

WLAN / 802.11 (II)

I. Objectives

The objectives of this practical work are:

- Observe authentication and association processes
- Understand how information is exchanged on an 802.11 network
- 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)
2. 1x laboratory PC per work group (STA C), with Linux
3. The Wireshark application installed at STA C for capturing and analysing network traffic
4. 2x student terminals with WLAN/802.11 interface (STA A and STA B)

IV. Diagram

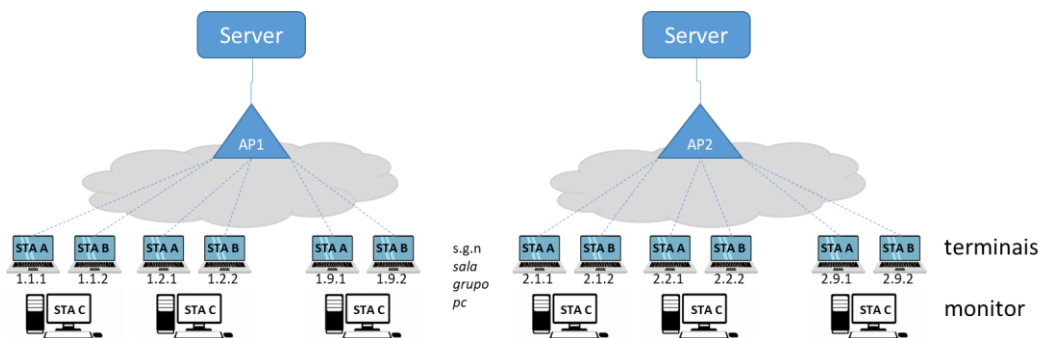


Figure 1: Network diagram for experimentation

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.330.2400	ComMoveis.331.2400
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) Experimentation: Procedures

A. Authentication and Association

- 1) Restart capture (STA C) in Wireshark on the WLAN network interface (wlp5s0 interface)

- 2) Connect STA A to SSID1 ('ComMoveis.330.2400') and stop the capture.

- 3) Configure a display filter for authentication, association and confirmation request frames (see fig. 2)

- View the STA A authentication and association process in the capture and note the sequence number of these messages in the Wireshark capture.
- Observe the Acknowledgment process.
- Compare the body of *Authentication* and *Association* messages.

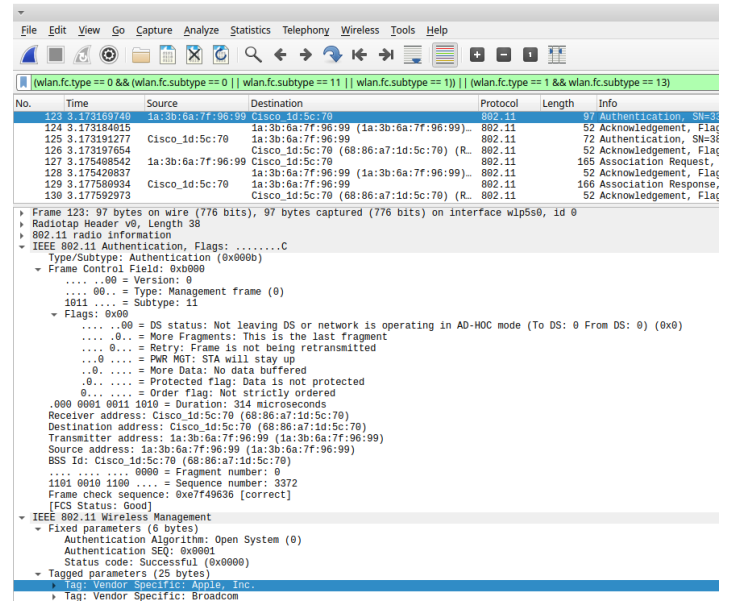


Figure 2

- 4) Change the viewing filter for DHCP packets and observe the message exchange; note the IP address assigned to STA A.
 - Relate chronologically these messages to previous ones by comparing the sequence numbers in the capture.

B. Data transfer

- 5) Restart capture in Wireshark on the WLAN network interface (wlp5s0 interface)
- 6) From STA A, ping the AccessPoint in use (10.0.2.1) for a few seconds (e.g. 10 seconds)
 - Although pings were successful on your machine (STA A), Wireshark may miss and replicate some of these packets.
- 7) Stop the capture and filter ICMP (ping) and ARP type packets in the view, analyzing the message exchanges.
 - Select one of these packages and, in the details area, note the frame and subframe type.
 - Look at the various encapsulations used until you get to the ICMP or ARP packet and explain them.

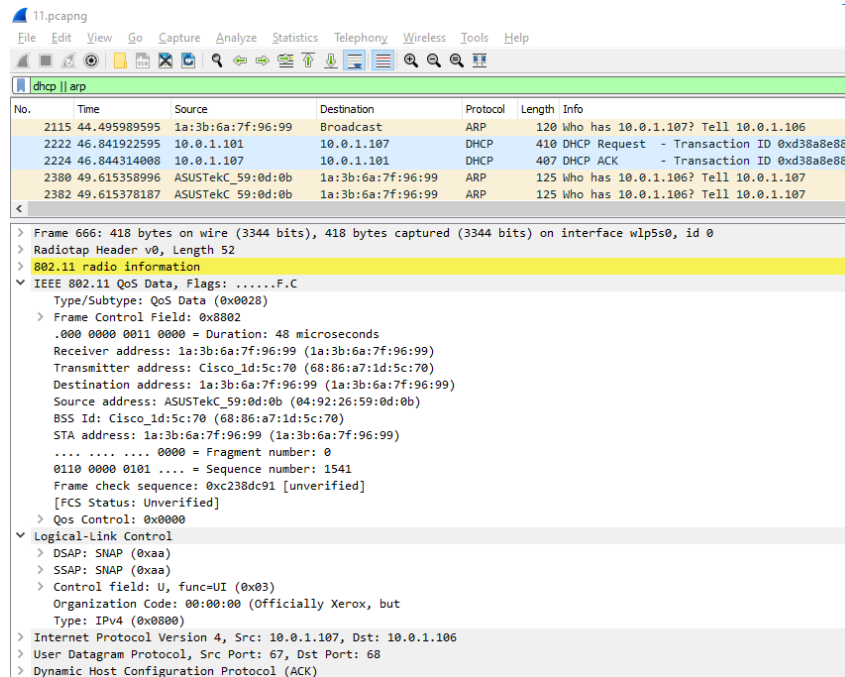


Figure 3

- 8) Now filters RTS, CTS and ICMP packets (*fc.type = 1 and subtype = 11 or 12*):
 - Check the packet exchange pattern between *ICMP Echo Request* requests and *ICMP Echo Reply* responses.
 - Note the type and subtype of captured frames.
 - Note the *DS status* flag of both *Echo Request* and *Reply* messages.

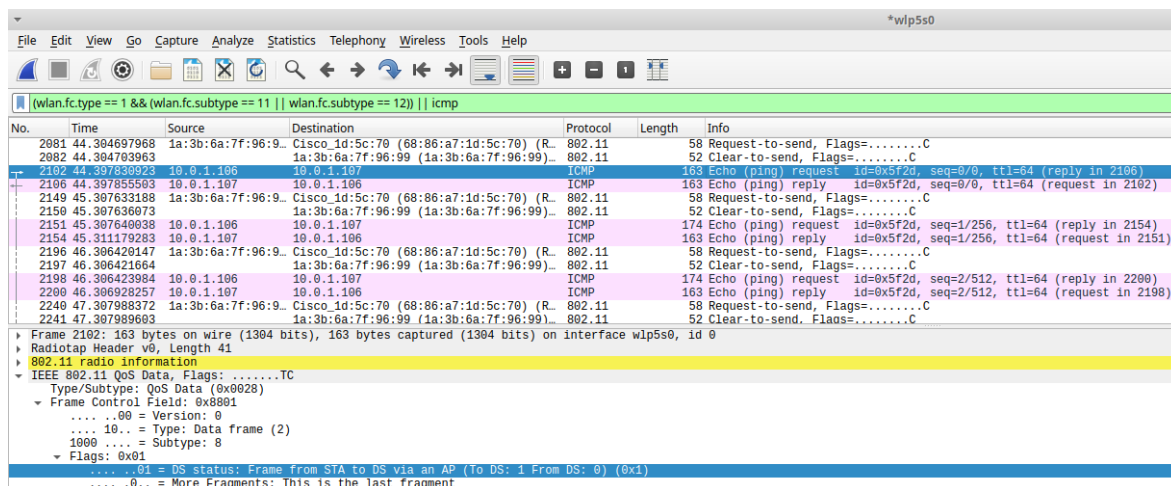


Figure 4

- 9) Place the STC on the 2.4GHz channel in your room (3 or 7); Restart capture in Wireshark on the WLAN network interface (wlp5s0 interface)
- 10) Connect STA B to the SSID of the same channel (authentication will not be requested)
 - Repeat applying a display filter to DHCP packets and note the address assigned to that station.
- 11) Ping from station STA A to STA B for a few seconds (e.g. 10 secs) and stop capturing
 - Filter RTS, CTS and ICMP packets

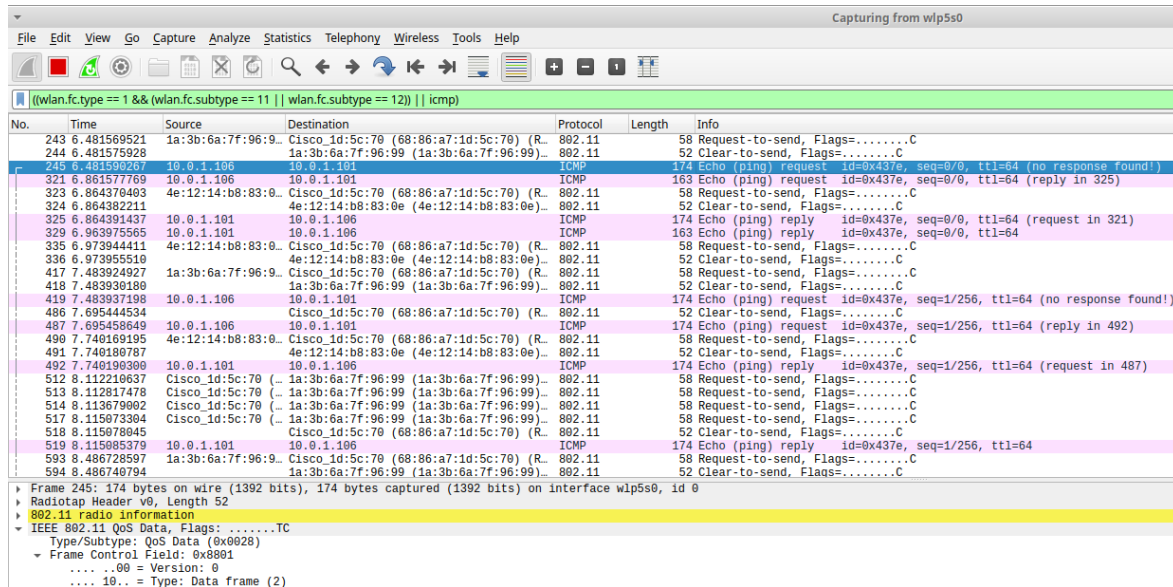


Figure 5

- Check the packet exchange pattern between ICMP Echo Request requests and ICMP Echo Reply responses; what differences do you find to the ping performed previously? Analyze based on observation of the following fields present in the 802.11 frame header:
 - *DS Status* and
 - *Receiver, Transmitter, Destination and Source Address.*

	Echo Req 1	Echo Req 2	Echo Rep 1	Echo Rep 2
	STA - AP	AP - STB	STB - AP	AP - STA
Receiver				
Transmitter				
Destination				
Source				

C. Association with security and disassociation (STA A)

For the following procedures, AP2 and SSID 2 will be used, with the following characteristics:

AP2
ComMoveis.331.2400
Channel 7 (2.442 MHz)
Authentication: WPAv2 ; Encryption: AES-CCM ; Password: "Lab.Com.WiFi"
10.0.2.[100-200]/24
Server: 10.0.2.2/24

Table 2: AP2/SSID2 configuration

- 1) Add the key in Wireshark to be able to decrypt the contents of the packets:
 - Edit → Preferences → ieee802.11 → Enable decryption → edit → '+' → key-type=wpa-pwd → key=Lab.Com.WiFi
- 2) Change STA C to channel 7 (2.422 MHz).
- 3) Restart capture on the WLAN network (wlp5s0 interface).
- 4) Connect STA A to SSID 2 ('CMAP3.331.2400'); go back to STA C and stop the capture
 - Note the EAPoL (EAP over LAN) 4-Way Handshake process used with WPAv2 and the parameters exchanged

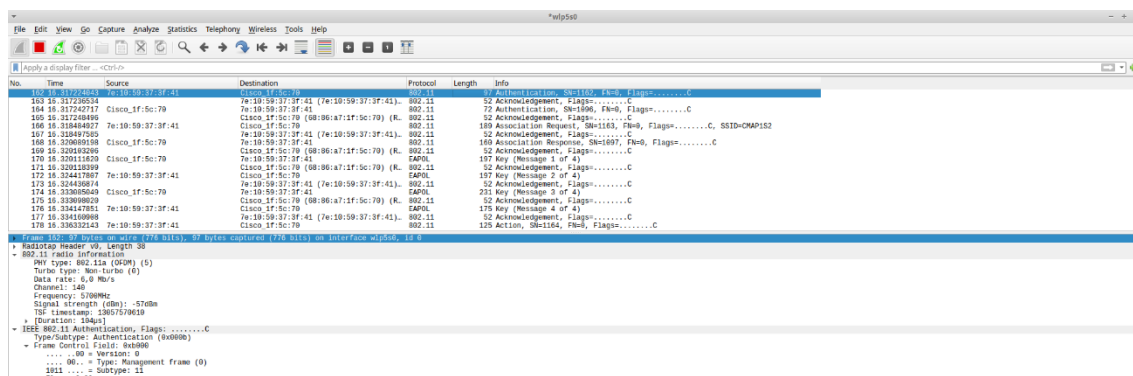


Figure 6

- 5) Restart capture on the WLAN network (wlp5s0 interface).
- 6) Return STA A to SSID 1 and stop capturing.
 - Note the single disassociation message.

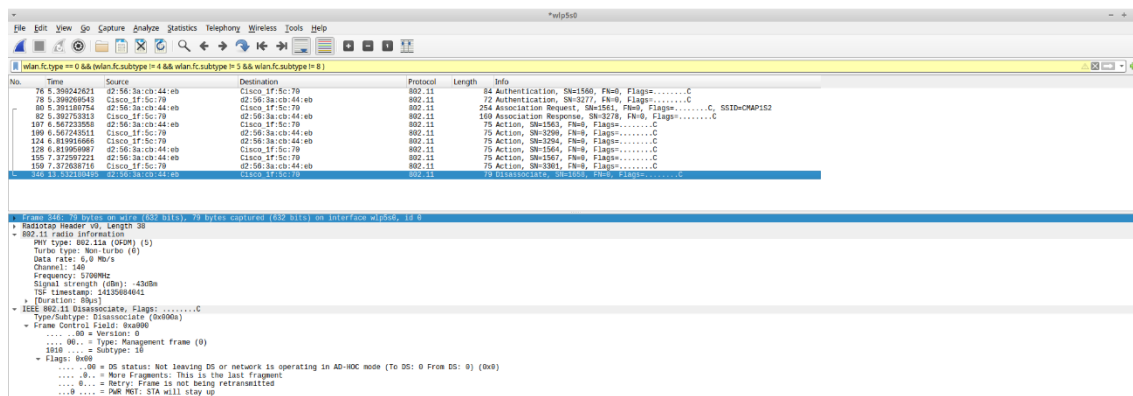


Figure 7

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. Wireshark usage and frame structure

Display filters

- 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 (see table below)

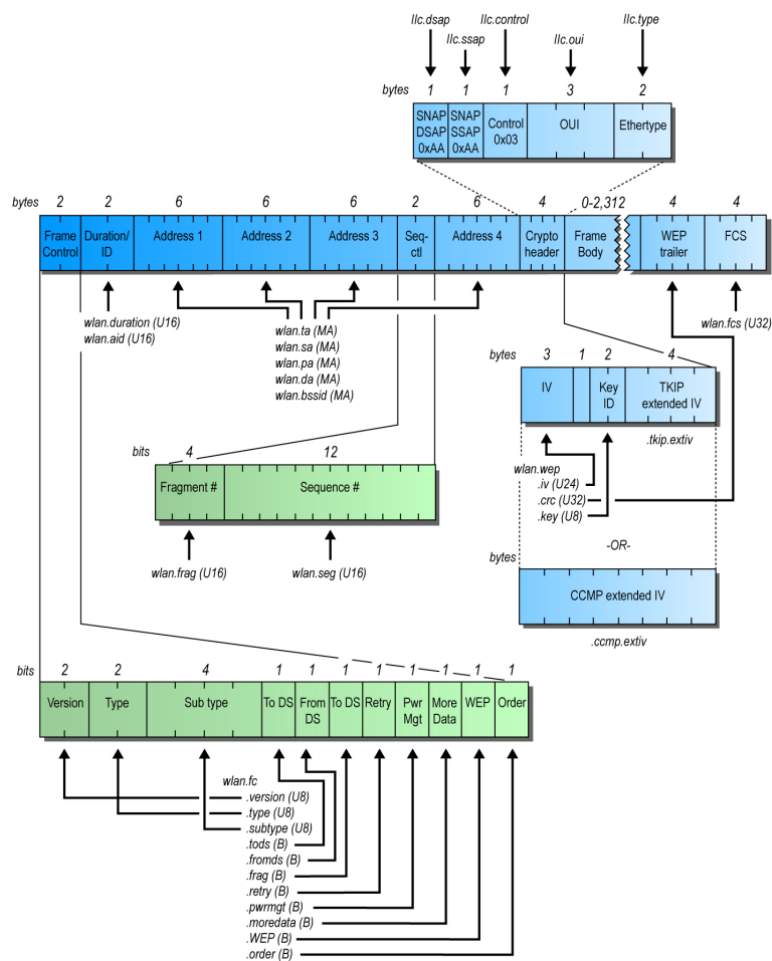


Figure 8

VII. 802.11 frames' structure and sub-types

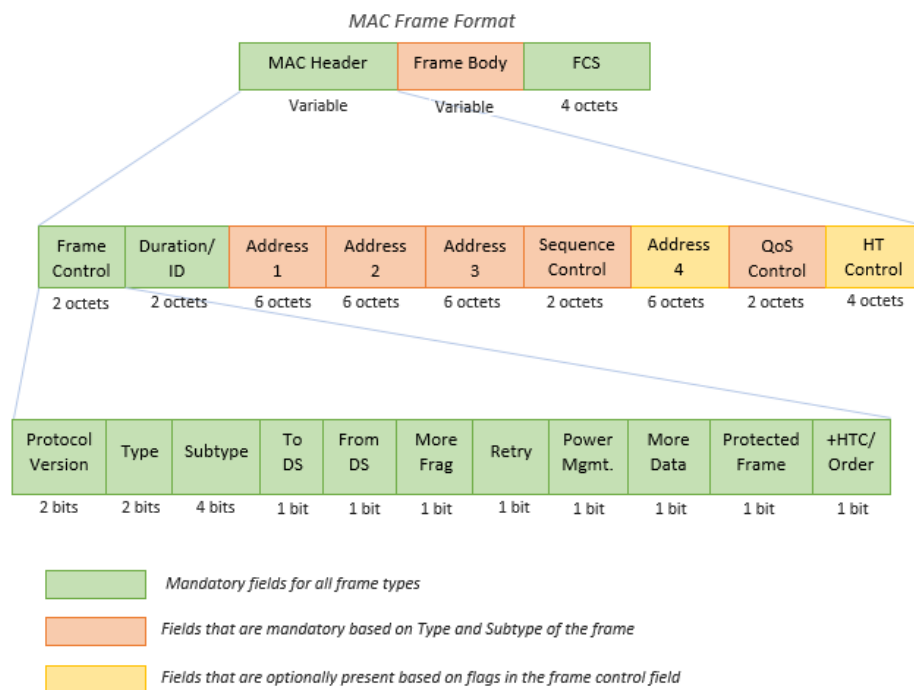


Figure 9

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 3

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 4

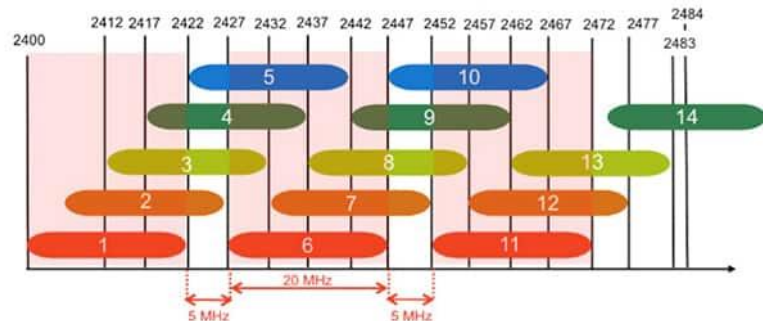


Figure 10

<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)				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					

Figure 11

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