# Lecture 10
# WiFi PHY

CS397/497 – Wireless Protocols for IoT

Branden Ghena – Winter 2023

Materials in collaboration with Pat Pannuto (UCSD)

# Administrivia

- Lab: Thread
  - Due Friday by end-of-day

- Hw: Matter
  - Renamed from Hw: Mesh, focus on understanding application clusters
  - Should be out today??
  - Won't be due until next week, since it was delayed

- See Piazza post with IoT companies
  - If you're looking for ideas to search for possible jobs
  - No idea about the real opportunities available right now

# Today's Goals

- Discuss WiFi physical layers
  - Get a feel for what choices are leading to more throughput
  - Think a little about what the costs of that are

# Outline

- **WiFi Overview**
- WiFi PHY
  - 802.11/802.11b
  - 802.11a/802.11g
  - 802.11n/802.11ac
  - 802.11ax
  - Real-World WiFi

# What is WiFi?

# What is WiFi?

(That title is a joke. Even my grandparents know what WiFi is.)

**WiFi is the most successful wireless protocol.**

# What is WiFi?

- Most successful wireless protocol (family)

- Small Area (~35m), high performance (up to 9,600 Mbit/s)

- ~30 years young
  - We'll do some history
  - Note the parallels in technology development
    - First: Maximize the performance of a single channel
    - Now: Improve performance through parallelism (more channels working together)

# 802.11 timeline

- 1985 – US FCC rules ISM band for unlicensed use
- 1990s – WaveLAN (NCR Corporation, Netherlands)
  - Wireless ethernet for cashier systems
- 1997 – 802.11 specification
- 1999 – 802.11b and 802.11a amendments
- 1999 – WiFi Alliance formed for certification of devices
- 1999 – Apple iBook is the first consumer WiFi product

# Major amendments

| | Protocol | Year | Frequency | PHY | Max Rate | Range |
|---|---|---|---|---|---|---|
| - | 802.11 | 1997 | 2.4 GHz | DSSS/FHSS | 2 Mbps | 20 m |
| 1 | 802.11b | 1999 | 2.4 GHz | DSSS | 11 Mbps | 35 m |
| 2 | 802.11a | 1999 | 5 GHz | OFDM | 54 Mbps | 35 m |
| 3 | 802.11g | 2003 | 2.4 GHz | OFDM | 54 Mbps | 38 m |
| 4 | 802.11n | 2009 | 2.4/5 GHz | OFDM + MIMO | 600 Mbps | 70 m |
| 5 | 802.11ac | 2013 | 5 GHz | OFDM + MU-MIMO (downlink only) | 3.4 Gbps | 35 m |
| 6 | 802.11ax | 2021 | 2.4/5/[6] GHz | OFDMA + MU-MIMO | 9.6 Gbps | 35 m |
| 7 | 802.11be | TBA | 2.4/5/6 GHz | OFDMA + MU-MIMO | 40 Gbps | 35 m |

- 802.11b was very popular but is now usually unsupported
- 802.11a never saw major deployment

- WiFi Alliance rebranded 802.11ac as “WiFi 5” and backported scheme

# Resources

- Peter Steenkiste – Carnegie Mellon University
  - https://www.cs.cmu.edu/~prs/wirelessS18/handouts/L11-AdHoc.pdf
  - https://www.cs.cmu.edu/~prs/wirelessS18/handouts/L12-LAN.pdf

- Raj Jain – Washington University in Saint Louis
  - https://www.cse.wustl.edu/~jain/cse574-14/ftp/j_05lan.pdf
  - https://www.cse.wustl.edu/~jain/cse574-14/ftp/j_06lan.pdf

- Honestly
  - https://en.wikipedia.org/wiki/IEEE_802.11

# Outline

- **WiFi Overview**

- **WiFi PHY**
  - 802.11/802.11b
  - 802.11a/802.11g
  - 802.11n/802.11ac
  - 802.11ax

  - Real-World WiFi

# WiFi Physical Layer

- Details start to get pretty messy here for multiple reasons:

1. Different countries/regions have different standards
   - Channels look a little different in different areas

2. WiFi has evolved over the last 20 years
   - Different features are designed for different amendments

3. WiFi is focused on improving throughput
   - Solutions that were initially "too complicated" no longer are

# Goal: improve throughput

- In twenty years, WiFi has gone from 2 Mbps to 9.6 Gbps
- **How does a network PHY improve its throughput?**

# Goal: improve throughput

- In twenty years, WiFi has gone from 2 Mbps to 9.6 Gbps
- **How does a network PHY improve its throughput?**

1. More capable modulation and/or bit transmission
   - Techniques like OFDM and MIMO

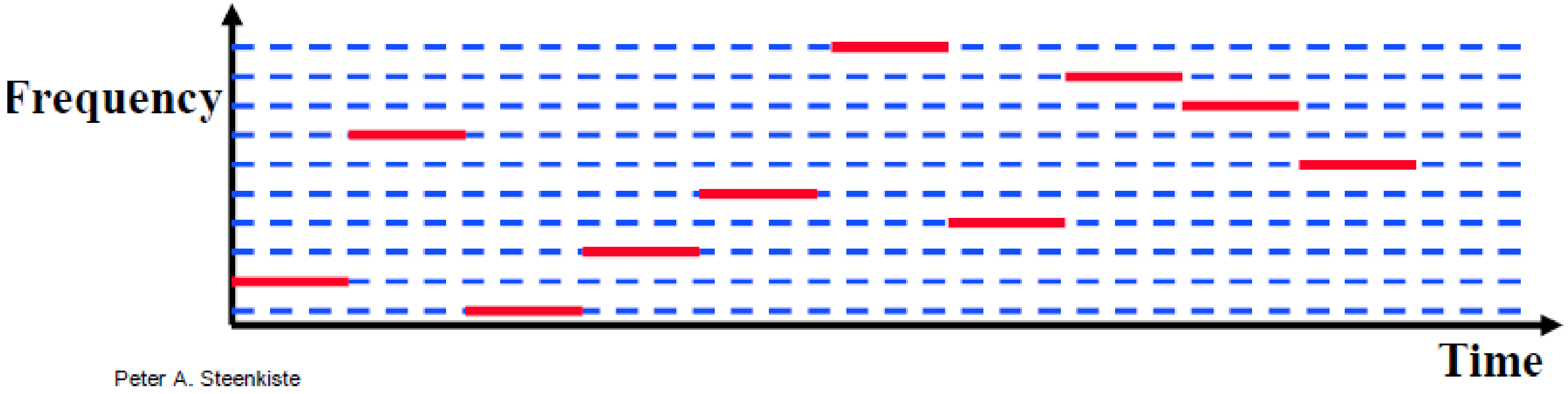
2. More bandwidth
   - Increased channel with at 2.4 Ghz and bigger 5 GHz channels

# Walking through PHY changes by amendment

| | Protocol | Year | Frequency | PHY | Max Rate | Range |
|---|---|---|---|---|---|---|
| - | **802.11** | 1997 | 2.4 GHz | DSSS/FHSS | 2 Mbps | 20 m |
| 1 | **802.11b** | 1999 | 2.4 GHz | DSSS | 11 Mbps | 35 m |
| 2 | 802.11a | 1999 | 5 GHz | OFDM | 54 Mbps | 35 m |
| 3 | 802.11g | 2003 | 2.4 GHz | OFDM | 54 Mbps | 38 m |
| 4 | 802.11n | 2009 | 2.4/5 GHz | OFDM + MIMO | 600 Mbps | 70 m |
| 5 | 802.11ac | 2013 | 5 GHz | OFDM + MU-MIMO | 3.4 Gbps | 35 m |
| 6 | 802.11ax | 2021 | 2.5/5/[6] GHz | OFDMA + MU-MIMO | 9.6 Gbps | 35 m |
| 7 | 802.11be | TBA | 2.5/5/6 GHz | OFDMA + MU-MIMO | 40 Gbps | 35 m |

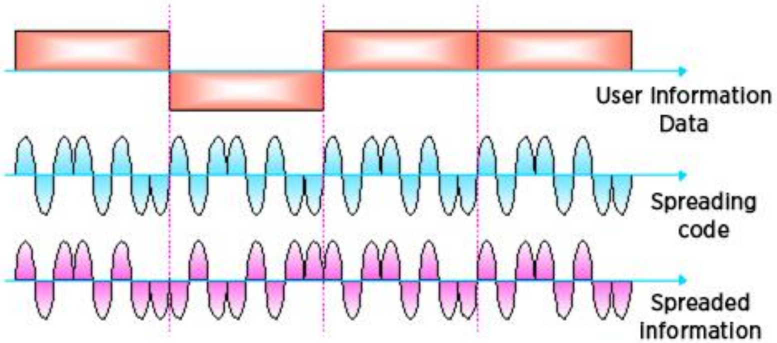
# Original WiFi specification (1997)

- Legacy WiFi
  - Frequency Hopping Spread Spectrum (FHSS)
  - GFSK (Gaussian Frequency-Shift Keying)
    - Relatively simple radio design
  - Frequency hopping over 80 channels (1 MHz each)
  - Actually supports an Infrared PHY as well!!

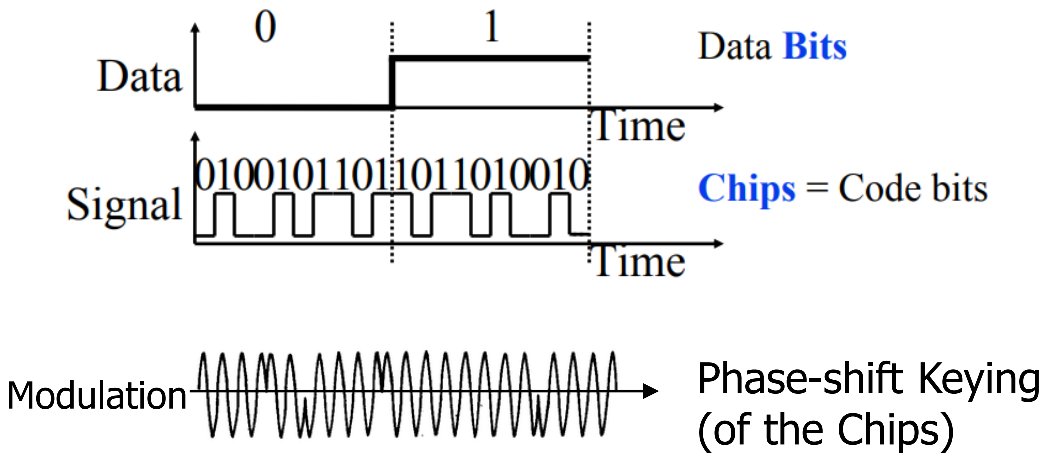


# 802.11b (1999)

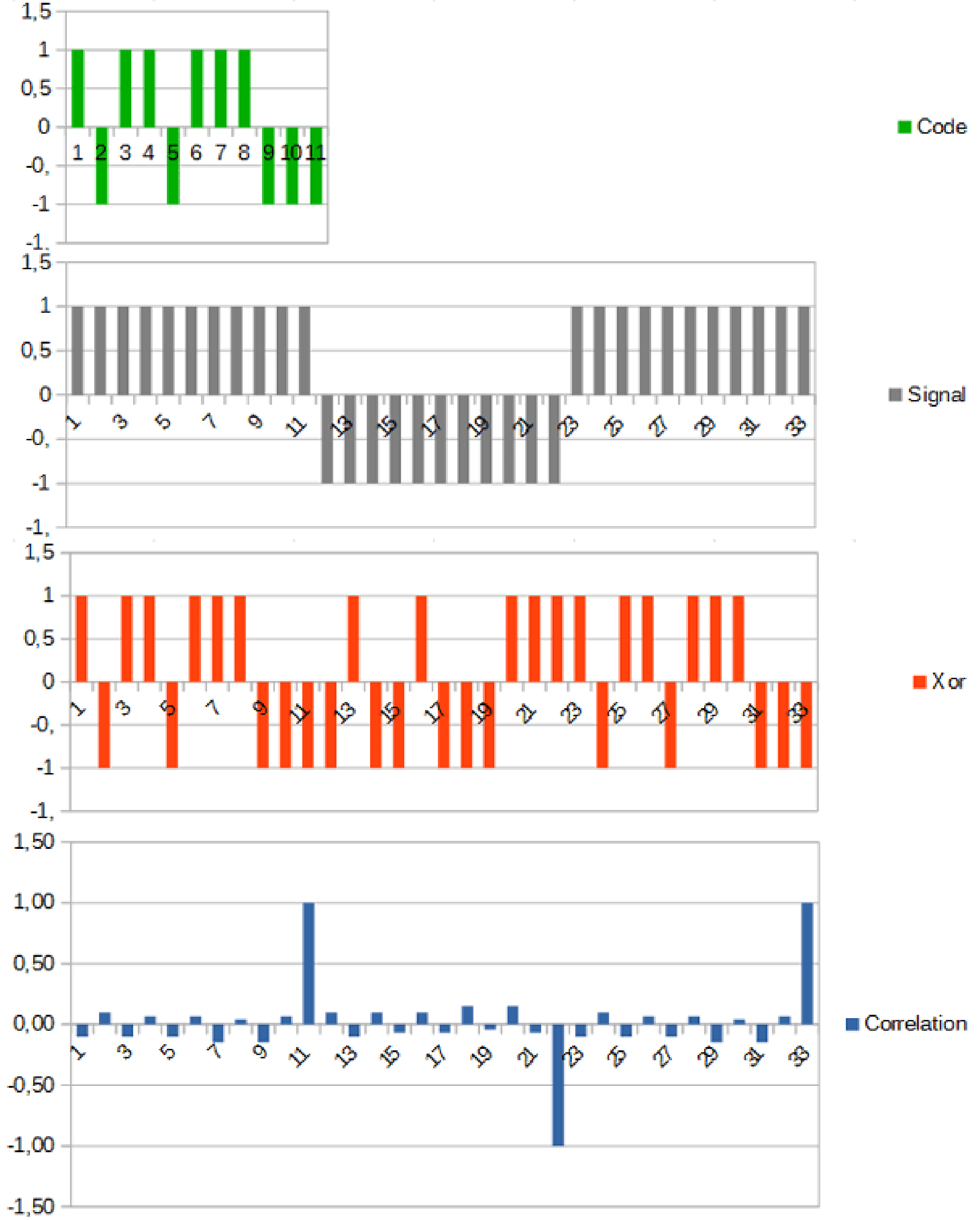
- 802.11b
  - Direct Sequence Spread Spectrum (DSSS)
  - DBPSK and DQPSK (Differential Binary/Quadrature Phase-Shift Keying)



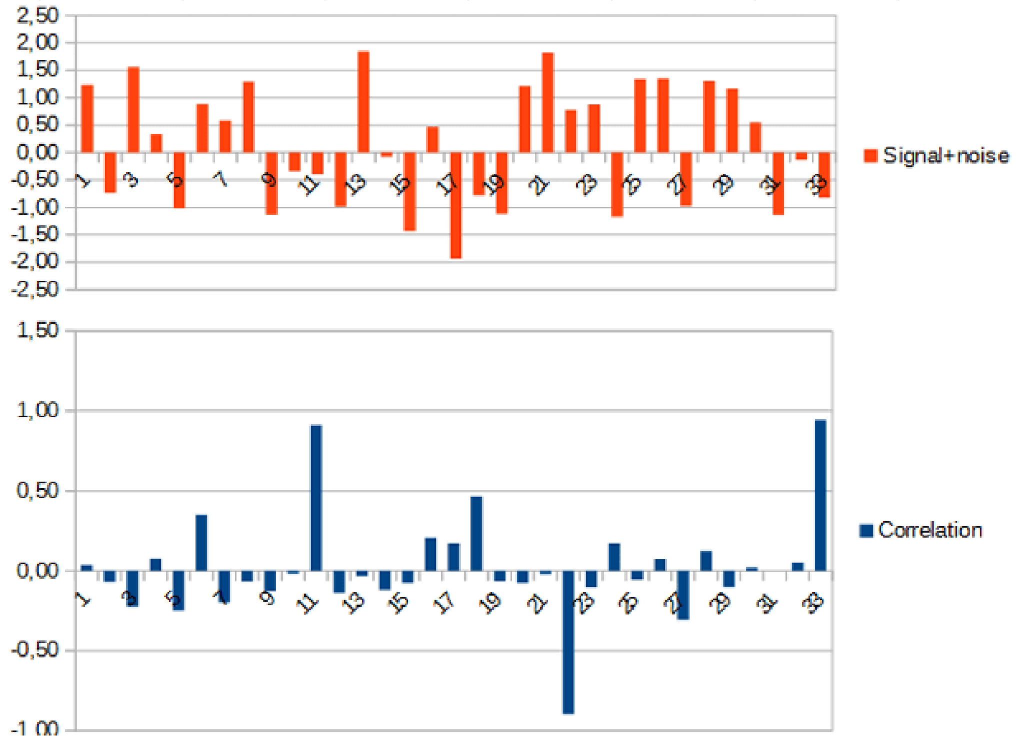

- Translate data into "codes"
  - Each data bit corresponds to several code bits (Chips)
  - Chips are what is actually modulated over the air
  - Data can be recovered by knowing the code patterns



# DSSS example from 802.15.4



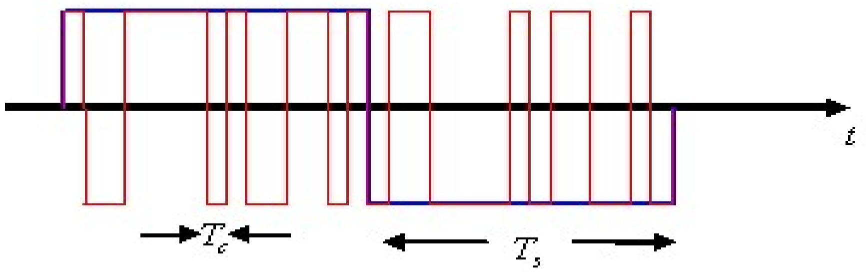

- Data sent is **101**
  - Code is longer than data, so we replicate bits
  - Data is recoverable, even with noise



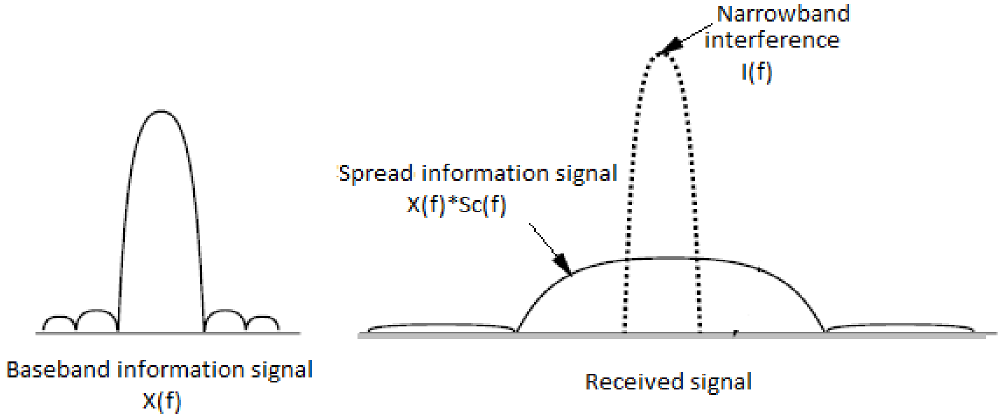

https://circuitcellar.com/research-design-hub/dsss-in-a-nutshell/

# DSSS goals

- DSSS increases bandwidth of a signal
  - Beyond what is needed for the data
  - Energy is smeared across the frequencies



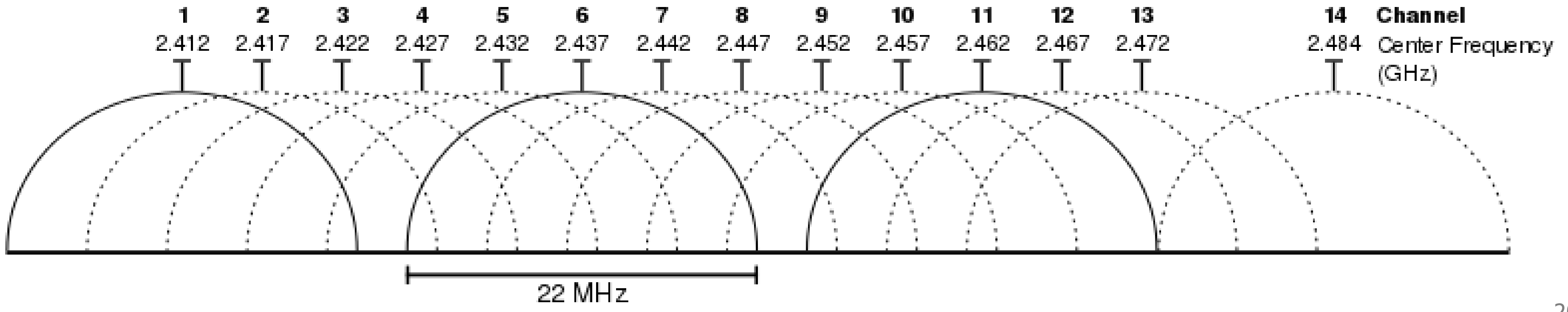

- More robust against interference
  - Narrowband signals knock out only part of the signal
  - Data can be recovered from partial code




- Cost: using a lot of bandwidth for only a little data

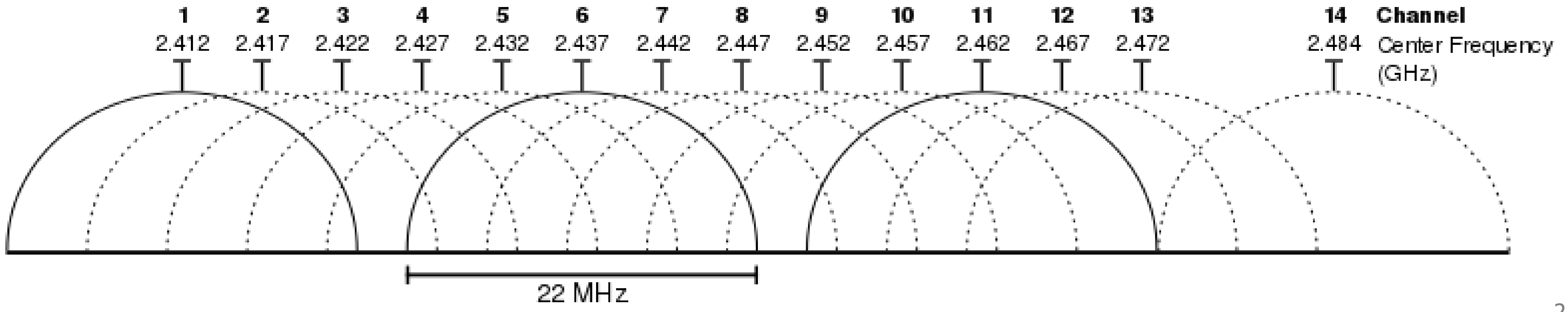
# 802.11b channels

- 14 channels total
  - 1-11 for US
  - 1-13 for most of the rest of the world
  - 1-14 for Japan (but 14 only for 802.11b)
- 22 MHz channels
  - 5 MHz spacing -> significant channel overlap
  - Channels 1, 6, and 11 can be used without overlap



# Break + Question

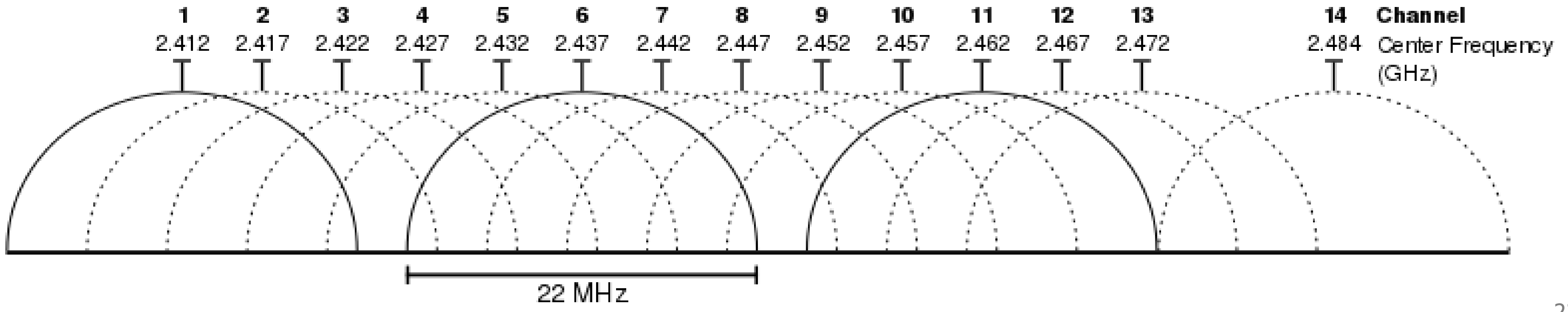
- If the majority of channels overlap, why even have them?



# Break + Question

- If the majority of channels overlap, why even have them?
  - Different options for different regions
  - Inside US use three channels: 1, 6, 11
  - Outside of North America can use four channels: 1, 5, 9, 13

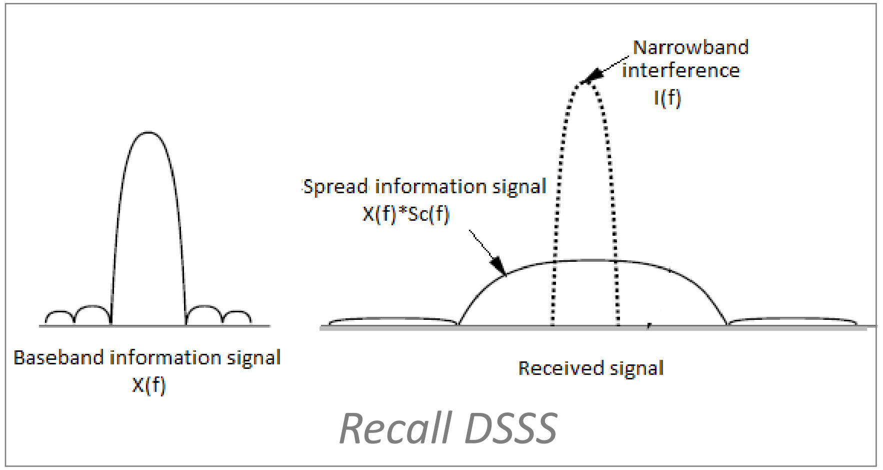
  - Historical: avoid other 2.4 GHz users
    - If they're at the low end of the band, you could switch to channel 2 or 3



# Walking through PHY changes by amendment

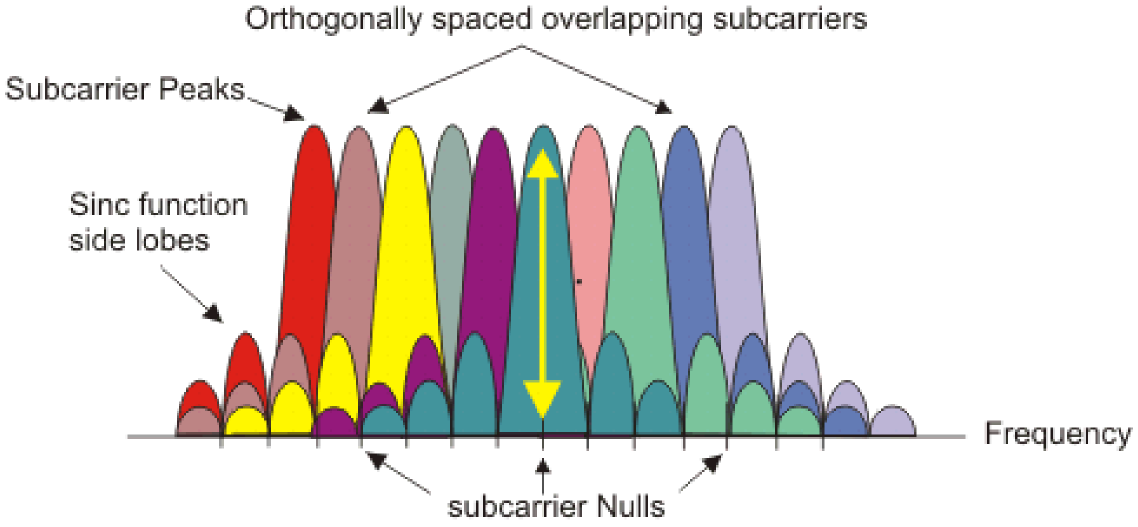
| | Protocol | Year | Frequency | PHY | Max Rate | Range |
|---|---|---|---|---|---|---|
| - | 802.11 | 1997 | 2.4 GHz | DSSS/FHSS | 2 Mbps | 20 m |
| 1 | 802.11b | 1999 | 2.4 GHz | DSSS | 11 Mbps | 35 m |
| 2 | **802.11a** | 1999 | 5 GHz | OFDM | 54 Mbps | 35 m |
| 3 | 802.11g | 2003 | 2.4 GHz | OFDM | 54 Mbps | 38 m |
| 4 | 802.11n | 2009 | 2.4/5 GHz | OFDM + MIMO | 600 Mbps | 70 m |
| 5 | 802.11ac | 2013 | 5 GHz | OFDM + MU-MIMO | 3.4 Gbps | 35 m |
| 6 | 802.11ax | 2021 | 2.5/5/[6] GHz | OFDMA + MU-MIMO | 9.6 Gbps | 35 m |
| 7 | 802.11be | TBA | 2.5/5/6 GHz | OFDMA + MU-MIMO | 40 Gbps | 35 m |

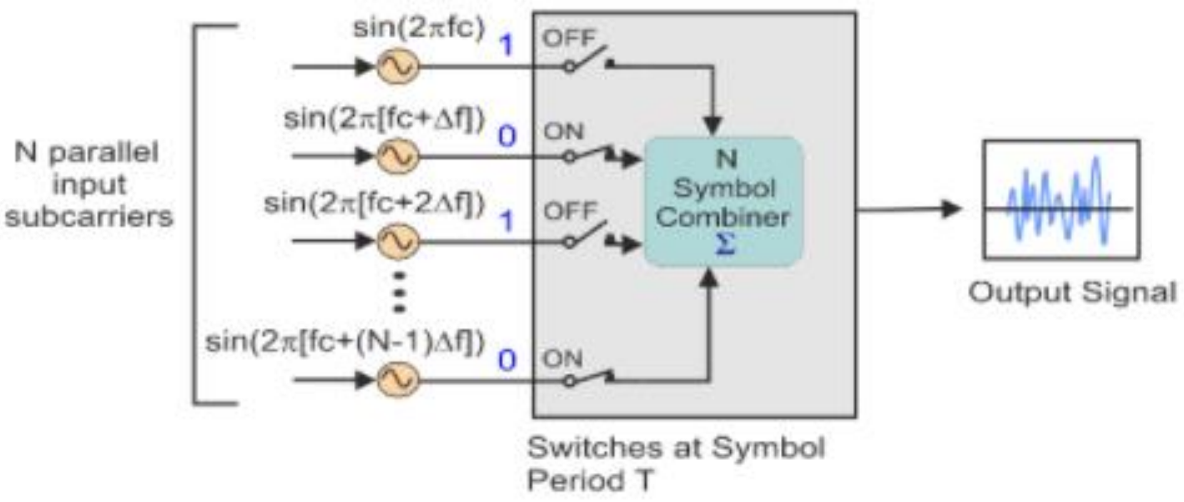
# OFDM enables higher throughput




- Replace DSSS with
  Orthogonal Frequency Division Multiplexing

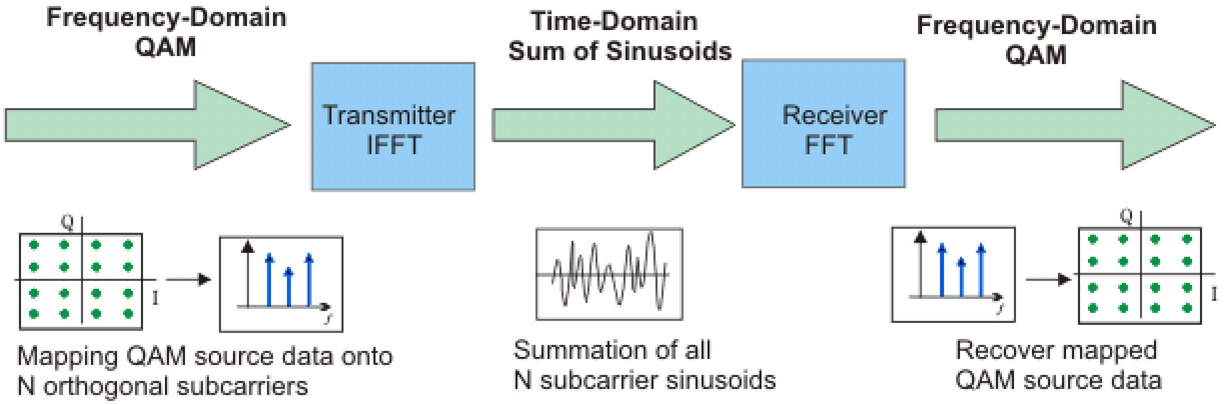
- OFDM idea
  - Split band into a number of narrow subcarriers
  - Subcarriers are spaced so that they don't interfere
  - Transmit on multiple subcarriers at once to increase throughput



# OFDM enables higher throughput at complexity cost

- Receivers collect signal from entire channel
  - And then can split it apart to gain the data on each subcarrier




- Tradeoffs
  - Benefits: more throughput, still robust against narrowband interference
  - Costs: more complicated and sensitive radio design

# 802.11a (1999)

- Applied OFDM techniques on the 5 GHz band
  - Enabled more data throughput 54 Mbps (compare to 11 Mbps for 802.11b)

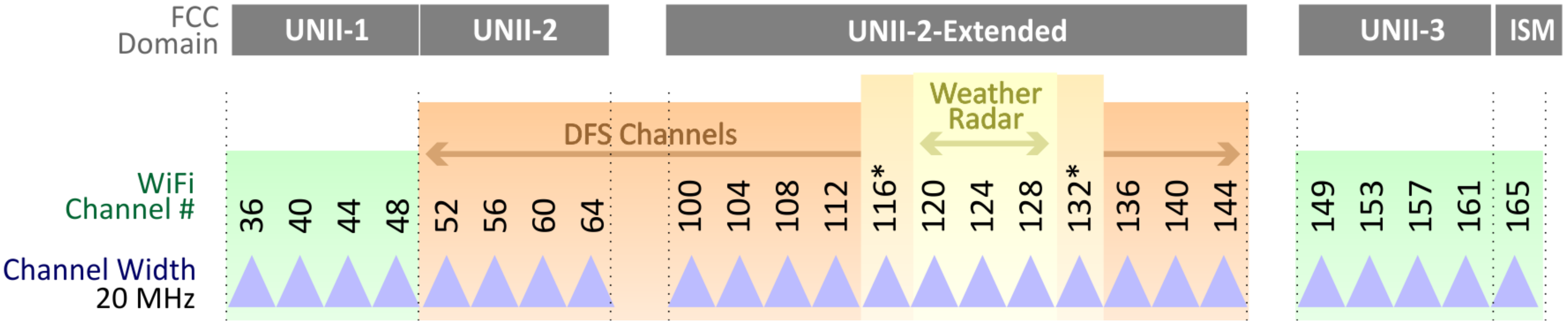
- Multiple rates available
  - BPSK/QPSK/QAM over OFDM
  - Quadrature Amplitude Modulation (QAM)

- Never reached widespread adoption
  - Regulatory hurdles in some regions
  - More complicated hardware delayed it

| RATE bits | Modulation type | Coding rate | Data rate (Mbit/s)[a] |
|---|---|---|---|
| 1101 | BPSK | 1/2 | 6 |
| 1111 | BPSK | 3/4 | 9 |
| 0101 | QPSK | 1/2 | 12 |
| 0111 | QPSK | 3/4 | 18 |
| 1001 | 16-QAM | 1/2 | 24 |
| 1011 | 16-QAM | 3/4 | 36 |
| 0001 | 64-QAM | 2/3 | 48 |
| 0011 | 64-QAM | 3/4 | 54 |

# 802.11a channels

- 802.11a did promote the use of 5 GHz band
  - Several 20 MHz channels with no overlap (9ish in the US)
    - Big increase from “three” channels of 2.4 GHz
  - Various regional rules on a number of different channels
    - Needs to avoid frequencies in use by existing radar deployments
    - Orange channels aren’t usually used in the US at least



# Walking through PHY changes by amendment

| | Protocol | Year | Frequency | PHY | Max Rate | Range |
|---|---|---|---|---|---|---|
| - | 802.11 | 1997 | 2.4 GHz | DSSS/FHSS | 2 Mbps | 20 m |
| 1 | 802.11b | 1999 | 2.4 GHz | DSSS | 11 Mbps | 35 m |
| 2 | 802.11a | 1999 | 5 GHz | OFDM | 54 Mbps | 35 m |
| 3 | **802.11g** | 2003 | 2.4 GHz | OFDM | 54 Mbps | 38 m |
| 4 | 802.11n | 2009 | 2.4/5 GHz | OFDM + MIMO | 600 Mbps | 70 m |
| 5 | 802.11ac | 2013 | 5 GHz | OFDM + MU-MIMO | 3.4 Gbps | 35 m |
| 6 | 802.11ax | 2021 | 2.5/5/[6] GHz | OFDMA + MU-MIMO | 9.6 Gbps | 35 m |
| 7 | 802.11be | TBA | 2.5/5/6 GHz | OFDMA + MU-MIMO | 40 Gbps | 35 m |

# 802.11g (2003)

- Applies OFDM to 2.4 GHz band
  - Increases throughput from 11 Mbps to 54 Mbps
  - Repeats rate choices of 802.11a but on more support 2.4 GHz band

- Same 2.4 GHz channels as 802.11b, but 20 MHz bandwidth
  - Still 1, 6, 11 in US
  - 1, 5, 9, 13 in other regions

- Backwards compatible with 802.11b
  - Capable of DSSS communication when required

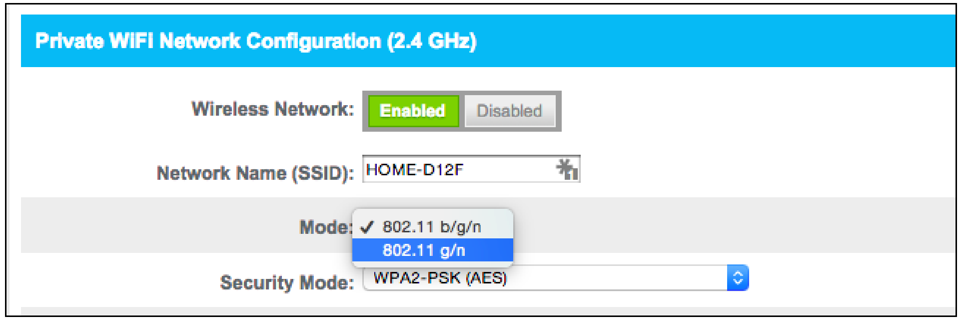
# Cost of supporting 802.11b

- 802.11g uses a completely different PHY layer than 802.11b
  - DSSS -> OFDM
  - Unintelligible to old receivers creating an interoperability problem

- Interoperability mode: send part of message in old format
  - DSSS header with OFDM payload
  - Adds overhead and slows down the entire network
    - Starting with 802.11n, routers don’t support 802.11b by default

# Truth or Fiction:
# "An 802.11b device slows your whole network to b speed"

- Aka, should you have followed all the blogs telling you to do this?:




- A: "Sort of", and "no"
  - When *active*, **b** devices slow networks simply because they occupy the channel
  - Cutting off your **b** devices doesn't cut off your neighbor's
    - *Contention* [without coordination] is the bigger problem
  - On own network, routers are "**b**-aware", and can schedule around efficiently
    - At cost of "talking **b**" to everyone a little

# Improved WiFi hardware is in high demand

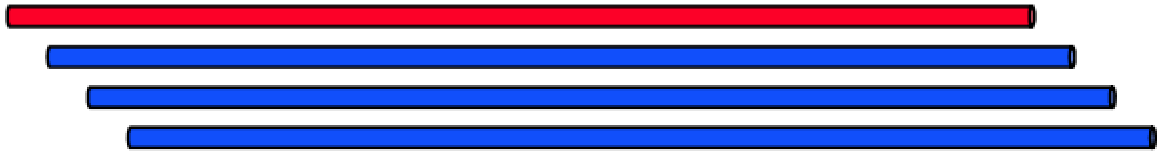
- Typically, standards lead hardware by several years
  - BLE 5.2 is out, but 5.0 is just being adopted in phones
- Development of 802.11g hardware started *before* finalization of standard
  - Demand for increased performance was already high in 2003
- Phenomena continues in modern WiFi and Cellular protocols
  - Hardware supports some features as soon as it’s clear they’ll exist

# Walking through PHY changes by amendment

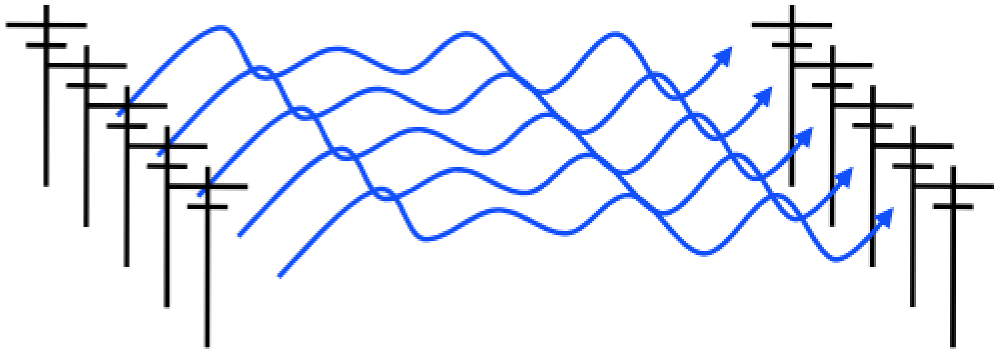
| | Protocol | Year | Frequency | PHY | Max Rate | Range |
|---|---|---|---|---|---|---|
| - | 802.11 | 1997 | 2.4 GHz | DSSS/FHSS | 2 Mbps | 20 m |
| 1 | 802.11b | 1999 | 2.4 GHz | DSSS | 11 Mbps | 35 m |
| 2 | 802.11a | 1999 | 5 GHz | OFDM | 54 Mbps | 35 m |
| 3 | 802.11g | 2003 | 2.4 GHz | OFDM | 54 Mbps | 38 m |
| 4 | **802.11n** | 2009 | 2.4/5 GHz | OFDM + MIMO | 600 Mbps | 70 m |
| 5 | 802.11ac | 2013 | 5 GHz | OFDM + MU-MIMO | 3.4 Gbps | 35 m |
| 6 | 802.11ax | 2021 | 2.5/5/[6] GHz | OFDMA + MU-MIMO | 9.6 Gbps | 35 m |
| 7 | 802.11be | TBA | 2.5/5/6 GHz | OFDMA + MU-MIMO | 40 Gbps | 35 m |

# How do we increase throughput?

- Wired world
  - Add more wires in parallel

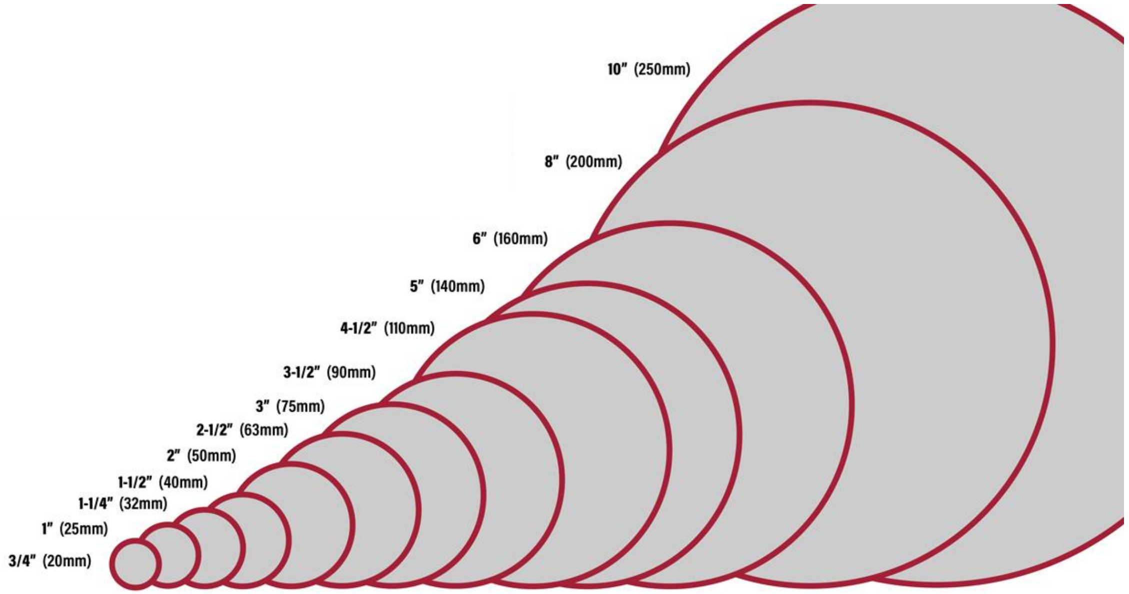


- Wireless world
  - Add more antennas?



# How do we increase throughput?

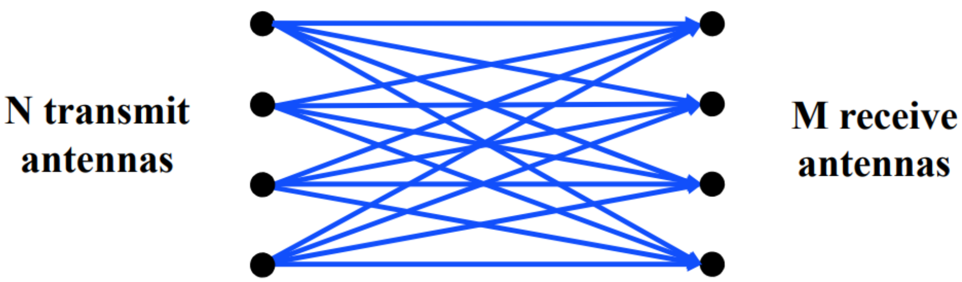
- Water world
  - Fatter pipes




- Wireless world
  - Fatter channels
    (with more bandwidth)

***802.11.n — Y NOT BOTH?***

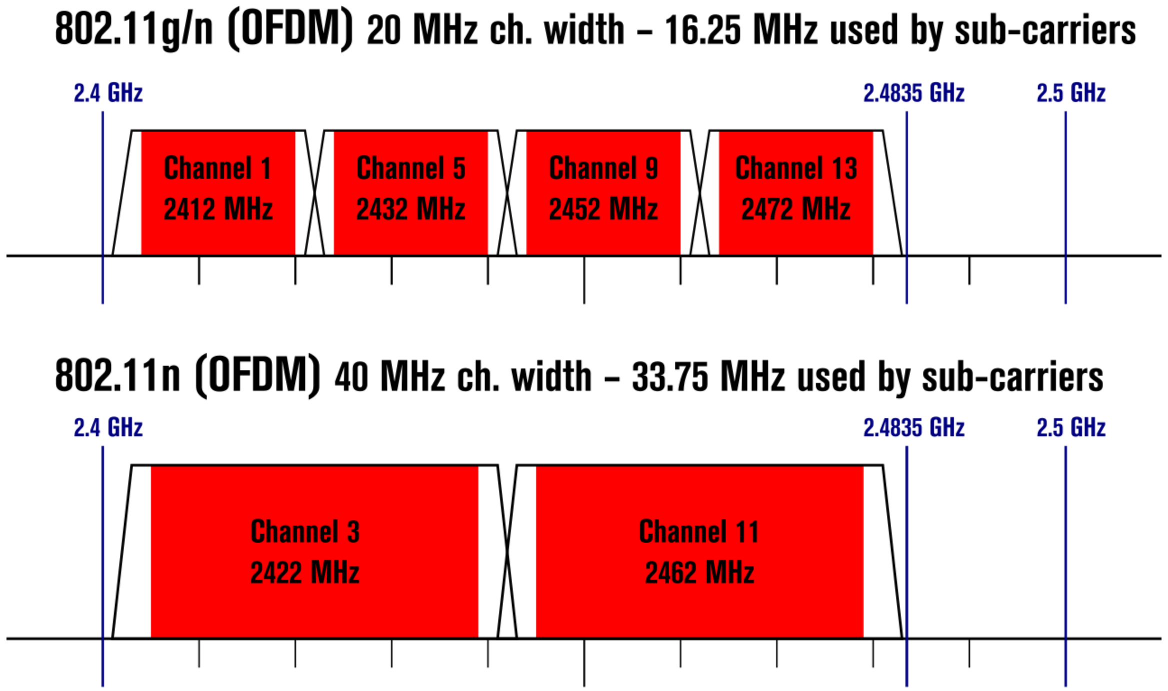
# MIMO – Multiple In Multiple Out




- N x M subchannels can be used to send data simultaneously
  - Huge boost in data throughput
  - Antenna diversity adds to reliability as well
- The signals may interfere with each other
  - But receiving all of them allows the data to be recovered
- Beamforming
  - Use interactions between array of antennas to focus energy on the receiver
  - Way outside of the scope of this class

# Expandable bandwidth

- OFDM allows many subcarriers within a channel to be used at once
  - Throughput scales with the amount of bandwidth available
  - Allow larger 40 MHz channels to be used



# 802.11n (2009)

- Supports OFDM and MIMO on 2.4 GHz and 5 GHz

- Supports 20 MHz and 40 MHz channels
  - Easier to create large channels in 5 GHz band

- Backwards compatible with 802.11g (tries not to be with 802.11b)

- Wildly successful
  - Still the 2.4 GHz band protocol (802.11ac is 5 GHz only)
  - A little less than half of the networks visible to me are still 802.11n
  - My apartment “building WiFi” is still 802.11g…

# 802.11n modulation and coding schemes

Modulation and coding schemes

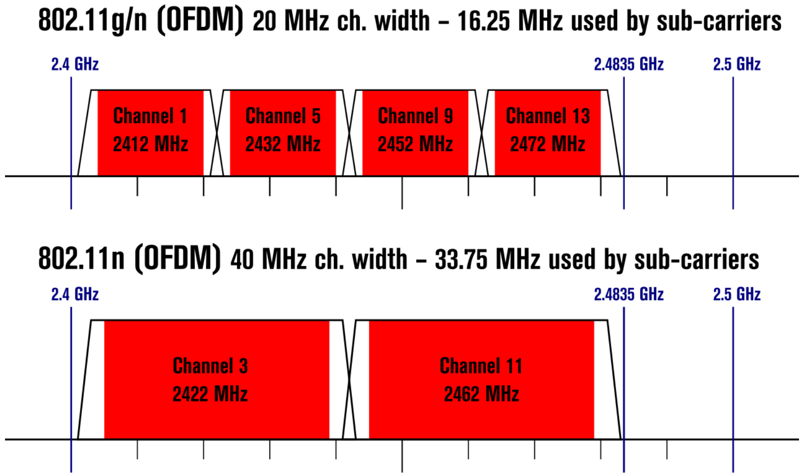
| MCS index | Spatial streams | Modulation type | Coding rate | Data rate (in Mbit/s)[a] | | | |
|---|---|---|---|---|---|---|---|
| | | | | 20 MHz channel | | 40 MHz channel | |
| | | | | 800 ns GI | 400 ns GI | 800 ns GI | 400 ns GI |
| 0 | 1 | BPSK | 1/2 | 6.5 | 7.2 | 13.5 | 15 |
| 1 | 1 | QPSK | 1/2 | 13 | 14.4 | 27 | 30 |
| 2 | 1 | QPSK | 3/4 | 19.5 | 21.7 | 40.5 | 45 |
| 3 | 1 | 16-QAM | 1/2 | 26 | 28.9 | 54 | 60 |
| 4 | 1 | 16-QAM | 3/4 | 39 | 43.3 | 81 | 90 |
| 5 | 1 | 64-QAM | 2/3 | 52 | 57.8 | 108 | 120 |
| 6 | 1 | 64-QAM | 3/4 | 58.5 | 65 | 121.5 | 135 |
| 7 | 1 | 64-QAM | 5/6 | 65 | 72.2 | 135 | 150 |
| 8 | 2 | BPSK | 1/2 | 13 | 14.4 | 27 | 30 |
| 9 | 2 | QPSK | 1/2 | 26 | 28.9 | 54 | 60 |
| 10 | 2 | QPSK | 3/4 | 39 | 43.3 | 81 | 90 |
| 11 | 2 | 16-QAM | 1/2 | 52 | 57.8 | 108 | 120 |
| 12 | 2 | 16-QAM | 3/4 | 78 | 86.7 | 162 | 180 |
| 13 | 2 | 64-QAM | 2/3 | 104 | 115.6 | 216 | 240 |
| 14 | 2 | 64-QAM | 3/4 | 117 | 130 | 243 | 270 |
| 15 | 2 | 64-QAM | 5/6 | 130 | 144.4 | 270 | 300 |
| 16 | 3 | BPSK | 1/2 | 19.5 | 21.7 | 40.5 | 45 |
| 17 | 3 | QPSK | 1/2 | 39 | 43.3 | 81 | 90 |
| 18 | 3 | QPSK | 3/4 | 58.5 | 65 | 121.5 | 135 |
| 19 | 3 | 16-QAM | 1/2 | 78 | 86.7 | 162 | 180 |

| MCS index | Spatial streams | Modulation type | Coding rate | Data rate (in Mbit/s)[a] | | | |
|---|---|---|---|---|---|---|---|
| | | | | 20 MHz channel | | 40 MHz channel | |
| | | | | 800 ns GI | 400 ns GI | 800 ns GI | 400 ns GI |
| 20 | 3 | 16-QAM | 3/4 | 117 | 130 | 243 | 270 |
| 21 | 3 | 64-QAM | 2/3 | 156 | 173.3 | 324 | 360 |
| 22 | 3 | 64-QAM | 3/4 | 175.5 | 195 | 364.5 | 405 |
| 23 | 3 | 64-QAM | 5/6 | 195 | 216.7 | 405 | 450 |
| 24 | 4 | BPSK | 1/2 | 26 | 28.8 | 54 | 60 |
| 25 | 4 | QPSK | 1/2 | 52 | 57.6 | 108 | 120 |
| 26 | 4 | QPSK | 3/4 | 78 | 86.8 | 162 | 180 |
| 27 | 4 | 16-QAM | 1/2 | 104 | 115.6 | 216 | 240 |
| 28 | 4 | 16-QAM | 3/4 | 156 | 173.2 | 324 | 360 |
| 29 | 4 | 64-QAM | 2/3 | 208 | 231.2 | 432 | 480 |
| 30 | 4 | 64-QAM | 3/4 | 234 | 260 | 486 | 540 |
| 31 | 4 | 64-QAM | 5/6 | 260 | 288.8 | 540 | 600 |

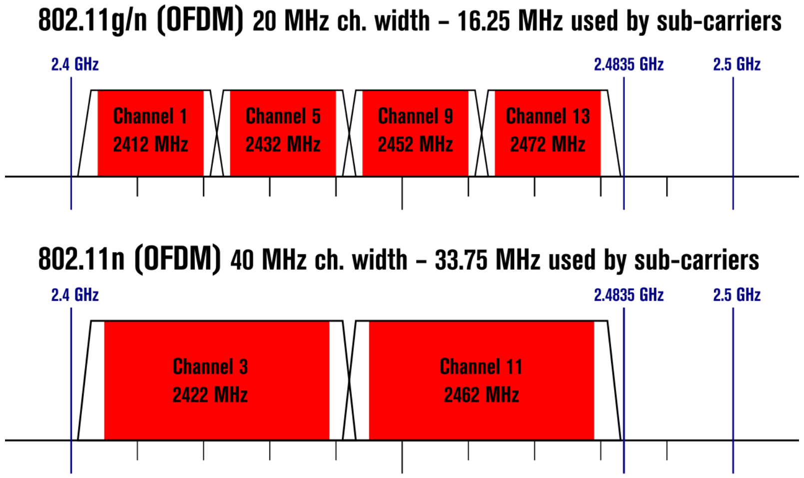
MCS – Modulation and Coding Scheme
GI – Guard Interval: delay between transmitted symbols

# Break + Open Question

- How much bandwidth is acceptable to use?
  - Is it okay for a WiFi network to use the entire 2.4 GHz spectrum?



# Break + Open Question




- How much bandwidth is acceptable to use?
  - Is it okay for a WiFi network to use the entire 2.4 GHz spectrum?

  - Maybe. At least the range is pretty short!
    - Only next-door neighbor's network interfere with your network
    - Someone further away isn't affected at all

  - Need to share with neighbors nearby though
    - Theoretically better to have separate allocations than to overlap and deal with the collisions

# Walking through PHY changes by amendment

| | Protocol | Year | Frequency | PHY | Max Rate | Range |
|---|---|---|---|---|---|---|
| - | 802.11 | 1997 | 2.4 GHz | DSSS/FHSS | 2 Mbps | 20 m |
| 1 | 802.11b | 1999 | 2.4 GHz | DSSS | 11 Mbps | 35 m |
| 2 | 802.11a | 1999 | 5 GHz | OFDM | 54 Mbps | 35 m |
| 3 | 802.11g | 2003 | 2.4 GHz | OFDM | 54 Mbps | 38 m |
| 4 | 802.11n | 2009 | 2.4/5 GHz | OFDM + MIMO | 600 Mbps | 70 m |
| 5 | **802.11ac** | 2013 | 5 GHz | OFDM + MU-MIMO | 3.4 Gbps | 35 m |
| 6 | 802.11ax | 2021 | 2.5/5/[6] GHz | OFDMA + MU-MIMO | 9.6 Gbps | 35 m |
| 7 | 802.11be | TBA | 2.5/5/6 GHz | OFDMA + MU-MIMO | 40 Gbps | 35 m |

# "The MIMO Gap"

- Access points have 3-4 [or more now] antennas
- Client devices have 1-2 [or more now] antennas
  - While absolute numbers keep going up, trend holds
  - **Asymmetric design pattern** again: More complexity in the AP than clients
- Original MIMO was one device at a time
- No expand to be multiple device simultaneously

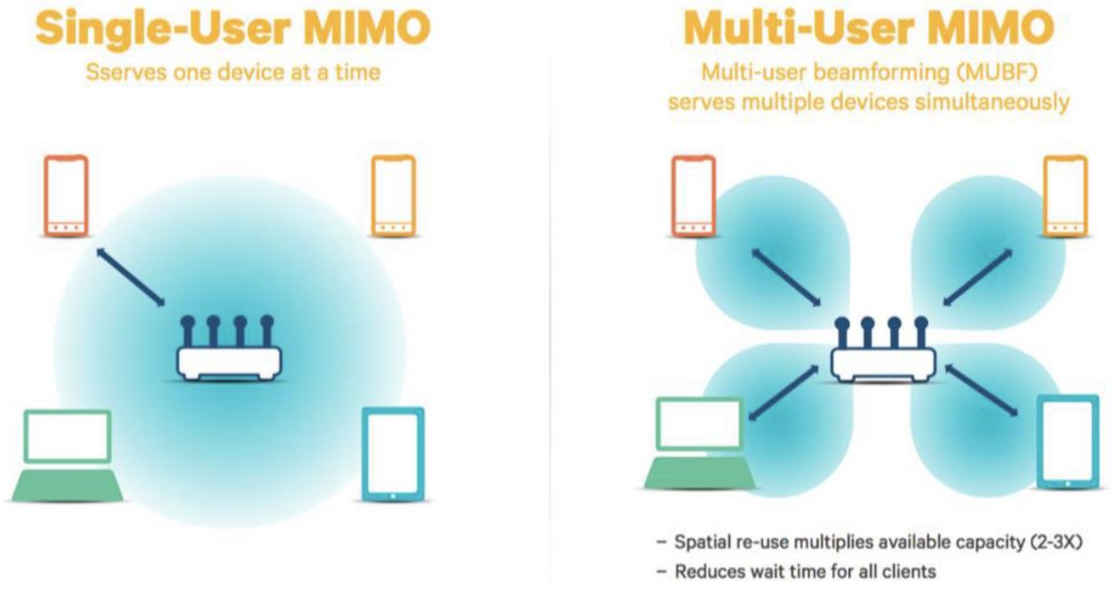
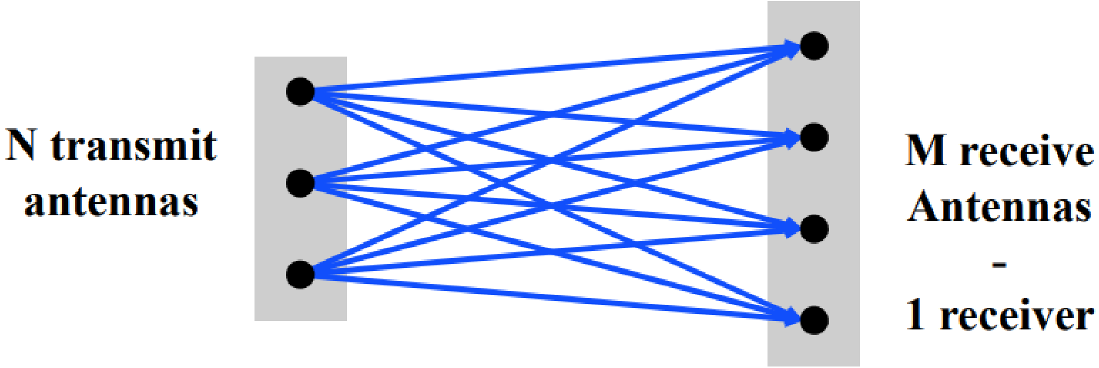
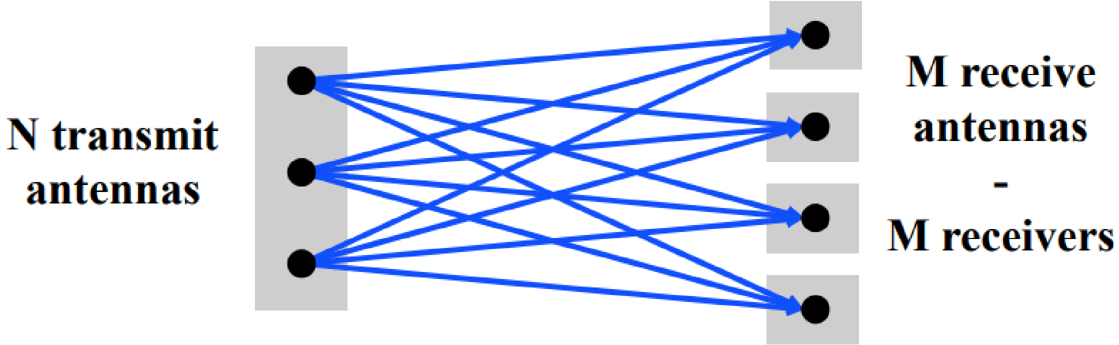



*Figure 1. SU-MIMO vs. MU-MIMO*

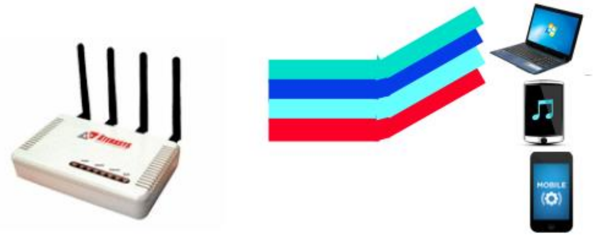
# Multi-user Multiple In Multiple Out (MU-MIMO)

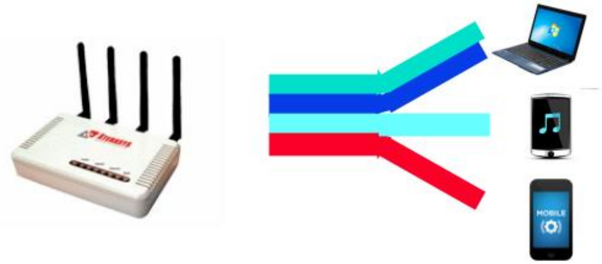



How is this Different?

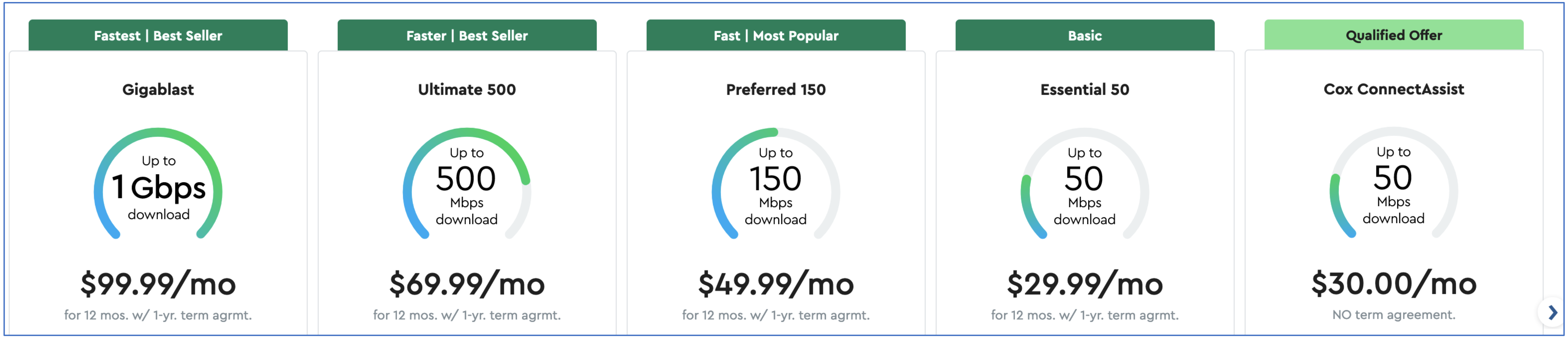


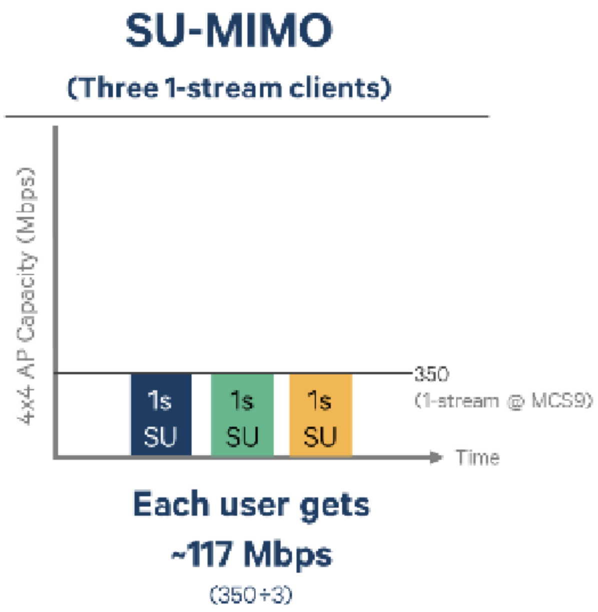

- Multi-user MIMO uses the same techniques to send in parallel to multiple devices
  - Devices cannot cancel out interference anymore
  - Send slower, more reliable data streams to overcome this

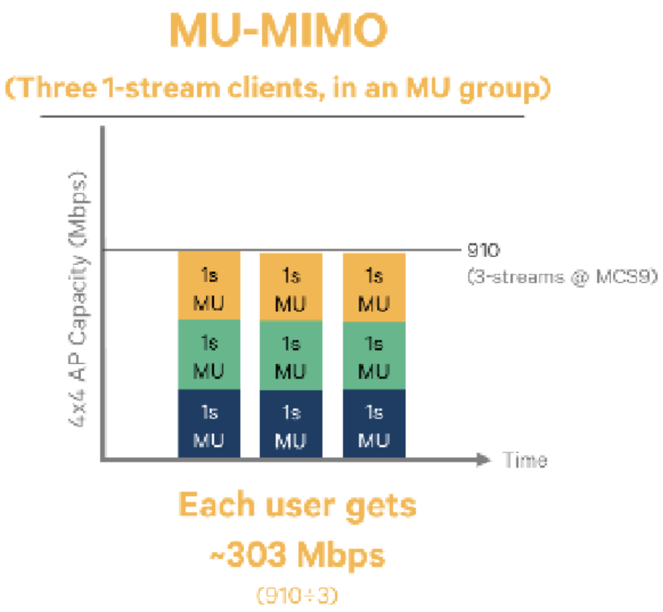




# How much data can a single device use?



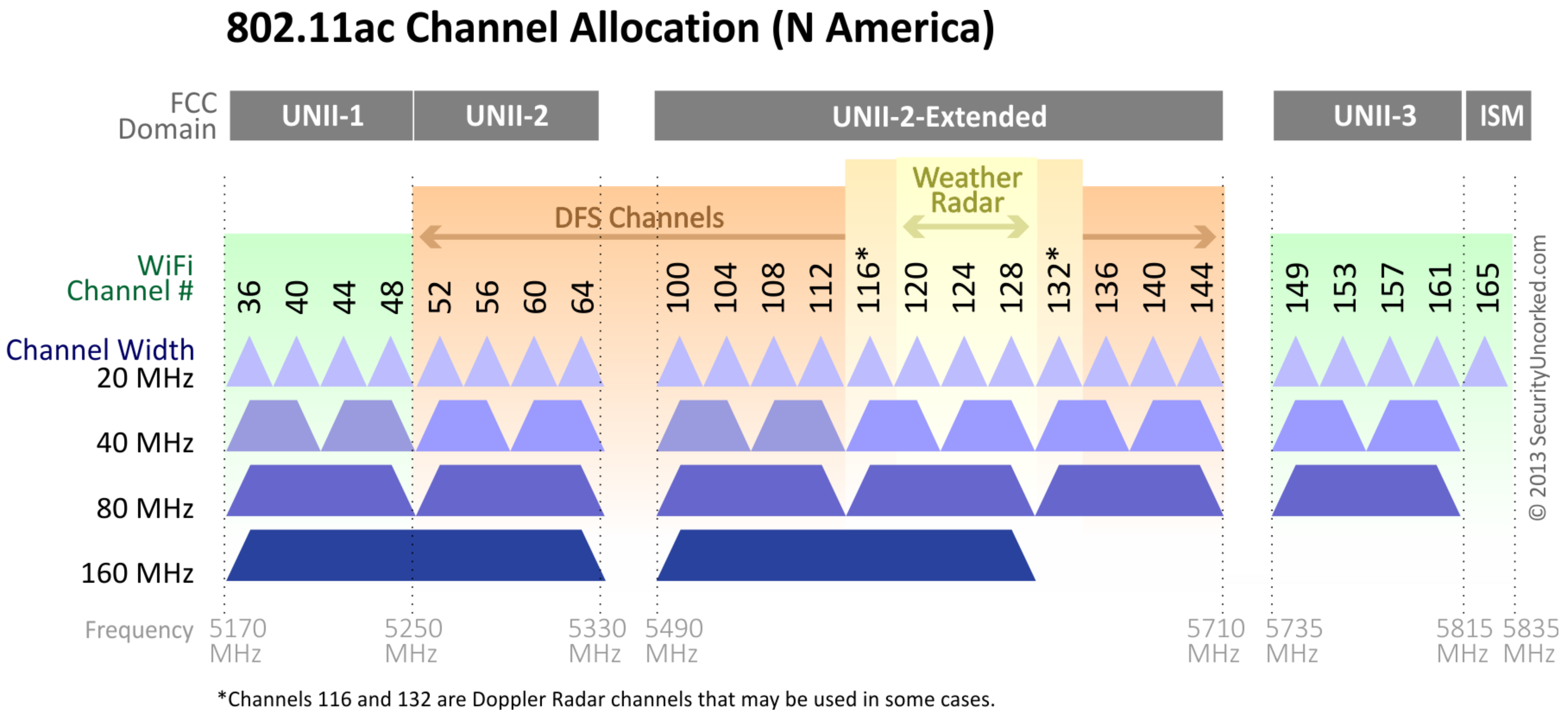
# 802.11ac (2013)

- Update for 5 GHz band only
  - Supports Downlink MU-MIMO (from AP to device)
  - Supports channels widths up to 160 MHz
  - Engineering updates: up to 256-QAM

- Routers apply 802.11ac to 5 GHz and 802.11n to 2.4 GHz

- Still in wide use (as of 2023)
  - Northwestern WiFi networks are 802.11ac (Eduraom, Device, Guest)

# 802.11ac channels



# 802.11ac modulation and coding schemes

802.11ac - VHT MCS, SNR and RSSI

| VHT MCS | Modulation | Coding | 20MHz | | | | 40MHz | | | | 80MHz | | | | 160MHz | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Data Rate 800ns | Data Rate 400ns | Min. SNR | RSSI | Data Rate 800ns | Data Rate 400ns | Min. SNR | RSSI | Data Rate 800ns | Data Rate 400ns | Min. SNR | RSSI | Data Rate 800ns | Data Rate 400ns | Min. SNR | RSSI |
| 1 Spatial Stream | | | | | | | | | | | | | | | | | | |
| 0 | BPSK | 1/2 | 6.5 | 7.2 | 2 | -82 | 13.5 | 15 | 5 | -79 | 29.3 | 32.5 | 8 | -76 | 58.5 | 65 | 11 | -73 |
| 1 | QPSK | 1/2 | 13 | 14.4 | 5 | -79 | 27 | 30 | 8 | -76 | 58.5 | 65 | 11 | -73 | 117 | 130 | 14 | -70 |
| 2 | QPSK | 3/4 | 19.5 | 21.7 | 9 | -77 | 40.5 | 45 | 12 | -74 | 87.8 | 97.5 | 15 | -71 | 175.5 | 195 | 18 | -68 |
| 3 | 16-QAM | 1/2 | 26 | 28.9 | 11 | -74 | 54 | 60 | 14 | -71 | 117 | 130 | 17 | -68 | 234 | 260 | 20 | -65 |
| 4 | 16-QAM | 3/4 | 39 | 43.3 | 15 | -70 | 81 | 90 | 18 | -67 | 175.5 | 195 | 21 | -64 | 351 | 390 | 24 | -61 |
| 5 | 64-QAM | 2/3 | 52 | 57.8 | 18 | -66 | 108 | 120 | 21 | -63 | 234 | 260 | 24 | -60 | 468 | 520 | 27 | -57 |
| 6 | 64-QAM | 3/4 | 58.5 | 65 | 20 | -65 | 121.5 | 135 | 23 | -62 | 263.3 | 292.5 | 26 | -59 | 526.5 | 585 | 29 | -56 |
| 7 | 64-QAM | 5/6 | 65 | 72.2 | 25 | -64 | 135 | 150 | 28 | -61 | 292.5 | 325 | 31 | -58 | 585 | 650 | 34 | -55 |
| 8 | 256-QAM | 3/4 | 78 | 86.7 | 29 | -59 | 162 | 180 | 32 | -56 | 351 | 390 | 35 | -53 | 702 | 780 | 38 | -50 |
| 9 | 256-QAM | 5/6 | | | 31 | -57 | 180 | 200 | 34 | -54 | 390 | 433.3 | 37 | -51 | 780 | 866.7 | 40 | -48 |
| 2 Spatial Streams | | | | | | | | | | | | | | | | | | |
| 0 | BPSK | 1/2 | 13 | 14.4 | 2 | -82 | 27 | 30 | 5 | -79 | 58.5 | 65 | 8 | -76 | 117 | 130 | 11 | -73 |
| 1 | QPSK | 1/2 | 26 | 28.9 | 5 | -79 | 54 | 60 | 8 | -76 | 117 | 130 | 11 | -73 | 234 | 260 | 14 | -70 |
| 2 | QPSK | 3/4 | 39 | 43.3 | 9 | -77 | 81 | 90 | 12 | -74 | 175.5 | 195 | 15 | -71 | 351 | 390 | 18 | -68 |
| 3 | 16-QAM | 1/2 | 52 | 57.8 | 11 | -74 | 108 | 120 | 14 | -71 | 234 | 260 | 17 | -68 | 468 | 520 | 20 | -65 |
| 4 | 16-QAM | 3/4 | 78 | 86.7 | 15 | -70 | 162 | 180 | 18 | -67 | 351 | 390 | 21 | -64 | 702 | 780 | 24 | -61 |
| 5 | 64-QAM | 2/3 | 104 | 115.6 | 18 | -66 | 216 | 240 | 21 | -63 | 468 | 520 | 24 | -60 | 936 | 1040 | 27 | -57 |
| 6 | 64-QAM | 3/4 | 117 | 130.3 | 20 | -65 | 243 | 270 | 23 | -62 | 526.5 | 585 | 26 | -59 | 1053 | 1170 | 29 | -56 |
| 7 | 64-QAM | 5/6 | 130 | 144.4 | 25 | -64 | 270 | 300 | 28 | -61 | 585 | 650 | 31 | -58 | 1170 | 1300 | 34 | -55 |
| 8 | 256-QAM | 3/4 | 156 | 173.3 | 29 | -59 | 324 | 360 | 32 | -56 | 702 | 780 | 35 | -53 | 1404 | 1560 | 38 | -50 |
| 9 | 256-QAM | 5/6 | | | 31 | -57 | 360 | 400 | 34 | -54 | 780 | 866.7 | 37 | -51 | 1560 | 1733.3 | 40 | -48 |
| 3 Spatial Streams | | | | | | | | | | | | | | | | | | |
| 0 | BPSK | 1/2 | 19.5 | 21.7 | 2 | -82 | 40.5 | 45 | 5 | -79 | 87.8 | 97.5 | 8 | -76 | 175.5 | 195 | 11 | -73 |
| 1 | QPSK | 1/2 | 39 | 43.3 | 5 | -79 | 81 | 90 | 8 | -76 | 175.5 | 195 | 11 | -73 | 351 | 390 | 14 | -70 |
| 2 | QPSK | 3/4 | 58.5 | 65 | 9 | -77 | 121.5 | 135 | 12 | -74 | 263.3 | 292.5 | 15 | -71 | 526.5 | 585 | 18 | -68 |
| 3 | 16-QAM | 1/2 | 78 | 86.7 | 11 | -74 | 162 | 180 | 14 | -71 | 351 | 390 | 17 | -68 | 702 | 780 | 20 | -65 |
| 4 | 16-QAM | 3/4 | 117 | 130 | 15 | -70 | 243 | 270 | 18 | -67 | 526.5 | 585 | 21 | -64 | 1053 | 1170 | 24 | -61 |
| 5 | 64-QAM | 2/3 | 156 | 173.3 | 18 | -66 | 324 | 360 | 21 | -63 | 702 | 780 | 24 | -60 | 1404 | 1560 | 27 | -57 |
| 6 | 64-QAM | 3/4 | 175.5 | 195 | 20 | -65 | 364.5 | 405 | 23 | -62 | | | 26 | -59 | 1579.5 | 1755 | 29 | -56 |
| 7 | 64-QAM | 5/6 | 195 | 216.7 | 25 | -64 | 405 | 450 | 28 | -61 | 877.5 | 975 | 31 | -58 | 1755 | 1950 | 34 | -55 |
| 8 | 256-QAM | 3/4 | 234 | 260 | 29 | -59 | 486 | 540 | 32 | -56 | 1053 | 1170 | 35 | -53 | 2106 | 2340 | 38 | -50 |
| 9 | 256-QAM | 5/6 | 260 | 288.9 | 31 | -57 | 540 | 600 | 34 | -54 | 1170 | 1300 | 37 | -51 | | | 40 | -48 |

4 spatial streams is also allowed, getting up to 3466 Mbps

# Walking through PHY changes by amendment

| | Protocol | Year | Frequency | PHY | Max Rate | Range |
|---|---|---|---|---|---|---|
| - | 802.11 | 1997 | 2.4 GHz | DSSS/FHSS | 2 Mbps | 20 m |
| 1 | 802.11b | 1999 | 2.4 GHz | DSSS | 11 Mbps | 35 m |
| 2 | 802.11a | 1999 | 5 GHz | OFDM | 54 Mbps | 35 m |
| 3 | 802.11g | 2003 | 2.4 GHz | OFDM | 54 Mbps | 38 m |
| 4 | 802.11n | 2009 | 2.4/5 GHz | OFDM + MIMO | 600 Mbps | 70 m |
| 5 | 802.11ac | 2013 | 5 GHz | OFDM + MU-MIMO | 3.4 Gbps | 35 m |
| 6 | **802.11ax** | 2021 | 2.5/5/[6] GHz | OFDMA + MU-MIMO | 9.6 Gbps | 35 m |
| 7 | **802.11be** | TBA | 2.5/5/6 GHz | OFDMA + MU-MIMO | 40 Gbps | 35 m |

# New directions in WiFi focus:
Aggregate throughput across all devices

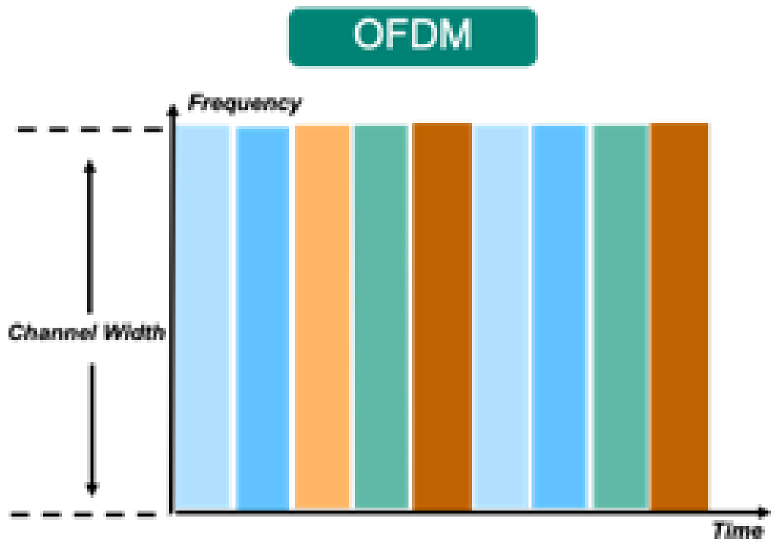
- For point-to-point, WiFi is “(more than) fast enough”

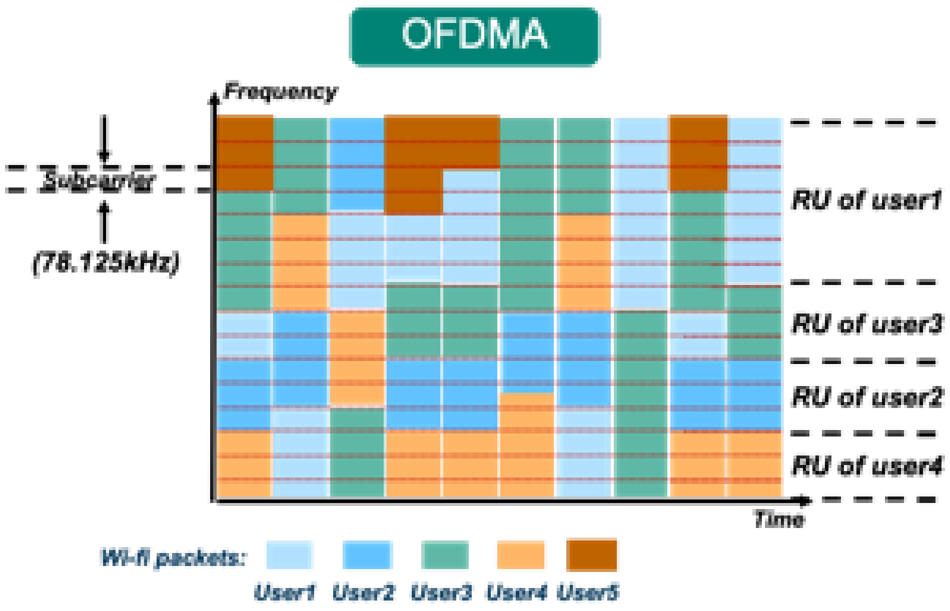
- Now the problem is the quantity of devices in a single space
  - Desktop, laptop, tablet, smartphone, smartwatch, IoT devices, etc.

- Insight: Bring established cellular techniques to WiFi

# Orthogonal Frequency Division Multiple Access

- OFDM: split channel into subcarriers and transmit on those
- OFDMA: allocate subcarriers to a device for an amount of time
  - Turns OFDM into an access control mechanism
  - Complicated question: which device gets which subcarriers at which time?



# OFDM vs OFDMA
Orthogonal Frequency Division Multiplexing vs. Orthogonal Frequency Division Multiple Access

- Net spectrum usage ~the same

- In same time slot, assign sub-carriers to different users
  - Effect: Lower bandwidth per user, but more simultaneous users

- This is the same strategy cellular “resource blocks” use
  - Called “Resource Units” in WiFi

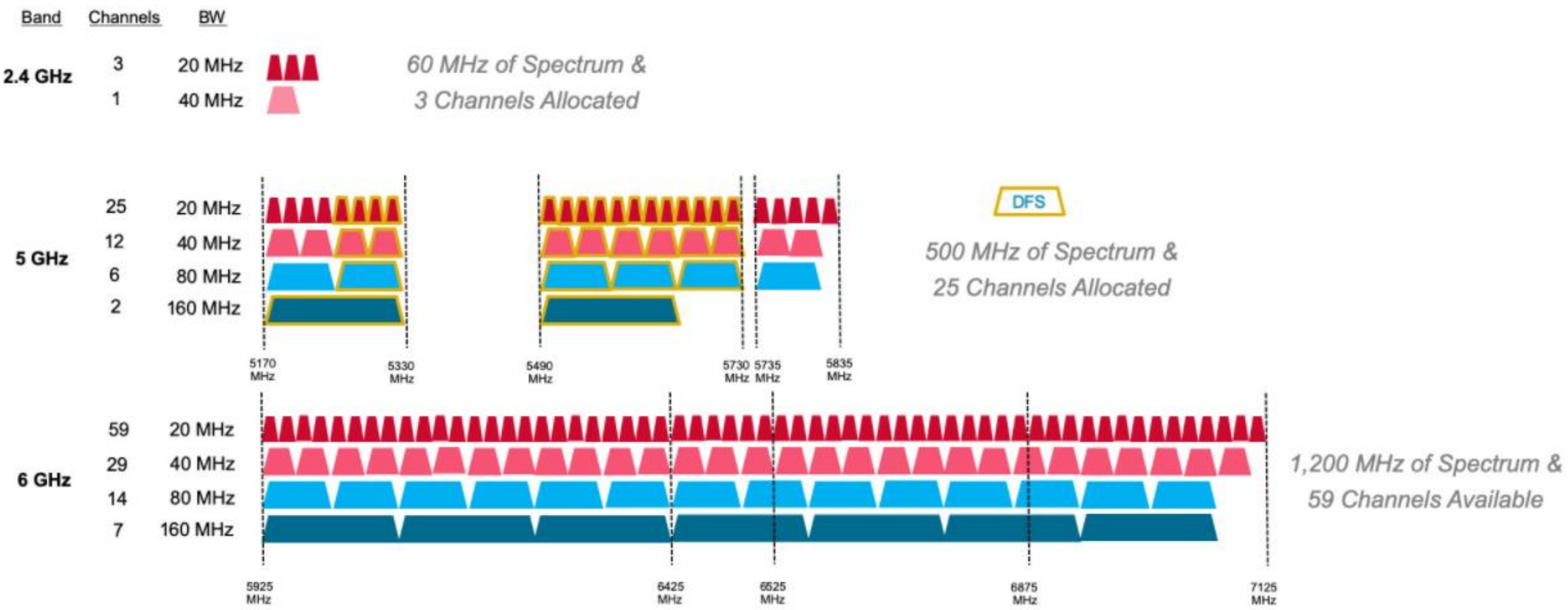
# 802.11ax (2021)

- Standard approved on February 9$^{th}$ 2021
  - First devices started supporting it in 2019 (WiFi 6)

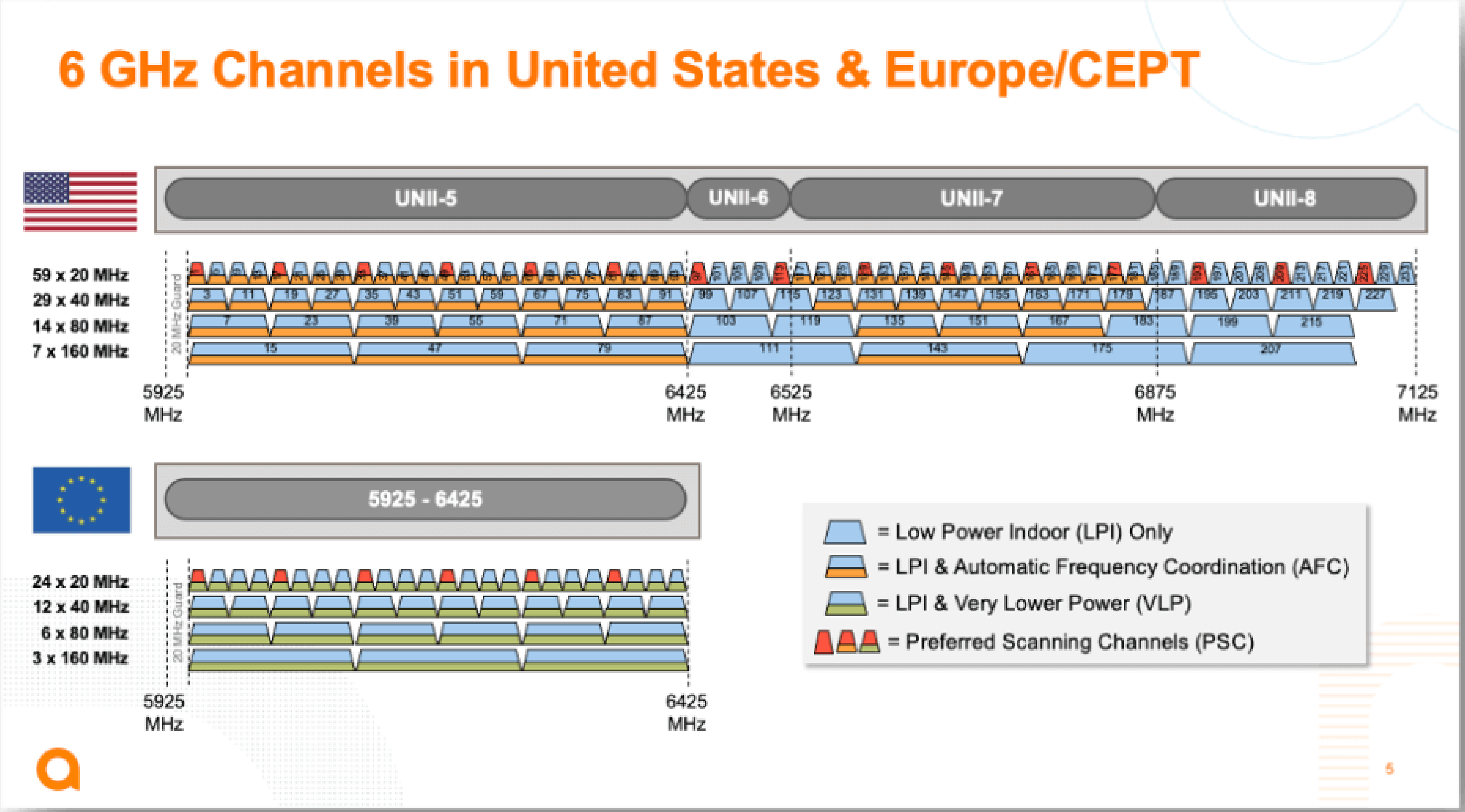
- 6 GHz band (WiFi 6E)
  - 1.2 GHz of bandwidth (5.925-7.125 GHz)
  - 2020: US FCC made band available for unlicensed use!!!
  - EU followed by June 2021

- OFDMA
  - MAC scheduling variant of OFDM
  - AP schedules devices based on time and subcarrier allocations

# 6 GHz band is an enormous amount of bandwidth



# Less bandwidth in the 6 GHz band in Europe



# Reminder: WiFi technology (and to some extent cellular) a unicorn – HW support rolls out *before* specification

Standard Finalized: Sep 2020
Standard Ratified: Feb 2021

Release: Sep 2019 → (iPhone 11 Pro Max)

| Model | 802.11ax | 802.11v | 802.11r | 802.11k |
|---|---|---|---|---|
| iPhone 13 Pro Max<br>iPhone 13 Pro<br>iPhone 13<br>iPhone 13 mini | ✓ | ✓ | ✓ | ✓ |
| iPhone 12 Pro Max<br>iPhone 12 Pro<br>iPhone 12<br>iPhone 12 mini | ✓ | ✓ | ✓ | ✓ |
| iPhone 11 Pro Max<br>iPhone 11 Pro<br>iPhone 11 | ✓ | ✓ | ✓ | ✓ |
| iPhone Xs Max<br>iPhone Xs<br>iPhone XR<br>iPhone X | | ✓ | ✓ | ✓ |

# WiFi 6 Hardware

- Two varieties:
  - WiFi 6
    - Most of the features, but NOT the new frequencies
  - WiFi 6E
    - Includes the extra 6 GHz channels
    - Basically entirely unused as of 2023

- WiFi 6E is the stuff you want for future proofing

# What’s coming next: 802.11.be

- Still in flux, “WiFi 7” aka “Extremely High Throughput” (EHT)
- Adds…
  - More channel bonding / wider bandwidth: up to 320 MHz
  - Up to 4096-QAM
  - Up to 16-stream MIMO
  - AP coordination for non-enterprise networks
  - Lots of fancy timing estimation stuff (802.1Q)
    - Primary focus seems to be AV-streaming Quality-of-Service (QoS)

# Outline

- **WiFi Overview**

- WiFi PHY
    - 802.11/802.11b
    - 802.11a/802.11g
    - 802.11n/802.11ac
    - 802.11ax

    - **Real-World WiFi**

# Goal: improve throughput

- In twenty years, WiFi has gone from 2 Mbps to 9.6 Gbps
- **How does a network PHY improve its throughput?**

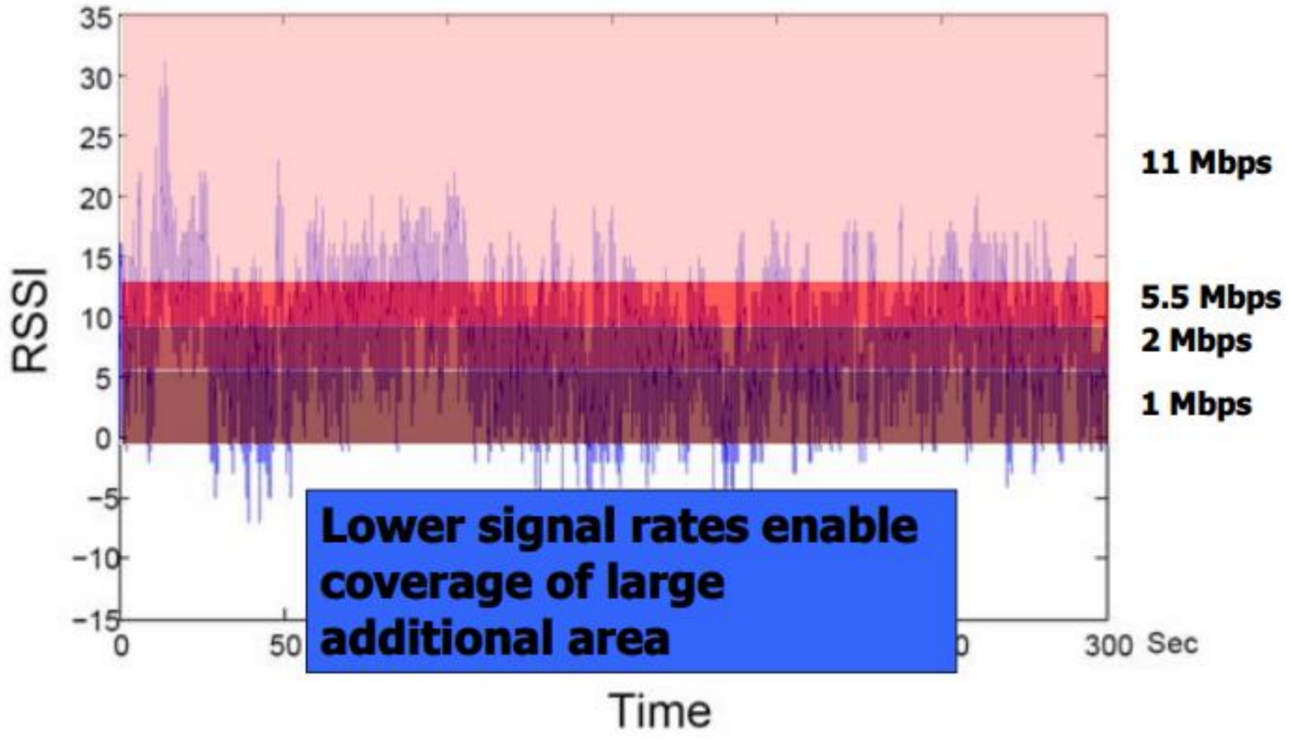
1. More capable modulation and/or bit transmission
    - Techniques like OFDM and MIMO
        - Original 2 Mbps -> 54 Mbps with OFDM -> 346 Mbps with MIMO **(100x)**
        - Engineering improvements are baked into these steps too

2. More bandwidth
    - Increased channel with at 2.4 Ghz and bigger 5 GHz channels
        - 346 Mbps with 20 MHz -> 3466 Mbps with 160 MHz **(10x)**

# Bit rate adaptation

- All modern WiFi standards support multiple bit rates (MCS)

- Many factors can influence the choice of bit rate
  - Capability of device: not all devices support all bit rates
  - Range and packet reliability (interference)



# Bit rate adaptation

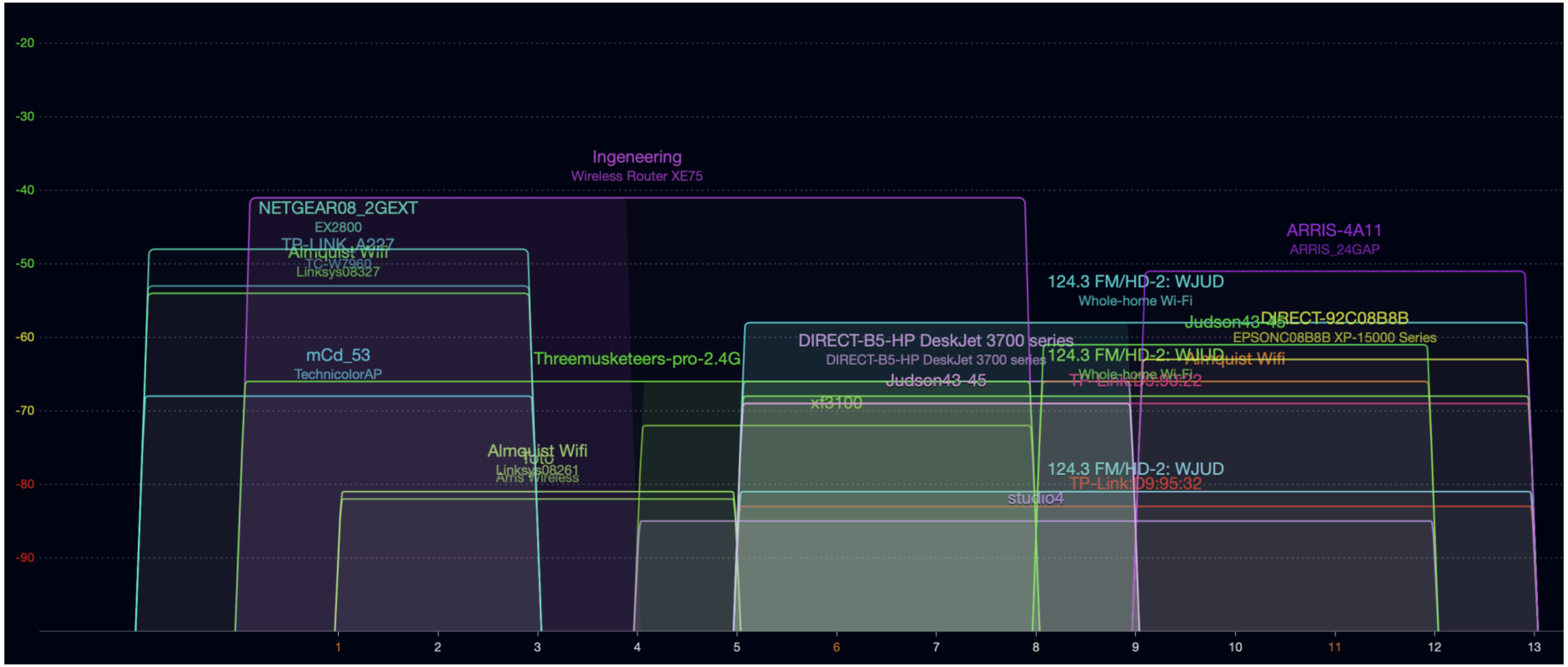
- Selecting the right rate at the right time is a complex problem
  - And needs to be decided per-device

  - Trial and Error
    - Failures -> reduce rate
    - Successes -> increase rate

  - Signal strength
    - Use channel state information to decide

  - Context sensitive
    - Mobile devices can use lower rates for higher reliability

# Real-world 802.11 channel use – 2.4 Ghz

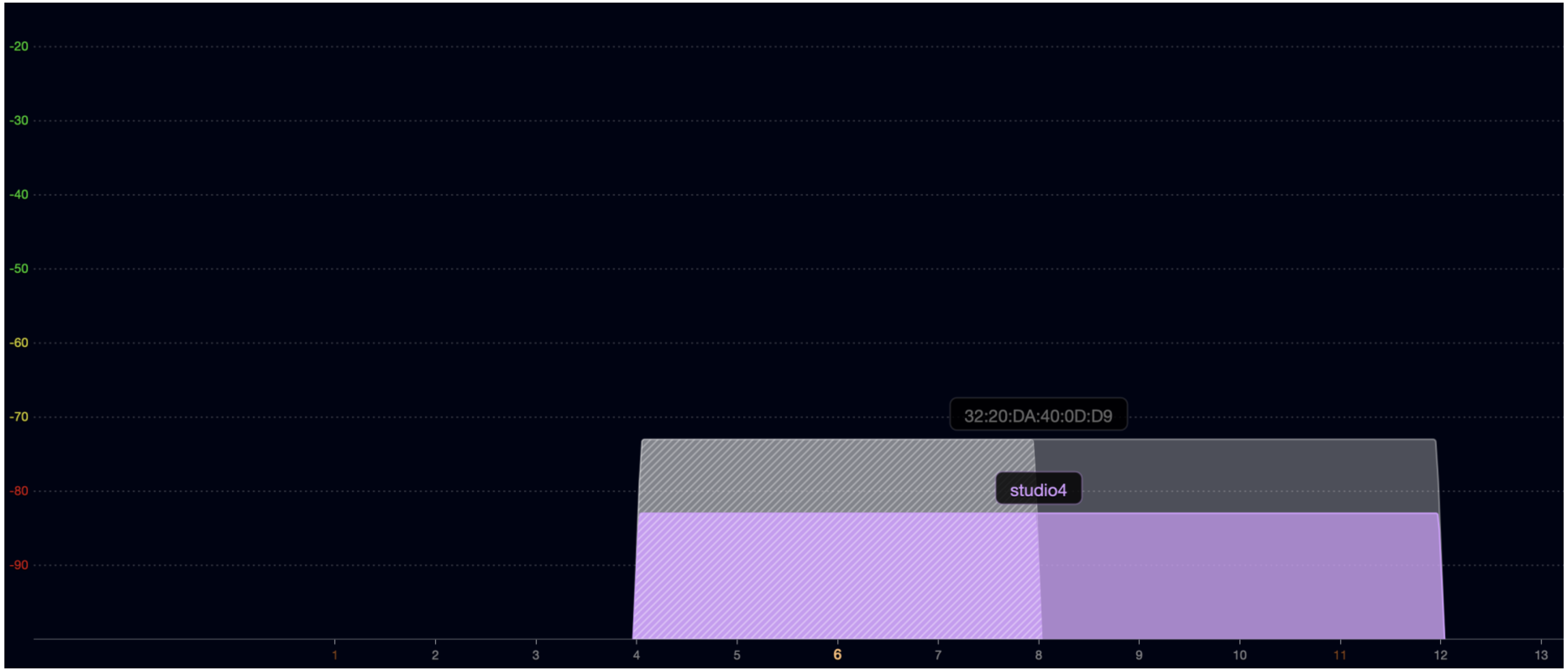



Collected from Branden's apartment building in Evanston

Tool: [WiFi Explorer]
(MacOS only)

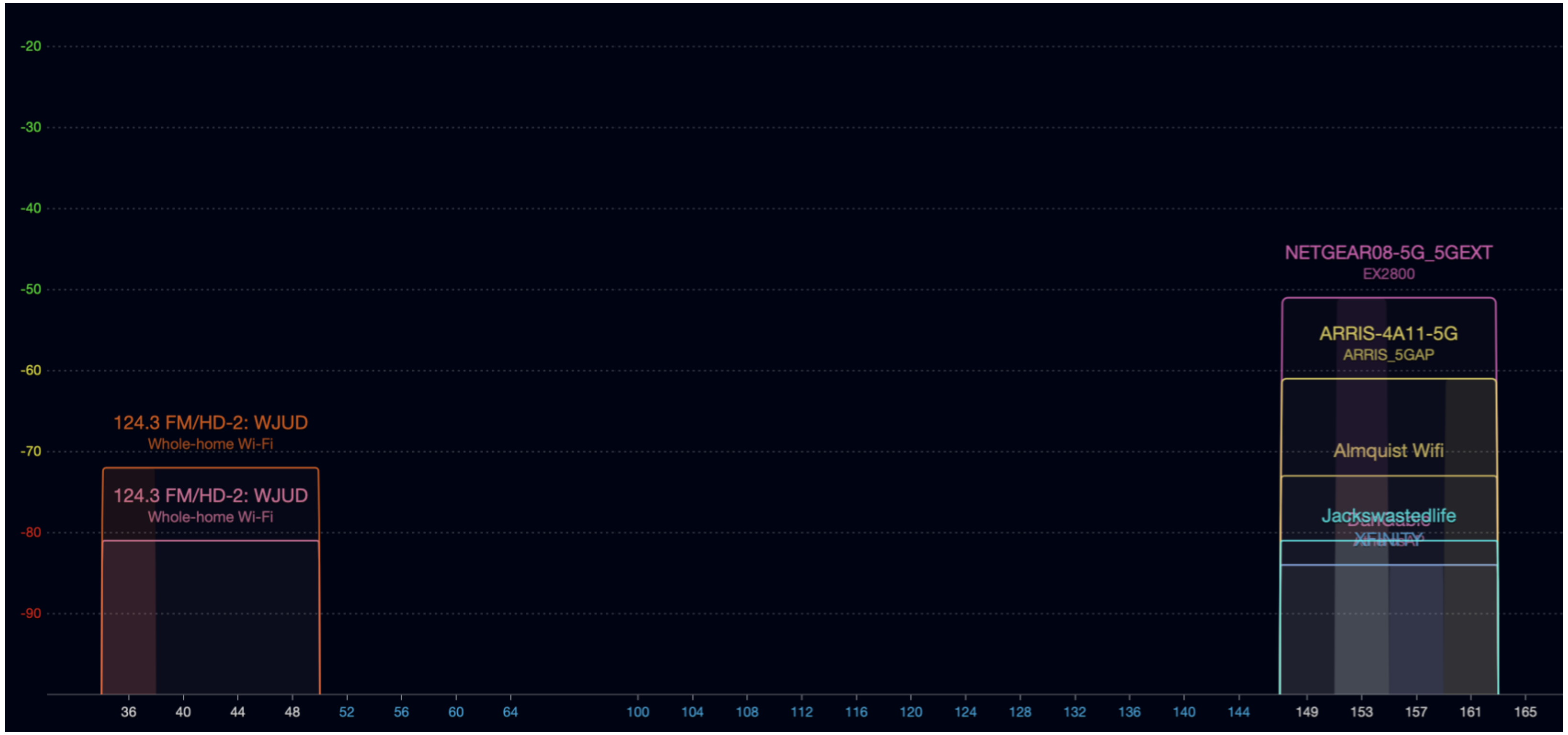
- Lots of congestion
  - Some devices only use 20 MHz bandwidth (mostly on channel 1 or 11 here)
  - Some devices use 40 MHz bandwidth (<1 through 8, or 5-13)

# Some real-world devices are weird



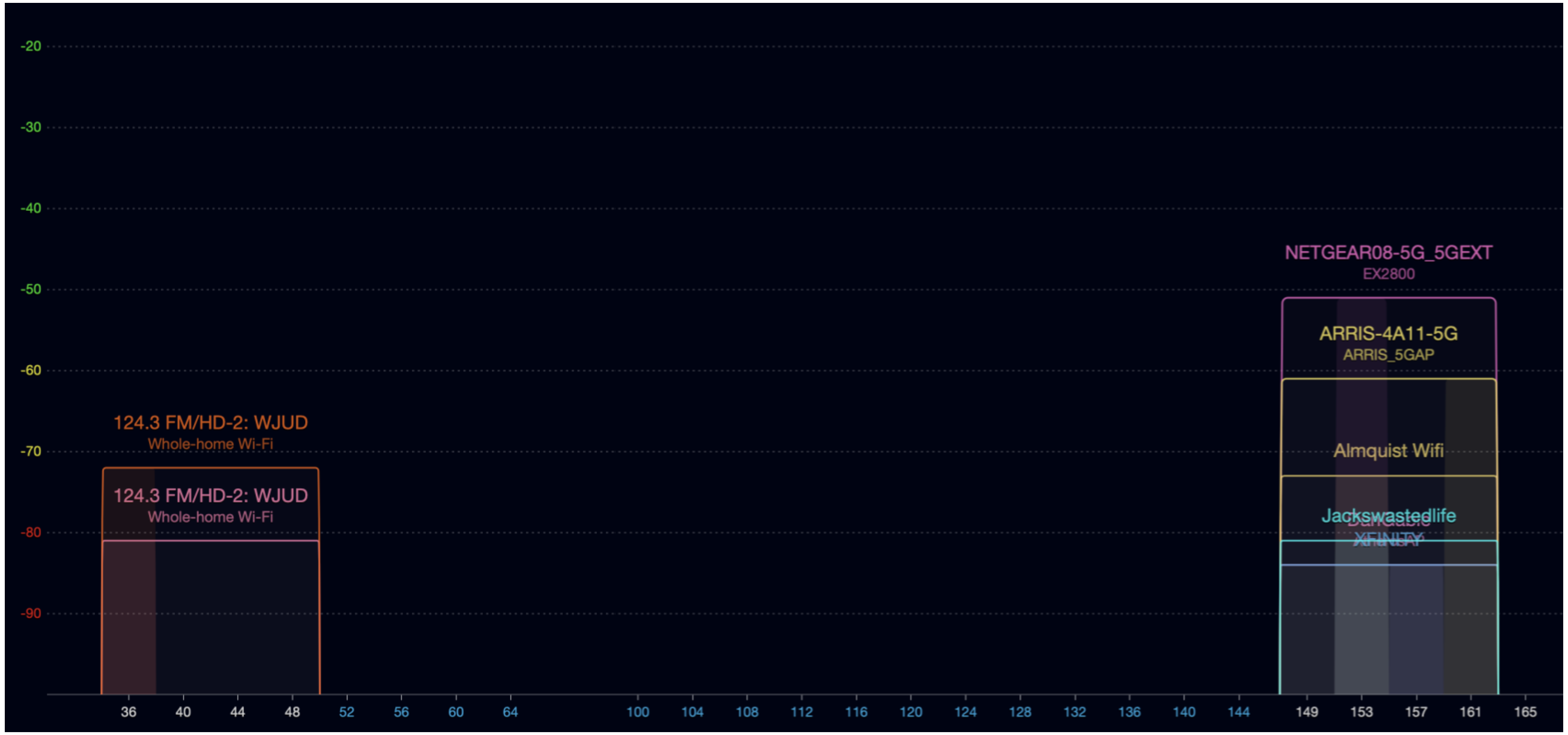

- Why make a 40 MHz allocation centered on channel 6??
- Similarly, some 20 MHz networks use channels 2, 9, or 10

# Real-world 802.11 channel use – 5 Ghz



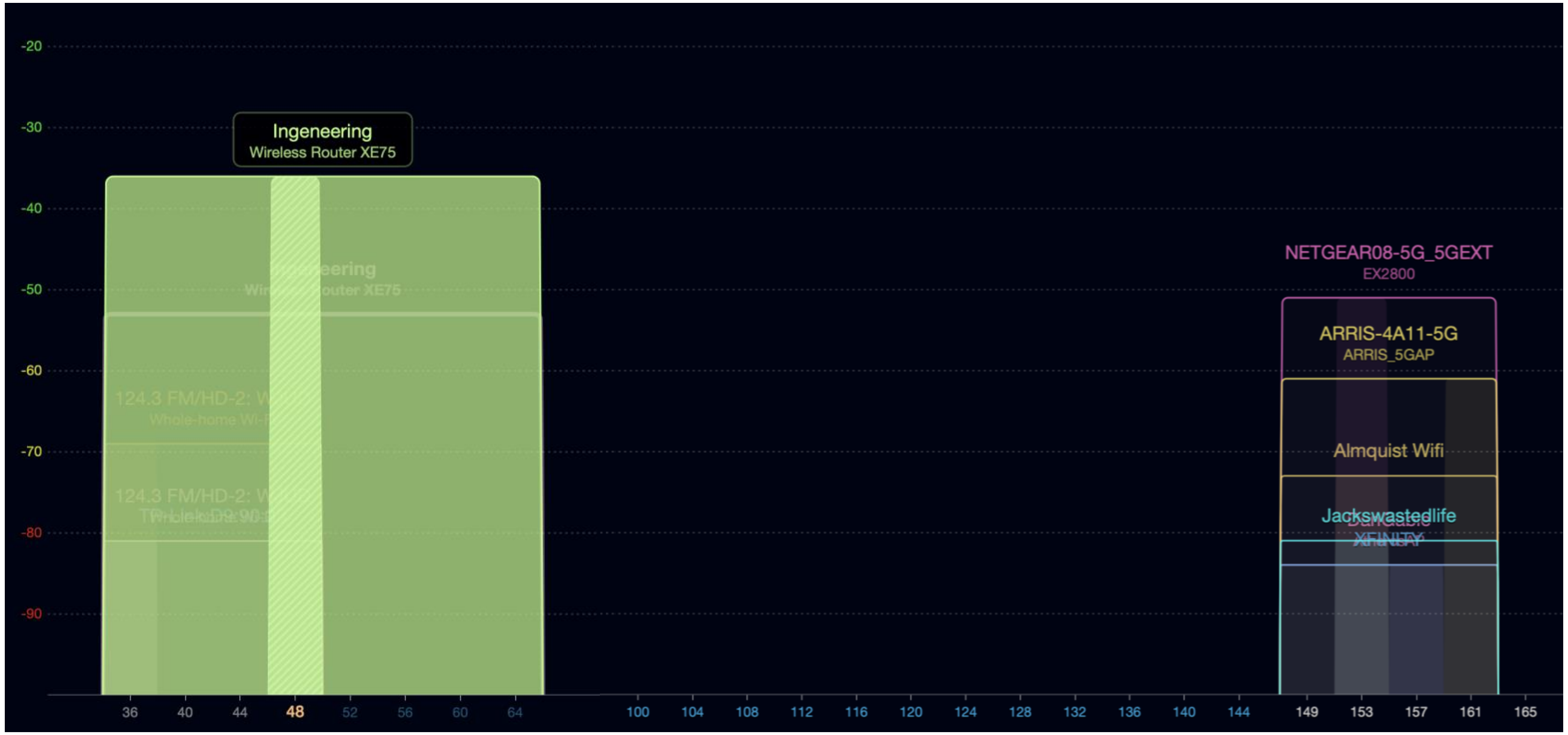

- Much less choice
  - 80 MHz bandwidth on lower channels or upper channels
  - **Why no use of channel 165?**

# Real-world 802.11 channel use – 5 Ghz




- Much less choice
  - 80 MHz bandwidth on lower channels or upper channels
  - **Why no use of channel 165?** Only 20 MHz, can't be 100 MHz in size

# What does a new, (moderately) expensive router get you?




TP-Link Deco XE75
WiFi 6E with Mesh

https://www.tp-link.com/us/deco-mesh-wifi/product-family/deco-xe75/

- 160 MHz bandwidth channel 💪
- Uses channels 52-64 which have special rules
  - Must detect radar use and leave channel if it occurs (DFS)
  - Must control transmission power between devices (TPC)

- Also has a 160 MHz bandwidth allocation on channels 33-61 of the 6 GHz space
  - My scans showed no other network in the 6 GHz bands

# Outline

- WiFi Overview

- WiFi PHY
    - 802.11/802.11b
    - 802.11a/802.11g
    - 802.11n/802.11ac
    - 802.11ax

    - Real-World WiFi