# RADIO FREQUENCIES, WI-FI & JARGON

*Chris Dawe & Tom Bridge*

# CHRIS DAWE

- CWNA
- Consulting Wireless Engineer
- Partner, Wheelwrights LLC,
  Seattle WA
- Fancy 🎩

- @ctdawe - Slack, Twitter

# TOM BRIDGE

- CWNA
- Consulting Wireless Engineer
- Partner, Technolutionary LLC, Washington DC
- Fancy 🐈

- @tbridge - Slack, Twitter, Github

# NONE OF THIS SHOULD WORK

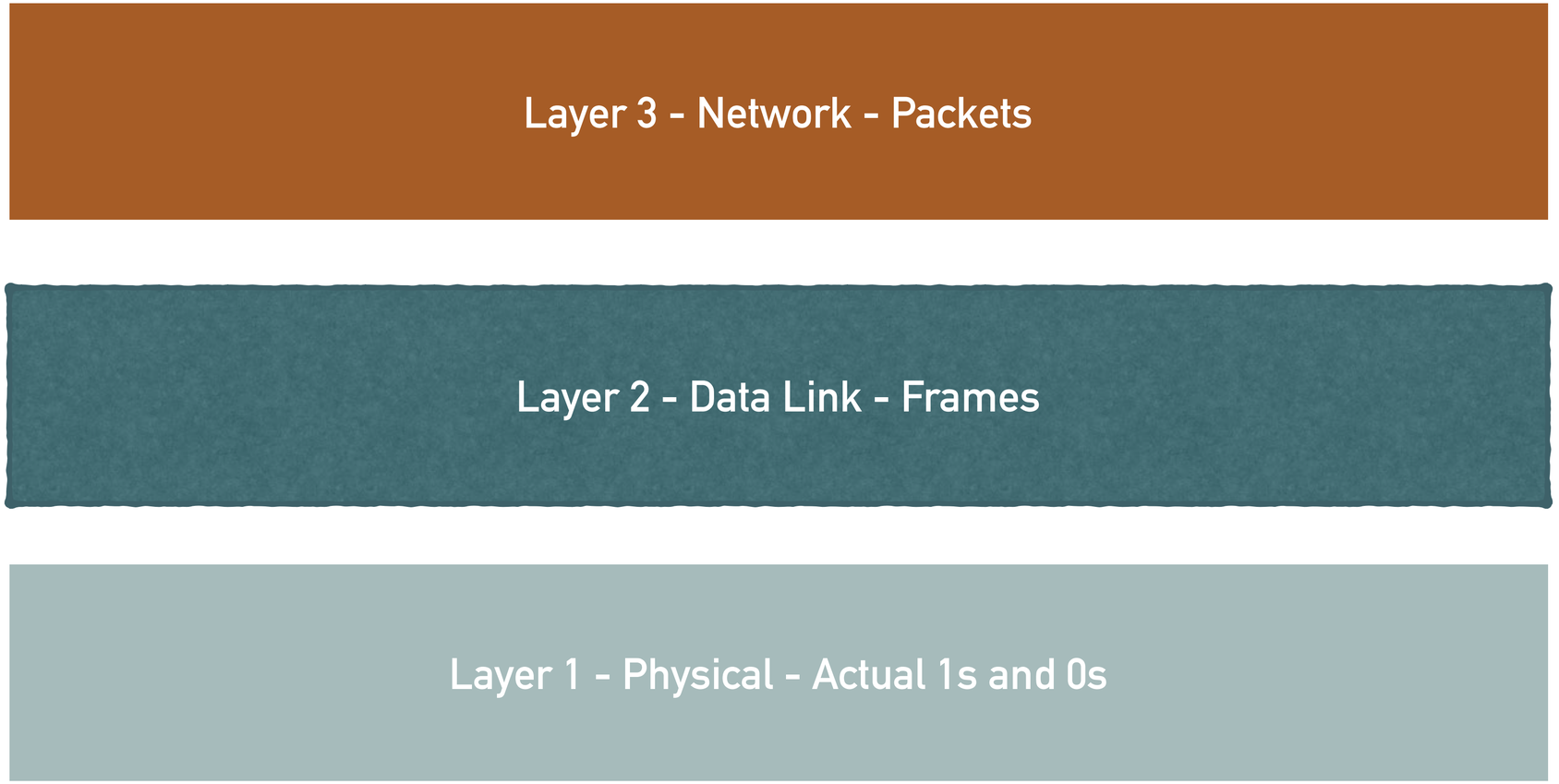
# WHAT IS WI-FI ANYWAY?

# WHAT IS WI-FI?

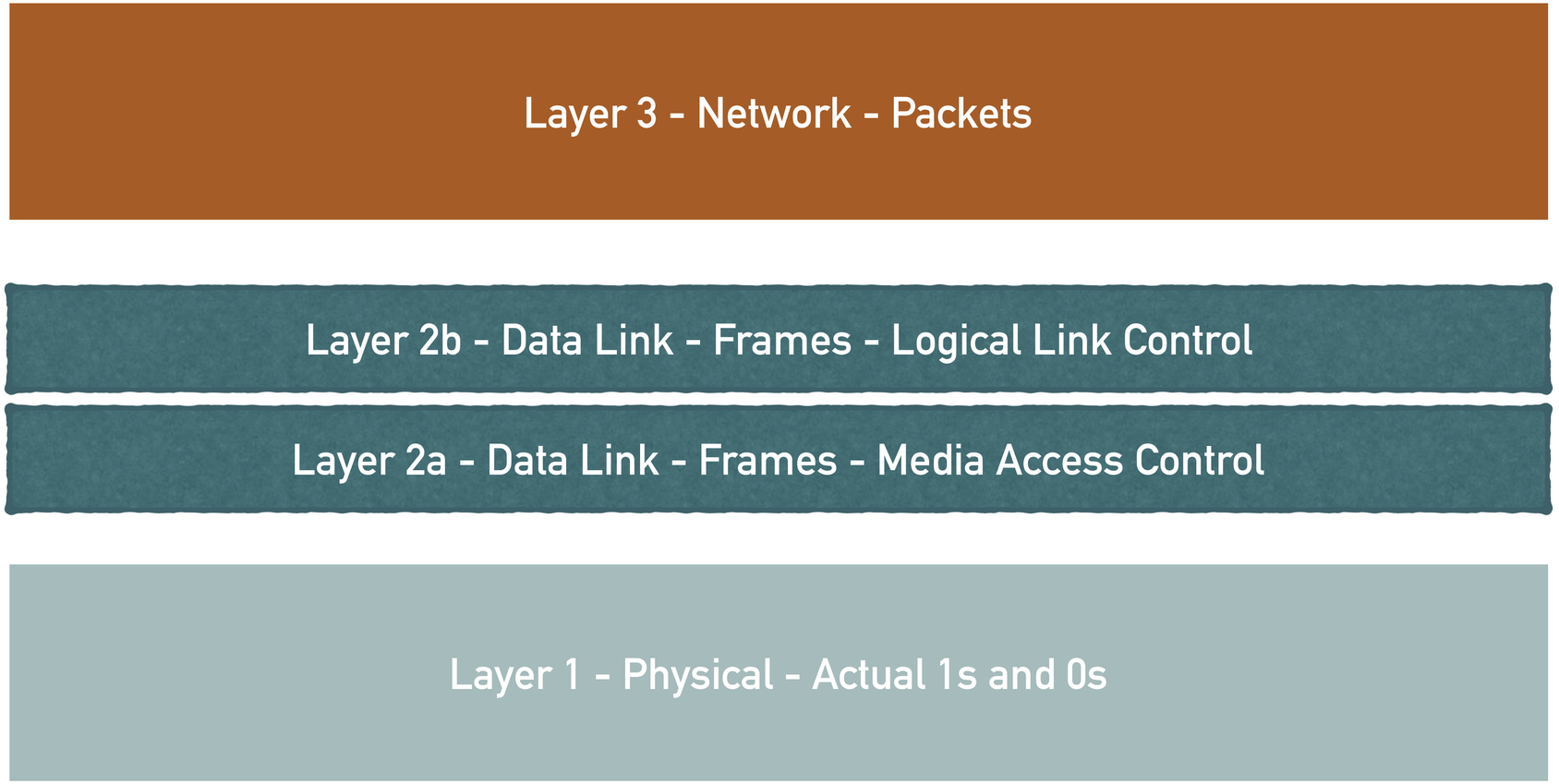
- Radio Frequency Communication
- 2.4GHz (2,400,000,000 cycles per second or so) or
  5Ghz (5,000,000,000 cycles per second or so) frequency range
- Usually between a central communication hub and one or many client devices
- Signal is generated by a transmitter, passed through an antenna, and interpreted by a receiver (also with an antenna), creating a transceiver pair.
- The receiver and transmitter are tuned to a specific frequency with resonators.
- The signal carries data, which is encapsulated into frames, which are then read by the client as structured signal and interpreted as network traffic.

# WI-FI IS A LAYER 1-2 TECHNOLOGY

# THE OSI MODEL – MEDIA LAYERS



# THE OSI MODEL – MEDIA LAYERS



# THIS IS NOT
# MY BEAUTIFUL HOUSE

# IN THE BEGINNING, THERE WAS 802.11

# THE 2.4 GHZ SPECTRUM

# THE STANDARD CONVENTIONS FOR BROADCAST WI-FI

*Adoption*

# 802.11 (1997)

- 2.4Ghz
- 2Mbps maximum throughput
- Sets the 20Mhz Channel Width (actually 22Mhz)
- Sets original 11 Channels
- Frequency Hopping or Direct Sequence Spread Spectrum
- Uses Barker Coding

# LET US PAUSE TO APPRECIATE HEDY LAMARR AND GEORGE ANTHEIL

# 802.11A/B (1999)

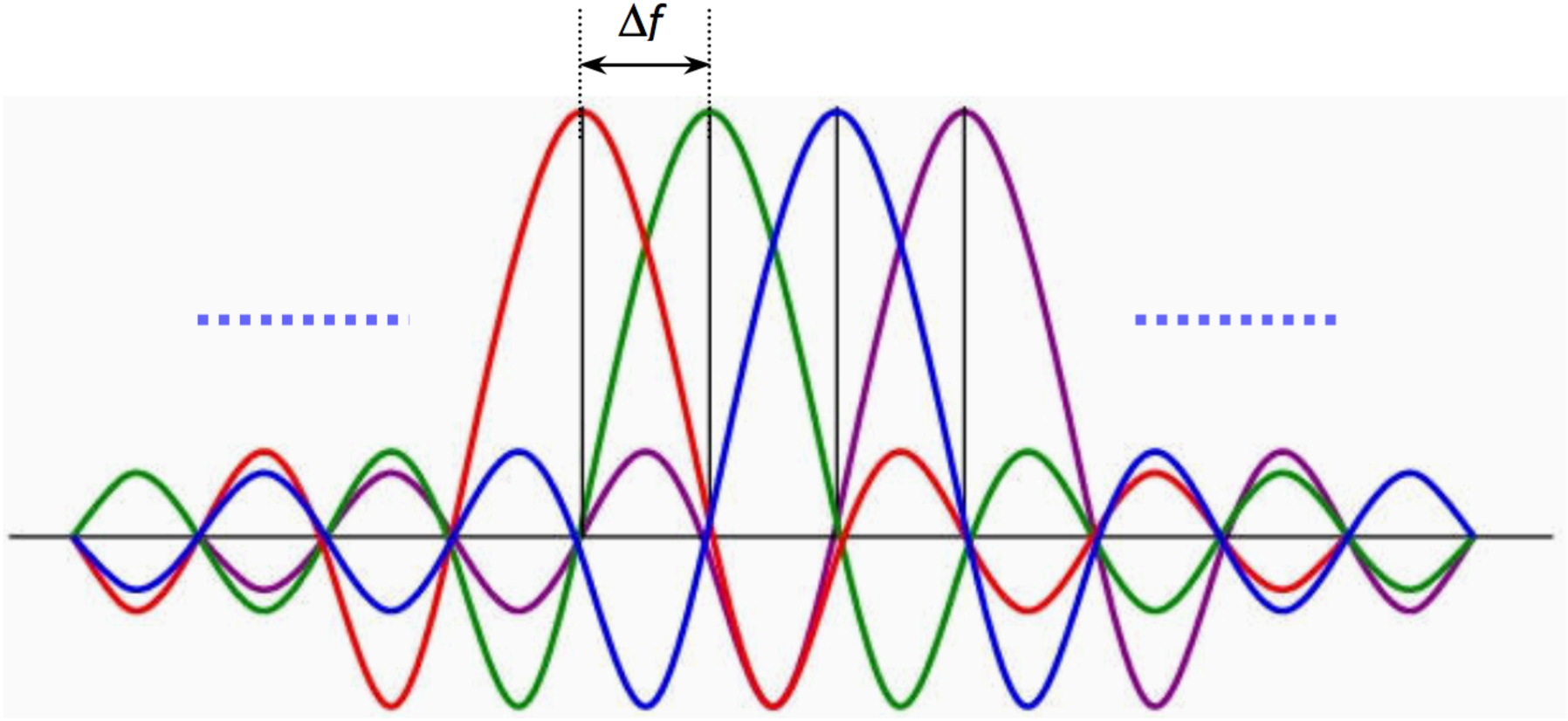
- 2.4GHz for b, 5.8 GHz for a
- 11Mbps for b, 54Mbps for a
- WEP Encryption only
  (40-bit, then 128-bit, both insecure)
- Beacon frames can slow the network substantially
- Uses DSSS in b, OFDM in a

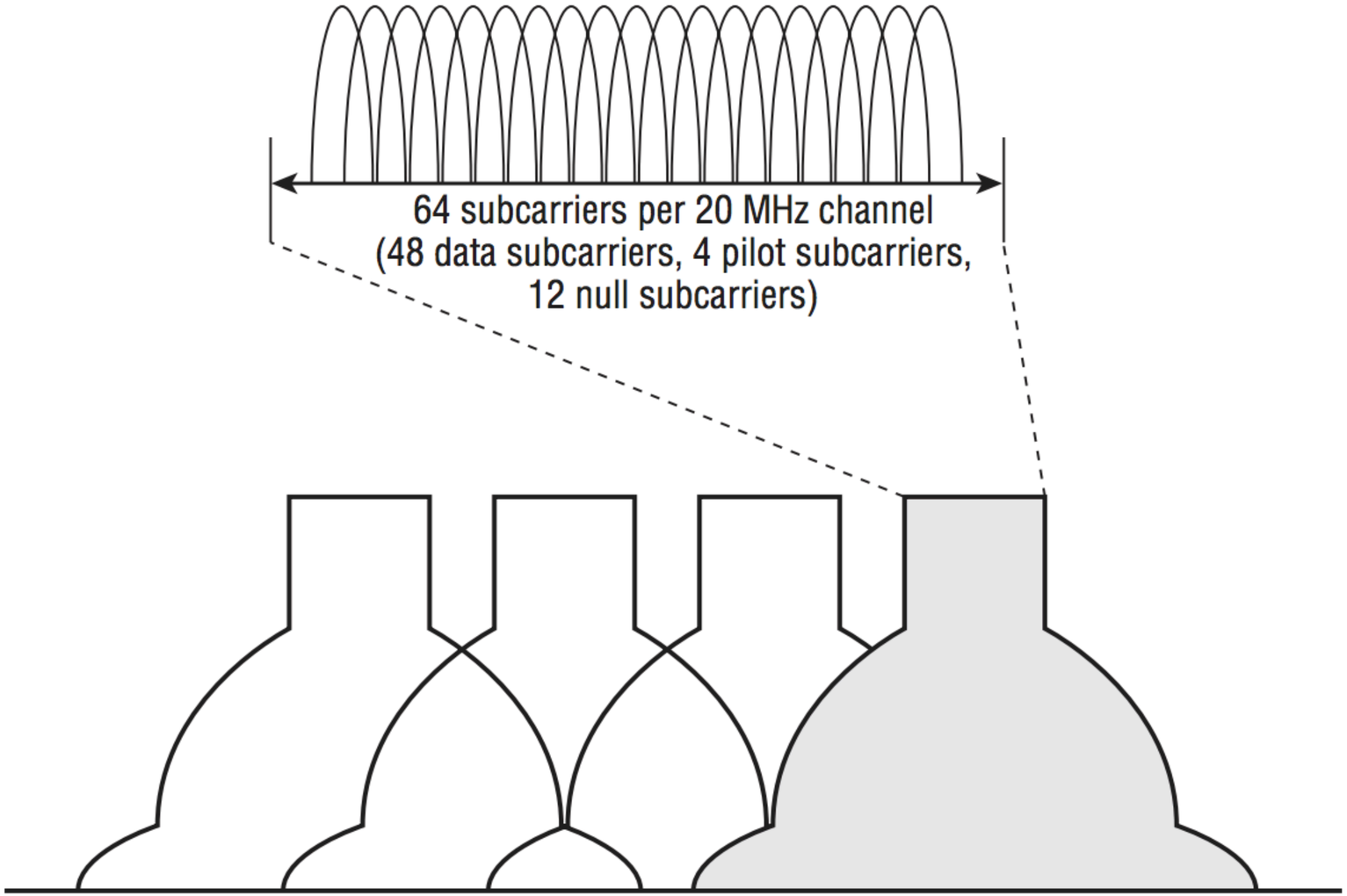
# 802.11G (2003–2006)

- Adds WPA Encryption (still vulnerable)
- Switch from DSSS to OFDM to improve interference handling
- But has to support DSSS mode for 802.11b compatibility, which can slow whole networks down
- 54Mbps comes to 2.4GHz

# ORTHOGONAL FREQUENCY–DIVISION MULTIPLEXING

# I PROMISE THE MATH WON'T GET CRAZY.


Δf

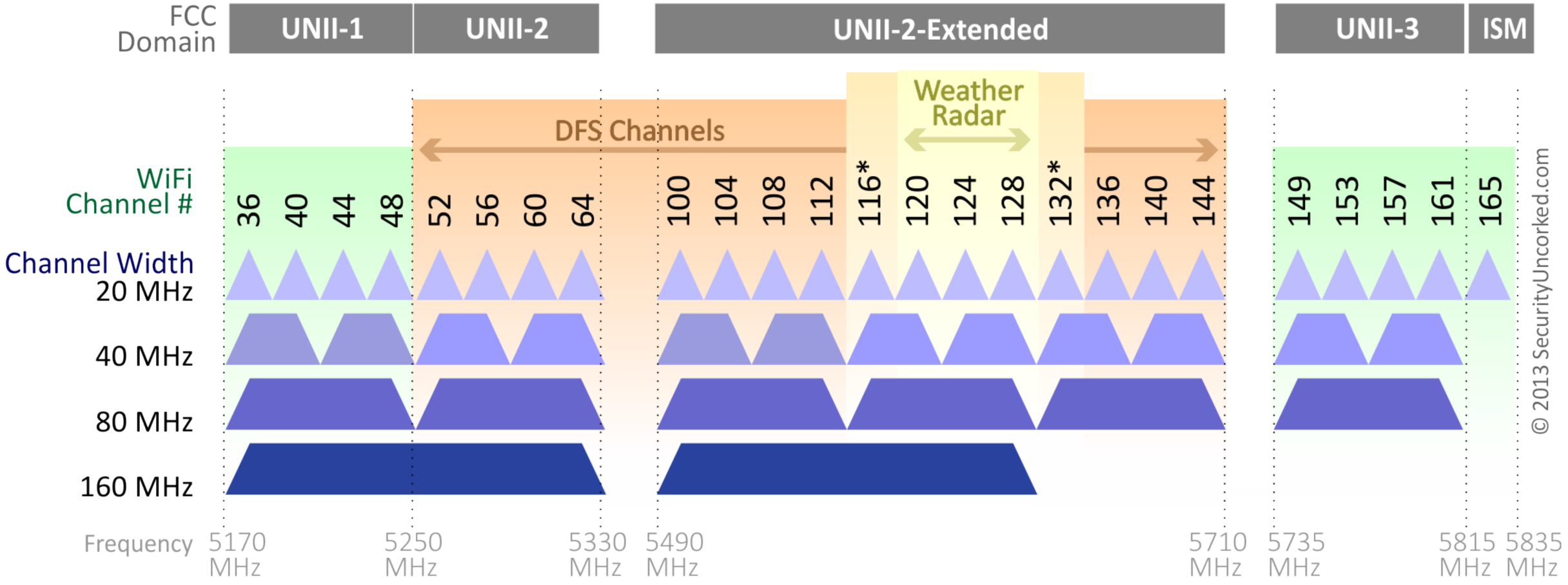

64 subcarriers per 20 MHz channel
(48 data subcarriers, 4 pilot subcarriers,
12 null subcarriers)

# THIS REALLY WORKS.
# REALLY.

# 802.11N (2006-2011)

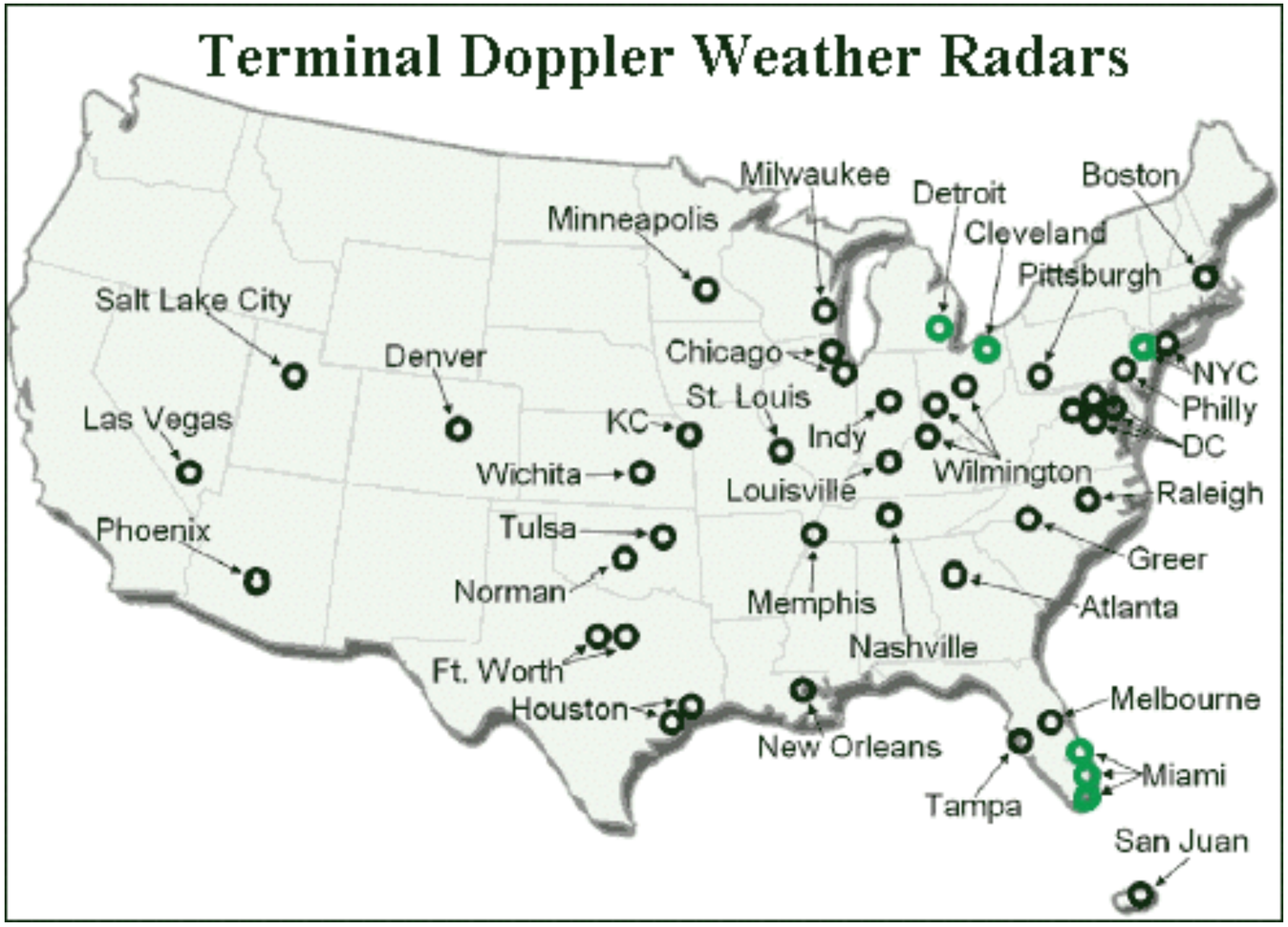
- 2.4 or 5GHz
- 20 or 40 MHz channel widths
- High Throughput (HT) Channels option
- Short Guard Interval Allowed (400ns)
- Introduces MCS Index
- Hello, MIMO
- WPA2 Introduced, TKIP deprecated, AES introduced
- Maximum Speed: 600Mbps, Theoretical
- 802.1X WPA Enterprise

# 802.11ac Channel Allocation (N America)




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

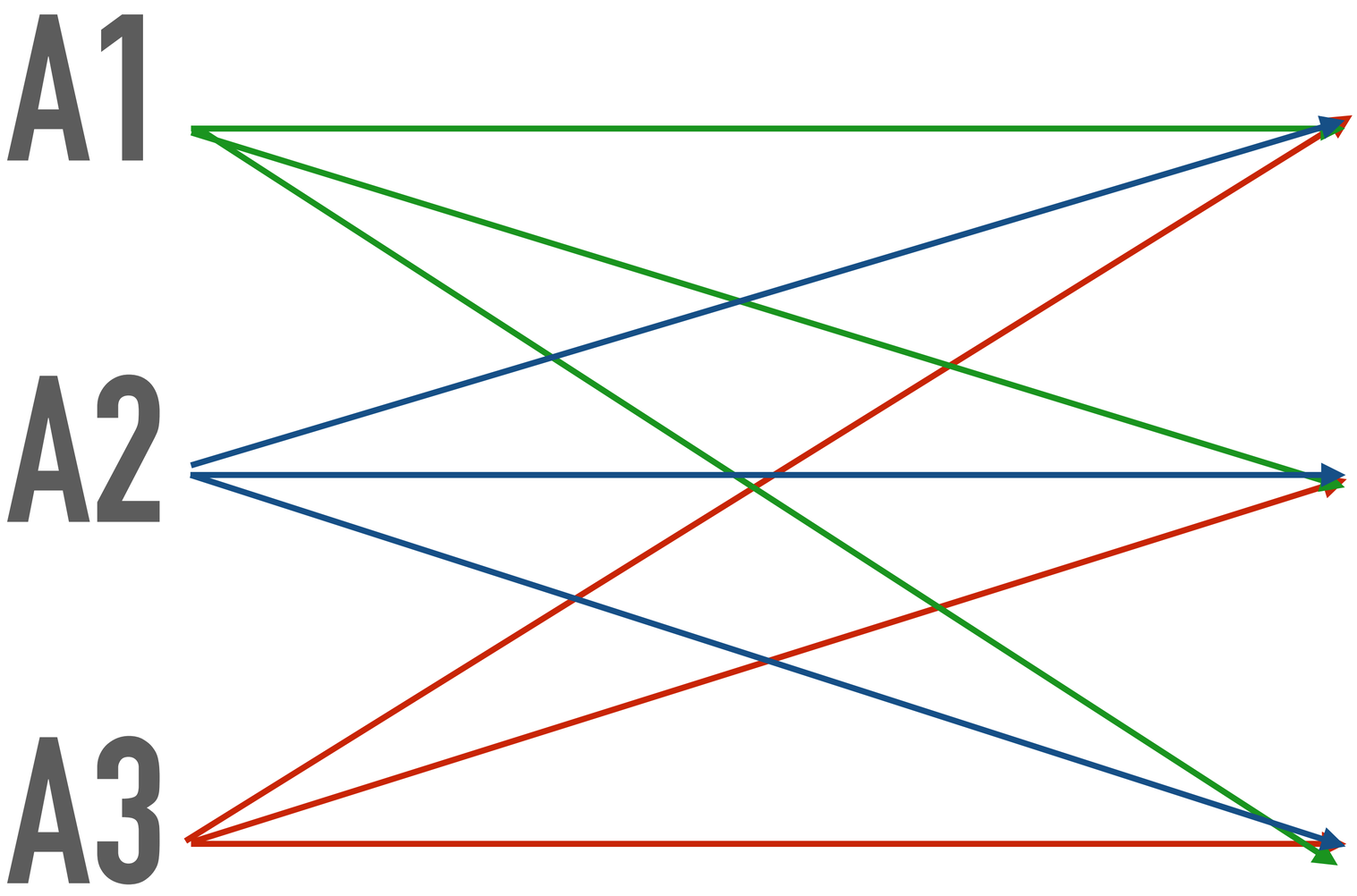
# WHAT'S DFS?




# DYNAMIC FREQUENCY SELECTION

# WHAT WAS (IS) SISO?

# WHAT'S MIMO?




# MULTIPLE IN, MULTIPLE OUT

# WHAT'S T × R : S?

# 802.11AC WAVE 1 (2013)

- 5GHz only
- 80 MHz channel widths
- 1.2Gbps Theoretical Max
- Can use up to 8 streams
- Can use 256 QAM

# 802.11AC WAVE 2 (2014)

- 5GHz only
- 80, or 160 MHz channel widths
- 6.9Gbps Theoretical Max
- That means you need 10GbE to your AP!
- MU-MIMO!

# MU-MIMO

# 802.11AX (DRAFT)

- 5GHz only
- 20, 40, 80, or 160 MHz channel widths
- Can Use 1024 QAM
- 6.9Gbps Theoretical Max
- That means you need 10GbE to your AP!
- MU-MIMO bi-directional use
- OFDMA - Orthogonal Frequency-Division Multiple Access

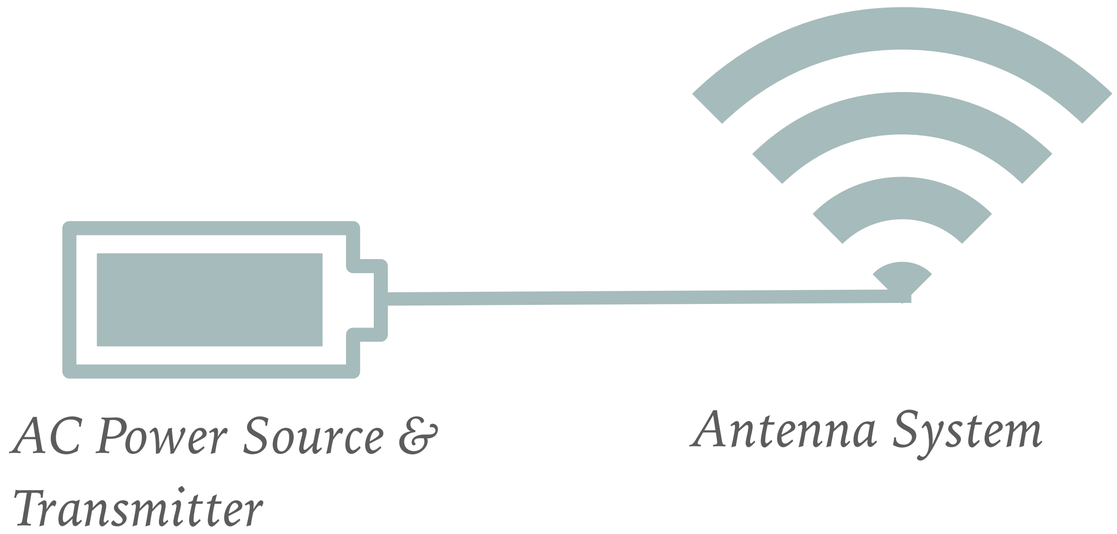
# WHAT'S OFDMA

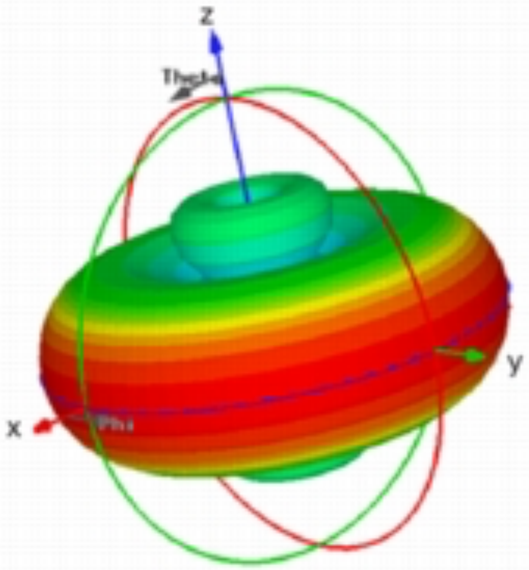
# WHAT ABOUT ALL THOSE OTHER LETTERS THAT WE SKIPPED?

# OTHER AMENDMENTS

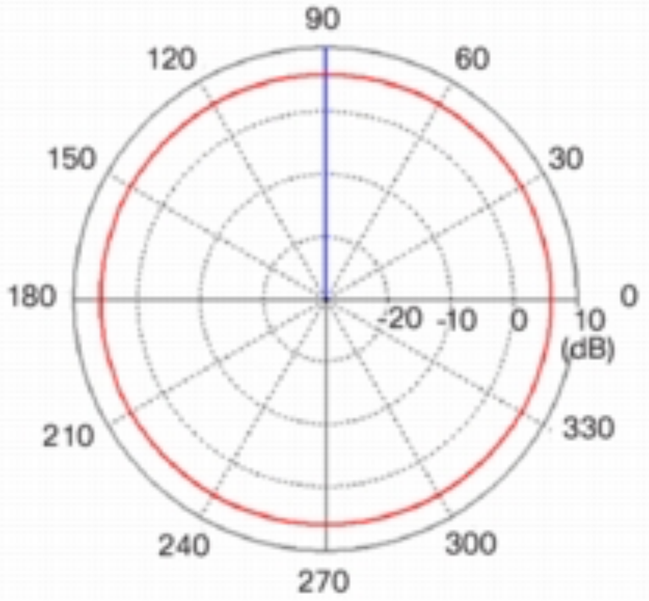
- 802.11e - QoS
- 802.11i - Enhanced Security (Introduces WPA)
- 802.11k - Radio Resource Management (Neighbor Reports)
- 802.11r - Fast Transition roaming (FT)
- 802.11v - Distributed Wireless Statistics Gathering
- 802.11w - Protected Management Frames

# THE BASICS OF TRANSMISSION

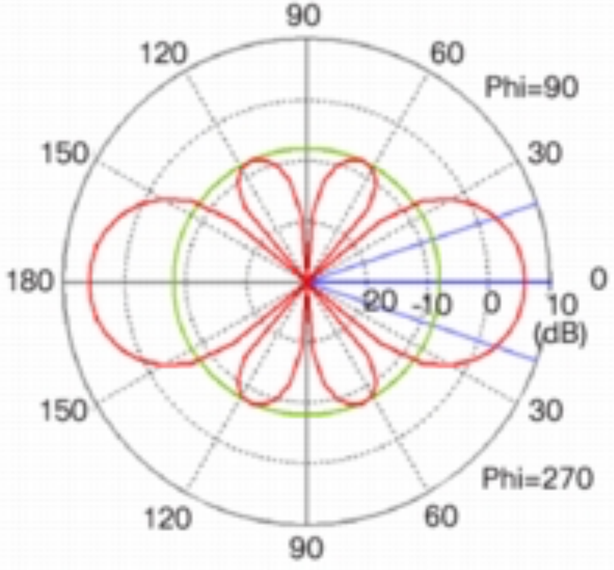

AC Power Source &
Transmitter
Antenna System



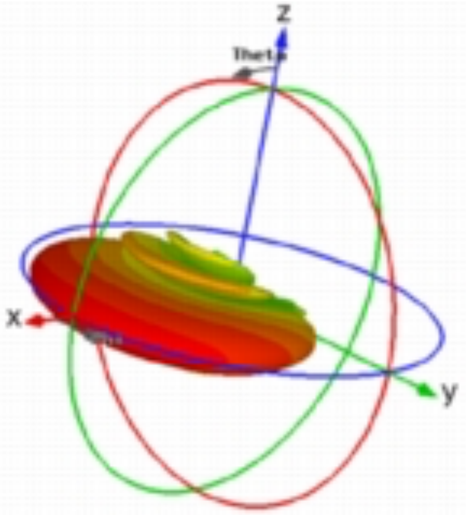

(a) 5.8 dBi Omni 3D Pattern



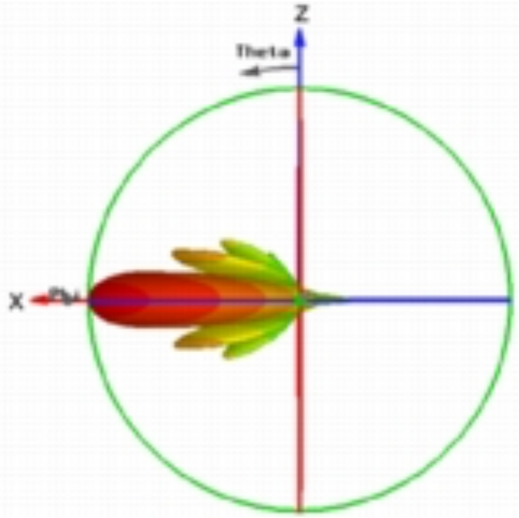

(b) 5.8 dBi Omni Azimuth Plane Pattern



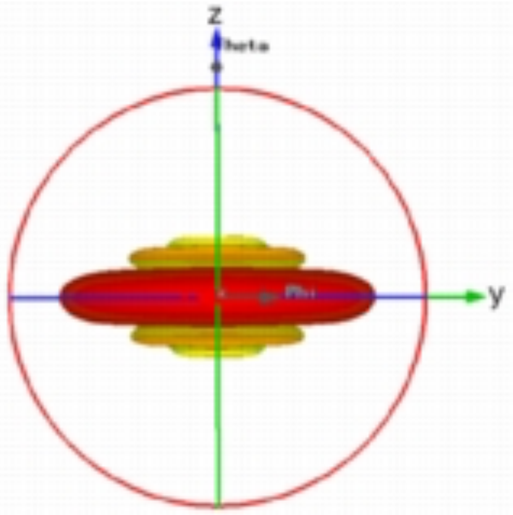

(c) 5.8 dBi Omni Elevation Plane Pattern



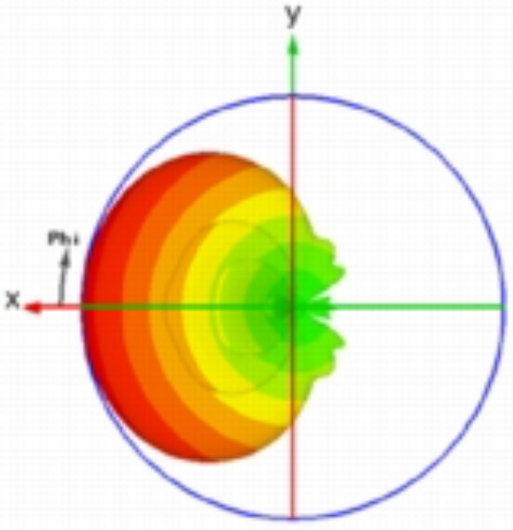

(a) Sector Antenna 3D Pattern



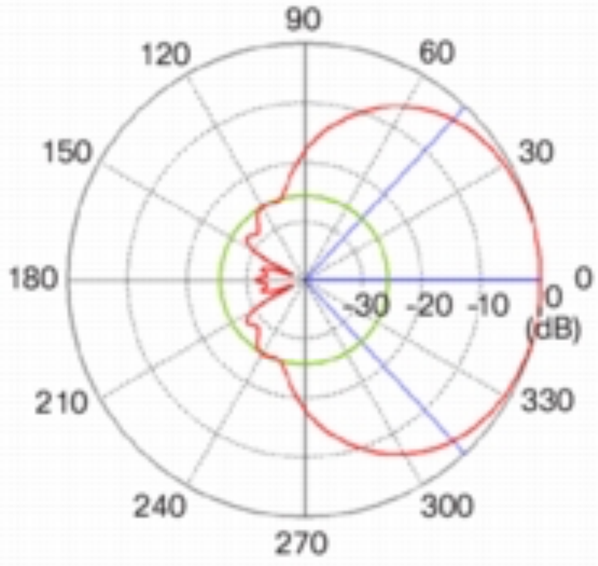

(b) Sector Antenna 3D Pattern Side View



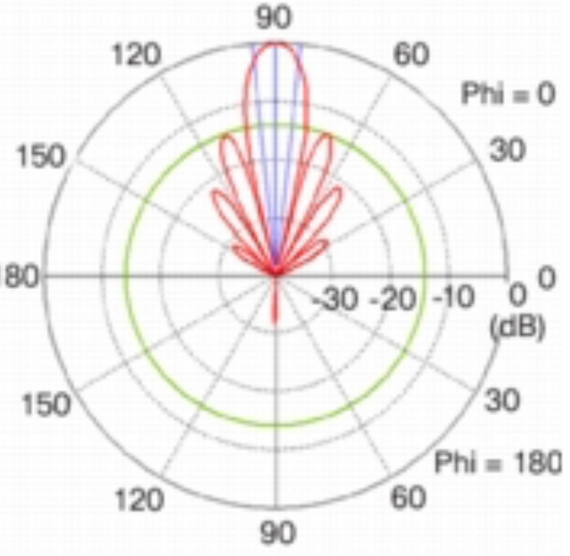

(c) Sector Antenna 3D Pattern Front View




(d) Sector Antenna 3D Pattern Top View




(e) Sector Antenna Azimuth Plane Pattern



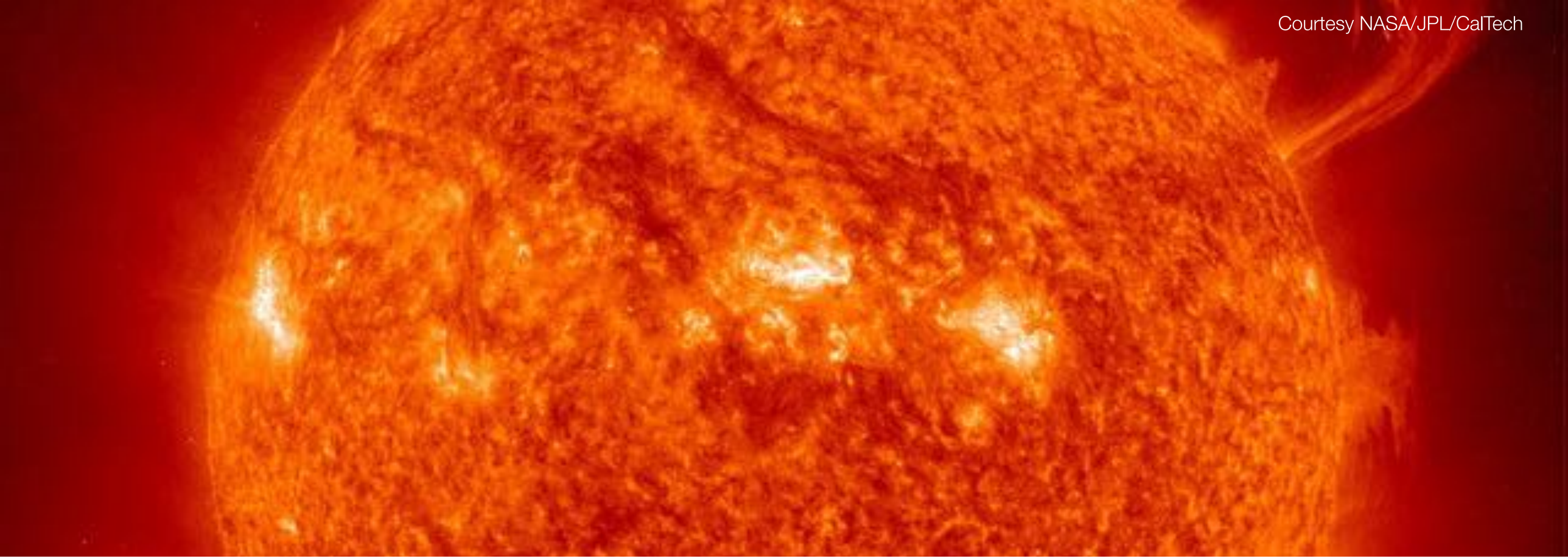

(f) Sector Antenna Elevation Plane Pattern

# HOW YOU MOUNT YOUR AP MATTERS

# THE STATISTICS OF WI-FI

SIGNAL CHANGES WITH THE INVERSE OF THE SQUARE OF THE DISTANCE BETWEEN THE TRANSMITTER AND THE RECEIVER

AS YOU GET FURTHER AWAY,
SIGNAL GETS EXPONENTIALLY WORSE.



Courtesy NASA/JPL/CalTech

# ATTENUATION AND THE INVERSE SQUARE LAW

*Intensity of signal radiating from a point source is inversely proportional to the square of the distance from the source.*

# ATTENUATION AND THE INVERSE SQUARE LAW

*In other words, the further you get away from a signal source, the less intense it is.*

Courtesy NASA/JPL/CalTech

# DECIBELS – A MEASURE OF SIGNAL STRENGTH

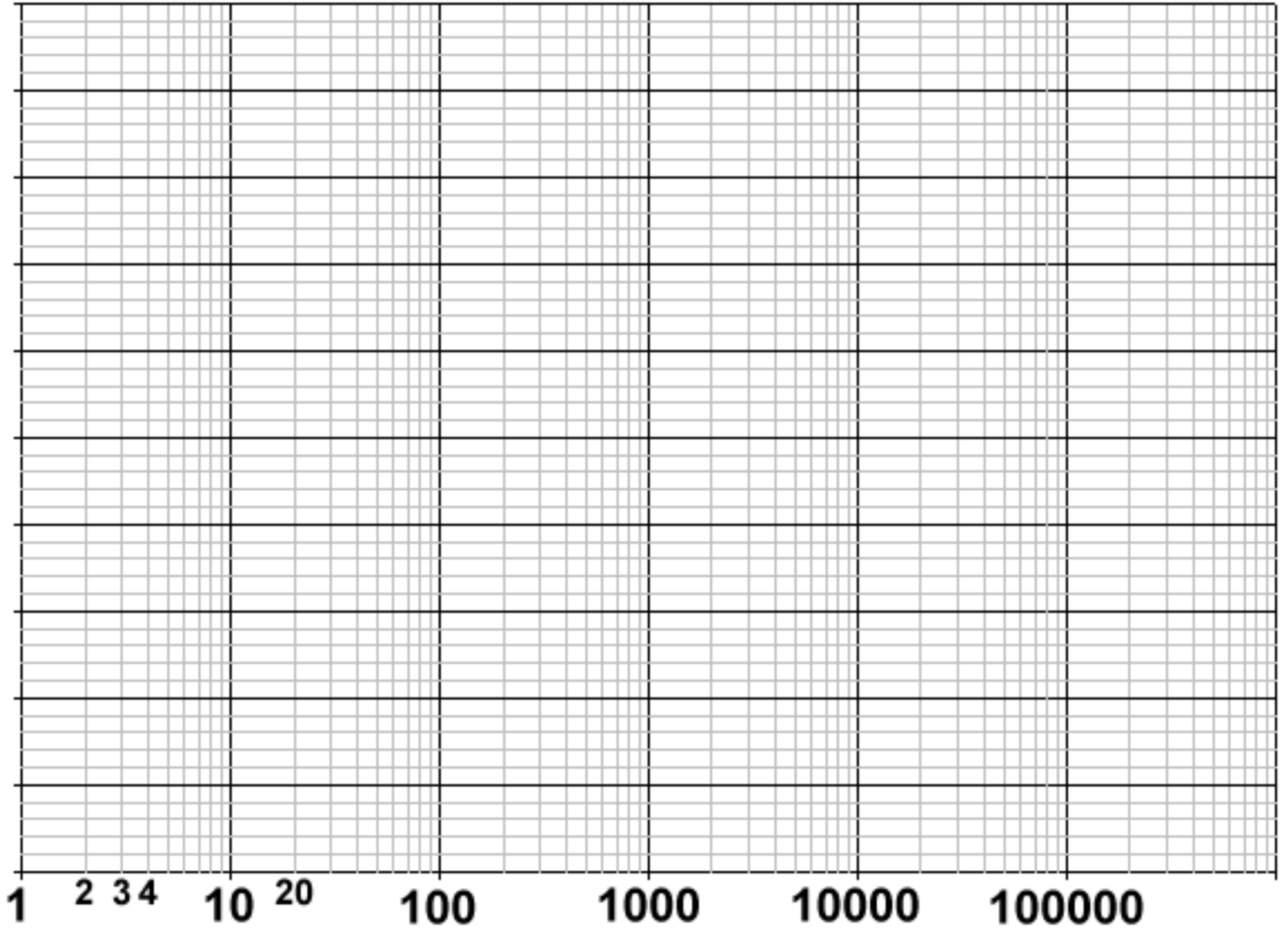
a unit used to measure the intensity of a sound or the power level of an electrical signal by comparing it with a given level on a logarithmic scale.

*dBm - A logarithmic representation of signal, as compared to 1mW of transmit power*

*Also called a decibel-milliwatt*

*Generally, all signal numbers you're going to see are negative if they're expressed in dBm.*

# LOGARITHMIC SCALES GIVE US A MENTAL "EASY BUTTON" FOR A COMPLEX MATHEMATICAL CONCEPT


1
2
3
4
10
20
100
1000
10000
100000

# RULES OF TENS AND THREES

- -3 dBm of signal means half the raw signal power.
- -10 dBm of signal means one tenth the raw signal power.
- +3 dBm of signal means double the raw signal power.
- +10 dBm of signal means ten times the raw signal power.

# FREE SPACE PATH LOSS

- In an unobstructed space, waves weaken as you get further away from the point source
- But there's diminishing returns to that weakness.
- Varies based on a number of environmental factor
- Critical to understand - along with fresnel zones - for point to point links over long distances, with directional antennae.

# SIGNAL MEASURES

# HELPFUL TERMS

- RSSI - Received Signal Strength Indicator
- Noise Floor
- SNR - Signal to Noise Ratio
- MCS Index - Modulation & Coding Scheme Index

# MODULATION & CODING SCHEME

# MCS INDEX: A LOOKUP TABLE FOR WI-FI SPEED

CHANNEL WIDTH
GUARD INTERVAL
SPATIAL STREAMS
MODULATION & CODING

# MODULATION & CODING

- From Weak to Strong
- Binary Phase-Shift Keying (Two Potential Values Per Subcarrier)
- Quadrature Phase-Shift Keying (Four Potential Values Per Subcarrier)
- 16 Quadrature Amplitude Modulation (Sixteen Potential Values Per Subcarrier)
- 64 Quadrature Amplitude Modulation
- 256 Quadrature Amplitude Modulation

- Coding can be 1/2, 2/3, 3/4, or 5/6

# DON'T BOTHER STARING – VISIT MCSINDEX.COM

MCS : Index

| 802.11n | | | | | | | | | | | 802.11ac |
|---|---|---|---|---|---|---|---|---|---|---|---|
| HT MCS Index | Spatial Streams | Modulation & Coding | Data Rate GI = 800ns 20MHz | Data Rate SGI = 400ns 20MHz | Data Rate GI = 800ns 40MHz | Data Rate SGI = 400ns 40MHz | Data Rate GI = 800ns 80MHz | Data Rate SGI = 400ns 80MHz | Data Rate GI = 800ns 160MHz | Data Rate SGI = 400ns 160MHz | VHT MCS Index |
| 0 | 1 | BPSK 1/2 | 6.5 | 7.2 | 13.5 | 15 | 29.3 | 32.5 | 58.5 | 65 | 0 |
| 1 | 1 | QPSK 1/2 | 13 | 14.4 | 27 | 30 | 58.5 | 65 | 117 | 130 | 1 |
| 2 | 1 | QPSK 3/4 | 19.5 | 21.7 | 40.5 | 45 | 87.8 | 97.5 | 175.5 | 195 | 2 |
| 3 | 1 | 16-QAM 1/2 | 26 | 28.9 | 54 | 60 | 117 | 130 | 234 | 260 | 3 |
| 4 | 1 | 16-QAM 3/4 | 39 | 43.3 | 81 | 90 | 175.5 | 195 | 351 | 390 | 4 |
| 5 | 1 | 64-QAM 2/3 | 52 | 57.8 | 108 | 120 | 234 | 260 | 468 | 520 | 5 |
| 6 | 1 | 64-QAM 3/4 | 58.5 | 65 | 121.5 | 135 | 263.3 | 292.5 | 526.5 | 585 | 6 |
| 7 | 1 | 64-QAM 5/6 | 65 | 72.2 | 135 | 150 | 292.5 | 325 | 585 | 650 | 7 |
| | 1 | 256-QAM 3/4 | 78 | 86.7 | 162 | 180 | 351 | 390 | 702 | 780 | 8 |
| | 1 | 256-QAM 5/6 | n/a | n/a | 180 | 200 | 390 | 433.3 | 780 | 866.7 | 9 |

# WAIT, WHAT'S A GUARD INTERVAL?

# GUARD INTERVAL

- The Symbol Period for Wi-Fi is 1/250,000th of a second or 4000ns
- Of that 4000ns, by default, 3200ns of it is used for transmission, 800ns is used for silence between symbols.
- If a symbol overruns its boundaries, or multi path reception causes it to be a little late, you want to make sure the computer can understand it still.
- Inter-Symbol Interference causes retransmits and is bad.
- Starting with 802.11n, Wi-Fi could handle 400ns Guard Intervals most of the time. This grants a 10% throughput increase at minimal risk for most setups.

# HOW SHORT IS A GUARD INTERVAL?

*One thousandth of a second is the smallest time differential we measure in competitive sports.*

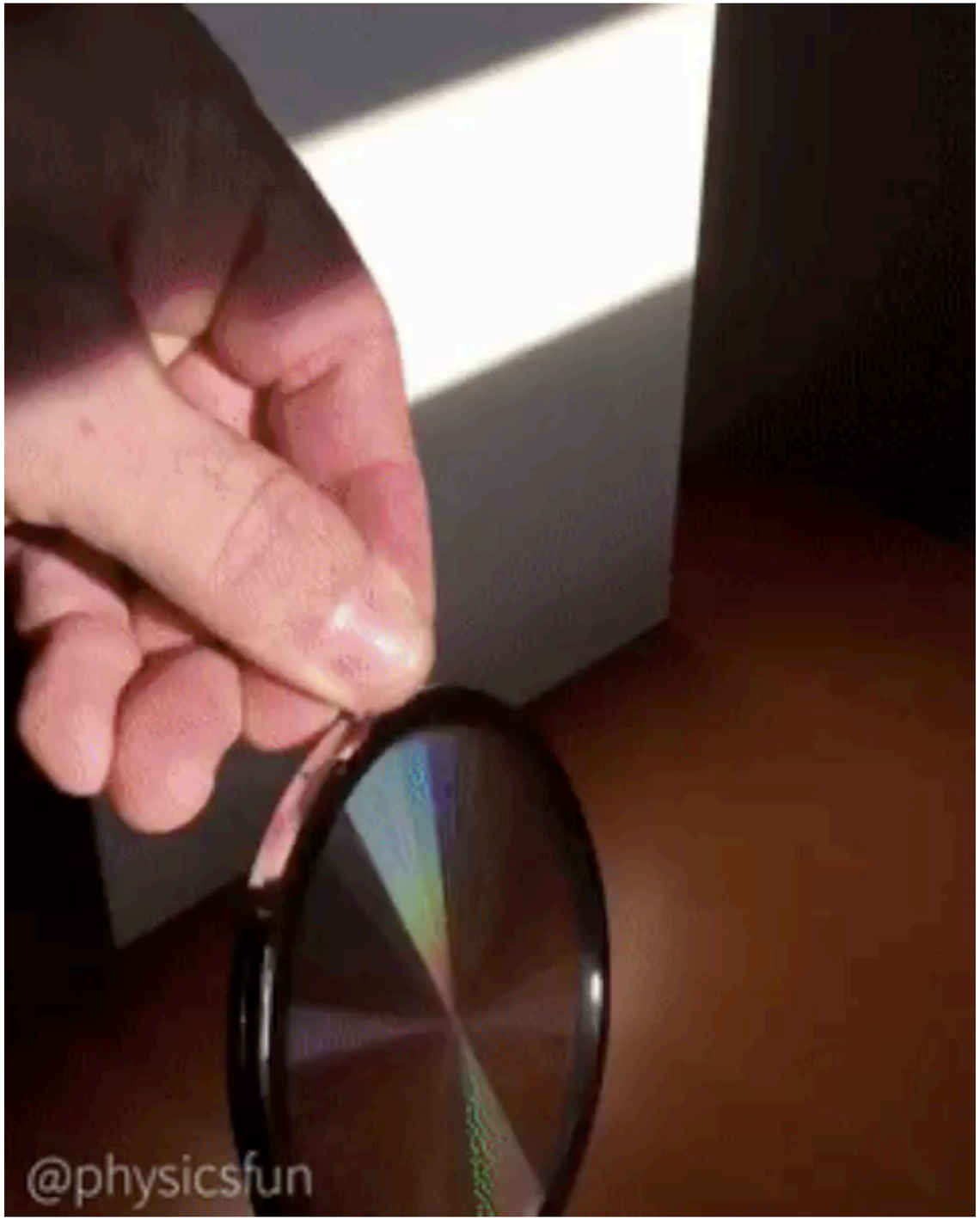
*That's still 250 symbol periods*

*That's 1,250 long guard intervals*

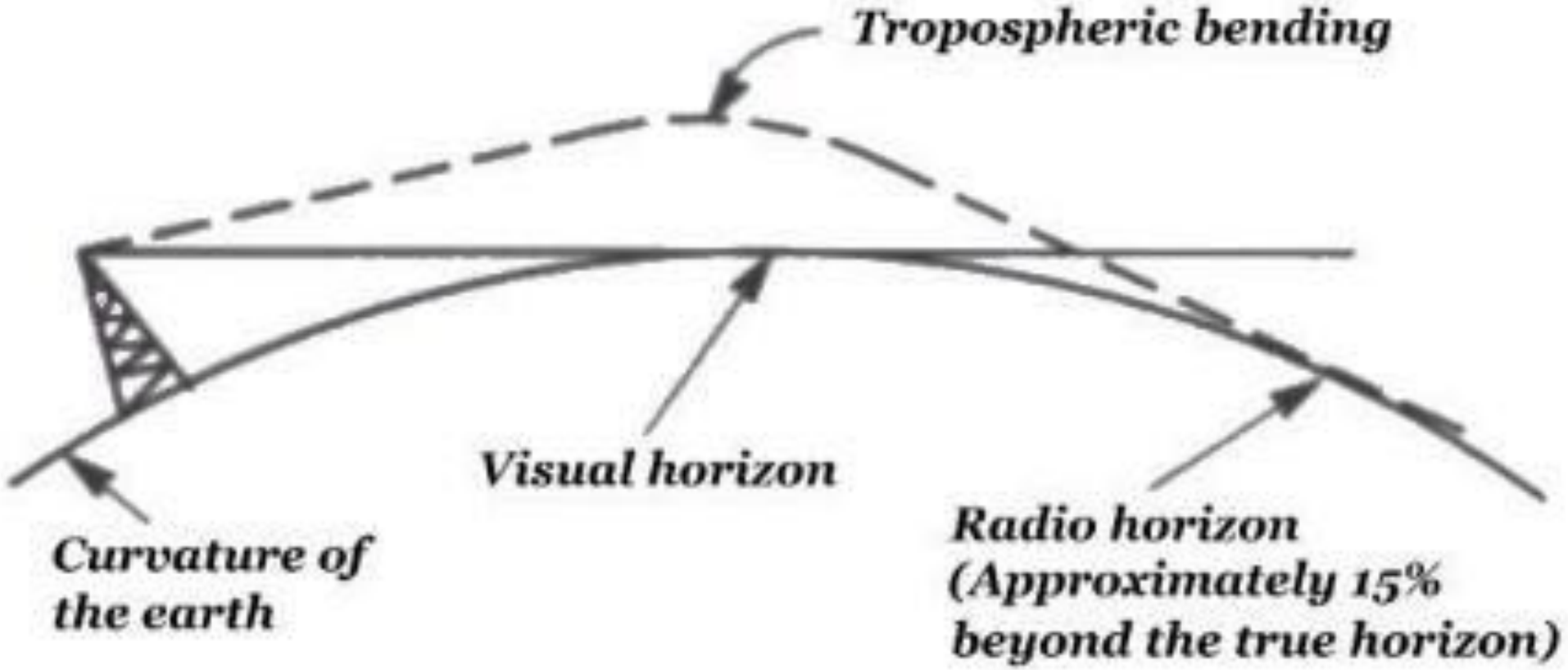
*That's 2,500 short guard intervals*

# RADIO-SPECIFIC PROBLEMS

# DIFFRACTION


@physicsfun

# REFRACTION


Tropospheric bending
Visual horizon
Curvature of the earth
Radio horizon (Approximately 15% beyond the true horizon)

# REFLECTION

# ABSORPTION

# INTERFERENCE

# SCATTERING

# ATTENUATION

# DON'T WORRY, THERE'S ONLY THIRTY MORE SLIDES NOW