Lecture 02
Network Fundamentals

CS397/497 – Wireless Protocols for IoT
Branden Ghena – Winter 2023

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

Materials in collaboration with Pat Pannuto (UCSD)

Northwestern

Administrivia

- Piazza
  - Everyone should have access to it
  - If you don’t, try going to the Piazza tab on the sidebar in Canvas
  - If that still doesn’t work, this is the exception when you should email me

- Canvas
  - Most important information is on the Canvas homepage
  - I’m posting slides there too

Today’s Goals

- Introduce OSI layer model of communication
- Provide background on Internet layering
- Overview of concerns for the Physical and Data link layers
  - Speak the “lingo” of wireless communication
  - Present technology aspects that we will return to in specific protocols
- Describe Medium Access Control mechanisms

Outline

- **OSI Layers**
- Internet Architecture (Upper Layers)
- Physical Layer
- Data Link Layer

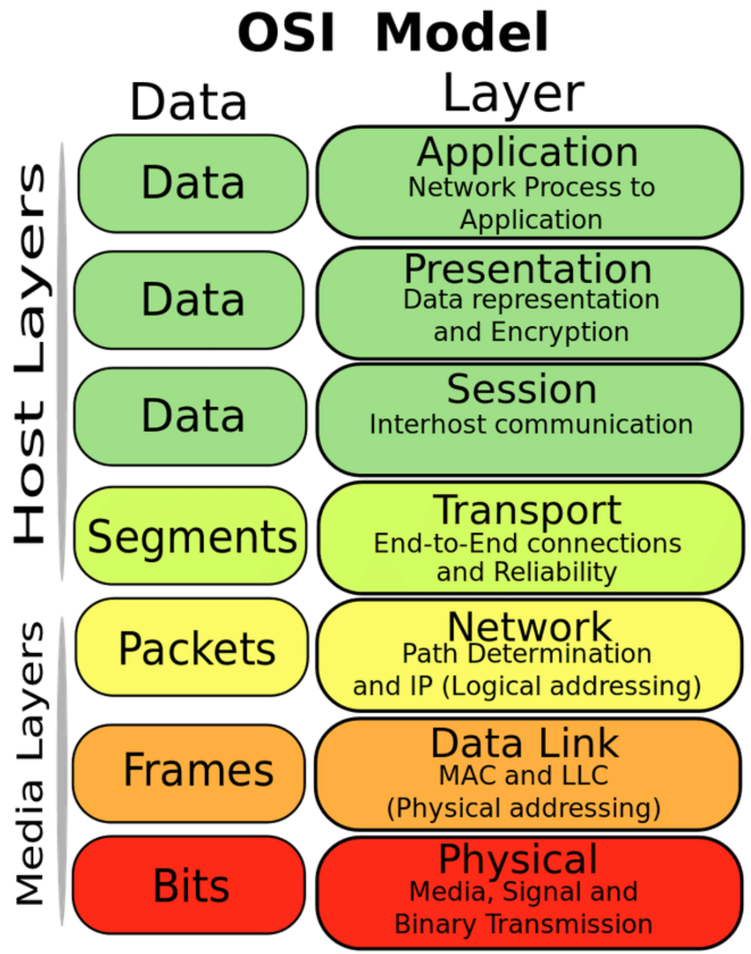
Communication layers

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

What goes on at each of these?

OSI model of communication layers

- Transport
  - How to form connections between computers
  - TCP and UDP
- Network
  - How to send packets between networks
  - IP
- Data Link
  - How to send frames of data
  - Ethernet, WiFi
- Physical
  - How to send individual bits
  - Ethernet, WiFi



OSI model of communication layers

- Transport
  - How to form connections between computers
  - TCP and UDP
- Network
  - How to send packets between networks
  - IP
- **Data Link**
  - **How to send frames of data**
  - **Ethernet, WiFi**
- Physical
  - How to send individual bits
  - Ethernet, WiFi

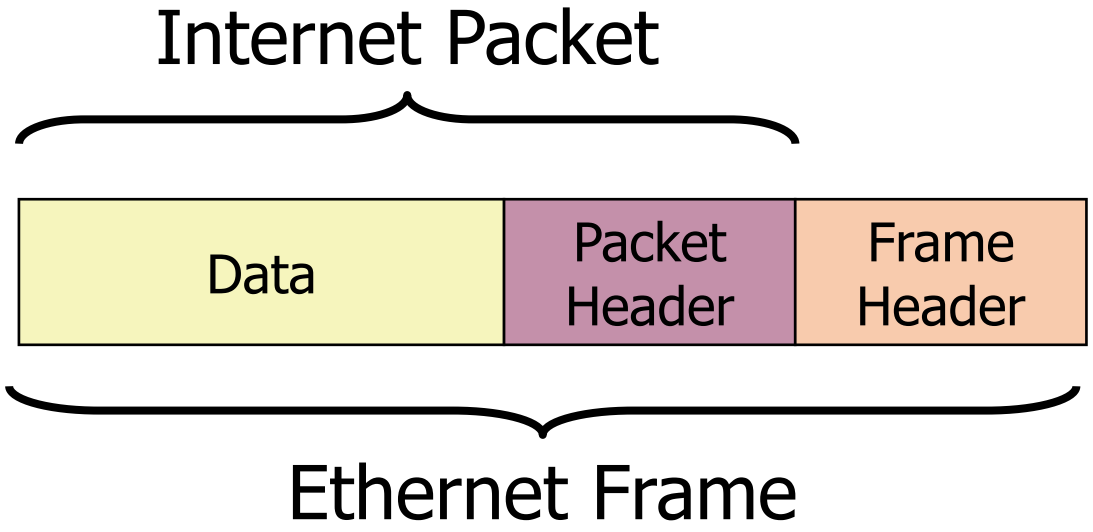
CS domain
CS340, CS440

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
  - Packet is wrapped with header for the link to make a frame



Protocols are "layered"

- Headers for each layer of communication wrap data
  - Data is wrapped with header for network to make a packet
  - Packet is wrapped with a header for the link to make a frame

Internet Packet

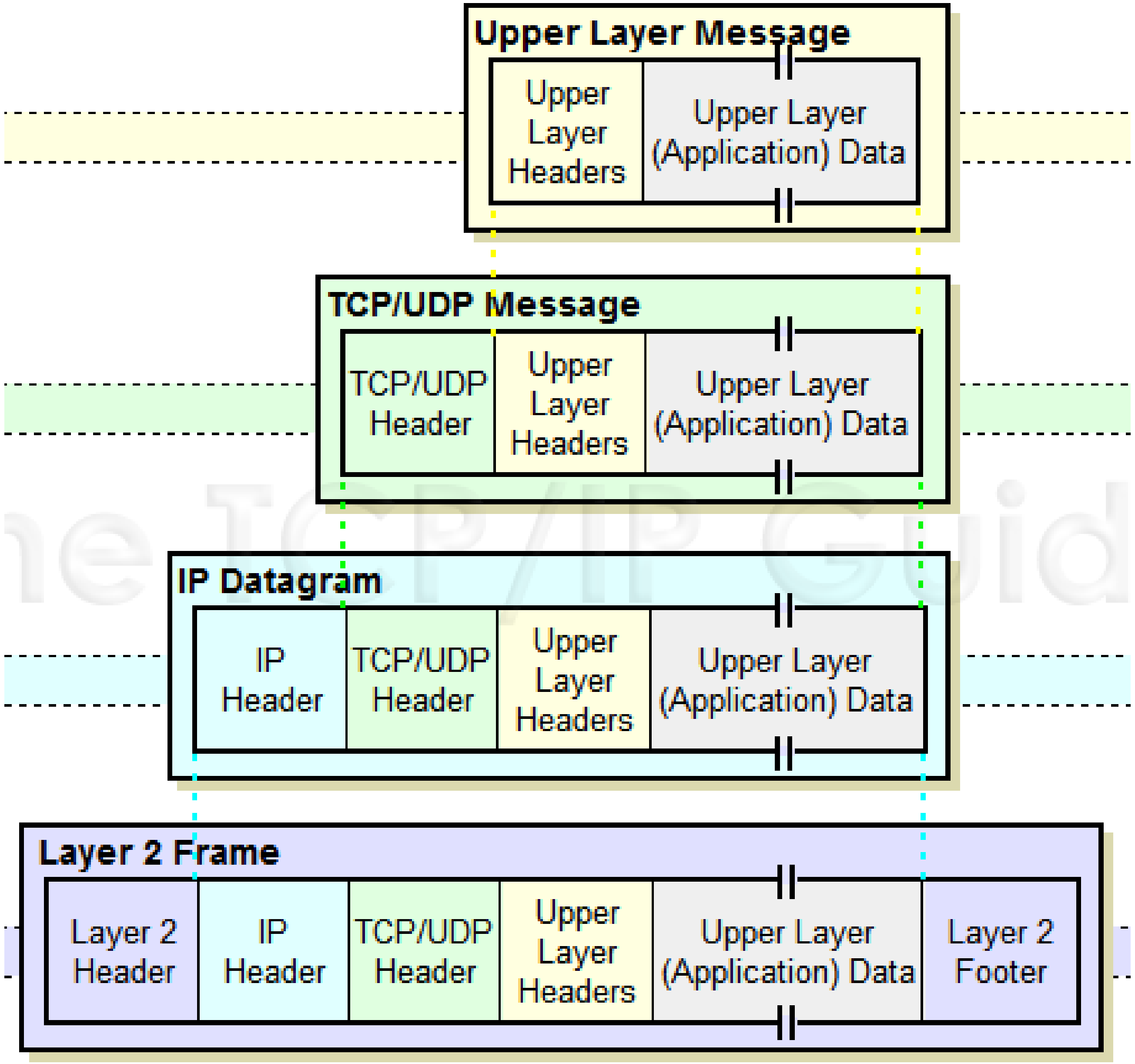
802.3 Ethernet packet and frame structure

Layer	Preamble	Start frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
Layer 2 Ethernet frame			← 64–1522 octets →						
Layer 1 Ethernet packet & IPG	← 72–1530 octets →								← 12 octets →

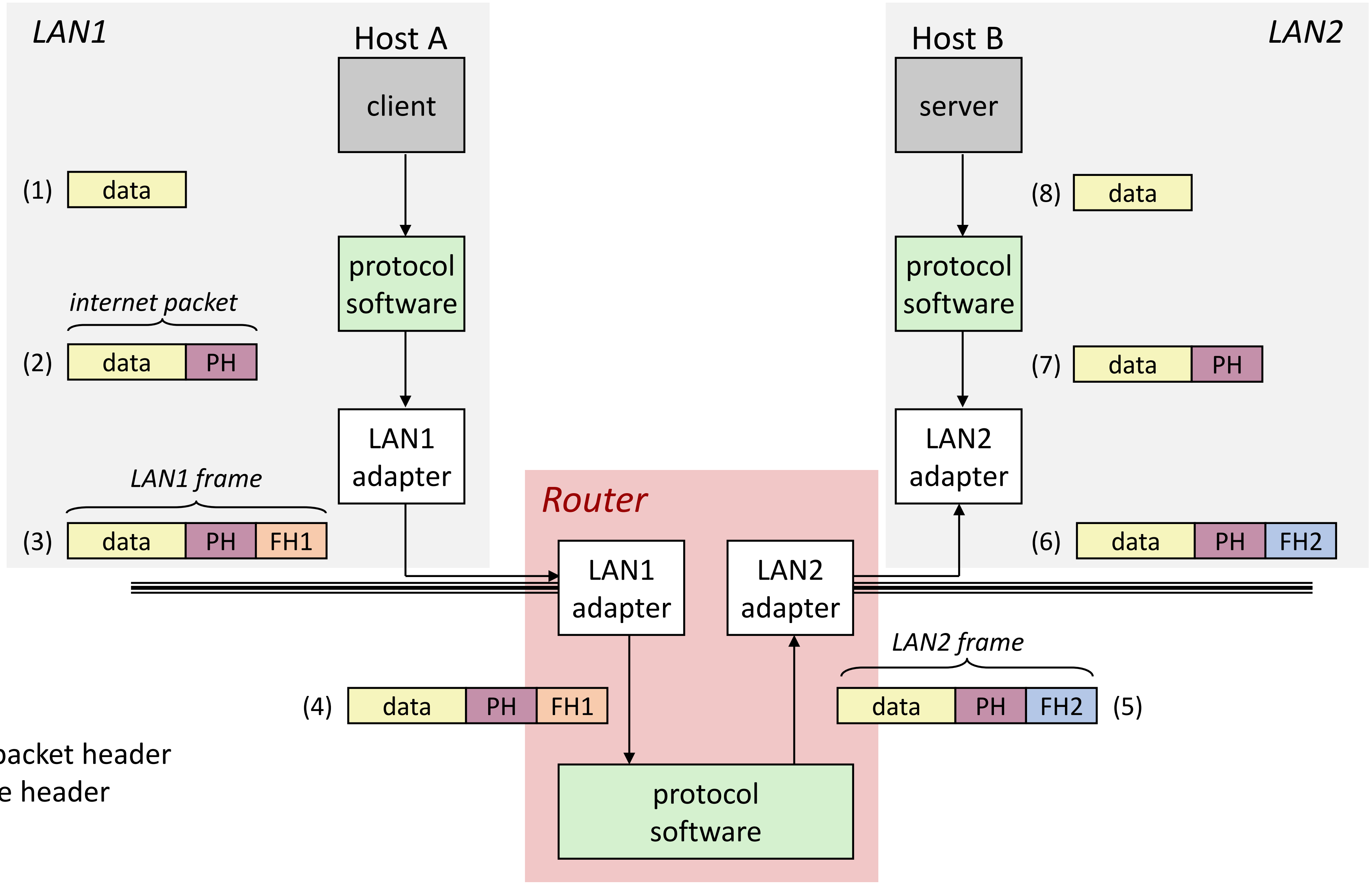
Ethernet Frame

Packet encapsulation

- Upper-layer packet is the payload for the lower-layer packet



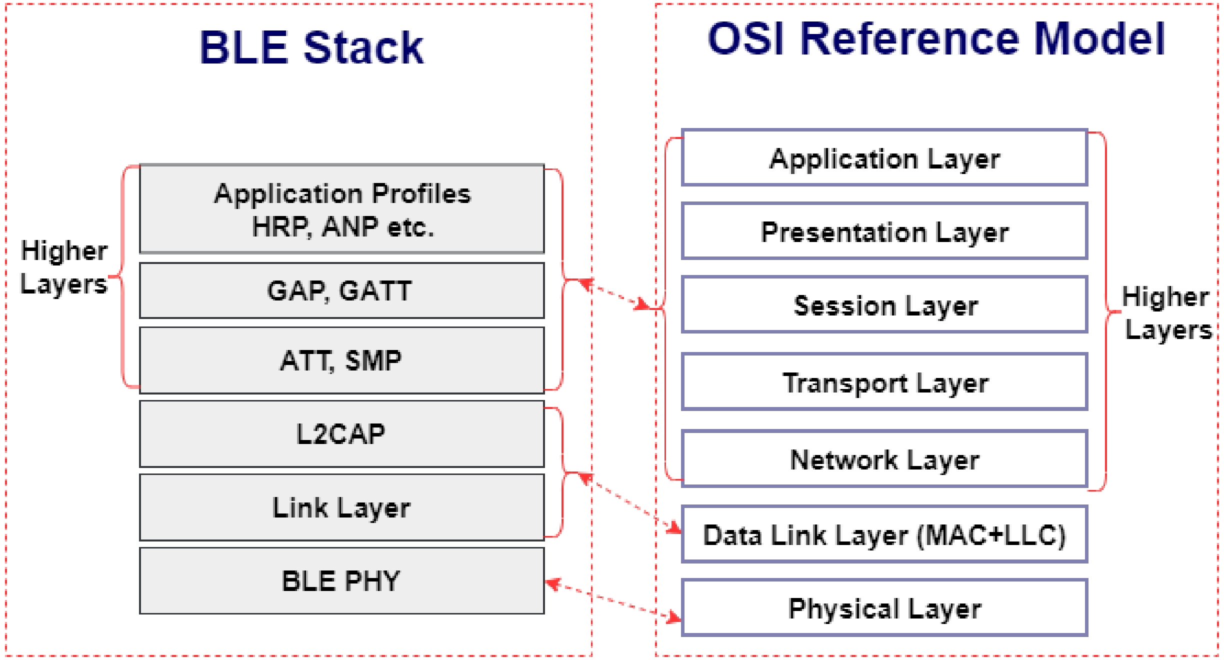
Transmitting data between networks

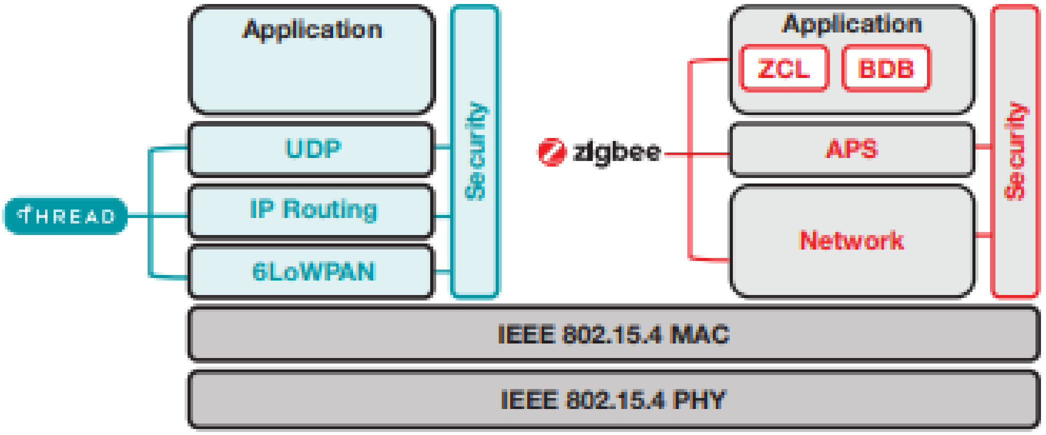


PH: Internet packet header
FH: LAN frame header

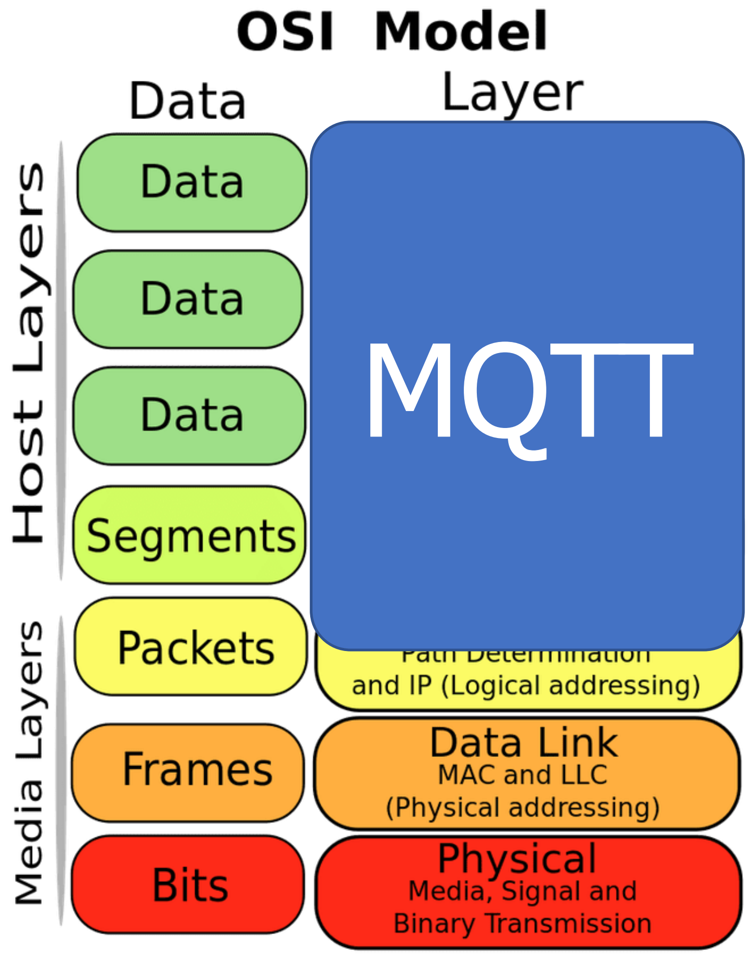
Model does not equal reality

- 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
- Data Link Layer

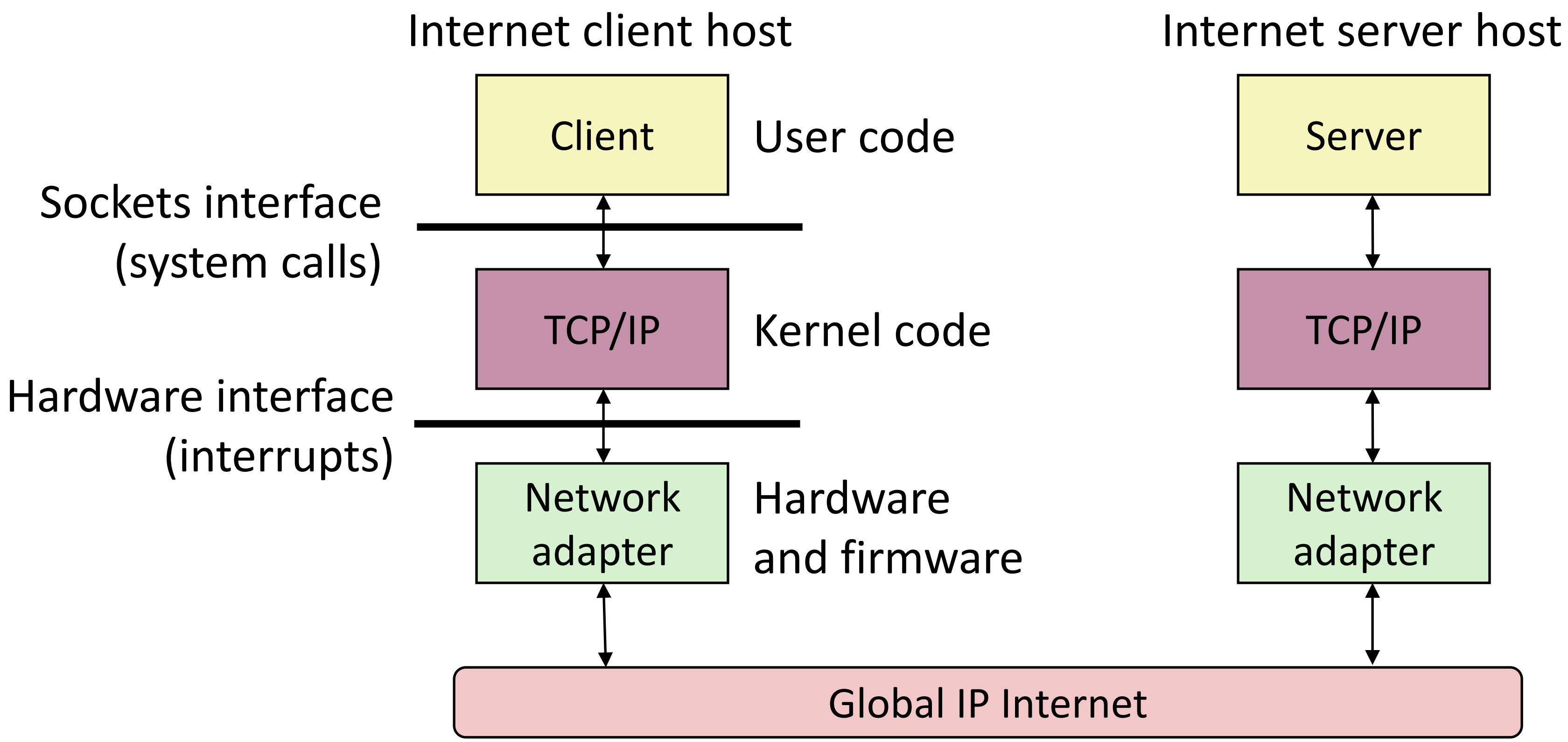
The global Internet

- 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**
    - 129.105.7.30

2. The set of IP addresses is mapped to a set of identifiers called Internet **domain names**
    - 129.105.7.30 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**

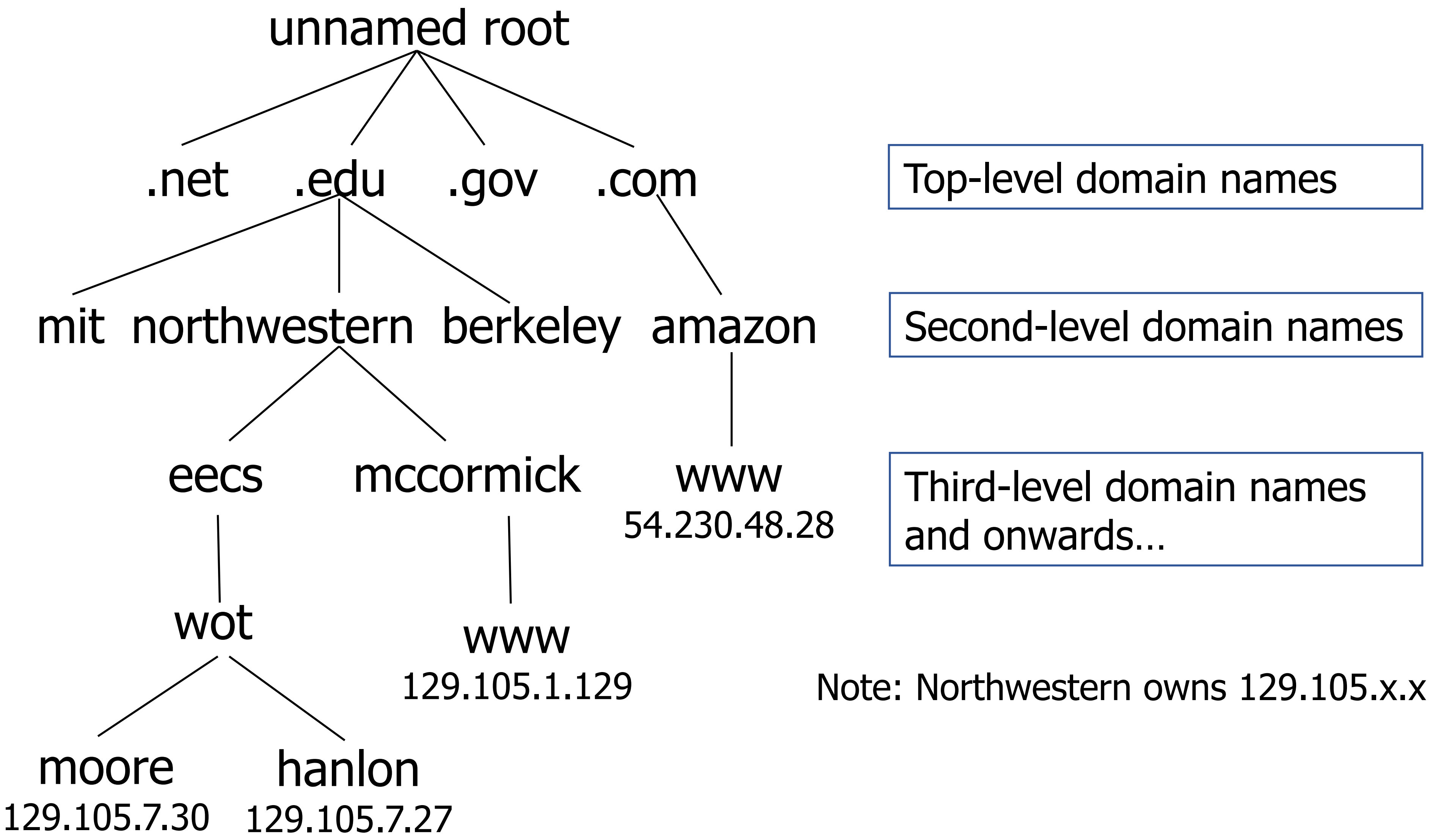
1. IP addresses

- 32-bit IP addresses are stored in an **IP address struct**
  - IP addresses are always stored in memory in *network byte order* (big-endian)
    - Remember: most computers use little-endian 😱
  - True in general for any integer transferred in a packet header from one machine to another
    - E.g., the port number used to identify an Internet connection

```
/* Internet address structure */
struct in_addr {
    uint32_t  s_addr; /* network byte order (big-endian) */
};
```

- By convention, each byte in a 32-bit IP address is represented by its decimal value and separated by a period
    - IP address: `0x8169071E = 129.105.7.30`

2. Internet domain names



Note: Northwestern owns 129.105.x.x

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

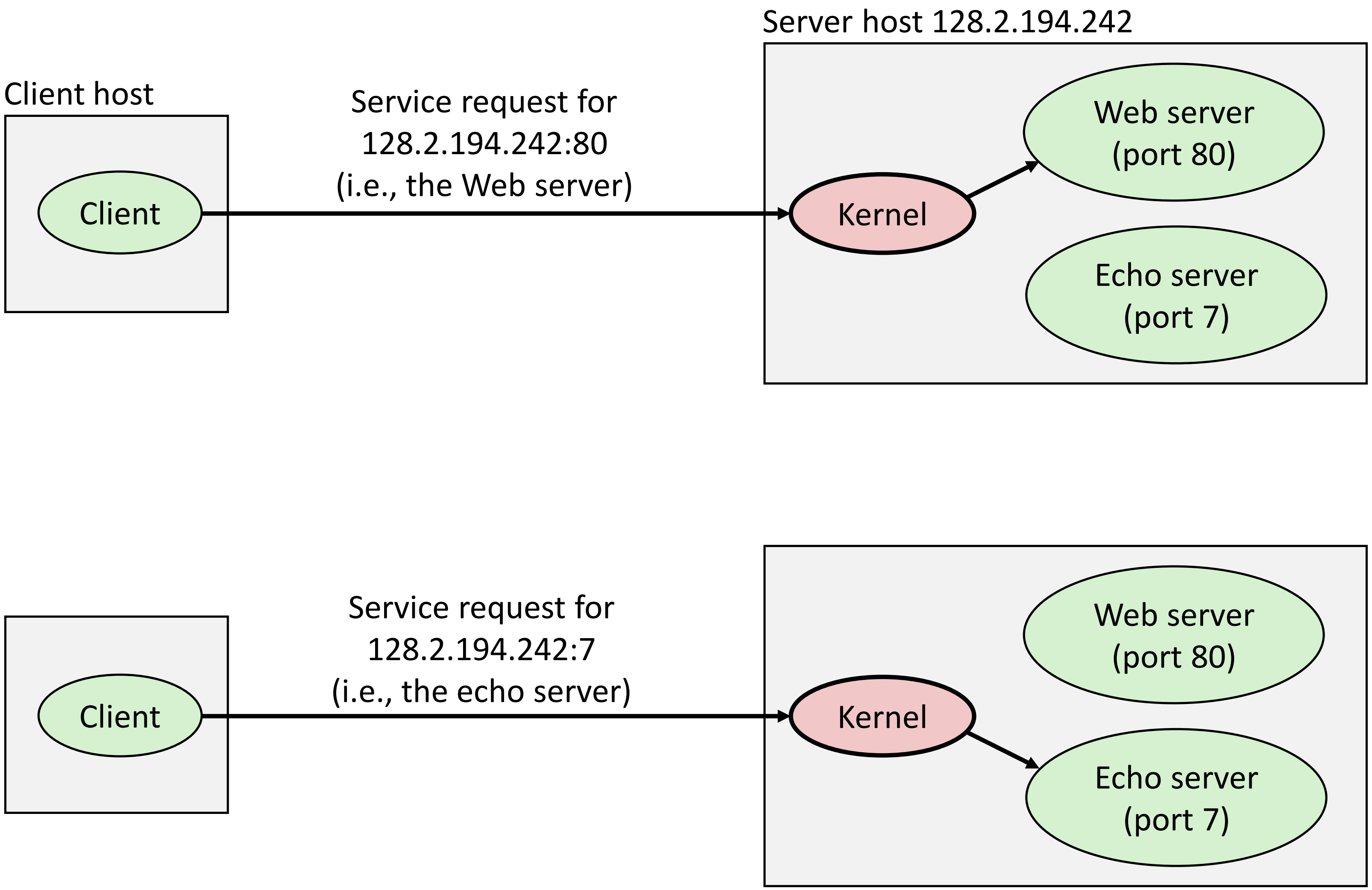
- A special name: **localhost**
  - Refers back to the computer being used (IP address 127.0.0.1)

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?

- IP layer
  - Describes the overall goal
    - Packets from my computer <---> Google

- 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

Addressing

- How to solve the routing problem?
  - I need to know how to get data from me to you
- How does the post office work?
  - I know where you live (your address)
    - Zip Code
    - City
    - Street
    - House Number
    - Name

The problem with addressing

- Your computer moves all the time
  - Home, school, Starbucks...

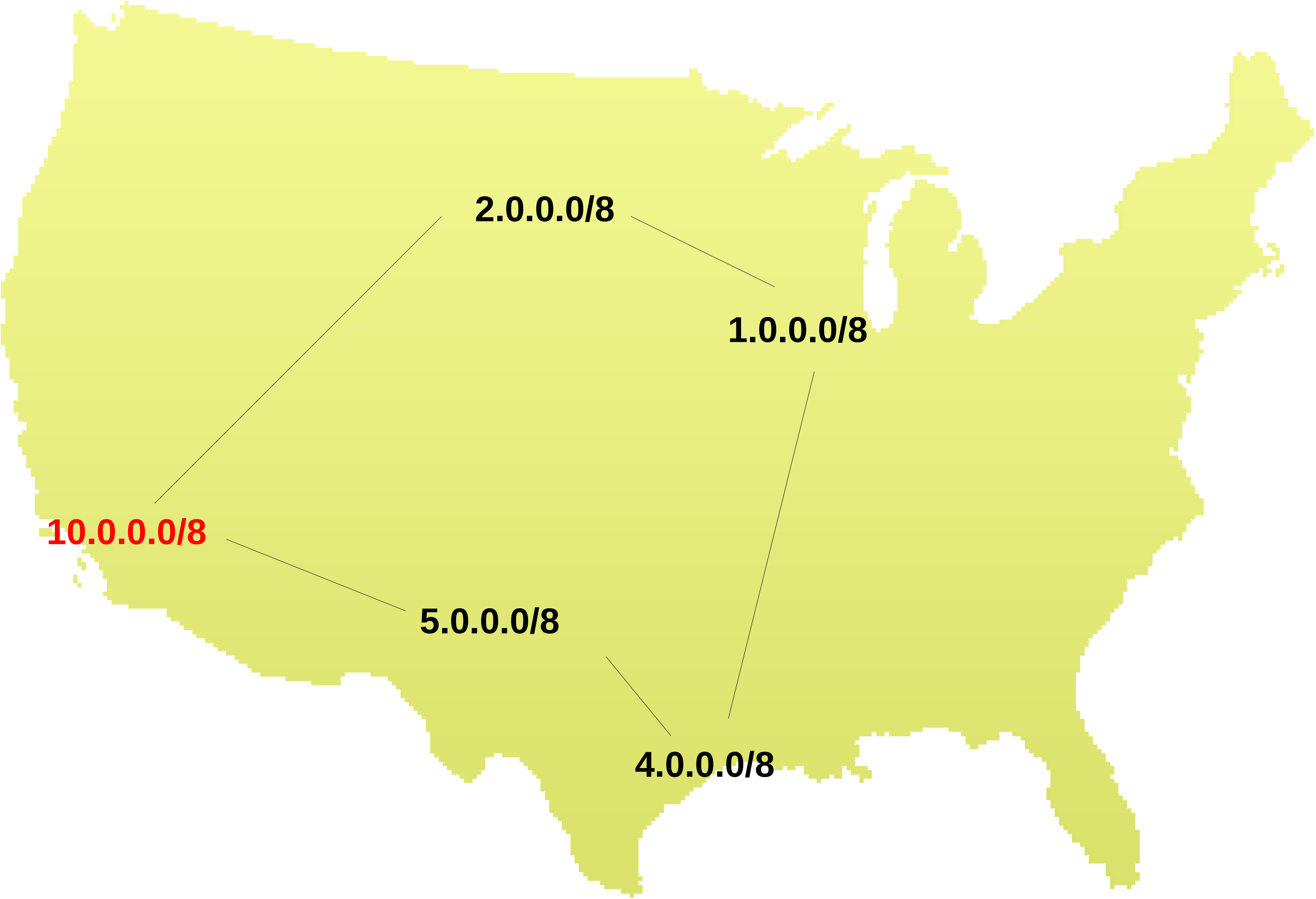
Assigning and finding IP address ranges

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

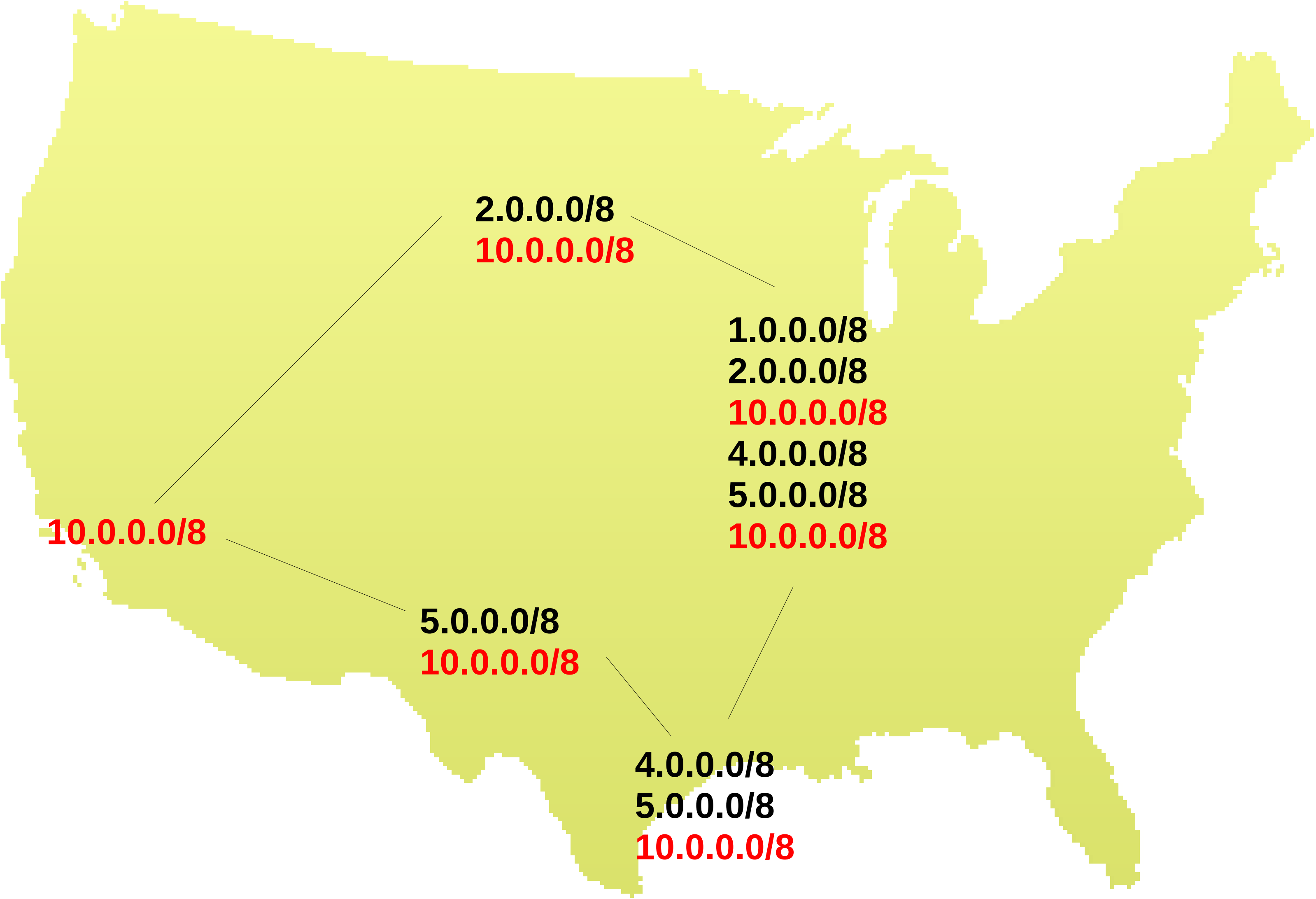
- Solution:
  - Tie IP addresses to network operators
  - Assign computers IPs as they join networks

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

Routing

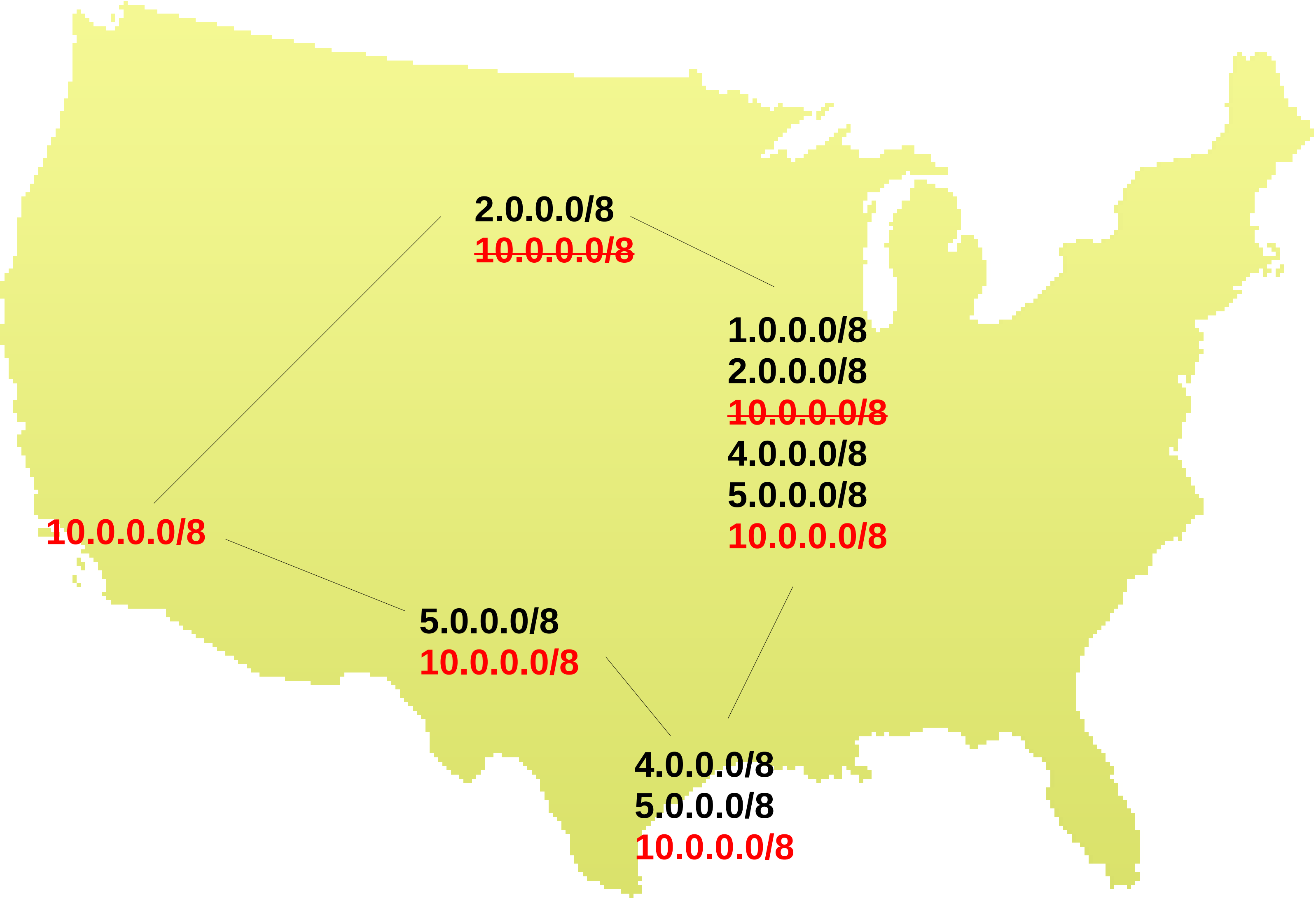


Routing



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 – "Adaptive"



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
    - Note: this overview ignores NATs, which are commonplace today

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


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

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 (11 pages!)
    - Keyboard events
    - Parsing URL
    - DNS lookup
    - Opening socket
    - HTTP protocol
    - HTML parsing
    - GPU rendering

Outline

- OSI Layers
- Internet Architecture (Upper Layers)
- **Physical Layer**
- Data Link Layer

Physical Layer

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

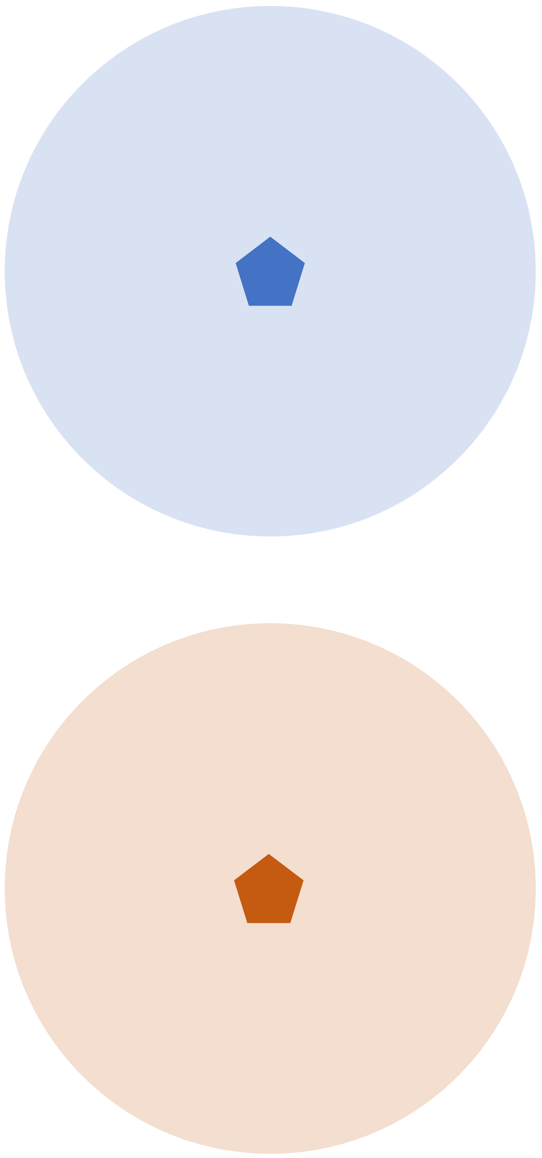
- Important considerations
  - Signal strength
  - Modulation
  - Frequency

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

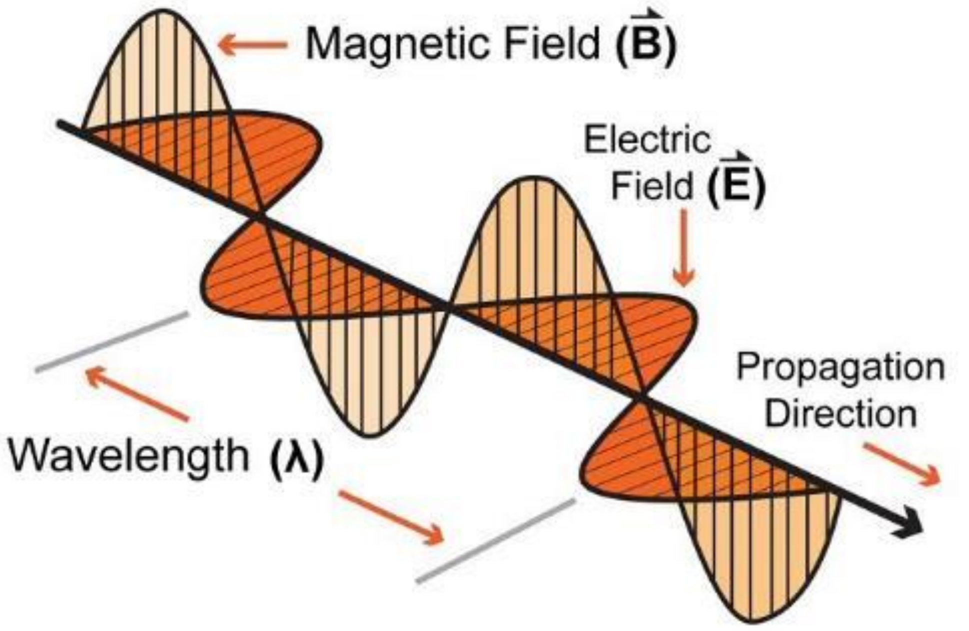


Signal qualities

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

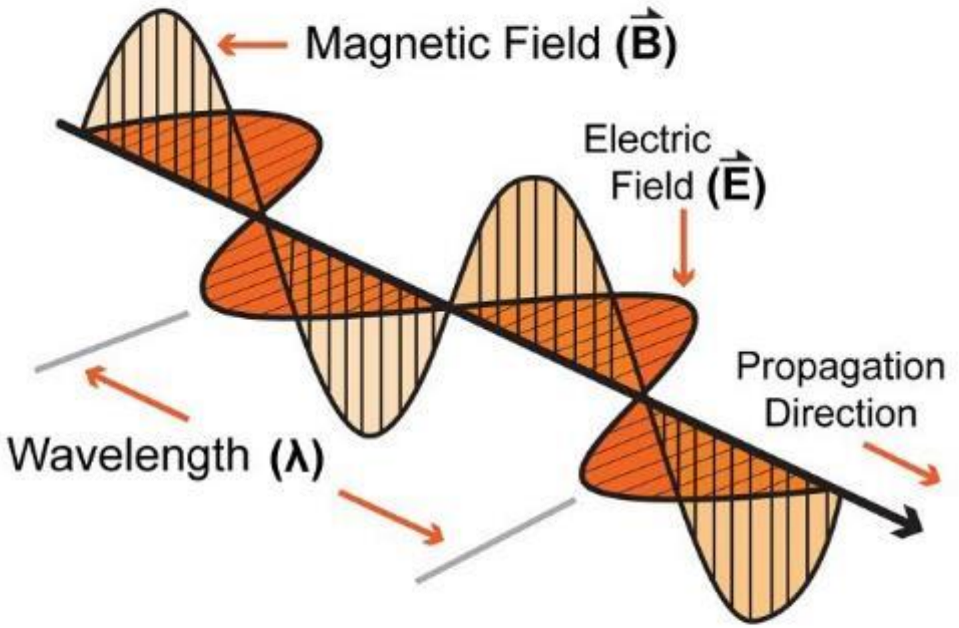


Signal qualities

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

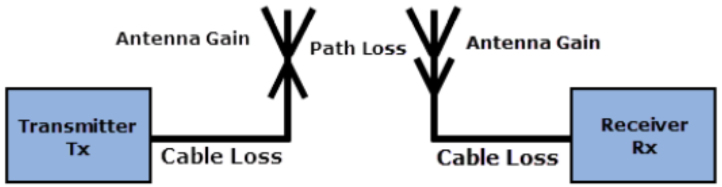
- Bluetooth Low Energy (local area)
    - nRF52840 transmit power: 8 dBm (6.31 mW)
    - nRF52840 receive sensitivity: -95 dBm (316.2 fW)

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

Propagation degrades RF signals

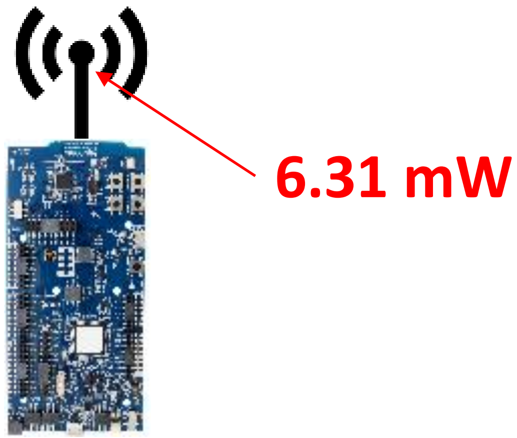
- Attenuation in free space
  - Signals get weaker as they travel over long distances
  - Signal spreads out → Free Space Path Loss (FSPL)

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



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)

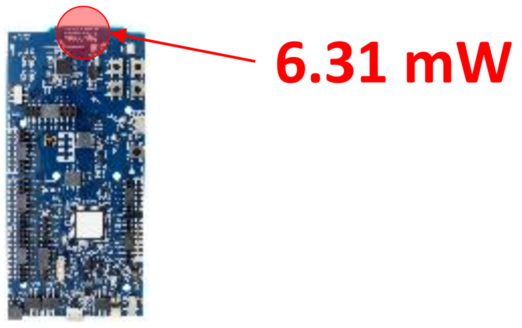


Wait, is not an antenna

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

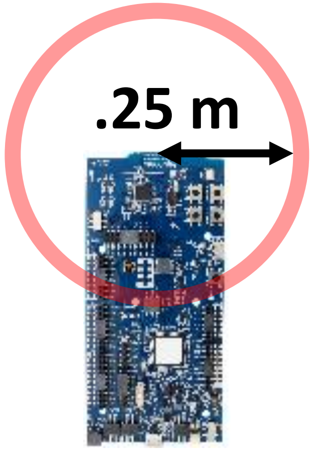
Some Intuitions for Signal Propagation, Power, Gain, etc.

- 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)



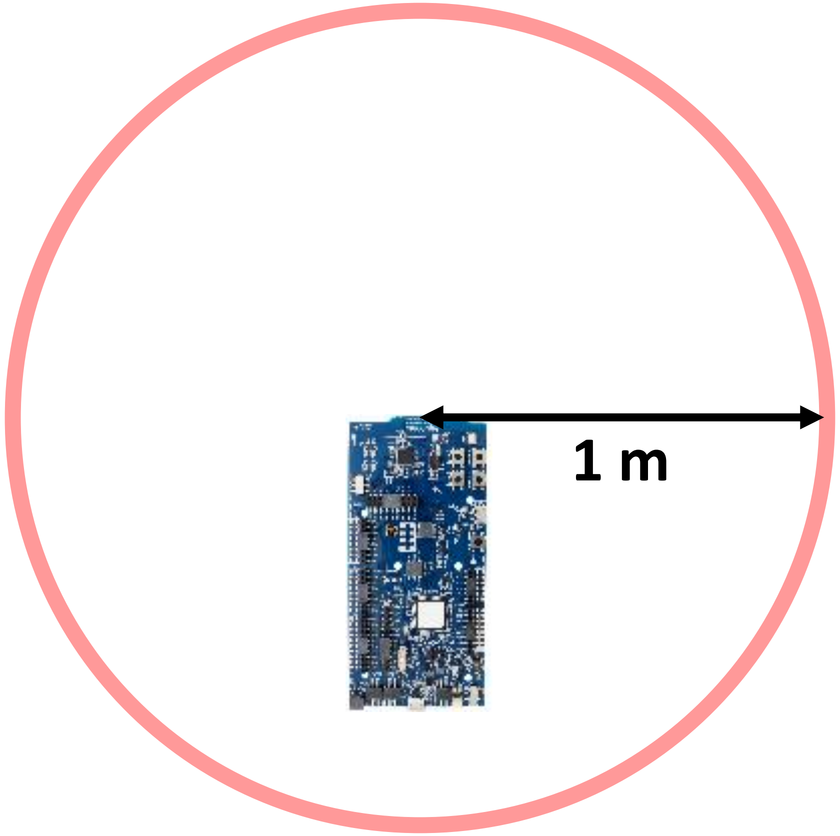
Some Intuitions for Signal Propagation, Power, Gain, etc.

- 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)

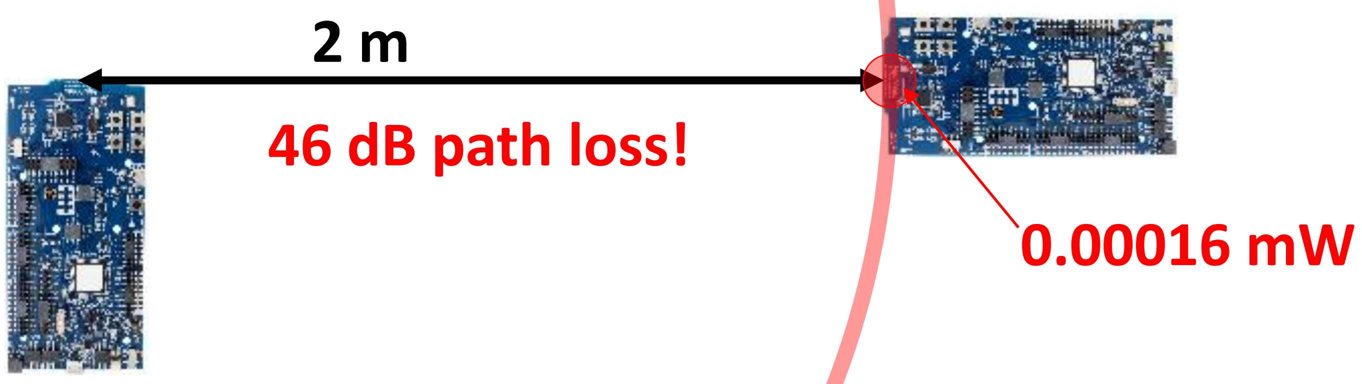


Some Intuitions for Signal Propagation, Power, Gain, etc.

- 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)



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
- For FSPL alone for a 2.4 GHz signal, 103 dB is 1,400 m!

Bluetooth does not go 1.4 km…

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

Many factors affect the ability to actually receive data

- Here's some examples, from DW1000 [ultra wideband transceiver]

3.4 Receiver Sensitivity Characteristics

T_{amb} = 25 ˚C, all supplies centered on typical values. 20 byte payload

Table 6: Typical Receiver Sensitivity Characteristics

Packet Error Rate	Data Rate	Typical Receiver Sensitivity	Units	Condition/Note		
1%	110 kbps	-106	dBm/500 MHz	Preamble 2048	Carrier frequency offset ±1 ppm. Requires use of the "tight" Rx operating parameter set – see [2]	All measurements performed on Channel 5, PRF 16 MHz. Channel 2 is approximately 1 dB less sensitive
10%	110 kbps	-107	dBm/500 MHz	Preamble 2048		
1%	110 kbps	-102	dBm/500 MHz	Preamble 2048	Carrier frequency offset ±10 ppm	
	850 kbps	-101	dBm/500 MHz	Preamble 1024		
	6.8 Mbps	-93 (*-97)	dBm/500 MHz	Preamble 256		
10%	110 kbps	-106	dBm/500 MHz	Preamble 2048		
	850 kbps	-102	dBm/500 MHz	Preamble 1024		
	6.8 Mbps	-94 (*-98)	dBm/500 MHz	Preamble 256		

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.

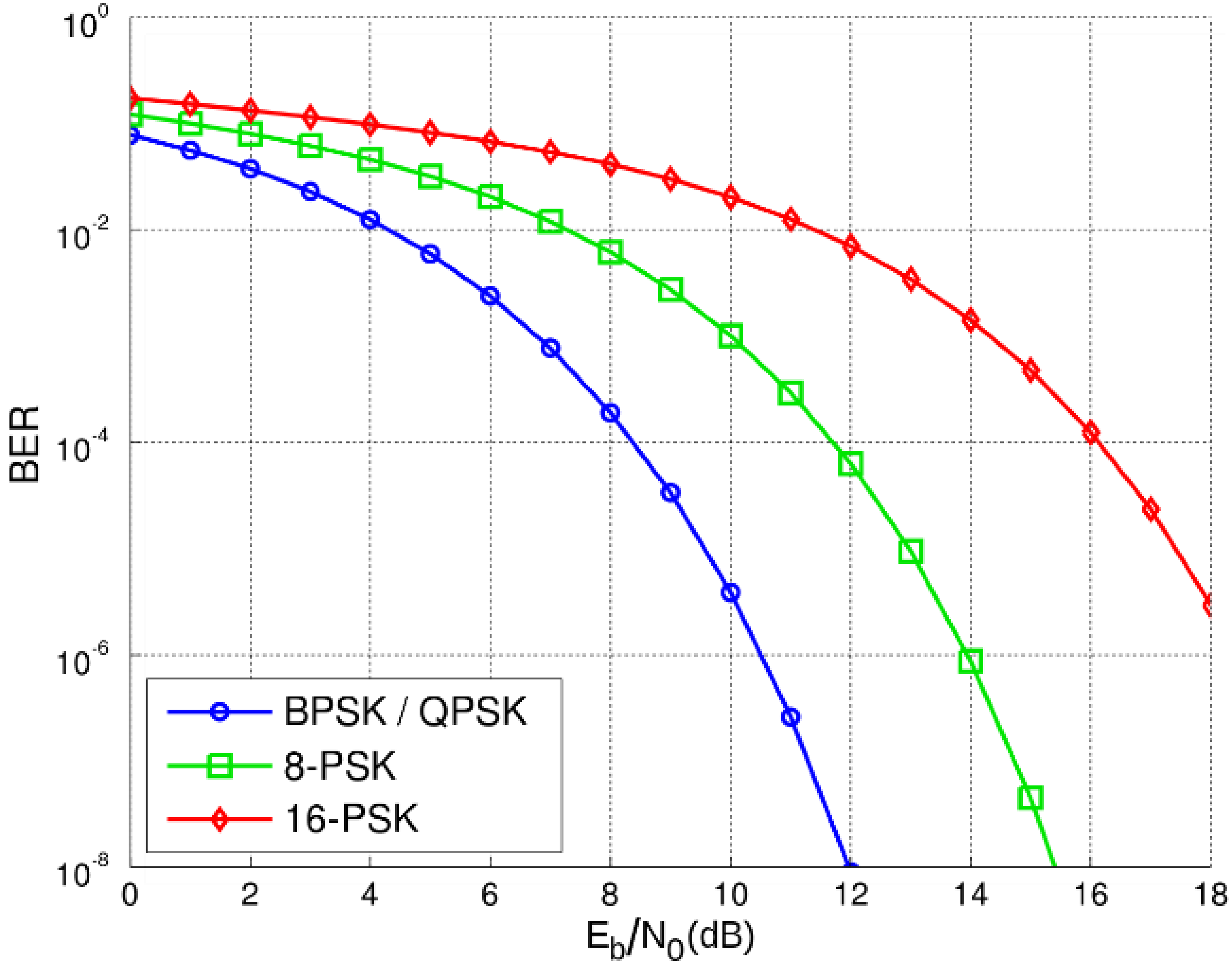
$P_f(n)$ = the floor loss penetration factor.

- Models like this are *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

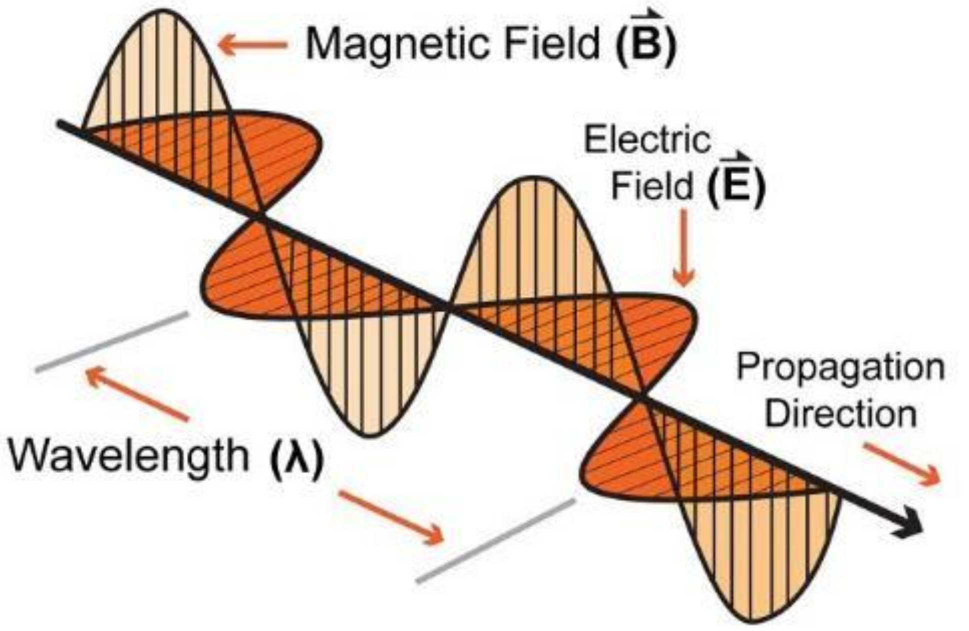
Odds that a transmitted bit will be received incorrectly

Signal qualities

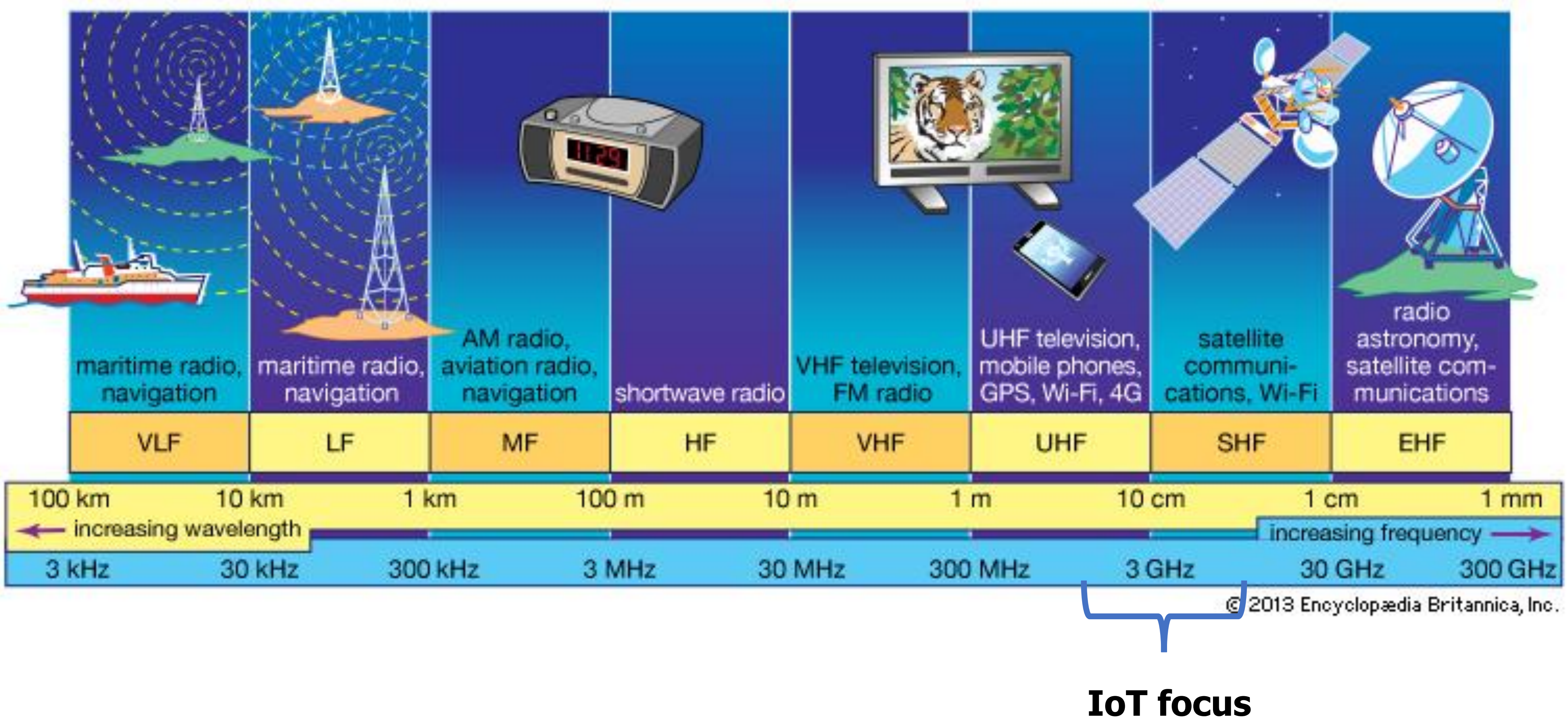
1. Signal strength
   - The amount of energy transmitted/received

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

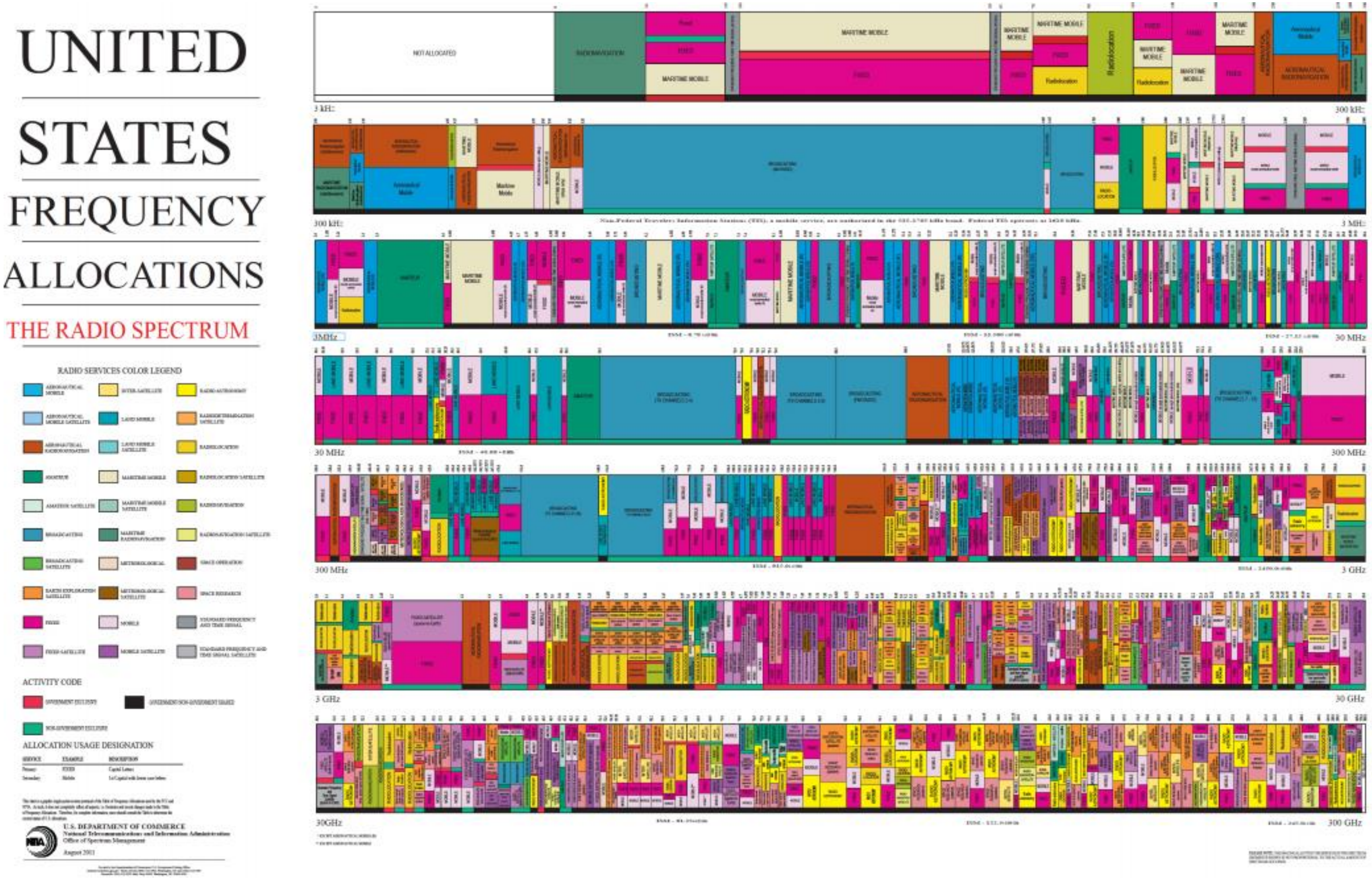
3. Signal modulation
   - How data is encoded in the signal



RF communication frequencies

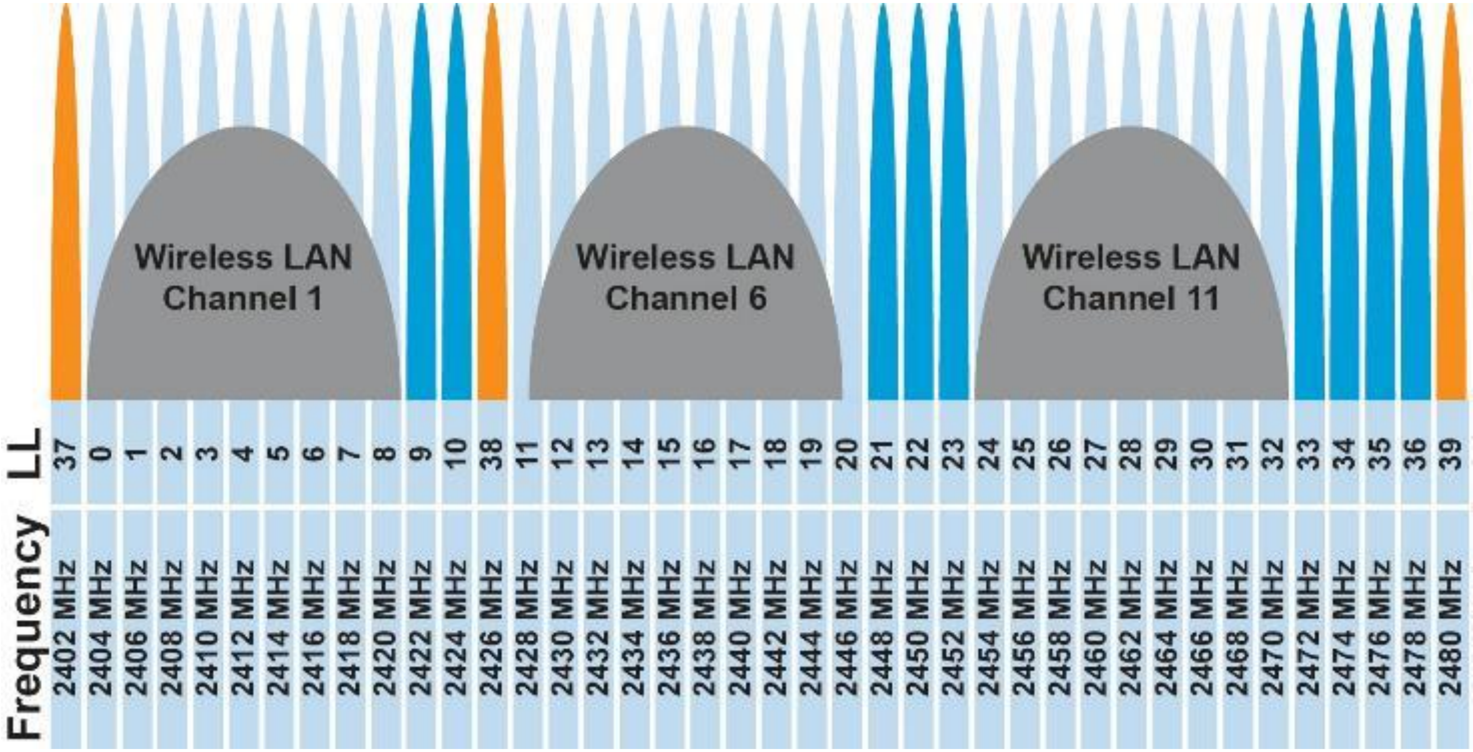


Wireless spectrum is allocated to specific uses



Unlicensed bands are where IoT thrives

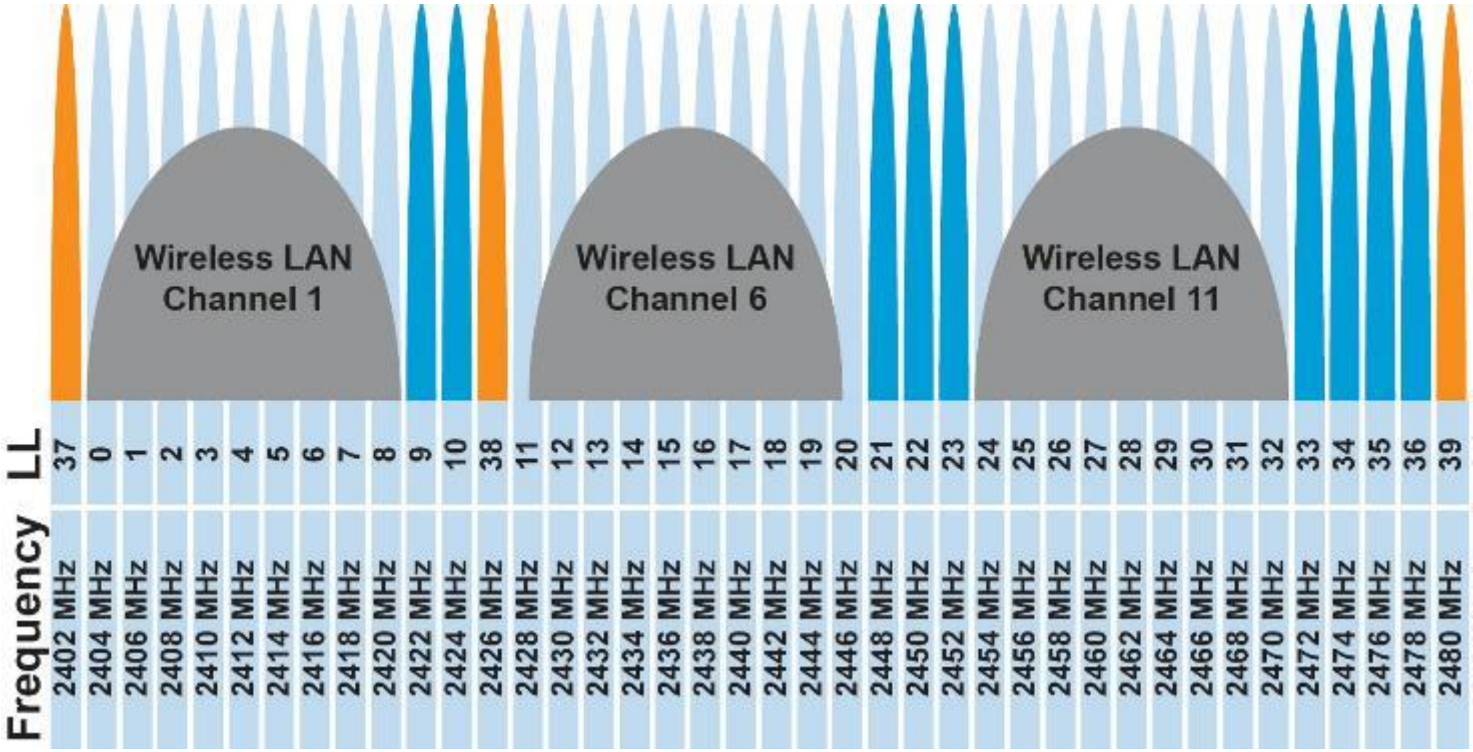
- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi



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

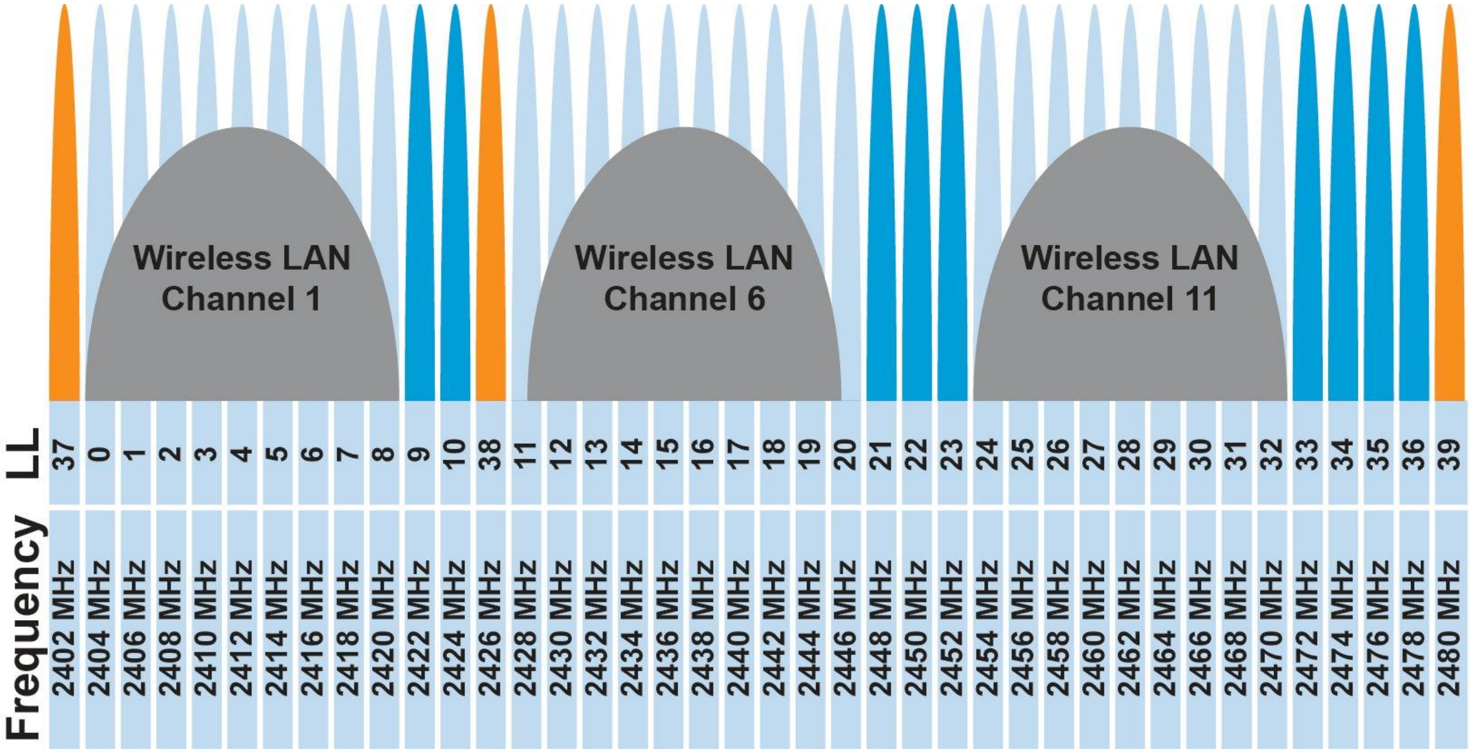
Unlicensed bands are where IoT thrives

- 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**

Different technologies use spectrum in different ways

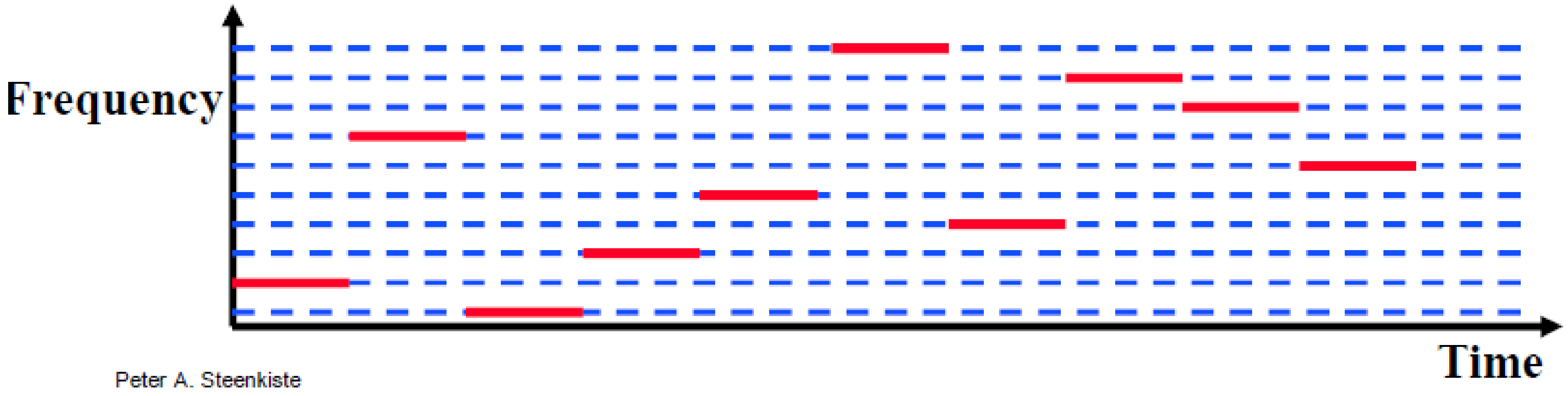


- How spectrum is used affects: cost ($), robustness, throughput…
  - We will talk about how each technology uses spectrum, and implications
- This graphic shows how BLE and WiFi interoperate; more on this next week

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



Sidebar: inventor of FHSS – Hedy Lamarr

- Actress and Inventor
  - Designed FHSS with George Antheil during WWII
  - Idea: torpedo control can’t be easily jammed if it jumps around

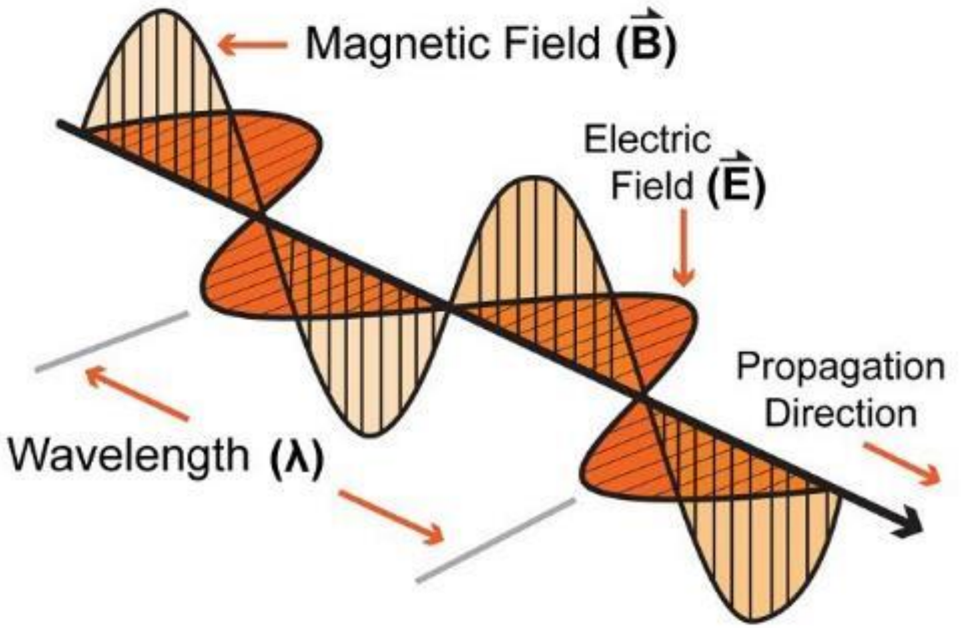
- https://en.wikipedia.org/wiki/Hedy_Lamarr#Inventor

Signal qualities

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

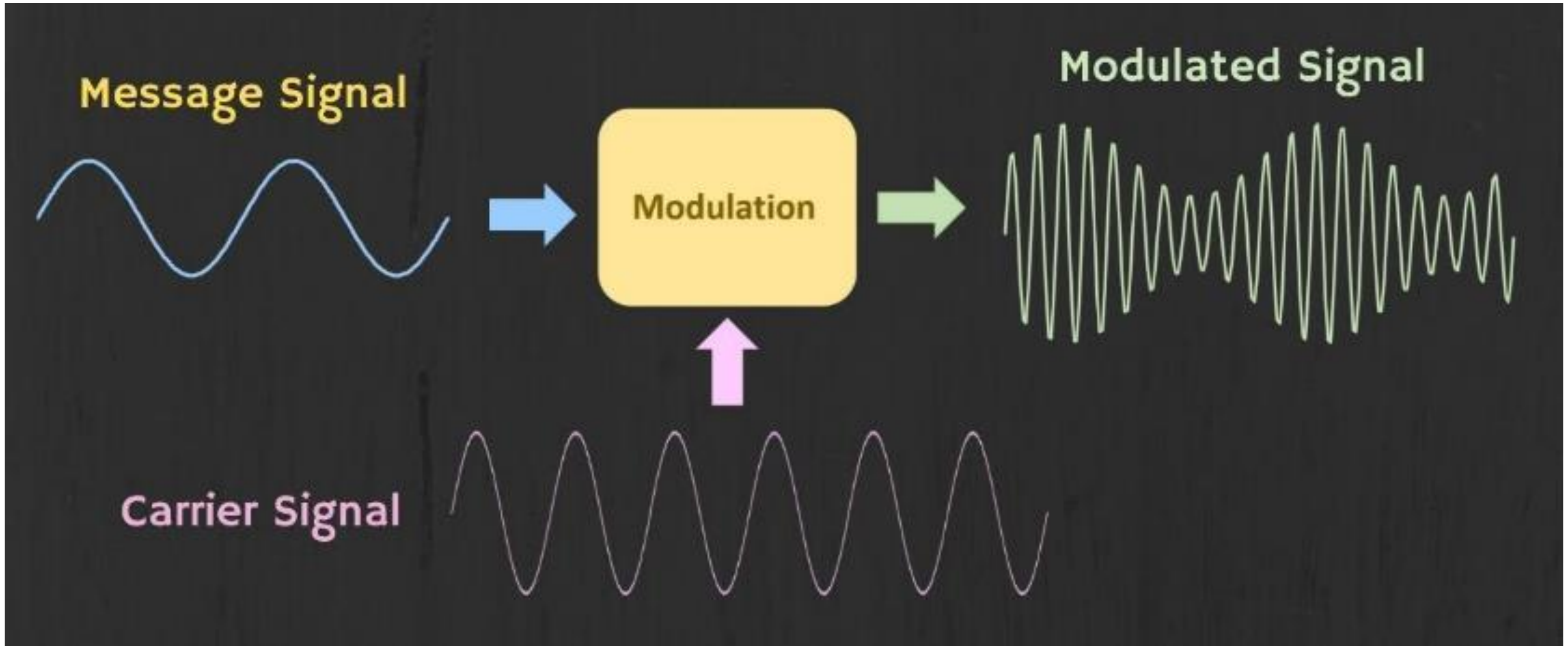
2. Signal frequency and bandwidth
   - Which “channel” the signal is sent on

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



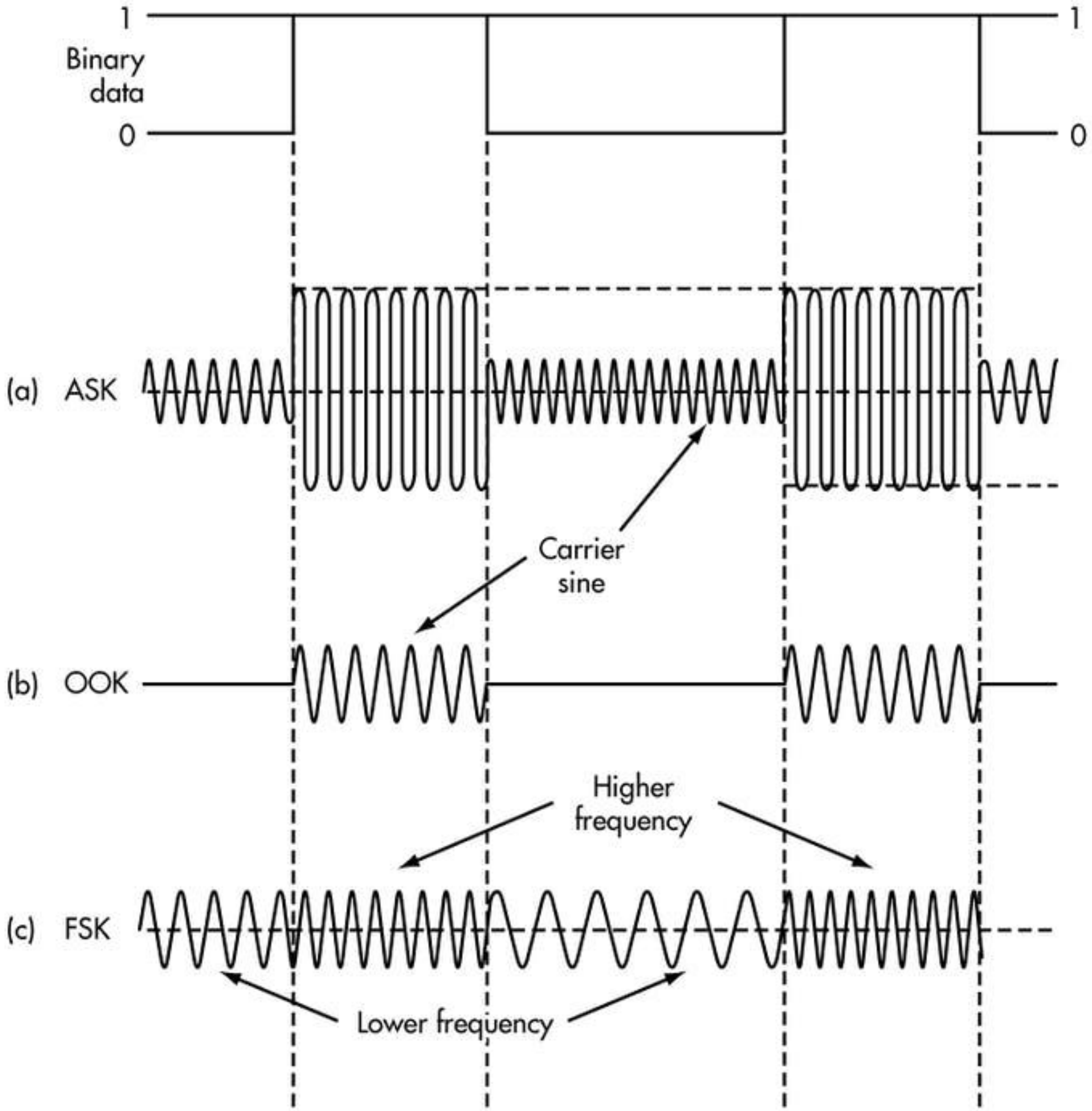
Modulation

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



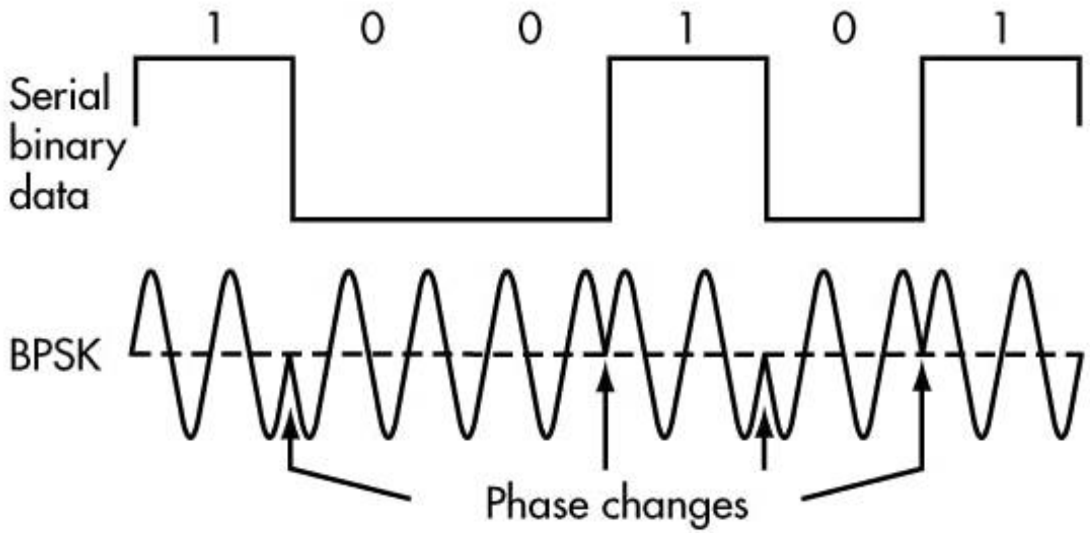
Modulation types

- 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 + 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
- **Data Link Layer**

Data Link Layer

- Framing
  - Combine arbitrary bits into a “packet” of data
- Logical link control
  - Manage transfer between transmitter and receiver
  - Error detection and correction
- Media access
  - Controlling which device gets to transmit next
- Inherently coupled to PHY and its decisions

Framing

- Typical packet structure
  - Preamble - Existence of packet and synchronization of clocks
  - Header - Addresses, Type, Length
  - Data - Payload plus higher layer headers (e.g. IP packet)
  - Trailer - Padding, CRC

Preamble	**Destination Address**	**Source Address**	**Type and Length**	**Data**	**CRC**

- Wireless considerations
  - Control information for Physical Layer
  - Ensure robustness for header
  - Explicit multi-hop routing
  - Possibly different data rates for different parts of packet

Error control: detection and recovery

- Detection: only detect errors
  - Make sure corrupted packets get discarded
  - Cyclical Redundancy Checks
    - Detect single bit errors
    - Detect “burst” errors of several contiguous bits

- Recovery: also try to recover from small bit errors
  - Forward error correction
  - Retransmissions
  - Far more important for wireless because the cost of transmission is higher

Medium Access Control

- How does a network determine which transmitter gets to transmit?

- Remember: the wireless medium is inherently broadcast
  - Two simultaneous transmitters may lose both packets

Analogy: wireless medium as acoustic

- **How do we determine who gets to speak?**
  - Two simultaneous speakers also lose both “transmissions”

- Task: in one minute you will have to recite the alphabet
  - We’ll jump by tables, one person per letter
  - You all fail if two people speak at the same time
  - I will ban any strategy that two tables use

Analogy: wireless medium as acoustic

- How do we determine who gets to speak?
  - Two simultaneous speakers also lose both “transmissions”

- Eye contact (or raise hand) -> out-of-band communication
- Wait until it’s quiet for some time -> carrier sense multiple access
- Strict turn order -> time division multiple access
- Just speak and hope it works -> ALOHA
- Everybody sing at different tones -> frequency division multiple access (stretching the metaphor)
- Everyone speak in different languages -> code division multiple access

- Others?

MAC protocol categorization

Medium Access Control Protocols

Contention-Based Protocols

- ALOHA
- CSMA

Contention-Free Protocols

- FDMA
- TDMA

Also, CDMA

ALOHA

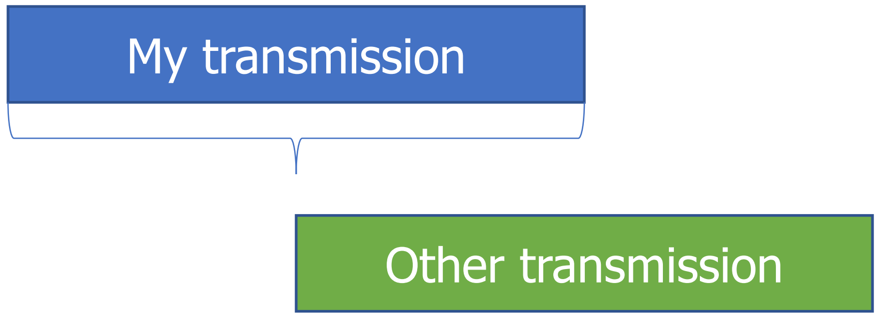
- ALOHAnet (1971)
  - University of Hawaii – Norman Abramson
  - First demonstration of wireless packet network

- Rules
  1. If you have data to send, send it

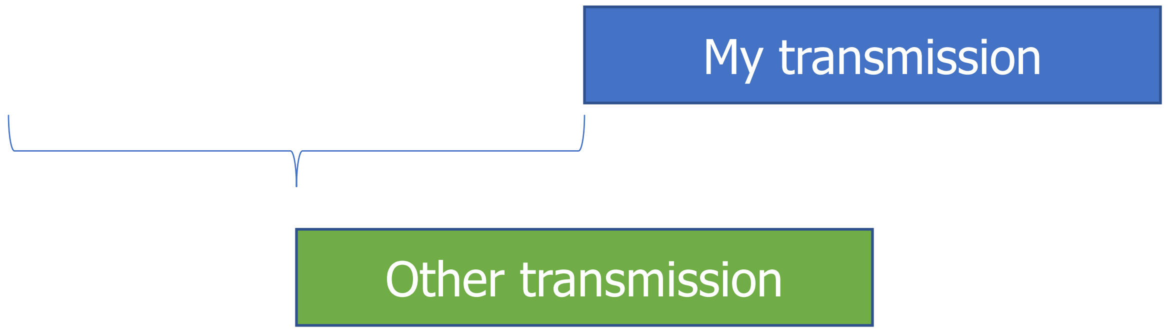
- Two (or more) simultaneous transmissions will collide and be lost
  - Wait a duration of time for an acknowledgement
  - If transmission was lost, try sending again “later”
    - Want some kind of exponential backoff scheme here

Packet collisions

- Each packet transmission has a window of vulnerability
  - Twice the on-air duration of a packet
  - Transmissions during the packet are bad

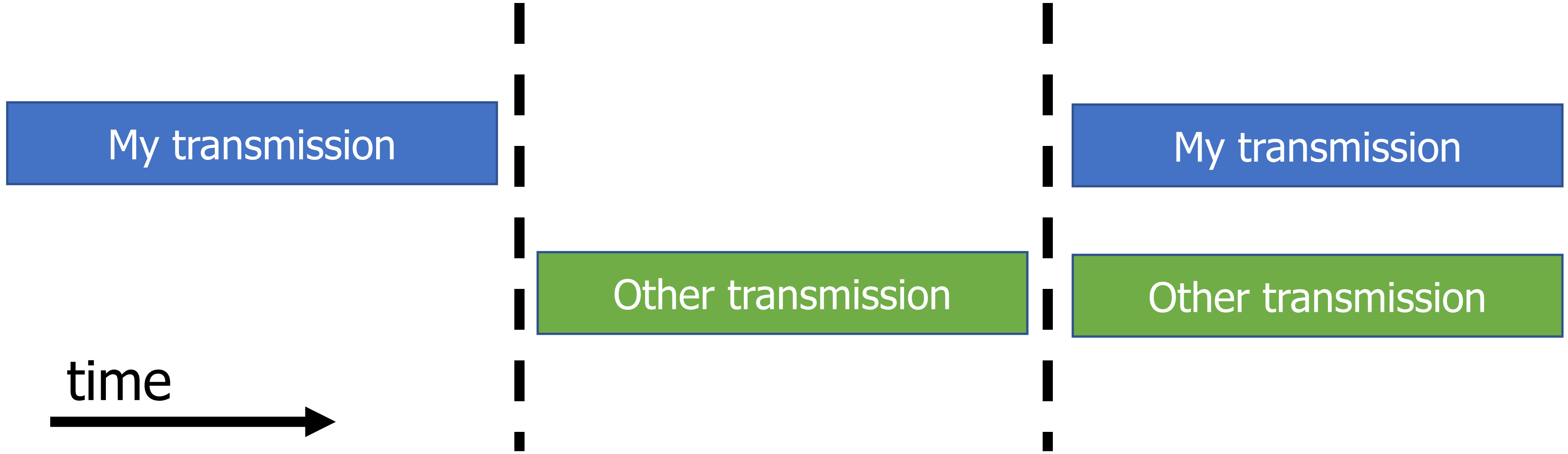


  - Transmissions before packet can also be bad



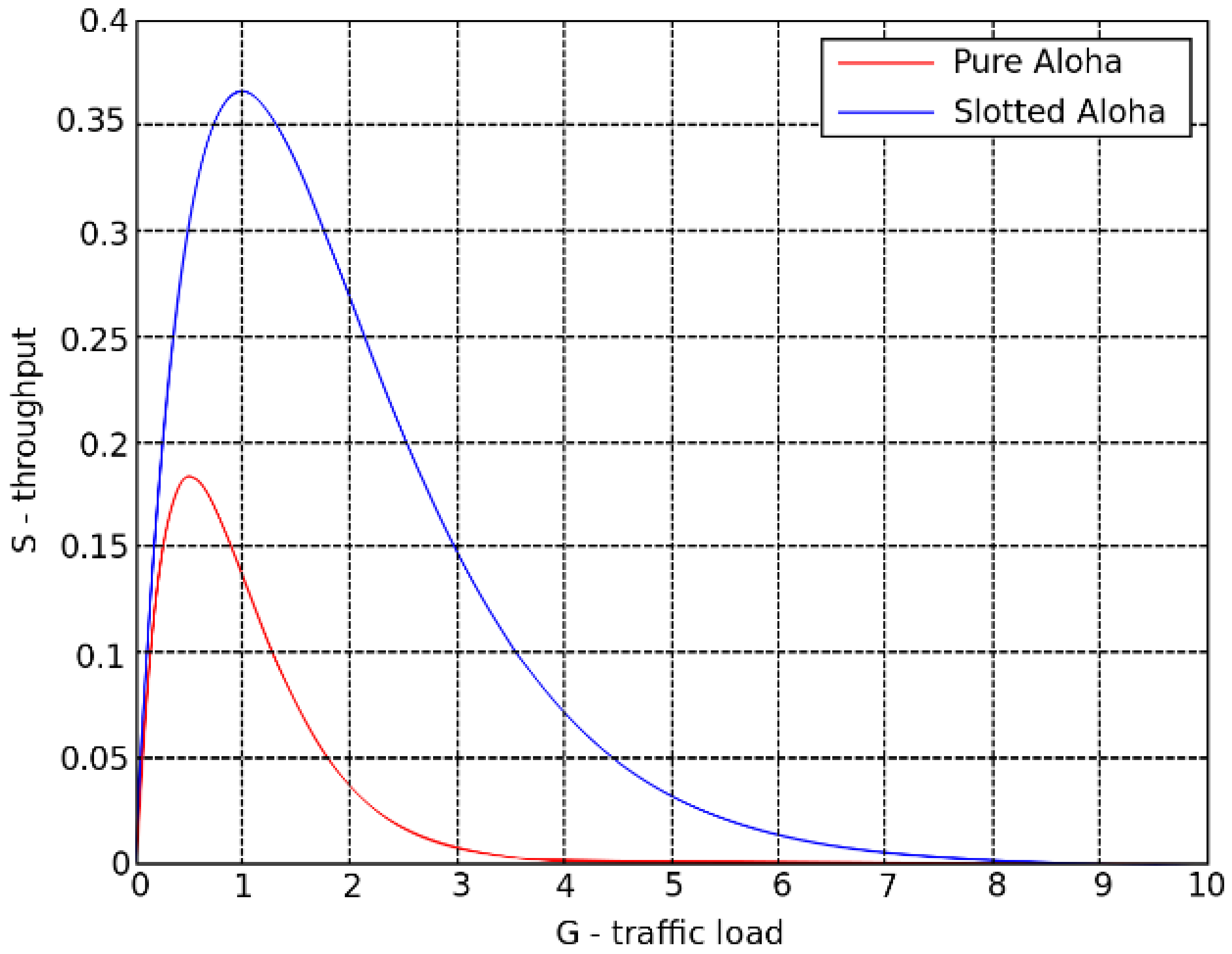
Slotted ALOHA

- Split time into synchronized "slots"
- Any device can transmit whenever it has data
  - But it must transmit at the start of a slot
  - And its transmission cannot be longer than a slot
  - Removes half of the possibilities for collisions!
    - At the cost of some synchronization method



ALOHA throughput

- It can be shown that traffic maxes out at
  - ALOHA: 18.4%
  - Slotted ALOHA: 36.8%
- Assuming Poisson distribution of transmission attempts
- Slotted throughput is double because the "before" collisions can no longer occur



Capture effect

- Actually, two packets at once isn't *always* a total loss
  - The louder packet can still sometimes be heard if loud enough

- How much louder?
  - Ballpark 12-14 dB

- When does this work?
  - Depends on the radio hardware
  - Louder packet first almost always works
  - Louder packet second *sometimes* works

MAC protocol categorization

Medium Access Control Protocols

Contention-Based Protocols

- ALOHA
- CSMA

Contention-Free Protocols

- FDMA
- TDMA

Also, CDMA

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

- First listen for a duration and determine if anyone is transmitting
  - If idle, you can transmit
  - If busy, wait and try again later

- "listen before send"

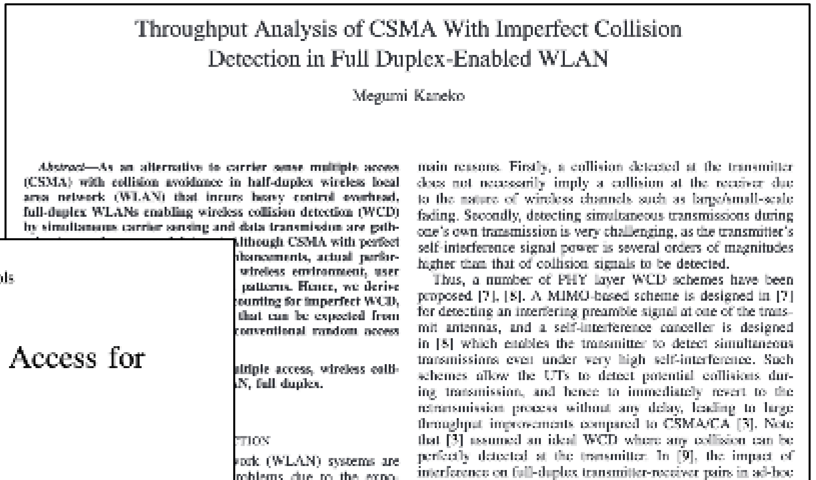
- Can be combined with notion of slotting
  - If current slot is idle, transmit in next slot
  - If current slot is busy, follow some algorithm to try again later

CSMA/CD – CSMA with Collision Detection

- Detect collisions during your own transmission
  - Works great on wired mediums (Ethernet, I2C)

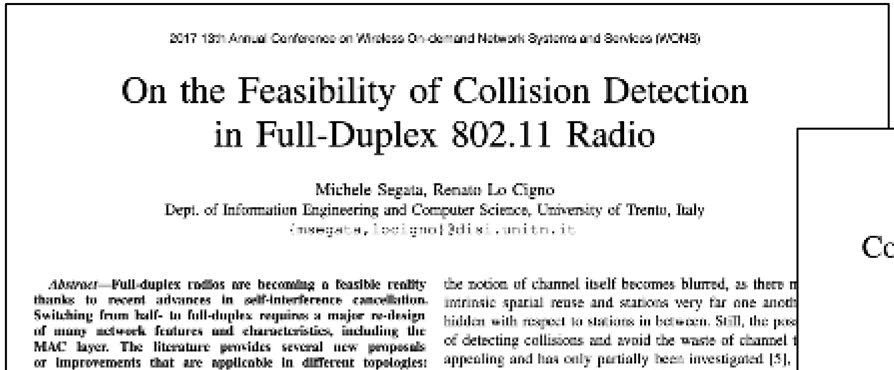
- Very challenging for wireless systems
  - Transmit and receive are usually the same antenna
  - Receiving while transmitting would be drowned out by transmission
    - Remember: TX at 8 dBm and RX at -95 dBm

  - Area of active research!



Throughput Analysis of CSMA With Imperfect Collision Detection in Full Duplex-Enabled WLAN

Megumi Kaneko



2017 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS)

On the Feasibility of Collision Detection in Full-Duplex 802.11 Radio

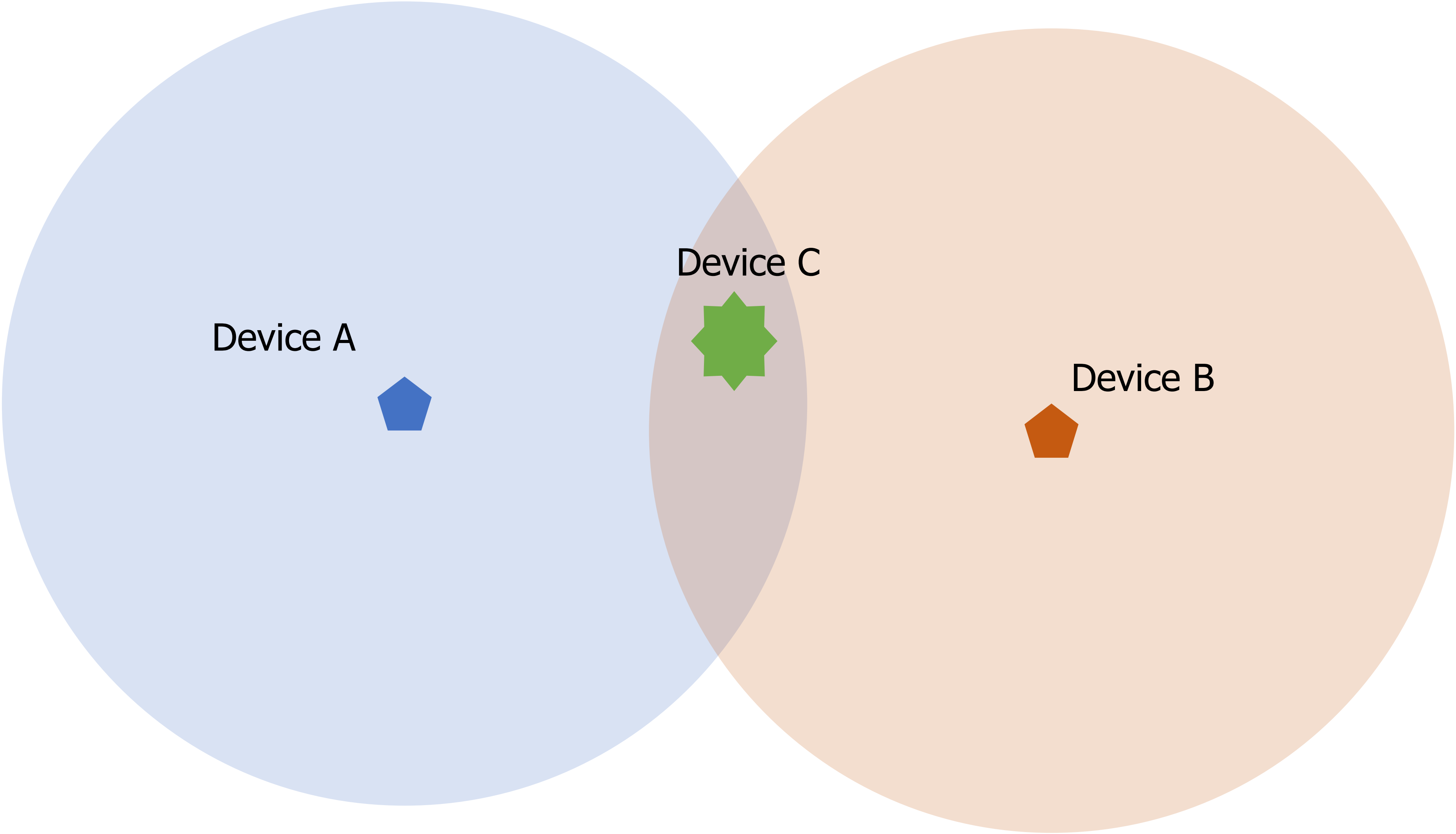
Michele Segata, Renato Lo Cigno
Dept. of Information Engineering and Computer Science, University of Trento, Italy

2014 IEEE 22nd International Conference on Network Protocols

Concise Paper: Semi-Synchronous Channel Access for Full-Duplex Wireless Networks

Xiufeng Xie and Xinyu Zhang
University of Wisconsin-Madison
Email: {xiufeng,xyzhang}@ece.wisc.edu

Hidden terminal problem



CSMA with RTS/CTS

- Hidden terminal problem means that two transmitters might never be able to detect each other’s transmissions

- A partial solution
  - When channel is idle, transmitter sends a short Request To Send (RTS)
  - Receiver will send a Clear To Send (CTS) to only one node at a time
  - RTS collisions are faster and less wasteful than hidden terminal collisions
  - Downside: overhead is high for waiting for CTS when contention is low

MAC protocol categorization

Medium Access Control Protocols

- Contention-Based Protocols
  - ALOHA
  - CSMA
- Contention-Free Protocols
  - FDMA
  - TDMA

Also, CDMA

Contention-free access control protocols

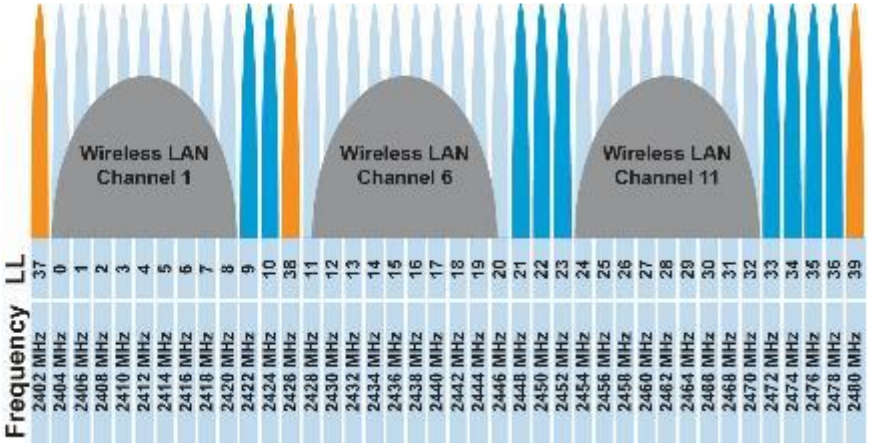
- Goal: split up communication such that devices will not conflict
- Can be predetermined or reservation-based
  - Devices might request to join the schedule and be given a slot
    - Devices lose their slot if it goes unused for some amount of time
    - Reservations often occur during a dedicated CSMA contention slot
  - Assignment of schedules can be complicated
- Really efficient at creating a high-throughput network
  - Assuming they are all following the same protocol
  - Otherwise, interference can be very problematic

FDMA – Frequency Division Multiple Access

- Split transmissions in frequency
  - Different carrier frequencies are independent
  - Fundamentally how RF spectrum is split

- Technically, each device uses a separate, fixed frequency
  - Walkie-talkies

- Conceptually, how RF channels work
  - WiFi networks pick different bands
  - 802.15.4 picks a channel to communicate on



TDMA – Time Division Multiple Access

- Split transmissions in time
  - Devices share the same channel

- Splits time into fixed-length windows
  - Each device is assigned one or more windows
  - Can build a priority system here with uneven split among devices

- Requires synchronization between devices
  - Often devices must listen periodically to resynchronize
  - Less efficient use of slots reduce synchronization
    - Large guard windows. E.g. 1.5 second slot for a 1 second transmission

Real-world protocol access control

- ALOHA
  - BLE advertisements
  - Unlicensed LPWANs: Sigfox, LoRaWAN

- CSMA
  - WiFi (slotted, CSMA/CA)

- TDMA
  - BLE connections
  - Cellular LPWANs: LTE-M and NB-IoT

Outline

- OSI Layers
- Internet Architecture (Upper Layers)
- Physical Layer
- Data Link Layer