Wireless Packet Capture on Linux

Follow along:

Alex Gavin (he/they)

github.com/a-gavin 🦀

https://github.com/a-gavin/talks/

$ whoami

Please interrupt me if you have questions!

What is wireless packet capture?

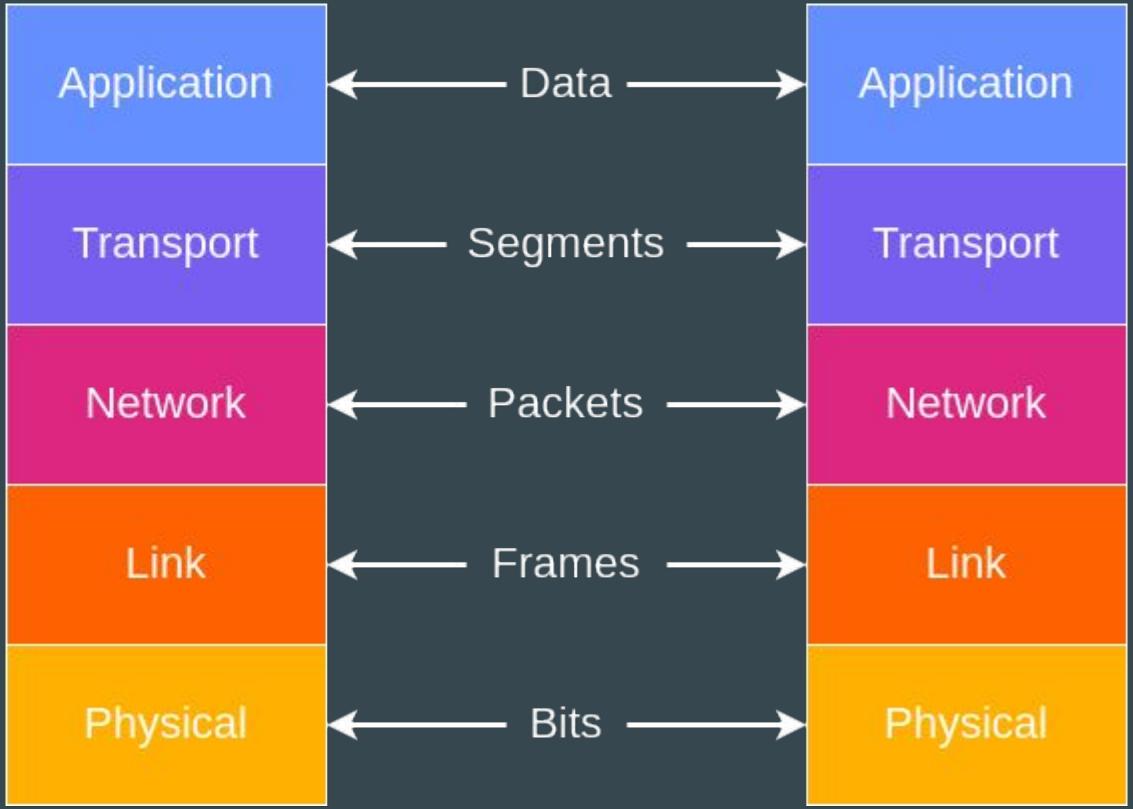
Why do packet capture?

🚨 DISCLAIMER! 🚨

This talk is for educational purposes only.

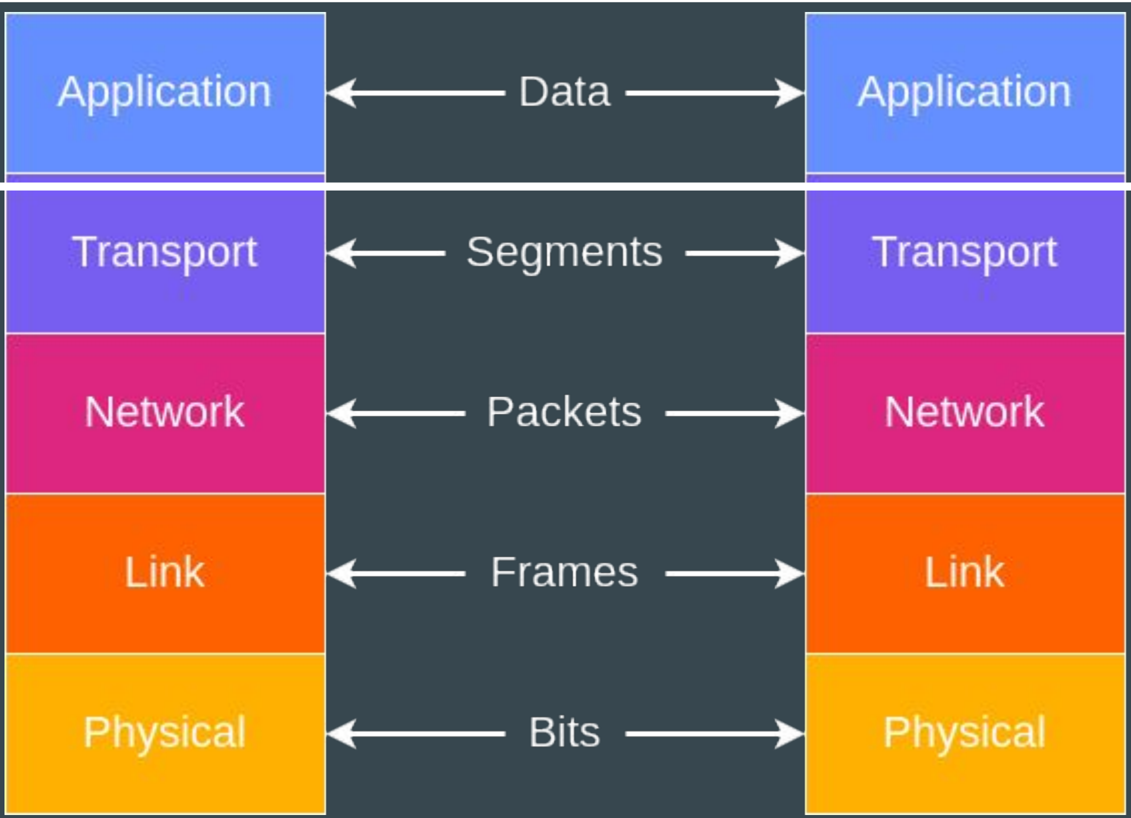
TCP/IP Model

TCP/IP Model



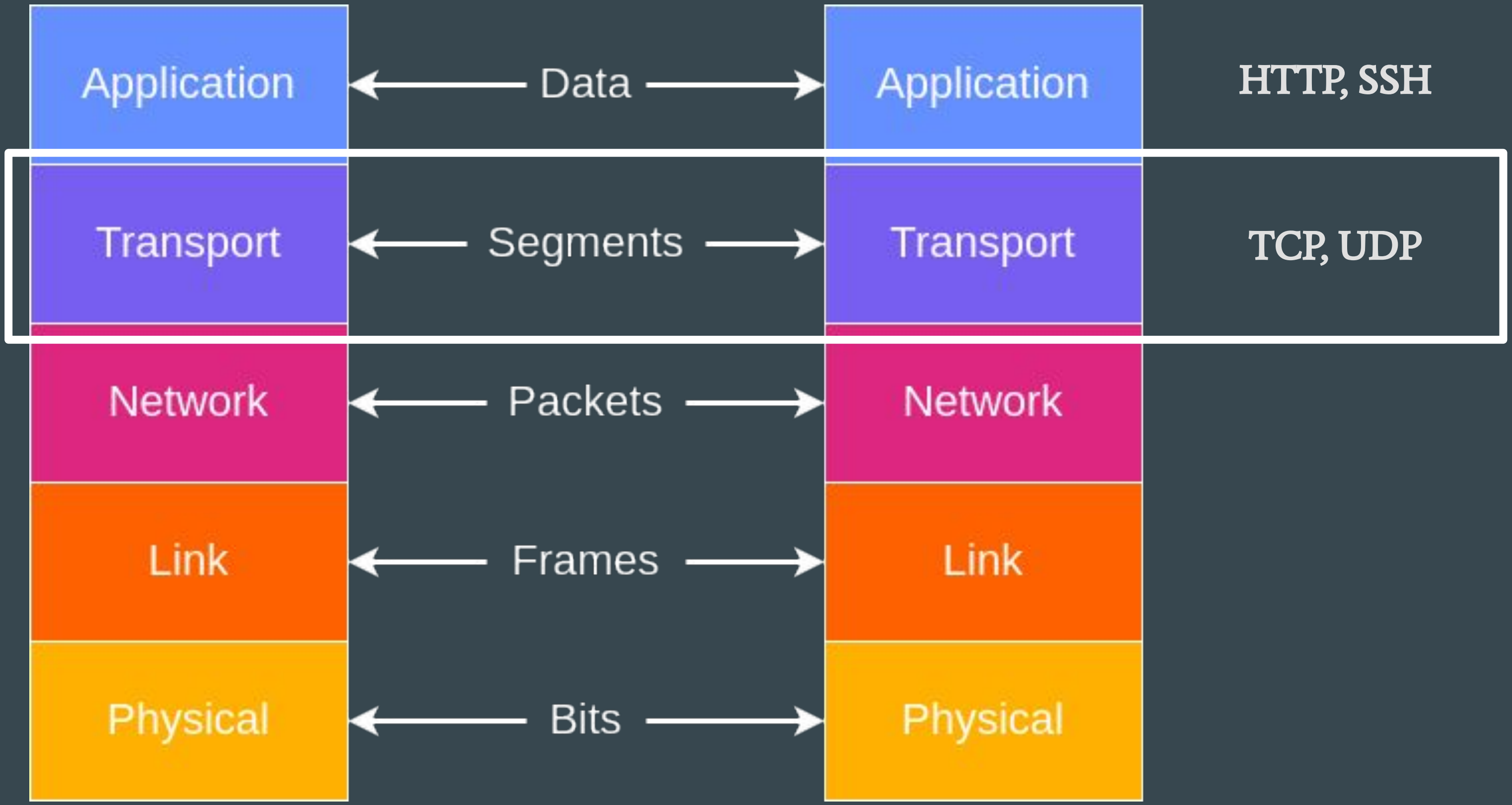
Application	← Data →	Application
Transport	← Segments →	Transport
Network	← Packets →	Network
Link	← Frames →	Link
Physical	← Bits →	Physical

TCP/IP Model



HTTP, SSH

TCP/IP Model



Application ← Data → Application HTTP, SSH

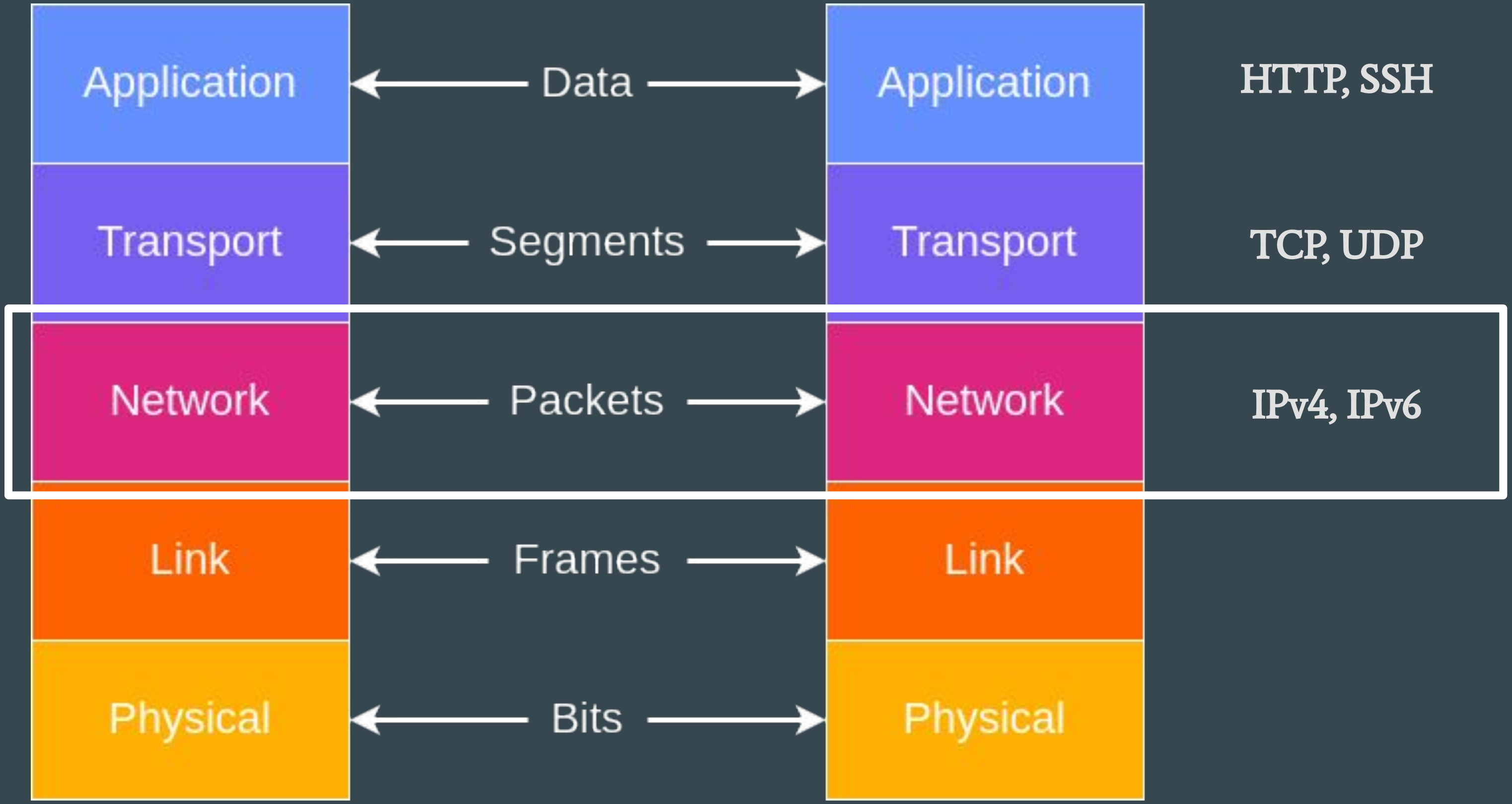
Transport ← Segments → Transport TCP, UDP

Network ← Packets → Network

Link ← Frames → Link

Physical ← Bits → Physical

TCP/IP Model



Application ← Data → Application HTTP, SSH

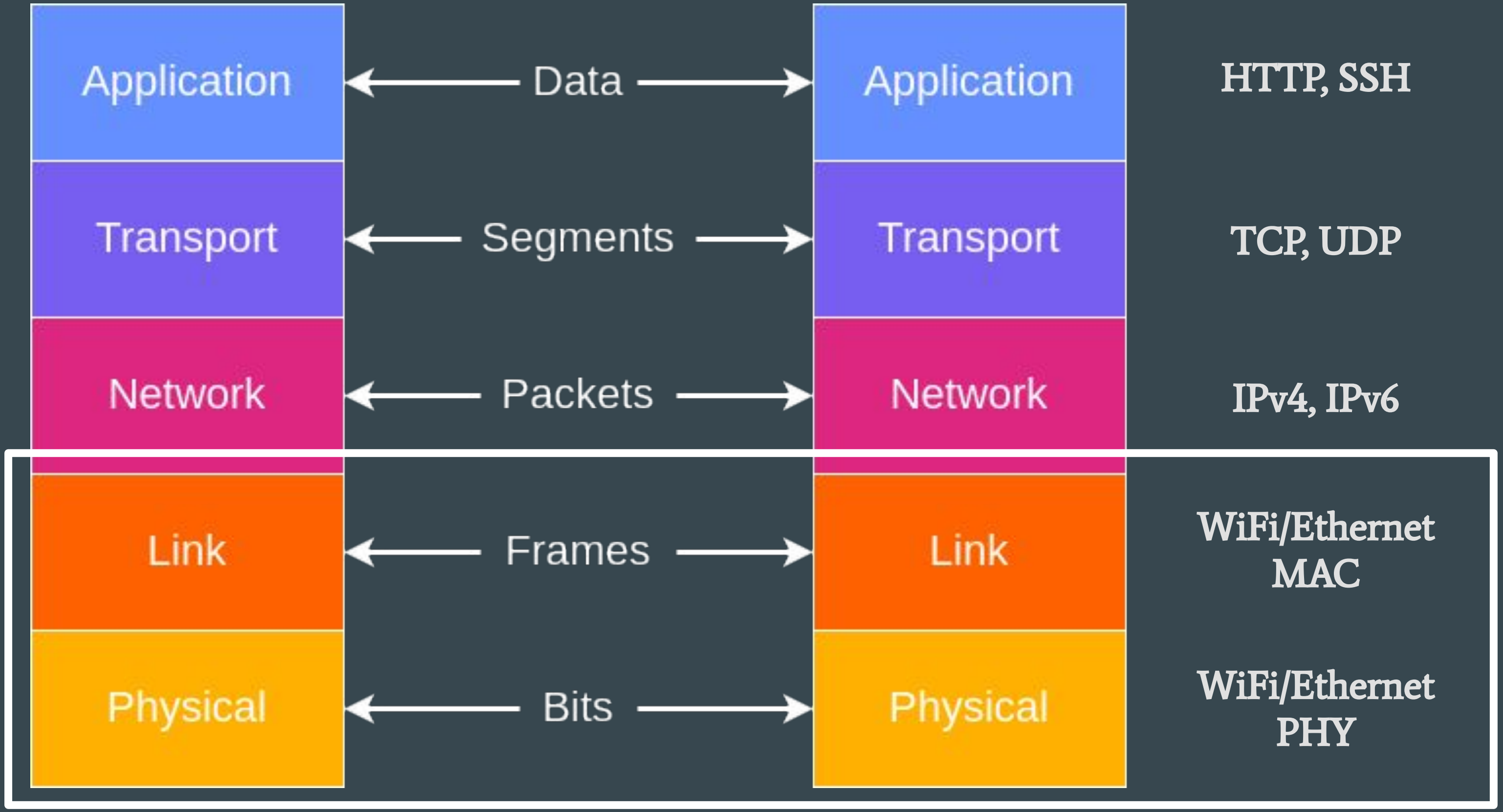
Transport ← Segments → Transport TCP, UDP

Network ← Packets → Network IPv4, IPv6

Link ← Frames → Link

Physical ← Bits → Physical

TCP/IP Model



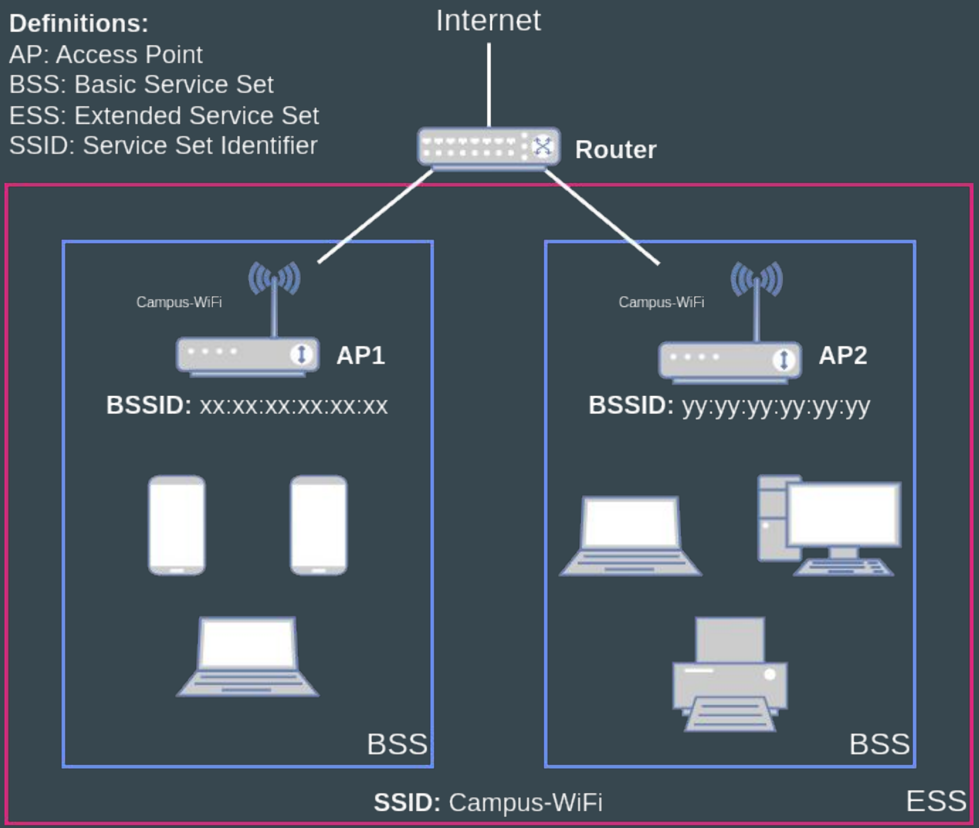
Application	← Data →	Application	HTTP, SSH
Transport	← Segments →	Transport	TCP, UDP
Network	← Packets →	Network	IPv4, IPv6
Link	← Frames →	Link	WiFi/Ethernet MAC
Physical	← Bits →	Physical	WiFi/Ethernet PHY

We’ll focus on WiFi

IEEE 802.11 standard

WiFi Basic Concepts

Definitions:
AP: Access Point
BSS: Basic Service Set
ESS: Extended Service Set
SSID: Service Set Identifier



Wireless devices communicate on channels

Slices of RF spectrum

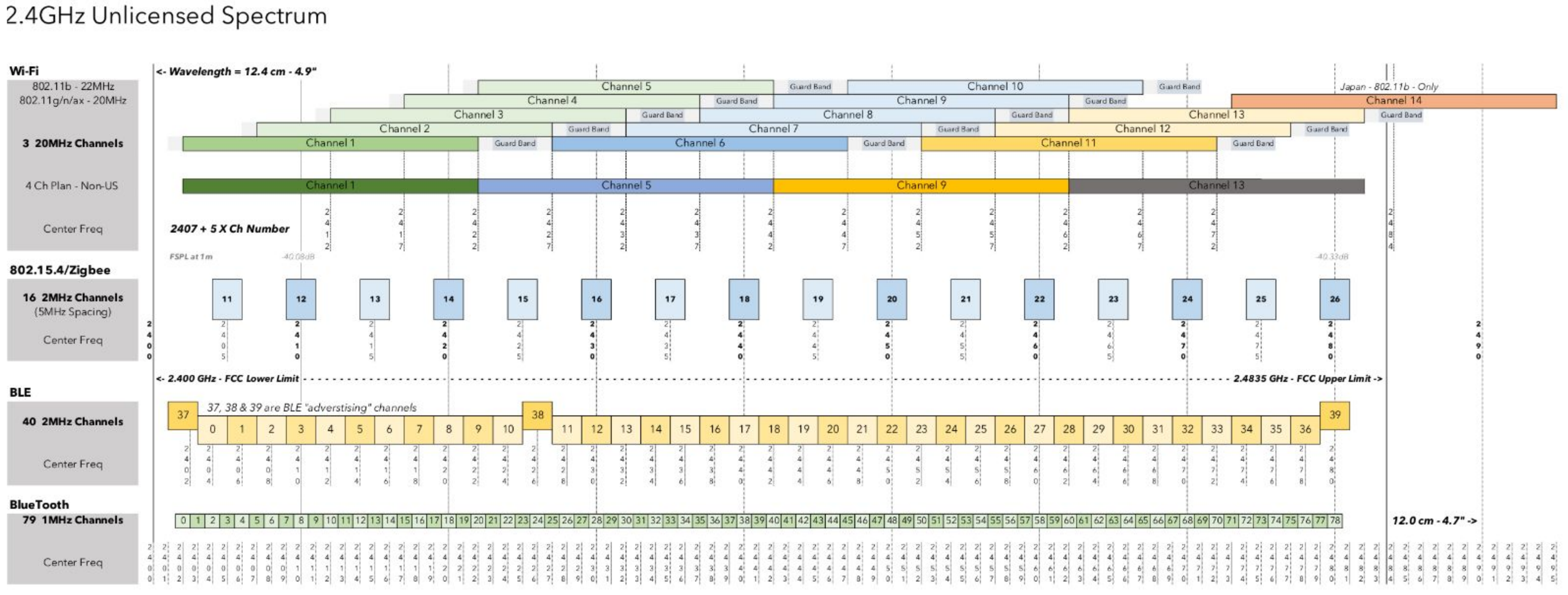
WiFi only uses part of RF spectrum

2.4GHz, 5GHz, & 6GHz* bands

* 6GHz band not permitted everywhere yet

Source: Keith Parsons, WLANProfessionals

WiFi Channels (2.4 GHz Band)



2.4GHz Unlicensed Spectrum

Wi-Fi

802.11b - 22MHz
802.11g/n/ax - 20MHz

3 20MHz Channels

4 Ch Plan - Non-US

Center Freq

<- Wavelength = 12.4 cm - 4.9"

Channel 1, Guard Band, Channel 6, Guard Band, Channel 11, Guard Band

Channel 2, Guard Band, Channel 7, Guard Band, Channel 12, Guard Band

Channel 3, Guard Band, Channel 8, Guard Band, Channel 13, Guard Band

Channel 4, Guard Band, Channel 9, Guard Band

Channel 5, Guard Band, Channel 10, Guard Band

Japan - 802.11b - Only

Channel 14

Channel 1, Channel 5, Channel 9, Channel 13

2407 + 5 X Ch Number

2412 2417 2422 2427 2432 2437 2442 2447 2452 2457 2462 2467 2472 2484

FSPL at 1m -40.08dB -40.33dB

802.15.4/Zigbee

16 2MHz Channels
(5MHz Spacing)

Center Freq

11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

2400 2405 2410 2415 2420 2425 2430 2435 2440 2445 2450 2455 2460 2465 2470 2475 2480 2490

<- 2.400 GHz - FCC Lower Limit *2.4835 GHz - FCC Upper Limit ->*

BLE

40 2MHz Channels

Center Freq

37, 38 & 39 are BLE "adverstising" channels

37 0 1 2 3 4 5 6 7 8 9 10 38 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 39

2402 2404 2406 2408 2410 2412 2414 2416 2418 2420 2422 2424 2426 2428 2430 2432 2434 2436 2438 2440 2442 2444 2446 2448 2450 2452 2454 2456 2458 2460 2462 2464 2466 2468 2470 2472 2474 2476 2478 2480

BlueTooth

79 1MHz Channels

Center Freq

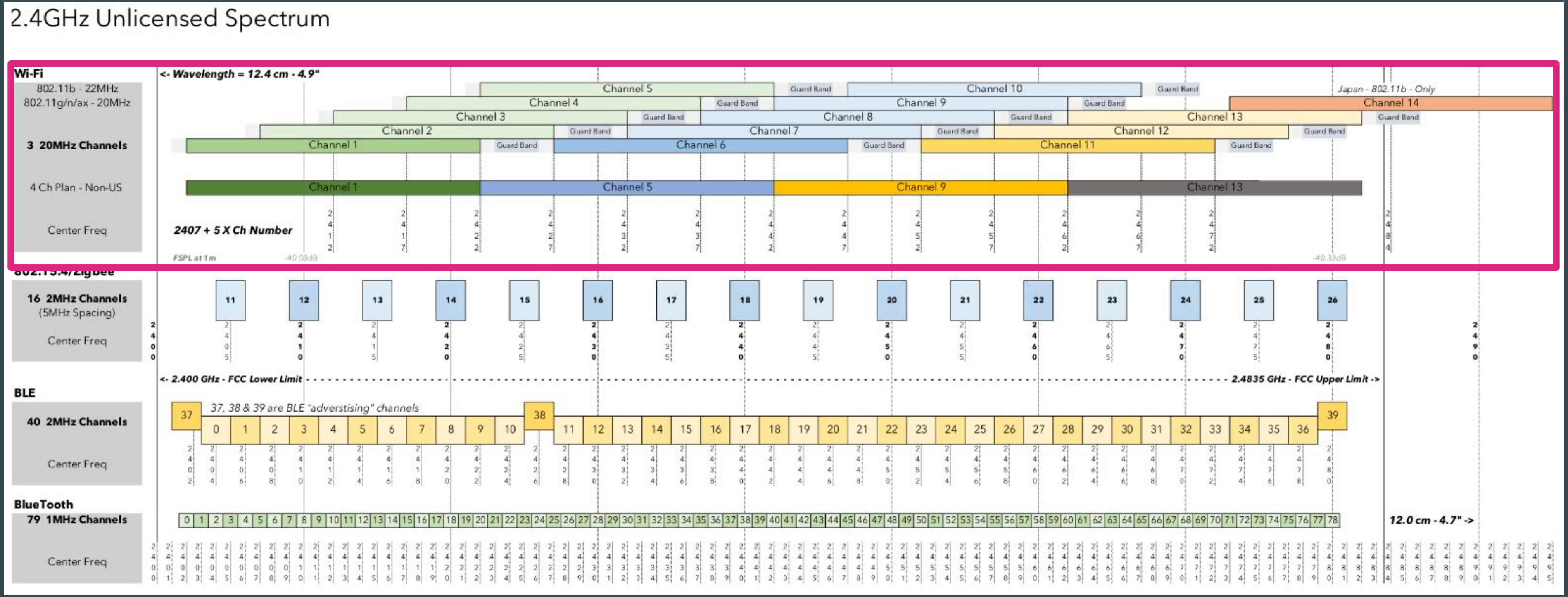
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78

12.0 cm - 4.7" ->

2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495

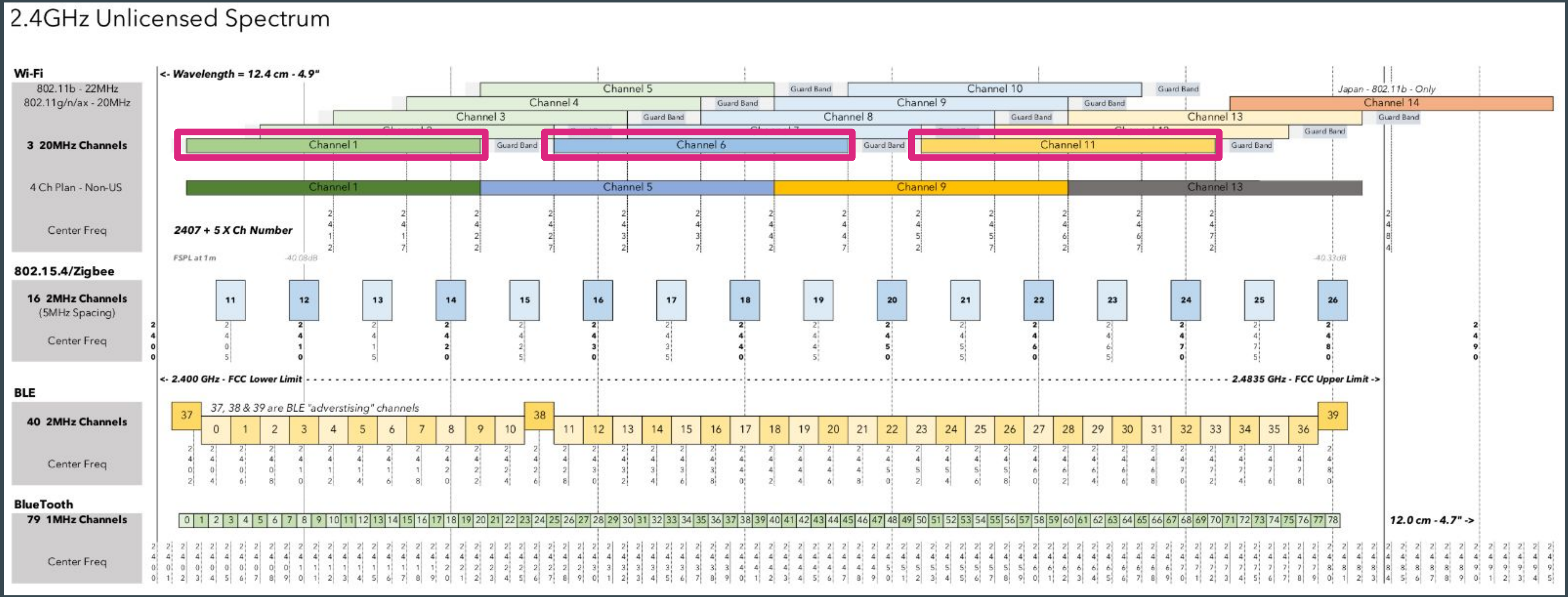
Source: Keith Parsons, WLANProfessionals

WiFi Channels (2.4 GHz Band)



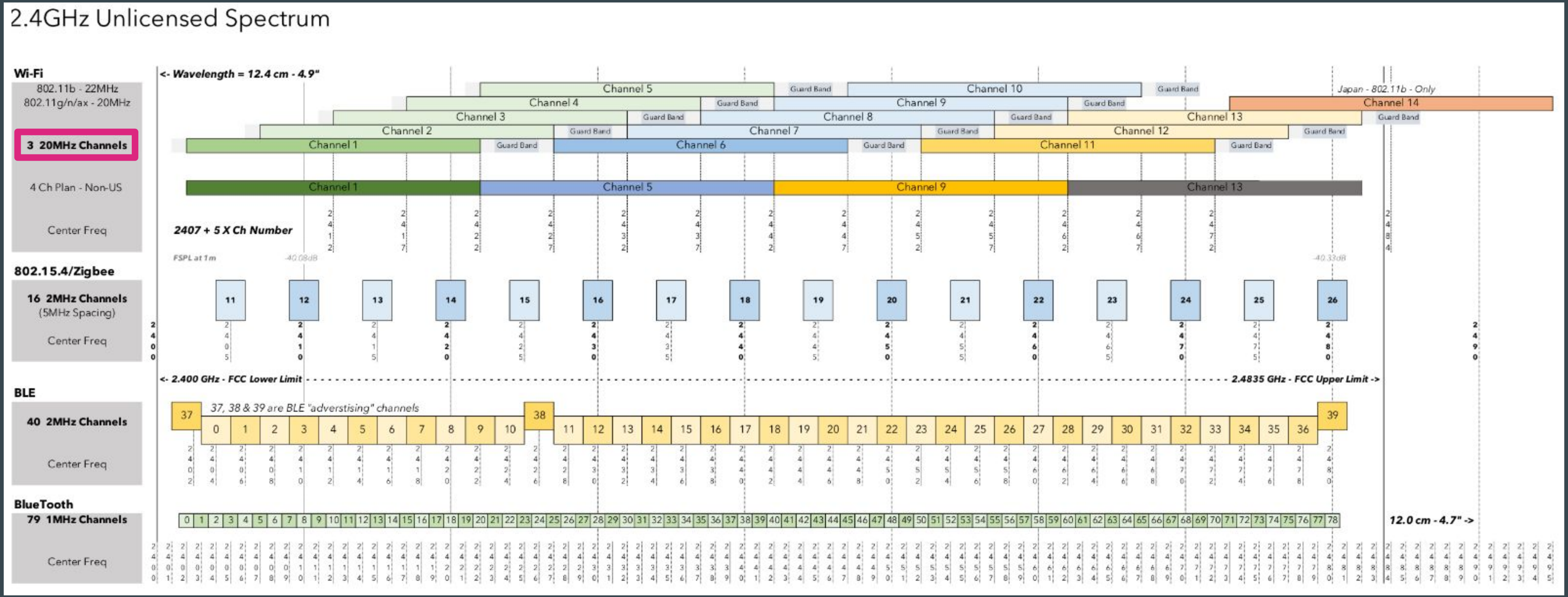
Source: Keith Parsons, WLANProfessionals

WiFi Channels (2.4 GHz Band)



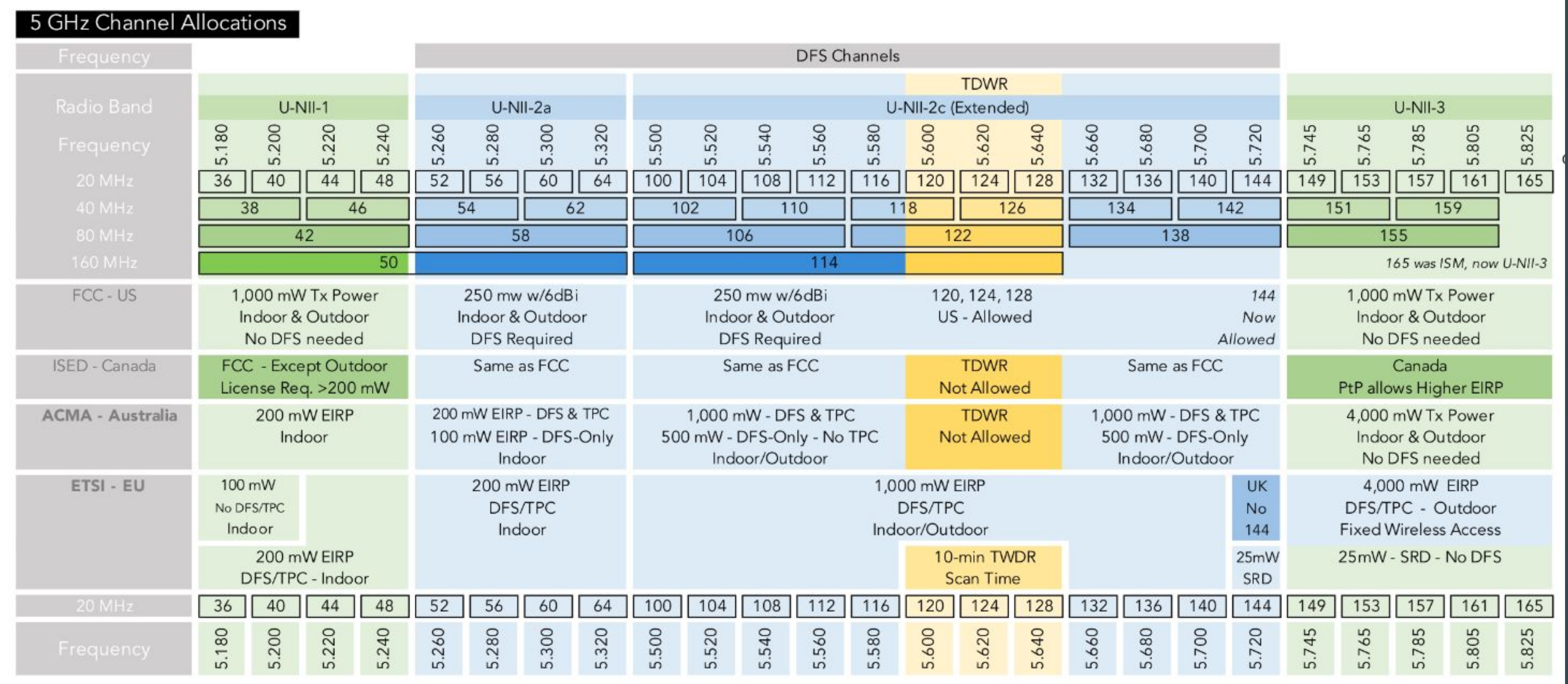
Source: Keith Parsons, WLANProfessionals

WiFi Channels (2.4 GHz Band)



Source: Keith Parsons, WLANProfessionals

WiFi Channels (5 GHz Band)

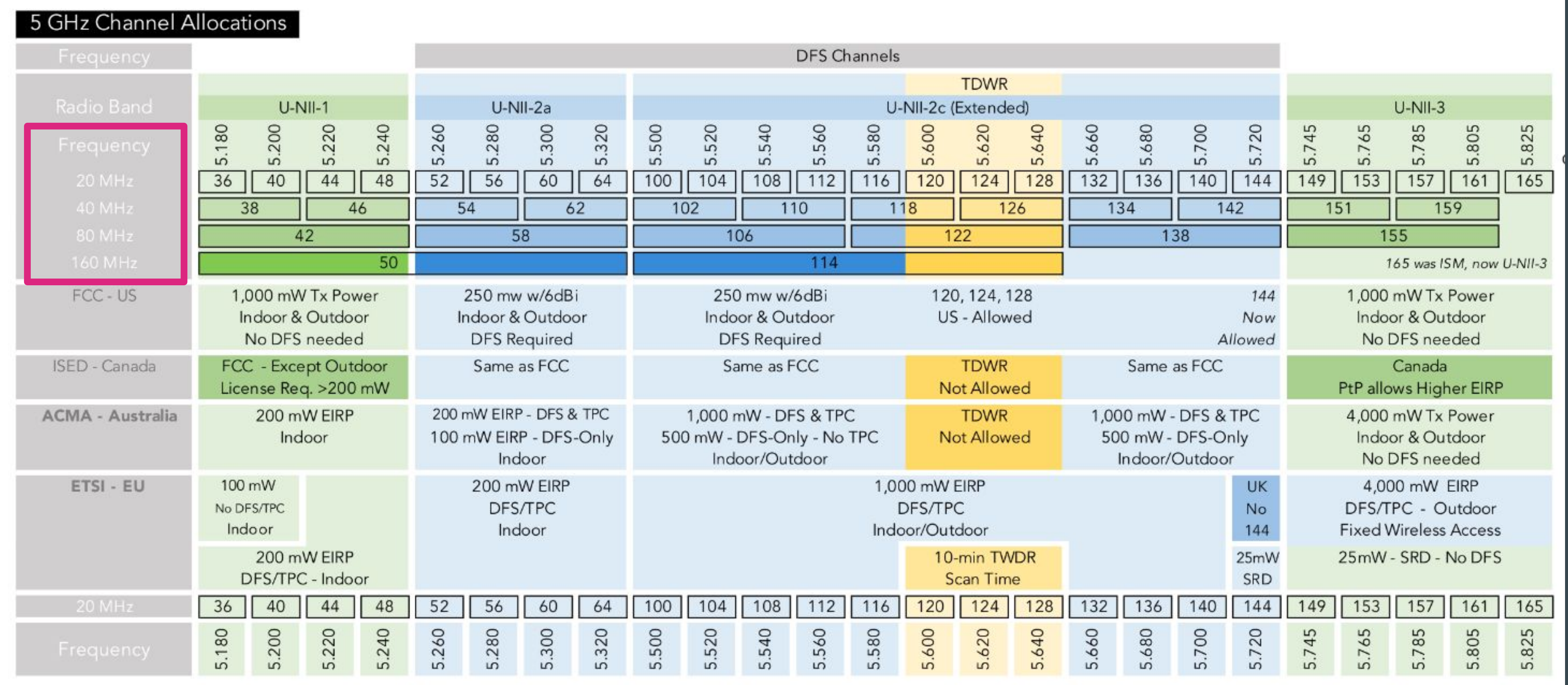


5 GHz Channel Allocations

Frequency					DFS Channels																				
														TDWR											
Radio Band	U-NII-1				U-NII-2a				U-NII-2c (Extended)												U-NII-3				
Frequency	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825
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												165 was ISM, now U-NII-3				
FCC - US	1,000 mW Tx Power Indoor & Outdoor No DFS needed				250 mw w/6dBi Indoor & Outdoor DFS Required				250 mw w/6dBi Indoor & Outdoor DFS Required					120, 124, 128 US - Allowed						144 Now Allowed	1,000 mW Tx Power Indoor & Outdoor No DFS needed				
ISED - Canada	FCC - Except Outdoor License Req. >200 mW				Same as FCC				Same as FCC					TDWR Not Allowed			Same as FCC				Canada PtP allows Higher EIRP				
ACMA - Australia	200 mW EIRP Indoor				200 mW EIRP - DFS & TPC 100 mW EIRP - DFS-Only Indoor				1,000 mW - DFS & TPC 500 mW - DFS-Only - No TPC Indoor/Outdoor					TDWR Not Allowed			1,000 mW - DFS & TPC 500 mW - DFS-Only Indoor/Outdoor				4,000 mW Tx Power Indoor & Outdoor No DFS needed				
ETSI - EU	100 mW No DFS/TPC Indoor				200 mW EIRP DFS/TPC Indoor				1,000 mW EIRP DFS/TPC Indoor/Outdoor											UK No 144	4,000 mW EIRP DFS/TPC - Outdoor Fixed Wireless Access				
	200 mW EIRP DFS/TPC - Indoor													10-min TWDR Scan Time						25mW SRD	25mW - SRD - No DFS				
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
Frequency	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825

Source: Keith Parsons, WLANProfessionals

WiFi Channels (5 GHz Band)

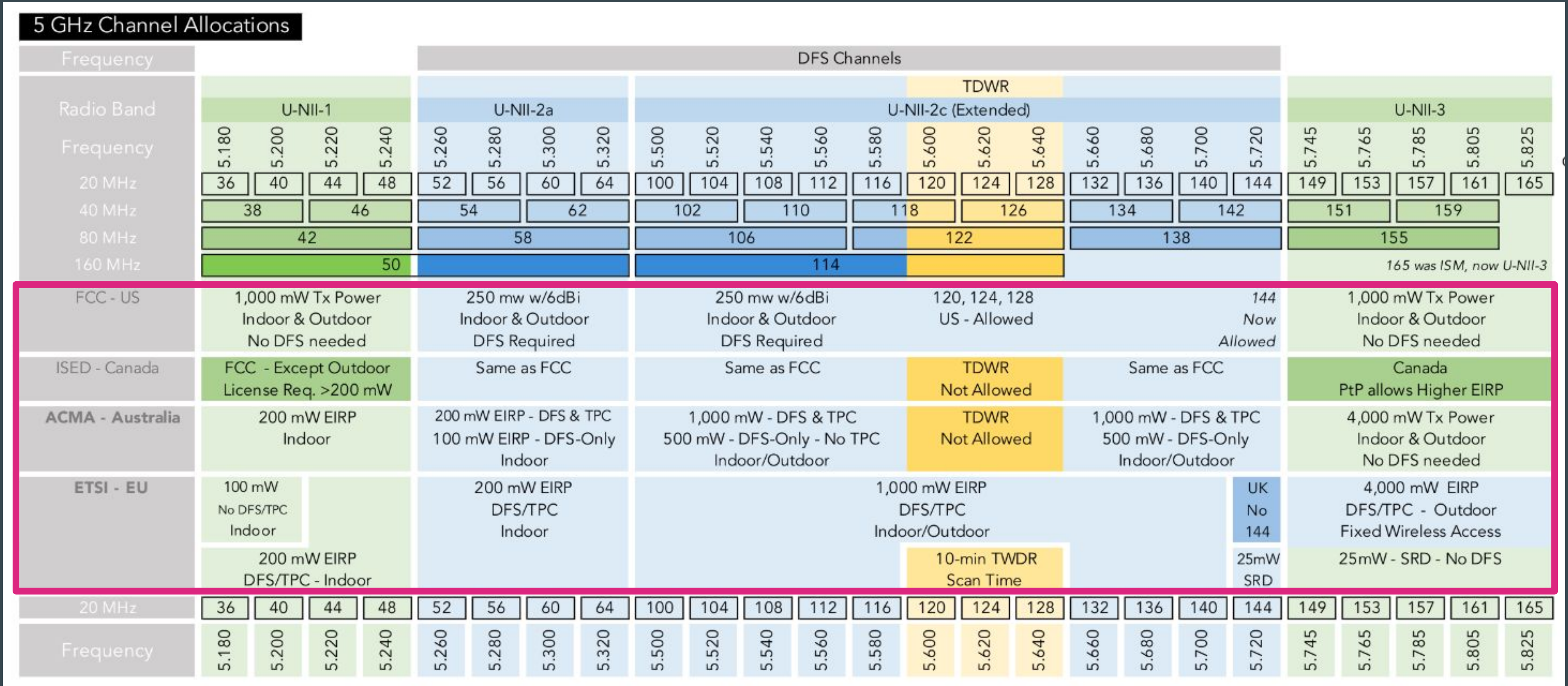


5 GHz Channel Allocations

Frequency					DFS Channels																				
														TDWR											
Radio Band	U-NII-1				U-NII-2a				U-NII-2c (Extended)												U-NII-3				
Frequency	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825
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												165 was ISM, now U-NII-3				
FCC - US	1,000 mW Tx Power Indoor & Outdoor No DFS needed				250 mw w/6dBi Indoor & Outdoor DFS Required				250 mw w/6dBi Indoor & Outdoor DFS Required					120, 124, 128 US - Allowed						144 Now Allowed	1,000 mW Tx Power Indoor & Outdoor No DFS needed				
ISED - Canada	FCC - Except Outdoor License Req. >200 mW				Same as FCC				Same as FCC					TDWR Not Allowed			Same as FCC				Canada PtP allows Higher EIRP				
ACMA - Australia	200 mW EIRP Indoor				200 mW EIRP - DFS & TPC 100 mW EIRP - DFS-Only Indoor				1,000 mW - DFS & TPC 500 mW - DFS-Only - No TPC Indoor/Outdoor					TDWR Not Allowed			1,000 mW - DFS & TPC 500 mW - DFS-Only Indoor/Outdoor				4,000 mW Tx Power Indoor & Outdoor No DFS needed				
ETSI - EU	100 mW No DFS/TPC Indoor				200 mW EIRP DFS/TPC Indoor				1,000 mW EIRP DFS/TPC Indoor/Outdoor											UK No 144	4,000 mW EIRP DFS/TPC - Outdoor Fixed Wireless Access				
	200 mW EIRP DFS/TPC - Indoor													10-min TWDR Scan Time						25mW SRD	25mW - SRD - No DFS				
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
Frequency	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825

Source: Keith Parsons, WLANProfessionals

WiFi Channels (5 GHz Band)

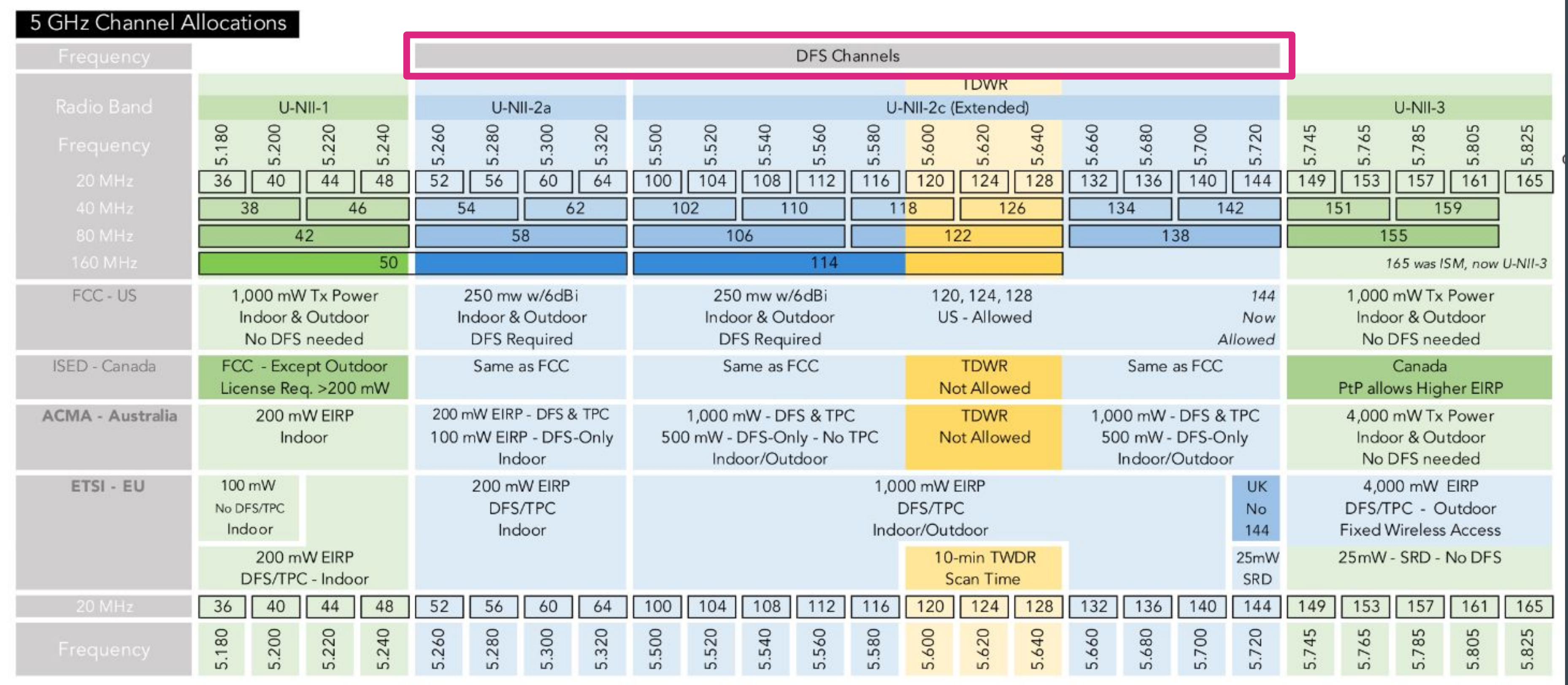


5 GHz Channel Allocations

Frequency					DFS Channels																				
														TDWR											
Radio Band	U-NII-1				U-NII-2a				U-NII-2c (Extended)												U-NII-3				
Frequency	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825
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												*165 was ISM, now U-NII-3*				
FCC - US	1,000 mW Tx Power Indoor & Outdoor No DFS needed				250 mw w/6dBi Indoor & Outdoor DFS Required				250 mw w/6dBi Indoor & Outdoor DFS Required					120, 124, 128 US - Allowed						*144 Now Allowed*	1,000 mW Tx Power Indoor & Outdoor No DFS needed				
ISED - Canada	FCC - Except Outdoor License Req. >200 mW				Same as FCC				Same as FCC					TDWR Not Allowed			Same as FCC				Canada PtP allows Higher EIRP				
ACMA - Australia	200 mW EIRP Indoor				200 mW EIRP - DFS & TPC 100 mW EIRP - DFS-Only Indoor				1,000 mW - DFS & TPC 500 mW - DFS-Only - No TPC Indoor/Outdoor					TDWR Not Allowed			1,000 mW - DFS & TPC 500 mW - DFS-Only Indoor/Outdoor				4,000 mW Tx Power Indoor & Outdoor No DFS needed				
ETSI - EU	100 mW No DFS/TPC Indoor				200 mW EIRP DFS/TPC Indoor				1,000 mW EIRP DFS/TPC Indoor/Outdoor											UK No 144	4,000 mW EIRP DFS/TPC - Outdoor Fixed Wireless Access				
	200 mW EIRP DFS/TPC - Indoor													10-min TWDR Scan Time						25mW SRD	25mW - SRD - No DFS				
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
Frequency	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825

Source: Keith Parsons, WLANProfessionals

WiFi Channels (5 GHz Band)



5 GHz Channel Allocations

Frequency					DFS Channels																				
														TDWR											
Radio Band	U-NII-1				U-NII-2a				U-NII-2c (Extended)												U-NII-3				
Frequency	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825
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												165 was ISM, now U-NII-3				
FCC - US	1,000 mW Tx Power Indoor & Outdoor No DFS needed				250 mw w/6dBi Indoor & Outdoor DFS Required				250 mw w/6dBi Indoor & Outdoor DFS Required					120, 124, 128 US - Allowed						144 Now Allowed	1,000 mW Tx Power Indoor & Outdoor No DFS needed				
ISED - Canada	FCC - Except Outdoor License Req. >200 mW				Same as FCC				Same as FCC					TDWR Not Allowed			Same as FCC				Canada PtP allows Higher EIRP				
ACMA - Australia	200 mW EIRP Indoor				200 mW EIRP - DFS & TPC 100 mW EIRP - DFS-Only Indoor				1,000 mW - DFS & TPC 500 mW - DFS-Only - No TPC Indoor/Outdoor					TDWR Not Allowed			1,000 mW - DFS & TPC 500 mW - DFS-Only Indoor/Outdoor				4,000 mW Tx Power Indoor & Outdoor No DFS needed				
ETSI - EU	100 mW No DFS/TPC Indoor				200 mW EIRP DFS/TPC Indoor				1,000 mW EIRP DFS/TPC Indoor/Outdoor											UK No 144	4,000 mW EIRP DFS/TPC - Outdoor Fixed Wireless Access				
	200 mW EIRP DFS/TPC - Indoor													10-min TWDR Scan Time						25mW SRD	25mW - SRD - No DFS				
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
Frequency	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825

Time for some packet capture!

Tools for the Job

- Wireshark
- iw
- aircrack-ng
- Kernel debugfs files (if you really wanted to)
    - Have to for some things

Tools for the Job

- Wireshark
- iw
- aircrack-ng
- Kernel debugfs files (if you really wanted to)
    - Have to for some things

Probably easiest to use these

Tools for the Job

- Wireshark
- iw
- aircrack-ng
- Kernel debugfs files (if you really wanted to)
  - Have to for some things

But we’ll use these instead