Lecture 02
Network Fundamentals

CS433 – Wireless Protocols for IoT

Branden Ghena – Spring 2026

Some slides borrowed from: Peter Steenkiste (CMU), Christian Poellabauer (Notre Dame)

Materials in collaboration with Pat Pannuto (UCSD) and Brad Campbell (UVA)

Administrivia

- Let me know if you don’t have access to something

- Hw: Background out now
  - Due Thursday

- First lab this Friday: Wireshark
  - Individual lab just playing around with Wireshark
  - Location: Frances Searle 3220 at 11:00 AM

- Temporary office hours
  - 1:00-3:50 PM on Wednesday (04/08)
  - Tech L368 (my office)
  - I hope to have a full schedule next week

Today’s Goals

- Introduce OSI layer model of communication
- Provide background on Internet layering
- Overview of concerns for the Physical layer
  - Speak the “lingo” of wireless communication
  - Present technology aspects that we will return to in specific protocols

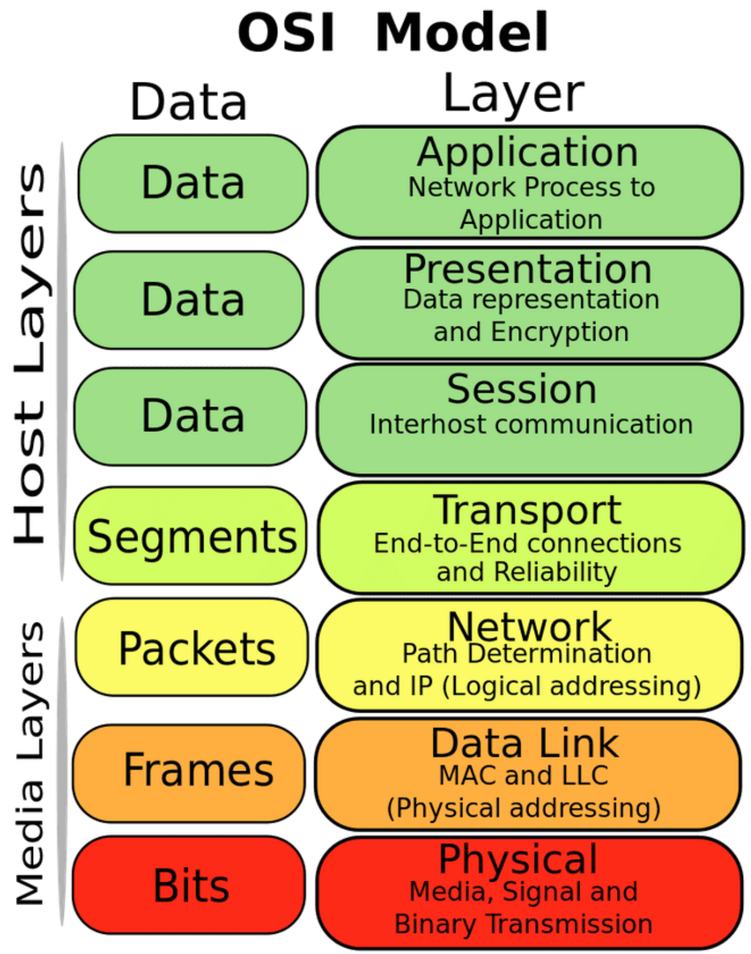
Outline

- **OSI Layers**
- Internet Architecture (Upper Layers)
- Physical Layer
  - Overview
  - Signal Strength
  - Signal Frequency and Bandwidth
  - Signal Modulation

OSI model of communication layers

- Transport
  - Sending data between applications
  - TCP and UDP
- Network
  - Sending data between networked computers
  - IP
- Data Link
  - Sending collections of bits
  - Ethernet, WiFi
- Physical
  - Sending individual bits
  - Ethernet, WiFi

Open Systems Interconnection (OSI)



Where does this class focus?

- Transport
  - Sending data between applications
  - TCP and UDP
- Network
  - Sending data between networked computers
  - IP
- Data Link
  - Sending collections of bits
  - Ethernet, WiFi
- Physical
  - Sending individual bits
  - Ethernet, WiFi

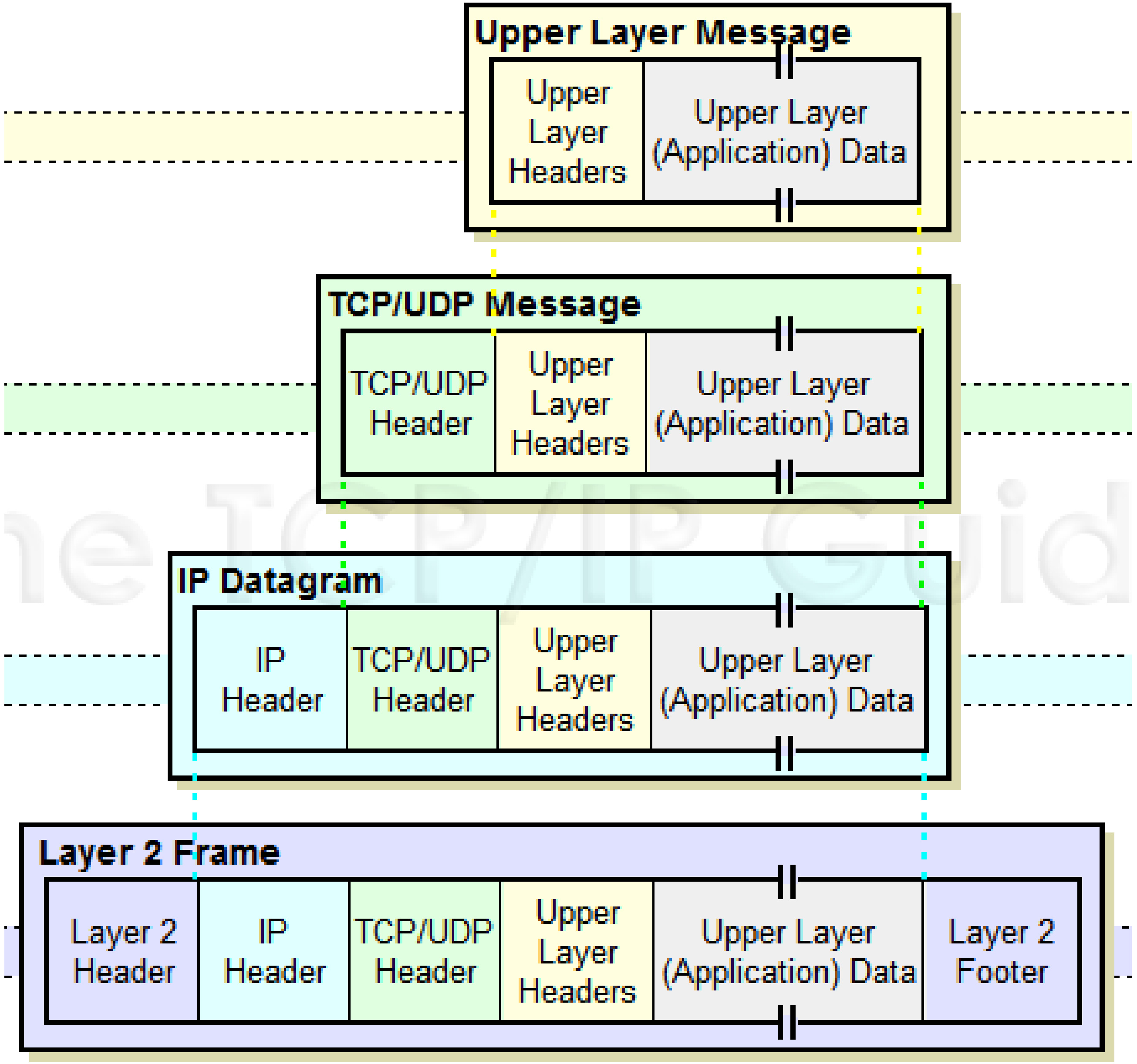
CS domain
CS340, CS440

This course!

EE domain
EE307, EE378, EE380

Protocols are "layered"

- Headers for each layer of communication wrap data
  - Data is wrapped with header for the network to make a packet
    - i.e., bytes are added to the start/end of it
  - Packet is wrapped with header for the link to make a frame
- Upper-layer packet is the payload for the lower-layer packet



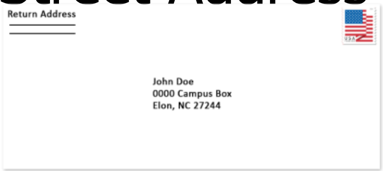
Analogy: Sending a letter

Application:
Purpose/type of letter

Transport:
Carrier service

Named recipient

Network:
Street Address

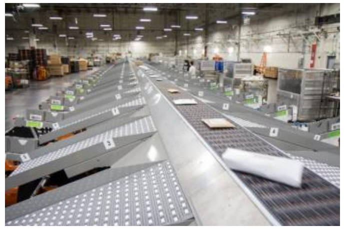


Courier

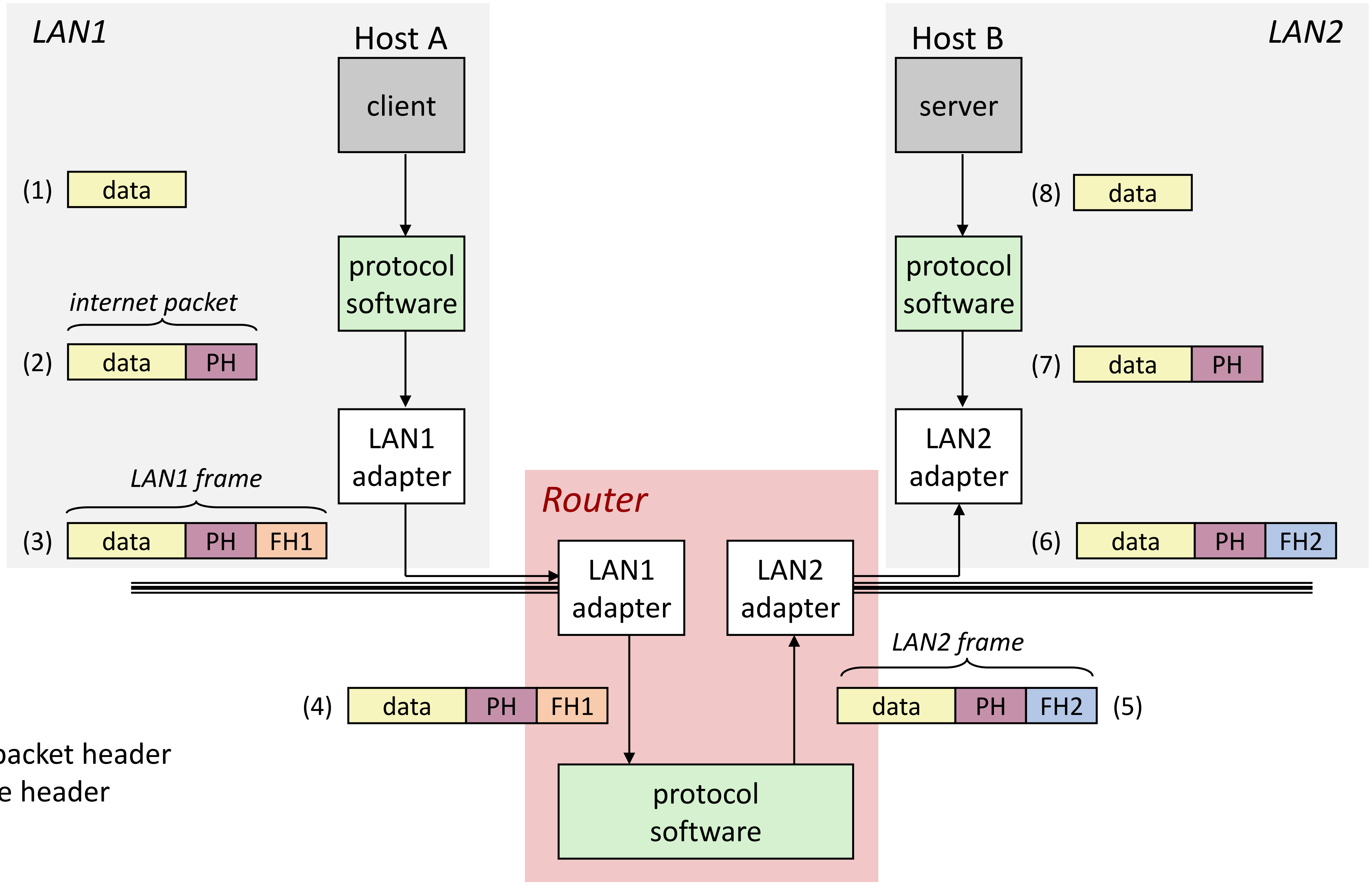
Mailing/shipping infrastructure

Link:
Transfer to post office

Physical:
Moving tangible object



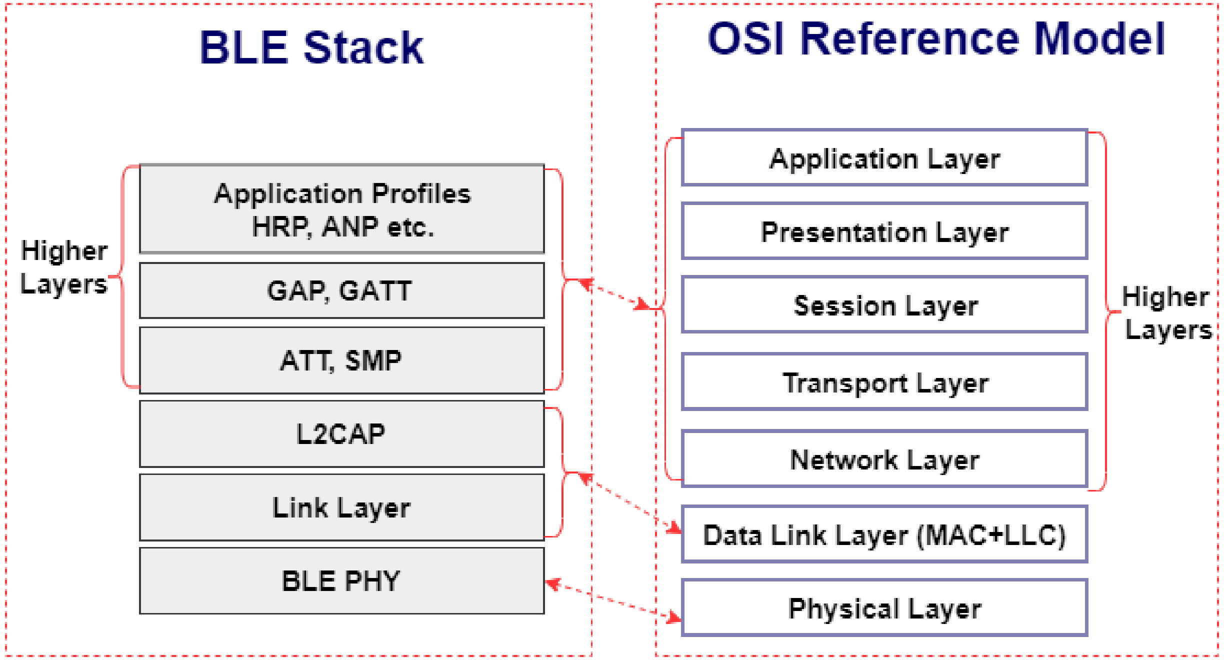
Transmitting data between networks

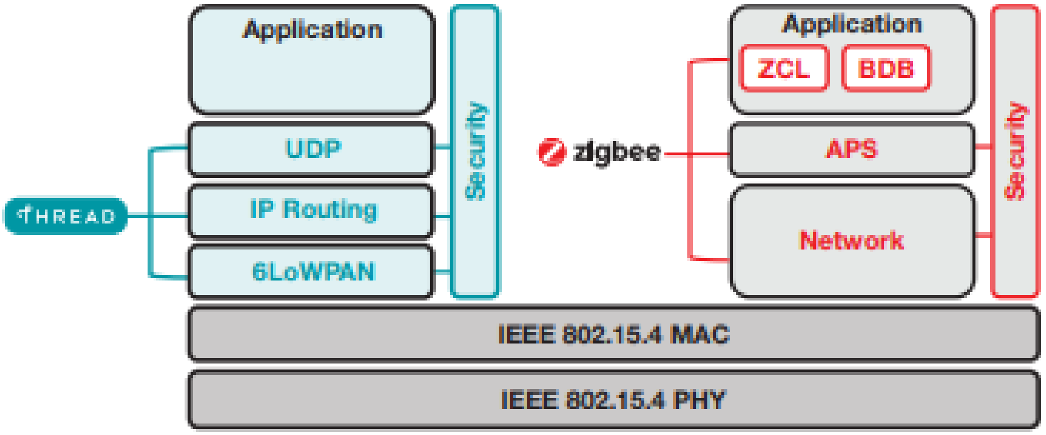


PH: Internet packet header
FH: LAN frame header

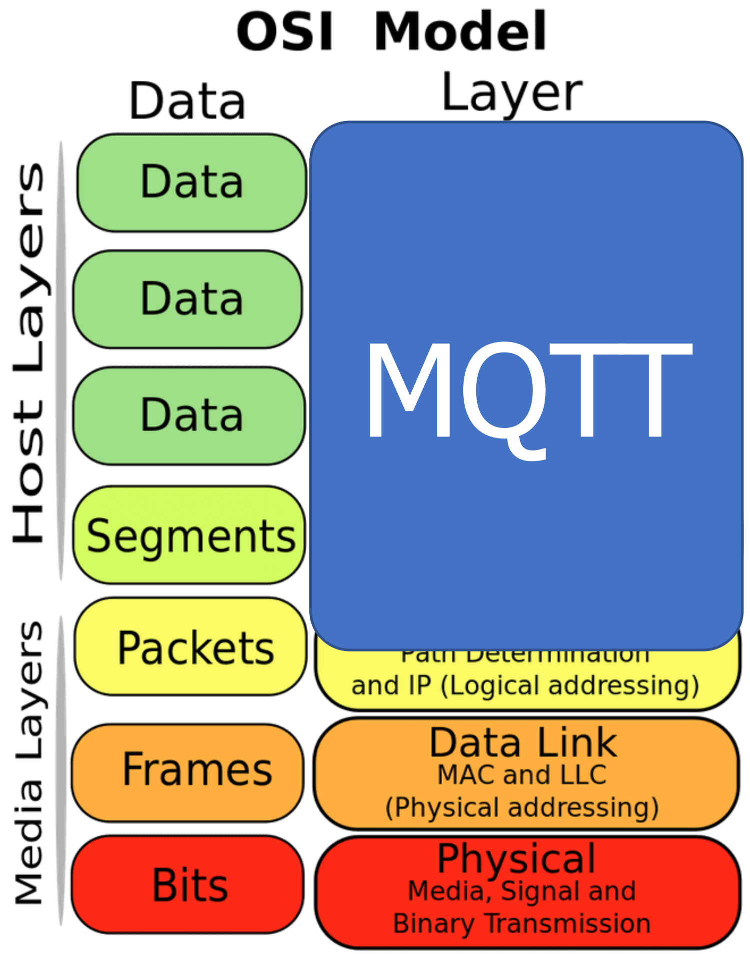
Model does not equal reality

- Wireless protocols don’t always split between layers cleanly
  - Usually explain parts of physical, data link, and possibly upper layers
- Model still helps conceptualize stack-up though
  - Layering of some type still occurs





Layering for IoT (joke) (kind of)



MQTT is a publish/subscribe message broker

Outline

- OSI Layers
- **Internet Architecture (Upper Layers)**
- Physical Layer
  - Overview
  - Signal Strength
  - Signal Frequency and Bandwidth
  - Signal Modulation

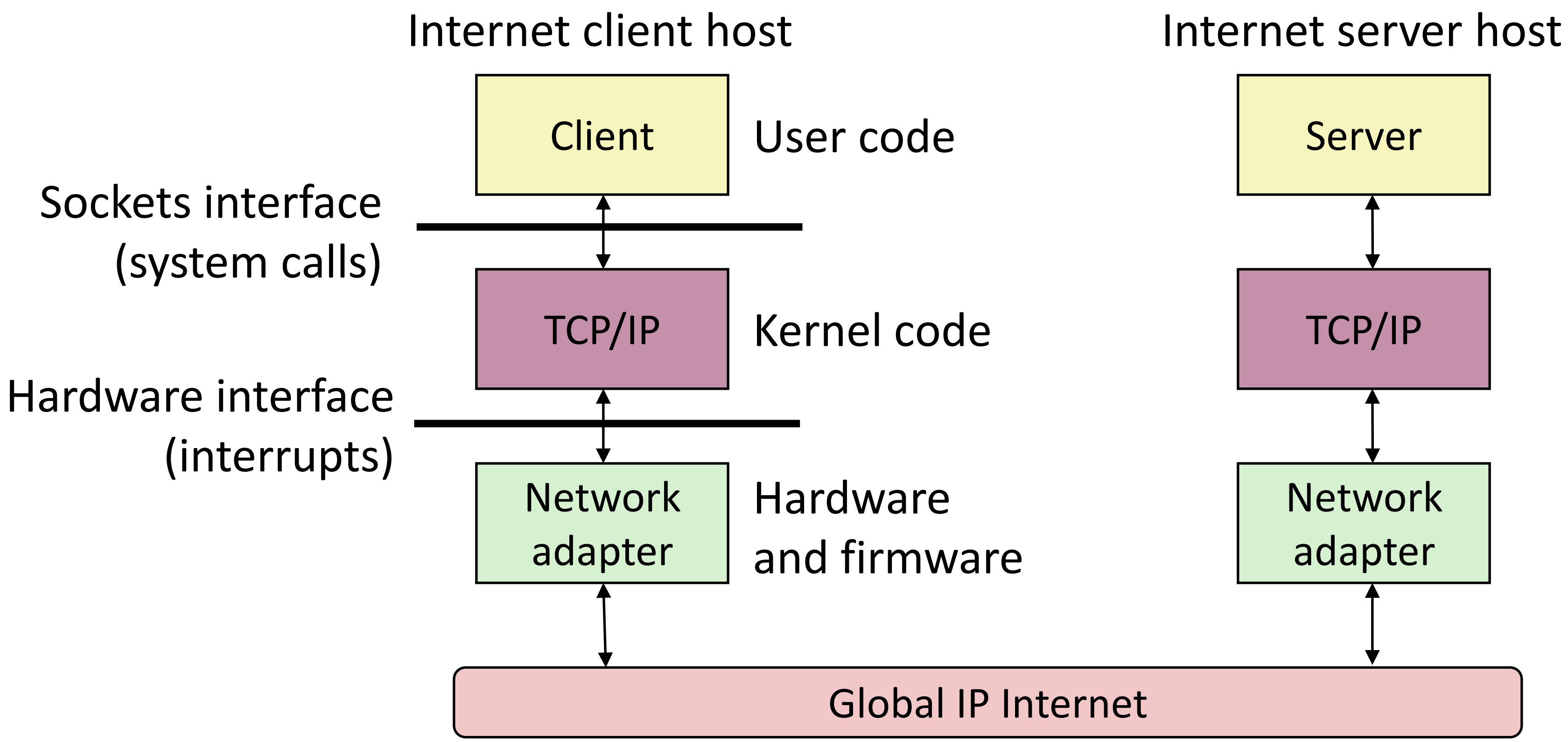
The global Internet

- Most famous example of an internet (uppercase to distinguish)

- Based on the TCP/IP protocol family
  - **IP** (Internet Protocol)
    - Provides a *naming scheme* and unreliable *delivery of packets* from **host-to-host**
  - **UDP** (Unreliable Datagram Protocol)
    - Uses IP to provide *unreliable data delivery* from **process-to-process**
  - **TCP** (Transmission Control Protocol)
    - Uses IP to provide *reliable data delivery* from **process-to-process**

- Accessed via a mix of Unix file I/O and the **sockets** interface

Hardware and software organization of an Internet application



A programmer's view of the internet

1. Hosts are mapped to a set of 32-bit **IP addresses**
    - 129.105.5.212

2. The set of IP addresses is mapped to a set of identifiers called Internet **domain names**
    - 129.105.5.212 is mapped to moore.wot.eecs.northwestern.edu

3. A process on one Internet host can communicate with a process on another Internet host over a **connection**

1. IP addresses

- 32-bit identifier for a computer on the Internet

- By convention, each byte in a 32-bit IP address is represented by its decimal value and separated by a period
    - IP address: `0x816905D4` = `129.105.7.212`

- Each computer you want to access needs a unique IP address
    - Blocks of IP addresses are owned by various network operators and distributed to computers on their networks
        - For servers, these need to be long-term consistent
        - For clients, they can be short-term leases

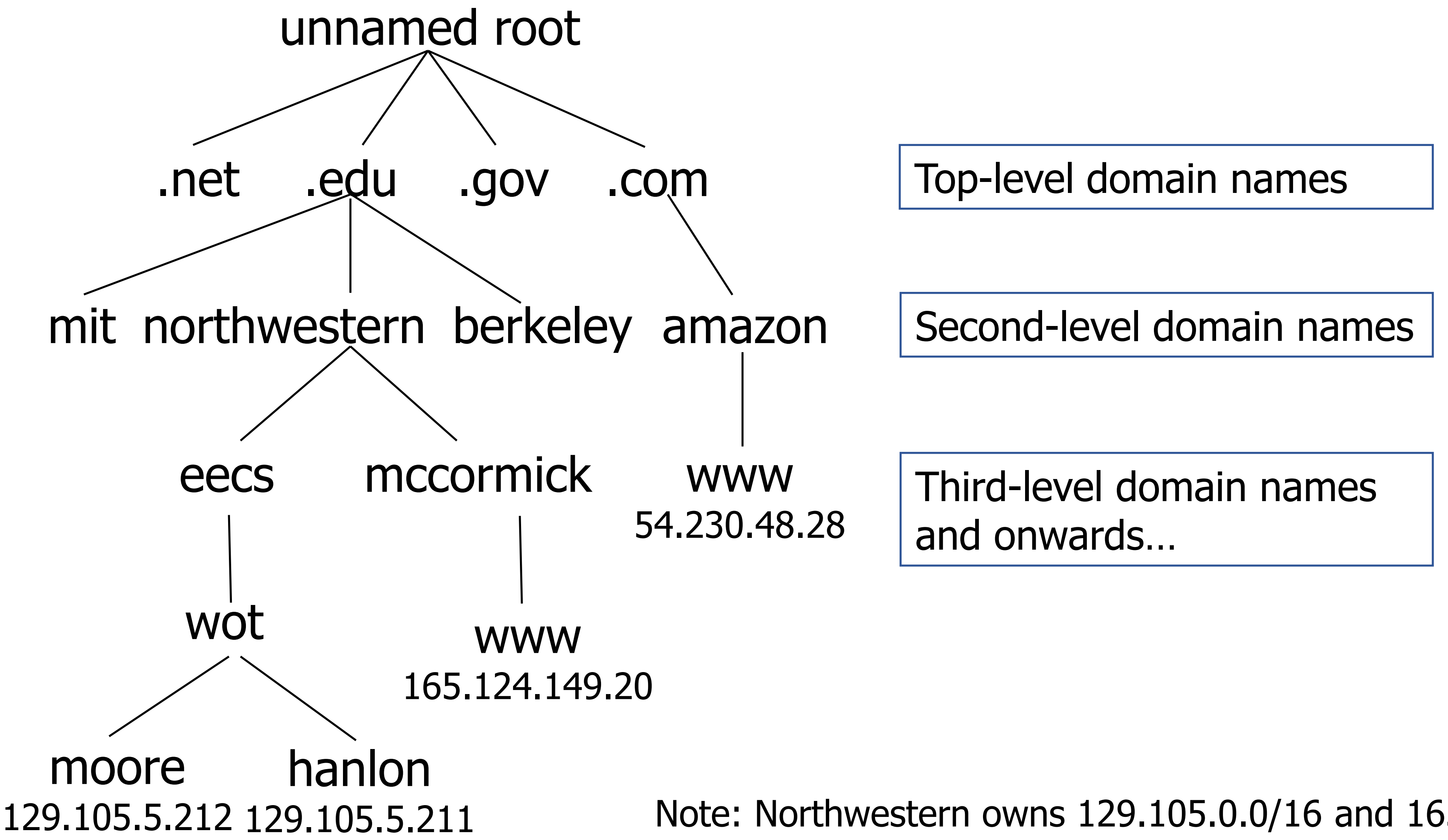
Northwestern IPv4 ranges

- Format: `ip.addr/`**`NUM`**
- **`NUM`** is the number of meaningful bits, from the most-significant bit
  - 129.105.0.0/16 means the most-significant 16 bits are meaningful
    i.e., 129.105.x.x
  - Remaining bits can be used for unique addresses
    - $2^{(32-\mathrm{NUM})}$ machines

Public IPv4 Address Ranges

Network	Description
129.105.0.0/16	Northwestern Administrative Mainly - Evanston
165.124.0.0/16	Northwestern Administrative Evanston and Chicago
165.124.188.0/22	Northwestern-Qatar1, all others (except NU-Qatar2) on main NU campus
165.124.236.0/22	Northwestern-Qatar2, all others (except NU-Qatar1) on main NU campus
192.5.143.0/24	Peering point to point links, various other usage
192.26.86.0/24	ABF Rubloff 4th floor
192.26.87.0/24	Starlight mgmt network
192.31.155.0/24	Northwestern Affiliate
192.31.253.0/24	Utility
199.74.64.0/18	Northwestern dorms
199.249.165.0/24	Northwestern Affiliate
199.249.166.0/24	Northwestern Affiliate
199.249.167.0/24	Northwestern Affiliate
199.249.168.0/24	Northwestern Affiliate

2. Internet domain names



Note: Northwestern owns 129.105.0.0/16 and 165.124.0.0/16

Domain Naming System (DNS)

- The Internet maintains a mapping between IP addresses and domain names in a huge worldwide distributed database called **DNS**

- Conceptually, programmers can view the DNS database as a collection of millions of **host entries**
  - Each host entry defines the mapping between a set of domain names and IP addresses

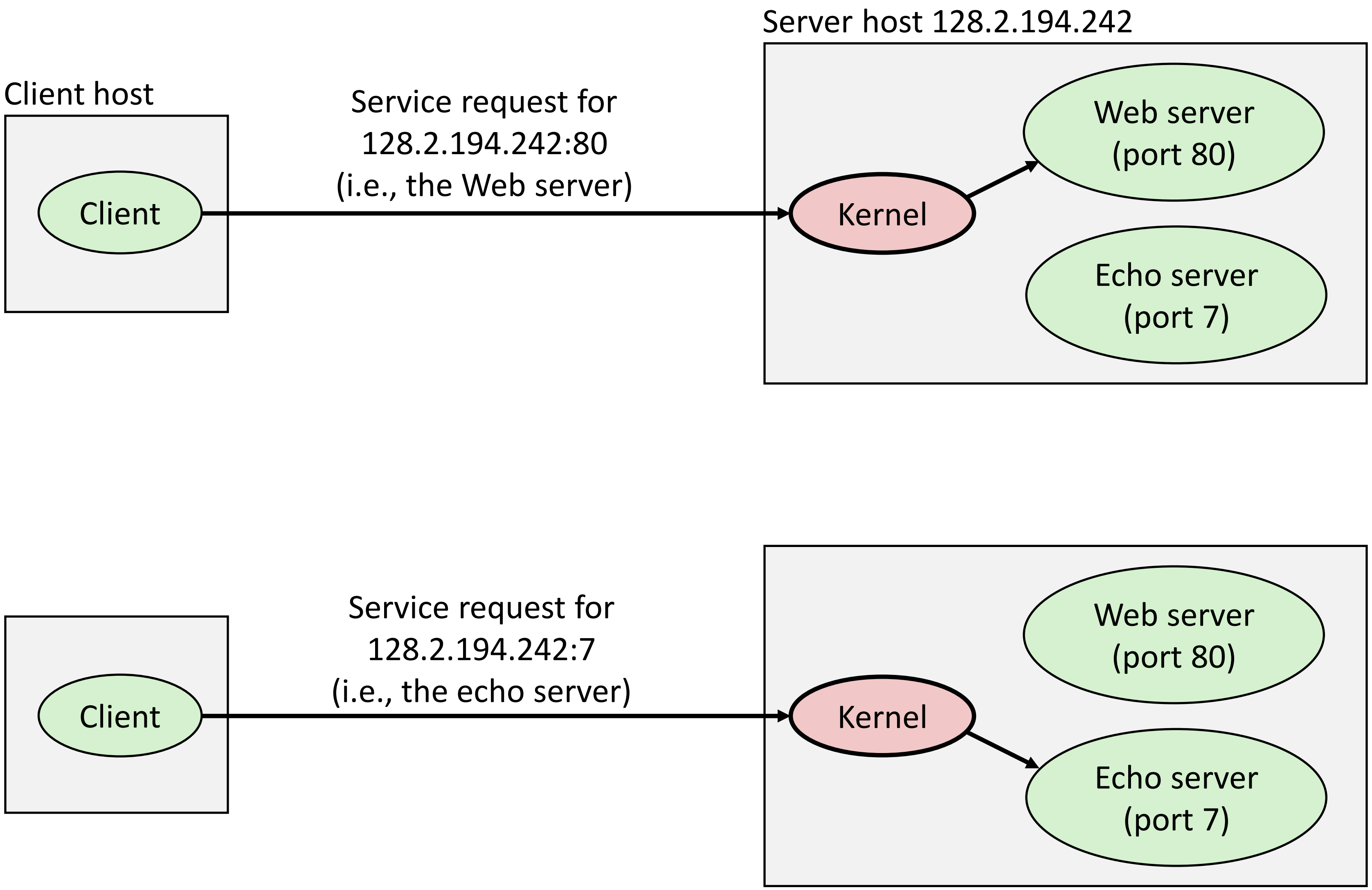
- A special name: **localhost**
  - Refers back to the computer being used (IP address 127.0.0.1)

3. Internet connections

- A socket is an endpoint of a connection
  - Socket address is an `IPaddress:port` pair
    - IP address identifies the computer
    - Port identifies the process on the computer

- Clients and servers communicate by sending streams of bytes over **connections**. Most connections are:
  - Point-to-point: connects a pair of processes.
  - Full-duplex: data can flow in both directions at the same time,
  - [TCP adds] Reliable: stream of bytes sent by the source is eventually received by the destination in the same order it was sent.

Ports are used to identify services to the kernel



How does the Internet handle routing packets?

- Network layer (IP)
  - Describes computer-to-computer connection
    - Packets from my computer <---> Google server

- Link layer (Ethernet)
  - Describes individual links
    - Packets from my computer <---> my router

- **Routing**
  - Using link-layer building blocks to get packets from one IP to another

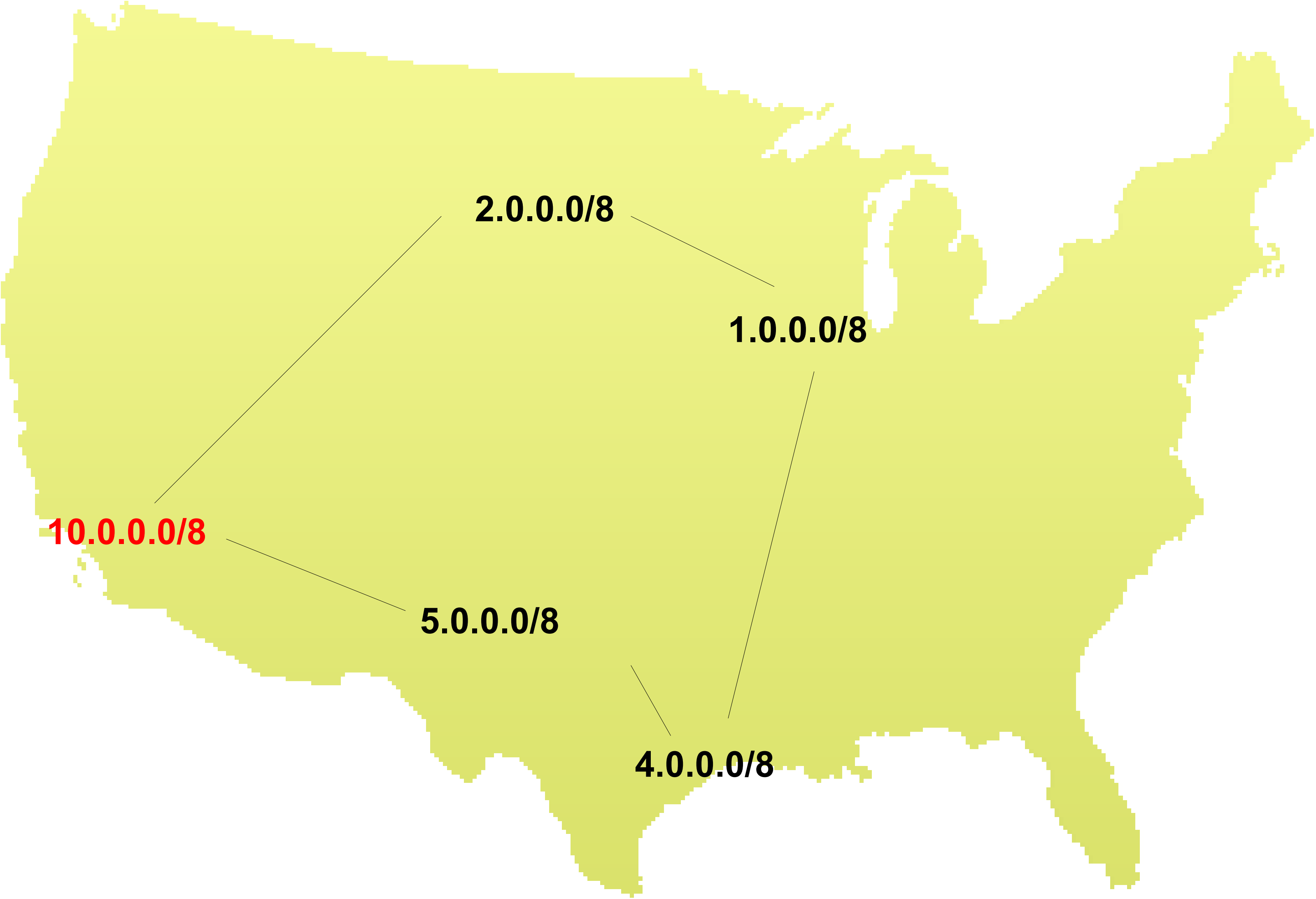
Assigning and finding IP address ranges

- In general, network operators don’t change that often

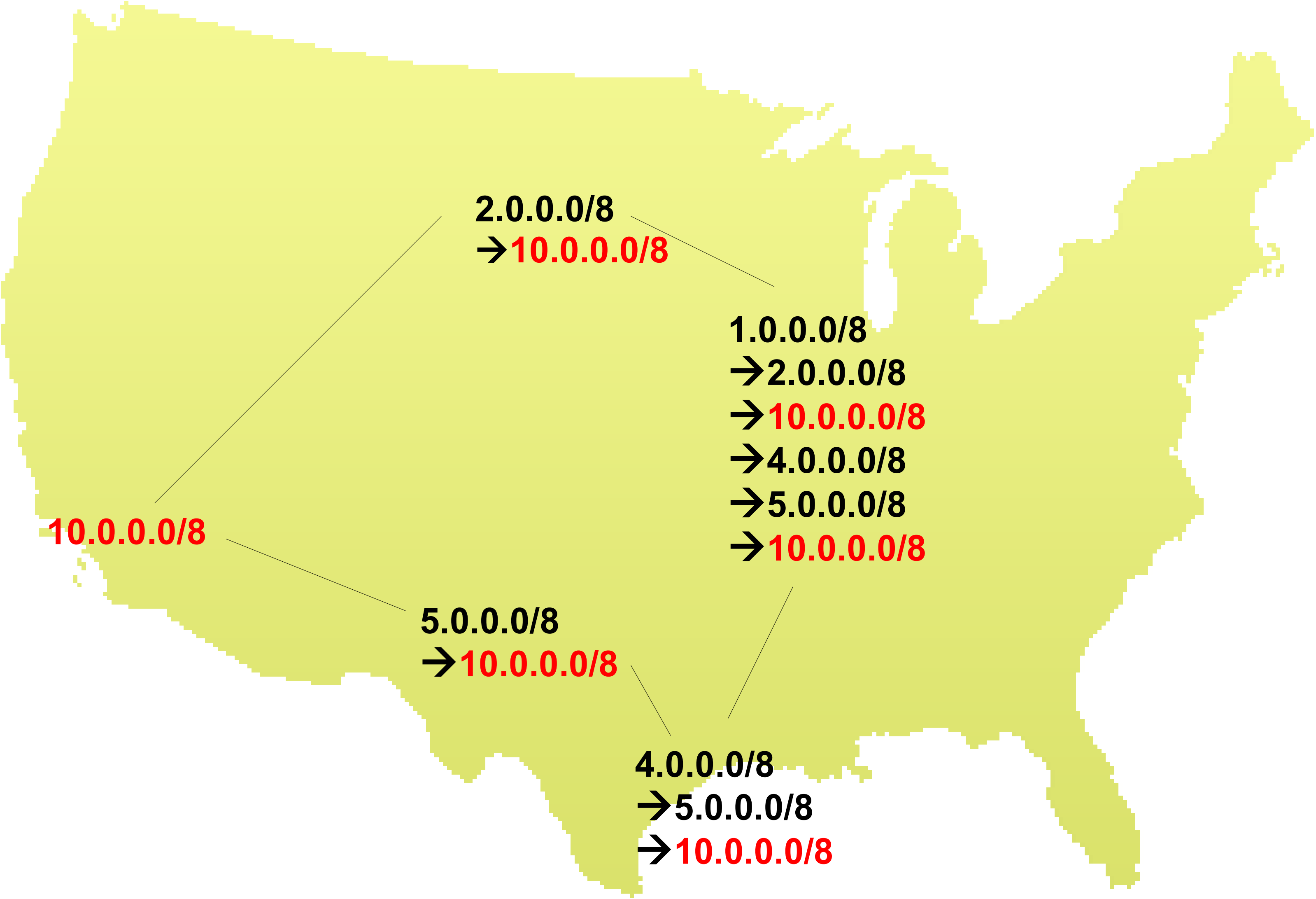
- Solution:
  - Tie IP addresses to network operators
  - Assign computers IPs as they join networks

- Key Point:
  - Networks ”own” a block of IP address space
  - ”The Internet” is a network of networks

Routing

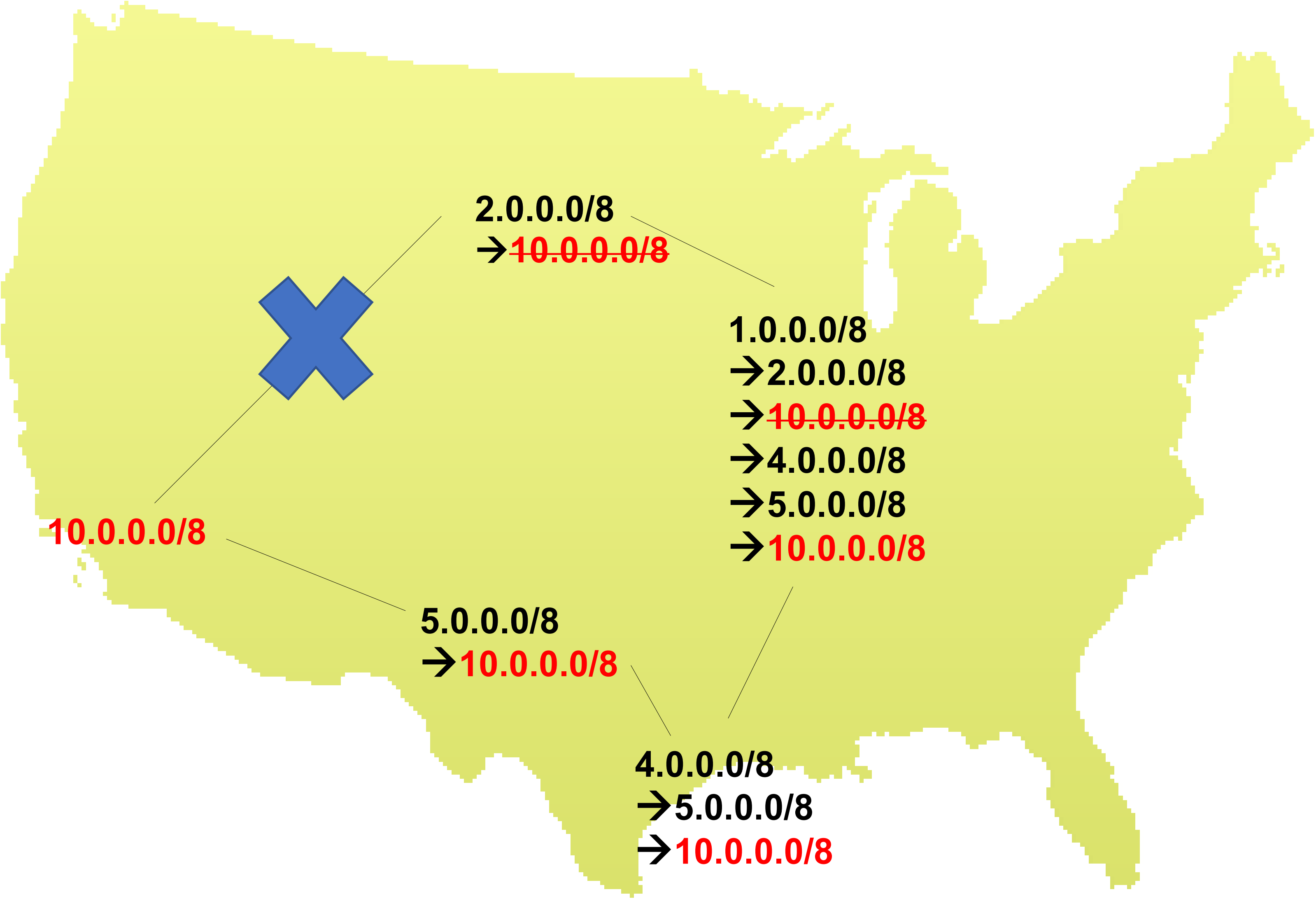


Routing



2.0.0.0/8
→10.0.0.0/8
1.0.0.0/8
→2.0.0.0/8
→10.0.0.0/8
→4.0.0.0/8
→5.0.0.0/8
→10.0.0.0/8
10.0.0.0/8
5.0.0.0/8
→10.0.0.0/8
4.0.0.0/8
→5.0.0.0/8
→10.0.0.0/8

Routing Adaptation



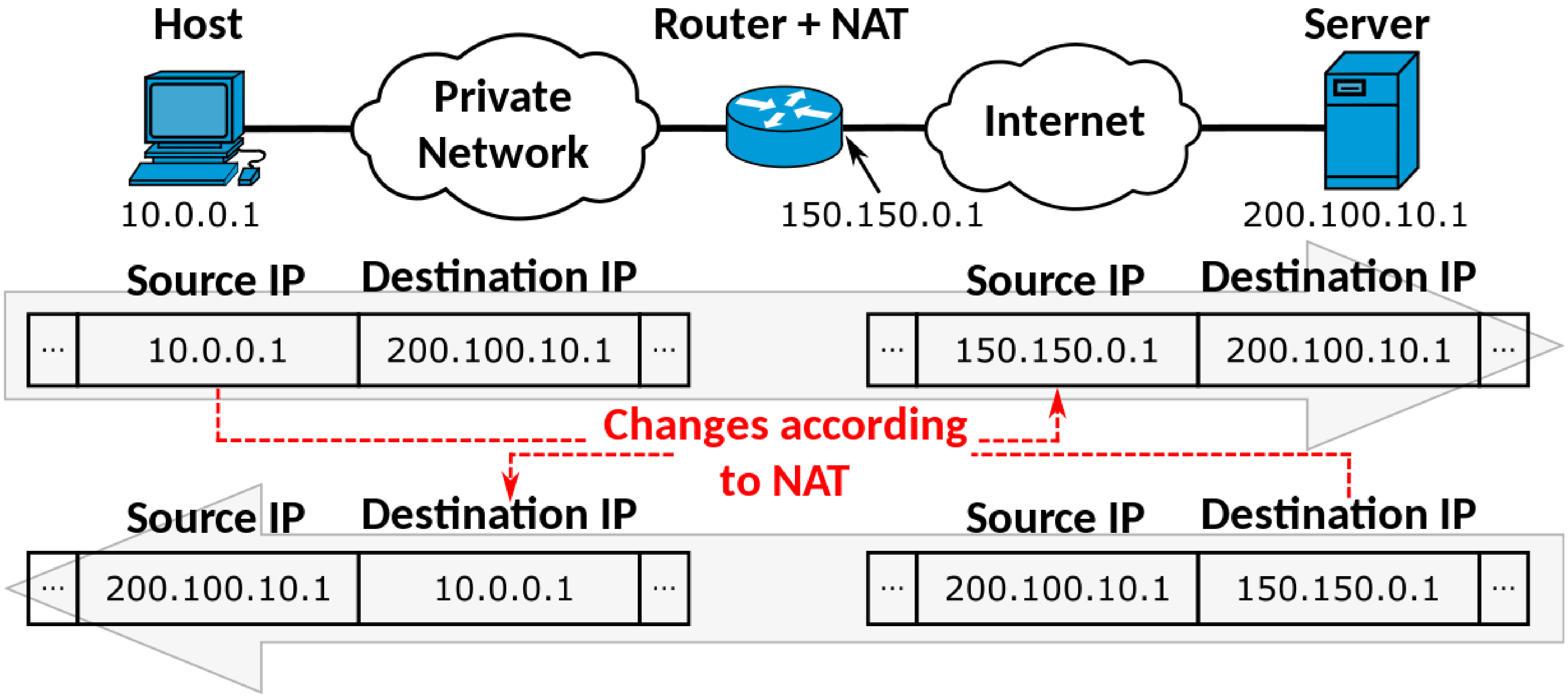
Identifying your computer?

- Every network card has its own MAC address
  - IPs are (somewhat) dynamic, ”owned” by local networks
  - MACs are hardware and static, ”owned” by specific computers
    - Manufacturers own blocks of MACs, ”spend” them each time they make a device

- ”Connecting” to a network
  - Your computer leases an IP from the local network
  - Only the local router knows your MAC, everyone else sees your IP

  - Actually, with NAT, you probably have a private IP address
    - This is how we make 32-bit addresses sufficient for the whole Internet

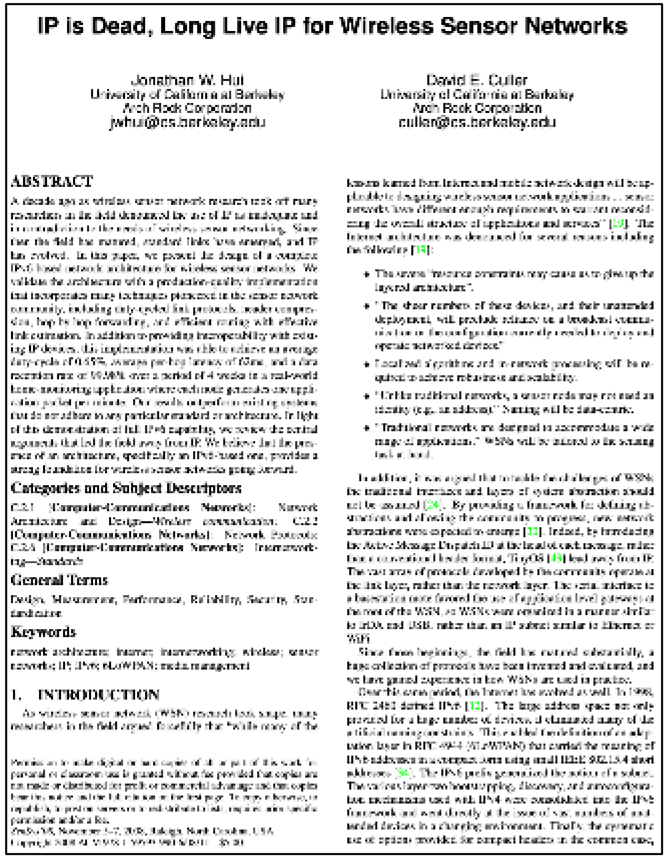
Network Address Translation (NAT)



- https://en.wikipedia.org/wiki/Network_address_translation

So how does the Internet of Things fit into the Internet?

- "IP is the Narrow Waist of the Internet"
  - [IP is Dead, Long Live IP for Wireless Sensor Networks]



IP is Dead, Long Live IP for Wireless Sensor Networks

Jonathan W. Hui
University of California at Berkeley
Arch Rock Corporation
jwhui@cs.berkeley.edu

David E. Culler
University of California at Berkeley
Arch Rock Corporation
culler@cs.berkeley.edu

ABSTRACT

Categories and Subject Descriptors

General Terms

Keywords

1. INTRODUCTION

- A recurring theme in this class:
  - How does this actually attach to the Internet
    - Physically, direct IP connection
      [hello Hue Hub, Wyze Hub, August Hub, …]
    - Logically, through another device
      [are BLE devices *really* part of the IoT?]

Break + Thinking

- What are the steps for viewing a website?

Break + Thinking

- What are the steps for viewing a website?

1. You enter a domain name for the website
2. Computer looks up domain name to get IP Address
3. Computer sends request to IP_address:80
4. Computer gets back data, which it renders into a website

ALL the layers

- A ‘famous’ interview question
  - “What happens when you type google.com into your browser’s address bar and press enter?”
  - https://github.com/alex/what-happens-when
    - 12 pages worth of material
      - Keyboard events
      - Parsing URL
      - DNS lookup
      - Opening socket
      - HTTP protocol
      - HTML parsing
      - GPU rendering

Outline

- OSI Layers
- Internet Architecture (Upper Layers)
- **Physical Layer**
  - **Overview**
  - Signal Strength
  - Signal Frequency and Bandwidth
  - Signal Modulation

Physical Layer

- How bits are transmitted
  - Wireless makes this entirely different from wired cases

- Important considerations
  - Signal strength
  - Modulation
  - Frequency

Why use wireless?

- There are no wires!

- No need to install and maintain wires
  - Reduces cost
  - Simplifies deployment – place devices wherever makes sense

- Supports mobile users
  - Move around office, campus, city
  - Move devices around home

What is hard about wireless?

- There are no wires!

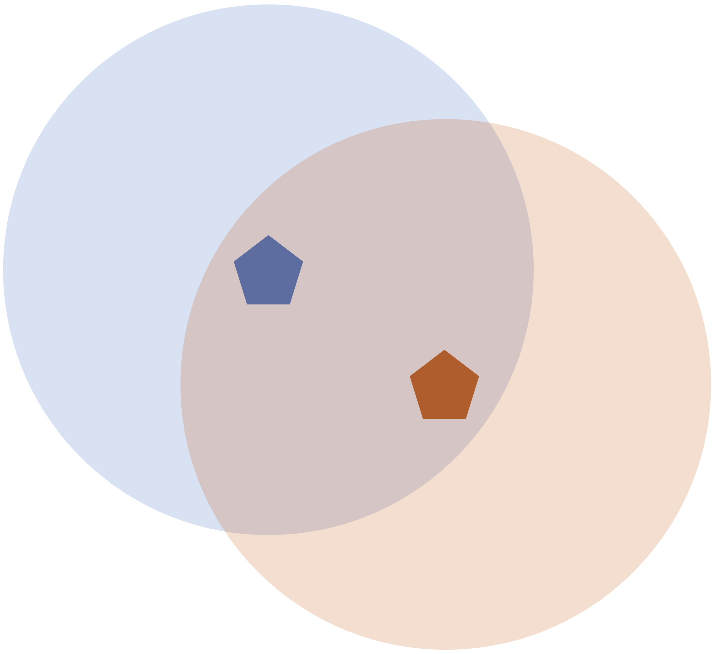
- Wired networks are constant, reliable, and physically isolated
  - Ethernet has the same throughput minute-to-minute
  - Bits sent through Ethernet or USB are (usually) received

- Wireless networks are variable, error-prone, and shared
  - WiFi throughput changes based on location and walls
  - Signals from nearby devices interfere with your signals
  - Individual bits might flip or never be heard at all

Wireless is a shared medium

- Wired communication has signals confined to a conductor
  - Copper or fiber
  - Guides energy to destination
  - Protects signal from interference

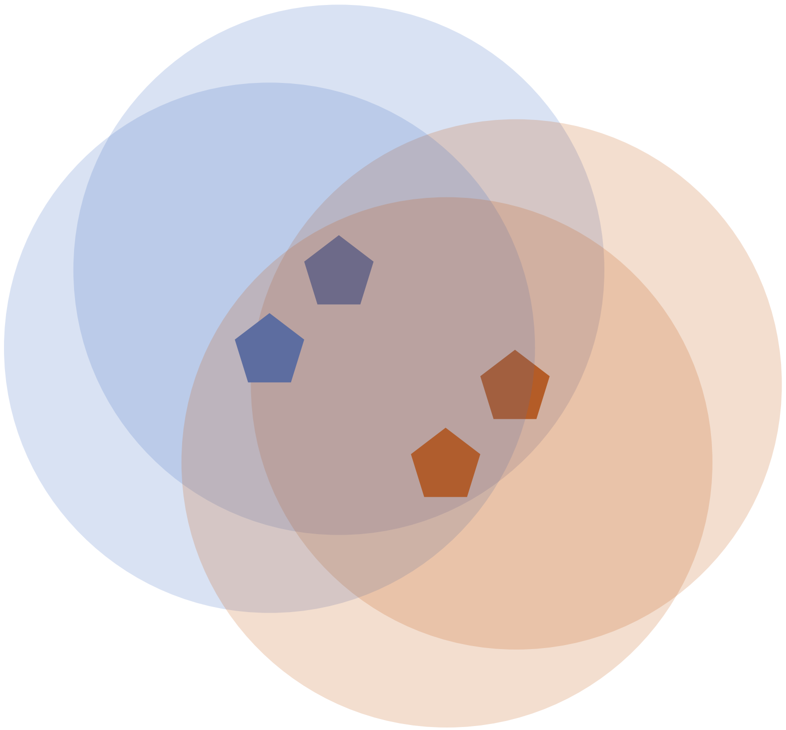
- Wireless communication is inherently broadcast
  - Energy is distributed in space
  - Signals must compete with other signals in same frequency band



Increasing network capacity is challenging

- Wired networks just add more wires
  - Buses are many signals in parallel to send more data

- Wireless networks are harder
  - Adding more links just increases interference
  - Need to expand to different frequencies

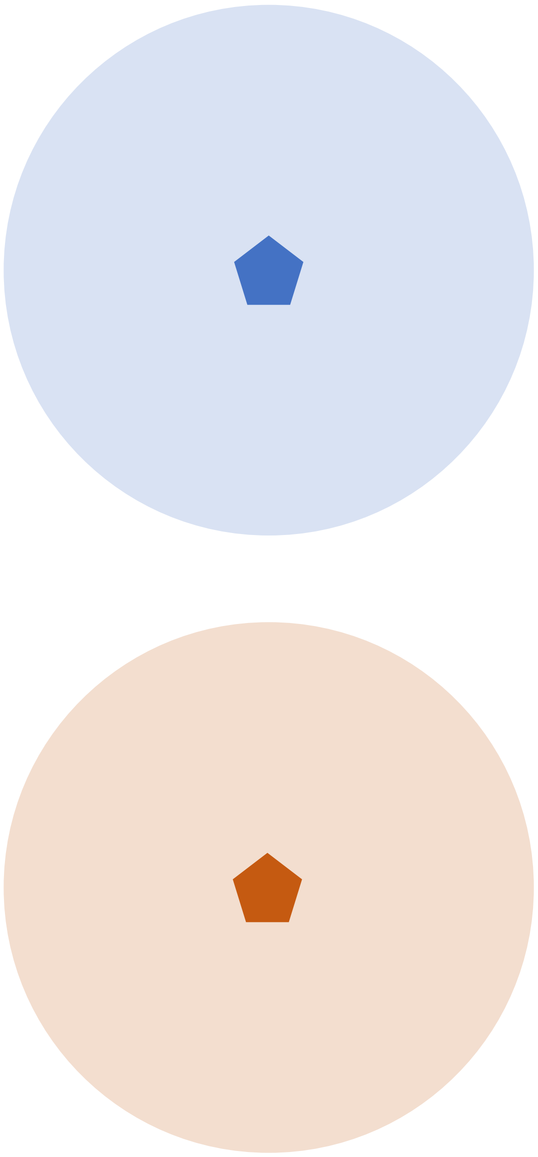


Model of RF communication

- Energy that radiates spherically from an antenna

- Attenuation with distance
    - Density of energy reduces over time, distance
    - Signal strength is reduced, errors go up

- Two key features
    - Error rates depend on distance
    - Spatial reuse of frequencies

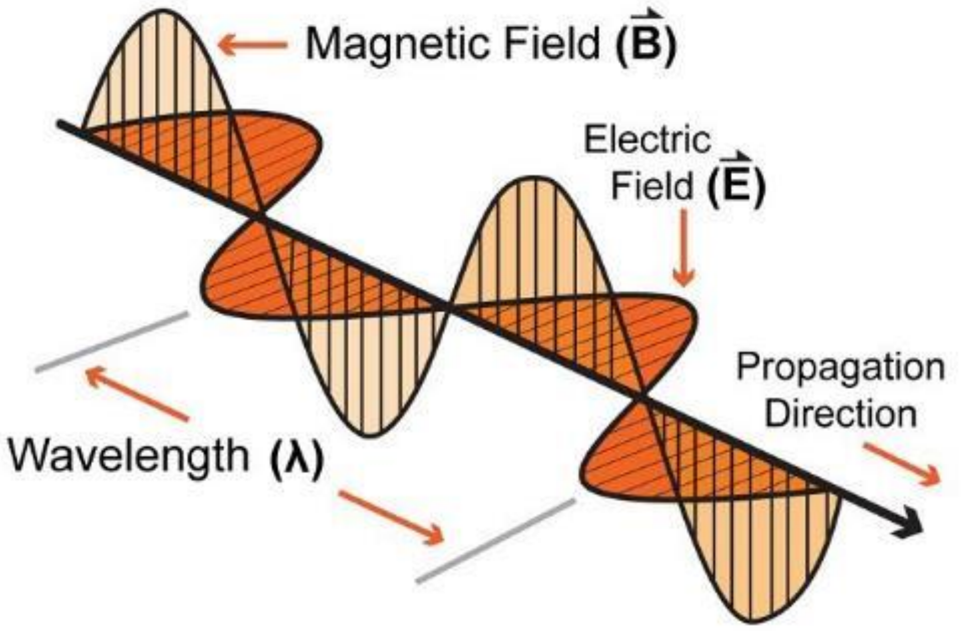


Signal qualities

1. Signal strength
   - The amount of energy transmitted/received

2. Signal frequency and bandwidth
   - Which "channel" the signal is sent on

3. Signal modulation
   - How data is encoded in the signal

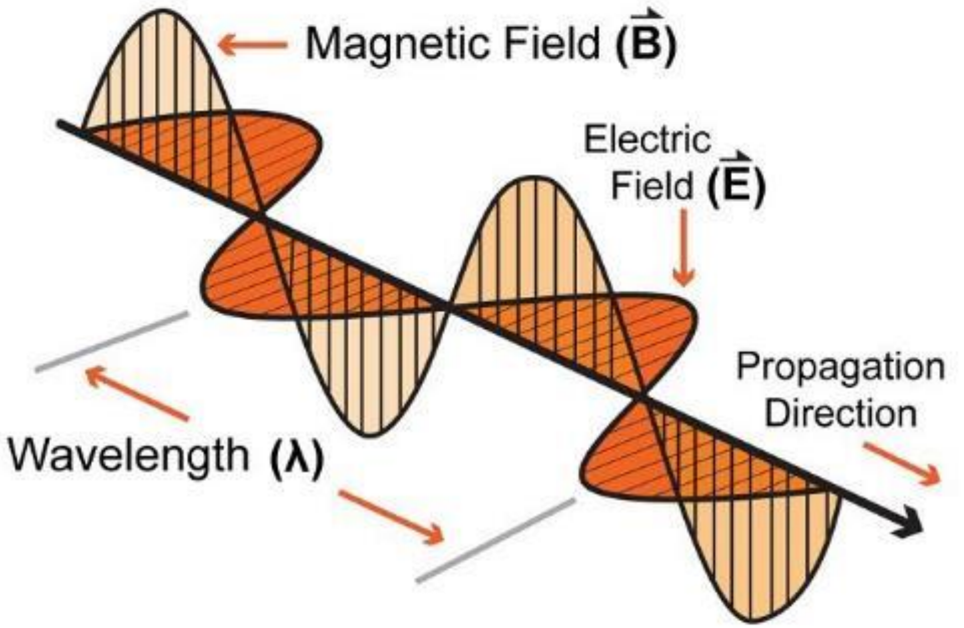


Outline

- OSI Layers
- Internet Architecture (Upper Layers)
- **Physical Layer**
  - Overview
  - **Signal Strength**
  - Signal Frequency and Bandwidth
  - Signal Modulation

Signal qualities

1. **Signal strength**
   - The amount of energy transmitted/received
2. Signal frequency and bandwidth
   - Which "channel" the signal is sent on
3. Signal modulation
   - How data is encoded in the signal



Signal strength is measured in decibels

- Power is measured in Watts or dBw or dBm
  - $Power_{\mathrm{dBw}} = 10 * \log_{10}(Power_{Watts})$
  - $Power_{\mathrm{dBm}} = 10 * \log_{10}(Power_{milliwatts})$

- dBm is most relevant to the IoT domain
  - 0 dBm equals 1 mW transmit power
  - Example
    - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
    - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)

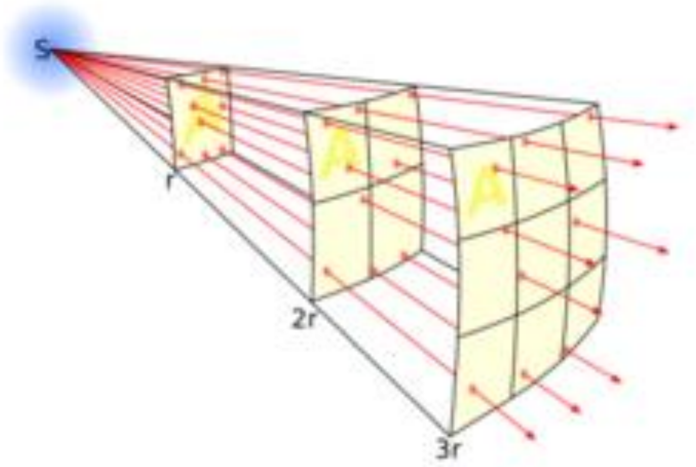
- Rule of thumb: +3 dB is double the power

Signal strength varies significantly across technologies

- Bluetooth Low Energy (local area)
  - nRF52840 transmit power: 8 dBm (6.31 mW)
  - nRF52840 receive sensitivity: -95 dBm (316.2 fW)

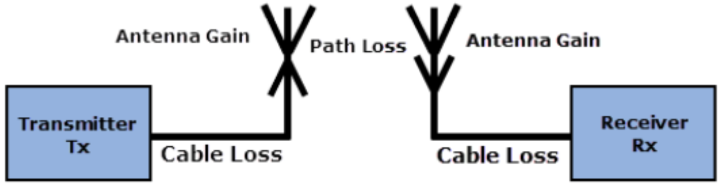
- LoRa (wide area)
  - SX127X LoRa transmit power: 20 dBm (100 mW)
  - SX127X LoRa receive sensitivity: -148 dBm (1.6 attoWatt)

Propagation degrades RF signals



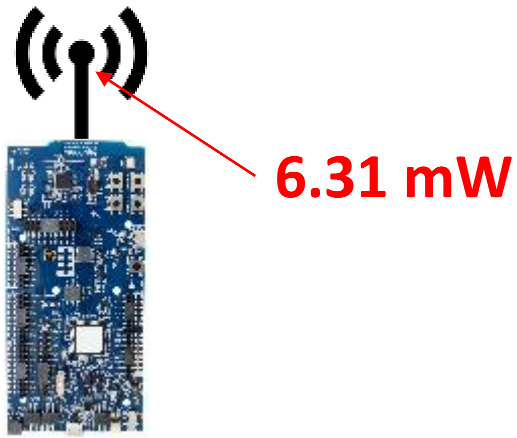
- Attenuation in free space
  - Signals get weaker as they travel over long distances
  - Signal spreads out → Free Space Path Loss (FSPL)

$$FSPL = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) - G_t - G_r$$



Some intuitions for signal propagation, power, gain, etc

- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840:   8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)



Wait, where is the antenna??

- This little strip of metal is the actual antenna
  - Receiver only recovers the part of the signal that hits its antenna ("aperture")

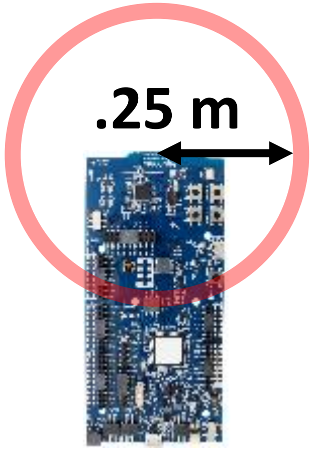
Some Intuitions for Signal Propagation, Power, Gain, etc.

- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)

6.31 mW

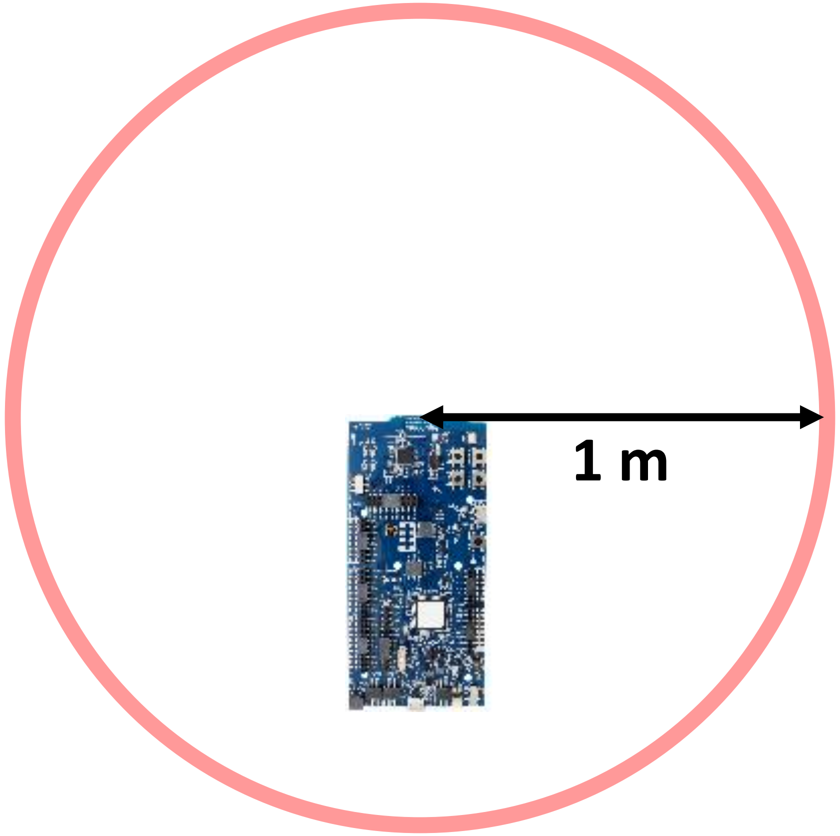
Some Intuitions for Signal Propagation, Power, Gain, etc.

- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)



Some Intuitions for Signal Propagation, Power, Gain, etc.

- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)

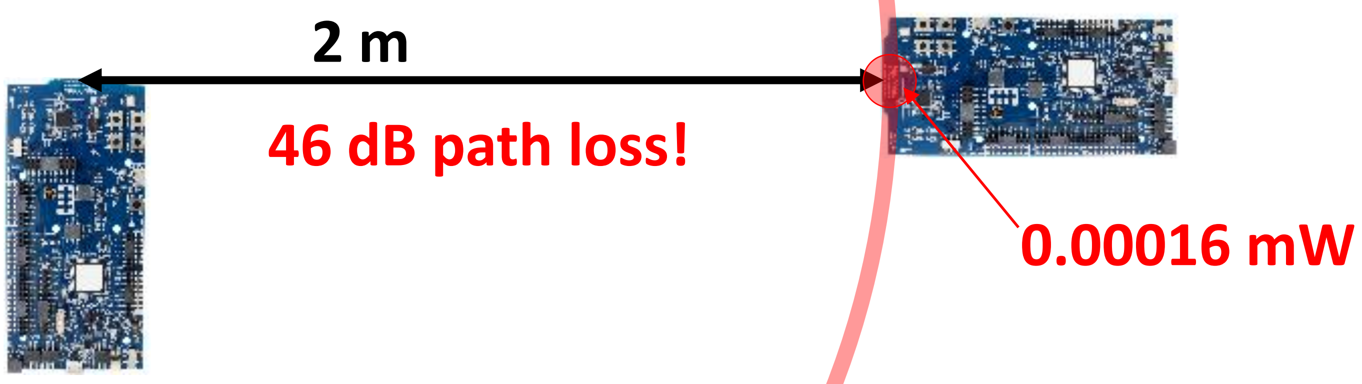


Some Intuitions for Signal Propagation, Power, Gain, etc.

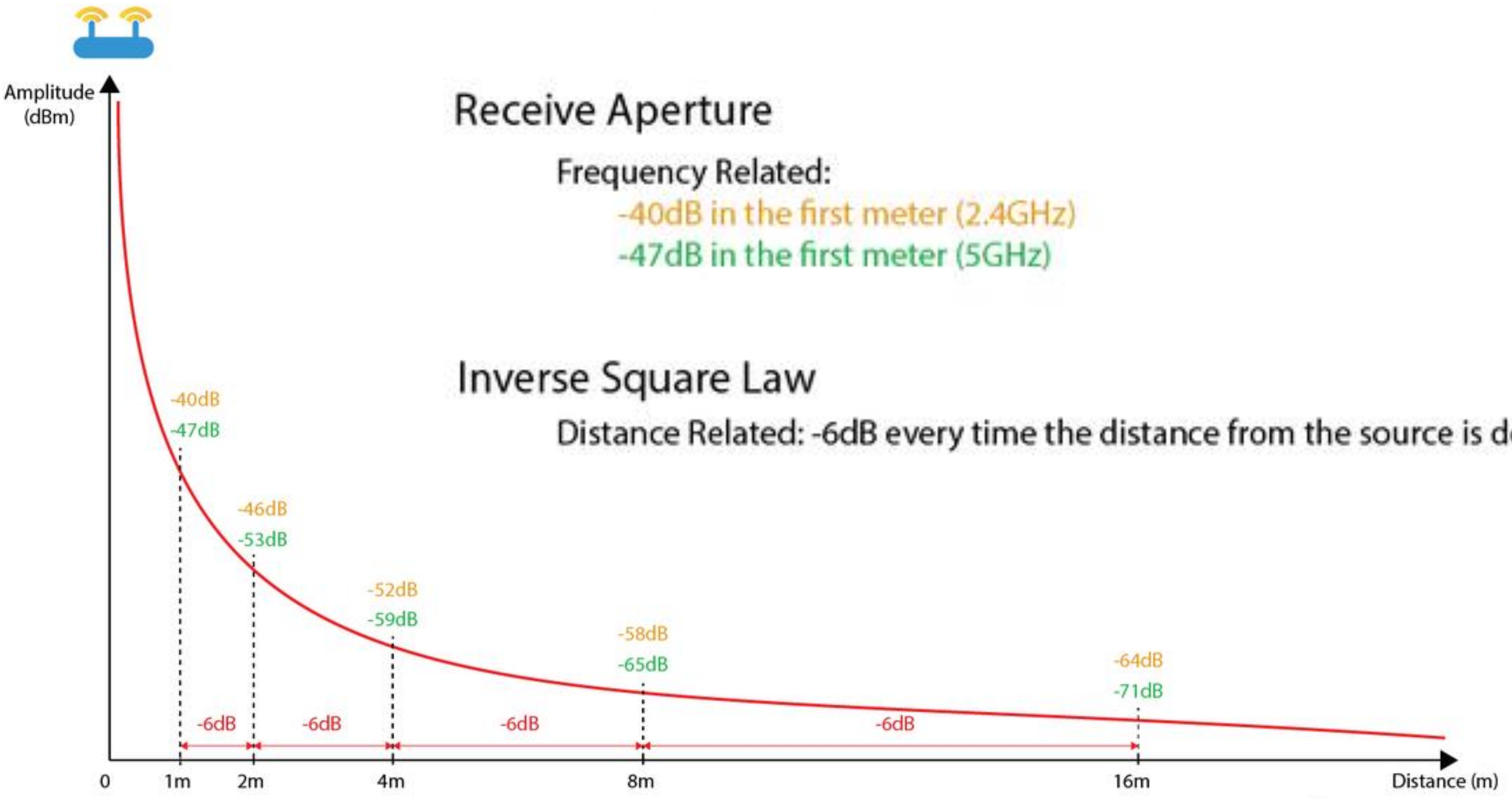
- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)

Some Intuitions for Signal Propagation, Power, Gain, etc.

- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)



Free-Space Path Loss Model



https://semfionetworks.com/blog/free-space-path-loss-diagrams/

Okay.. So what's the limit?

- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)

- 8 dBm - -95 dBm = 103 dB link margin

- With Free Space Path Loss model:
  - 103 dB corresponds to 1400 meter range!
  - Can anyone get 1.4 km on their Bluetooth headphones?

Propagation is *one thing* that degrades RF signals

- Attenuation in free space
  - Signals get weaker as they travel over long distances
  - Signal spreads out -> free space path loss

- Important: distance is NOT the only signal strength loss
  - Free space path loss calculation will not give you accurate range for a signal

- Obstacles can weaken signal through absorption or reflection
  - Precise quantitative details are in the EE domain
  - We'll use examples to develop qualitative instincts in this class

ITU model for Indoor Attenuation

$$L = 20 \log_{10} f + N \log_{10} d + P_f(n) - 28$$

where,

L = the total path loss. Unit: decibel (dB).

f = Frequency of transmission. Unit: megahertz(MHz).

d = Distance. Unit: meter (m).

N = The distance power loss coefficient.

n = Number of floors between the transmitter and receiver.

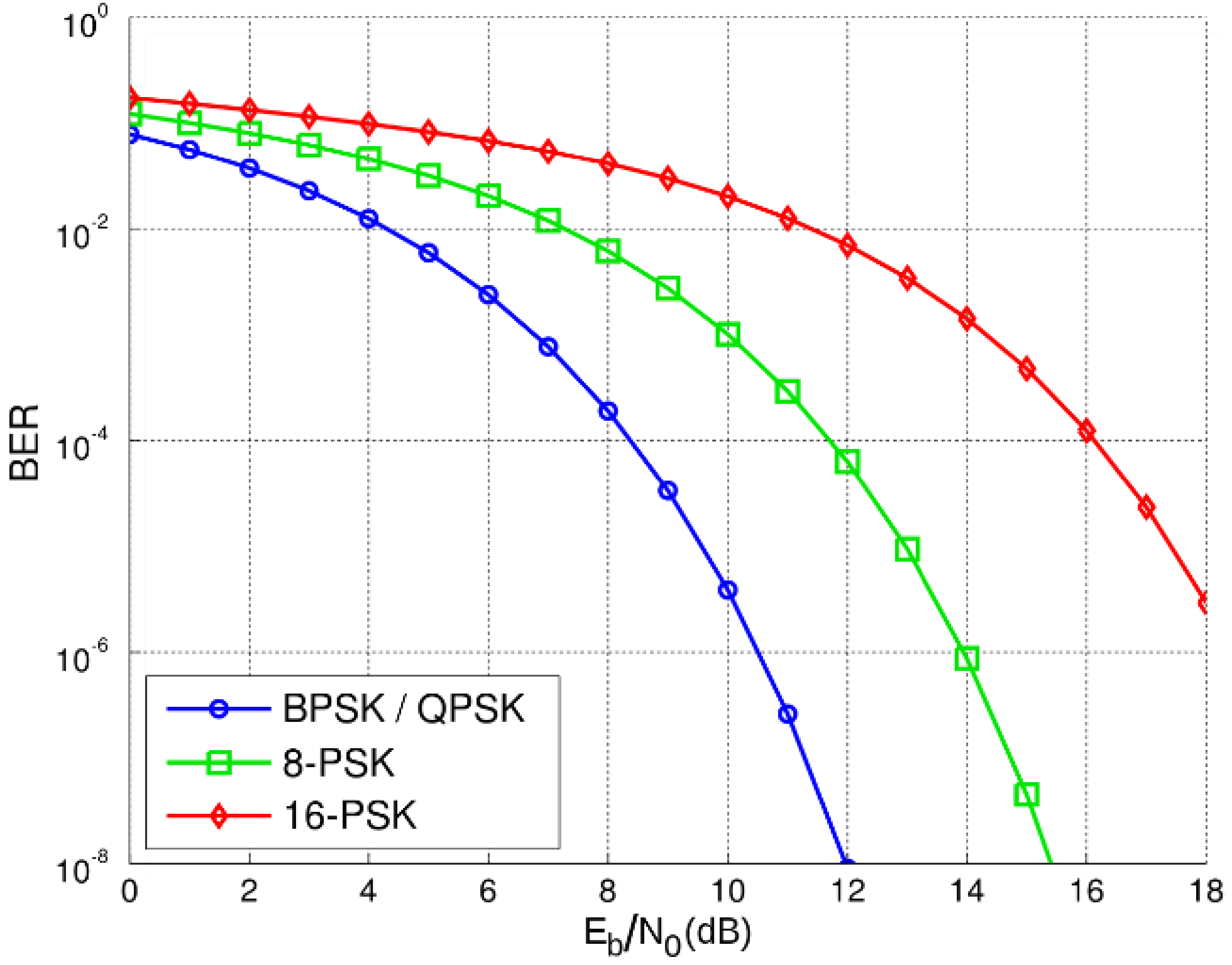
$P_f(n)$ = the floor loss penetration factor.

- Models like this are ~~more trustworthy~~ *less bad* than Free-Space Path Loss
  - https://en.wikipedia.org/wiki/ITU_model_for_indoor_attenuation

Lower received energy increases error rates

More Errors

Less Errors



Less Energy Received

More Energy Received

BER:
Bit Error Rate

Odds that a transmitted bit will be received incorrectly

Big Idea: many RF factors are interconnected

- Energy, Distance, Throughput, and Reliability are all interconnected in communication

- Protocols make choices of some and get the results on the others

- To get more distance, choose one or more:
  - Increase energy
  - Communicate slower
  - Accept a higher error rate

Break + Say hi to your neighbors

- Things to share
  - Name

  - Major

  - One of the following
    - Favorite Candy
    - Favorite Pokemon
    - Favorite Emoji

Break + Say hi to your neighbors

- Things to share
  - Name -Branden
  - Major -EE, CE, and CS
  - One of the following
    - Favorite Candy - Twix
    - Favorite Pokemon - Eevee
    - Favorite Emoji - 🍢

Outline

- OSI Layers

- Internet Architecture (Upper Layers)

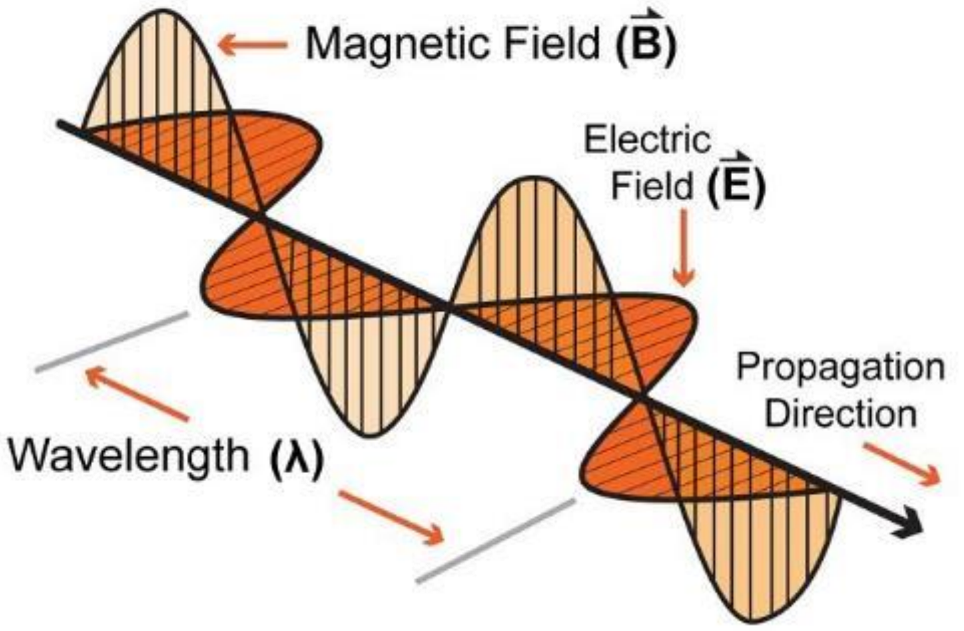
- **Physical Layer**
  - Overview
  - Signal Strength
  - **Signal Frequency and Bandwidth**
  - Signal Modulation

Signal qualities

1. Signal strength
   - The amount of energy transmitted/received

2. **Signal frequency and bandwidth**
   - Which “channel” the signal is sent on

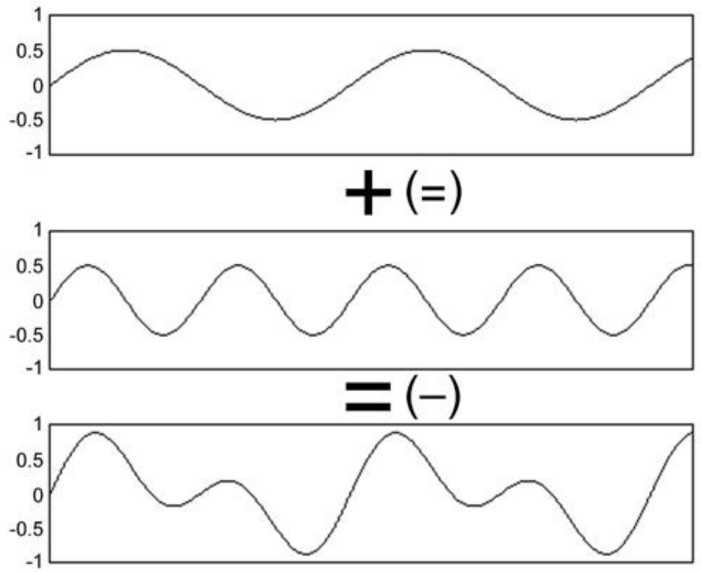
3. Signal modulation
   - How data is encoded in the signal

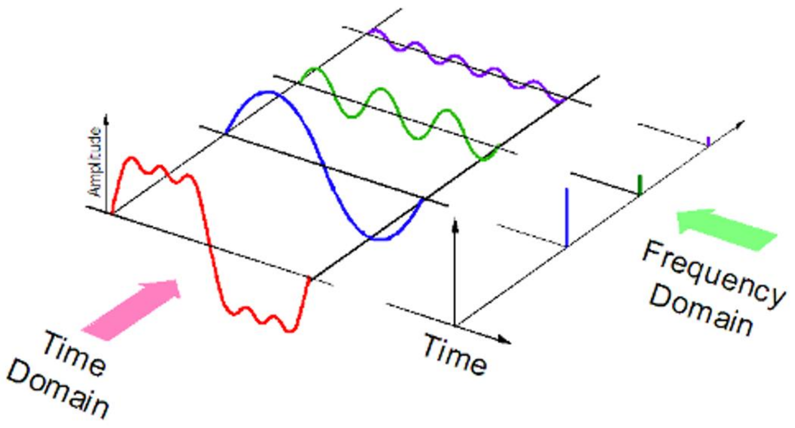


Sum of sinusoids can be reversed

- RF signals are fundamentally sinusoids of electromagnetic energy

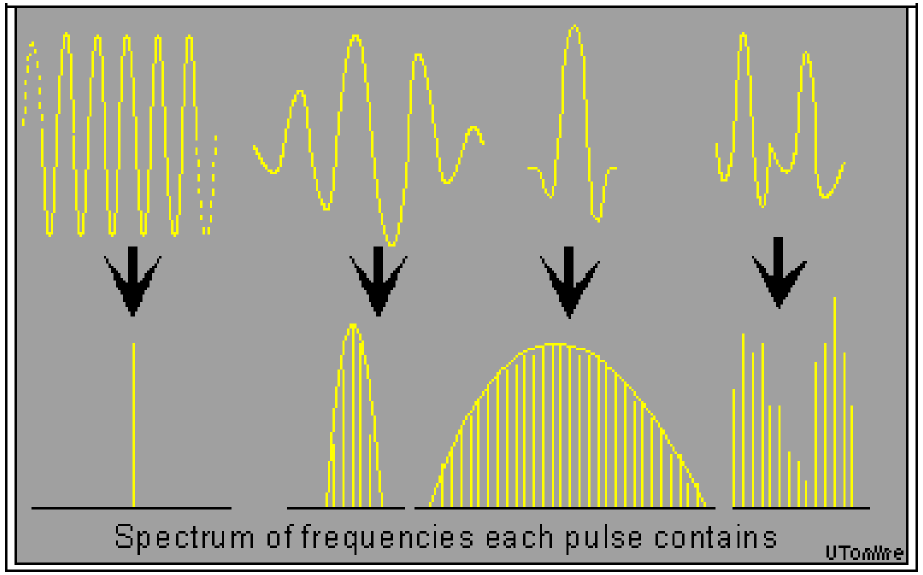
- Sinusoids at different frequencies can be combined and pulled apart again later
  - Particularly, it's relatively easy for hardware to determine if there's energy present on a given frequency
  - Although very close frequencies might be difficult to disentangle





Complex waveforms have a center frequency and a width

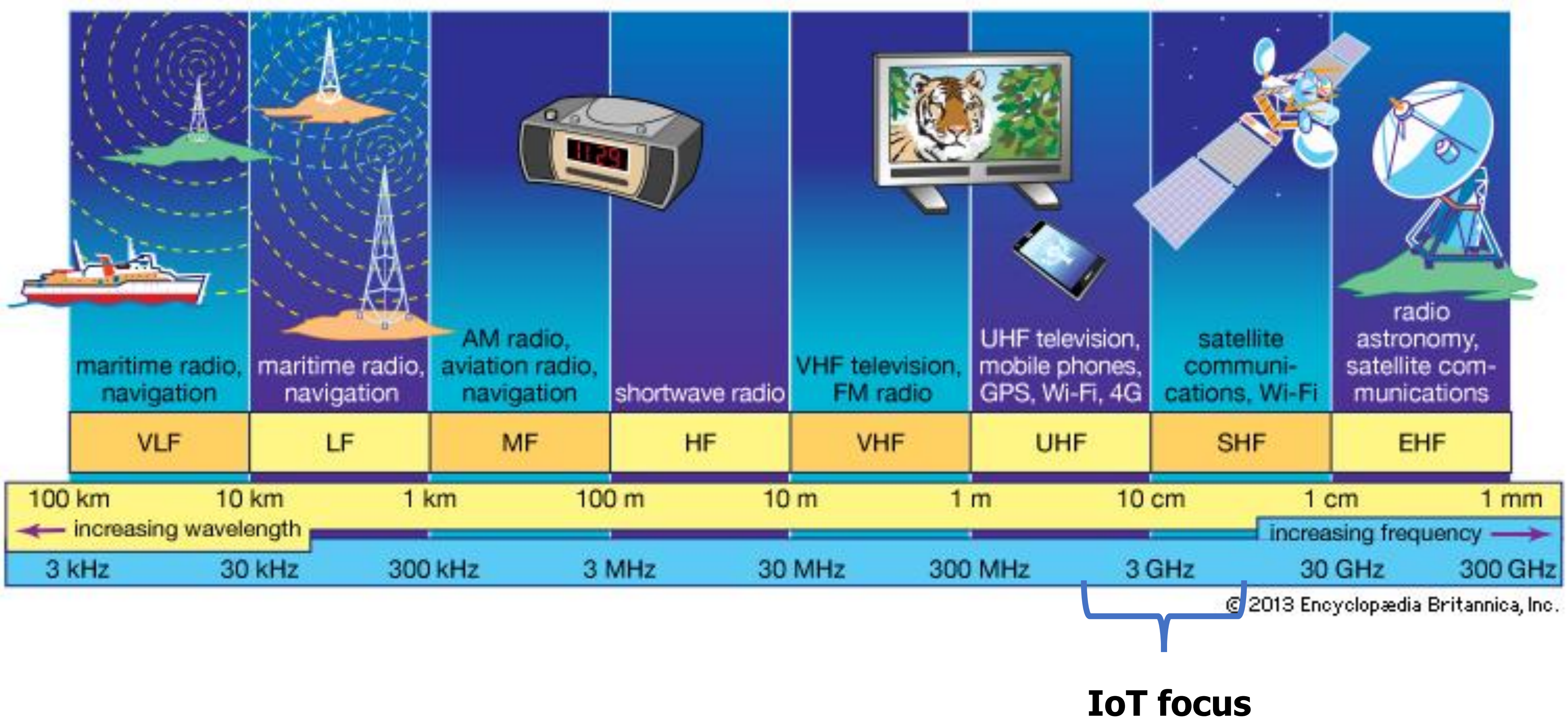
- A pure sinusoid is energy at exactly one frequency
- A messy sinusoid with data layered on top of it has nearby energy
  - There's a center of the signal energy
  - Plus some amount of width, which depends on how complicated the data layered on top is



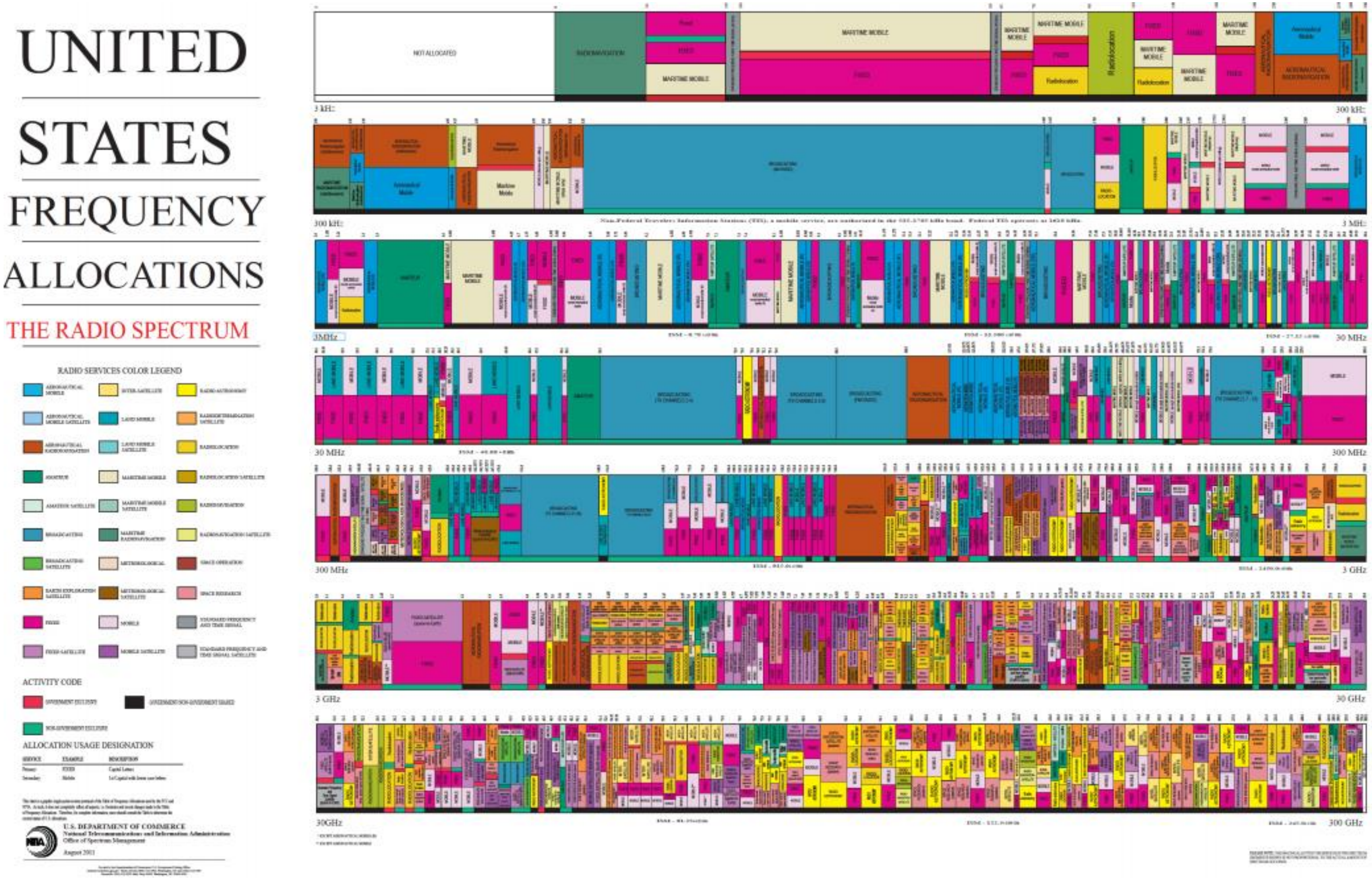
How do radio stations work?

- FM radio in cars is a good example of frequencies
  - All of FM radio has an allocation of 87.5 to 108.0 MHz
  - Each station takes has up to ~200 kHz of bandwidth
- First station is 87.7 MHz +/- 100 kHz
  - Ranges from 87.6 to 87.8
- Second station is 87.9 MHz +/- 100 kHz
  - Ranges from 87.8 to 88.0
- What if they overlapped? They interfere with each other
  - You’d possibly hear both. Or get junk data that’s neither.

RF communication frequencies



Wireless spectrum is allocated to specific uses

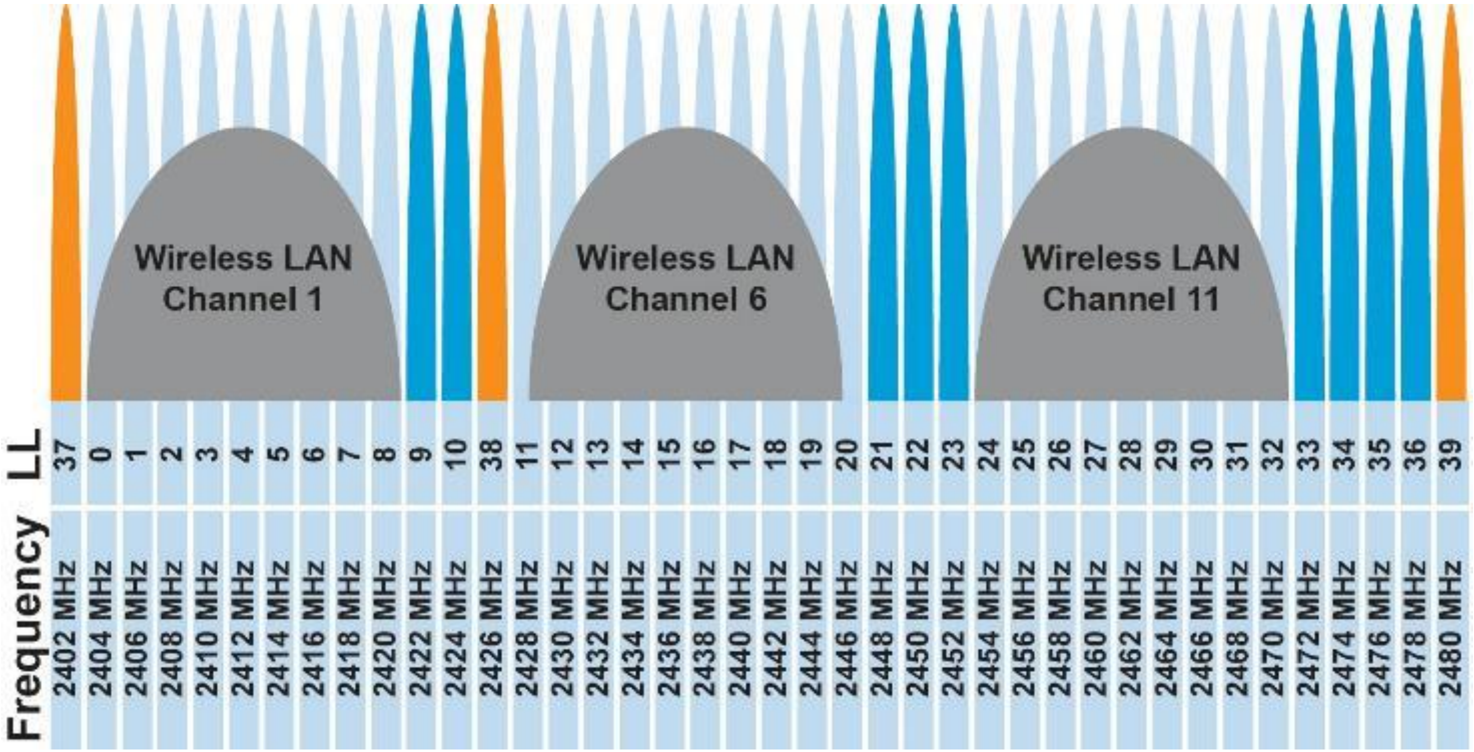


433 MHz Band

- Amateur radio (ham radio) was provided with specific frequencies to use
  - There are quite a few: https://en.wikipedia.org/wiki/Amateur_radio_frequency_allocations
- 433 MHz is within one of these bands in the US but globally is set aside as its own thing
  - Designated for low-power devices
  - Unlicensed use
  - Vehicle key-less entry devices, garage door openers, weather stations
    - Some IoT protocols use it as well! LoRa for example

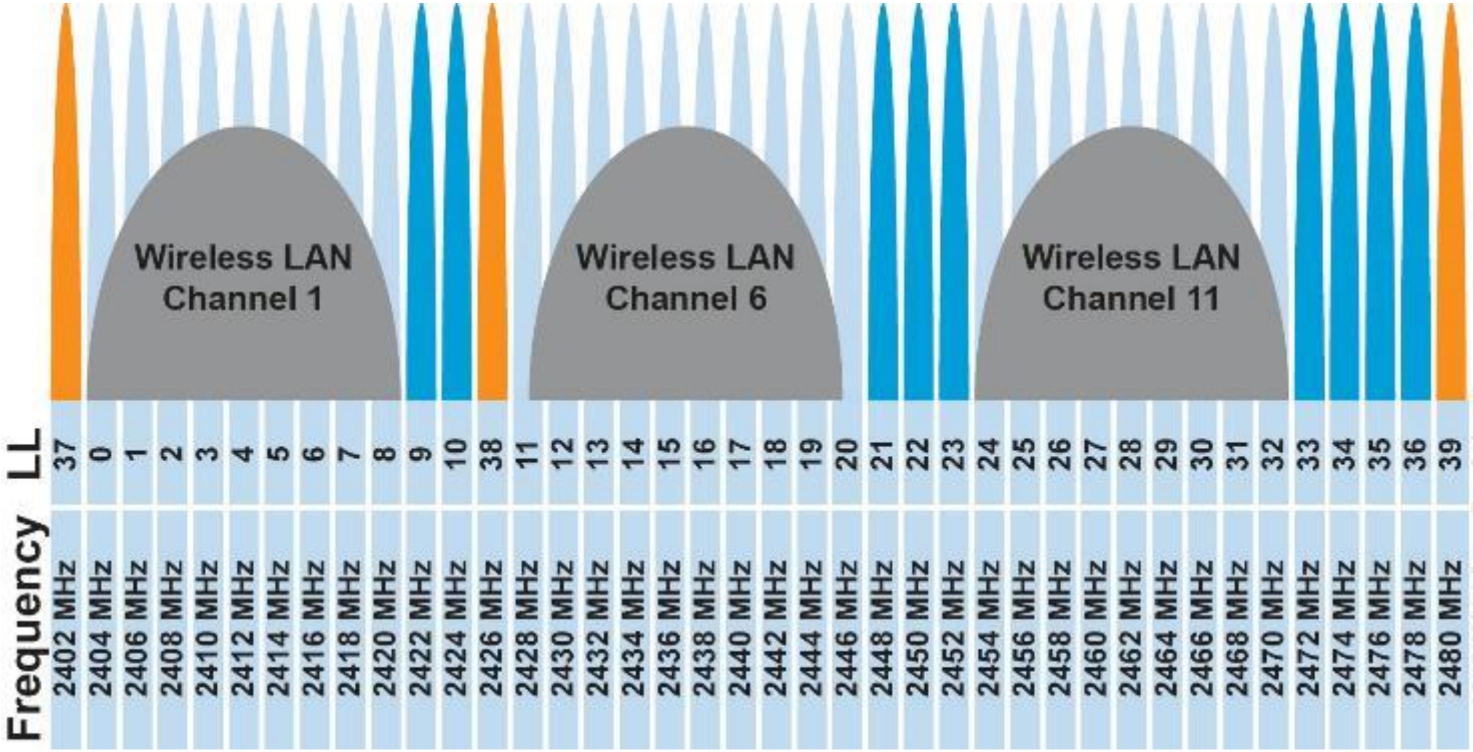
Unlicensed bands are where IoT thrives

- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi



Unlicensed bands are where IoT thrives

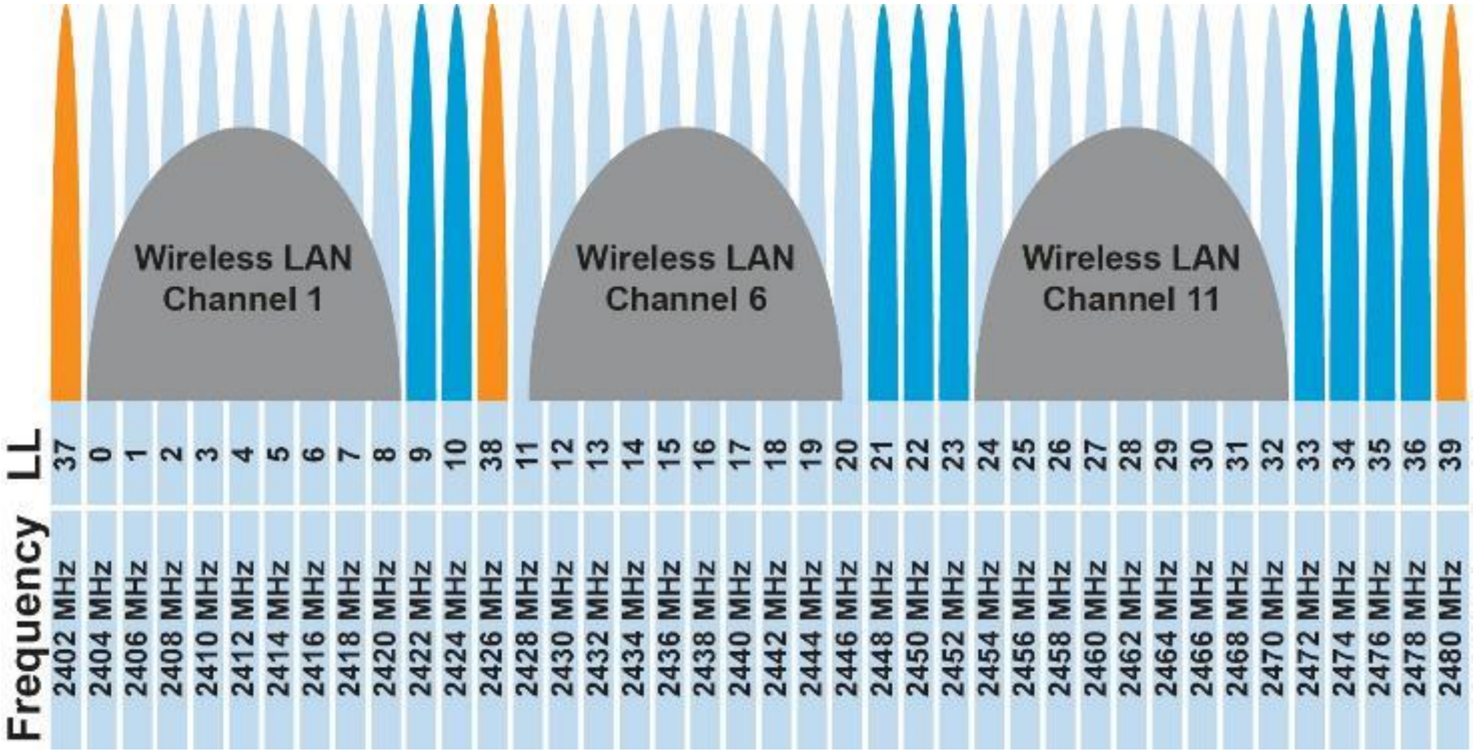
- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi



- Cellular uses licensed bands at great cost
  - **Why?**

Unlicensed bands are where IoT thrives

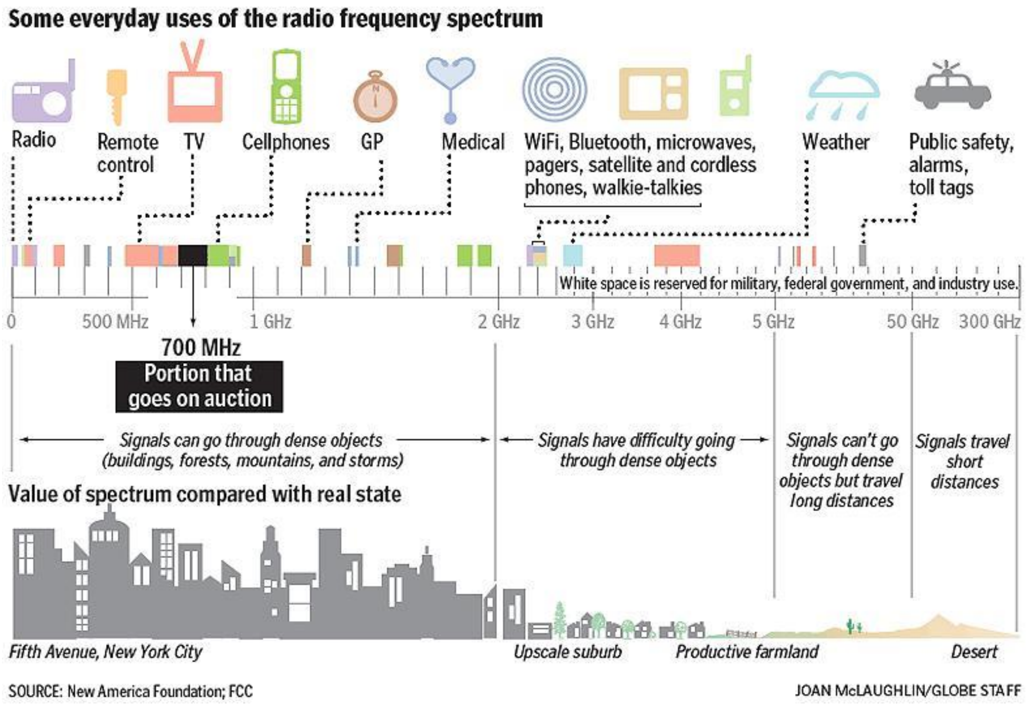
- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi

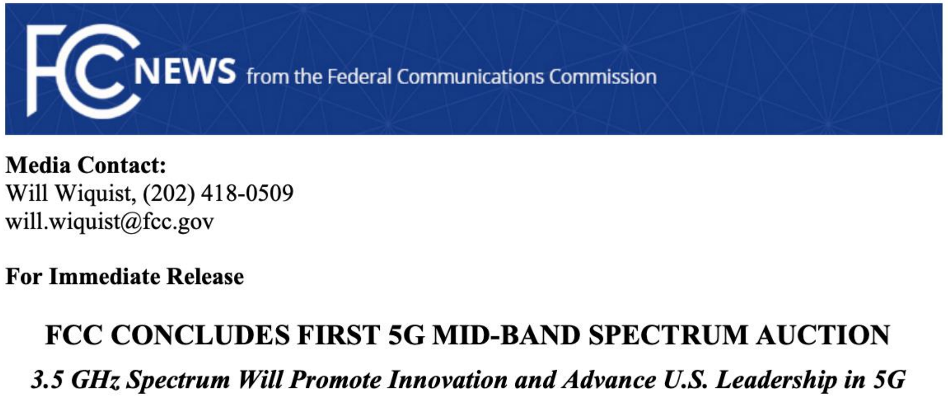


- Cellular uses licensed bands at great cost
  - **Why? No interference from other users**

Wireless spectrum is limited…and valuable

- FCC auctions blocks in US
- August 2020
  - 70 MHz in 3.5 GHz spectrum
  - $4.6 billion
- February 2021
  - 300 MHz in 3.7-9 GHz spectrum
  - $81 billion




FCC NEWS from the Federal Communications Commission

Media Contact:
Will Wiquist, (202) 418-0509
will.wiquist@fcc.gov

For Immediate Release

FCC CONCLUDES FIRST 5G MID-BAND SPECTRUM AUCTION

3.5 GHz Spectrum Will Promote Innovation and Advance U.S. Leadership in 5G


WIRELESS

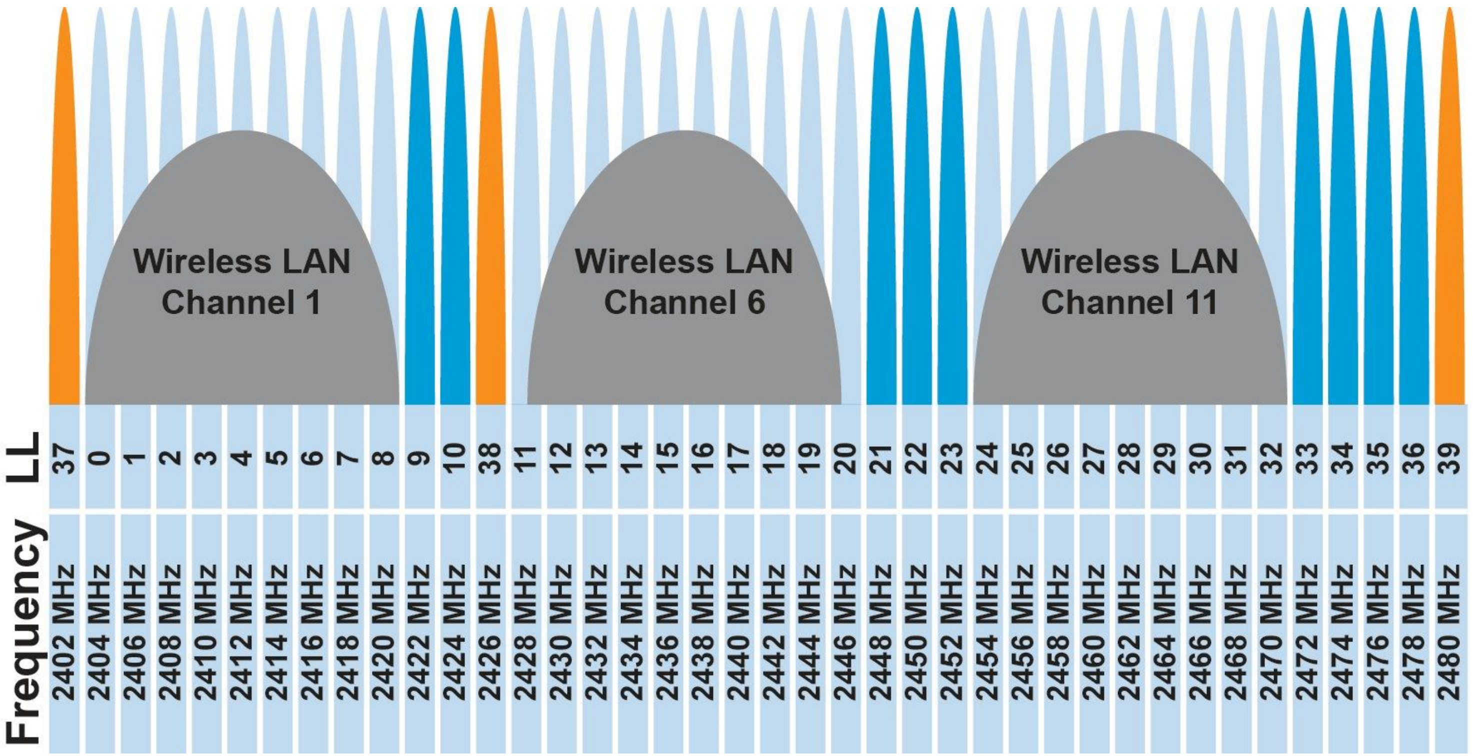
T-Mobile pays $304M to fill in holes in its 2.5 GHz spectrum

By Linda Hardesty · Sep 1, 2022 5:39pm

T-Mobile | 2.5 GHz | spectrum auction

https://www.fiercewireless.com/wireless/t-mobile-pays-304m-fill-holes-its-25-ghz-spectrum

Different technologies use spectrum in different ways

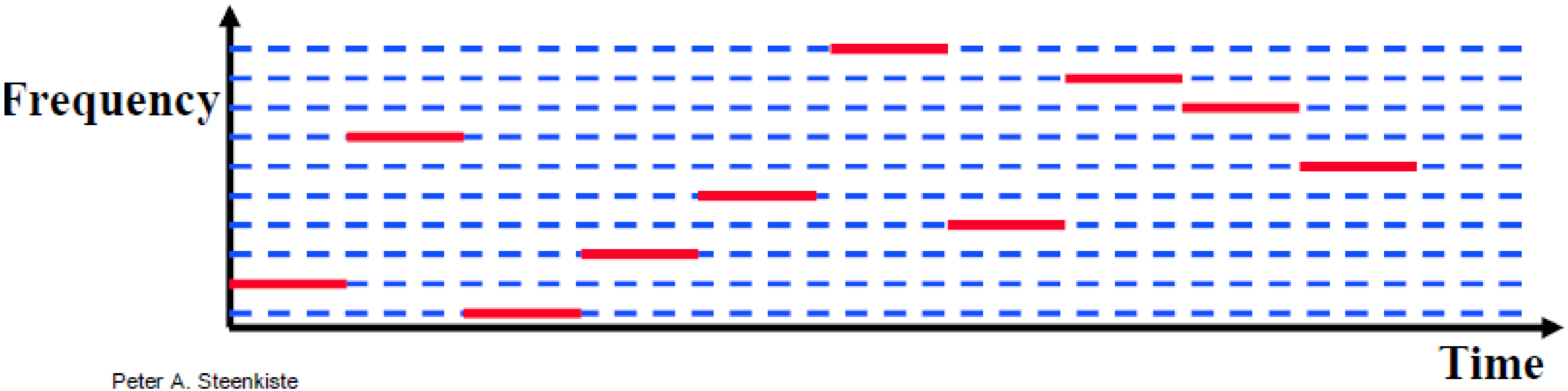


- How spectrum is used affects: cost ($), robustness, throughput…
  - We will talk about how each technology uses spectrum, and implications
- This graphic shows how BLE and WiFi interoperate; more on this next week

Frequency Hopping Spread Spectrum

- Transmitter hops through a sequence of transmit channels
  - Spend some "dwell time" on each channel before hopping again
  - Receiver must know the hopping pattern

- Avoid causing or receiving prolonged interference



Peter A. Steenkiste

Sidebar: inventor of FHSS – Hedy Lamarr

- Actress, inventor, and all-around badass
  - Designed FHSS with George Antheil during WWII based on music ideas
  - Idea: torpedo control can’t be easily jammed if it jumps around

- https://en.wikipedia.org/wiki/Hedy_Lamarr#Inventing_career

Frequency and Data Rate

- Which can send data faster (more bits/second)?
  - Signal at 2 GHz frequency with 1 MHz of bandwidth
  - Signal at 20 GHz frequency with 1 MHz of bandwidth

Frequency and Data Rate

- Which can send data faster (more bits/second)?
  - Signal at 2 GHz frequency with 1 MHz of bandwidth
  - Signal at 20 GHz frequency with 1 MHz of bandwidth
  - **They are identical!**

- Data rate is a function of bandwidth and power (not frequency)
  - Shannon-Hartley Theorem: $C = B\log_2(1 + \frac{S}{N})$
    - C – channel capacity in bits per second
    - B – bandwidth
    - $\mathrm{S/N}$ – signal to noise ratio (measure of signal power)

Frequency and Range

- Oof. This gets a little tricky

- Does frequency affect range: yes and no
  - Identical energy would mean identical range regardless of frequency
  - BUT
  - Lower frequencies use larger antennas
  - Larger antennas collect more energy
  - More energy allows for farther range

- Also, RF waves may or may not be affected by obstacles
  - Depends on wavelength (frequency) with obstacles much smaller than the wavelength having a minimal effect
    - Low frequencies can diffract around obstacles
  - Also depends on the materials of the obstacle

Outline

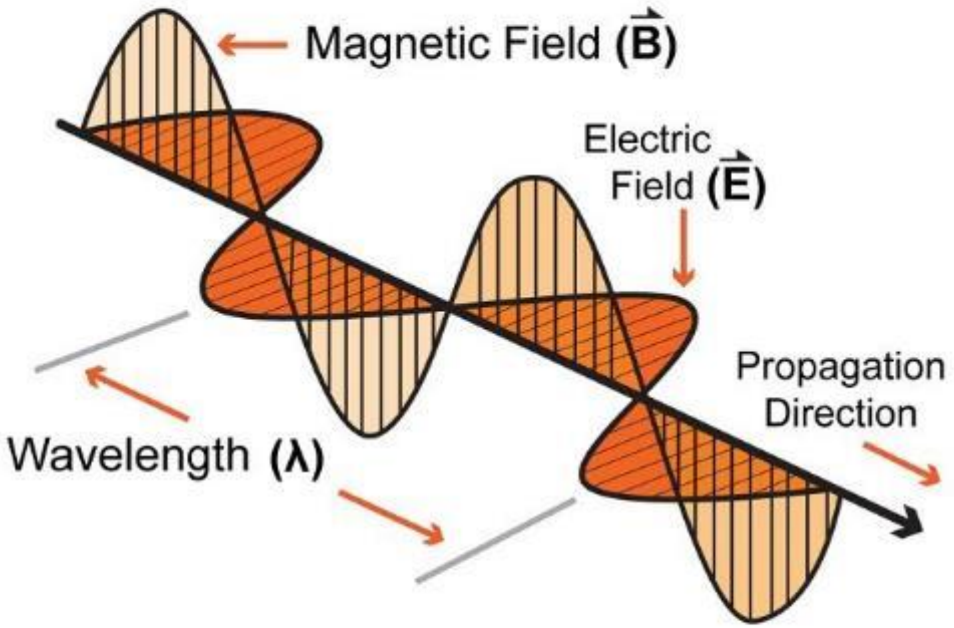
- OSI Layers
- Internet Architecture (Upper Layers)
- **Physical Layer**
  - Overview
  - Signal Strength
  - Signal Frequency and Bandwidth
  - **Signal Modulation**

Signal qualities

1. Signal strength
   - The amount of energy transmitted/received

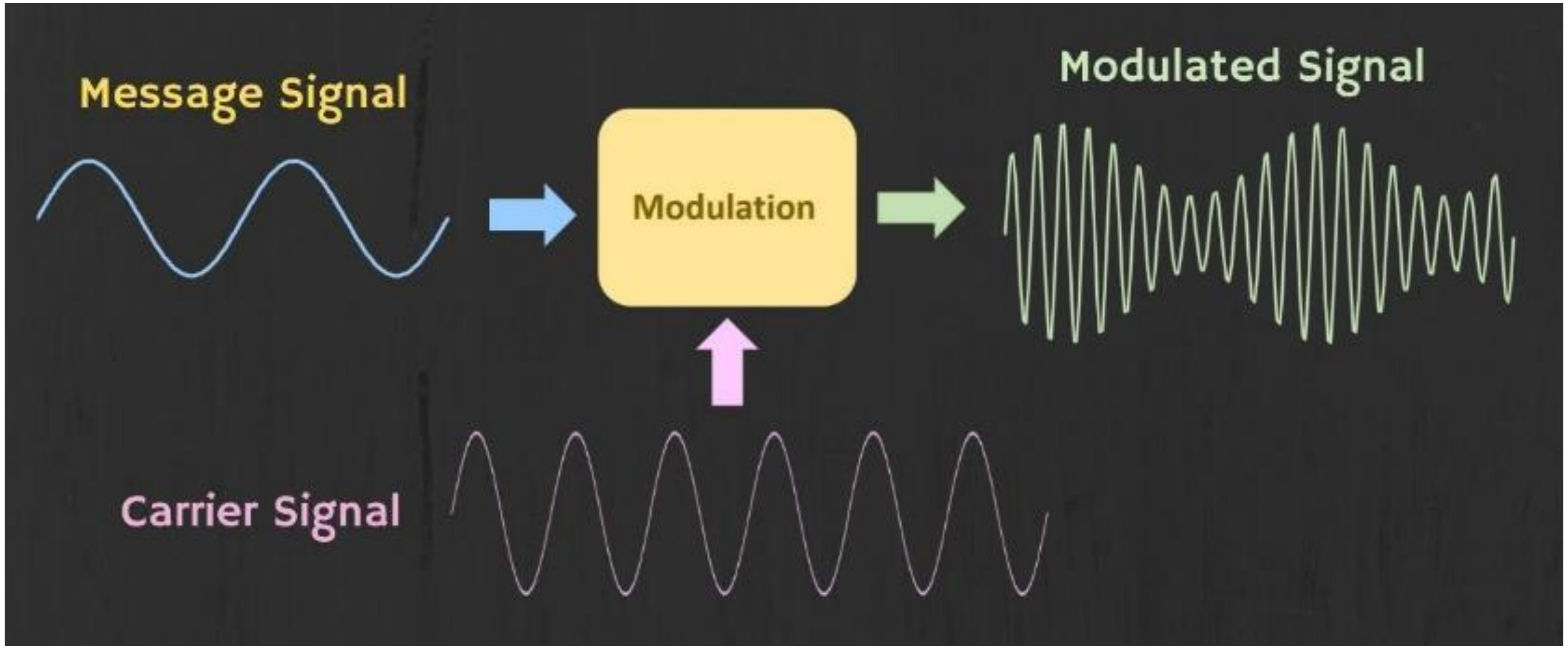
2. Signal frequency and bandwidth
   - Which "channel" the signal is sent on

3. **Signal modulation**
   - How data is encoded in the signal



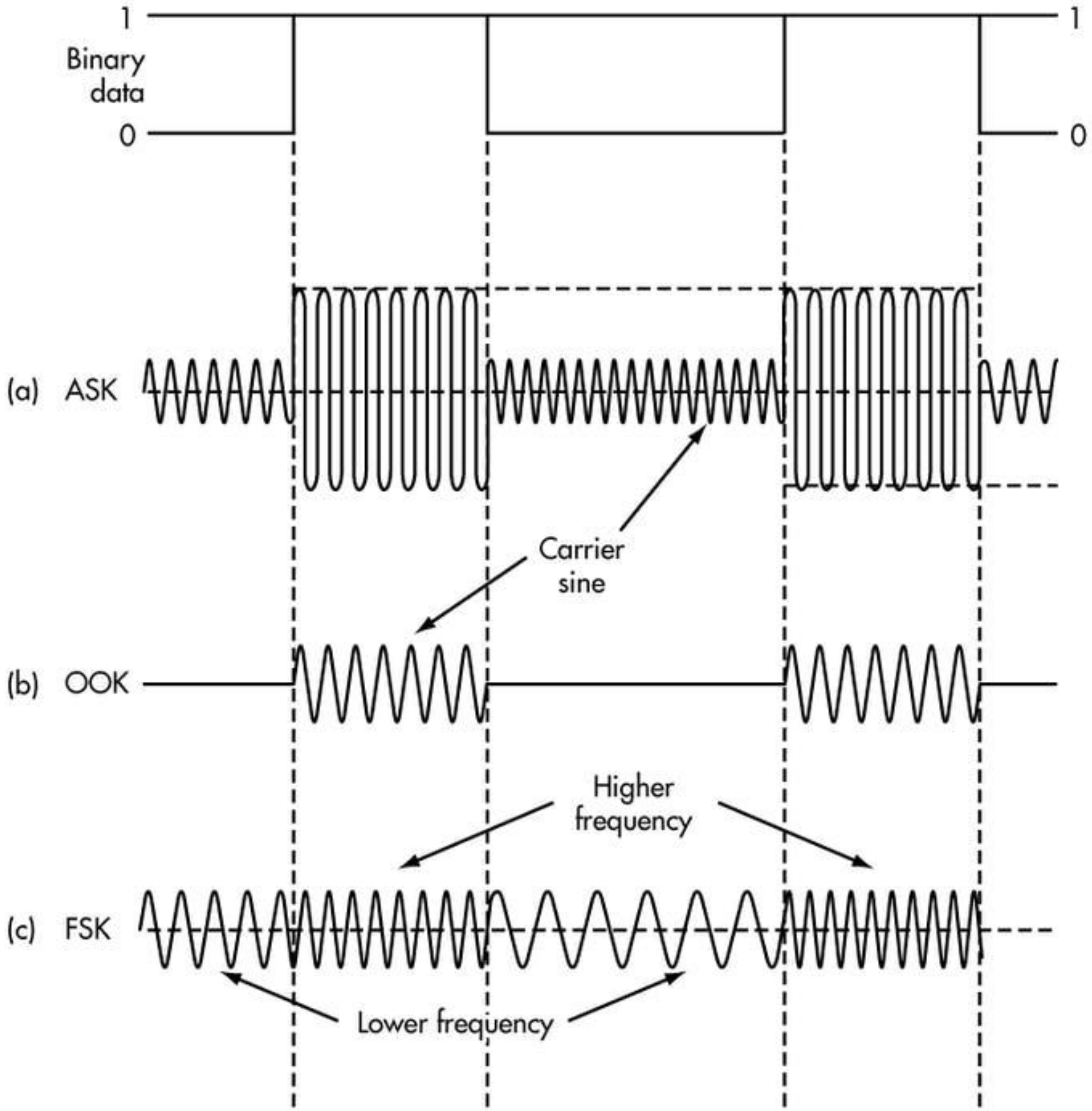
Modulation

- Encoding signal data in an analog "carrier" signal
  - Carrier signal defines the frequency
  - Modulation scheme + data define bandwidth required



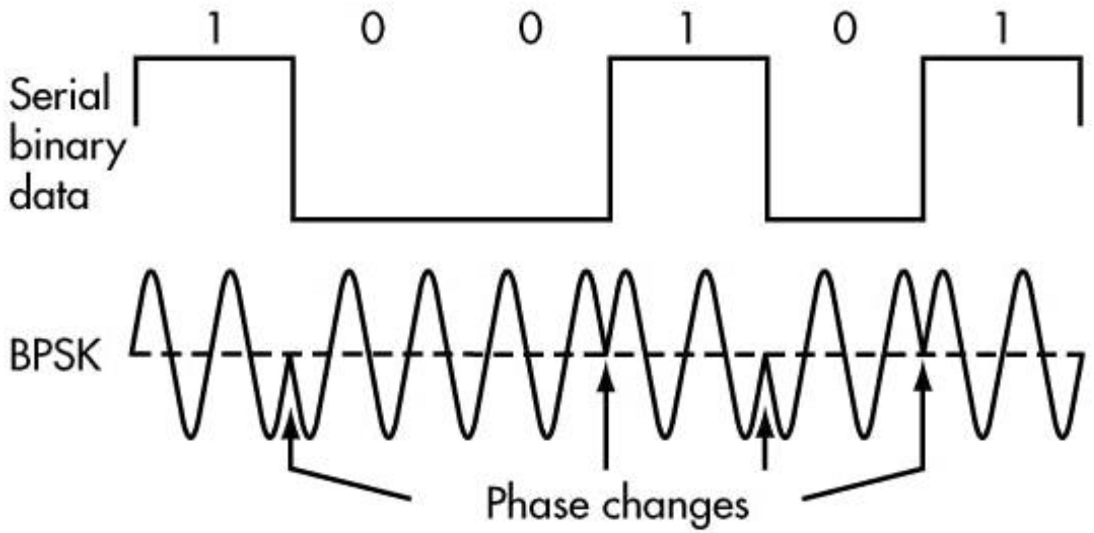
Modulation types

- Encoding binary data on a signal
- Amplitude-shift Keying (ASK)
  - Modify amplitude of carrier signal
  - On-Off Keying (OOK) is an extreme example
- Frequency-shift Keying (FSK)
  - Modify frequency of carrier signal



Modulation types

- Phase-shift keying (PSK)
  - Modify phase of carrier signal
  - Usually differential:
    the change signifies data



- More complicated possibilities exist
  - QAM (Quadrature Amplitude Modulation) combines amplitude and phase shift keying
    - Allows for more than one bit per “symbol”

Modulation tradeoffs

- Various tradeoffs between different modulation schemes
  - Bandwidth requirements, transceiver hardware, immunity to noise, etc.

- ASK (amplitude) is simple but susceptible to noise
  - Noise exists in the real world

- FSK (frequency) is relatively simple and robust to noise, but uses more bandwidth
  - Bandwidth is limited, but still commonly used

- PSK (phase) energy efficient and robust, but more complex hardware
  - More expensive hardware, but very commonly used

Break + Video

- Excellent explanation of modulation techniques: https://youtu.be/0faCad2kKeg?si=kK6l0g63XGVPdut9&t=240
    - Listen for 3.5 minutes until 7:30 in the video

    - "How Cell Service Actually Works" by Wendover Productions

Outline

- OSI Layers
- Internet Architecture (Upper Layers)
- Physical Layer
  - Overview
  - Signal Strength
  - Signal Frequency and Bandwidth
  - Signal Modulation