Lecture 02
Physical and Link Layers

CS397/497 – Wireless Protocols for IoT

Branden Ghena – Winter 2021

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

Today’s Goals

- Introduce OSI layer model of communication
- 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**
- Physical Layer
- Data Link Layer

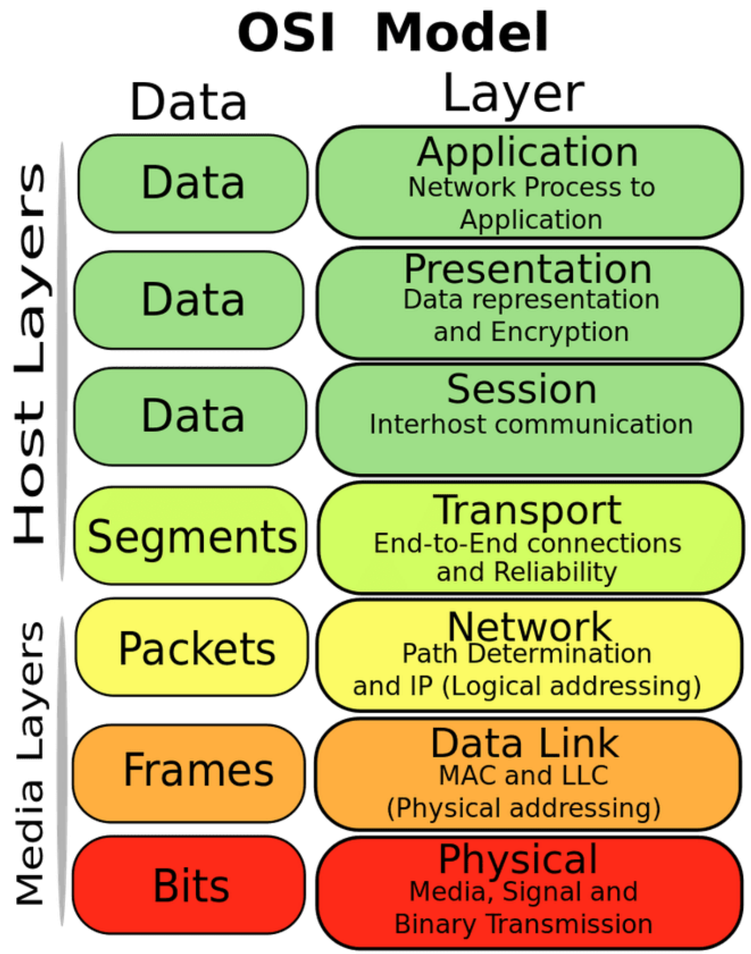
Communication layers

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

What goes on at each of these?

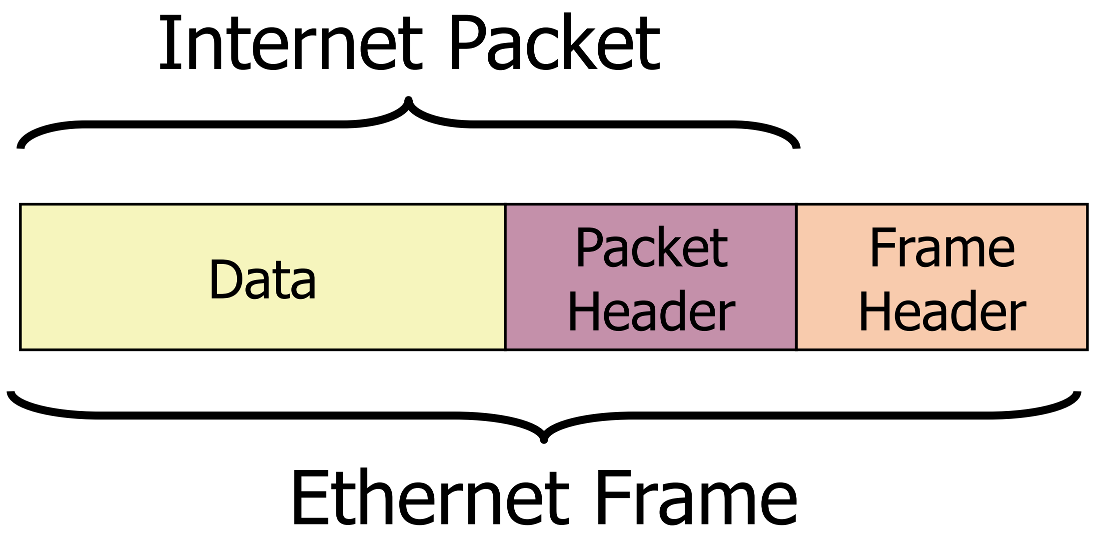
OSI model of communication layers

- Transport
  - How to form connections between computers
  - TCP and UDP
- Network
  - How to send packets between networks
  - IP
  - CS domain: CS340
- Data Link
  - How to send frames of data
  - Ethernet, WiFi
  - **Our focus**
- Physical
  - How to send individual bits
  - Ethernet, WiFi
  - EE domain: EE307, EE380, EE395

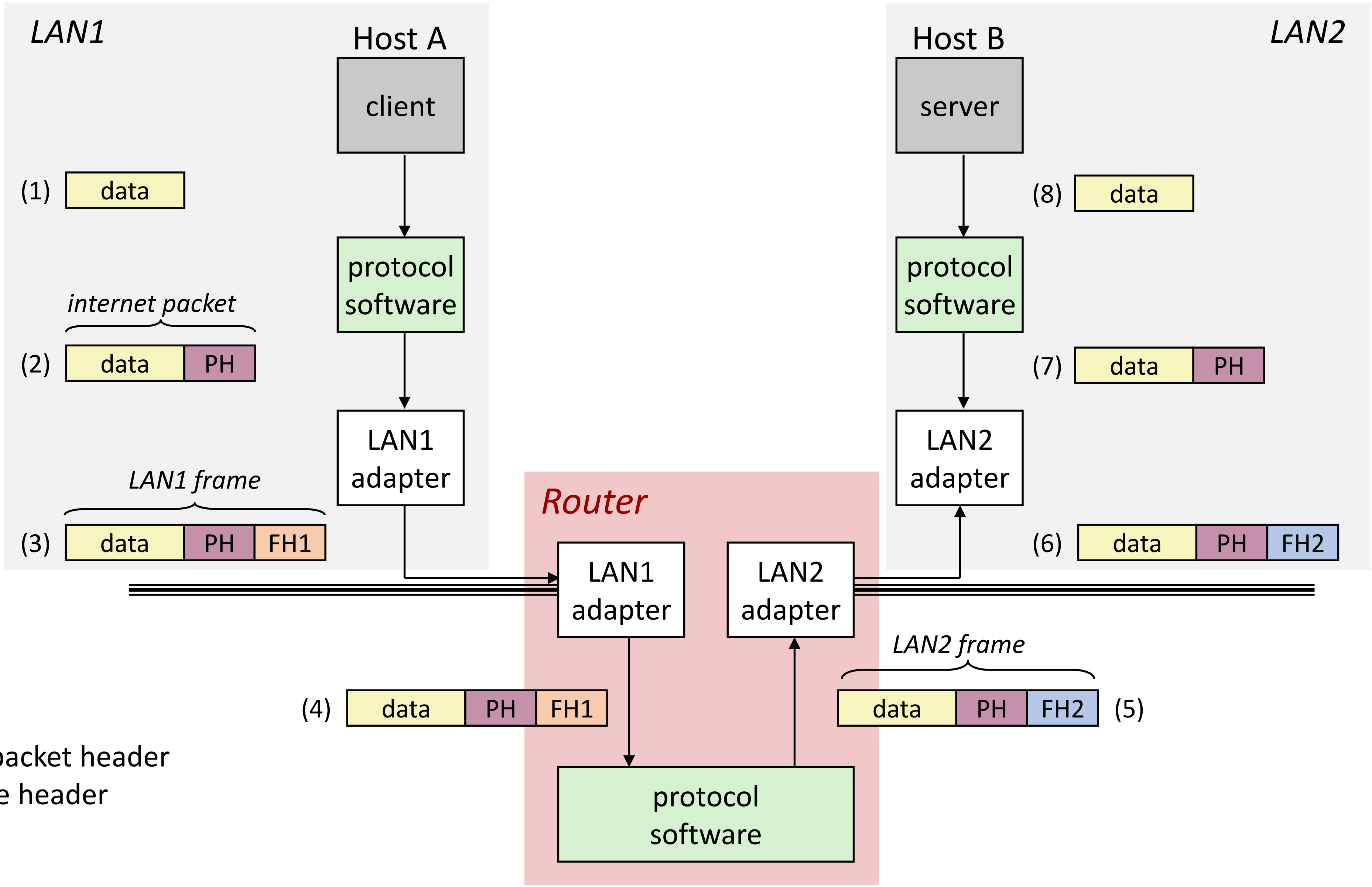


Protocols are "layered"

- 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



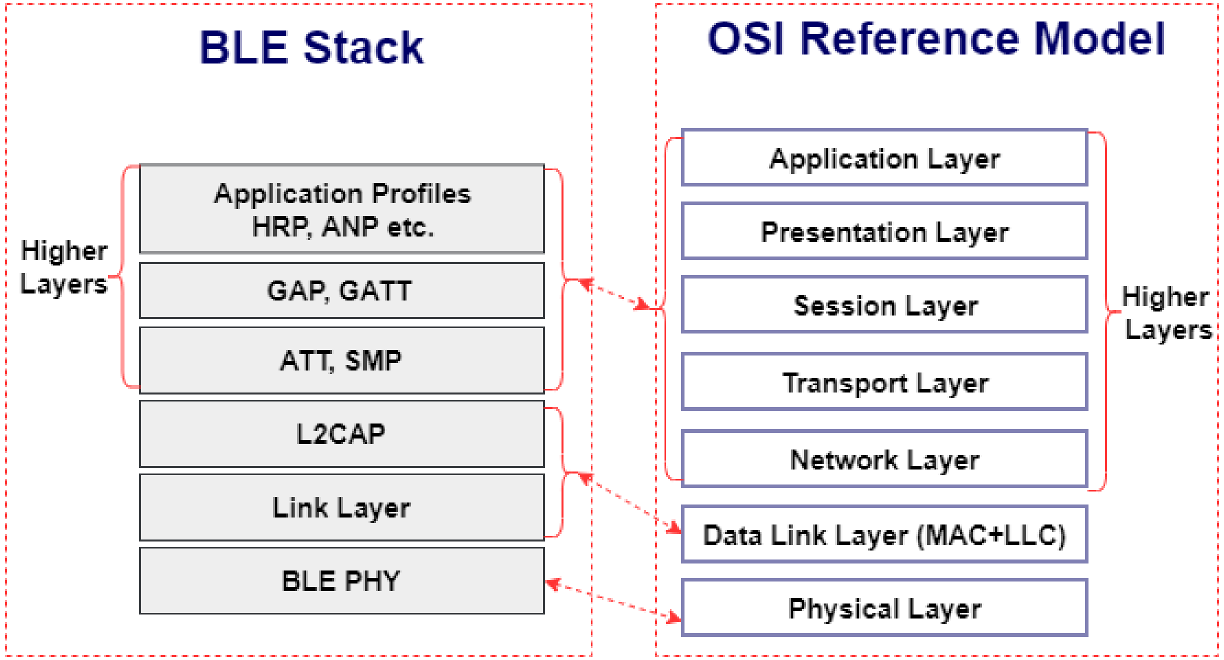
Transmitting data between networks

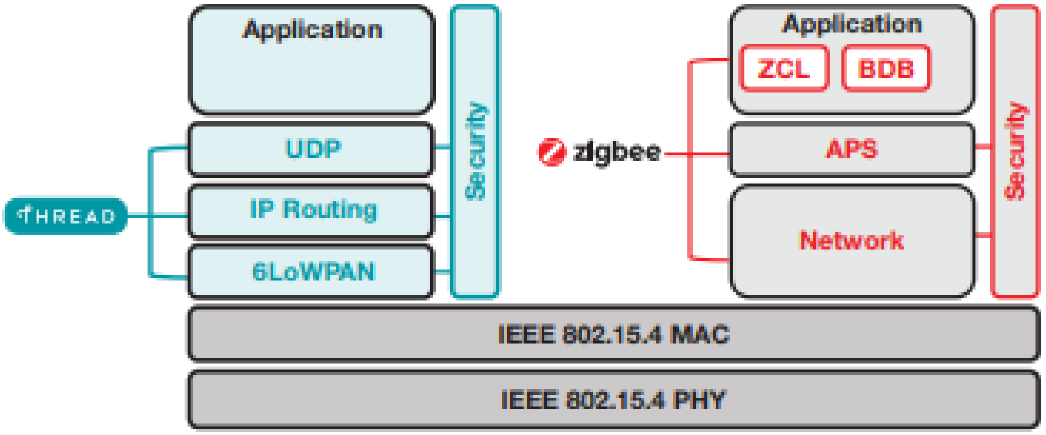


PH: Internet packet header
FH: LAN frame header

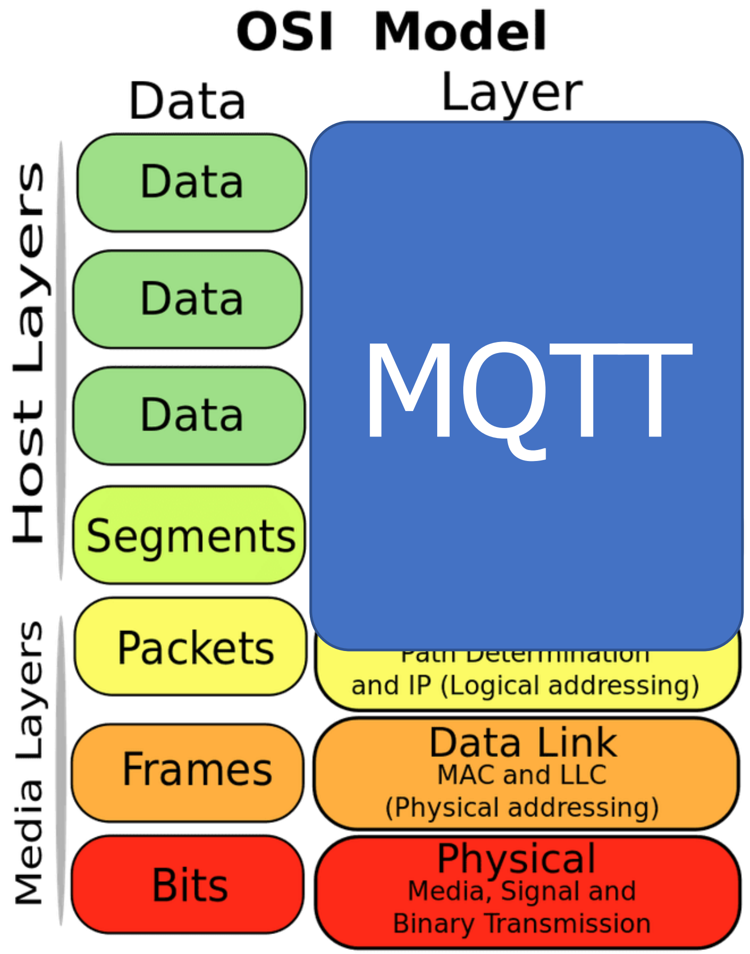
Model != reality

- 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
- **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

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!

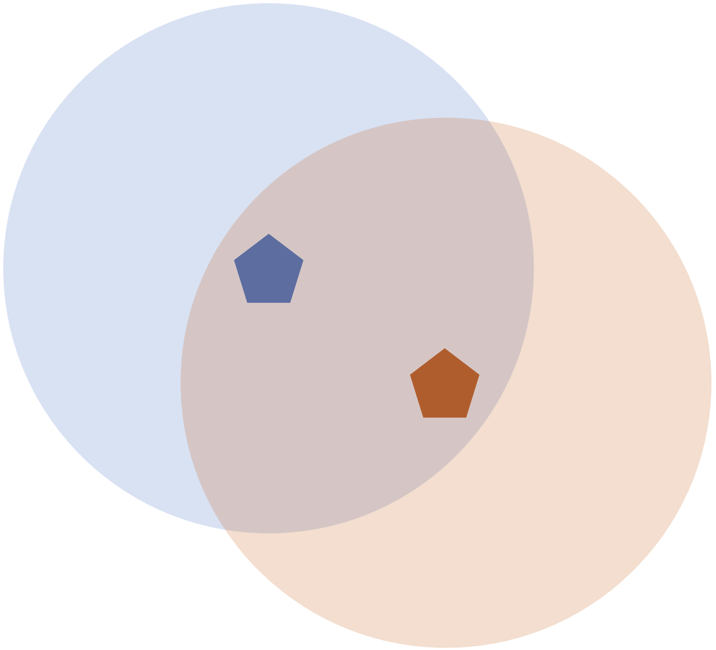
- Wired networks are constant, reliable, and physically isolated
  - Ethernet has the same throughput minute-to-minute
  - Bits sent through Ethernet or USB are (usually) received

- 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

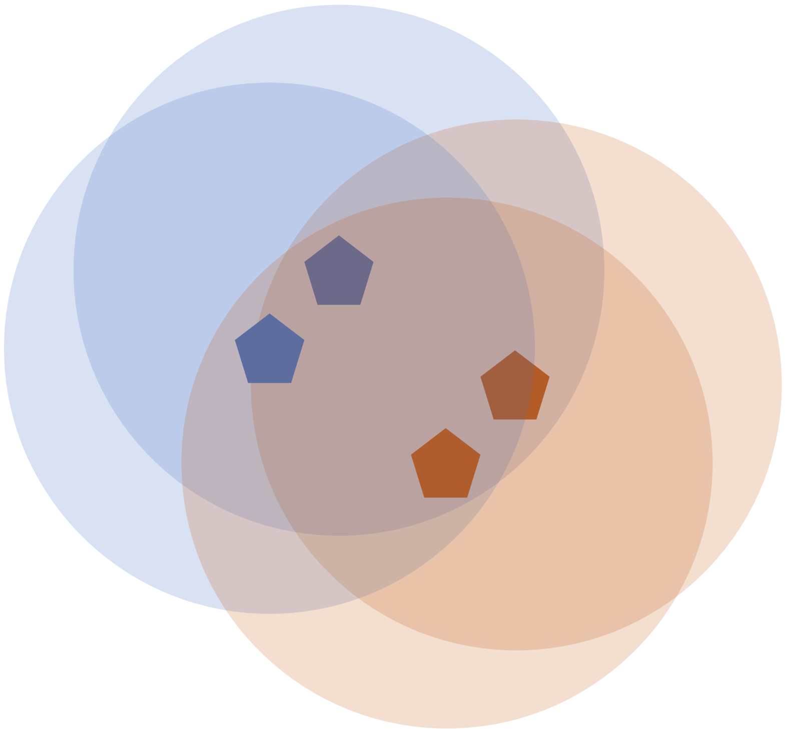
- Wireless communication is inherently broadcast
  - Energy is distributed in space
  - Signals must compete with other signals in same frequency band



Increasing network capacity is challenging

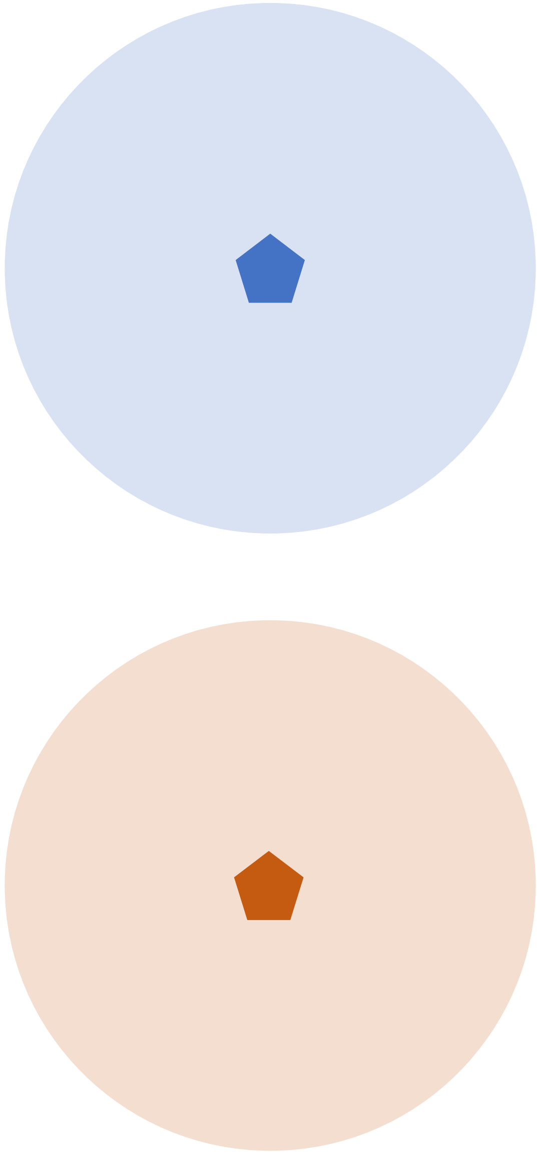
- Wired networks just add more wires
  - Buses are many signals in parallel to send more data

- 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 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

Propagation degrades RF signals

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

- Obstacles can weaken signal through absorption or reflection

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

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.

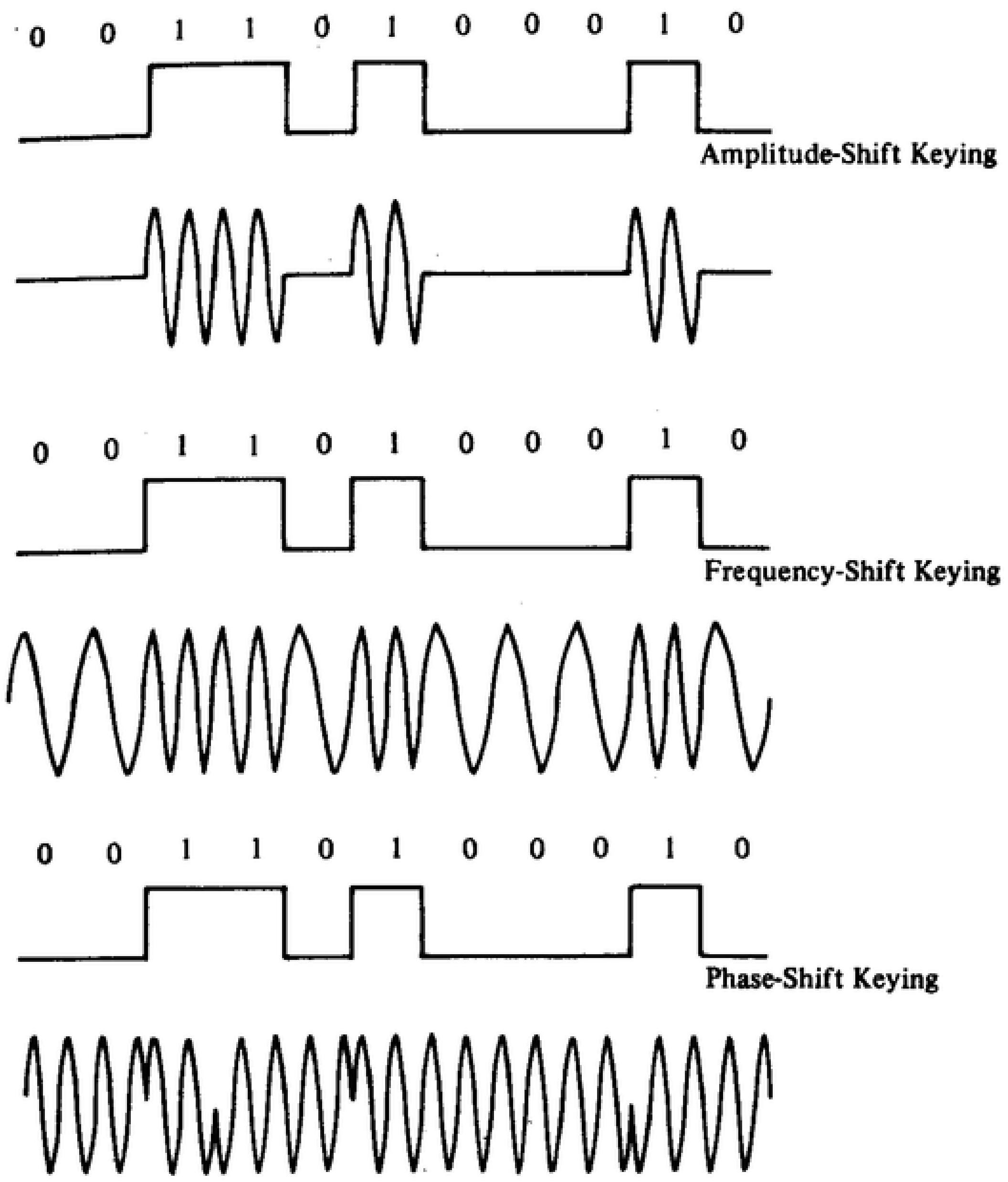
$P_f(n)$ = the floor loss penetration factor.

- Models like this are *more* trustworthy than FSPL
  - https://en.wikipedia.org/wiki/ITU_model_for_indoor_attenuation

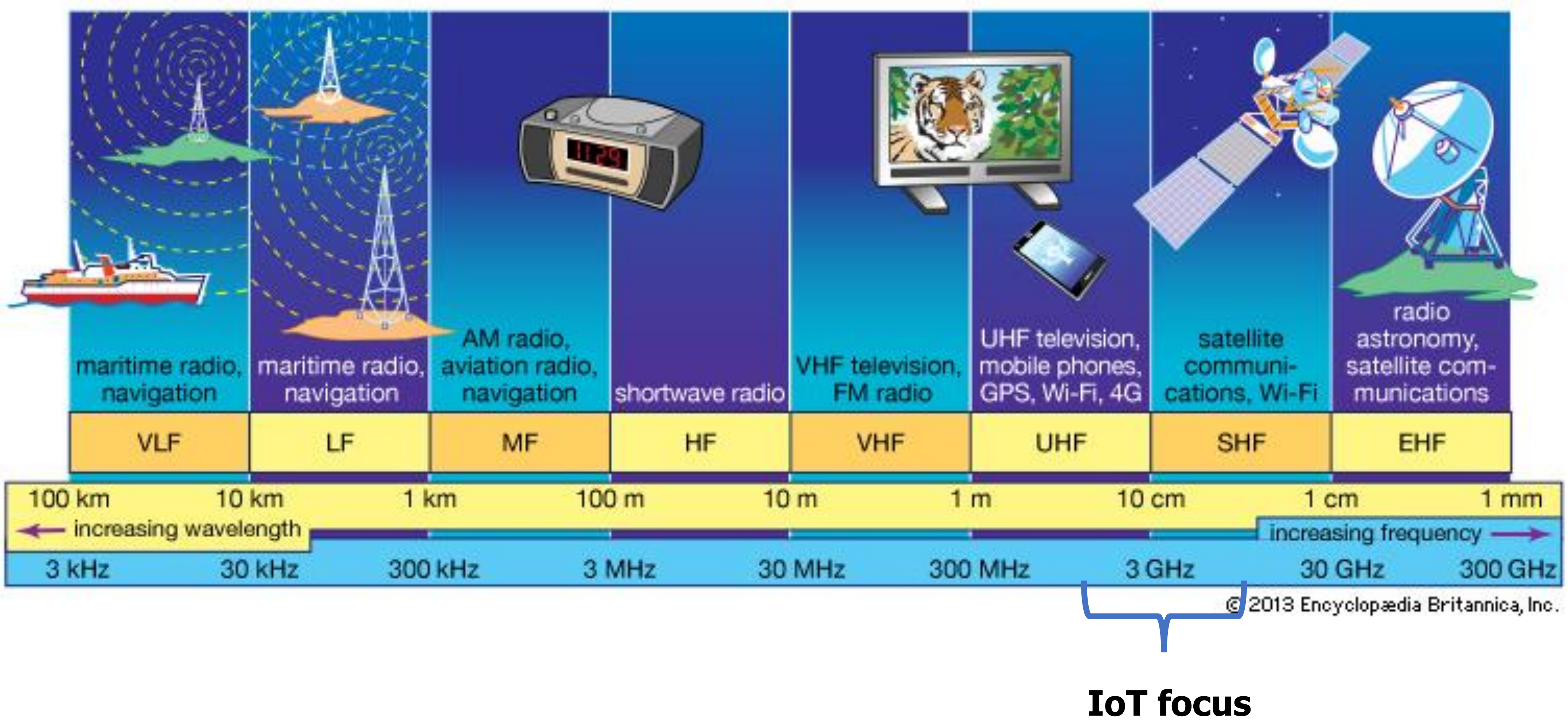
Modulation

- Encoding digital data in an analog “carrier” signal

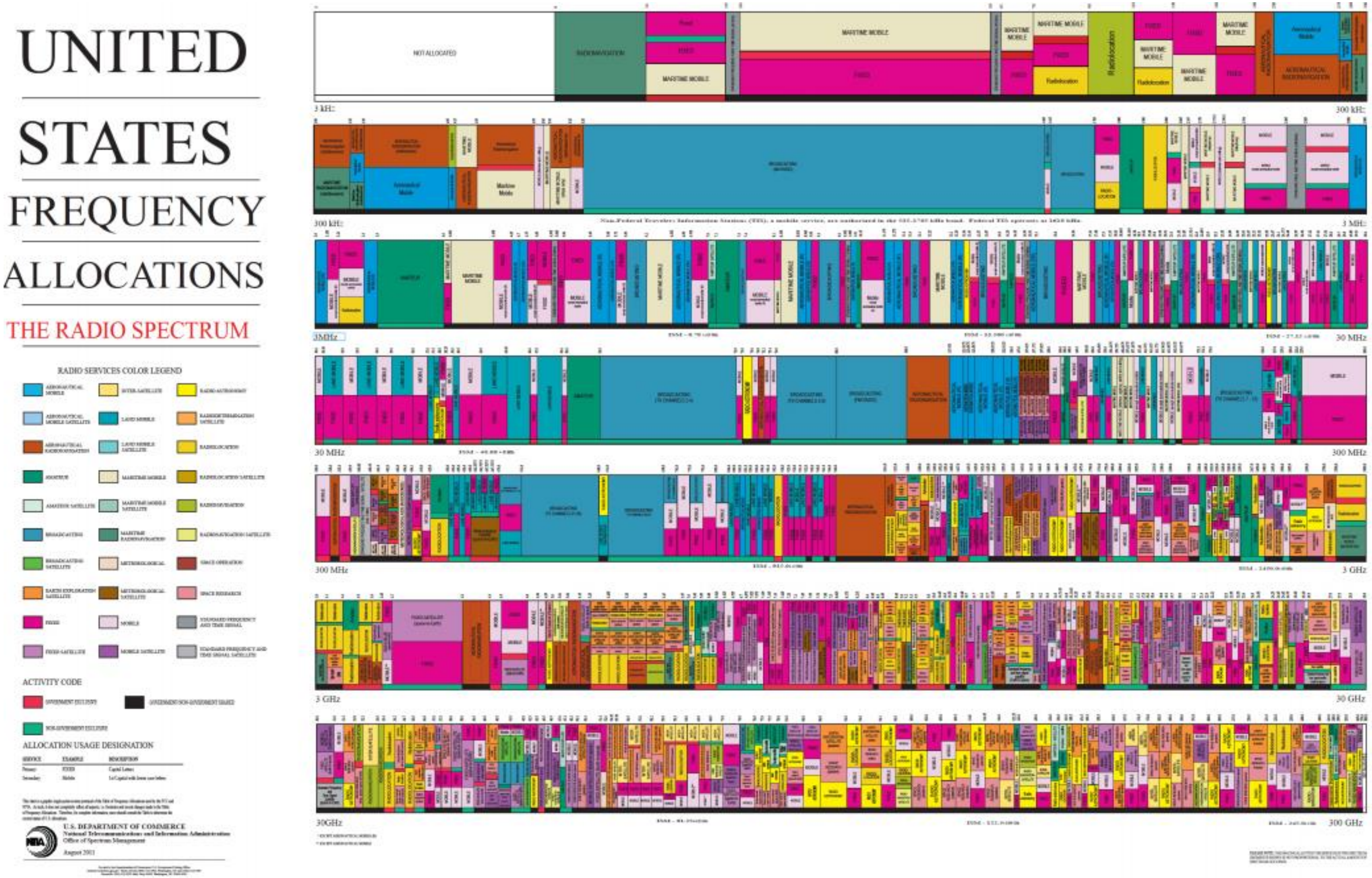
- Basic forms:
- Amplitude-shift Keying (ASK)
  - Modify amplitude of carrier signal
- Frequency-shift Keying (FSK)
  - Modify frequency of carrier signal
- Phase-shift Keying (PSK)
  - Modify phase of carrier signal



RF communication frequencies

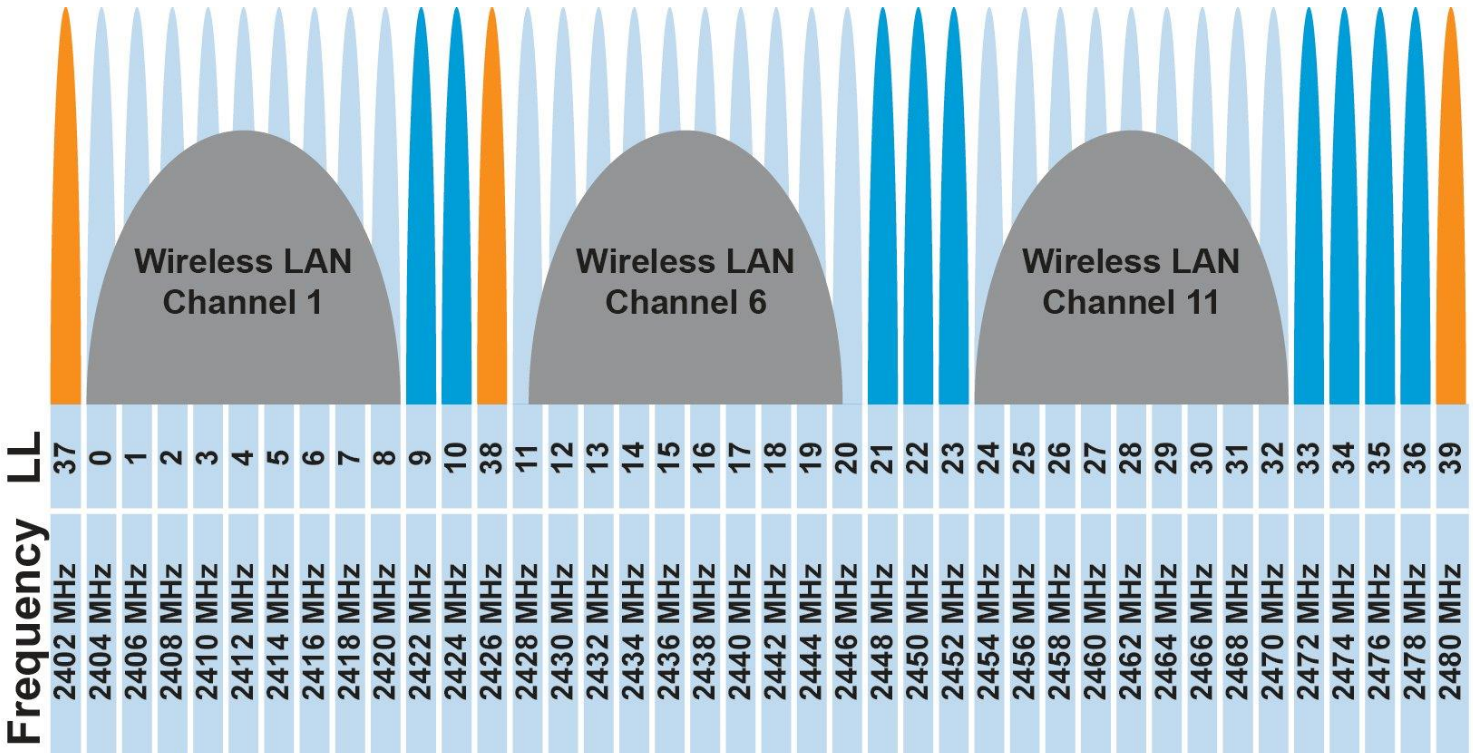


Wireless spectrum is allocated to specific uses



Unlicensed bands are where IoT thrives

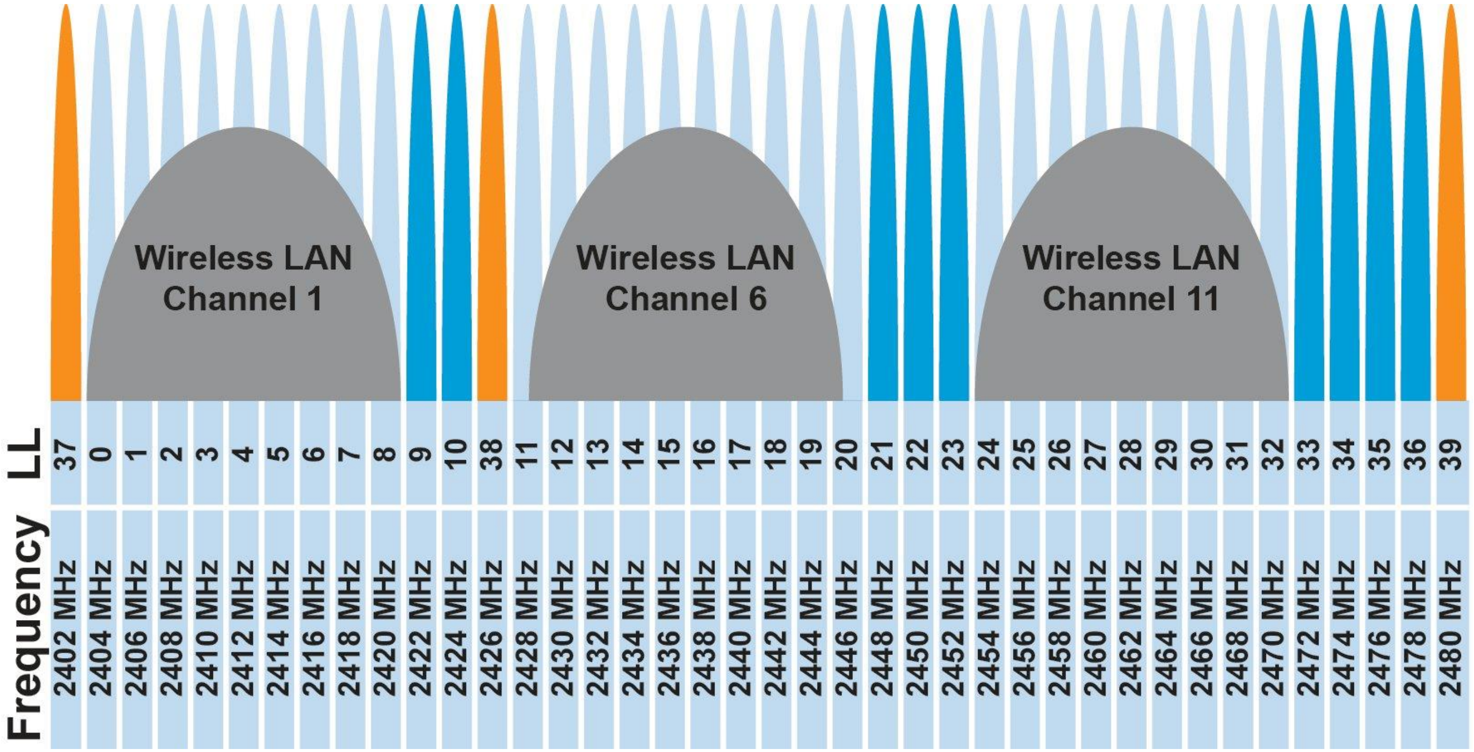
- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi



- 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

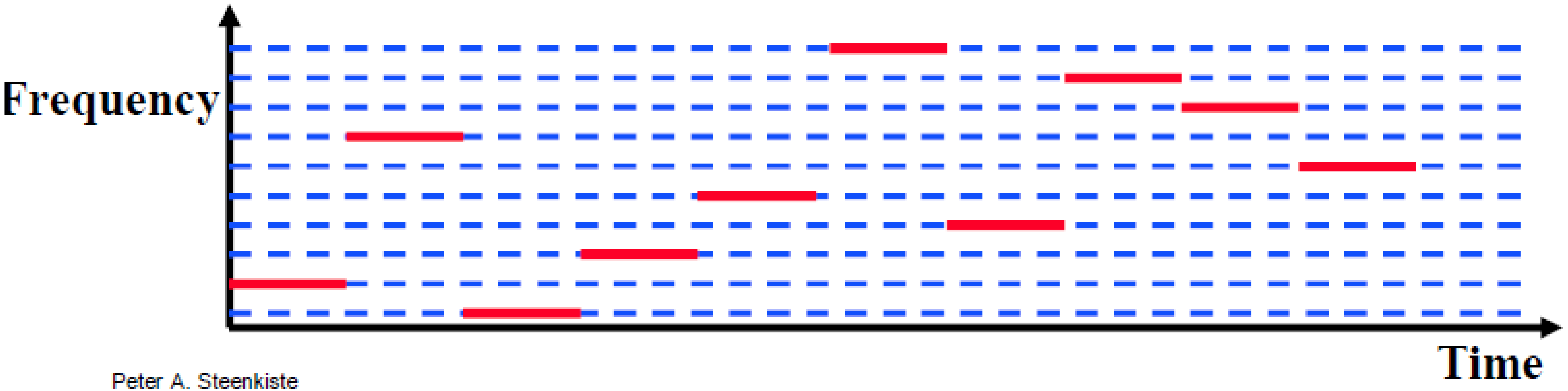


- Cellular uses licensed bands at great cost
  - **Why? No interference from other users**

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 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

Outline

- OSI 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

- 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”

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)

- Others?

MAC protocol categorization

Medium Access Control Protocols

Contention-Based Protocols

- ALOHA
- CSMA

Contention-Free Protocols

- FDMA
- TDMA

Also, CDMA

ALOHA

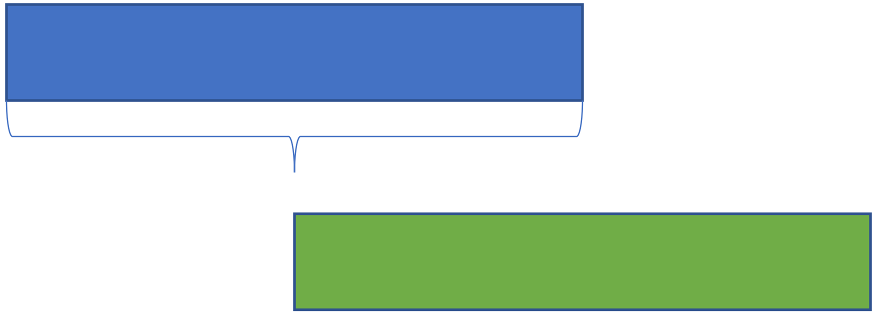
- ALOHAnet (1971)
  - University of Hawaii – Norman Abramson
  - First demonstration of wireless packet network

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

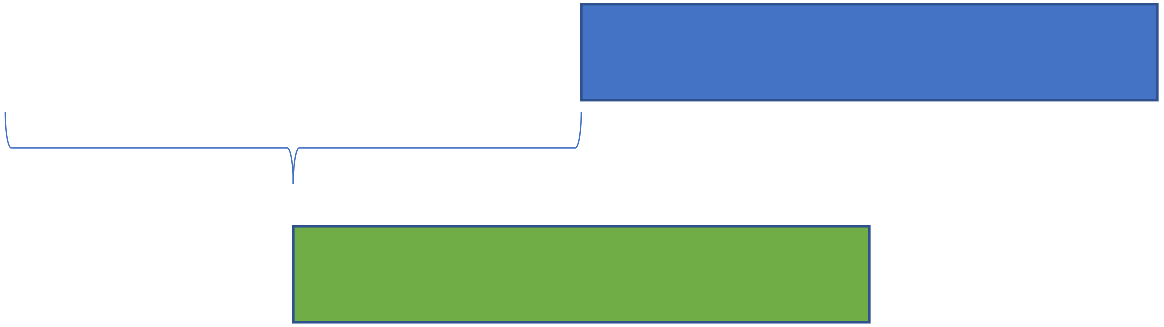
- Two (or more) simultaneous transmissions will collide and be lost
  - Wait a duration of time for an acknowledgement
  - If transmission was lost, try sending again “later”
    - Want some kind of exponential backoff scheme here

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

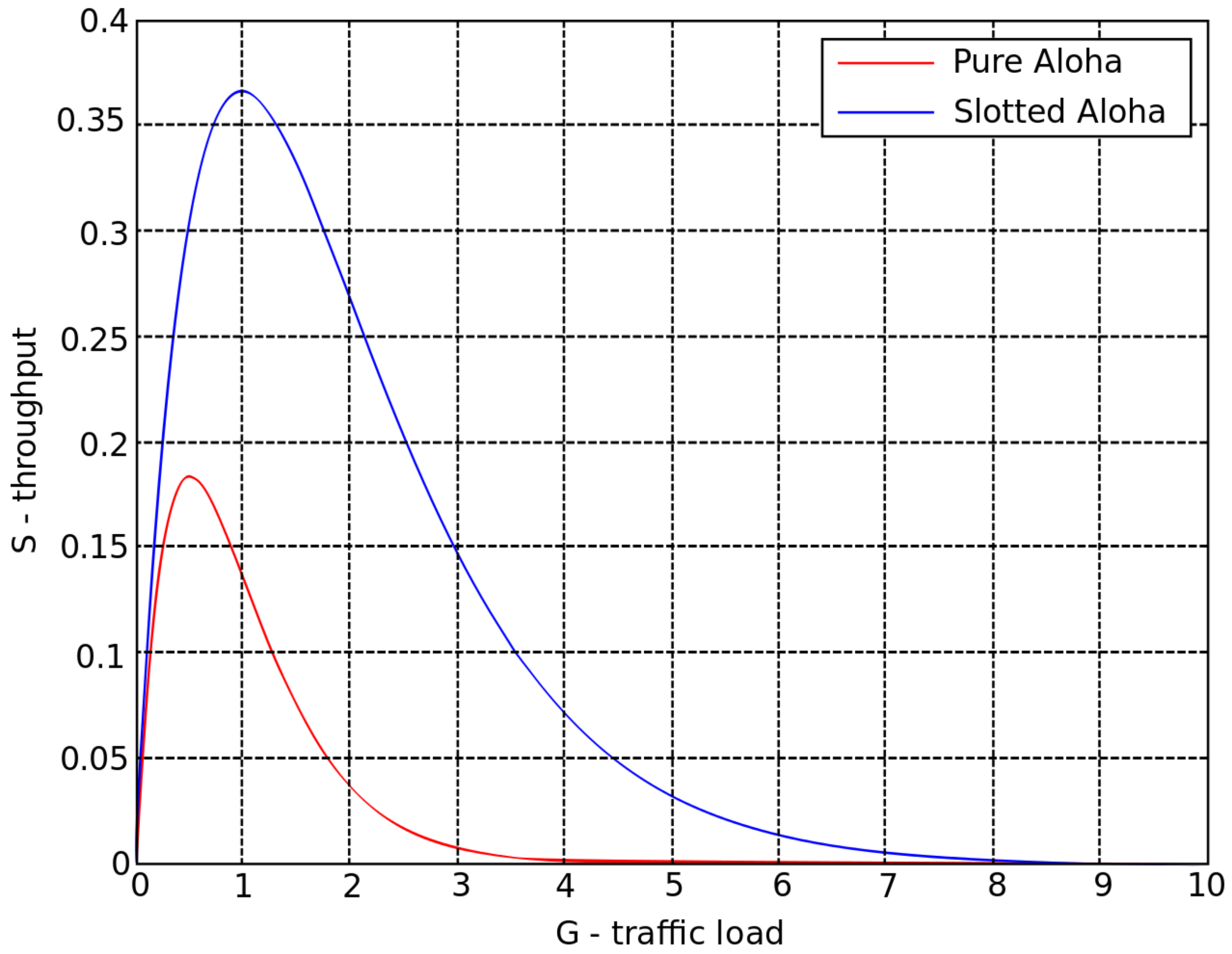


Slotted ALOHA

- 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

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”

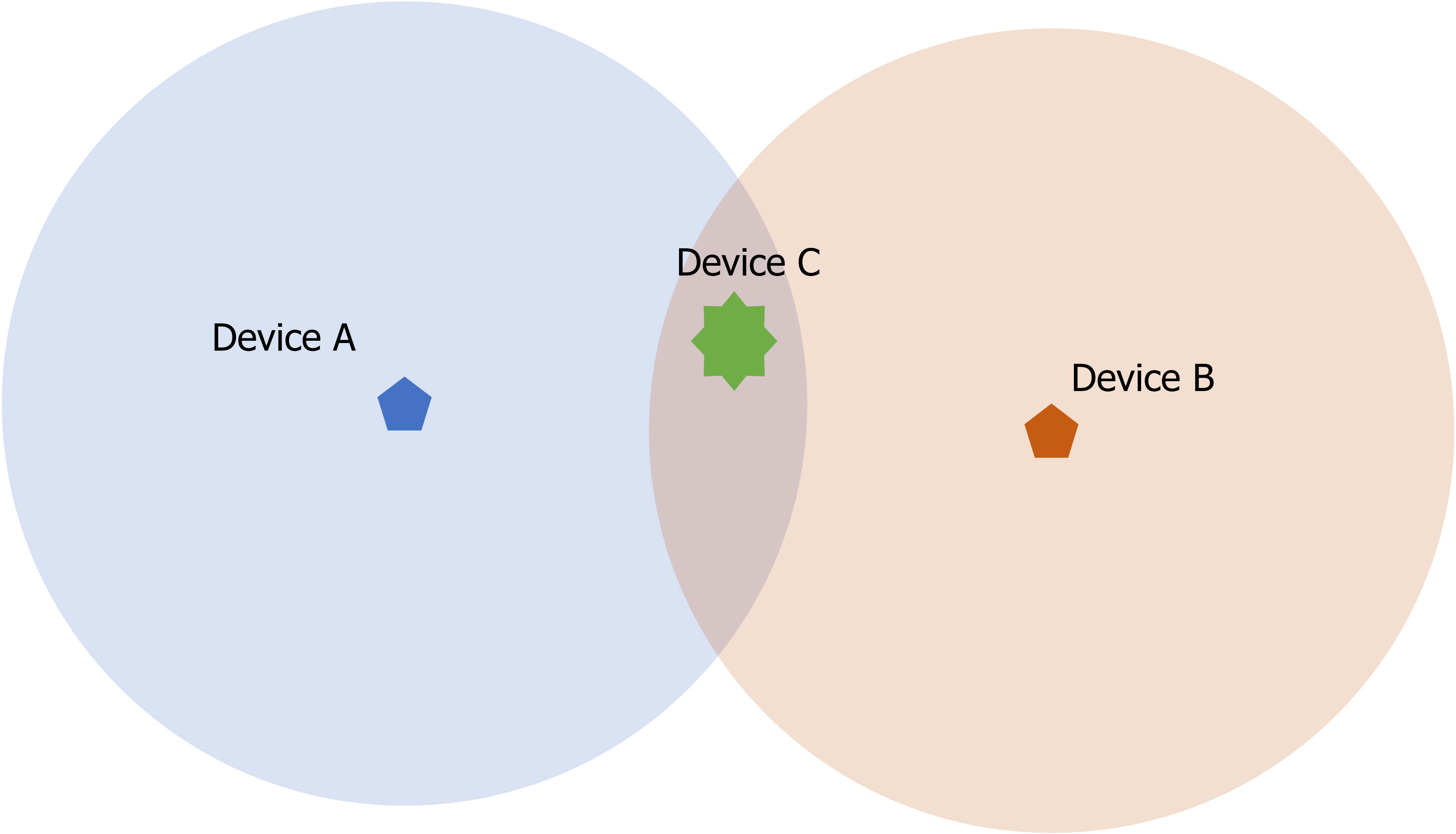
- Can be combined with notion of slotting
  - If current slot is idle, transmit in next slot
  - If current slot is busy, follow some algorithm to try again later

CSMA/CD – CSMA with Collision Detection

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

- Somewhere between challenging and impossible for wireless
  - 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

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

Contention-free access control protocols

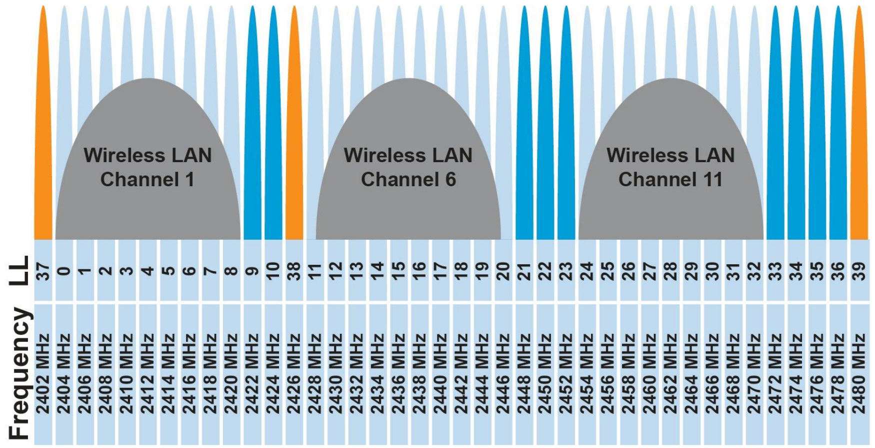
- Goal: split up communication such that devices will not conflict
- Can be predetermined or reservation-based
  - Devices might request to join the schedule and be given a slot
    - Devices lose their slot if it goes unused for some amount of time
    - Reservations often occur during a dedicated CSMA 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
- Physical Layer
- Data Link Layer