WLAN / 802.11

I. Objectives

The objectives of this practical work are:

- Observe the main 802.11 frames
- Observe the 802.11 network discovery processes
- Become familiar with network observation and diagnostic tools

II. Duration

This work should last one class, practical component (1h15)

III. Equipment

This Work will use:

1. 2x Cisco Access Point (AP), 1 per room
2. 1x laboratory PC per work group (STA C), with Linux
3. LinSSID application installed at STA C to analyse available WLAN channles
4. The Wireshark application installed at STA C for capturing and analysing network traffic

IV. Diagram

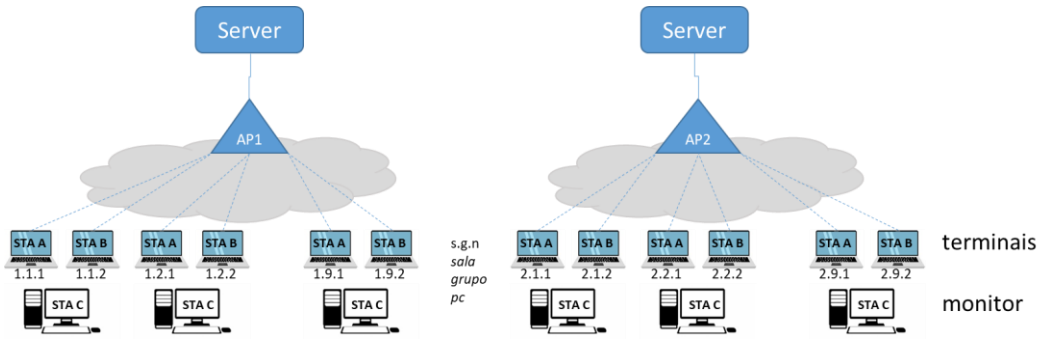


Figura 1: Network diagram for experimentation

Each AP has one SSID configured in the 2.4GHz WLAN band and has DHCPv4 server functionality, assigning IP addresses in the indicated range, as shown in the following table; one AP has open security while the other is secured:

	AP1	**AP2**
SSID	ComMoveis.33**0**.2400	ComMoveis.33**1**.2400
Channel	Channel **3** (2.422 MHz)	Channel **7** (2.442 MHz)
Security	Open	Authentication: WPAv2 Encryption: AES-CCM Password: "**Lab.Com.WiFi**"
IPv4 addressing	10.0.**1**.[100-200]/24 Server: 10.0.**1.2**/24	10.0.**2**.[100-200]/24 Server: 10.0.**2.2**/24

Table 1: WLANs configuration

1. Preparation

1) Using the "LinSSID" application installed on the STA C, observe the active 802.11 networks; choose the correct tab at the bottom of the app: Time Graph, 2.4 GHz channels, 5 GHz channels.
   - Observe the information provided: SSID, channels used, security, signal level, bandwidth and supported protocols.

2.4 GHz

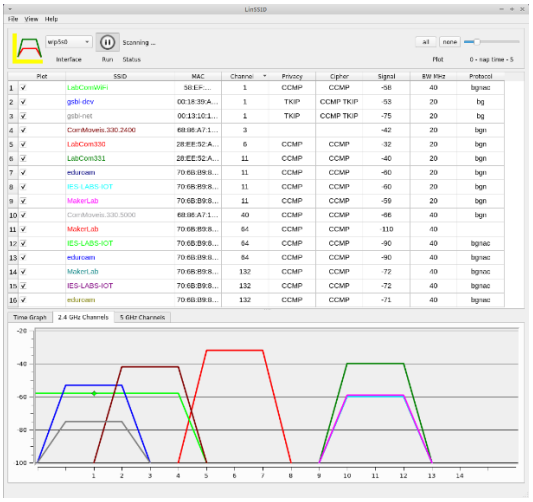


Figure 2.a: Example of LinSSID screen (2.4GHz)

5 GHz

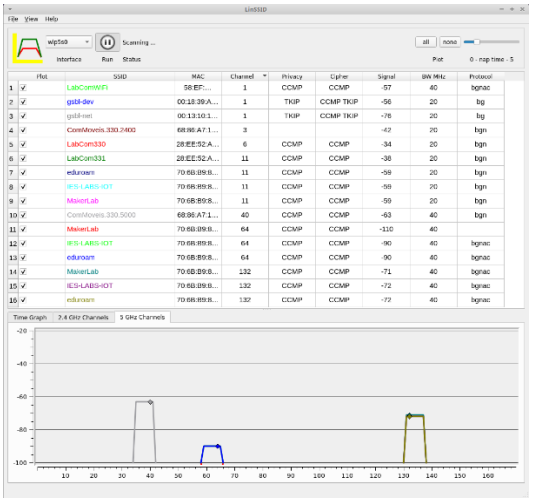


Figure 2.b: LinSSID screenshot example (5GHz)

2) Take a screenshot and save it (for 2.4 GHz and 5 GHz) for later reference (you will not be able to do this operation after the next steps).

3) Check if the monitoring station (STA C) is in ***Managed mode*** (if in Monitor mode, you may jump to step 4):
   - To check the status of interfaces or change their configuration, use the command ***iwconfig***:

```
$ iwconfig
```

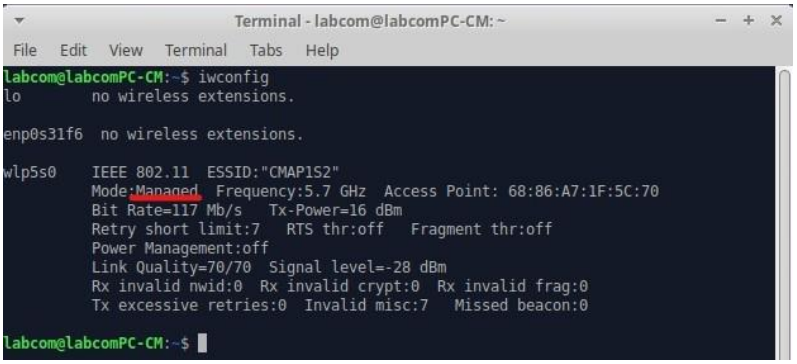


Figure 3

2) Disconnect the STA C from any WLAN network that it may be connected ("Disconnect"), in the Linux interface, checking that the STA C becomes *Not-Associated*

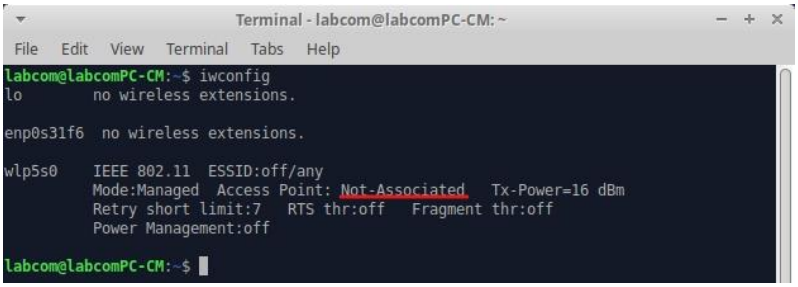
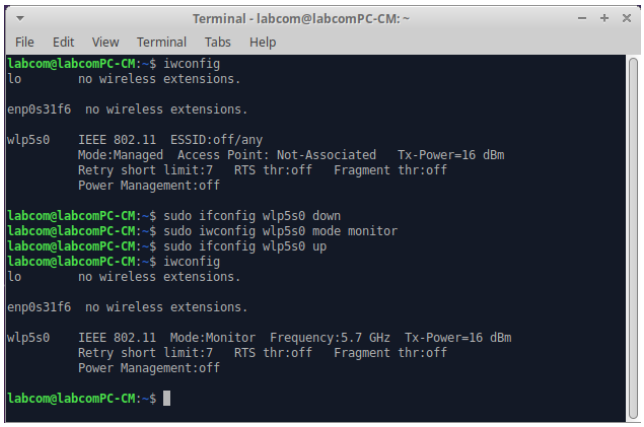


Figure 4

3) Place the STA C in ***Monitor*** mode on the specific AP1 channel (3), where SSID1 is being announced.
   - To put in monitoring mode:

```
$ sudo ifconfig wlpxs0 down
$ sudo iwconfig wlpxs0 mode monitor
$ sudo ifconfig wlpxs0 up
```



4) To change channels or frequencies:

```
$ sudo iwconfig wlpxs0 [channel c | freq f]
```

   - Check the final result:

```
$ iwconfig
```

Figure 5

5) Switch to another 2.4 GHz channel (e.g. 9/2.452 MHz) or even a 5 GHz channel, if available (e.g. Channel 108/5.540 MHz):

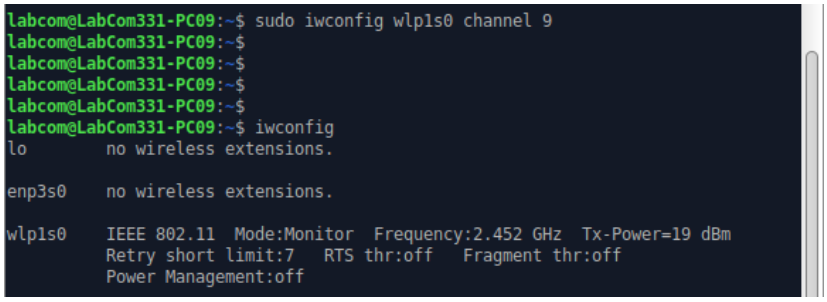


Figure 6

6) Pay attention to the output produced by the *ifconfig* and *iwconfig* commands, before and after placing the interface in monitor mode, and conclude on the information they presented to you, considering the procedures you carried out.

7) Before proceeding, set STA C to the associated frequency for SSID 1 (channel 3):

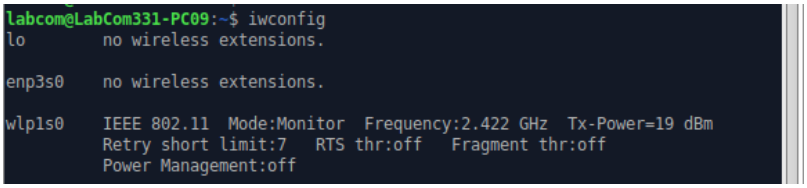


Figure 7

   - This ensures that the STA C 802.11 interface has the radio working on the correct frequency to continue the work.

2. Experimentation: Channels and Frames

1) Start Wireshark on STA C.

2) Check (*Capture* → *Options*, *Input* tab) that the WLAN interface (wlp***x***s0) is in monitoring mode (do not proceed if this is not verified):

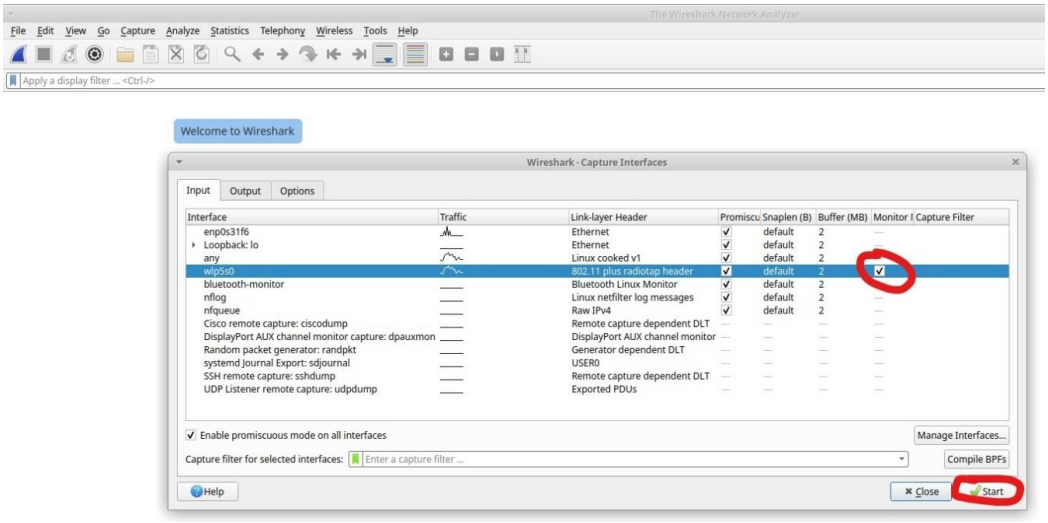


Figure 8

3) Start capturing on the WLAN network by selecting the line with the wlp***x***s0 interface and pressing 'Start' in the bottom right corner; wait a few seconds; stop capture in Wireshark (red square button, top left)

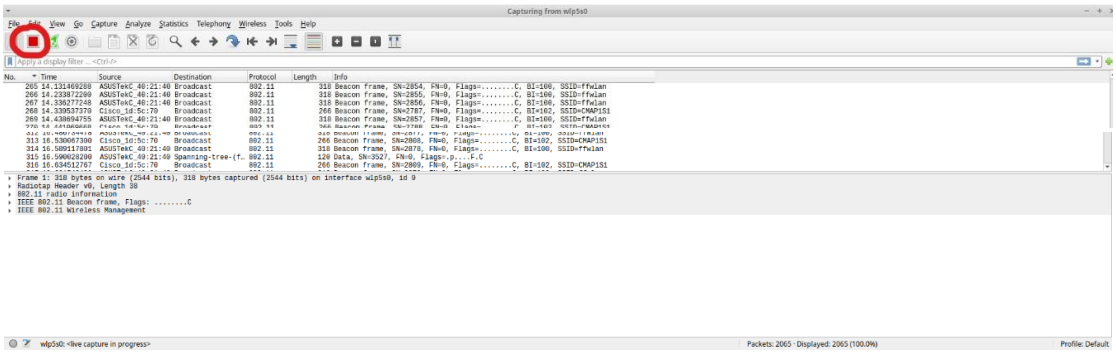


Figure 9

4) Note that while capturing on channel 3 (AP1) you do not observe the SSID1 Beacons of AP2 ("ComMoveis.331.2400")

    1. Place the interface to be monitored on the other channel (7 vs 3) and observe the difference.

    2. Now place the WLAN monitoring on channel 5 and observe the difference. Is the behaviour the same? Consult Annex VIII to provide your answer.

5) Select any frame (you can group them by type, clicking at the top of the '*Info*' column) and observe the information in the details area ('*Packet details*'); see the following example for a ***Beacon frame*** type (*passive scanning*); you can use a ***Display Filter*** (*wlan.fc.type==0 && wlan.fc.subtype==8*; compare these values with those in Annex VII at the end of this guide) for this purpose:

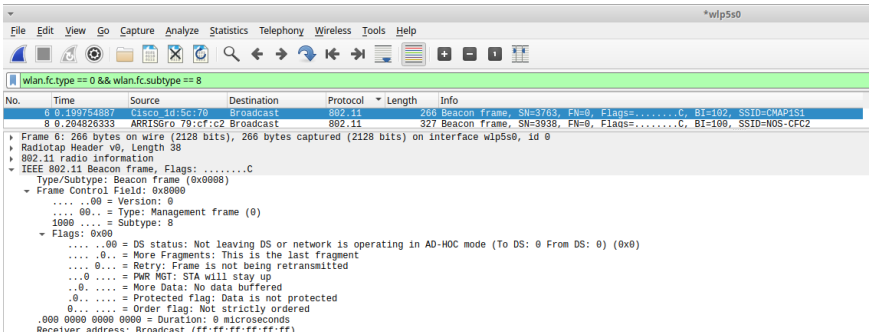


Figure 10

- Identify the frame structure (*Header, Body, FCS*) and the fields that make it up (see Annex VII) and record the **frame type and subtype**, expanding the fields in the *Packet Details* window.

6) Search for **active search** frames (*Probe Request/Response*); you can use a *Display Filter* for this (change the *subtype* to 4 and 5):

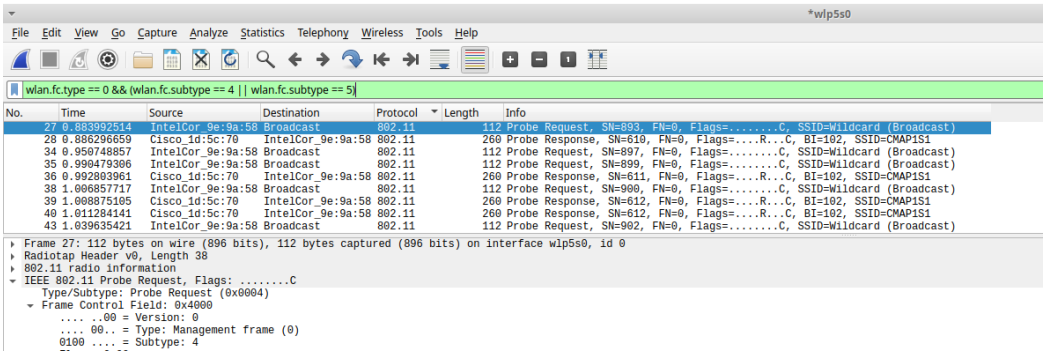


Figure 11

7) Restart the capture in Wireshark (Capture → Start); with the ***iwconfig*** command, change monitoring to other 2.4GHz channels (for example 1, 6 and 12)

   - Observe the different **SSIDs** announced in the captured **Beacons**, on each channel; why are the same Beacons are observed at various frequencies?
   - Will you be able to observe the beacons from both APs? Take action to check it.

8) Move back monitoring in STA C to channel 3 and stop the capture; order the captured frames by the *Info* field and apply the display filter to ***Management*** type frames without indicating subtype ("wlan.fc.type == 0")

   - Record the types and subtypes for each of the groups you find (initial information indicated in the *Info* column) and compare with the information in Appendix VII
   - Change the display filter for ***Control*** frames ("wlan.fc.type == 1"); repeat previous step.
   - Change the display filter to ***Data*** frames ("wlan.fc.type == 2"); repeat the first step.

9) Repeat the previous steps, now observing the origin information present in the 'Source' and 'Destination' columns; identify the types of addresses (MAC) that appear; Relate to the types of plots.

Addresses	*Beacon*	*Probe req*	*Probe resp*	*Ack*	*Data (ping PC→AP)*
Receiver					
Destination					
Transmitter					
Source					
BSS Id					

10) Remove the display filter or set it to frames of type 0; select a frame of type 'Beacon frame' and where SSID1 ('ComMoveis.330.2400') is indicated

- Calculate the sending frequency of Beacons based on the information in the *Time* column (you can set the time reference in one of these frames with *Ctrl+T*)
- In the frame detail area, observe the information present in the frame body, in the *Fixed parameters* and *Tagged parameters* groups (*IEEE 802.11 Wireless Management* Field)
- Check previous information.
- Check the various features advertised by APs (e.g. *Supported Rates*)

V. Useful links

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
- https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html

Wireshark

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

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

VI. Utilização do Wireshark e estrutura de tramas

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.subtype == n (ver tabela abaixo)

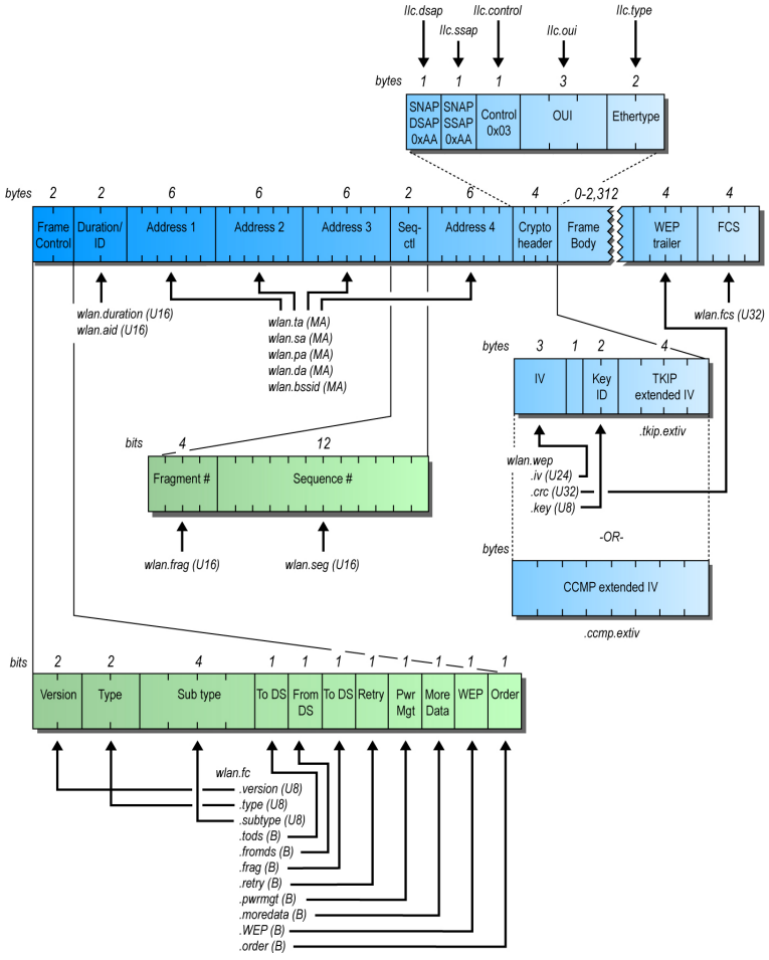


Figure 20

VII. 802.11 frames' structure and sub-types

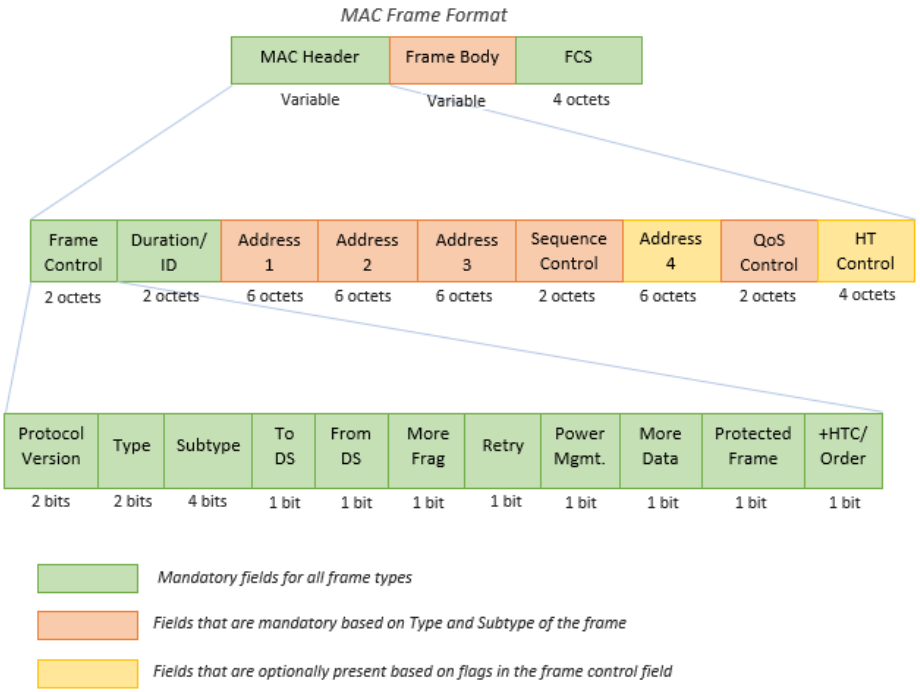


Figure 21

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)

Table 2

VIII. Channels and frequencies

2.4 GHz

Channel	F_0 (MHz)	Frequency Range (20 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

Table 3

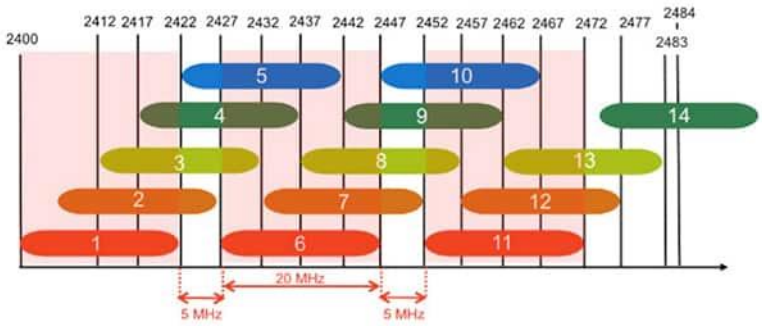


Figure 21

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

5GHZ

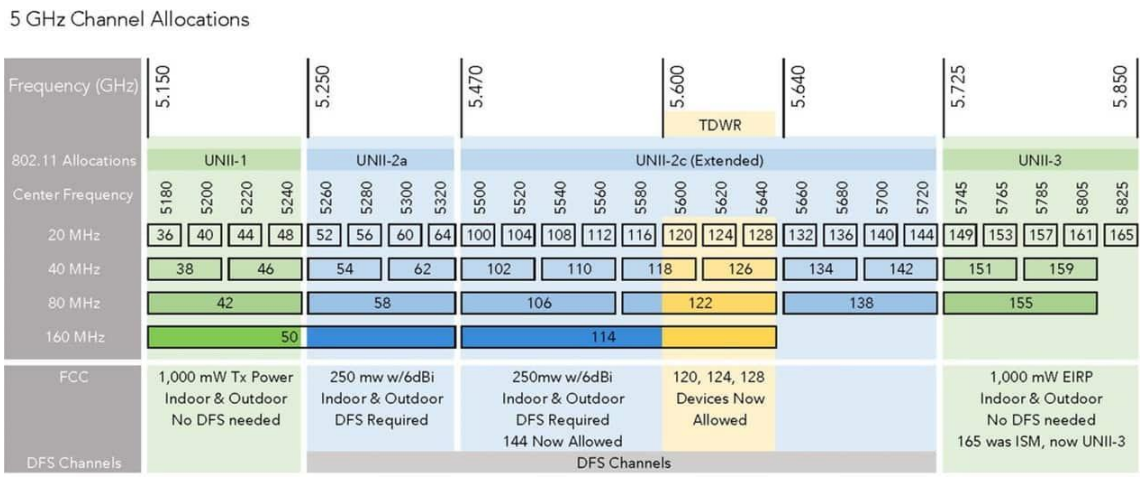


Figure 22

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