



Computer Networks II

Lecture No. 5 *Wireless LAN*

4th Year/ 1st semester

DR. Lecturer . Taqwa.F.Hassan

Computer Department - College of Engineering
University of Diyala

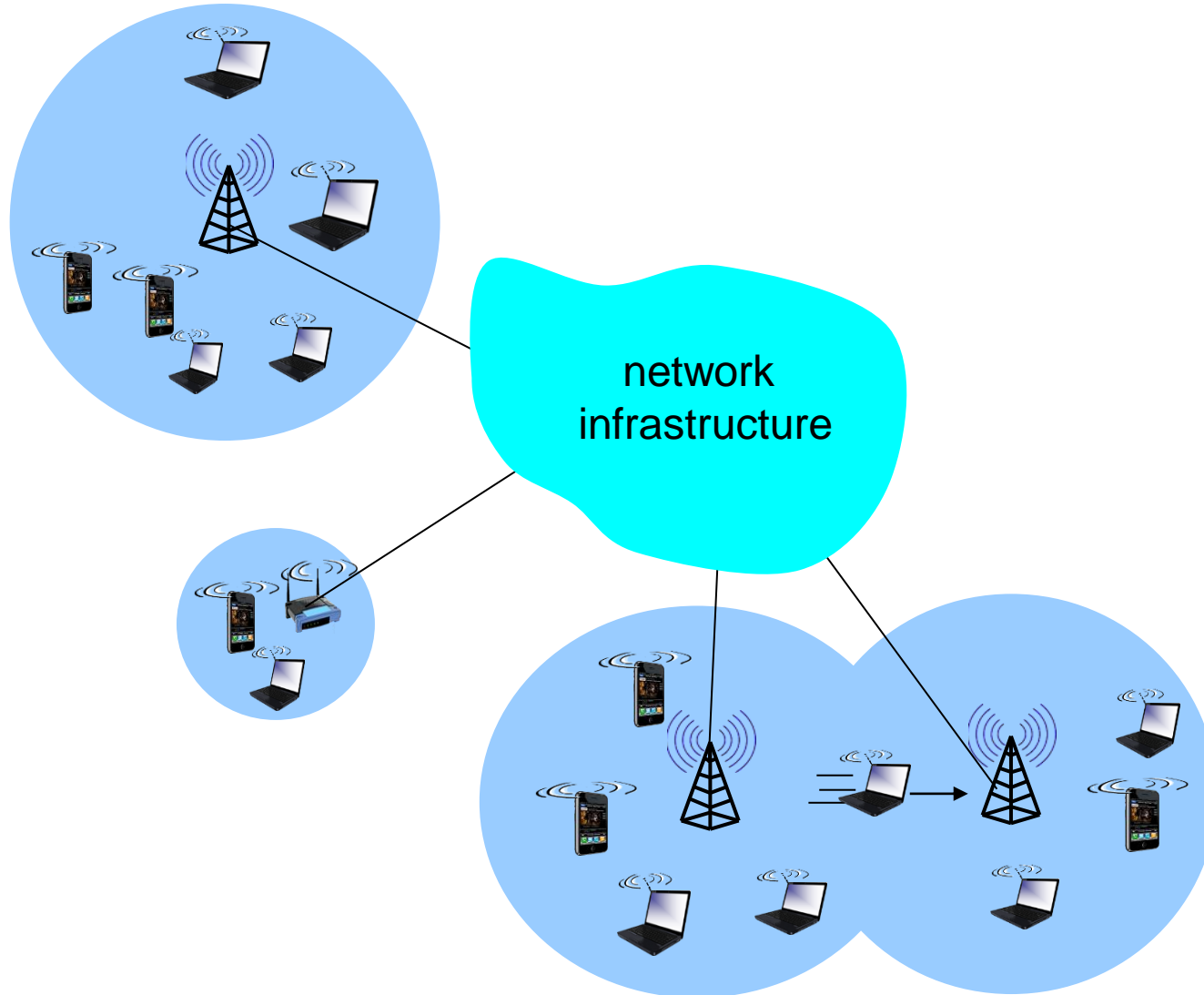
2021-2022

Wireless and Mobile Networks

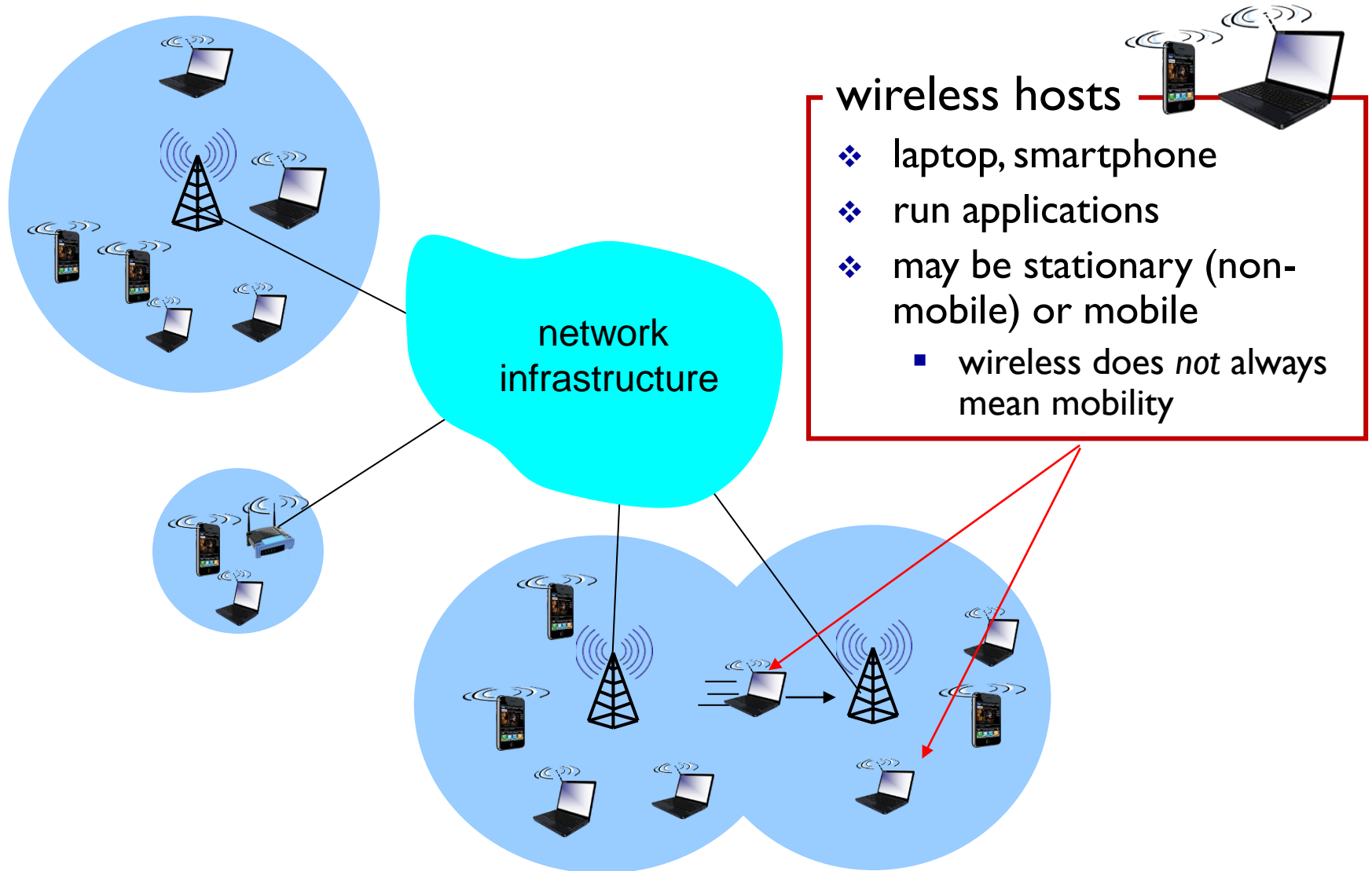
Background:

- ❖ # wireless (mobile) phone subscribers now exceeds # wired phone subscribers (5-to-1)!
- ❖ # wireless Internet-connected devices equals # wireline Internet-connected devices
 - laptops, Internet-enabled phones promise anytime untethered Internet access
- ❖ two important (but different) challenges
 - *wireless*: communication over wireless link
 - *mobility*: handling the mobile user who changes point of attachment to network

Elements of a wireless network



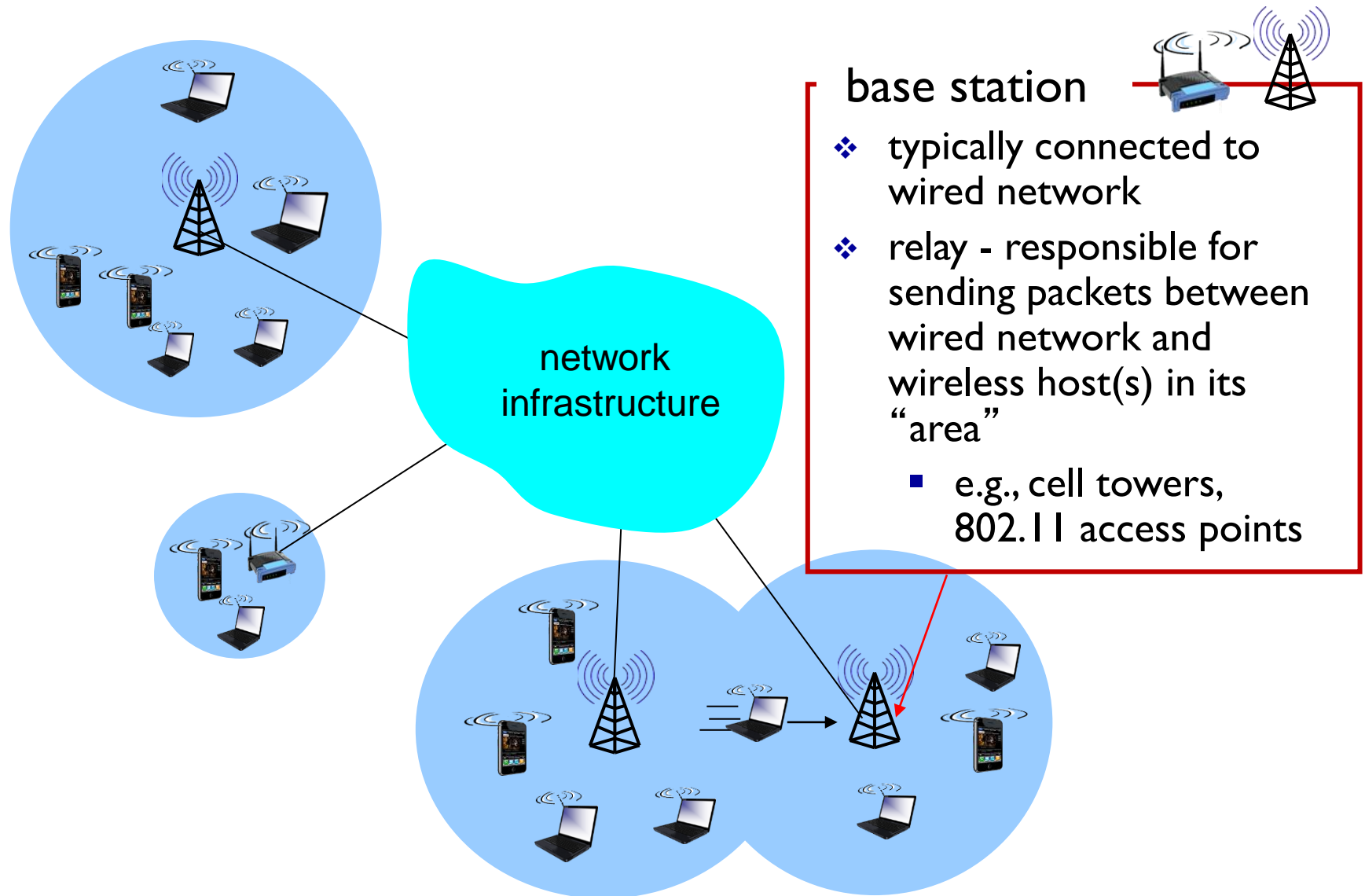
Elements of a wireless network



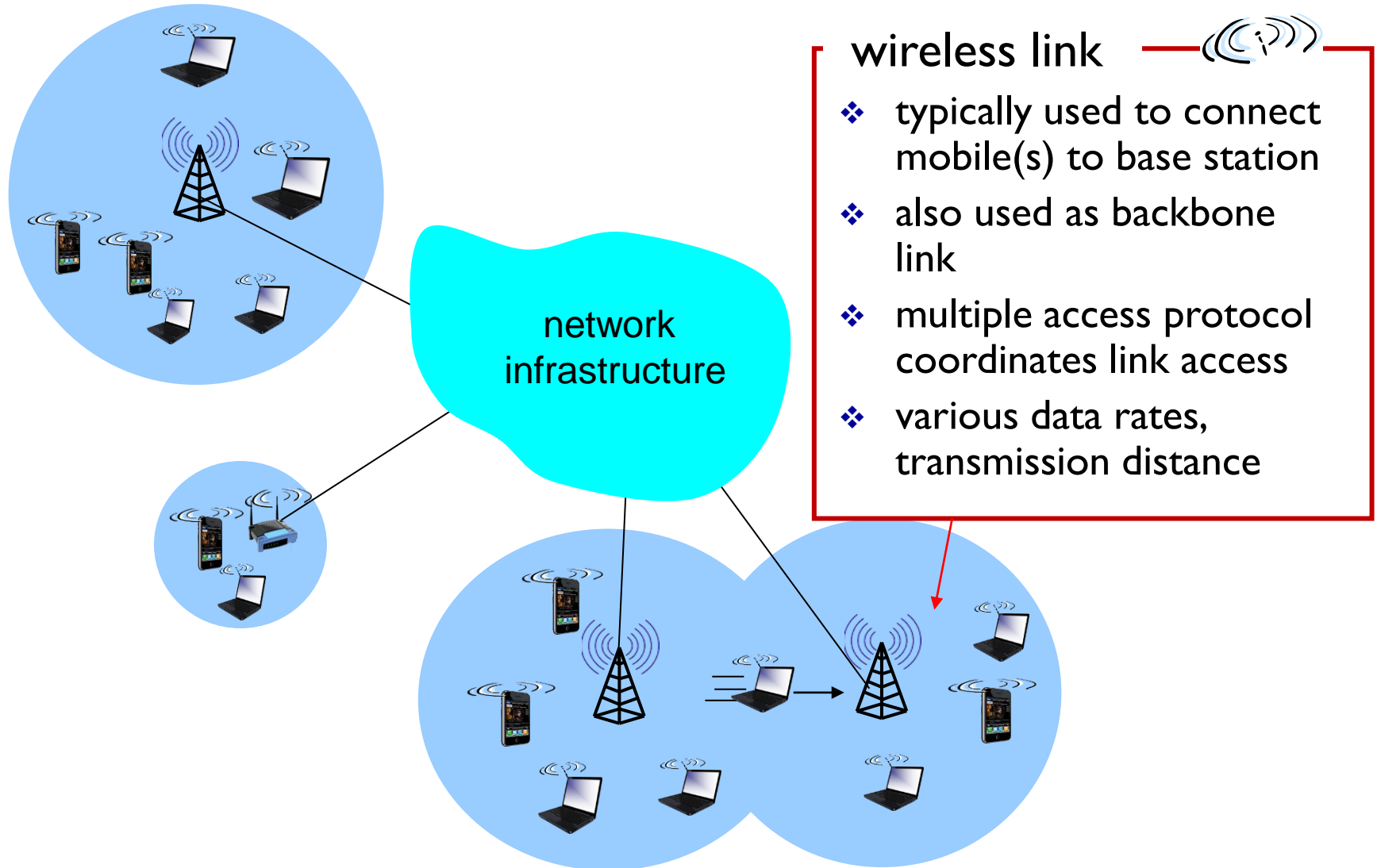
wireless hosts

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

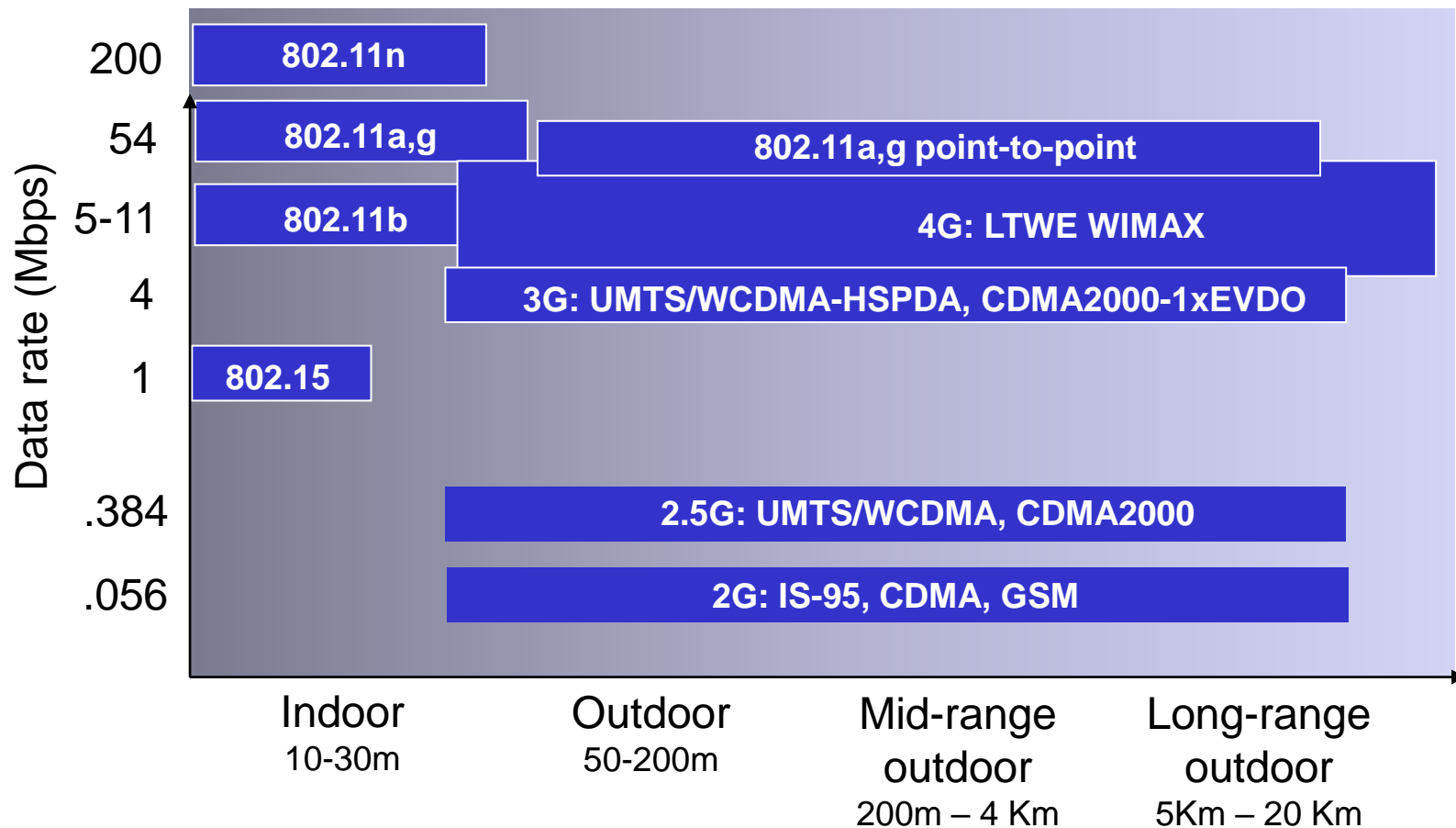
Elements of a wireless network



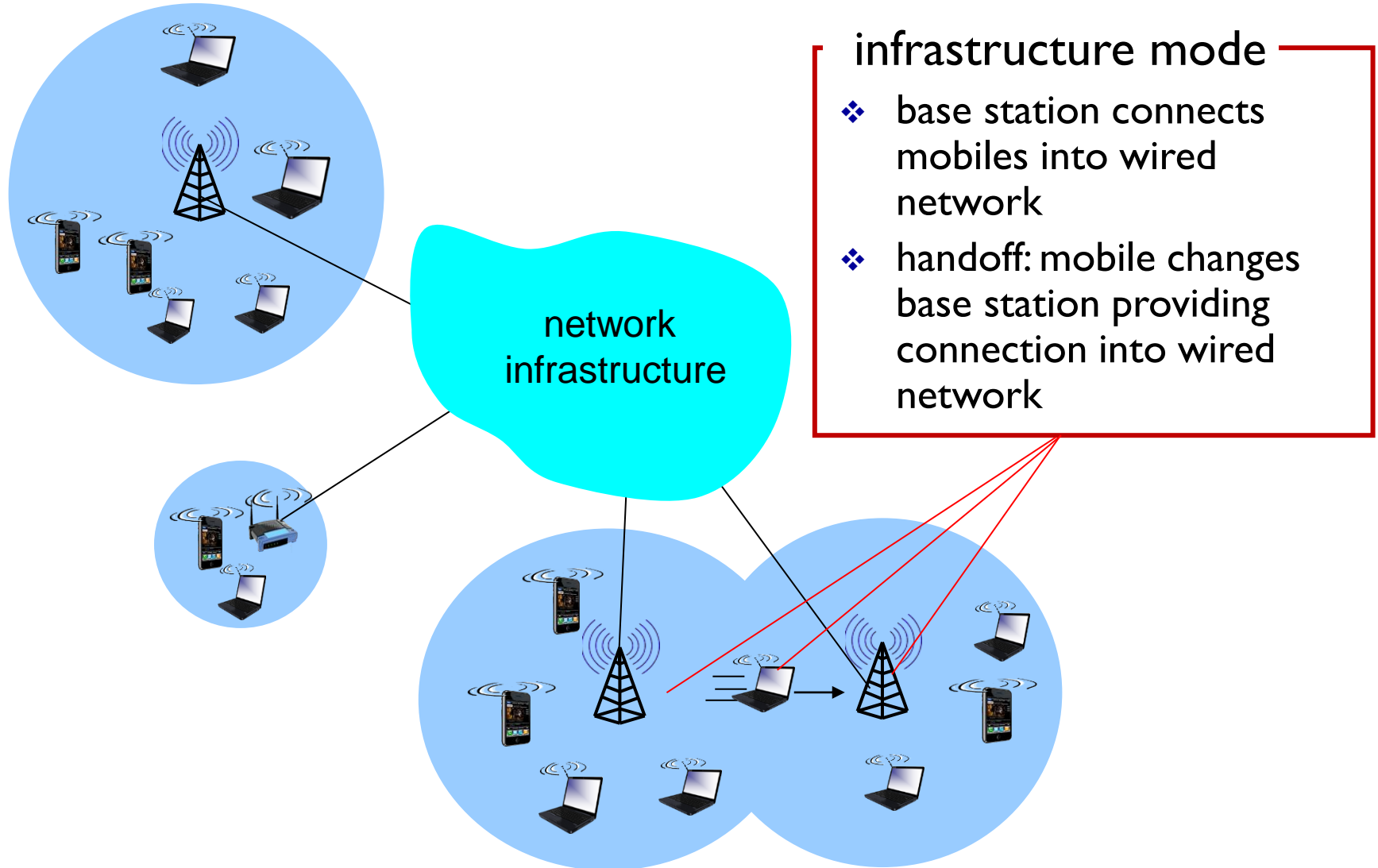
Elements of a wireless network



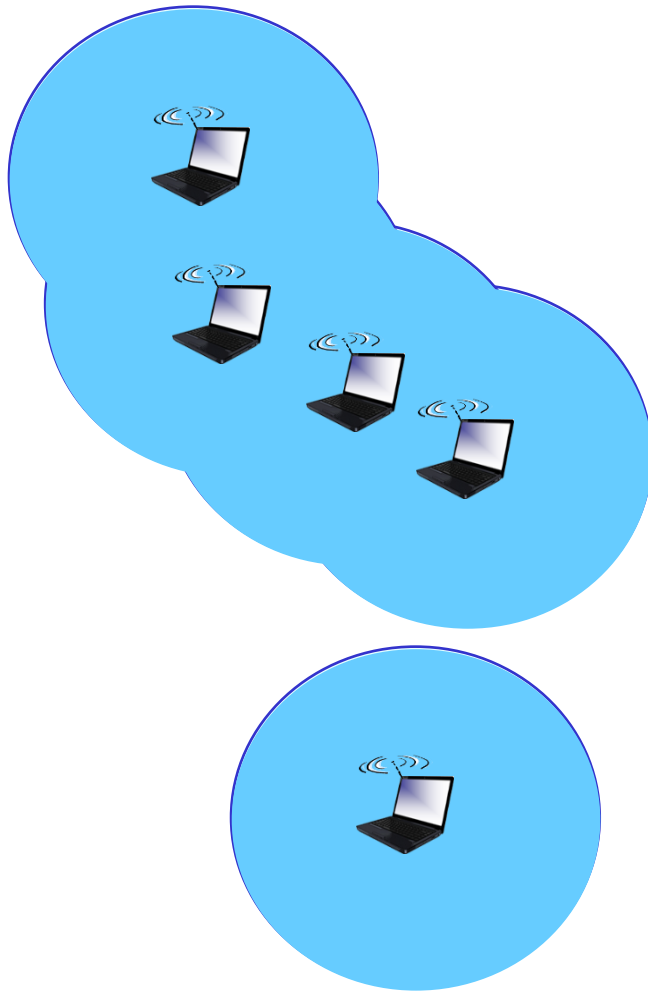
Characteristics of selected wireless links



Elements of a wireless 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, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: <i>mesh net</i>
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 (I)

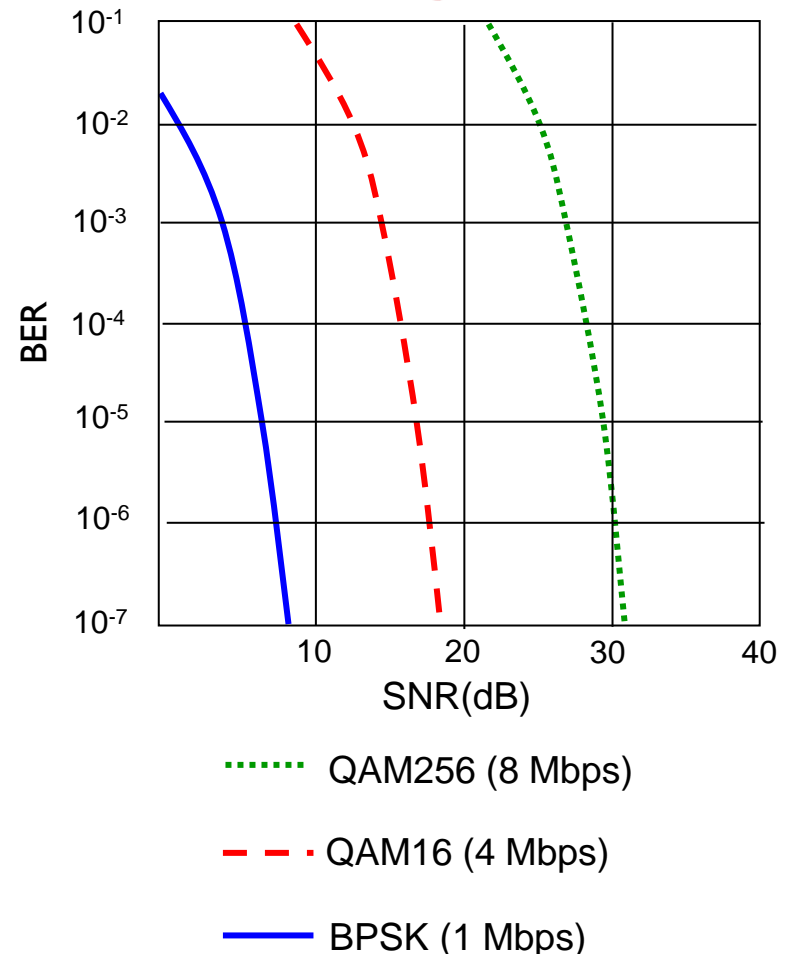
important differences from wired link

- *decreased signal strength*: radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources*: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- *multipath propagation*: radio signal reflects off objects ground, arriving at destination at slightly different times

.... make communication across (even a point to point) wireless link much more “difficult”

Wireless Link Characteristics (2)

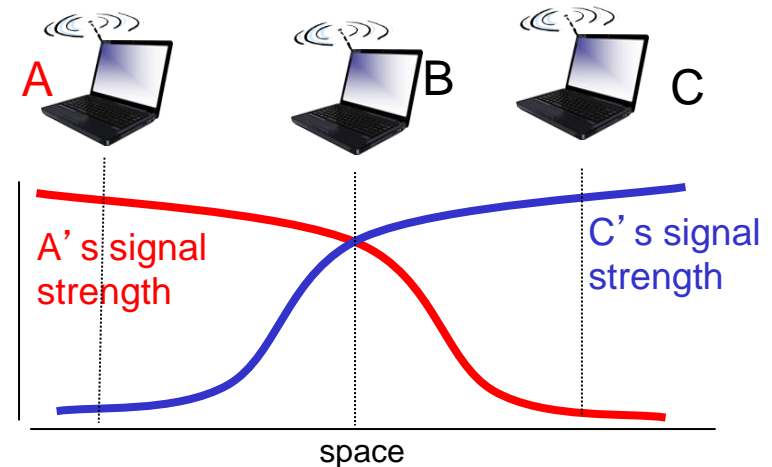
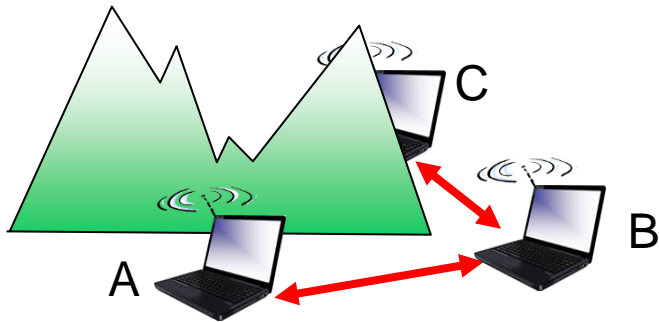
- ❖ SNR: signal-to-noise ratio
 - larger SNR – easier to extract signal from noise (a “good thing”)
- ❖ *SNR versus BER tradeoffs*
 - *given physical layer*: increase power → increase SNR → decrease BER
 - *given SNR*: choose physical layer that meets BER requirement, giving highest throughput
 - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



BER : The **bit error rate (BER)** is the number of bit errors per unit time. The **bit error ratio** (also **BER**) is the number of bit errors divided by the total number of transferred bits during a studied time interval

Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):



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

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”)
- ❖ *encoded signal* = (original data) \times (chipping sequence)
- ❖ *decoding*: inner-product of encoded signal and chipping sequence

IEEE 802.11 Wireless LAN

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

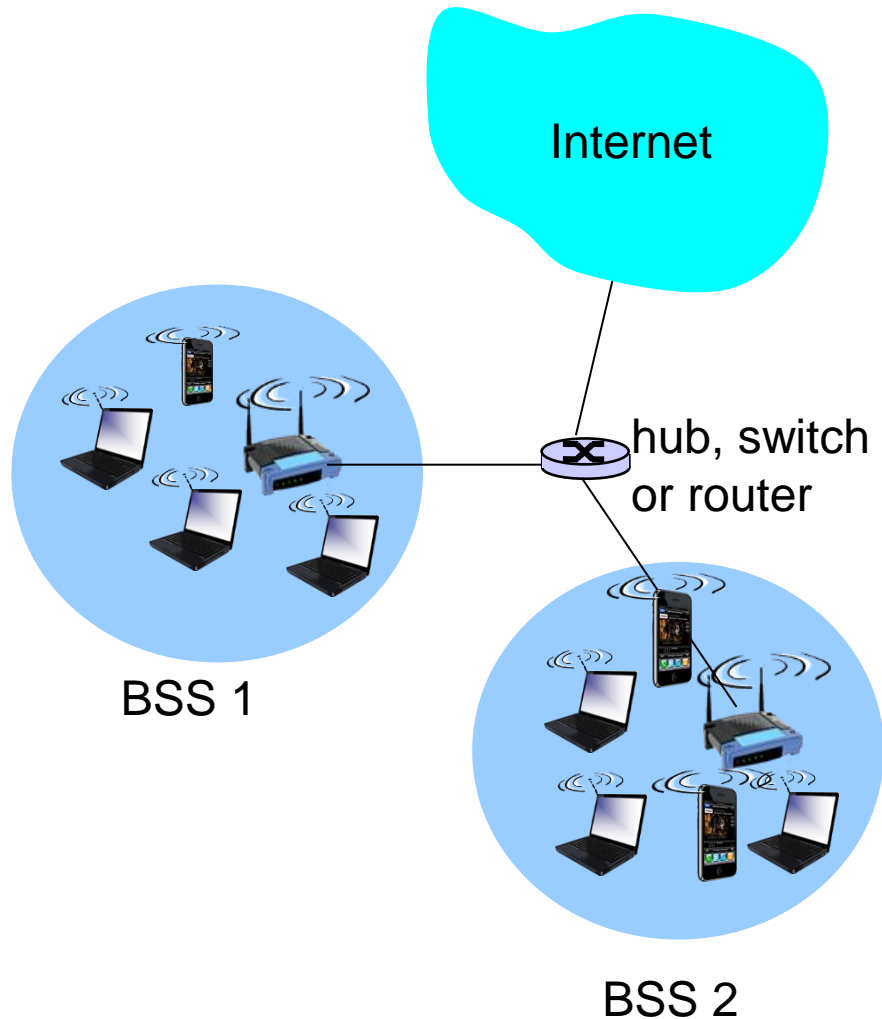
- 2.4-5 GHz range
- up to 54 Mbps

802.11n: multiple antennae

- 2.4-5 GHz range
- up to 200 Mbps

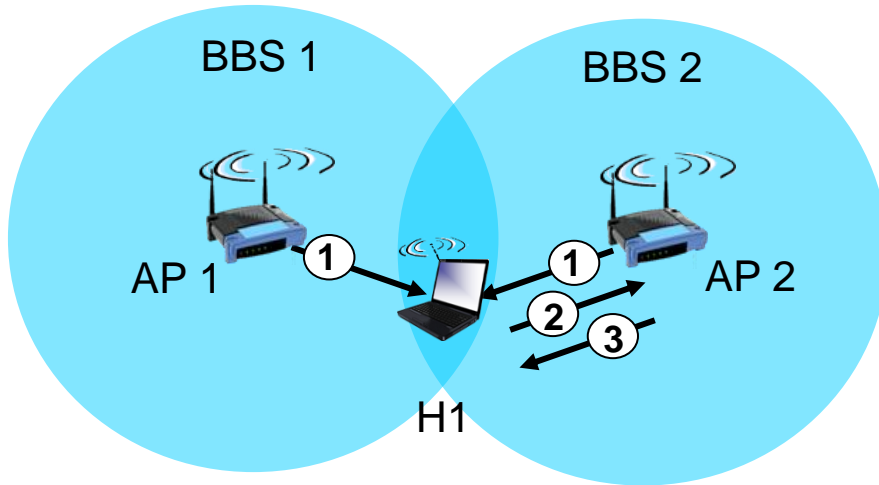
-
- ❖ all use CSMA/CA for multiple access
 - ❖ all have base-station and ad-hoc network versions

802.11 LAN architecture



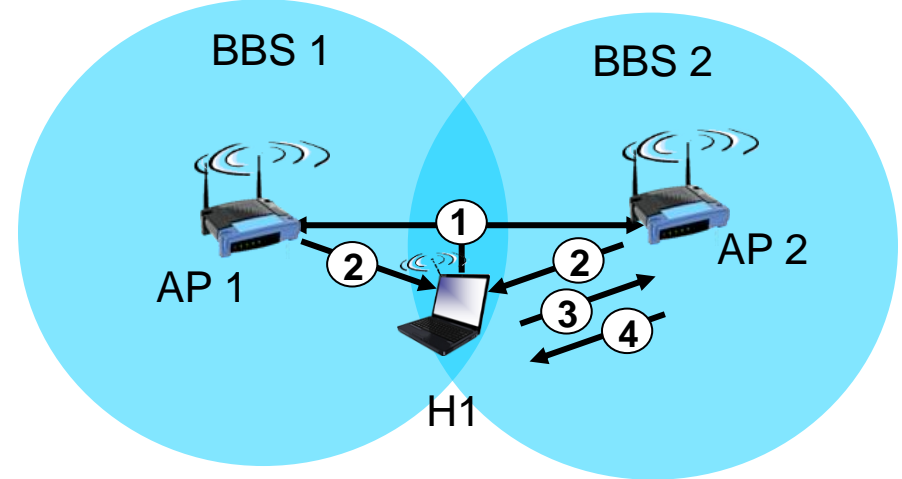
- ❖ wireless host communicates with base station
 - base station = access point (AP)
- ❖ **Basic Service Set (BSS)** (aka “cell”) in infrastructure mode contains:
 - wireless hosts
 - access point (AP): base station
 - ad hoc mode: hosts only

802.11: 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

What is Scanning & Why its required

- Before joining any network first client or stations or mobile stations need to find it first.
- In the wired world, just plugging the cable or jack will find the network.
- In the wireless world, this requires identification of the compatible network before joining process can begin.
- This identification process of the network or discovering the network is referred as **Scanning**.
- The reason for client scanning is to determine a suitable AP to which the client may need to connect/roam now or in the future.

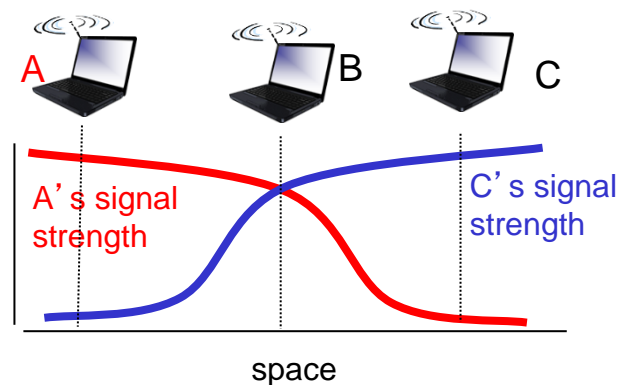
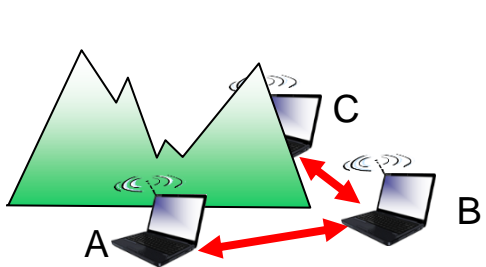
Types of Scanning

- A client can use two scanning methods:
 - Active Scanning
 - Passive Scanning
- During an active scan, the client radio transmits a probe request and listens for a probe response from an AP.
- With a passive scan, the client radio listens on each channel for beacons sent periodically by an AP.
- A passive scan generally takes more time, since the client must listen and wait for a beacon versus actively probing to find an AP.
- Another limitation with a passive scan is that if the client does not wait long enough on a channel, then the client may miss an AP beacon.

Beacon frame is one of the management frames in [IEEE 802.11](#) based WLANs. It contains all the information about the network

IEEE 802.11: multiple access

- ❖ avoid collisions: 2^+ nodes transmitting at same time
- ❖ 802.11: CSMA - sense before transmitting
 - don't collide with ongoing transmission by other node
- ❖ 802.11: *no* collision detection!
 - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
 - can't sense all collisions in any case: hidden terminal, fading
 - goal: *avoid collisions*: CSMA/CA (Collision Avoidance)



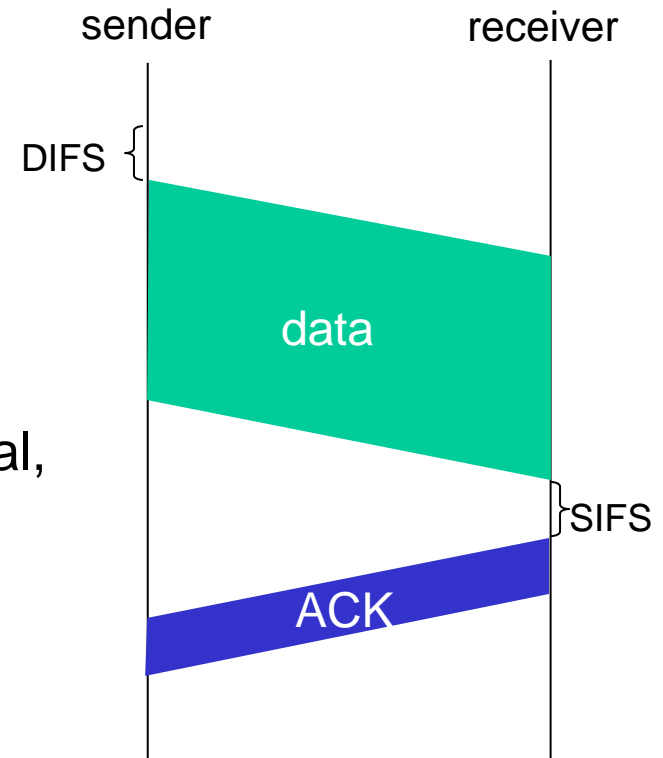
IEEE 802.11 MAC Protocol: CSMA/CA

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:* allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames
- ❖ sender first transmits *small* request-to-send (RTS) packets 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!*

Collision Avoidance: RTS-CTS exchange



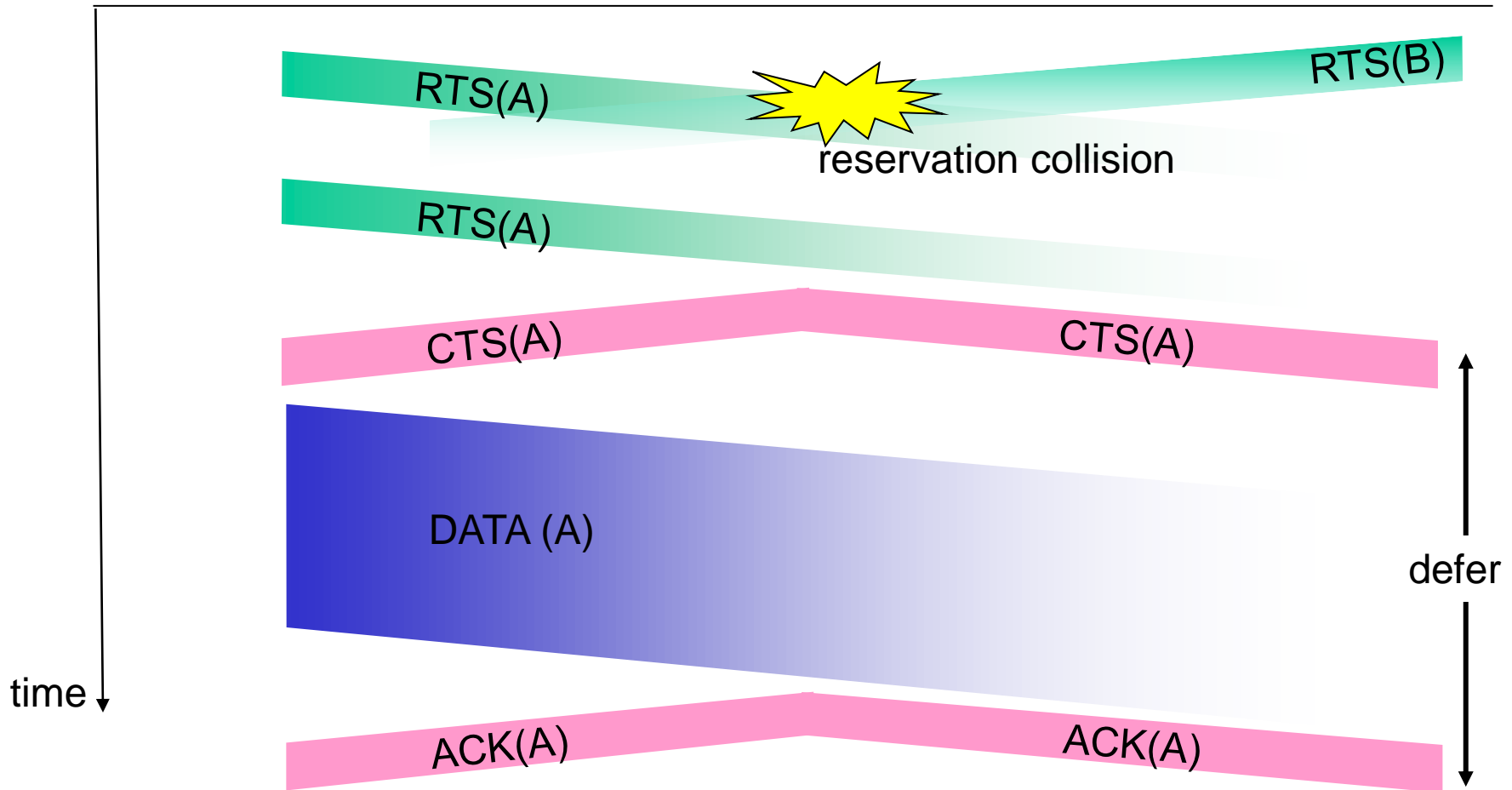
A



AP

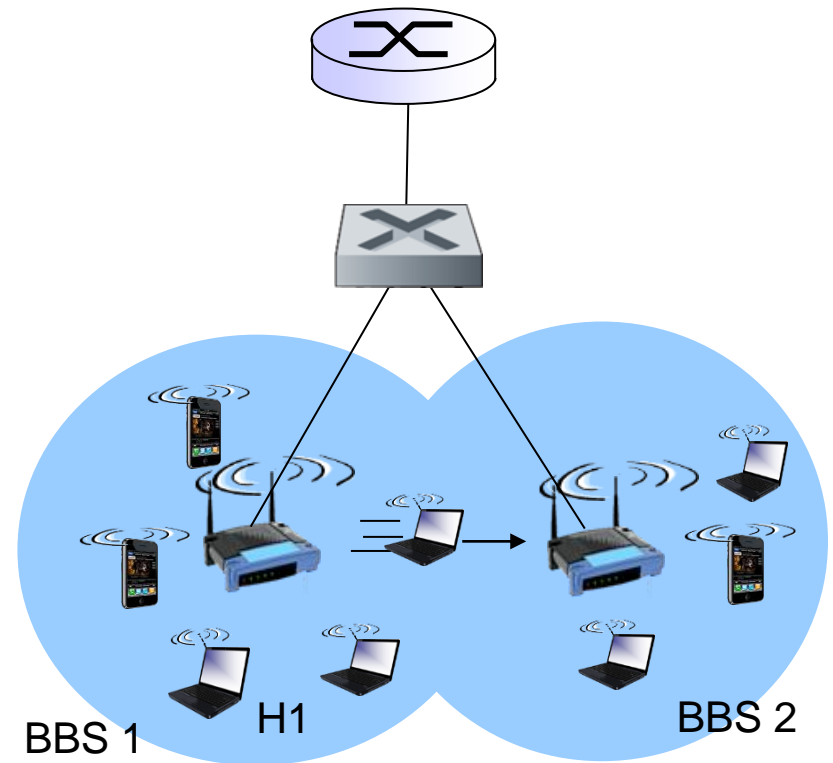


B



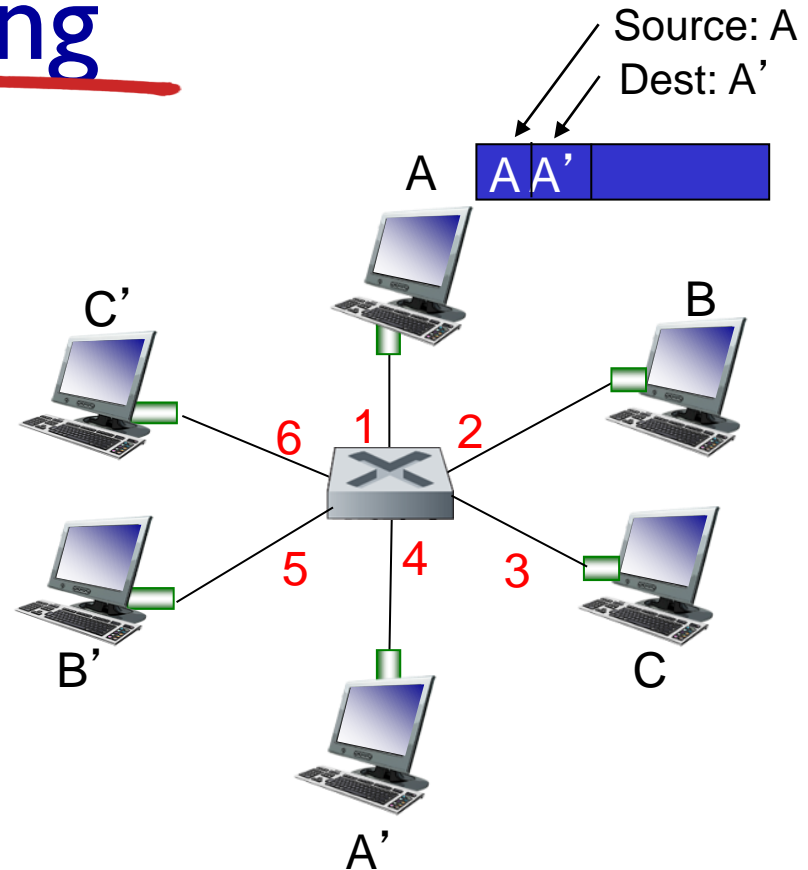
802.11: mobility within same subnet

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



Switch: self-learning

- ❖ switch *learns* which hosts can be reached through which interfaces
 - when frame received, switch “learns” location of sender: incoming LAN segment
 - records sender/location pair in switch table

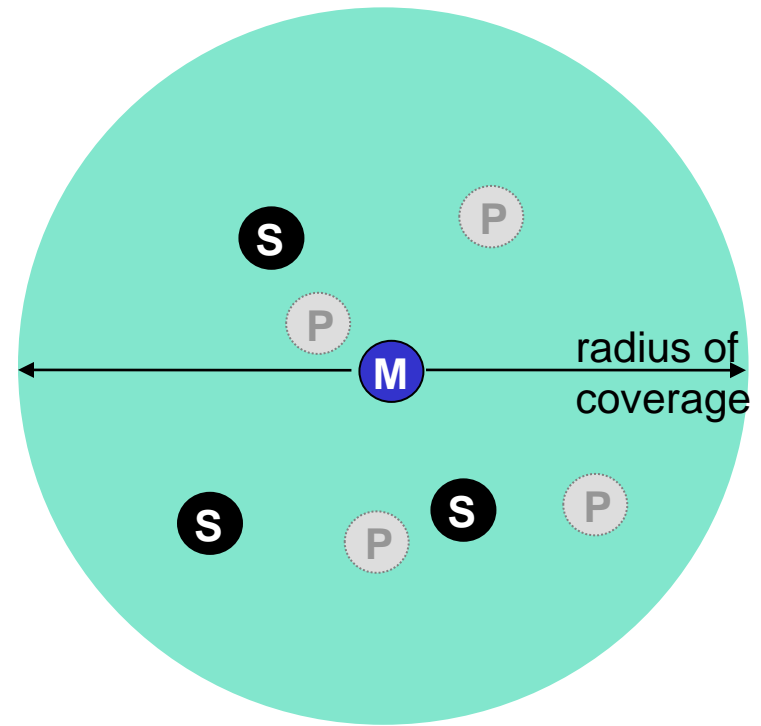


MAC addr	interface	TTL
A	1	60

*Switch table
(initially empty)*

802.15: personal area network

- ❖ less than 10 m diameter
- ❖ replacement for cables (mouse, keyboard, headphones)
- ❖ ad hoc: no infrastructure
- ❖ master/slaves:
 - slaves request permission to send (to master)
 - master grants requests
- ❖ 802.15: evolved from Bluetooth specification
 - 2.4-2.5 GHz radio band
 - up to 721 kbps



- M** Master device
- S** Slave device
- P** Parked device (inactive)

Thank you for listening

Taqwa Altameemi