2/5/16
radio gaga notes

brainstorm go-around

1. yuchi
    a. watch tv programs on cell phone;
    b. visualize something you can't see;
2. dhruv
    a. detect fake cell towers
    b. pick up freq that drones communicate in
    c. picking up ambient rf and sonify/visualize it
3. leon
    a. build a browser that visualizes packets coming in/out, lets you see behind the scenes
4. chino
    a. radio applications in/for consumer electronics, IoT
    b. RFID- using radio waves and the tags on whatever you're trying to steal
        i. see sammy kamkar talk: http://samy.pl/defcon2015/
5. greg
    a. torrent equivalent of data
    b. create hot spot in the city by tethering wi fi into a single data stream
    c. converting radio signals into energy and storing it
        i. extracting value from nothing
6. karthik
    a. tesla hack: HackRF to open the tesla charging port
    b. highway signage hacked to play tetris on
    c. heart rate art
        i. hack heart rate monitor and visualize it
7. jen
    a. hacking ankle monitor
    b. who owns spectrum? who goes to the auction?
8. edwin
    a. what can be done with the dumb phone? how to create smart-like applications for the dumb phone
    b. mobile money, emergency stuff w sms
        i. dumbsto.re
    c. new white space that's available
9. dana
    a. politics of who controls rf spectrum
    b. lawsuits against fcc
    c. rf as a scarce natural resource
    d. creeping on ems
        i. openmhz.com/scanner

10. kevin
    a. raspberry pi with sdr
11. melanie
    a. rf spectrum as ephemeral space to make site-specific stuff
        i. network in places where people are looking for public open free wifi
    b. time lapse of rf spectrum maps
12. renata
    a. radio and freq directivity
        i. talk to pedro

wifi

hedy lamarr- actress, researcher, scientist

- frequency jamming, submarines
- frequency hopping to resist jamming
    - "**Frequency Hopping** Spread Spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many **frequency** channels, using a pseudorandom sequence known to both transmitter and receiver."
- freq. hopping is the foundation of wifi, bluetooth, gsm

wifi explorer visualizer: https://www.adriangranados.com/apps/wifi-explorer

IEEE determines

- 802.11.b, g, n
- b and g are in 2.4 ghz, n is in 5 mhz
- lower frequency, more bandwidth, travels far
- higher frequency, less bandwidth, can't travel as far

claude shannon

- information theory: you only need to send a base amount of information, and the message can be reconstructed on the other side
- all file compression is based on his work
- mathematical theory of communication: http://worrydream.com/refs/Shannon%20-%20A%20Mathematical%20Theory%20of%20Communication.pdf
- ultimate machine: https://www.youtube.com/watch?v=cZ34RDn34Ws

types of packets that are sent over wifi

- data frames
    - actual information
- management frames
    - used to:
        - set up a connection

        - stop a connection
        - reconnect when we disconnect
    - where all the fun stuff happens, where you understand what's hard about getting devices to talk to each other

important management frames

probe request frame

- coming from phones and laptops, trying to connect to different networks

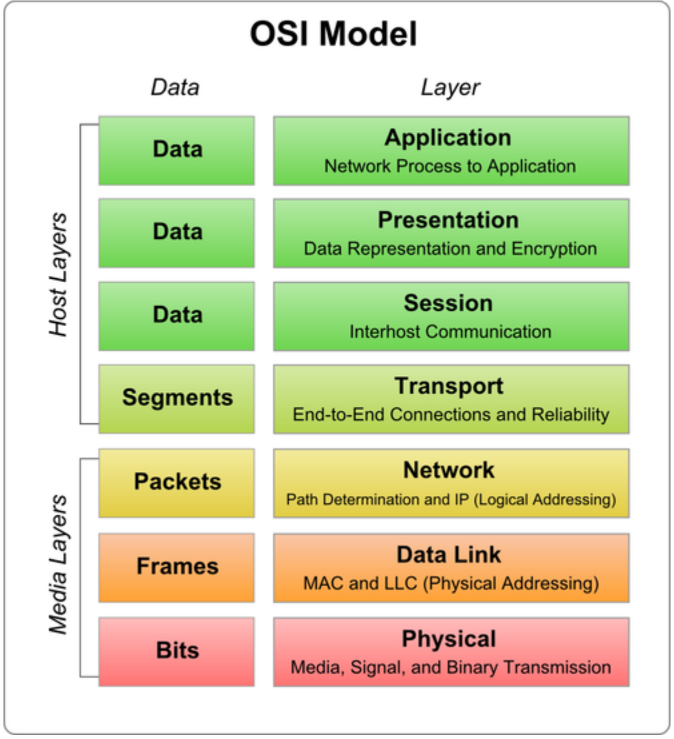
beacon frame

info being sent out from a wifi router
tells you what type of encryption the network is using
tells you freq that info is being sent out

- WPA
- WPA2
- WPA Ent

OSI stack

- recipe of what a packet is



OSI Model

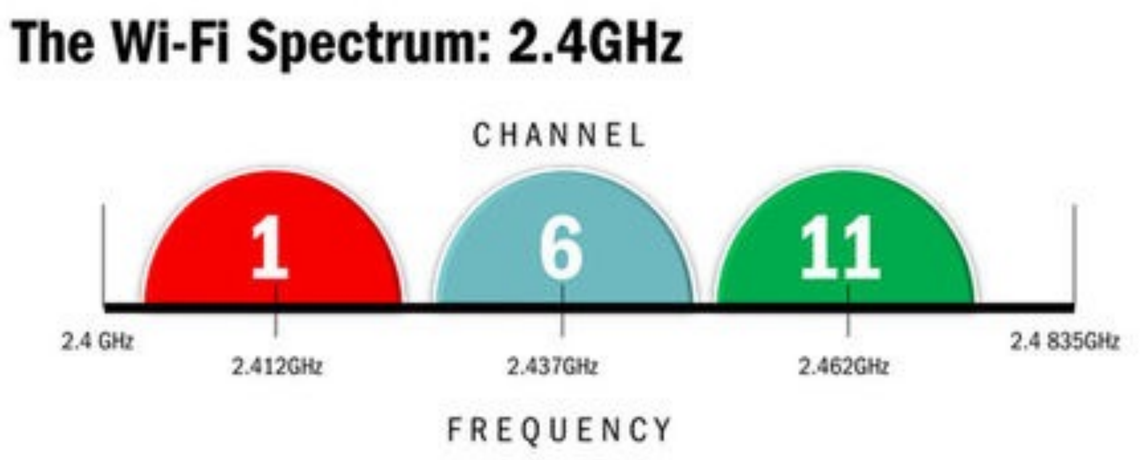
	Data	Layer
Host Layers	Data	**Application** Network Process to Application
	Data	**Presentation** Data Representation and Encryption
	Data	**Session** Interhost Communication
	Segments	**Transport** End-to-End Connections and Reliability
Media Layers	Packets	**Network** Path Determination and IP (Logical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

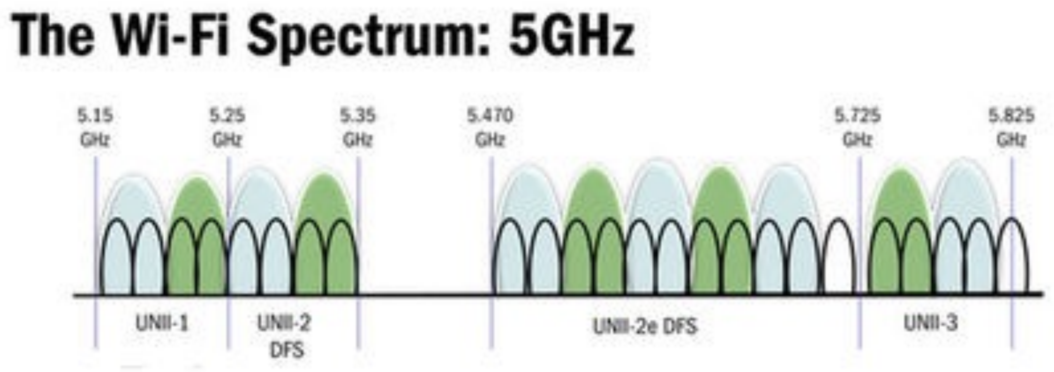
- lots of things have to happen for my computer to get information from google
- the hard part is knowing where in the stack you are at what time
    - http://suryamattu.com/packet-sniffing-tutorial
    - IP address : apartment building; host name : which specific apartment
    - devices on a network: https://www.iwaxx.com/debookee/

- hypothetically possible and highly not recommended to spoof mac address to get free wifi on a plane

extra stuff

- https://plugunplug.net/
- https://wigle.net/
-


The Wi-Fi Spectrum: 2.4GHz
CHANNEL
1
6
11
2.4 GHz
2.412GHz
2.437GHz
2.462GHz
2.4 835GHz
FREQUENCY


The Wi-Fi Spectrum: 5GHz
5.15 GHz
5.25 GHz
5.35 GHz
5.470 GHz
5.725 GHz
5.825 GHz
UNII-1
UNII-2 DFS
UNII-2e DFS
UNII-3