
Trabalho Prático Nº4 – Redes Sem Fios (Wi-Fi)

TRABALHO REALIZADO POR:

BEATRIZ RIBEIRO MONTEIRO
CARLOS EDUARDO CULOLO DANTAS DA COSTA
HUGO RICARDO MACEDO GOMES



A95437
Beatriz Monteiro



A88551
Carlos Costa



A96842
Hugo Gomes

Índice

1	Introdução	1
2	Acesso Rádio	1
2.1	Execício 1	1
2.2	Execício 2	1
2.3	Execício 3	2
2.4	Execício 4	2
3	Scanning Passivo e Scanning Ativo	3
3.1	Execício 5	3
3.2	Execício 6	3
3.3	Execício 7	4
3.4	Execício 8	4
3.5	Execício 9	5
3.6	Execício 10	5
3.7	Execício 11	6
3.8	Execício 12	6
4	Processo de Associação	7
4.1	Execício 13	7
4.2	Execício 14	7
5	Transferência de Dados	8
5.1	Execício 15	8
5.2	Execício 16	8
5.3	Execício 17	9
5.4	Execício 18	9
5.5	Execício 19	9
6	Conclusão	10

List of Figures

1	Trama de ordem 55	1
2	IEEE 802.11 Wireless LAN	2
3	Trama de ordem 55	3
4	Excerto do Anexo - Trama 802.11 + Tipos e subtipos de tramas	3
5	Frame Check Sequence	4
6	Débitos suportados pelo AP	5
7	Tramas beacon consecutivas provenientes do mesmo AP	5
8	Probing Request e respetiva Probing Response	6
9	Sequência de tramas	7
10	Diagrama da Sequência de tramas	7
11	Campo Frame Control da Trama 8053	8
12	Totalidade da Trama 8053	8
13	Trama 8521	9
14	Sequencia de Tramas 8519,8520 e 8521	9
15	Trama 8519 - Request to Send	10
16	Trama 382	10

1 Introdução

Este relatório é referente ao último trabalho prático da Unidade Curricular de Redes de Computação proposto pela equipa docente.

Este trabalho tem como objetivo explorar vários aspetos do protocolo IEEE 802.11, tais como o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, bem como a operação do protocolo.

2 Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui meta-informação do nível físico (*radiotap header*, *radio information*) obtida do *firmware* da interface Wi-Fi, para além dos bytes correspondentes a tramas 802.11. Seleccionamos a trama de ordem 55 correspondente ao nosso identificador de grupo.

```
▶ Frame 55: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits) on interface en0, id 0
  ▼ Radiotap Header v0, Length 60
    Header revision: 0
    Header pad: 0
    Header length: 60
    ▶ Present flags
    MAC timestamp: 507207
    ▶ Flags: 0x10
    Channel frequency: 2412 [BG 1]
    ▶ Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
    Antenna signal: -92dBm
    Antenna noise: -93dBm
    Antenna: 0
    Channel number: 1
    Channel frequency: 2412
    ▶ Channel flags: 0x00010480, 2 GHz spectrum, Dynamic CCK-OFDM, HT Channel (20MHz Channel Width)
    MCS information
    [Data Rate: 6,5 Mb/s]
    ▶ A-MPDU status
    ▶ Vendor namespace: Broadcom-3
  ▼ 802.11 radio information
    PHY type: 802.11n (HT) (7)
    MCS index: 0
    Bandwidth: 20 MHz (0)
    Short GI: False
    Greenfield: False
    FEC: BEC (0)
    Data rate: 6,5 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -92dBm
    Noise level (dBm): -93dBm
    Signal/noise ratio (dB): 1dB
    TSF timestamp: 507207
    .....1 = Last part of an A-MPDU: True
    .....0 = A-MPDU delimiter CRC error: False
    A-MPDU aggregate ID: 0
    ▶ [Duration: 440µs]
  ▶ IEEE 802.11 Beacon frame, Flags: .....C
  ▶ IEEE 802.11 Wireless Management
```

Figure 1: Trama de ordem 55

2.1 Execício 1

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

Na figura 1 podemos ver que a frequência do espectro onde a rede sem fios está a operar é 2412 MHz, que corresponde ao canal 1.

2.2 Execício 2

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

A versão da norma IEEE 802.11 que está a ser usada é 802.11n (HT).

2.3 Execício 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 débito a que a trama foi enviada foi 6,5 Mb/s. Não corresponde ao débito máximo, uma vez que este é 600 Mb/s (figura 2).

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30m	2.4 GHz
802.11g	2003	54 Mbps	30m	2.4 GHz
802.11n (WiFi 4)	2009	600 Mbps	70m	2.4, 5 GHz
802.11ac (WiFi 5)	2013	3.47 Gbps	70m	5 GHz
802.11ax (WiFi 6)	2020	14 Gbps	70m	2.4, 5 GHz
802.11af	2014	35 – 560 Mbps	1 km	unused TV bands (54-790 MHz)
802.11ah	2017	347 Mbps	1 km	900 MHz

Figure 2: IEEE 802.11 Wireless LAN

2.4 Execício 4

Verifique qual a força do sinal (*Signal strength*) e a qualidade expectável de receção da trama, sabendo que:

Signal strength	Expected Quality
-90dBm	Chances of connecting are very low at this level
-80dBm	Unreliable signal strength
-67dBm	Reliable signal strength– the edge of what Cisco considers to be adequate to support Voice over WLAN
-55dBm	Anything down to this level can be considered excellent signal strength.
-30dBm	Maximum signal strength, you are probably standing right next to the access point.

A força do sinal é de -92dBm, como podemos ver na figura 1. Como podemos ver pela tabela acima quando a força do sinal é -90 dBm, a probabilidade da conexão ser estabelecida é bastante reduzida, o que significa que, a probabilidade de receber tramas, nestas condições, é ainda menor.

3 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 55 (nosso nº de TurnoGrupo), responda às seguintes questões.

3.1 Execício 5

Selecione uma trama *beacon* cuja ordem (ou terminação) corresponda a 55. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

Uma vez que a trama que já estávamos analisar (trama de ordem 55) é uma trama *beacon* decidimos continuar a analisar essa mesma trama.

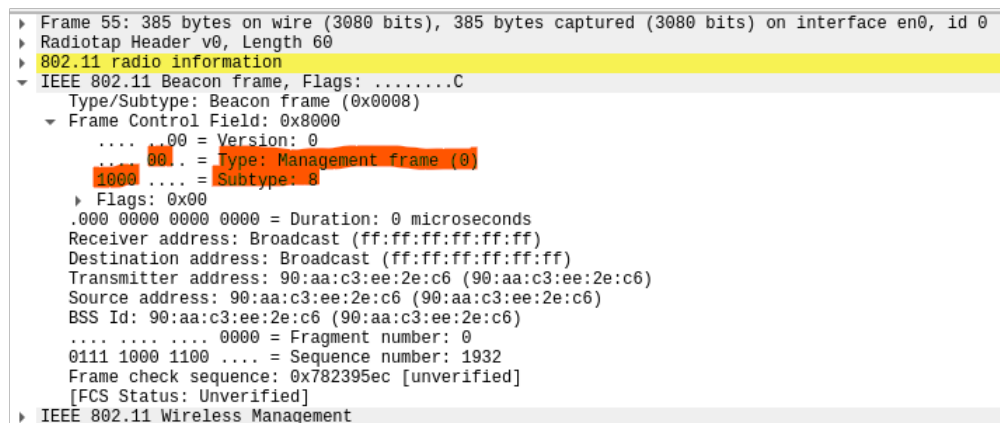


Figure 3: Trama de ordem 55

A trama é do tipo *Management* e o seu subtipo é 8 ('1000'), cuja descrição é *Beacon*, como podemos ver na figura 4. Na figura 3 estão destacados os campos do cabeçalho em que nos baseamos para responder à questão.

Type value B3 B2	Type description	Subtype value B7 B6 B5 B4	Subtype description
00	Management	0111	Reserved
00	Management	1000	Beacon

Figure 4: Excerto do Anexo - Trama 802.11 + Tipos e subtipos de tramas

3.2 Execício 6

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

Os endereços MAC em uso, na trama 55, são:

Receiver Address ff:ff:ff:ff:ff:ff

Destination Address ff:ff:ff:ff:ff:ff

Transmitter Address 90:aa:c3:ee:2e:c6

Source Address 90:aa:c3:ee:2e:c6

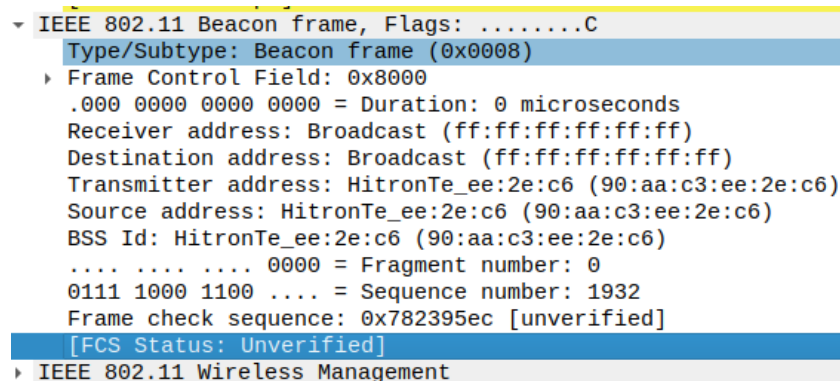
Tanto o *Receiver Address* como o *Destination Address* têm como endereço MAC um endereço de *broadcast*, o que indica que a trama está a ser transmitida para todos os dispositivos na área de alcance do ponto de acesso, enquanto o endereço de origem é 90:aa:c3:ee:2e:c6.

3.3 Execício 7

Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

Como podemos verificar pela figura 5 (*flag* destacada), o método de deteção de erros (CRC), não é verificado nesta camada, pois o uso do CRC depende do protocolo da camada superior que é usado.

É necessário usar deteção de erros em redes sem fios, pois devido a existir interferência com o meio ambiente, como, por exemplo, dispositivos eletrónicos e ruídos elétricos; existir atenuação do sinal devido a obstáculos físicos e a própria distância entre o transmissor e o recetor; erros de transmissão, como colisões, ruídos do canal e colisões; e, por fim, mobilidade, pois é uma rede bastante usada em dispositivos móveis, como telemóveis. Todos estes motivos fazem com que exista erros em redes sem fios, daí a sua importância no seu uso.



```
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ▶ Frame Control Field: 0x8000
    .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_ee:2e:c6 (90:aa:c3:ee:2e:c6)
    Source address: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
    BSS Id: HitronTe_ee:2e:c6 (90:aa:c3:ee:2e:c6)
    .... .... 0000 = Fragment number: 0
    0111 1000 1100 .... = Sequence number: 1932
    Frame check sequence: 0x782395ec [unverified]
  [FCS Status: Unverified]
  ▶ IEEE 802.11 Wireless Management
```

Figure 5: Frame Check Sequence

As tramas *beacon* permitem especificar parâmetros de funcionamento úteis para apoiar a operação e a gestão das ligações em fios.

3.4 Execício 8

Uma trama *beacon* anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (*extended supported rates*). Indique quais são esses débitos.

```

> Frame 55: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
    Timestamp: 26976768387
    Beacon Interval: 0,102400 [Seconds]
    Capabilities Information: 0x0431
  > Tagged parameters (285 bytes)
    > Tag: SSID parameter set: NOS-2EC6
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
      > Tag Number: Supported Rates (1)
      > Tag length: 8
      > Supported Rates: 1(B) (0x82)
      > Supported Rates: 2(B) (0x84)
      > Supported Rates: 5.5(B) (0x8b)
      > Supported Rates: 11(B) (0x96)
      > Supported Rates: 6(B) (0x8c)
      > Supported Rates: 9 (0x12)
      > Supported Rates: 12(B) (0x98)
      > Supported Rates: 18 (0x24)
    > Tag: DS Parameter set: Current Channel: 1
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    > Tag: Country Information: Country Code PT, Environment Any
    > Tag: ERP Information
    > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
      > Tag Number: Extended Supported Rates (50)
      > Tag length: 4
      > Extended Supported Rates: 24(B) (0xb0)
      > Extended Supported Rates: 36 (0x48)
      > Extended Supported Rates: 48 (0x60)
      > Extended Supported Rates: 54 (0x6c)
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    > Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
    > Tag: Vendor Specific: Qualcomm Inc.
    > Tag: Vendor Specific: Qualcomm Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    > Tag: RSN Information
    > Tag: Vendor Specific: Microsoft Corp.: WPS

```

Figure 6: Débitos suportamos pelo AP

Os débitos são:

Supported Rates: 1, 2, 5.5, 11, 6, 9, 12, 18 Mb/s

Extended Supported Rates: 24, 36, 48, 54 Mb/s

3.5 Execício 9

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 é anunciado na trama, em **Fixed parameters** -> **Beacon Interval** que, neste caso, é 0.102400 segundos (visível na figura 6).

Na figura 7 podemos ver uma sequencia de 3 tramas *beacons* consecutivas provenientes do mesmo AP. Após calcularmos a diferença dos tempos de receção das tramas:

Diferença entre a trama de ordem 68 e 55 : 0.102378 segundos

Diferença entre a trama de ordem 80 e 68 : 0.101284 segundos

Apesar de não ser exatamente 0.102400 segundos, o intervalo de tempo é bastante próximo.

```

55 0.462093 90:aa:c3:ee:2e:c6 Broadcast 802.11 385 Beacon frame, SN=1932, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
68 0.564471 90:aa:c3:ee:2e:c6 Broadcast 802.11 385 Beacon frame, SN=1933, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6
80 0.665755 90:aa:c3:ee:2e:c6 Broadcast 802.11 385 Beacon frame, SN=1934, FN=0, Flags=.....C, BI=100, SSID=NOS-2EC6

```

Figure 7: Tramas beacon consecutivas provenientes do mesmo AP

3.6 Execício 10

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).

1. MEO_WiFi;
2. MEO-9E9BB0;
3. NOS-2EC6;
4. NOS-C876;
5. MEO-FCF0A0;
6. FlyingNet;
7. MEO-D68850;
8. Masmorra do Sexo;

O filtro usado foi para obter apenas tramas de Beacon, que são enviadas pelos APs na vizinhança. (*wlan.fc.type_subtype == 8*)

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.

3.7 Execício 11

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

(*wlan.fc.type_subtype == 4*) or (*wlan.fc.type_subtype == 5*)

3.8 Execício 12

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?

No.	Time	Source	Destination	Protocol	Length	Info
151.1	3.02387	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R...C, BI=100, SSID="FlyingNet"
152.1	3.91750	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....R...C, BI=100, SSID="FlyingNet"
153.1	3.91879	HitronTe_ee:2e:c6	SamsungE_1a:10:f6	802.11	485	Probe Response, SN=2192, FN=0, Flags=.....R...C, BI=100, SSID="NOS-2EC6"
155.1	3.99123	SamsungE_1a:10:f6	Broadcast	802.11	122	Probe Request, SN=1124, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
277.2	7.18713	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
279.2	7.20237	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
314.3	2.97187	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
335.3	2.97177	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
336.3	3.00315	PTInovac_45:be:32	ea:52:54:89:2b:72	802.11	224	Probe Response, SN=2424, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
788.7	8.02632	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
789.7	8.32355	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
791.7	8.35604	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
793.7	8.38631	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
796.7	8.59430	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
797.7	8.62565	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
798.7	8.68818	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
962.9	3.98948	PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....C, BI=100, SSID="Masmorra do Sexo"
963.9	3.996704	PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....C, BI=100, SSID="Masmorra do Sexo"
964.9	3.997631	PTInovac_29:a9:c0	ARRISGro_a9:9e:98	802.11	434	Probe Response, SN=3266, FN=0, Flags=.....C, BI=100, SSID="Masmorra do Sexo"

Figure 8: Probing Request e respetiva Probing Response

A probe request vai para broadcast e a response vai para quem emitiu a request (AltoBeam_08:32:99). Isto é o host a 'perguntar' à rede pelos APs disponíveis com pelo menos um débito suportado em comum. Os APs compatíveis enviam uma probe response a publicitar o seu SSID, débitos suportados e outras capacidades 802.11 que possam.

4 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:

4.1 Execício 13

Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

```
8472 73.450739 AzureWav_0f:0e:9b HitronTe_f3:9a:46 802.11 79 Authentication, SN=262, FN=0, Flags=.....C
8473 73.450745 AzureWav_0f:0e:9b (- 802.11 48 Acknowledgement, Flags=.....C
8474 73.450775 HitronTe_f3:9a:46 AzureWav_0f:0e:9b 802.11 78 Authentication, SN=1965, FN=0, Flags=.....C
8475 73.450789 AzureWav_0f:0e:9b HitronTe_f3:9a:46 (- 802.11 48 Acknowledgement, Flags=.....C
8476 73.459546 AzureWav_0f:0e:9b HitronTe_f3:9a:46 802.11 164 Association Request, SN=263, FN=0, Flags=.....C, SSID=FlyingNet
8477 73.459553 HitronTe_f3:9a:46 AzureWav_0f:0e:9b (- 802.11 48 Acknowledgement, Flags=.....C
8478 73.459638 AzureWav_0f:0e:9b HitronTe_f3:9a:46 802.11 210 Association Response, SN=1966, FN=0, Flags=.....C
8479 73.459643 HitronTe_f3:9a:46 (- 802.11 48 Acknowledgement, Flags=.....C
```

Figure 9: Sequência de tramas

Na figura 9 conseguimos ver a sequência de tramas correspondente ao processo de associação entre o STA AzureWav_0f:0e:9b e o AP HiltroTe_f3:9a:46.

4.2 Execício 14

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

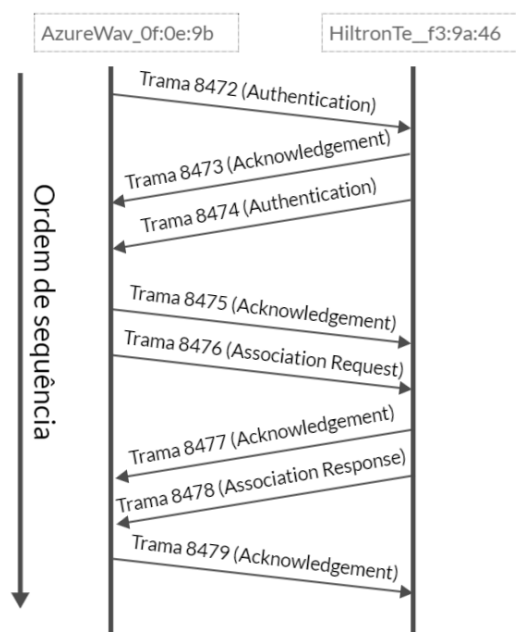


Figure 10: Diagrama da Sequência de tramas

5 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.

5.1 Execício 15

Considere a trama de dados nº8503. 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?

```
▼ IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
  ▼ Frame Control Field: 0x8841
    ....0000 = 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 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
```

Figure 11: Campo Frame Control da Trama 8053

A trama vem do STA, com destino ao sistema de distribuição, através do AP. Ou seja, não é local à WLAN.

5.2 Execício 16

Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao *router* de acesso ao sistema de distribuição (DS)?

```
▼ IEEE 802.11 QoS Data, Flags: .p.....TC
  Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8841
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    Destination address: IPv6mcast_16 (33:33:00:00:00:16)
    Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
    STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
    .... .... 0000 = Fragment number: 0
    0000 0000 0000 .... = Sequence number: 0
    Frame check sequence: 0x57cf2fa2 [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0000
  > CCMP parameters
```

Figure 12: Totalidade da Trama 8053

STA: 80:c5:f2:0f:0e:9b ; **AP:** 74:9b:e8:f3:9a:46 ; **DS:** 33:33:00:00:00:16

5.3 Execício 17

Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?

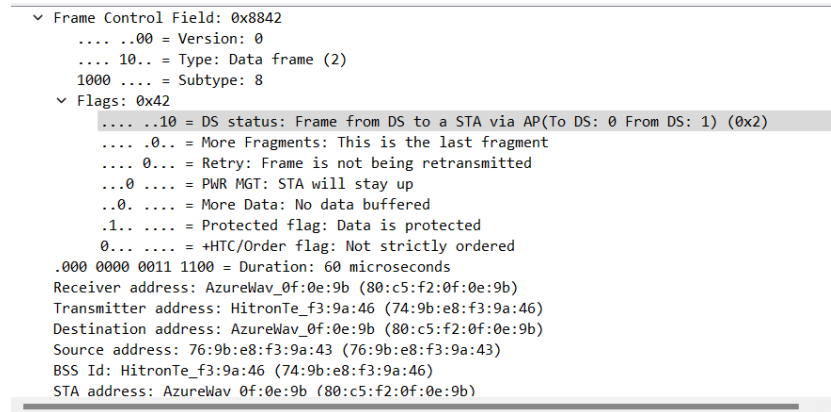


Figure 13: Trama 8521

A trama vem do sistema de distribuição, com destino ao STA, através do AP.

5.4 Execício 18

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

São transmitidas tramas de subtipos RTS, CTS, Ack e Block Ack. Estes subtipos de tramas, mais especificamente as RTS e CTS, existem para o STA poder requisitar tempo de transmissão para o AP, evitando assim o problema do terminal escondido e reduzindo eventuais erros devido a colisões.

5.5 Execício 19

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 RTS/CTS e um outro em que não é usada.

Sim, está a ser usado a opção RTS(Request to Send)/CTS(Clear to Send) para efetuar uma "pré-reserva" do acesso ao meio, como podemos verificar na figura 14.

8519 73.544155	HitronTe_f3:9a:46 (.. AzureWav_0f:0e:9b (.. 802.11	76 Request-to-send, Flags=.....C
8520 73.544159	HitronTe_f3:9a:46 (.. 802.11	72 Clear-to-send, Flags=.....C
8521 73.544163	76:9b:e8:f3:9a:43 AzureWav_0f:0e:9b 802.11	444 QoS Data, SN=2, PN=0, Flags=p....F.C

Figure 14: Sequencia de Tramas 8519,8520 e 8521

Como as *flags To Ds* e *From DS* estão a 0 (zero), então podemos concluir que as redes estão a operar localmente. O AP envia um RTS ao STA e, em seguida, o STA envia um

CTS ao AP. Desta forma, os únicos sistemas envolvidos são o AP (HitronTe_f3:9a:46) e o STA(AzureWav_0f:0e:9b).

```

> Frame 8519: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Request-to-send, Flags: .....C
  Type/Subtype: Request-to-send (0x001b)
  > Frame Control Field: 0xb400
    ....0000 = Version: 0
    ....01.. = Type: Control frame (1)
    1011 .... = Subtype: 11
    > Flags: 0x00
      ....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... .... = +HTC/Order flag: Not strictly ordered

```

Figure 15: Trama 8519 - Request to Send

Exemplo de transferência de dados em que não é usada a opção RTS/CTS:

388 3.783108	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	88 QoS Null function (No data), SN=457, FN=0, Flags=.....TC
381 3.783119	AzureWav_0f:0e:9b	AzureWav_0f:0e:9b (-	802.11	48 Acknowledgement, Flags=.....C
382 3.783121	AzureWav_0f:0e:9b	76:9b:e8:f3:9a:43	802.11	1/2 QoS Data, SN=910, FN=0, Flags=p.....TC

Figure 16: Trama 382

6 Conclusão

Este trabalho prático mostrou ser o mais desafiante até agora, talvez por ser o último, ou por consistir na consolidação e uso de todos os conhecimentos retidos até agora na UC de Redes de Computadores. O desafio motivou uma aprendizagem mais sólida dos conteúdos - mais concretamente nas diferenças entre o funcionamento de redes WiFi 802.11 e redes Ethernet.