Tecnologias Avançadas de Redes

2º Trabalho

Compreensão do protocolo 802.11

Aluno: João Dragovic nº48015

Docente: Pedro Ribeiro

1.Que SSIDs(distintos) são anunciados pelos diferentes access-point (AP) incluídos na captura?

Nesta captura os SSIDs anunciados pelos diferentes APs são:

- eduroam
- TAR-WAP2-CHALLENGE
- Wi-Fi CARRIS
- HUAWEI-B525-FAFC
- Eduroam5G

2.Que APs (BSSID/MAC) estão a anunciar a rede eduroam?

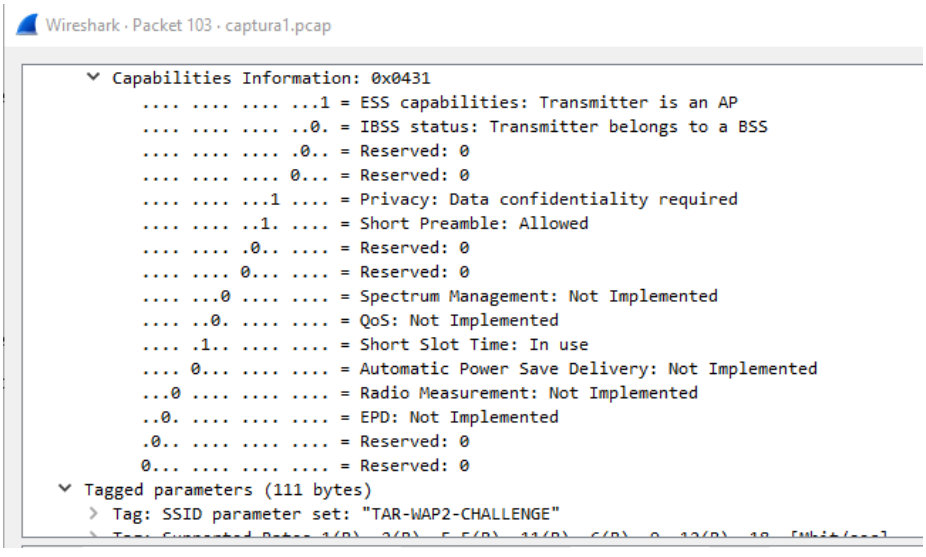
Na rede eduroam estão a anunciar vários BSSIDs/MACs:

- 00:17:0e:aa:e7:70
- 00:81:c4:c2:c3:d0
- 64:d1:54:a9:af:90
- cc:2d:e0:10:58:79
- cc:d5:39:e3:c3:70
- cc:d5:39:e3:dd:10
- cc:d5:39:e3:e1:10
- ff:ff:ff:ff:ff:ff

Nos elementos de informação incluídos na trama BEACON correspondente ao datagrama #103 capturado, o AP indica:

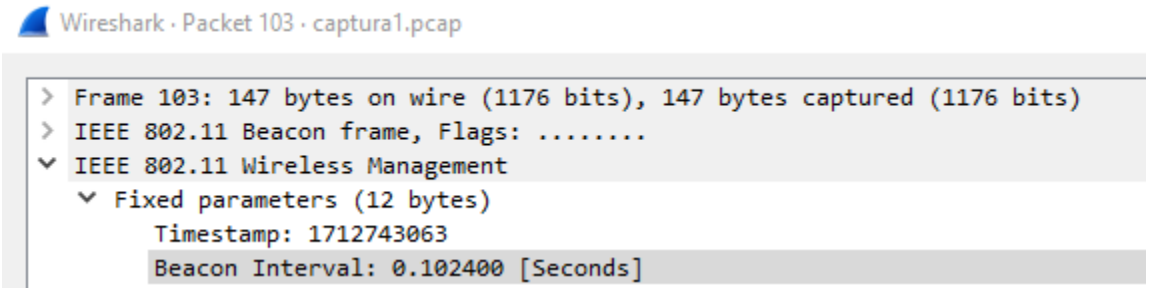
3.Suporta o uso de Short Slot Time?

Sim, não só suporta o Short Slot Time como também está em uso.



4.Qual a periodicidade anunciada para os BEACON?

O BEACON vai ter uma periodicidade com cerca de 0,1024 segundos



5.Que débitos são suportados? (nota: podem aparecer em mais que um elemento de informação)

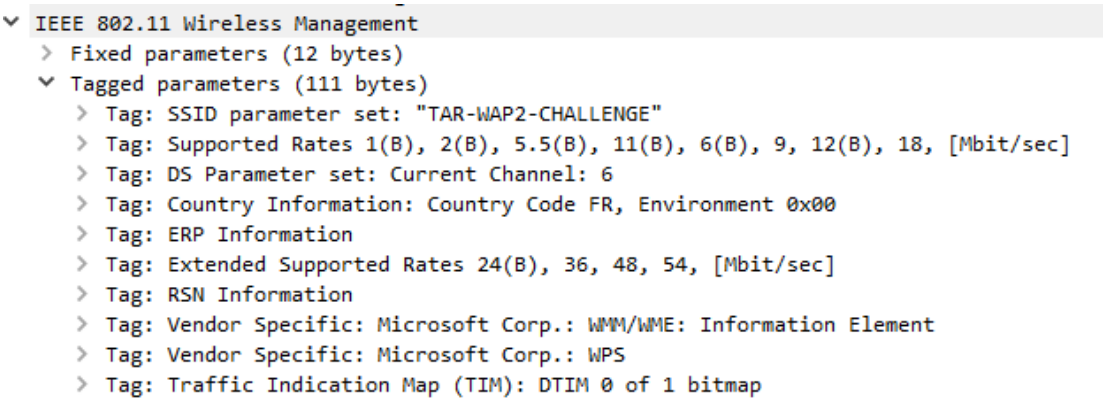
6.Quais desses débitos são considerados BASIC RATE?

Os débitos suportados são:

- 1 (BSSBasicRateSet) Mbit/s
- 2 (BSSBasicRateSet) Mbits/s
- 5,5 (BSSBasicRateSet) Mbits/s
- 6 (BSSBasicRateSet) Mbits/s
- 9 Mbits/s
- 11 (BSSBasicRateSet) Mbits/s
- 12 (BSSBasicRateSet) Mbits/s
- 18 Mbits/s

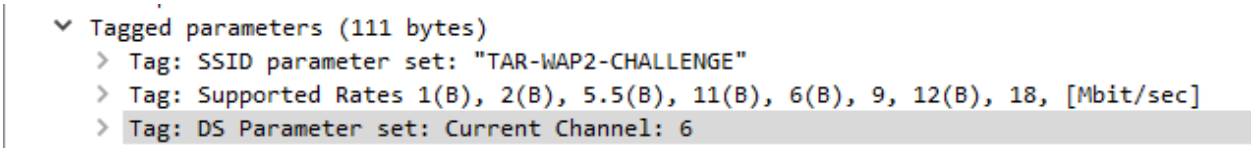
Mas também existem as “Extended Supported Rates”:

- 24 (BSSBasicRateSet) Mbits/s
- 36 Mbits/s
- 48 Mbits/s
- 54 Mbits/s



7.Em que canal está a operar o AP?

O AP está a operar no Canal 6.



8.Que adendas de IEEE802.11 são suportadas no que se refere à camada física/rádio/débitos?

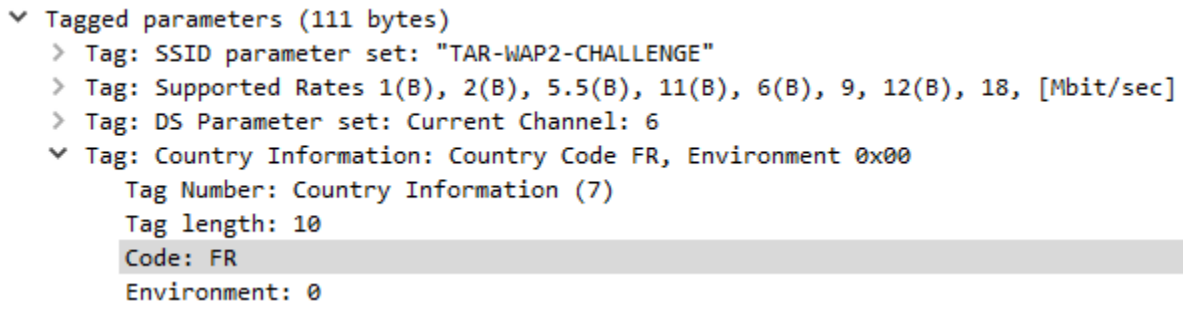
Consoante os débitos binário já referidos e a seguinte tabela, podemos assumir que este AP suporta o 802.11g.

Wi-Fi generations

Generation	IEEE standard	Adopted	Maximum link rate (Mbit/s)	Radio frequency (GHz)
Wi-Fi 7	802.11be	(2024)	1376 to 46120	2.4/5/6
Wi-Fi 6E	802.11ax	2020	574 to 9608[3]	6[4]
Wi-Fi 6		2019		2.4/5
Wi-Fi 5	802.11ac	2014	433 to 6933	5[5]
Wi-Fi 4	802.11n	2008	72 to 600	2.4/5
*(Wi-Fi 3)**	802.11g	2003	6 to 54	2.4
*(Wi-Fi 2)**	802.11a	1999	6 to 54	5
*(Wi-Fi 1)**	802.11b	1999	1 to 11	2.4
*(Wi-Fi 0)**	802.11	1997	1 to 2	2.4

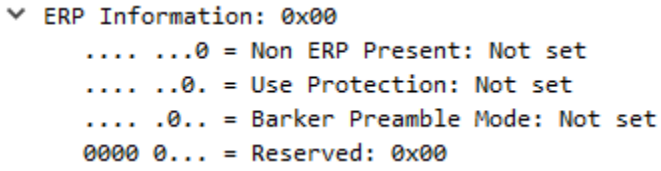
9.Em que país indica o AP estar a operar?

O AP indica estar a Operar da França pelo que se pode observar na tag “FR”.



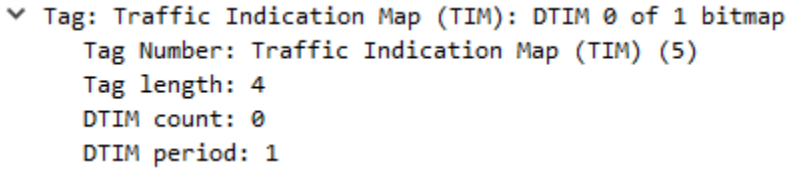
10.O AP está a recomendar aos equipamentos cliente que usem proteção CTS-to-self?

O AP não recomenda os equipamentos cliente que usem proteção pois não é necessária já que todos usam a norma 802.11g.



11.Qual a periodicidade dos BEACON que incluem anúncios DTIM?

Cada BEACON têm um DTIM, pois como podemos observar o DTIM count está a 0 e o DTIM period está a 1.



12.Que tipos de cifra são suportados nas tramas unicast?

São suportados o tipo de cifra TKIP e o AES (CCMP), consoante o código e observando a tabela:

Cypher Suit Selectors:

OUI	Suite type	Meaning
00-0F-AC	0	Use group cipher suite
00-0F-AC	1	WEP-40
00-0F-AC	2	TKIP
00-0F-AC	3	Reserved
00-0F-AC	4	CCMP – default pairwise cipher suite and default group cipher suite for data frames in an RSNA
00-0F-AC	5	WEP-104
00-0F-AC	6	BIP—default group management cipher suite in an RSNA with management frame protection enabled
00-0F-AC	7	Group addressed traffic not allowed
00-0F-AC	8–255	Reserved
Vendor OUI	Other	Vendor-specific
Other	Any	Reserved

```
▾ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) TKIP 00:0f:ac (Ieee 802.11) AES (CCM)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: TKIP (2)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: AES (CCM) (4)
```

13.Que tipos de cifra são suportados nas tramas de multicast/broadcast?

Nas tramas de multicast/Broadcast são suportadas o tipo de cifra TKIP.

```
Group Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: TKIP (2)
  Pairwise Cipher Suite Count: 2
```

14.É suportado o uso de canal de 40MHz?

Não é suportado o uso de canais com 40MHz. Apenas com 20Mhz.

```
.... .... .... ..0. = HT Support channel width: Transmitter only supports 20MHz operation
```

15.É suportado o uso de GuardInterval de 400ns em canais de 20MHz?

Sim é suportado o GI em canais de 20Mhz.

```
.... .... ..1. .... = HT Short GI for 20MHz: Supported
.... .... .0.. .... = HT Short GI for 40MHz: Not supported
```

16.Que dimensão máxima de A-MSDU é suportada?

A dimensão Máxima de A-MSDU suportada é de 7935 bytes.

```
.... 1... .... .... = HT Max A-MSDU length: 7935 bytes
```

17.Que dimensão máxima de A-MPDU é suportada?

A dimensão máxima de A-MPDU suportada é de 65535 bytes (16 bit).

```
A-MPDU Parameters: 0x1b
    .... ..11 = Maximum Rx A-MPDU Length: 0x3 (65535[Bytes])
    ...1 10.. = MPDU Density: 8 [usec] (0x6)
    000. .... = Reserved: 0x0
```

18.Qual o valor máximo de parâmetros MCS suportado? A que débito binário, modulação e número de spatial streams corresponde?

O valor máximo de parâmetros MCS suportados é de 3 (Modulação, Codificação, numero de spatial streams).

Neste caso como temos 15 de índice de MCS vamos ter 2 spatial streams, cerca de 144Mbps (em 400ns de GI) e usando modulação 64-QAM.

Lista MCS – 20MHz (Obrigatórios com Nss=1)

MCS Index	Nss	Modulation	R	Nbpsc	Nsd	Nsp	Ncbps	Ndbps	Mbps (800ns GI)	Mbps (400ns GI)
0	1	BPSK	1/2	1	52	4	52	26	6.5	7.2
1	1	QPSK	1/2	2	52	4	104	52	13.0	14.4
2	1	QPSK	3/4	2	52	4	104	78	19.5	21.7
3	1	16-QAM	1/2	4	52	4	208	104	26.0	28.9
4	1	16-QAM	3/4	4	52	4	208	156	39.0	43.3
5	1	64-QAM	2/3	6	52	4	312	208	52.0	57.8
6	1	64-QAM	3/4	6	52	4	312	234	58.5	65.0
7	1	64-QAM	5/6	6	52	4	312	260	65.0	72.2
8	2	BPSK	1/2	1	52	4	104	52	13.0	14.4
9	2	QPSK	1/2	2	52	4	208	104	26.0	28.9
10	2	QPSK	3/4	2	52	4	208	156	39.0	43.3
11	2	16-QAM	1/2	4	52	4	416	208	52.0	57.8
12	2	16-QAM	3/4	4	52	4	416	312	78.0	86.7
13	2	64-QAM	2/3	6	52	4	624	416	104.0	115.6
14	2	64-QAM	3/4	6	52	4	624	468	117.0	130.0
15	2	64-QAM	5/6	6	52	4	624	520	130.0	144.0

```
▾ Rx Supported Modulation and Coding Scheme Set: MCS Set
  ▾ Rx Modulation and Coding Scheme (One bit per modulation): 2 spatial streams
      .... .... .... .... .... .... 1111 1111 = Rx Bitmask Bits 0-7: 0xff
      .... .... .... .... 1111 1111 .... .... = Rx Bitmask Bits 8-15: 0xff
      .... .... 0000 0000 .... .... .... .... = Rx Bitmask Bits 16-23: 0x00
      0000 0000 .... .... .... .... .... .... = Rx Bitmask Bits 24-31: 0x00
      .... .... .... .... .... .... .... ...0 = Rx Bitmask Bit 32: 0x0
      .... .... .... .... .... .... .000 000. = Rx Bitmask Bits 33-38: 0x00
      .... .... ...0 0000 0000 0000 0... .... = Rx Bitmask Bits 39-52: 0x0000
      ...0 0000 0000 0000 0000 0000 000. .... = Rx Bitmask Bits 53-76: 0x000000
    .... ..00 0000 0000 = Highest Supported Data Rate: 0x000
    .... .... .... ...0 = Tx Supported MCS Set: Not defined
    .... .... .... ..0. = Tx and Rx MCS Set: Equal
    .... .... .... 00.. = Maximum Number of Tx Spatial Streams Supported: 0x0, TX MCS Set Not Defined
    .... .... ...0 .... = Unequal Modulation: Not supported
```

19.Que SSIDs procura o equipamento cliente?

O equipamento cliente (InterCol_97:ba:c9) está á procura de uma rede com SSID qualquer, ou seja está á procura de uma rede que esteja disponível pois não tem SSID no parâmetros.

```
Tag: SSID parameter set: Wildcard SSID
    Tag Number: SSID parameter set (0)
    Tag length: 0
    SSID: <MISSING>
```

20.Que débitos básicos são suportados pelo AP?

O Único débito básico suportado pelo AP é de 6 Mbits/s, como podemos observar.

```
Tag: Supported Rates 6(B), 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 6(B) (0x8c)
    Supported Rates: 9 (0x12)
    Supported Rates: 12 (0x18)
    Supported Rates: 18 (0x24)
    Supported Rates: 24 (0x30)
    Supported Rates: 36 (0x48)
    Supported Rates: 48 (0x60)
    Supported Rates: 54 (0x6c)
```

21.Que canais e restrições de potência são anunciados pelo AP?

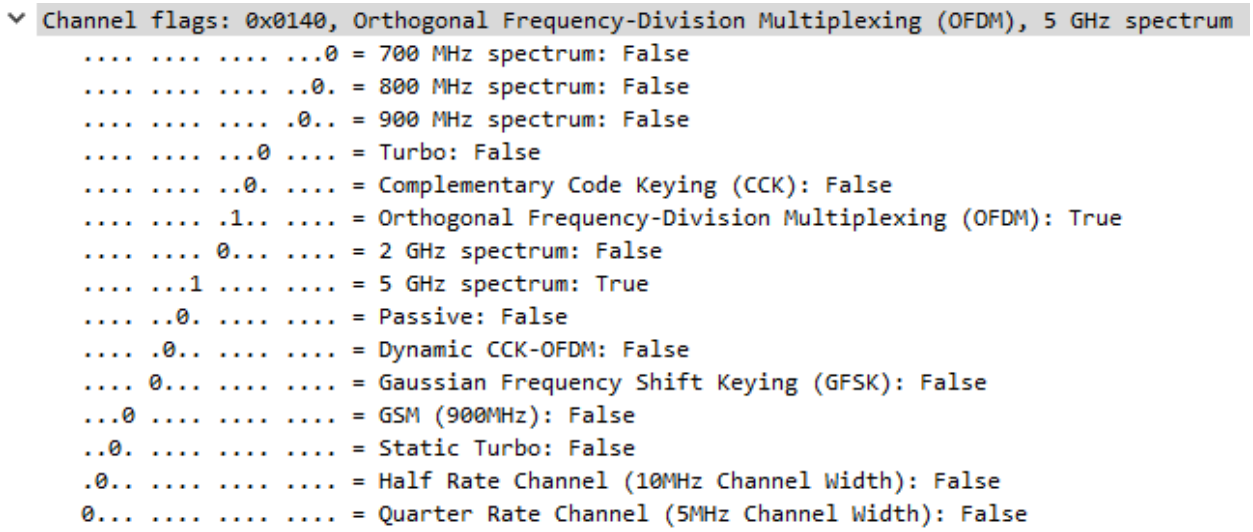
Como podemos observar o AP usa vários intervalos de canais e máximos de potência:

- 36 até 44 (8 canais), 23 dBm
- 100 até 105 (5 canais), 23 dBm
- 132 até 135 (3 canais), 30 dBm

```
Country Info: First Channel Number: 36, Number of Channels: 8, Maximum Transmit Power Level: 23 dBm
    First Channel Number: 36
    Number of Channels: 8
    Maximum Transmit Power Level: 23 dBm
Country Info: First Channel Number: 100, Number of Channels: 5, Maximum Transmit Power Level: 23 dBm
    First Channel Number: 100
    Number of Channels: 5
    Maximum Transmit Power Level: 23 dBm
Country Info: First Channel Number: 132, Number of Channels: 3, Maximum Transmit Power Level: 30 dBm
    First Channel Number: 132
    Number of Channels: 3
    Maximum Transmit Power Level: 30 dBm
```

22.Em que banda wireless foi realizada esta captura?

A banda wireless na qual foi retirada esta captura foi nos 5Ghz.



23.Que adendas de IEEE802.11 são suportadas no que se refere à camada física/rádio/débitos?

Como nesta captura podemos observar que apenas é usado o espetro 5Ghz e o máximo débito suportado é 54 Mbits/s concluímos que é usada a norma 802.11a.