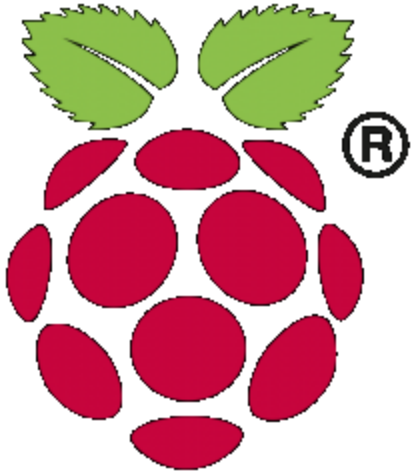
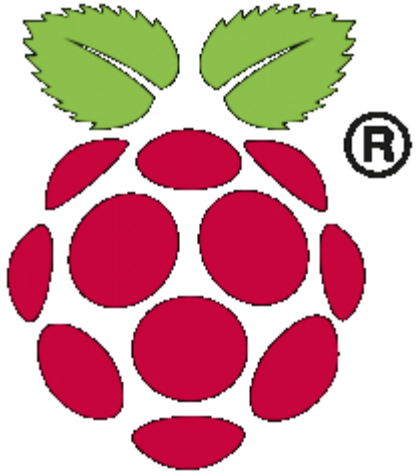
NetSIG: 802.11 MIMO and RF Technology Primer



Electromagnetics and Pushing Packets with Magic

Thursday, May 28, 2020

Michael Hansen

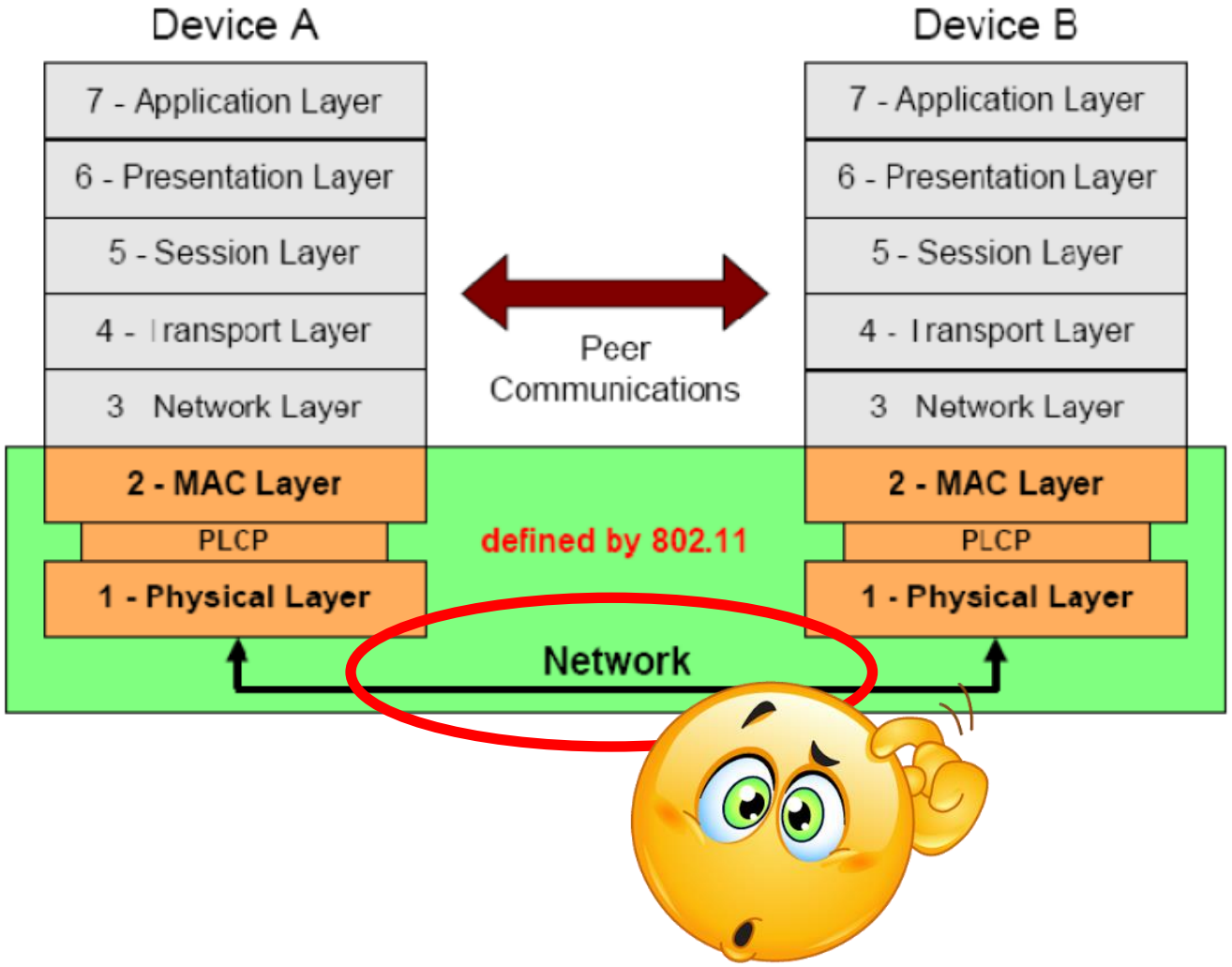


Presentation Overview

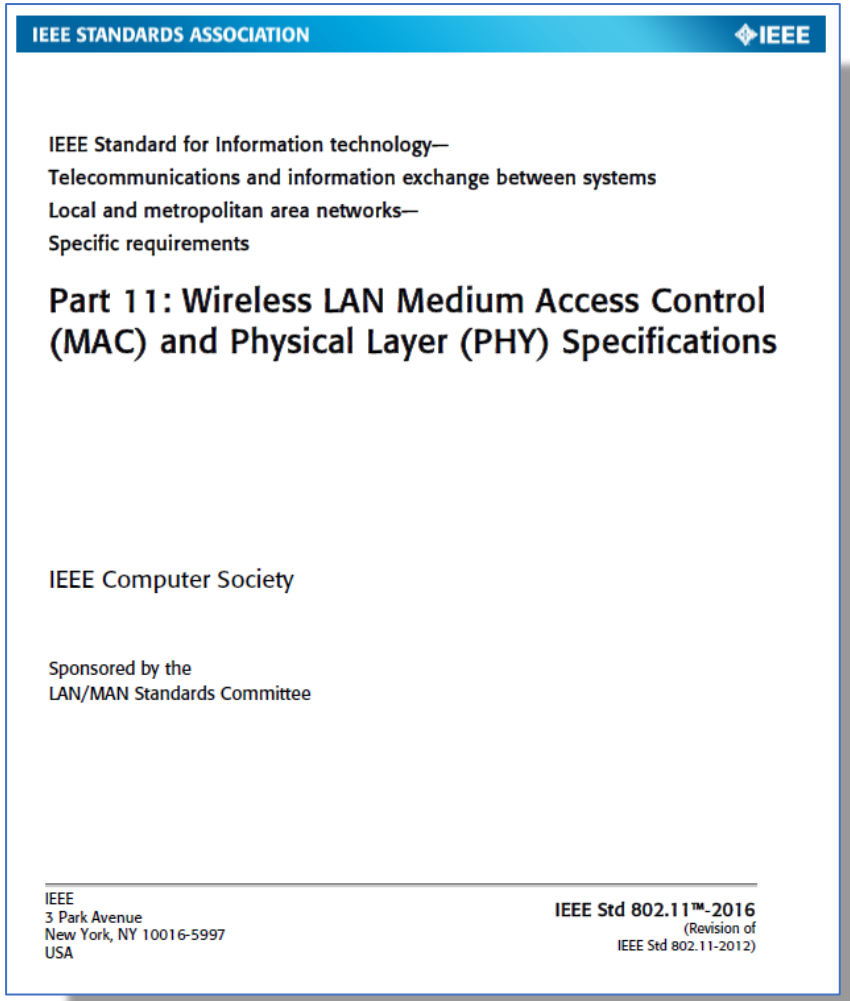
- Introduction with 802.11
- Electromagnetics without Math but not without History
- Signals, Noise and more Signals
- RF propagation – if you could see it.
- Information Theory and Capacities
- MIMO – Rise of the Antenna Engineer!
- Spooky action at a distance with CSI.

IEEE 802.11 Position in the ISO OSI Layers

- We think of 802.11 as just a wireless adapter allowing mobile connection of our phones, laptops, tablets.
- BUT what of this under stated word “Network”
- You might as well just say “Magic Goes Here”



The Respectful way to Draw the 802.11 Layers


IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for Information technology—
Telecommunications and information exchange between systems
Local and metropolitan area networks—
Specific requirements

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

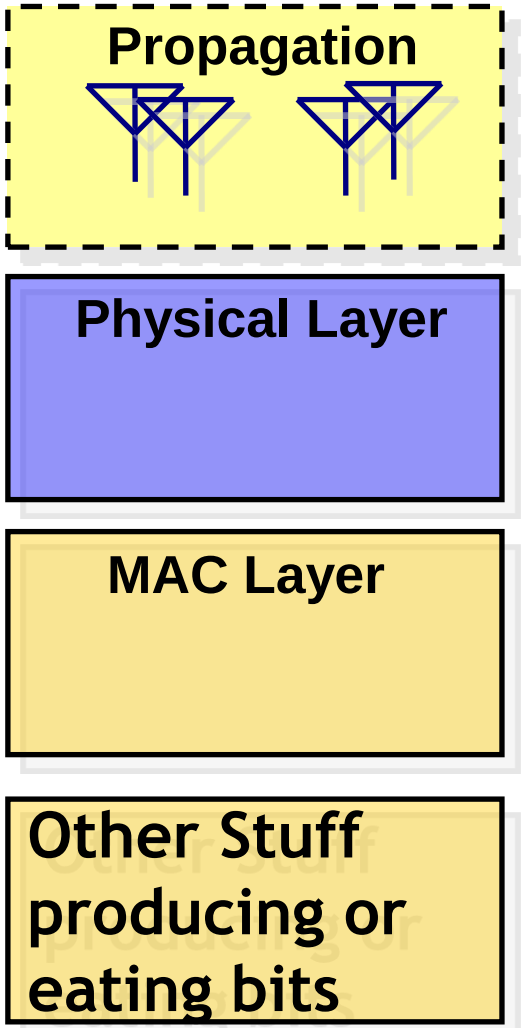
IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

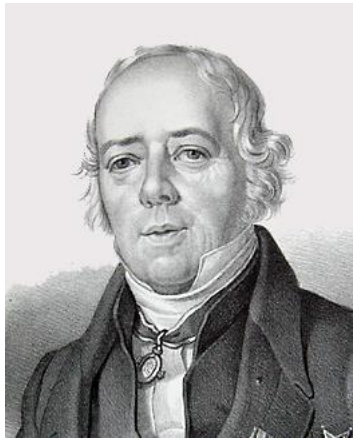
IEEE Std 802.11™-2016
(Revision of
IEEE Std 802.11-2012)

- From its start in 1999 the IEEE has been defining faster rates in the 802.11 wireless LAN standard. But something in addition to fast changed with the introduction of 802.11n in 2009.



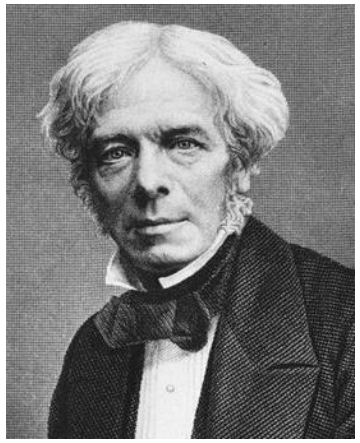
The Academic History of Electromagnetics

Oersted
1777-1851



1820
Discovery of Electromagnetism

Faraday
1791-1867

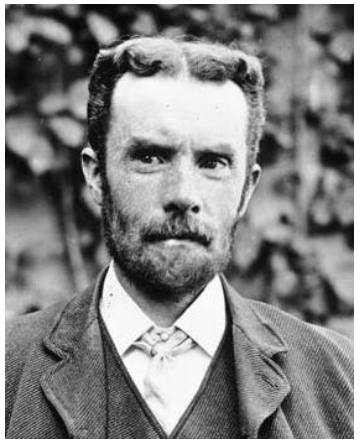


1831
Discovery of Electromagnetic induction

Maxwell
1831-1879

1864
A Dynamical Theory of the Electromagnetic Field

Heaviside
1850-1925



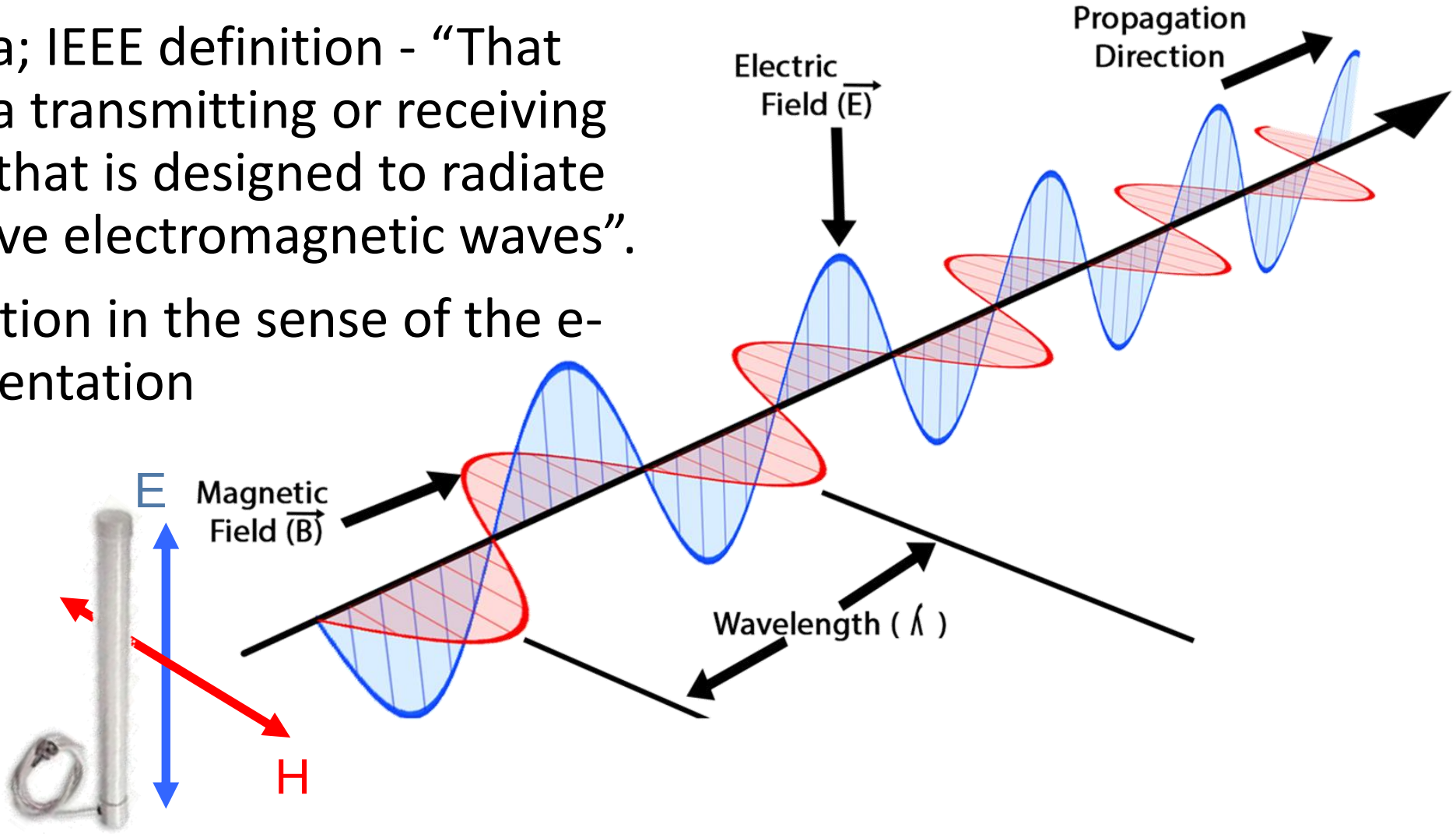
1884
Reduction of Maxell Equations to modern form

Hertz
1857-1894

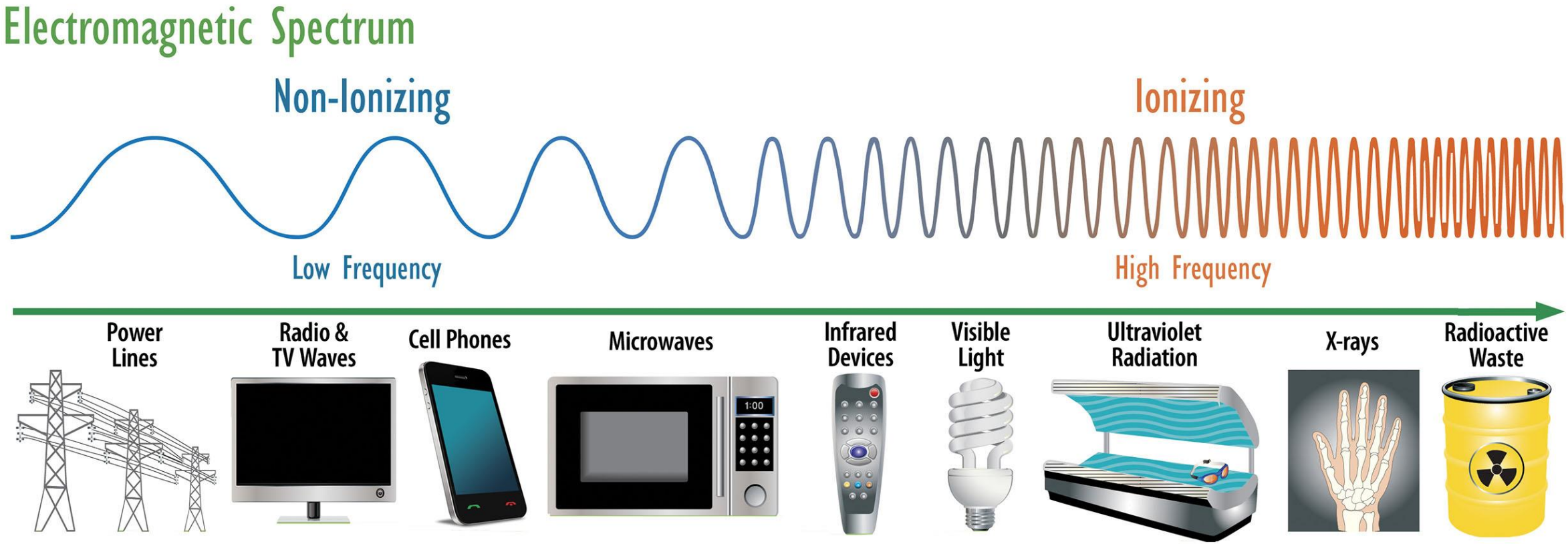
1887
Electromagnetic Waves confirmed experimentally

Electromagnetic Waves and Propagation

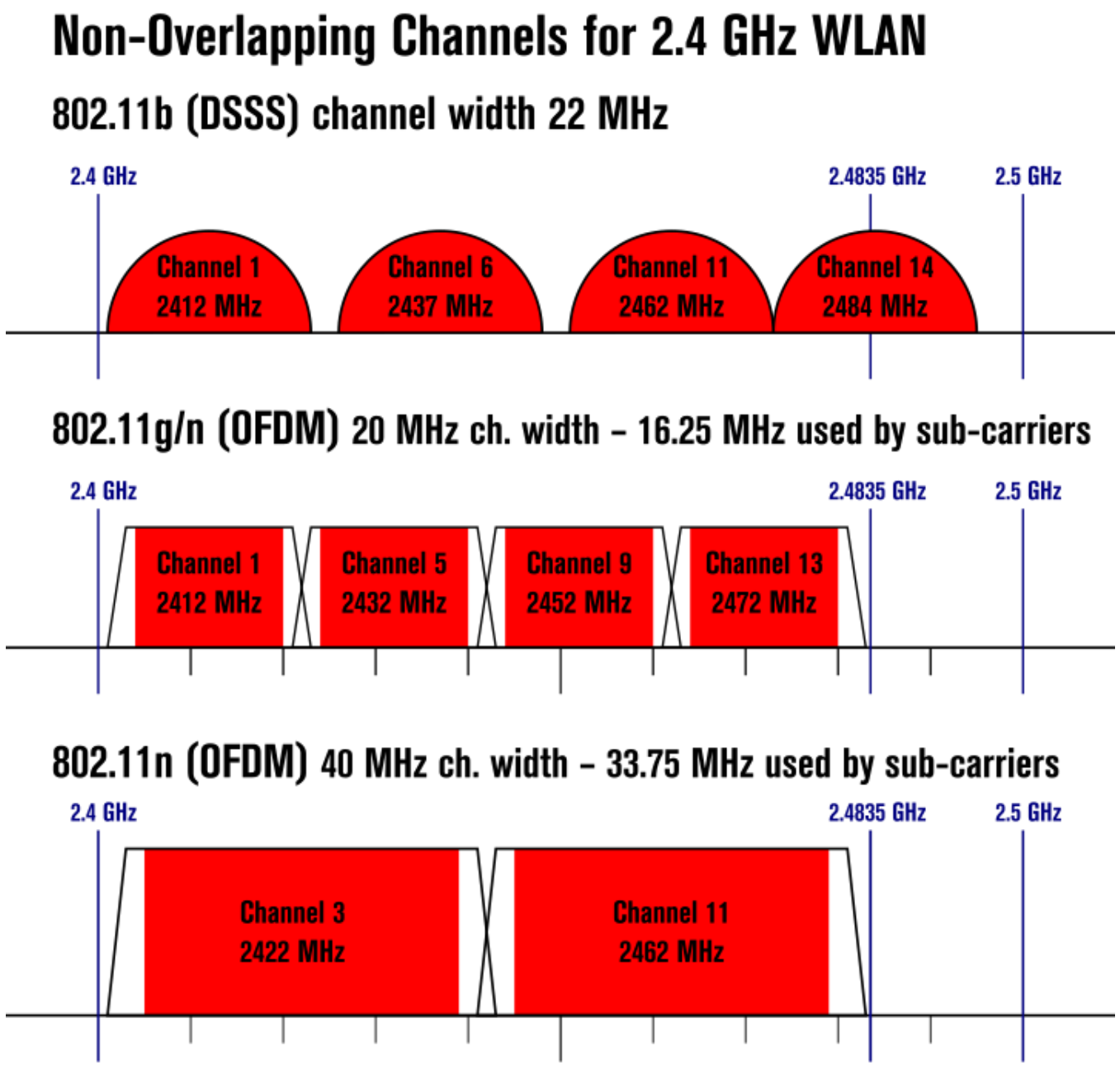
- Antenna; IEEE definition - “That part of a transmitting or receiving system that is designed to radiate or receive electromagnetic waves”.
- Polarization in the sense of the e-field orientation



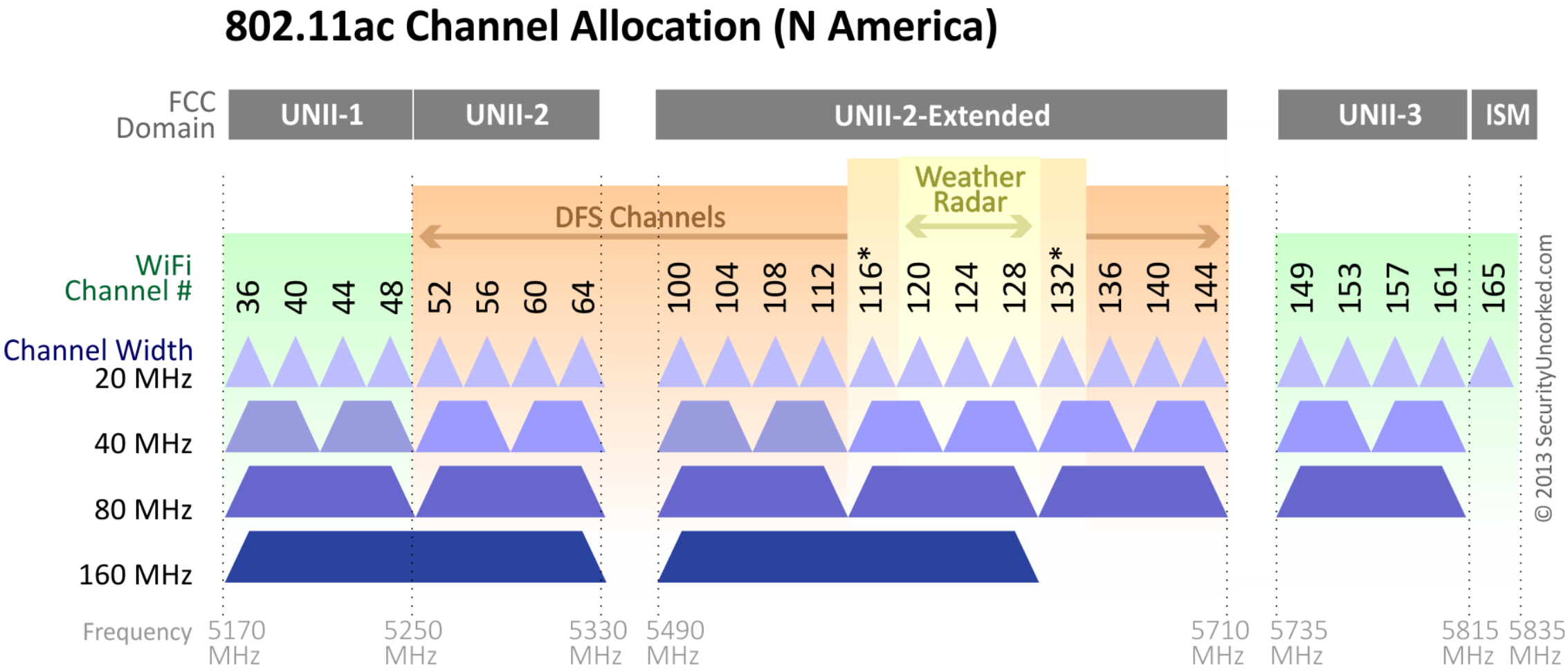
Electromagnetic Spectrum from DC well past Daylight.



- IEEE 802.11 b/g/n all use 2.4 GHz Spectrum.
- Channels are 5 MHz apart BUT Channels are in fact 22 MHz wide.
- Only 3 non-overlapping channels



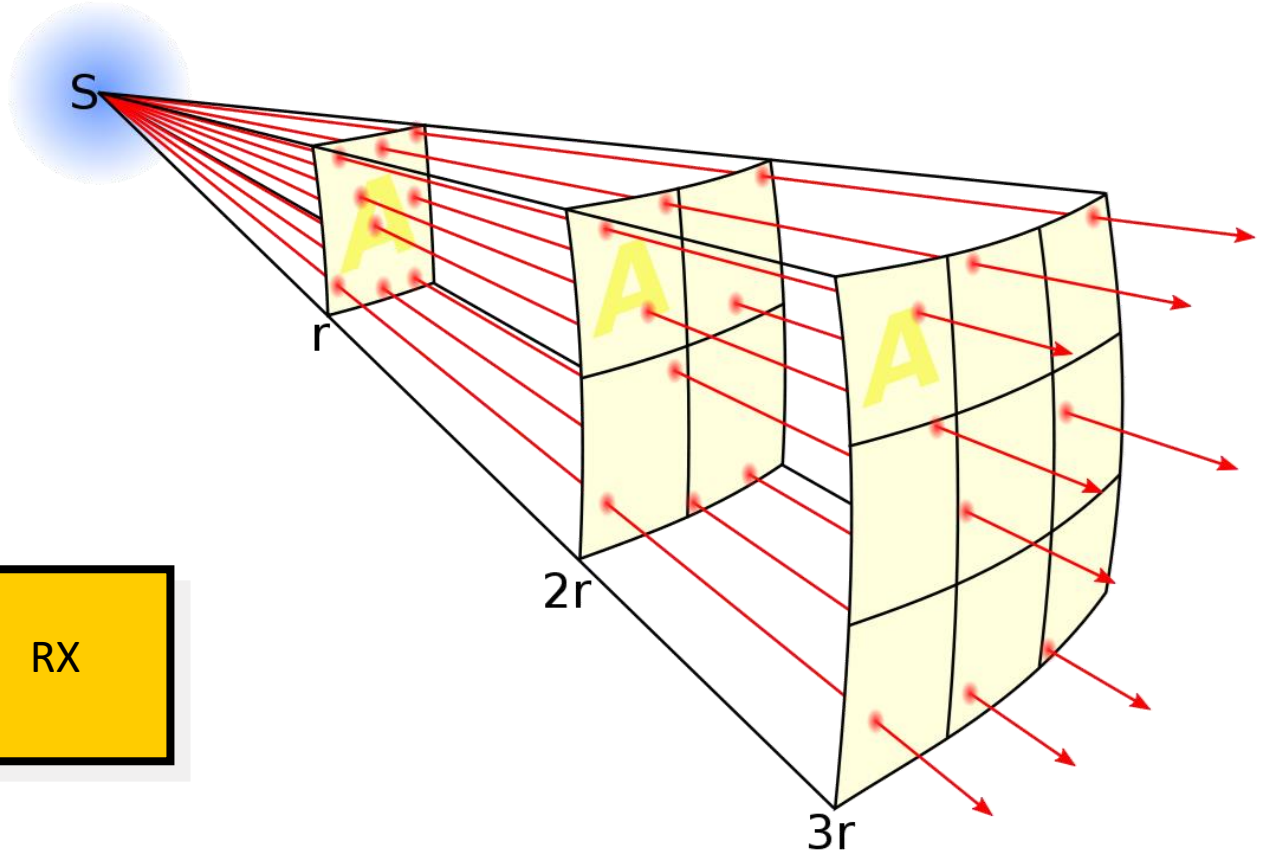
5 GHz Channels



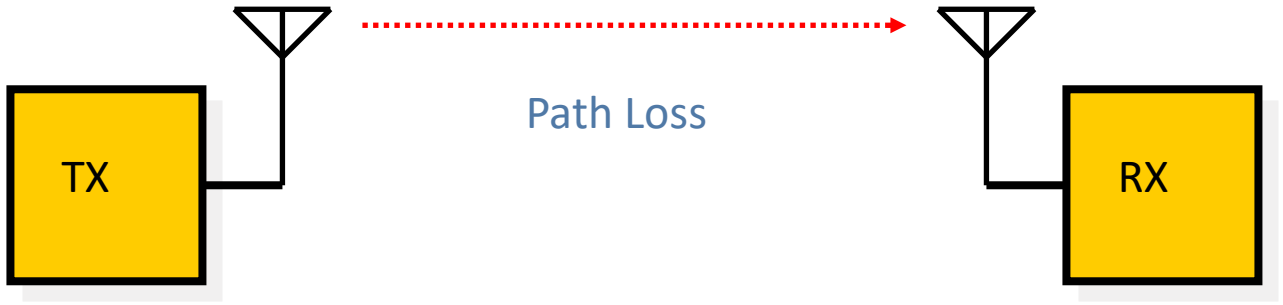
*Channels 116 and 132 are Doppler Radar channels that may be used in some cases.

Path Loss From Distance and Wavelength

- As the Energy radiates from antenna it drops as a power of r squared.



Path Loss = $20\log(4\pi/\lambda) + 20\log(r)$



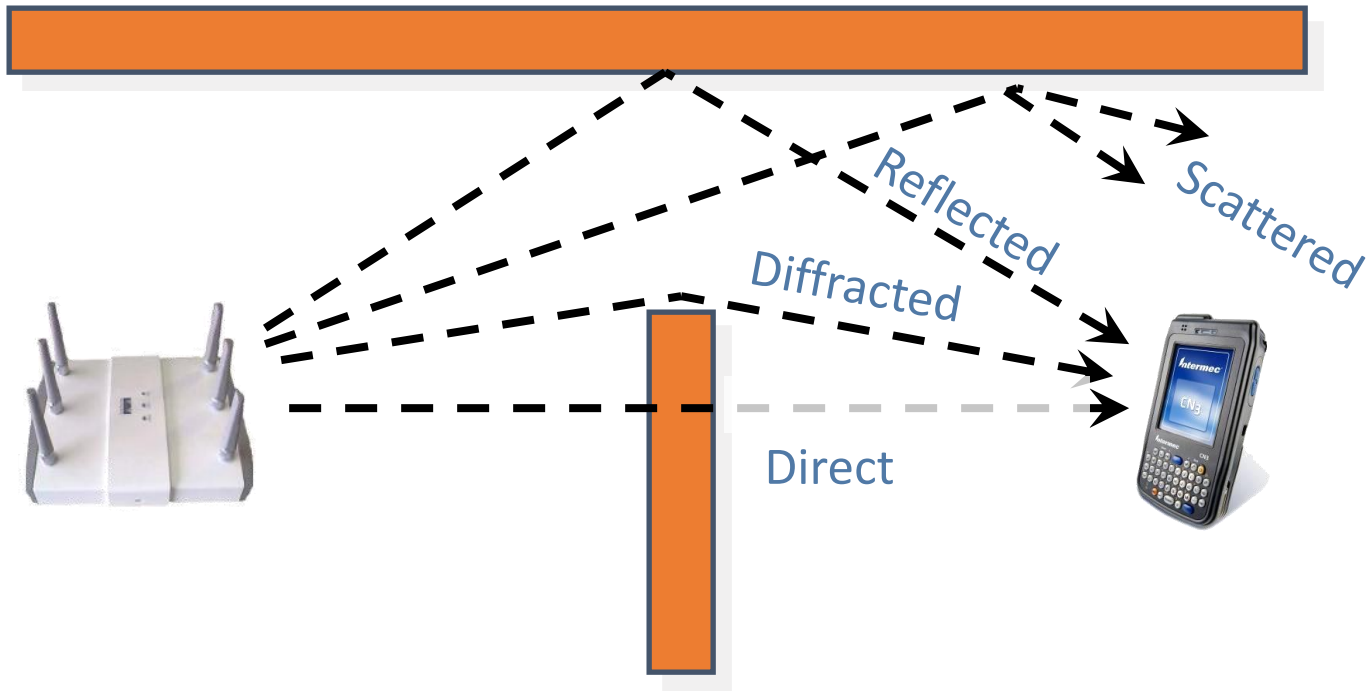
Notice the dependence on wavelength

For 5 GHz the Frequency dependent loss is ~ 47 dB

For 2.4 GHz the Frequency dependent loss is ~ 40 dB

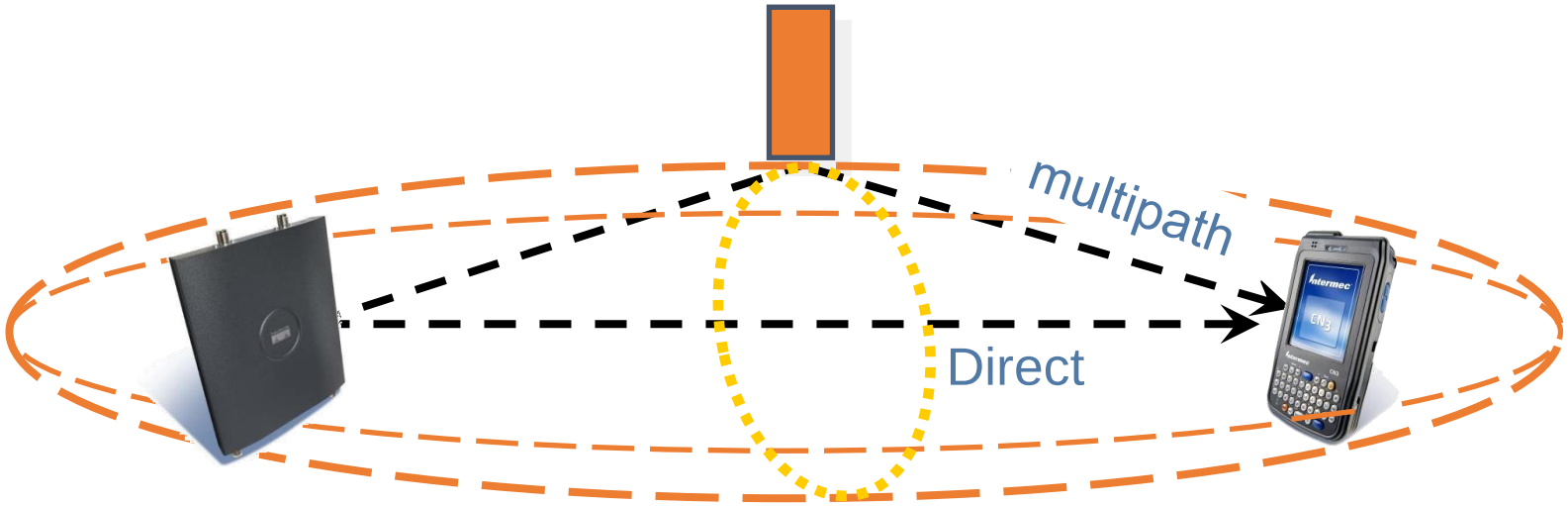
Propagation Modes

- The signal can propagate via multiple modes
- Direct may be obstructed or non-obstructed



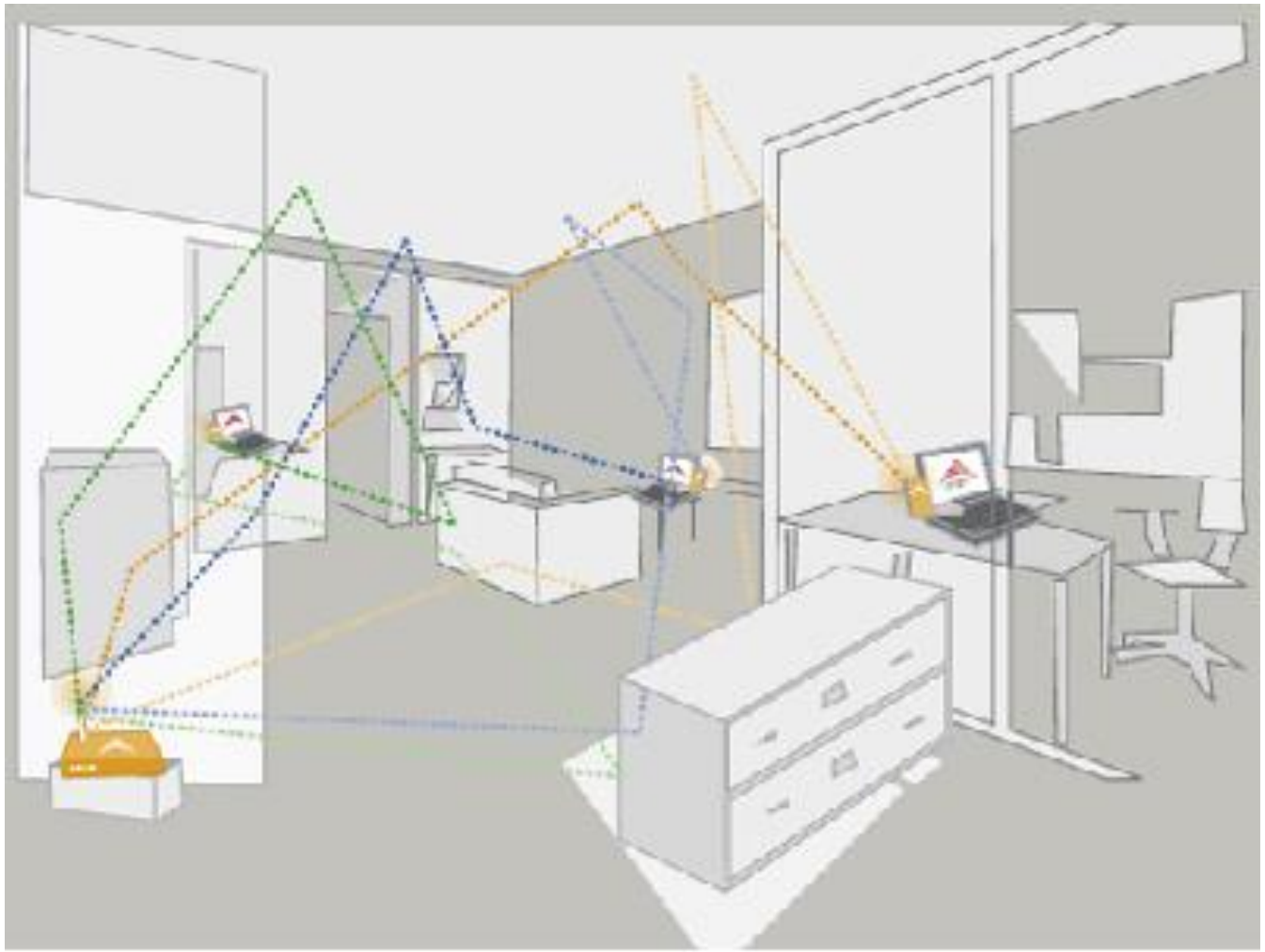
Multipath - Fresnel Zones - RF Line of Site

- **RF line of site means no visual obstruction between router and laptop**
- **A path is only line of site if the First Fresnel Zone is not obscured - rule of thumb by at least 60%**
- **Fresnel Zones are elliptical (from side view) chords 1/2 wavelength longer than the direct path**
- **Signals destructively add at the receiver antenna giving a 'Fade'**



Multipath Propagation Indoors

- Consider we have all modes of propagation in indoor settings giving rise to constructive and destructive interference ALL over the place.
- Signals can drop at least 20 to 30 dB in a Fade..

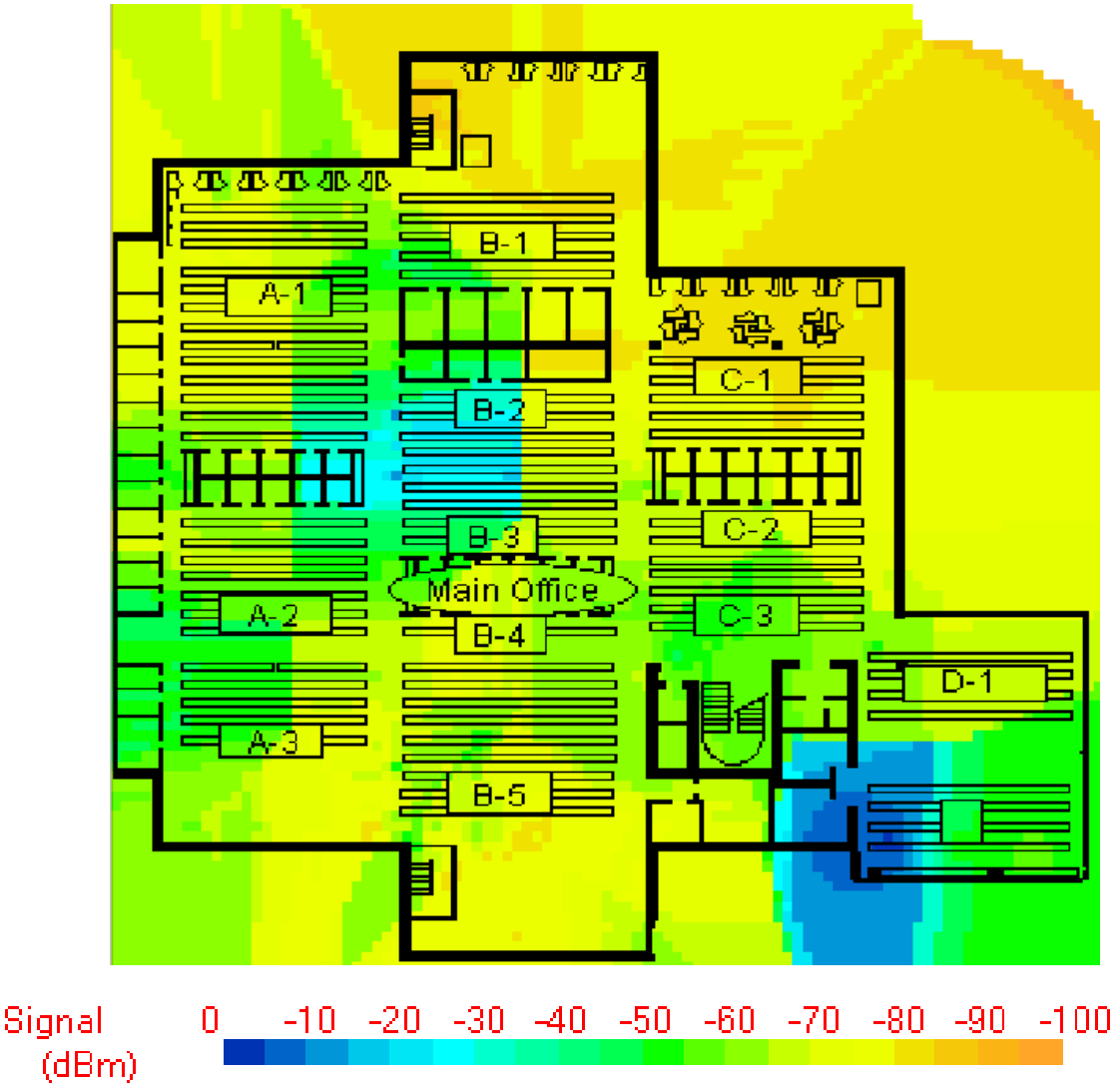


Signal Levels and Noise

- Decibals, Power levels, mW and dBm
- dB is a logarithmic ratio of values (voltages, power, gain, losses)
- Working in dB you to “add” or “subtract” gains, losses, ratios..
- dBm dB(1 mW) — power measurement relative to 1 milliwatt.
- 0 dBm →1 mW,
- 10 dBm →10 mW,
- 20 dBm → 100mW
- -90dBm → 0.0000000001 mW

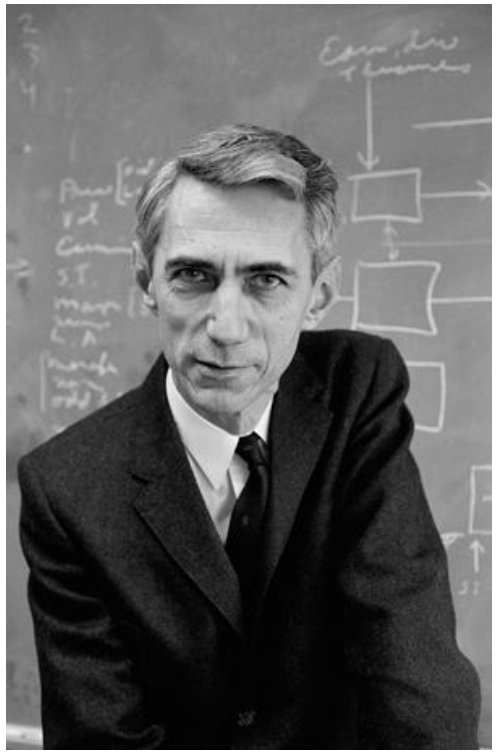
Old School Site Survey Map

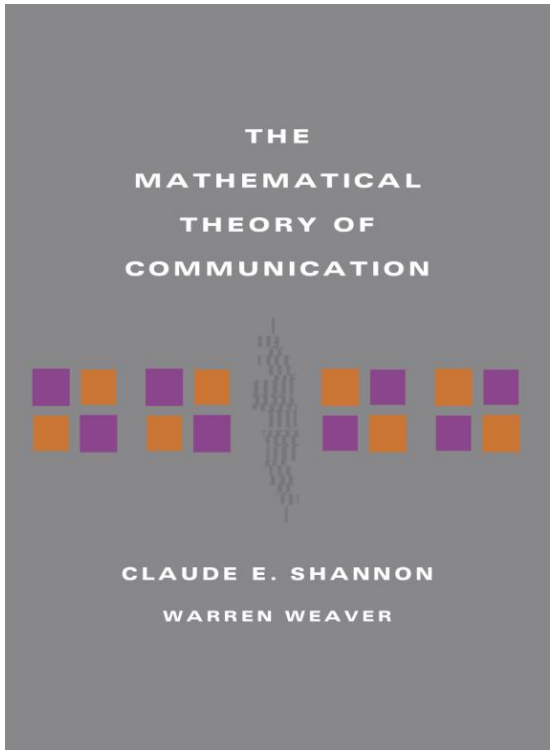
- In the site survey plot the signal levels can range from -10 dBm to -90 dBm.
- In linear this is from 0.1 milliWatt to 0.000000001 milliWatt
- Awkward to deal with in a linear scale.
- Hence dB scales



Information Theory – the beginning of the Bit

- “A Mathematical Theory of Communication,” published in 1948, Claude Shannon presented a unifying theory for the transmission of information that could be applied to telephones, radio, television, or any other system.
- John W. Tukey, in a Bell Labs memo on 9 January 1947 contracted "binary information digit" to simply ***"bit"***





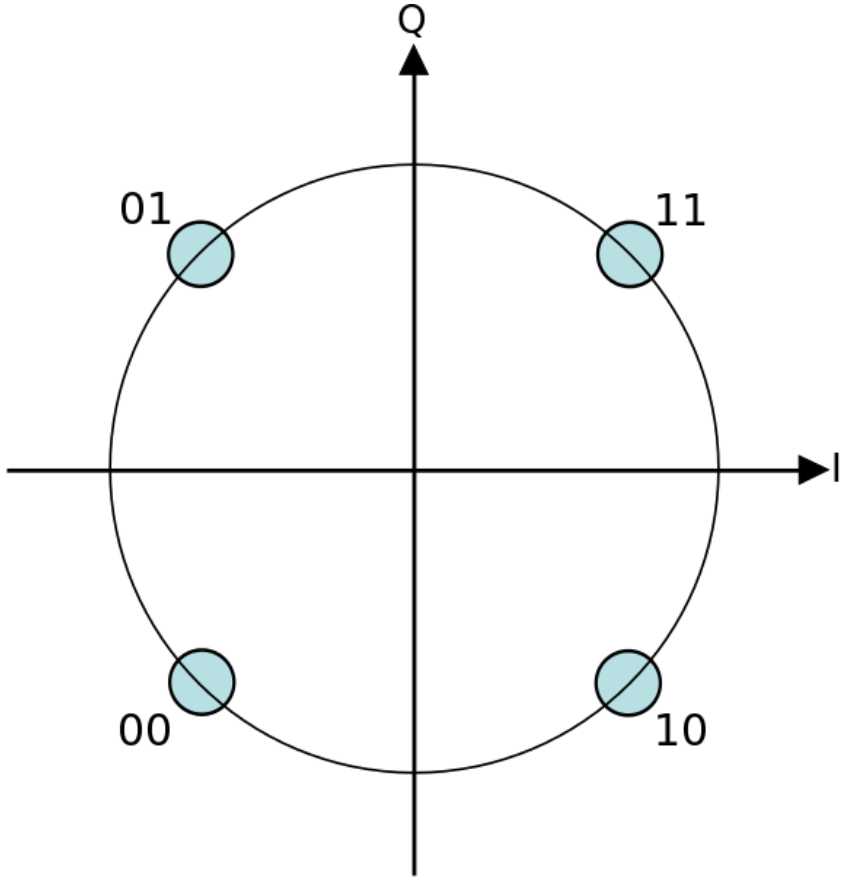
802.11 The Legacy…

- 802.11 – basic 1 and 2Mbps 2.4GHz WLAN (1997)
- 802.11b – 11Mbps 2.4GHz WLAN (1999)

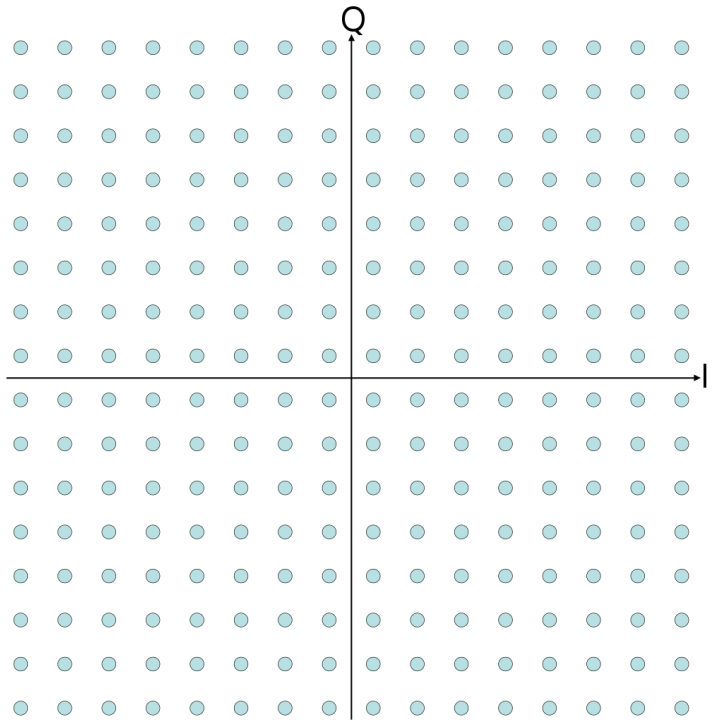
- 802.11a – 54Mbps 5.15GHz OFDM WLAN (1999)
- 802.11g – 54Mbps 2.4GHz WLAN (2003)
- 802.11n – 100Mbps Throughput 2.4 and 5.15GHz WLAN (2009)

Comparing 802.11 QPSK and 256 QAM

- QPSK – 2 bits/Symbol

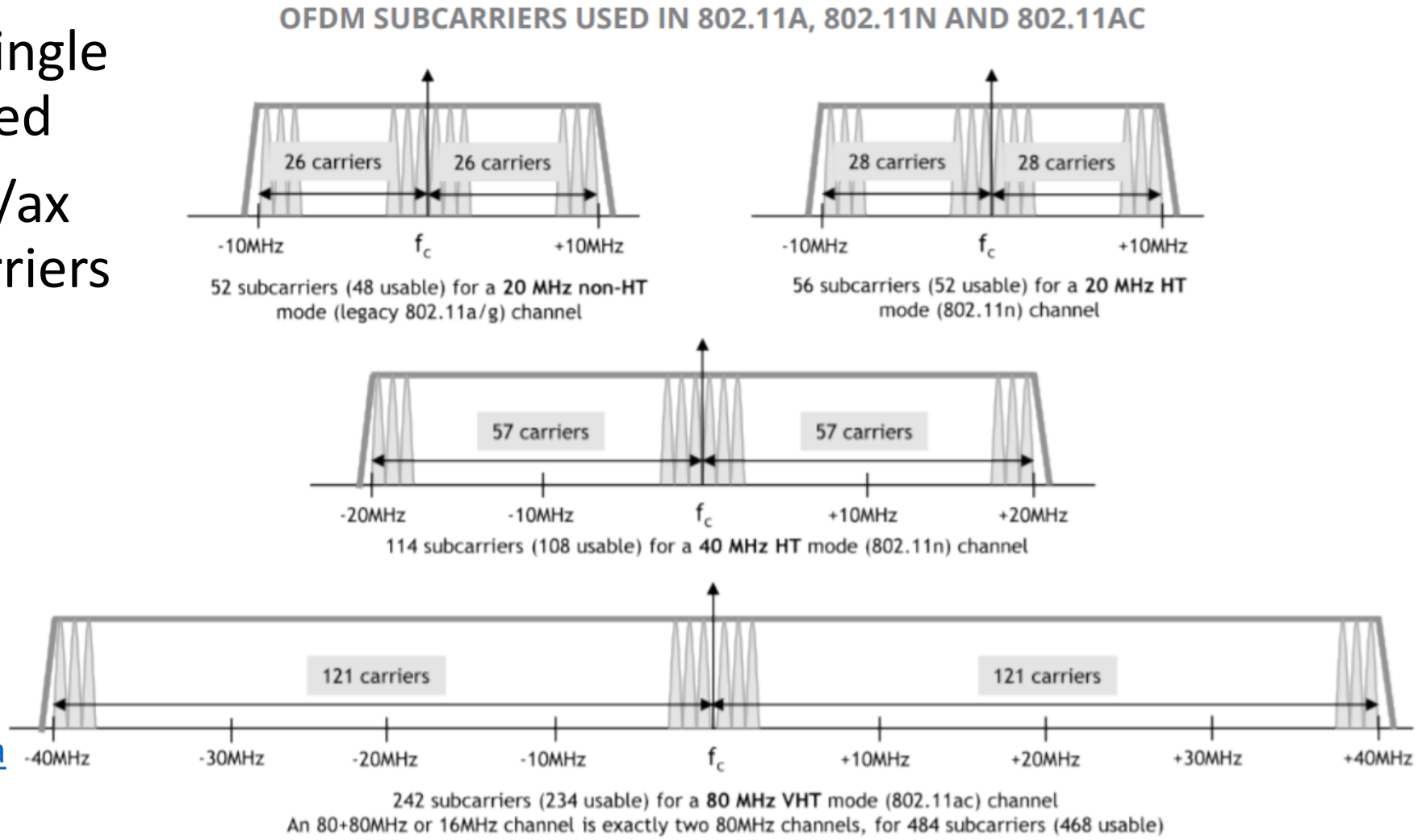


256 QAM – 16 bits/Symbol



OFDM – Many carriers of our bits

- 802.11b use a single carrier modulated
- 802.11a/g/n/ac/ax use multiple carriers all modulated independently



https://www.arubanetworks.com/assets/wp/WP_80211acInDepth.pdf

802.11ac Capacity at Max Rate

All rates assume 256-QAM, rate 5/6:

Scenario	Typical client form factor	PHY link rate	Aggregate capacity (speed)
One-antenna AP, one-antenna STA, 80 MHz	Handheld	433 Mbit/s	433 Mbit/s
Two-antenna AP, two-antenna STA, 80 MHz	Tablet, laptop	867 Mbit/s	867 Mbit/s
One-antenna AP, one-antenna STA, 160 MHz	Handheld	867 Mbit/s	867 Mbit/s
Three-antenna AP, three-antenna STA, 80 MHz	Laptop, PC	1.27 Gbit/s	1.27 Gbit/s
Two-antenna AP, two-antenna STA, 160 MHz	Tablet, laptop	1.69 Gbit/s	1.69 Gbit/s
Four-antenna AP, four one-antenna STAs, 160 MHz (MU-MIMO)	Handheld	867 Mbit/s to each STA	3.39 Gbit/s
Eight-antenna AP, 160 MHz (MU-MIMO) • one four-antenna STA • one two-antenna STA • two one-antenna STAs	Digital TV, Set-top Box, Tablet, Laptop, PC, Handheld	• 3.39 Gbit/s to four-antenna STA • 1.69 Gbit/s to two-antenna STA • 867 Mbit/s to each one-antenna STA	6.77 Gbit/s
Eight-antenna AP, four 2-antenna STAs, 160 MHz (MU-MIMO)	Digital TV, tablet, laptop, PC	1.69 Gbit/s to each STA	6.77 Gbit/s

https://en.wikipedia.org/wiki/IEEE_802.11ac

802.11ac Data Rates Min and Max

MCS index[a]	Spatial Streams	Modulation type	Coding rate	Data rate (in Mbit/s)[16][b]							
				20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195

A bunch of other streams, rates vs channel band widths

8	4	256-QAM	3/4	312	346.8	648	720	1404	1560	2808	3120
9	4	256-QAM	5/6	N/A	N/A	720	800	1560	1733.3	3120	3466.7

https://en.wikipedia.org/wiki/IEEE_802.11ac

IEEE 802.11n-2009

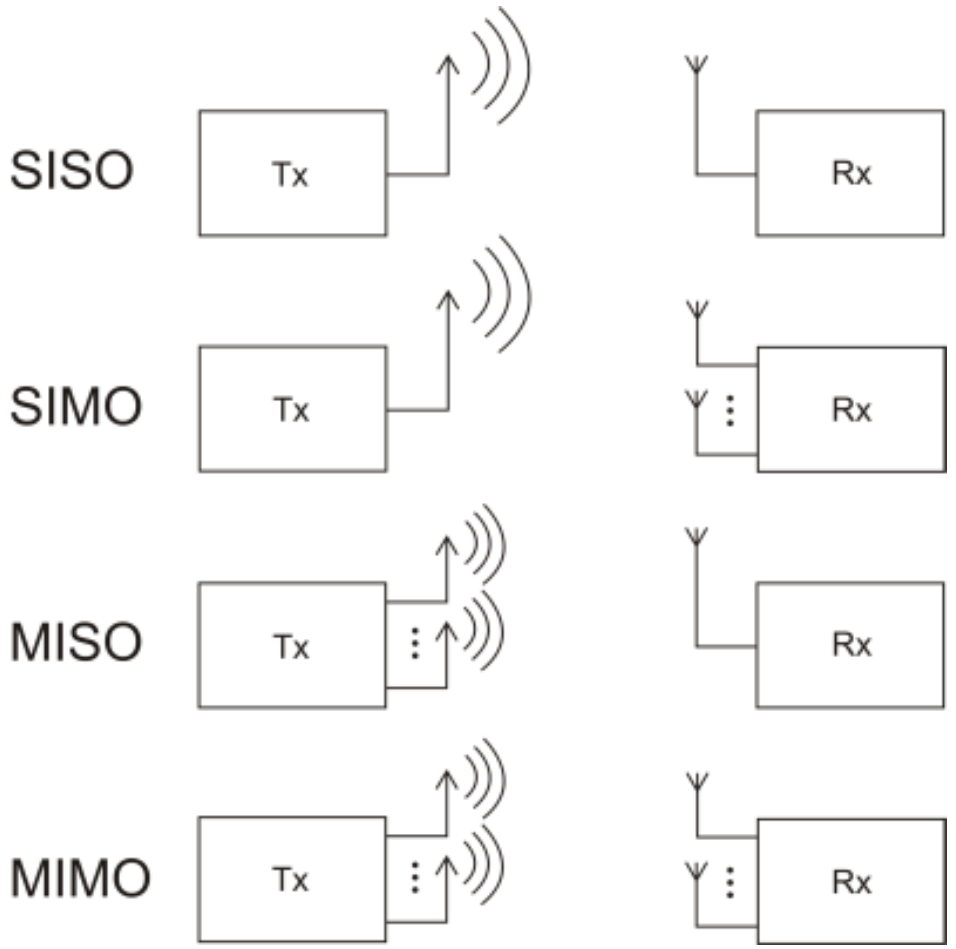
- **Multiple Input Multiple Output (MIMO)**
  - Beam forming
  - Maximal Ratio Combining (MRC)
  - Spatial multiplexing
  - Space-Time Block Coding
- **Improved modulations**
  - Greater bits/Hertz
  - Short Guard Intervals
- **40 MHz Channels**
  - combined 20 MHz channels for 40 MHz BW
- **Improved MAC Efficiency**
  - MAC packet aggregation to reduce overhead
  - Block Acknowledgements
  - Reduced Interframe Spacing
- **Power Savings**
  - Spatial Mulitplexing Power Saving
  - Power Save Multiple-Poll

IEEE 802.11ac

- Borrowed from the 802.11a/802.11g specifications:
  - 800 ns regular guard interval
  - Binary convolutional coding (BCC)
  - Single spatial stream
- Newly introduced by the 802.11ac specification:
  - 80 MHz channel bandwidths
- **Optional**
- Borrowed from the 802.11n specification:
  - Two to four spatial streams
  - Low-density parity-check code (LDPC)
  - Space–time block coding (STBC)
  - Transmit beamforming (TxBF)
  - 400 ns short guard interval (SGI)
- Newly introduced by the 802.11ac specification:
  - five to eight spatial streams
  - 160 MHz channel bandwidths (contiguous 80+80)
  - 80+80 MHz channel bonding (discontiguous 80+80)
  - MCS 8/9 (256-QAM)

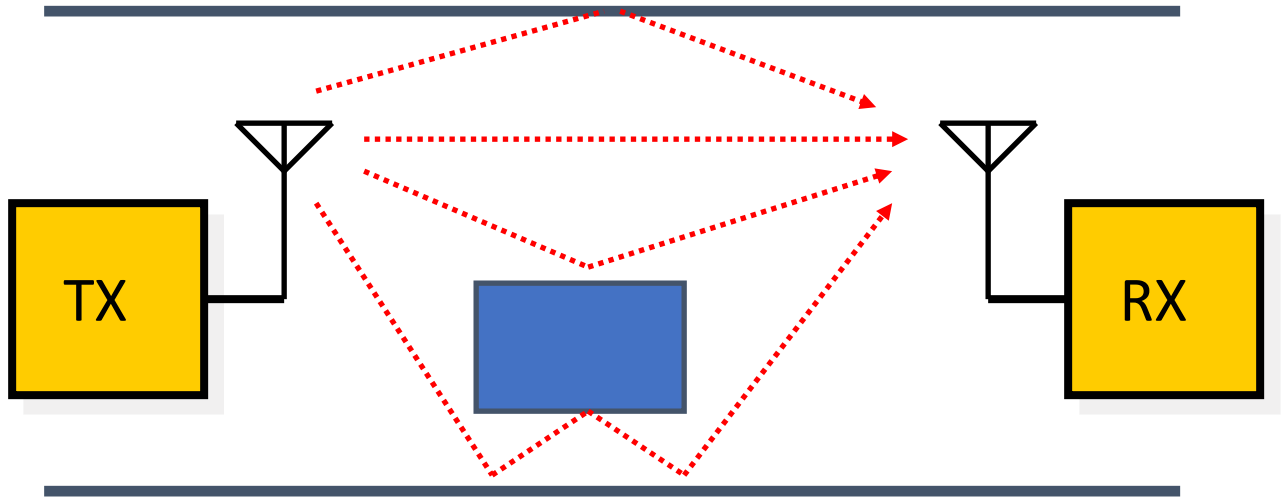
IEEE 802.11n: Enter MIMO

- Multiple Input Multiple Outpt
- MIMO refers to the “Channel” with TX antennas as inputs and RX antennas as outputs
- MIMO refers to the “Channel” with TX antennas as inputs and RX antennas as outputs



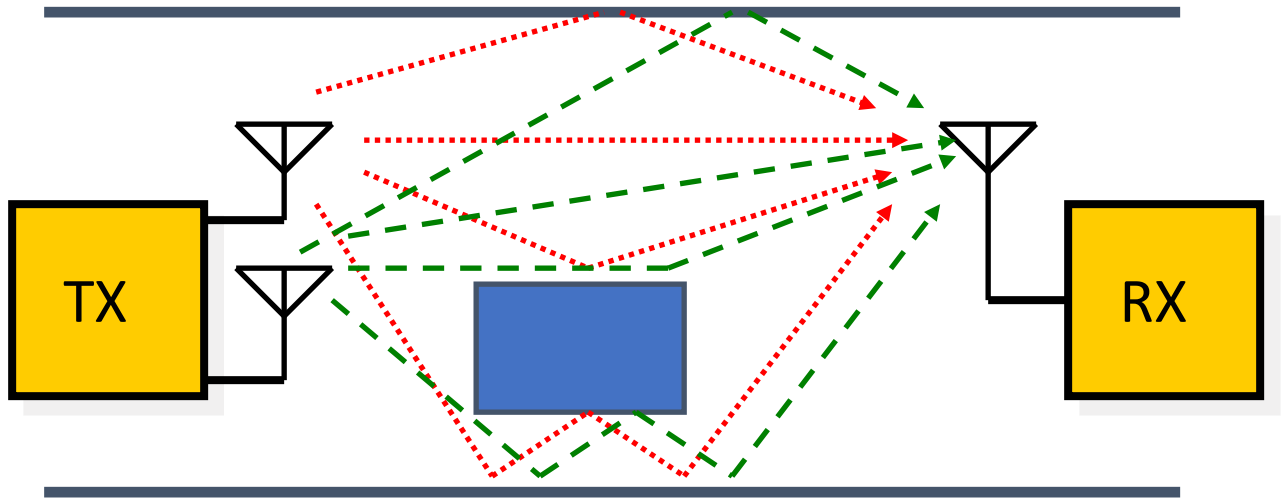
SISO – Single Input Single Output

- This is the legacy radio technology of 802.11abg
- One antenna at a time for both TX and RX is used
- Diversity, if used, is based on an antenna “selection”



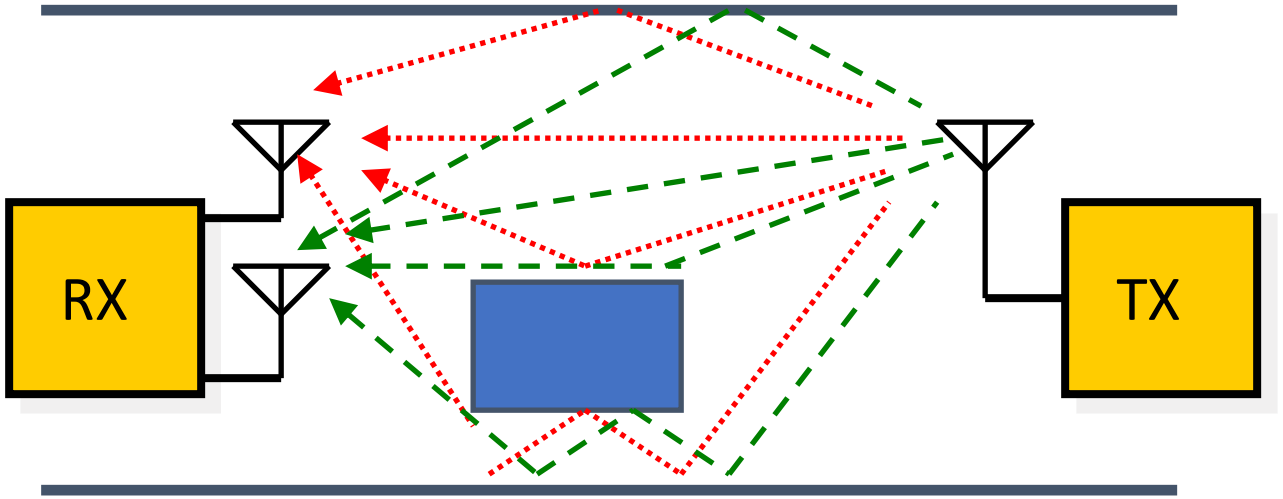
MISO – Multiple Input Single Output

- More than one antenna at TX - one on RX
- Beam-forming focuses radio signals directly on the target antenna to improve range and performance.
- TX Diversity – TX&RX must “sound” the channel to establish the signal coding



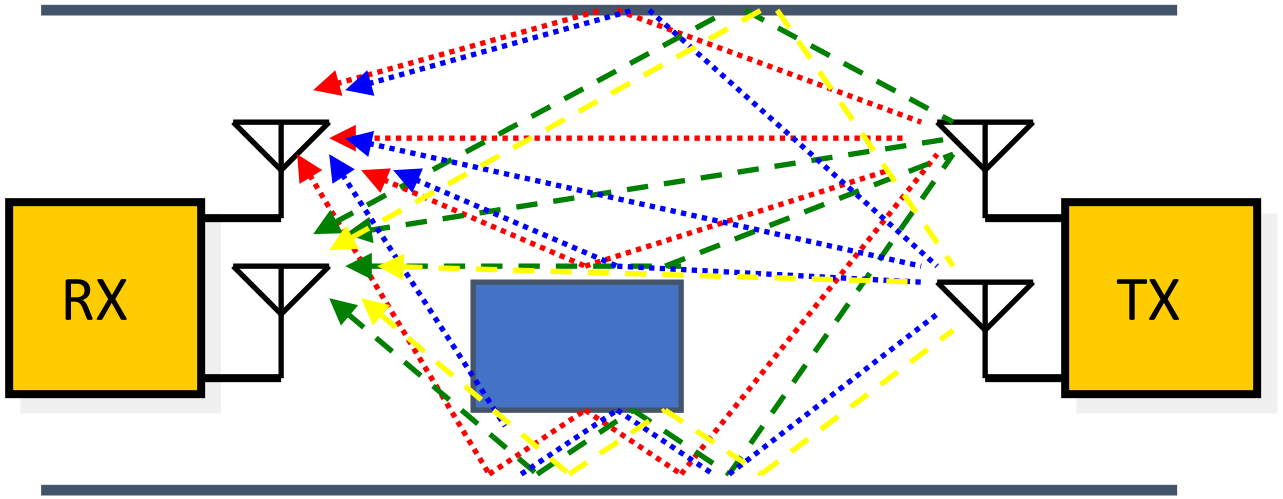
SIMO – Single Input Multiple Output

- Single TX antenna, more than one RX antenna.
- Maximum Ratio Combining – process and add the signals.
- RX Diversity – RX chooses best signal on the fly.



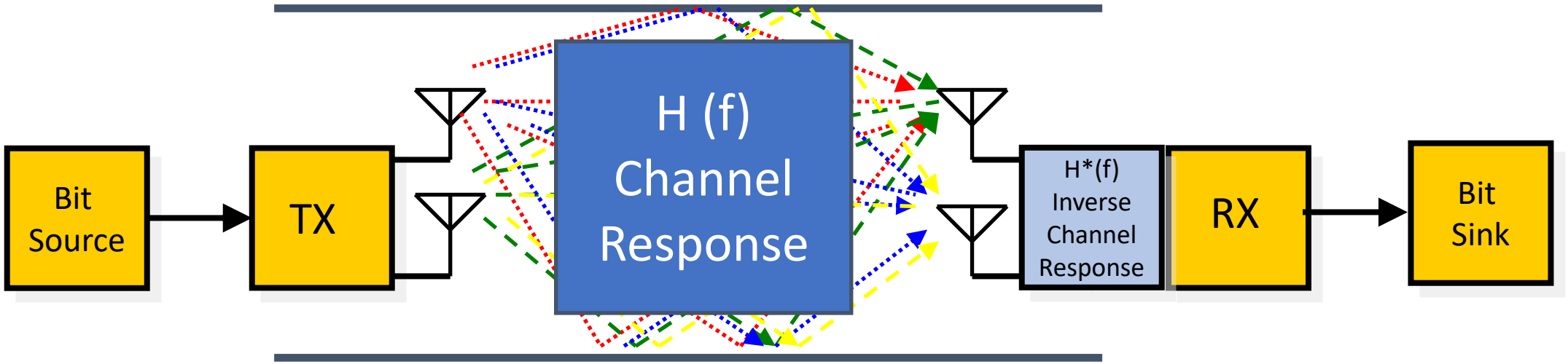
MIMO – Multiple Input Multiple Output

- Channel has multiple **Spatial Streams.**
- Classified in an NxM fashion
- N TX (input) antennas, M RX (output) antennas
- MUST have multipath to work!



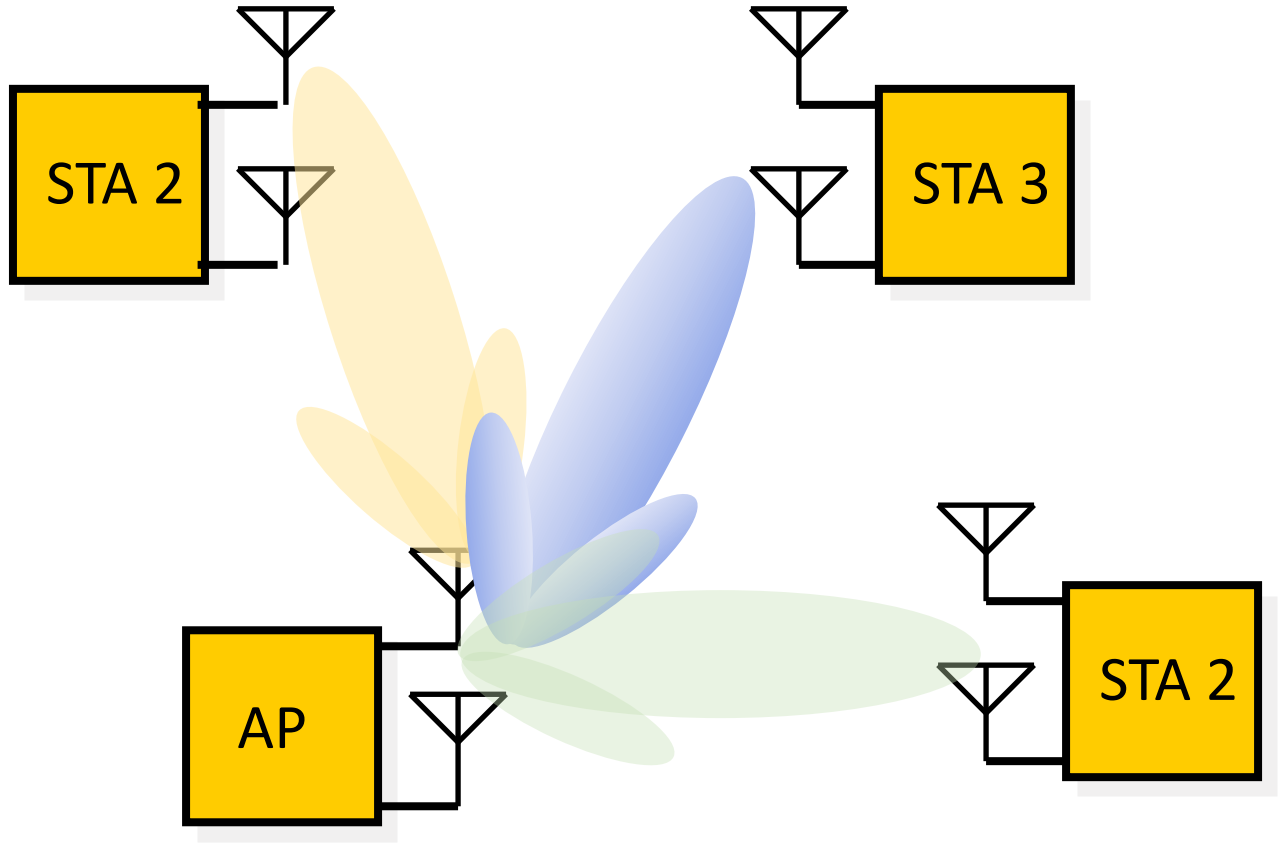
What is going on here?

- MIMO with simple algebra – Important to keep in mind for later
- Goal is bits in equals bits out.
- MIMO you can select a trade-off of capacity for reliability



MU-MIMO (Multi-User MIMO)

- Steer the beam to the user to which the data is intended.
- Another form of channel access that allows even more users in a dense area.



Spooky Action At a Distance (Sort-of)

- Or… How Wi-Fi can be used to see where you are, what you are doing and what you are typing….. Really….

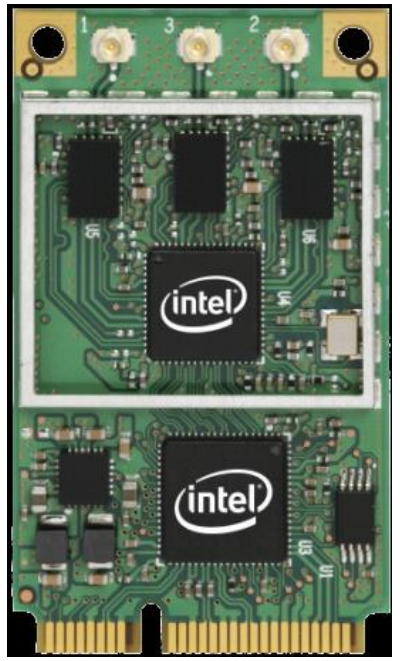
- TUNE IN TO FIND OUT MORE!!!!

Linux 802.11n CSI Tool

CSI (Carrier State Information) allows for the capture of amplitude and phase of each -11n subcarrier.

This is a very very useful tool……

Because in short it is Radar with your Router!



Using the Intel 5300 to detect finger motion

- https://www.youtube.com/watch?v=xGOdSJS2dWk

Atheros CSI Tool

- Works with OpenWRT and correct chipsets. AR93xx, AR94xx, and AR95xx are all capable of CSI extraction

- https://wands.sg/research/wifi/AtherosCSI/
- https://github.com/xieyaxiongfly/Atheros_CSI_tool_OpenWRT_src

Some Examples…

- **Jian Ding, Ranveer Chandra**
  - **Towards Low Cost Soil Sensing Using Wi-Fi**
- Kai Niu, Fusang Zhang, Yuhang Jiang, Zhaoxin Chang, Leye Wang, and Daqing Zhang.
  - A contactless Morse code text input system using COTS wifi devices.

Gee this was fun!