# COMP 3331/9331: Computer Networks and Applications

## Week 5

## Data Link Layer + Wireless Networks

Reading Guide: Chapter 6, Sections 6.4, 6.7

Chapter 7, Sections 7.1 – 7.3

# Link layer, LANs: outline

6.1 introduction, services

6.2 error detection, correction

6.3 multiple access protocols

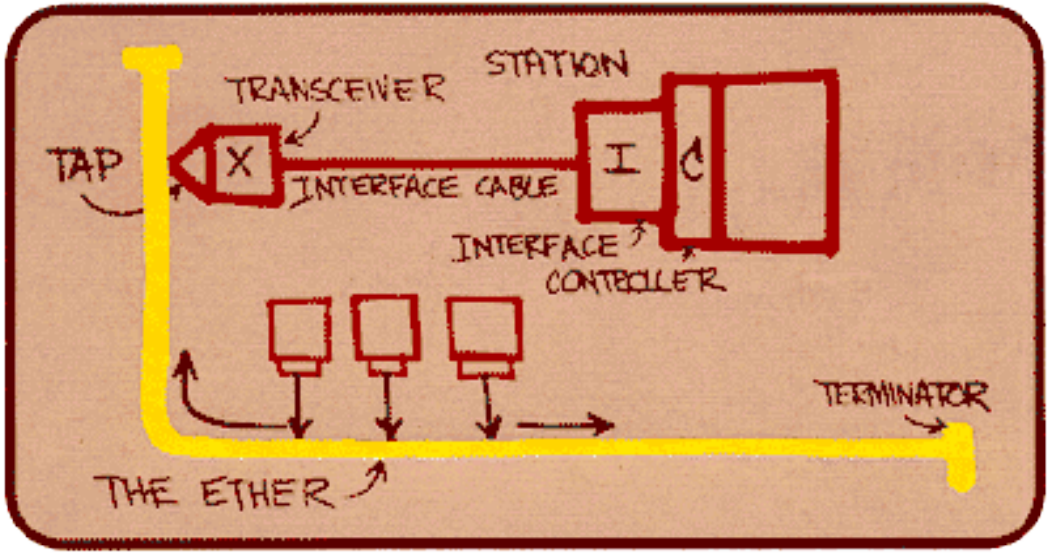
6.4 LANs

- addressing, ARP
- Ethernet
- switches

6.7 a day in the life of a web request

# Ethernet

Bob Metcalfe, Xerox PARC, visits Hawaii and gets an idea!



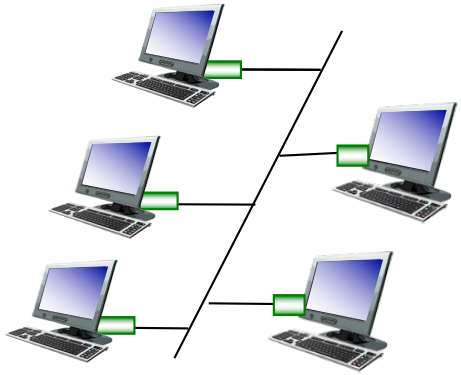

*Metcalfe's Ethernet sketch*

"dominant" wired LAN technology:

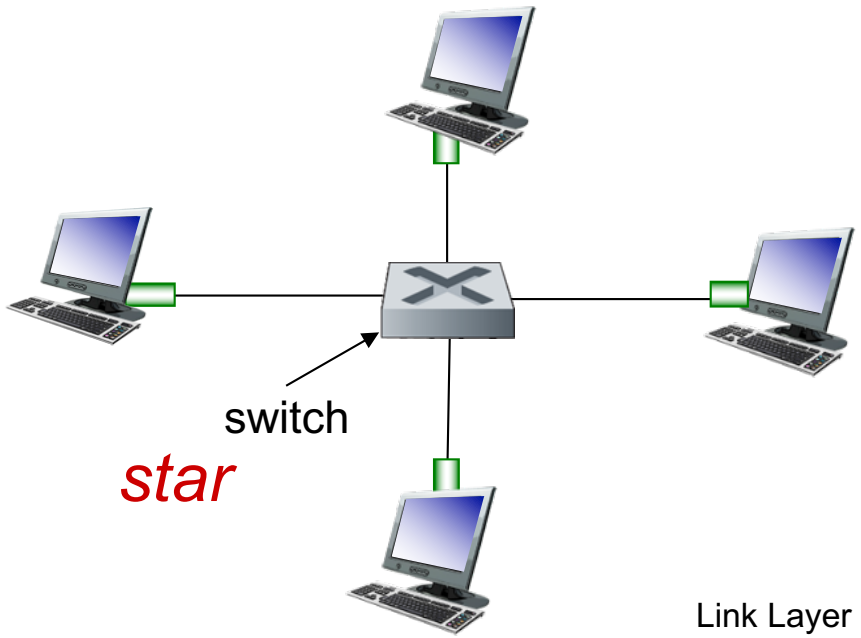
- first widely used LAN technology
- simpler, cheaper than token LANs and ATM
- kept up with speed race: 10 Mbps – 10 Gbps

# Ethernet: physical topology

- *bus:* popular through mid 90s
  - all nodes in same collision domain (can collide with each other)
  - CSMA/CD for media access control
- *star:* prevails today
  - active *switch* in center
  - each "spoke" runs a (separate) Ethernet protocol (nodes do not collide with each other)
  - No sharing, no CSMA/CD



*bus:* coaxial cable



# Ethernet frame structure

Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

| Preamble 7 Bytes | SFD 1 Byte | Dest MAC 6 Bytes | Source MAC 6 Bytes | Type/Length 2 Bytes | Payload 46-1500 Bytes | FCS/CRC 4 Bytes | Inter Frame Gap |
|---|---|---|---|---|---|---|---|

*preamble:*

- Start of frame is recognized by
  - Preamble : Seven bytes with pattern 10101010
  - Start of Frame Delimiter (SFD) : 10101011
- used to synchronize receiver, sender clock rates
- Inter Frame Gap is 12 Bytes (96 bits) of idle state
  - 0.96 microsec for 100 Mbit/s Ethernet
  - 0.096 microsec for Gigabit/s Ethernet

# Ethernet frame structure (more)

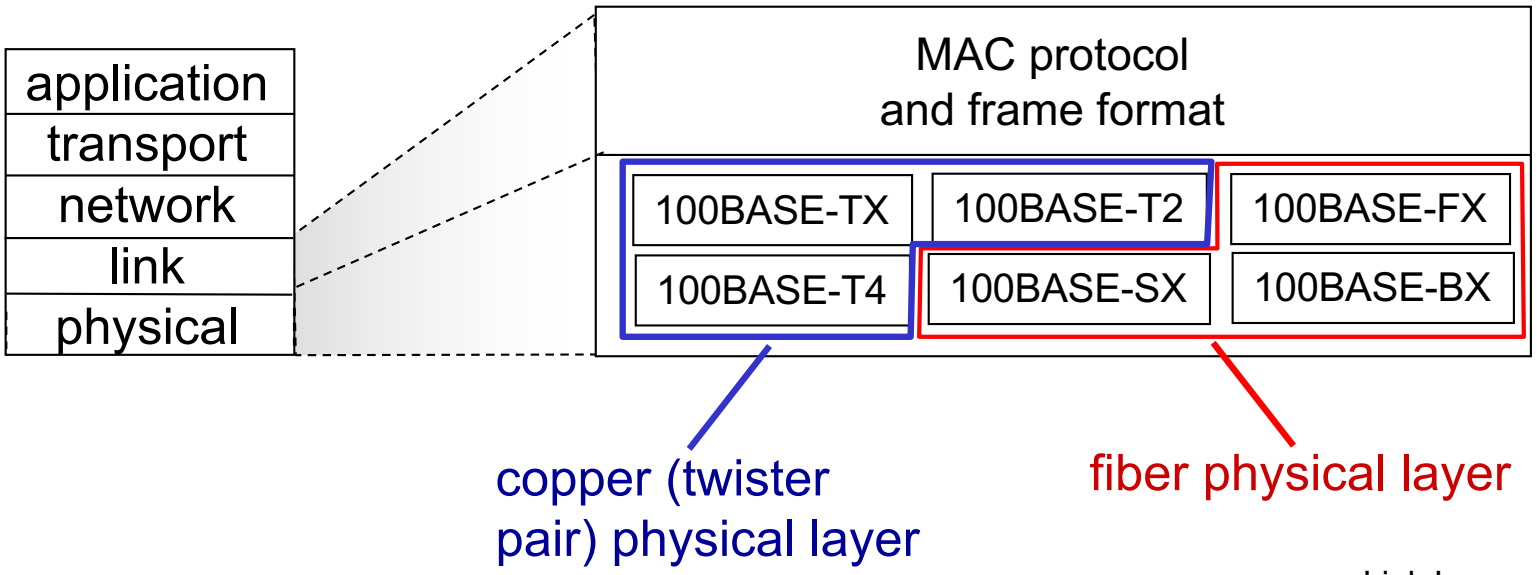
- *addresses:* 6 byte source, destination MAC addresses
  - if adapter receives frame with matching destination address, or with broadcast address (e.g. ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- *type:* indicates higher layer protocol (mostly IP but others possible, e.g., ARP, Novell IPX, AppleTalk)
- *CRC:* cyclic redundancy check at receiver
  - error detected: frame is dropped

# Ethernet: unreliable, connectionless

- *connectionless:* no handshaking between sending and receiving NICs
- *unreliable:* receiving NIC doesnt send acks or nacks to sending NIC
  - data in dropped frames recovered only if initial sender uses higher layer rdt (e.g., TCP), otherwise dropped data lost
- Ethernet's MAC protocol: unslotted *CSMA/CD with binary backoff*

# 802.3 Ethernet standards: link & physical layers

- *many* different Ethernet standards
  - common MAC protocol and frame format
  - different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10Gbps, 40Gbps, 100Gbps,
  - different physical layer media: fiber, cable



# Link layer, LANs: outline

6.1 introduction, services

6.2 error detection, correction

6.3 multiple access protocols

6.4 LANs

- addressing, ARP
- Ethernet
- switches

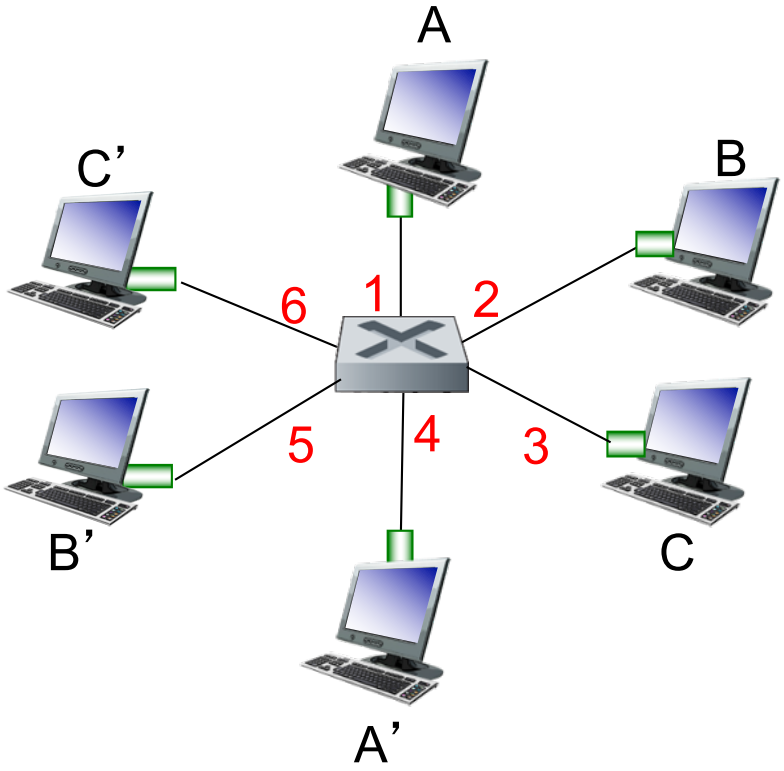
6.7 a day in the life of a web request

# Ethernet switch

- link-layer device: takes an *active* role
  - store, forward Ethernet frames
  - examine incoming frame's MAC address, selectively forward frame to one-or-more outgoing links
- *transparent*
  - hosts are unaware of presence of switches
- *plug-and-play, self-learning*
  - switches do not need to be configured

# Switch: *multiple* simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, but no collisions; full duplex
  - each link is its own collision domain
- *switching:* A-to-A' and B-to-B' can transmit simultaneously, without collisions




*switch with six interfaces (1,2,3,4,5,6)*

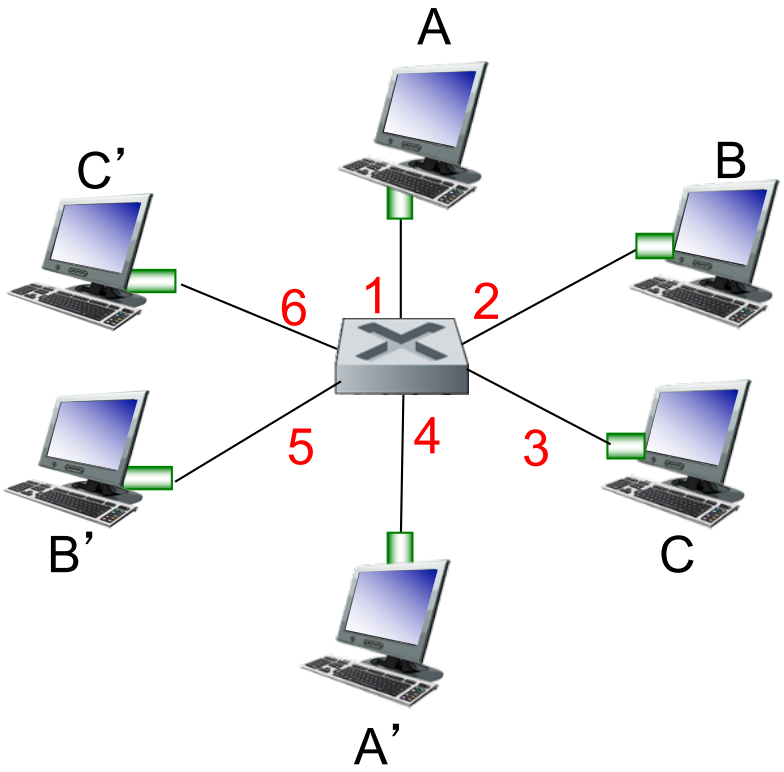
# Switch forwarding table

*Q:* how does switch know A' reachable via interface 4, B' reachable via interface 5?

- *A: each switch has a switch table, each entry:*
  - *(MAC address of host, interface to reach host, time stamp)*
  - *looks like a routing table!*

*Q: how are entries created, maintained in switch table?*

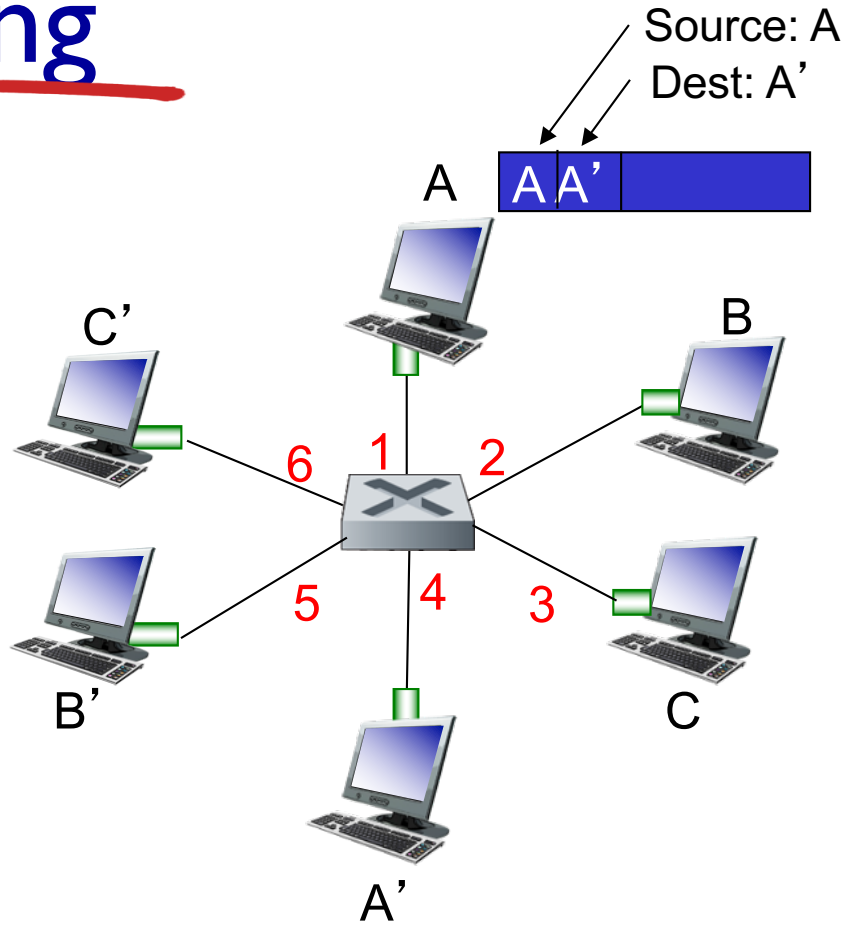
- *something like a routing protocol?*




*switch with six interfaces (1,2,3,4,5,6)*

# 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)*

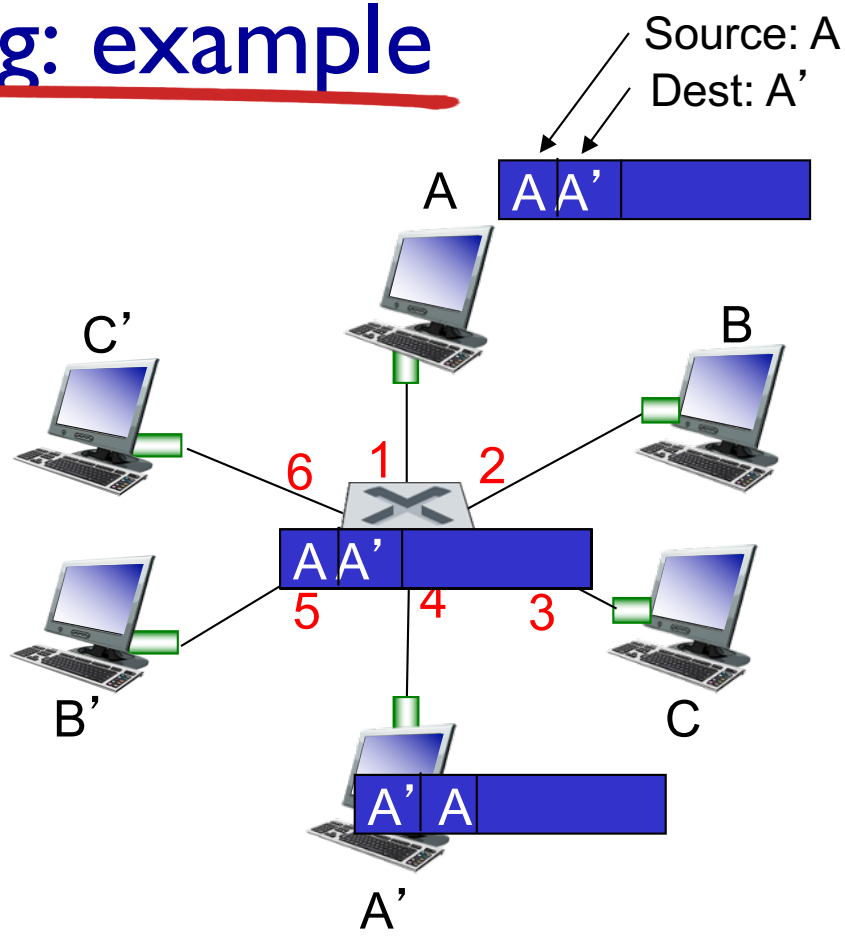
# Switch: frame filtering/forwarding

when frame received at switch:

1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination
   then {
   if destination on segment from which frame arrived
   then drop frame
   else forward frame on interface indicated by entry
   }
   else flood /* forward on all interfaces except arriving interface */

# Self-learning, forwarding: example

- frame destination, A', locaton unknown: *flood*
- destination A location known: *selectively send on just one link*

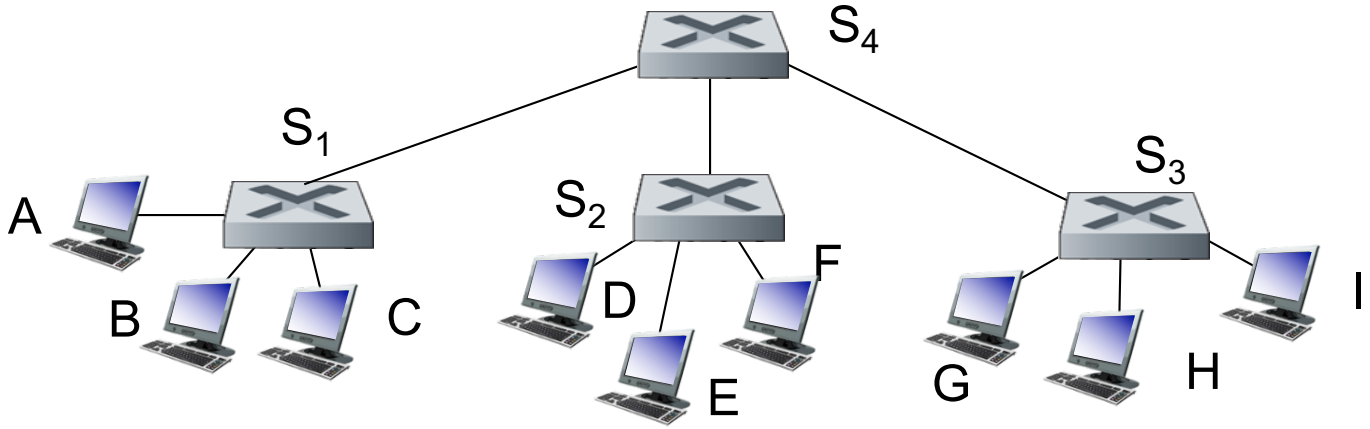



| MAC addr | interface | TTL |
|---|---|---|
| *A* | *1* | *60* |
| *A'* | *4* | *60* |

*switch table (initially empty)*

# Interconnecting switches

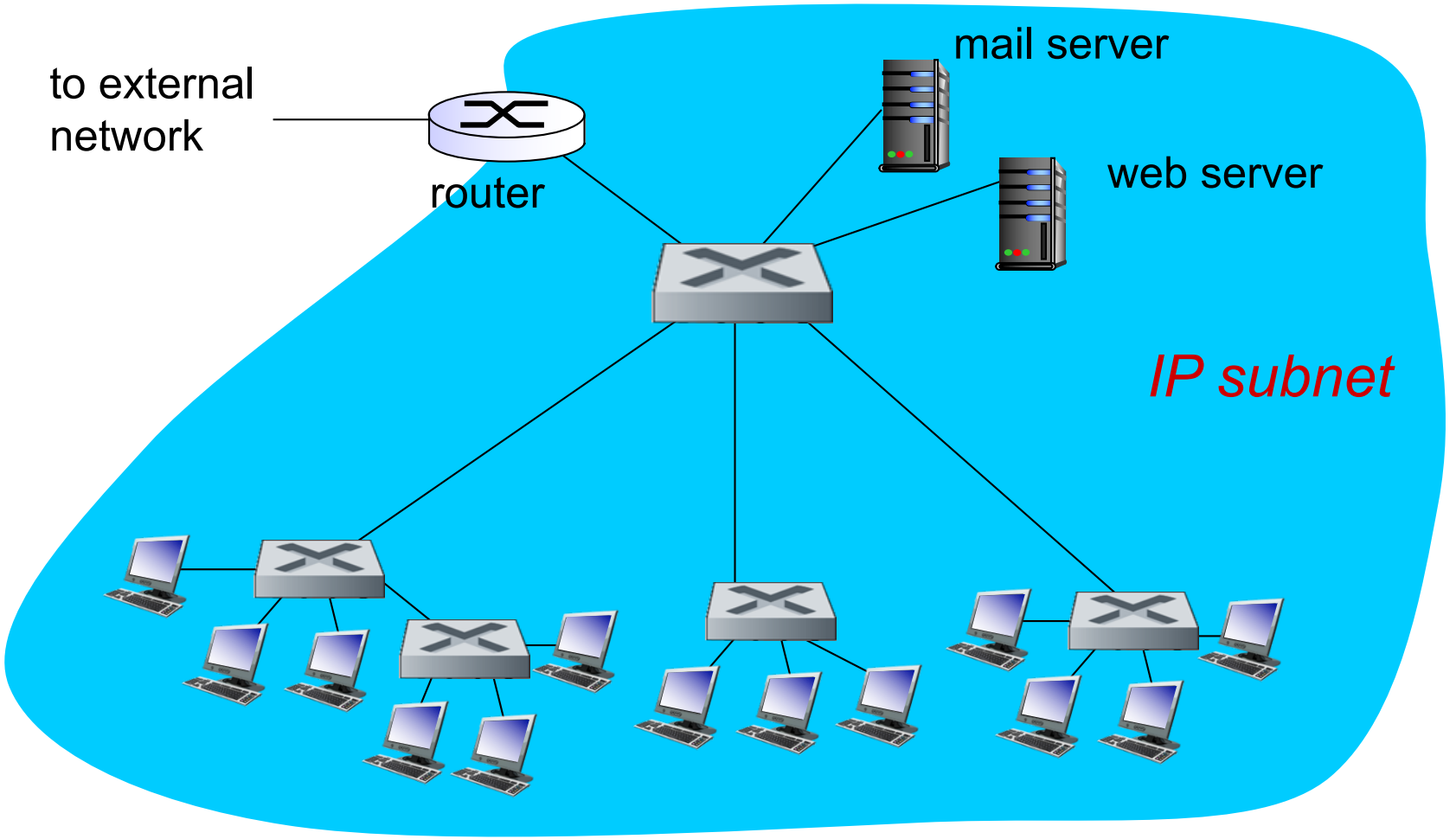
- switches can be connected together




Q: sending from A to G - how does $S_1$ know to forward frame destined to G via $S_4$ and $S_3$?

- A: self learning! (works *exactly* the same as in single-switch case!)

# Institutional network



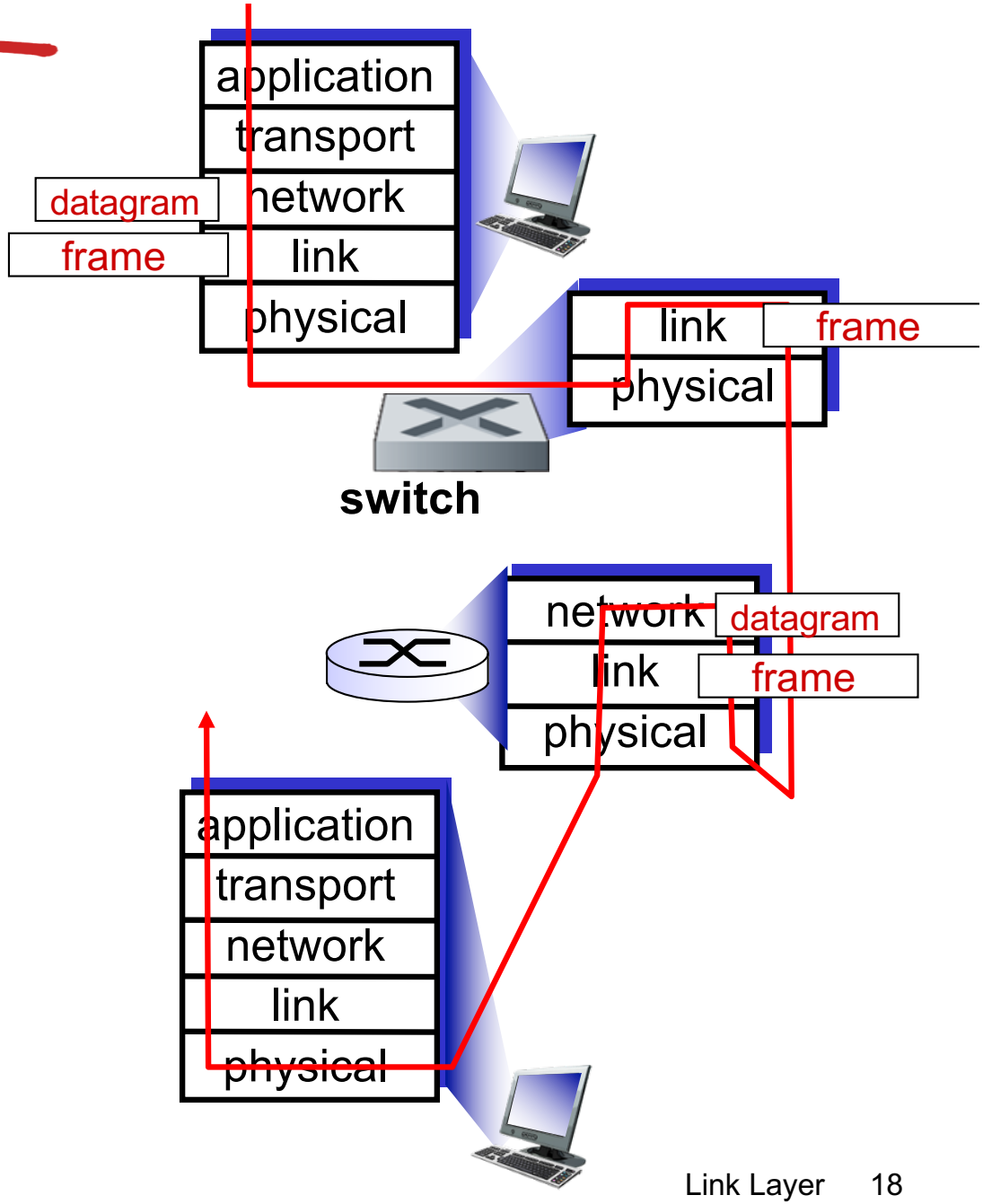
# Switches vs. routers

both are store-and-forward:

- *routers:* network-layer devices (examine network-layer headers)
- *switches*: link-layer devices (examine link-layer headers)

both have forwarding tables:

- *routers:* compute tables using routing algorithms, IP addresses
- *switches:* learn forwarding table using flooding, learning, MAC addresses



# Security Issues

- In a switched LAN once the switch table entries are established frames are not broadcast
  - Sniffing frames is harder than pure broadcast LANs
  - Note: attacker can still sniff broadcast frames and frames for which there are no entries (as they are broadcast)
- Switch Poisoning: Attacker fills up switch table with bogus entries by sending large # of frames with bogus source MAC addresses
- Since switch table is full, genuine packets frequently need to be broadcast as previous entries have been wiped out

# Link Layer: Summary

- principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing
- instantiation and implementation of various link layer technologies
  - Ethernet
  - switched LANS

# Link Layer: let's take a breath

- journey down protocol stack *complete* (except PHY)
- solid understanding of networking principles, practice
- ….. could stop here …. but *lots* of interesting topics!
  - **wireless**
  - multimedia
  - security
  - network management

# Wireless 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

*We will only focus on wireless challenges*

# Outline

7.1 Introduction

## Wireless

7.2 Wireless links, characteristics

7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

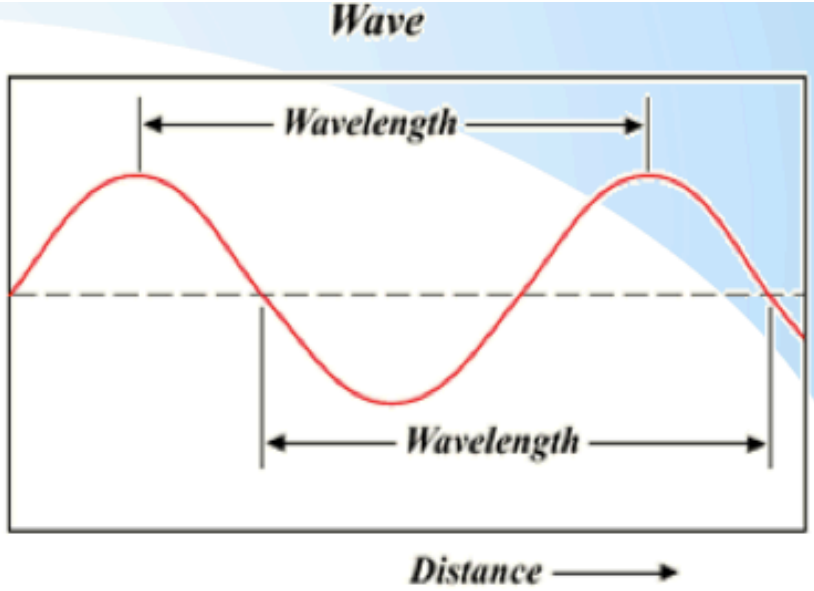
# Wireless 101

- **Frequency/Wave-Length –**

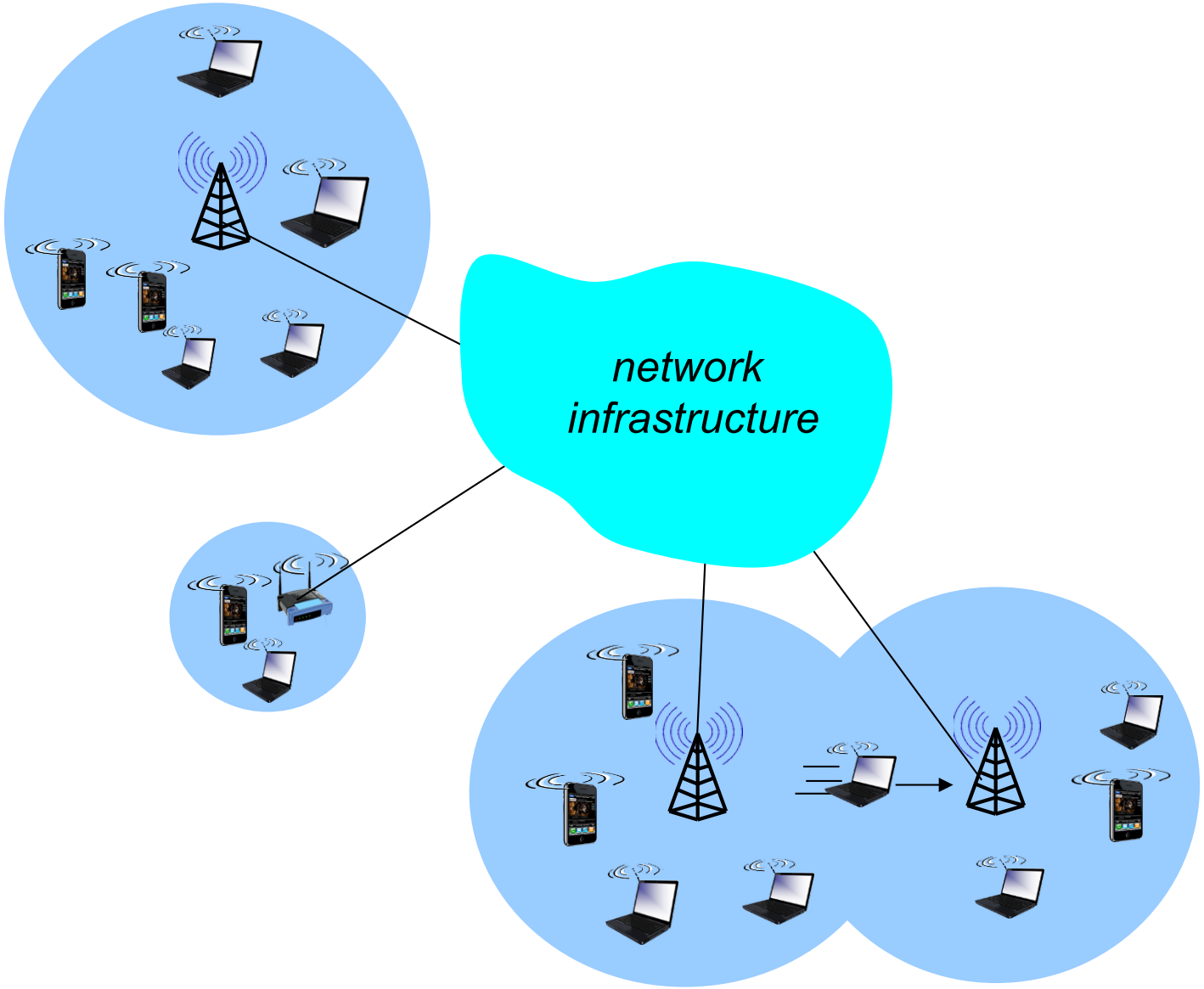
C is the speed of light
$f$ is frequency
$\lambda$ (lambda) is wavelength

Wavelength $\lambda = \frac{C}{f}$

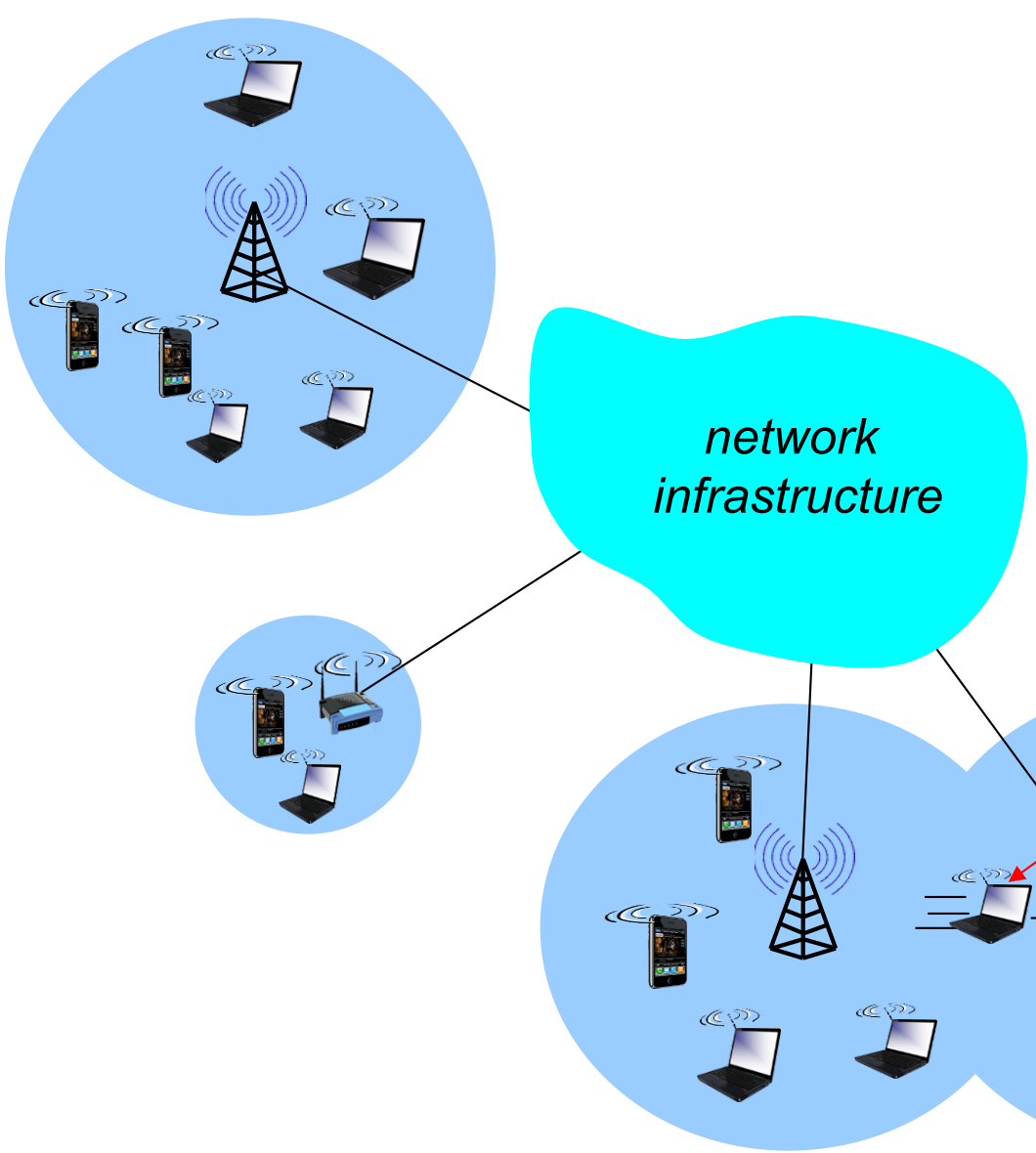
Frequency $f = \frac{C}{\lambda}$



# Elements of a wireless network



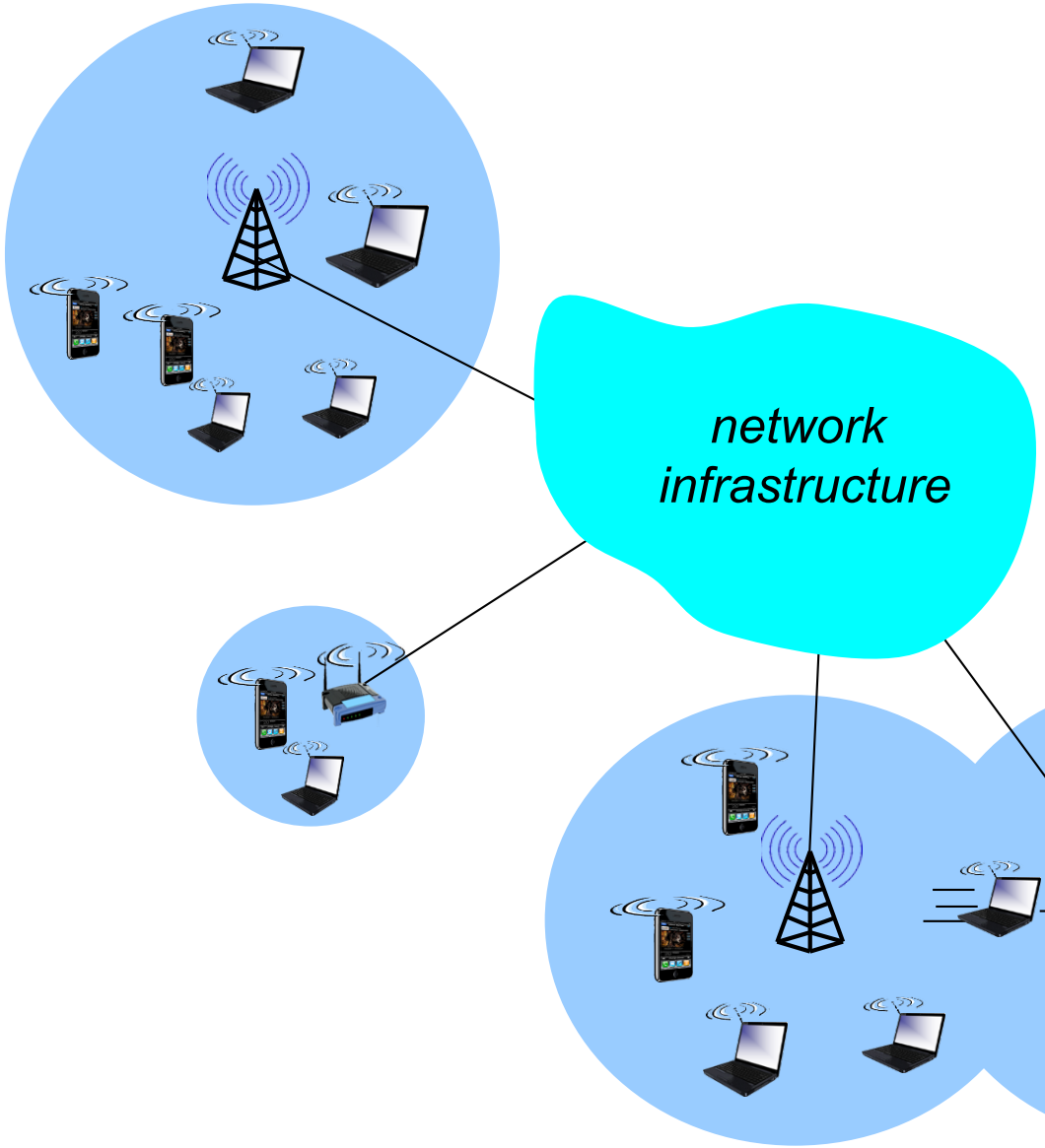
# Elements of a wireless network




*wireless hosts*

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

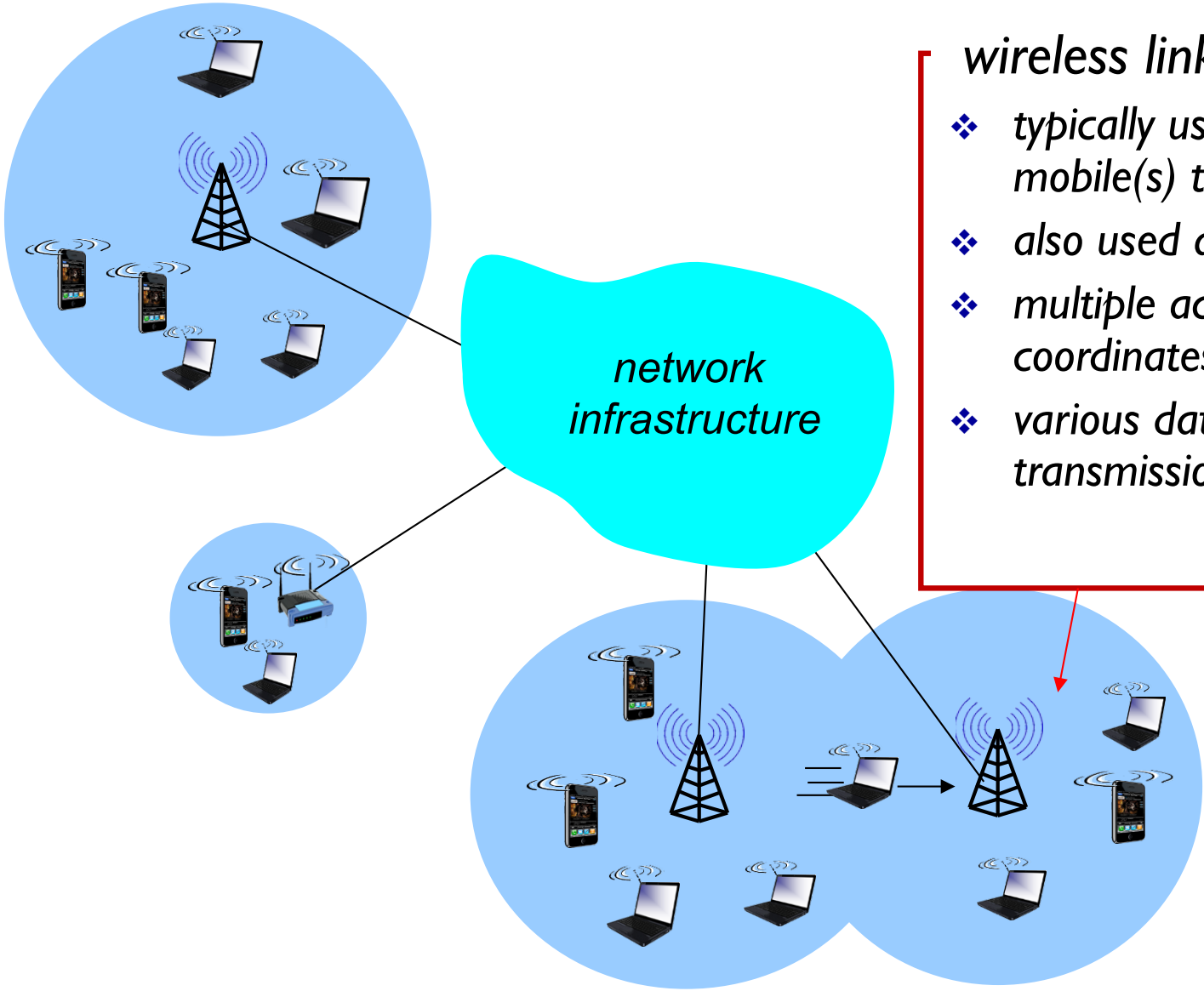
# Elements of a wireless network




*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*

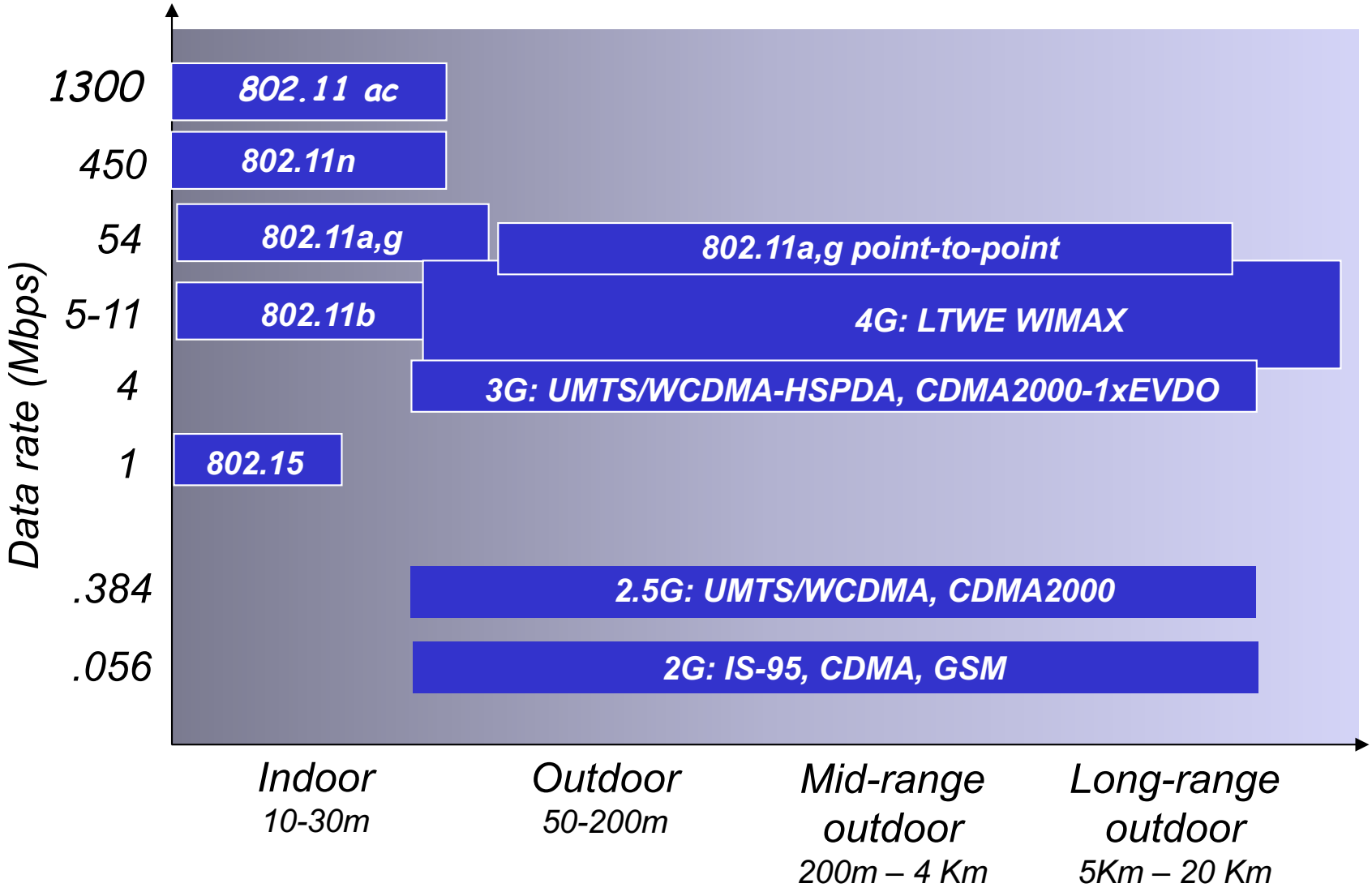
# Elements of a wireless network




*wireless link*

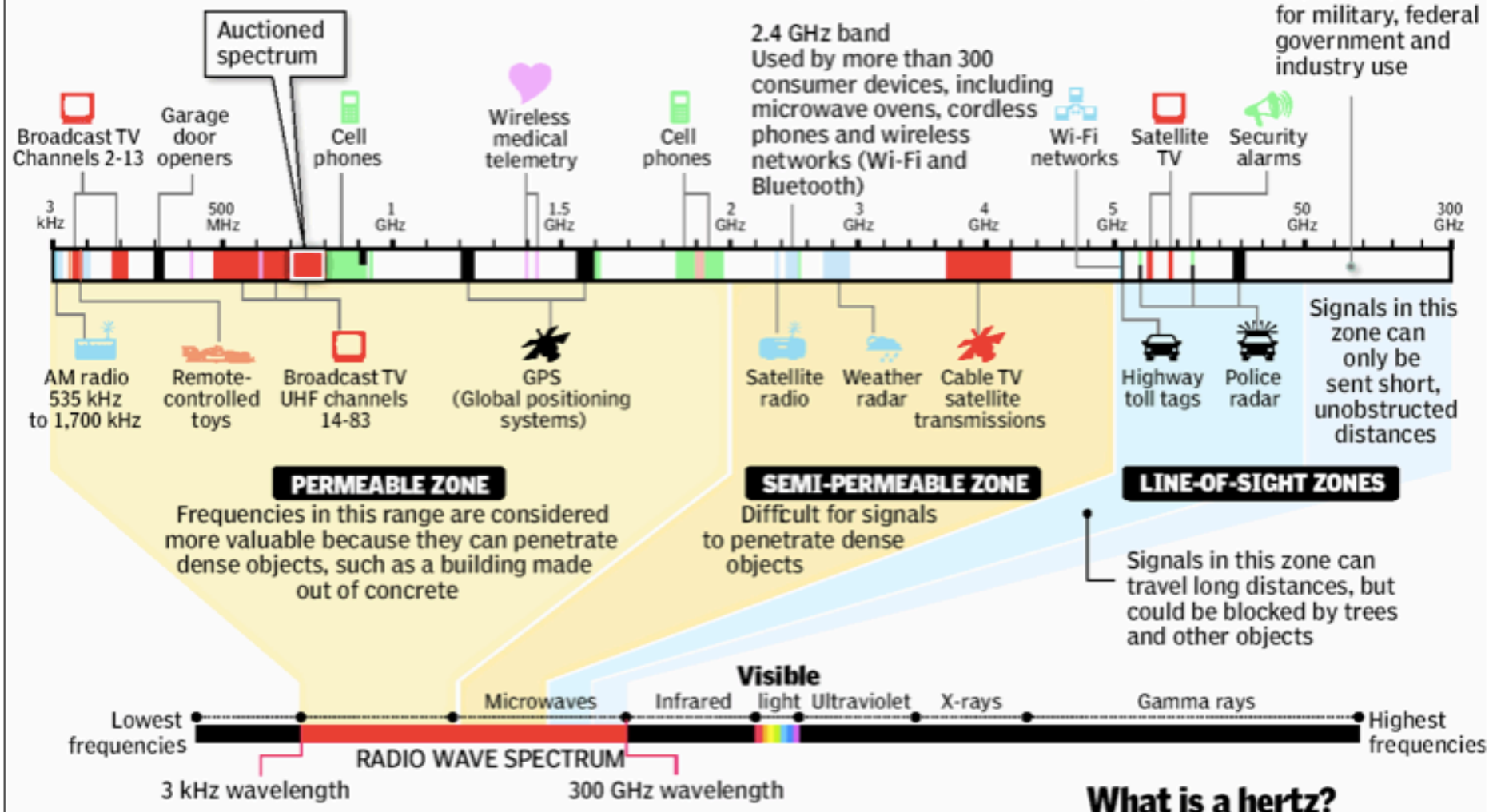
- *typically used to connect mobile(s) to base station*
- *also used as backbone link*
- *multiple access protocol coordinates link access*
- *various data rates, transmission distance*

# Characteristics of selected wireless links



# Inside the radio wave spectrum

Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:




## The electromagnetic spectrum

Radio waves occupy part of the electromagnetic spectrum, a range of electric and magnetic waves of different lengths that travel at the speed of light; other parts of the spectrum include visible light and x-rays; the shortest wavelengths have the highest frequency, measured in hertz


## What is a hertz?

One hertz is one cycle per second. For radio waves, a cycle is the distance from wave crest to crest

1 kilohertz (kHz) = 1,000 hertz

1 megahertz (MHz) = 1 million hertz

1 gigahertz (GHz) = 1 billion hertz

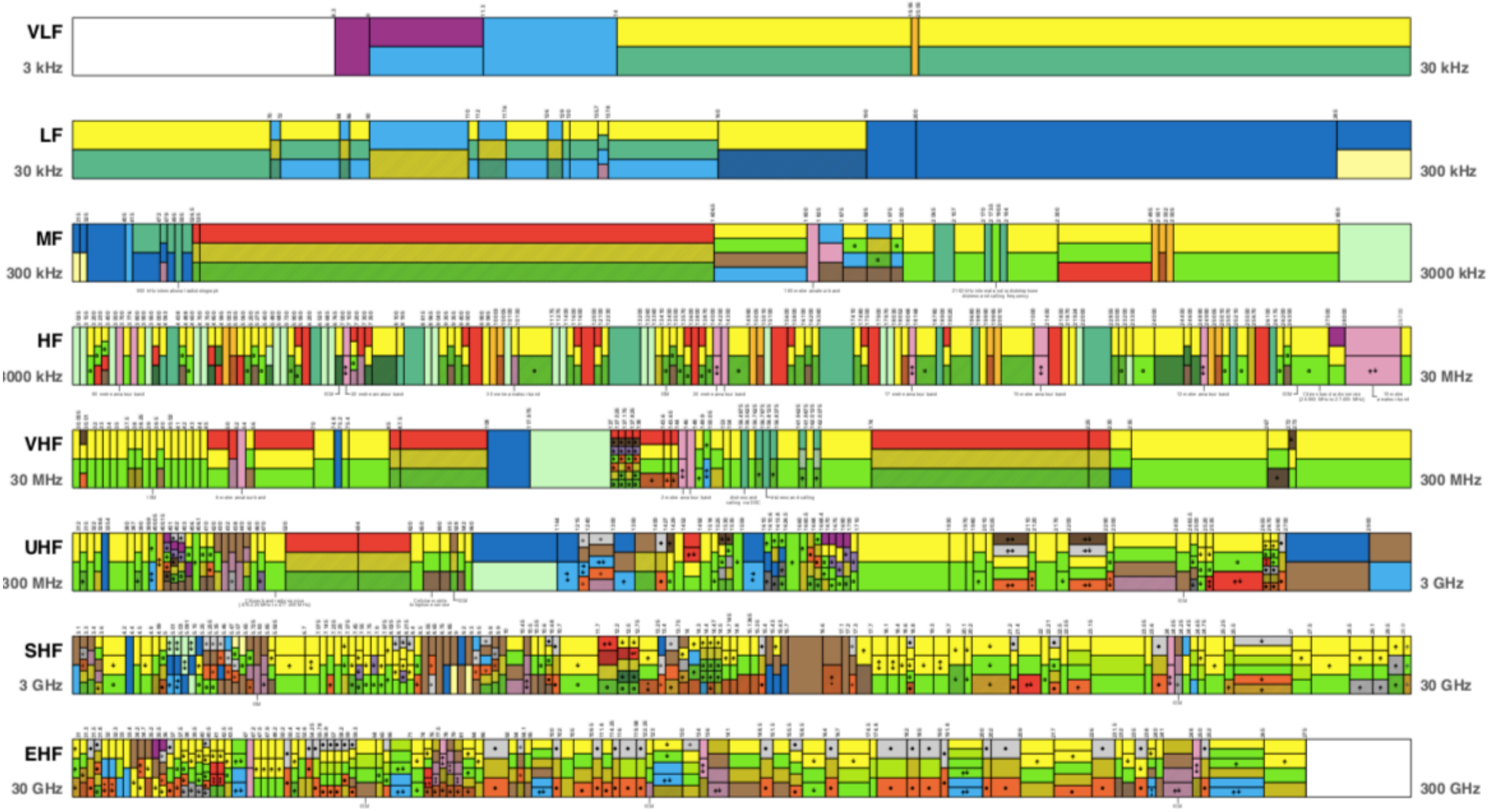
Source: New America Foundation, MCT, Howstuffworks.com
Graphic: Nathaniel Levine, Sacramento Bee

# Australian radiofrequency spectrum

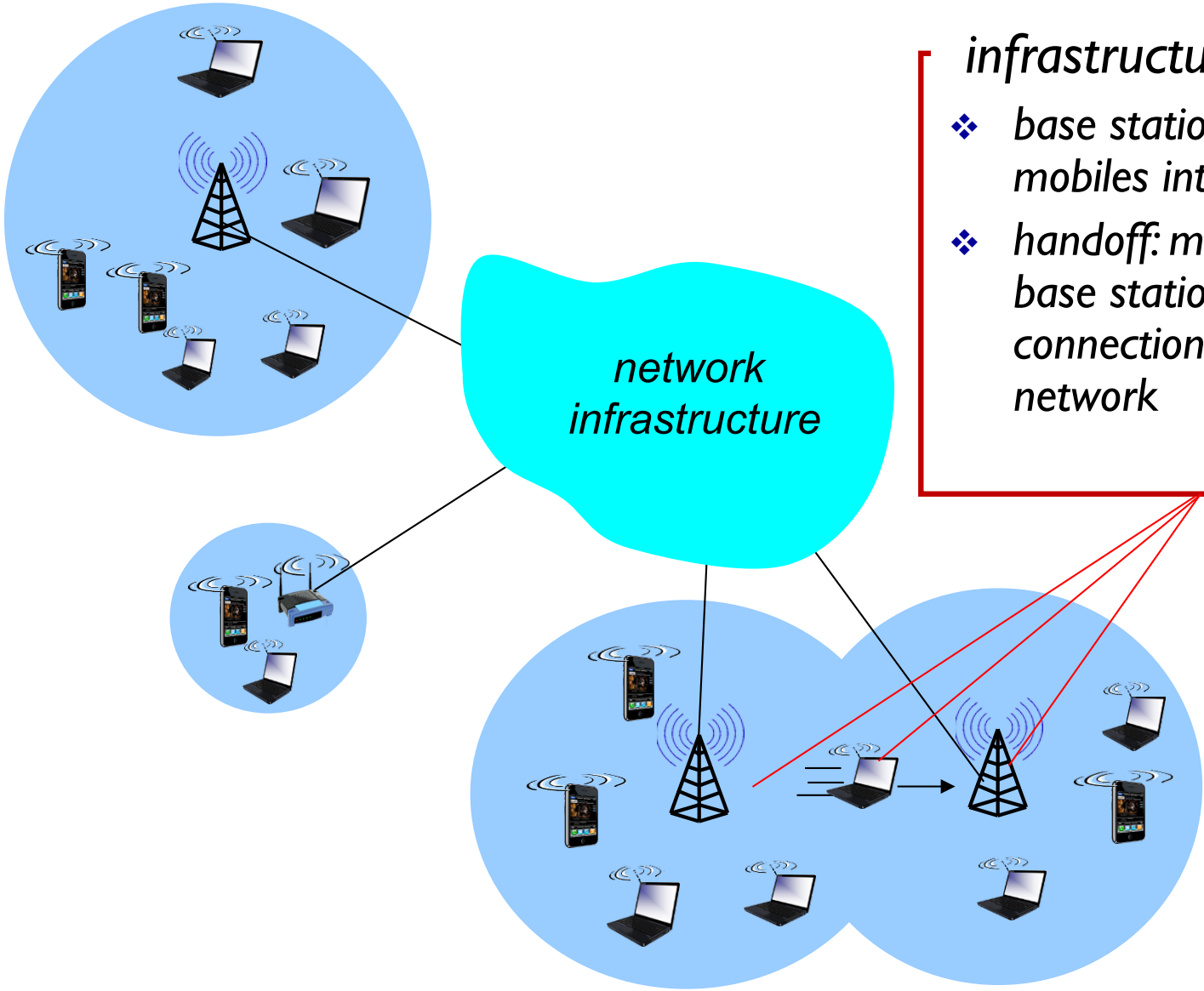
## allocations chart

Australian Government

acma
Australian Communications and Media Authority

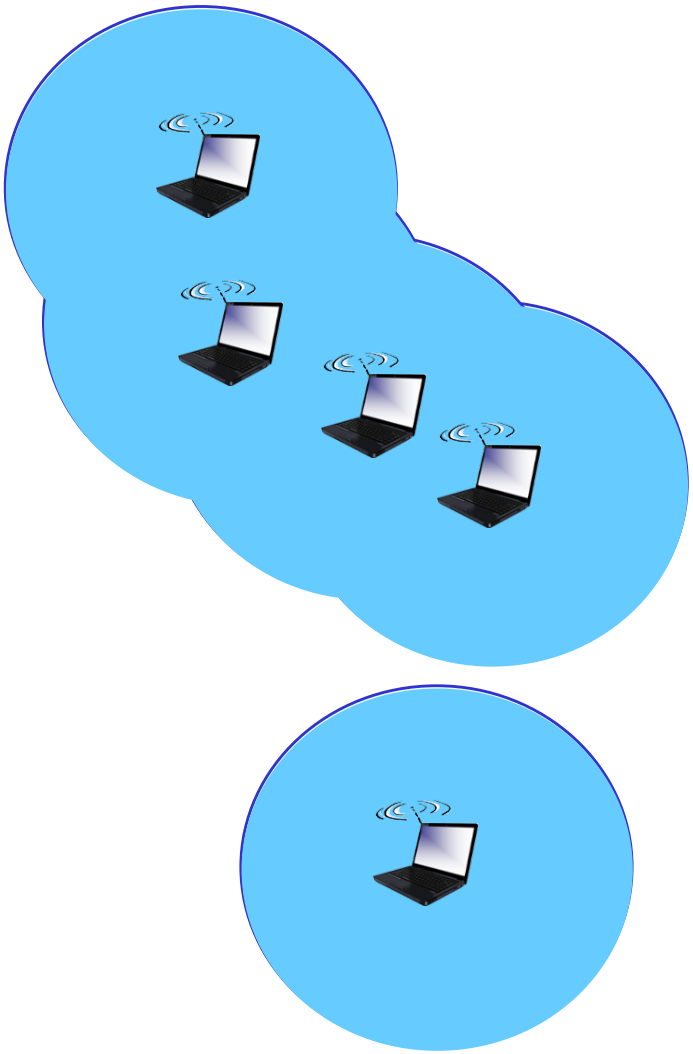
# Elements of a wireless network




*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, WiMAX, 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* |

# Outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics

7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

# Wireless Link Characteristics (1)

*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"

# Path Loss/Path Attenuation

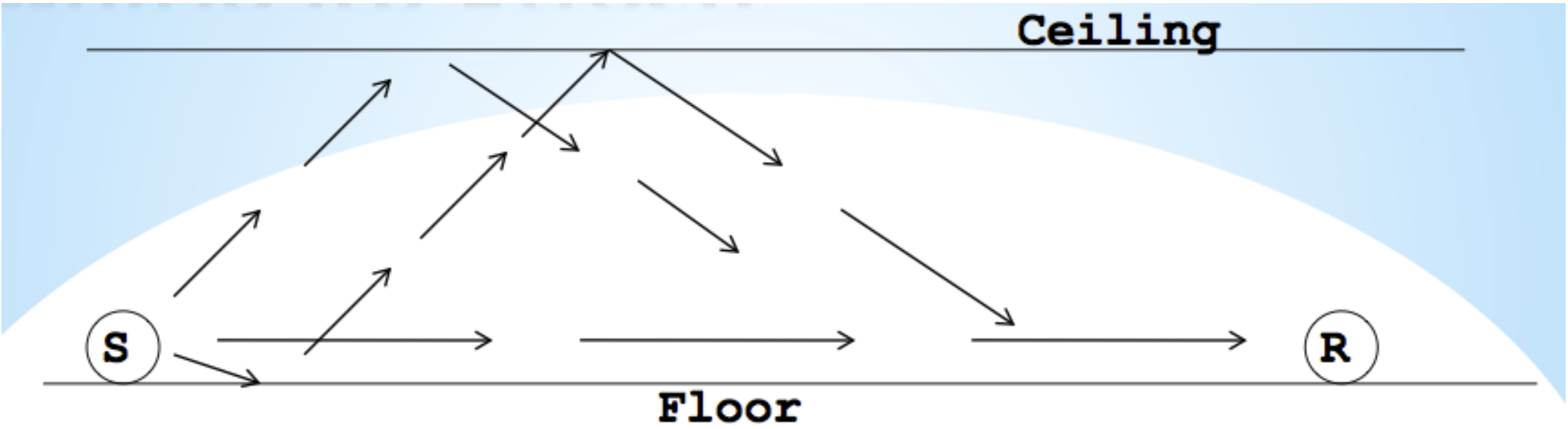
- Free Space Path Loss
  - d: distance
  - λ: wavelength
  - f: frequency
  - c: speed of light

$$\mathrm{FSPL} = \left(\frac{4\pi d}{\lambda}\right)^2$$

$$= \left(\frac{4\pi df}{c}\right)^2$$

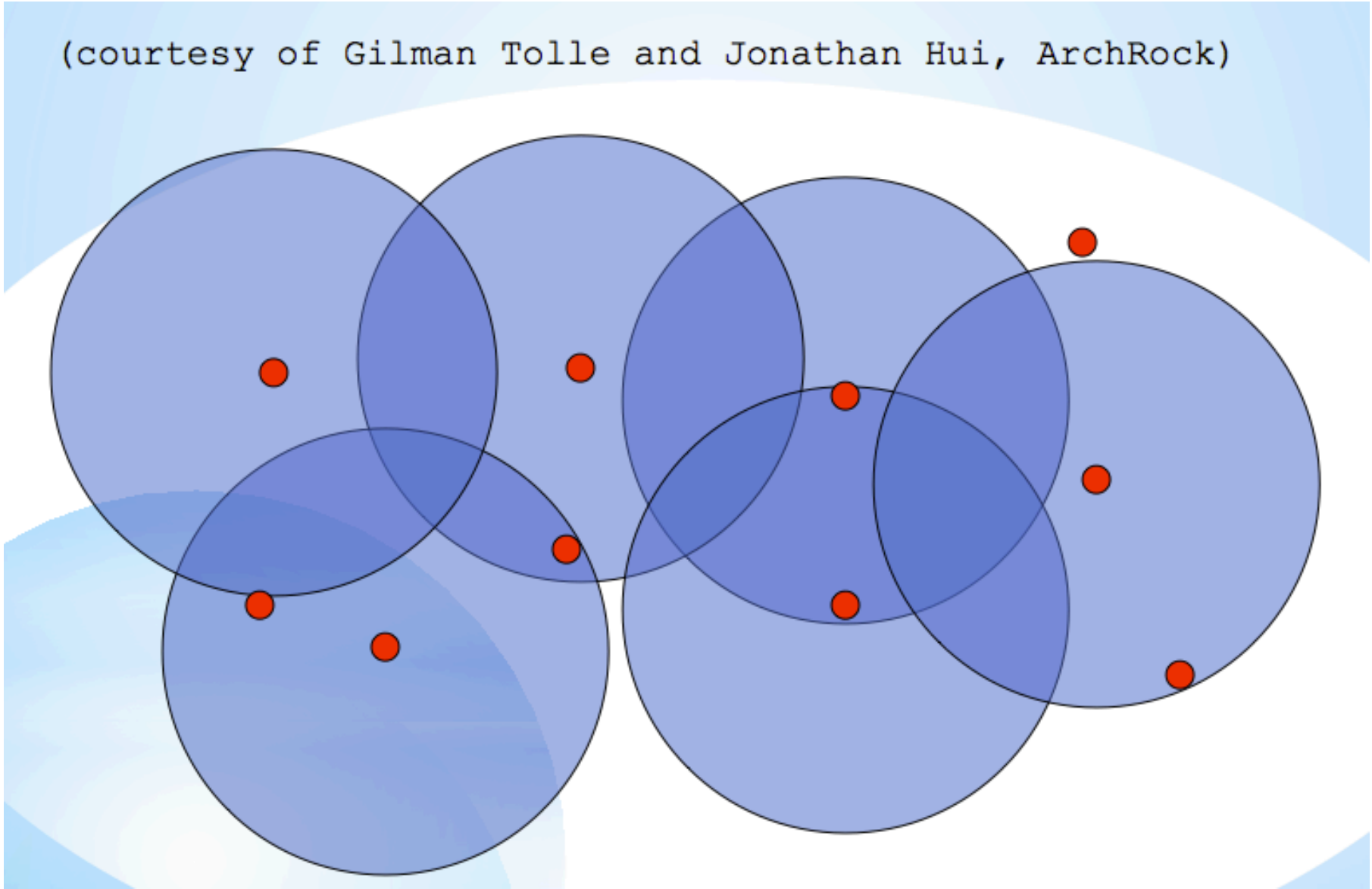
- Reflection, Diffraction, Absorption
- Terrain contours (urban, rural, vegetation)
- Humidity

# Multipath Effects

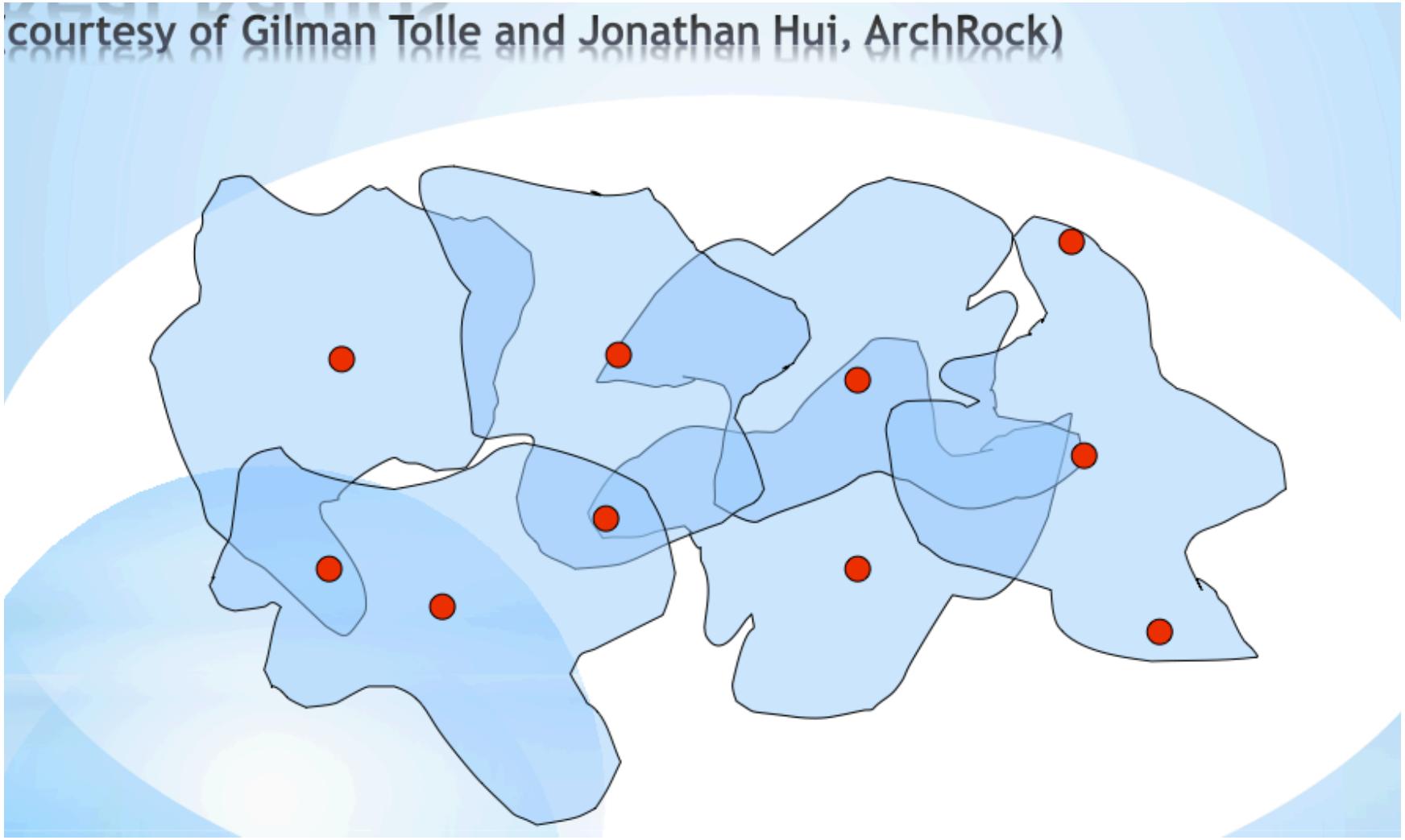



- Signals bounce off surface and interfere (constructive or destructive) with one another
- Self-interference

# Ideal Radios

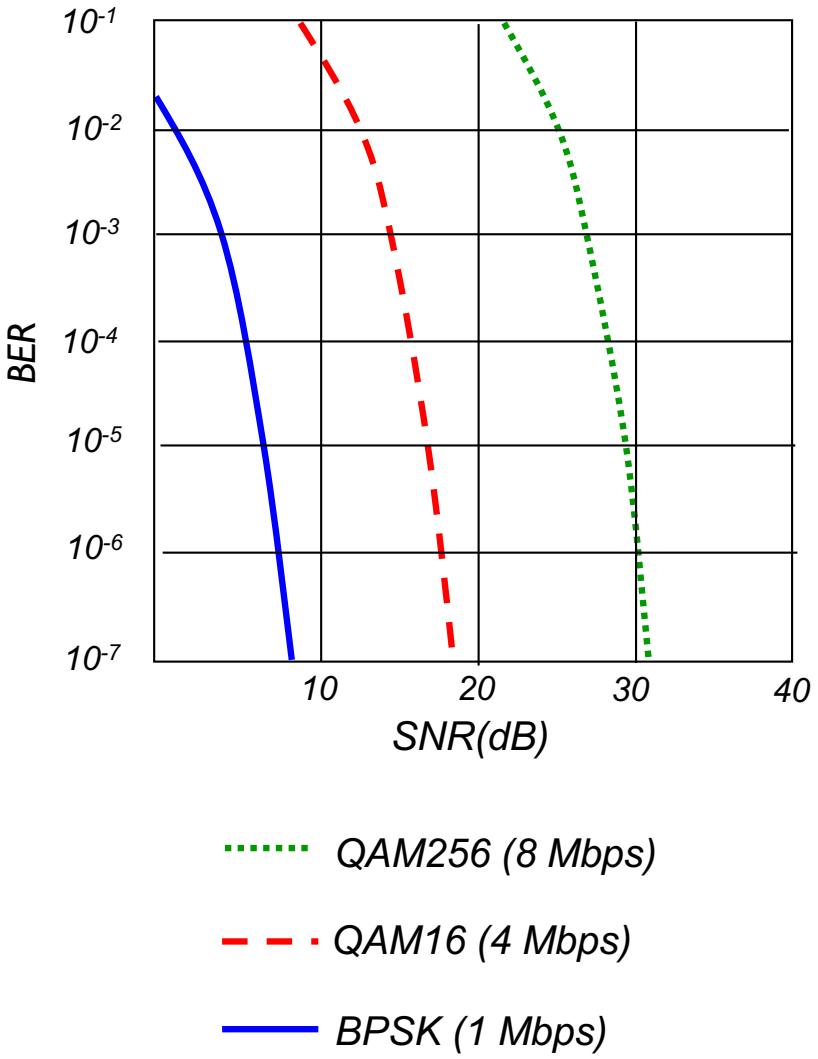


# Real Radios



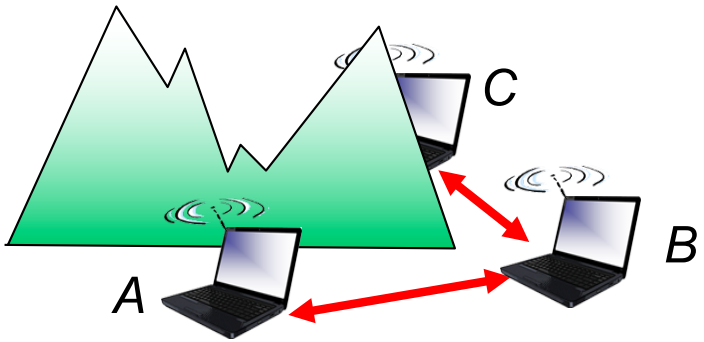
# Wireless Link Characteristics (2)

- 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 thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



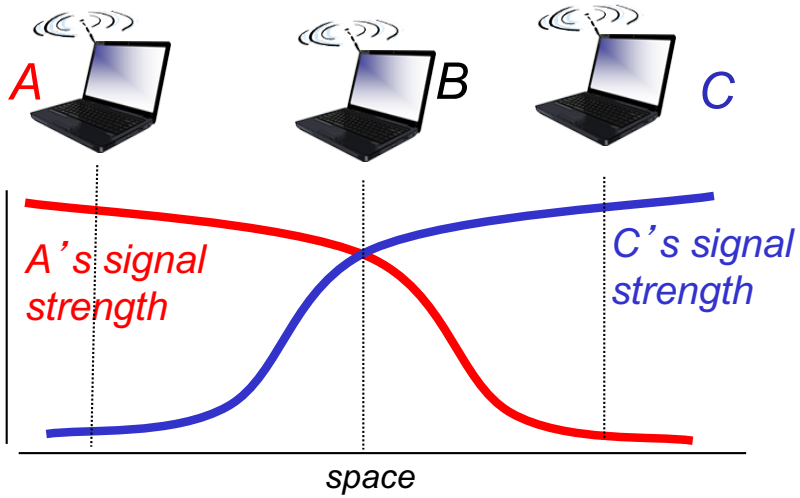
# Wireless network characteristics

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*
- *Carrier sense will be ineffective*

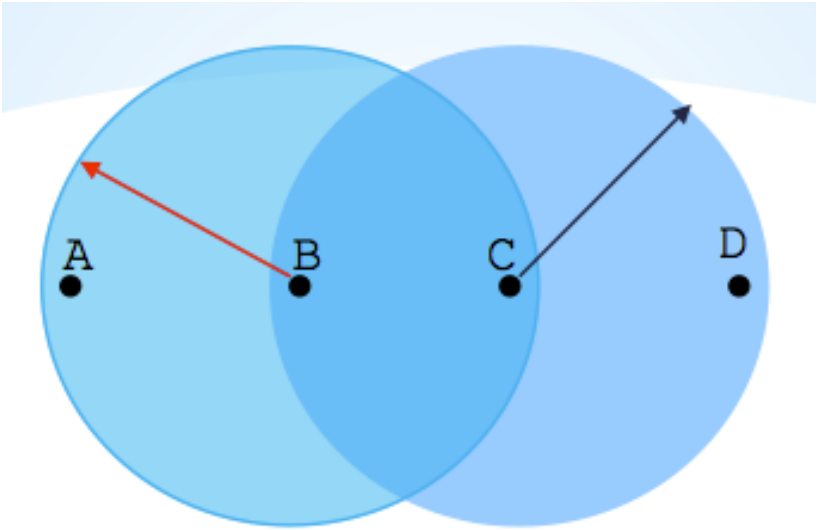



*Signal attenuation:*

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

# Wireless network characteristics

- Exposed Terminals




- Node B sends a packet to A; C hears this and decides not to send a packet to D (despite the fact that this will not cause interference) !!
- Carrier sense would prevent a successful transmission

# Outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics

7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

# 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

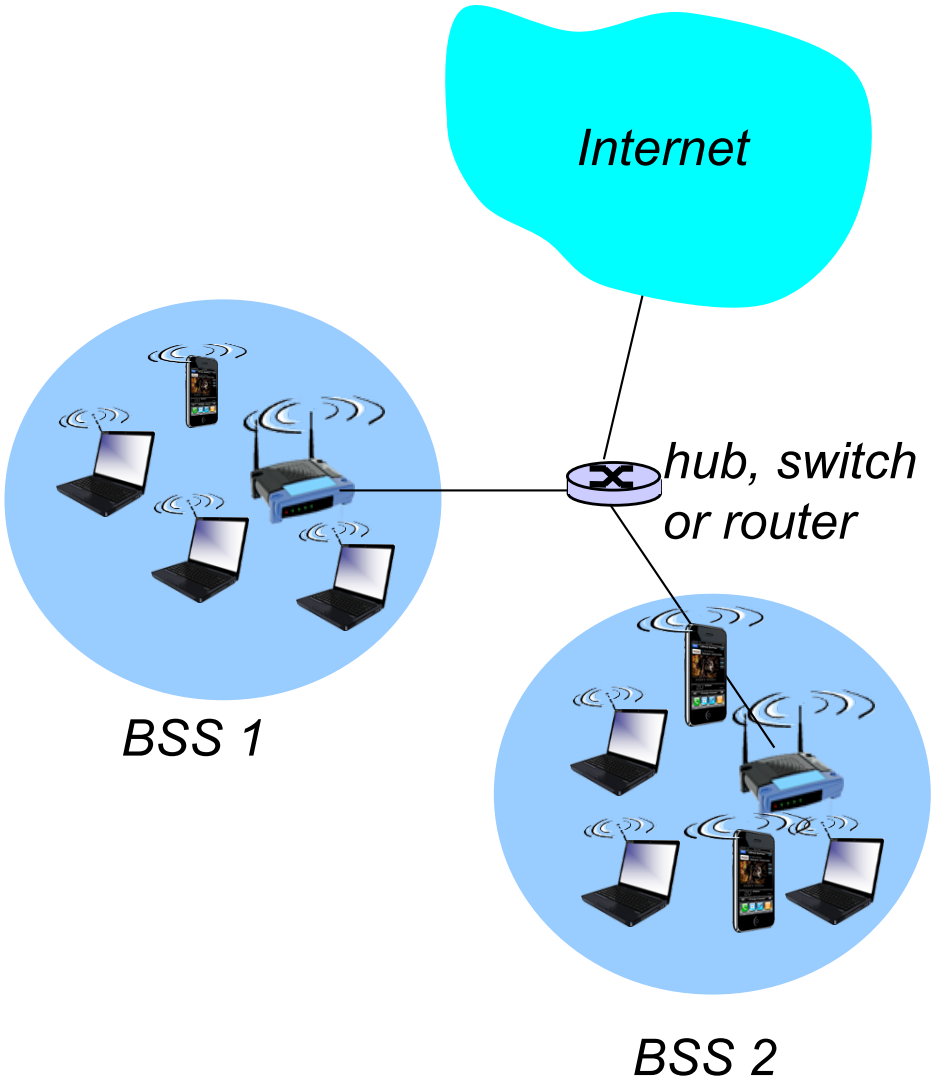
802.11n: multiple antennae

- 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

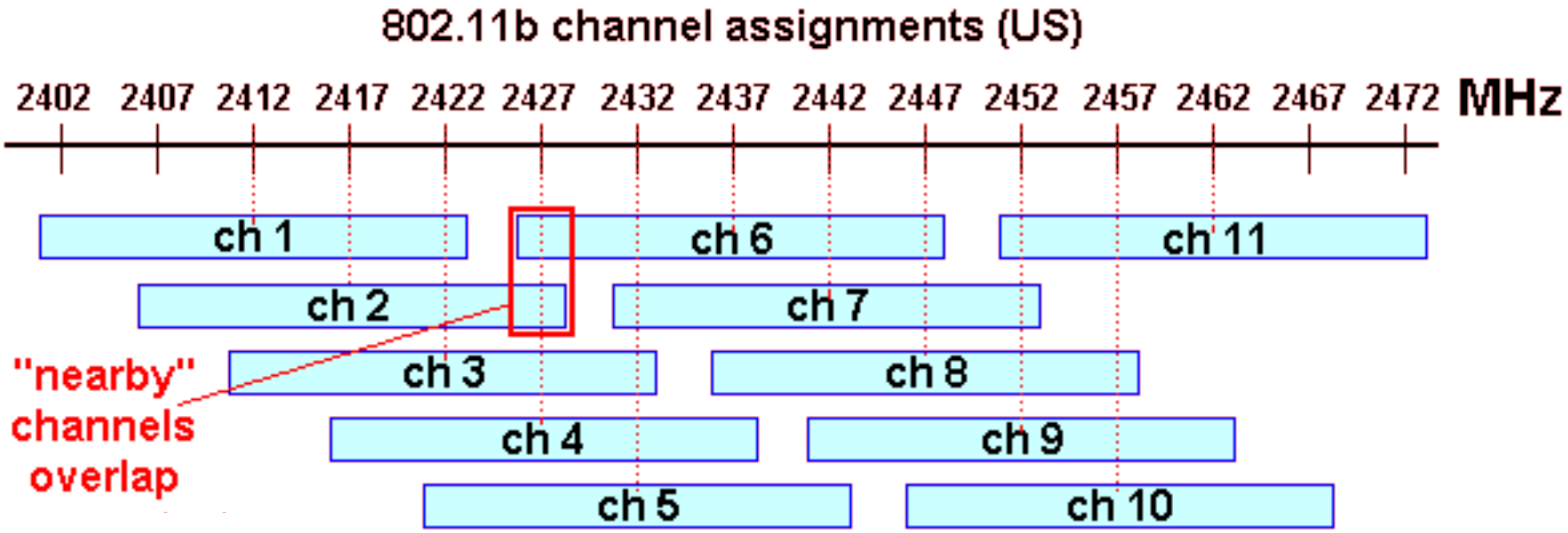



- *wireless host communicates with base station*
  - *base station = access point (AP)*
- *Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:*
  - *wireless hosts*
  - *access point (AP): base station*
  - *ad hoc mode: hosts only*

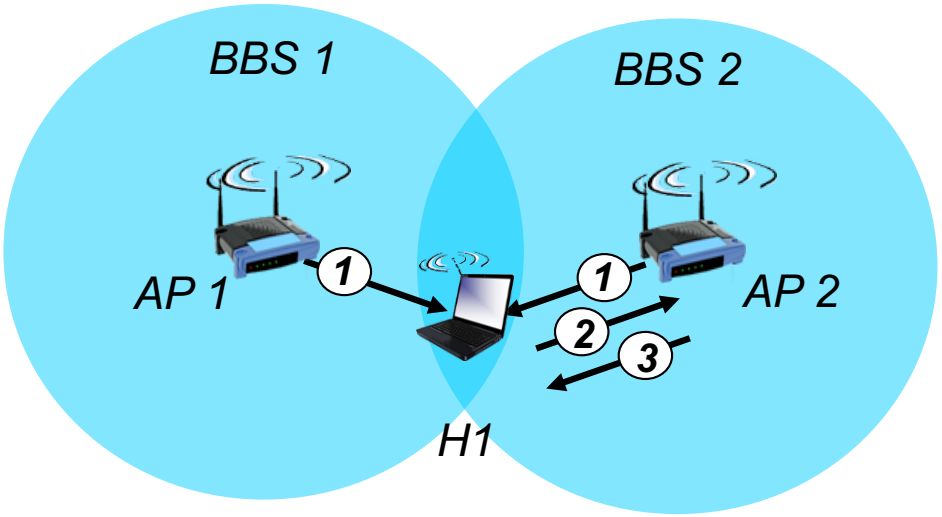
# 802.11: Channels, association

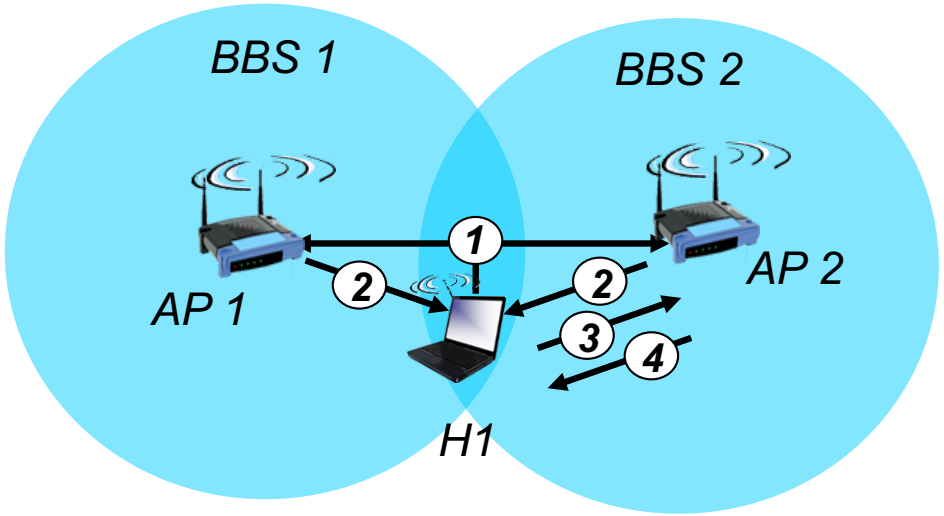
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing 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

# 802.11b channels



# 802.11: passive/active scanning




*passive scanning:*

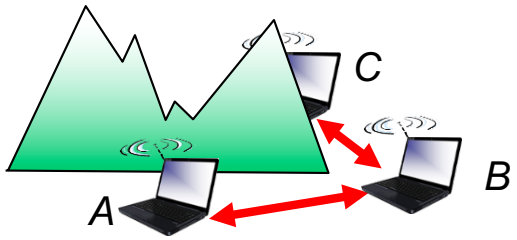
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

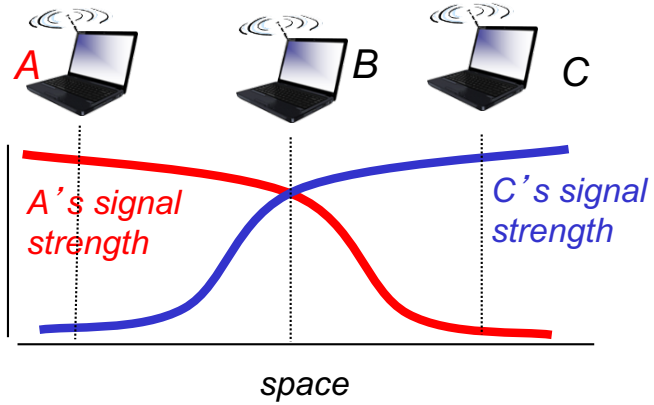
*active scanning:*

(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: $2^+$ 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/C(ollision)A(voidance)



# Multiple access: Key Points

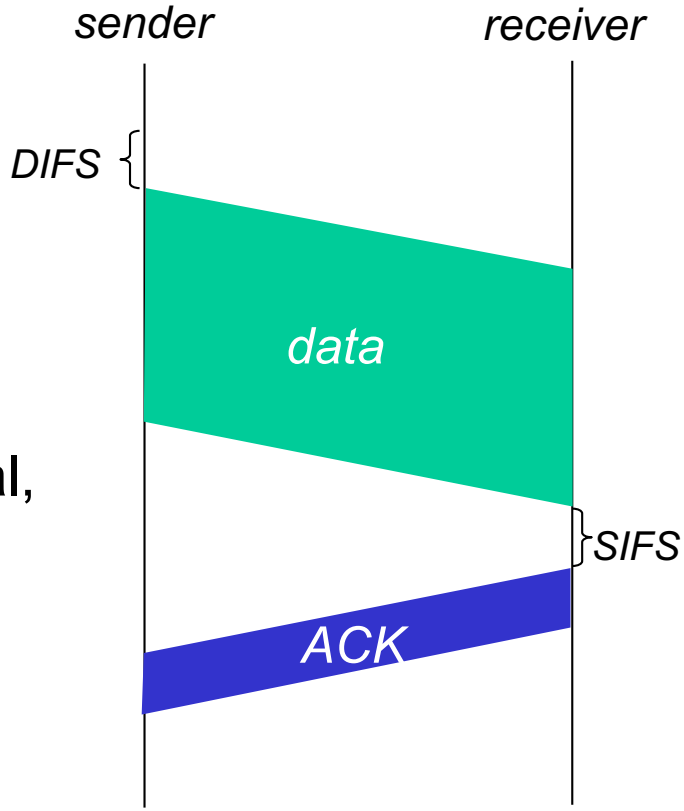
- No concept of a global collision
  - Different receivers hear different signals
  - Different senders reach different receivers
- Collisions are at receiver, not sender
  - Only care if receiver can hear the sender clearly
  - It does not matter if sender can hear someone else
  - As long as that signal does not interfere with receiver
- Goal of protocol
  - Detect if receiver can hear sender
  - Tell senders who might interfere with receiver to shut up

# IEEE 802.11 MAC Protocol: CSMA/CA

## *Distributed Coordination Function (DCF)*

### *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)

***DIFS = DCF Inter Frame space***
***SIFS = Short Inter Frame Space***

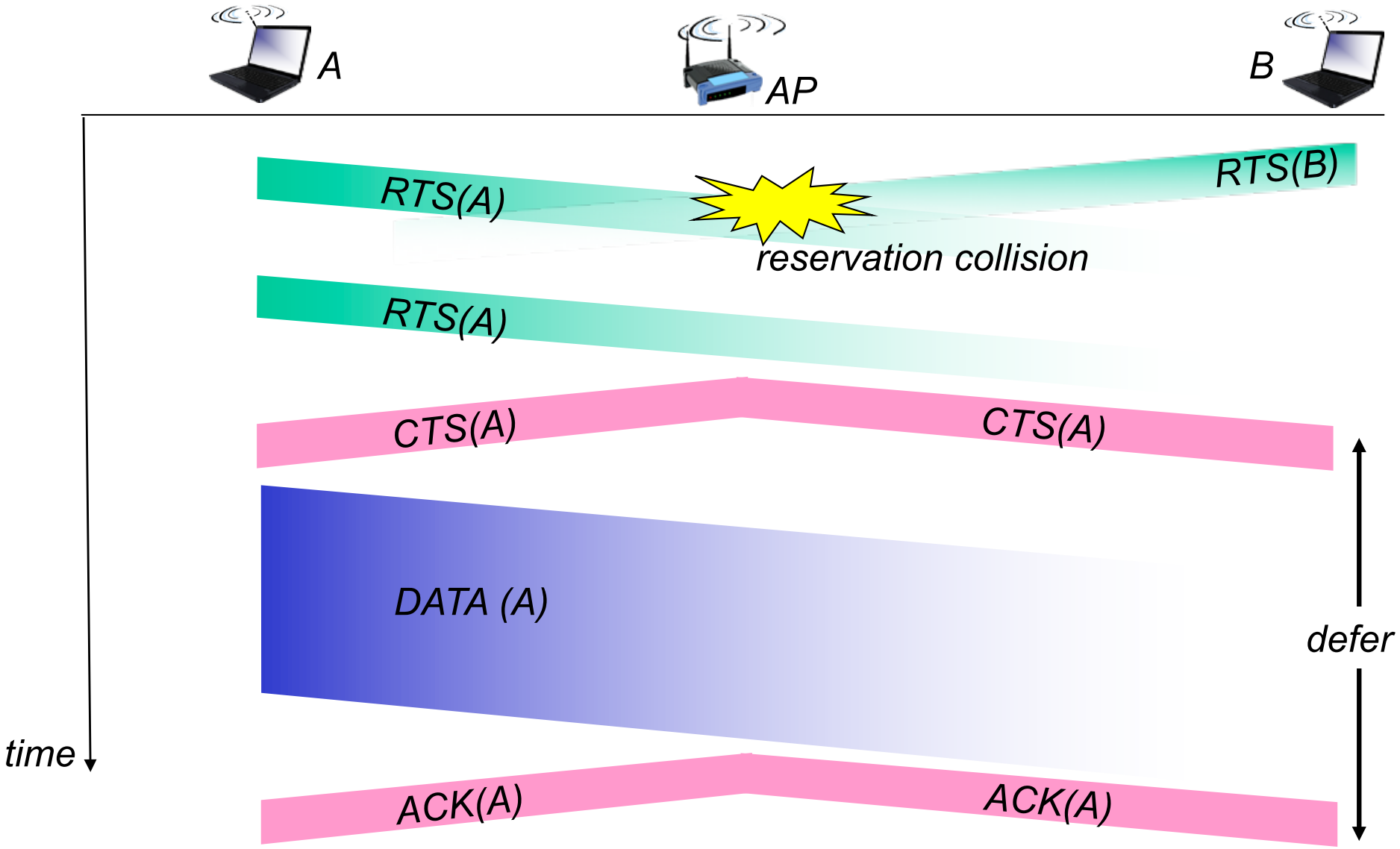
# Avoiding collisions (more)

*idea:* allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

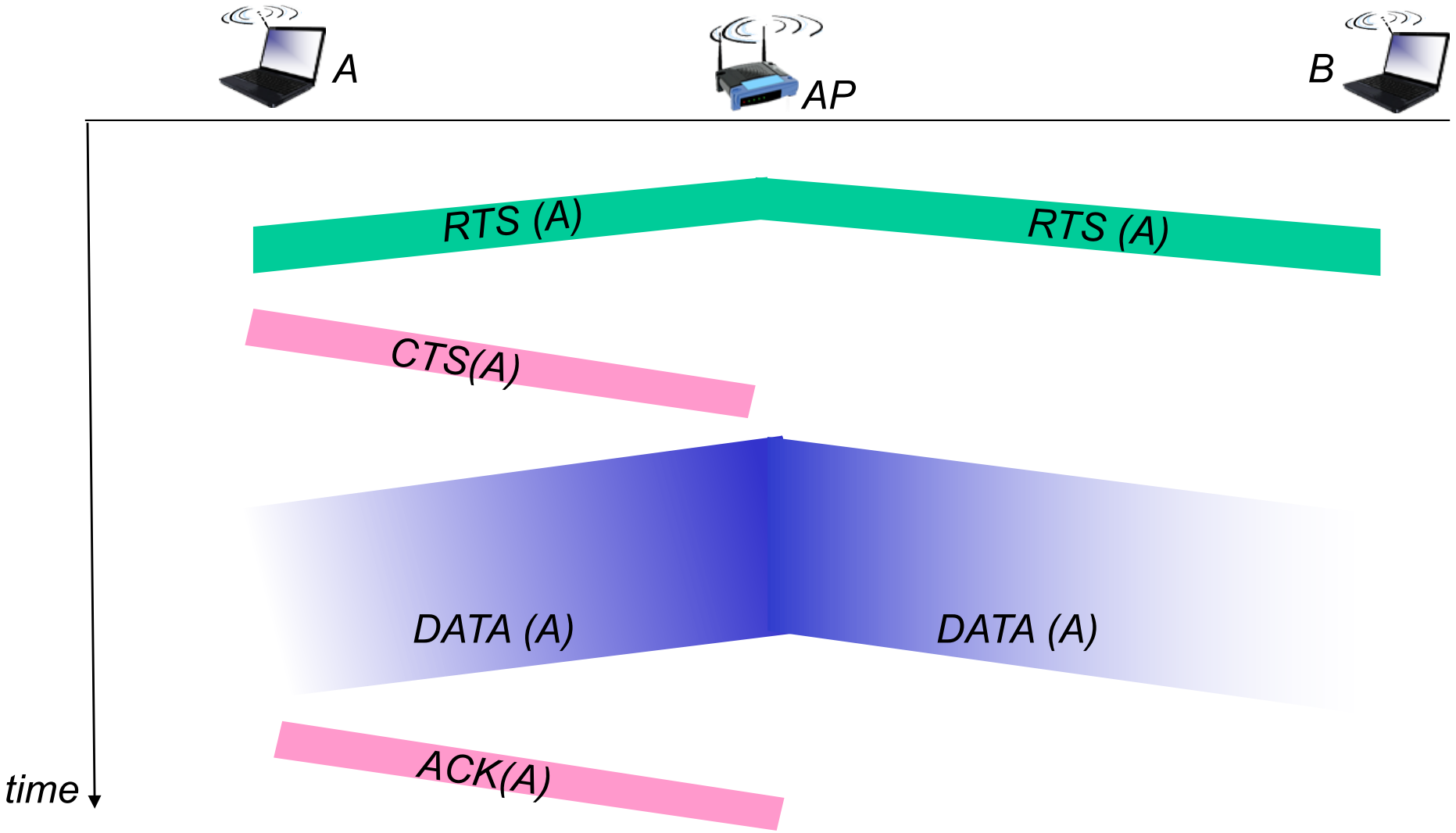
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

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

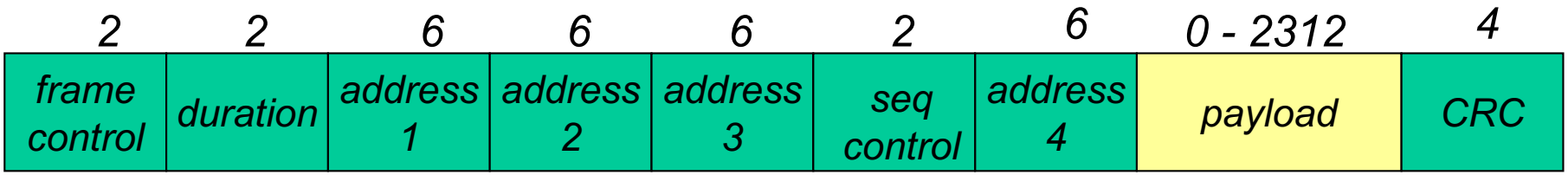
# Collision Avoidance: RTS-CTS exchange



# Collision Avoidance: RTS-CTS exchange



# 802.11 frame: addressing



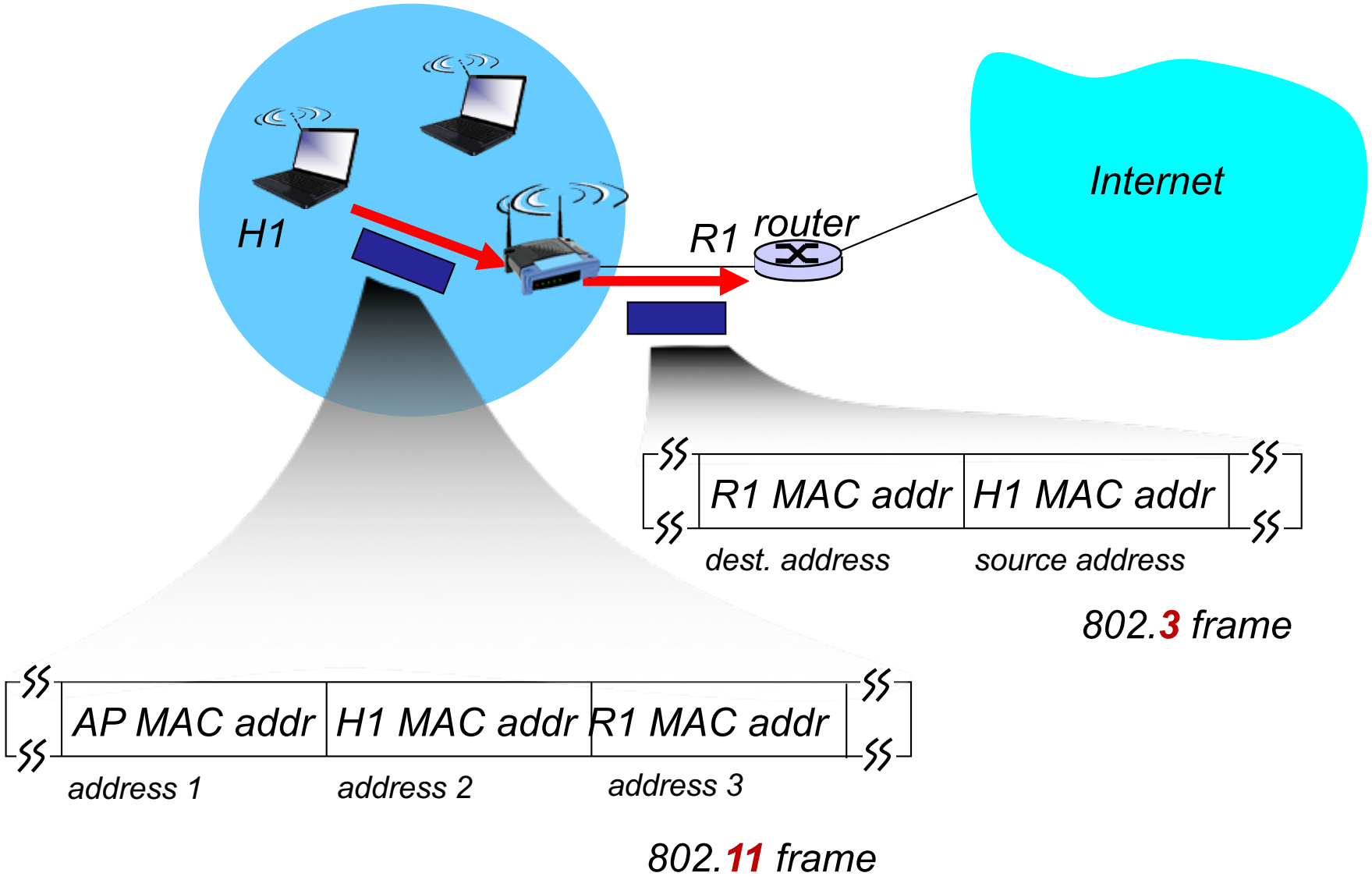

Address 1: MAC address of wireless host or AP to receive this frame

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

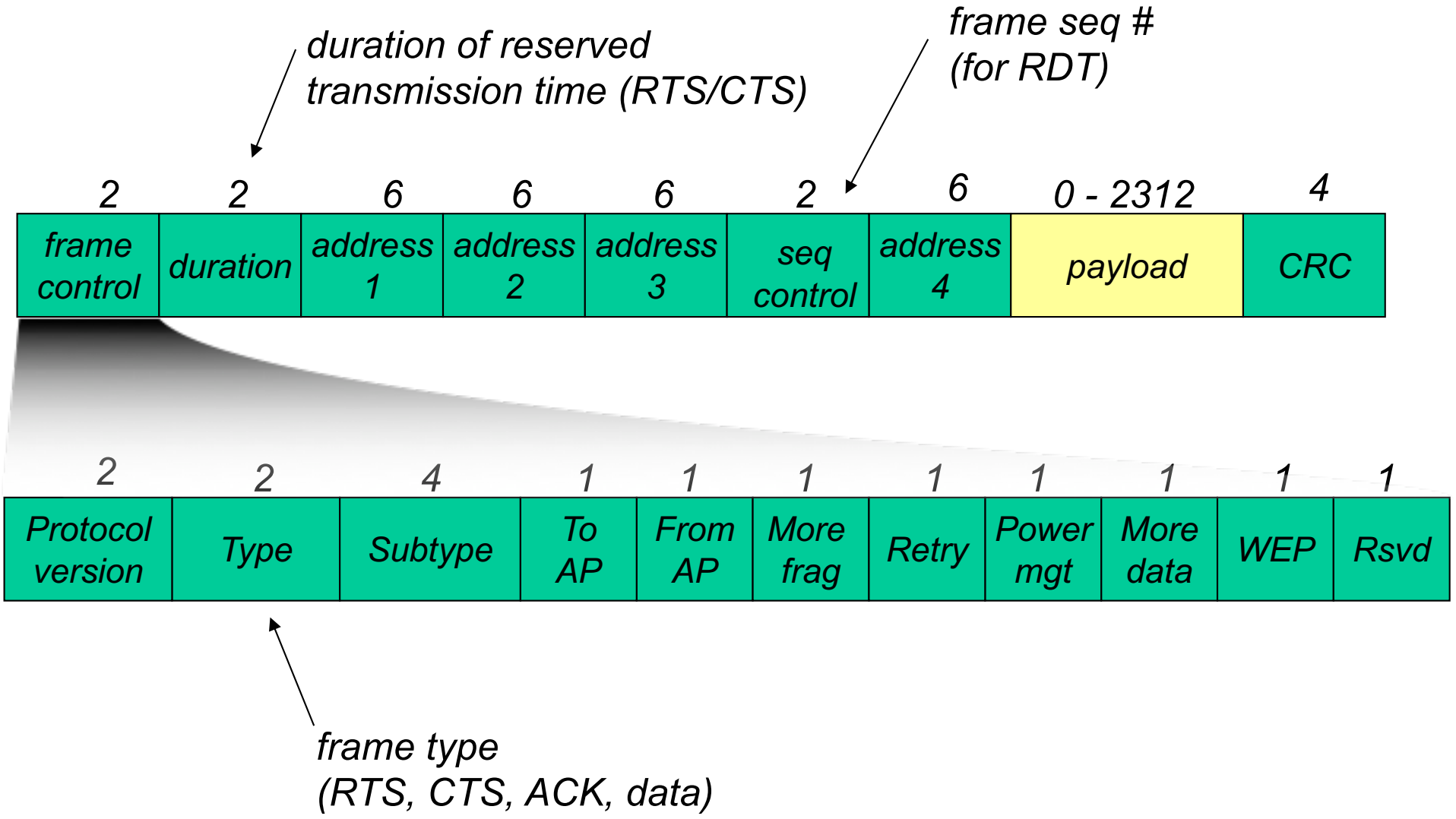
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

# 802.11 frame: addressing



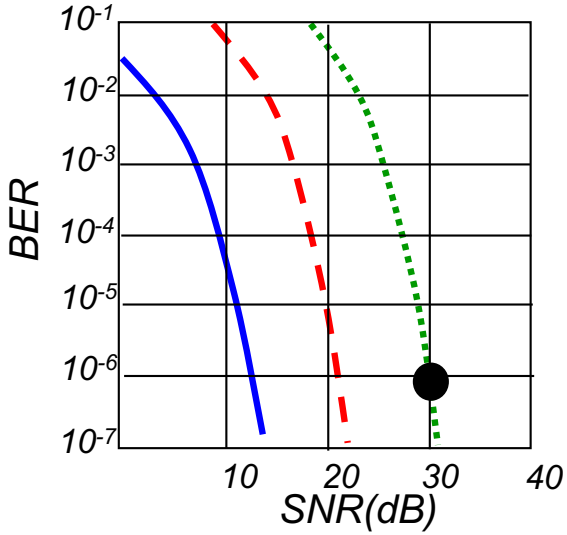
# 802.11 frame: more

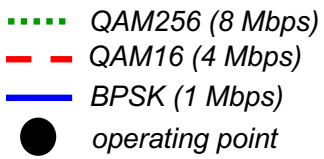


# 802.11: advanced capabilities

## 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*

# Summary

## *Wireless*

- wireless links:
  - capacity, distance
  - channel impairments
- IEEE 802.11 ("Wi-Fi")
  - CSMA/CA reflects wireless channel characteristics