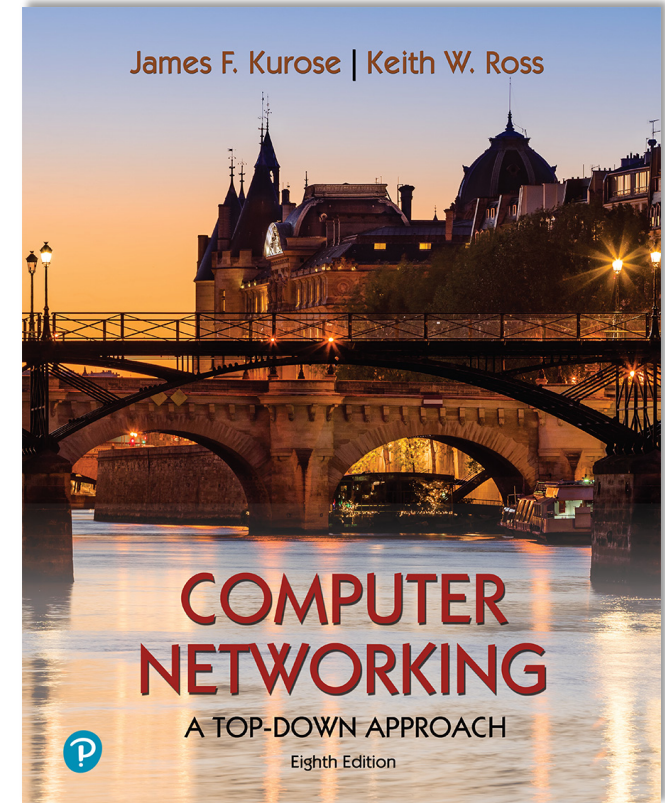


# Chapter 7

## Wireless and Mobile Networks



### *Computer Networking: A Top-Down Approach*

8<sup>th</sup> edition

Jim Kurose, Keith Ross  
Pearson, 2020

Acknowledgement: Based on the textbook's website:  
[https://gaia.cs.umass.edu/kurose\\_ross/index.php](https://gaia.cs.umass.edu/kurose_ross/index.php)

# 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 (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

# Chapter 7 outline

## ■ Introduction

### Wireless

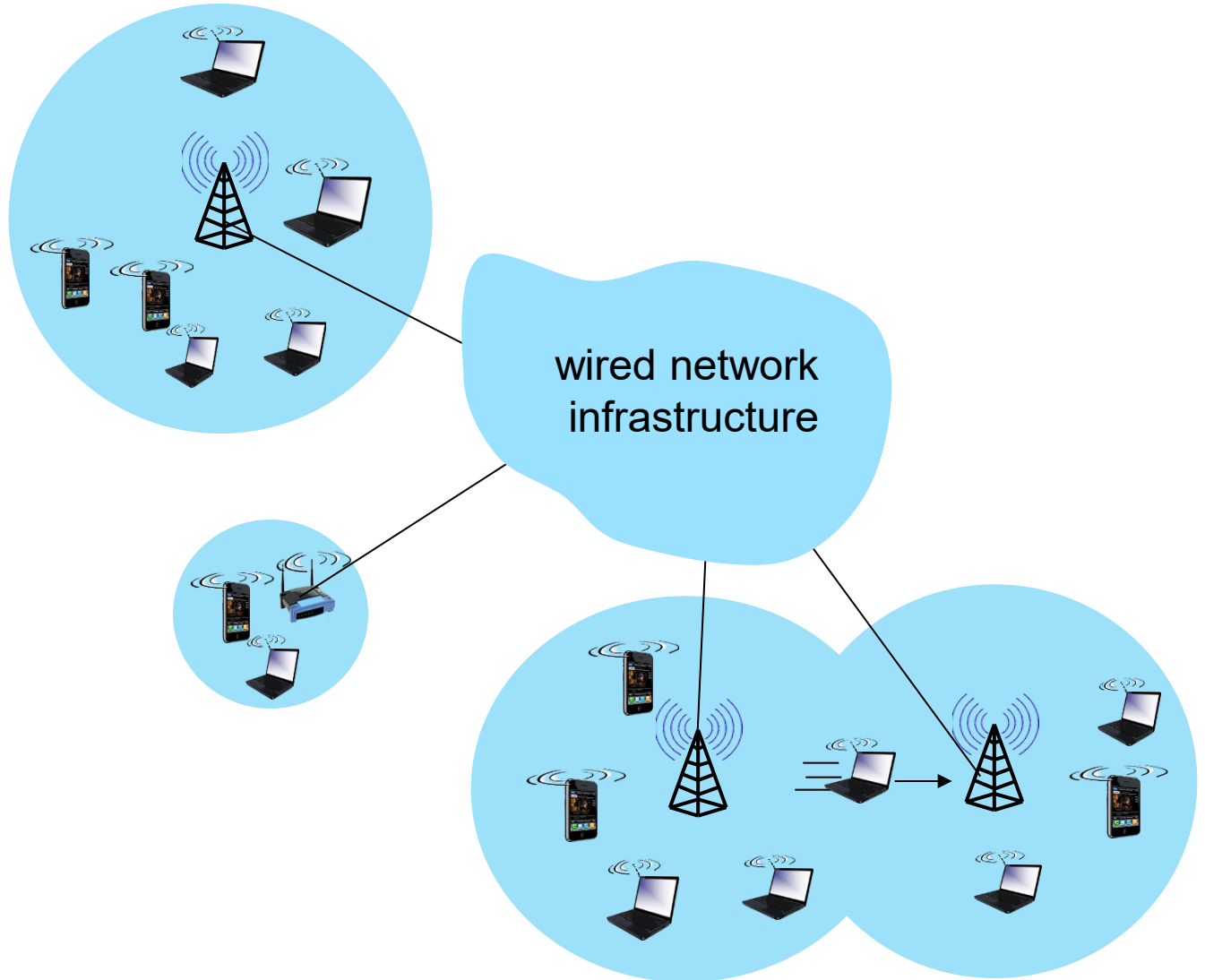
- Wireless Links and network characteristics
- WiFi: 802.11 wireless LANs
- Cellular networks: 4G and 5G

### Mobility

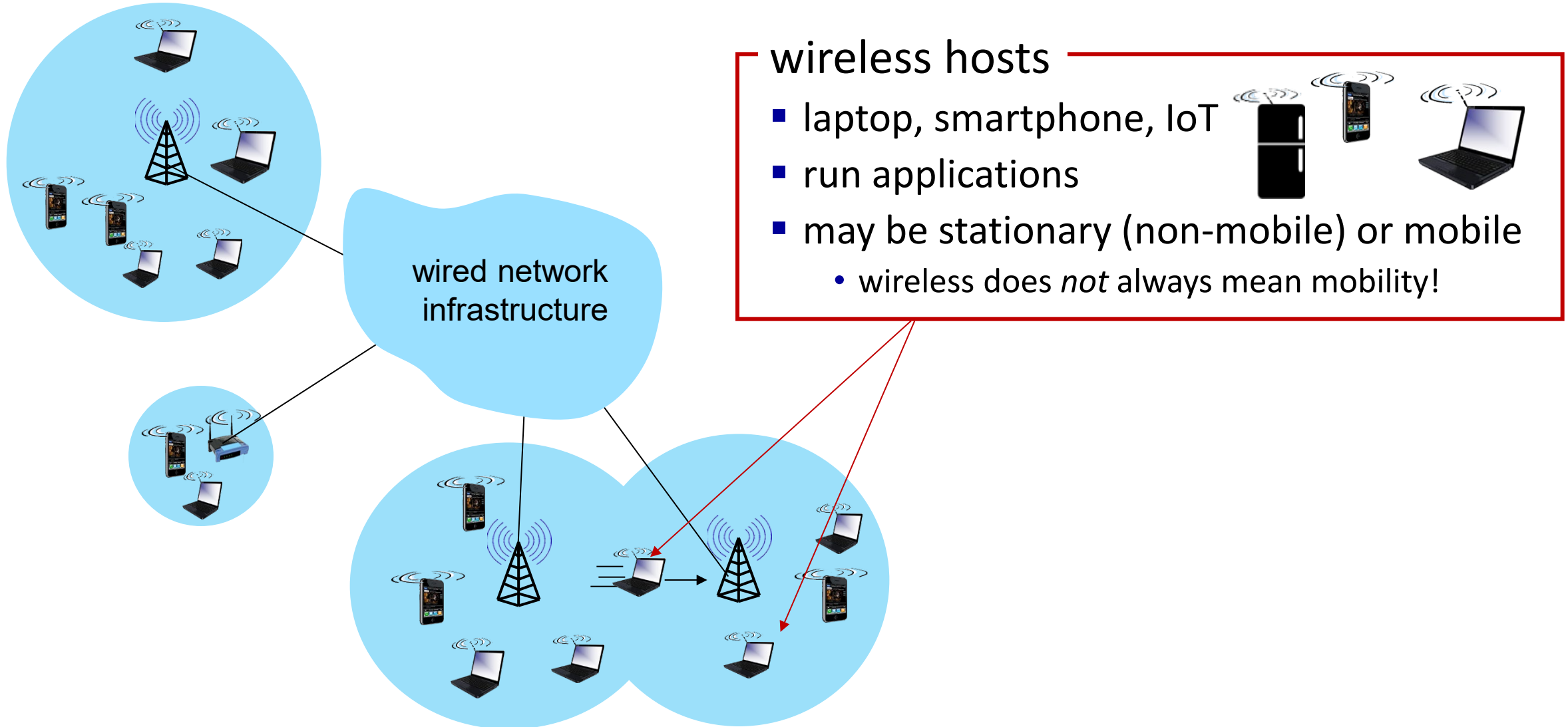
- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols



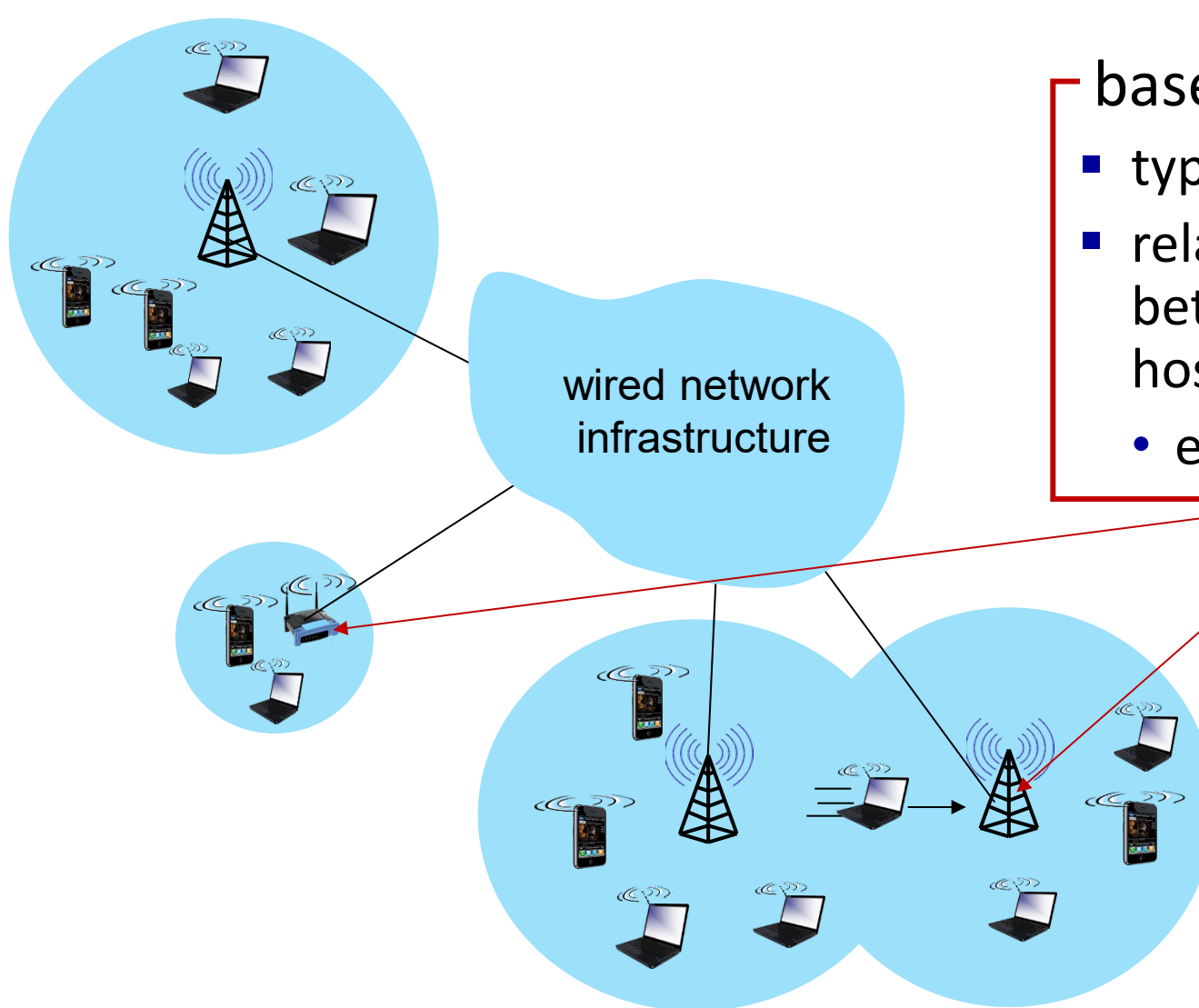
# Elements of a wireless network



# Elements of a wireless network



# Elements of a wireless network

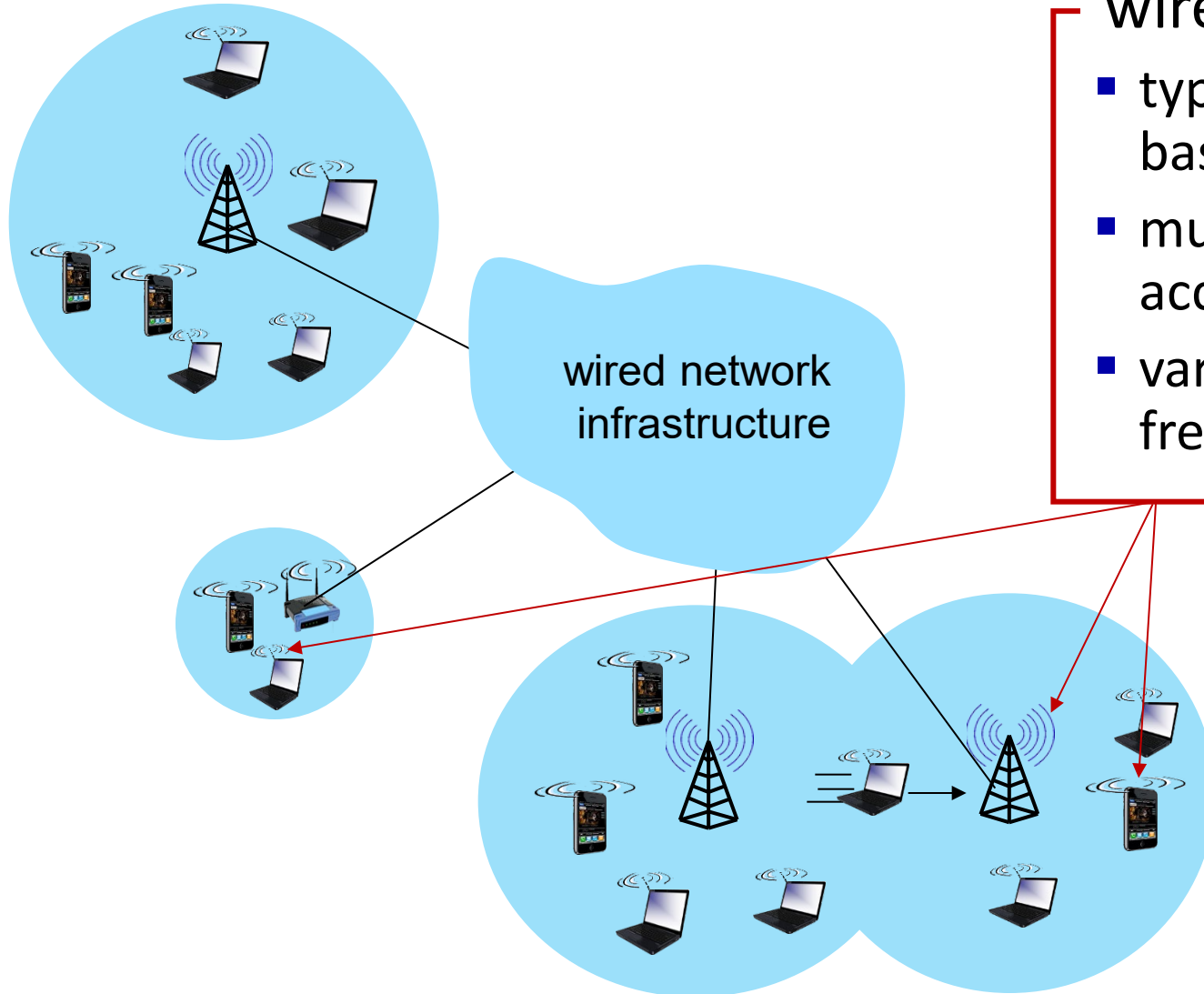


base station



- 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

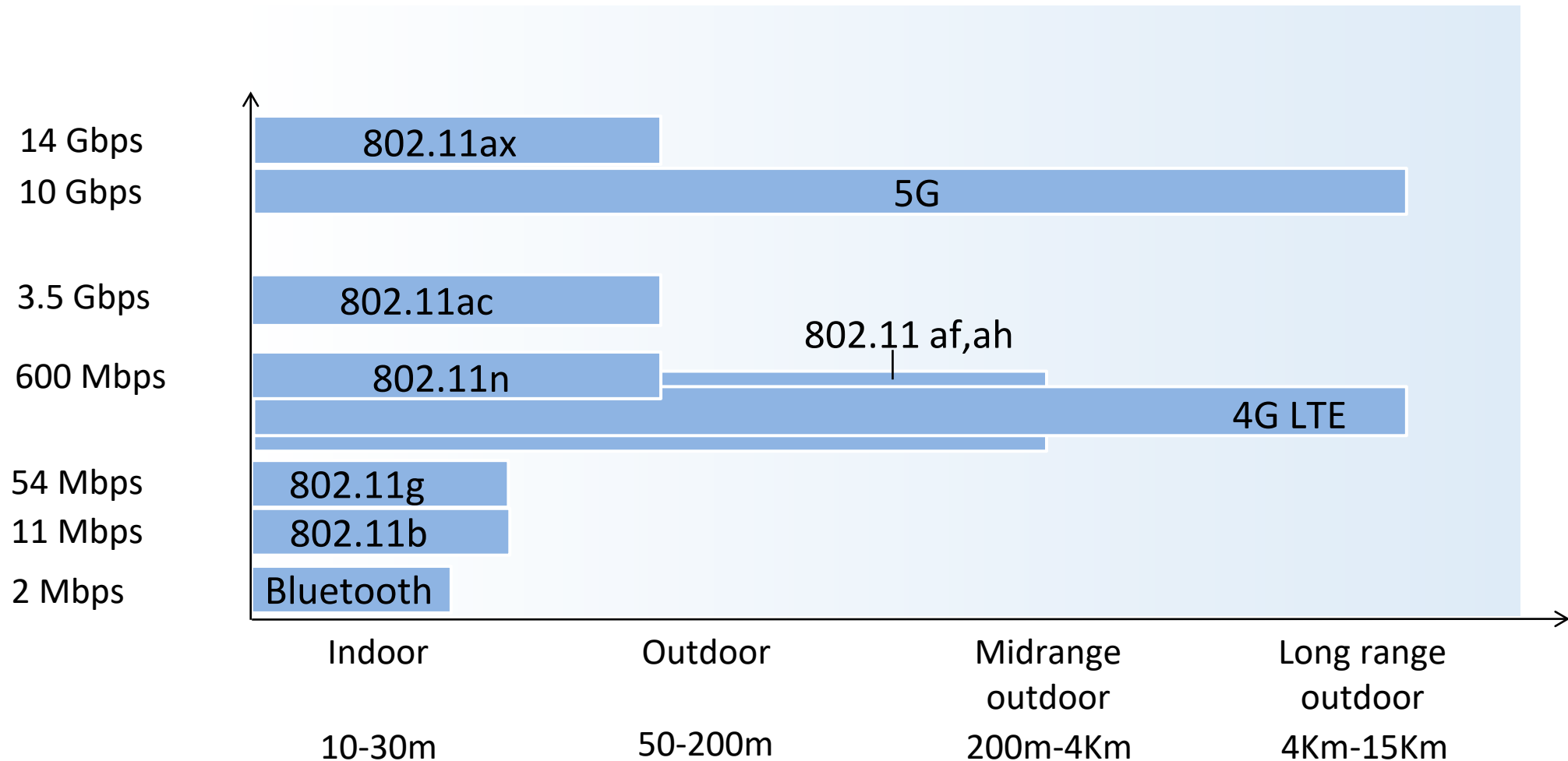


wireless link



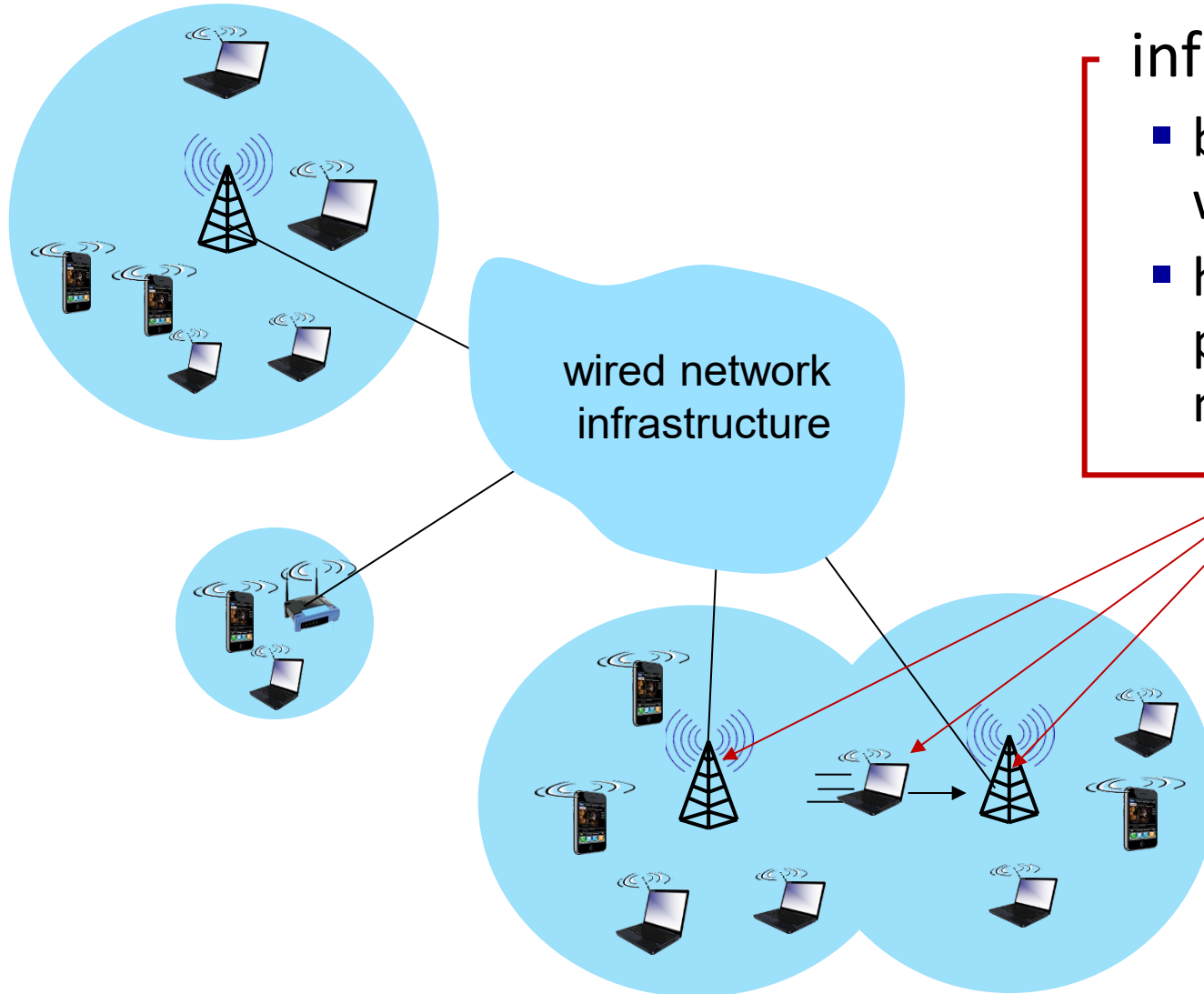
- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

# Characteristics of selected wireless links





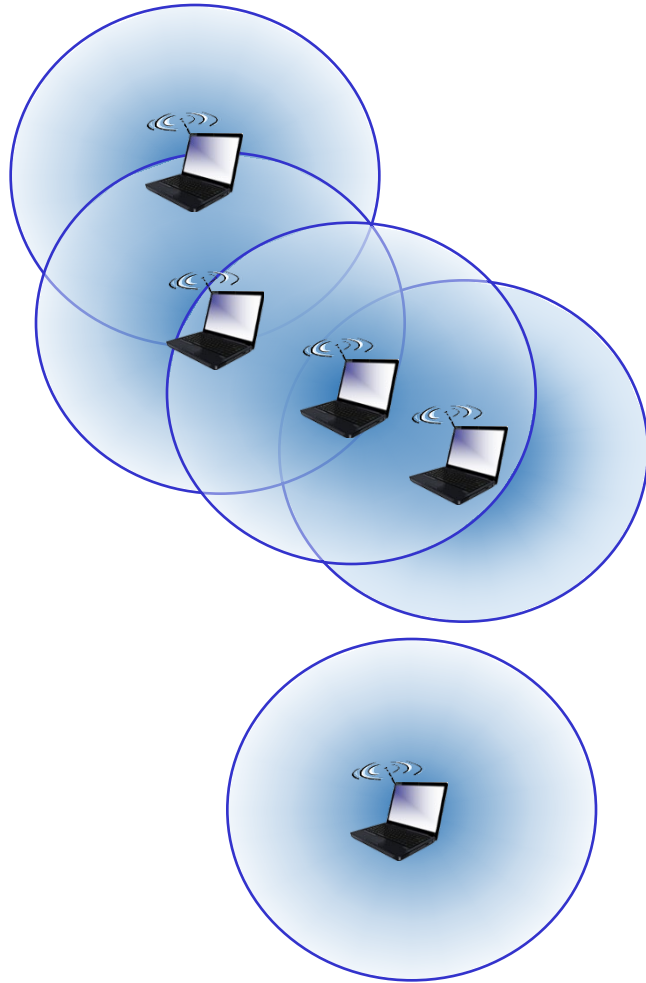
# Elements of a wireless network



## 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 among themselves

# 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: <i>mesh net</i>
<i>no infrastructure</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

# Chapter 7 outline

- Introduction

## Wireless

- Wireless links and network characteristics
- WiFi: 802.11 wireless LANs
- Cellular networks: 4G and 5G



## Mobility

- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols

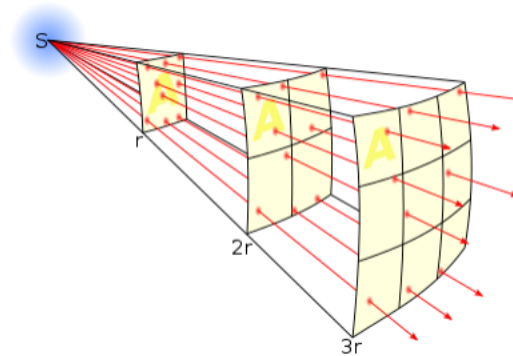
# Wireless link characteristics: fading (attenuation)

**Wireless** radio signal attenuates (loses power) as it propagates (free space “path loss”)

Free space path loss  $\sim (fd)^2$

$f$ : frequency

$d$ : distance



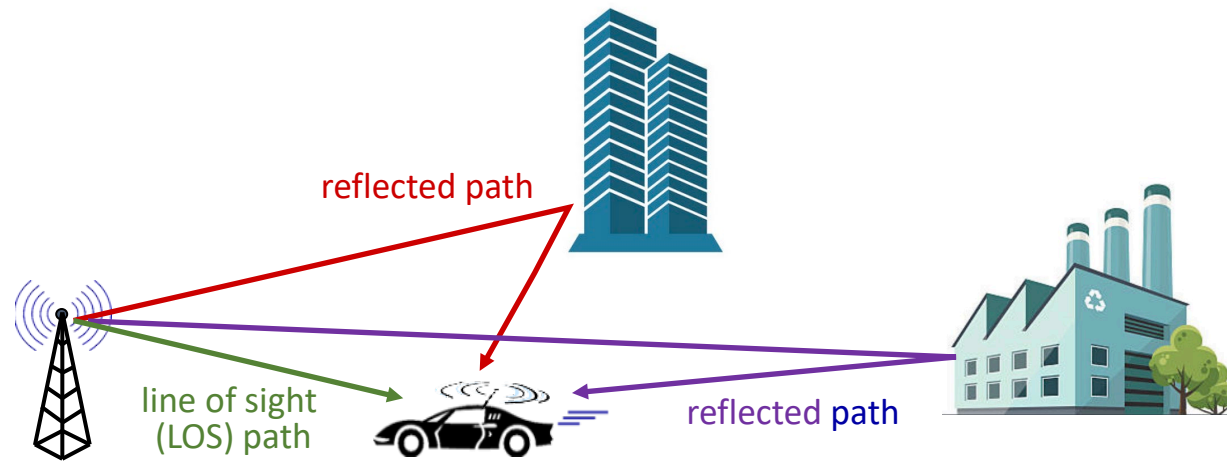
higher frequency or  
longer distance



larger free space  
path loss

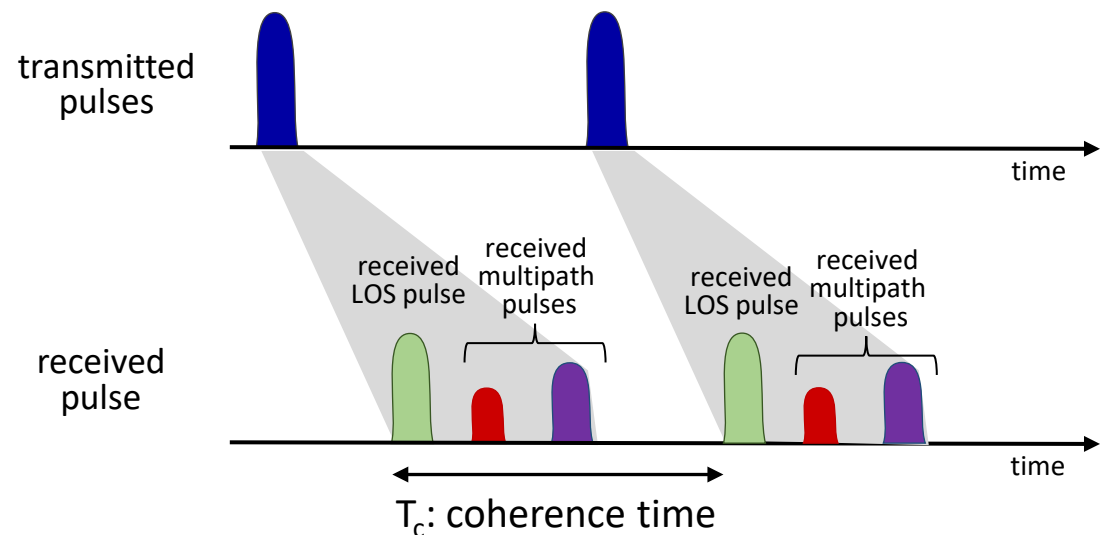
# Wireless link characteristics: multipath

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



# Wireless link characteristics: multipath

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

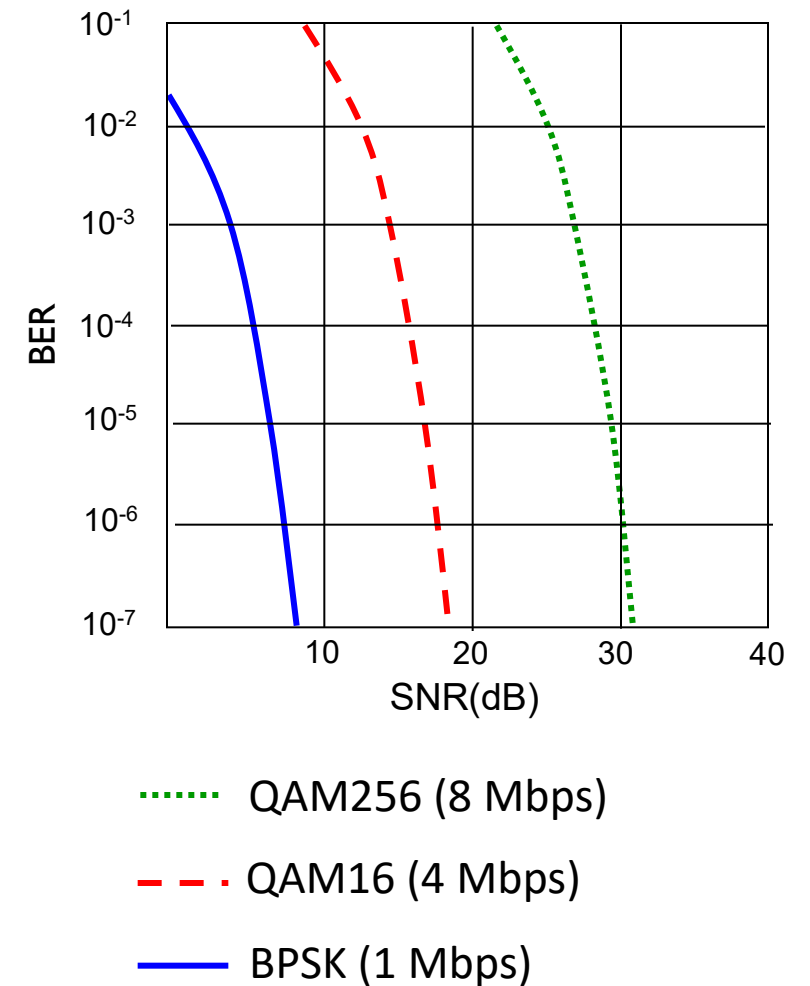


## Coherence time:

- amount of time bit is present in channel to be received
- influences maximum possible transmission rate, since coherence times can not overlap
- inversely proportional to
  - frequency
  - receiver velocity

# Wireless link characteristics: noise

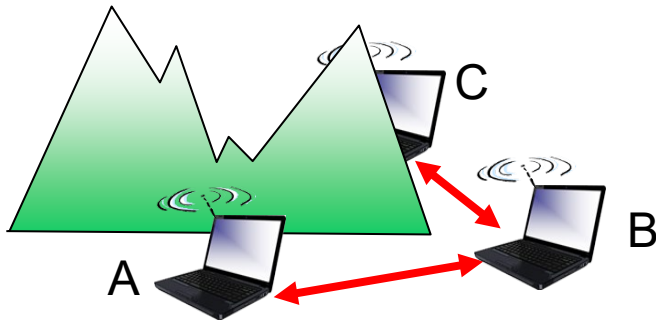
- **interference from other sources on** wireless network frequencies: motors, appliances
- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a “good thing”)
- **SNR versus BER tradeoff**
  - *given physical layer*: increase power -> increase SNR->decrease BER
  - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)





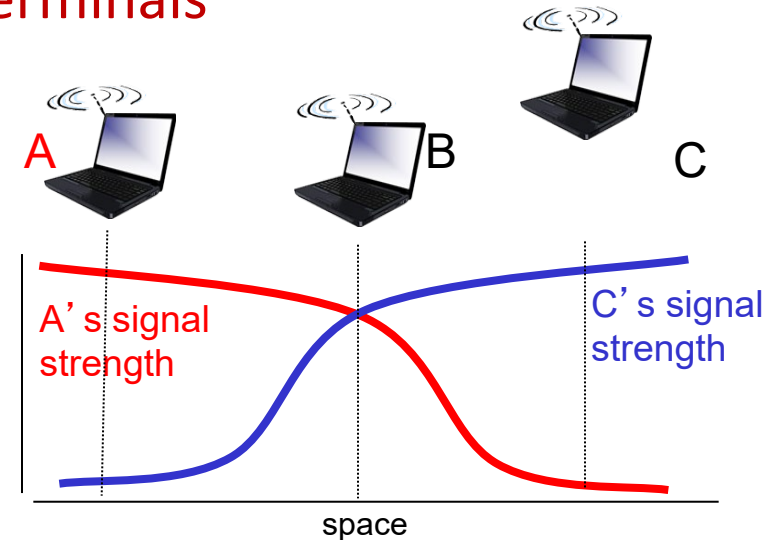
# Wireless link characteristics: hidden terminals

## 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

## Attenuation also causes “hidden terminals”



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

# Chapter 7 outline

- Introduction

## Wireless

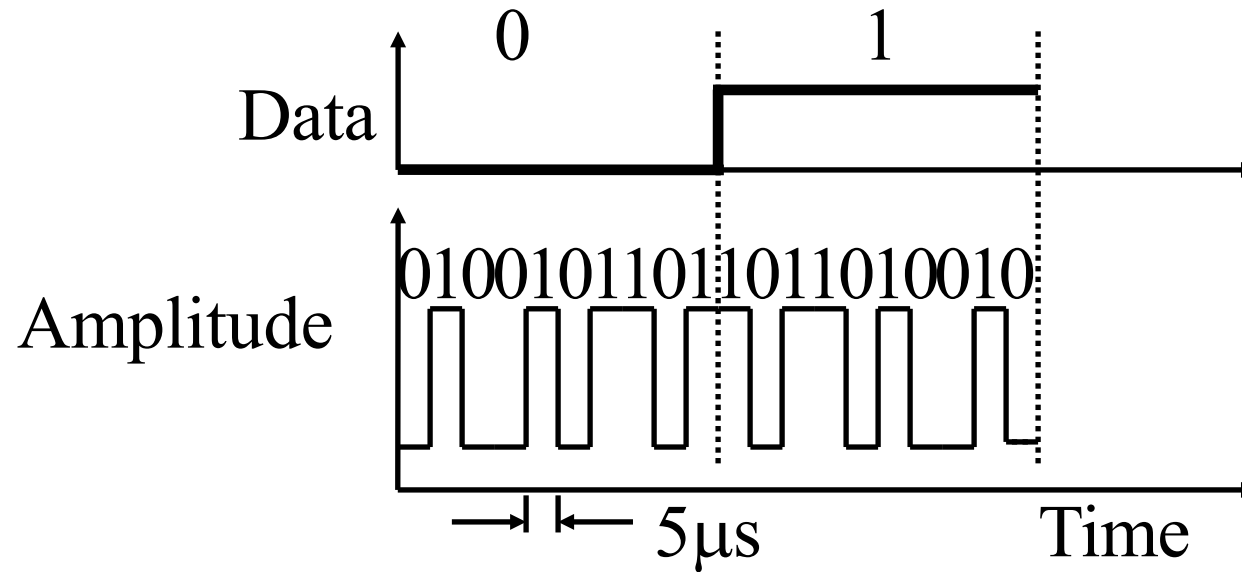
- Wireless links and network characteristics
- **CDMA: code division multiple access**
- WiFi: 802.11 wireless LANs
- Bluetooth



# Code Division Multiple Access (CDMA)

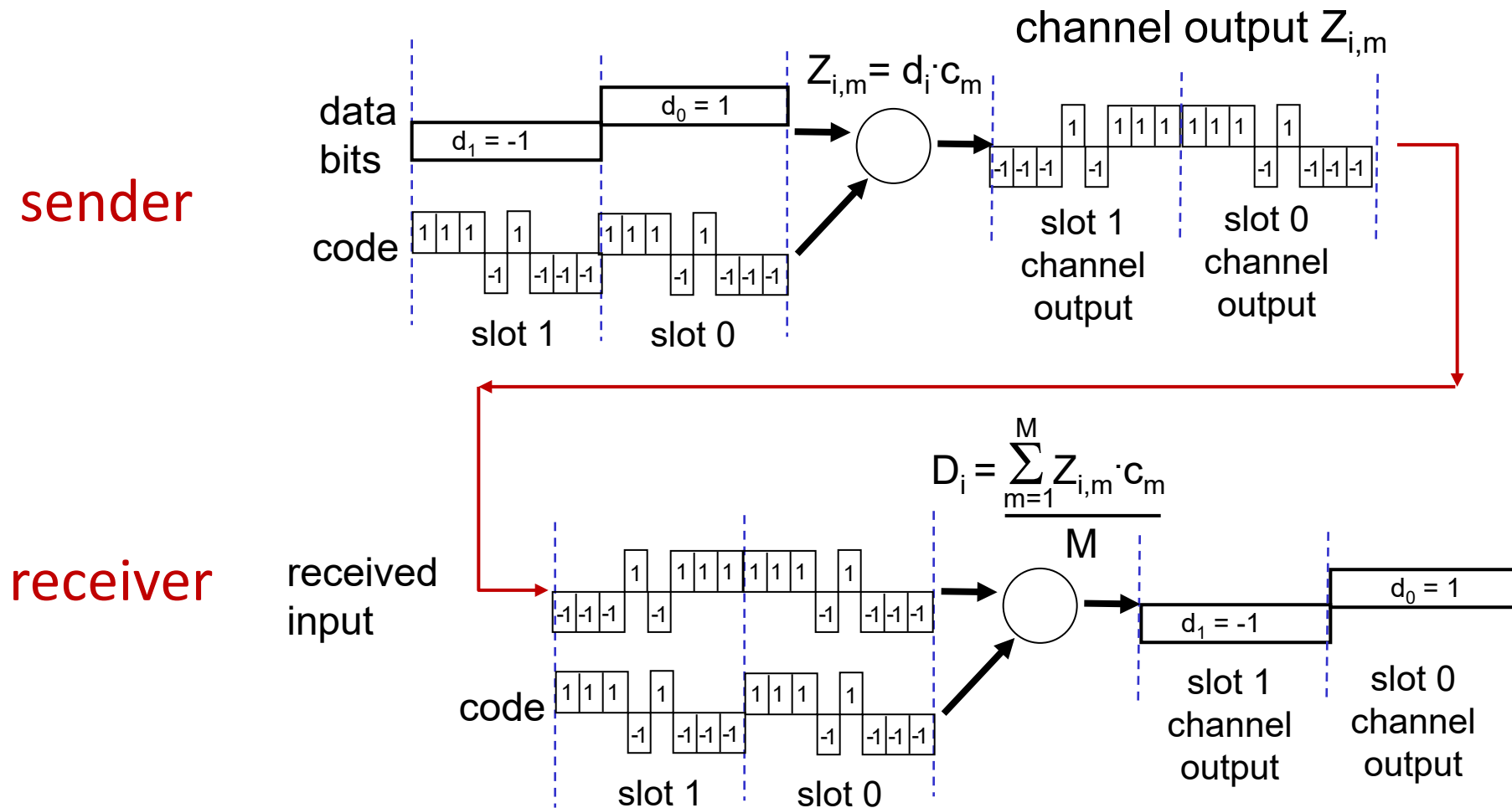
- unique “code” assigned to each user; i.e., code set partitioning
  - all users share same frequency, but each user has own “chipping” sequence (i.e., code) to encode data
  - allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)
  - Analogy: people speaking different languages in the same room do not interfere with each other
- **encoding:** inner product: (original data)  $\times$  (chipping sequence)
- **decoding:** summed inner-product: (encoded data)  $\times$  (chipping sequence)
- Used by Wifi but not 4G/5G

# Direct-Sequence Spread Spectrum CDMA



- ❑ The 10-bit code 0100101101 encodes data bit 0
- ❑ The 10-bit code 1011010010 encodes data bit 1
- ❑ Spreading factor = Code bits/data bit, 10-100 commercial (Min 10 by FCC), 10,000 for military

# CDMA encode/decode

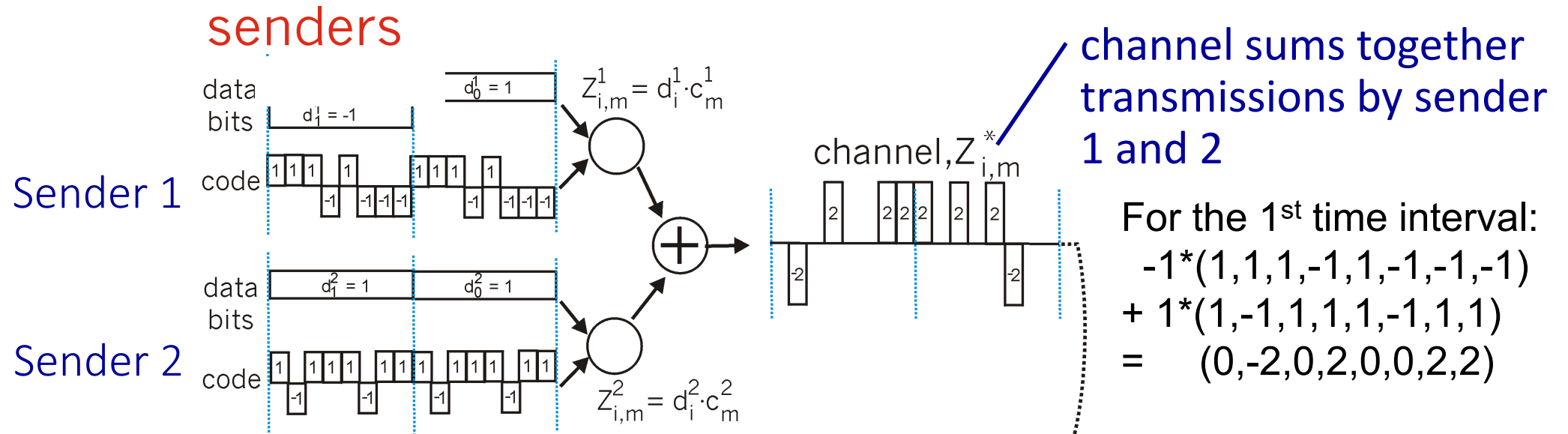


$$Z_{i,m} = d_i \cdot c_m$$

$$-1 * (1, 1, 1, -1, 1, -1, -1, -1) = (-1, -1, -1, 1, -1, 1, 1, 1)$$

$$1 * (1, 1, 1, -1, 1, -1, -1, -1) = (1, 1, 1, -1, 1, -1, -1, -1)$$

# CDMA: two-sender interference



For the 1<sup>st</sup> time interval:

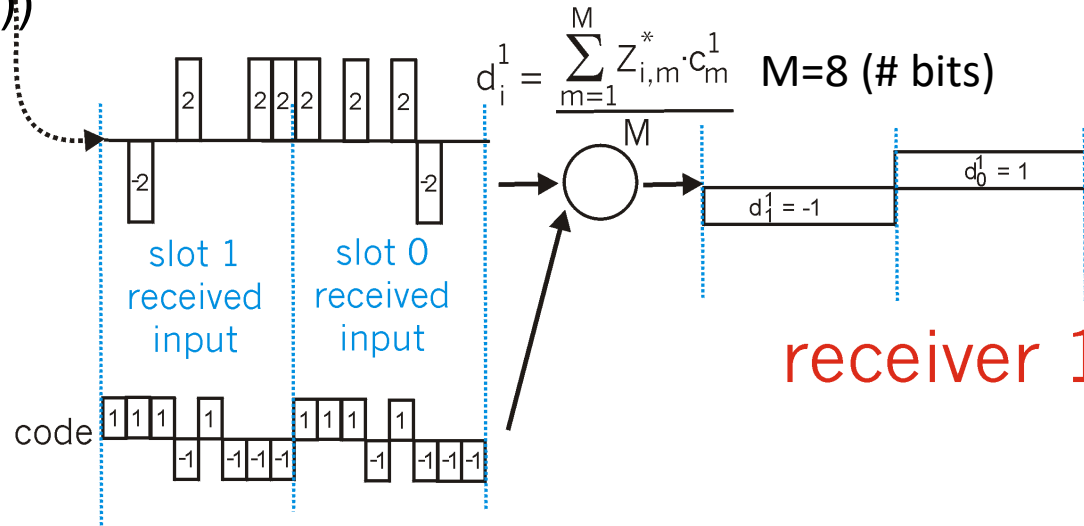
$$d = (1/8) \cdot (0 \cdot 1 + (-2) \cdot 1 + 0 \cdot 1 + 2 \cdot (-1) + 0 \cdot 1 + 0 \cdot (-1) + 2 \cdot (-1) + 2 \cdot (-1))$$

$$= (1/8) \cdot (-8) = -1$$

Sender 1 Code:  
 $(1, 1, 1, -1, 1, 1, -1, -1)$

Sender 2 Code:  
 $(1, -1, 1, 1, 1, -1, 1, 1)$

Orthogonal since their inner product =  $1 \cdot 1 + 1 \cdot (-1) + 1 \cdot 1 + (-1) \cdot 1 + 1 \cdot 1 + (-1) \cdot (-1) + (-1) \cdot 1 + (-1) \cdot 1 = 0$



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

provided the codes for different senders are orthogonal

# CDMA: two-sender interference

- $(-1 * (1, 1, 1, -1, 1, -1, -1, -1) + 1 * (1, -1, 1, 1, 1, -1, 1, 1)) \text{ IP } (1, 1, 1, -1, 1, -1, -1, -1)$
- $= (-1 * (1, 1, 1, -1, 1, -1, -1, -1) \text{ IP } (1, 1, 1, -1, 1, -1, -1, -1) + (1/8) * 1 * (1, -1, 1, 1, 1, -1, 1, 1) \text{ IP } (1, 1, 1, -1, 1, -1, -1, -1))$
- $= -1 * (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) + 1 * (1 * 1 + 1 * (-1) + 1 * 1 + (-1) * 1 + 1 * 1 + (-1) * (-1) + (-1) * 1 + (-1) * 1)$

(**First addition term**: A vector's inner product with itself is sum of n 1's, n is its dimension. **Second addition term**: equals 0 due to assumption that the codes for different senders are orthogonal)

- $-1 * 8 + 1 * 0 = -8$
- Hence the recovered bit is  $(1/8) * (-8) = -1$

# Chapter 7 outline

- Introduction

## Wireless

- Wireless links and network characteristics
- **WiFi: 802.11 wireless LANs**
- Cellular networks: 4G and 5G



## Mobility

- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols



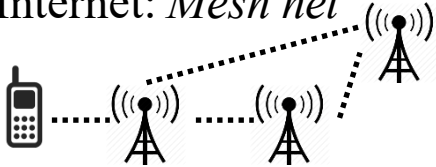
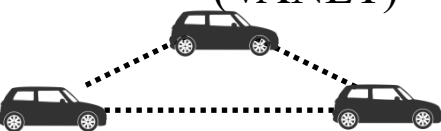


# IEEE 802.11 Wireless LAN

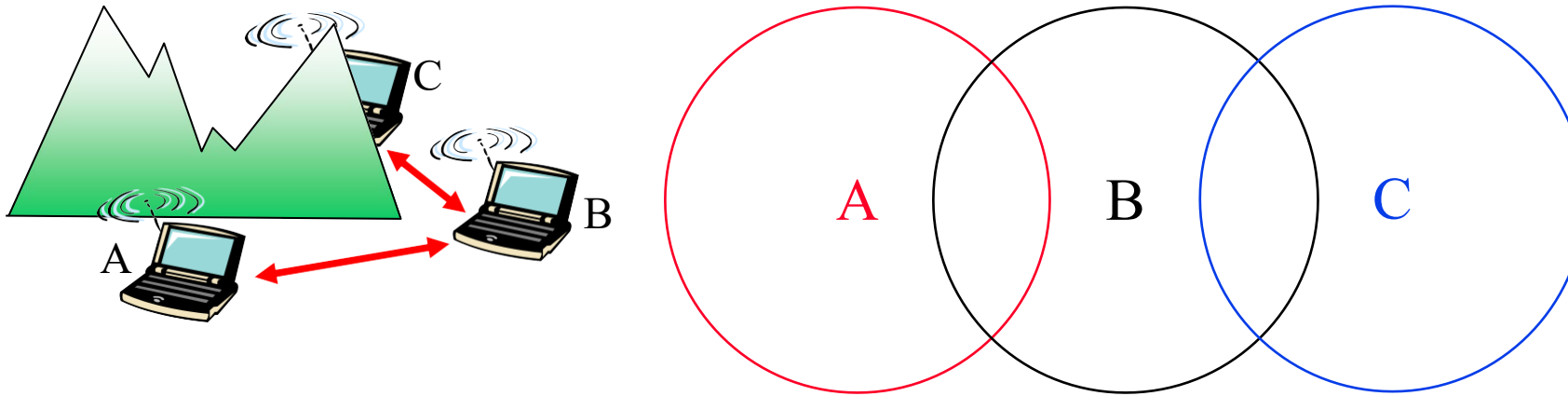
IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV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

- all use CSMA/CA for multiple access, and differ in the physical layer (frequency range)
- For the same power and coding, higher frequency (longer wavelengths) will have lower data rate and longer distances.

# Wireless Network Taxonomy

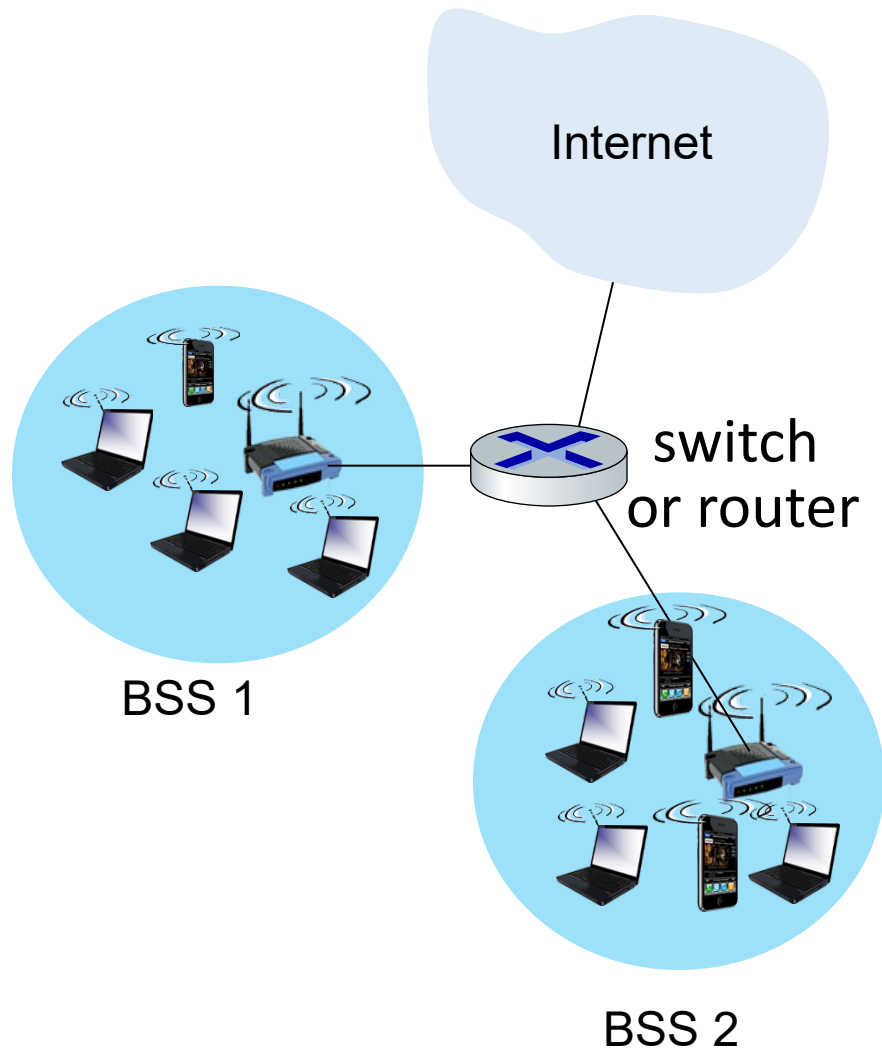
	Single hop	Multiple hops
<p>Infrastructure (Access Points, Towers)</p> <p>No Infrastructure</p>	<p>Host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet</p>  <p>No base station (Bluetooth, ad hoc nets)</p> 	<p>Host may have to relay through several wireless nodes to connect to larger Internet: <i>Mesh net</i></p>  <p>Relay to reach other a given wireless node. Mobile Ad-hoc Network (MANET), Vehicular Ad-hoc Network (VANET)</p> 

# Hidden Node Problem



- ❑ B and A can hear each other  
B and C can hear each other  
A and C cannot hear each other  
⇒ C is hidden for A and vice versa
- ❑ C may start transmitting while A is also transmitting  
A and C can't detect collision.
- ❑ Only the receiver can help avoid collisions

# 802.11 LAN architecture

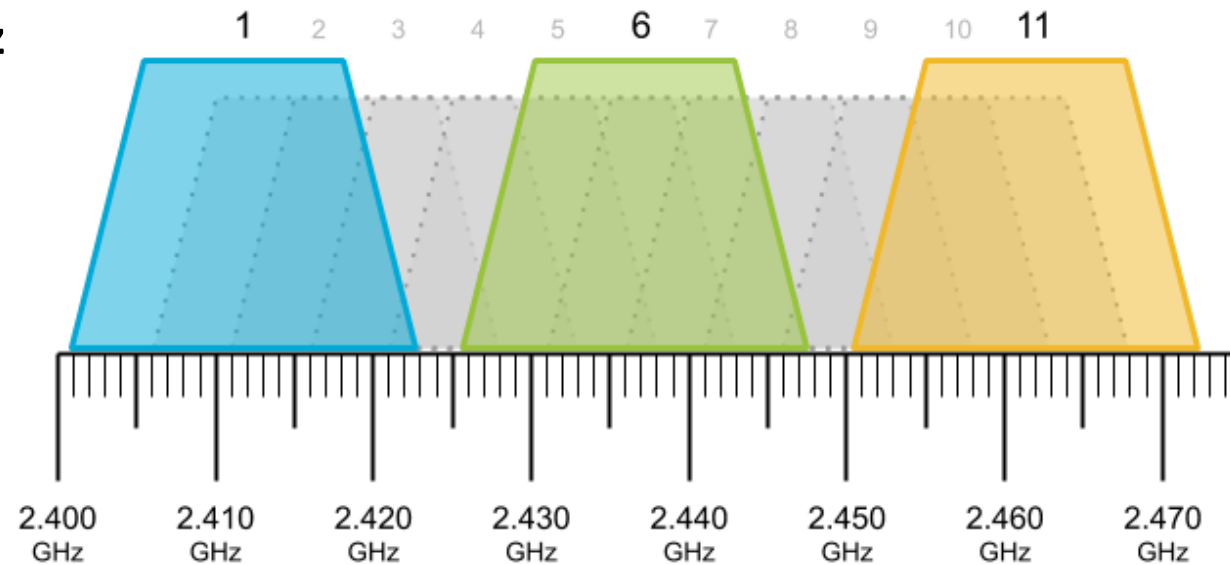


- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

# 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**

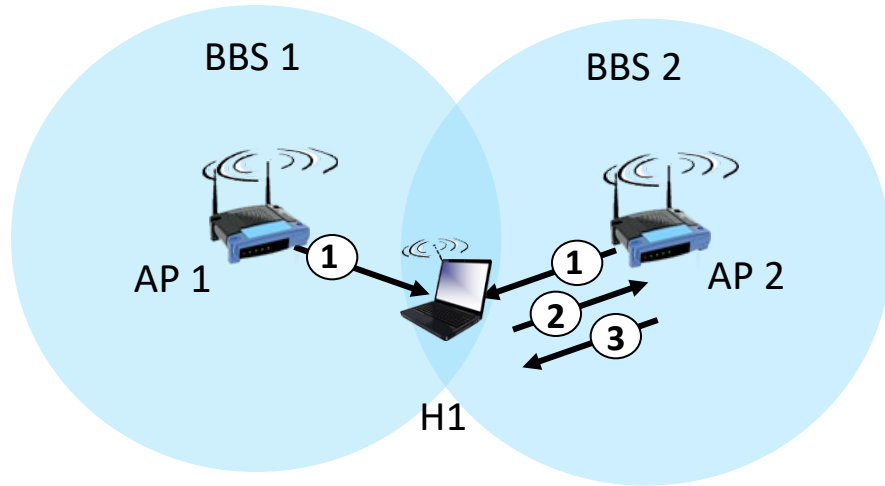


# 802.11: Association

- 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 [Chapter 8]
  - then typically run DHCP to get IP address in AP's subnet

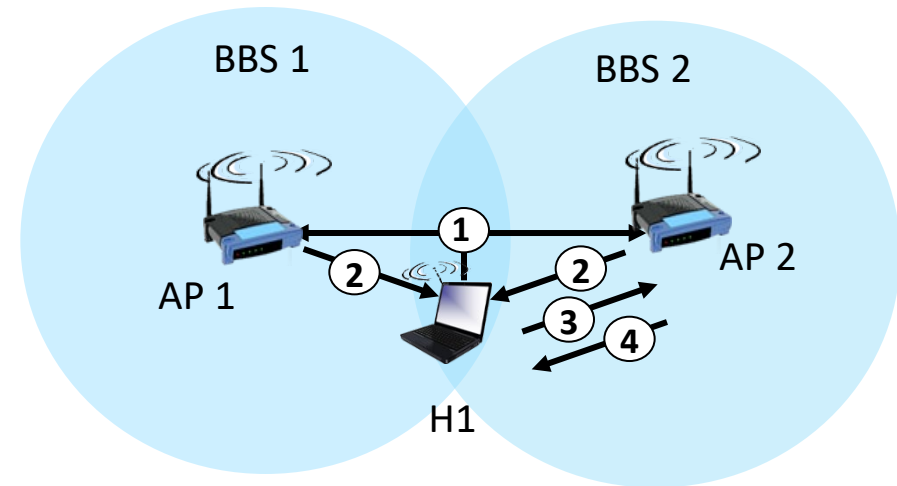


# 802.11: passive/active scanning



## 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

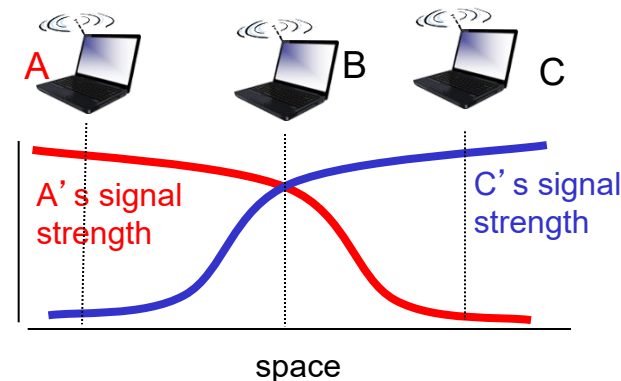
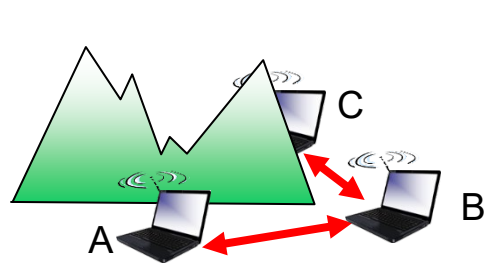


## active scanning:

- (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

# IEEE 802.11: multiple access

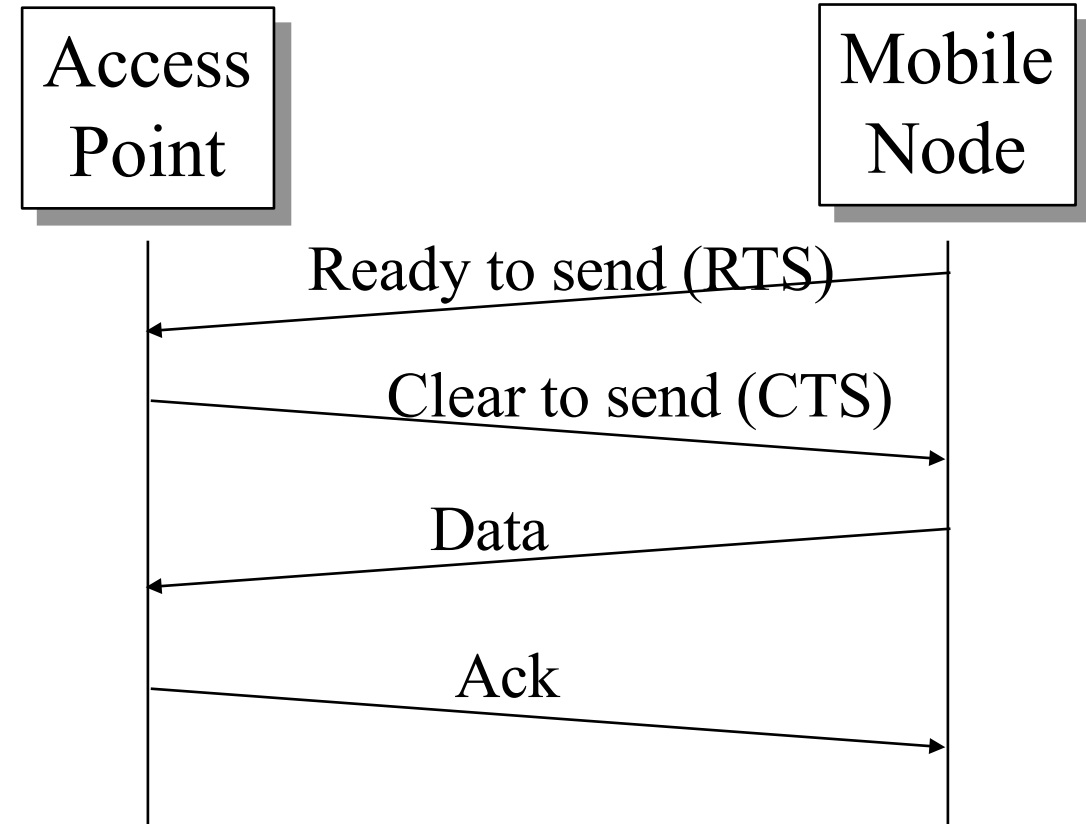
- avoid collisions: 2<sup>+</sup> nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with detected ongoing transmission by another node
- 802.11: *no* collision detection!
  - difficult to sense collisions: high transmitting signal, weak received signal due to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



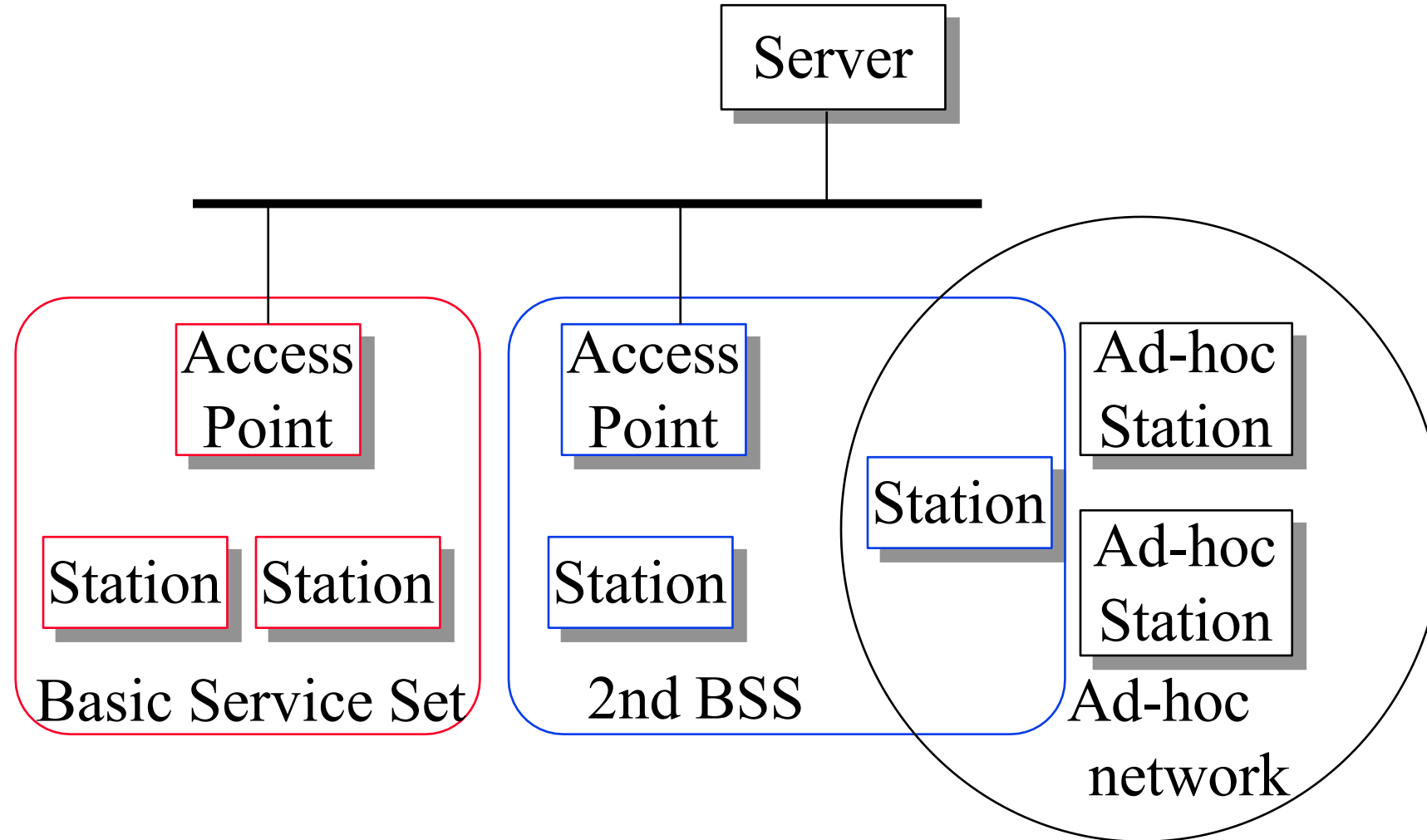


# 4-Way Handshake

- ❑ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- ❑ Listen before you talk. If the medium is busy, the transmitter backs off for a random period.
- ❑ Avoids collision by sending a short message:  
Ready to send (RTS)
  - RTS contains dest. address and duration of message.  
Tells everyone to backoff for the duration.
- ❑ Destination sends: Clear to send (CTS)
- ❑ Can not detect collision  $\Rightarrow$  Each packet is acked.
- ❑ MAC level retransmission if not acked.



# IEEE 802.11 Architecture



# IEEE 802.11 Architecture Cont

- ❑ Basic Service Area (BSA) = Cell
  - Area: Geographical area = a room, or a building
- ❑ Each BSA may have several wireless LANs
- ❑ Extended Service Area (ESA) = Multiple BSAs interconnected via Access Points (AP) = Multiple rooms in your home with different extenders advertising the same SSID
- ❑ Basic Service Set (BSS)
  - = Set of stations associated with an AP =  $\{MAC_1, \dots, MAC_n\}$ . Each BSS has a Service Set ID (SSID), e. g., WUSTL-Guest
- ❑ Extended Service Set (ESS)
  - = Set of stations in an ESA
- ❑ Ad-hoc networks coexist and interoperate with infrastructure- based networks.

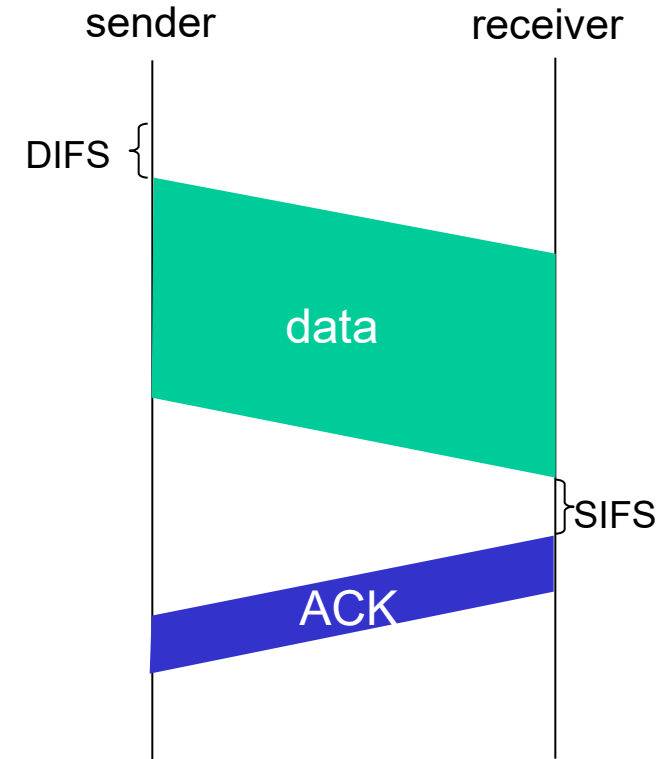
# IEEE 802.11 MAC Protocol: CSMA/CA

## 802.11 sender

- 1 if sense channel idle for **DIFS (Distributed Interframe Space)** 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 (Short Interframe Space)** (ACK needed due to hidden terminal problem)  
SIFS is a shorter interframe space used between frames of an ongoing communication session where no contention is required.

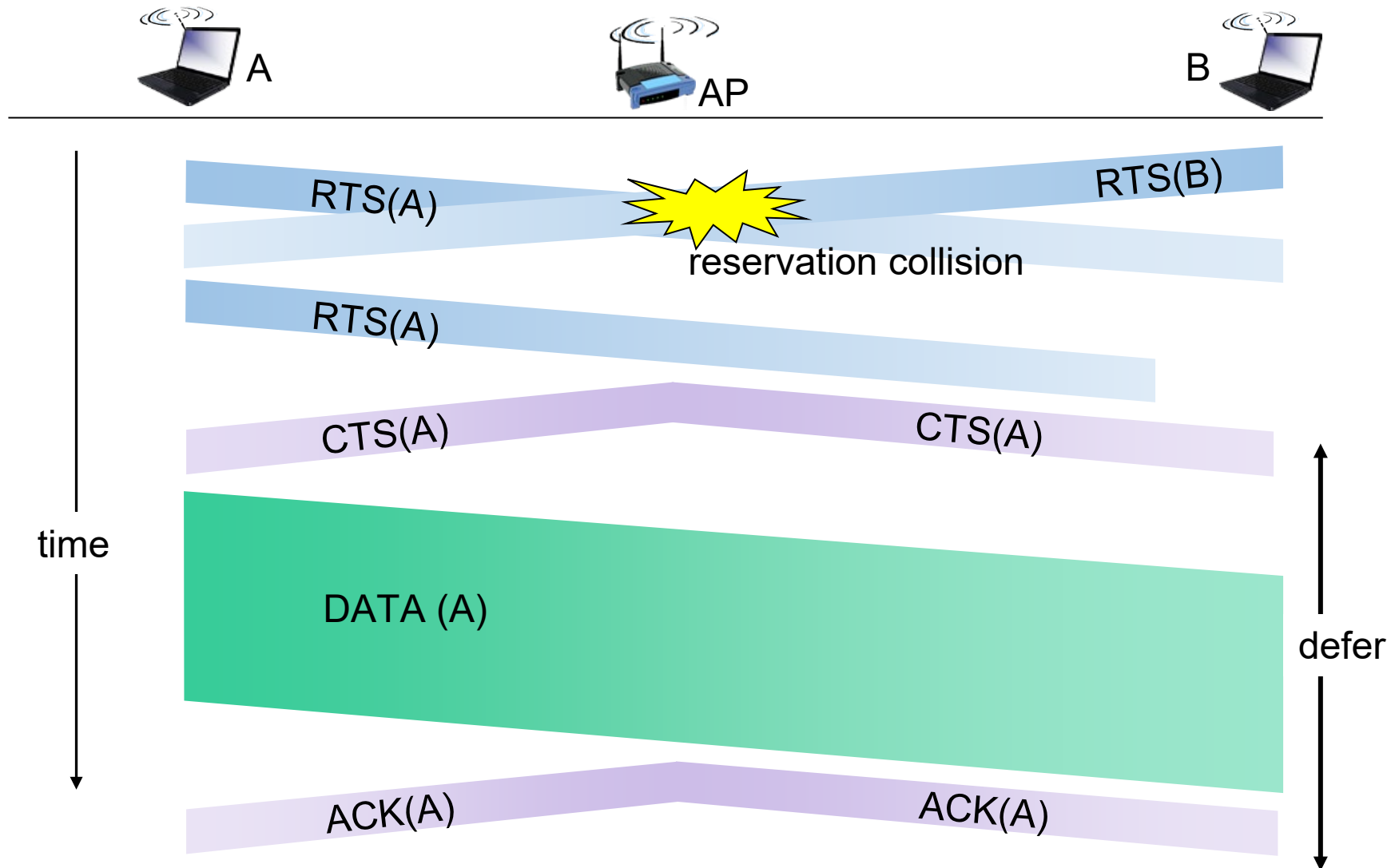


# Avoiding collisions (more)

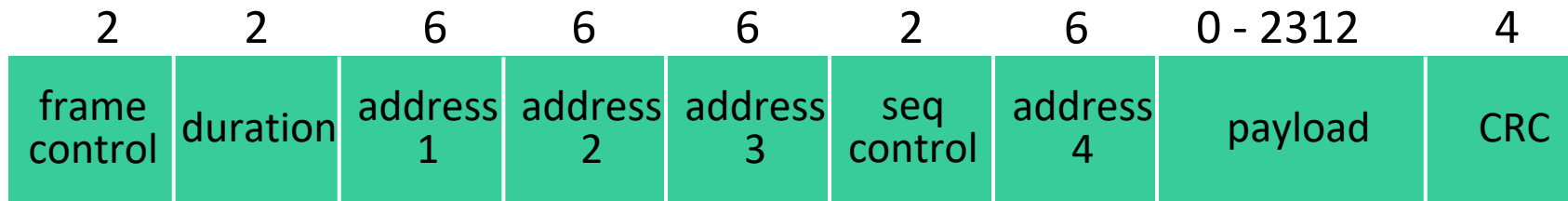
**idea:** sender “reserves” channel use for data frames using small reservation packets

- 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

# Collision Avoidance: RTS-CTS exchange



# 802.11 frame: addressing



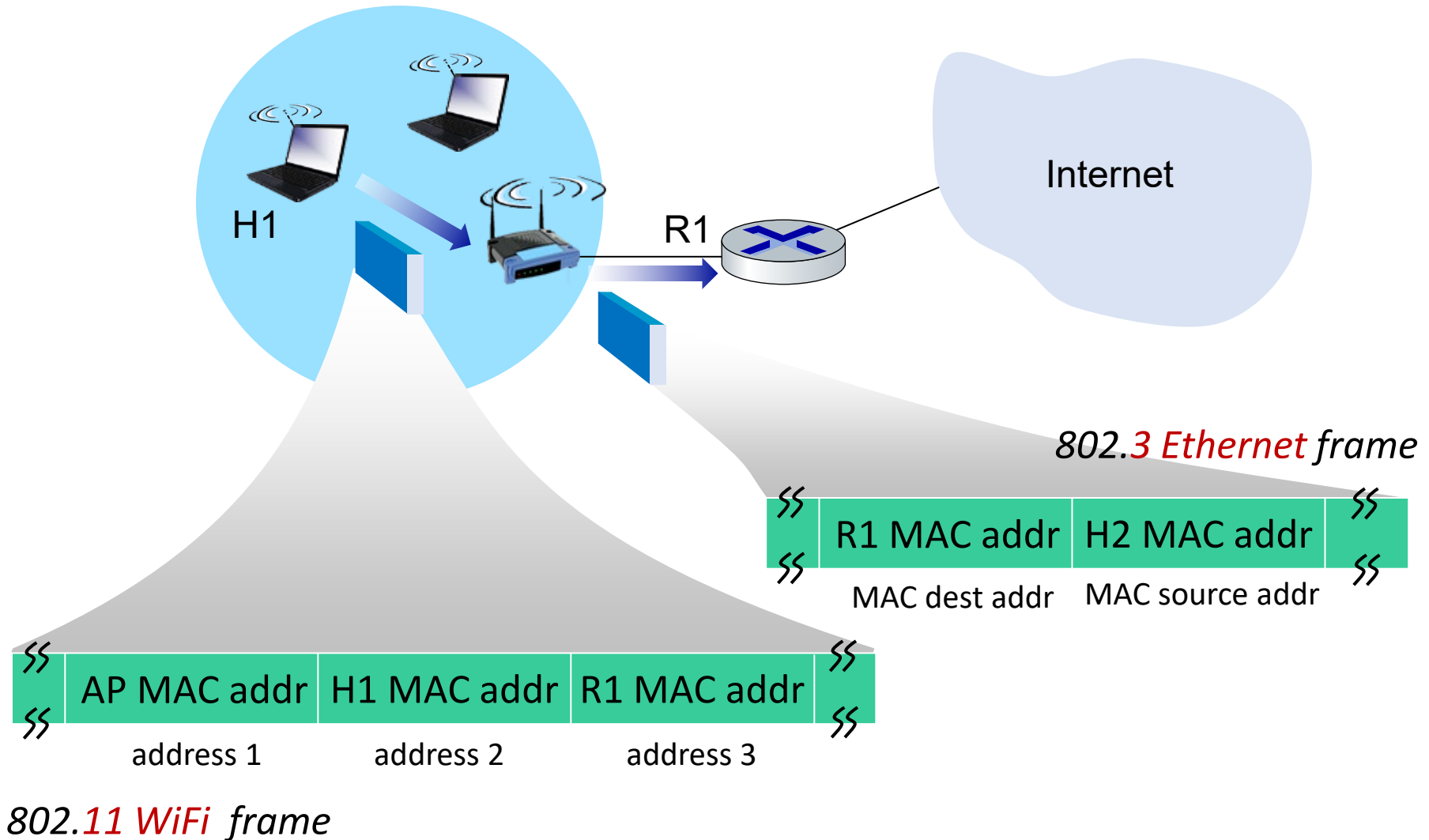
**Address 1:** MAC address of wireless host or AP to receive this frame

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

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

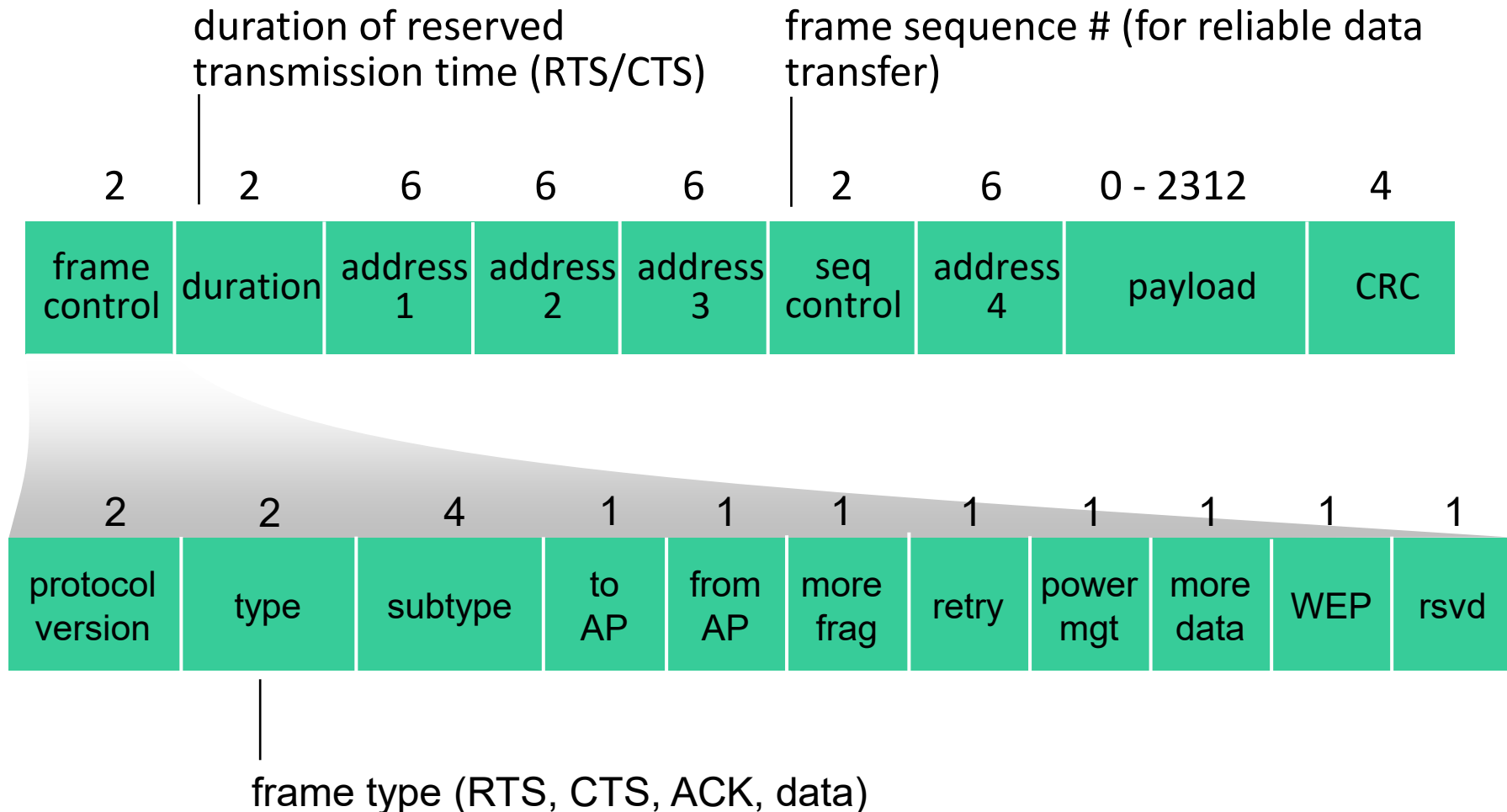
**Address 4:** used only in ad hoc mode

# 802.11 frame: addressing



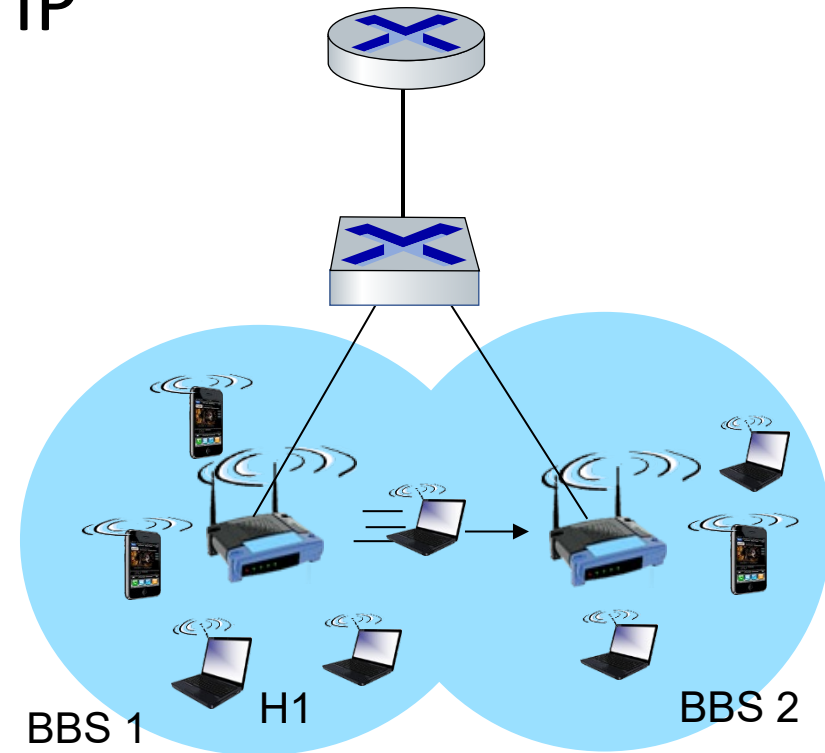


# 802.11 frame: addressing



# 802.11: mobility within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 6): switch will see frame from H1 and “remember” which switch port can be used to reach H1

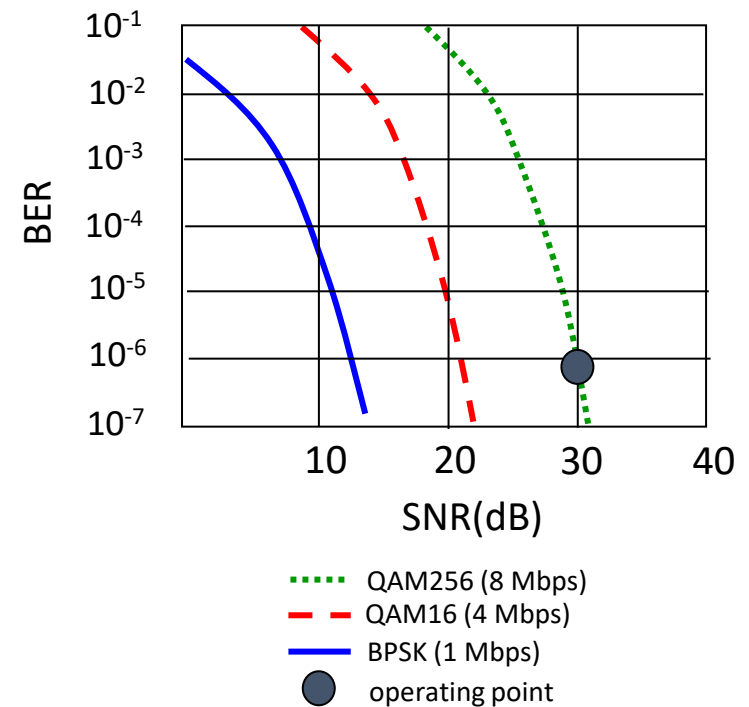


# 802.11: advanced capabilities

## Rate adaptation

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

1. SNR decreases, BER (Bit Error Rate) increases as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but with lower BER



QAM=Quadrature Amplitude Modulation

$\text{QAM}2^n = n \text{ bits/Hz}$

dB = Deci-Bel

$$= 10 \log_{10} \frac{\text{Power Out}}{\text{Power In}}$$

# 802.11: advanced capabilities

## power management

- A node can be in one of three states:
  - Transmitter on
  - Receiver only on
  - Dozing: Both transmitter and receivers off.
- AP buffers traffic for dozing nodes.
- node-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobile nodes with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

# Chapter 7 outline

- Introduction

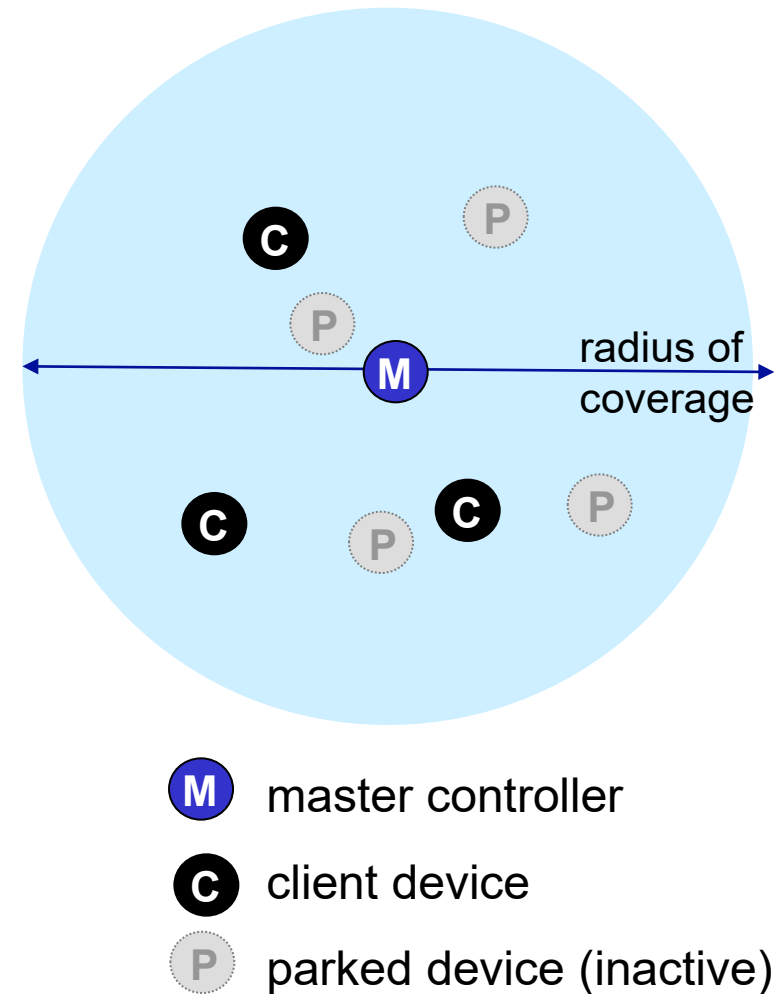
## Wireless

- Wireless links and network characteristics
- CDMA: code division multiple access
- WiFi: 802.11 wireless LANs
- Bluetooth



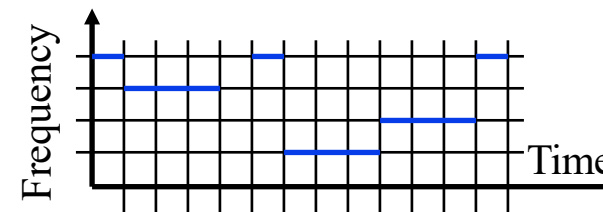
# Personal area networks: Bluetooth

- 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



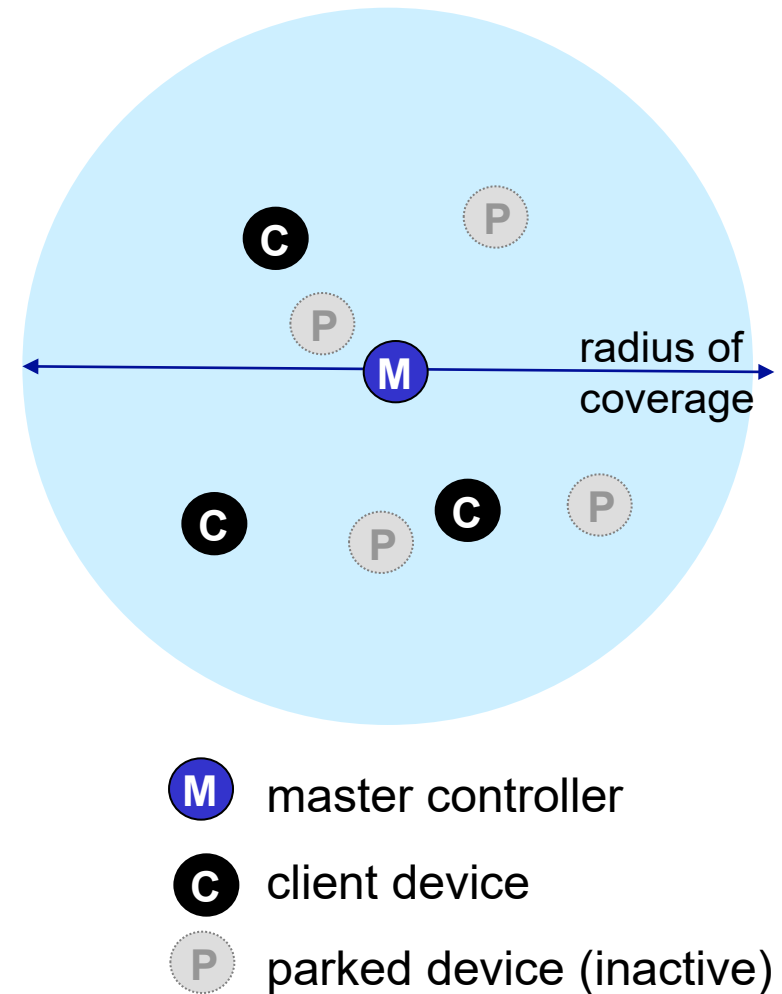
# Personal area networks: Bluetooth

- Started with Ericsson's Bluetooth Project in 1994
- Named after Danish king Herald Blatand (AD 940-981) who was fond of blueberries
- Radio-frequency communication between cell phones over short distances
- IEEE 802.15.1 approved in early 2002 is based on Bluetooth
- Key Features:
  - Lower Power: 10 mA in standby, 50 mA while transmitting
  - Cheap: \$5 per device
- A piconet consists of a master and several slaves. Master determines the timing and polls slaves for transmission.
- Frequency hopping spread spectrum



# Personal area networks: Bluetooth

- TDM, 625  $\mu$ sec sec. slot
- FDM: sender uses 79 frequency channels in known, pseudo-random order slot-to-slot (spread spectrum)
  - other devices/equipment not in piconet only interfere in some slots
- **parked mode:** clients can “go to sleep” (park) and later wakeup (to preserve battery)
- **bootstrapping:** nodes self-assemble (plug and play) into piconet





# Summary

- IEEE 802.11 PHYs: 11, 11b, 11g, 11a, 11n, ...
- IEEE 802.11 MAC uses CSMA/CA with a 4-way handshake: RTS, CTS, data, and ack
- IEEE 802.11 network consists of ESS consisting of multiple BSSs each with an AP.
- 802.11 Frame Format may have up to 4 addresses and includes final destination's MAC which may not be wireless
- Power management allows stations to sleep.
- Bluetooth uses frequency hopping spread spectrum