



Redes de Computadores  
(3<sup>o</sup> ano LEI)

## **Trabalho Prático 4**

### Relatório de Desenvolvimento

Grupo 4

a93241 Francisco Reis Izquierdo  
a89526 Duarte Augusto Rodrigues Lucas  
a96277 Diogo Miguel Serra Silva

3 de Maio de 2022

## Conteúdo

<b>1</b>	<b>Acesso Rádio</b>	<b>3</b>
1.1	Pergunta 1 . . . . .	3
1.2	Resposta 1 . . . . .	3
1.3	Pergunta 2 . . . . .	3
1.4	Resposta 2 . . . . .	3
1.5	Pergunta 3 . . . . .	3
1.6	Resposta 3 . . . . .	4
<b>2</b>	<b>Scanning Passivo e Scanning Ativo</b>	<b>4</b>
2.1	Pergunta 4 . . . . .	4
2.2	Resposta 4 . . . . .	4
2.3	Pergunta 5 . . . . .	4
2.4	Resposta 5 . . . . .	5
2.5	Pergunta 6 . . . . .	5
2.6	Resposta 6 . . . . .	5
2.7	Pergunta 7 . . . . .	5
2.8	Resposta 7 . . . . .	5
2.9	Pergunta 8 . . . . .	6
2.10	Resposta 8 . . . . .	6
2.11	Pergunta 9 . . . . .	6
2.12	Resposta 9 . . . . .	7
2.13	Pergunta 10 . . . . .	7
2.14	Resposta 10 . . . . .	7
2.15	Pergunta 11 . . . . .	7
2.16	Resposta 11 . . . . .	7
<b>3</b>	<b>Processo de Associação</b>	<b>9</b>
3.1	Pergunta 12 . . . . .	9
3.2	Resposta 12 . . . . .	9
3.3	Pergunta 13 . . . . .	10
3.4	Resposta 13 . . . . .	10
<b>4</b>	<b>Transferência de Dados</b>	<b>11</b>
4.1	Pergunta 14 . . . . .	11
4.2	Resposta 14 . . . . .	11
4.3	Pergunta 15 . . . . .	11
4.4	Resposta 15 . . . . .	11
4.5	Pergunta 16 . . . . .	12
4.6	Resposta 16 . . . . .	12
4.7	Pergunta 17 . . . . .	13
4.8	Resposta 17 . . . . .	13
4.9	Pergunta 18 . . . . .	13
4.10	Resposta 18 . . . . .	14

## Listings

## Lista de Figuras

1	Trama 134 . . . . .	3
2	Trama 264 . . . . .	4
3	IEEE 802.11 Wireless Management . . . . .	6
4	Secção de captura. . . . .	6
5	Probe request. . . . .	7
6	Probe response. . . . .	8
7	Tramas de autenticação . . . . .	9
8	Sequência de tramas relativas ao processo de associação. . . . .	9
9	Sequência de tramas trocadas . . . . .	10
10	Frame Control da Trama 431. . . . .	11
11	IEEE 802.11 da Trama 431. . . . .	12
12	IEEE 802.11 da Trama 433. . . . .	13
13	RTS/CTS. . . . .	14

# 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).

```
▸ Frame 134: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▸ Radiotap Header v0, Length 25
▸ 802.11 radio information
  PHY type: 802.11g (ERP) (6)
  Short preamble: False
  Proprietary mode: None (0)
  Data rate: 1,0 Mb/s
  Channel: 12
  Frequency: 2467MHz
  Signal strength (dBm): -65dBm
  Noise level (dBm): -88dBm
  Signal/noise ratio (dB): 23dB
  TSF timestamp: 25022449
▸ [Duration: 2360µs]
```

Figura 1: Trama 134

## 1.1 Pergunta 1

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

## 1.2 Resposta 1

Ao analisar o cabeçalho da trama 134, através dos campos *Frequency* e *Channel* conseguimos perceber que a rede sem fios opera sobre a frequência 2467 MHz no canal 12.

## 1.3 Pergunta 2

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

## 1.4 Resposta 2

De forma alusiva, através do cabeçalho da trama 134, no campo *PHY type* conseguimos verificar que a norma *IEEE 802.11g* que está a ser usada corresponde à *802.11g*

## 1.5 Pergunta 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.

## 1.6 Resposta 3

Ao analisar o campo *Data rate*, vemos que o débito a que foi enviada é 1.0 Mb/s. Após analisar as especificações da versão que está a ser usada, vemos que o debito máximo corresponde a 54 Mb/s

## 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:

```
* Frame 264: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
* Radiotap Header v0, Length 25
* 802.11 radio information
- IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  Frame Control Field: 0x8000
    .... 0000 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
  - Flags: 0x000
    .... 0000 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
    .... 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 0000 0000 = Duration: 0 microseconds
  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  Transmitter address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
  Source address: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
  BSS Id: HitronTe_af:b1:99 (bc:14:01:af:b1:99)
  .... 0000 0000 = Fragment number: 0
  1000 1110 0100 .... = Sequence number: 2276
  Frame check sequence: 0x7fca2a6c [unverified]
  [FCS Status: Unverified]
```

Figura 2: Trama 264

### 2.1 Pergunta 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)?

### 2.2 Resposta 4

Ao analisar o campo *Frame Control Field* da trama 264, percebemos que pertence ao tipo *Management Frame* cujo identificador é o 0 e o subtipo é Beacon, cujo identificador é o 8.

### 2.3 Pergunta 5

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

## 2.4 Resposta 5

Pelo MAC destino (ff:ff:ff:ff:ff:ff), endereço de broadcast, concluímos que esta trama vai ser enviada para todos os dispositivos conectados ao *Access Point*(AP), isto implica que o MAC de origem seja do AP.

## 2.5 Pergunta 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?

## 2.6 Resposta 6

Os dados abaixo estão contidos na figura 3.

Os débitos suportados pela trama:

- 1 Mb/s (Básico)
- 2 Mb/s (Básico)
- 5.5 Mb/s (Básico)
- 11 Mb/s (Básico)

Débitos adicionais suportados:

- 9 Mb/s
- 18 Mb/s
- 36 Mb/s
- 54 Mb/s

## 2.7 Pergunta 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.

## 2.8 Resposta 7

O intervalo de tempo previsto entre tramas beacon consecutivas é de 0.102400 segundos (figura 3).

Na prática, a periodicidade entre tramas não se verifica. O fato do próprio AP, no momento ocupado por outra tarefa, não conseguir enviar uma trama beacon no tempo preciso.

- IEEE 802.11 Wireless Management
  - Fixed parameters (12 bytes)
    - Timestamp: 1149680438034
    - Beacon Interval: 0,102400 [Seconds]
    - Capabilities Information: 0x0c21
  - Tagged parameters (140 bytes)
    - Tag: SSID parameter set: NOS\_WIFI\_Fon
    - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    - Tag: DS Parameter set: Current Channel: 12
    - Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
    - Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
    - Tag: ERP Information
    - Tag: HT Capabilities (802.11n D1.10)
    - Tag: HT Information (802.11n D1.10)
    - Tag: Extended Capabilities (1 octet)
    - Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    - Tag: QBSS Load Element 802.11e CCA Version
    - Tag: Vendor Specific: Ralink Technology, Corp.

Figura 3: IEEE 802.11 Wireless Management

## 2.9 Pergunta 8

Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

## 2.10 Resposta 8

Os SSIDs dos APs que estão a operar na vizinhança da STA de captura são, NOS\_WIFI\_Fon e FlyingNet (figura 4). Para tal usamos o filtro *wlan.ssid*.

No.	Time	Source	Destination	Protocol	Length	Info
262	9.729775	Hitronte_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2274, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
263	9.839432	Hitronte_af:b1:99	Broadcast	802.11	206	Beacon frame, SN=2275, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
264	9.832034	Hitronte_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2276, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
265	9.932816	Hitronte_af:b1:99	Broadcast	802.11	206	Beacon frame, SN=2277, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
266	9.934460	Hitronte_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2278, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
267	10.035221	Hitronte_af:b1:99	Broadcast	802.11	206	Beacon frame, SN=2279, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
268	10.036839	Hitronte_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2280, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
269	10.137624	Hitronte_af:b1:99	Broadcast	802.11	206	Beacon frame, SN=2281, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
270	10.139252	Hitronte_af:b1:99	Broadcast	802.11	205	Beacon frame, SN=2282, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
271	10.240140	Hitronte_af:b1:99	Broadcast	802.11	206	Beacon frame, SN=2283, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 4: Secção de captura.

## 2.11 Pergunta 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.

## 2.12 Resposta 9

Ao aplicar o filtro (`wlan.fc.type_subtype == 0x08`) && (`wlan.fcs.status == bad`) não foram apresentadas nenhuma trama, assim concluímos que o CRC não está a ser usado.

Deteção de erros em redes sem fios é necessário para verificar se houve alguma trama que sofreu interferência, levando à mal formação de pacotes de dados.

## 2.13 Pergunta 10

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

## 2.14 Resposta 10

Filtro estabelecido, `wlan.fc.type_subtype == 0x04 || wlan.fc.type_subtype == 0x05`

## 2.15 Pergunta 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?

## 2.16 Resposta 11

A STA envia um *probe request* em *broadcast* para descobrir redes com protocolo 802.11.

O AP envia um *probe response* para a STA, com informações relativas ao AP.

wlan.fc.type_subtype == 0x04    wlan.fc.type_subtype == 0x05						
No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=ZWIRE-PT-431
2468	70.149792	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2547, FN=0, Flags=.....C, SSID=710Card (Broadcast)
2469	70.149792	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a 802.11	411	Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a 802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a 802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=FlyingNet	
2475	70.151709	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a 802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon	
2477	70.152099	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a 802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon	
2479	70.152570	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a 802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon	
* Frame 2468: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)						
Radiotap Header v0, Length 25						
802.11 radio information						
IEEE 802.11 Probe Request, Flags: .....C						
Type/Subtype: Probe Request (0x0004)						
Frame Control Field: 0x4000						
0000 0000 0000 0000 = Duration: 0 microseconds						
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)						
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)						
Transmitter address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)						
Source address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)						
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)						
..... 0000 = Fragment number: 0						
1001 1110 1101 ..... = Sequence number: 2541						
Frame check sequence: 0xb4f532e2 [unverified]						
[FCS Status: Unverified]						
IEEE 802.11 Wireless Management						

Figura 5: Probe request.



wlan.fc.type_subtype == 0x04    wlan.fc.type_subtype == 0x05						
No.	Time	Source	Destination	Protocol	Length	Info
1369	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, Flags=.....C, SSID=2WIRE-PT-431
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
2469	70.149702	MitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2471	70.150537	MitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2473	70.151237	MitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2475	70.151709	MitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2477	70.152099	MitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2336, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2479	70.152570	MitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
<ul style="list-style-type: none"> <li>Frame 2469: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits)</li> <li>Radiotap Header v0, Length 25</li> <li>802.11 radio information</li> <li>IEEE 802.11 Probe Response, Flags: .....C <ul style="list-style-type: none"> <li>Type/Subtype: Probe Response (0x0005)</li> <li>Frame Control Field: 0x5000 <ul style="list-style-type: none"> <li>.0000.0000.0011.0010 = Duration: 50 microseconds</li> <li>Receiver address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)</li> <li>Destination address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)</li> <li>Transmitter address: MitronTe_af:b1:98 (bc:14:01:af:b1:98)</li> <li>Source address: MitronTe_af:b1:98 (bc:14:01:af:b1:98)</li> <li>BSS Id: MitronTe_af:b1:98 (bc:14:01:af:b1:98)</li> <li>.... .... 0000 = Fragment number: 0</li> <li>1001.0001.1100 .... = Sequence number: 2332</li> <li>Frame check sequence: 0xbce842e3 [unverified]</li> <li>[FCS Status: Unverified]</li> </ul> </li> </ul> </li> <li>IEEE 802.11 Wireless Management</li> </ul>						

Figura 6: Probe response.

### 3 Processo de Associação

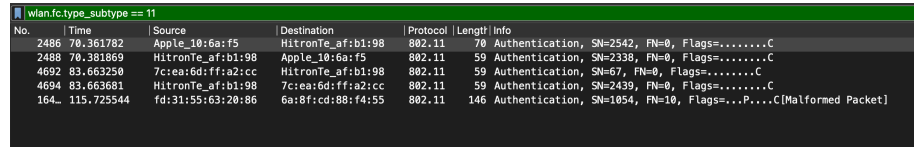
Numa rede Wi-Fi estruturada, um host deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para a sequência de tramas capturada:

#### 3.1 Pergunta 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.

#### 3.2 Resposta 12

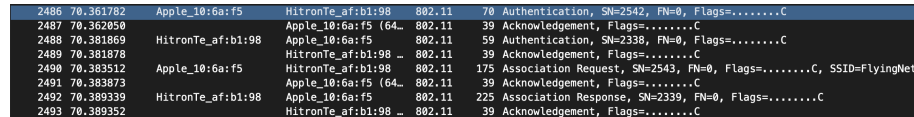
Utilizando o comando `wlan.fc.type_subtype == 11`, conseguimos filtrar apenas as tramas de autenticação:



No.	Time	Source	Destination	Protocol	Length	Info
2486	70.361782	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70	Authentication, SN=2542, FN=0, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, Flags=.....C
4692	83.663250	7c:ea:6d:ff:a2:cc	HitronTe_af:b1:98	802.11	59	Authentication, SN=67, FN=0, Flags=.....C
4694	83.663681	HitronTe_af:b1:98	7c:ea:6d:ff:a2:cc	802.11	59	Authentication, SN=2439, FN=0, Flags=.....C
164	115.725544	fd:31:55:63:20:86	6a:8f:cd:88:f4:55	802.11	146	Authentication, SN=1854, FN=10, Flags=...P....C[Malformed Packet]

Figura 7: Tramas de autenticação

Após a análise das tramas e retirando o filtro anteriormente mencionado, bastou irmos a uma das tramas e verificarmos a existência de troca de tramas entre a STA e o AP de modo a que se realize um processo de associação completo, onde se inclui 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
2487	70.362050	Apple_10:6a:f5 (64_	Apple_10:6a:f5 (64_	802.11	39	Acknowledgement, Flags=.....C
2488	70.381869	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59	Authentication, SN=2338, FN=0, Flags=.....C
2489	70.381878	HitronTe_af:b1:98	HitronTe_af:b1:98	802.11	39	Acknowledgement, Flags=.....C
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175	Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2491	70.383873	Apple_10:6a:f5 (64_	Apple_10:6a:f5 (64_	802.11	39	Acknowledgement, Flags=.....C
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C
2493	70.389352	HitronTe_af:b1:98	HitronTe_af:b1:98	802.11	39	Acknowledgement, Flags=.....C

Figura 8: Sequência de tramas relativas ao processo de associação.

### 3.3 Pergunta 13

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

### 3.4 Resposta 13

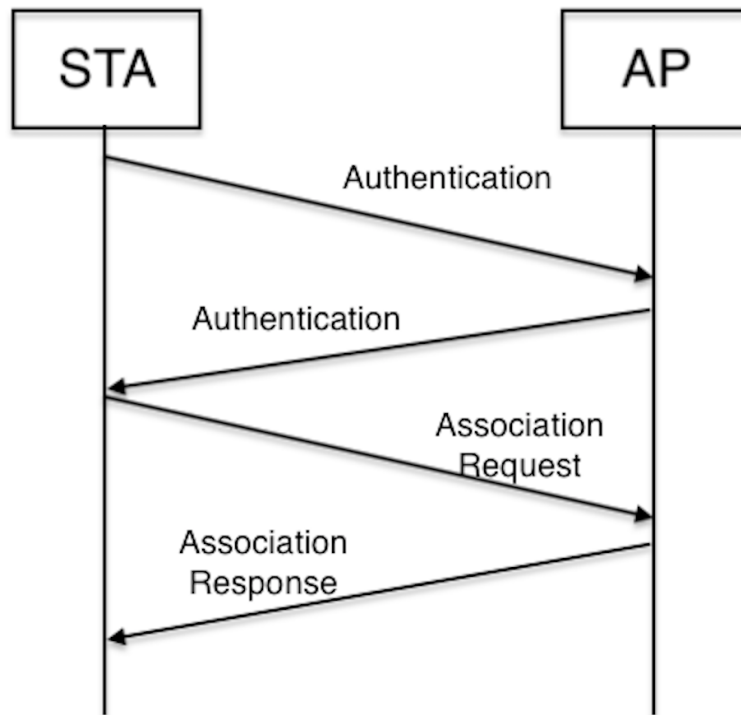


Figura 9: Sequência de tramas trocadas

## 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 Pergunta 14

Considere a trama de dados no 431. 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?

### 4.2 Resposta 14

Através do campo DS status é possível verificar as flags presentes de To DS e From DS que por sua vez, permitem concluir a direcionalidade dessa trama. Deste modo, através da figura a baixo é possível concluir que a flag de To DS está a 0 e a do From DS está a 1, o que significa que o pacote não é local à WLAN.

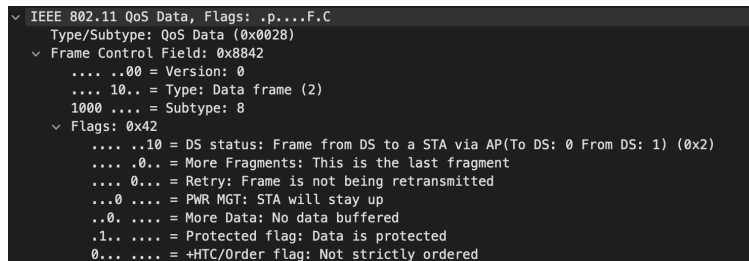


Figura 10: Frame Control da Trama 431.

### 4.3 Pergunta 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?

### 4.4 Resposta 15

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

Endereço AP → (bc:14:0l:af:b1:98) - Transmitter Address

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

```
IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8842
    .000 0000 0010 0100 = Duration: 36 microseconds
    Receiver address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Destination address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    .... .... 0000 = Fragment number: 0
    0011 0011 1110 .... = Sequence number: 830
    Frame check sequence: 0x793feef8 [unverified]
    [FCS Status: Unverified]
```

Figura 11: IEEE 802.11 da Trama 431.

## 4.5 Pergunta 16

Como interpreta a trama no<sup>o</sup>433 face à sua direccionalidade e endereçamento MAC?

## 4.6 Resposta 16

Novamente, verificando a figura a baixo facilmente vemos que a flag To DS é 1 e flag From DS é 0, deste modo concluímos que a trama vem de STA para DS. Sobre o endereçamento :

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

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

Endereço router de acesso → (bc:14:01:af:61:98) - Destination Address

Concluimos então que esta trama vai no sentido contrário da trama 431, da STA para DS.

```

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... .... = +HTC/Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Transmitter address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Source address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_10:6a:f5 (64:9a:be:10:6a:f5)
    .... .... 0000 = Fragment number: 0
    1110 0110 0000 .... = Sequence number: 3680
    Frame check sequence: 0x841b593c [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000

```

Figura 12: IEEE 802.11 da Trama 433.

## 4.7 Pergunta 17

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

## 4.8 Resposta 17

O subtipo de tramas de controlo transmitidas ao longo da transferência de dados a cima mencionada são tramas de controlo ACK, acknowledge. Estas tramas revelam uma grande importância ao longo de uma transferência pois são elas que dão a conhecer ao *sender* que o dados a serem transmitidos chegaram com sucesso ao destino. Caso o *sender* não receba uma trama de controlo ACK de volta a cerca de um pacote, ele saberá que algo aconteceu negativamente em relativamente ao pacote em questão e reenviará de novo.

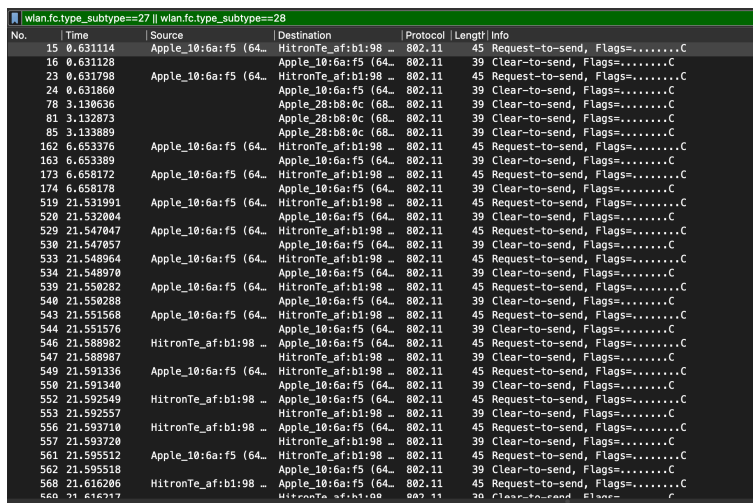
## 4.9 Pergunta 18

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.

## 4.10 Resposta 18

De modo a analisar as tramas que usaram a opção RTS/CTS usamos o comando:  
`wlan.fc.type_subtype==27 || wlan.fc.type_subtype==28.`

Através da figura a baixo podemos verificar que no exemplo a cima não está a ser usada a opção RTS/CTS.



No.	Time	Source	Destination	Protocol	Length	Info
15	0.631114	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
16	0.631128		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
23	0.631798	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
24	0.631868		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
78	3.138636		Apple_28:b8:0c (68..)	802.11	39	Clear-to-send, Flags=.....C
81	3.138873		Apple_28:b8:0c (68..)	802.11	39	Clear-to-send, Flags=.....C
85	3.138889		Apple_28:b8:0c (68..)	802.11	39	Clear-to-send, Flags=.....C
162	6.653376	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
163	6.653389		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
173	6.658172	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
174	6.658178		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
519	21.531991	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
520	21.532004		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
529	21.547047	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
530	21.547057		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
533	21.548964	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
534	21.548970		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
539	21.550282	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
540	21.550288		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
543	21.551568	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
544	21.551576		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
546	21.588982	HitronTe_af:b1:98 ..	Apple_10:6a:f5 (64..)	802.11	45	Request-to-send, Flags=.....C
547	21.588987		HitronTe_af:b1:98 ..	802.11	39	Clear-to-send, Flags=.....C
549	21.591336	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
550	21.591340		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
552	21.592549	HitronTe_af:b1:98 ..	Apple_10:6a:f5 (64..)	802.11	45	Request-to-send, Flags=.....C
553	21.592557		HitronTe_af:b1:98 ..	802.11	39	Clear-to-send, Flags=.....C
556	21.593710	HitronTe_af:b1:98 ..	Apple_10:6a:f5 (64..)	802.11	45	Request-to-send, Flags=.....C
557	21.593720		HitronTe_af:b1:98 ..	802.11	39	Clear-to-send, Flags=.....C
561	21.595512	Apple_10:6a:f5 (64..)	HitronTe_af:b1:98 ..	802.11	45	Request-to-send, Flags=.....C
562	21.595518		Apple_10:6a:f5 (64..)	802.11	39	Clear-to-send, Flags=.....C
568	21.616206	HitronTe_af:b1:98 ..	Apple_10:6a:f5 (64..)	802.11	45	Request-to-send, Flags=.....C
569	21.616217		HitronTe_af:b1:98 ..	802.11	39	Clear-to-send, Flags=.....C

Figura 13: RTS/CTS.

## 5 Conclusão

Este trabalho revelou-se bastante útil e educativo na medida em que permitiu a consolidação dos temas abordados nas aulas teóricas relativas às redes Wireless, por outro lado, foi possível um melhor contacto com o wireshark, tendo sido utilizados filtros de pesquisa para restringir certas tramas. Se salientar também a aprendizagem sobre novos temas tais como endereçamento de tramas Wi-Fi e mecanismos de controlo de acesso.