

CSCI 466: Networks

Wireless Networks, WiFi, Cellular Networks (4G/5G)

Reese Pearsall
Fall 2022

Announcements

PA3 Due Friday @ 11:59 PM

HW4 Posted, due Friday December 9th @ 11:59 PM

Final Exam Study Guide Posted

Intrusion Detection System

An **intrusion detection system (IDS)** will generate an alert when potentially malicious traffic is observed

Two types –

1. Signature-Based Detection Systems

Maintain a large database of **known** “signatures” for malicious packets

- Malicious IP addresses or URLs
- Email Addresses
- Specific String of Bits
- File/Message Hashes
- Protocol Specific (nmap)

When would signature-based detection **not work** ?

Signature-based detection will never work for **new threats**, so we need a way to dynamically analyze threats

2. Anomaly-based Detection System

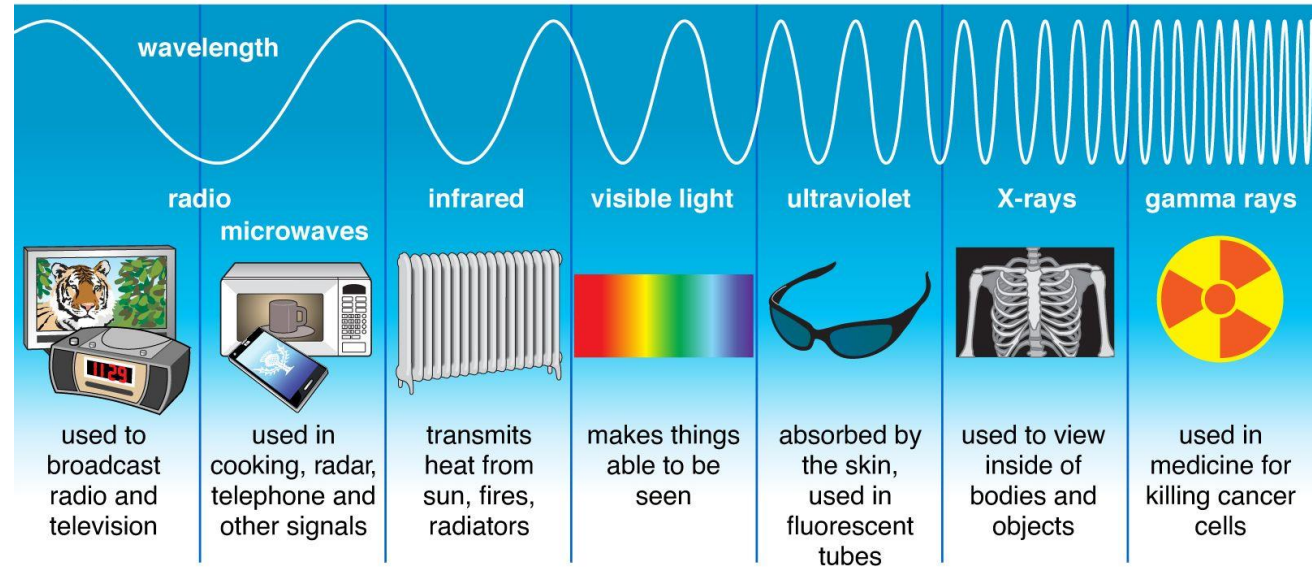
If you know what “normal” traffic looks like, you can identify unusual, potentially malicious traffic

You get a large spike in ICMP packets? Someone might be trying to NMAP you

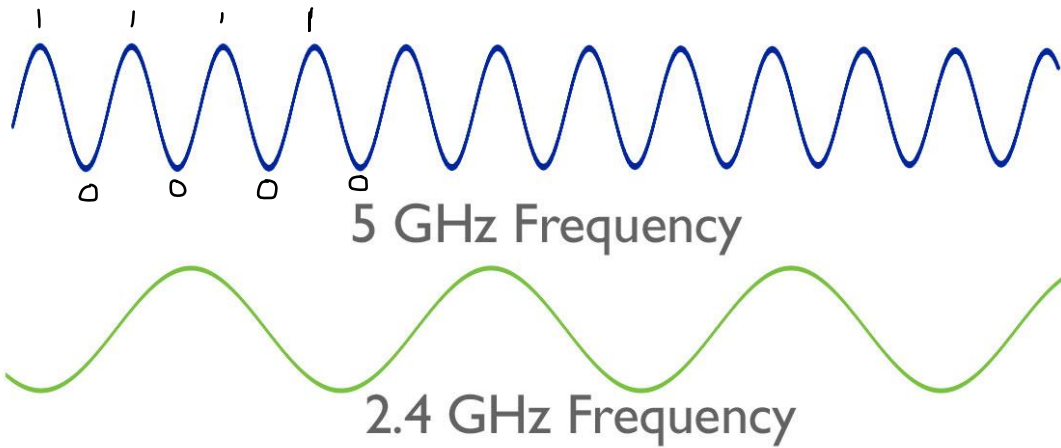
Wireless Networks

Transmission Medium = waves in the air

Types of Electromagnetic Radiation



© Encyclopædia Britannica, Inc.



We can transmit waves at different **frequencies**

UNITED STATES FREQUENCY ALLOCATIONS THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND

AERONAUTICAL MOBILE	INTER-SATELLITE	RADIO ASTRONOMY
AERONAUTICAL MOBILE SATELLITE	LAND MOBILE	RADIO DETERMINATION SATELLITE
AERONAUTICAL RADIO NAVIGATION	LAND MOBILE SATELLITE	RADIOLOCATION
AMATEUR	MARITIME MOBILE	RADIOLOCATION SATELLITE
AMATEUR SATELLITE	MARITIME MOBILE SATELLITE	RADIO NAVIGATION
BROADCASTING	MARITIME RADIO NAVIGATION	RADIO NAVIGATION SATELLITE
BROADCASTING SATELLITE	METEOROLOGICAL AID	SPACE OPERATION
EARTH EXPLORATION SATELLITE	METEOROLOGICAL SATELLITE	SPACE RESEARCH
FIXED	MOBILE	STANDARD FREQUENCY AND TIME SIGNAL
FIXED SATELLITE	MOBILE SATELLITE	STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

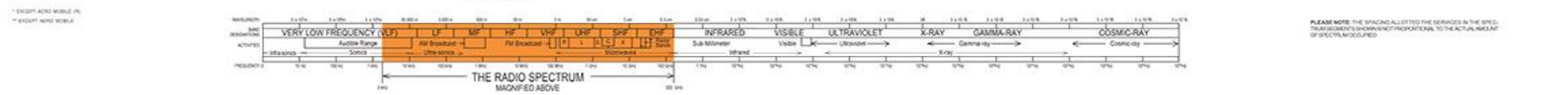
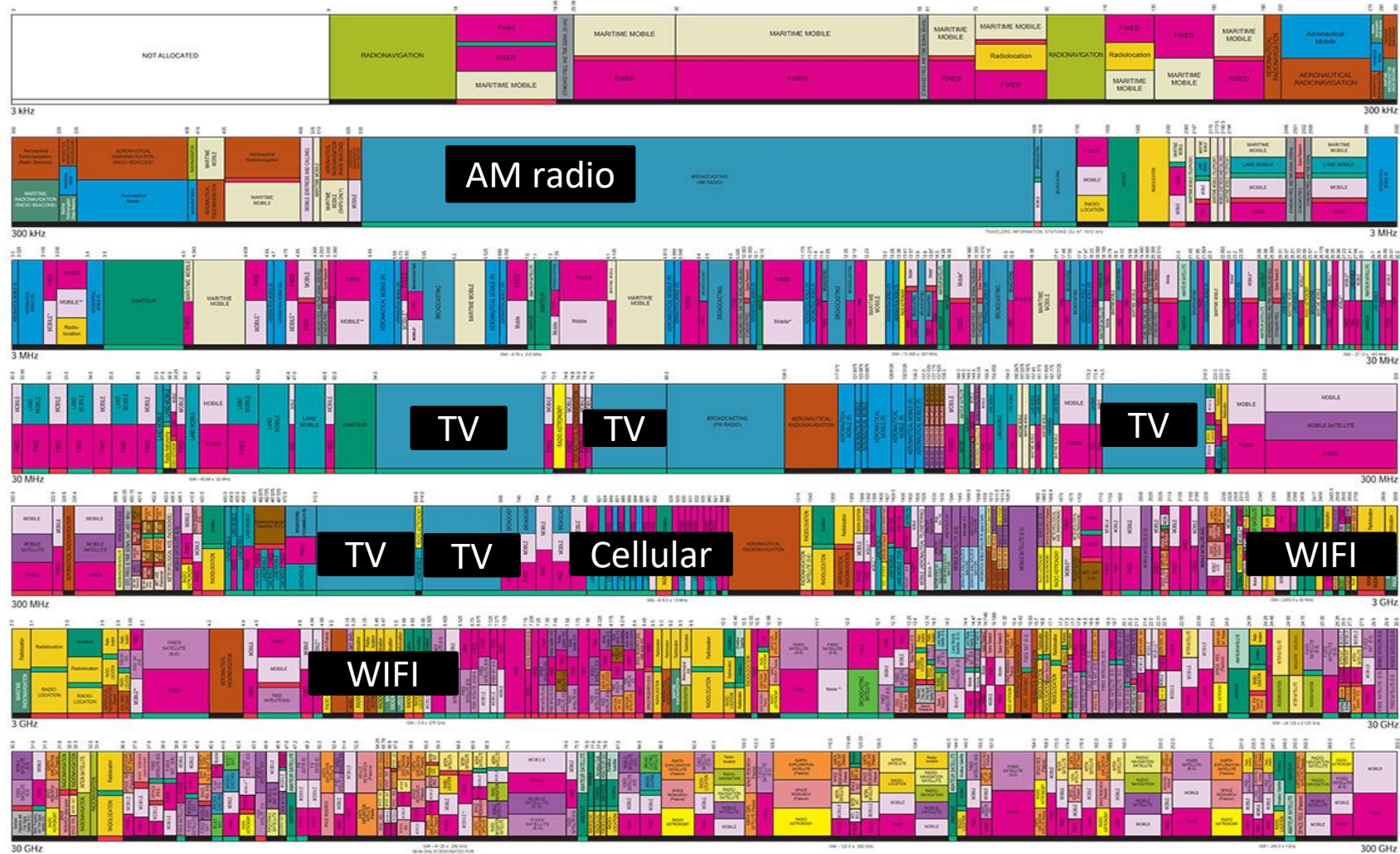
ACTIVITY CODE

GOVERNMENT EXCLUSIVE	GOVERNMENT/NON-GOVERNMENT SHARED
NON-GOVERNMENT EXCLUSIVE	

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

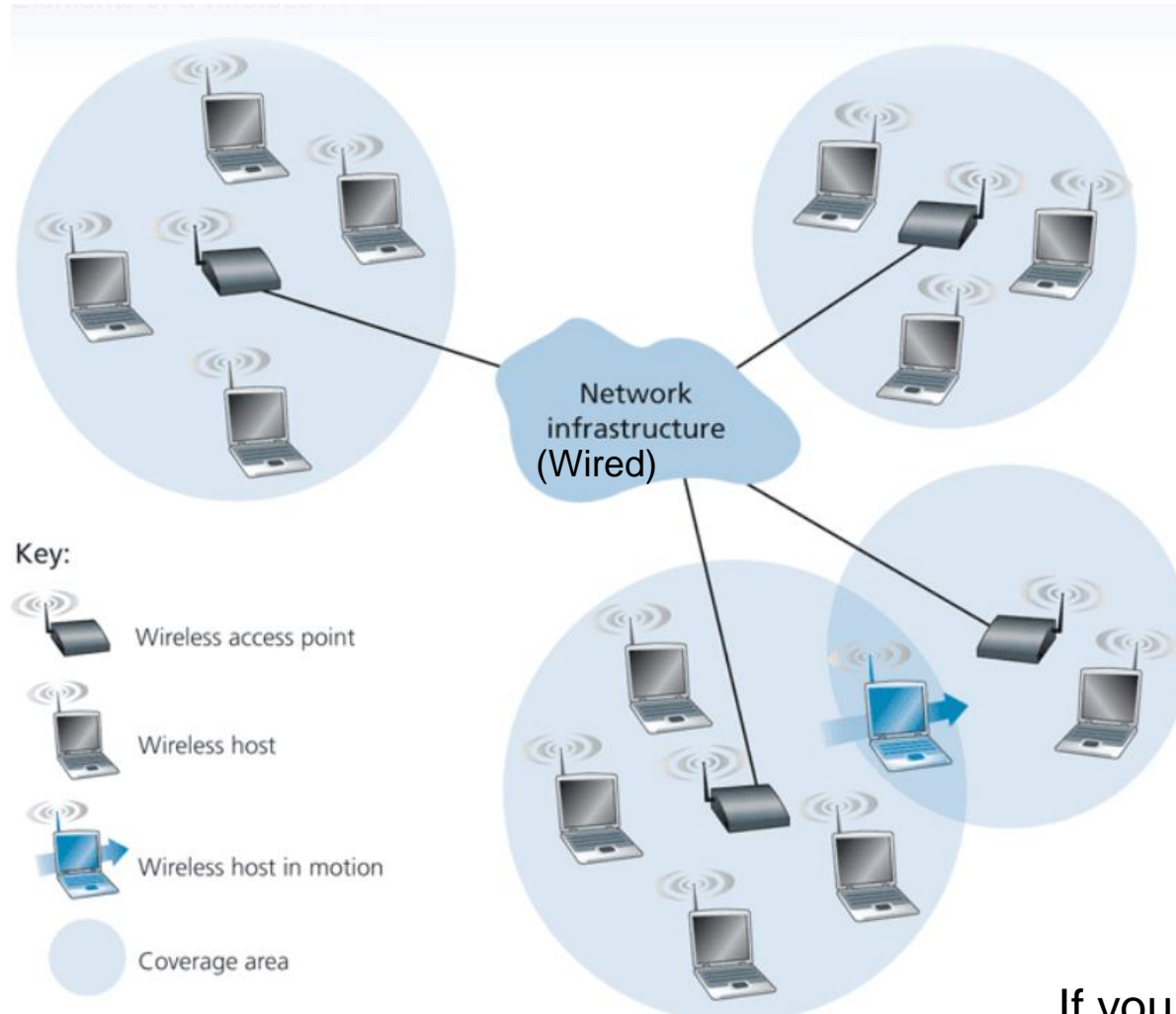
This chart is a graphic representation of the Table of Frequency Allocations used by the FCC and is not a substitute for the Table of Frequency Allocations. It does not contain all the information contained in the Table of Frequency Allocations. For complete information, users should consult the Table to determine the current status of U.S. allocations.



PLEASE NOTE: THE SPACING BETWEEN THE SERVICES IN THE SPECTRUM CHART IS NOT PROPORTIONAL TO THE ACTUAL AMOUNT OF SPECTRUM OCCUPIED.

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

Anatomy of a Wireless Network

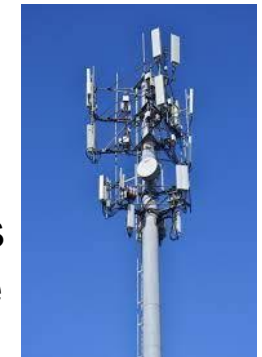


Wireless networks are an *extension* of the standard internet, and usually only occur at the *network edge*

Wireless hosts are devices that require a wireless connection (laptop, cell phone, IoT, Bluetooth)
This can be mobile, or stationary

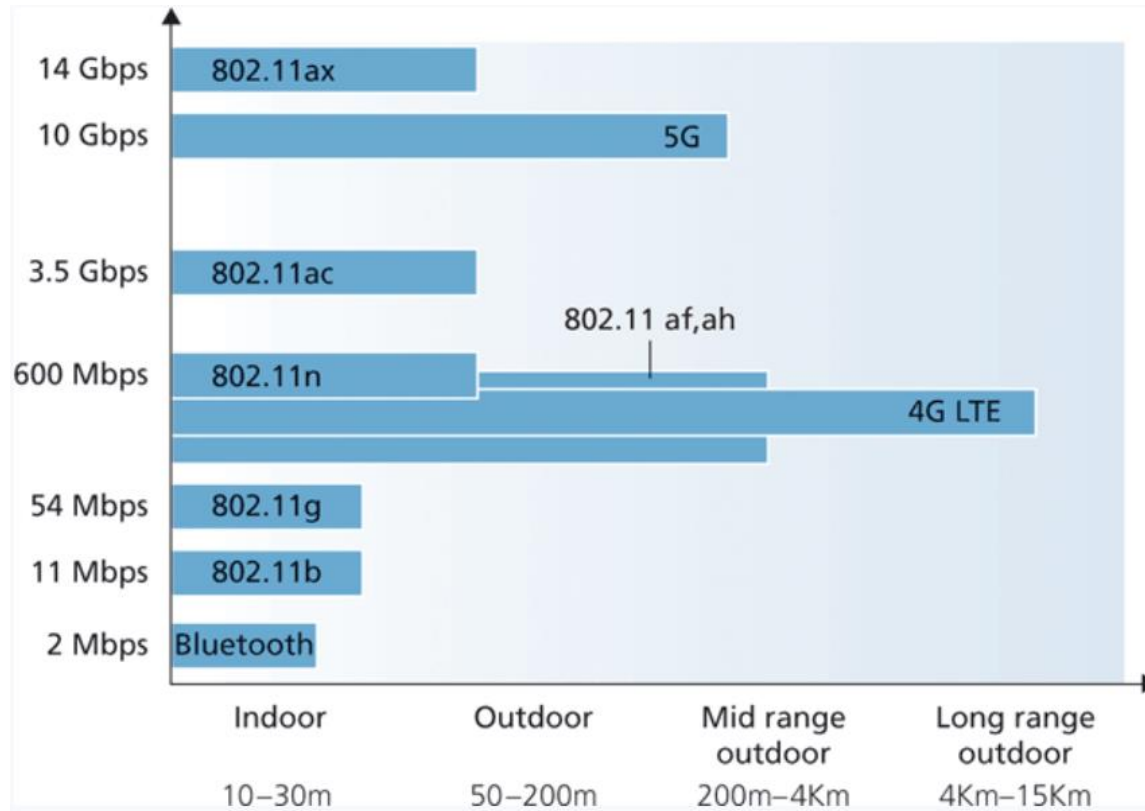
Wireless hosts connect to a **wireless access point** that will connect them to the greater internet.
Typically linked to a geographic location

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

Wireless Network Tradeoffs



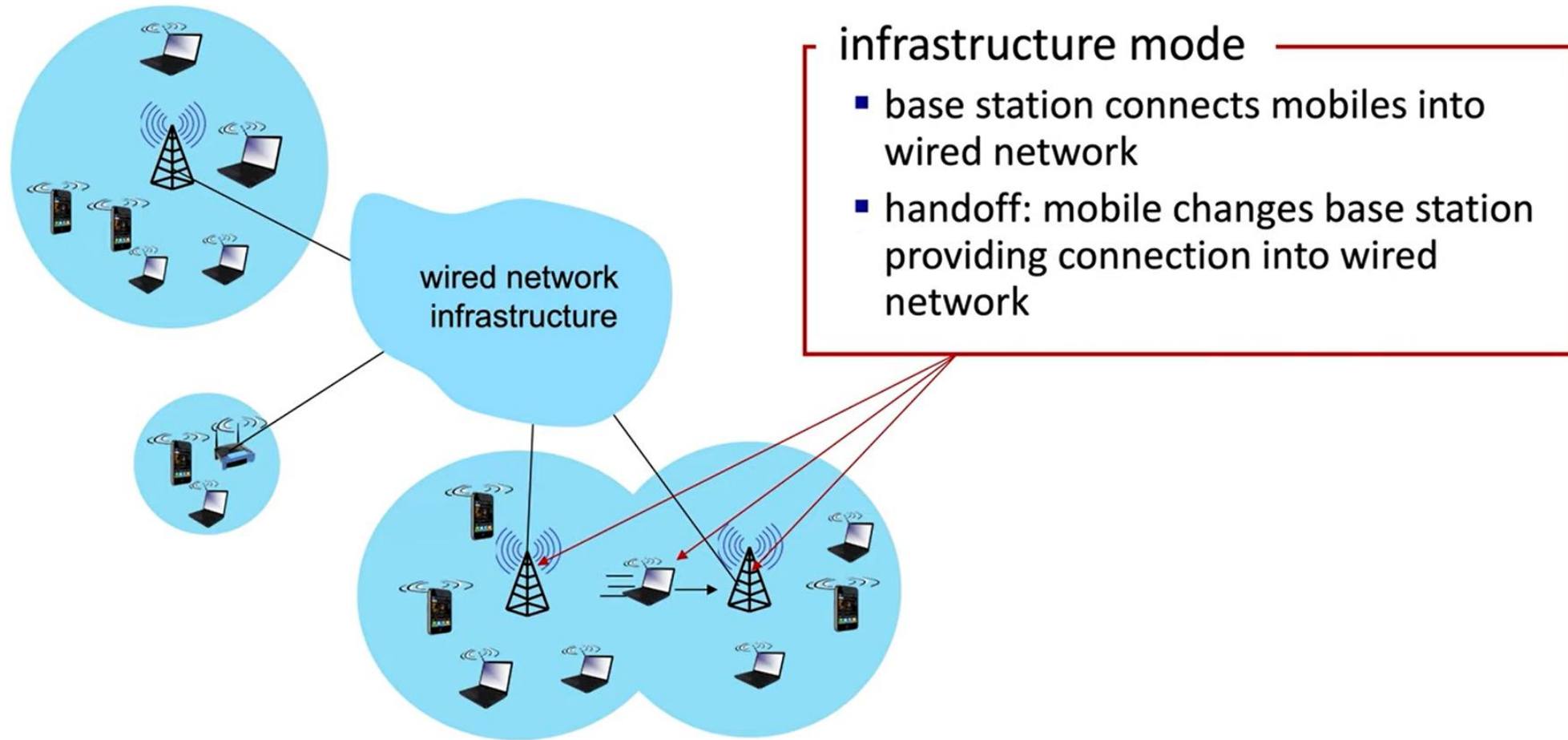
In wireless networks, we see a **tradeoff** between throughput, and effective range

Easier 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

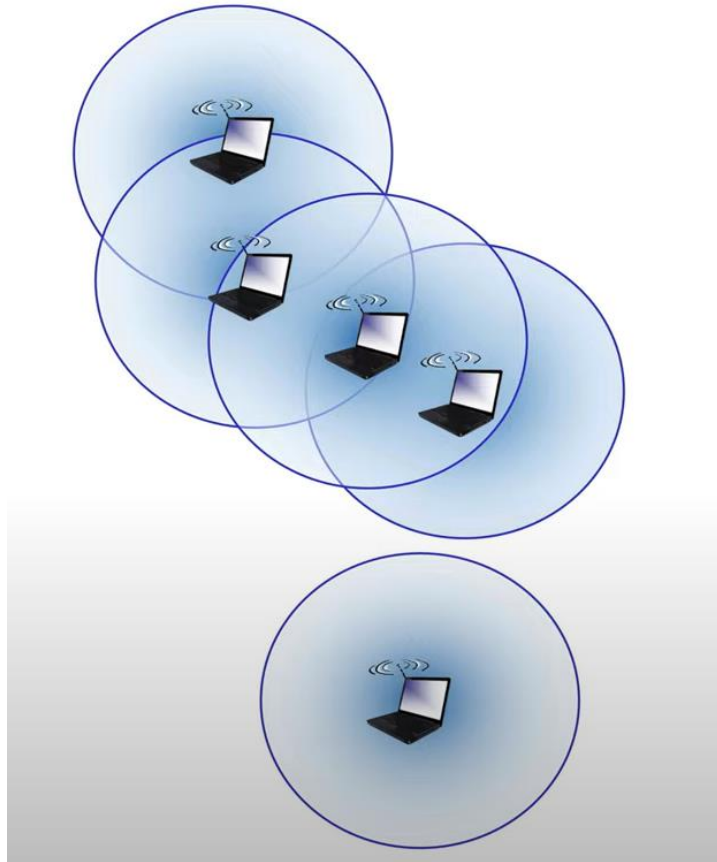
Wireless Network Tradeoffs



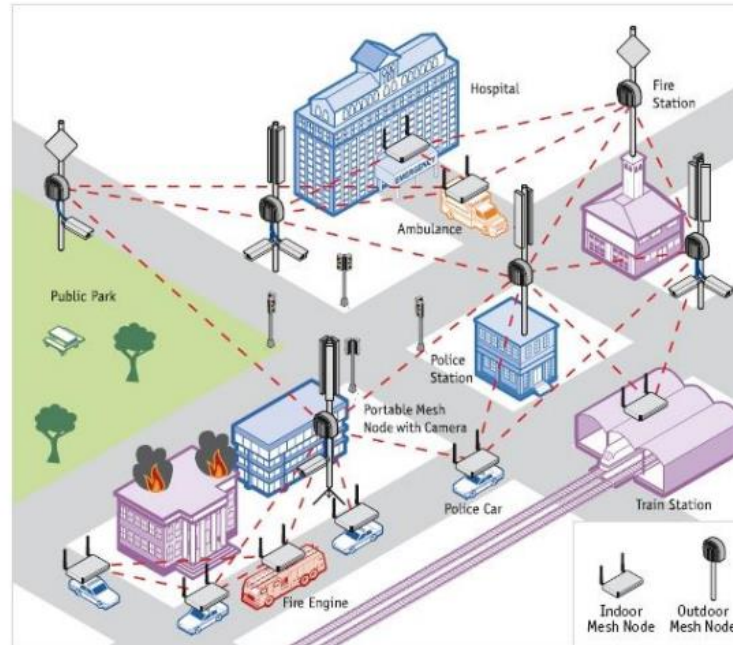
Wireless Network Structure

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

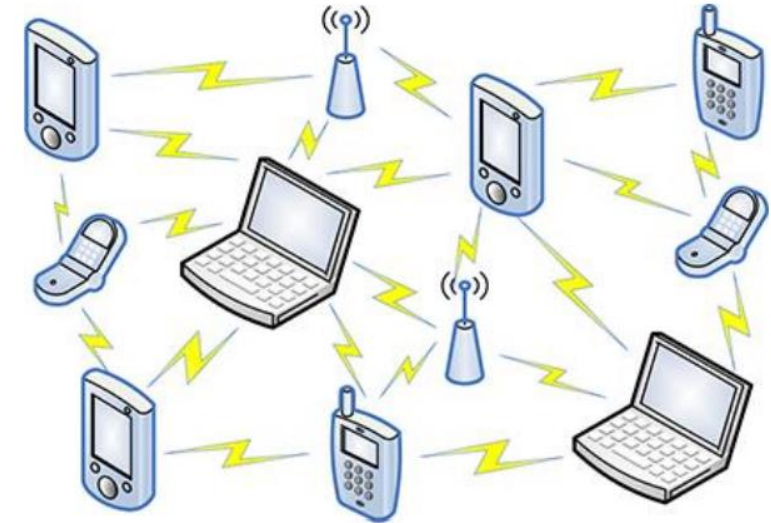


Mesh (Ad Hoc) Mode



Nodes themselves must provide services such as DNS and DHCP

Mobile Ad Hoc Nets (MANETs)



No central administration

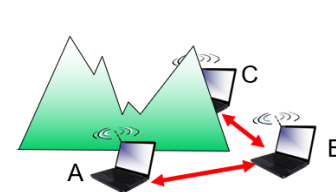
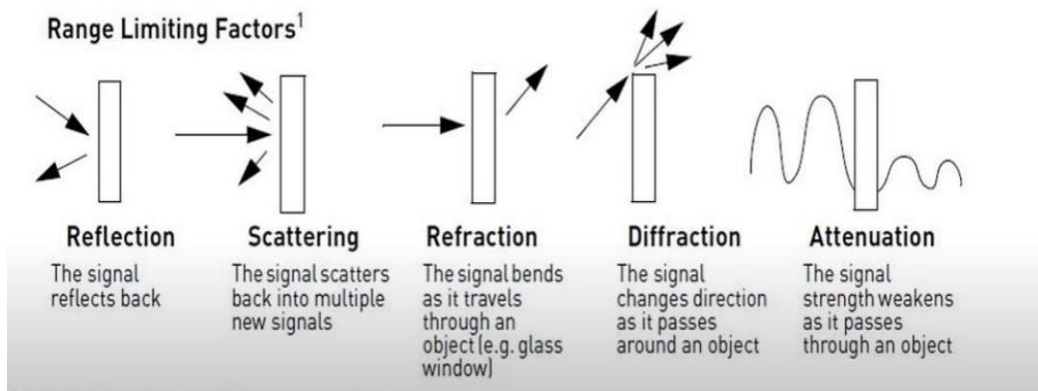
This is advantageous where infrastructure may be damaged or not available

	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: <i>mesh net</i>
<i>no infrastructure (ad hoc)</i>	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

Important differences from wired link...

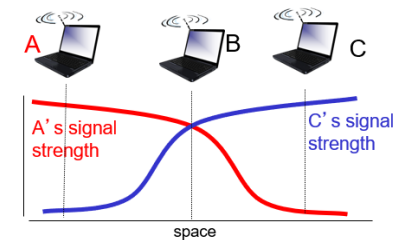
- **Decreased signal strength:** radio signal attenuates as it propagates through matter (path loss)
- **Interference from other sources:** wireless network frequencies (such as 2.4 ghz) shared by many devices will cause interferences
- **Multipath propagation:** radio signal reflects off objects ground,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

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 (good thing)

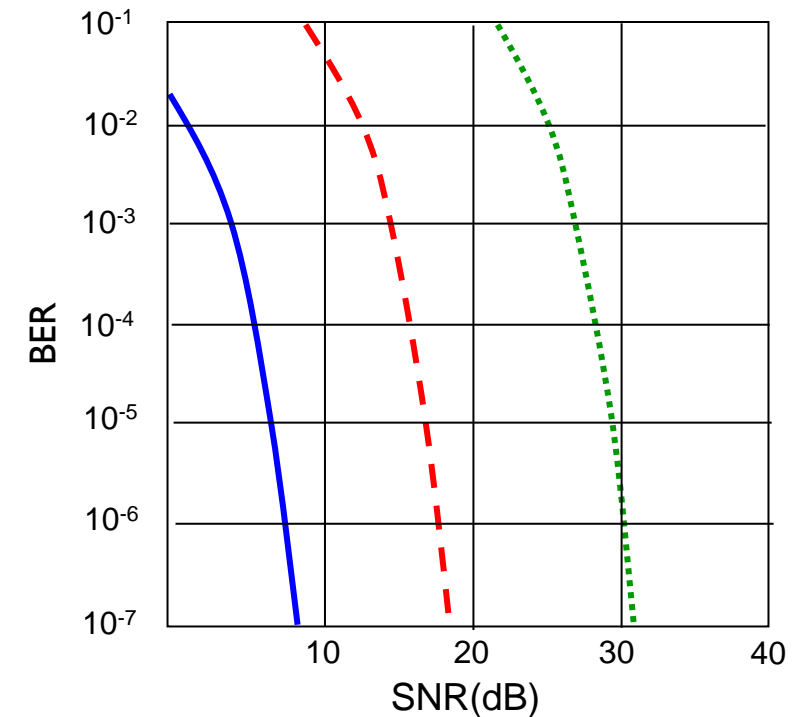
BER: Bit Error Rate

→ 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

Some BER is acceptable... remember that we do always have error checking happening at link layer/transport layer

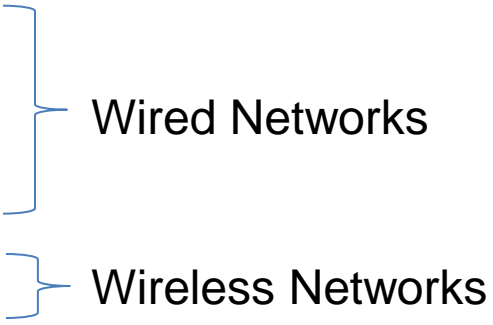


..... QAM256 (8 Mbps)

- - - QAM16 (4 Mbps)

— BPSK (1 Mbps)

Shared Broadcast

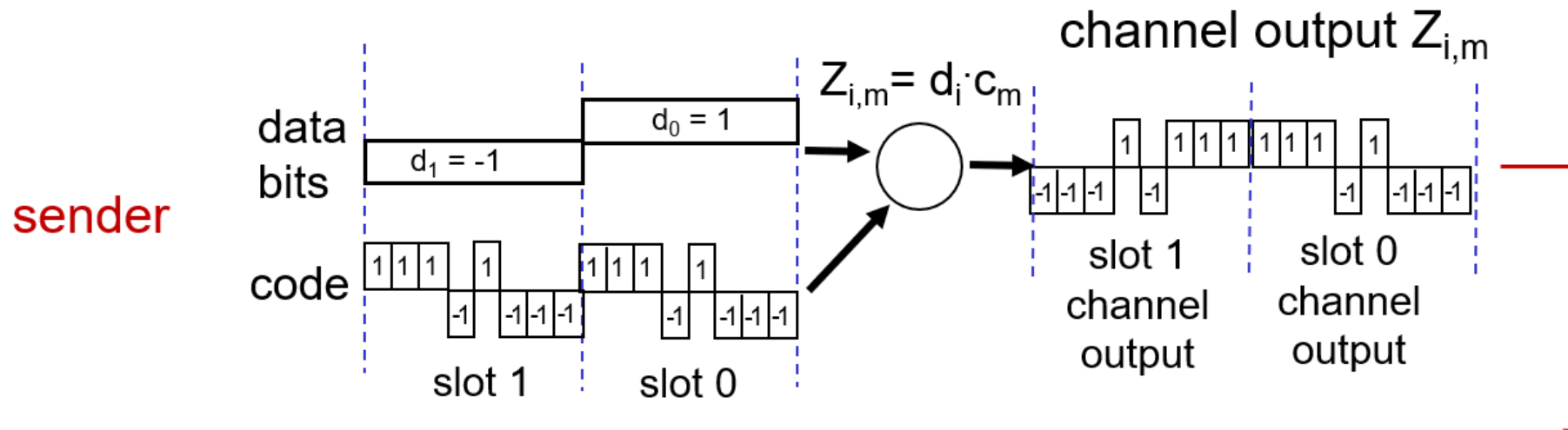
- Because wireless networks are sharing a medium/frequency, we need mechanisms for **sharing bandwidth** so that collisions don't occur
 - In the link layer we have three types
 - 1. **TDMA** (Time division Multiple Access)
 - 2. **FDMA** (Frequency Division Multiple Access)
 - 3. **CDMA** (Code Division Multiple Access)
- 
- The diagram uses blue curly braces to group the three access methods. A large brace on the right side of the first two items (TDMA and FDMA) is labeled 'Wired Networks'. A smaller brace on the right side of the third item (CDMA) is labeled 'Wireless Networks'.

CDMA (Code Division Multiple Access)

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

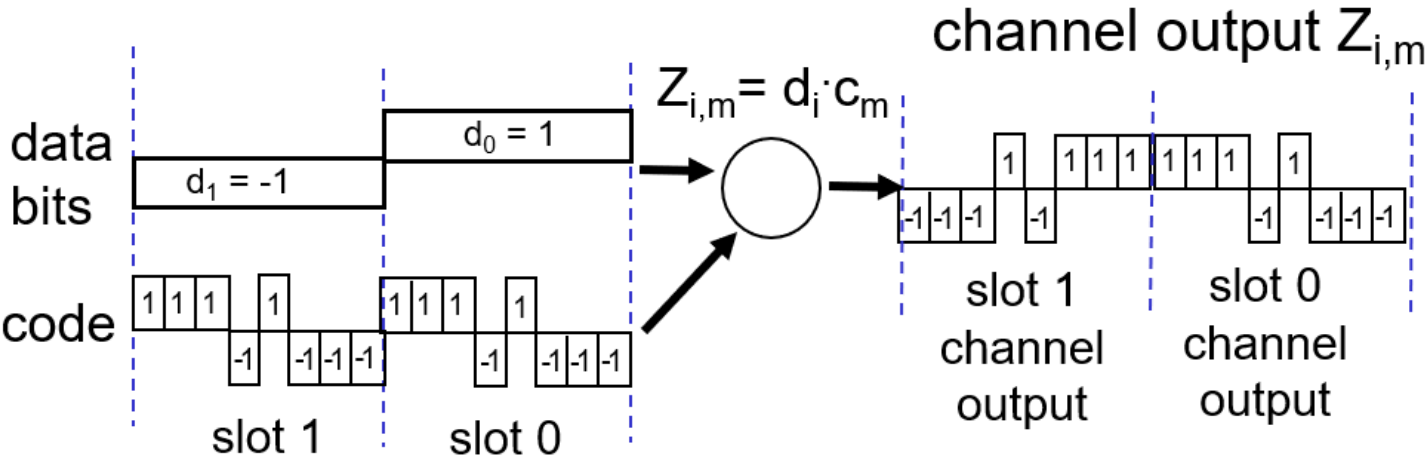
In a CDMA protocol, each bit being sent is encoded by multiplying the bit by a signal (the code)

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



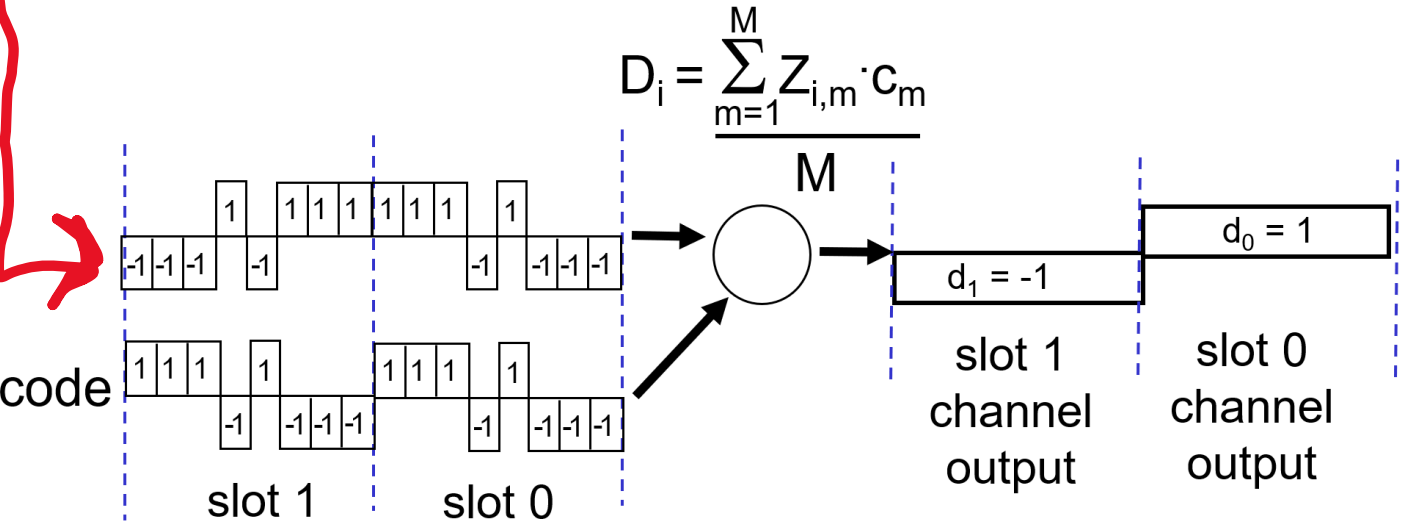
CDMA (Code Division Multiple Access)

sender

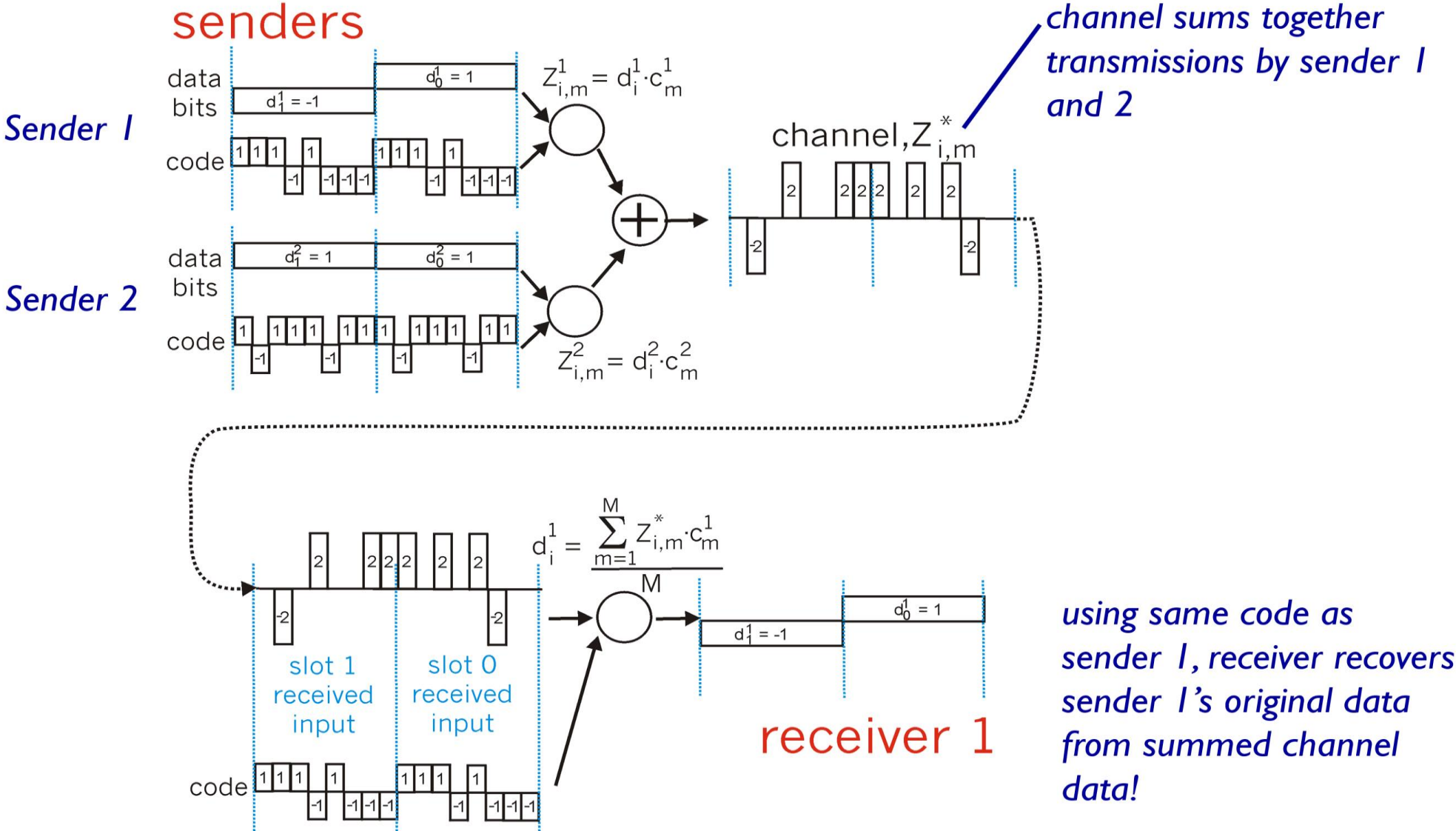


received input

receiver



CDMA (Code Division Multiple Access)



802.11 (Wifi) (Wireless LANs)

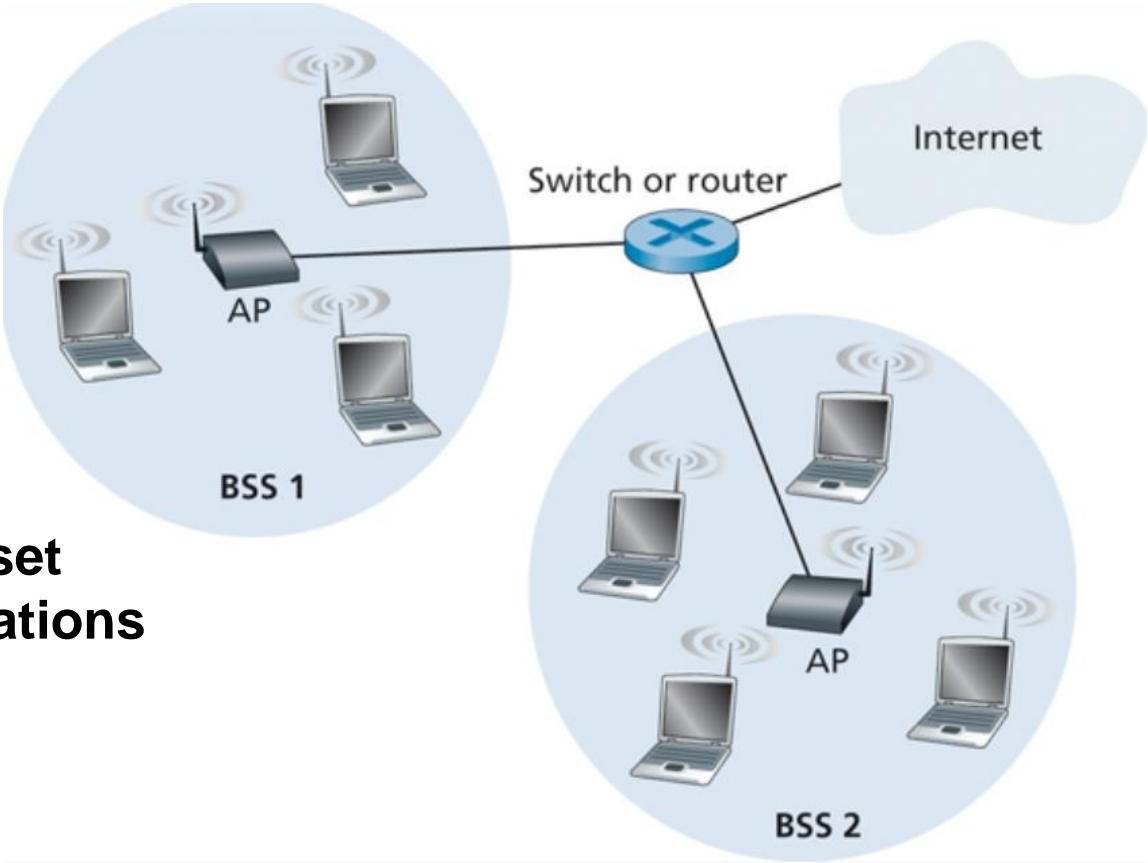
IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11 b	1999	11 Mbps	30 m	2.4 Ghz
802.11 g	2003	54 Mbps	30 m	2.4 Ghz
802.11 n (WiFi 4)	2009	600	70 m	2.4, 5 Ghz
802.11 ac (WiFi 5)	2013	3.47 Gpbs	70 m	5 Ghz
802.11 ax (WiFi 6)	2020 (expected)	14 Gbps	70 m	2.4, 5 Ghz
802.11 af	2014	35–560 Mbps	1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

802.11 architecture consists of a **basic service set (BSS)**. A BSS contains one or more **wireless stations** and an **access point**

Identified by **Service Set Identifier (SSID)**

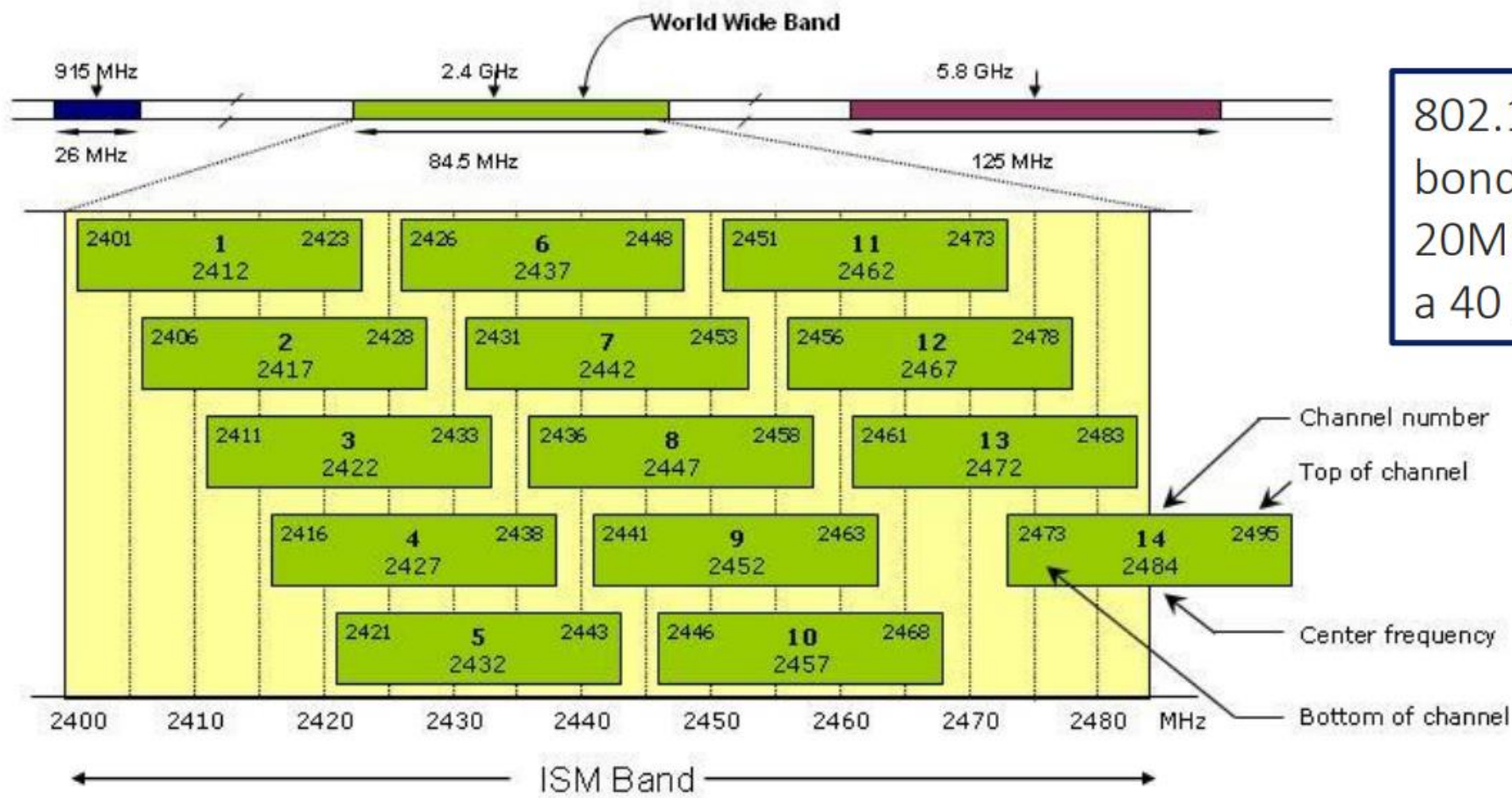


We could also have an 802.11 ad hoc network



- ❑ 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
 - AP admin chooses frequency for AP
 - interference possible: channel can be same as that chosen by neighboring AP!
- ❑ 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
 - may perform authentication [Chapter 8]
 - will typically run DHCP to get IP address in AP's subnet

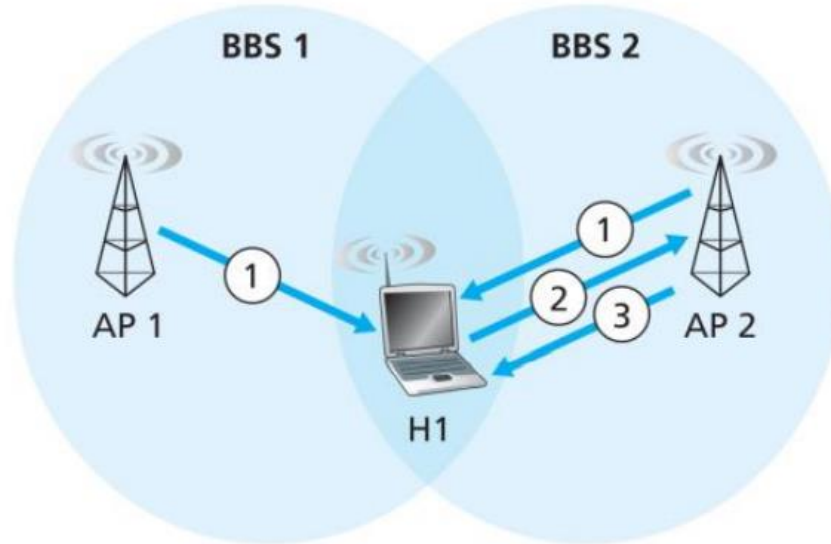
802.11 (Wifi) (Wireless LANs)



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

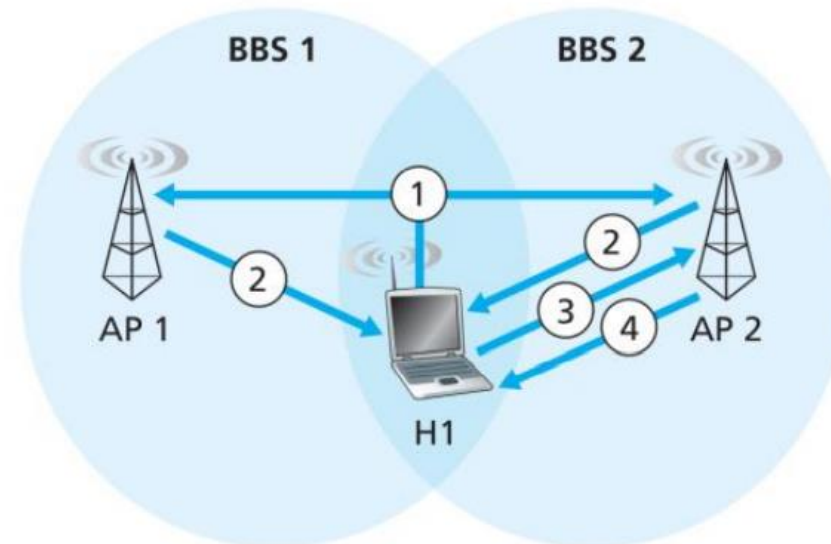
Establishing Connectivity

Passive Scanning



1. Beacon frames sent from APs
2. Association Request frame sent:
H1 to selected AP 2
3. Association Response frame sent:
Selected AP 2 to H1

Active Scanning



1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP 2
4. Association Response frame sent: Selected AP 2 to H1

Useful for hiding APs – need to know SSID to beacon

347

New devices will be allowed to join the network typically after authentication (password, username/password, MAC address, Captcha)

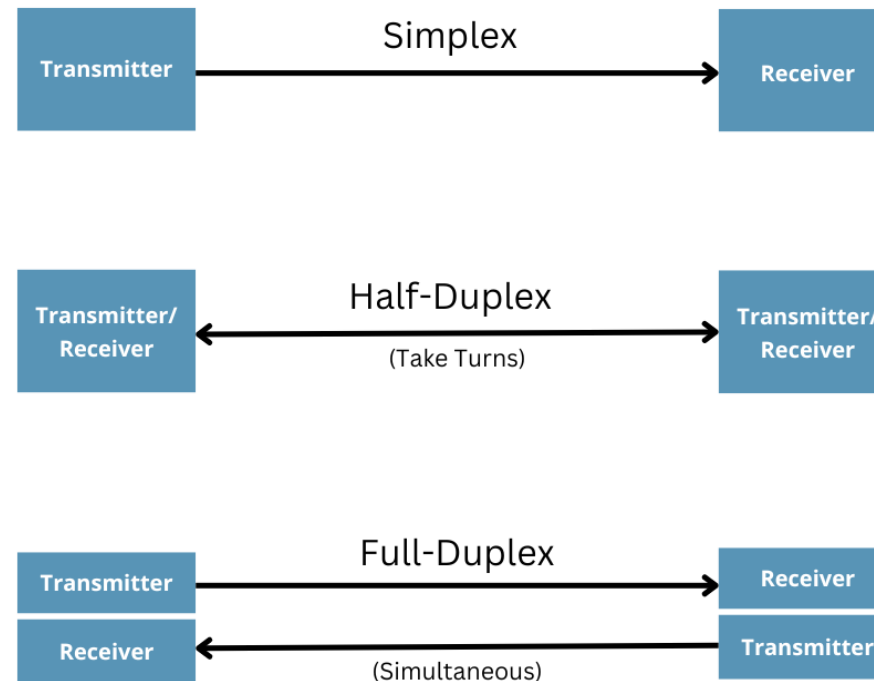
Collision Detection/Avoidance in 802.11

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



Collision Detection/Avoidance in 802.11

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

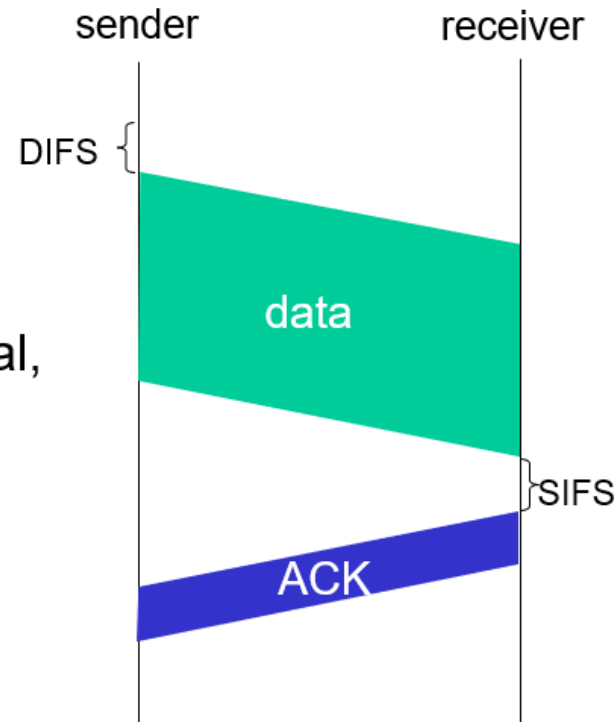
WiFi uses Carrier-Sense Multiple Access with Collision Avoidance (**CSMA/CA**)

802.11 sender

- 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)

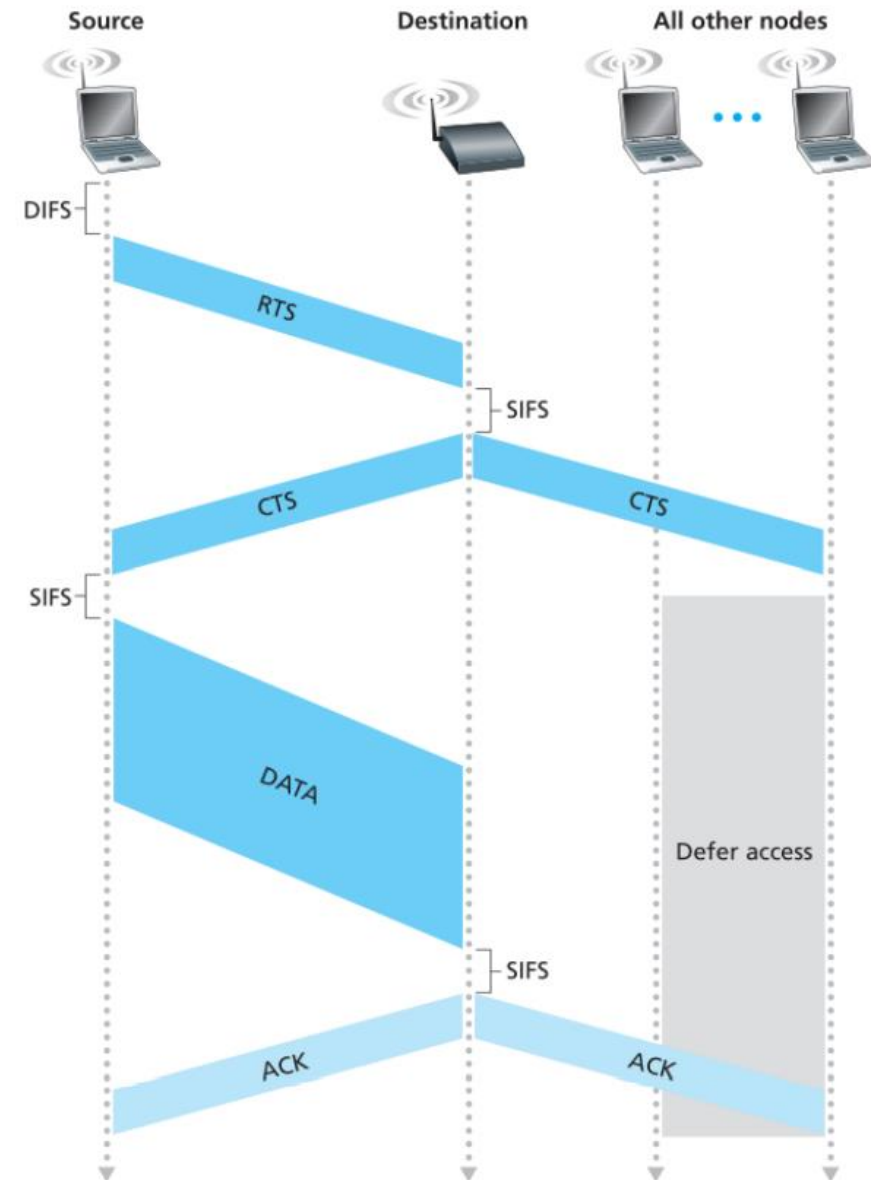


Introduces ACKs at a link-layer level

Distributed Inter-frame Space (DIFS)

Short Inter-frame Spacing (SIFS)

Collision Detection/Avoidance in 802.11



The sender first transmits a **request to send (rts)** frame

If the AP is free, then it will send back a **clear to send (cts)** packet

The AP denies access to all other nodes until the AP sends an ACK

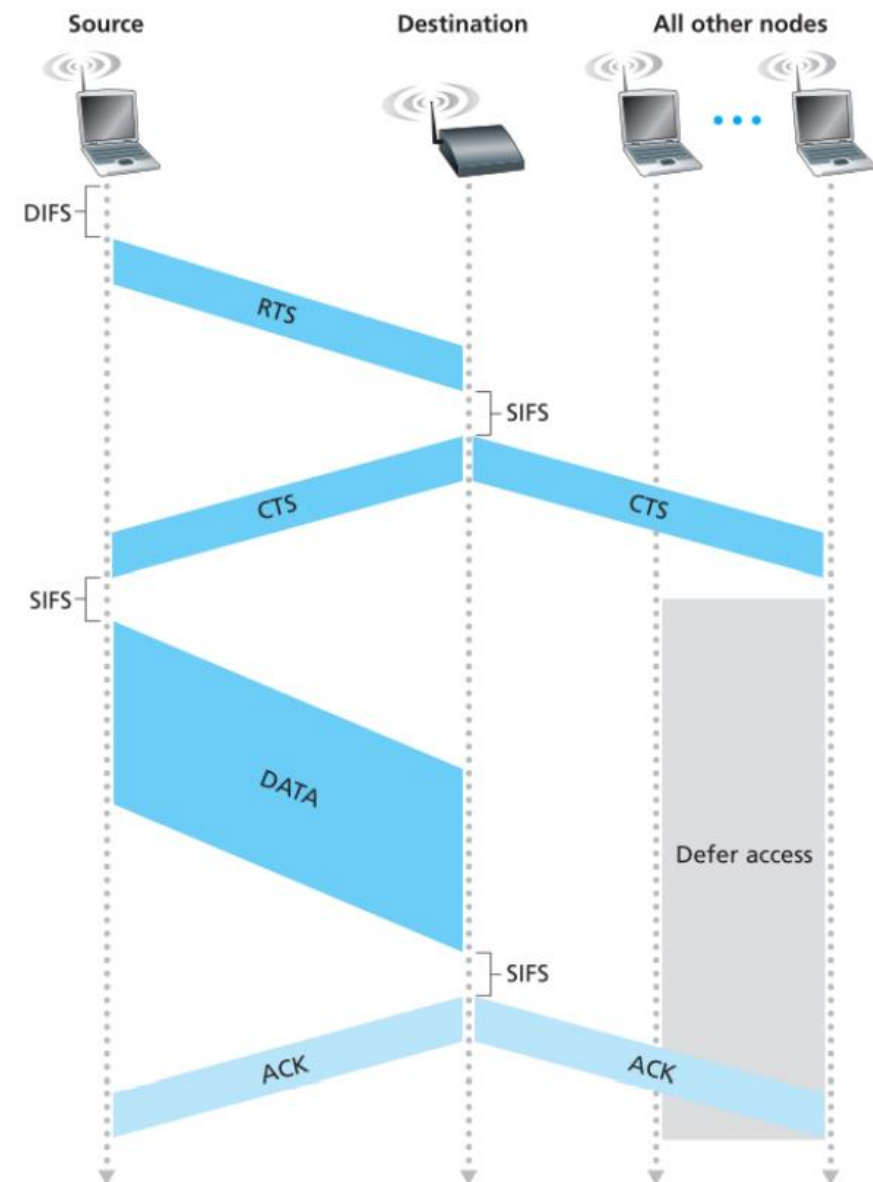
Main Idea: Ask for permission, and reserve channel before transmitting data

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

WiFi uses Carrier-Sense Multiple Access with Collision Avoidance (**CSMA/CA**)

All other nodes get the CTS/ACK, but they ignore it

Collision Detection/Avoidance in 802.11



The sender first transmits a **request to send (rts)** frame

If the AP is free, then it will send back a **clear to send (cts)** packet

The AP denies access to all other nodes until the AP sends an ACK

Main Idea: Ask for permission, and reserve channel before transmitting data

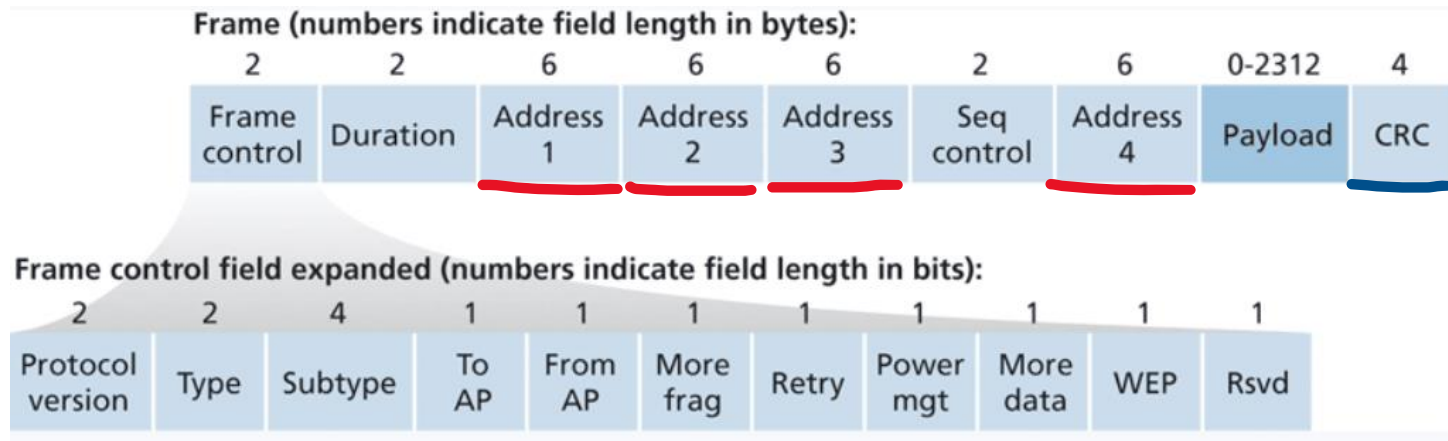
WiFi is not full-duplex, which means it cannot *detect* collisions, so we must *avoid* collisions instead

WiFi uses Carrier-Sense Multiple Access with Collision Avoidance (**CSMA/CA**)

https://wps.pearsoned.com/ecs_kurose_com_pnetw_6/216/55463/14198702.cw/index.html

All other nodes get the CTS/ACK, but they ignore it

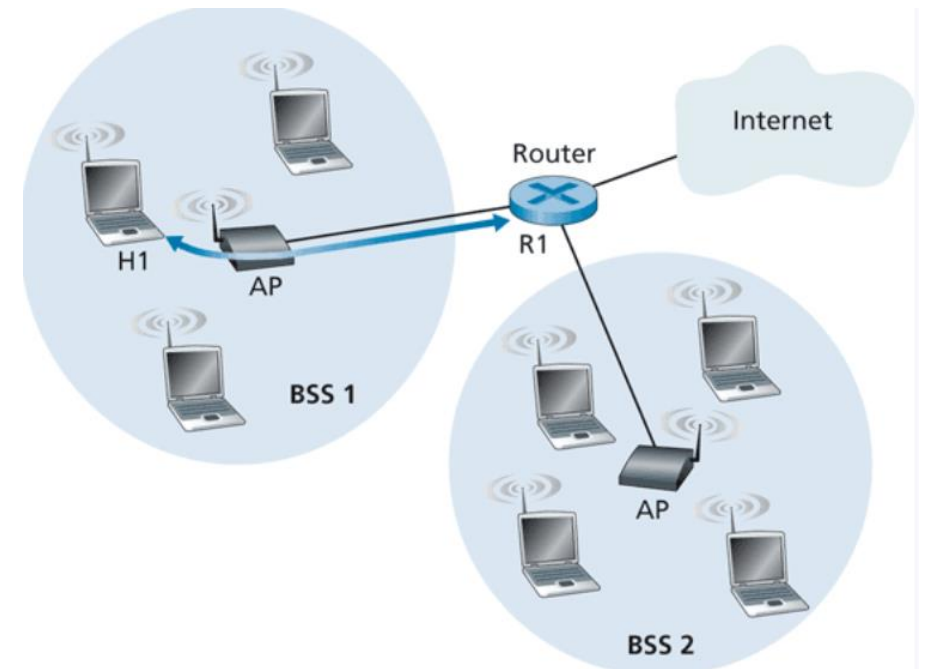
WiFi Frame



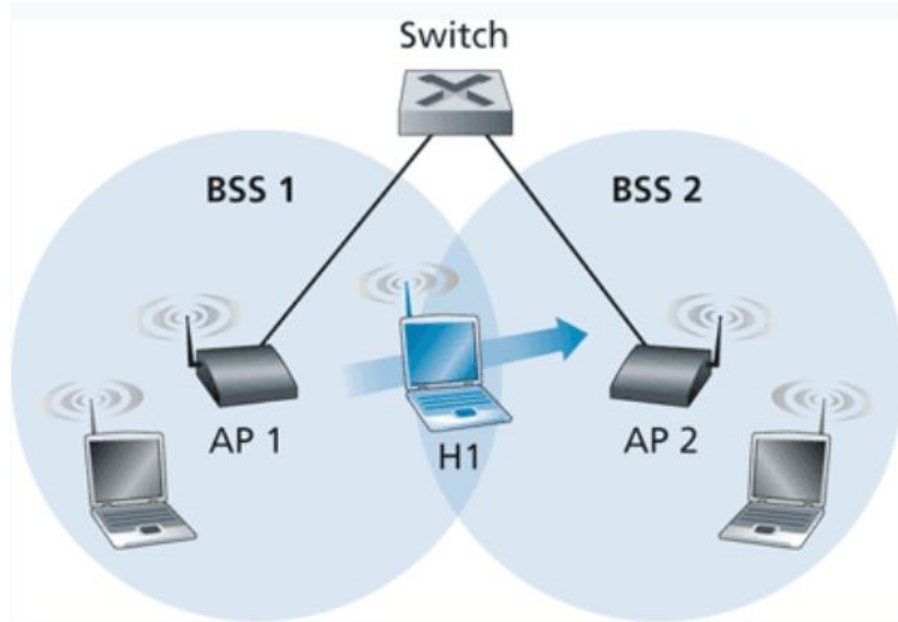
A WiFi frame can fit **four** 6-byte MAC addresses

We need the MAC address of the source host, destination host, **and the AP**

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



WiFi Mobility



If a device is moving, it may be moving in and out of WiFi networks

Need to handle routing and IP addressing

What to do when a device switches networks in the middle of a TCP stream, for example?

→ Send an ethernet frame from old network to new network and update routing tables if needed