

Redes de Computadores

Trabalho Prático 4: Redes Sem Fios (802.11)

Ana Rita Peixoto, Sara Queirós, and Sofia Santos

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a89612,a89491,a89615}@alunos.uminho.pt

Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (radio information), para além dos bytes correspondentes a tramas 802.11. Para a trama correspondente 3XX em que XX corresponde ao seu número de TurnoGrupo (e.g., 11),

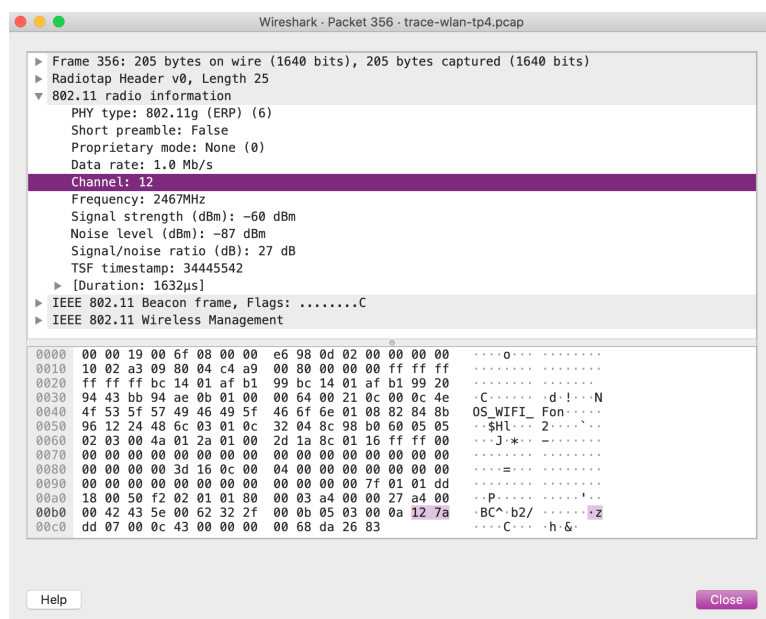


Fig. 1. Trama 802.11 correspondente ao nosso grupo.

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

A rede sem fios está a operar a 2467MHz, no canal 12, tal como é possível ver na figura 1

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

Está a ser usada a versão 802.11g. Podemos verificar isto no campo *PHY type* da figura 1.

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.

Esta trama foi enviada a um débito de 1Mb/s. Este valor não corresponde ao débito máximo desta interface Wi-Fi, visto que o débito máximo da versão 802.11g da norma IEEE 802.11 é 54Mb/s.

Scanning Passivo e Scanning Ativo

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

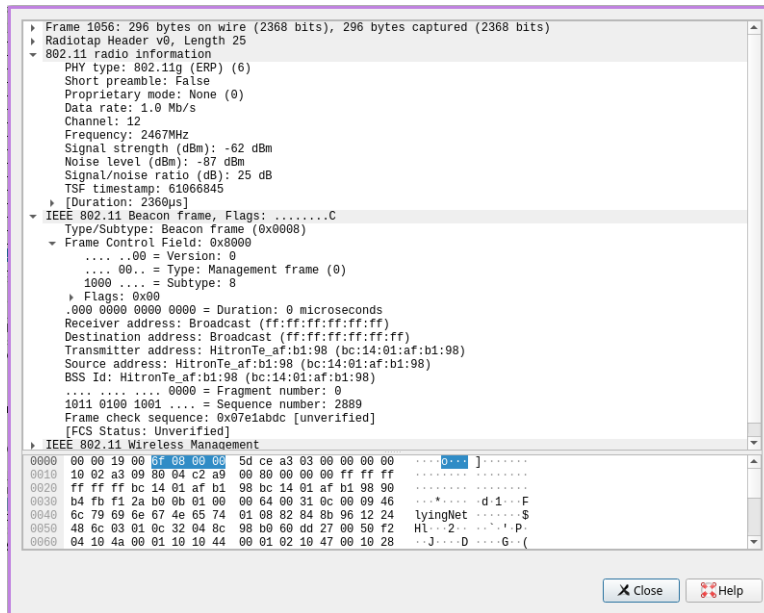


Fig. 2. Trama beacon 802.11 correspondente ao nosso grupo.

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)?

Esta trama é do tipo 0 (*Management frame*) e do subtipo 8 (*Beacon*). Estes valores estão especificados na secção "frame control" do cabeçalho, tal como é possível ver na figura 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:b1:98
 Source address: bc:14:01:af:b1:98

Podemos concluir que a origem da trama é o *Access Point* e, como o endereço MAC de destino é ff:ff:ff:ff:ff:ff, ou seja, um endereço de broadcast, concluímos que a trama é enviada para todos os dispositivos capazes de a receber no alcance do AP.

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?

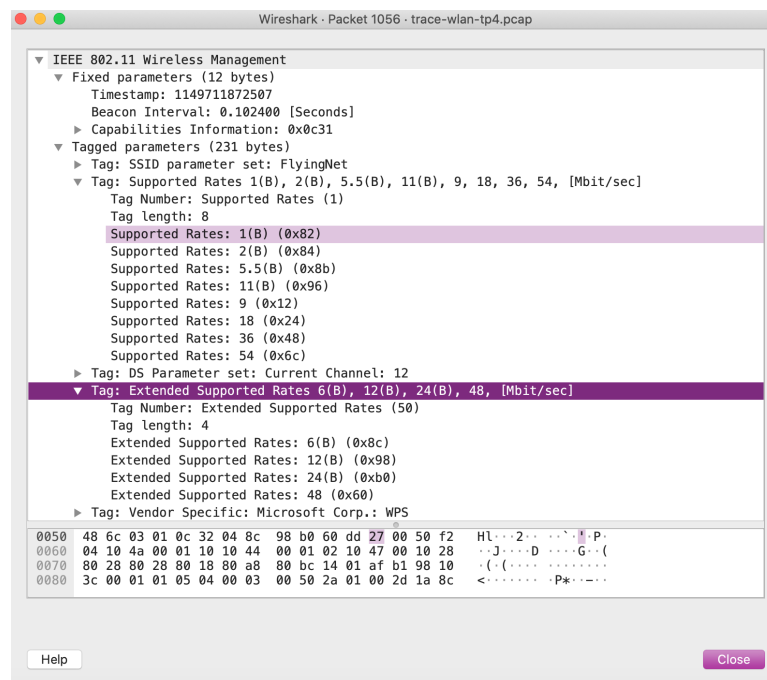


Fig. 3. Débitos da trama beacon 802.11 correspondente ao nosso grupo.

Os débitos suportados pela trama são:

- 1 Mb/s (Básico)
- 2 Mb/s (Básico)
- 5.5 Mb/s (Básico)
- 11 Mb/s (Básico)
- 9 Mb/s
- 18 Mb/s
- 36 Mb/s
- 54 Mb/s

Os débitos adicionais são:

- 6 Mb/s (Básico)

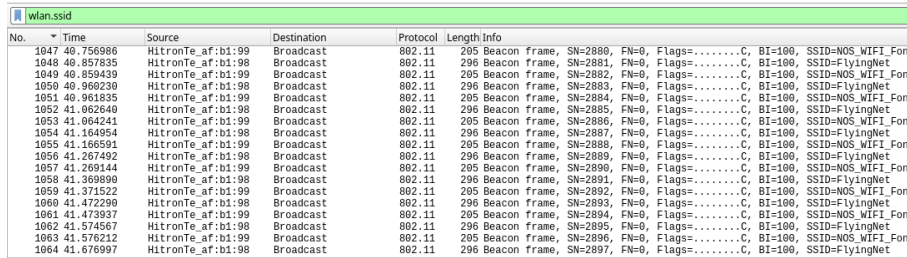
- 12 Mb/s (Básico)
- 24 Mb/s (Básico)
- 48 Mb/s

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.

Tal como é possível ver na figura 3, o intervalo de tempo previsto entre tramas é 0.102400 segundos. Na prática, este valor acaba por ser mais uma aproximação do que um valor exato, visto que o AP pode estar ocupado no momento exato em que deve enviar a trama beacon, ocorrendo um ligeiro atraso no envio da mesma.

Exercício 8. Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura? Explique o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

Os SSIDs que estão a operar na vizinhança da STA de captura são *FlyingNet* e *NOS_WIFI_Fon*. Para obter esta informação utilizamos o filtro *wlan.ssid*. Através deste filtro, podemos ver que, para um certo intervalo de tempo, apenas são recebidas tramas beacon provenientes dos dois APs que mencionámos, sendo assim bastante improvável a existência de mais APs.

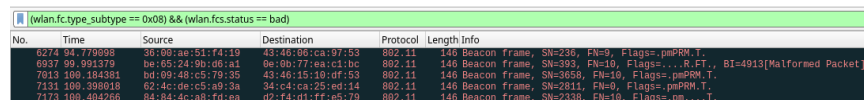


No.	Time	Source	Destination	Protocol	Length	Info
1047	40.756986	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2880, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1048	40.857835	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2881, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1049	40.858439	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2882, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1050	40.960230	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2883, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1051	40.961835	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2884, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1052	41.062640	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2885, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1053	41.064241	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2886, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1054	41.164954	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2887, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1055	41.166591	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2888, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1056	41.267492	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2889, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1057	41.269144	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2890, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1058	41.368990	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2891, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1059	41.371522	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2892, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1060	41.472290	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2893, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1061	41.473937	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2894, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1062	41.574567	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2895, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
1063	41.576212	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2896, FN=0, Flags=.....C, BI=100, SSID=NOS_WIFI_Fon
1064	41.676997	HitronTe_af:b1:99	Broadcast	802.11	296	Beacon frame, SN=2897, FN=0, Flags=.....C, BI=100, SSID=FlyingNet

Fig. 4. Tramas beacon recebidas num intervalo de tempo aproximadamente igual a 1 segundo.

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.



No.	Time	Source	Destination	Protocol	Length	Info
6274	94.779098	36:08:ae:51:f4:19	43:46:06:ca:97:53	802.11	146	Beacon frame, SN=236, FN=9, Flags=pmPRM.T.
6937	99.991379	be:65:24:9b:d6:a1	0e:9b:77:ea:c1:bc	802.11	146	Beacon frame, SN=393, FN=10, Flags=...R.F.T., BI=4913[Malformed Packet]
7013	100.104081	be:65:24:9b:d6:a1	0e:9b:77:ea:c1:bc	802.11	146	Beacon frame, SN=393, FN=10, Flags=pmPRM.T.
7131	100.398018	62:4c:9e:c5:89:3a	34:c4:ca:25:e9:14	802.11	146	Beacon frame, SN=2811, FN=0, Flags=pmPRM.T.
7173	100.484266	84:84:4c:a8:fd:ea	d2:f4:d1:ff:e5:79	802.11	146	Beacon frame, SN=2338, FN=10, Flags=pm....T.

Fig. 5. Resultados obtidos ao aplicar o filtro `(wlan.fc.type_subtype == 0x08) && (wlan.fcs.status == bad)`.

Ao aplicar o filtro, somos capazes de detetar cinco tramas de beacon com erros, através do campo *FCS Status*. A existência deste campo mostra-nos que está a ser usado um método de deteção de erros.

A deteção de erros em redes sem fios é utilizada como forma de detetar qualquer tipo de interferência ou obstrução nas tramas.

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.

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

O filtro que permite visualizar as tramas *probing request* ou *probing response* é:

```
wlan.fc.type_subtype == 4 || wlan.fc.type_subtype == 5.
```

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?

Uma estação envia um *probing request* em broadcast, para descobrir quais as redes 802.11 na sua proximidade. O *probing response* é enviado pelo AP para a estação com informações relativas ao AP.

wlan.fc.type_subtype == 4 wlan.fc.type_subtype == 5						
No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0, F
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0, F
2468	70.149098	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0, F
2469	70.149792	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0, F
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0, F
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0, F
2475	70.151789	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	281	Probe Response, SN=2335, FN=0, F
2477	70.152099	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	281	Probe Response, SN=2336, FN=0, F
2479	70.152570	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	281	Probe Response, SN=2337, FN=0, F
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0, F

▶ 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 .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: 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						
--	--	--	--	--	--	--

Fig. 6. Probing request enviado.

wlan.fc.type_subtype == 4 wlan.fc.type_subtype == 5						
No.	Time	Source	Destination	Protocol	Length	Info
1300	53.746911	Apple_10:6a:f5	Broadcast	802.11	155	Probe Request, SN=2516, FN=0,
2467	70.147855	ea:a4:64:7b:b9:7a	Broadcast	802.11	167	Probe Request, SN=2540, FN=0,
2468	70.149898	ea:a4:64:7b:b9:7a	Broadcast	802.11	155	Probe Request, SN=2541, FN=0,
2469	70.149792	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2332, FN=0,
2471	70.150537	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2333, FN=0,
2473	70.151237	HitronTe_af:b1:98	ea:a4:64:7b:b9:7a	802.11	411	Probe Response, SN=2334, FN=0,
2475	70.151709	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2335, FN=0,
2477	70.152099	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2336, FN=0,
2479	70.152570	HitronTe_af:b1:99	ea:a4:64:7b:b9:7a	802.11	201	Probe Response, SN=2337, FN=0,
2603	72.179215	Apple_10:6a:f5	Broadcast	802.11	164	Probe Request, SN=2563, FN=0,

▶ Frame 2469: 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: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
Destination address: ea:a4:64:7b:b9:7a (ea:a4:64:7b:b9:7a)
Transmitter address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
Source address: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
BSS Id: HitronTe_af:b1:98 (bc:14:01:af:b1:98)
.... 0000 = Fragment number: 0
1001 0001 1100 = Sequence number: 2332
Frame check sequence: 0xbce842e3 [unverified]
[FCS Status: Unverified]
▶ IEEE 802.11 Wireless Management

Fig. 7. Respetivo *Probing Response* ao *Probing Request* anterior.

Processo de Associação

Numa rede WiFi 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:

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 `wlan.fc.type == 0 && (wlan.fc.type_subtype == 0 || wlan.fc.type_subtype == 1 || wlan.fc.type_subtype == 11 || wlan.fc.type_subtype == 8)` é possível observar, na figura 8, uma sequência 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.

wlan.fc.type == 0 && (wlan.fc.type_subtype == 0 wlan.fc.type_subtype == 1 wlan.fc.type_subtype == 11 wlan.fc.type_subtype == 8)						
No.	Time	Source	Destination	Protocol	Length	Info
2483	70.348997	HitronTe_af:b1:98	Broadcast	802.11	296	Beacon frame, SN=3457, FN=0, Flags=.....C, BI=100, SSID=FlyingNet
2484	70.350698	HitronTe_af:b1:98	Broadcast	802.11	285	Beacon frame, SN=3458, FN=0, Flags=.....C, BI=100, SSID=N05_WIFI_Fon
2486	70.351702	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
2490	70.383512	Apple_10:6a:f5	HitronTe_af:b1:98	802.11	175	Association Request, SN=2543, FN=0, Flags=.....C, SSID=FlyingNet
2492	70.389339	HitronTe_af:b1:98	Apple_10:6a:f5	802.11	225	Association Response, SN=2339, FN=0, Flags=.....C

Fig. 8. Sequência de tramas relativas ao processo de associação.

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

O seguinte diagrama permite ilustrar a sequência de todas as tramas trocadas no processo:

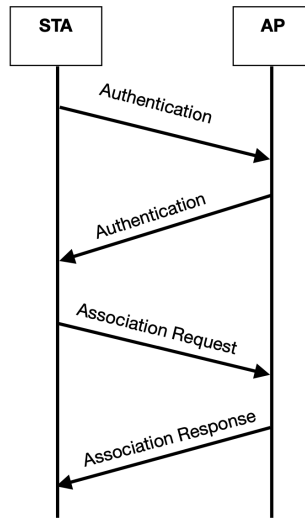


Fig. 9. Sequência de tramas trocadas no processo.

Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e de controlo da transferência desses mesmos dados.

Exercício 14. Considere a trama de dados n.º455. 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?

Através do campo *DS status* conseguimos observar que o valor de *to DS* é 0 e o de *from DS* é 1. O valor destas *flags* permite inferir a direcionalidade dessa trama. Assim, podemos concluir que a trama vem do DS para o STA, ou seja, não é local à WLAN, apenas entra na WLAN.

```

v Frame Control Field: 0x8842
  .... ..00 = Version: 0
  .... 10.. = Type: Data frame (2)
  1000 .... = Subtype: 8
  v 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
  
```

Fig. 10. Frame Control da trama de dados n.º 455.

Exercício 15. Para a trama de dados nº 455, 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?

Endereço STA: **d8:a2:5e:71:41:a1** (Receiver address)

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

Endereço router de acesso: **d8:a2:5e:71:41:a1** (Destination address)

```
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)
```

Fig. 11. Trama de dados nº 455

Exercício 16. Como interpreta a trama nº457 face à sua direcionalidade e endereçamento MAC?

Podemos inferir a direcionalidade da trama a partir da análise das flags *to DS* e *from DS*, que assumem os valores 1 e 0, respetivamente. Assim, conseguimos concluir que a trama vem do STA para o DS.

```
> Frame 457: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
> Radiotap Header v0, Length 25
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
  v Frame Control Field: 0x8841
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
    v 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)
      .... .... 0000 = Fragment number: 0
      0100 1011 1001 .... = Sequence number: 1209
      Frame check sequence: 0x88cbfe48 [unverified]
      [FCS Status: Unverified]
    > Qos Control: 0x0000
    > CCMP parameters
  > Data (115 bytes)
```

Fig. 12. Trama de dados nº 457.

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.)

São transmitidas as tramas de controlo ACK (acknowledge). Estas tramas são necessárias como indicador de que a transmissão foi efetuada com sucesso. Quando a estação recebe uma trama ACK, esta é um aviso positivo por parte do AP a indicar que tudo correu bem.

```

455 18.536644 HitronTe_af:b1:98 Apple_71:41:a1 802.11 226 QoS Data, SN=276, FN=0, Flags=.p....F.C
456 18.536653 HitronTe_af:b1:98 (... 802.11 39 Acknowledgement, Flags=.....C
457 18.539762 Apple_71:41:a1 HitronTe_af:b1:98 802.11 178 QoS Data, SN=1209, FN=0, Flags=.p....TC
458 18.540043 Apple_71:41:a1 (d8:... 802.11 39 Acknowledgement, Flags=.....C

```

Fig. 13. Trama de dados ACK.

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 direcionalidade das tramas e os sistemas envolvidos.

Para o exemplo acima não está a ser utilizada a opção RTS/CTS na troca de dados. No entanto, é utilizada noutras situações tal como se pode verificar na figura 14.

```

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
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 ... Apple_10:6a:f5 (64... 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... 802.11 39 Acknowledgement, Flags=.....C

```

Fig. 14. Utilização da opção RTS/CTS

Conclusão

Com este trabalho prático conseguimos consolidar os temas abordados nas aulas teóricas relativos às redes *Wireless*. Assim, foi possível apreender diversos conceitos tais como: as características e elementos das redes *Wireless*, endereçamento de tramas *Wi-Fi* e mecanismos de controlo de acesso. Para além disso, a utilização do *Wireshark* foi bastante útil na medida em que praticamos a utilização e pesquisa de filtros, que facilitavam as nossas pesquisas e obtenção de respostas.