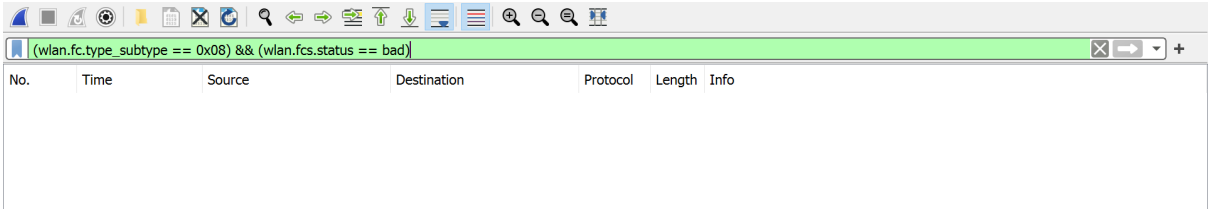


Figura 4: Aplicação do filtro sugerido

Verificando apenas com o filtro *(wlan.fc.type_subtype == 0x08)* concluímos que a deteção dos erros não está a ser verificada, isto pode ser confirmado no campo *FC Status* que está como *unverified,* tal como apresentado na figura 5.

Assim sendo, não está a ser usado um método de detecção de erros.

A necessidade dum método deste tipo passa pela possível existência de colisões e eventuais perturbações nas tramas relativas a estas redes.

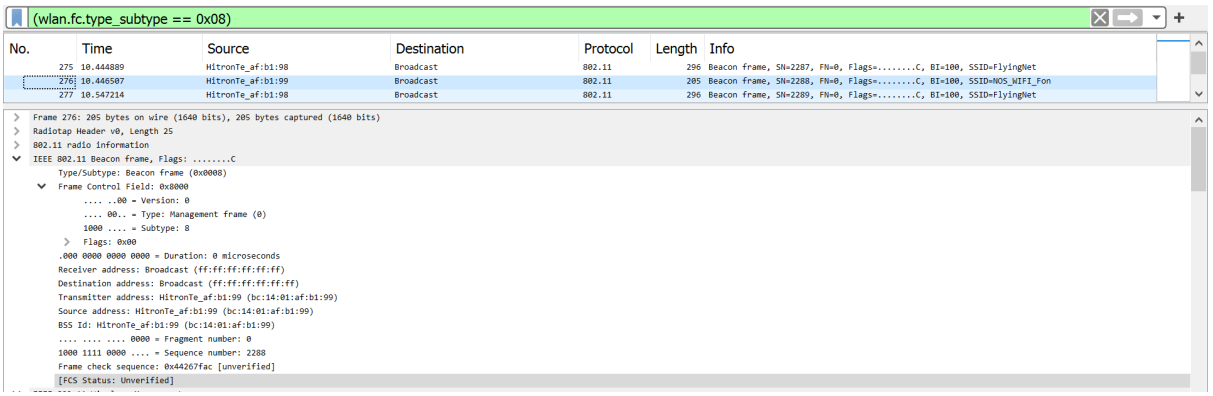


Figura 5: Aplicação do filtro

No trace disponibilizado foi também registado scanning ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.

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

    R: Convertendo os valores binários da tabela no enunciado, verificamos que o filtro a ser aplicado é *(wlan.fc.type_subtype == 0x04)* ||

(wlan.fc.type_subtype == 0x05). Os valores 0x04 e 0x05 correspondem ao *Probe request* e *Probe response*, respetivamente.

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?

    R: O *Probe request* é enviado através de um endereço MAC *Broadcast*, ou seja, para a sua vizinhança e é o *Probe response* que o vai receber. É o *Probe response* que "responde" ao pedido efetuado através do MAC da origem inicial.

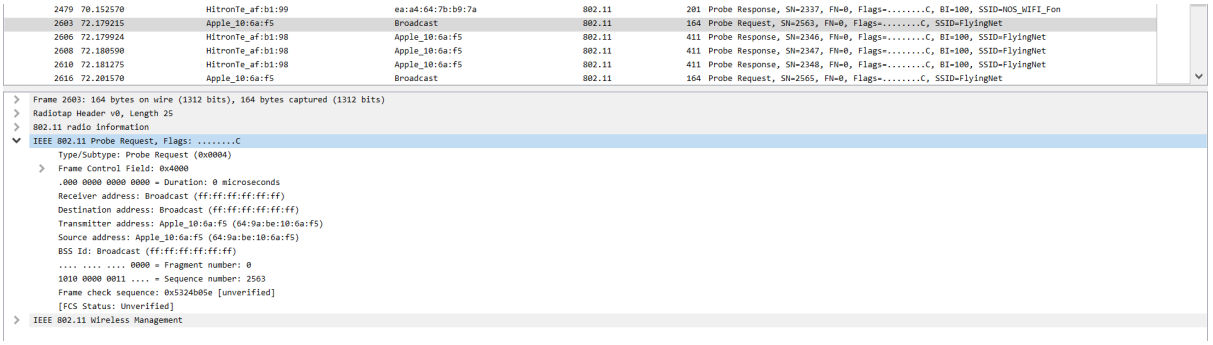


Figura 6: *Probe request*

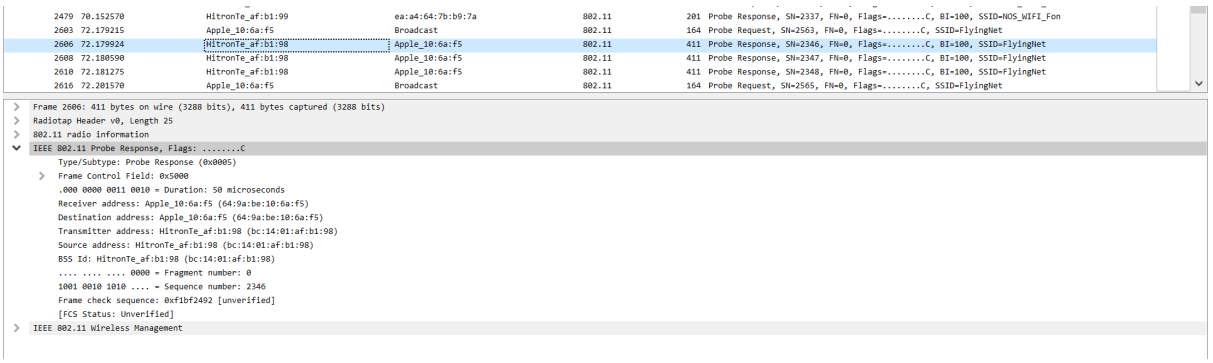


Figura 7: *Probe response* respetivo

Processo de Associação

Numa rede Wi-Fi 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.

    R: Para ter acesso a estas tramas foram necessários os filtros do tipo *Management* disponíveis no anexo. Recorremos ao subtipo *Authentication*, *Association Request* e *Association Response* que correspondem respetivamente a *(wlan.fc.type_subtype == 11 || wlan.fc.type_subtype == 0 || wlan.fc.type_subtype == 1).*

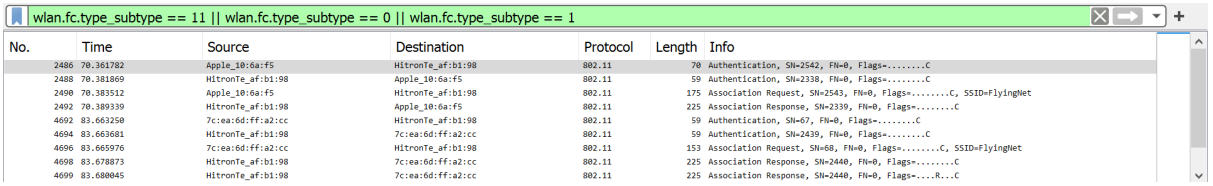
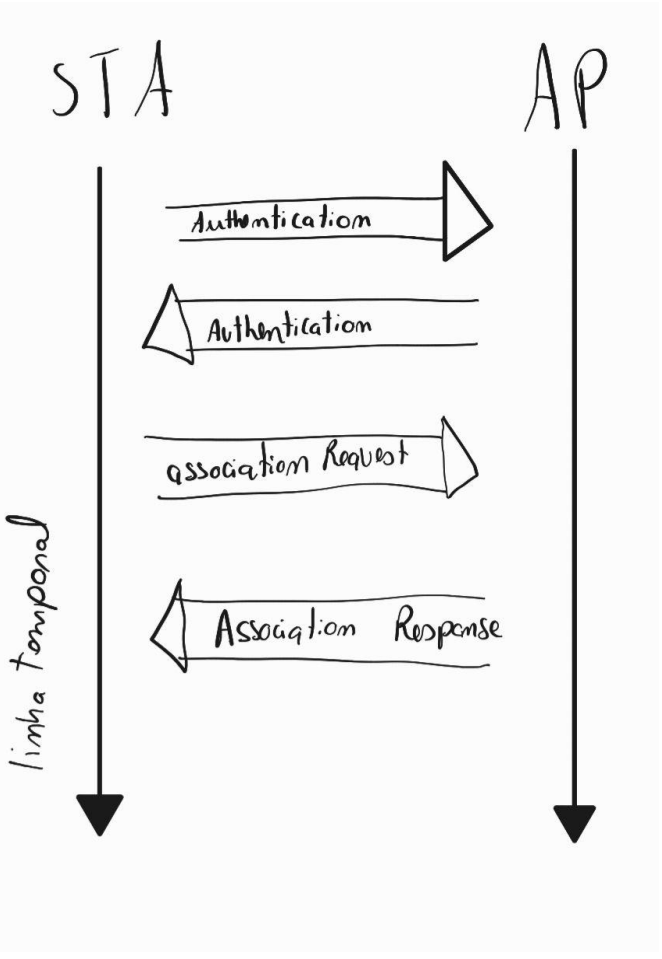


Figura 8: Tramas correspondentes ao filtro indicado

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

    R: Aqui é apresentado o processo completo de associação entre uma STA e um AP.



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.

14. Considere a trama de dados nº431. 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?

    R: Na figura 9 podemos ver a direcionalidade (pela *flag* DS) que a trama de dados nº431 tem, ou seja, não vai para fora (To DS:0) e vem de fora(From DS:1). A trama não é local a WLAN pois vem de fora.

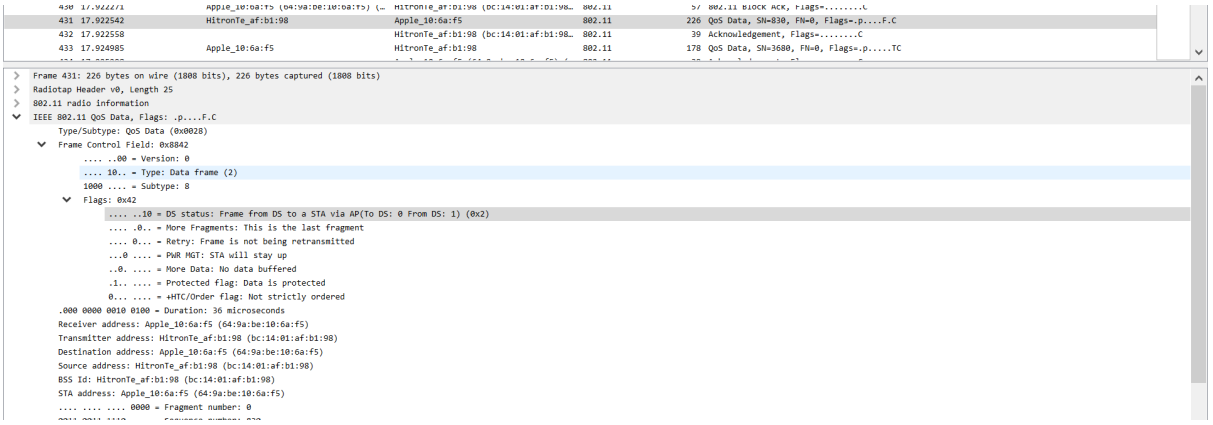


Figura 9: Trama de dados nº431

15. Para a trama de dados no 431, 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?

    R: Na figura 9 podemos observar os endereços MAC em uso:

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

    Transmitter address: bc:14:01:af:b1:98 - (Endereço AP)

    Destination address: 64:9a:be:10:6a:f5 - (Endereço do router de acesso)

16. Como interpreta a trama nº433 face à sua direcionalidade e endereçamento MAC?

    R: Tendo em atenção a direcionalidade verificou-se através da análise das flags *To DS: 1 From DS: 0*, que a trama vem do STA para o DS.

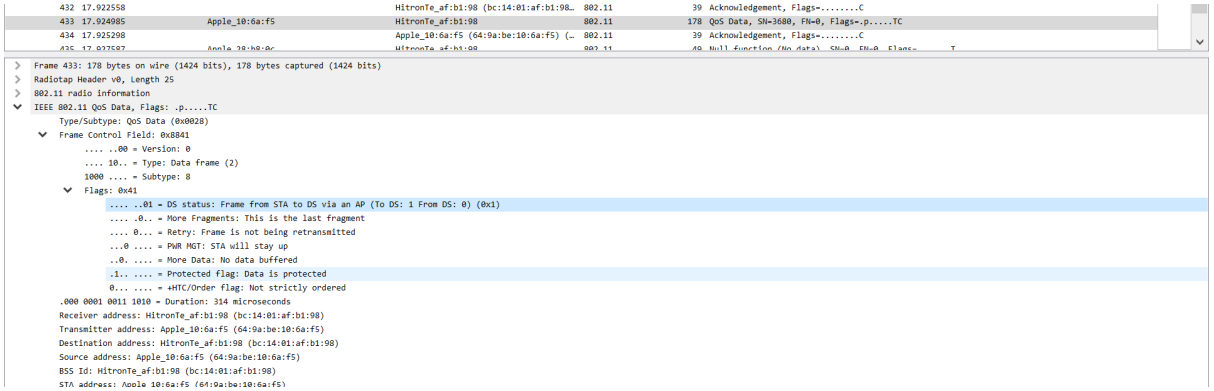
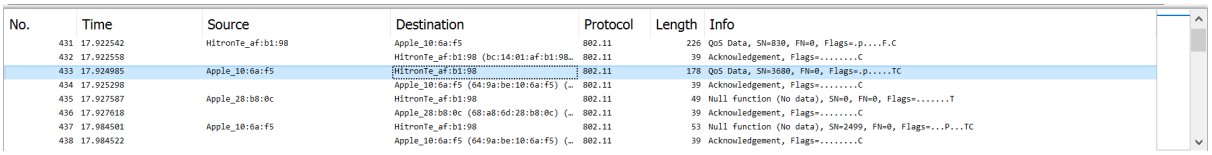


Figura 10: Trama de dados nº433

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.)

    R: Na transferência de dados são enviadas tramas de controlo do tipo *Acknowledgment.* Numa rede sem fios, para termos uma verificação que o *router* recebeu a mensagem, vai ser enviada esta última trama referida. No entanto, numa rede *Ethernet* não era necessário esta mensagem de confirmação.

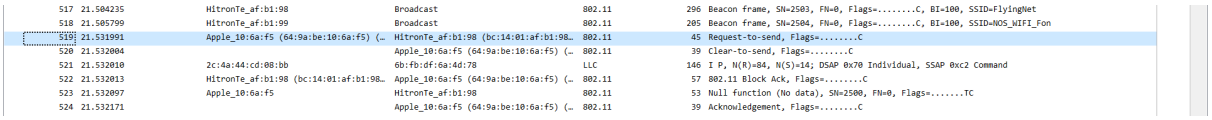


No.	Time	Source	Destination	Protocol	Length	Info
431	17.922542	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	226	QoS Data, SN=830, FN=0, Flags=.p....F.C
432	17.922558		HitronTe_af:b1:98 (bc:14:01:af:b1:98…	802.11	39	Acknowledgement, Flags=.....C
433	17.924985	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	178	QoS Data, SN=3680, FN=0, Flags=.p.....TC
434	17.925298		Apple_10:6a:f5 (64:9a:be:10:6a:f5) (…	802.11	39	Acknowledgement, Flags=.....C
435	17.927587	Apple_28:b8:0c	HitronTe_af:b1:98	802.11	49	Null function (No data), SN=0, FN=0, Flags=.....T
436	17.927618		Apple_28:b8:0c (68:a8:6d:28:b8:0c) (…	802.11	39	Acknowledgement, Flags=.....C
437	17.984501	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2499, FN=0, Flags=...P...TC
438	17.984522		Apple_10:6a:f5 (64:9a:be:10:6a:f5) (…	802.11	39	Acknowledgement, Flags=.....C

Figura 11: Trama de Controlo *Acknowledgment*

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 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.

    R: No exemplo acima, da figura 11, não está a ser usada a opção RTS/CTS. Já na figura 12 pode-se verificar exatamente o contrário.



517	21.504235	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=2503, FN=0, Flags=........C, BI=100, SSID=FlyingNet
518	21.505799	HitronTe_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2504, FN=0, Flags=........C, BI=100, SSID=NOS_WIFI_Fon
519	21.531991	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (…	HitronTe_af:b1:98 (bc:14:01:af:b1:98…	802.11	45	Request-to-send, Flags=........C
520	21.532004		Apple_10:6a:f5 (64:9a:be:10:6a:f5) (…	802.11	39	Clear-to-send, Flags=........C
521	21.532010	2c:4a:44:cd:08:bb	6b:fb:df:6a:4d:78	LLC	146	I P, N(R)=84, N(S)=14; DSAP 0x70 Individual, SSAP 0xc2 Command
522	21.532013	HitronTe_af:b1:98 (bc:14:01:af:b1:98…	Apple_10:6a:f5 (64:9a:be:10:6a:f5) (…	802.11	57	802.11 Block Ack, Flags=........C
523	21.532097	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2500, FN=0, Flags=.......TC
524	21.532171		Apple_10:6a:f5 (64:9a:be:10:6a:f5) (…	802.11	39	Acknowledgement, Flags=........C

Figura 12: Trama com a opção RTS/CTS

Conclusão

Neste trabalho prático foi possível explorar o conhecimento das redes sem fios, mais especificamente, as redes Wi-Fi.

Desenvolveram-se conceitos mencionados nos trabalhos práticos anteriores e apresentados nas aulas teóricas que são bastante relevantes para o objetivo final de aprendizagem desta UC.

Neste exercício não foram sentidas muitas dificuldades e o sentimento em comum de grupo é que os conceitos foram bem interiorizados.