Redes sem Fios (Wi-Fi)

Filipa Rebelo and Joana Oliveira

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
email: {a90234,a87956}@alunos.uminho.pt

1 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 XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

1.1 Exercício 1

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

Através da Figura 1 verifica-se que a frequência do espetro é 2467MHz e que o canal correspondente é 12.

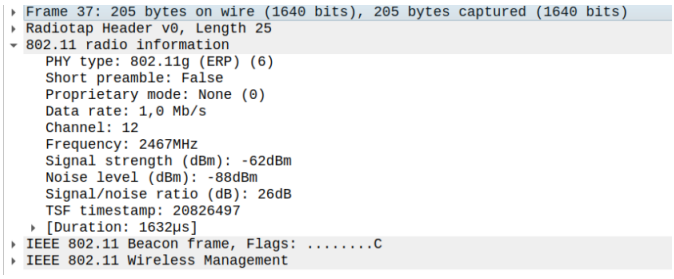

Fig. 1. Trama 802.11

1.2 Exercício 2

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

A versão que está a ser utilizada é a 802.11g, tal como observado no campo *PHY type* da Figura 1.

1.3 Exercício 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.

O valor correspondente ao débito de envio da trama escolhida encontra-se no campo *Data Rate* e tem o valor de 1,0 Mb/s. Este valor é inferior a 54.0 Mb/s, que corresponde ao débito máximo permitido pela norma IEE 802.11g.

2 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:

2.1 Exercício 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)?

O tipo e subtipo da trama estão contidos nos campos *Type* e *Subtype* do *Frame Control Field* e têm, respetivamente, os valores 0 e 8.

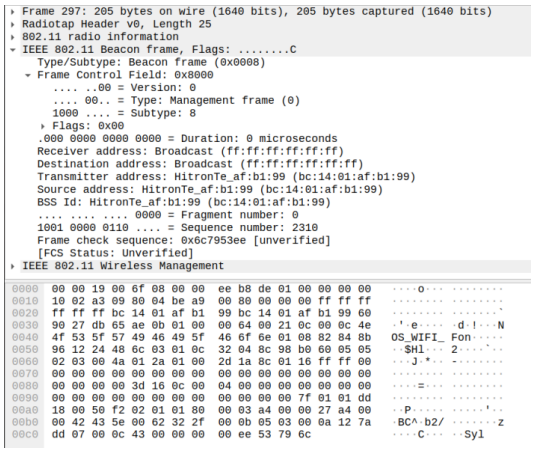

Fig. 2. Trama 802.11

Observando a seguinte entrada da tabela fornecida no enunciado, é possível concluir que se trata de uma trama do tipo Management (00) e do subtipo Beacon (1000).

00	Management	1000	Beacon

Fig. 3. Entrada da tabela fornecida no enunciado

2.2 Exercício 5

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

Receiver address: ff:ff:ff:ff:ff:ff
Destination address: ff:ff:ff:ff:ff:ff
Transmitter address: bc:14:01:af:b1:99
Source adress: bc:14:01:af:b1:99
É possível concluir que a origem da trama se trata de um *Access Point*, e que o endereço de destino (ff:ff:ff:ff:ff:ff) se trata de um endereço de *Broadcast*, o que significa que a trama é enviada para todos os hosts.

2.3 Exercício 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?

Tal como é possível observar na figura abaixo, os débitos de base são: 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. Os débitos adicionais são: 6 Mb/s, 12 Mb/s, 24 Mb/s, 48 Mb/s.

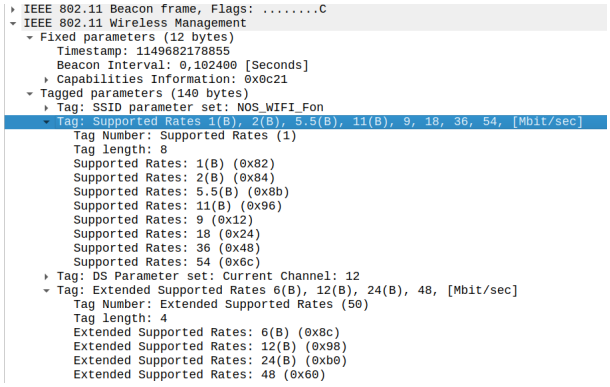

Fig. 4. Débitos de base e débitos adicionais

2.4 Exercício 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.

O intervalo de tempo previsto entre tramas beacon consecutivas encontra-se no campo *Beacon Interval* da Figura 5 e tem o valor de 0.102400 segundos. Observando o campo *Timestamp* de duas tramas beacon provenientes do mesmo AP e fazendo a sua subtração, $1149682383659 - 1149682281252 = 102407$, é possível perceber que o seu valor é ligeiramente superior ao teórico, devido à existência de colisões.

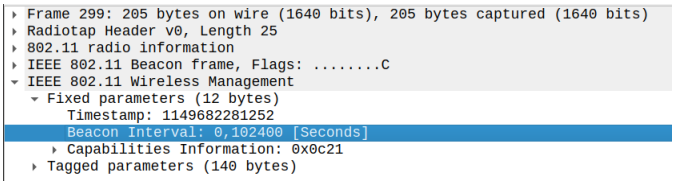

Fig. 5. Primeira trama capturada

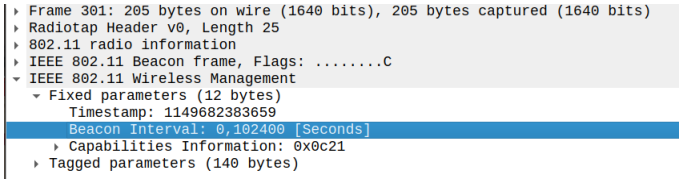

Fig. 6. Segunda trama capturada

2.5 Exercício 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).

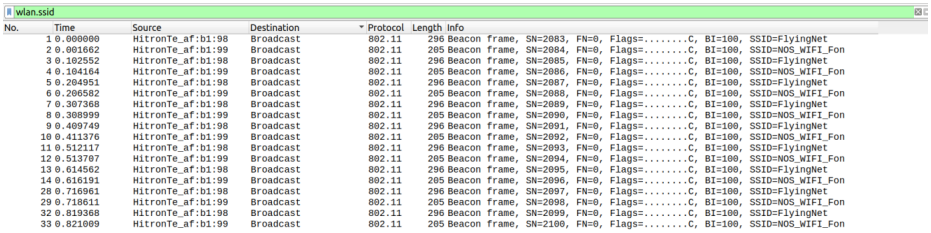

Fig. 7. Lista de SSIDs

Os SSIDs dos APs que estão a operar na vizinhança da STA de captura são o *FlyingNet* e o *NOS_WIFI_FON*. Para obter esta informação utilizamos então o filtro *wlan.ssid* e observamos o campo *Info*, sendo que apenas encontramos os SSIDs mencionados acima.

2.6 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.

Usando o filtro sugerido no enunciado, obtivemos 5 tramas com erros, tal como se vê na Figura 8. Isto prova a existência do campo *FCS Status*, o que significa que está a ser usado o método de deteção de erros (CRC).

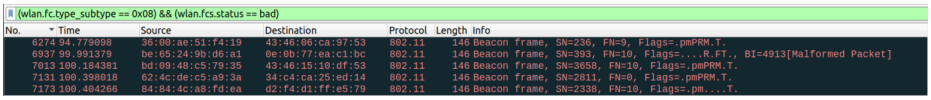

Fig. 8. Tramas Beacon com erros

O uso deste mecanismo é importante no sentido em que permite detetar qualquer tipo de interferência, corrompimento ou perda de informação no envio das tramas.

2.7 Exercício 10

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

Com o filtro *wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5* conseguimos então visualizar as tramas pedidas.

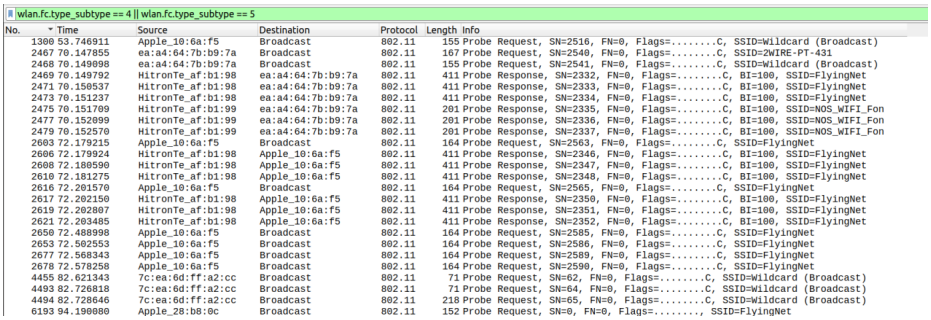

Fig. 9. Tramas Probing Request e Probing Response

De modo a sabermos os valores relativos a cada subtipo de trama consultamos a tabela fornecida no enunciado e observamos os seguintes valores.

00	Management	0100	Probe request
00	Management	0101	Probe response

Fig. 10. Excerto da tabela dada no enunciado

2.8 Exercício 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?

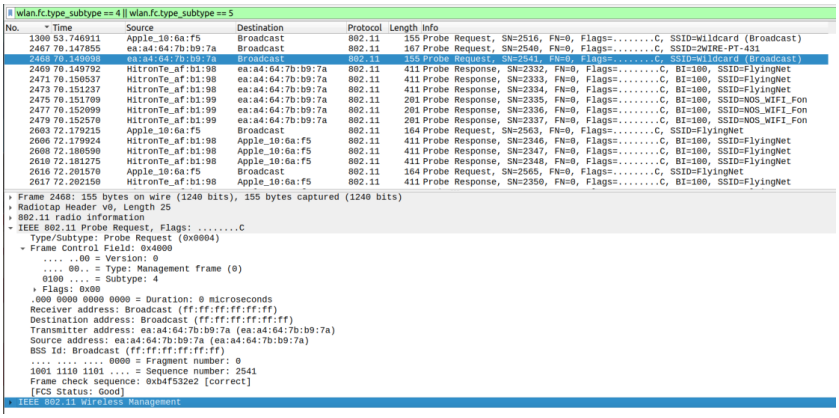

Fig. 11. Probing Request

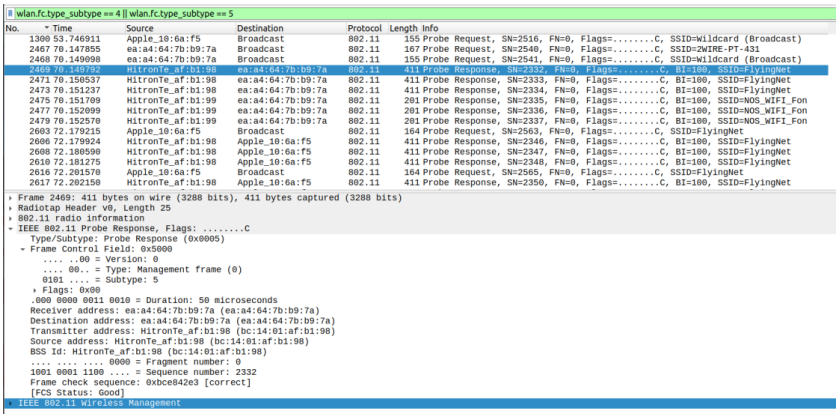

Fig. 12. Probing Response

O *Probing Request* é enviado para um endereço *Broadcast* e tem como objetivo receber informações relativamente a outros AP. O *Probing Response* responde ao pedido anterior com as informações do AP respetivo.

3 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.

3.1 Exercício 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.

Através do filtro presente na Figura 13 foi possível obter uma sequência de tramas que corresponde a um processo de associação completo entre STA e o AP, juntamente com a fase de autenticação.

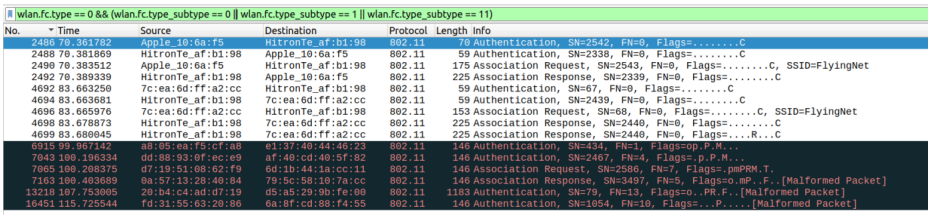

Fig. 13. Sequência de tramas correspondente a um processo de associação

3.2 Exercício 13

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

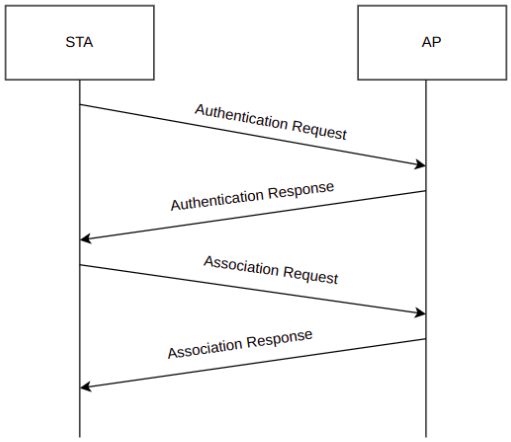

Fig. 14. Sequência de tramas trocadas no processo

4 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.

4.1 Exercício 14

Considere a trama de dados nº431. 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?

Através da observação da flag *DS status*, contida no campo *Frame Control*, é possível verificar que o valor de *to DS* é 0 e o valor de *from DS* é 1. Isto significa que a trama vem do DS para o STA, ou seja, não é local à WLAN.

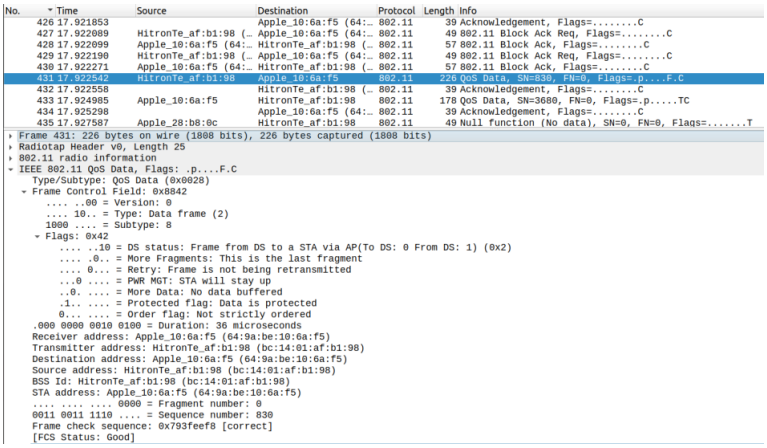

Fig. 15. Trama de dados n.º431

4.2 Exercício 15

Para a trama de dados nº431, 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?

Observando mais uma vez a Figura 15 é possível concluir que os endereços MAC em uso são:
STA (Receiver Adress): 64:9a:be:10:6a:f5
AP (Transmitter Adress): bc:14:01:af:b1:98
Router de Acesso (Destination Adress): 64:9a:be:10:6a:f5

4.3 Exercício 16

Como interpreta a trama nº433 face à sua direccionalidade e endereçamento MAC?

Uma vez que os valores contidos na flag *DS status* são de 1 no *to DS* e de 0 no *from DS*, é possível concluir que a trama vai do STA para o DS.
Relativamente aos endereços MAC é possível ver que que o *Receiver adress* e *Destination adress* são iguais, bem como o *Transmitter adress* e o *Source adress*.
Uma vez que o *Receiver Adress* se refere ao recetor imediato do pacote, isto significa que este é enviado diretamente para o seu destino, sem necessidade de recorrer a pontos intermédios.

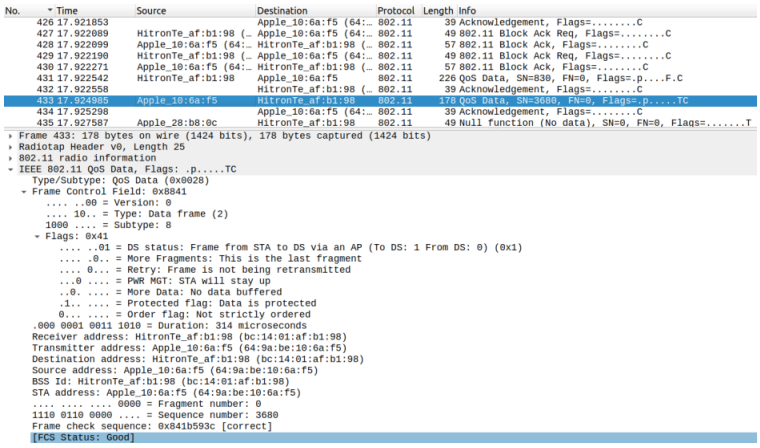

Fig. 16. Trama de dados n.º433

4.4 Exercício 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.)

O subtipo de tramas de controlo que são transmitidas é Acknowledgement (ACK). Estas tramas permitem indicar que a transmissão foi efetuada com sucesso e que as tramas foram recebidas corretamente e são necessárias devido à suscetibilidade para erros que as redes Wi-Fi possuem.

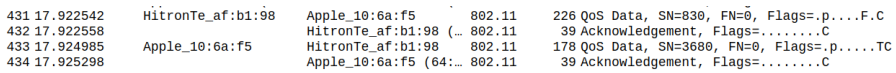

Fig. 17. Tramas de Controlo

4.5 Exercício 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. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

No exemplo acima não está a ser usada a opção RTS/CTS. No entanto, é possível verificar a sua utilização no exemplo apresentado na figura seguinte.

670	25.295262	HitronTe_af:b1:98 (…	Apple_10:6a:f5 (64:…	802.11	45	Request-to-send, Flags=........C
671	25.295267		HitronTe_af:b1:98 (…	802.11	39	Clear-to-send, Flags=........C
672	25.295335	HitronTe_af:b1:96	Apple_10:6a:f5	802.11	146	QoS Data, SN=841, FN=0, Flags=.p....F.C
673	25.295413	Apple_10:6a:f5 (64:…	HitronTe_af:b1:98 (…	802.11	57	802.11 Block Ack, Flags=........C
674	25.311730	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	53	Null function (No data), SN=2505, FN=0, Flags=...P...TC
675	25.311751		Apple_10:6a:f5 (64:…	802.11	39	Acknowledgement, Flags=........C

Fig. 18. Exemplo de utilização da opção RTC/CTS

5 Conclusão

A realização deste trabalho prático permitiu-nos consolidar alguns dos conhecimentos abordados nas aulas teóricas relativamente às redes sem fios.
No que diz respeito à ferramenta *Wireshark*, esta foi utilizada com o recurso a filtros de pesquisa, elaborados por nós, e que nos permitiram obter respostas mais facilmente.
Foram ainda analisadas diversas tramas e identificados os seus tipos e subtipos, bem como a sua direcionalidade.
Em conclusão, acreditamos ter obtido o aproveitamento esperado na realização deste trabalho e também conhecimentos importantes relativos ao tema do mesmo.