

# Chapter 7

## Wireless and Mobile Networks

A note on the use of these PowerPoint slides:

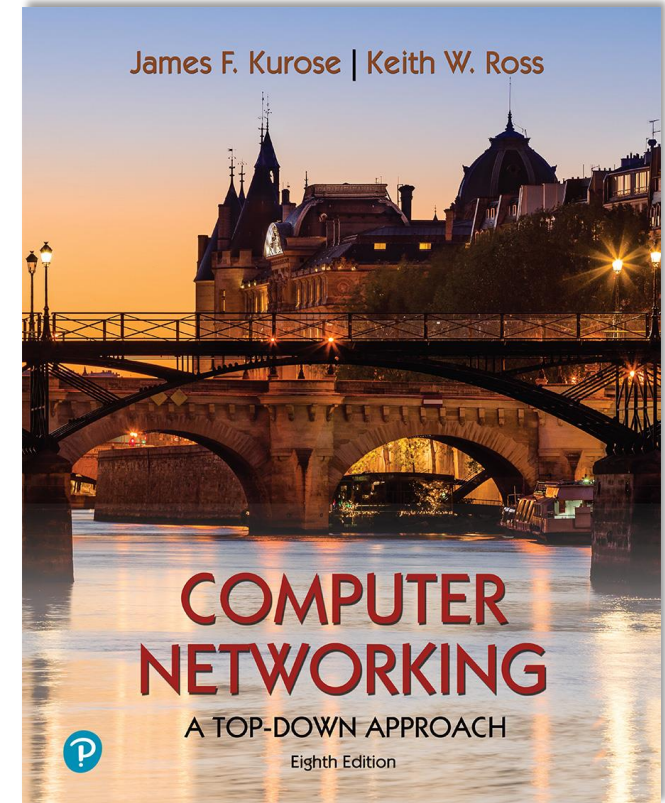
We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

For a revision history, see the slide note for this page.

Thanks and enjoy! JFK/KWR

All material copyright 1996-2023  
J.F Kurose and K.W. Ross, All Rights Reserved



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

8<sup>th</sup> edition

Jim Kurose, Keith Ross  
Pearson, 2020

# Chapter 7 outline

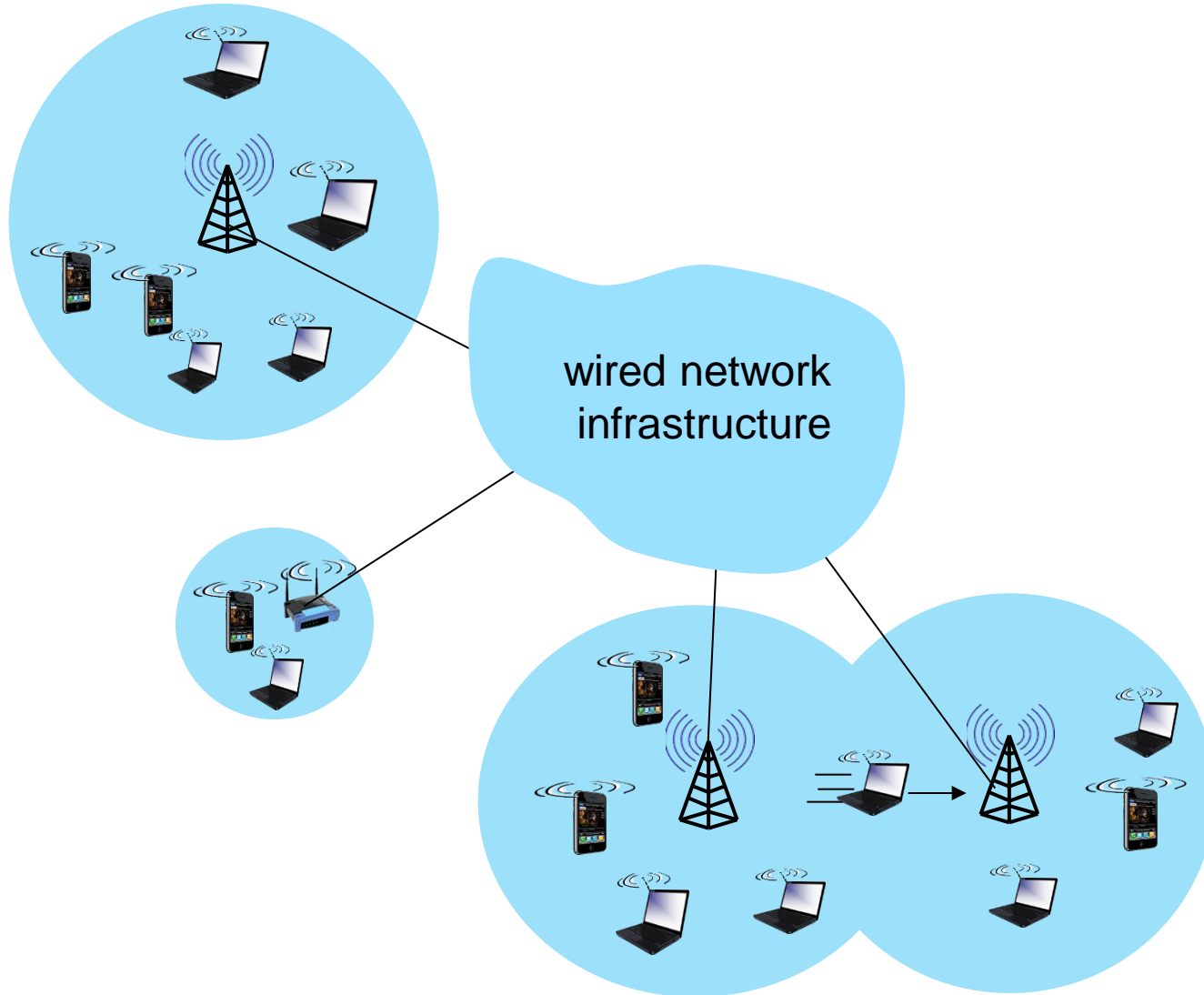
- Introduction

## Wireless

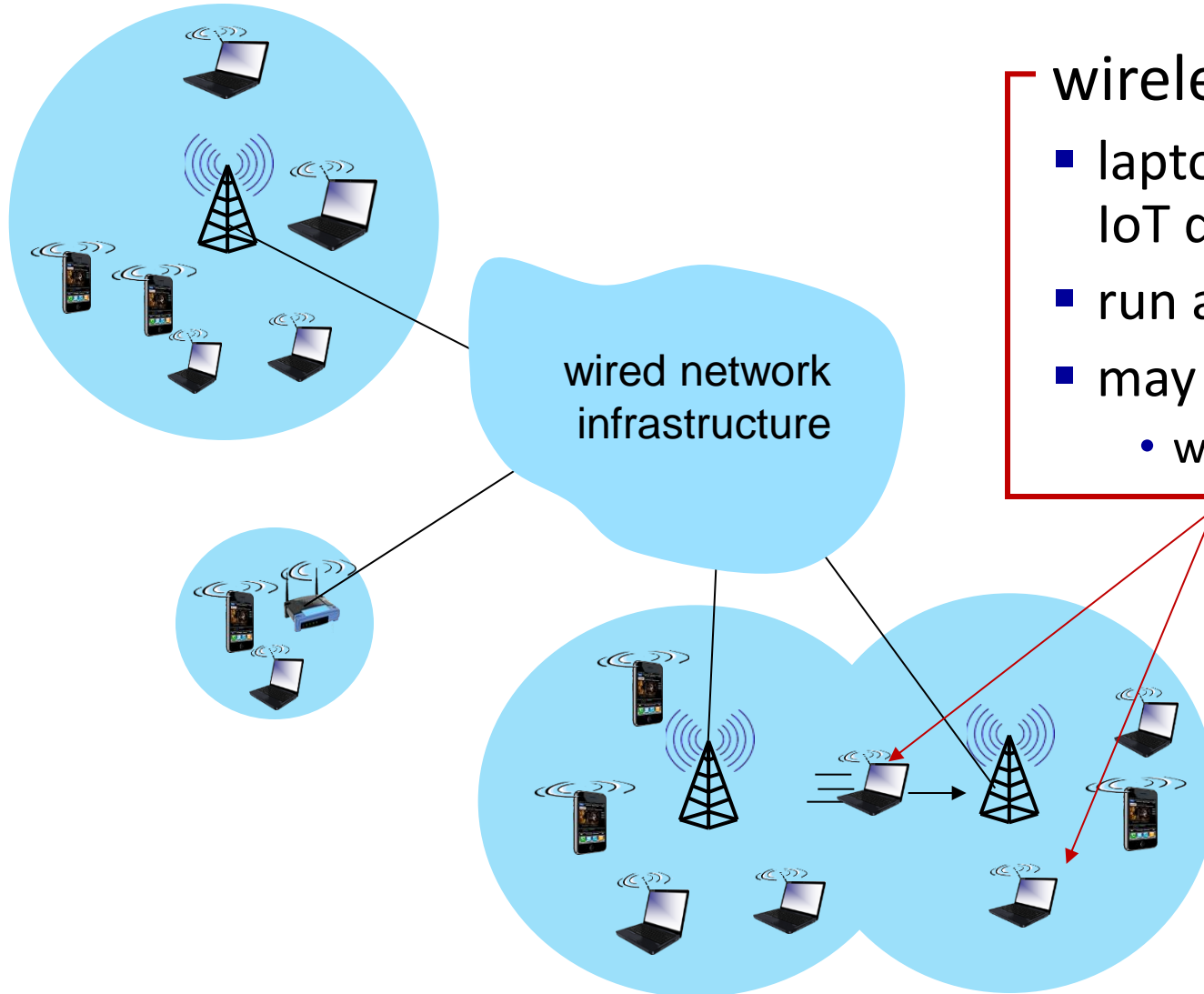
- Wireless Links and network characteristics
- WiFi: 802.11 wireless LANs



# Elements of a wireless network



# Elements of a wireless network

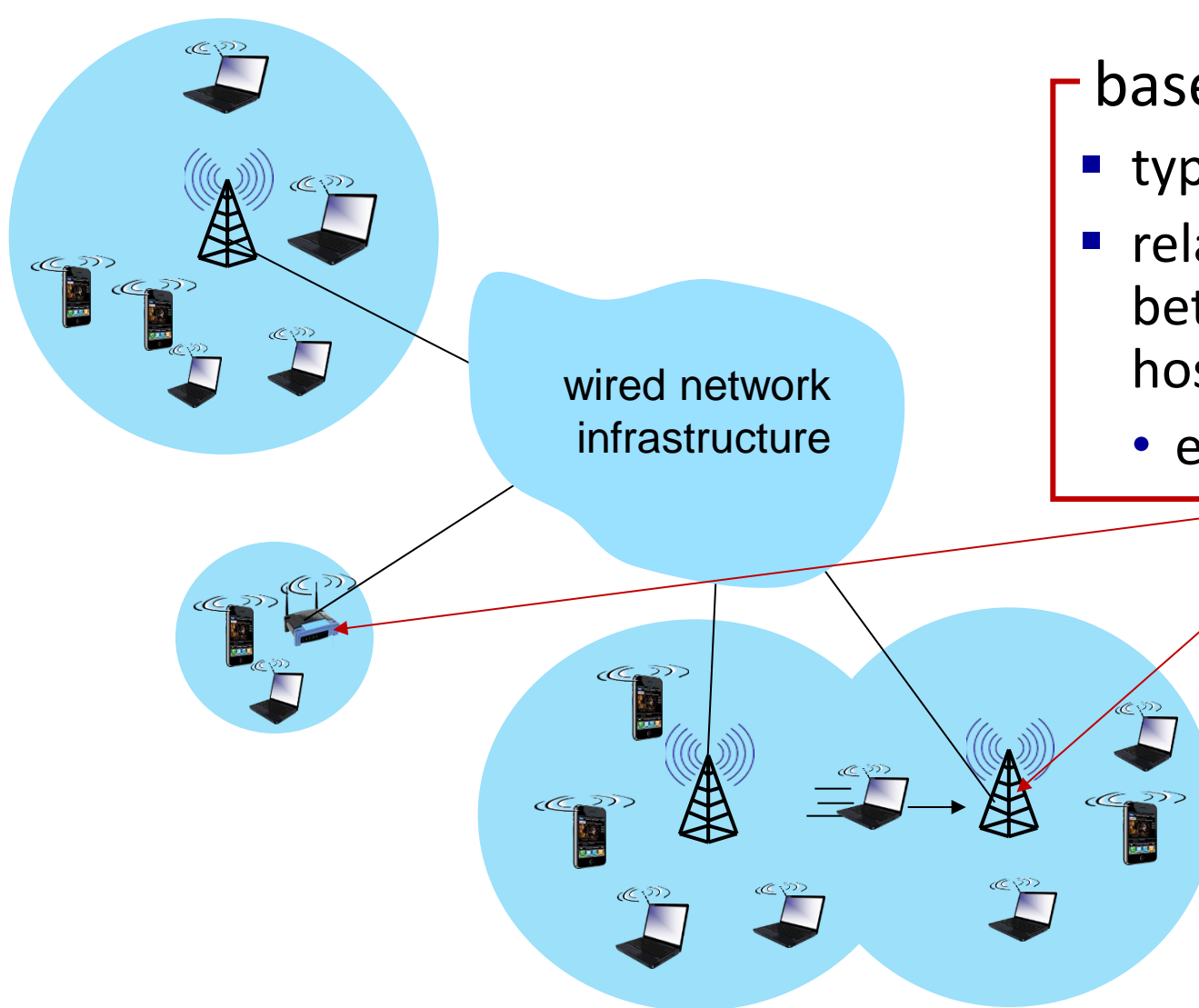


## wireless hosts

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



# Elements of a wireless network

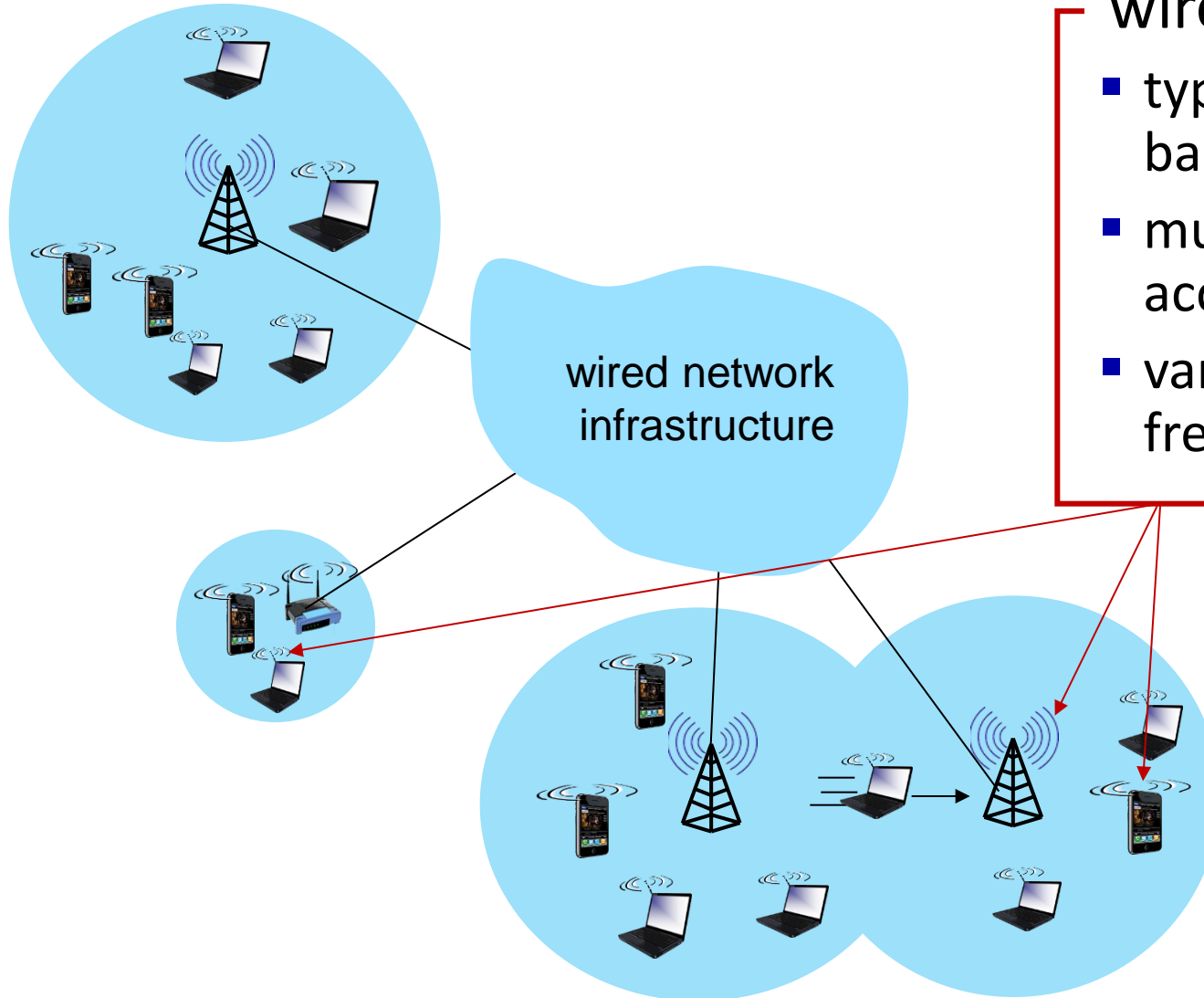


base station



- 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

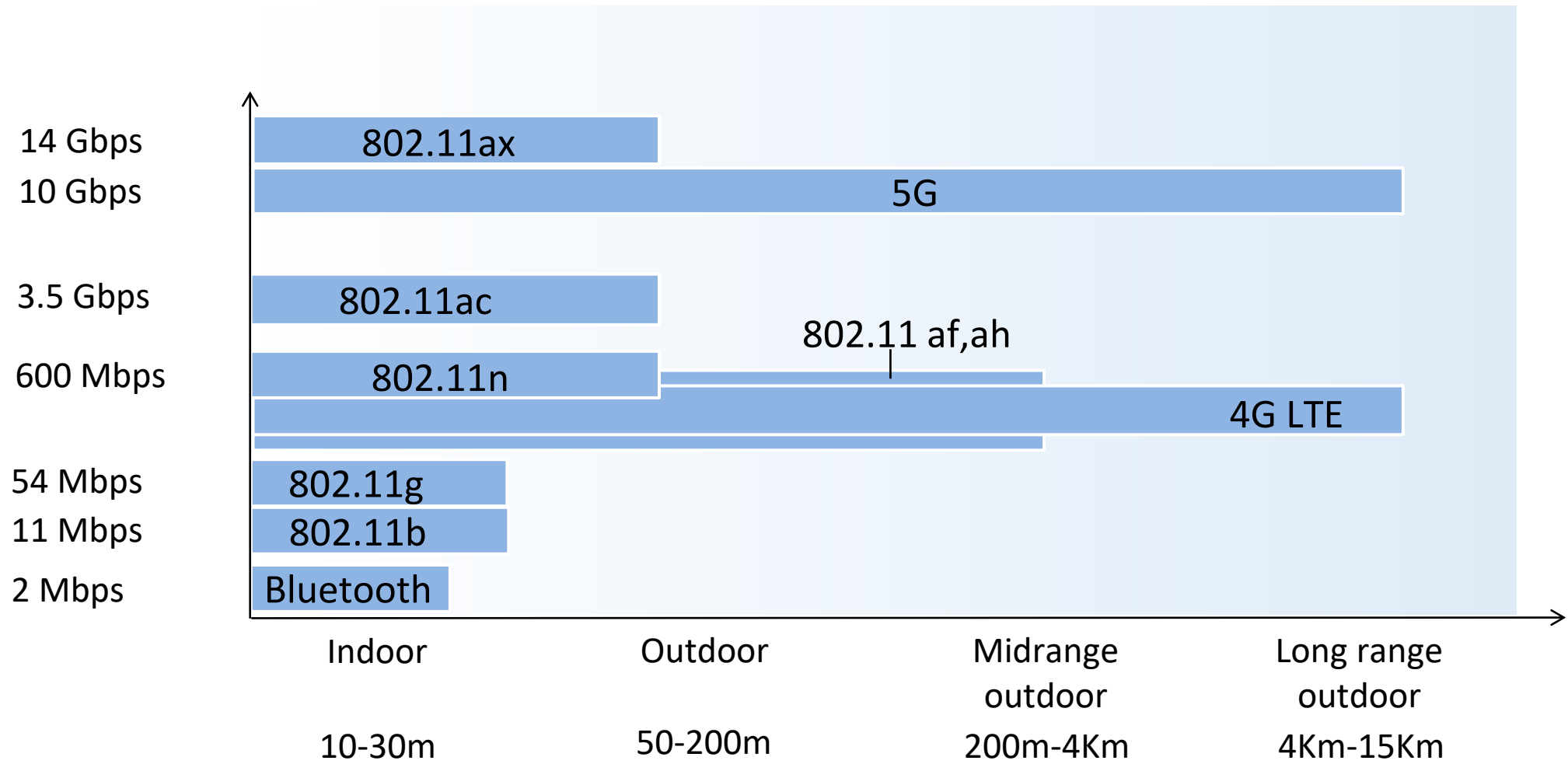


wireless link

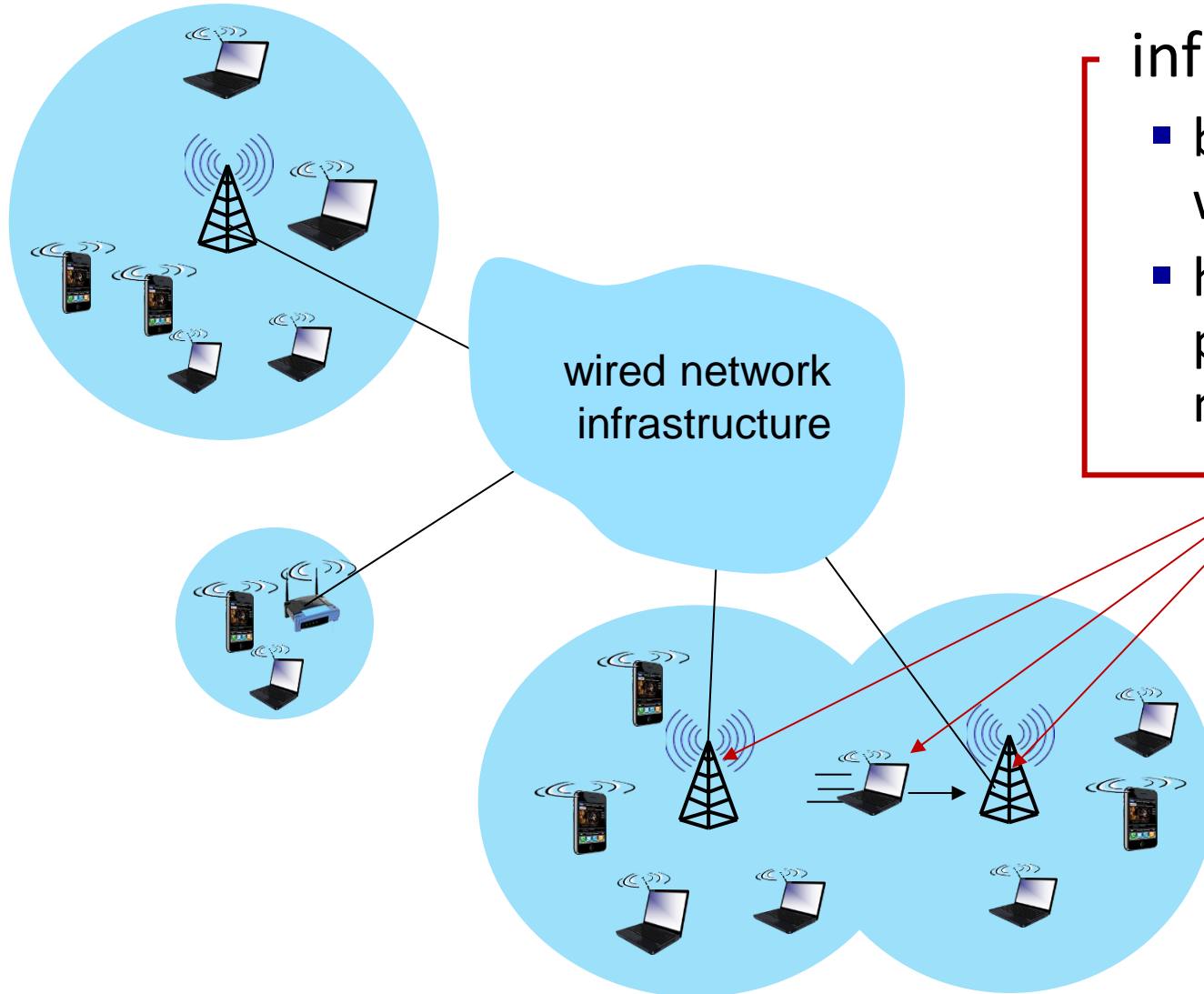


- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

# Characteristics of selected wireless links



# Elements of a wireless network

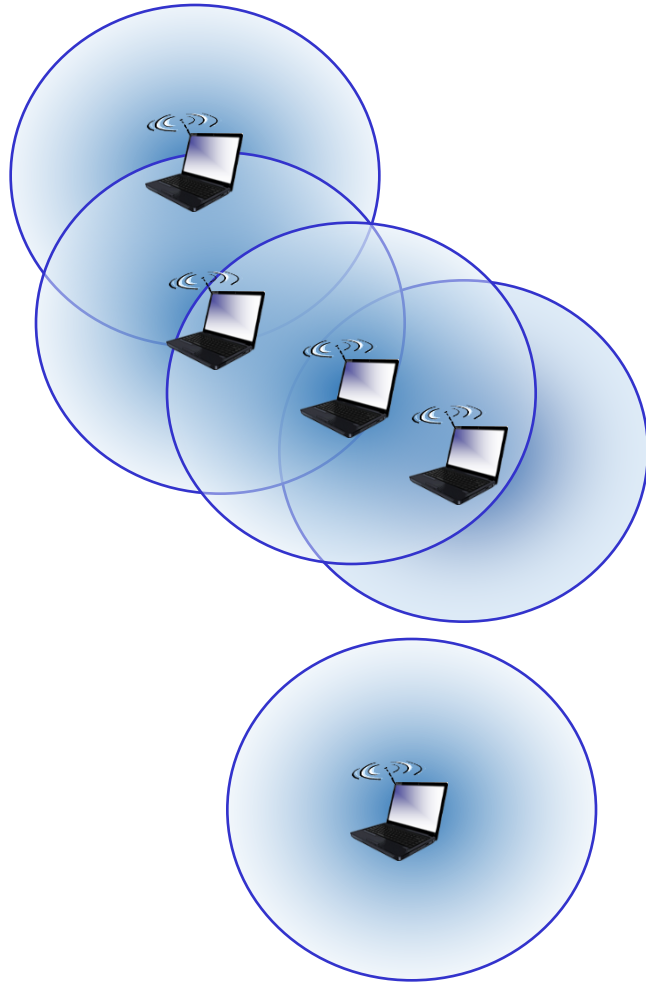


## infrastructure mode

- 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



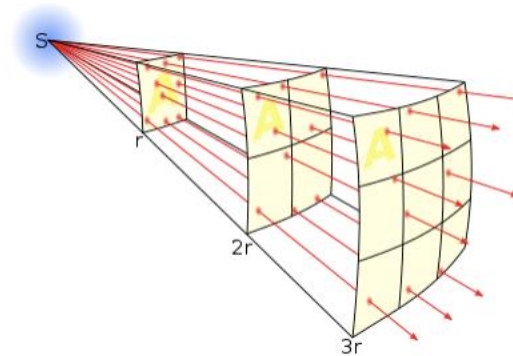
# Wireless link characteristics: fading (attenuation)

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

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

$f$ : frequency

$d$ : distance



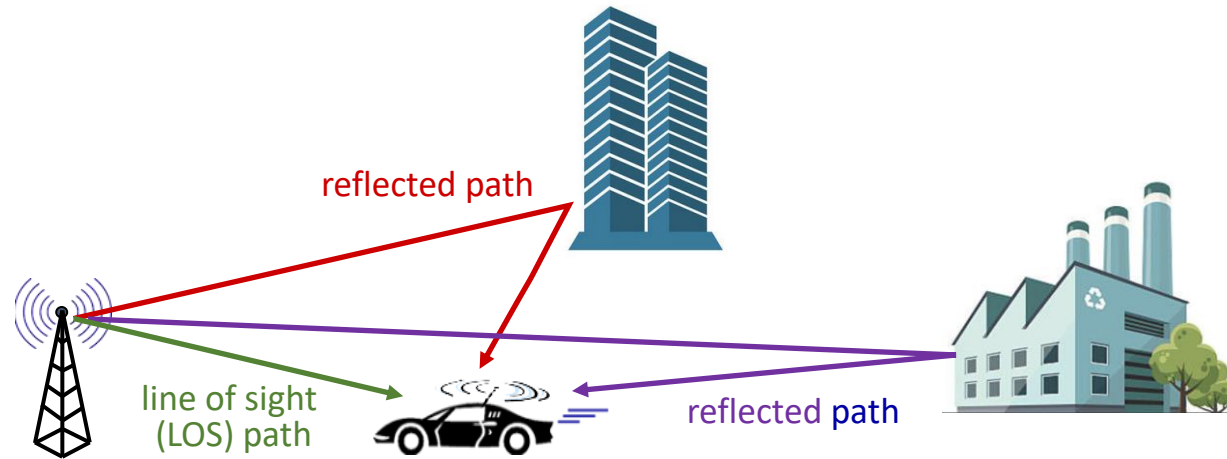
higher frequency or  
longer distance



larger free space  
path loss

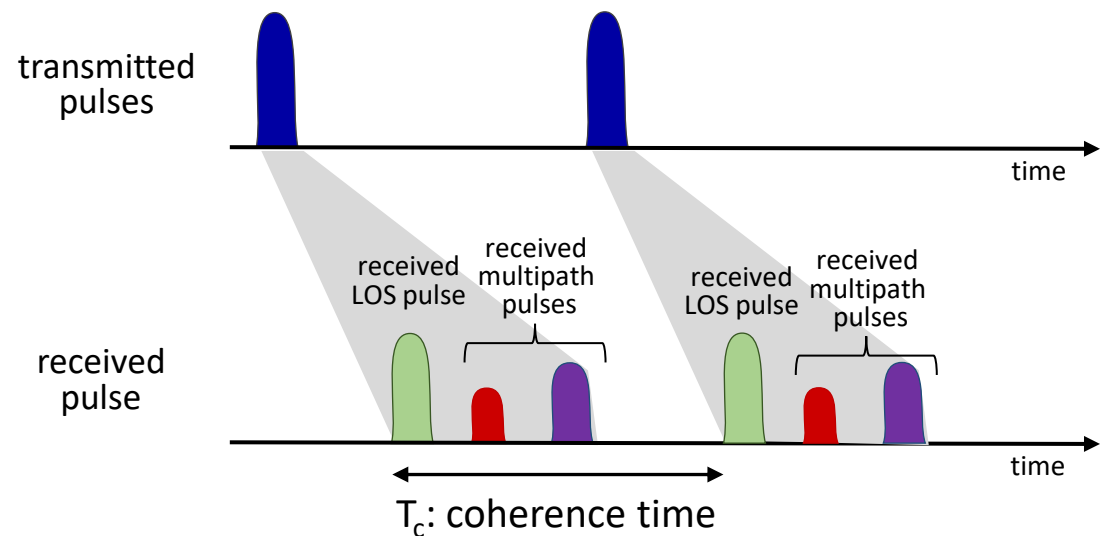
# Wireless link characteristics: multipath

**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

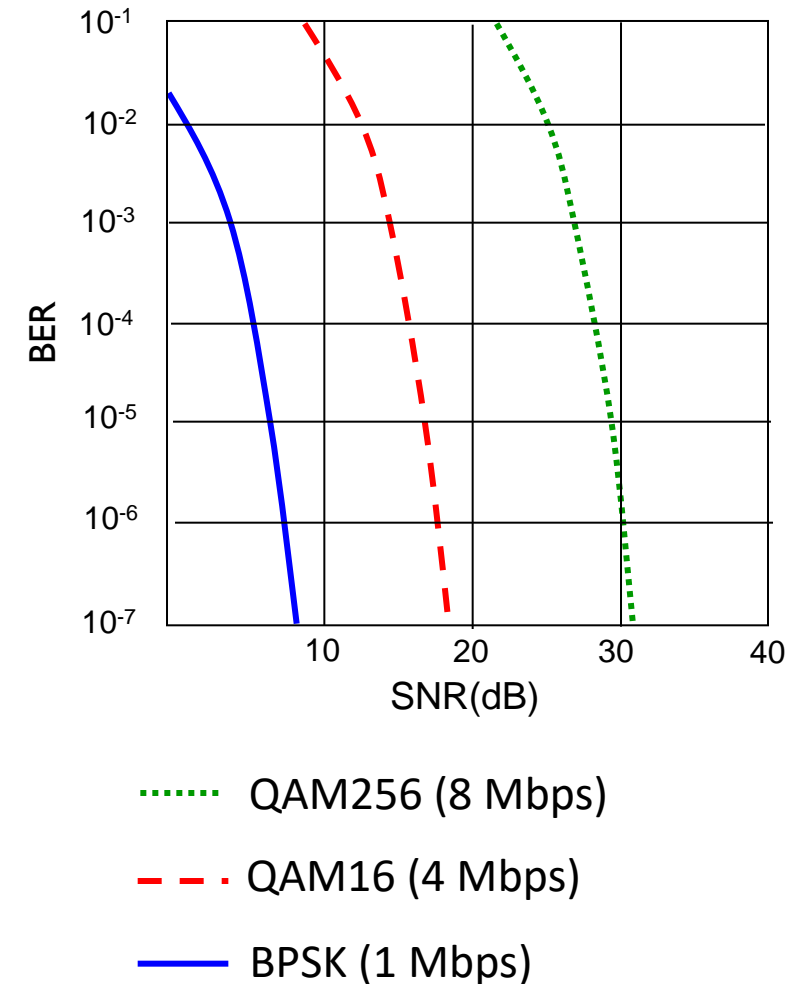


## Coherence time:

- 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

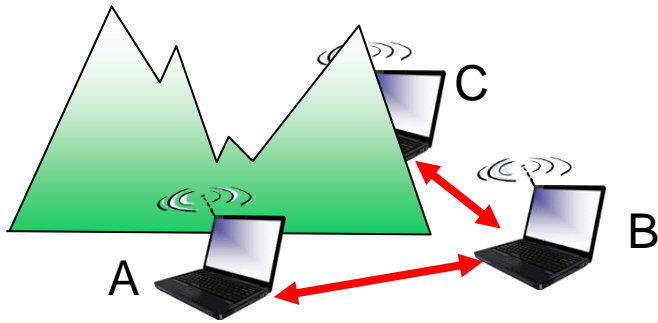
# Wireless link characteristics: noise

- **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)



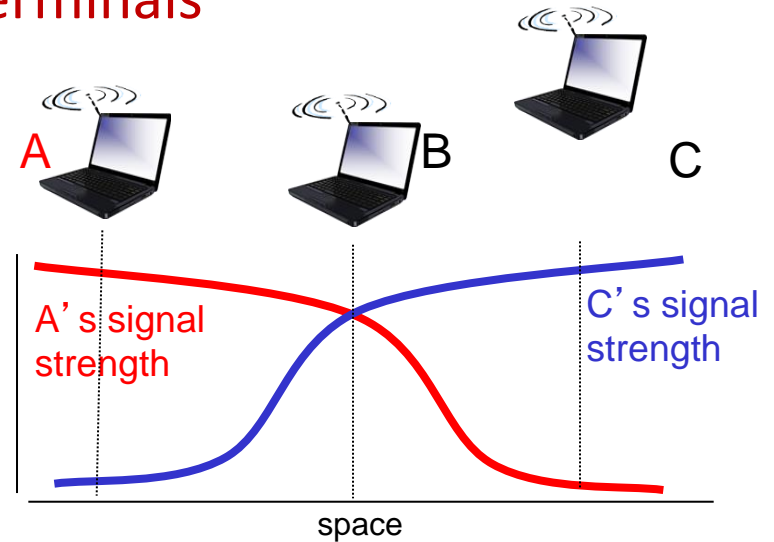
# Wireless link characteristics: hidden terminals

## 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
- WiFi: 802.11 wireless LANs



# IEEE 802.11 Wireless LAN Technology

## 802.11b

- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer
  - all hosts use same chipping code

## 802.11a

- 5-6 GHz range
- up to 54 Mbps

## 802.11g

- 2.4-5 GHz range
- up to 54 Mbps

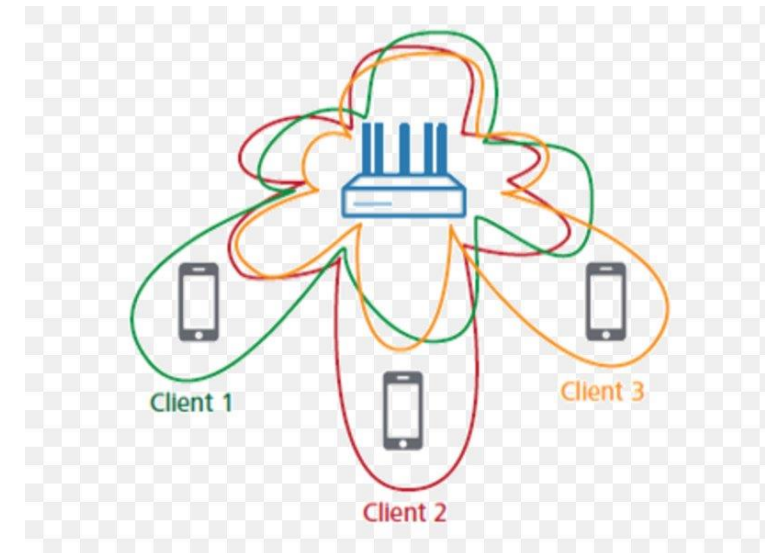
## 802.11n: multiple antennae

- 2.4-5 GHz range
- up to 450 Mbps

## 802.11ac

- 5 GHz range
- up to 1300 Mbps

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

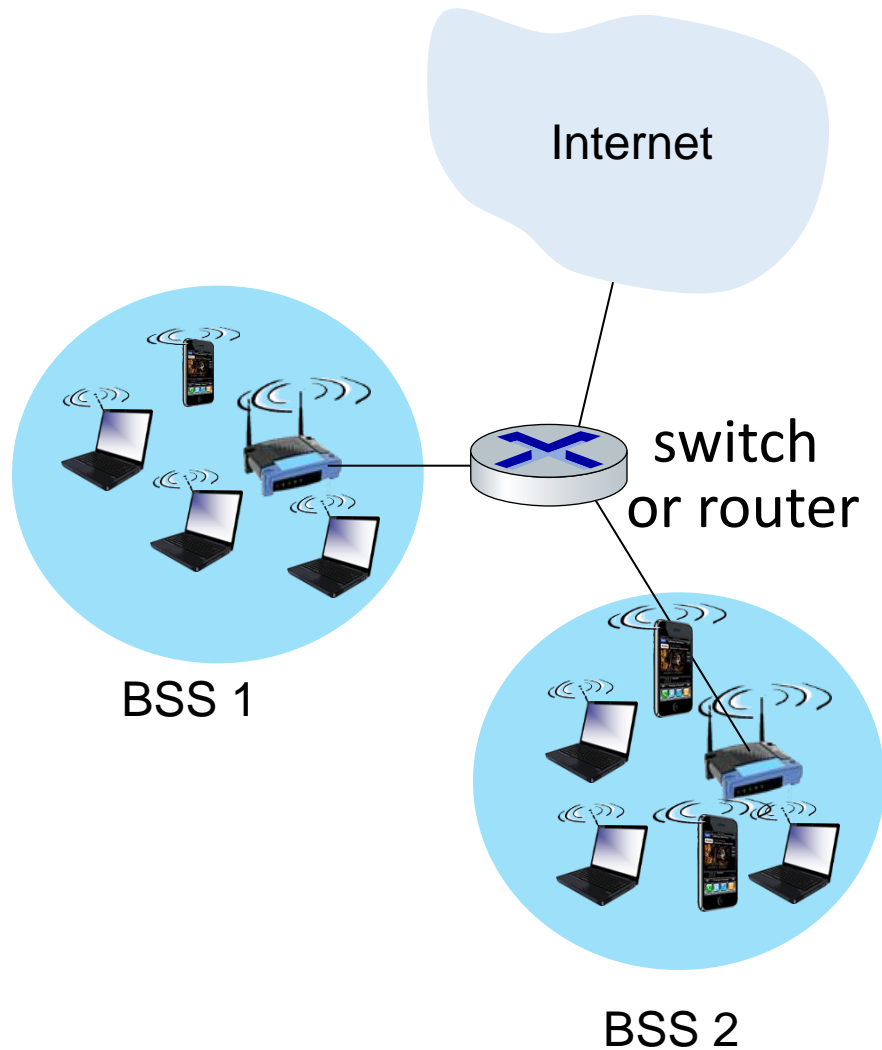


# IEEE 802.11 Wireless LAN

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

# 802.11 LAN architecture

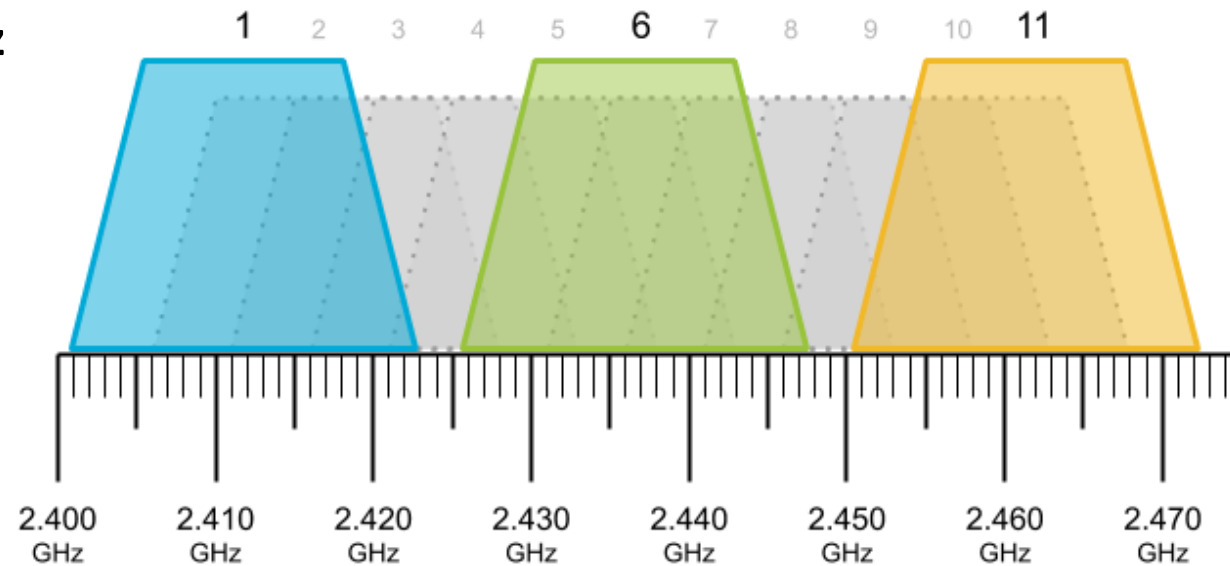


- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

# 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**

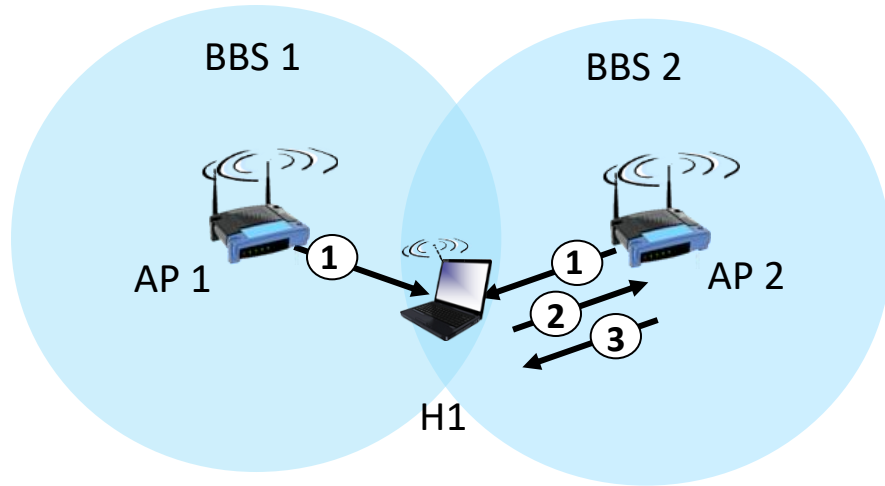


# 802.11: Association

- 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

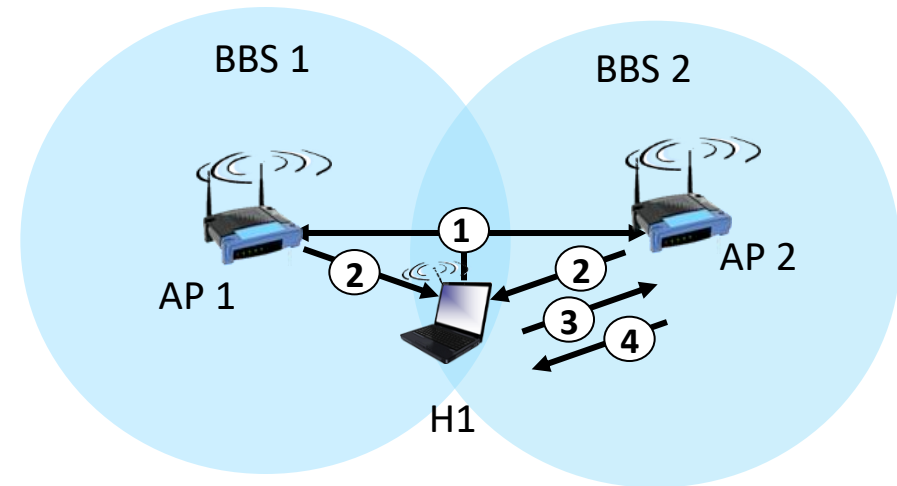


# 802.11: passive/active scanning



## 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

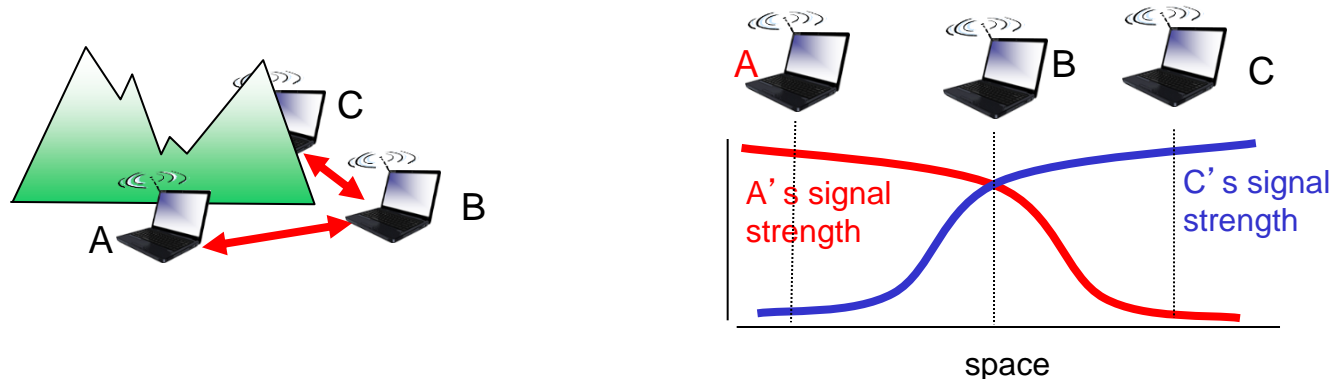


## active scanning:

- (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





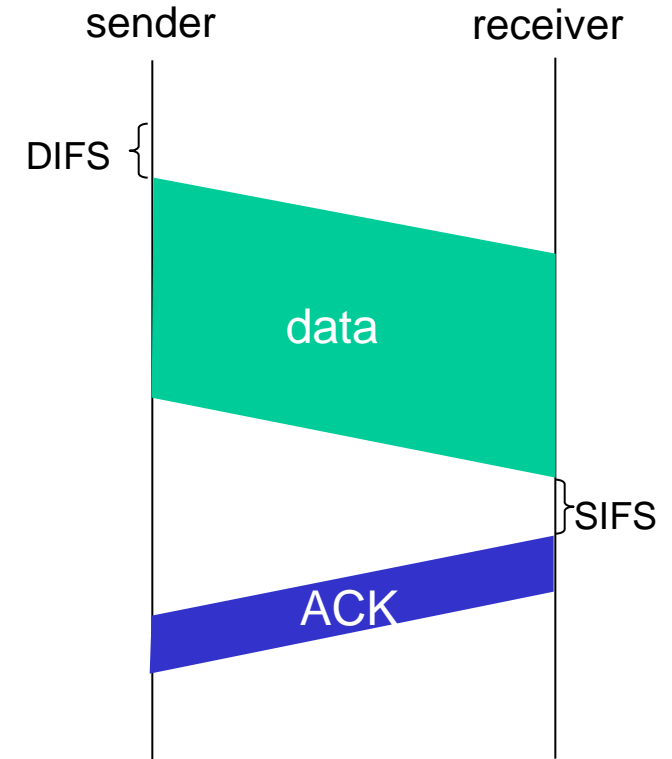
# IEEE 802.11 MAC Protocol: CSMA/CA

## 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)



# 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

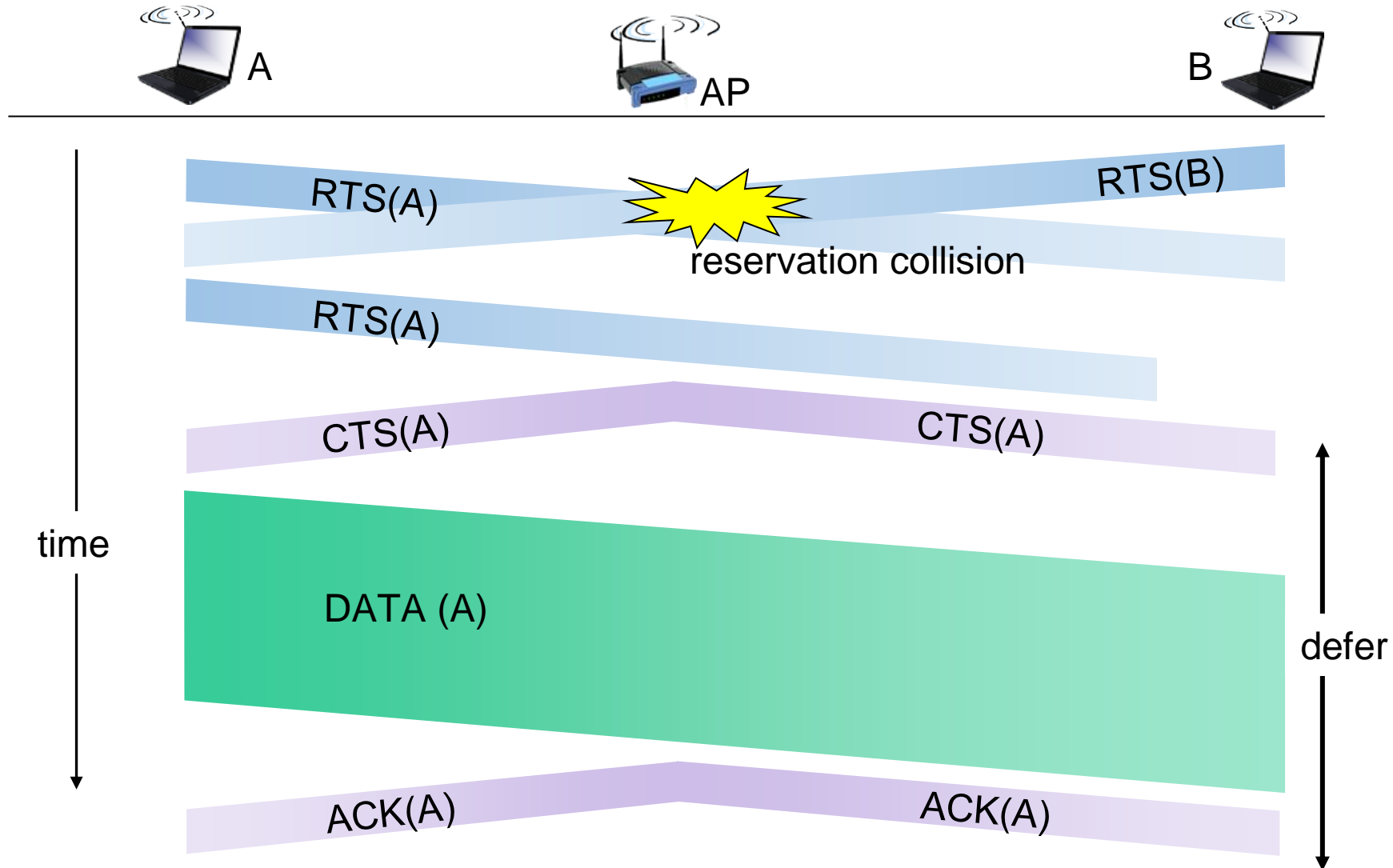
*avoid data frame collisions completely  
using small reservation packets!*

# RTS and CTS

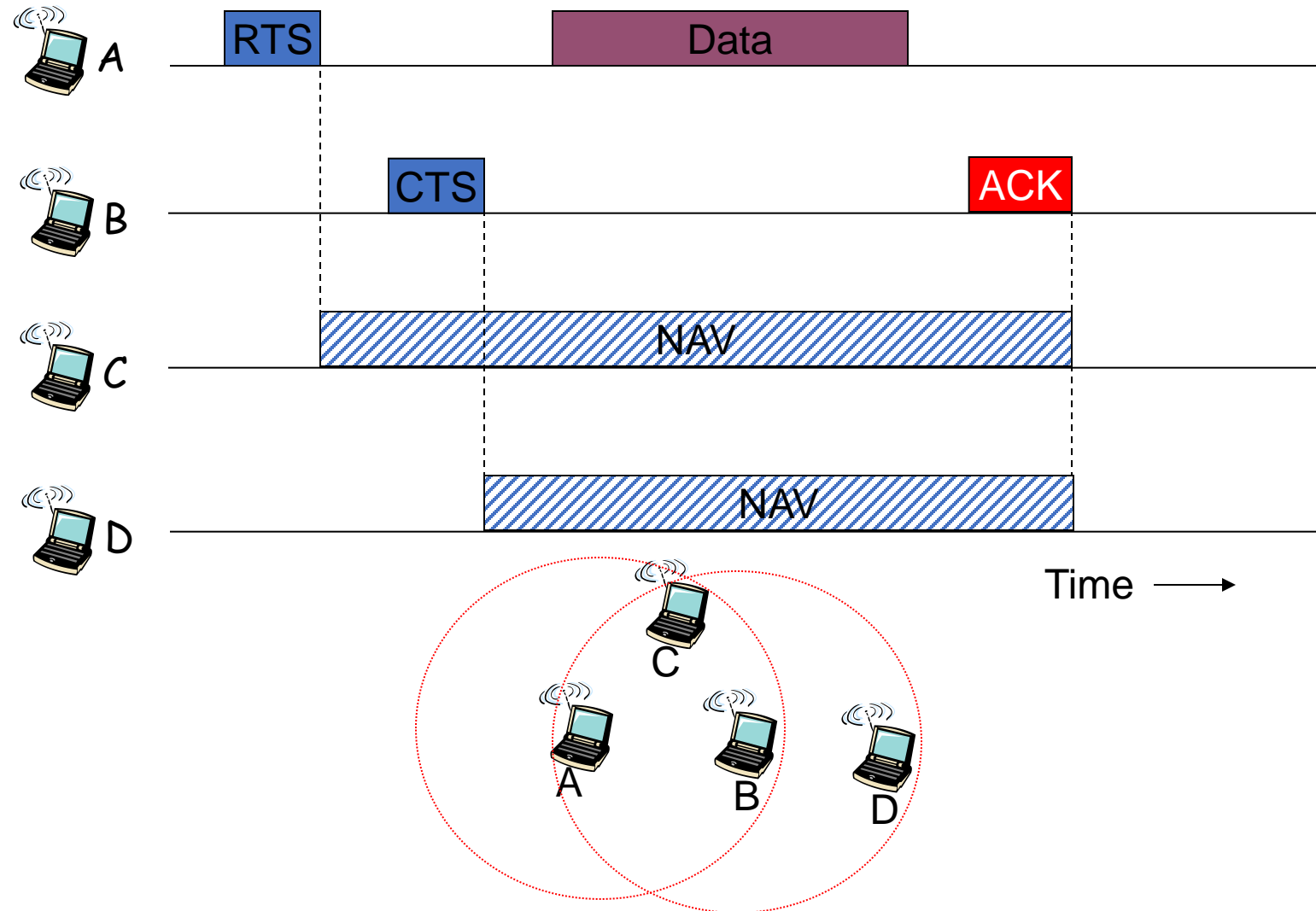
- RTS indicates the duration of data packet and ACK packet.
  - This time duration is called **NAV** (Network Allocation Vector)
- CTS gives explicit permission and transmission period.
- All stations hearing the RTS/CTS then know about the pending data transmission and can avoid interfering with other transmission.

IEEE 802.11 sender either can operate using the RTS/CTS control frames or can simply send its data without first using the RTS control frame.

# Collision Avoidance: RTS-CTS exchange

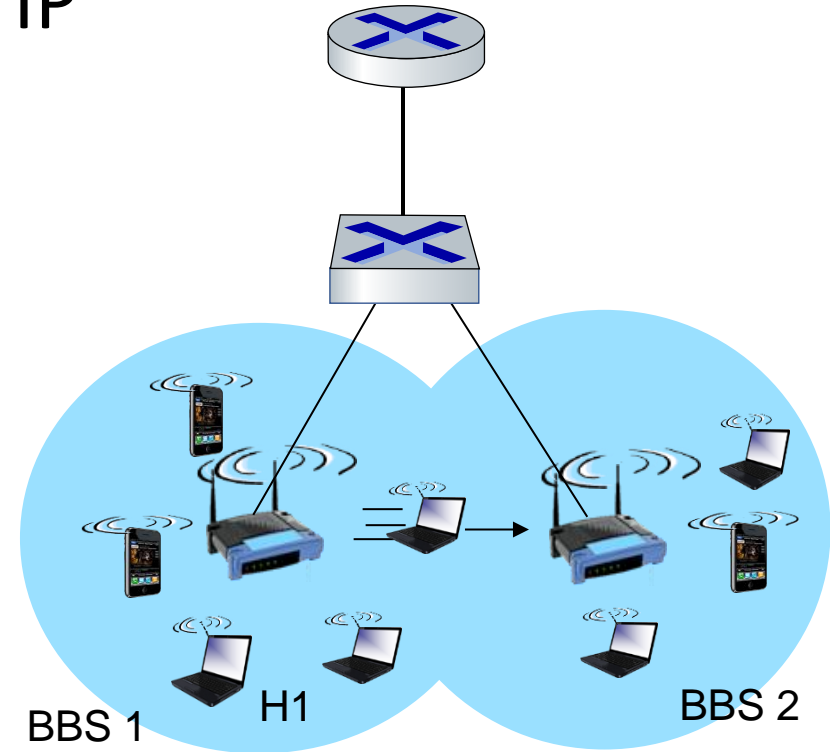


# Virtual Channel Sensing Using CSMA/CA



# 802.11: mobility within same subnet

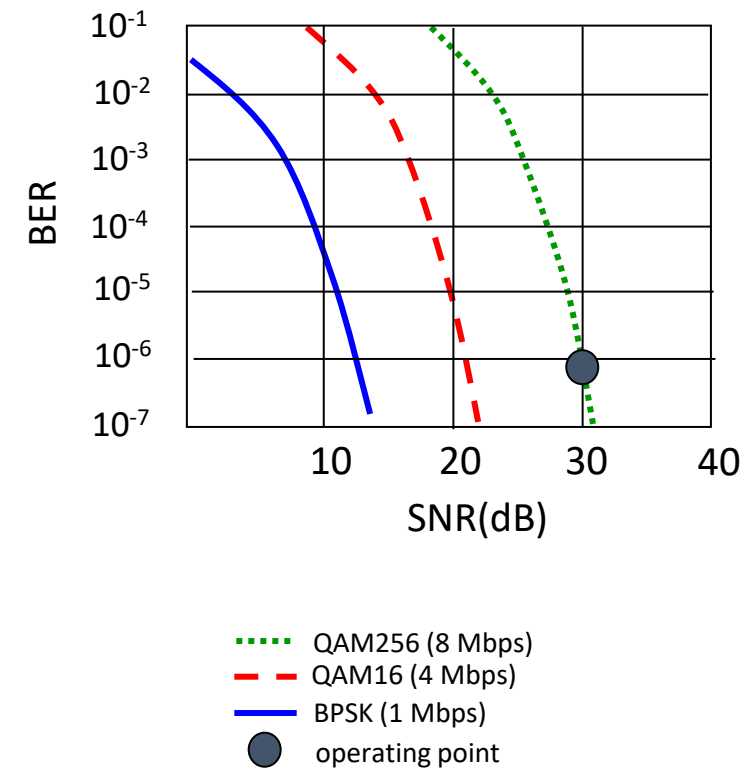
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 6): switch will see frame from H1 and “remember” which switch port can be used to reach H1



# 802.11: advanced capabilities

## Rate adaptation

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



# 802.11: advanced capabilities

## power management

- 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 mobiles 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



# Wireless: impact on higher layer protocols

- logically, impact *should* be minimal ...
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- ... but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handover loss
  - TCP interprets loss as congestion, will decrease congestion window unnecessarily
  - delay impairments for real-time traffic
  - bandwidth a scarce resource for wireless links