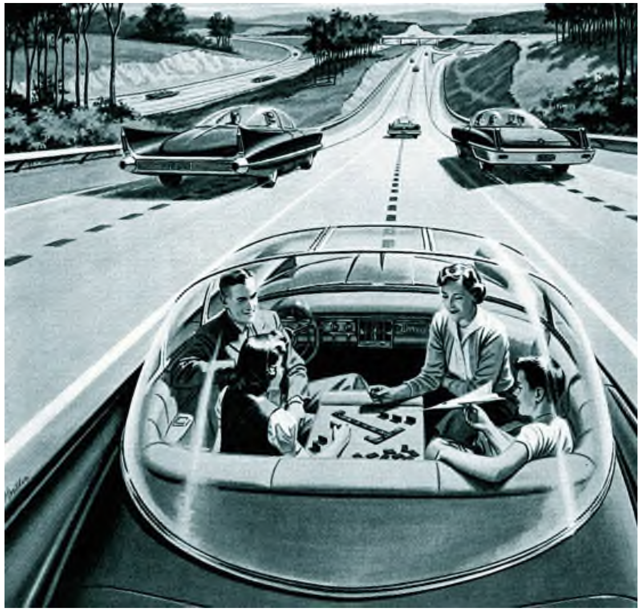


Connected Vehicle

H.Perrault
herve.perrault@ext.isep.fr

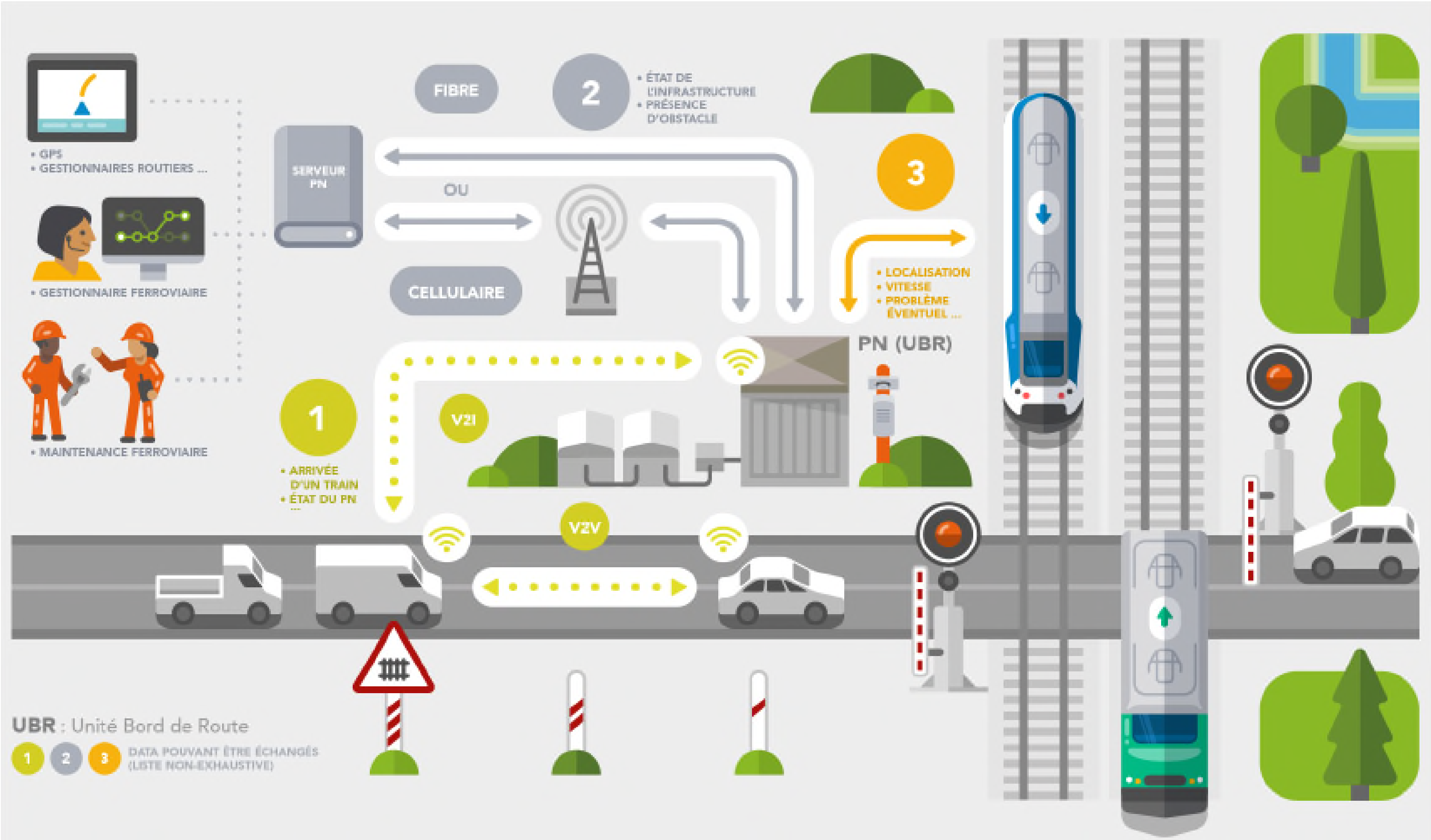
Wifi – Spectrum analysis LAB

15/10/2024

Agenda

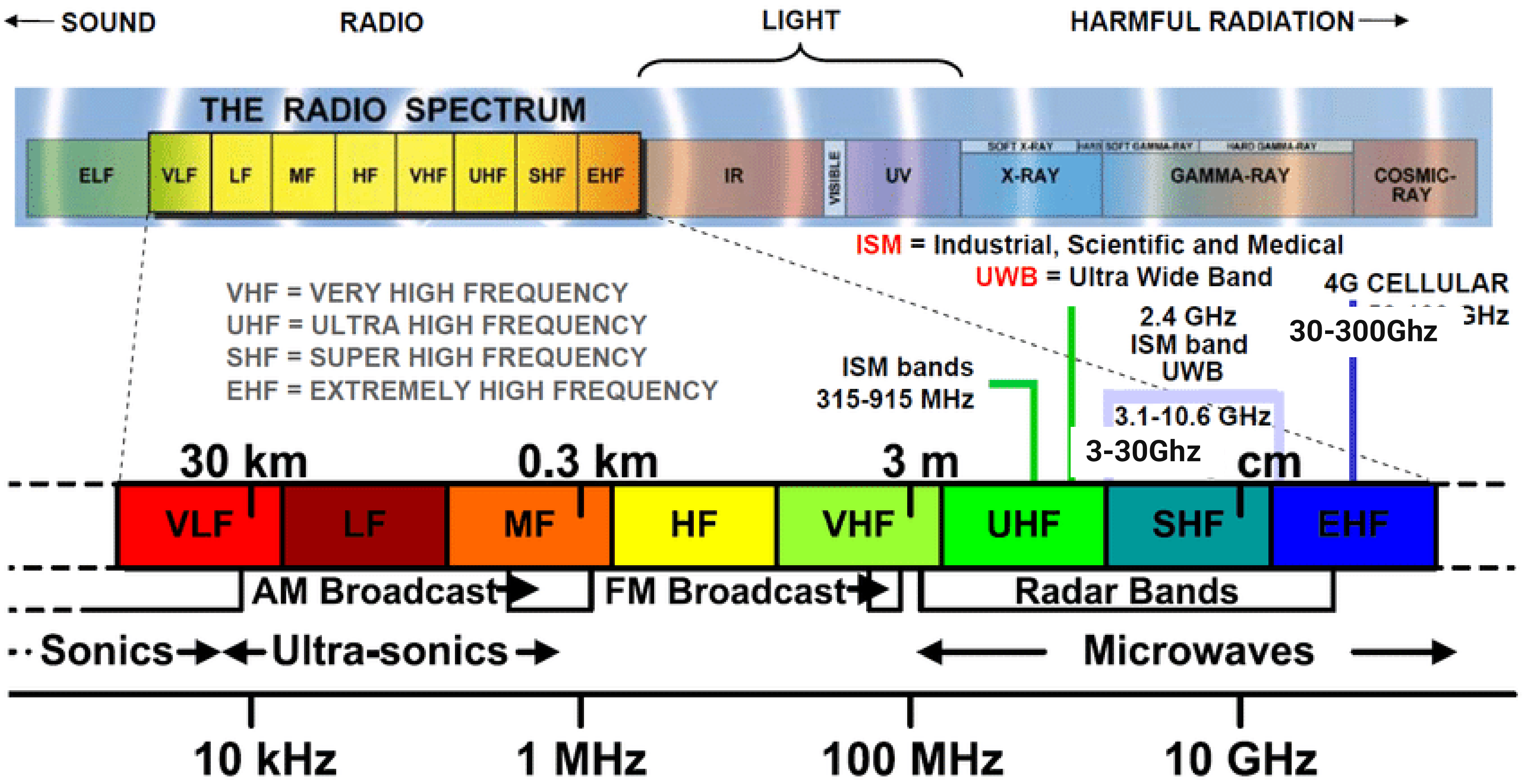
- Connected vehicle : Reminder
  - 802.11p
- Standard Wifi
  - Norms,
  - Channels
  - Mechanism overview
- Spectrum analysis
  - Analyzer,
  - AP
- LAB

Road infra & Vehicle connected



European Scoop project - 2019

Electromagnetic Spectrum frequency band



Wifi 2.4G : 2,400 GHz et 2,500 GHz
Wifi 5G : 5,15 – 5,875 GHz
Wifi 6G (E) : 5,945 – 6,425 GHz (France)

3G : 900 MHz et 2,1 GHz
4G : 700 et 800 MHz, 1,8 ; 2,1 et 2,6 GHz
5G : Bandes 4G + ~3,5 GHz puis 26 GHz (futur).

Wifi - Norms

Standard	Année	Fréquence	Vitesse	Taille de canal
802.11	1997	2,4GHz	2Mbits	22MHz
802.11a	1999	5GHz	54Mbits	20Mhz
802.11b	1999	2,4GHz	11Mbits	22MHz
802.11g	2003	2,4GHz	54Mbits	20MHz
802.11n	2009	2,4GHz/5GHz	450Mbits	20/40MHz
802.11ac	2014	5GHz	1300Mbits	20/40/80/160MHz

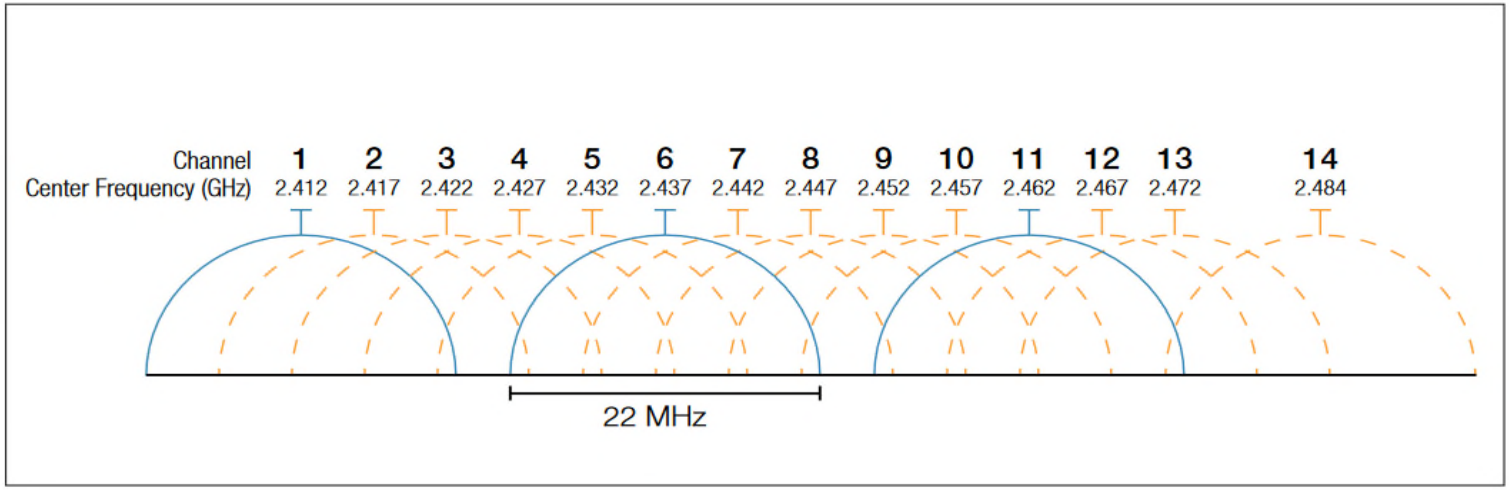
Wi-Fi is a standardized communication technology for Wireless Local Area Network (WLAN)

➔ Well known as IEEE 802.11.

This technology was popularized with 802.11b (11Mbps), in 1999.

11 to 14 channels are available, 3 (1, 6 and 11) are non overlapped.

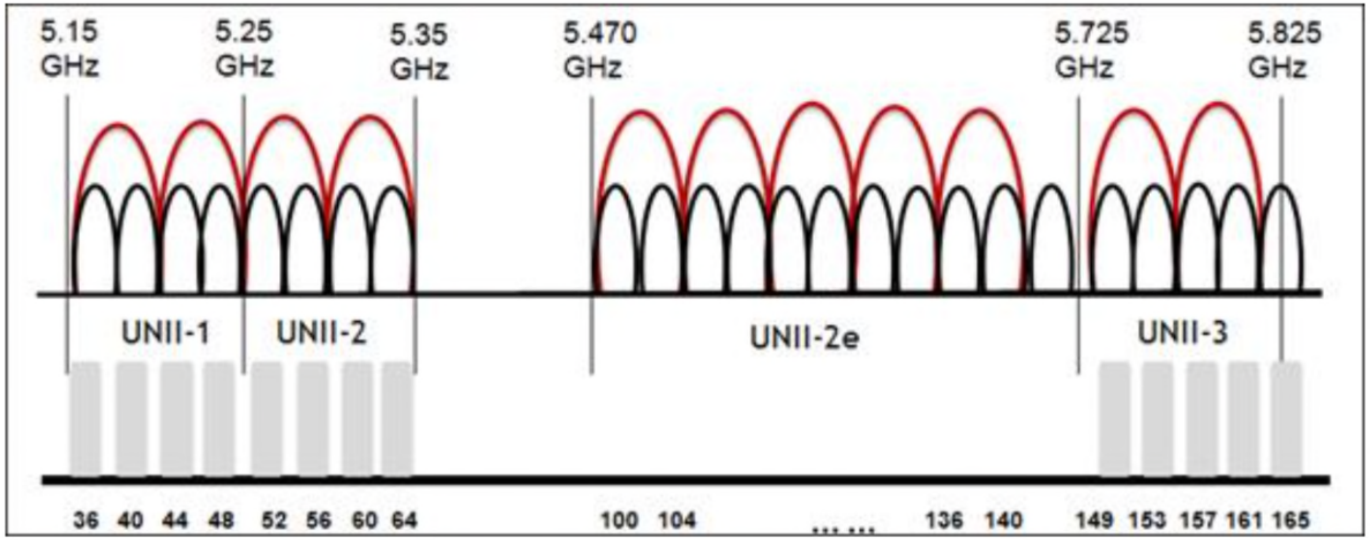
Wifi 2.4GHz



These frequencies are the central frequencies of each channel. Around this central frequency the signal is modulated over a frequency range of 20 MHz to 22 MHz. Each channel therefore occupies a frequency range of +/-11 MHz around its central frequency (+/-10 MHz for the latest versions of 802.11g and 802.11n).

Channels are largely overlapping, so it is desirable to use free channels if you want to avoid causing and suffering radio interference. At the time of 802.11b, each channel occupied a frequency range of 22 MHz, and it was then better to use only channels 1 - 6 - 11 in Europe. These 3 channels remain the most used, specially AP.

Wifi 5 GHz



The frequencies usable in this band are defined by the standards IEEE 802.11n and IEEE 802.11ac.

Some of these frequencies may, in some countries, conflict with other uses, Especially military or weather radars. IEEE recommends dynamic channel selection by the hotspot, rather than the static allocation usually used in the 2.4 GHz band.

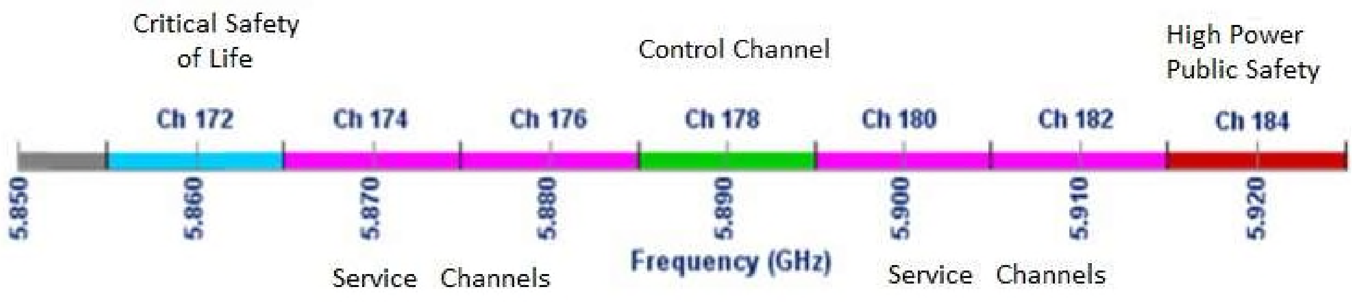
802.11ac ➔ There are 22 channels in Europe:

- Channels numbered 32 to 68 (core frequencies of 5.160 to 5.340 GHz)
- Channels numbered 96 to 140, modulo 4 (core frequencies of 5.480 to 5.700 GHz).
- 6 channels Additional channels are available in the US: 144 channel (5.720 GHz) and 149 to 165 channels (core frequencies of 5.745 to 5.825 GHz).

Each channel has a width of 20 MHz; they are spaced 20 MHz apart, are not overlapped and can be aggregated by group of 2 (802.11n) or groups of 2, 4 or 8 (802.11ac). A Wi-Fi terminal, compatible with 802.11ac, must be able to use 80 MHz and optionally up to 160 MHz bandwidth .

IEEE 802.11p - Physical Layer

Channels splitting



802.11p WAVE frequency spectrum

Channels available for IEEE 802.11p

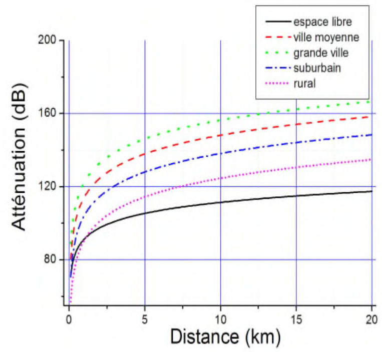
Negotiation for service channels is done on control channel

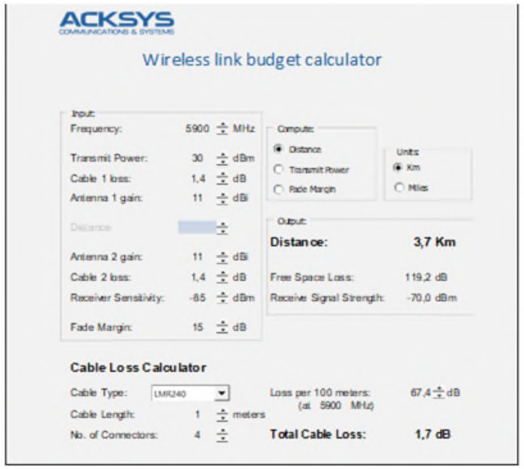
- The device listens to the channel before sending a packet and sends a packet only if the channel is clear.

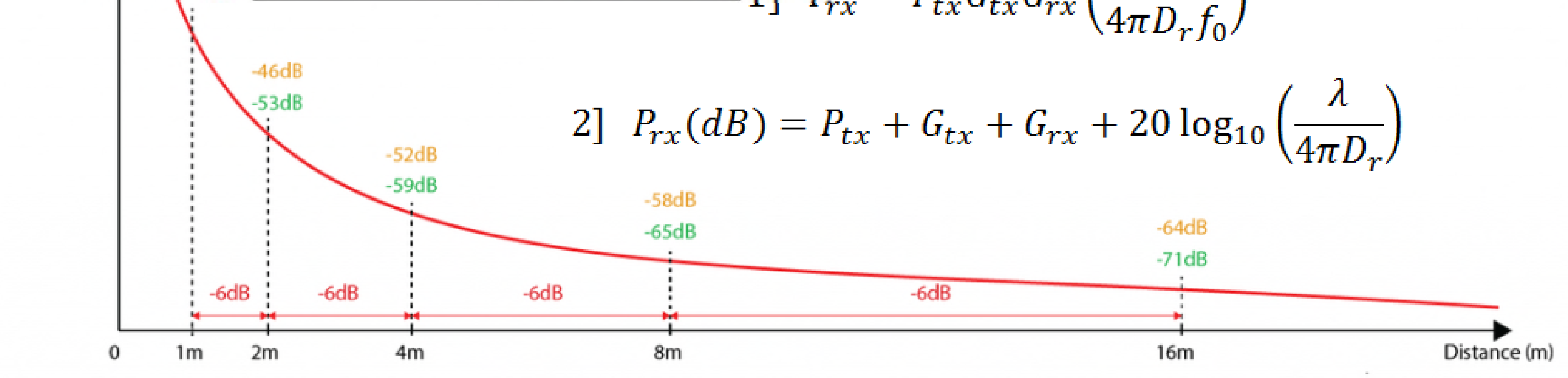
Standard is established…but no standard activities running to enhance performances

Friis formula

Free Space Path Loss







Receive Aperture

Frequency Related:

-40dB in the first meter (2.4GHz)

-47dB in the first meter (5GHz)

Inverse Square Law

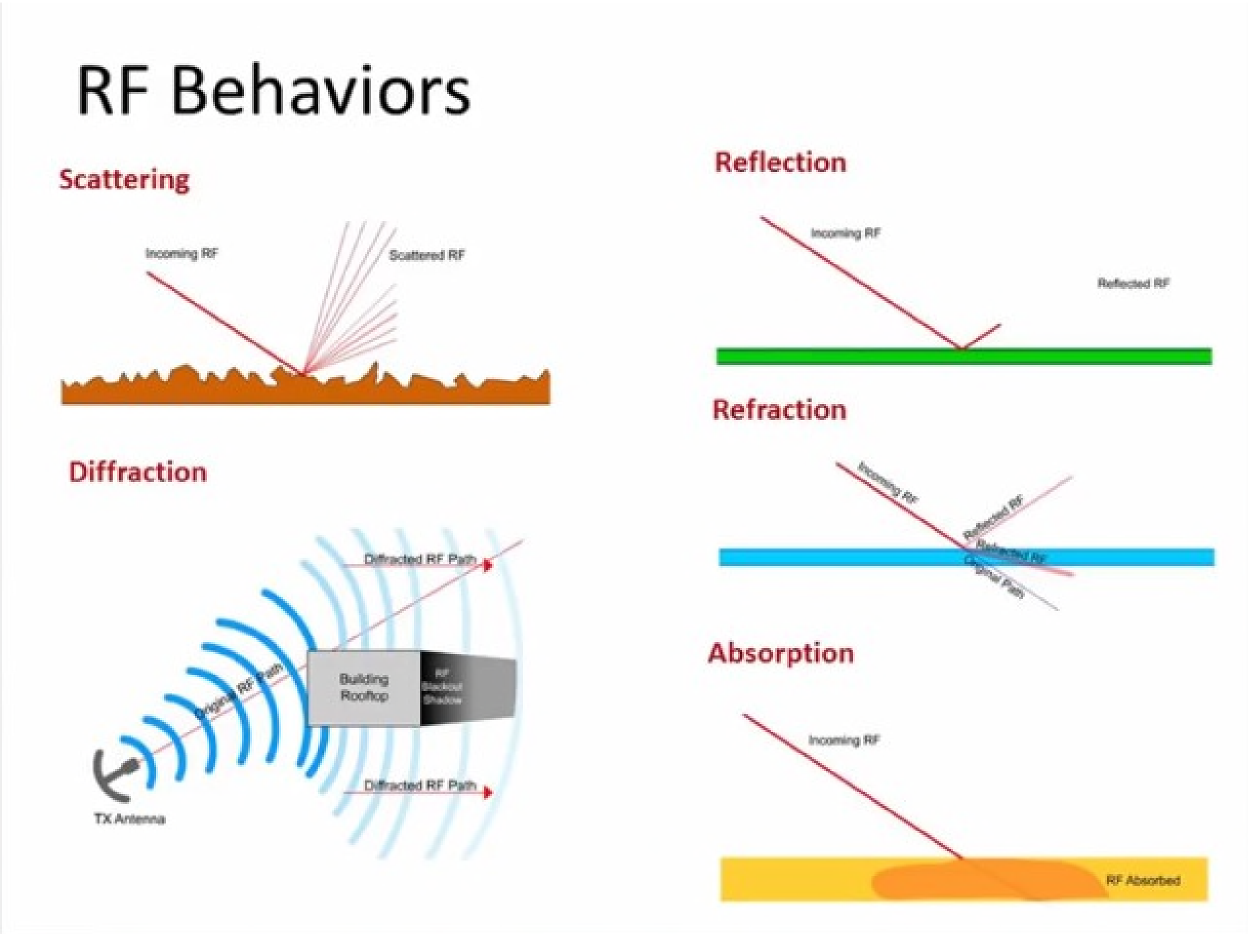
Distance Related: -6dB every time the distance from the source is doubled

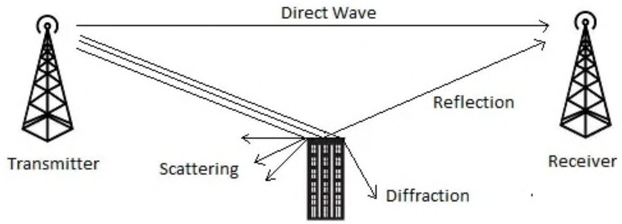
1] $$P_{rx} = P_{tx} G_{tx} G_{rx} \left(\frac{c}{4\pi D_r f_0} \right)^2$$

2] $$P_{rx}(dB) = P_{tx} + G_{tx} + G_{rx} + 20 \log_{10} \left(\frac{\lambda}{4\pi D_r} \right)$$

At 5.9Ghz, first 100m free space loss = 87dBm. Calculator.
And we need to take into account Fading loss (25dBm), vehicle masking effect, wearing,… (>20dBm more).

E.M Waves propagation





Absorption : Capability of some materials to absorb (+/-) energy of RF waves. Ex : Walls, glass, metallic part,… These absorption reduce strength signals.

Reflection : when an E.M wave arrives on a reflective surface and bounces to another direction. this effect can be harmful or helpful (ex: Radio inside a tunnel).

Scattering : Spreading of signal, when it encounters an uneven surface. The effect is a multiple reflected signals, generally harmful for the receiver.

Diffraction : Angular and sharp surfaces modify EM wave into secondary smaller waves.

These effects are cumulative with air losses, interferences or fugitive obstacles

Survey analysis - Motivations

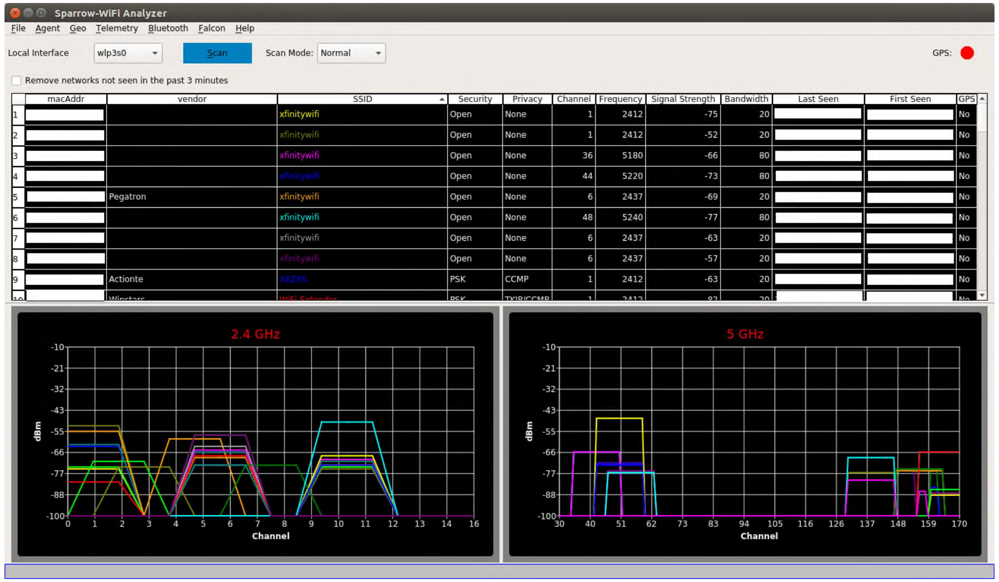
Historically firstly introduced, as 2.4GHz Wifi band is not licensed, many other wireless devices use this these overcrowded band. This situation leads to find new bandwidth and it continue.

The most common devices that create interference and noise in a wireless infrastructure are:

- Microwave ovens, CCTV wireless surveillance video cameras, Wireless baby monitors,
- Bluetooth devices, Some car alarms, Wireless phones, Wireless microphones,
- ZigBee (802.15.4), Wi-Fi jammers.

Many tools are available to discover the Service Set Identifier (SSID) for each access point (AP) and channels used by the AP.
A.P broadcast every ~100 ms : an “I’m here” beacon – Survey tool picks up that beacon and adds the SSID to its list.
Handled tools have also the capability to detect strength field, busy ratio, find “white zone”,…

Spectrum analysis



A bit of practice !

Spectrum analysis – Motivations

Radio Waves spectrum, in principle, is shared !

What could occur ?

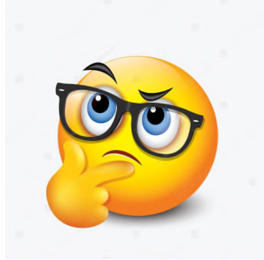
MATÉRIAUX	AFFAIBLISSEMENT		EXEMPLES
	2,4 GHz	5 GHz	
Air	0 dB	0 dB	Espace ouvert intérieur ou extérieur
Porte de bois pleine	3 dB	6 dB	Porte, plancher, cloison
Porte en acier	15 dB	25 dB	Porte Coupe-feu, issue secours
Verre simple (5 mm)	1 dB	2 dB	Fenêtre simple vitrage
Double vitrage athermique	10 dB	18 dB	Fenêtre haute performance thermique
Cloison sèche (plaque plâtre)	3 dB	4 dB	Cloisons internes
Briques pleine, Béton (150 mm)	8 dB	15 dB	Murs porteurs

Troubles :
- Interferences,
- Congestion,
- Lack of performances

- Functional problems
  - Wifi credential and/or connection,
  - Resources access.

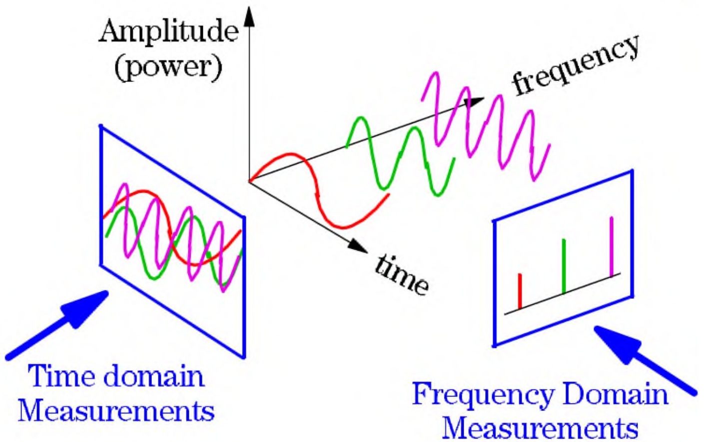
To solve problem, it’s fundamental to master Wifi radio/protocol mechanism and…have dedicated tools

Spectrum analysis – What is that ?



Wikipedia : A **spectrum analyzer** measures the magnitude of an input signal versus frequency within the full frequency range of the instrument. The primary use is to measure the power of the spectrum of known and unknown signals. The input signal that most common spectrum analyzers measure is electrical; however, spectral compositions of other signals, such as acoustic pressure waves and optical light waves, can be considered through the use of an appropriate transducer.

The most common spectrum analyzer measurements are : modulation, distortion, and noise.



Spectrum Analysis Basics
CMB 12/96

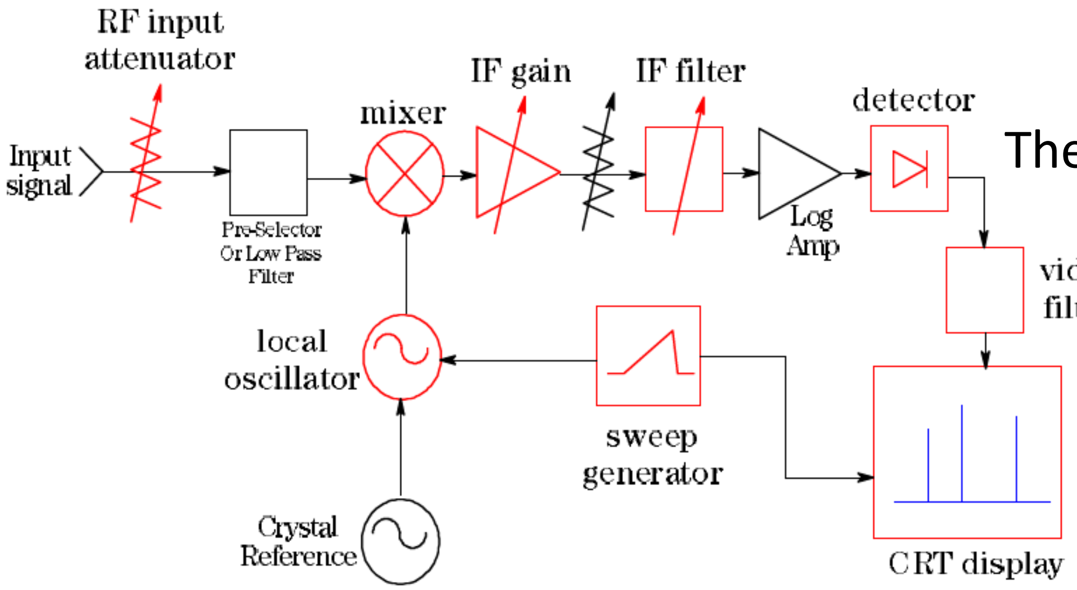
$$s(t) = \frac{a0}{2} + \sum_{i=1}^{n} an \sin \omega t + bn \cos \omega t$$

Electrical signal Time domain observation : We use an oscilloscope to see how the signal varies with time.

Frequency-domain allow to deeply analyze characteristics of a signal and performances of device/system.

Spectrum analyzer, much more complex to use compare with scope, are capable to demodulate signals, inject carrier, digital filtering and computations,…
It’s the essential tool of RF analysis

Spectrum analysis – Inside



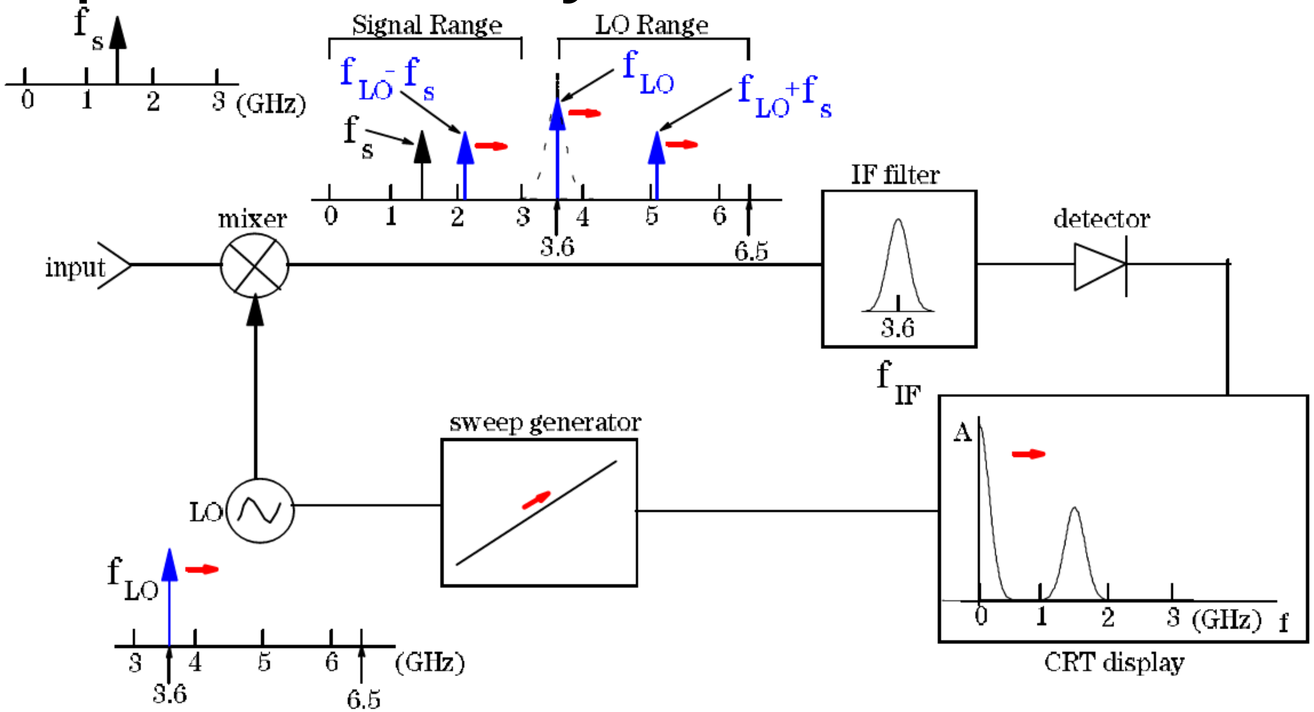
The major components in a spectrum analyzer are :

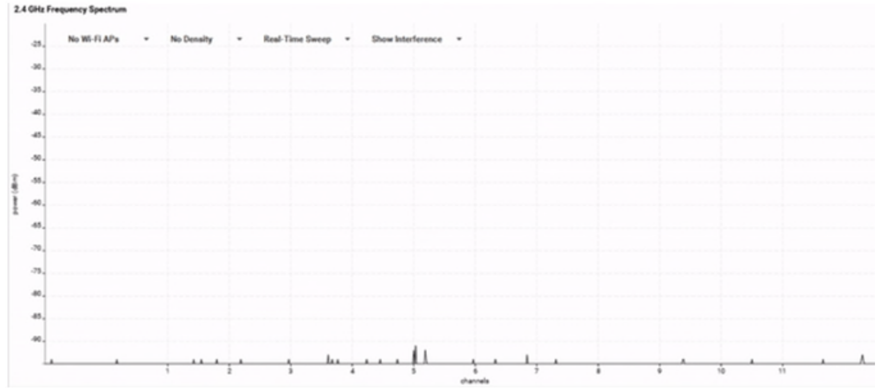
- RF input attenuator, mixer, IF (Intermediate Frequency) gain,
- IF filter, detector, video filter, local oscillator, sweep generator, and CRT display.

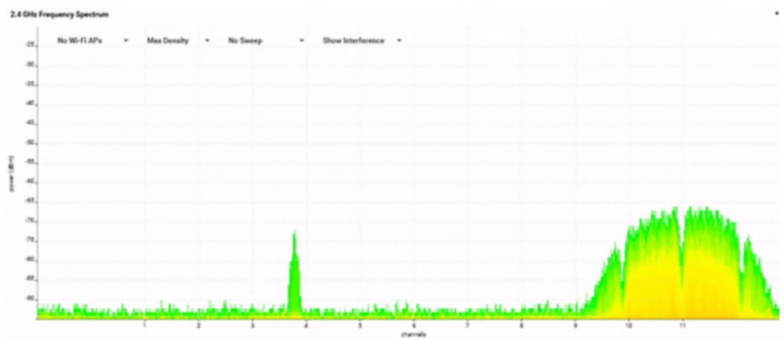
A mixer is a device that converts a signal from one frequency to another. Therefore, it is sometimes called a frequency-translation device.

The IF filter is a bandpass filter which is used as the "window" for detecting signals. Its bandwidth is also called the resolution bandwidth (RBW) of the analyzer and can be changed via the front panel of the analyzer.

Spectrum analysis – Inside



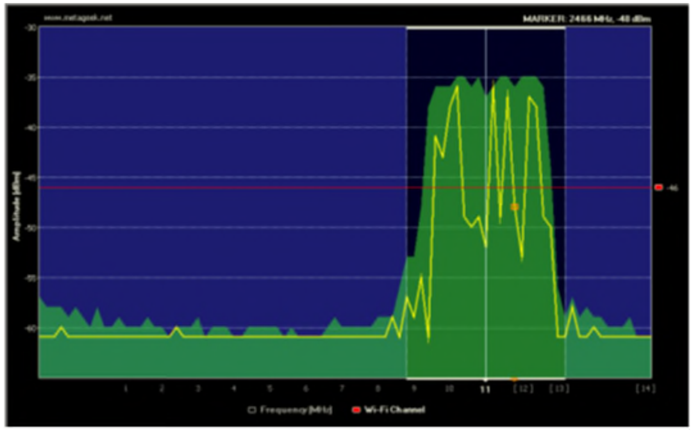




1. Input signal is firstly connected to RF attenuator and Low pass filter (if required),
2. This signal is then combined with the local Oscillator (LO) through the mixer, to convert (or translate) it to an intermediate frequency (IF).
3. IF is sent to the IF filter, then output of this filter is detected, indicating the presence of a signal component at the analyzer's tuned frequency.
4. Output voltage of the detector is used to drive the vertical axis (amplitude) of the analyzer display.
5. Sweep generator provides synchronization between the horizontal axis of the display (frequency) and tuning of the LO. The resulting display shows amplitude versus frequency of spectral components of each incoming signal.

Sweep Cycle – reading the energy across frequencies over a period of time. Faster sweep times make finding interferers easier and allow you to better visualize modulations. Focusing on a channel makes finding interference sources faster by limiting the amount of frequency space being inspected.

Spectrum analyzer – Basic Setup



- Frequency Center: Frequency setting in the middle of the x-axis of the screen reticle, in Hz, kHz, MHz or GHz.
  Frequency Start / Stop: Frequency adjustment at the beginning to end of the screen reticle abscissa axis. Both frequencies automatically define the portion of tape displayed on the screen and thus the frequency scan range of the spectrum.
- Span: Spread of the frequency scan of the analyzer, that is the portion of the frequency band displayed on the screen between the start and end, in Hz, kHz, MHz, or GHz for the ten horizontal divisions.
- Amplitude Reference Level: this is the adjustment of the amplitude level displayed at the top of the reticle in dBm, dBµV, dBmV, V or W. This amplitude therefore represents a power or a voltage.

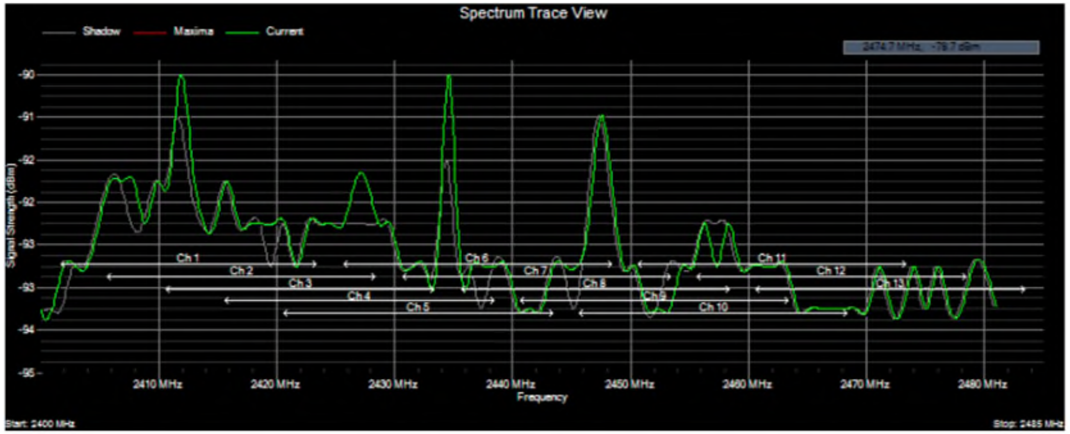
The resolution bandwidth filter or **RBW** filter is the bandpass filter in the IF path. It's the bandwidth of the RF chain before the detector (power measurement device). It determines the RF noise floor and how close two signals can be and still be resolved by the analyzer into two separate peaks. Adjusting the bandwidth of this filter allows for the discrimination of signals with closely spaced frequency components, while also changing the measured noise floor. Decreasing the bandwidth of an RBW filter decreases the measured noise floor and vice versa. This is due to higher RBW filters passing more frequency components through to the envelope detector than lower bandwidth RBW filters, therefore a higher RBW causes a higher measured noise floor.

Video bandwidth : The video bandwidth filter or VBW filter is the low-pass filter directly after the envelope detector. It's the bandwidth of the signal chain after the detector. Averaging or peak detection then refers to how the digital storage portion of the device records samples—it takes several samples per time step and stores only one sample, either the average of the samples or the highest one. The video bandwidth determines the capability to discriminate between two different power levels. This is because a narrower VBW will remove noise in the detector output. This filter is used to "smooth" the display by removing noise from the envelope. Similar to the RBW, the VBW affects the sweep time of the display if the VBW is less than the RBW. If VBW is less than RBW, this relation for sweep time is useful:

Detector : Used to adequately map the correct signal power to the appropriate frequency point on the display. There are in general three types of detectors :

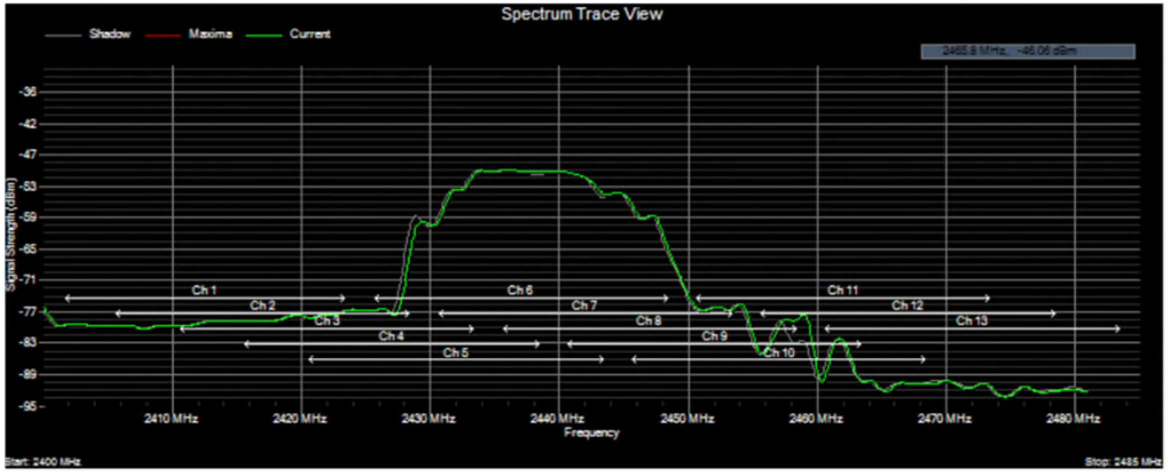
- ✓ Sample, peak, and average

Wifi Spectrum

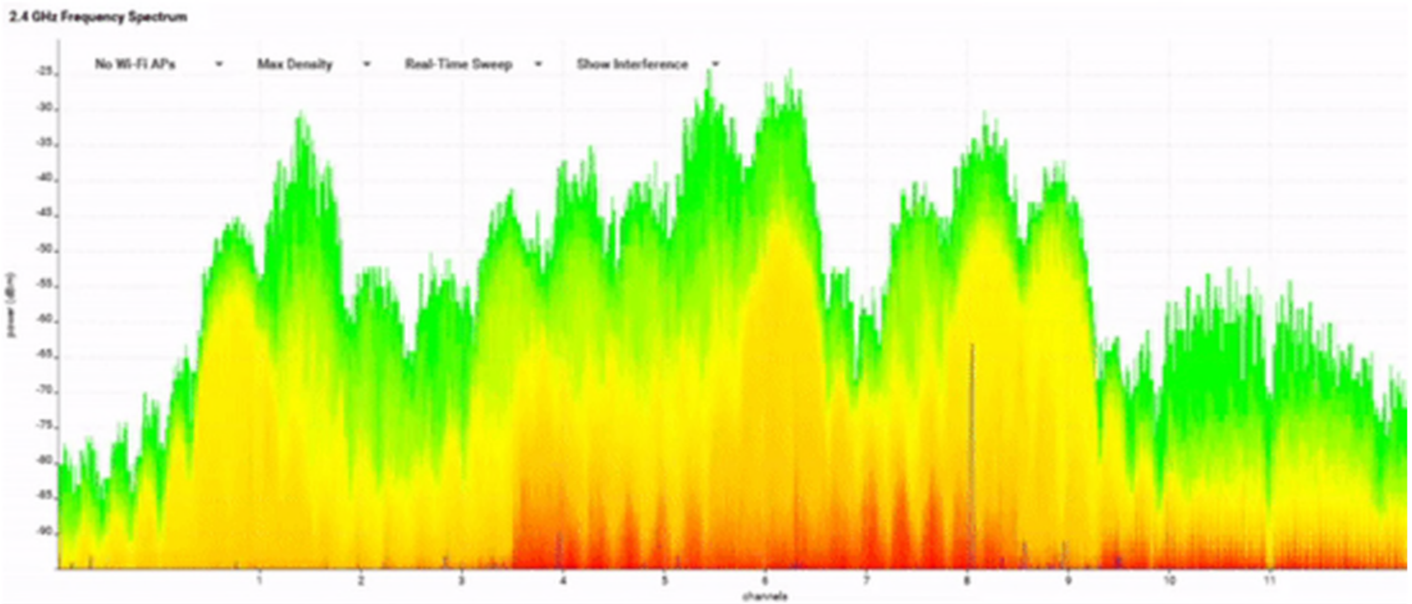


In this capture, Wifi band is relatively quiet and there are no wireless devices transmitting in the 2.4 GHz band.
As maximum strength value of the signal is bellow -90 dBm (weak level, closed to current receiver limit).
Note that analyzer has the capability to automatically modify X scaling to zoom signal and improve readability.

Highlight pattern of communication from a wireless network (WiFi channel 6 in this exemple) as it is actively transmitting a large stream of data.



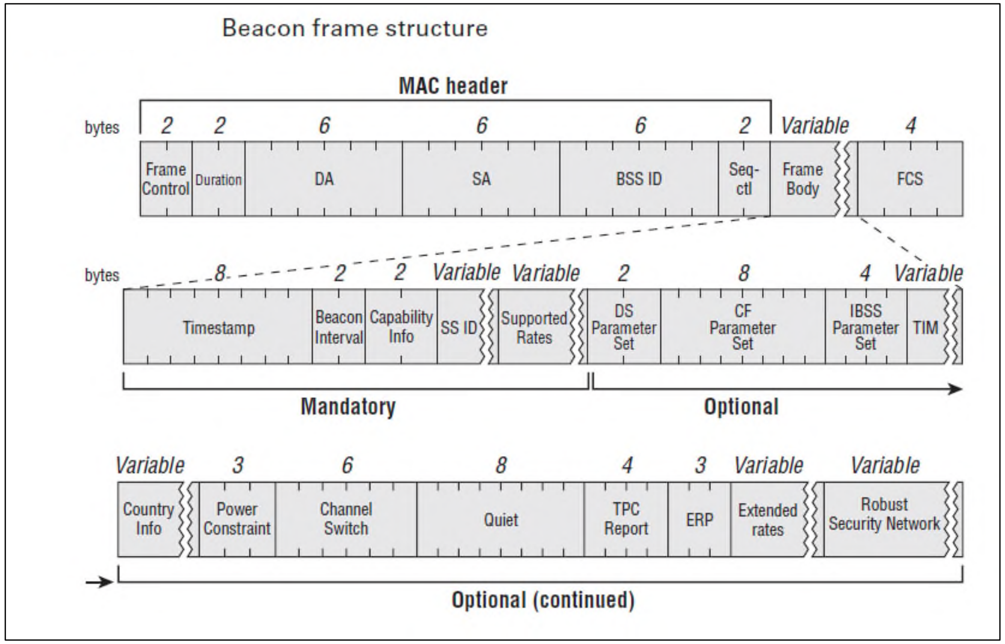
Wifi Spectrum



Channel	Radios	Interference	Channel Utilization	Noise (Adapter)
1	0	0	21%	N/A
2	0	0	40%	N/A
3	0	0	50%	N/A
4	0	0	52%	N/A
5	0	0	55%	N/A
6	0	0	48%	N/A
7	0	0	52%	N/A
8	0	4	52%	N/A
9	0	4	40%	N/A
10	0	4	32%	N/A
11	5	4	16%	-79 dBm

In this capture, spectrum analyzer overlays the max levels, real time levels and recurrence of those. The table above allows you to identify on which wifi channels are the exchanges.

Wifi Beacon

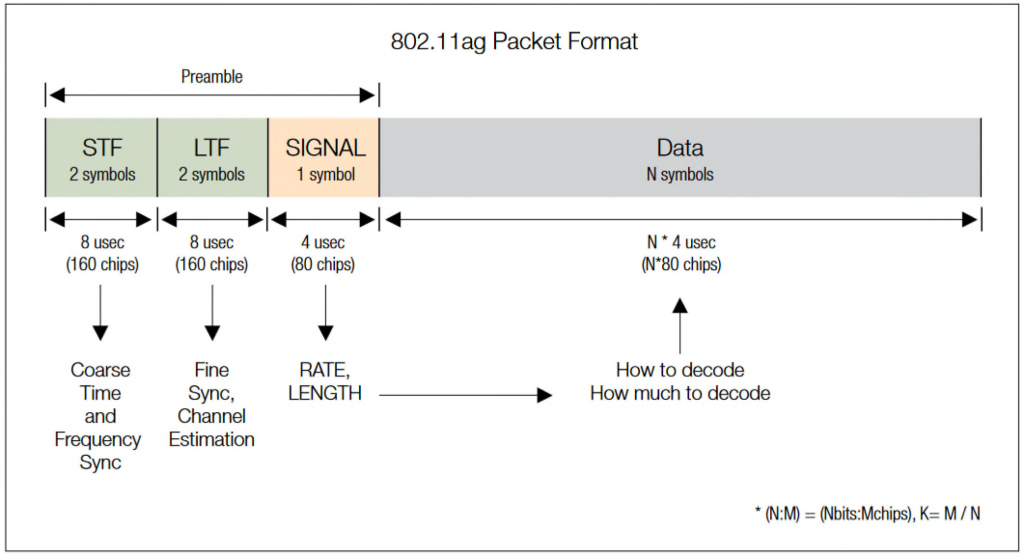


In the frame body slots there are few mandatory fields & few optional fields. Mandatory fields in a Beacon frame :

1. Timestamp (8 byte)
2. Beacon Interval (2 byte)
3. Capability info (2 byte)
4. SSID (variable size)
5. Supported Rates (variable size)

The access point broadcasts at a regular time interval (~100 ms) a Beacon frame. This frame can be considered as a “I’m here” signal for stations wishing to connect. It contains the different information that the client must know to initiate an association, for example: channel used, rate, security information, access point load, network name (SSID).

Wifi Packet



	802.11a/g Packet Format (refer to figure)
Preamble	**STF**: Short Training Field (2 symbols) - Uses on 1/4 of subcarriers. Repeats every 16 chips. - Initial timing sync and frequency estimate. **LTF**: Long Training Field (2 symbols) - Uses all 52 subcarriers (same as Data symbols). - Fine timing and frequency sync, and channel response estimation. **SIGNAL**: (1 symbol) - Encoded similar to a Data symbol, but always uses BPSK modulation. 24 bits of configuration data. - Fields: - RATE (4 bits): Indicates Data FEC coding and modulation (8 combinations), aka "MCS" - LENGTH (12 bits): Number of octets (bytes) carried in Payload - PARITY (1 bit): Even parity-check on RATE+LENGTH data - TAIL (7 bits): Used for SIGNAL symbol FEC decoding
Data	52 subcarriers, 48 Data + 4 Pilot Data subcarriers use BPSK, QPSK, 16QAM or 64QAM modulation. Same in all symbols Pilots subcarriers (BPSK only) are used to track frequency/phase and amplitude variations over the burst