Wireless and Communication in the Internet of Things

Networking Speedrun

Pat Pannuto, UC San Diego

ppannuto@ucsd.edu

Today's Goals

- Introduce OSI layer model of communication

- Refresh how services find each other, operate

- 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
- ”The Upper Layers”
- Physical Layer
- Data Link Layer

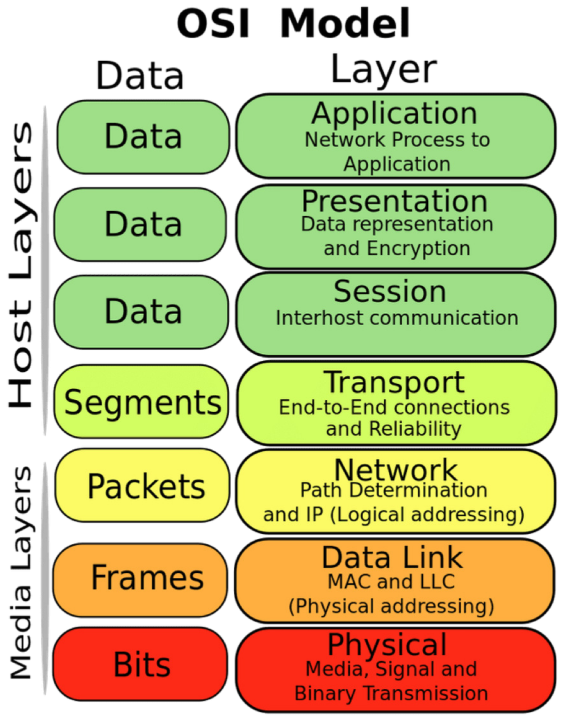
Communication layers

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

What goes on at each of these?

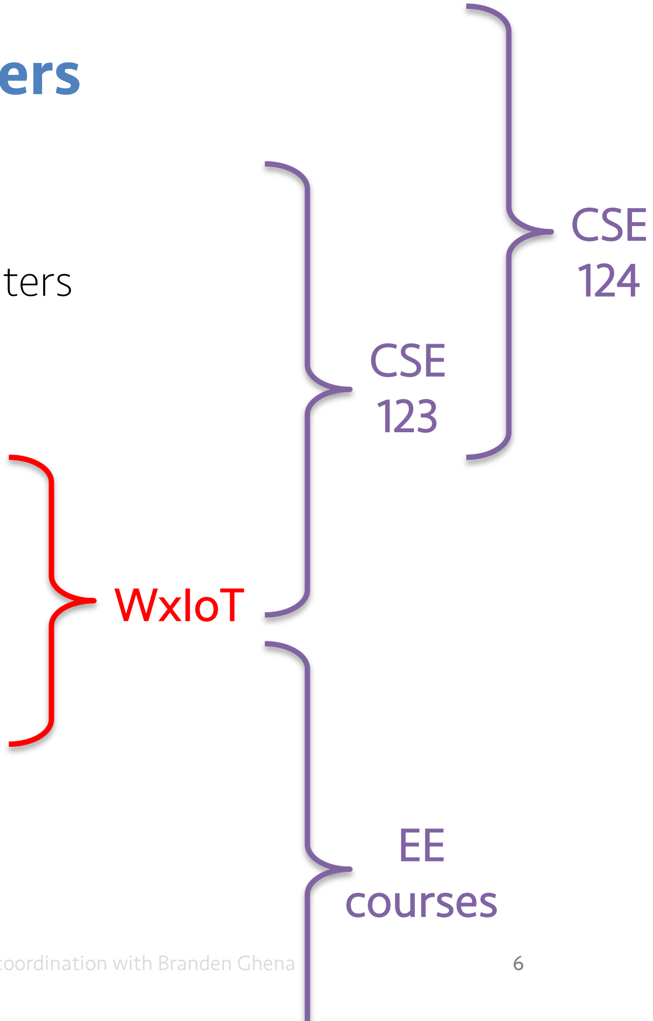
OSI model of communication layers

- 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
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

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



CSE 124

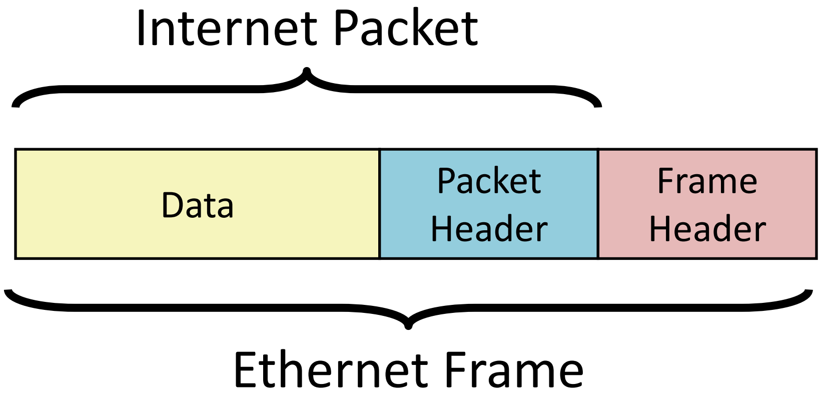
CSE 123

WxIoT

EE courses

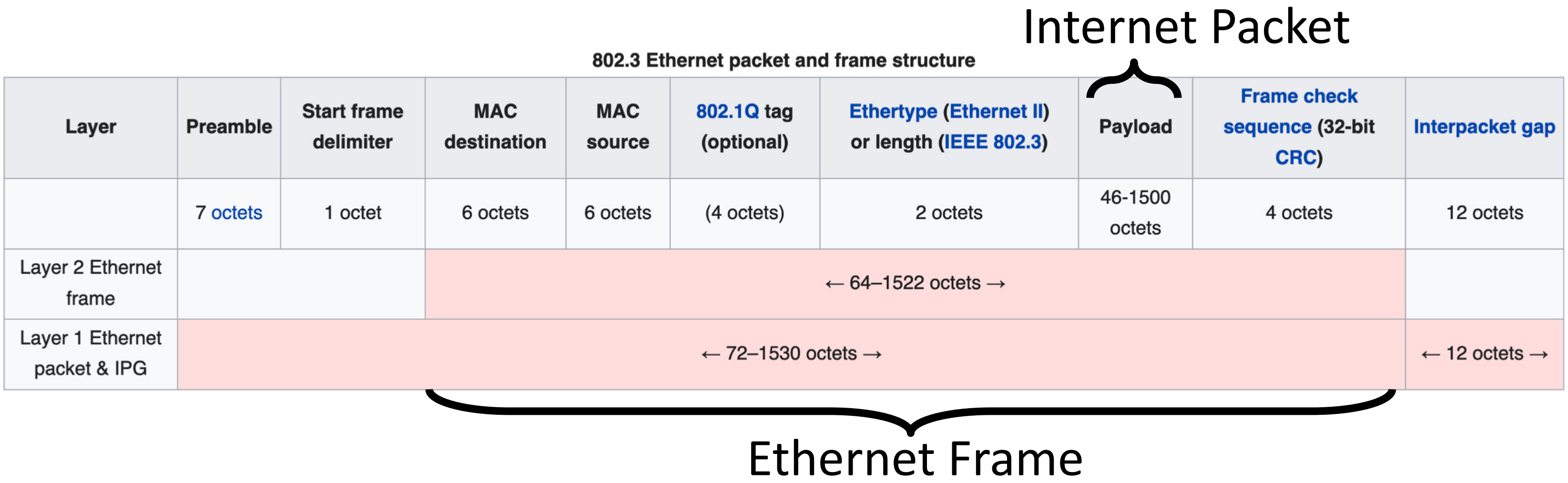
Protocols are "layered"

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



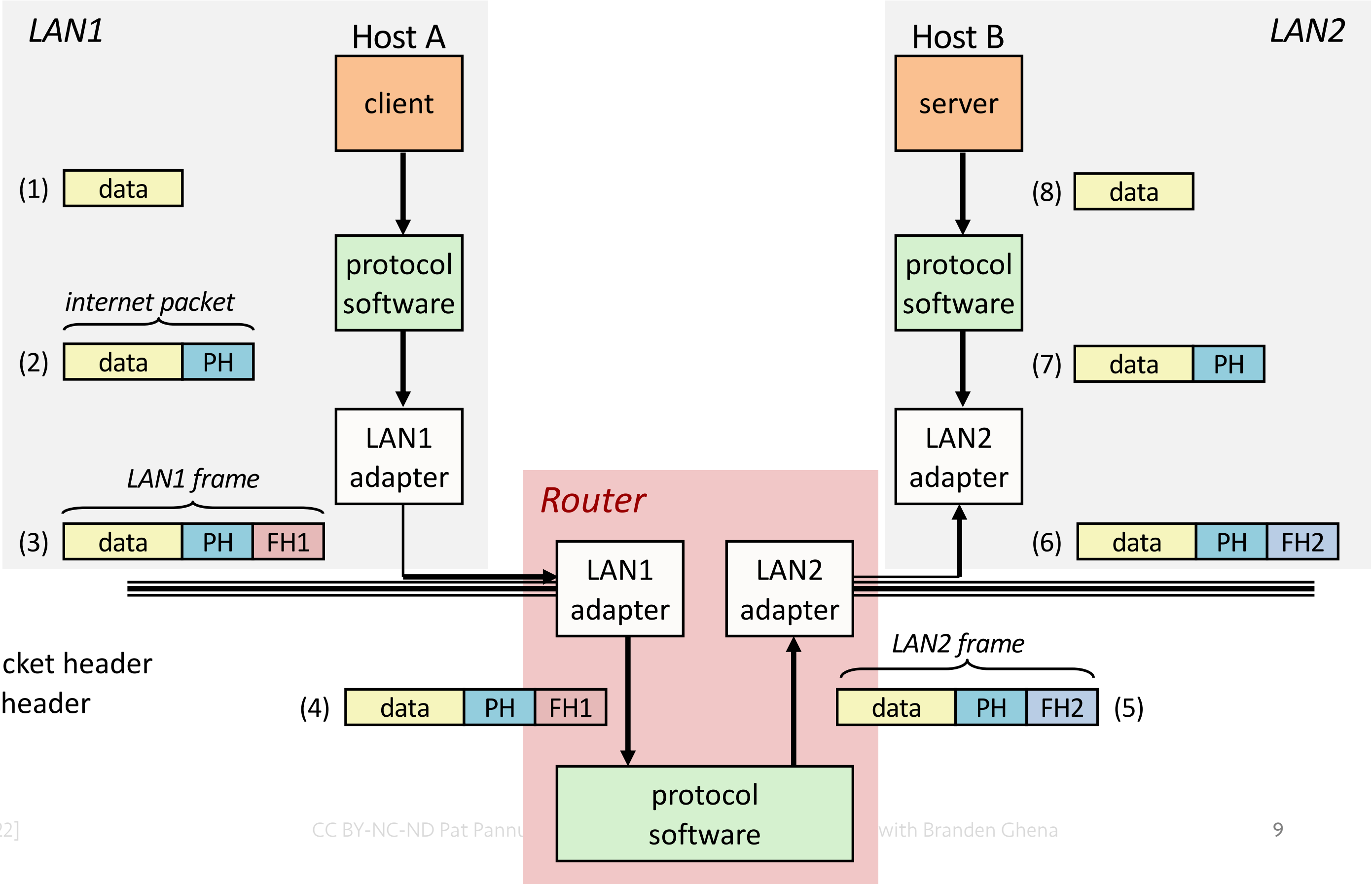
Internet Packet

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

Transmitting data between networks

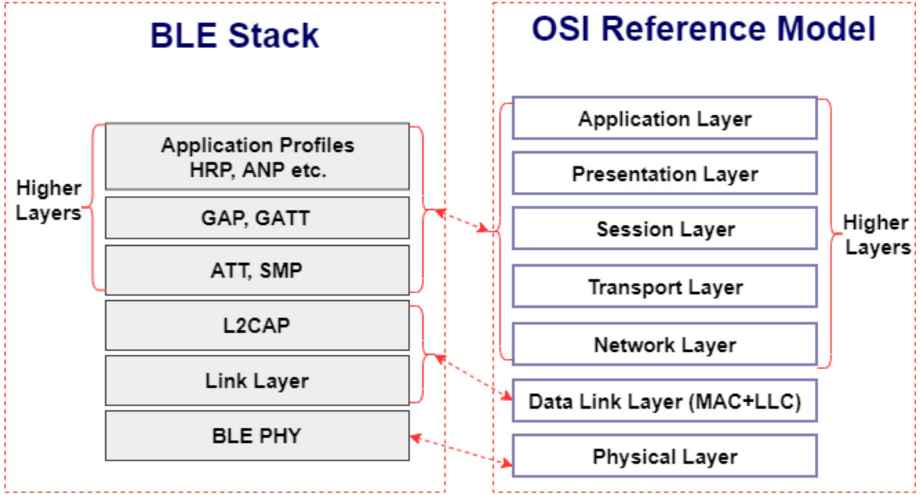


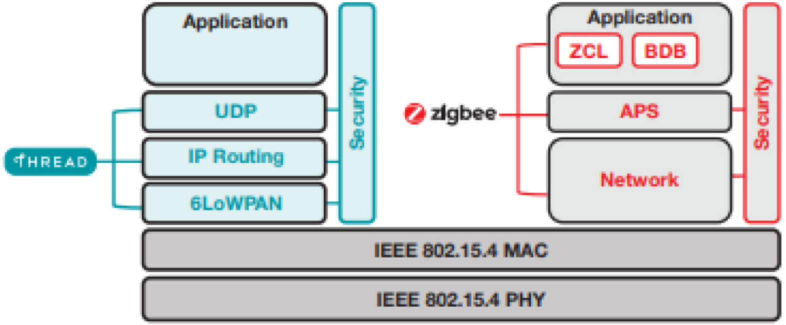
PH: Internet packet header

FH: LAN frame header

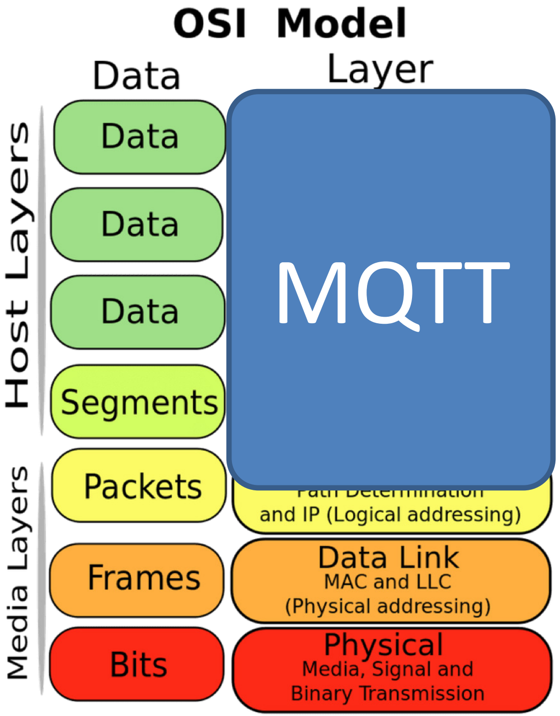
Model != reality

- 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 for IoT (joke) (kind of)



MQTT is a publish/subscribe message broker

Outline

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

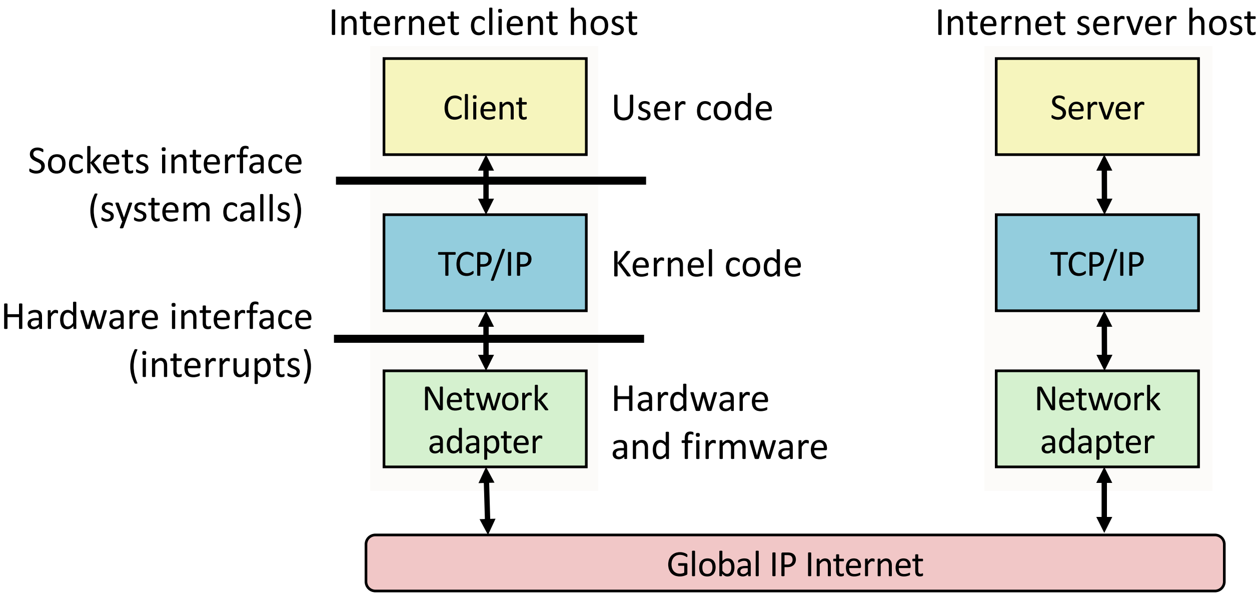
The global Internet

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

- 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**
   - 132.239.8.169

2. The set of IP addresses is mapped to a set of identifiers called Internet **domain names**
   - 132.239.8.169 is mapped to cse.ucsd.edu

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

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`**

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

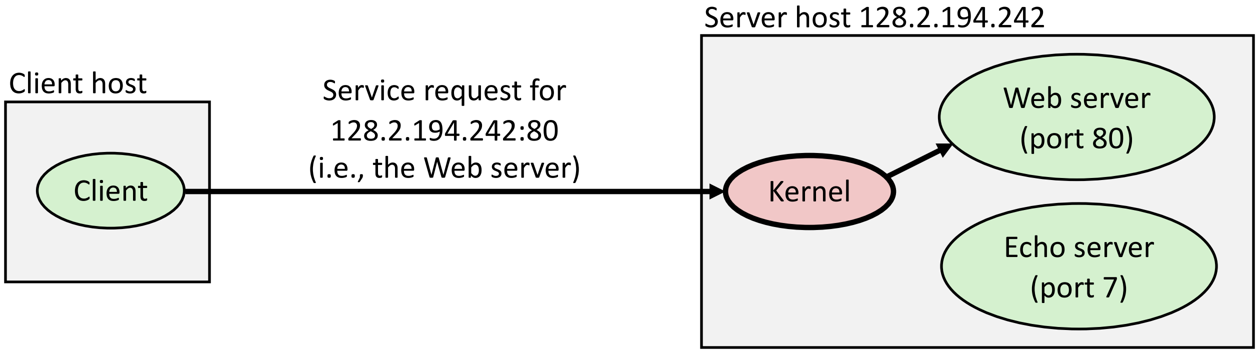
- A special name: **localhost**
  - Refers back to the computer being used (IP address 127.0.0.1)

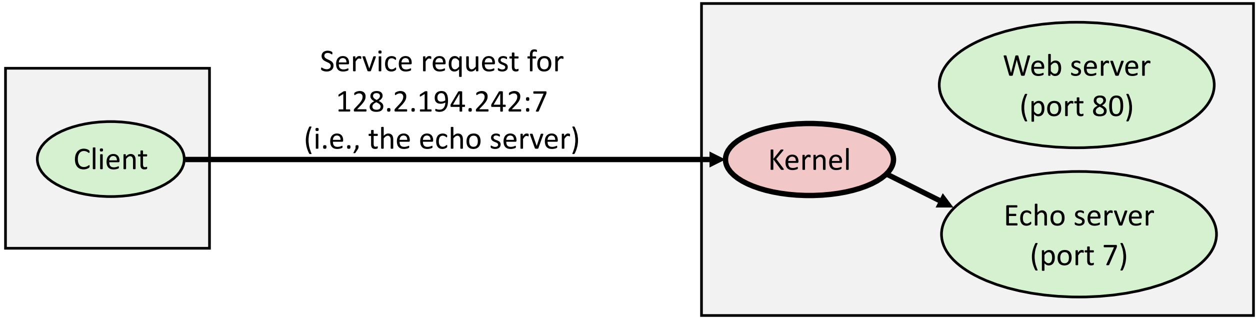
Internet connections

- 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 route packets? *(simplified...)*

- IP layer
  - – Describes the overall goal
    - Packets from my computer <---> Google
- Link layer (Ethernet)
  - – Describes individual links
    - Packets from my computer <---> EBU3 Router
- Routing
  - – Using ethernet building blocks to get packets from one host 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

Addressing

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

Addressing - *Intra*net and *Inter*net

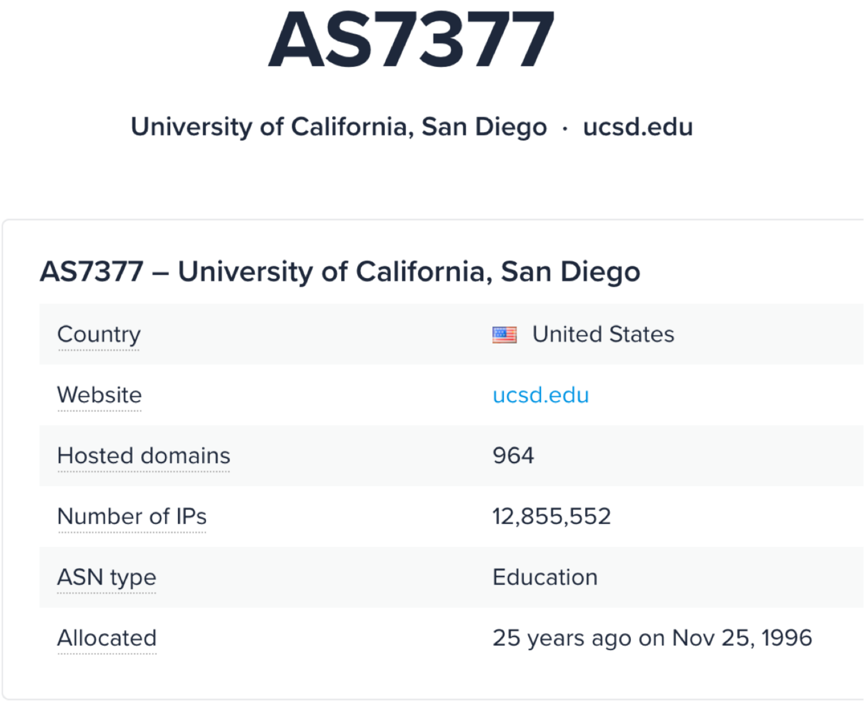
- **In general, network operators don’t change that often**
- Solution:
  - Tie IP addresses to network operators
  - Assign computers IPs as they join networks
- Key Point:
  - Networks ”own” a block of IP address space
  - ”The Internet” is a network of networks

Getting an IP from `your building's network`

- The 1st Floor EBU3 router "owns" 132.239.8.0-255
  - This is notated as 132.239.8.0/24
  - The first 24 bits "matter"
- cse.ucsd.edu "owns" 132.239.8.169
  - 132.239.8.169/32, usually omit the /32

Aside: Who owns what?

https://ipinfo.io/AS7377

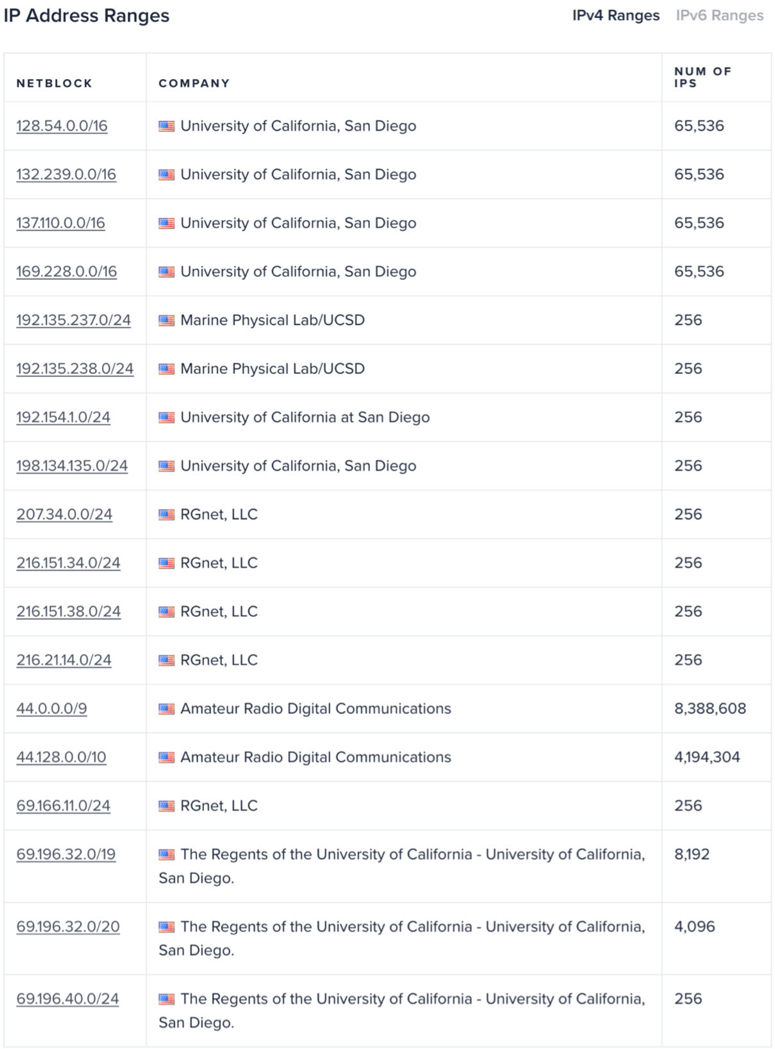


AS7377

University of California, San Diego · ucsd.edu

AS7377 – University of California, San Diego

Country	United States
Website	ucsd.edu
Hosted domains	964
Number of IPs	12,855,552
ASN type	Education
Allocated	25 years ago on Nov 25, 1996



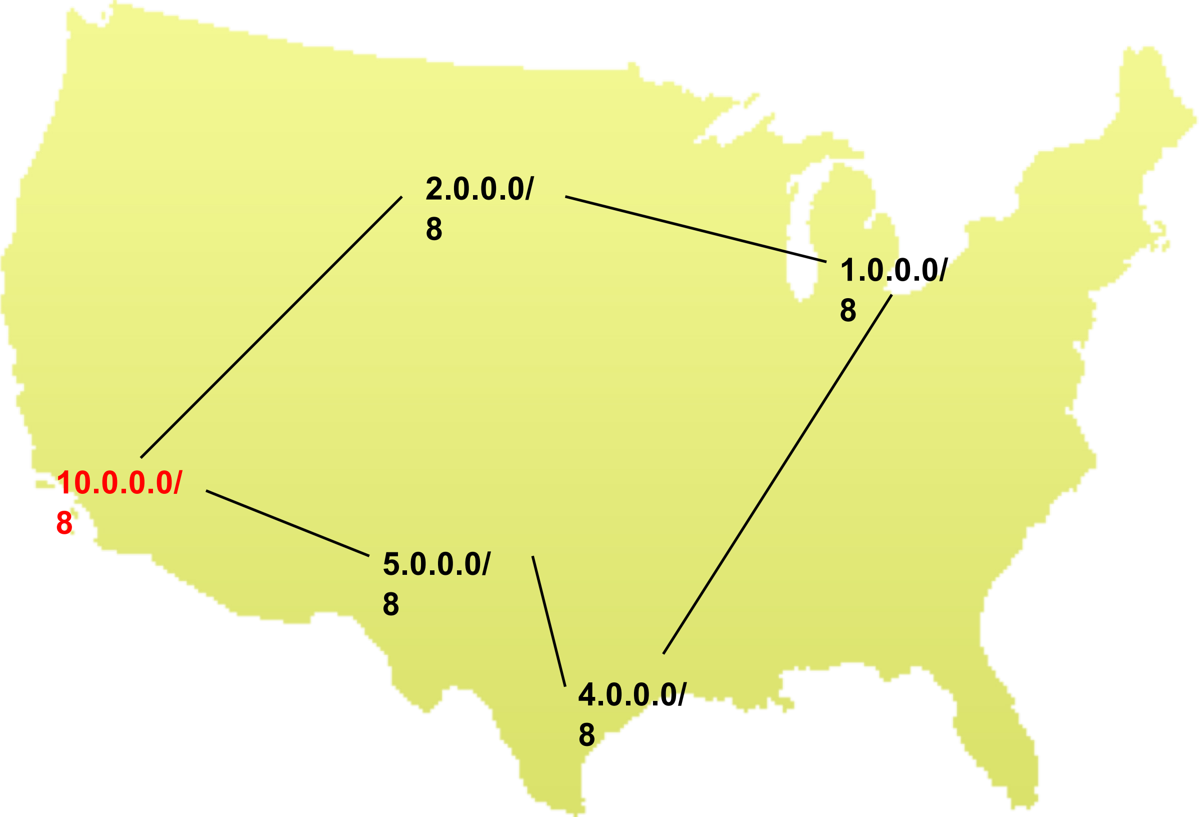
IP Address Ranges

NETBLOCK	COMPANY	NUM OF IPS
128.54.0.0/16	University of California, San Diego	65,536
132.239.0.0/16	University of California, San Diego	65,536
137.110.0.0/16	University of California, San Diego	65,536
169.228.0.0/16	University of California, San Diego	65,536
192.135.237.0/24	Marine Physical Lab/UCSD	256
192.135.238.0/24	Marine Physical Lab/UCSD	256
192.154.1.0/24	University of California at San Diego	256
198.134.135.0/24	University of California, San Diego	256
207.34.0.0/24	RGnet, LLC	256
216.151.34.0/24	RGnet, LLC	256
216.151.38.0/24	RGnet, LLC	256
216.21.14.0/24	RGnet, LLC	256
44.0.0.0/9	Amateur Radio Digital Communications	8,388,608
44.128.0.0/10	Amateur Radio Digital Communications	4,194,304
69.166.11.0/24	RGnet, LLC	256
69.196.32.0/19	The Regents of the University of California - University of California, San Diego.	8,192
69.196.32.0/20	The Regents of the University of California - University of California, San Diego.	4,096
69.196.40.0/24	The Regents of the University of California - University of California, San Diego.	256

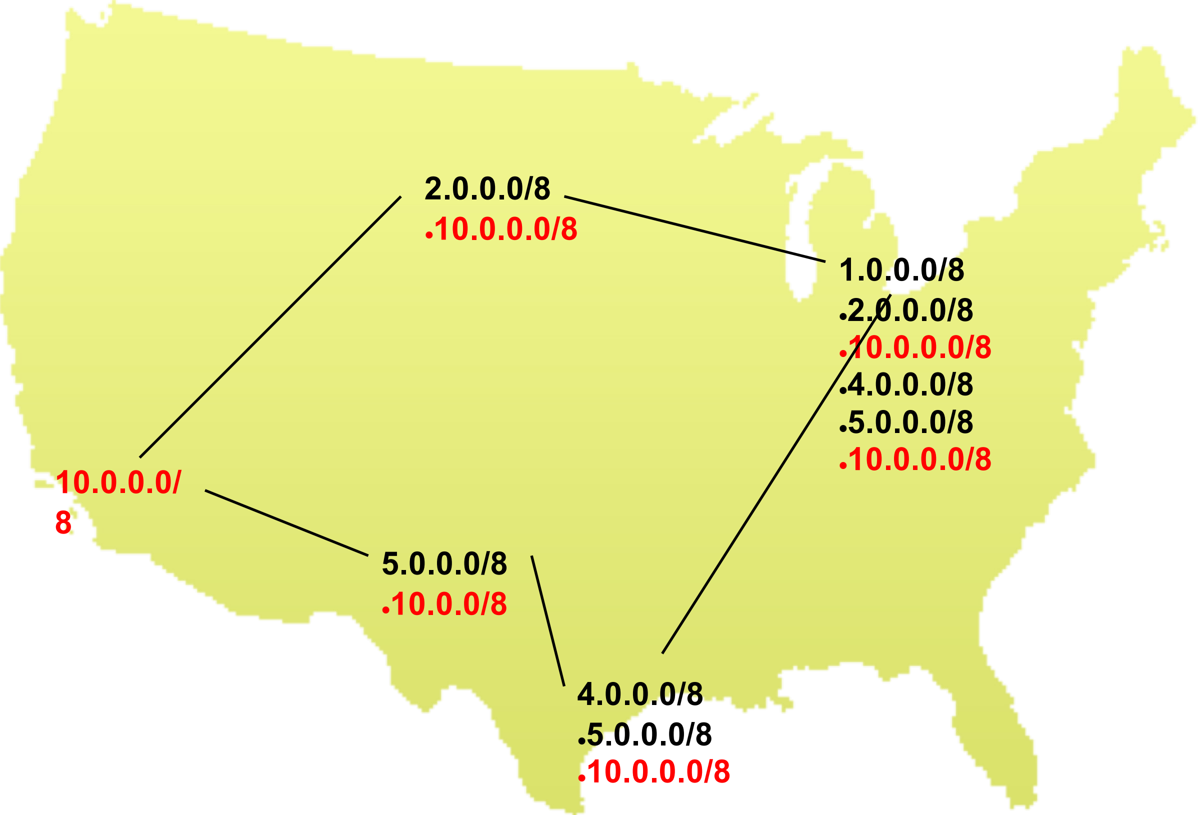
Identifying your computer?

- 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
    - [n.b. this overview ignores NATs, which are commonplace today]

Routing



Routing



2.0.0.0/8
- 10.0.0.0/8

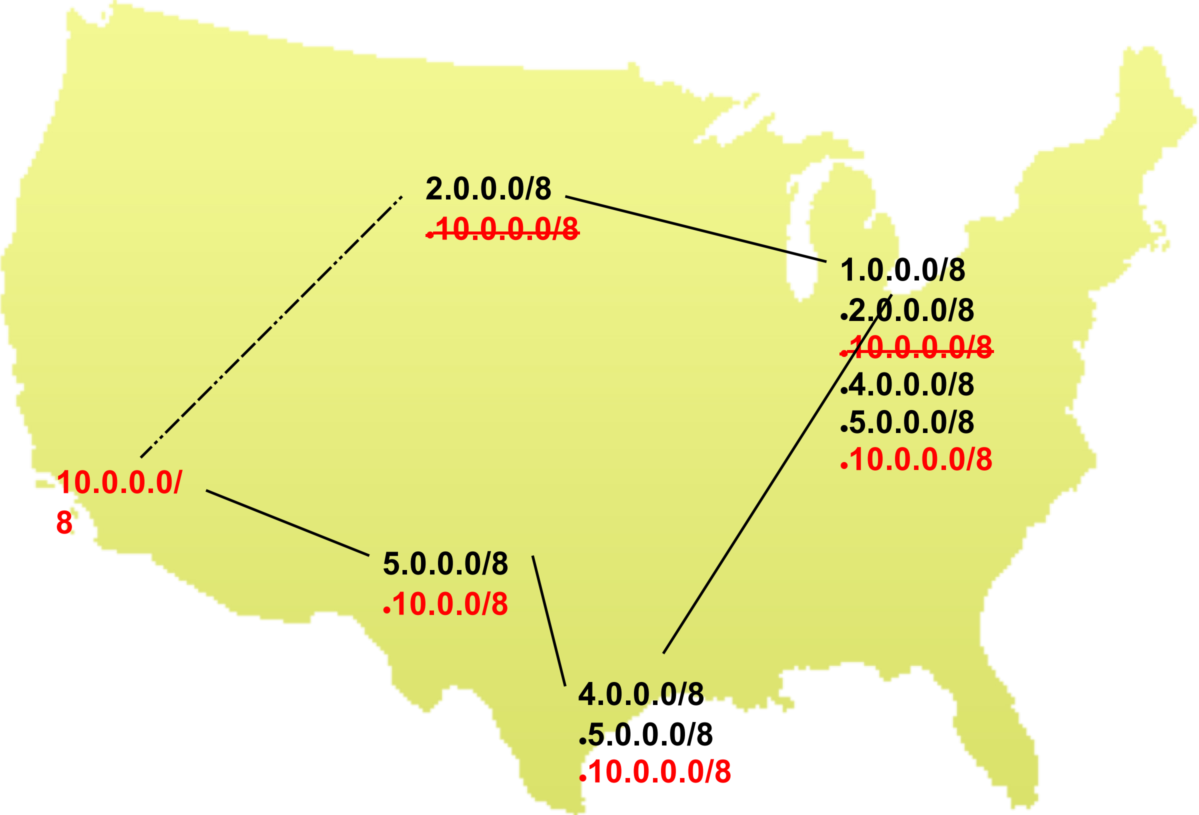
1.0.0.0/8
- 2.0.0.0/8
- 10.0.0.0/8
- 4.0.0.0/8
- 5.0.0.0/8
- 10.0.0.0/8

10.0.0.0/
8

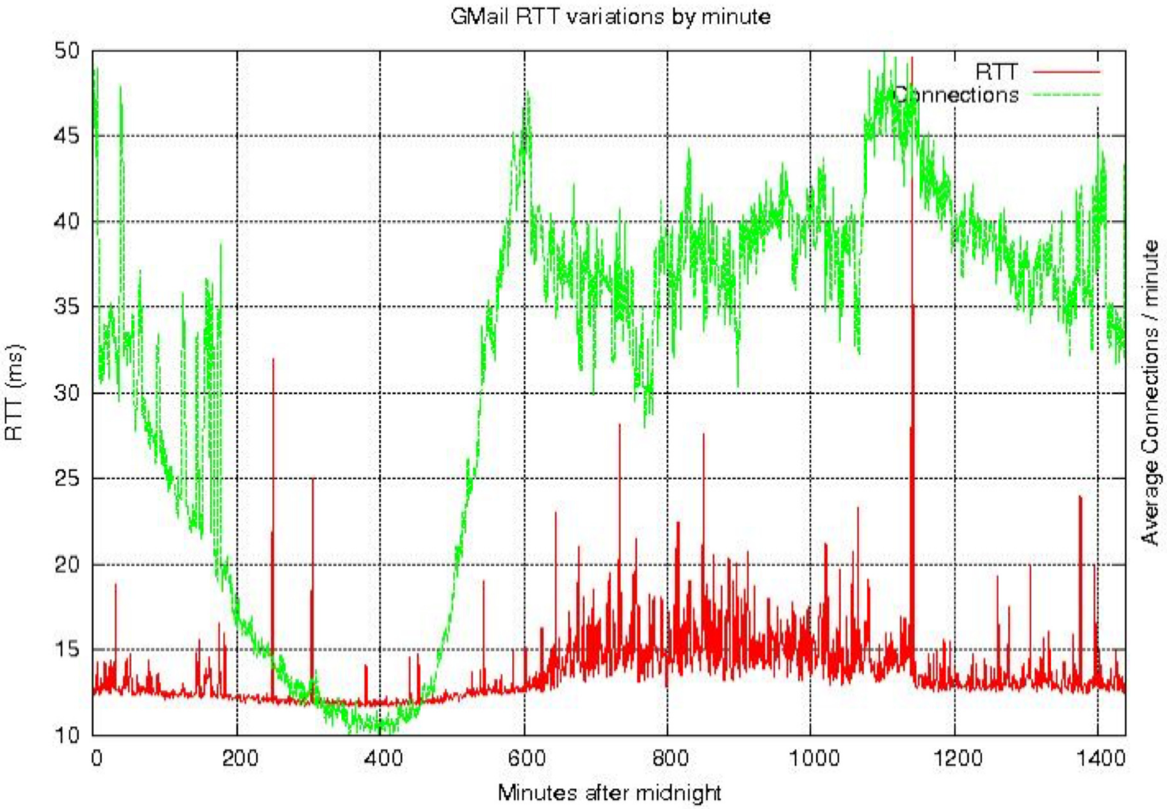
5.0.0.0/8
- 10.0.0/8

4.0.0.0/8
- 5.0.0.0/8
- 10.0.0.0/8

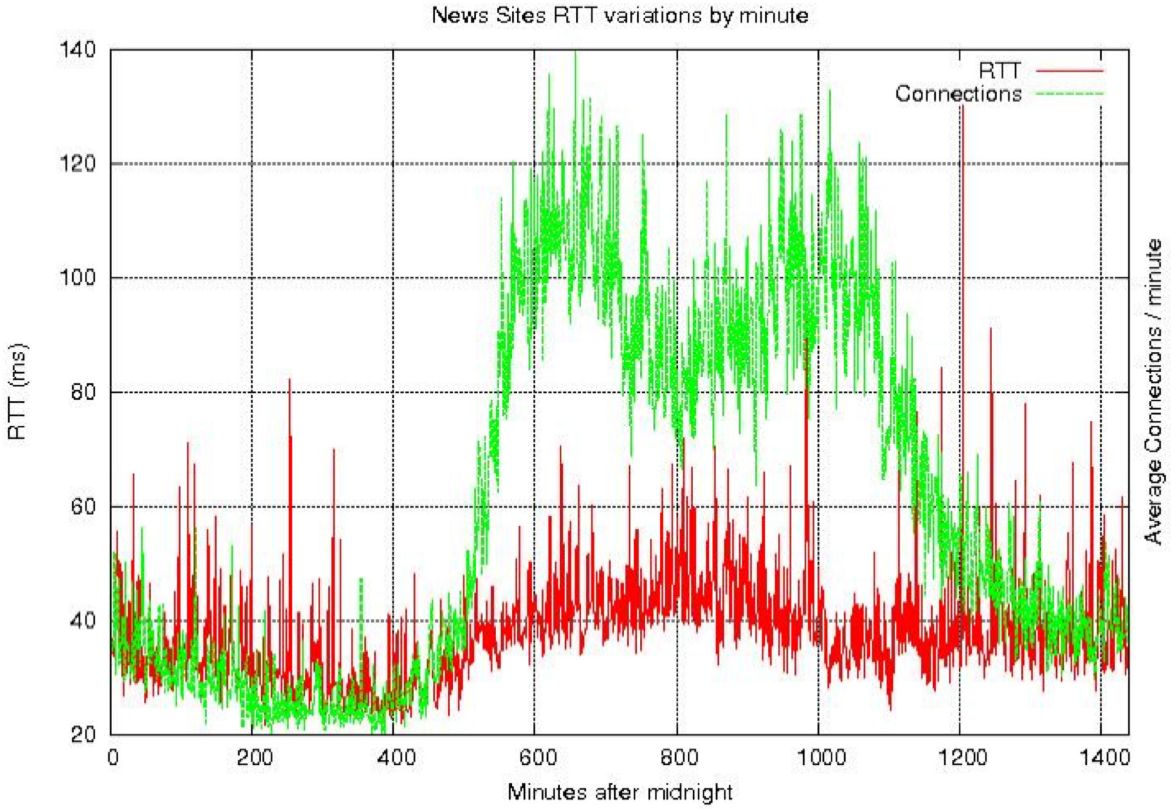
Routing – "Adaptive"



Routing – Congestion + Time



Routing – Congestion + Time



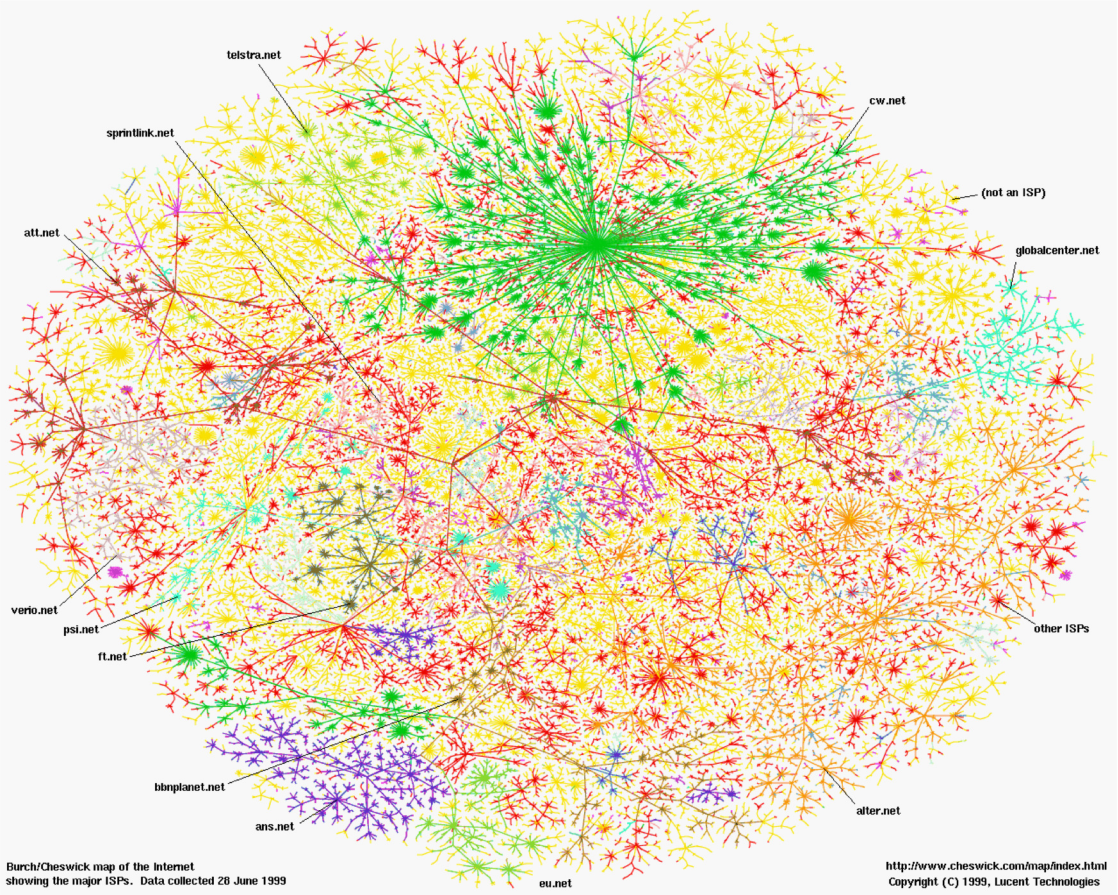
Routing – Other considerations [pre-2010, hah!]

- Most ethernet packets have a Maximum Transmission Unit (MTU) of 1500 bytes
- The fastest routers run at 10 GB/s

$$\frac{1500\, bytes/packet}{1073741824\, bytes/second} \approx 1.4\text{x}10^{-6}\, seconds/packet$$

- A 1 GHz processor can only do ~1000 instructions / packet
- Tables must fit in cache
  - Memory accesses would cost ~100 instructions each

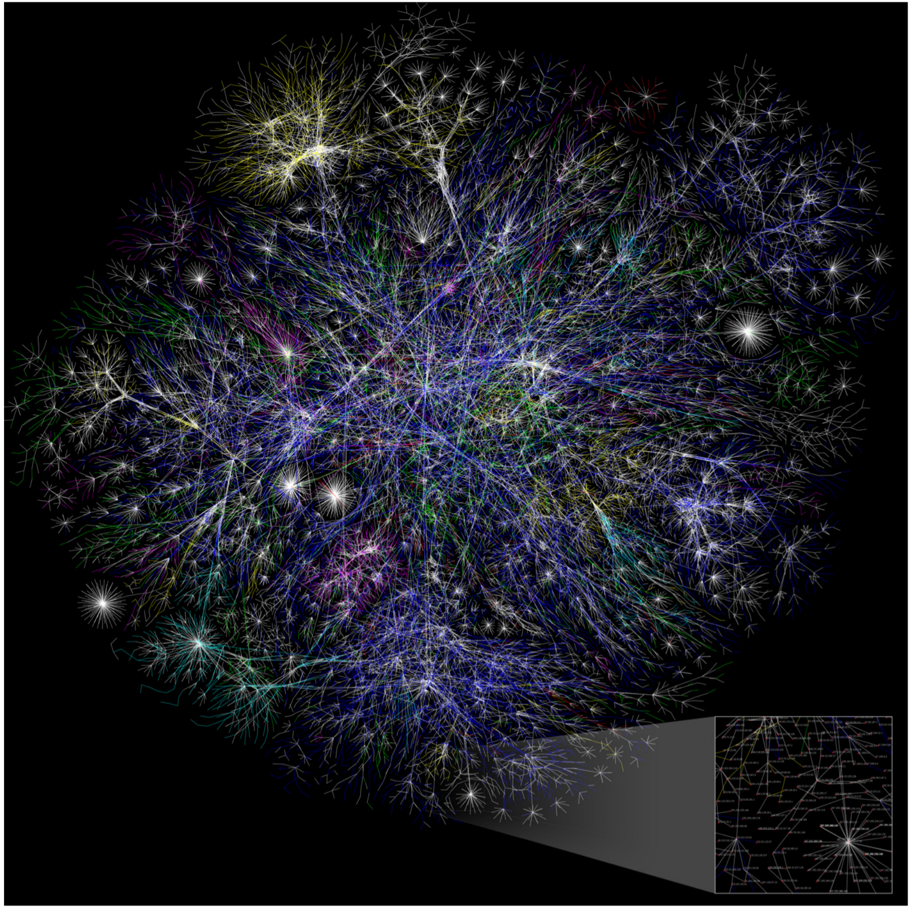
Some Perspective: North America (in June, 1999)



Burch/Cheswick map of the Internet
showing the major ISPs. Data collected 28 June 1999

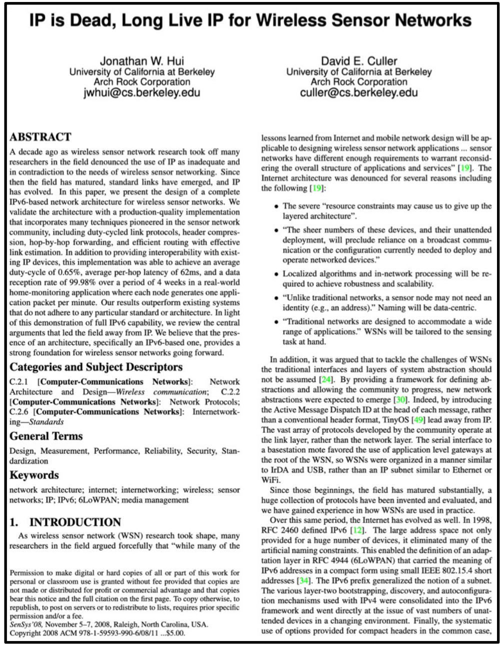
http://www.cheswick.com/map/index.html
Copyright (C) 1999, Lucent Technologies

Some Perspective: The Internet



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

A decade ago as wireless sensor network research took off many researchers in the field denounced the use of IP as inadequate and in contradiction to the needs of wireless sensor networking. Since then the field has matured, standard links have emerged, and IP has evolved. In this paper, we present the design of a complete IPv6-based network architecture for wireless sensor networks. We validate the architecture with a production-quality implementation that incorporates many techniques pioneered in the sensor network community, including duty-cycled link protocols, header compression, hop-by-hop forwarding, and efficient routing with effective link estimation. In addition to providing interoperability with existing IP devices, this implementation was able to achieve an average duty-cycle of 0.65%, average per-hop latency of 62ms, and a data reception rate of 99.98% over a period of 4 weeks in a real-world home-monitoring application where each node generates one application packet per minute. Our results outperform existing systems that do not adhere to any particular standard or architecture. In light of this demonstration of full IPv6 capability, we review the central arguments that led the field away from IP. We believe that the presence of an architecture, specifically an IPv6-based one, provides a strong foundation for wireless sensor networks going forward.

Categories and Subject Descriptors

C.2.1 [**Computer-Communications Networks**]: Network Architecture and Design—*Wireless communication*; C.2.2 [**Computer-Communications Networks**]: Network Protocols; C.2.6 [**Computer-Communications Networks**]: Internetworking—*Standards*

General Terms

Design, Measurement, Performance, Reliability, Security, Standardization

Keywords

network architecture; internet; internetworking; wireless; sensor networks; IP; IPv6; 6LoWPAN; media management

1. INTRODUCTION

As wireless sensor network (WSN) research took shape, many researchers in the field argued forcefully that “while many of the lessons learned from Internet and mobile network design will be applicable to designing wireless sensor network applications ... sensor networks have different enough requirements to warrant reconsidering the overall structure of applications and services” [19]. The Internet architecture was denounced for several reasons including the following [19]:

- The severe “resource constraints may cause us to give up the layered architecture”.
- “The sheer numbers of these devices, and their unattended deployment, will preclude reliance on a broadcast communication or the configuration currently needed to deploy and operate networked devices.”
- Localized algorithms and in-network processing will be required to achieve robustness and scalability.
- “Unlike traditional networks, a sensor node may not need an identity (e.g., an address).” Naming will be data-centric.
- “Traditional networks are designed to accommodate a wide range of applications.” WSNs will be tailored to the sensing task at hand.

In addition, it was argued that to tackle the challenges of WSNs the traditional interfaces and layers of system abstraction should not be assumed [24]. By providing a framework for defining abstractions and allowing the community to progress, new network abstractions were expected to emerge [30]. Indeed, by introducing the Active Message Dispatch ID at the head of each message, rather than a conventional header format, TinyOS [49] lead away from IP. The vast array of protocols developed by the community operate at the link layer, rather than the network layer. The serial interface to a basestation mote favored the use of application level gateways at the root of the WSN, so WSNs were organized in a manner similar to IrDA and USB, rather than an IP subnet similar to Ethernet or WiFi.

Since those beginnings, the field has matured substantially, a huge collection of protocols have been invented and evaluated, and we have gained experience in how WSNs are used in practice.

Over this same period, the Internet has evolved as well. In 1998, RFC 2460 defined IPv6 [12]. The large address space not only provided for a huge number of devices, it eliminated many of the artificial naming constraints. This enabled the definition of an adaptation layer in RFC 4944 (6LoWPAN) that carried the meaning of IPv6 addresses in a compact form using small IEEE 802.15.4 short addresses [34]. The IPv6 prefix generalized the notion of a subnet. The various layer-two bootstrapping, discovery, and autoconfiguration mechanisms used with IPv4 were consolidated into the IPv6 framework and went directly at the issue of vast numbers of unattended devices in a changing environment. Finally, the systematic use of options provided for compact headers in the common case,

SenSys'08, November 5–7, 2008, Raleigh, North Carolina, USA.
Copyright 2008 ACM 978-1-59593-990-6/08/11 ...$5.00.

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

Lab 1: How does *your* Internet work?

- What can you learn about the network around you?
- Play with Wireshark
- Protocol analysis, introspection

Outline

- OSI Layers
- ”The Upper Layers”
- **Physical Layer**
- Data Link Layer

Physical Layer

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

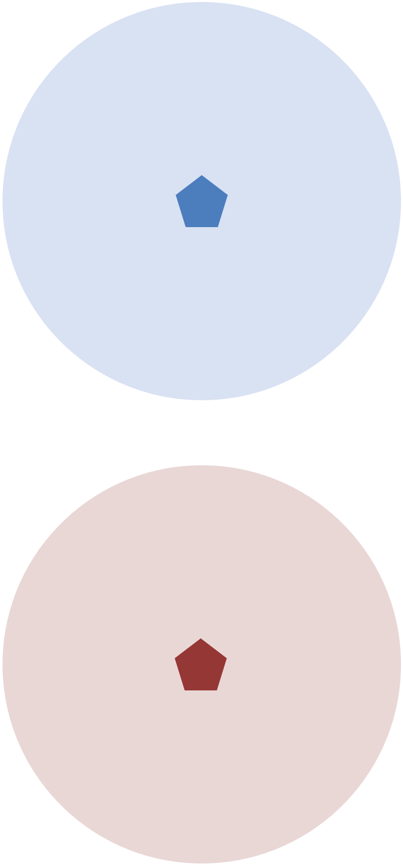
- Important considerations
  - Signal strength
  - Modulation
  - Frequency

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

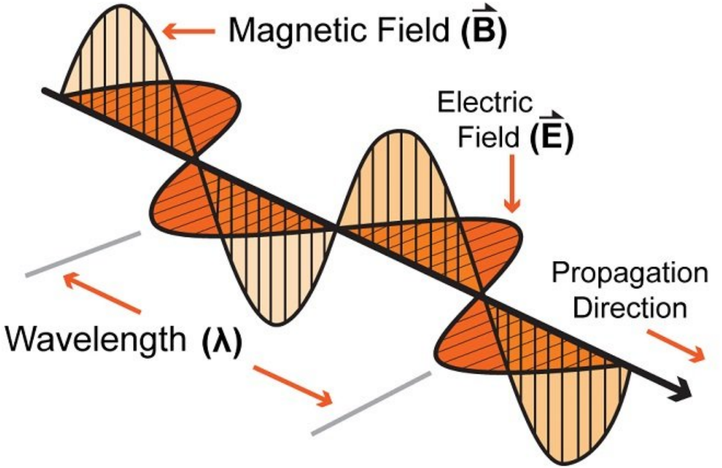


Signal qualities

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

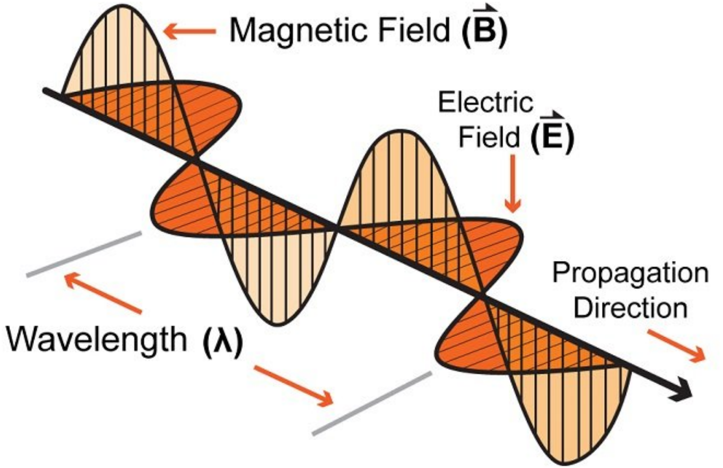


Signal qualities

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)

- Rules of thumb: +3 dB is double the power, 10 dB is 10x power

Signal strength varies significantly across technologies

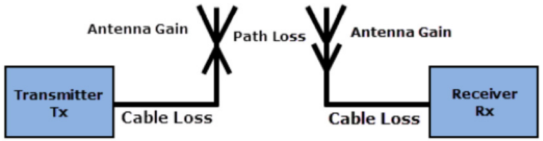
- Bluetooth Low Energy (local area)
  - nRF52840 transmit power: 8 dBm (6.31 mW)
  - nRF52840 receive sensitivity: -95 dBm (316.2 fW)

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

Propagation degrades RF signals

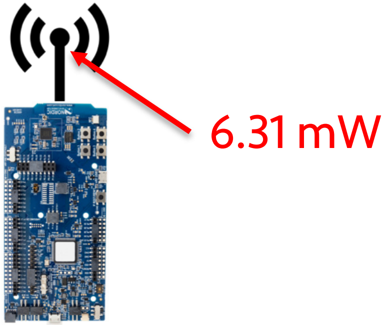
- Attenuation in free space
  - Signals get weaker as they travel over long distances
  - Signal spreads out → free space path loss

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



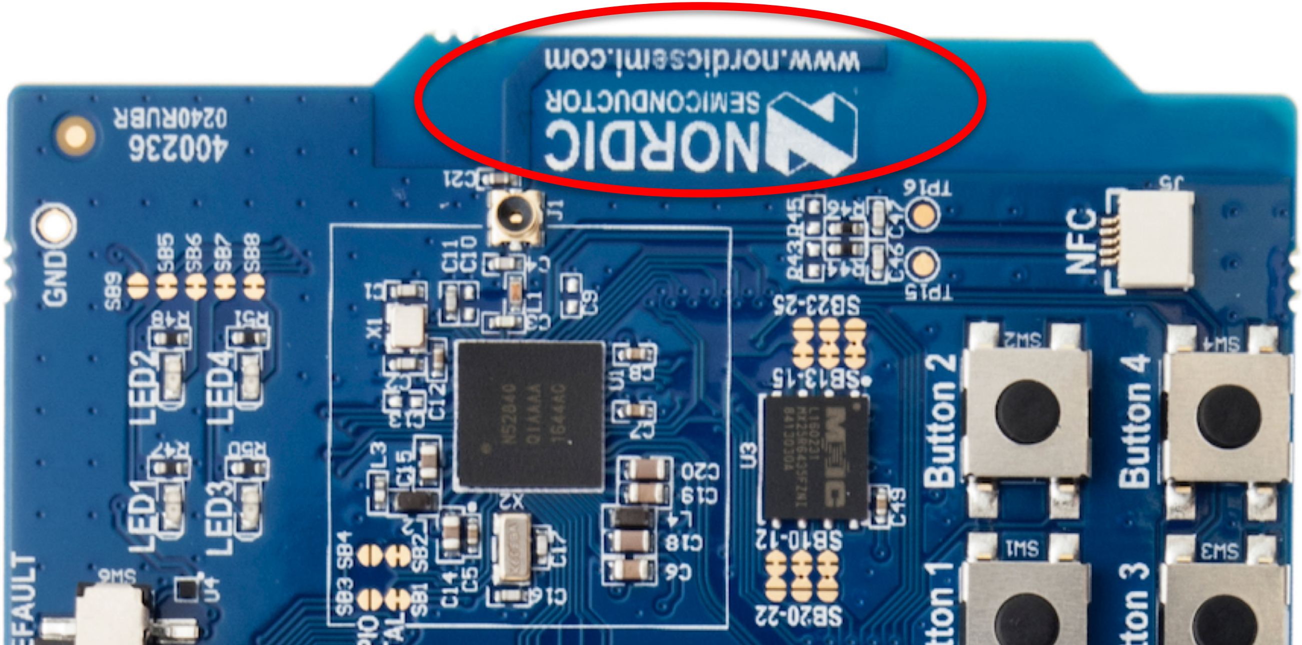
Some Intuitions for Signal Propagation, Power, Gain, etc

- 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)



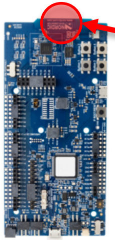
Wait, 📡 is not an antenna

- 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.

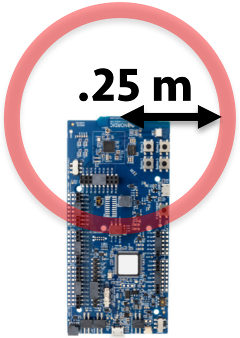
- We will use the nrf52840 in lab:
  - Max BLE transmit power for nRF52840: 8 dBm (6.31 mW)
  - Min BLE receive sensitivity for nRF52840: -95 dBm (316.2 fW)



6.31 mW

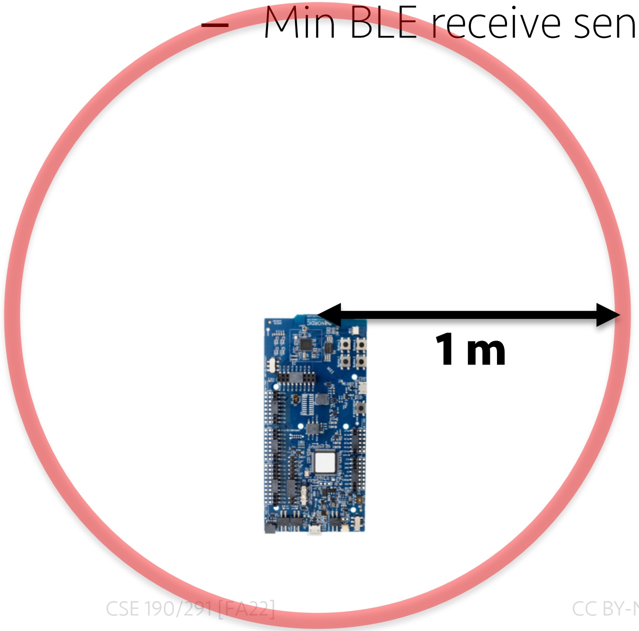
Some Intuitions for Signal Propagation, Power, Gain, etc.

- 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)



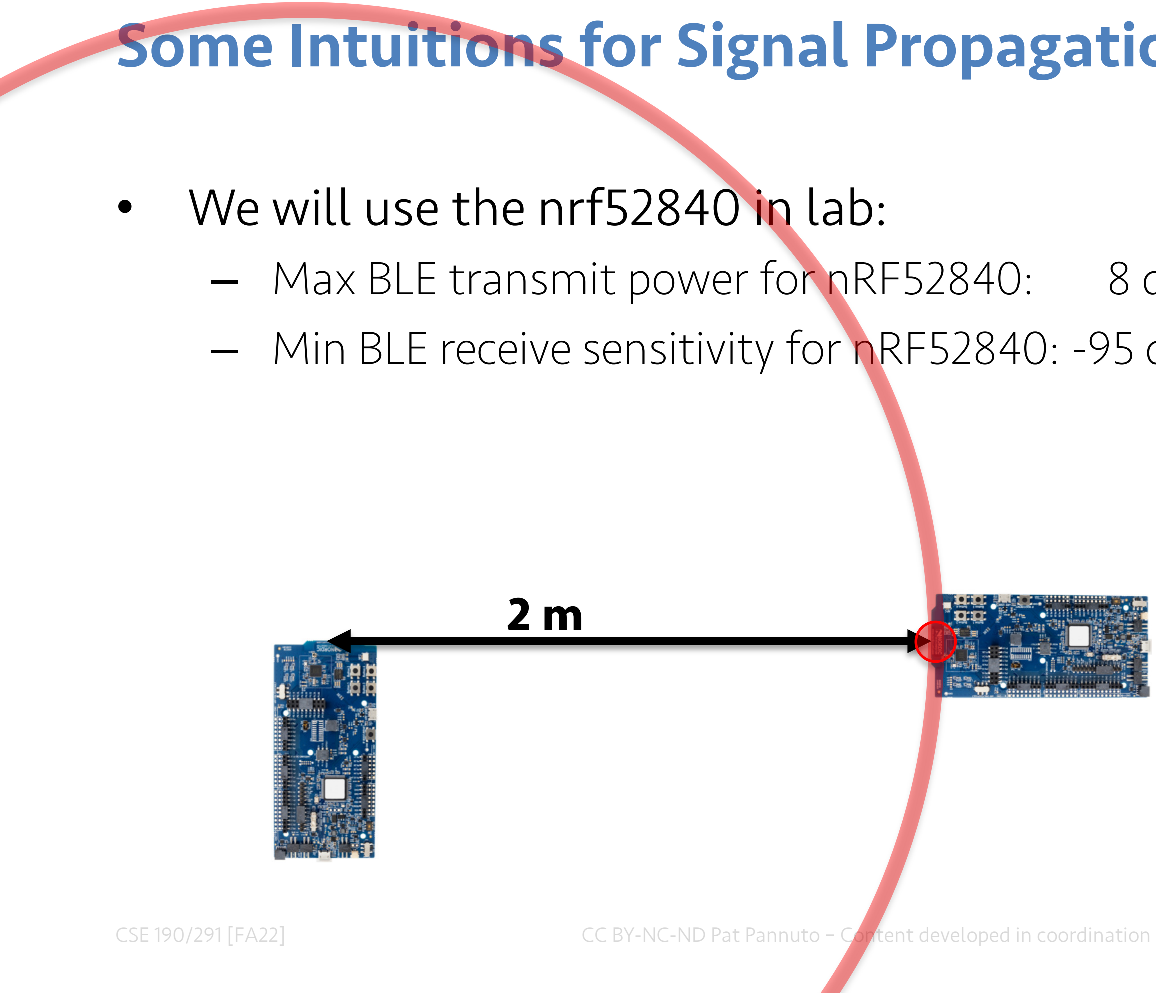
Some Intuitions for Signal Propagation, Power, Gain, etc.

- 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)



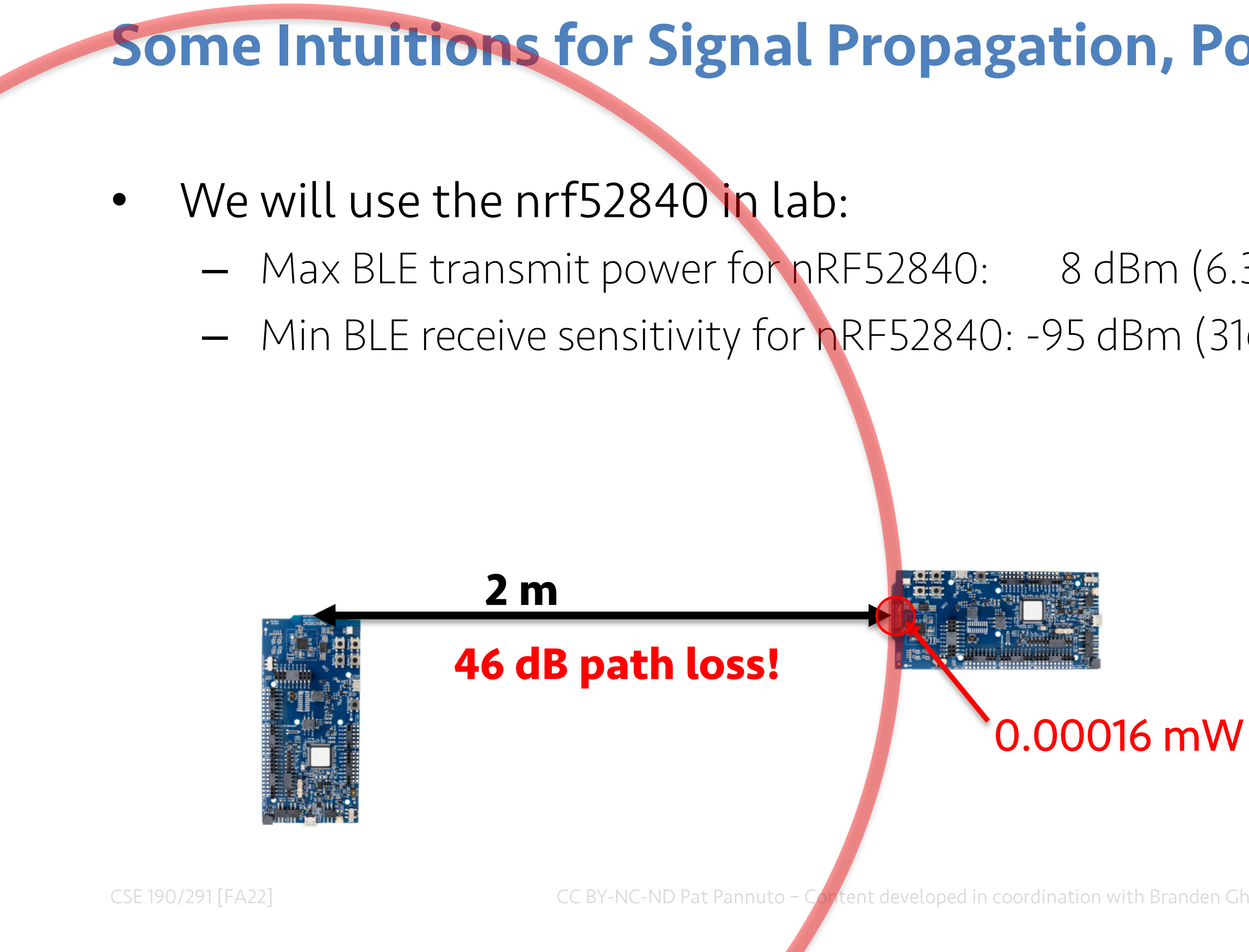
Some Intuitions for Signal Propagation, Power, Gain, etc.

- 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)



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

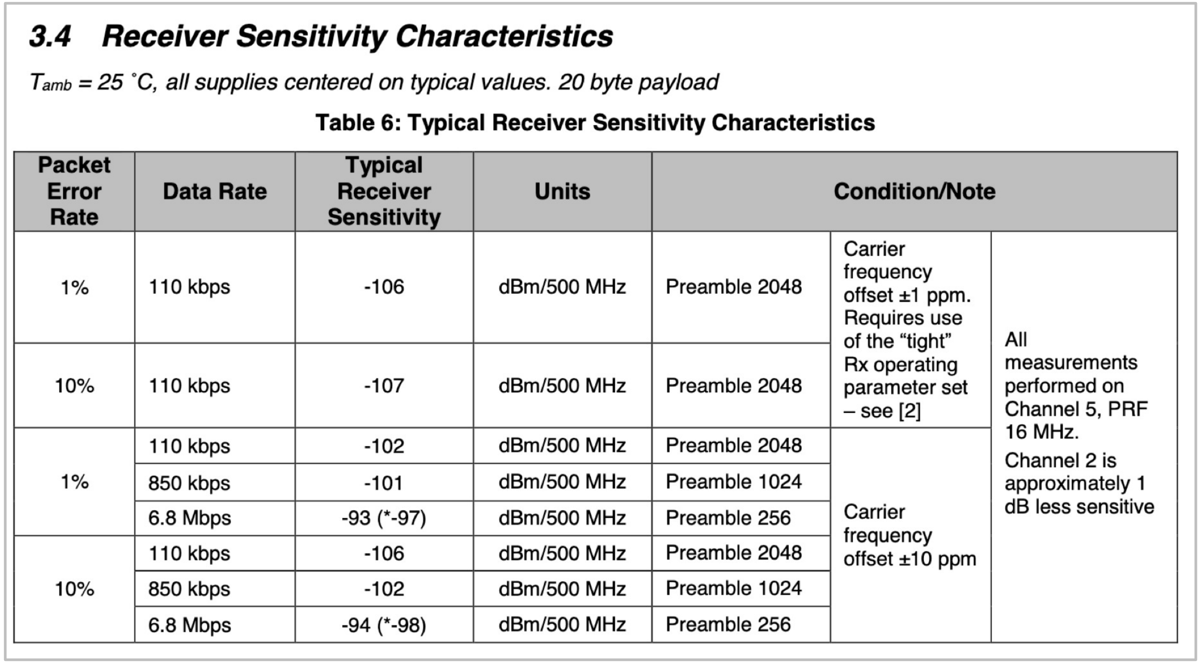
- Attenuation in free space
  - Signals get weaker as they travel over long distances
  - Signal spreads out → free space path loss

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

- Many other factors (e.g. physical obstacles, interference, reflections,…)
  - Precise *quantitative* details are in the EE domain
  - We will use quantitative 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]



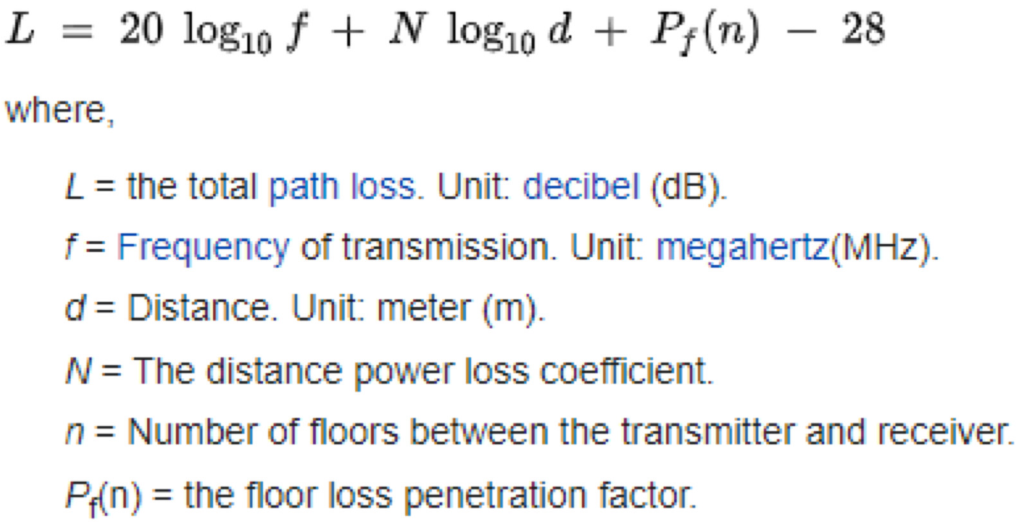
3.4 Receiver Sensitivity Characteristics

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.

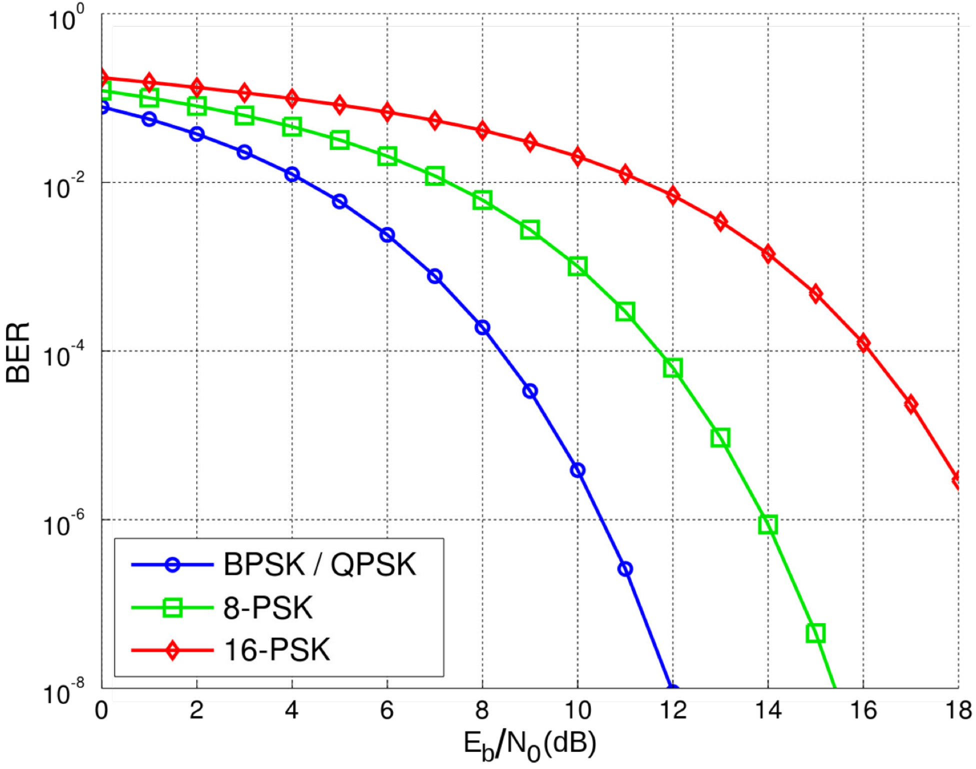
$P_f(n)$ = the floor loss penetration factor.

- Models like this are ~~more trustworthy~~ less bad than FSPL
  - 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

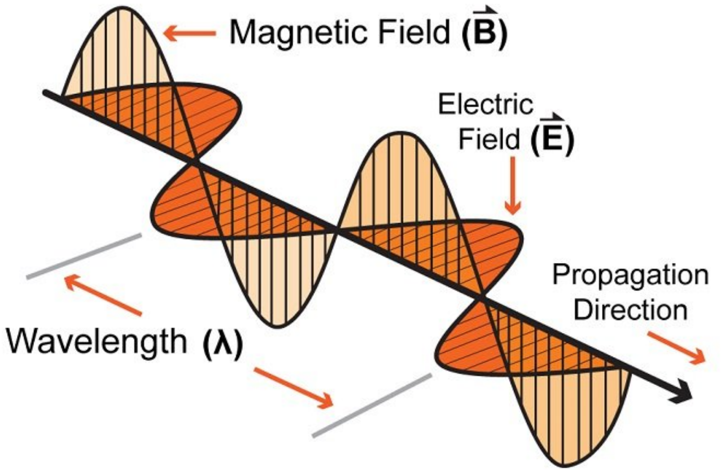
Odds that a transmitted bit will be received incorrectly

Signal qualities

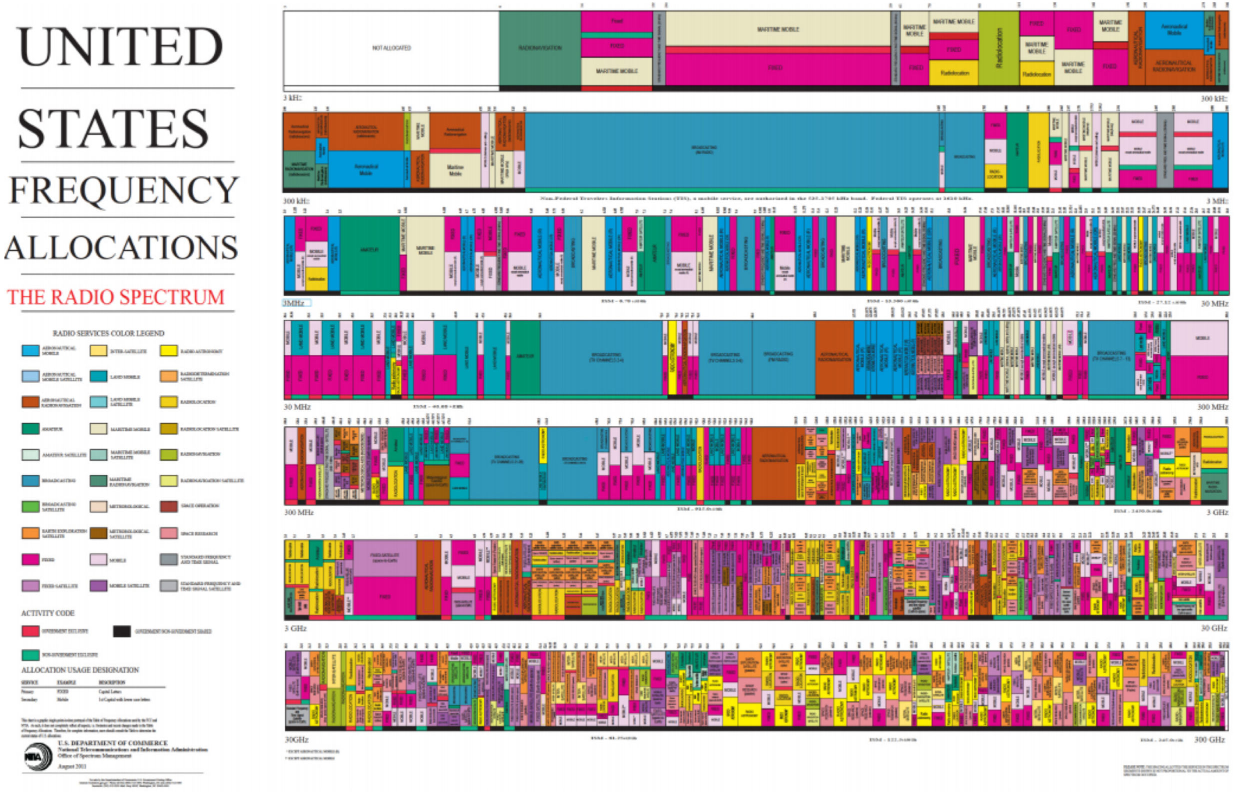
1. Signal strength
   - The amount of energy transmitted/received

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

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

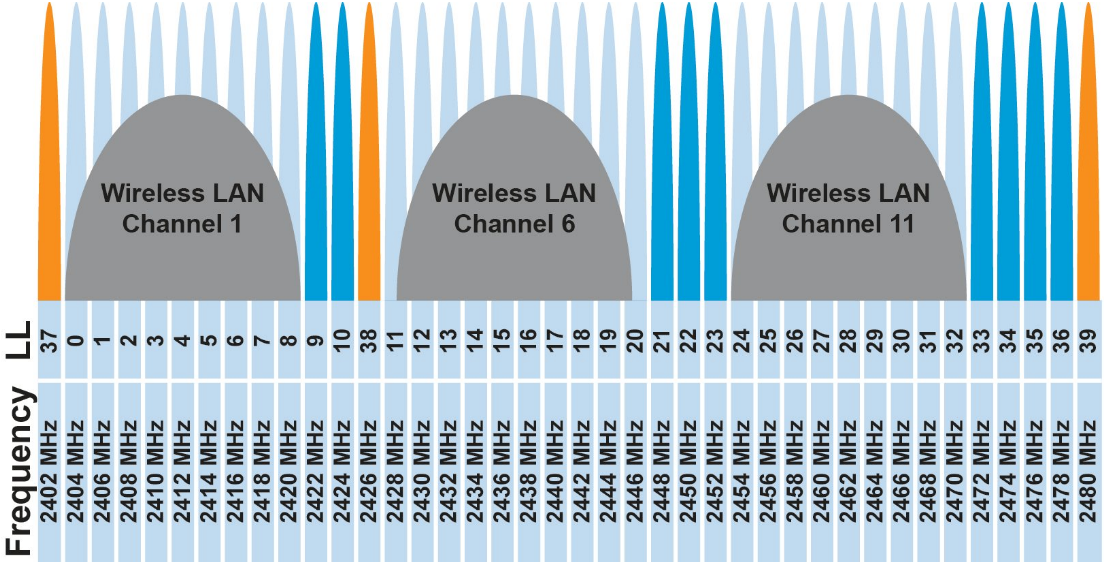


Frequency separation enables different wireless technologies to operate in operation



Unlicensed bands are where the IoT thrives

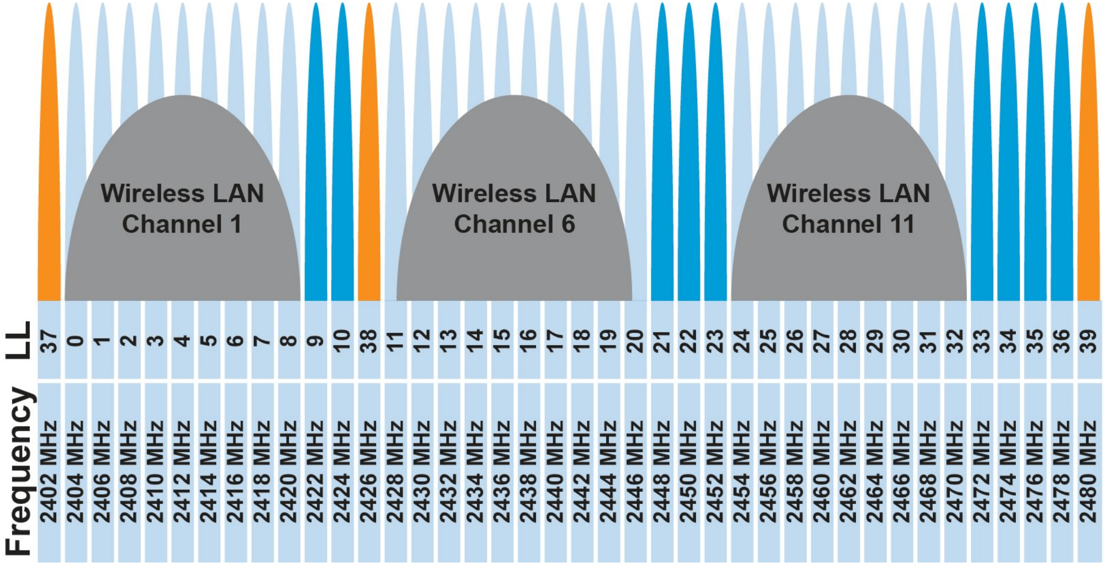
- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi
- Cellular uses licensed bands at great cost
  - Why?



LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

Unlicensed bands are where the IoT thrives

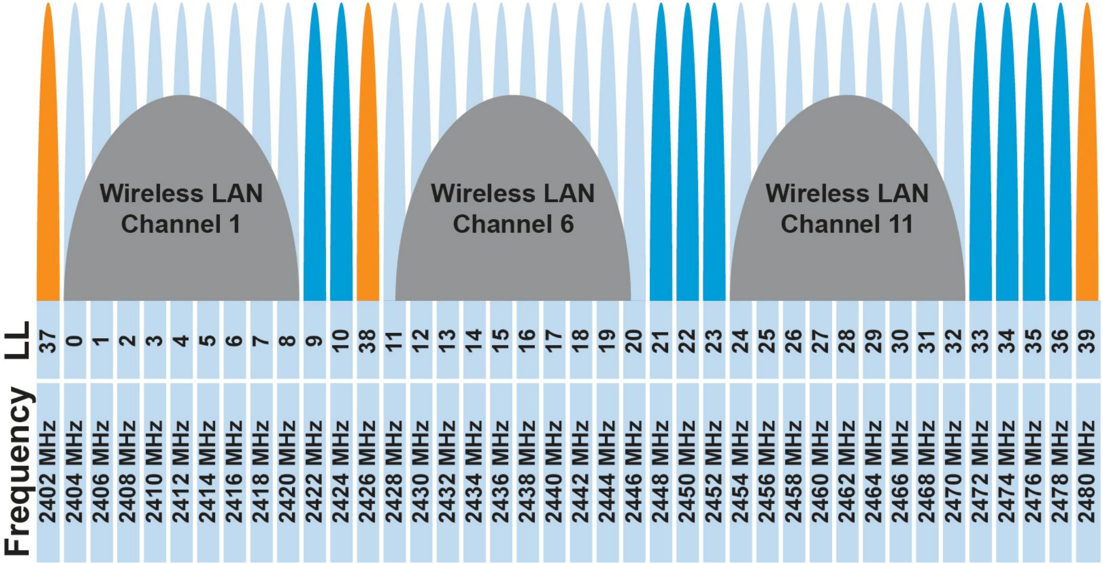
- 902 MHz – 928 MHz
  - LPWANs
- 2.4 GHz to 2.5 GHz
  - WiFi, BLE, Thread
- 5 GHz
  - Faster WiFi



LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

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

Different technologies use spectrum in different ways

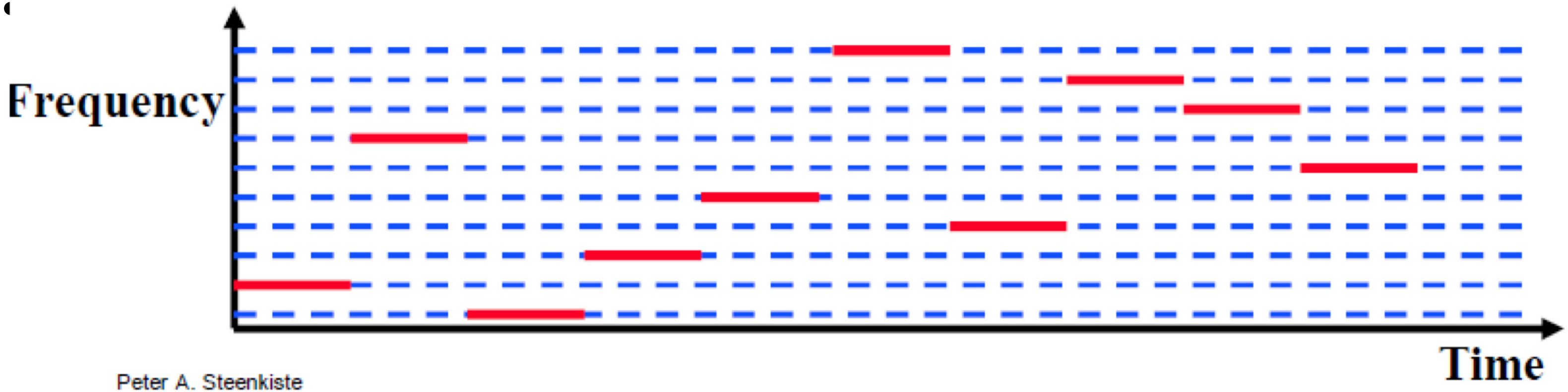


LL	37	0	1	2	3	4	5	6	7	8	9	10	38	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	39
Frequency	2402 MHz	2404 MHz	2406 MHz	2408 MHz	2410 MHz	2412 MHz	2414 MHz	2416 MHz	2418 MHz	2420 MHz	2422 MHz	2424 MHz	2426 MHz	2428 MHz	2430 MHz	2432 MHz	2434 MHz	2436 MHz	2438 MHz	2440 MHz	2442 MHz	2444 MHz	2446 MHz	2448 MHz	2450 MHz	2452 MHz	2454 MHz	2456 MHz	2458 MHz	2460 MHz	2462 MHz	2464 MHz	2466 MHz	2468 MHz	2470 MHz	2472 MHz	2474 MHz	2476 MHz	2478 MHz	2480 MHz

- How spectrum is used affects: cost ($, e−), 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

One Example / Bluetooth Preview: Frequency Hopping Spread Spectrum (FHSS)

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



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

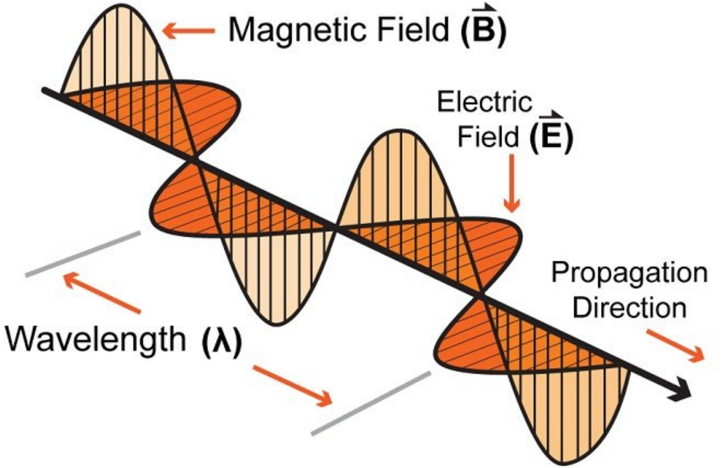
- https://en.wikipedia.org/wiki/Hedy_Lamarr#Inventor

Signal qualities

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

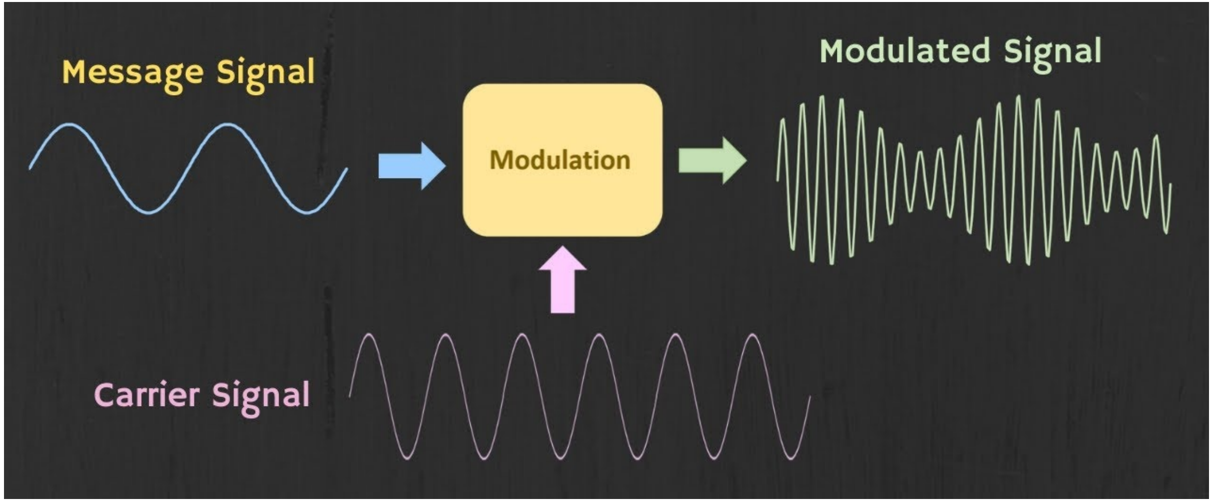
2. Signal frequency and bandwidth
   - Which "channel" the signal is sent on

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


Magnetic Field ($\vec{\mathbf{B}}$)
Electric Field ($\vec{\mathbf{E}}$)
Propagation Direction
Wavelength (λ)

Modulation

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

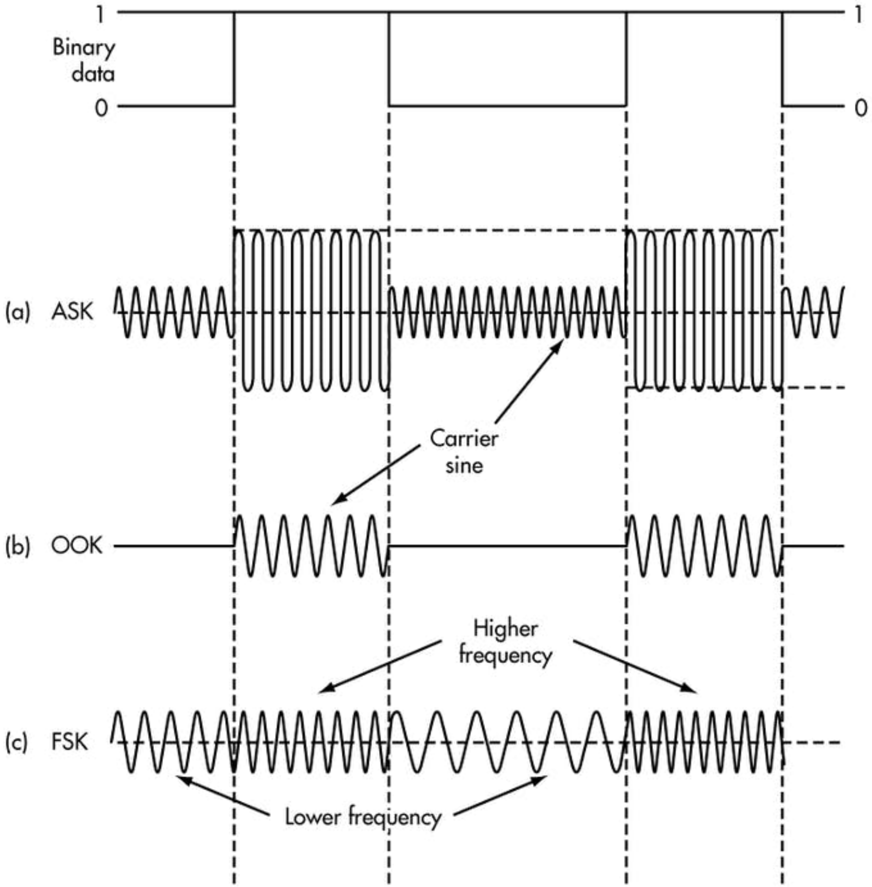


Modulation types

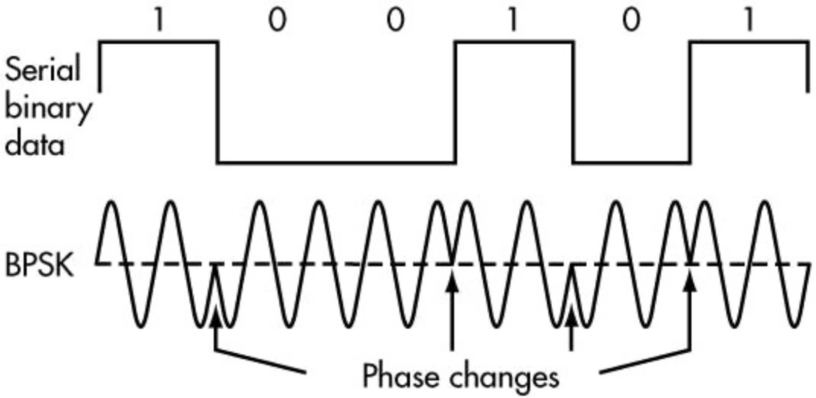
- Encoding binary data on a signal

- 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

Outline

- OSI Layers
- ”The Upper Layers”
- Physical Layer
- **Data Link Layer**

Data Link Layer

- Framing
  - Combine arbitrary bits into a “packet” of data

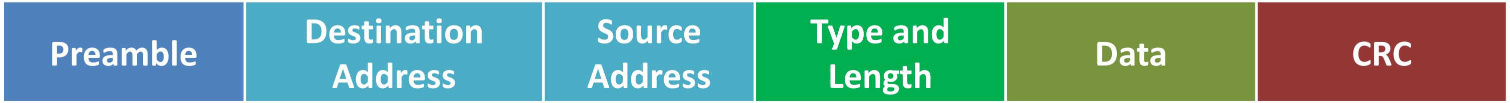
- Logical link control
  - Manage transfer between transmitter and receiver
  - Error detection and correction

- 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”

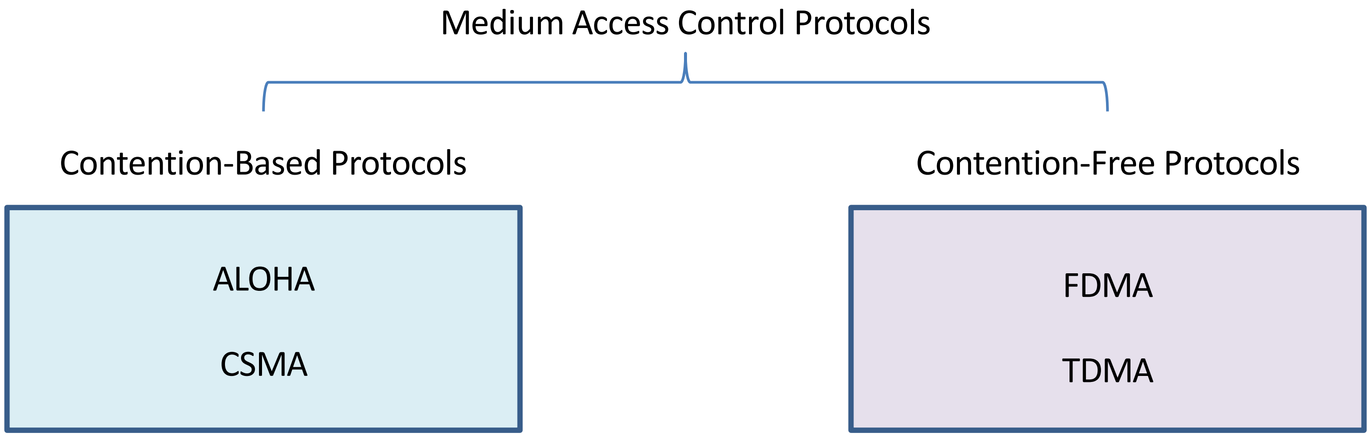
Analogy: wireless medium as acoustic

- 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

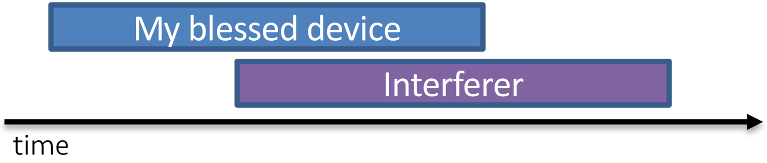
- Rules

  1. If you have data to send, send it

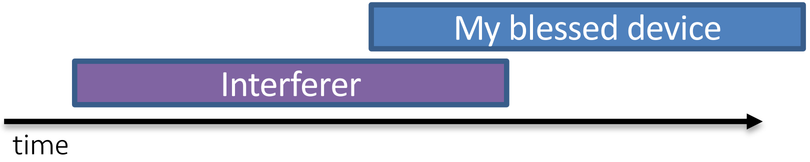
- Two (or more) simultaneous transmissions will collide and be lost
  - Wait a duration of time for an acknowledgement
  - If transmission was lost, try sending again "later"
    - Want some kind of exponential backoff scheme with entropy here

Packet collisions

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

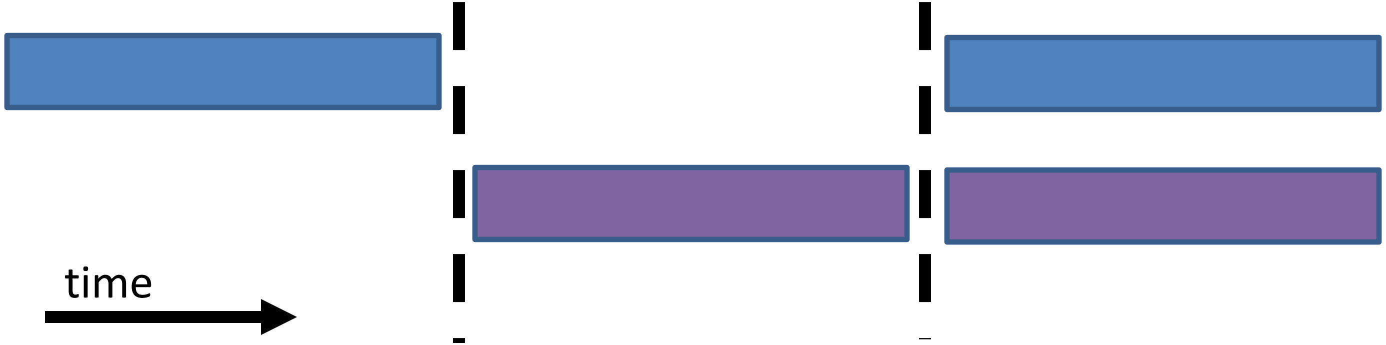


  - Transmissions before packet can also be bad



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

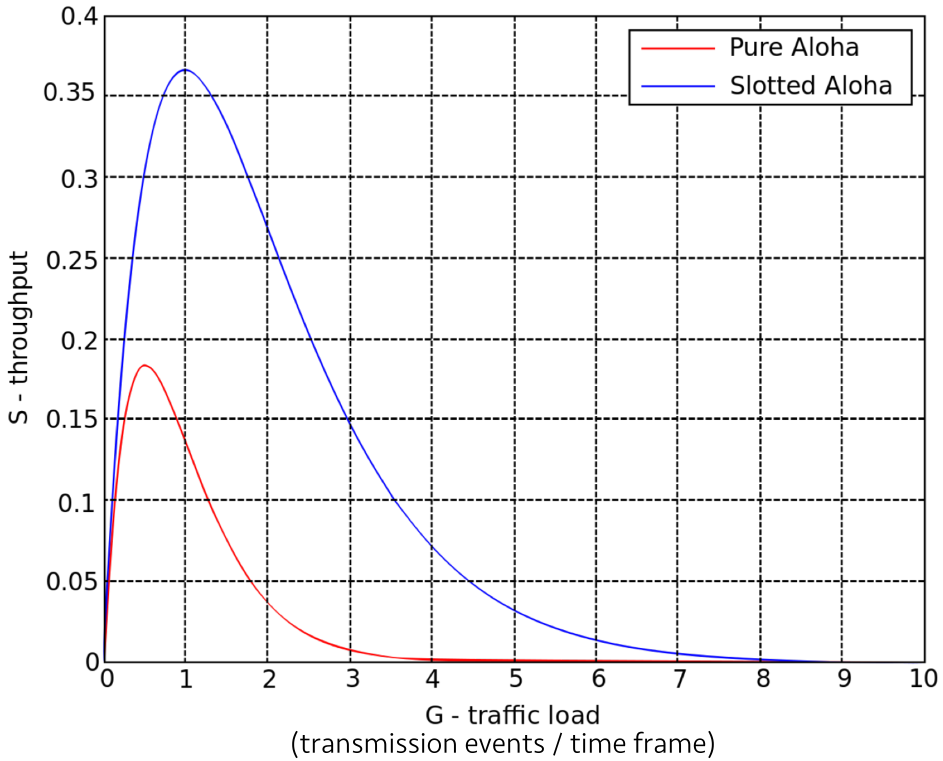


ALOHA throughput

- It can be shown that traffic maxes out at
  - ALOHA: 18.4%
  - Slotted ALOHA: 36.8%

- Assuming Poisson distribution of transmission attempts

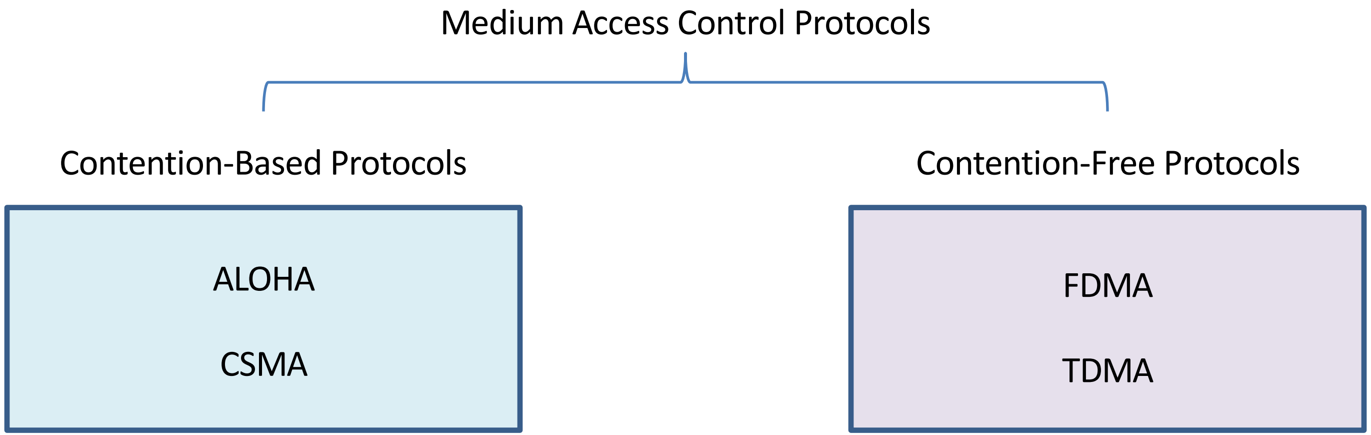
- Slotted throughput is double because the “before” collisions can no longer occur



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

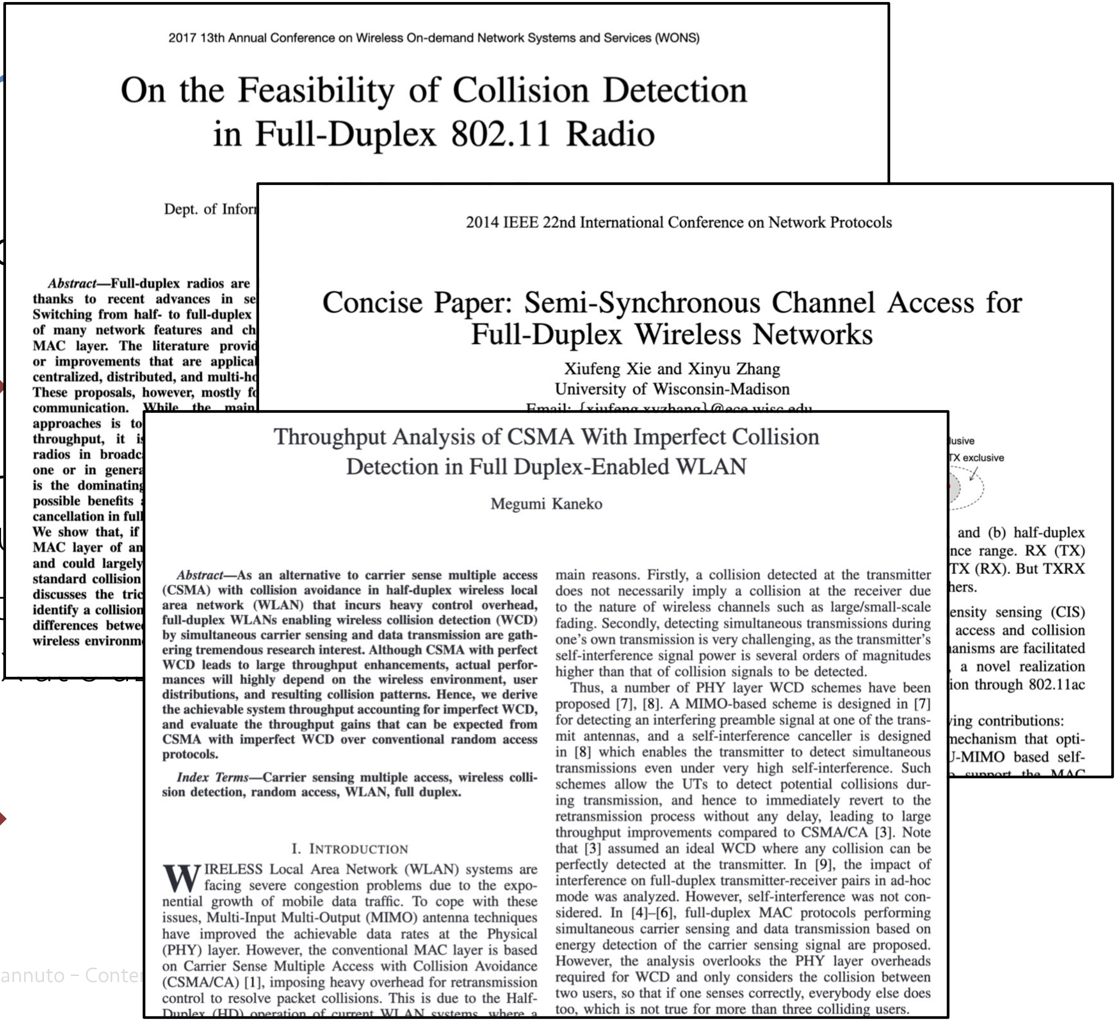
- First listen for a duration and determine if anyone is transmitting
  - If idle, you can transmit
  - If busy, wait and try again later

- “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

- Detect collisions during yo
  - Works great on wired me
- Somewhere between chal
  - Transmit and receive are u
  - Receiving while transmitt
    - Remember: nRF52840 TX at 0 d



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

Dept. of Infor

Abstract—Full-duplex radios are
thanks to recent advances in se
Switching from half- to full-duplex
of many network features and ch
MAC layer. The literature provid
or improvements that are applica
centralized, distributed, and multi-ho
These proposals, however, mostly fo
communication. While the main
approaches is to
throughput, it is
radios in broadc
one or in genera
is the dominating
possible benefits
cancellation in full
We show that, if
MAC layer of an
and could largely
standard collision
discusses the tric
identify a collision
differences betwe
wireless environm

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

and (b) half-duplex
nce range. RX (TX)
TX (RX). But TXRX
hers.

ensity sensing (CIS)
access and collision
anisms are facilitated
, a novel realization
ion through 802.11ac

ing contributions:
mechanism that opti-
U-MIMO based self-
support the MAC

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

Megumi Kaneko

Abstract—As an alternative to carrier sense multiple access (CSMA) with collision avoidance in half-duplex wireless local area network (WLAN) that incurs heavy control overhead, full-duplex WLANs enabling wireless collision detection (WCD) by simultaneous carrier sensing and data transmission are gathering tremendous research interest. Although CSMA with perfect WCD leads to large throughput enhancements, actual performances will highly depend on the wireless environment, user distributions, and resulting collision patterns. Hence, we derive the achievable system throughput accounting for imperfect WCD, and evaluate the throughput gains that can be expected from CSMA with imperfect WCD over conventional random access protocols.

Index Terms—Carrier sensing multiple access, wireless collision detection, random access, WLAN, full duplex.

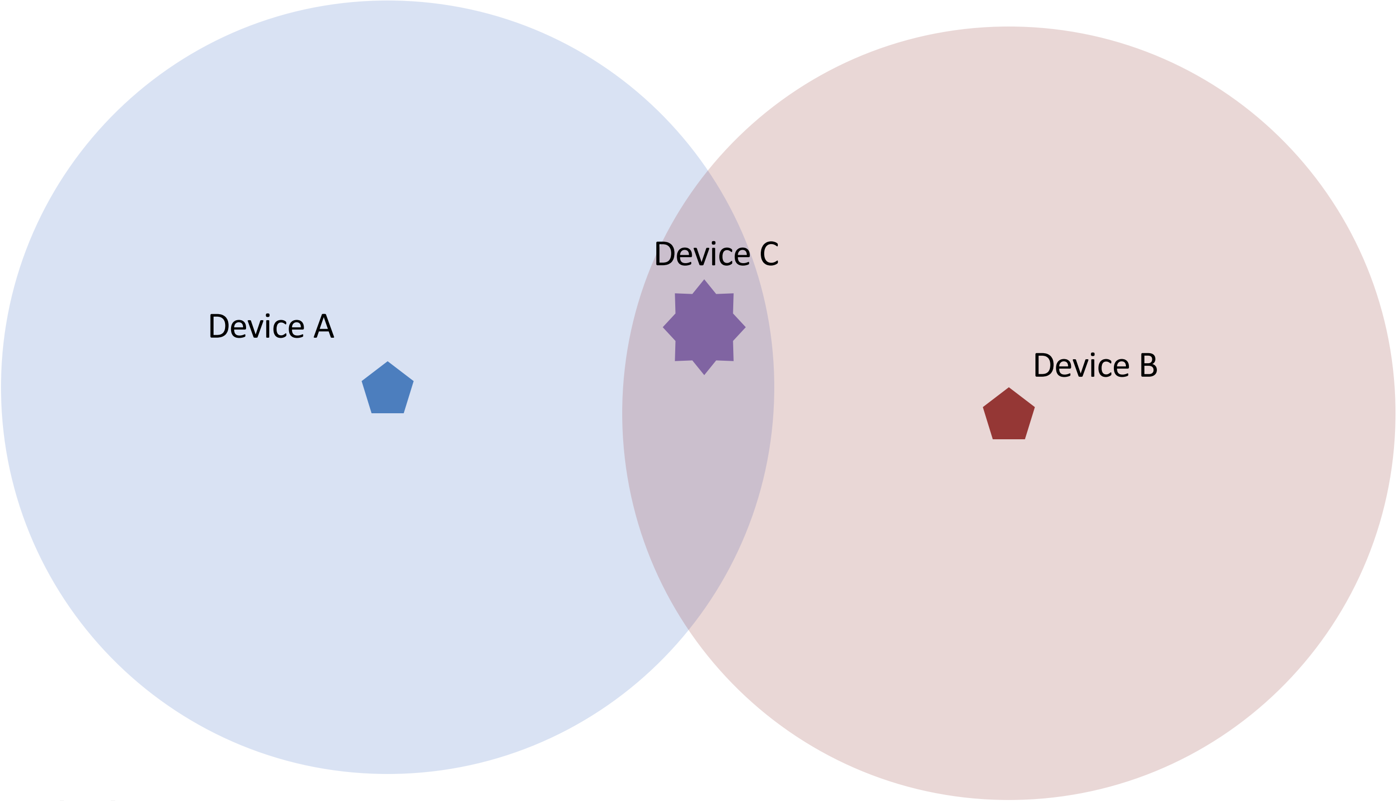
I. Introduction

WIRELESS Local Area Network (WLAN) systems are facing severe congestion problems due to the exponential growth of mobile data traffic. To cope with these issues, Multi-Input Multi-Output (MIMO) antenna techniques have improved the achievable data rates at the Physical (PHY) layer. However, the conventional MAC layer is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [1], imposing heavy overhead for retransmission control to resolve packet collisions. This is due to the Half-Duplex (HD) operation of current WLAN systems, where a

main reasons. Firstly, a collision detected at the transmitter does not necessarily imply a collision at the receiver due to the nature of wireless channels such as large/small-scale fading. Secondly, detecting simultaneous transmissions during one's own transmission is very challenging, as the transmitter's self-interference signal power is several orders of magnitudes higher than that of collision signals to be detected.

Thus, a number of PHY layer WCD schemes have been proposed [7], [8]. A MIMO-based scheme is designed in [7] for detecting an interfering preamble signal at one of the transmit antennas, and a self-interference canceller is designed in [8] which enables the transmitter to detect simultaneous transmissions even under very high self-interference. Such schemes allow the UTs to detect potential collisions during transmission, and hence to immediately revert to the retransmission process without any delay, leading to large throughput improvements compared to CSMA/CA [3]. Note that [3] assumed an ideal WCD where any collision can be perfectly detected at the transmitter. In [9], the impact of interference on full-duplex transmitter-receiver pairs in ad-hoc mode was analyzed. However, self-interference was not considered. In [4]–[6], full-duplex MAC protocols performing simultaneous carrier sensing and data transmission based on energy detection of the carrier sensing signal are proposed. However, the analysis overlooks the PHY layer overheads required for WCD and only considers the collision between two users, so that if one senses correctly, everybody else does too, which is not true for more than three colliding users.

Hidden terminal problem

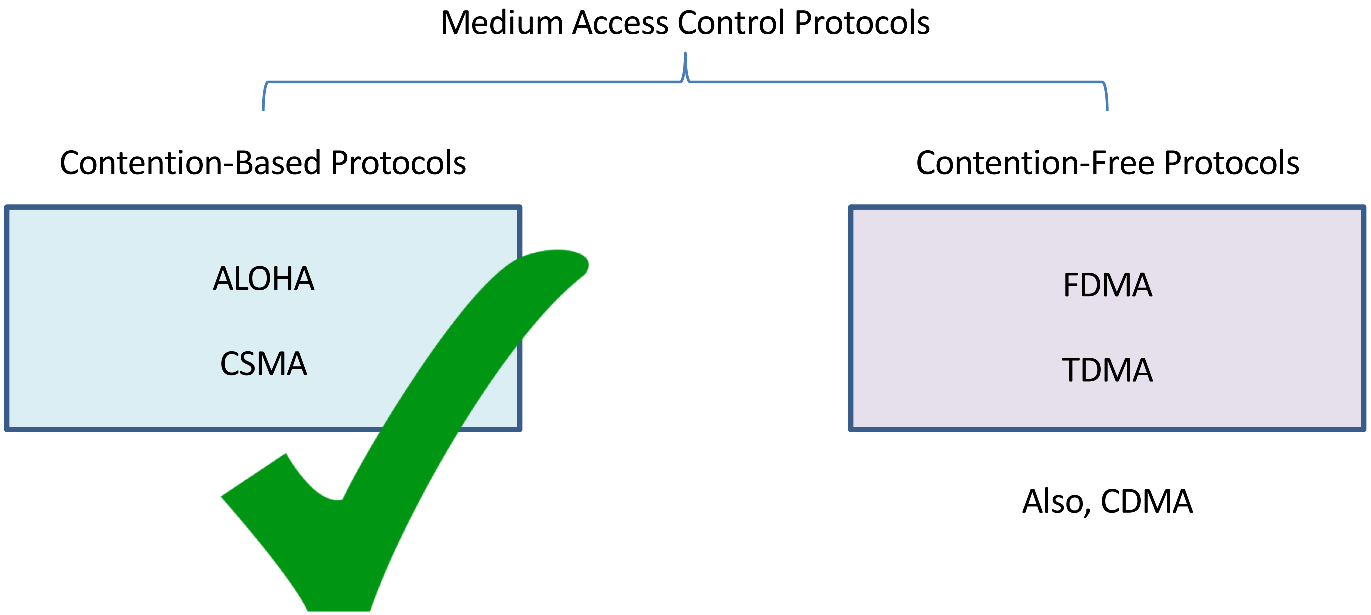


CSMA with RTS/CTS

- 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

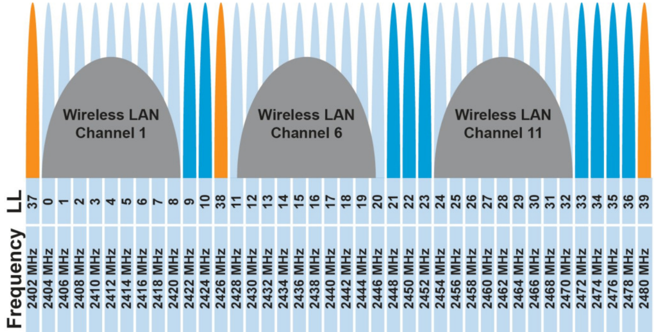
- Really efficient at creating a high-throughput network
  - Assuming they are all following the same protocol
  - Otherwise, interference can be very problematic

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

CDMA – Code Division Multiple Access

- Split transmissions in ‘codes’
  - Not new; original applications in radar and early satellite communications
- Analogy: Multiple speakers in the same room all in different languages
  - [The human brain is crazy good at ignoring what it doesn’t understand ☺]
- Requires signal power coordination
  - [everyone needs to speak ~the same volume]
  - Can be hard in uncontrolled / dynamic environments
- Also can be more performant with highly synchronized clocks
  - i.e. if the code clock is known to both devices; intractable in mobile settings

Real-world protocol access control

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

- CSMA
  - WiFi (slotted, CSMA/CA)
  - 802.15.4

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

- CDMA
  - Most modern cellular networks

Lab 1: How does *your* Internet work?

- What can you learn about the network around you?
- Play with Wireshark
- Protocol analysis, introspection

Now: Hang out for a bit and find a group if you need

Pre-lab 1 is due *before* the start of lab (i.e., in 43 hours)

Need to have group to do pre-lab 1!

If you don't have a group, stay here and make one now

- Groups of 3, three, and only three
  - [Except at-most-one group of four if needed — group of two not okay]