CSCI 466: Networks

Wireless Networks, WiFi

Reese Pearsall

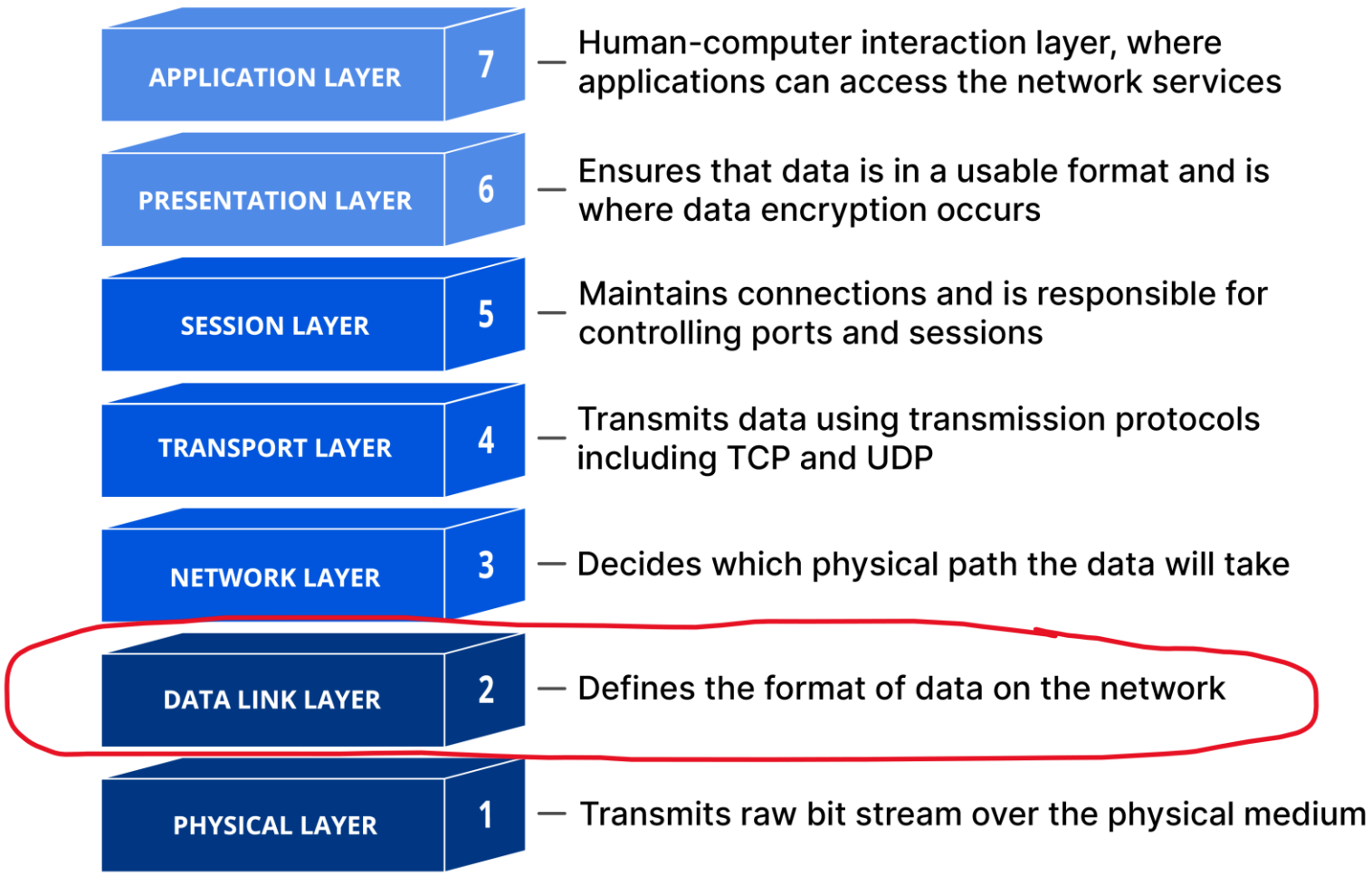
Fall 2024

Announcements

Quiz on Friday (no class)

- Message Confidentiality (Encryption)
- Message Integrity and Authentication (Hashing)
- Network Attacks (SYN flooding, SYN reset, SYN Hijacking, DNS attacks, BGP attacks, Smurf Attack)
- Security Protocols (TLS, Ipsec)
- Operational Security (Firewalls, IDS, IOCs)
- Wireless Networks, WiFi

PA3 due on Sunday @ 11:59 PM

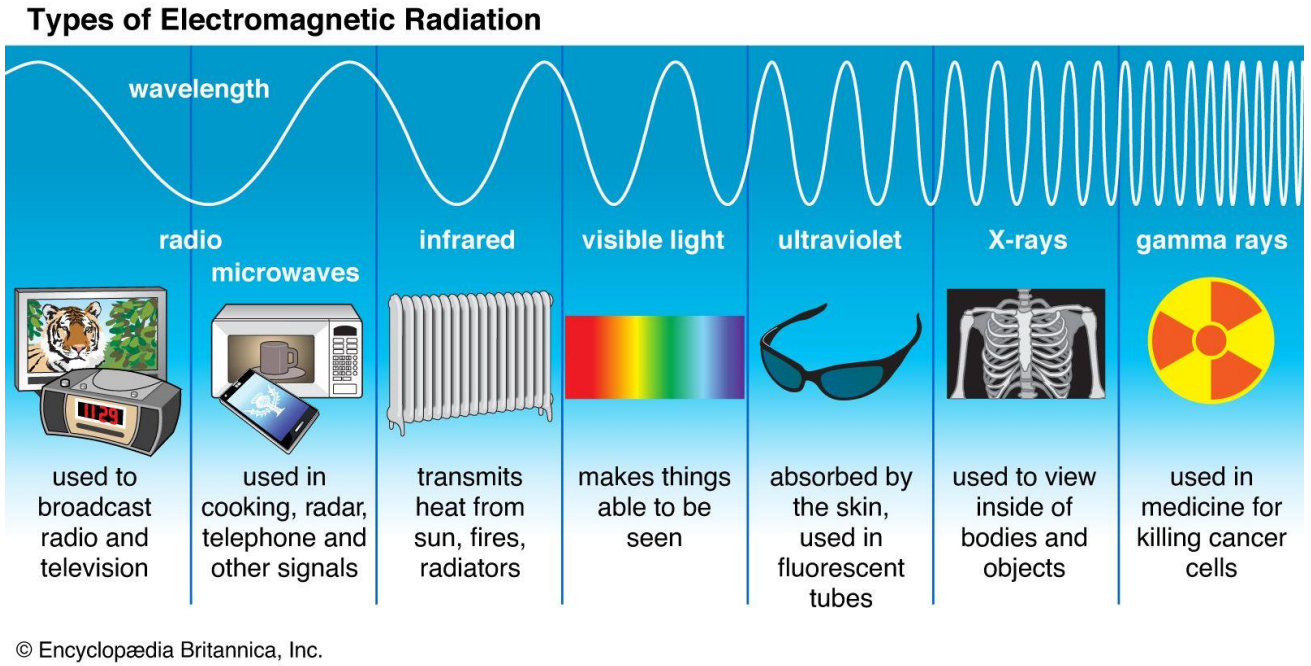

APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATA LINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

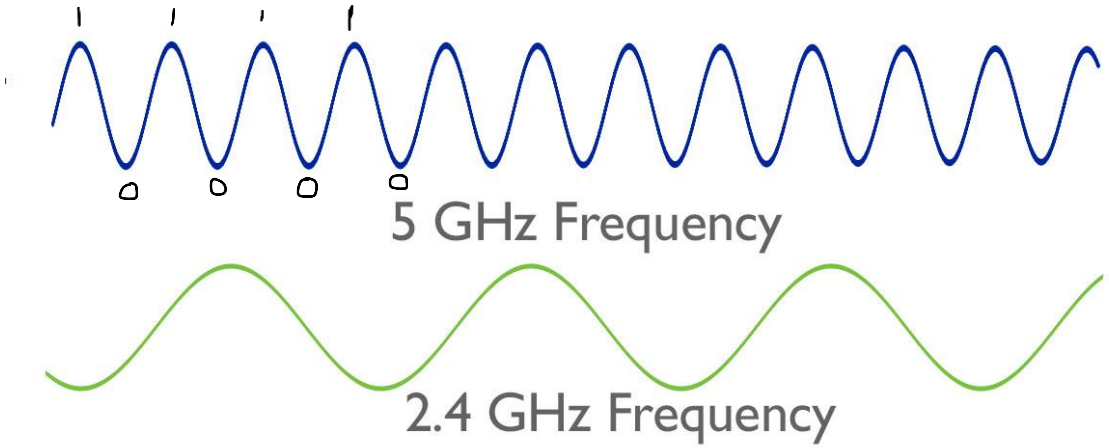
Wireless and Mobile Networks: context

- more wireless (mobile) phone subscribers than fixed (wired) phone subscribers (10-to-1 in 2019)!
- more mobile-broadband-connected devices than fixed-broadband-connected devices devices (5-1 in 2019)!
  - 4G/5G cellular networks now embracing Internet protocol stack, including SDN
- two important (but different) challenges
  - wireless: communication over wireless link
  - mobility: handling the mobile user who changes point of attachment to network

Wireless Networks

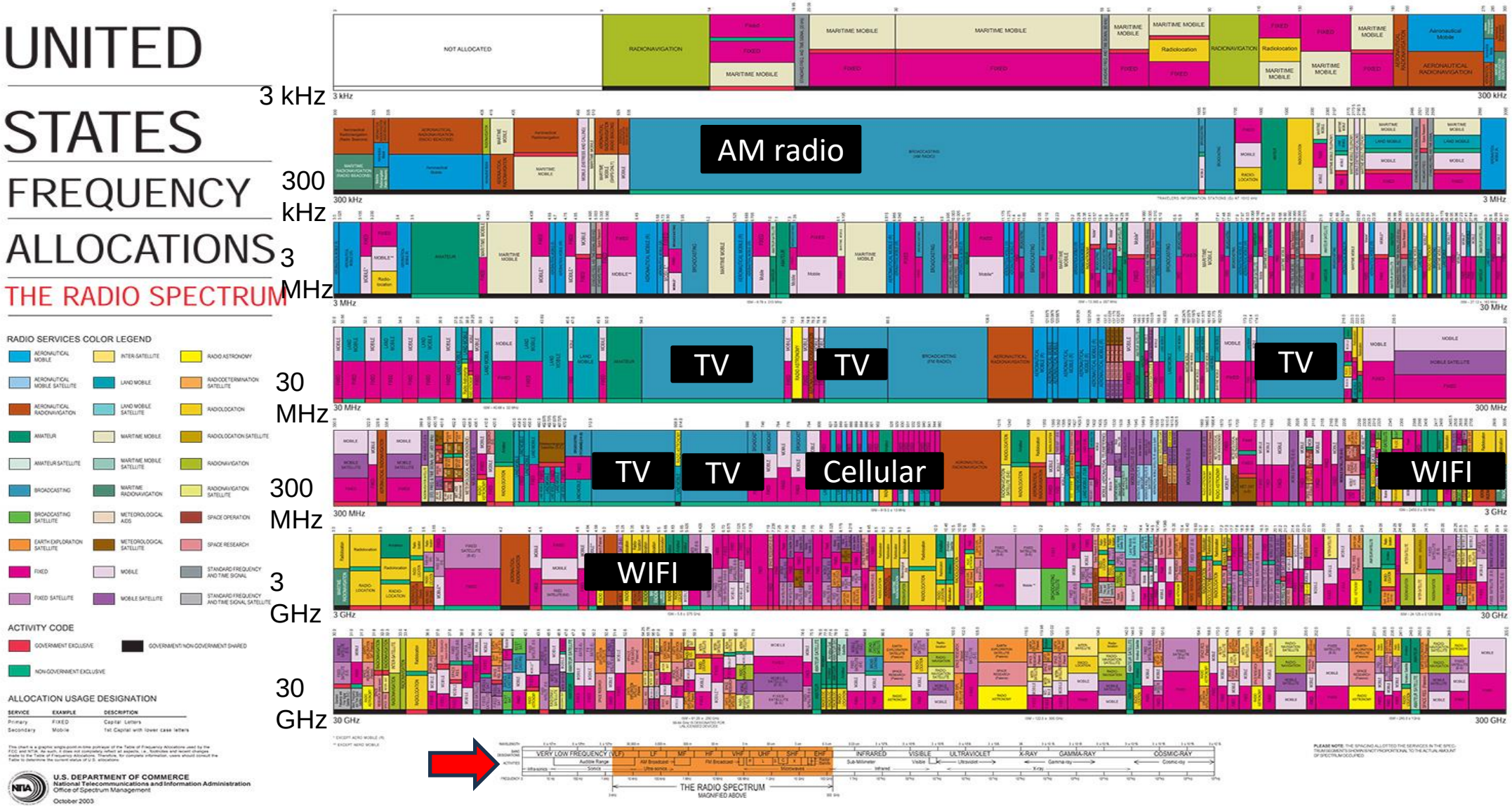
Transmission Medium = waves in the air





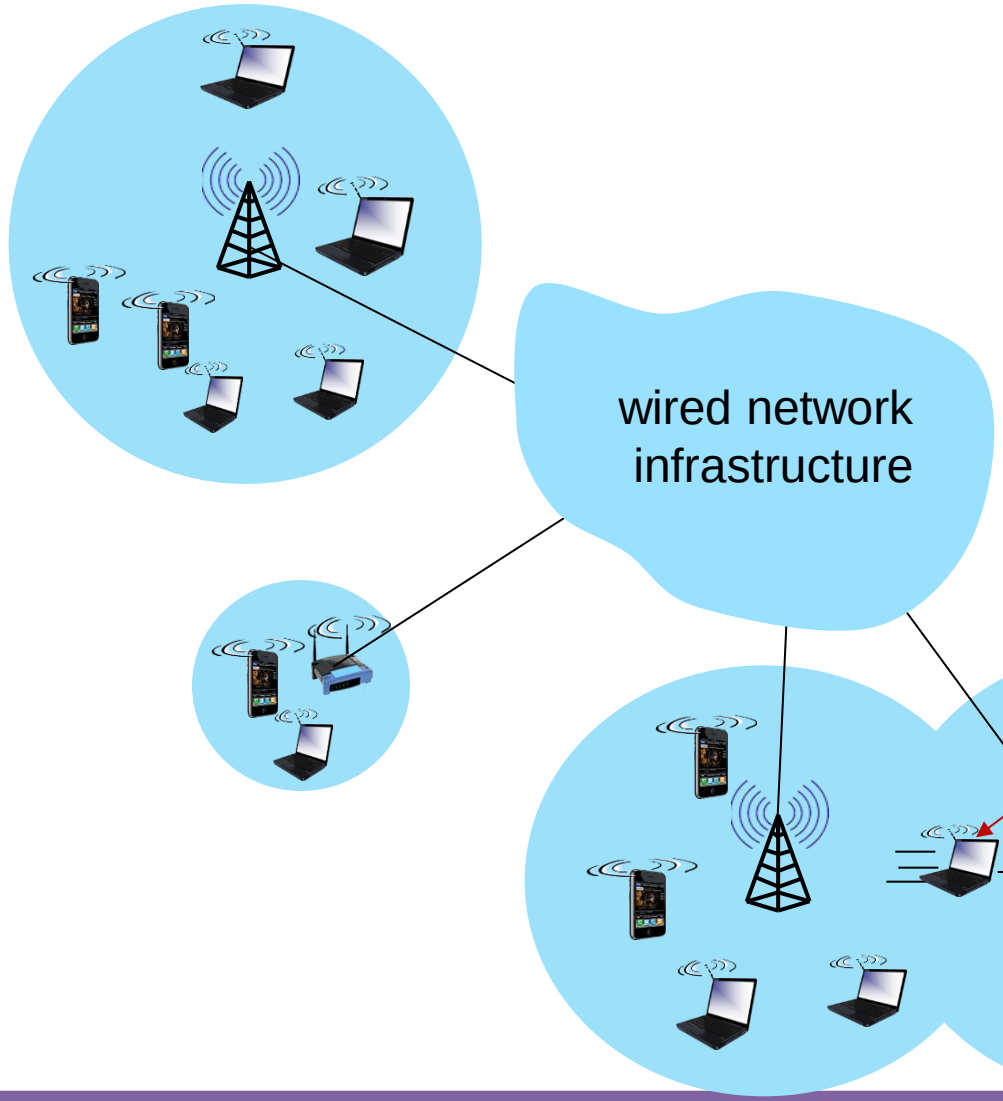
We can transmit waves at different ***frequencies***

Lower frequency→ The farther the wave can travel



The government controls which frequencies should be used for different technologies/services

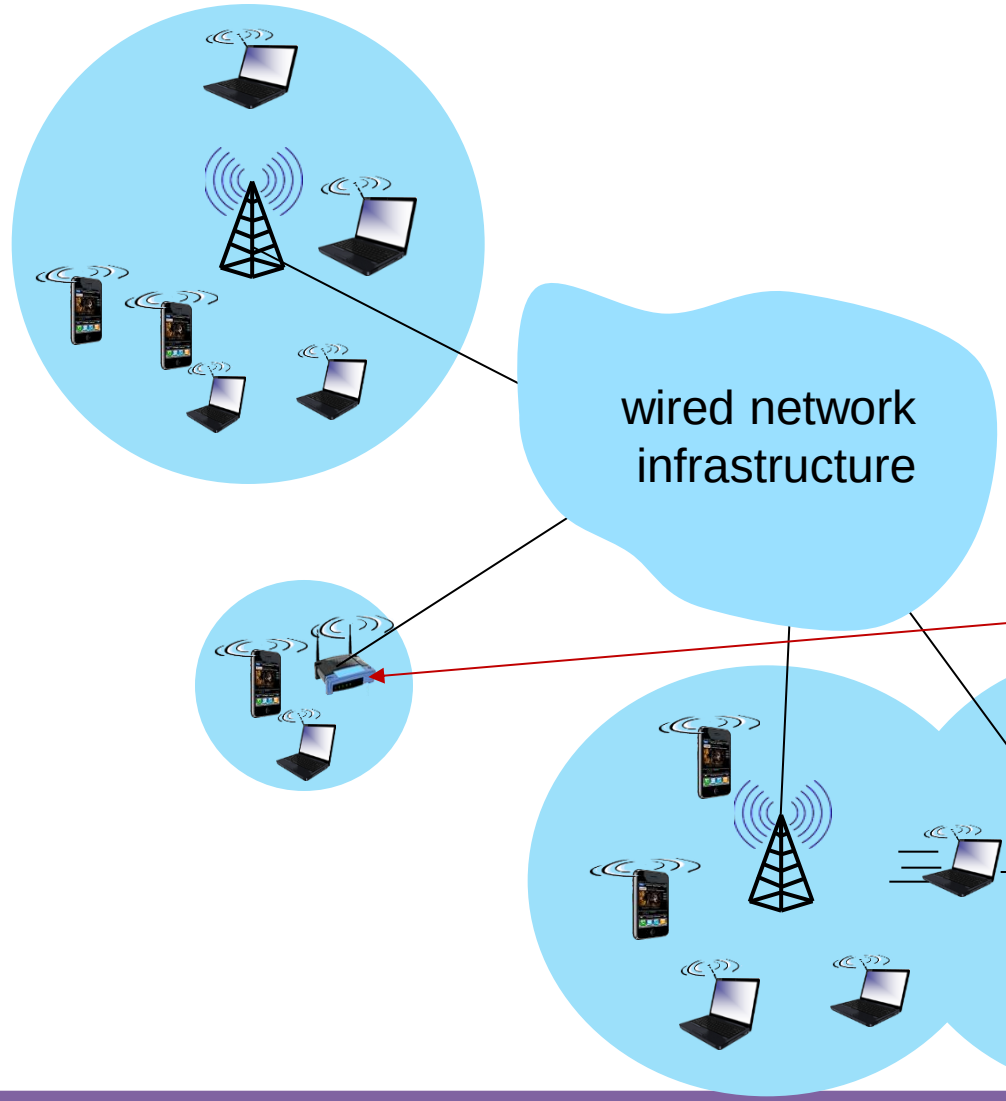
Elements of a wireless network



wireless hosts

- laptop, smartphone, IoT
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility!

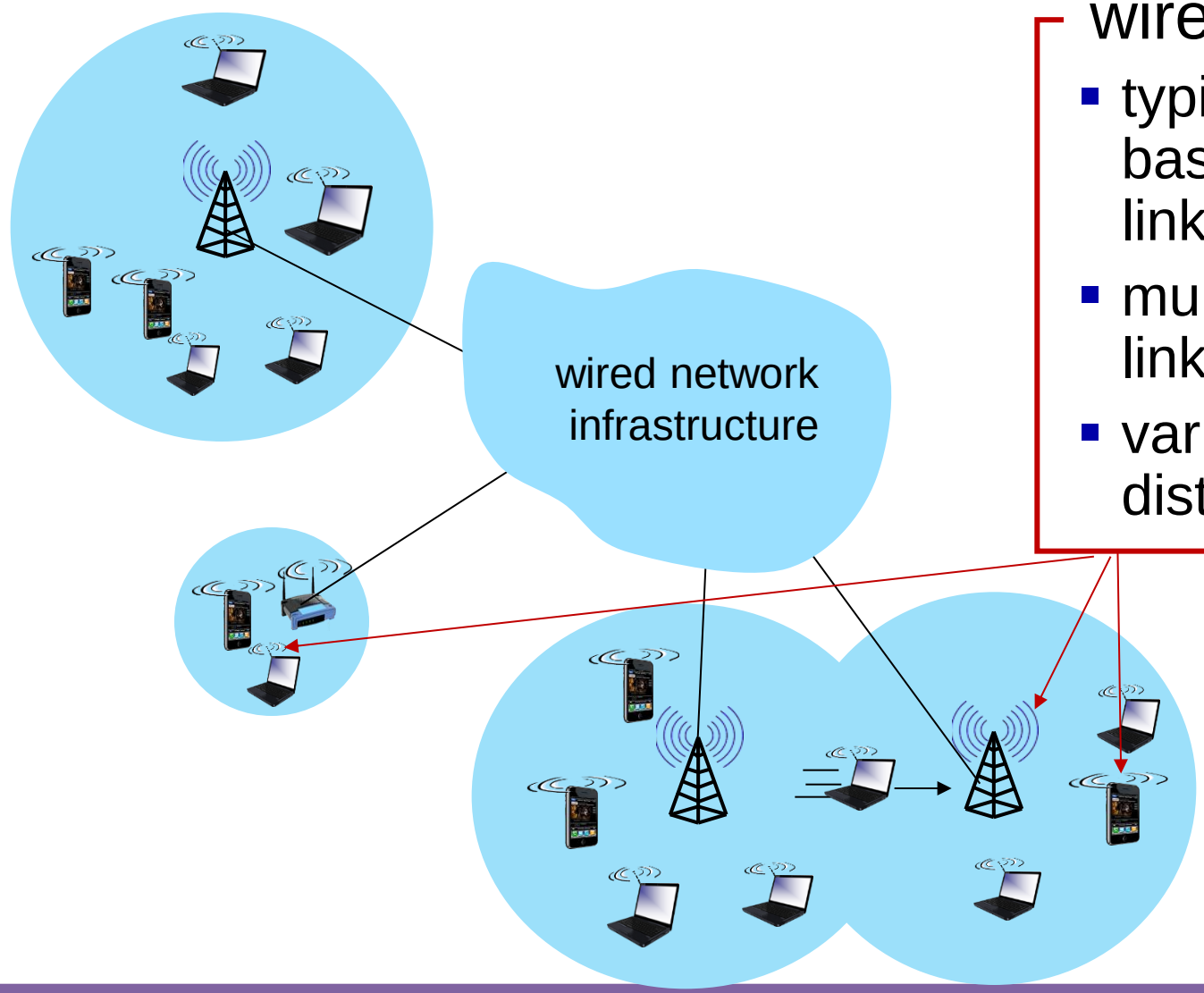
Elements of a wireless network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its “area”
  - e.g., cell towers, 802.11 access points

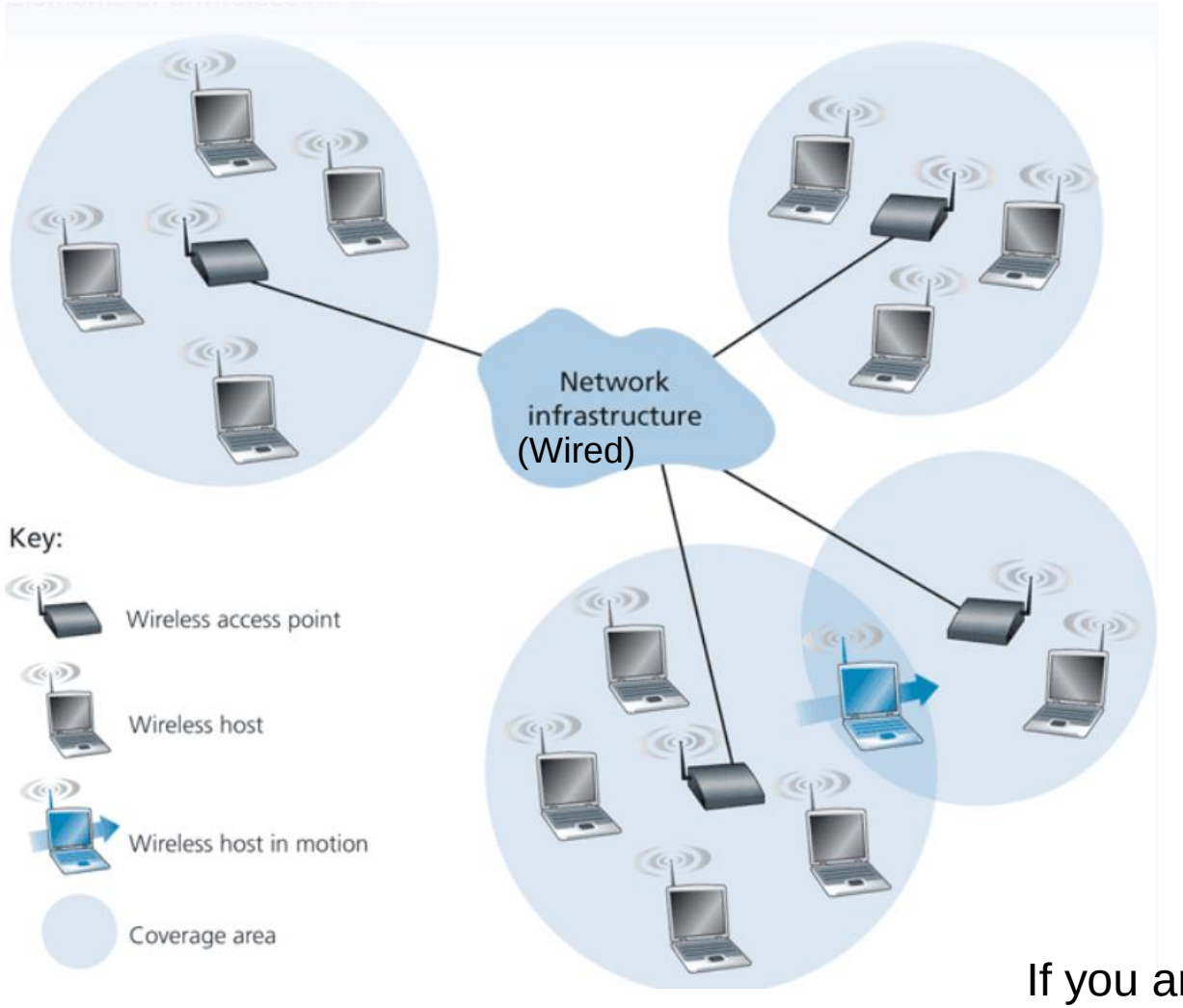
Elements of a wireless network



wireless link

- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

Elements of a wireless network



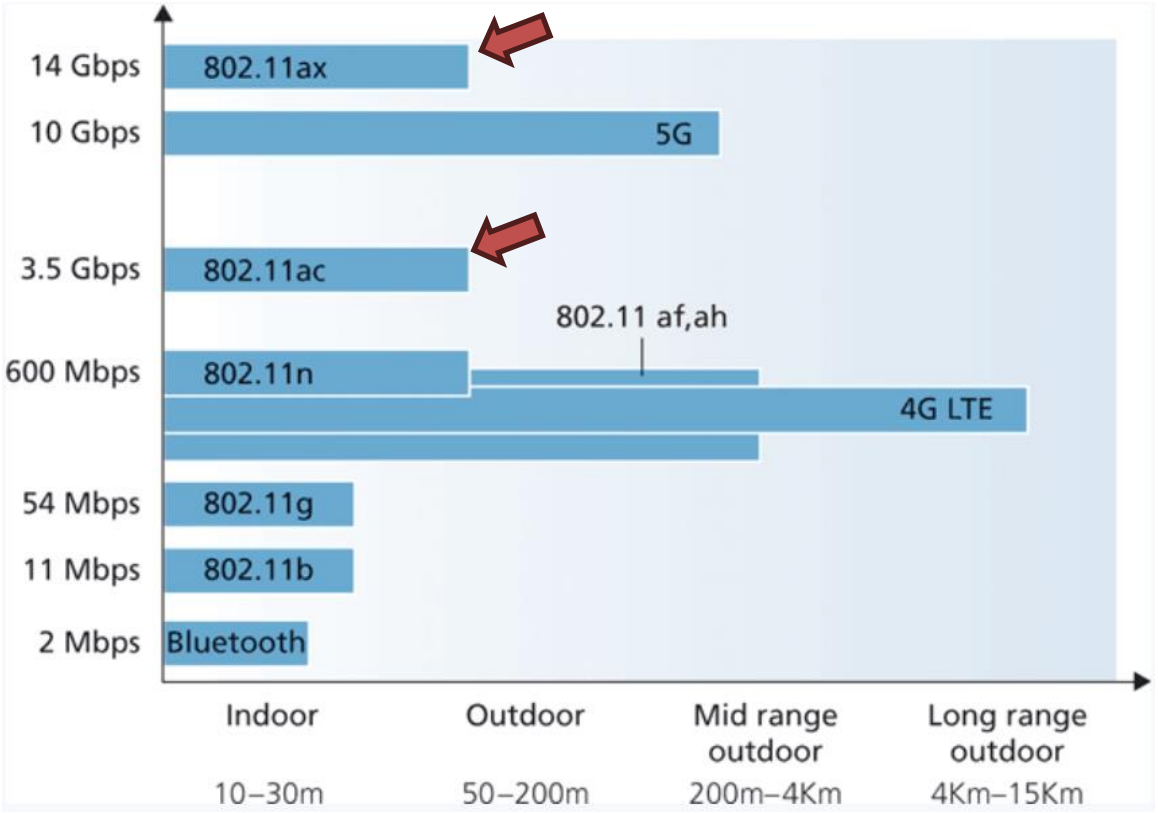
Wireless networks are an *extension* of the standard internet, and usually only occur at the *network edge*

Wireless hosts connect to a **wireless access point** that will connect them to the greater internet. Typically linked to a geographic location

Cell towers are the access points in cellular networks

If you are not in range of a wireless access point, you will not be able to connect to the internet

Elements of a wireless network



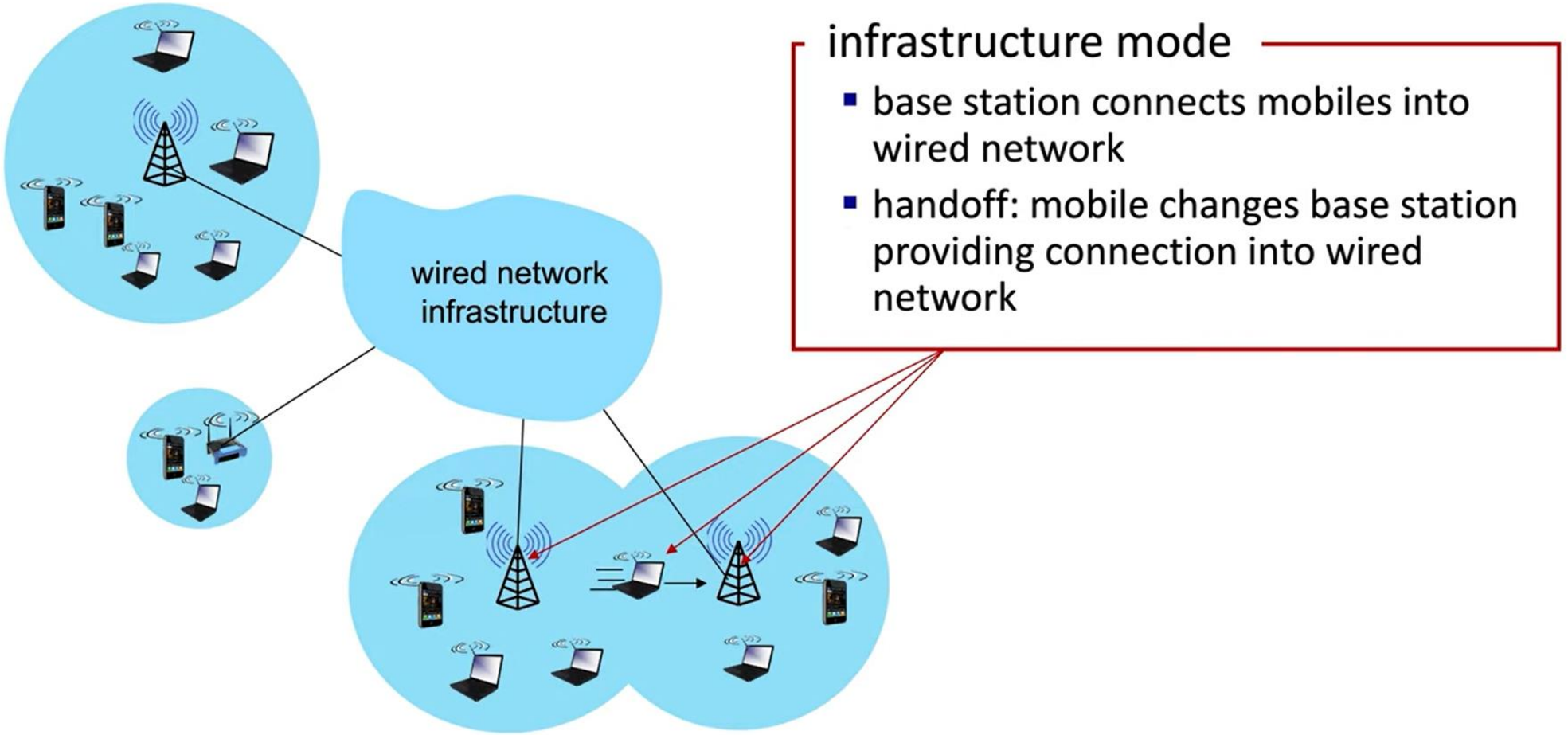
Easer to create high bandwidth links over high frequency carriers, but higher frequencies lose energy more rapidly and it propagates

Generally, lower frequencies are better for long distance communication

802.11 = WiFi

(These are just Wireless and wireless LAN protocols, there are many more ways!)

Elements of a wireless network



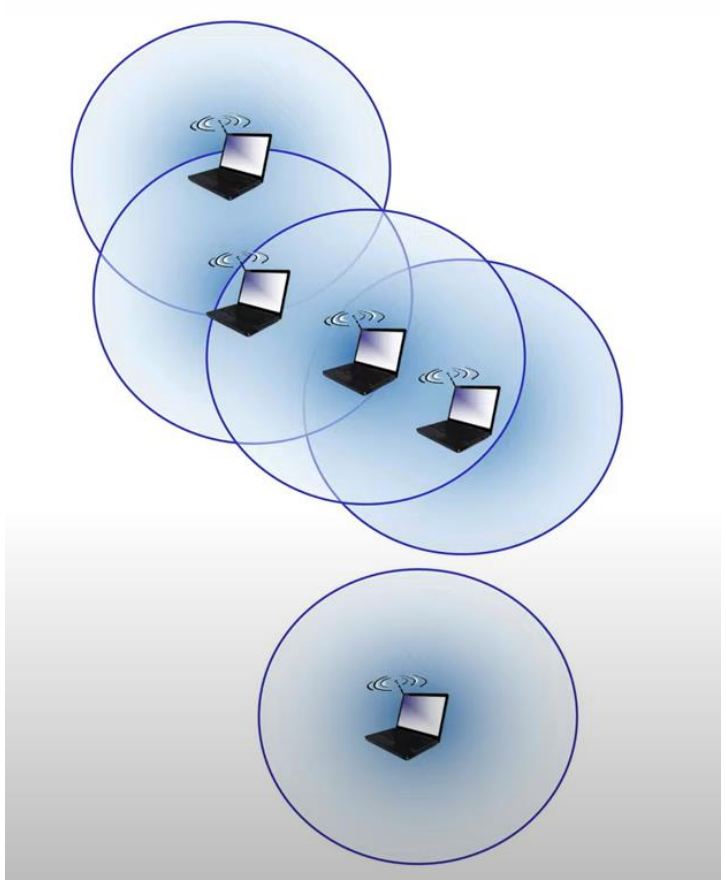
infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

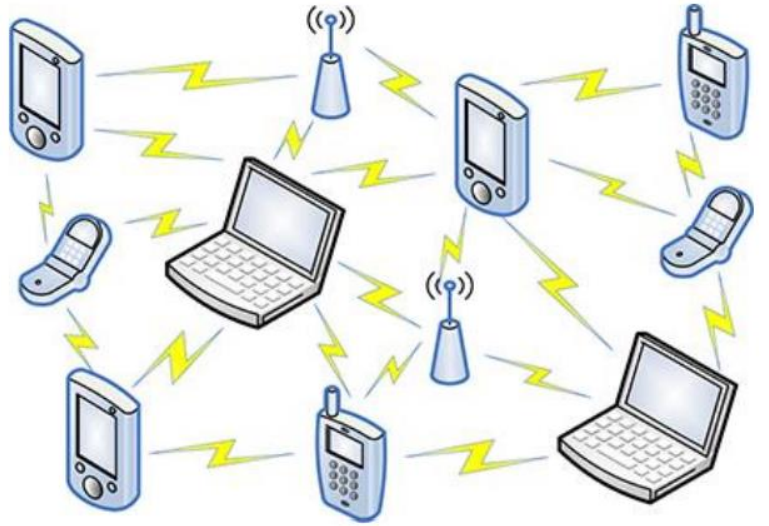
Elements of a wireless network

Ad hoc mode

- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes organize themselves into a network: route amongst themselves

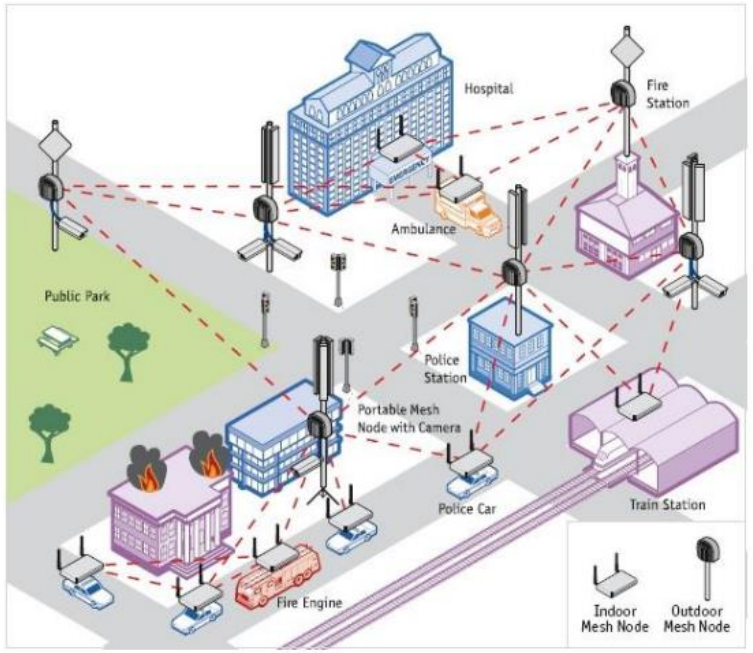


Mobile Ad Hoc Nets (MANETs)



No central administration

Mesh (Ad Hoc) Mode



Nodes themselves must provide services such as DNS and DHCP

This is advantageous where infrastructure may be damaged or not available

Wireless network taxonomy

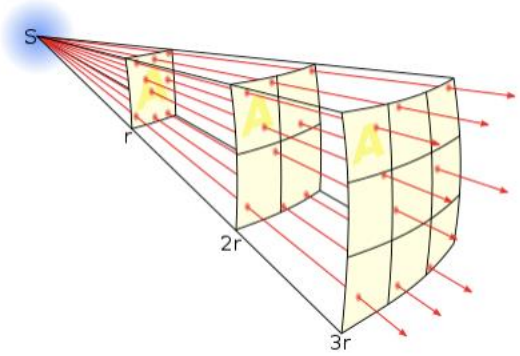
	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Wireless link characteristics: fading (attenuation)

Wireless radio signal attenuates (loses power) as it propagates (free space "path loss")

Free space path loss ~ $(fd)^2$

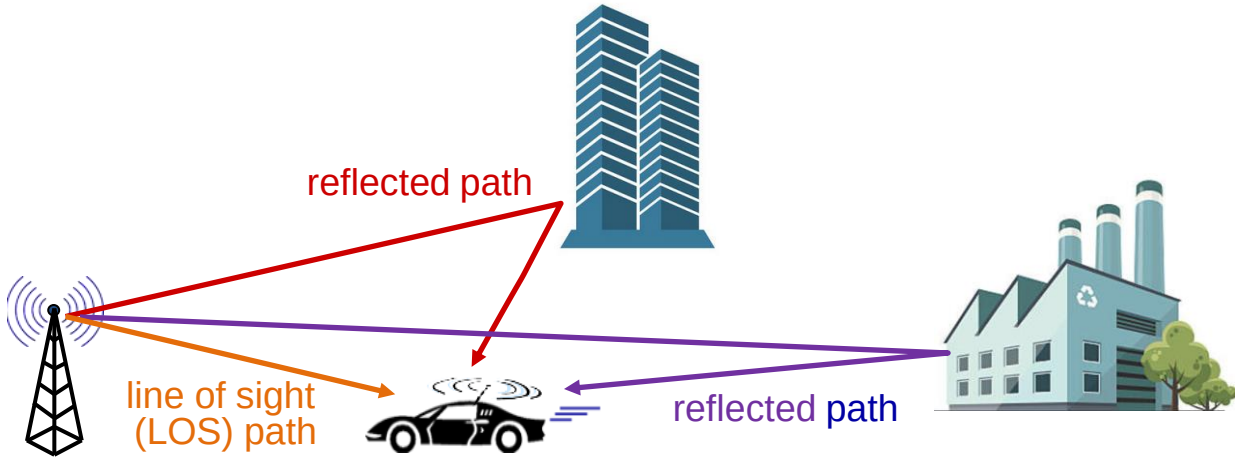
f: frequency
d: distance



higher frequency or longer distance → larger free space path loss

Wireless link characteristics: multipath

multipath propagation: radio signal reflects off objects ground, built environment, arriving at destination at slightly different times

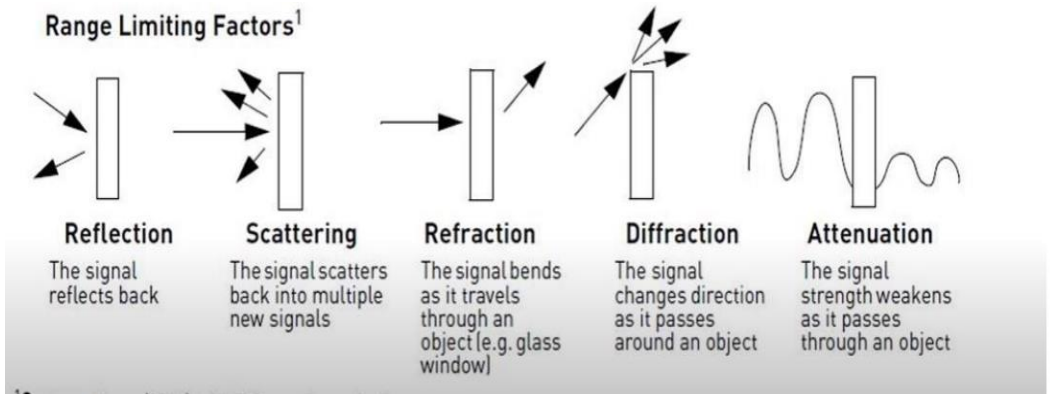


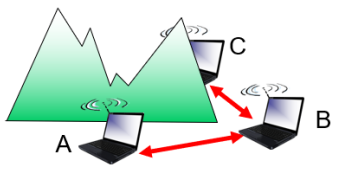
Wireless link characteristics: multipath

Important differences from wired link…

- **Decreased signal strength**: radio signal attenuates as it propagates through matter (path loss)
- **Interference from other sources**: wireless network frequencies (such as 2.4 ghz) shared by many devices will cause interferences
- **Multipath propagation**: radio signal reflects off objects ground, arriving at destination at slightly different speeds

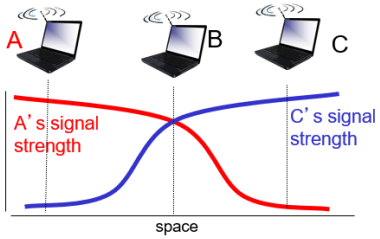
This makes wireless link communication much more challenging, compared to wired links





Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B



Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

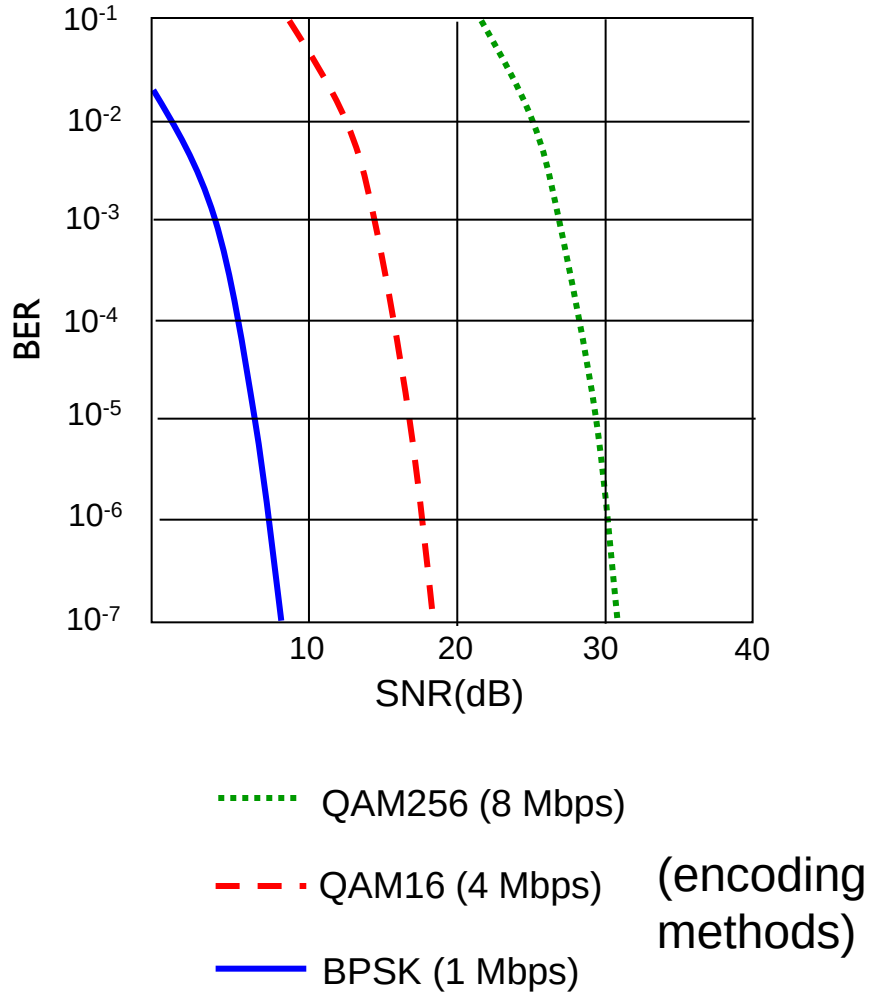
Wireless link characteristics: multipath

Wireless links have a threshold value they must operate over
→ If the wireless link does not meet this threshold, then a receiver cannot extract signal

SNR: signal-to-noise ratio
→ Larger SNR – easier to extract signal from noise (more power) (good thing)

BER: Bit Error Rate
→ Large BER – data is corrupted more frequently

SNR vs BER tradeoff
- *Given physical layer*: increase power → increase SNR → decrease BER
- *Given SNR*: choose physical layer that meets BER requirement, giving highest throughput



Shared Medium

- Because wireless networks are sharing a medium/frequency, we need mechanisms for **sharing bandwidth** so that collisions don't occur

- In the link layer we have three types

1. TDMA (Time division Multiple Access)
2. FDMA (Frequency Division Multiple Access)

} Wired Networks

3. CDMA (Code Division Multiple Access)

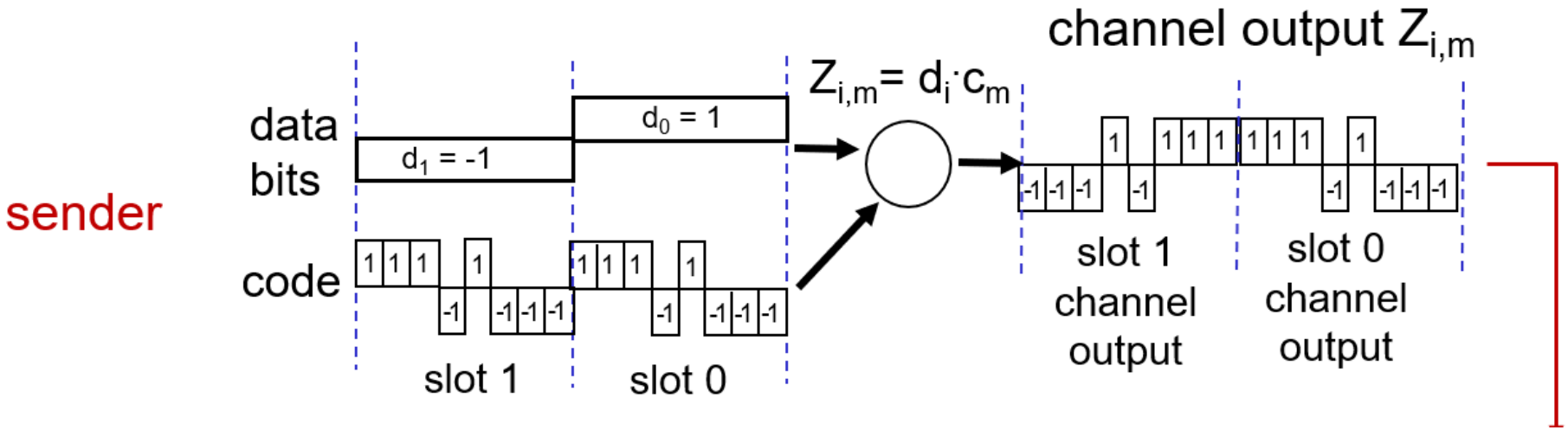
} Wireless Networks

CDMA (Code Division Multiple Access)

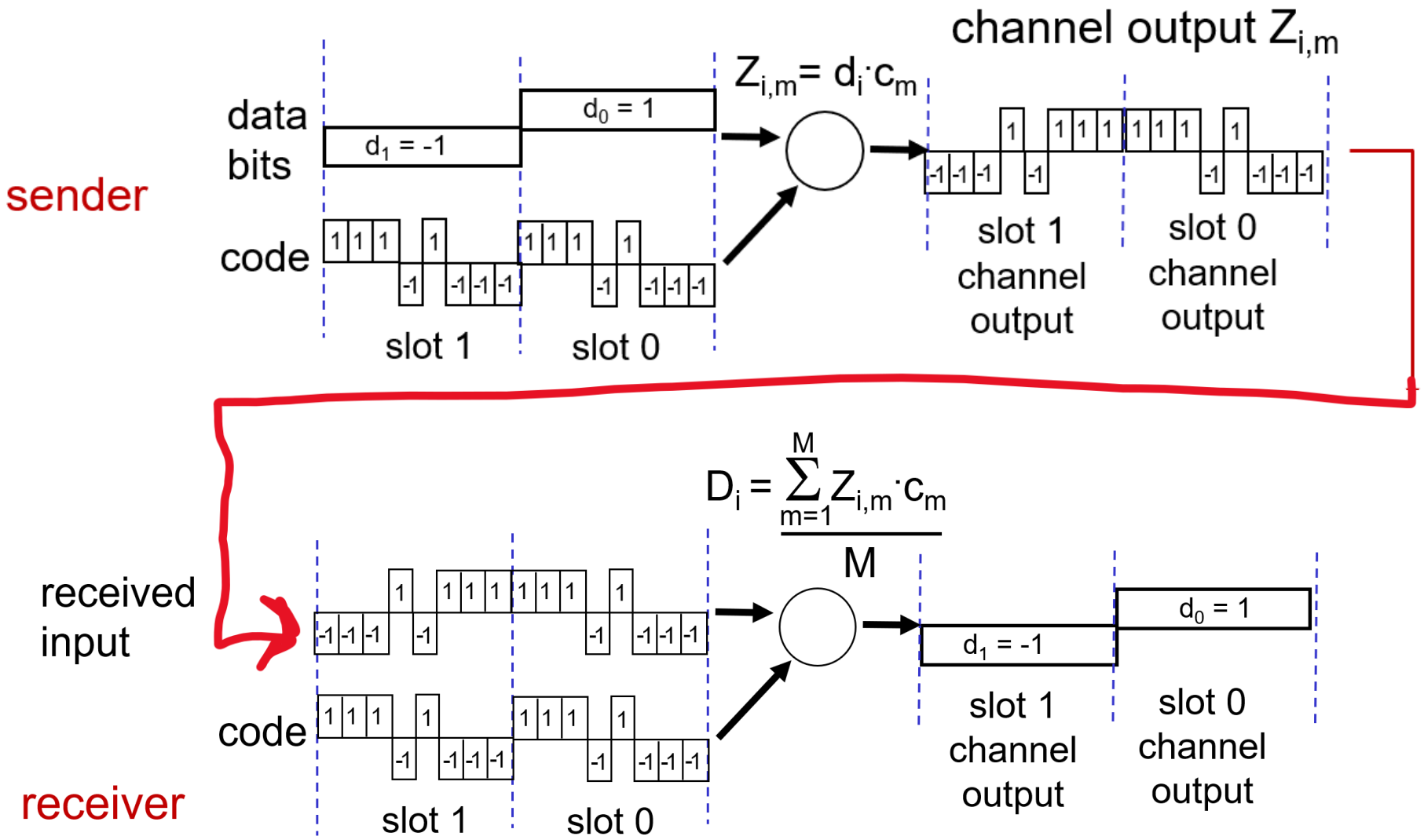
All users transmit on the same frequency, but are assigned a unique code (chipping sequence)

In a CDMA protocol, each bit being sent is encoded by multiplying the bit by a signal (the code)

- **Encoding**: inner product: (original data) * (chipping sequence)
- **Decoding**: summed inner-product: (encoded data) * (chipping sequence)



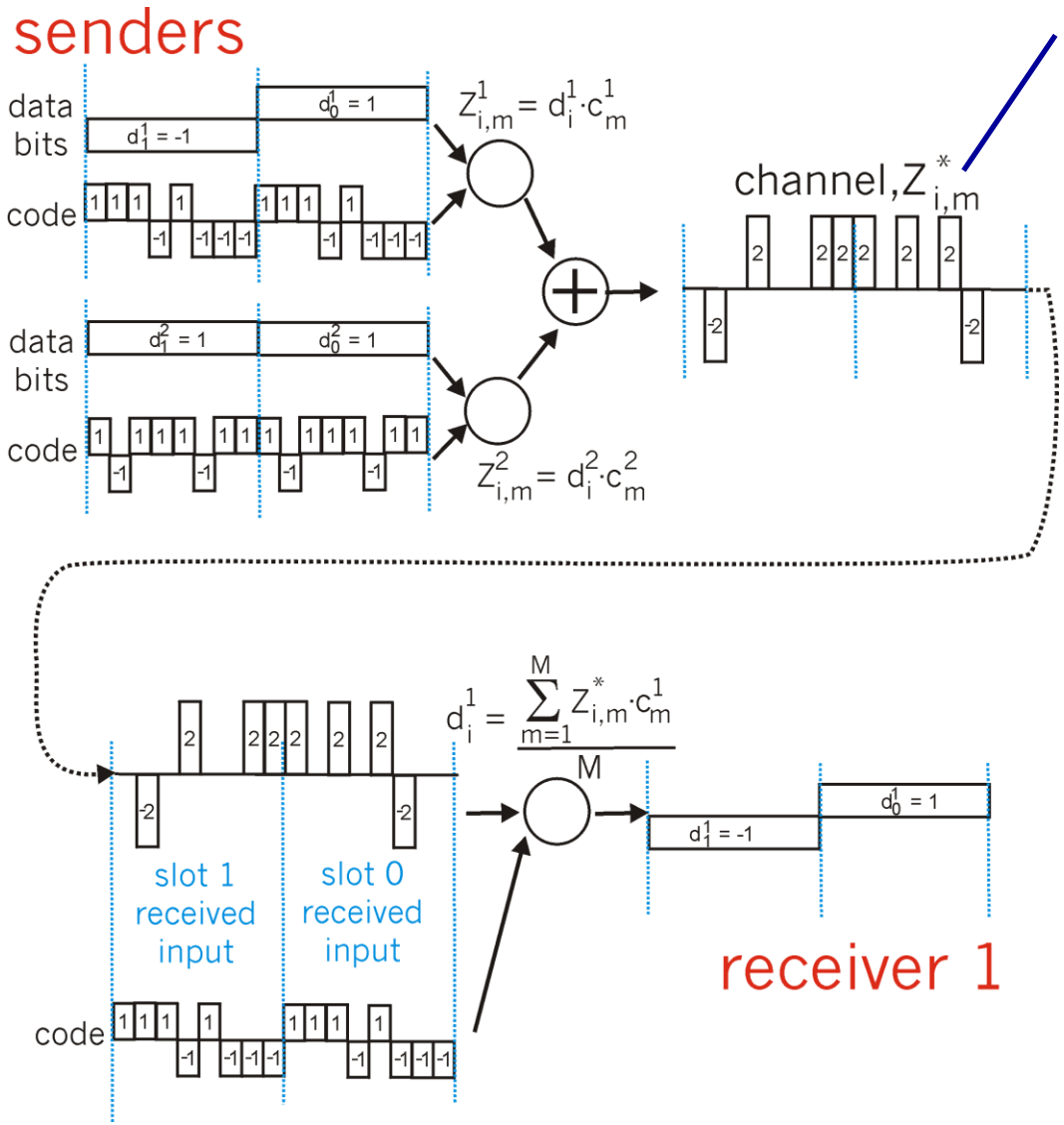
CDMA (Code Division Multiple Access)



CDMA (Code Division Multiple Access) (Multiple Senders)

Sender 1

Sender 2



channel sums together transmissions by sender 1 and 2

using same code as sender 1, receiver recovers sender 1's original data from summed channel data!

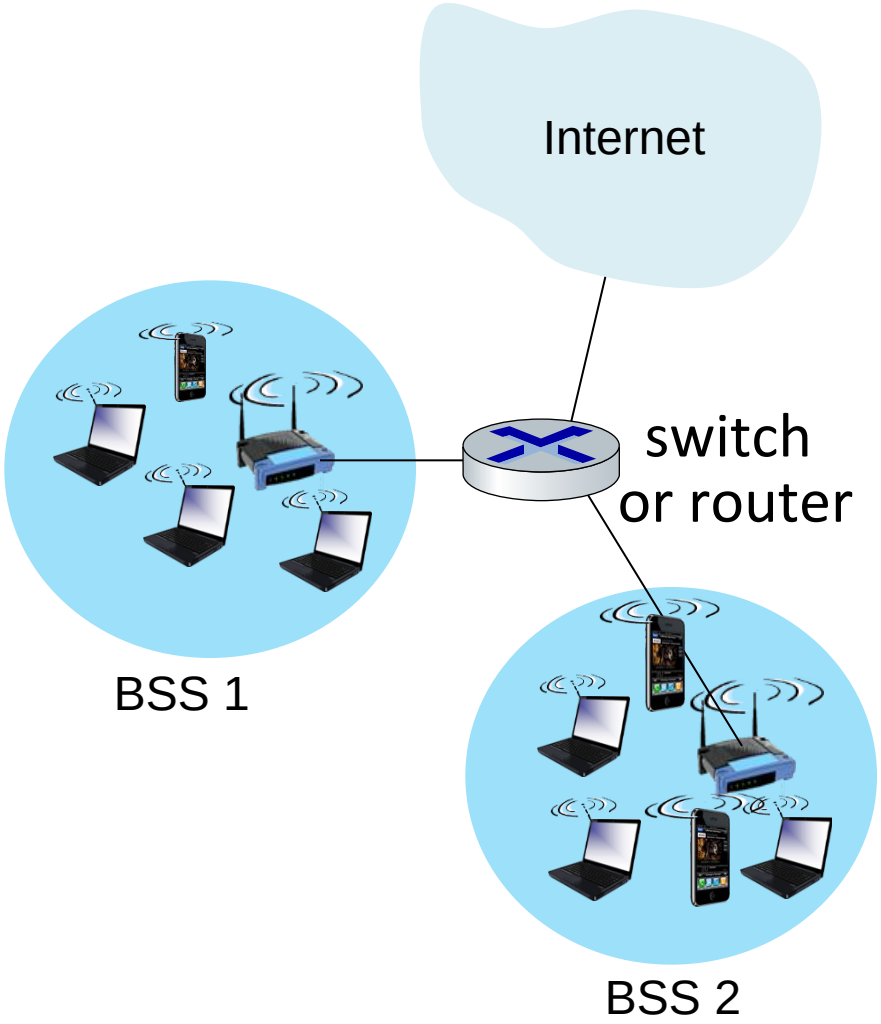
… now *that's* useful!

IEEE 802.11 Wireless LAN

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

- all use CSMA/CA for multiple access, and have base-station and ad-hoc network versions

IEEE 802.11 Wireless LAN Architecture

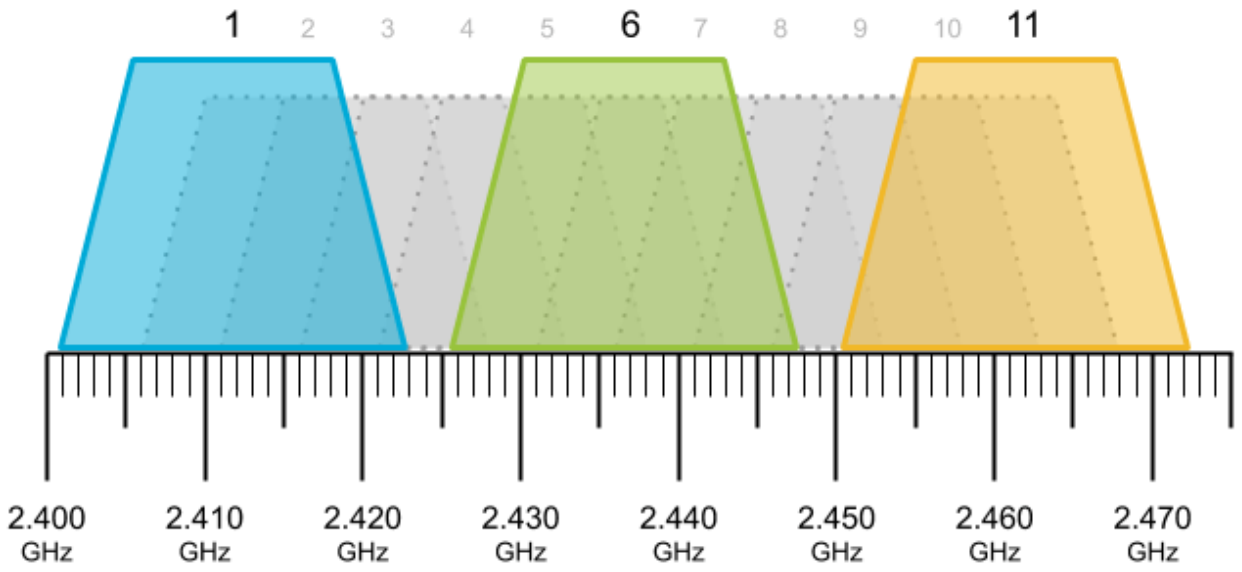


- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

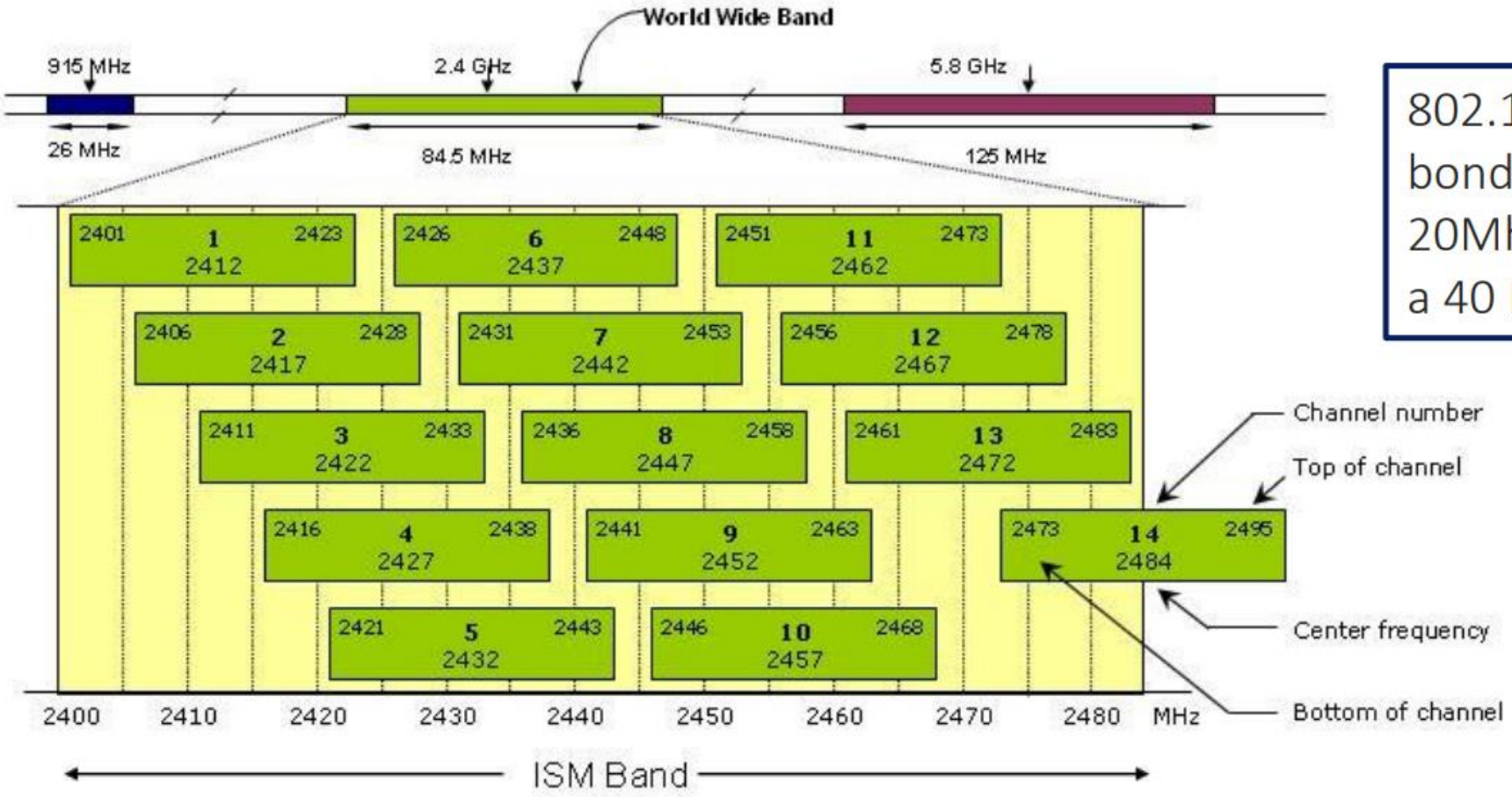
802.11: Channels

- spectrum divided into channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!

Example: 2.4 GHz



802.11: Channels



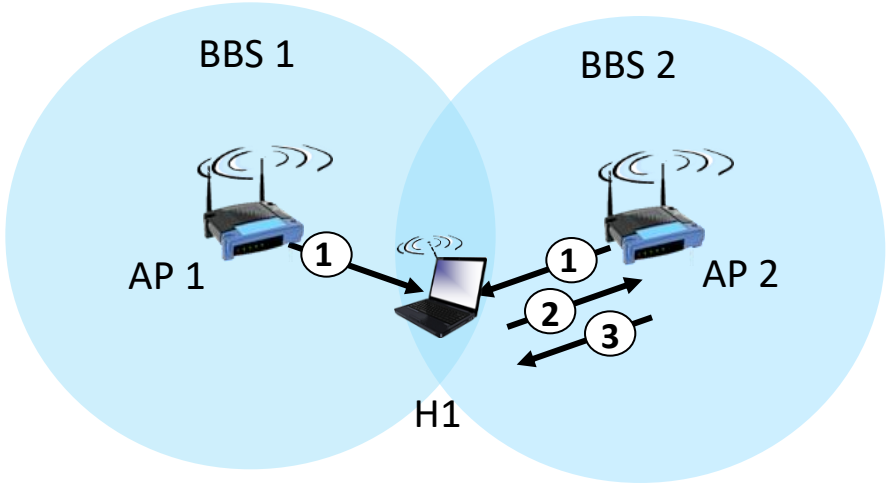
802.11n allows channel bonding, where adjacent 20Mhz channels can form a 40 Mhz channel

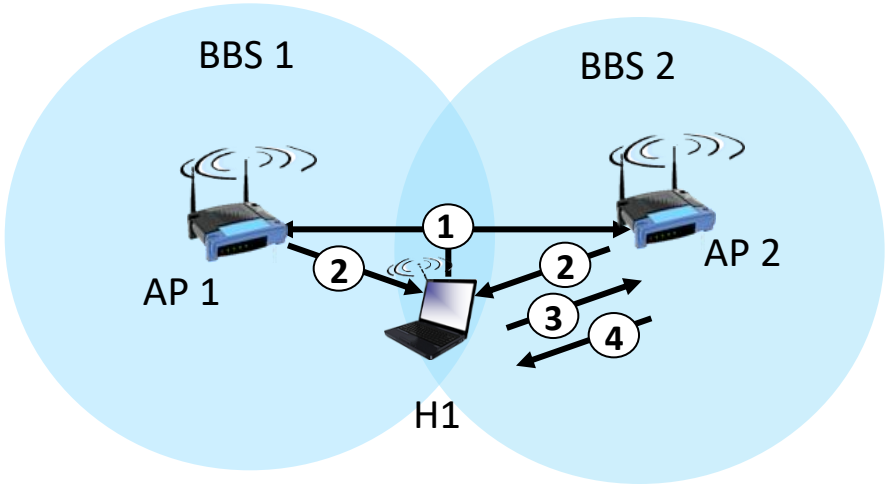
802.11: Association

- arriving host: must associate with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - then may perform authentication
  - then typically run DHCP to get IP address in AP's subnet

BSS

802.11: Association





passive scanning:

(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

active scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

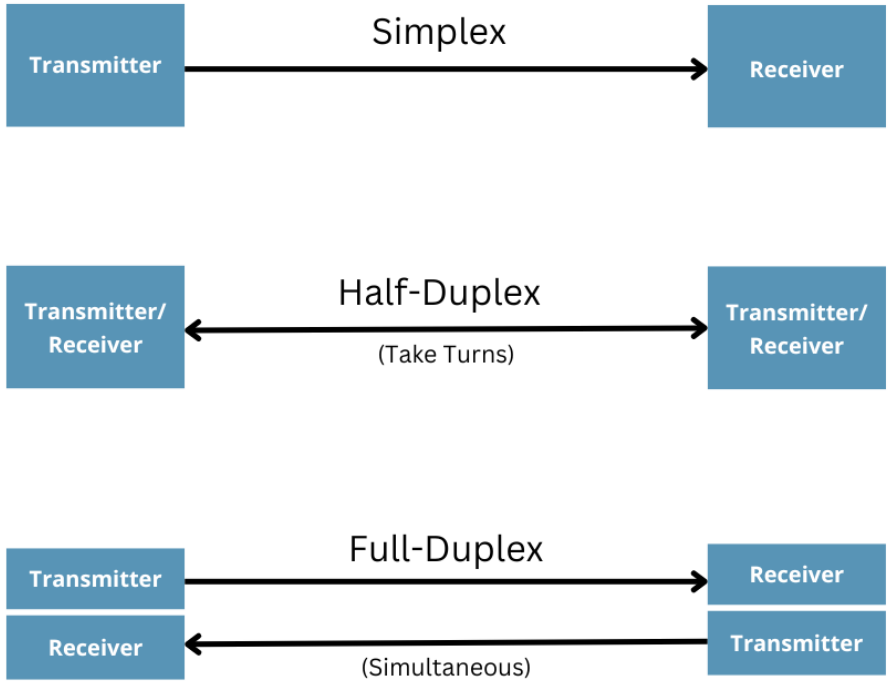
802.11: Association

In (wired) ethernet, we had MAC protocols that would listen on a channel, and only transmit if the channel was empty

- → Requires the ability to **listen** and **transmit** at the same time (full-duplex)

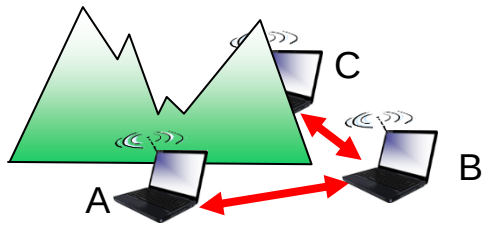
When WiFi begins to transmit a frame, it transmits the frame in its entirety; there is no going back

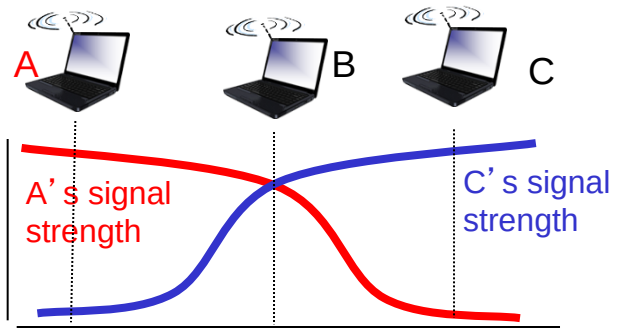
WiFi is not full-duplex, which means it cannot *detect* collisions, so we must *avoid* collisions instead



IEEE 802.11: multiple access

- avoid collisions: 2^+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with detected ongoing transmission by another node
- 802.11: *no* collision detection!
  - difficult to sense collisions: high transmitting signal, weak received signal due to fading
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/CollisionAvoidance





IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

(time to wait before transmitting)

1 if sense channel idle for **DIFS** then
  transmit entire frame (no CD)

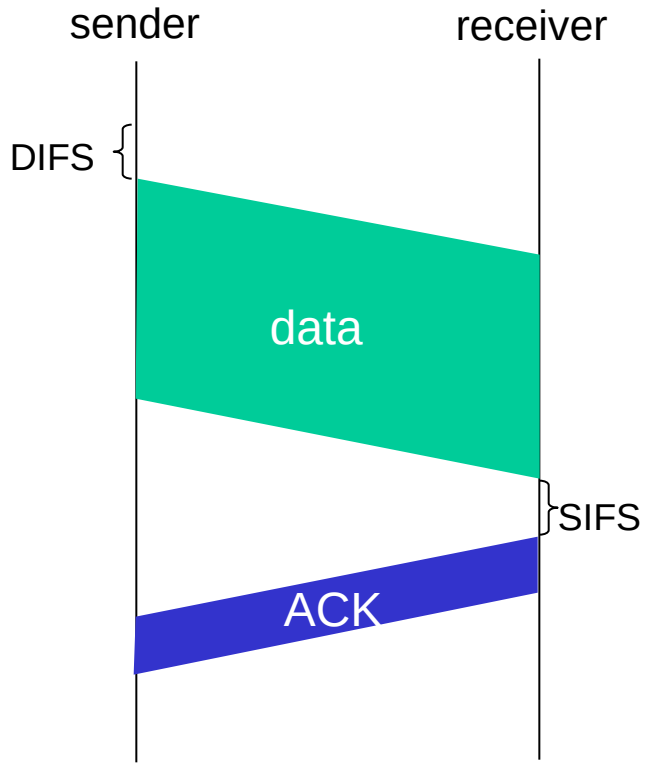
2 if sense channel busy then
  start random backoff time
  timer counts down while channel idle
  transmit when timer expires
  if no ACK, increase random backoff interval, repeat 2

802.11 receiver

if frame received OK
  return ACK after **SIFS** (ACK needed due to hidden terminal problem)

Distributed Inter-frame Space (DIFS)

Short Inter-frame Spacing (SIFS)

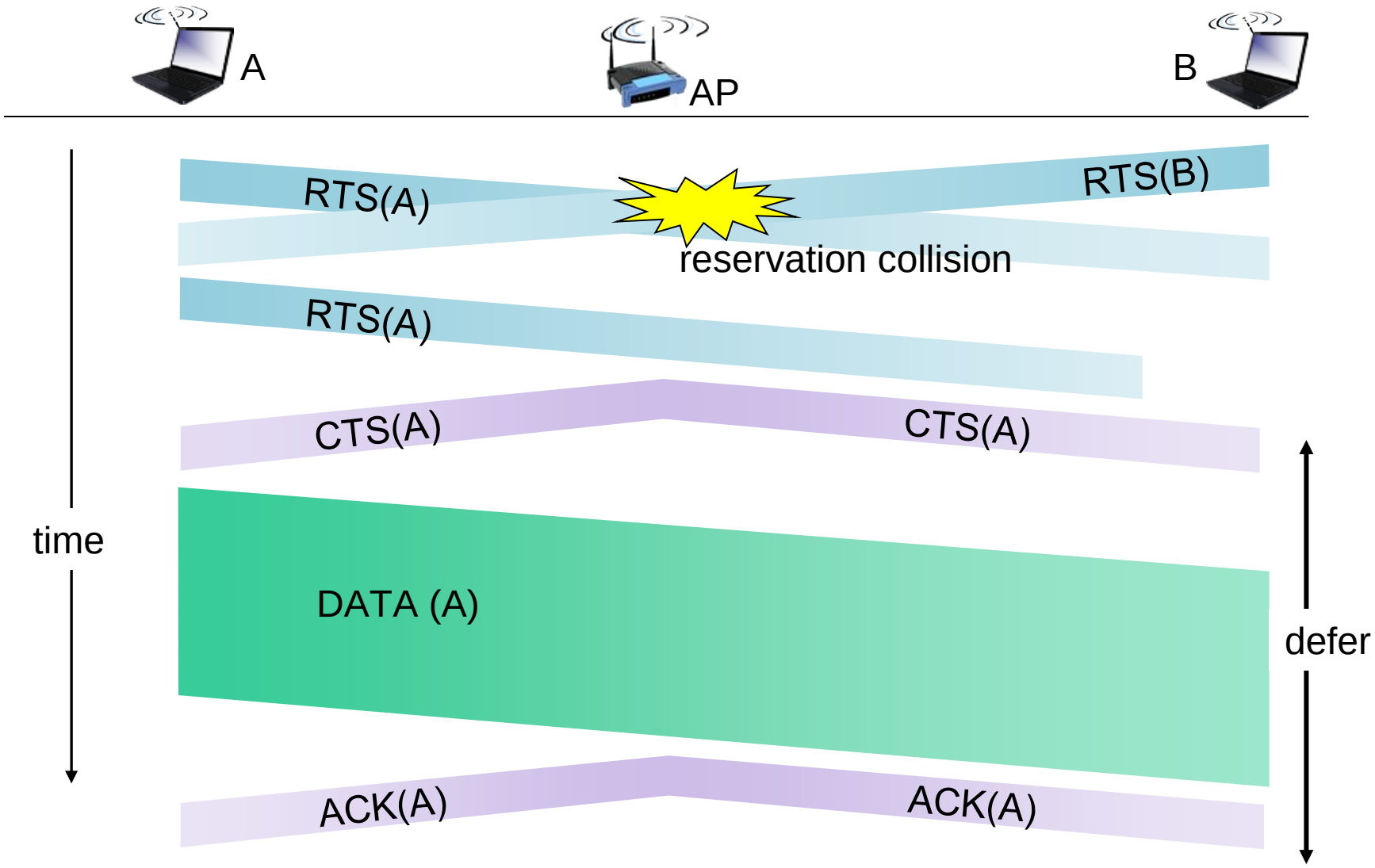


IEEE 802.11 MAC Protocol: CSMA/CA

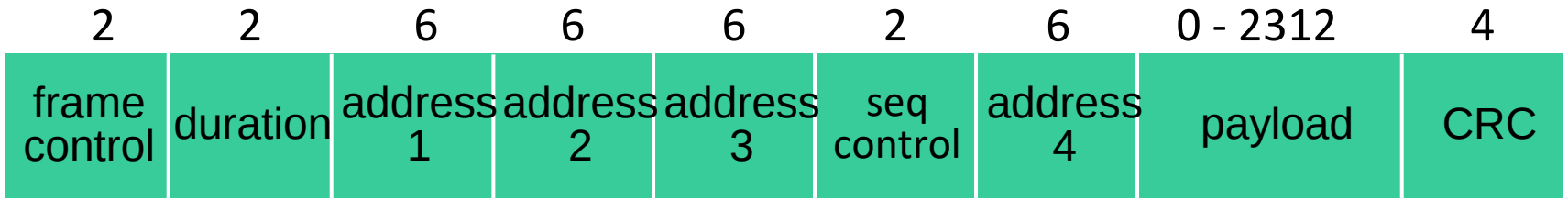
idea: sender "reserves" channel use for data frames using small reservation packets

- sender first transmits *small* request-to-send (RTS) packet to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

IEEE 802.11 MAC Protocol: CSMA/CA



IEEE 802.11 frame: addressing



Address 1: MAC address of wireless host or AP to receive this frame

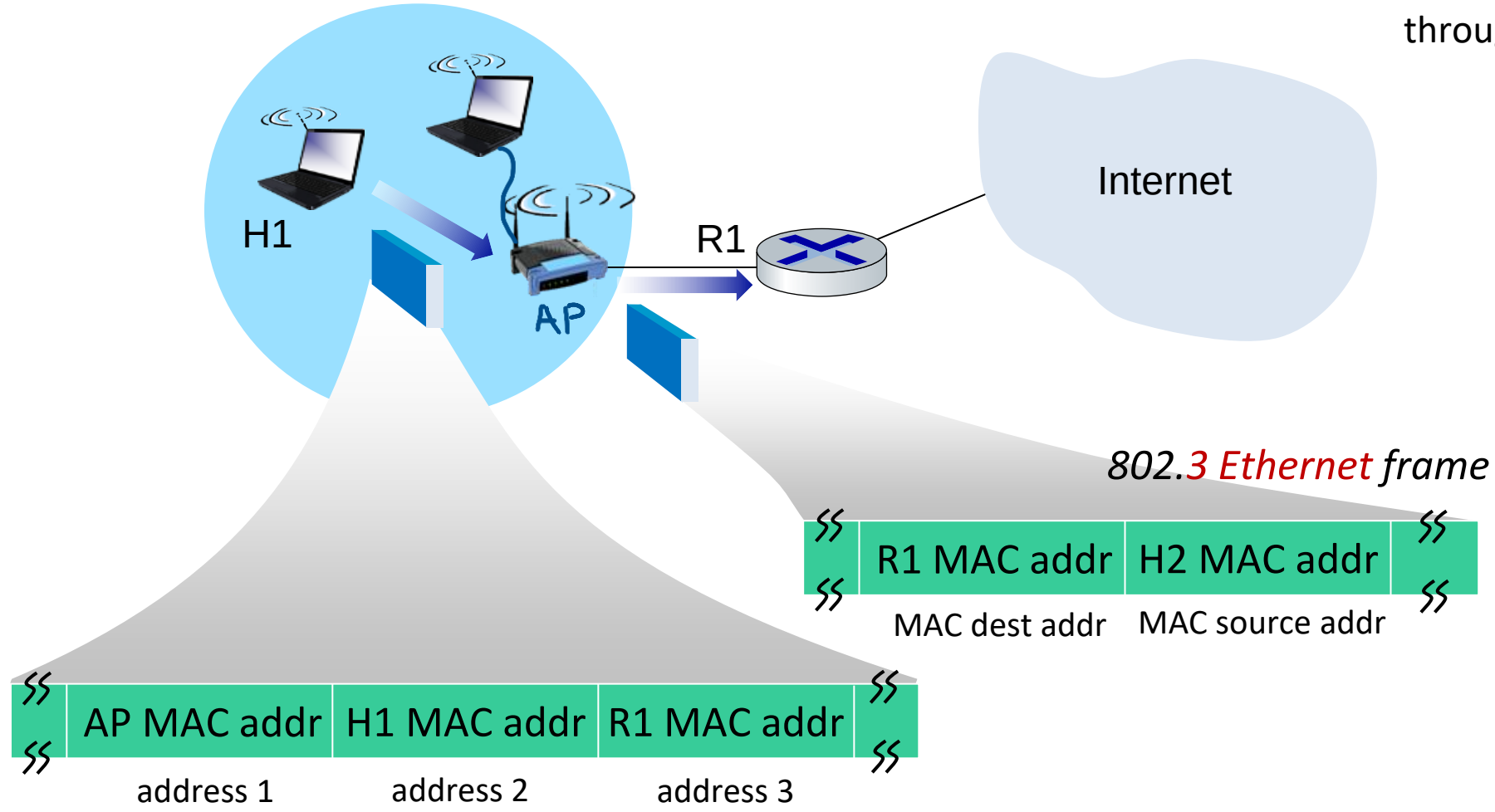
Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

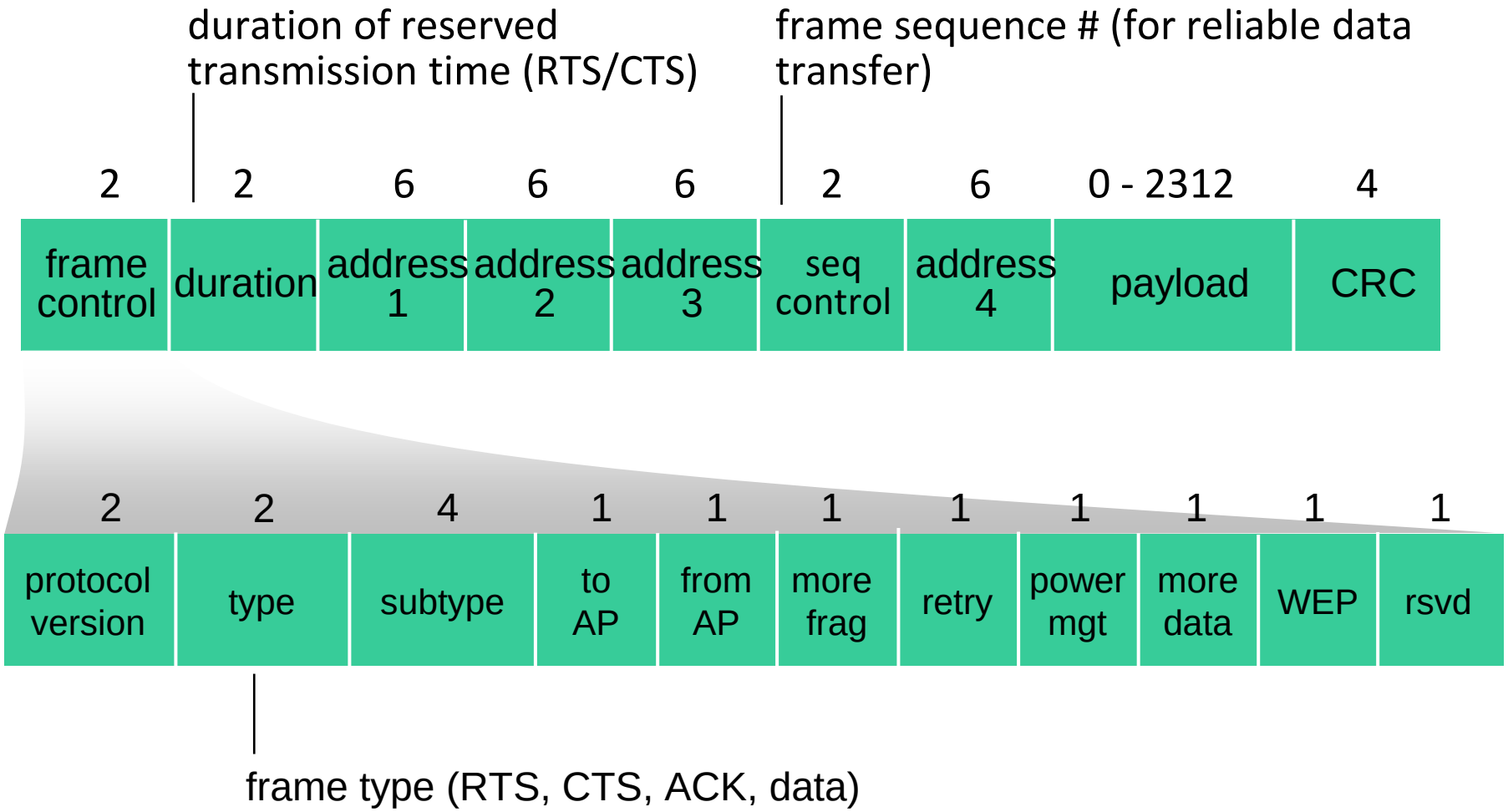
Address 4: used only in ad hoc mode

IEEE 802.11 frame: addressing

Once the AP gets the WiFi frame, it can convert it to a ethernet frame and send it through the main internet



IEEE 802.11 frame: addressing



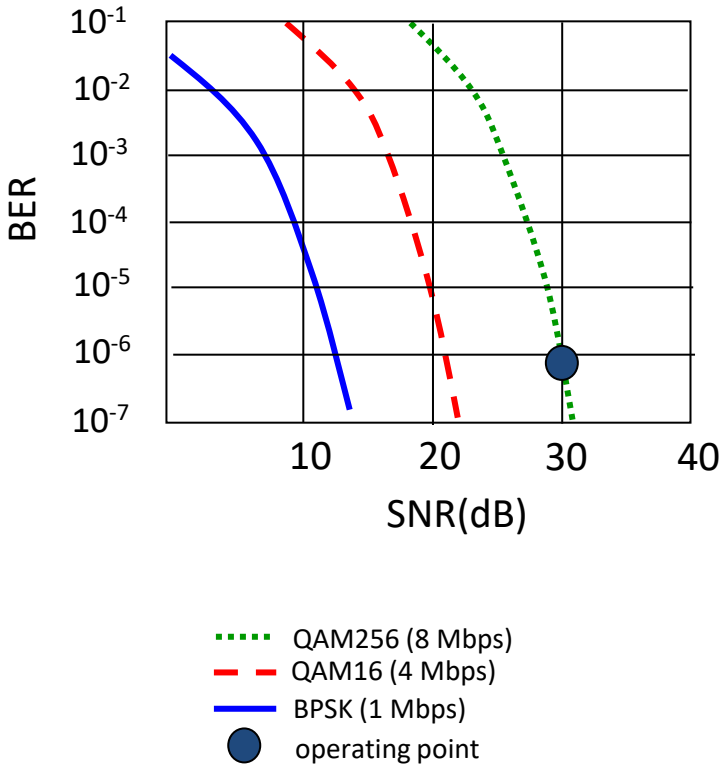
802.11: advanced capabilities

Rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies

1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER



Personal area networks: Bluetooth

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- 2.4-2.5 GHz ISM radio band, up to 3 Mbps
- master controller / client devices:
  - master polls clients, grants requests for client transmissions