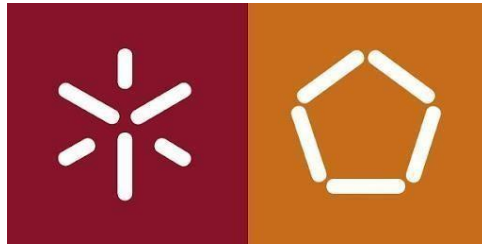


Universidade do Minho
Licenciatura em Engenharia Informática



Redes de Computadores
Trabalho prático 3

Braga, Maio 2023

Trabalho realizado por:

João Ricardo Ribeiro Rodrigues – a100598

Rafael Lima Mesquita - a95097

Sandra Fabiana Pires Cerqueira – a100681

Índice

Trabalho realizado por:

Exercício 1	1
Exercício 2	3
Exercício 3	4
Exercício 4	4
Exercício 5	5
Exercício 6	6
Exercício 7	7
Exercício 8	8
Exercício 9	9
Exercício 10	10
Exercício 11	10
Exercício 12	11
Exercício 13	11
Exercício 14	13
Exercício 15	13
Exercício 16	14
Exercício 17	15
Exercício 18	15
Exercício 19	16
Conclusões	17
	18

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.

Selecione a trama de ordem XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

Tendo então em consideração o nosso número de grupo seleccionámos a trama de ordem 36 (Fig.1).

No.	Time	Source	Destination	Protocol	Length	Info
33	0.219227	PTInovac_29:a9:c2	Broadcast	802.11	270	Beacon frame, SN=3067, FH=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
34	0.220535	PTInovac_d6:88:50 (00:06:91:d6:...	ce:90:6f:21:42:3a (ce:90:6f:21:...	802.11	68	802.11 Block Ack, Flags=.....C
35	0.235486	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=2406, FH=0, Flags=.....C, BI=100, SSID="MEO-9E9BB0"
36	0.235491	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2407, FH=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
37	0.235592	PTInovac_d6:88:50 (00:06:91:d6:...	ce:90:6f:21:42:3a (ce:90:6f:21:...	802.11	76	Request-to-send, Flags=.....C
38	0.235595	PTInovac_d6:88:50 (00:06:91:d6:...	ce:90:6f:21:42:3a (ce:90:6f:21:...	802.11	76	Request-to-send, Flags=.....C
39	0.241778	PTInovac_d6:88:50 (00:06:91:d6:...	ce:90:6f:21:42:3a (ce:90:6f:21:...	802.11	68	802.11 Block Ack, Flags=.....C
40	0.257305	HitronTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1930, FH=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
41	0.257311	HitronTe_ee:2e:c6	Broadcast	802.11	452	Beacon frame, SN=1765, FH=0, Flags=.....C, BI=100, SSID="NOS-2EC6"


```

> Frame 36: 254 bytes on wire (2032 bits), 254 bytes captured (2032 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
0000 00 00 3c 00 6b 88 1c 40 4f 4d 04 00 00 00 00 00
0010 10 b2 6c 09 80 04 ab a3 00 01 00 00 80 04 01 00
0020 6c 09 01 22 1f 08 00 69 00 00 00 00 00 00 00 96
0030 00 10 18 03 06 00 01 05 10 06 b6 b3 80 00 00 00
0040 ff ff ff ff ff ff 06 91 9e 9b b2 00 06 91 9e
0050 9b b2 70 96 a4 ff 53 7f b8 01 00 00 64 00 01 14
0060 00 08 4d 45 4f 2d 57 69 46 69 01 08 82 84 8b 96
0070 24 30 48 6c 03 01 01 05 04 00 01 00 00 2a 01 04
0080 32 04 0c 12 18 60 0b 05 00 00 1d 00 00 42 01 00
0090 46 05 00 00 00 00 65 2d 1a ad 08 17 ff ff ff 00
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0 00 00 00 3d 16 01 08 04 00 00 00 00 00 00 00
00c0 00 00 00 00 00 00 00 00 00 00 7f 08 04 00 00
00d0 00 00 00 00 4d 09 00 10 18 02 00 00 1c 00 00
00e0 dd 18 00 50 f2 02 01 01 84 00 03 a4 00 00 27 a4
00f0 00 00 42 43 5e 00 62 32 2f 00 4d 50 72 77

```

Figura 1-Trama de ordem 36

Exercício 1

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

Tendo então em consideração a trama de ordem 36, a rede sem fios está a operar na frequência 2412 MHz e no canal 1, tal como se pode ver na Fig.2.

>	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: True
	FEC: BEC (0)
	Data rate: 6,5 Mb/s
	Channel: 1
	Frequency: 2412MHz
	Signal strength (dBm): -85 dBm
	Noise level (dBm): -93 dBm
	Signal/noise ratio (dB): 8 dB
	TSF timestamp: 281935

Figura 2-Trama 802.11 correspondente ao nosso grupo (36)

Exercício 2

Questão: *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. Podemos verificar isto no campo *PHY type* da figura 3.

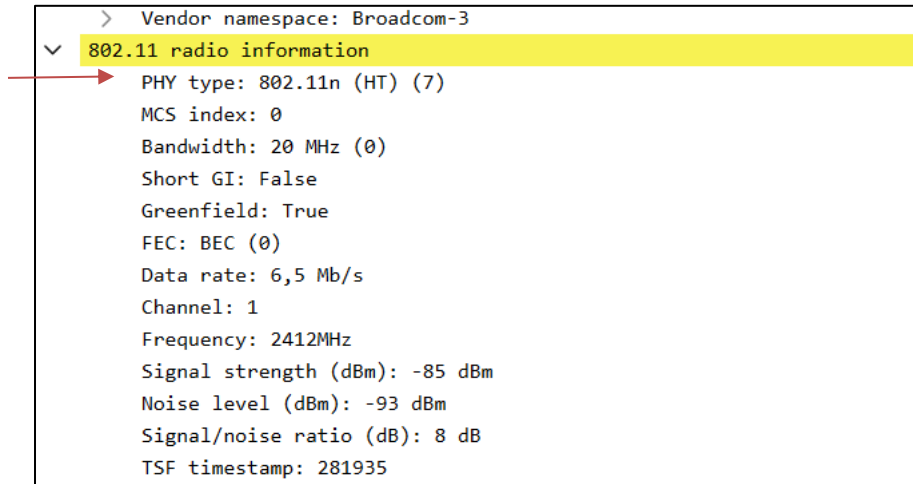


Figura 3- Trama 802.11 correspondente ao nosso grupo (36)

Exercício 3

Questão: *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 com um débito de 6,5 Mb/s. Este valor não corresponde ao débito máximo desta interface Wi-Fi, uma vez que o débito máximo da versão 802.11n da norma IEEE 802.11 é de 600 Mb/s.

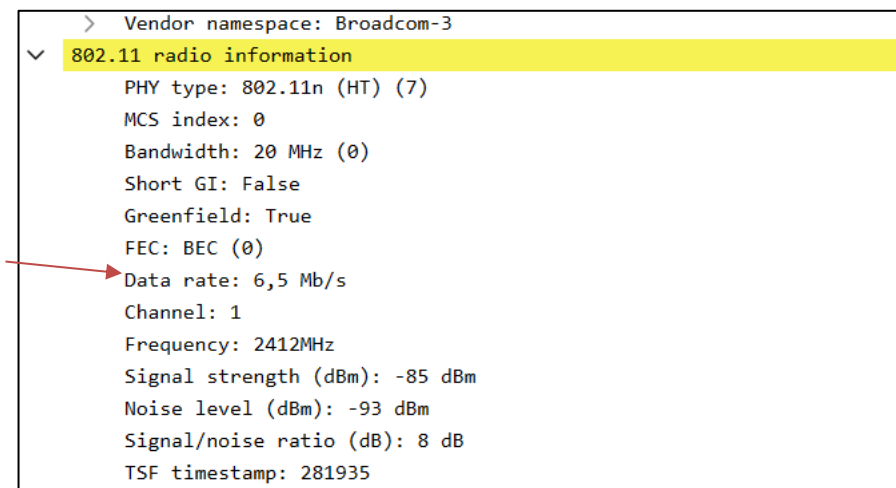


Figura 4-Trama 802.11 correspondente ao nosso grupo (36)

Exercício 4

Questão: 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 -85 dBm, tal como se verifica na Fig.5, a qualidade expectável da receção da trama está entre -80dBm e -90dBm, ou seja, entre “Unreliable signal strength” e “Chances of connecting are very low at this level”, logo não é expectável uma boa qualidade na receção da trama.

```

802.11 radio information
PHY type: 802.11n (HT) (7)
MCS index: 0
Bandwidth: 20 MHz (0)
Short GI: False
Greenfield: True
FEC: BEC (0)
Data rate: 6,5 Mb/s
Channel: 1
Frequency: 2412MHz
Signal strength (dBm): -85 dBm
Noise level (dBm): -93 dBm
Signal/noise ratio (dB): 8 dB
TSF timestamp: 281935
.... = Last part of an A-MPDU: True
.... = A-MPDU delimiter CRC error: False
A-MPDU aggregate ID: 0
    
```

Figura 5-Trama 802.11 correspondente ao nosso grupo (36)

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 TurnoGrupo (PLXX), responda às seguintes questões:

Exercício 5

Questão: *Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. 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)?*

Utilizámos o filtro “wlan.fc.type_subtype == 0x08” para obtermos apenas as tramas beacon, e como somos o grupo 36, selecionamos a trama de ordem 36, que por coincidência já era a mesma trama que estávamos a analisar nos exercícios anteriores.

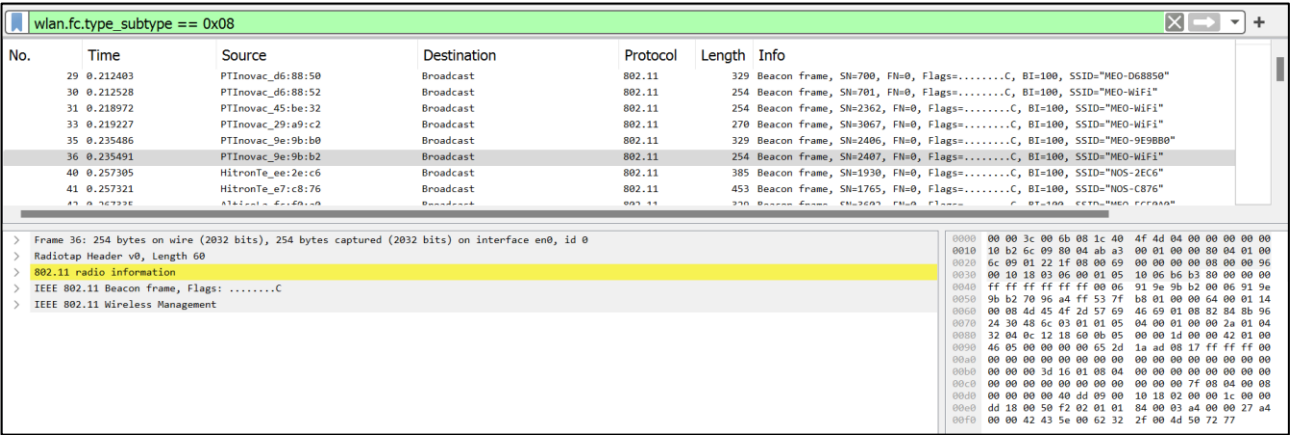


Figura 6-Seleção da trama beacon número 36

A trama selecionada é do tipo 0 (Management frame / Trama de Gestão) e de subtipo 8, estes valores estão especificados na secção “frame control” do cabeçalho, tal como se verifica na Fig.7.

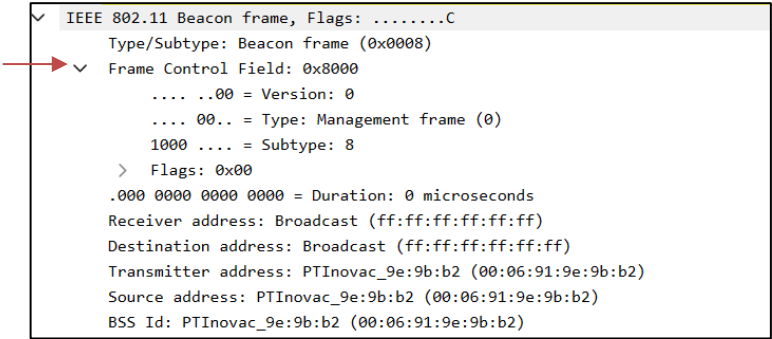


Figura 7-Tipo da trama

Com base na tabela em anexo do enunciado, podemos verificar que a nossa trama corresponde a uma trama do tipo *Management* e subtipo *Beacon* (tal como se vê na Fig.8).

00	Management	1000	Beacon
----	------------	------	--------

Figura 8- Entrada na tabela em anexo

Exercício 6

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

Os endereços MAC, tal como se verifica na Fig.9, em uso são :

Receiver address : ff:ff:ff:ff:ff:ff
 Destination address : ff:ff:ff:ff:ff:ff
 Transmitter address : 00:06:91:9e:9b:b2
 Source address: 00:06:91:9e:9b:b2

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.

```
> Frame 36: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
> 802.11 radio information
✓ 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: PTInovac_9e:9b:b2 (00:06:91:9e:9b:b2)
        → Source address: PTInovac_9e:9b:b2 (00:06:91:9e:9b:b2)
        BSS Id: PTInovac_9e:9b:b2 (00:06:91:9e:9b:b2)
        .... .... 0000 = Fragment number: 0
        1001 0110 0111 .... = Sequence number: 2407
        Frame check sequence: 0x7772504d [unverified]
        [FCS Status: Unverified]
```

Figura 9- Endereços MAC em uso

Exercício 7

Questão: *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.*

A deteção de erros em redes sem fios é necessária devido às interferências existentes no meio, atenuação do sinal, mobilidade dos dispositivos, taxas de erro de bits mais altas e transmissão em canais partilhados. Estes desafios específicos podem levar a que ocorram perdas de pacotes, distorções e erros de transmissão. A deteção de erros permite identificar e corrigir estes erros, melhorando, portanto, a confiabilidade e a integridade dos dados transmitidos. Ela desempenha um papel crucial na garantia de uma comunicação confiável em redes sem fios.

```
> Frame 36: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface en0, id 0
> Radiotap Header v0, Length 60
> 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: PTInovac_9e:9b:b2 (00:06:91:9e:9b:b2)
  Source address: PTInovac_9e:9b:b2 (00:06:91:9e:9b:b2)
  BSS Id: PTInovac_9e:9b:b2 (00:06:91:9e:9b:b2)
  .... .... 0000 = Fragment number: 0
  1001 0110 0111 .... = Sequence number: 2407
  Frame check sequence: 0x7772504d [correct]
  [FCS Status: Good]
> IEEE 802.11 Wireless Management
```

Figura 10- Verificação do FCS

Exercício 8

Questão: 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.

Através da figura abaixo conseguimos observar que o Access Point suporta os seguintes débitos de base:

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

Os débitos adicionais são:

- ➔ 6 Mb/s
- ➔ 9 Mb/s
- ➔ 12 Mb/s
- ➔ 48 Mb/s

```
IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 Wireless Management
> Fixed parameters (12 bytes)
✓ Tagged parameters (154 bytes)
  > Tag: SSID parameter set: "MEO-WiFi"
  ✓ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [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: 18 (0x24)
    Supported Rates: 24 (0x30)
    Supported Rates: 36 (0x48)
    Supported Rates: 54 (0x6c)
  > Tag: DS Parameter set: Current Channel: 1
  > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
  > Tag: ERP Information
  ✓ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 4
    Extended Supported Rates: 6 (0x0c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12 (0x18)
    Extended Supported Rates: 48 (0x60)
```

Figura 11-Débitos da trama beacon do nosso grupo

Exercício 9

Questão: 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, tal como se vê no campo “Beacon Interval” da Fig.12, é de 0.102400 segundos. Na prática este valor corresponde a uma aproximação do valor real/preciso, uma vez que o AP pode estar ocupado no preciso momento em que é suposto enviar a trama beacon, originando então um pequeno atraso no envio da mesma.

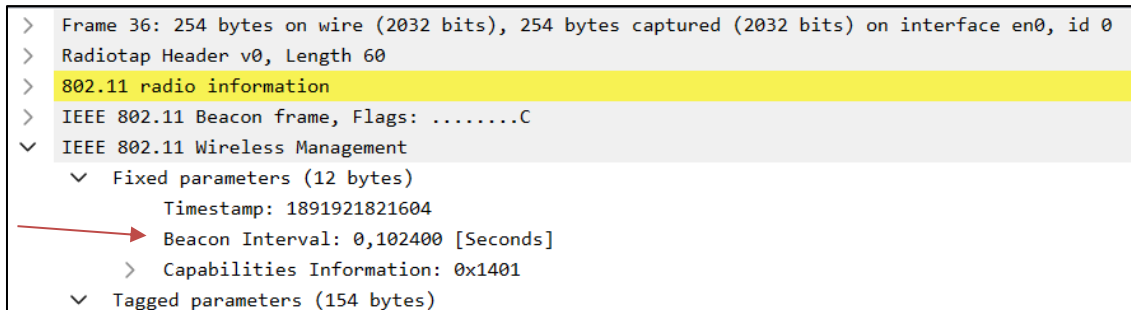


Figura 12-Fixed parameters da nossa trama beacon

Exercício 10

Questão: 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).

Alguns dos SSIDs dos APs que estão a operar na vizinhança da STA de captura são:

MEO – D68850
 MEO – FCF0A0
 MEO – 9E9BB0
 NOS – 2EC6
 NOS – C876
 FlyingNet

Para obter esta informação recorreremos ao uso do filtro “wlan.ssid” e analisámos o campo ssid .

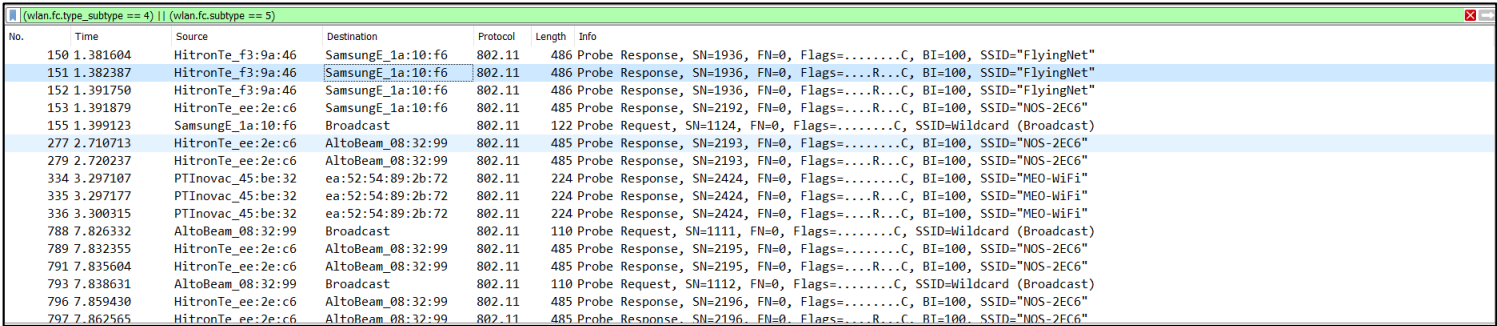
No.	Time	Source	Destination	Protocol	Length	Info
3	0.005857	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=696, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
4	0.008710	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=697, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
5	0.011922	PTInovac_45:be:32	Broadcast	802.11	254	Beacon frame, SN=2358, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
6	0.028491	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2403, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
8	0.050713	HitronTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1928, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
9	0.053270	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1763, FN=0, Flags=.....C, BI=100, SSID="NOS-C876"
10	0.062174	AlticeLa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3598, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"
11	0.062181	AlticeLa_fc:f0:a2	Broadcast	802.11	254	Beacon frame, SN=3599, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
12	0.087642	HitronTe_f3:9a:a2	Broadcast	802.11	386	Beacon frame, SN=956, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
15	0.110775	PTInovac_d6:88:50	Broadcast	802.11	329	Beacon frame, SN=698, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
16	0.110784	PTInovac_d6:88:52	Broadcast	802.11	254	Beacon frame, SN=699, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
17	0.131556	PTInovac_9e:9b:b0	Broadcast	802.11	329	Beacon frame, SN=2404, FN=0, Flags=.....C, BI=100, SSID="MEO-9E9BB0"
18	0.131662	PTInovac_9e:9b:b2	Broadcast	802.11	254	Beacon frame, SN=2405, FN=0, Flags=.....C, BI=100, SSID="MEO-WiFi"
19	0.154876	HitronTe_ee:2e:c6	Broadcast	802.11	385	Beacon frame, SN=1929, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
20	0.154922	HitronTe_e7:c8:76	Broadcast	802.11	453	Beacon frame, SN=1764, FN=0, Flags=.....C, BI=100, SSID="NOS-C876"
21	0.164886	AlticeLa_fc:f0:a0	Broadcast	802.11	329	Beacon frame, SN=3600, FN=0, Flags=.....C, BI=100, SSID="MEO-FCF0A0"

Figura 13- Parte do output do filtro "wlan.ssid"

Exercício 11

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

O filtro `(wlan.fc.type_subtype == 4) || (wlan.fc.subtype == 5)` permite-nos visualizar todas as tramas probing request e probing response simultaneamente.



No.	Time	Source	Destination	Protocol	Length	Info
150	1.381604	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
151	1.382387	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
152	1.391750	HitronTe_f3:9a:46	SamsungE_1a:10:f6	802.11	486	Probe Response, SN=1936, FN=0, Flags=.....C, BI=100, SSID="FlyingNet"
153	1.391879	HitronTe_ee:2e:c6	SamsungE_1a:10:f6	802.11	485	Probe Response, SN=2192, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
155	1.399123	SamsungE_1a:10:f6	Broadcast	802.11	122	Probe Request, SN=1124, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
277	2.710713	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	2.720237	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2193, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"
334	3.297107	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	3.297177	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	3.300315	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	7.826332	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
789	7.832355	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	7.835604	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	7.838631	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1112, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
796	7.859430	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	7.862565	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2196, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"

Figura 14- Filtro `wlan.fc.type_subtype == 4 || wlan.fc.subtype == 5`

Exercício 12

Questão: 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?

Um probing request tem a função de obter informações acerca de Aps. A probing response irá ser proveniente de um Ap, fornecendo-lhe informações de si mesmo.

Neste caso, como o receiver address e o destination address do probing request são endereçados ao Broadcast address, entende-se que esta trama foi enviada com o objetivo de alcançar todos os AP ao alcance da STA a enviar o probing request.

788	7.826332	AltoBeam_08:32:99	Broadcast	802.11	110	Probe Request, SN=1111, FN=0, Flags=.....C, SSID=wildcard (Broadcast)
789	7.832355	HitronTe_ee:2e:c6	AltoBeam_08:32:99	802.11	485	Probe Response, SN=2195, FN=0, Flags=.....C, BI=100, SSID="NOS-2EC6"

Figura 15- Probing request com probing response

```

> Frame 788: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface en0, id 0
> Radiotap Header v0, Length 36
> 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: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
    Source address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... 0000 = Fragment number: 0
    0100 0101 0111 .... = Sequence number: 1111
    Frame check sequence: 0x098f83be [unverified]
    [FCS Status: Unverified]
  > IEEE 802.11 Wireless Management

```

Figura 16- Detalhes do probing request enviado

```

Frame 789: 485 bytes on wire (3880 bits), 485 bytes captured (3880 bits) on interface en0, id 0
Radiotap Header v0, Length 36
802.11 radio information
IEEE 802.11 Probe Response, Flags: .....C
  Type/Subtype: Probe Response (0x0005)
  > Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
    Destination address: AltoBeam_08:32:99 (a4:ef:15:08:32:99)
    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
    1000 1001 0011 .... = Sequence number: 2195
    Frame check sequence: 0xd9b31174 [unverified]
    [FCS Status: Unverified]

```

Figura 17- Detalhes do probing response ao proving request anterior

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:

Exercício 13

Questão: *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.*

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 filtrar as tramas de modo a encontrar mais facilmente tramas com “Authentication”, “Association Request” e “Association Response”, após a remoção do filtro é possível observar, tal como na Fig.18, 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 da autenticação.

8472 73.450730	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70 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	70 Authentication, SN=1965, FN=0, Flags=.....C
8475 73.450780		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		AzureWav_0f:0e:9b (...)	802.11	48 Acknowledgement, Flags=.....C
8478 73.459638	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	210 Association Response, SN=1966, FN=0, Flags=.....C
8479 73.459643		HitronTe_f3:9a:46 (...)	802.11	48 Acknowledgement, Flags=.....C

Figura 18- Sequência de tramas relativas ao processo de associação

Exercício 14

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

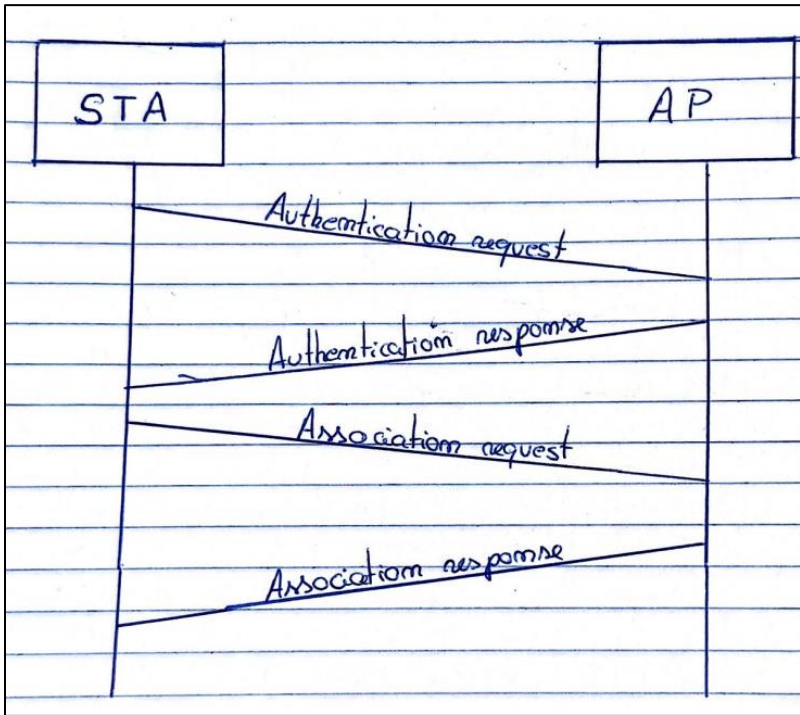


Figura 19- Diagrama da sequência de todas as tramas

Processo de Associação

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.

Exercício 15

Questão: 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?

Pelo campo “*DS status*” conseguimos verificar que o valor do “*To DS*” é 1 e o do campo “*From DS*” é 0. O valor destas flags permite-nos tirar conclusões acerca da direcionalidade da trama, esta vem para o DS a partir do STA. Assim podemos concluir que a direcionalidade da trama é local à WLAN.

No.	Time	Source	Destination	Length	Protocol	Info
8501	73.511579	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	73	802.11	Action, SN=0, FN=0, Flags=.....
8502	73.511582		HitronTe_f3:9a:46 (74:9b:e8:f3:...	48	802.11	Acknowledgement, Flags=.....C
8503	73.511585	AzureWav_0f:0e:9b	IPv6mcast_16	188	802.11	QoS Data, SN=0, FN=0, Flags=.p...
8504	73.511588	HitronTe_f3:9a:46 (74:9b:e8:f3:...	AzureWav_0f:0e:9b (80:c5:f2:0f:...	68	802.11	802.11 Block Ack, Flags=.....C
8505	73.530748	PTinovac_d6:88:50	Broadcast	329	802.11	Beacon frame, SN=2251, FN=0, Flag
8506	73.530757	AzureWav_0f:0e:9b	Broadcast	440	802.11	QoS Data, SN=1, FN=0, Flags=.p...
8507	73.530760	HitronTe_f3:9a:46 (74:9b:e8:f3:...	AzureWav_0f:0e:9b (80:c5:f2:0f:...	68	802.11	802.11 Block Ack, Flags=.....C
8508	73.531678	PTinovac_d6:88:52	Broadcast	254	802.11	Beacon frame, SN=2252, FN=0, Flag
8509	73.534969	PTinovac_45:be:32	Broadcast	254	802.11	Beacon frame, SN=3831, FN=0, Flag
8510	73.542828	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	73	802.11	Action, SN=1, FN=0, Flags=.....
8511	73.542835		HitronTe_f3:9a:46 (74:9b:e8:f3:...	48	802.11	Acknowledgement, Flags=.....C

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... = +HTC/Order flag: Not strictly ordered

000 0000 0011 0000 = Duration: 48 microseconds

Figura 20 - Frame Control da trama nº8503

Exercício 16

Questão: 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)?

Endereço STA: 74:9b:e8:f3:9a:46 (Receiver address)

Endereço AP: 80:c5:f2:0f:0e:9b (Transmitter address)

Endereço router de acesso: 33:33:00:00:00:16 (Destination address)

```

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
  
```

Figura 20- Endereços MAC da trama de dados nº8503

Exercício 17

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

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

No.	Time	Source	Destination	Length	Protocol	Info
8514	73.544132	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	73	802.11	Action, SH=2, FH=0, Flags=.....C, Dialog Token=1
8515	73.544136	HitronTe_f3:9a:46	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	48	802.11	Acknowledgement, Flags=.....C
8516	73.544143	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	73	802.11	Action, SH=613, FH=0, Flags=.....C, Dialog Token=1
8517	73.544147	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	73	802.11	Action, SH=613, FH=0, Flags=.....R...C, Dialog Token=1
8518	73.544151	HitronTe_f3:9a:46	AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	48	802.11	Acknowledgement, Flags=.....C
8519	73.544155	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	76	802.11	Request-to-send, Flags=.....C
8520	73.544159	HitronTe_f3:9a:46	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	72	802.11	Clear-to-send, Flags=.....C
8521	73.544163	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	444	802.11	QoS Data, SH=2, FH=0, Flags=p....F.C
8522	73.544167	AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	68	802.11	802.11 Block Ack, Flags=.....C
8523	73.544170	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)	76	802.11	Request-to-send, Flags=.....C
8524	73.544174	HitronTe_f3:9a:46	HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)	72	802.11	Clear-to-send, Flags=.....C

IEEE 802.11 QoS Data, Flags: .p....F.C		0000 00 10 18 03 04 00 ec 39 c4 01 88 42 3c 00 80 c5
Type/Subtype: QoS Data (0x0028)		0040 f2 0f 0e 9b 74 9b e8 f3 9a 46 76 9b e8 f3 9a 43
Frame Control Field: 0x8842		0050 20 00 00 00 05 00 00 20 00 00 00 00 1d b1 23 ae
.... 00 = Version: 0		0060 32 cc a0 b6 57 e7 da 3c 66 0a 5d 61 6a 9c 00 af
.... 10.. = Type: Data frame (2)		0070 fe 9b 6a e4 f9 7e ec 39 dd 87 73 3a 96 02 94 38
1000 = Subtype: 8		0080 0d 8f 6b b0 7f 05 7b a0 a5 40 4f 6d 9a 1d 1b 17
Flags: 0x42		0090 0d 60 65 4e 56 d5 ef ad 03 04 0e 88 fe 2c e1 bb
.... 10 = DS status: Frame from DS to a STA via AP (To DS: 0 From DS: 1) (0x2)		00a0 1f c2 9f e8 73 c6 d6 98 5e d1 bb 43 83 f7 fb 65
.... 0... = More Fragments: This is the last fragment		00b0 e3 6b 8a 61 7c dd 3f d7 f8 01 84 0c 14 db 41 37
.... 0... = Retry: Frame is not being retransmitted		00c0 47 f7 98 77 4e c7 ba 96 94 cf d6 b2 39 47 54 0b
...0 = PWR MGT: STA will stay up		00d0 91 6d 68 3c 25 3d 51 dd 99 ba 74 91 1c 80 62 8f
..0 = More Data: No data buffered		00e0 ba 69 39 49 c0 a0 44 3c 29 04 26 cd bb ad 63 73
..1 = Protected flag: Data is protected		00f0 1d f4 dd 98 22 58 d0 7c 7e e7 32 35 b7 dd 67 fc
0... = HT/Order flag: Not strictly ordered		0100 3c b1 53 01 03 e5 29 95 93 97 05 46 9c 65 5b 53
.000 0000 0011 1100 = Duration: 60 microseconds		0110 12 39 2a 58 eb 75 af 6a dc 99 d6 cb c0 58 b6 fd
Receiver address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)		0120 4e 1a f8 d7 2c 3a b0 e1 b8 05 cf c0 eb 51 bd 95
Transmitter address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)		0130 91 53 fd 61 d1 e8 17 08 c4 25 7d d4 92 b7 48 0e
Destination address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)		0140 9f 85 a1 de 84 b5 dd ce 89 0a 72 da c9 6f ad 33
		0150 4e 1a f8 d7 2c 3a b0 e1 b8 05 cf c0 eb 51 bd 95
		0160 48 6c b2 e4 ff e1 a6 ed fe 93 94 07 63 da 7b 9a
		0170 37 a1 cb eb 68 10 fe 1e 08 0e 1e 7b 37 28 c7 81
		0180 57 bd 53 7b 7f ab 88 2a 75 48 6d 6d 00 a6 fa ae

Figura 21- Trama Nº 8521

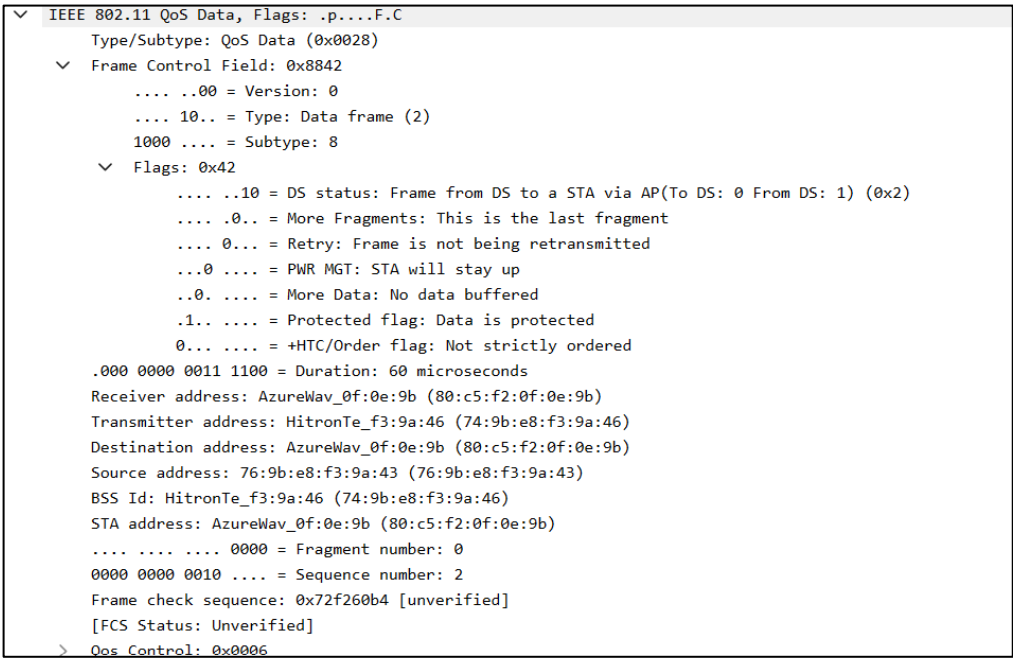


Figura 22- Frame Control Field da Trama Nº 8521

Exercício 18

Questão: 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.)

Na transferência de dados acima mencionada são transmitidas as tramas de controlo ACK (Acknowledge). Estas tramas são necessárias como indicador de que a transmissão foi efetuada com sucesso, servindo como aviso positivo de que a transferência ocorreu sem erros. Isto não é necessário numa rede Ethernet pois essas tramas são enviadas por cabo e, nesse caso, o envio de uma trama é considerado bem-sucedido se nenhum problema de colisão ocorrer durante a transmissão. Se um problema ocorrer, os dispositivos na rede irão detetar essas colisões sem necessidade das tramas ACK.

8516	73.544143	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=613, FN=0, Flags=.....C, Dialog Token=1
8517	73.544147	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	73 Action, SN=613, FN=0, Flags=...R...C, Dialog Token=1
8518	73.544151		AzureWav_0f:0e:9b (...	802.11	48 Acknowledgement, Flags=.....C
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, FN=0, Flags=.p....F.C

Figura 23 – Exemplo de uma trama ACK

Exercício 19

Questão: 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.

Como podemos verificar pela figura 24, no exemplo acima é de facto utilizada a opção RTS/CTS no envio do DS para uma STA, no entanto podemos ver na figura 25 um exemplo em que a opção RTS/CTS não é utilizada.

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, FN=0, Flags=.p....F.C
8522	73.544167	AzureWav_0f:0e:9b (... HitronTe_f3:9a:46 (... 802.11	68	802.11 Block Ack, Flags=.....C

Figura 24 – Uso de RTC/CTS na transferência de dados que engloba a trama Nº 8521

8499	73.511568	AzureWav_0f:0e:9b HitronTe_f3:9a:46 802.11	73	Action, SN=611, FN=0, Flags=.....C, Dialog Token=1
8500	73.511572	AzureWav_0f:0e:9b (... 802.11	48	Acknowledgement, Flags=.....C
8501	73.511579	HitronTe_f3:9a:46 AzureWav_0f:0e:9b 802.11	73	Action, SN=0, FN=0, Flags=.....C, Dialog Token=1
8502	73.511582	HitronTe_f3:9a:46 (... 802.11	48	Acknowledgement, Flags=.....C
8503	73.511585	AzureWav_0f:0e:9b IPv6mcast_16 802.11	188	QoS Data, SN=0, FN=0, Flags=.p....TC
8504	73.511588	HitronTe_f3:9a:46 (... AzureWav_0f:0e:9b (... 802.11	68	802.11 Block Ack, Flags=.....C
8505	73.530748	PTInovac_d6:88:50 Broadcast 802.11	329	Beacon frame, SN=2251, FN=0, Flags=.....C, BI=100, SSID="MEO-D68850"
8506	73.530757	AzureWav_0f:0e:9b Broadcast 802.11	440	QoS Data, SN=1, FN=0, Flags=.p....TC

Figura 25 – Não utilização de RTC/CTS na transferência de dados

Conclusões

Com este trabalho, foi possível a consolidação de alguns temas lecionados na unidade curricular de Redes de Computadores.

Em particular, a realização deste trabalho prático permitiu que o grupo de trabalho tivesse a oportunidade de aprofundar conhecimentos relativos às redes Wireless e endereçamento de tramas WI-FI, para além de mecanismos de controlo e acesso.