

## TP4: Redes Sem Fios (802.11)

Adriana Gonçalves, Eduardo Semanas, and Leonardo Neri

University of Minho, Department of Informatics, 4710-057 Braga, Portugal  
e-mail: {ae4481,a75536,a80056}@alunos.uminho.pt

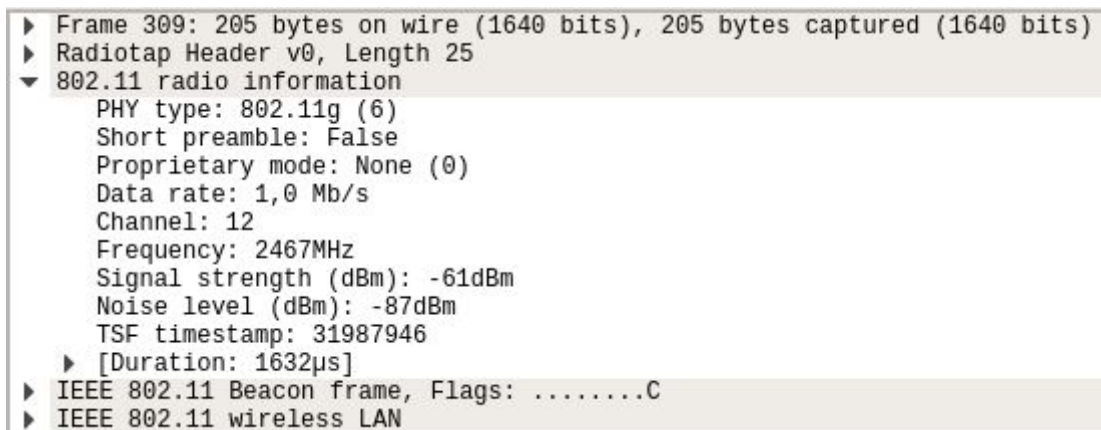
**Introdução** Este trabalho realizado no âmbito da unidade curricular de Redes de Computadores pretende explorar e compreender o funcionamento das redes sem fio e o respetivo protocolo IEEE 802.11. Através do estudo e observação dos vários tipos de tramas presentes no tráfego, seremos capazes de responder às questões propostas, bem como aprofundar conceitos como acesso rádio, scanning passivo e ativo e processos de associação e transferência de dados.

### Resolução das questões:

#### 4. Acesso Rádio

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

A rede sem fio está a operar no canal 12 e na frequência 2467MHz.



```
▶ Frame 309: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
▶ Radiotap Header v0, Length 25
▼ 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): -61dBm
  Noise level (dBm): -87dBm
  TSF timestamp: 31987946
  ▶ [Duration: 1632µs]
▶ IEEE 802.11 Beacon frame, Flags: .....C
▶ IEEE 802.11 wireless LAN
```

Figura 1: Trama Beacon analisada

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

Está a ser usada a norma 802.11g.

**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.**

A trama foi enviada a um débito de 1Mbps.

Não corresponde ao débito máximo, uma vez que a norma 802.11g pode operar a 54Mbps.

## 5. 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 (ver anexo)?

O valor do identificador de tipo é 0 (Management frame), com o subtipo 8 (Beacon). Estes valores encontram-se no campo “Frame Control Field” do cabeçalho da trama.

```
► Frame 309: 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
    .... ..00 = Version: 0
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
    ► Flags: 0x00
    .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 = Fragment number: 0
    1001 0001 0010 .... = Sequence number: 2322
    Frame check sequence: 0x14e6d6e9 [correct]
    [FCS Status: Good]
► IEEE 802.11 wireless LAN
```

Figura 2: Cabeçalho de uma trama IEEE 802.11 Beacon

5) Liste todos os SSIDs dos APs (Access Points) que estão a operar na vizinhança da STA de captura? Explícite o modo como obteve essa informação. Como sugestão pode construir um filtro de visualização apropriado (tomando como base a resposta da alínea anterior) que lhe permita obter a listagem pretendida.

Os Access Points que estão a operar na vizinhança da STA de captura são NOS\_WIFI\_Fon e FlyingNet.

Para a obtenção destes SSIDs aplicamos à captura um filtro que apenas mostrasse as tramas que têm o campo do subtipo a 8, que indica que é uma trama beacon e ordenamos pela coluna source.

wlan.fc.type_subtype eq 8					
No.	Time	Source	Destination	Protocol	Length Info
6	0.206582	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2088, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
4	0.104164	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2086, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
2	0.001662	HitronTe_af:b1:99	Broadcast	802.11	205 Beacon frame, SN=2084, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
175...	132.915741	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=583, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
175...	132.813348	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=581, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
175...	132.710857	HitronTe_af:b1:98	Broadcast	802.11	296 Beacon frame, SN=579, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Figura 3: Access Points que estão a operar na vizinhança da STA

**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 usado o método de detecção de erros, a Figura 4 mostra uma trama beacon que não foi recebida corretamente.

A importância de usar um método de detecção de erros neste tipo de redes é porque as tramas não são transmitidas num meio fiável.

```
▶ Frame 7131: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
▶ Radiotap Header v0, Length 40
▶ 802.11 radio information
▼ IEEE 802.11 Beacon frame, Flags: .pmPRM.T.
  Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x827d
    .... ..10 = Version: 2
    .... 00.. = Type: Management frame (0)
    1000 .... = Subtype: 8
    ▶ Flags: 0x7d
    Duration/ID: 7292 (reserved)
    Receiver address: 34:c4:ca:25:ed:14
    Destination address: 34:c4:ca:25:ed:14
    Transmitter address: 62:4c:de:c5:a9:3a
    Source address: 62:4c:de:c5:a9:3a
    BSS Id: 55:0e:b7:95:b0:54
    STA address: 62:4c:de:c5:a9:3a
    .... ..0000 = Fragment number: 0
    1010 1111 1011 .... = Sequence number: 2811
    ▶ Frame check sequence: 0x20c4ca4e incorrect, should be 0x7d318e93
    [FCS Status: Bad]
    ▶ TKIP/CCMP parameters
  ▶ Data (70 bytes)
```

Figura 4: Trama Beacon recebida incorretamente

**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.**

Relativamente aos intervalos de tempo previstos para os dois APs identificados obtivemos os seguintes valores:

```
▶ Frame 17516: 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
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 0x0000010bb59cbb40
    Beacon Interval: 0.102400 [Seconds]
    ▶ Capabilities Information: 0x0c21
  ▼ Tagged parameters (140 bytes)
    ▶ Tag: SSID parameter set: NOS_WIFI_Fon
```

Figura 5: Intervalo de tempo previsto para o AP NOS\_WIFI\_Fon (0,1024 segundos)

```

▶ Frame 8513: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: .....C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 0x0000010bb3d2e1d7
    Beacon Interval: 0.102400 [Seconds]
    ▶ Capabilities Information: 0x0c31
  ▼ Tagged parameters (231 bytes)
    ▶ Tag: SSID parameter set: FlyingNet

```

Figura 6: Intervalo de tempo previsto para o AP FlyingNet (0,1024 segundos)

Verifica-se então um período de 0,1024 segundos entre “Beacons” para ambos os APs. Na prática a periodicidade das tramas beacon é verificada de modo a garantir que não existem problemas, esta também pode ser manipulada de forma a ocupar menos capacidade da rede.

**8) Identifique e registre 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.**

Todas as tramas Beacon são enviadas para o broadcast (ff:ff:ff:ff:ff:ff).

O anexo possui tramas que são de um único AP mas com endereços MAC diferentes, bc:14:01:af:b1:99 e bc:14:01:af:b1:98.

Os 3 primeiros bytes do endereço MAC são iguais, isto sugere que pertencem ao mesmo AP mas a SSIDs diferentes.

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?

Os débitos suportados são 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 e 54 Mbps.

```

▶ Frame 320: 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
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 0x0000010bae789b31
    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 2 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 7: Débitos suportados pelo AP

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

O filtro que nos permite visualizar todas as tramas probing request e response é o *wlan.fc.type\_subtype eq 4 or wlan.fc.type\_subtype eq 5* e está explícito no print screen em baixo.

wlan.fc.type_subtype eq 4 or wlan.fc.type_subtype eq 5						
No.	Time	Source	Destination	Protocol	Length	Info
2473	07:01:02.135797	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
2471	07:01:02.135097	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
2469	07:01:02.134352	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
171...	07:01:55.590381	Apple_28:b8:0c	Broadcast	802.11	146	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
171...	07:01:55.579218	Apple_28:b8:0c	Broadcast	802.11	146	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet
171...	07:01:55.565993	Apple_28:b8:0c	Broadcast	802.11	146	Probe Request, SN=0, FN=0, Flags=....., SSID=FlyingNet

Figura 8: Trama probing request e response



**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?**

O probe Request é enviado do endereço MAC 64:9a:be:10:61:f5 e direcionado ao broadcast, buscando pela rede com SSID igual a FlyingNet.

O propósito das tramas probe request é de obter informação sobre as redes que estão ao seu alcance, bem como suas características (taxa de dados suportadas, canal de transmissão, ...). Probe response é a resposta de um AP ou estação a este pedido.

```
▶ Frame 2677: 164 bytes on wire (1312 bits), 164 bytes captured (1312 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
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: ff:ff:ff:ff:ff:ff
    Destination address: ff:ff:ff:ff:ff:ff
    Transmitter address: 64:9a:be:10:6a:f5
    Source address: 64:9a:be:10:6a:f5
    BSS Id: ff:ff:ff:ff:ff:ff
    .... 0000 = Fragment number: 0
    1010 0001 1101 .... = Sequence number: 2589
    Frame check sequence: 0xb5019d86 [correct]
    [FCS Status: Good]
▼ IEEE 802.11 wireless LAN
  ▼ Tagged parameters (111 bytes)
    ▶ Tag: SSID parameter set: FlyingNet
    ▶ Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
    ▶ Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 11
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: Extended Capabilities (8 octets)
    ▶ Tag: Interworking
    ▶ Tag: Vendor Specific: Apple, Inc.
    ▶ Tag: Vendor Specific: Microsoft Corp.: Unknown 8
    ▶ Tag: Vendor Specific: Broadcom
```

Figura 9: Probe Request

```

▶ Frame 2608: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Probe Response, Flags: .....C
  Type/Subtype: Probe Response (0x0005)
  ▶ Frame Control Field: 0x5000
    .000 0000 0011 0010 = Duration: 50 microseconds
    Receiver address: 64:9a:be:10:6a:f5
    Destination address: 64:9a:be:10:6a:f5
    Transmitter address: bc:14:01:af:b1:98
    Source address: bc:14:01:af:b1:98
    BSS Id: bc:14:01:af:b1:98
    .... .... 0000 = Fragment number: 0
    1001 0010 1011 .... = Sequence number: 2347
    Frame check sequence: 0x1f4c4ee5 [correct]
    [FCS Status: Good]
▼ IEEE 802.11 wireless LAN
  ▶ Fixed parameters (12 bytes)
  ▼ Tagged parameters (346 bytes)
    ▶ Tag: SSID parameter set: FlyingNet
    ▶ 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: ERP Information
    ▶ Tag: Extended Supported Rates 6(B), 12(B), 24(B), 48, [Mbit/sec]
    ▶ Tag: HT Capabilities (802.11n D1.10)
    ▶ Tag: HT Information (802.11n D1.10)
    ▶ Tag: Secondary Channel Offset (802.11n D1.10)
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    ▶ Tag: RSN Information
    ▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▶ Tag: QBSS Load Element 802.11e CCA Version
    ▶ Tag: Extended Capabilities (1 octet)
    ▶ Tag: Vendor Specific: Ralink Technology, Corp.
    ▶ Tag: Vendor Specific: Microsoft Corp.: WPS

```

Figura 10: Probe Response

## 6. 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.**

Na imagem abaixo podemos encontrar um processo de associação entre a STA e o AP.

2486	07:01:02.346342	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	70 Authentication, SN=2542, FN=0, Flags=.....C
2488	07:01:02.366429	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	59 Authentication, SN=2338, FN=0, Flags=.....C
2490	07:01:02.368072	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175 Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2492	07:01:02.373899	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225 Association Response, SN=2339, FN=0, Flags=.....C

Figura 11: Processo de associação entre a STA e o AP

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

Em baixo está representado o diagrama correspondente a todas a tramas trocadas desde o início do processo de autenticação até ao fim do processo de associação.

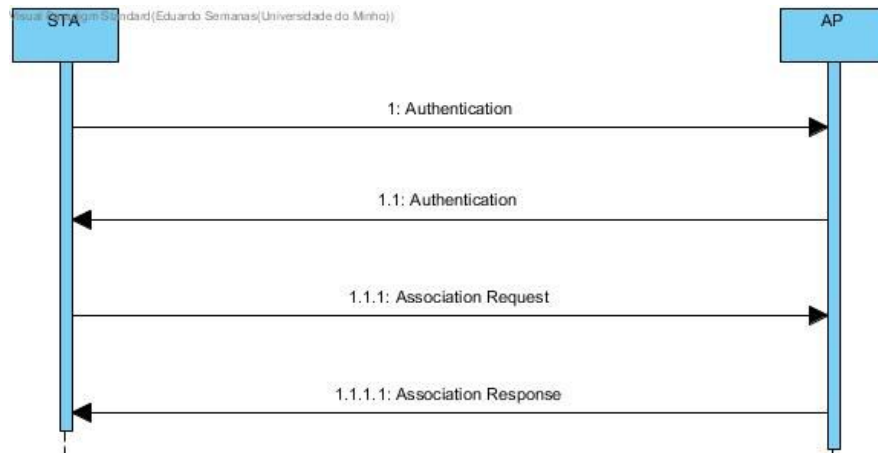


Figura 12: Diagrama das sequências de todas as tramas trocadas no processo

## 7. Transferência de Dados

**14) Considere a trama de dados nº455. 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?**

Pelo campo *DS status*, na Figura 13, verificamos que a direcionalidade da trama é *To DS:0 From DS:1*, logo a trama não é local à WLAN.

```

▶ Frame 455: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .p....F.C
  Type/Subtype: QoS Data (0x0028)
  ▼ Frame Control Field: 0x8842
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
    ▼ Flags: 0x42
      .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
      .... .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... .... = Order flag: Not strictly ordered
    .000 0000 0010 0100 = Duration: 36 microseconds
  Receiver address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
  Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
  Destination address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
  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_71:41:a1 (d8:a2:5e:71:41:a1)
  
```

Figura 13: Control Frame da trama 455



**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 Figura 13 constam os endereços MAC da trama 455, onde:

**STA** - d8:a2:5e:71:41:a1, identifica o endereço do host;

**AP** - bc:14:01:af:b1:98, que está associado ao endereço de origem;

**Router** - bc:14:01:af:b1:98, identifica o endereço de quem está transmitindo a trama;

**16) Como interpreta a trama nº457 face à sua direcionalidade e endereçamento MAC?**

Podemos observar no campo *DS status*, representado na Figura 14, que a direcionalidade da trama 475 é definida por *To DS:1 From DS:0*. Logo, o pacote sai da STA para o sistema de distribuição através do AP, ou seja, o pacote está a ser enviado para uma rede externa à WLAN, logo não é local à WLAN.

```
► Frame 457: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
► Radiotap Header v0, Length 25
► 802.11 radio information
▼ 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... .... = 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_71:41:a1 (d8:a2:5e:71:41:a1)
    Destination address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    Source address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
    BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
    STA address: Apple_71:41:a1 (d8:a2:5e:71:41:a1)
```

Figura 14: Conteúdo da Frame Control da trama 457

**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.)**

Como mostra a Figura 14, são transmitidas tramas de *Acknowledgment* (confirmação de recebimento) já que estas tramas não são transmitidas em um meio fiável.

455 18.536644	bc:14:01:af:b1:98	d8:a2:5e:71:41:a1	802.11	226 QoS Data, SN=276, FN=0, Flags=.p...F.C
456 18.536653	bc:14:01:af:b1:98	bc:14:01:af:b1:98 (...)	802.11	39 Acknowledgement, Flags=.....C
457 18.539762	d8:a2:5e:71:41:a1	bc:14:01:af:b1:98	802.11	178 QoS Data, SN=1209, FN=0, Flags=.p....TC
458 18.540043	d8:a2:5e:71:41:a1	d8:a2:5e:71:41:a1 (...)	802.11	39 Acknowledgement, Flags=.....C

Figura 15: Tramas transmitidas entre as tramas 455 e 457

**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.**

Como mostra a Figura 14, não estão sendo usadas as tramas RTS/CTS.

## Conclusões

Neste trabalho fomos introduzidos, desta vez, ao protocolo IEEE 802.11/Redes sem fios(WiFi). Isto envolve o conhecimento relativo a vários tipos de “Tramas de Gestão” diferentes, como é o caso da Trama de Autenticação, de Pedido de Associação, de Anúncio, Pedido de Prova, entre outras. Envolve também conhecimento relativo a “Tramas de Controlo”, tramas estas que servem de auxílio à troca de dados entre estações sem fios, e “Tramas de Dados”, tramas estas que contêm a informação relativa à informação/dados que está sendo transmitida.

Em contraste com os trabalhos práticos anteriores, nos quais tivemos que realizar capturas com o software “Wireshark” nas nossas próprias máquinas, neste trabalho foi-nos dada uma captura “Wireshark” já realizada, a qual foi usada como referência para responder às questões apresentadas ao longo do trabalho.

A partir da captura recebida foram-nos postas várias questões, relativas aos cabeçalhos das diferentes tramas presentes na captura ou mesmo a informação que se encontrava diretamente na mesma (caso do tipo de trama, a origem/o destino da mesma, etc...).

Para obter uma resposta relativa a estas questões tivemos que estudar mais a fundo conceitos como os de “Scanning Passivo/Ativo” , “Access Point”, “STA”(ou estação”, entre outros...

Relativamente aos tipos de Scanning obtivemos a capacidade de associar, por exemplo, “Tramas Beacon” ao tipo de Scanning Passivo e “Tramas de Probe request/response” ao Scanning Ativo. Isto no sentido em que beacons servem de uma forma de controlo do estado da rede “periódico” e os probe requests (com as suas respectivas “responses”) de um controlo “manual”. Relativamente a estes últimos foi-nos ainda pedido que aplicássemos um filtro no “Wireshark” que nos permitisse visualizar todas as tramas probing request ou probing response, o que nos obrigou a compreender melhor o funcionamento não só do software como da captura que estávamos a analisar.

Obtivemos também um conhecimento mais aprofundado relativamente ao processo de associação entre uma STA e um Access Point graças á questão 6, questão esta que nos pediu que indentificássemos um processo de associação completo, i.e. processo de autenticação (Authentication Request/Response) e só de seguida de associação em si (Association Request/Response), terminando com o pedido para a construção de um diagrama que nos permitiu visualizar este mesmo processo.

A última questão (nº 7), relativa à transferência de dados em si, fez com que nos deparássemos com questões como a “Direcionalidade das tramas” (que nos permite verificar a localidade da trama relativamente à WLAN), a origem/destino dos dados em transmissão e também a necessidade de identificar as diferentes tramas que realizaram o “controlo” ao longo de uma dada transferência de dados.

Concluindo pensamos ter sido capazes de compreender toda a informação pretendida por este trabalho prático obtendo assim um conhecimento já bastante abrangente não só relativamente a Redes Sem Fios mas também a Redes Computacionais em geral.