

# WLAN / 802.11

## I. Objectivos

Os objectivos deste trabalho prático são:

- Observar as principais tramas 802.11
- Observar os processos de descoberta da rede 802.11
- Observar os processos de autenticação e associação
- Entender como se processa a troca de informação sobre uma rede 802.11
- Familiarizar-se com ferramentas de observação e diagnóstico de redes

## II. Duração

Este trabalho deve durar uma aula (3h).

## III. Procedimentos

Este Trabalho irá utilizar:

- 1x Access Point (AP) Cisco por sala
- 1x Servidor por sala
- 1x PC do laboratório por grupo de trabalho (STA C), com Linux
- A aplicação Wireshark disponível na STA C (d) para a captura e análise de tráfego de rede
- Aplicação iperf3 em execução como servidor da sala (b) e com clientes nos terminais dos alunos (c)
- 2x terminais dos alunos com interface WLAN/802.11 (STA A e STA B)

Diagrama:

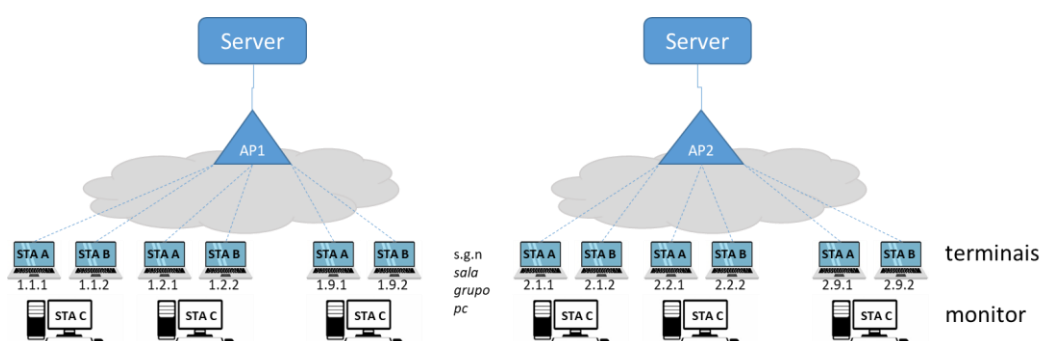


Figura 1: Diagrama de rede para a experimentação

Cada AP tem dois SSID configurados:

	AP1 (Sala 1)	AP2 (Sala 2)	Características
SSID1	ComMoveis.330.2400	ComMoveis.331.2400	2.422MHz/canal 3 e 2.442MHz/canal 7 Segurança: aberto
SSID2	ComMoveis.330.5000	ComMoveis.331.5000	5GHz, 5.200MHz/canal 40 e 5.500MHz/100, seguro: <ul style="list-style-type: none"> <li>• Password: "Lab.Com.WiFi")</li> <li>• Autenticação: WPAv2</li> <li>• Encriptação: AES-CCM</li> </ul>

Tabela 1: Diagrama da rede utilizada para o trabalho prático nº1

Os AP têm a funcionalidade de DHCPv4 server, atribuindo endereços IP na gama 10.0.{1|2}.[100-200]. O servidor da sala tem o endereço 10.0. {1|2}.2. Os AP respondem a ping, no endereço 10.0. {1|2}.1.

## 1. Preparação

- Utilizando a aplicação “LinSSID” instalada nas STA C, observe as redes 802.11 activas (escolha a aba correcta na parte inferior da aplicação: *Time Graph, 2.4 GHz Channels, 5 GHz Channels*)
  - Faça uma captura do ecrã e guarde-a (para os 2.4GHz e 5GHz) para posterior referência; não poderá fazer esta operação após os próximos passos.

### 2.4 GHz

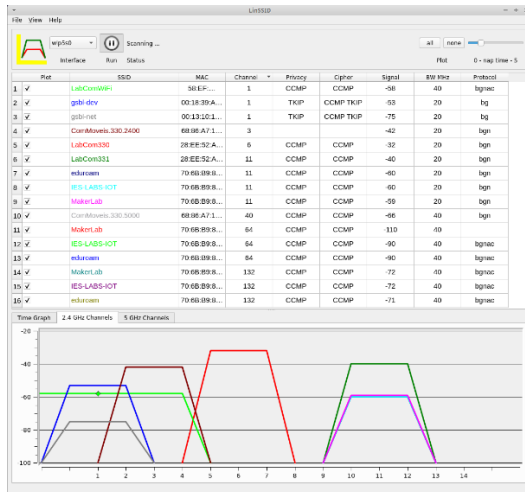


Figura 2.a: Exemplo de ecrã do LinSSID (2.4GHz)

### 5 GHz

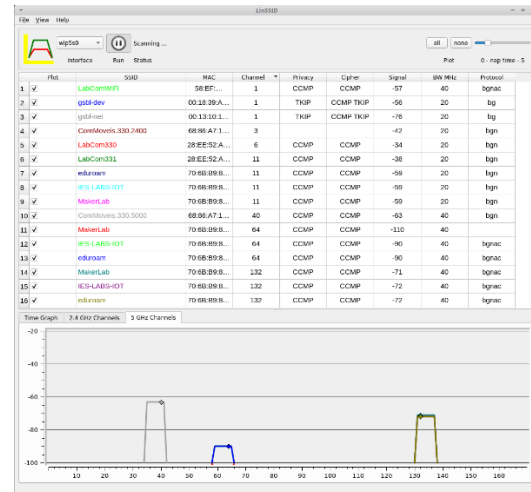


Figura 2.b: Exemplo de ecrã do LinSSID (5GHz)

- Verifique que a estação de monitorização (STA C) está no modo *Managed*:
  - Para verificar o estado dos interfaces ou alterar a sua configuração, utilize o comando **iwconfig**:

```
$ iwconfig
```

```
Terminal - labcom@labcomPC-CM: ~
File Edit View Terminal Tabs Help

labcom@labcomPC-CM:~$ iwconfig
lo        no wireless extensions.

enp0s31f6 no wireless extensions.

wlp5s0    IEEE 802.11 ESSID:"CMAP1S2"
Mode:Managed Frequency:5.7 GHz Access Point: 68:86:A7:1F:5C:70
Bit Rate=117 Mb/s   Tx-Power=16 dBm
Retry short limit:7  RTS thr:off   Fragment thr:off
Power Management:off
Link Quality=70/70  Signal level=-28 dBm
Rx invalid nwid:0  Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:7  Missed beacon:0

labcom@labcomPC-CM:~$
```

Figura 3

- Desligue a STA C de qualquer rede WLAN a que possa estar desligada (“Disconnect”), no interface do Linux, verificando que a STA C fica *Not-Associated*

```
Terminal - labcom@labcomPC-CM: ~
File Edit View Terminal Tabs Help

labcom@labcomPC-CM:~$ iwconfig
lo        no wireless extensions.

enp0s31f6 no wireless extensions.

wlp5s0    IEEE 802.11 ESSID:off/any
Mode:Managed Access Point:Not-Associated Tx-Power=16 dBm
Retry short limit:7  RTS thr:off   Fragment thr:off
Power Management:off

labcom@labcomPC-CM:~$
```

Figura 4

- Coloque a STA C em modo de monitorização e num canal específico (por exemplo o canal onde o SSID1 está a ser difundido: canais 3 e 7):

- Para colocar em modo de monitorização:

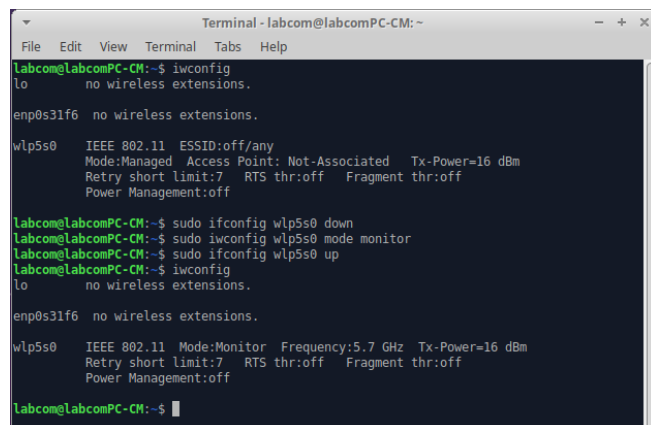
```
$ sudo ifconfig wlp5s0 down  
$ sudo iwconfig wlp5s0 mode monitor  
$ sudo ifconfig wlp5s0 up
```

- Para mudar de canal ou de frequência:

```
$ sudo iwconfig wlp5s0 [channel c | freq f]
```

- Verifique o resultado final:

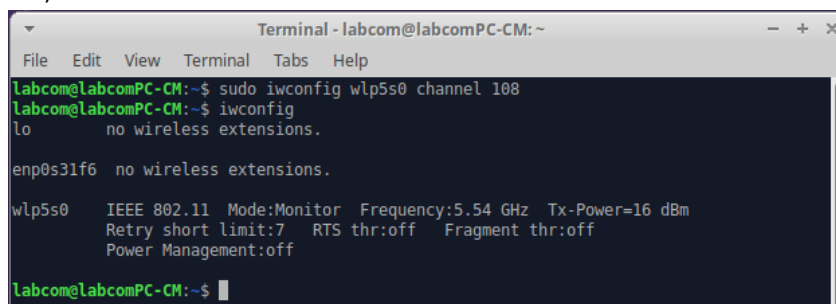
```
$ iwconfig
```



```
Terminal - labcom@labcomPC-CM: ~  
File Edit View Terminal Tabs Help  
labcom@labcomPC-CM:~$ iwconfig  
lo        no wireless extensions.  
enp0s31f6 no wireless extensions.  
wlp5s0    IEEE 802.11  ESSID:off/any  
          Mode:Managed Access Point: Not-Associated Tx-Power=16 dBm  
          Retry short limit:7 RTS thr:off Fragment thr:off  
          Power Management:off  
  
labcom@labcomPC-CM:~$ sudo ifconfig wlp5s0 down  
labcom@labcomPC-CM:~$ sudo iwconfig wlp5s0 mode monitor  
labcom@labcomPC-CM:~$ sudo ifconfig wlp5s0 up  
labcom@labcomPC-CM:~$ iwconfig  
lo        no wireless extensions.  
enp0s31f6 no wireless extensions.  
wlp5s0    IEEE 802.11  Mode:Monitor Frequency:5.7 GHz Tx-Power=16 dBm  
          Retry short limit:7 RTS thr:off Fragment thr:off  
          Power Management:off  
  
labcom@labcomPC-CM:~$
```

Figura 5

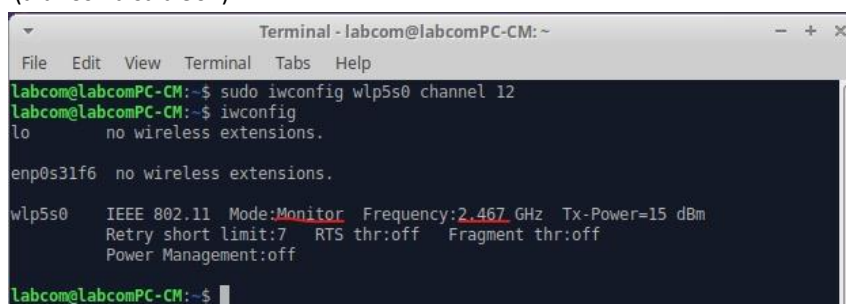
- 4) Mude para outro canal nos 2.4GHz ou mesmo para um canal nos 5GHz, se disponível (p.ex. Canal 100/5.5GHz):



```
Terminal - labcom@labcomPC-CM: ~  
File Edit View Terminal Tabs Help  
labcom@labcomPC-CM:~$ sudo iwconfig wlp5s0 channel 108  
labcom@labcomPC-CM:~$ iwconfig  
lo        no wireless extensions.  
enp0s31f6 no wireless extensions.  
wlp5s0    IEEE 802.11  Mode:Monitor Frequency:5.54 GHz Tx-Power=16 dBm  
          Retry short limit:7 RTS thr:off Fragment thr:off  
          Power Management:off  
  
labcom@labcomPC-CM:~$
```

Figura 6

- 5) Atente no output produzido pelos comandos *ifconfig* e *iwconfig*, antes e depois de colocação do interface em modo monitor, e conclua sobre a informação que os mesmos lhe apresentaram, tendo em conta os procedimentos que realizou.
- 6) Antes de prosseguir, coloque a STA C na frequência desejada para o SSID 1, canais 3 (alunos na sala 300) e 7 (alunos na sala 301):



```
Terminal - labcom@labcomPC-CM: ~  
File Edit View Terminal Tabs Help  
labcom@labcomPC-CM:~$ sudo iwconfig wlp5s0 channel 12  
labcom@labcomPC-CM:~$ iwconfig  
lo        no wireless extensions.  
enp0s31f6 no wireless extensions.  
wlp5s0    IEEE 802.11  Mode:Monitor Frequency:2.467 GHz Tx-Power=15 dBm  
          Retry short limit:7 RTS thr:off Fragment thr:off  
          Power Management:off  
  
labcom@labcomPC-CM:~$
```

Figura 7

- Está assim a garantir que a interface 802.11 da STA C tem o rádio a funcionar na frequência correcta para prosseguir o trabalho.

## 2. Experimentação: Frames

- 1) Inicie o Wireshark na STA C.
- 2) Verifique (*Capture* → *Options*, aba *Input*) que o interface WLAN (wlp5s0) está em modo de monitoria (não avance caso isso não se verifique):

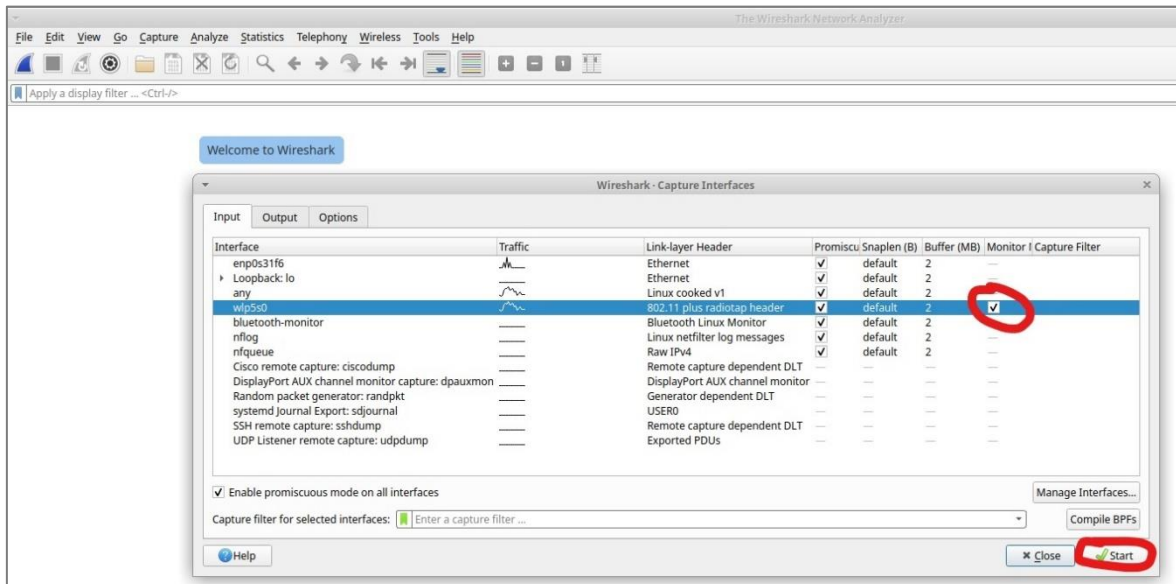


Figura 8

- 3) Inicie a captura na rede WLAN selecionando a linha com o interface wlp5s0 e premindo 'Start', no canto inferior direito; guarde alguns segundos; pare a captura no Wireshark (botão quadrado vermelho, em cima, à esquerda)

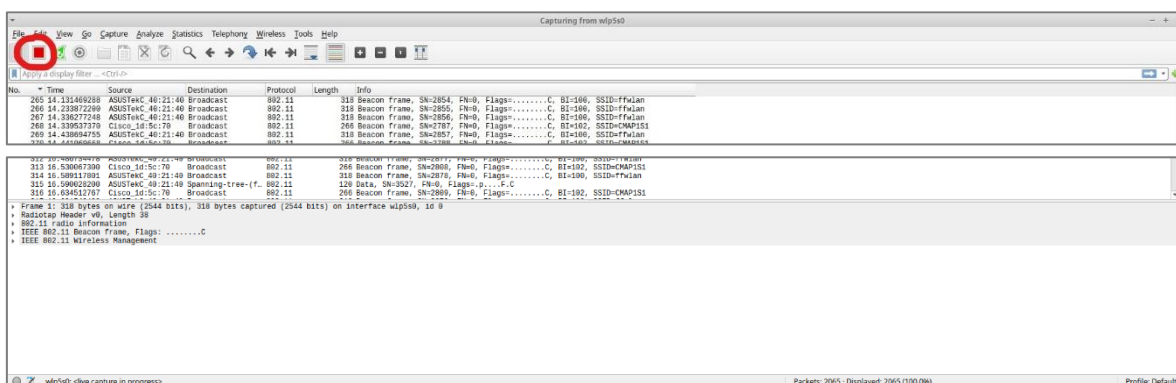


Figura 9

- 4) Observe que na sala 330 (estando a capturar no canal 3) não observa os Beacons do SSID1 da sala 331 ("ComMoveis.331.2400") e vice-versa (estando na sala 331 no canal 7). Explique a razão para tal.
  1. Coloque o interface a monitorar no outro canal (3 vs 7) e observe a diferença.
  2. Coloque agora o interface a monitorar no canal 5 e observe a diferença. O comportamento é o mesmo?
- 5) Selecciona uma qualquer trama (pode agrupá-las por tipo, carregando no topo da coluna 'Info') e observe a informação na área de detalhes (*Packet details*); exemplo para uma trama do tipo *Beacon frame (passive scanning)*; pode utilizar um *Display Filter* (`wlan.fc.type==0&&wlan.fc.subtype==8`; compare estes valores com os da Tabela 2 no final do guião) para o efeito:

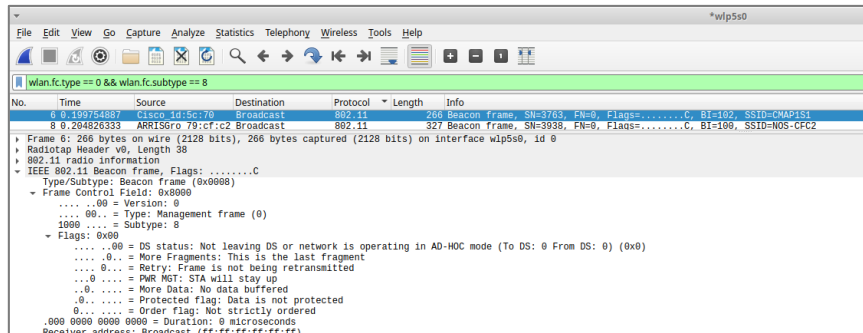


Figura 10

- Identifique a estrutura da trama (*Header, Body, FCS*) e os campos que a compõe (consulte o Anexo VII) e, em particular, registe o **tipo** e **subtipo** da trama, expandindo os campos na janela de *Packet Details*.
- 6) Procure tramas de **pesquisa activa** (*Probe Request/Response*); pode utilizar um *Display Filter* para o efeito (mude o *subtype* para 4 e 5):

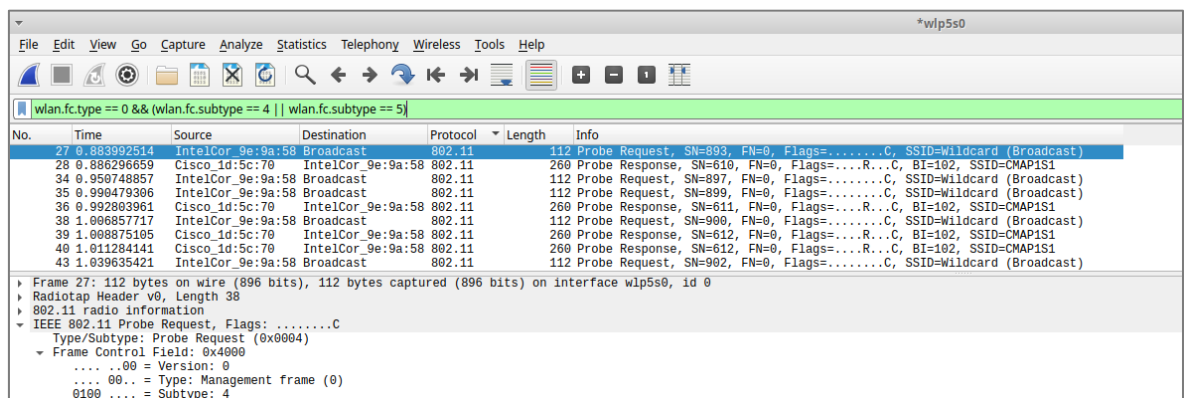


Figura 11

- 7) Reinicie a captura no Wireshark (*Capture → Start*); com o comando **iwconfig**, mude a monitorização para outros canais de 2.4GHz (por exemplo 1, 6 e 12) e 5GHz (por exemplo 100, 120 e 140)
- Observe os diferentes **SSIDs** anunciados nos *Beacons* capturados, em cada canal; porque se observam os mesmos Beacon em várias frequências?
  - Conseguirá observar os beacons de ambos AP? Actue no sentido de o verificar.
  - Observe o diferente comportamento na faixa dos 5GHz. Explique-o.
- 8) Volte a colocar a STA C no canal 3 e 7, conforme a sala, e pare a captura; ordene as tramas capturadas pelo campo *Info* e aplique o filtro de visualização para tramas de tipo **Management** sem indicar subtipo ("wlan.fc.type == 0")
- Registe os tipos e sub-tipos para cada um dos grupos que encontra (informação inicial indicada na coluna *Info*) e compare com a informação no Anexo VII.
  - Mude o filtro de visualização para tramas de **Control** ("wlan.fc.type == 1"); repita o passo anterior.
  - Mude o filtro de visualização para tramas de **Data** ("wlan.fc.type == 2"); repita o primeiro passo.
- 9) Repita os passos anteriores, observando agora a informação de origem e presente nas colunas 'Source' e 'Destination'; identifique os tipos de endereços (MAC) que aparecem; Relacione com os tipos de tramas.

- 10) Remova o filtro de visualização ou coloque-o para tramas do tipo 0; selecione uma trama do tipo 'Beacon frame' e onde seja indicado o SSID1 'ComMoveis.33x.2400'
- Calcule a periodicidade de envio dos Beacons com base na informação na coluna *Time* (pode colocar a referencia temporal em uma dessas tramas com *Ctrl+T*).
  - Na área de detalhe da trama, observe a informação presente no corpo da trama, nos grupos *Fixed parameters* e *Tagged parameters* (Campo *IEEE 802.11 Wireless Management*)
  - Confira a informação anterior.
  - Verifique as várias características anunciadas pelos AP (p.ex *Supported Rates*)

### 3. Experimentação: *Procedimentos*

#### A. Autenticação e Associação

11) Reinicie a captura (STA C) no Wireshark no interface de rede WLAN (interface wlp5s0)

12) Ligue a STA A ao SSID1 ('ComMoveis.33x.2400') e pare a captura.

13) Configure um filtro de visualização para as tramas de pedido de autenticação, associação e confirmação (veja a fig. 12)

- Visualize na captura o processo de autenticação e associação da STA A e anote o número de sequência dessas mensagens na captura do Wireshark.
- Observe o processo de pedido e confirmação (*Acknowledgment*).
- Compare o corpo das mensagens de Autenticação e de Associação.

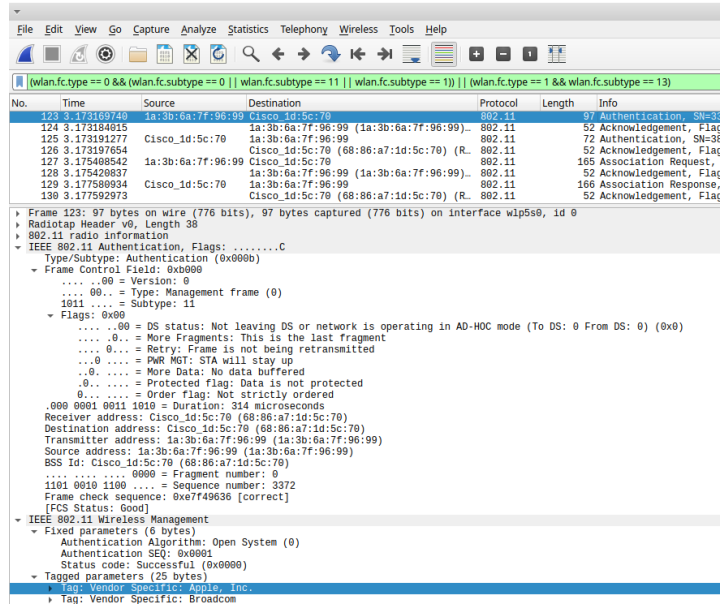


Figura 12

14) Mude o filtro de visualização para pacotes DHCP e observe a troca de mensagens (pode visualizar este processo porque a rede é aberta e sem encriptação); anote o endereço IP atribuído à STA A.

- Relacione temporalmente estas mensagens com as anteriores, comparando os números de sequência na captura.

#### B. Transferência de dados

15) Reinicie a captura no Wireshark no interface de rede WLAN (interface wlp5s0)

16) Desde a STA A faça um ping para o AccessPoint da sala (10.0.1{2}.1) por alguns segundos (p.ex. 10 segs)

- Apesar de os ping terem tido sucesso na sua máquina (STA A), o wireshark perde e replica alguns desses pacotes.

17) Pare a captura e filtre na visualização pacotes do tipo ICMP (ping) e ARP, analisando as trocas de mensagens.

- Selecione um destes pacotes e, na área de detalhes, observe o tipo de trama e de subtrama.
- Observe os vários encapsulamentos utilizados até chegar ao pacote ICMP ou ARP e explique-o.



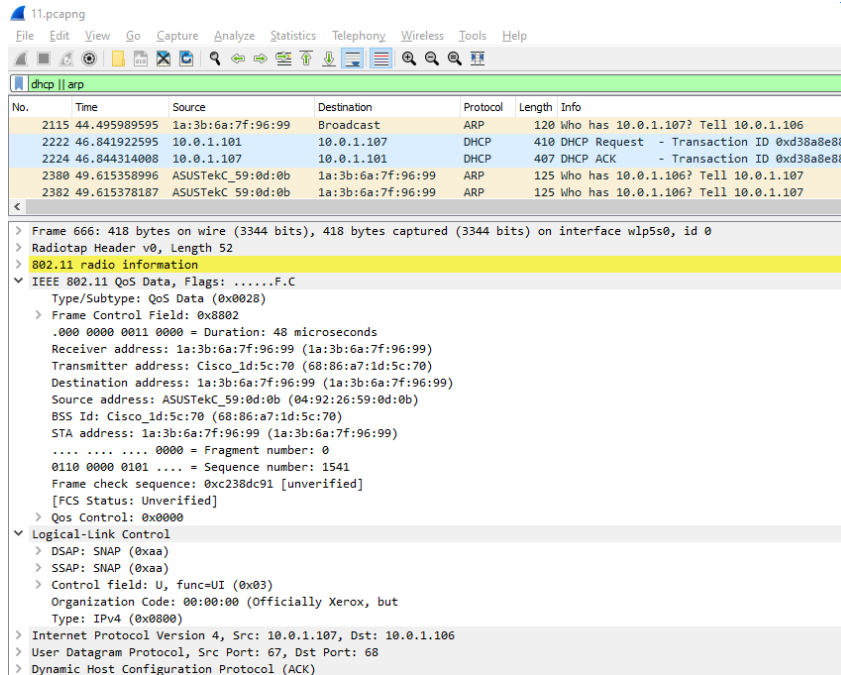


Figura 13

18) Filtre agora pacotes RTS, CTS e ICMP (fc.type = 1 e subtype = 11 ou 12):

- Verifique o padrão da troca de pacotes entre os pedidos *ICMP Echo Request* e as respostas *ICMP Echo Reply*.
- Observe o tipo e subtipo das tramas capturadas.
- Observe a flag *DS status* de ambas as mensagens de *Echo Request* e *Reply*.

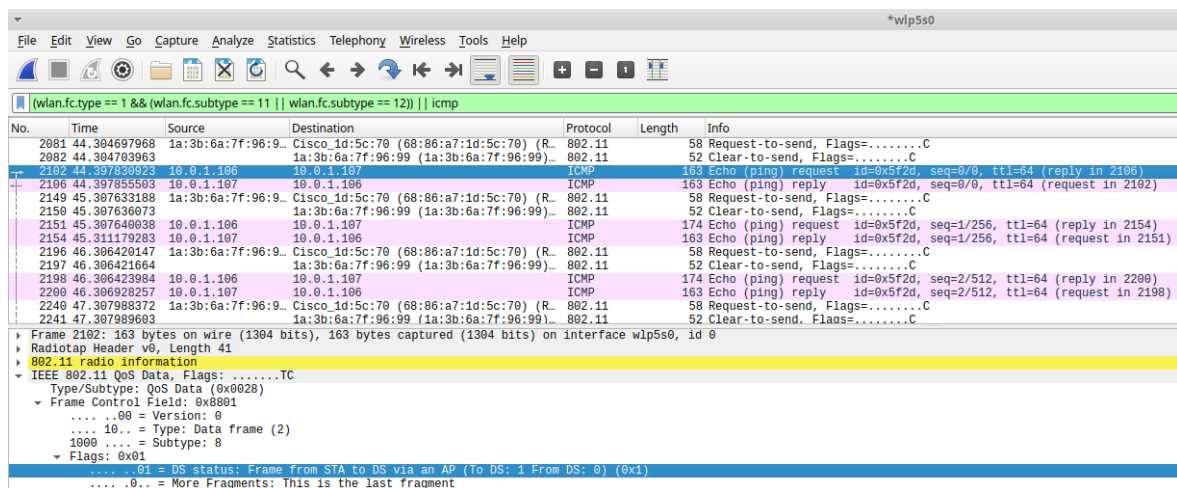


Figura 14

19) Reinicie a captura no Wireshark no interface de rede WLAN (interface wlp5s0)

20) Ligue a STA B ao SSID (não será pedida autenticação)

- Repita a aplicação de um filtro de visualização para pacotes DHCP e anote o endereço atribuído a essa estação.

21) Faça um ping entre da estação STA A para STA B por alguns segundos (p.ex. 10) e pare a captura

- Filtre pacotes RTS, CTS e ICMP



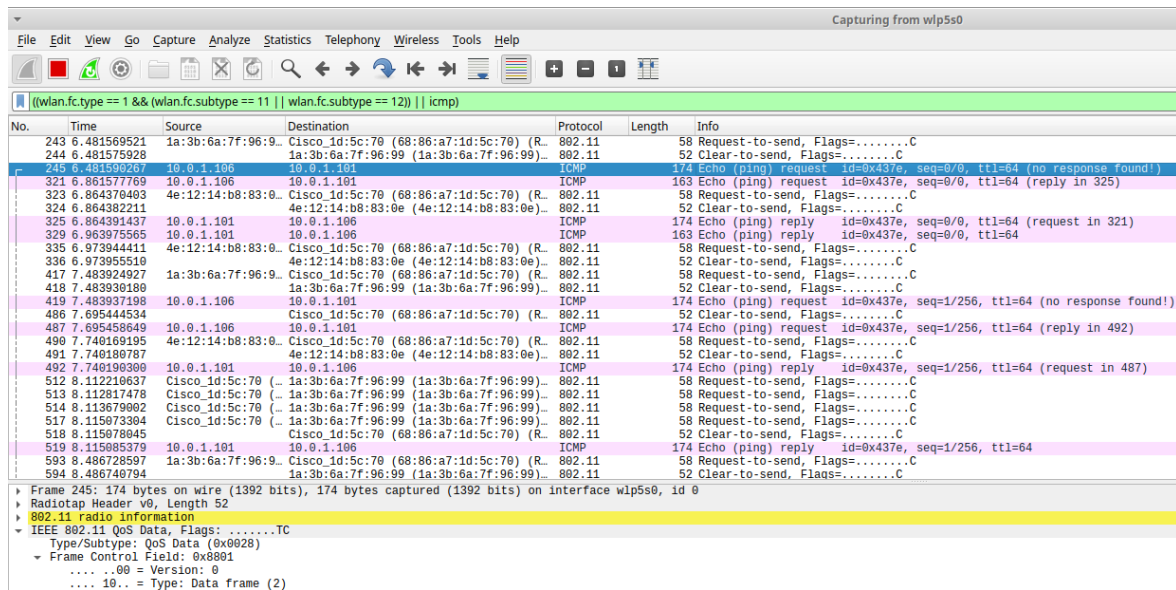


Figura 15

- Verifique o padrão da troca de pacotes entre os pedidos *ICMP Echo Request* e as respostas *ICMP Echo Reply*; que diferenças encontra para o *ping* efectuado anteriormente? Analise com base na observação dos seguintes campos presentes no cabeçalho da trama 802.11:
  - DS Status* e
  - Receiver, Transmitter, Destination* e *Source Address*.

### C. Associação com segurança e desassociação (STA A)

- Mude a STA C para o canal 40 (5.200 MHz).
- Reinicie a captura na rede WLAN (interface wlp5s0).
- Ligue a STA A no SSID 2 ('ComMoveis.33x.5000') e introduza a chave de autenticação ('Lab.Com.WiFi'); pare a captura.
  - Observe o processo *4-Way Handshake* do EAPoL (EAP over LAN) utilizado com o WPAv2 e os parâmetros trocados

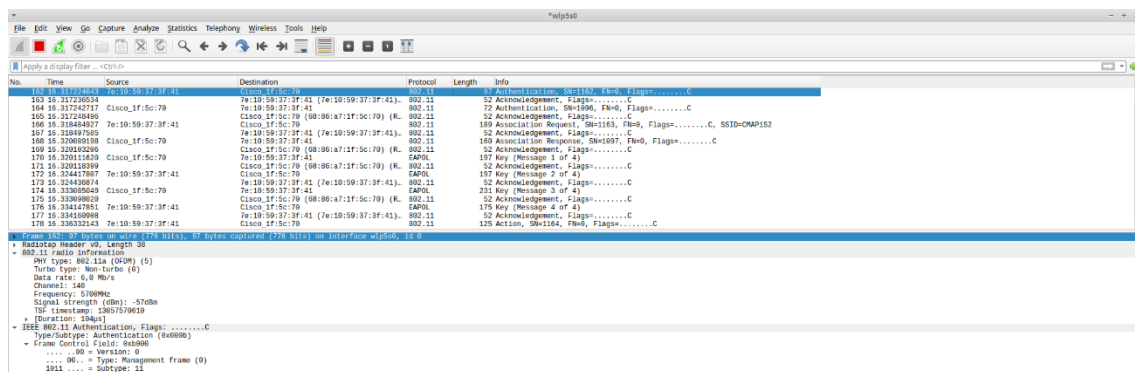


Figura 16

- Reinicie a captura na rede WLAN (interface wlp5s0).
- Volte a colocar a STA A no SSID 1 e pare a captura.
  - Observe a única mensagem de desassociação.

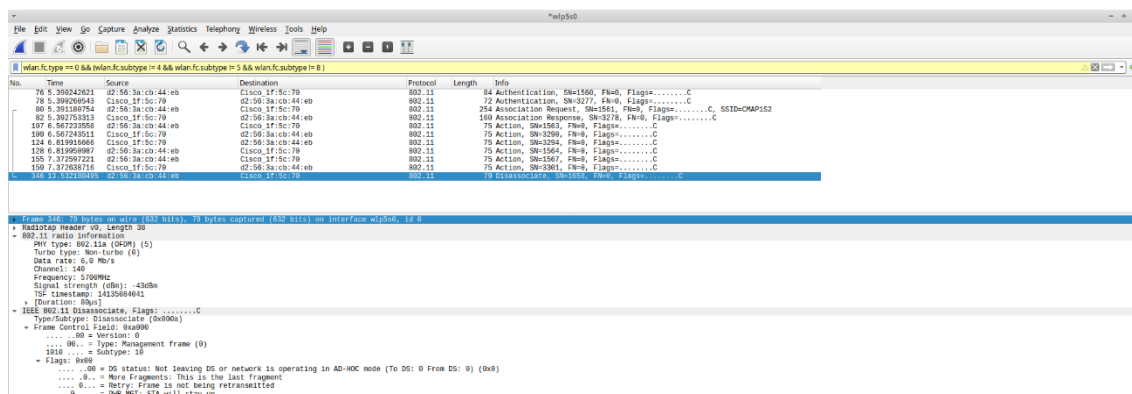


Figura 17

## D. Desempenho

27) Como primeiro passo preparatório, instale o *iperf3* na STA A e na STA B (ver a Secção VI)

28) Ligue a STA A e STA B no SSID1; coloque a STA C no canal 3.

29) Reinicie a captura na rede WLAN na STA C (interface wlp5s0).

30) Na linha de comandos ou na aplicação que utilizar, ligue o *iperf3* ao servidor da sala no porto de correspondente ao seu grupo de trabalho, com intervalos de visualização de 1 seg e no sentido servidor → cliente (opcionalmente, inicie do cliente para o servidor, ou seja, sem a opção '-R' e compare os resultados):

- `iperf3 -c 10.0.1.2 -p 520x -i 1 -R`

31) Quando o *iperf3* termine (10 seg), pare a captura no Wireshark

- Registe os débitos obtidos.
- Configure um filtro de visualização para tramas RTS, CTS e pacotes TCP; visualize a sequência de pacotes, incluindo os TCP.

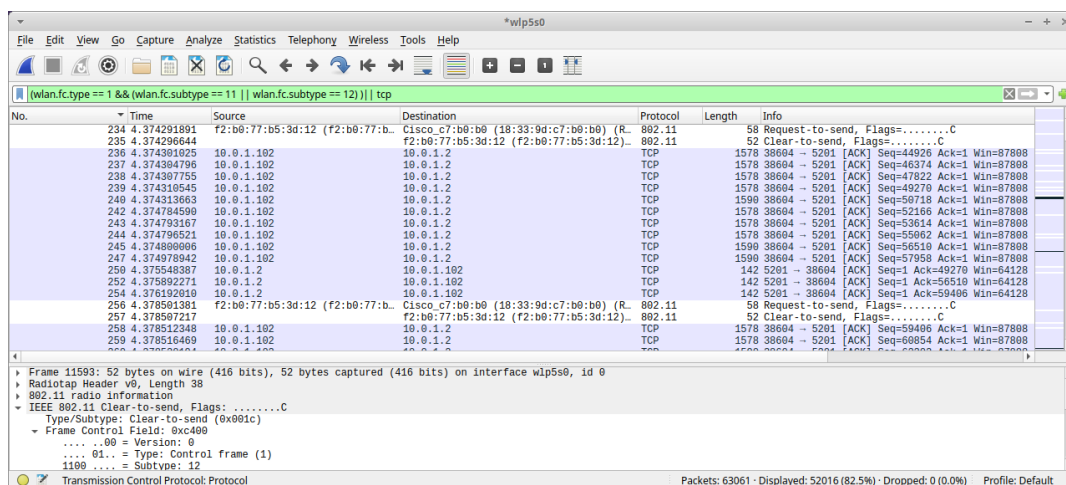


Figura 18

- Selecione uma trama RTS e ordene a captura pelo campo 'Info' (ficará com todas as tramas RTS agrupadas e ordenadas); percorra a lista observando a frequência com que estas foram geradas durante o *iperf3* e as durações solicitadas nas tramas RTS.

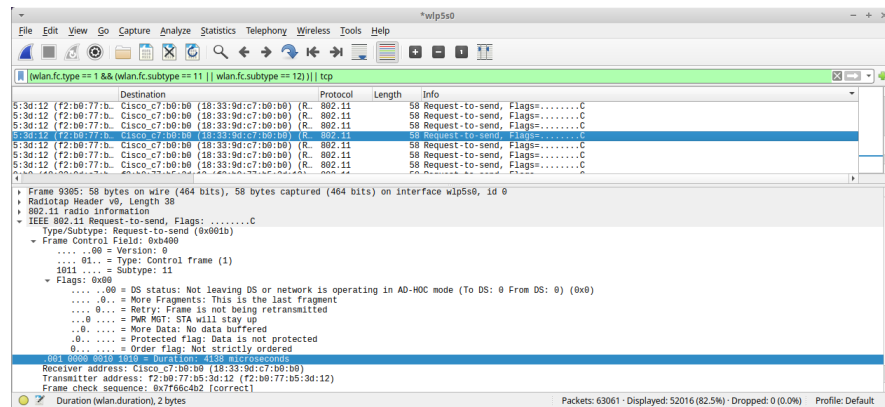


Figura 19

32) Repita o anterior colocando as estações no canal 40 (5GHz).

## IV. Links úteis

### WLAN

- <https://howiwifi.com/2020/07/13/802-11-frame-types-and-formats/>
- <https://howiwifi.com/2020/07/16/802-11-frame-exchanges/>
- <https://www.wifi-professionals.com/2019/01/4-way-handshake>

### IPERF3

- Windows:

<https://iperf.fr/iperf-download.php#windows>

- Android

<https://play.google.com/store/apps/details?id=com.nextdoordeveloper.miperf.miperf&hl=en&gl=US>

### Wireshark

<https://wiki.wireshark.org/CaptureSetup/WLAN>

<https://www.wireshark.org/docs/dfref/w/wlan.html>

## V. Utilização do Wireshark

### Filtros de visualização

- wlan.bssid == MAC AP
- wlan.ra == MAC addr; wlan.sa == MAC addr
- wlan.fc.type == n (0: management; 1: control; 2: data)
- wlan.fc.type\_subtype == n (ver tabela abaixo)

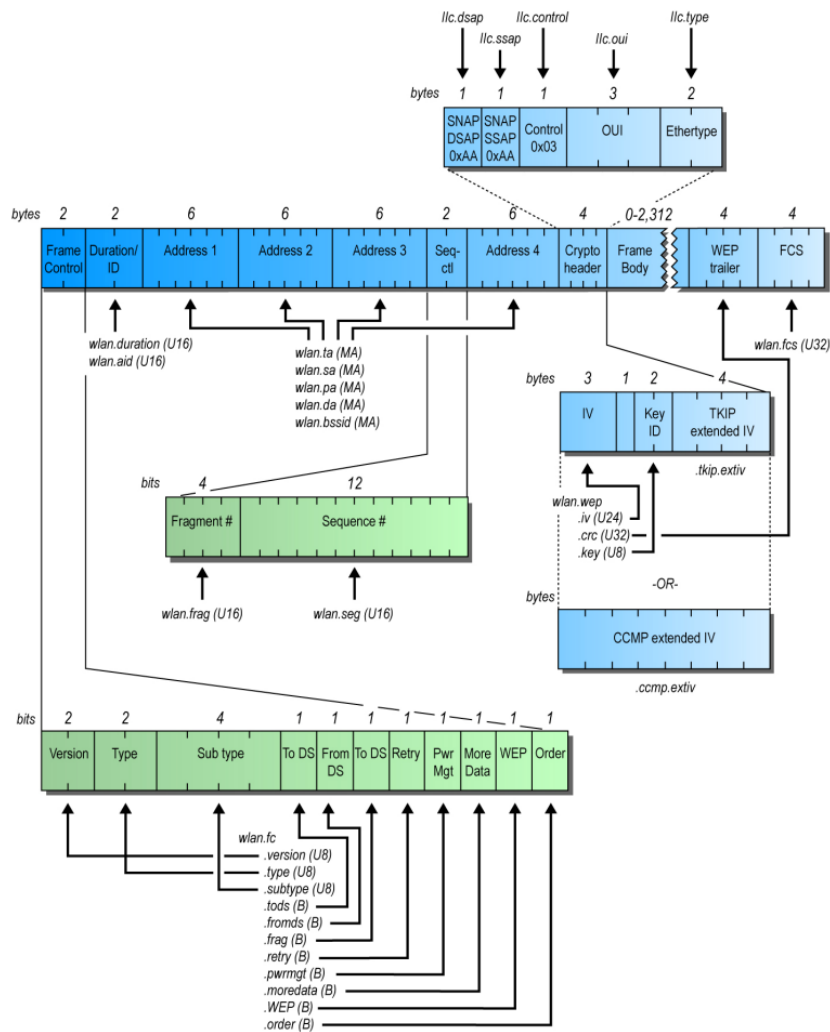


Figura 20

## VI. Utilização do iperf3

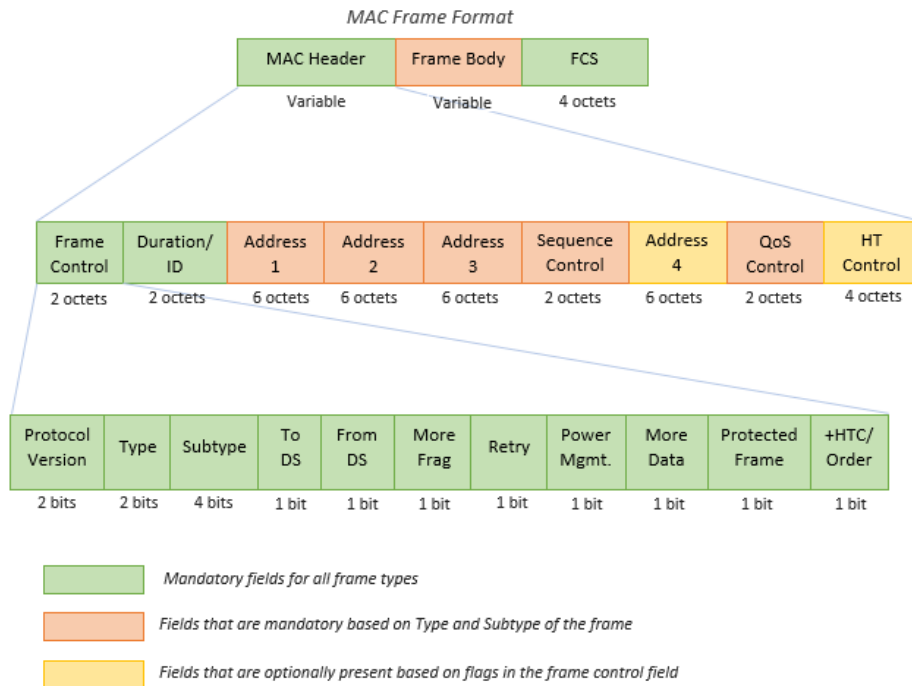
### Servidor

- \$ iperf3 -s -p port

### Cliente

- \$ iperf3 -c server\_address -p port

## VII. Tramas 802.11 e subtipos de tramas



**Figura 21**

Type = 0 (Management)		Type = 1 (Control)		Type = 2 (Data)	
Association request	0000 (0)			Data	0000 (0)
Association response	0001 (1)			Data + CF-ACK	0001 (1)
Reassociation request	0010 (2)			Data + CF-Poll	0010 (2)
Reassociation response	0011 (3)			Data + CF-ACK + CF-Poll	0011 (3)
Probe request	0100 (4)	Beamforming Report Poll	0100 (4)	Null (no data)	0100 (4)
Probe response	0101 (5)	VHT/HE NDP Announcement	0101 (5)	CF-ACK (no data)	0101 (5)
Timing advertisement	0110 (6)	Control Frame Extension	0110 (6)	CF-Poll (no data)	0110 (6)
Reserved	0111 (7)	Control wrapper	0111 (7)	CF-ACK + CF-Poll (no data)	0111 (7)
Beacon	1000 (8)	Block ACK Request	1000 (8)	QoS Data	1000 (8)
		Block ACK	1001 (9)	QoS Data + CF-ACK	1001 (9)
Disassociation	1010 (10)	PS-Poll	1010 (10)	QoS Data + CF-Poll	1010 (10)
Authentication	1011 (11)	RTS	1011 (11)	QoS Data + CF-ACK + CF-Poll	1011 (11)
Deauthentication	1100 (12)	CTS	1100 (12)	QoS Null (no data)	1100 (12)
Action	1110 (13)	ACK	1101 (13)	Reserved	1101 (13)
		CF-End	1110 (14)	QoS CF-Poll (no data)	1110 (14)
		CF-END+CF-ACK	1111 (15)	QoS CF-ACK + CF-Poll (no data)	1111 (15)

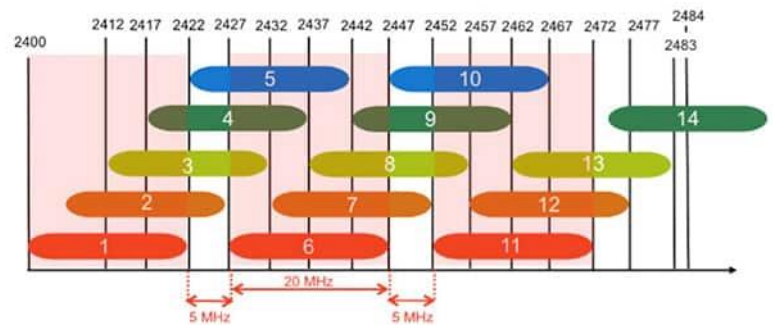
**Tabela 2**

## VIII. Canais e frequências

### 2.4 GHz

Channel	F <sub>0</sub> (MHz)	Frequency Range (MHz)
1	2412	2401–2423
2	2417	2406–2428
3	2422	2411–2433
4	2427	2416–2438
5	2432	2421–2443
6	2437	2426–2448
7	2442	2431–2453
8	2447	2436–2458
9	2452	2441–2463
10	2457	2446–2468
11	2462	2451–2473
12	2467	2456–2478
13	2472	2461–2483
14	2484	2473–2495

**Tabela 3**



**Figura 21**

<https://www.digikey.com/en/articles/compare-24-ghz-5-ghz-wireless-lan-industrial-applications>

### 5GHZ

#### 5 GHz Channel Allocations

Frequency (GHz)	5.150	5.250	5.470	5.600	5.640	5.725	5.850
802.11 Allocations	UNII-1	UNII-2a	UNII-2c (Extended)	TDWR		UNII-3	
Center Frequency	5180, 5200, 5220, 5240	5260, 5280, 5300, 5320	5500, 5520, 5540, 5560, 5580, 5600, 5620, 5640	5660, 5680, 5700, 5720	5745, 5765, 5785, 5805, 5825		
20 MHz	36, 40, 44, 48	52, 56, 60, 64	100, 104, 108, 112, 116, 120, 124, 128	132, 136, 140, 144	149, 153, 157, 161, 165		
40 MHz	38, 46	54, 62	102, 110	118, 126	134, 142	151, 159	
80 MHz	42	58	106	122	138	155	
160 MHz	50		114				
FCC	1,000 mW Tx Power Indoor & Outdoor No DFS needed	250 mw w/6dBi Indoor & Outdoor DFS Required	250mw w/6dBi Indoor & Outdoor DFS Required 144 Now Allowed	120, 124, 128 Devices Now Allowed		1,000 mW EIRP Indoor & Outdoor No DFS needed 165 was ISM, now UNII-3	
DFS Channels			DFS Channels				

**Figura 22**

<https://www.ekahau.com/blog/channel-planning-best-practices-for-better-wi-fi/>