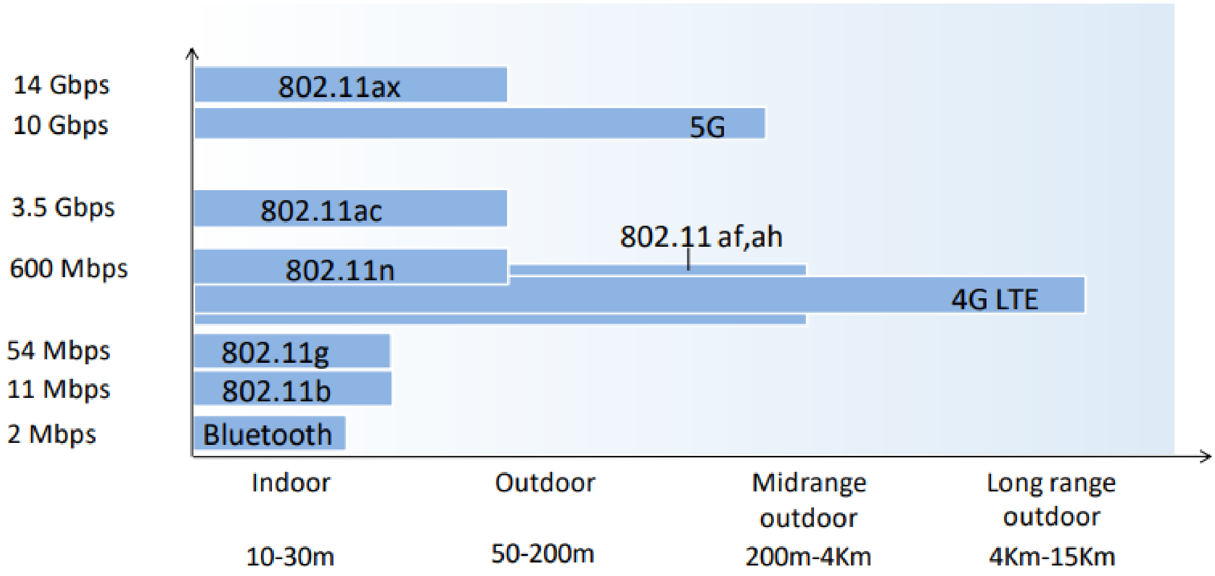
07. Wireless and Mobile Networks

7.1 Introduction

Wireless networks are, well, networks that are not connected by wire. They consist of:

- Wireless hosts: end-system devices that run applications that are connected to the network. They may be stationary, wireless doesn't always mean mobile. Examples are your phone, tablet, or laptop.
- Base stations: infrastructure responsible for relaying packets between wireless hosts. Examples are cell towers or 802.11 access points.
- Wireless links: links to connect devices to the base station. Examples are satellite communication, Bluetooth or 5G

Different wireless links have different characteristics, so they should be selected wisely.



There are two operation modes for wireless networks:

1. Infrastructure mode: base station connects mobiles to a wired network, and mobile changes base station providing connection into a wired network

2. Ad-hoc mode: no base stations and nodes can only transmit to other nodes within link coverage. Nodes organize themselves into a network, routing among themselves

	Single Hop	Multiple Hops
Infrastructure	Hosts connect to base station, which connects to larger internet	Hosts may have to relay through several wireless nodes to larger internet (mesh net)
No infrastructure	No base station to connect to larger internet (Bluetooth, ad-hoc nets)	No base station, no connection, may have to relay to reach other a nodes (MANET, VANET)

7.2 Wireless Links and Network Characteristics

Wireless linking and networking has some key problems such as:

1. Decreasing signal strength: electromagnetic radiation attenuates as it passes through matter, leading to possible path loss.
2. Interference from other sources: radio sources transmitting in the same frequency will interfere with each other
3. Multipath propagation: happens when electromagnetic waves reflect off objects and the ground, taking paths of different lengths between a sender and receiver. Moving objects between sender and receiver might also cause this.

Signal Noise Ratio (SNR) is a measurement to measure the strength of a received wireless signal. The higher the SNR, the better.

- Given the physical layer, increase power, leads to increased SNR, which leads to decreased bit error rate (BER)
- Given SNR, choose a physical layer that meets BER requirements, giving the highest throughput.

There are also other problems that you wouldn't typically come across in a traditional wired network. An example is the hidden terminal problem. Say link A is transmitting to B, but at the same time, C is also transmitting to B. This would be fine, however, A and C are on the opposite sides of a mountain with a lot of interference. Neither A nor C is then capable of knowing that they're interfering with B.

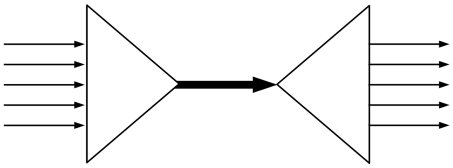
Code Division Multiple Access (CDMA) is a way for multiple nodes to communicate simultaneously.

Each node or user is assigned a unique code that is used to encode data. This allows multiple nodes to coexist and transmit because their data can be distinguished.

Code-division multiple access - Wikipedia

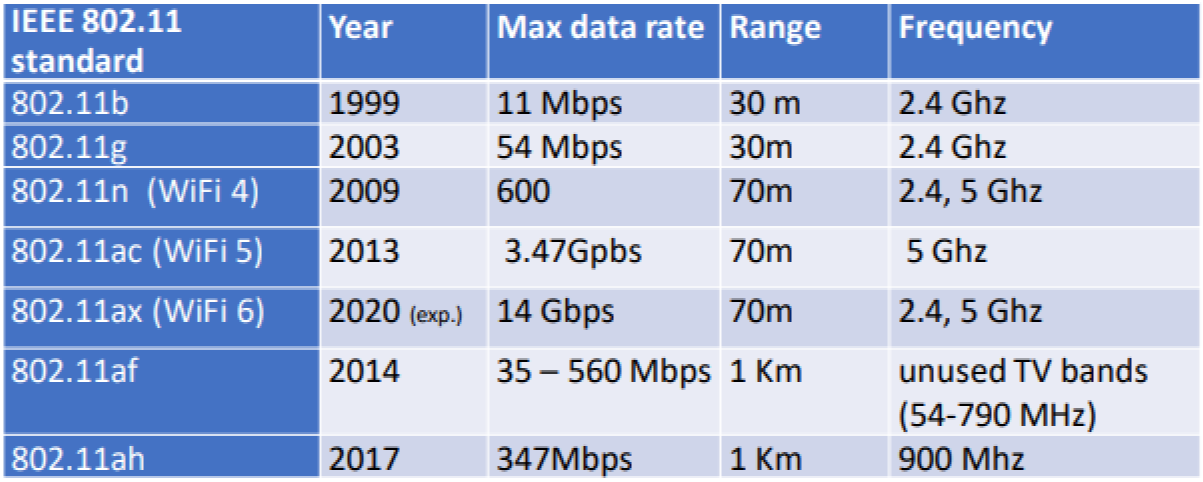
Code-division multiple access (CDMA) is a channel access method used by various radio communication technologies. CDMA is an example of multiple access, where several transmitters can send

W https://en.wikipedia.org/wiki/Code-division_multiple_access



7.3 WiFi: 802.11 Wireless LANs

IEEEs 802.11 Wireless LAN standard has become the main standard for wireless LAN networking, with multiple versions featuring different characteristics over the years.



IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

The 802.11 architecture consists of a wireless host that communicates with a base station (AP). (or in the case of ad-hoc mode, hosts only).

The AP node admin selects a frequency for the AP which means interference between AP nodes is possible. When the arriving hosts connect, they must associate with an AP on the network.

AP nodes send out beacon frames which arriving hosts can listen for and respond to establish a connection with the AP. These frames are typically sent out every 100 milliseconds. An arriving host can also do active scanning, probing for APs in range, and establishing a connection this way.

802.11 also needs a media access control scheme to work with multiple hosts on the same AP station. It uses the same random access CSMA protocol as Ethernet, except it uses collision avoidance instead of collision detection. Collision detection is a problem with wireless LANs as you end up just blocking the channel, and it's also impossible to detect if other users on the network are using the channel (due to the terminal problem described above)

An extension to this CSMA/CA standard is adding an RTS (right to send)/CTS (clear to send) packets to the AP, which acts as a controller for which hosts may send. Hosts must send an RTS packet and receive a CTS before transmitting.

802.11 also has some advanced capabilities when changing stations, allowing connections like TCP connections to stay open while the host changes AP stations on the same network. It also has a power management feature, allowing hosts to tell the AP they're going to "sleep" until the next beacon frame, informing the AP not to send any frames to the host, and instead buffer them until the host is awake again.

7.4 Cellular Networks: 4G and 5G