

Universidade do Minho

Departamento de Informática

TP4 - Redes Sem Fios (802.11)

Redes de Computadores

Grupo 37

Catarina Pais Vieira (a89524)

José Duarte Pereira de Castro Alves (a89563)

Leonardo de Freitas Marreiros (a89537)

**Conteúdo**

[**Questões e Respostas** 3](#_Toc60257270)

[**4. Acesso Rádio** 3](#_Toc60257271)

[**Exercício 1** 3](#_Toc60257272)

[**Exercício 2** 3](#_Toc60257273)

[**Exercício 3** 3](#_Toc60257274)

[**5. *Scanning* Passivo e *Scanning* Ativo** 3](#_Toc60257275)

[**Exercício 4** 3](#_Toc60257276)

[**Exercício 5** 4](#_Toc60257277)

[**Exercício 6** 5](#_Toc60257278)

[**Exercício 7** 5](#_Toc60257279)

[**Exercício 8** 6](#_Toc60257280)

[**Exercício 9** 6](#_Toc60257281)

[**Exercício 10** 7](#_Toc60257282)

[**Exercício 11** 7](#_Toc60257283)

[**6. Processo de Associação** 8](#_Toc60257284)

[**Exercício 12** 8](#_Toc60257285)

[**Exercício 13** 8](#_Toc60257286)

[**7. Transferência de Dados** 9](#_Toc60257287)

[**Exercício 14** 9](#_Toc60257288)

[**Exercício 15** 9](#_Toc60257289)

[**Exercício 16** 9](#_Toc60257290)

[**Exercício 17** 10](#_Toc60257291)

[**Exercício 18** 10](#_Toc60257292)

[**Conclusão** 11](#_Toc60257293)

# **Questões e Respostas**

## **4. Acesso Rádio**

Figura 1 - Trama 337

### **Exercício 1**

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

Frequência: 2467MHz.

Canal: 12.

### **Exercício 2**

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

A versão da norma que está a ser usada é 802.11g (PHY type).

### **Exercício 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 verificar o débito a que foi enviada a trama no campo “Data rate” que mostra um valor de 1,0 Mb/s. O débito máximo da norma IEEE 802.11g corresponde a 54 Mb/s pelo que não foi enviada com o débito máximo possível. Isto acontece de forma a garantir que seja enviada a todos os *hosts*, para isso utilizando o menor débito possível.

## **5. *Scanning* Passivo e *Scanning* Ativo**

### **Exercício 4**

Selecione uma trama *beacon* (e.g., trama 10XX). 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)?

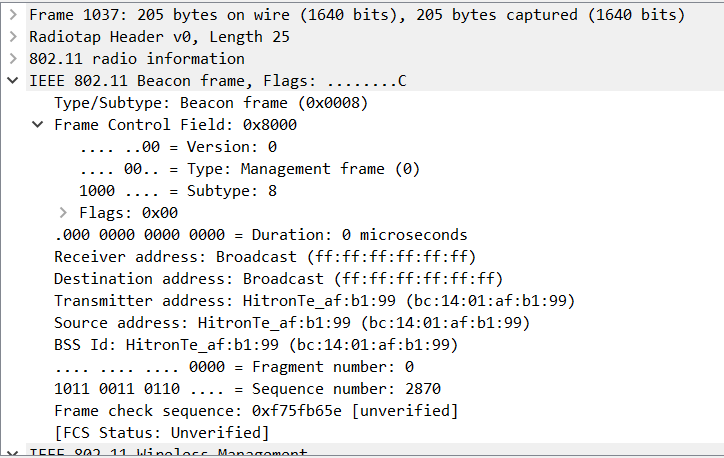
A trama pertence ao tipo Management que tem tipo 00 e subtipo 1000. Estão especificadas no campo “Frame Control Field”.

Figura 2 - Trama 1037

### **Exercício 5**

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

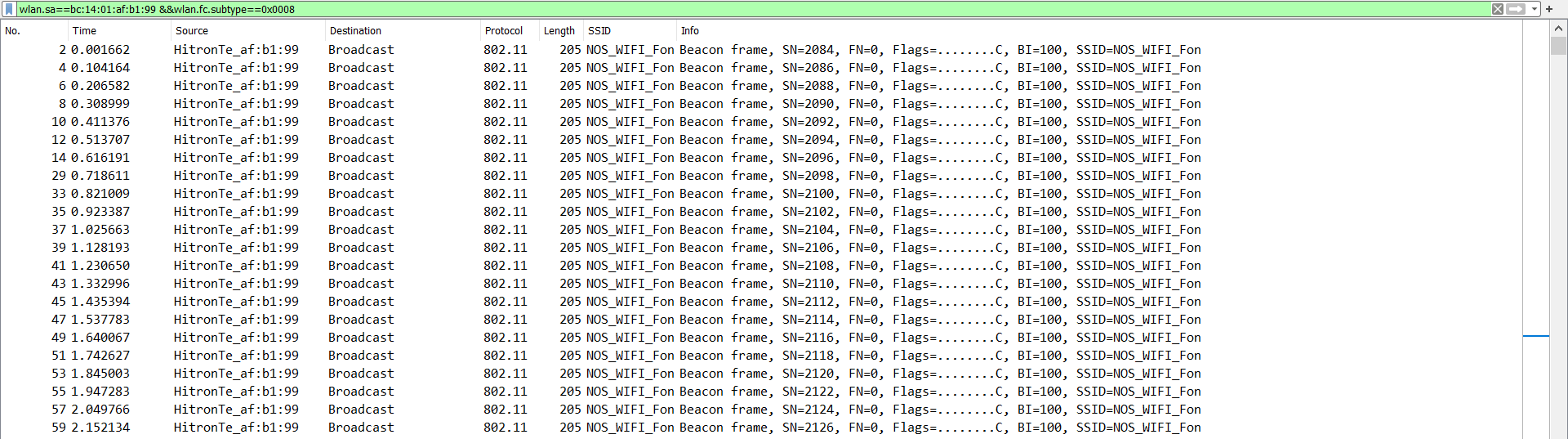
O endereço MAC de origem é bc:14:01:af:b1:99 e de destino é ff:ff:ff:ff:ff:ff. Para identificar os endereços MAC em uso utilizamos o filtro: “wlan.sa== bc:14:01:af:b1:99 && wlan.fc.subtype == 0x0008” (Figura 3) e analisamos as *Conversations* com a opção “Limit to display filter” ativada para mostrar apenas o endereço MAC pretendido. O resultado encontra-se na Figura 4.

Figura 3 - Resultado do filtro utilizado

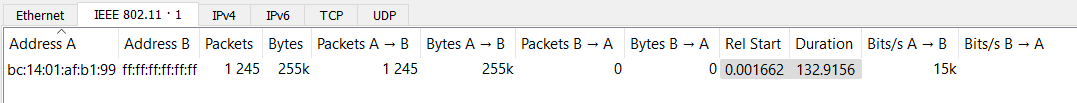


Figura 4 - Conversations

### **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?

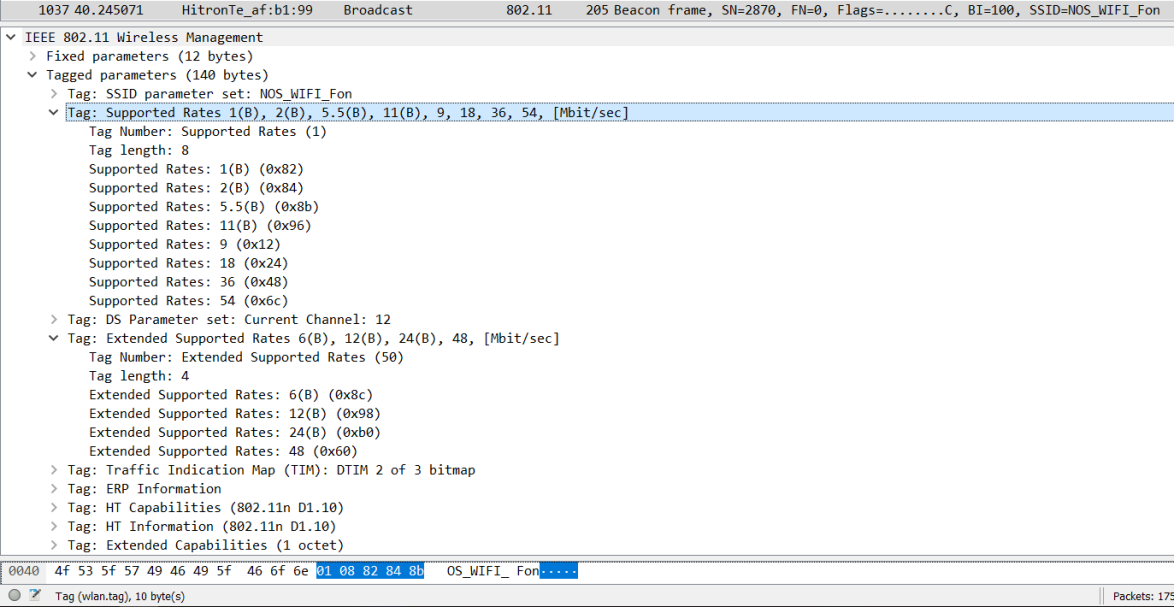


Figura - Supported Rates e Extended Supported Rates

### **Exercício 7**

Qual 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 provenientes do mesmo AP é verificada? Tente explicar porquê.

O intervalo de tempo previsto entre tramas beacon é igual para os dois AP’s e igual a 0.1024s.

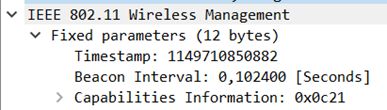


Figura 6 - Beacon Interval

Na prática o intervalo de tempo previsto não se verifica. Isto acontece, pois, se o meio estiver ocupado no TBTT (Target Beacon Transmission Time), o ponto de acesso precisa de disputar o acesso normalmente e a transmissão pode não ocorrer exatamente em 0.1024s desde a última transmissão de beacon.

### **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).

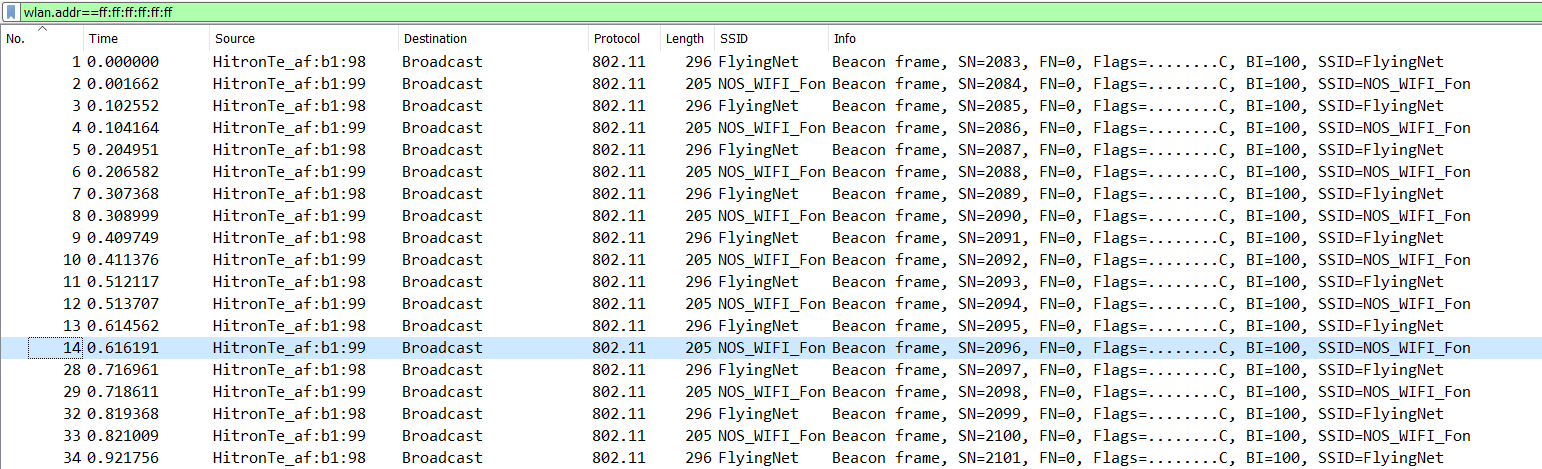
Utilizamos um filtro de visualização onde adicionamos uma coluna referente aos SSIDs: “wlan.addr==ff:ff:ff:ff:ff:ff”. Sendo assim os SSIDs são: FlyingNet e NOS\_WIFI\_Fon.

Figura 7 - SSIDs

### **Exercício 9**

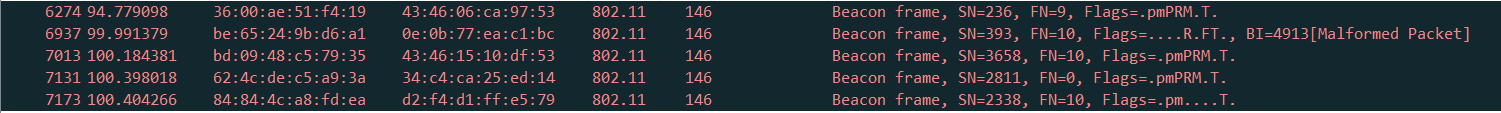
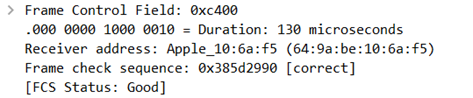
Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Use o filtro: (wlan.fc.type\_subtype == 0x08) && (wlan.fcs.status == bad). Que conclui? Justifique o porquê de usar deteção de erros em redes sem fios.

Figura 8 - Resultado do filtro

Nem todas as tramas foram recebidas corretamente (Figura 8) e está a ser utilizado o método de deteção de erros CRC. A deteção de erros é necessária porque o tipo de rede local representa uma rede Wi-Fi, e a probabilidade de haver erros nestas redes é alta, o que implica que seja utilizado um campo que verifique se as tramas de Beacon são recebidas corretamente ou não.



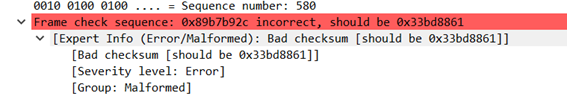
Figura - Trama recebida corretamente

Figura - Trama recebida incorretamente

Como podemos ver na Figura 9, a trama foi recebida corretamente, enquanto que a trama da Figura 10 foi recebida incorretamente.

### **Exercício 10**

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

O filtro utilizado foi “(wlan.fc.type\_subtype == 0x04) || (wlan.fc.type\_subtype == 0x05)”.

### **Exercício 11**

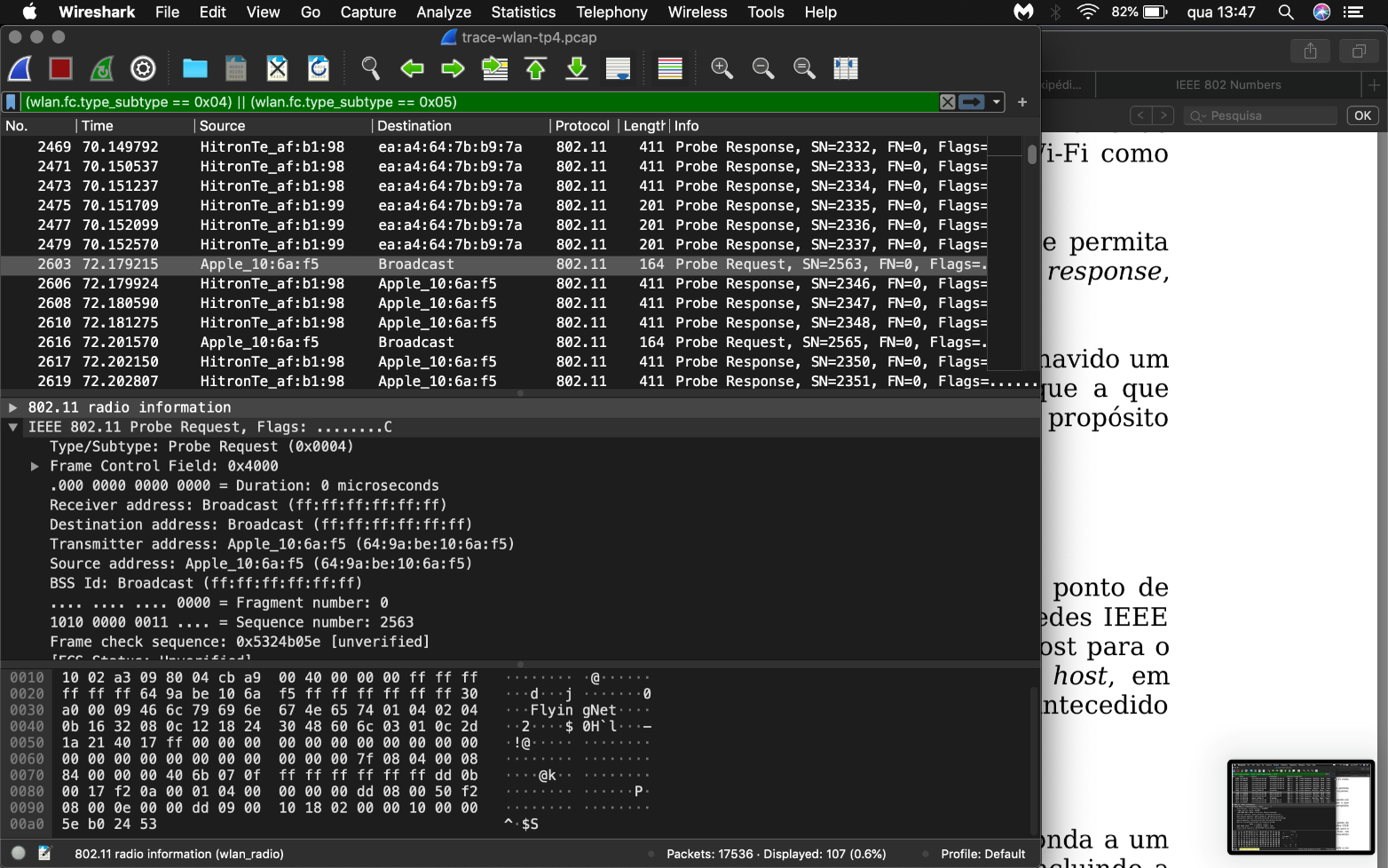
Identifique um *probing reques*t para o qual tenha havido um *probing response*. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

Figura 11 - Probe Request

A trama *probing request* tem origem no sistema de endereço 64:9a:be:10:6a:f5 que corresponde a uma STA (estação) e tem como destino qualquer AP (ponto de acesso) no seu alcance (endereço ff:ff:ff:ff:ff:ff). Esta trama é usada para a STA pedir informação dos APs no seu alcance (*active* *scanning*). A trama *probing* *response* tem como origem o AP de endereço bc:14:01:af:b1:98 e destino a STA de endereço 64:9a:be:10:6a:f5. Esta trama contém as informações do AP e vai ser recebida pela STA que fez o *probe* *request*.

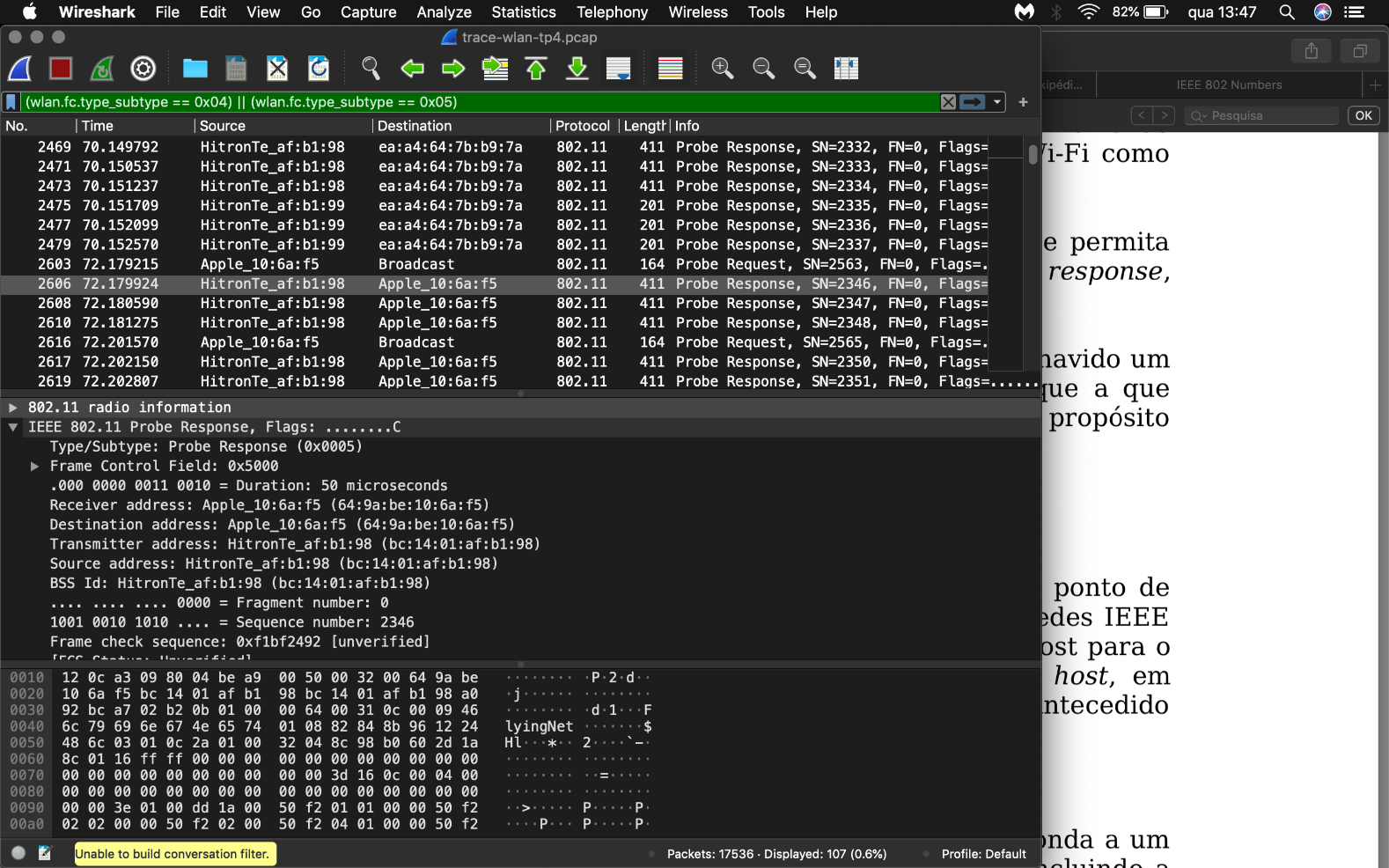


Figura 12 - Probe Response

## **6. Processo de Associação**

### **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.

Para o efeito foi utilizado o filtro “(wlan.fc.type\_subtype == 0x0) | | (wlan.fc.type\_subtype == 0x1) | | (wlan.fc.type\_subtype == 0xB)” cujo resultado pode ser visto na Figura 13.

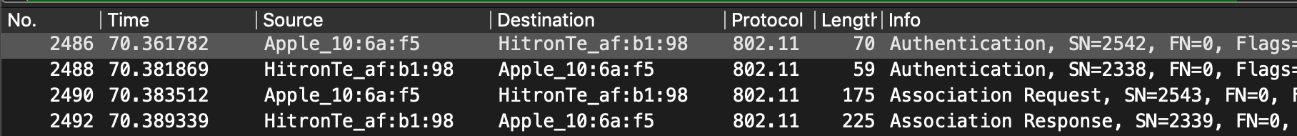


Figura 13 - fase de autenticação

### **Exercício 13**

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

70.361782 |-- authentication ---------> |

70.381869 |<- authentication ---------- |

STA | | AP

70.383512 |-- Association request --->|

70.389339 |<- Association response --|

## **7. Transferência de Dados**

### **Exercício 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?

Através da flag DS status pode-se concluir que a trama está a ir do DS (sistema de distribuição) para STA através do AP.

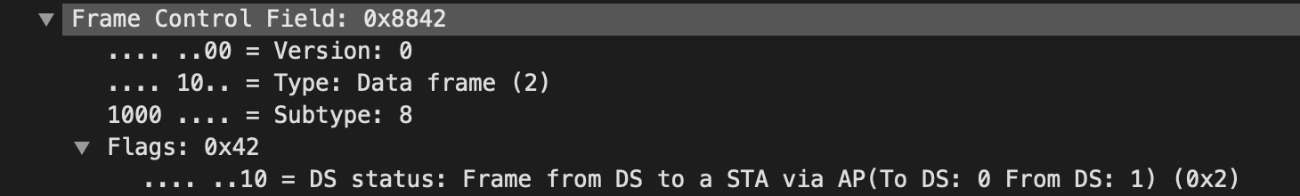


Figura 14 - Trama 455

### **Exercício 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?

Na questão anterior verificamos a direccionalidade da trama e, em relação ao datagrama da trama, a correspondência dos endereços MAC é a seguinte:

1. Destination
2. BSSID
3. Source

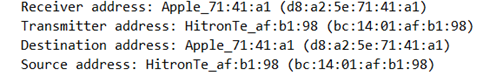
Podemos verificar os valores dos endereços MAC na Figura 15.

Figura 15 - Endereços MAC trama 455

### **Exercício 16**

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

Na trama nº457 através da flag DS status pode-se concluir que a trama está a ir do STA para o DS (sistema de distribuição) através do AP, como mostra a Figura 16. Com isto podemos concluir que o pacote está a sair do ambiente wireless, dirigindo-se para um computador na rede do centro de distribuição. Em relação aos endereços MAC na frame, a correspondência será a seguinte:

1. BSSID
2. Origem
3. Destino

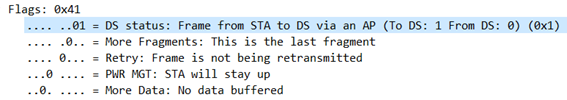


Figura 16 - Trama 457

### **Exercício 17**

Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar por que razão têm de existir (contrariamente ao que acontece numa rede Ethernet.)

Os subtipos das tramas de controlo transmitidas são *acknowledgment* (Figura 17). Como a rede wi-fi tem mais probabilidade de falhar, então são enviadas tramas de controlo que têm como objetivo enviar uma confirmação de que as tramas enviadas foram corretamente recebidas.

Figura 17 - subtipos das tramas

### **Exercício 18**

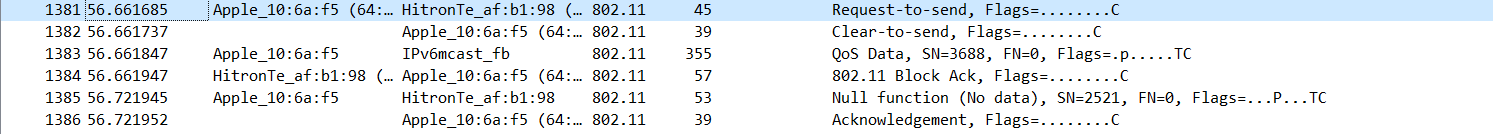
O uso de tramas *Request To Send* e *Clear To Send*, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está 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.

Figura 18 - tramas RTS e CTS

No caso anterior verificamos que não existem estes tipos de tramas. Mas na Figura 18 podemos verificar o uso de tramas *Request To Send* e *Clear To Send*

# **Conclusão**

Com este trabalho, foram colocados em prática conhecimentos referentes ao capítulo *Wireless LANs* adquiridos durante as aulas teóricas anteriores, o que nos levou a consolidar melhor a matéria.

Com a ajuda do Wireshark aprofundamos tópicos como acesso rápido, scanning, processo de associação e transferência de dados. Foram aplicados conceitos como tipos e subtipos de tramas, STA, AP e direcionalidade de tramas.

Uma parte que consideramos interessante neste trabalho foi a filtragem de dados no Wireshark que não seria possível sem a pesquisa em fontes webgráficas que nos permitiu encontrar os filtros adequados e ideais para resolver os exercícios.

Com este trabalho prático abordamos melhor as Redes Wireless mais concretamente o funcionamento das redes wi-fi ao nível da rede.

Assim, podemos afirmar que este trabalho nos permitiu ter um conhecimento mais abrangente sobre esta matéria, que nos pode vir a ser útil futuramente.