Chapter 7

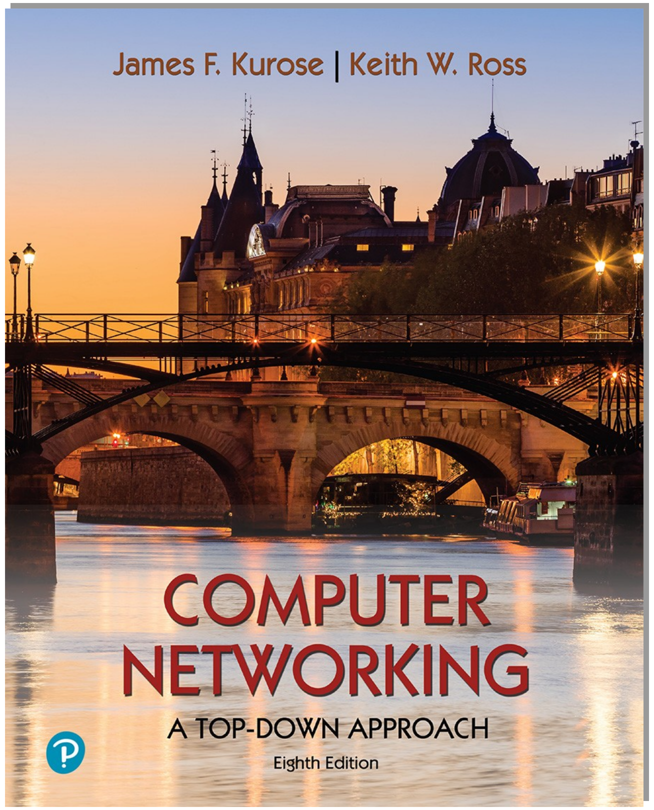
Wireless and Mobile Networks

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



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

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 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

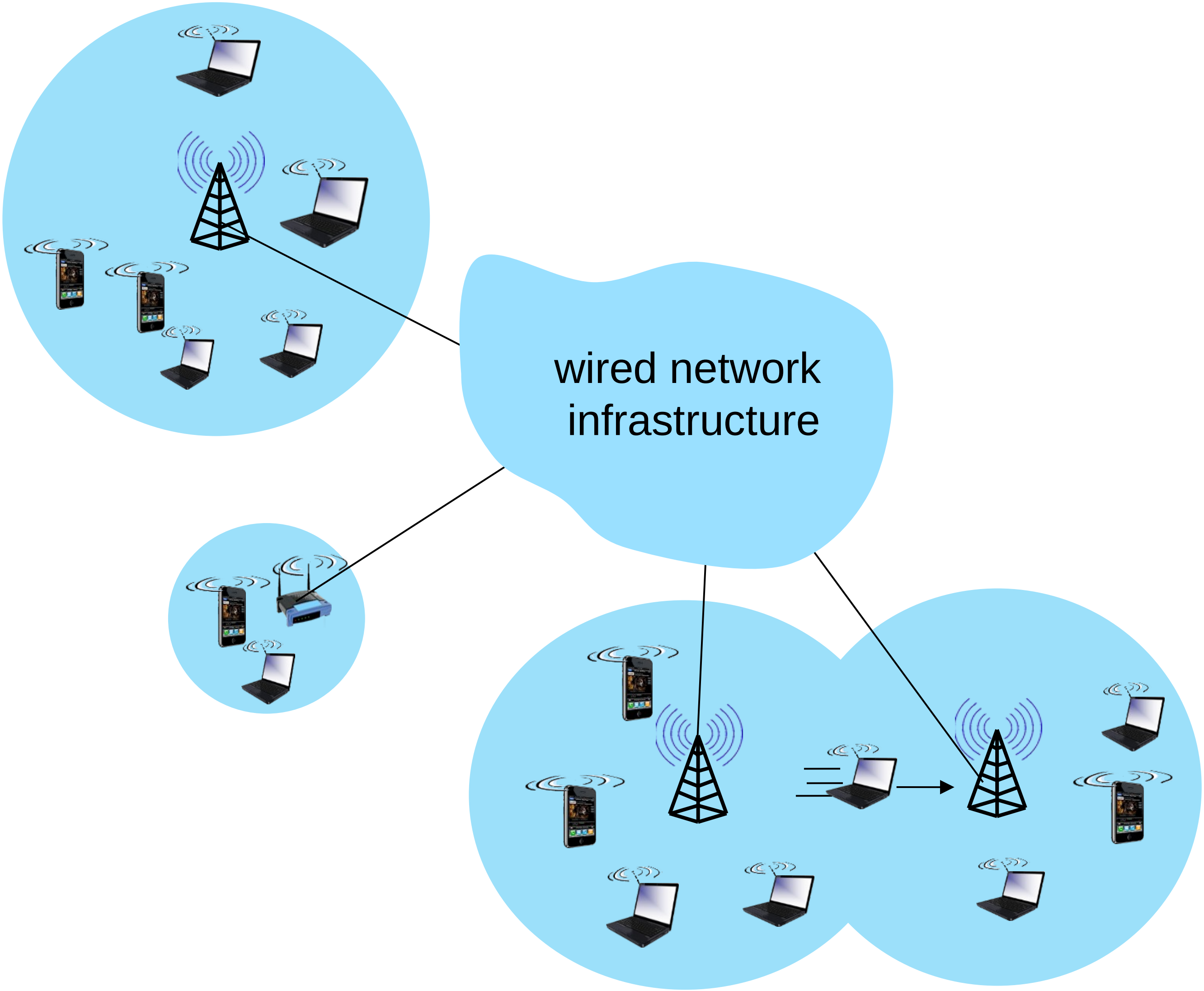
Wireless

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

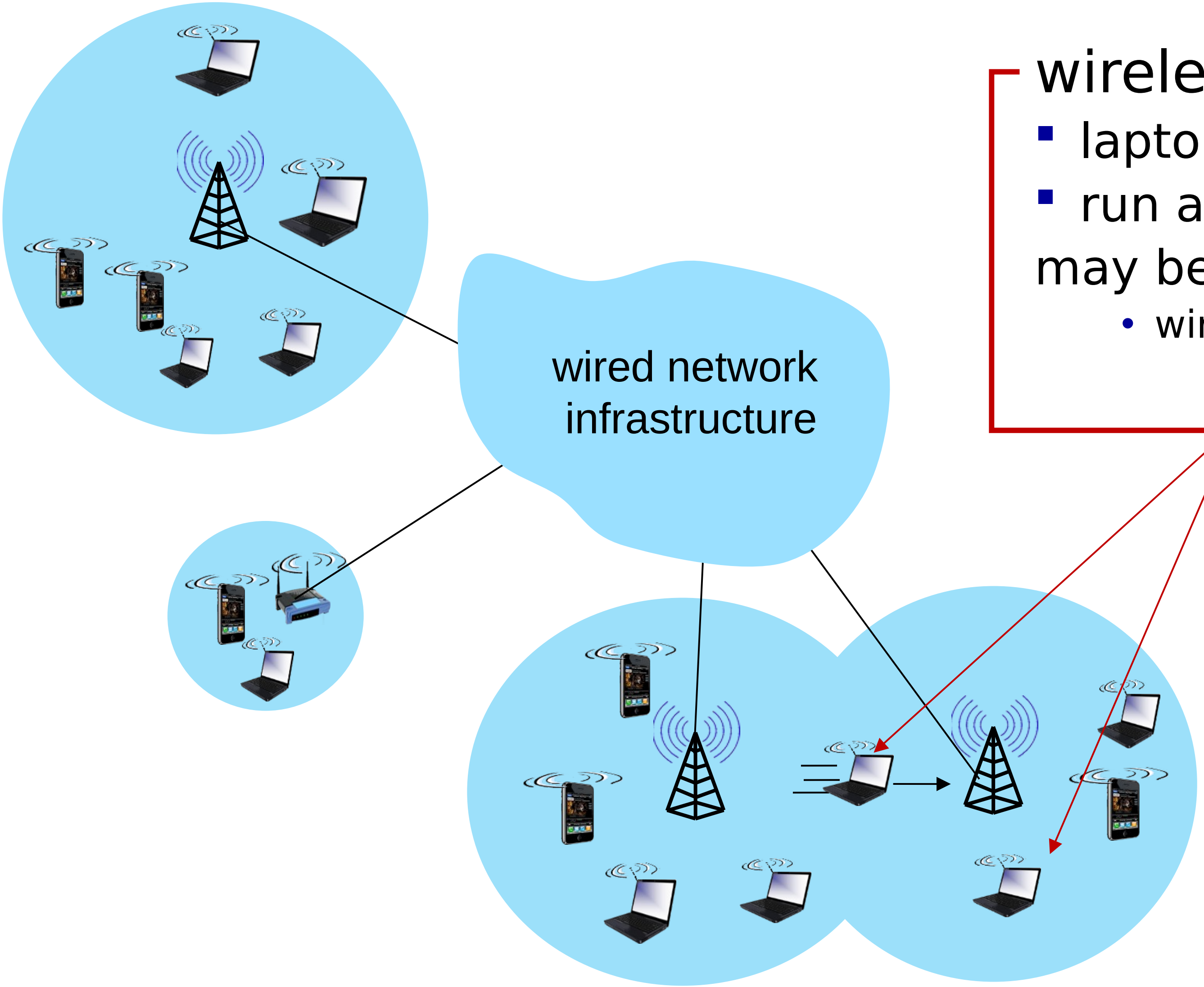
Mobility

- 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



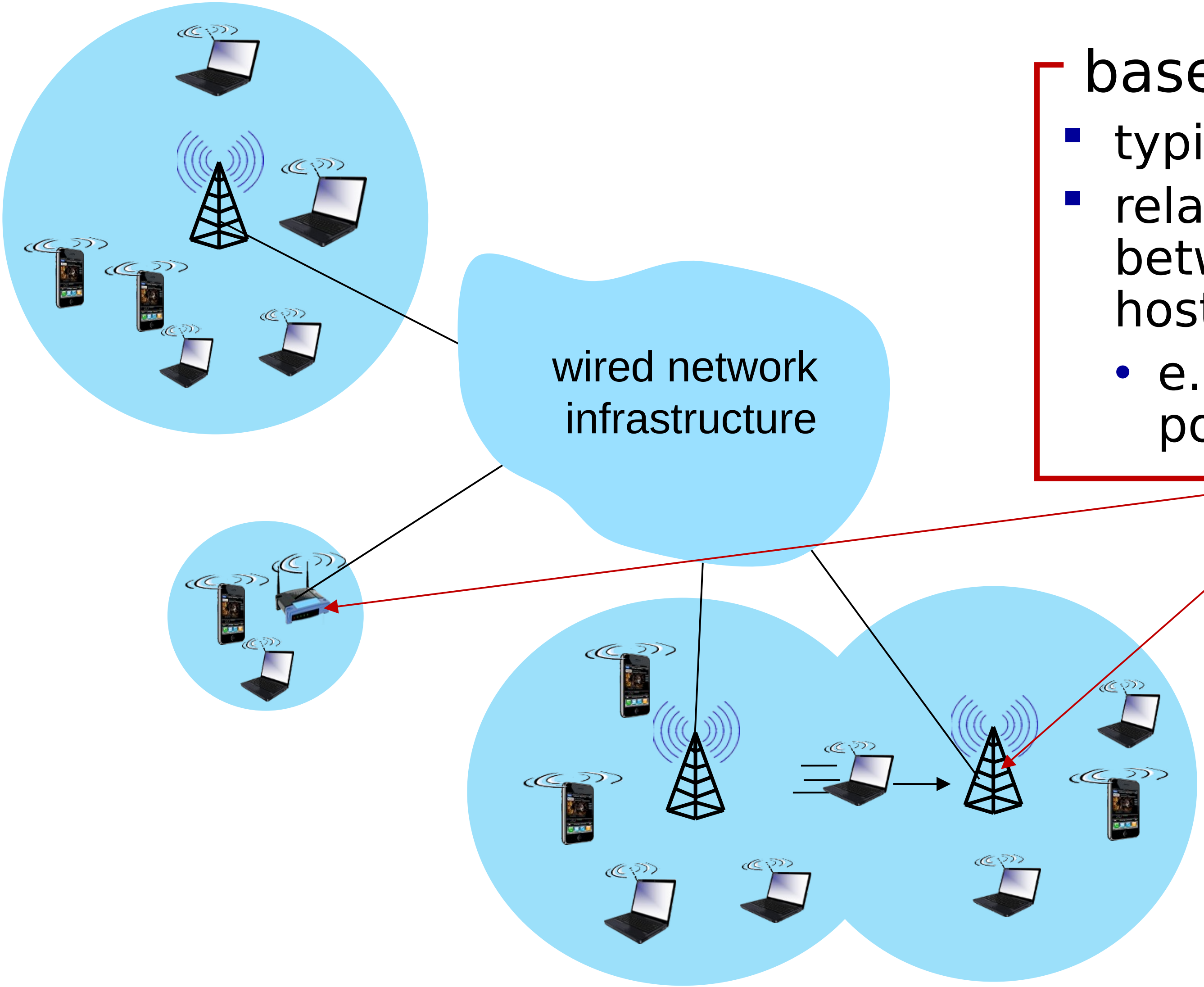
wireless hosts

- laptop, smartphone, IoT
- run applications

may be stationary (non-mobile) or mobile

- wireless does *not* always mean mobility!

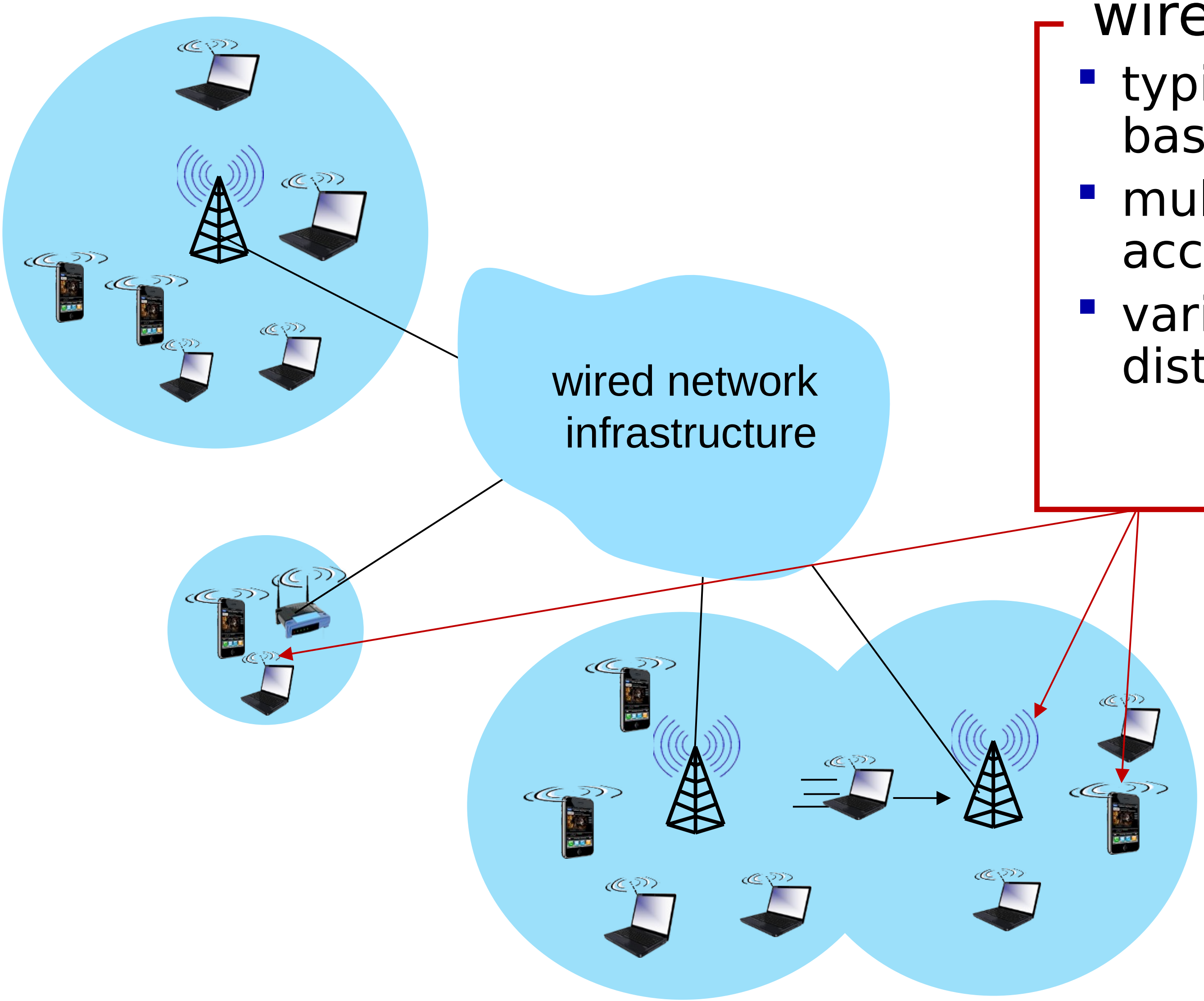
Elements of a wireless network



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

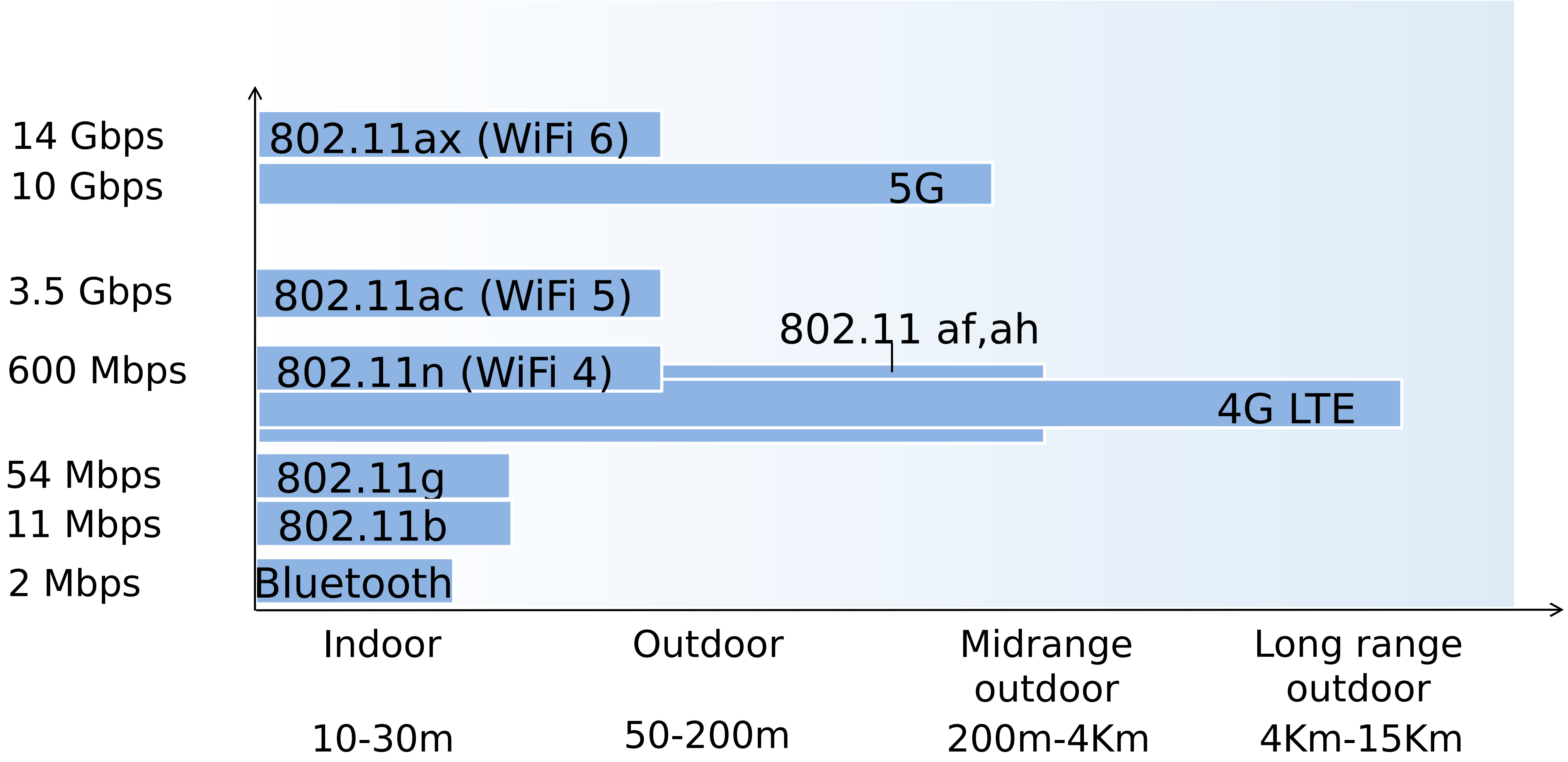
Elements of a wireless network



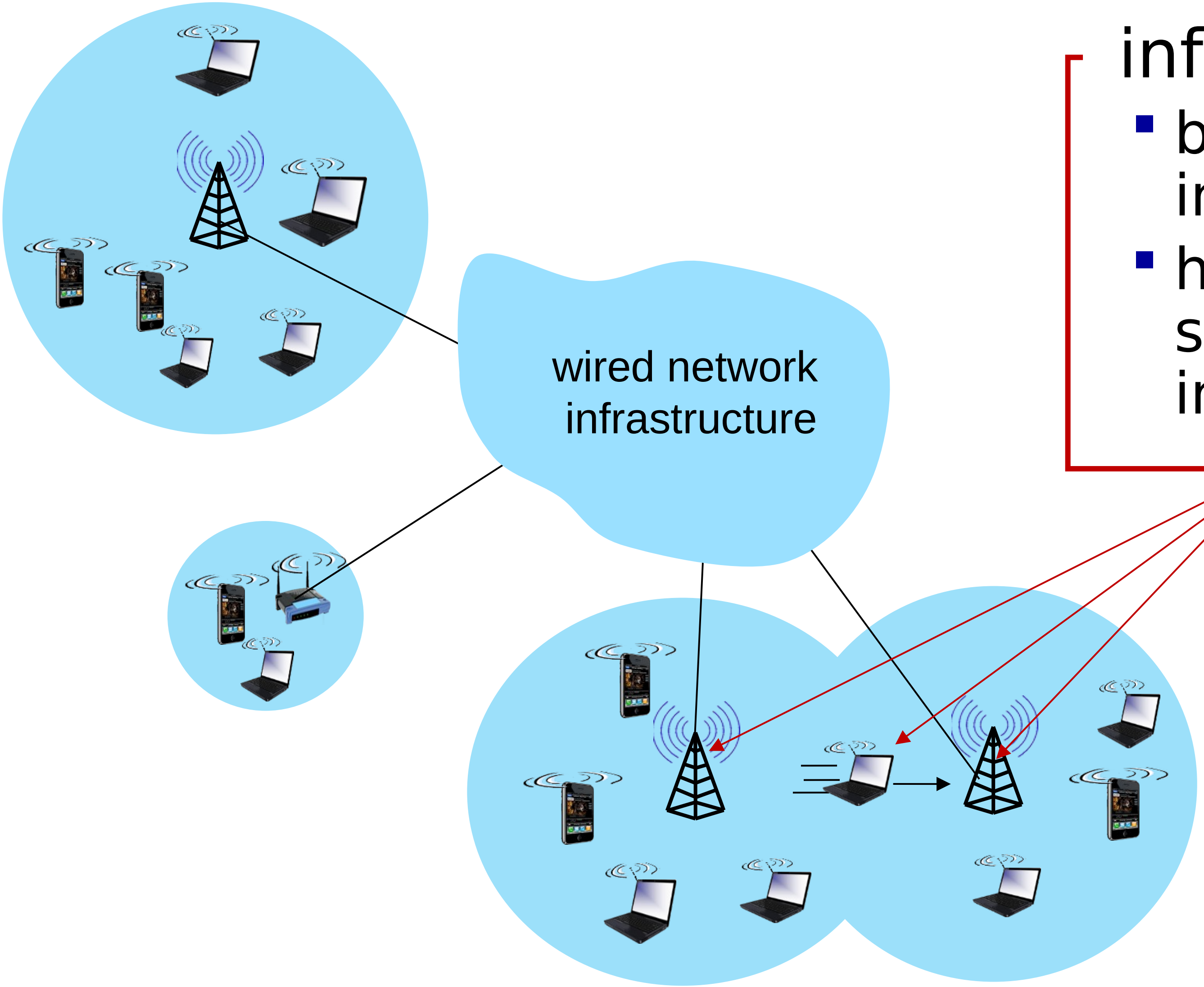
wireless link

- 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



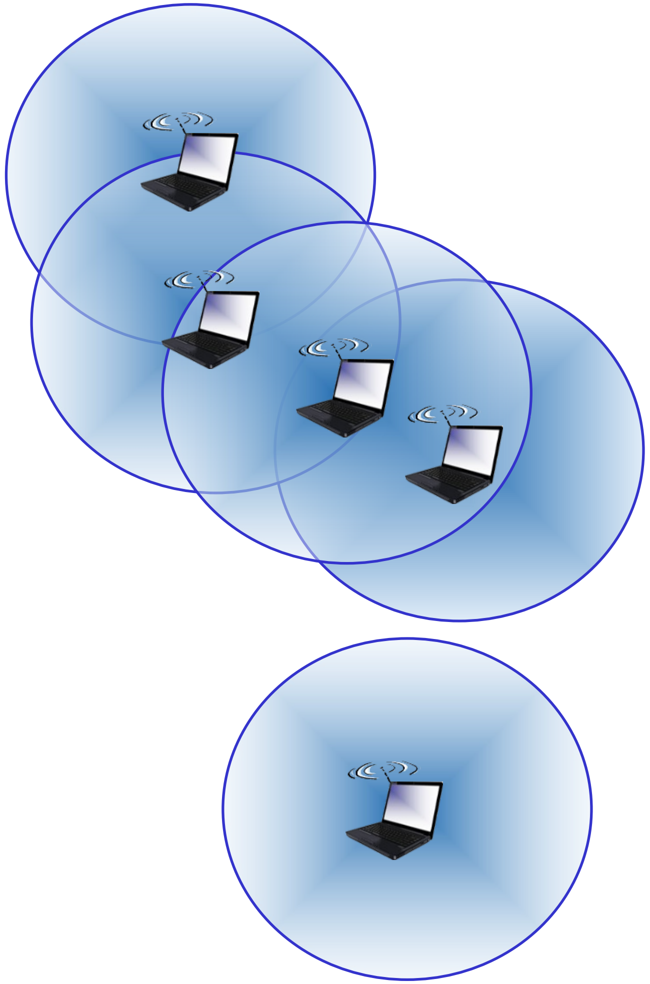
Elements of a wireless network



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: *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

Chapter 7 outline

- Introduction

Wireless

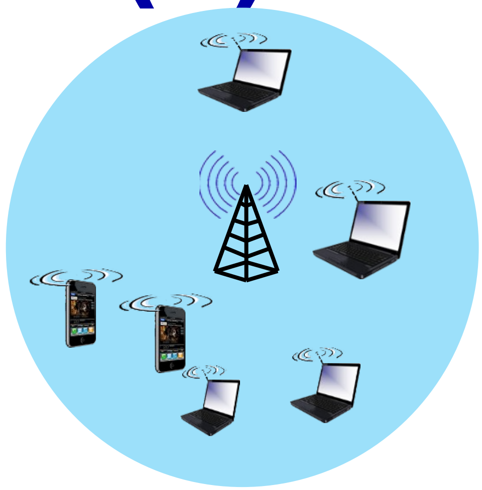
- Wireless links and network characteristics
- WiFi: 802.11 wireless LANs
- Cellular networks: 4G and 5G

Mobility

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

Wireless link characteristics (1)

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 (e.g., 2.4 GHz) shared by many devices (e.g., WiFi, cellular, motors): interference
- 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)

- *decreased signal strength:* radio signal attenuates as it propagates through matter (path loss)

Tipo di barriera	Potenziale di interferenza
Legno	Basso
Materiale sintetico	Basso
Vetro	Basso
Acqua	Medio
Mattoni	Medio
Marmo	Medio
Intonaco	Alto
Cemento	Alto
Vetro antiproiettili	Alto
Metallo	Molto alto

Source: https://support.apple.com/it-it/HT201542

Wireless Link Characteristics (3)

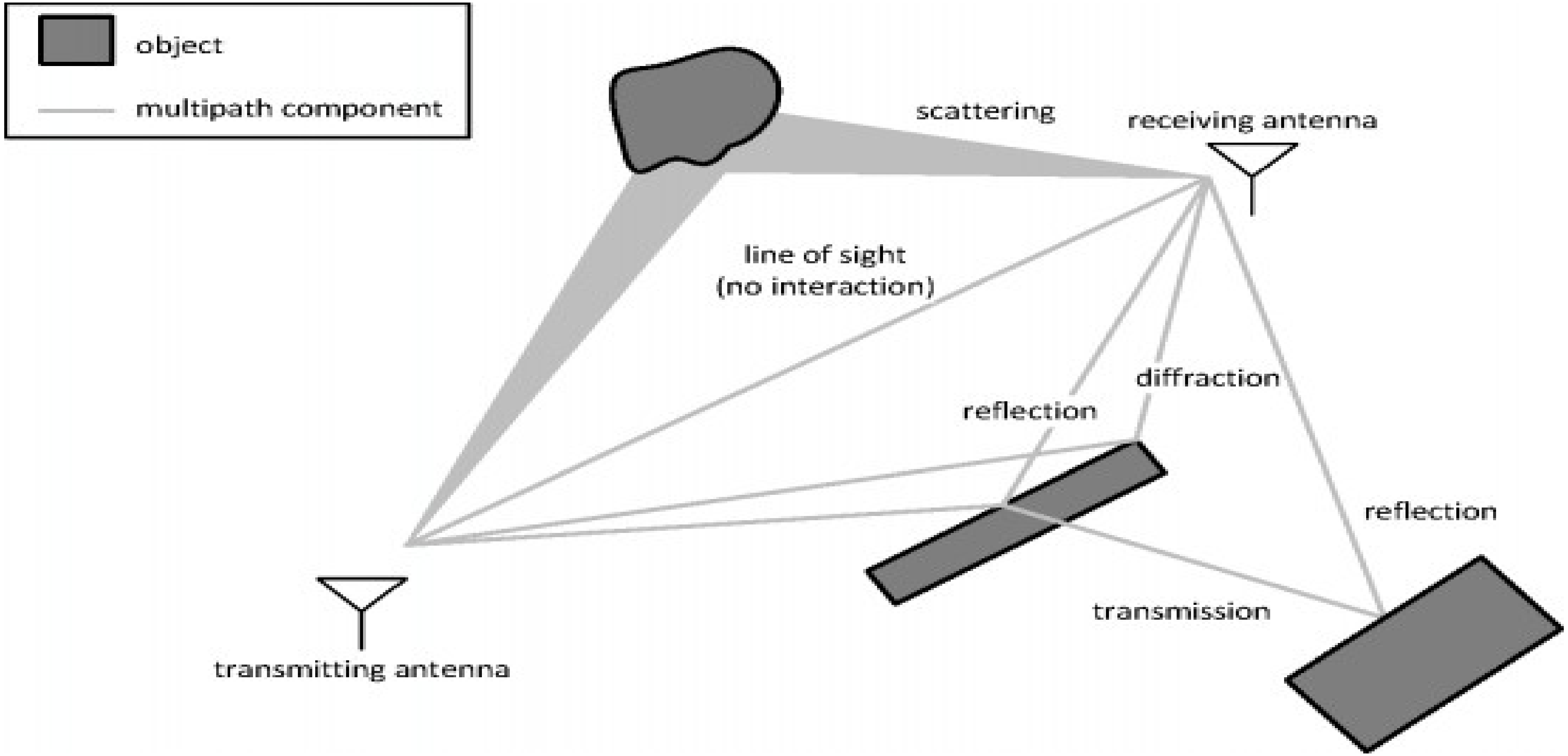
interference from other sources:

- *Microwave oven*
- *Coax cables of Direct Satellite Service*
- *Power line/sources*
- *Cordless phones*
- *Wireless audio devices*
- *Monitor and LCD display*
- *Unshielded cables*
- *…*

Source: **https://support.apple.com/it-it/HT201542**

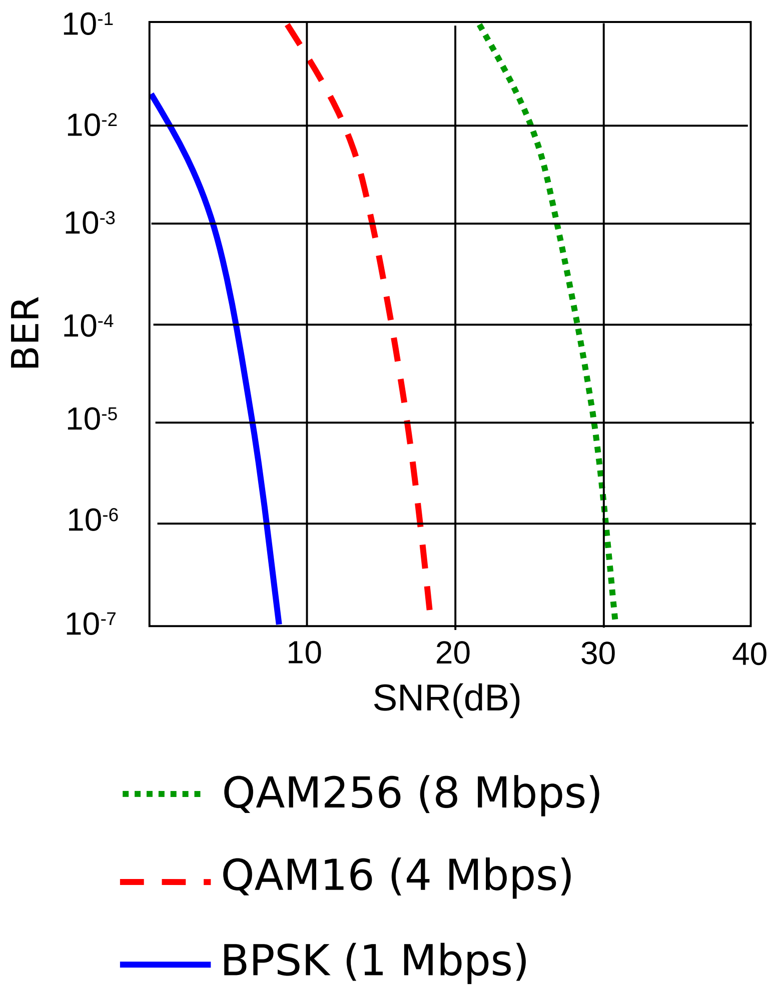
Wireless Link Characteristics (4)

multipath propagation:



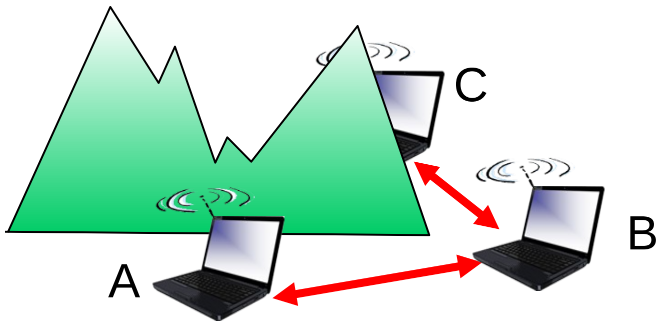
Wireless link characteristics (2)

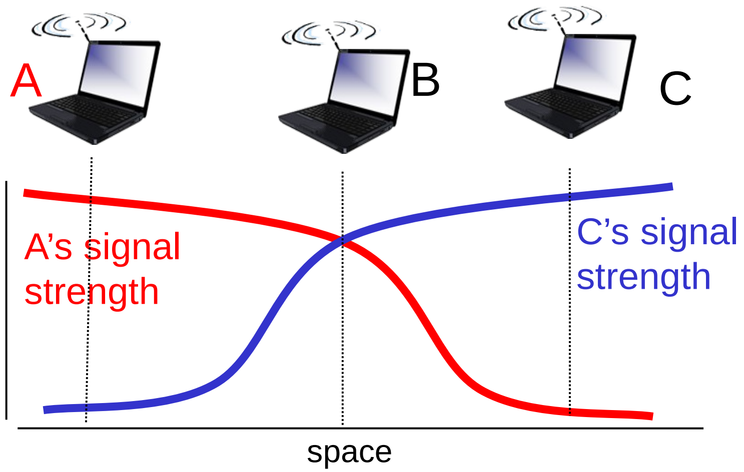
- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a “good thing”)
- SNR versus bit error rate (BER) tradeoffs
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput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



Wireless link characteristics (3)

Multiple wireless senders, 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

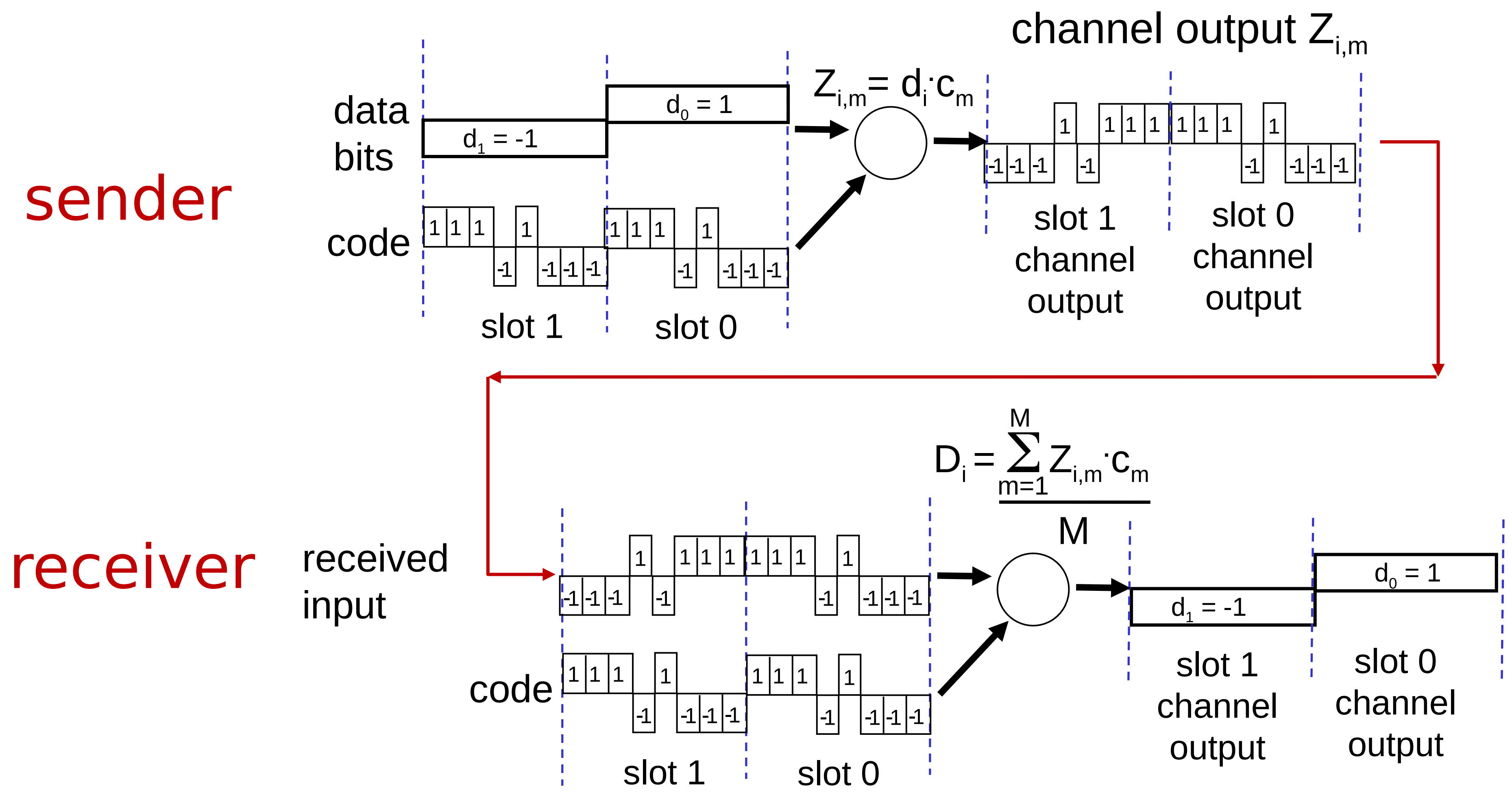
Signal attenuation:

- 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”)
- encoding: inner product: (original data) X (chipping sequence)
- decoding: summed inner-product: (encoded data) X (chipping sequence)

CDMA encode/decode

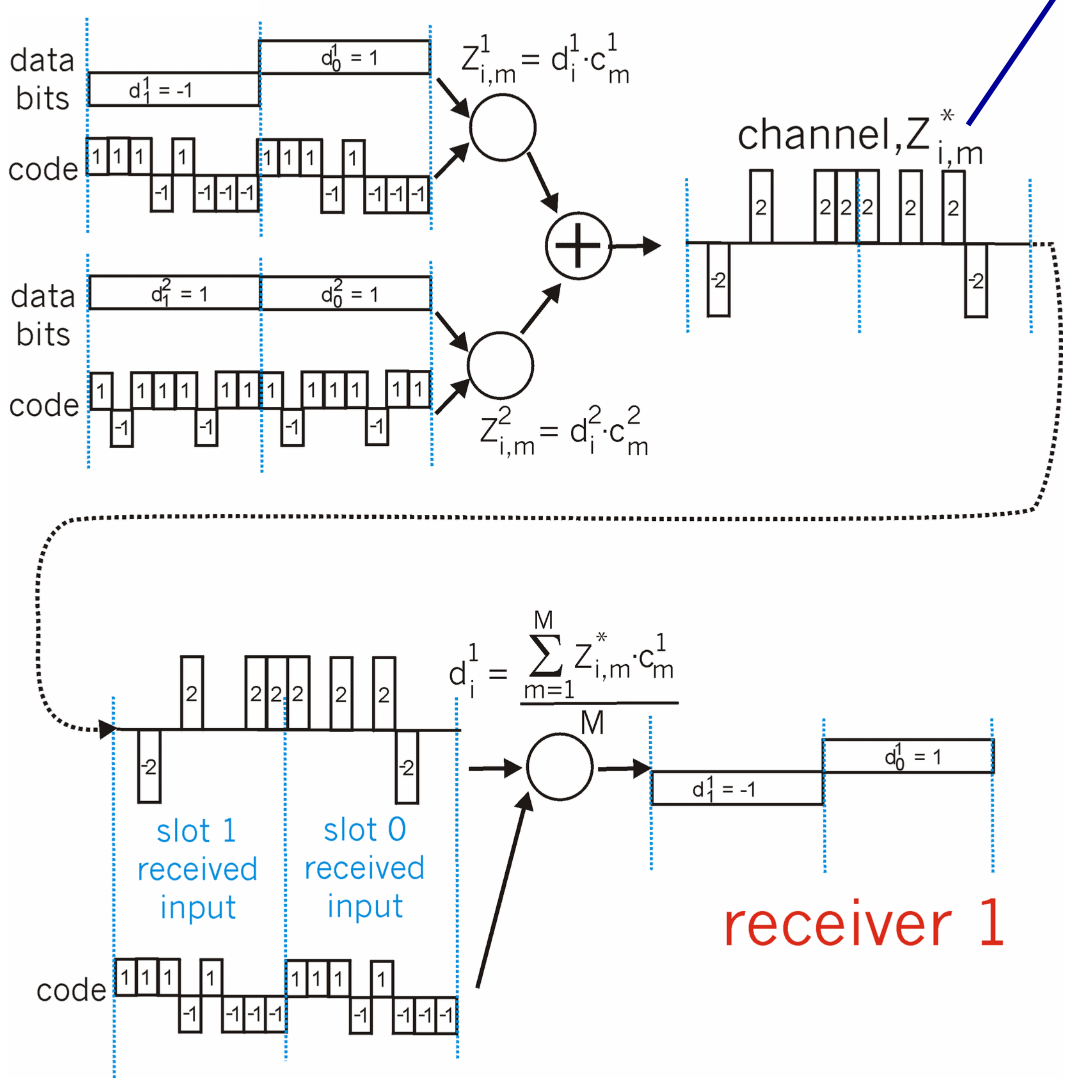


... but this isn't really useful yet!

CDMA: two-sender interference

Sender 1

Sender 2



channel sums together transmissions by sender 1 and 2

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

receiver 1

… now *that's* useful!

CDMA: how it works?

- The chip sequences must be pair-wise orthogonal:

$$\mathbf{S}\bullet\mathbf{T} \equiv \frac{1}{m}\sum_{i=1}^{m} S_i T_i = 0$$

For any **S, T**

- Moreover by definition:

$$\mathbf{S}\bullet\mathbf{S} = \frac{1}{m}\sum_{i=1}^{m} S_i S_i = \frac{1}{m}\sum_{i=1}^{m} S_i^2 = \frac{1}{m}\sum_{i=1}^{m} (\pm 1)^2 = 1$$

For any **S**

- Assuming A,B, C send bit 1, 0,1 respectively, we have:

$$\mathbf{S} = \mathbf{A} + \overline{\mathbf{B}} + \mathbf{C}$$

- At reception C decoding will be:

$$\mathbf{S}\bullet\mathbf{C} = (\mathbf{A} + \overline{\mathbf{B}} + \mathbf{C})\bullet\mathbf{C} = \mathbf{A}\bullet\mathbf{C} + \overline{\mathbf{B}}\bullet\mathbf{C} + \mathbf{C}\bullet\mathbf{C} = 0 + 0 + 1 = 1$$

Chapter 7 outline

- Introduction

Wireless

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

Mobility

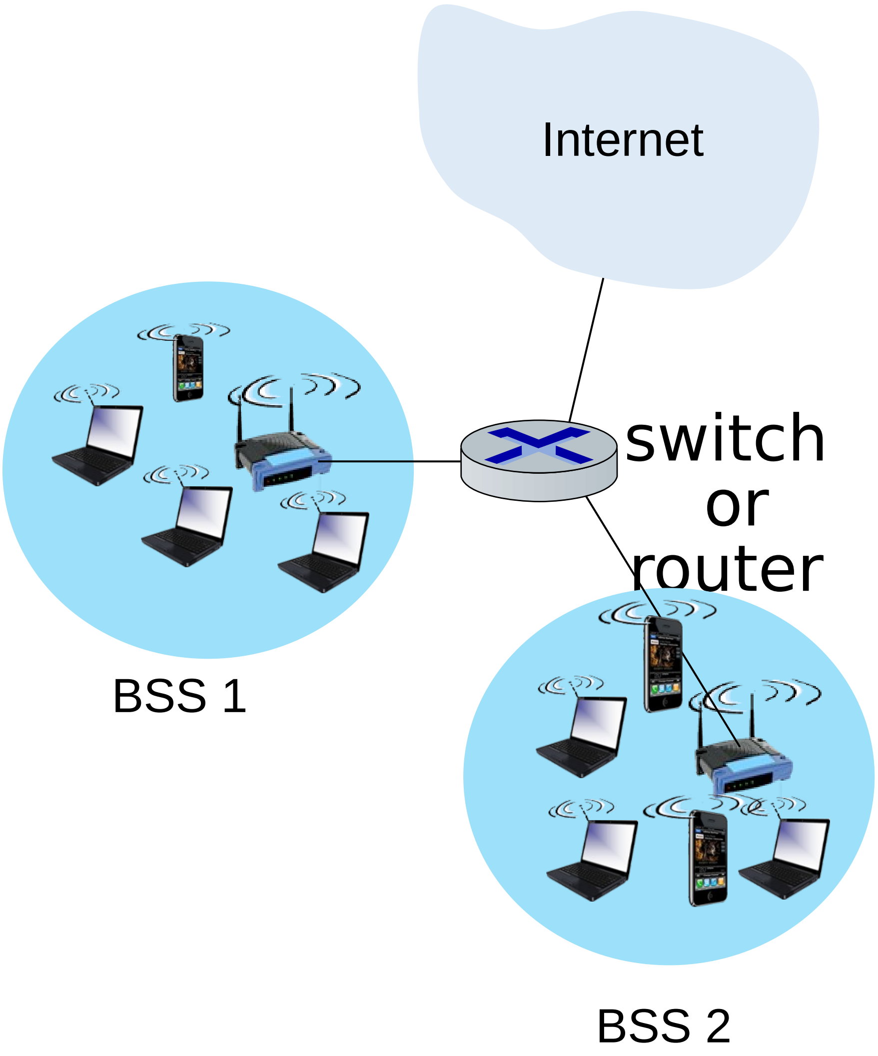
- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols

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 have base-station and ad-hoc network versions

802.11 LAN architecture

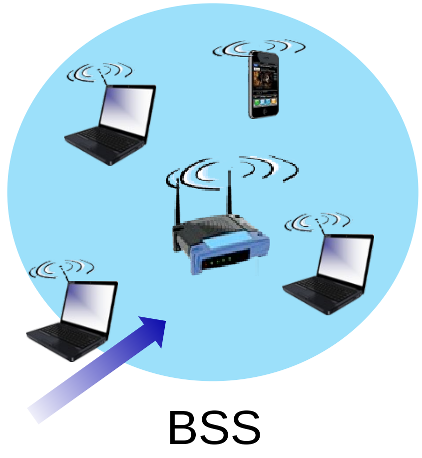


- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.11: Channels, association

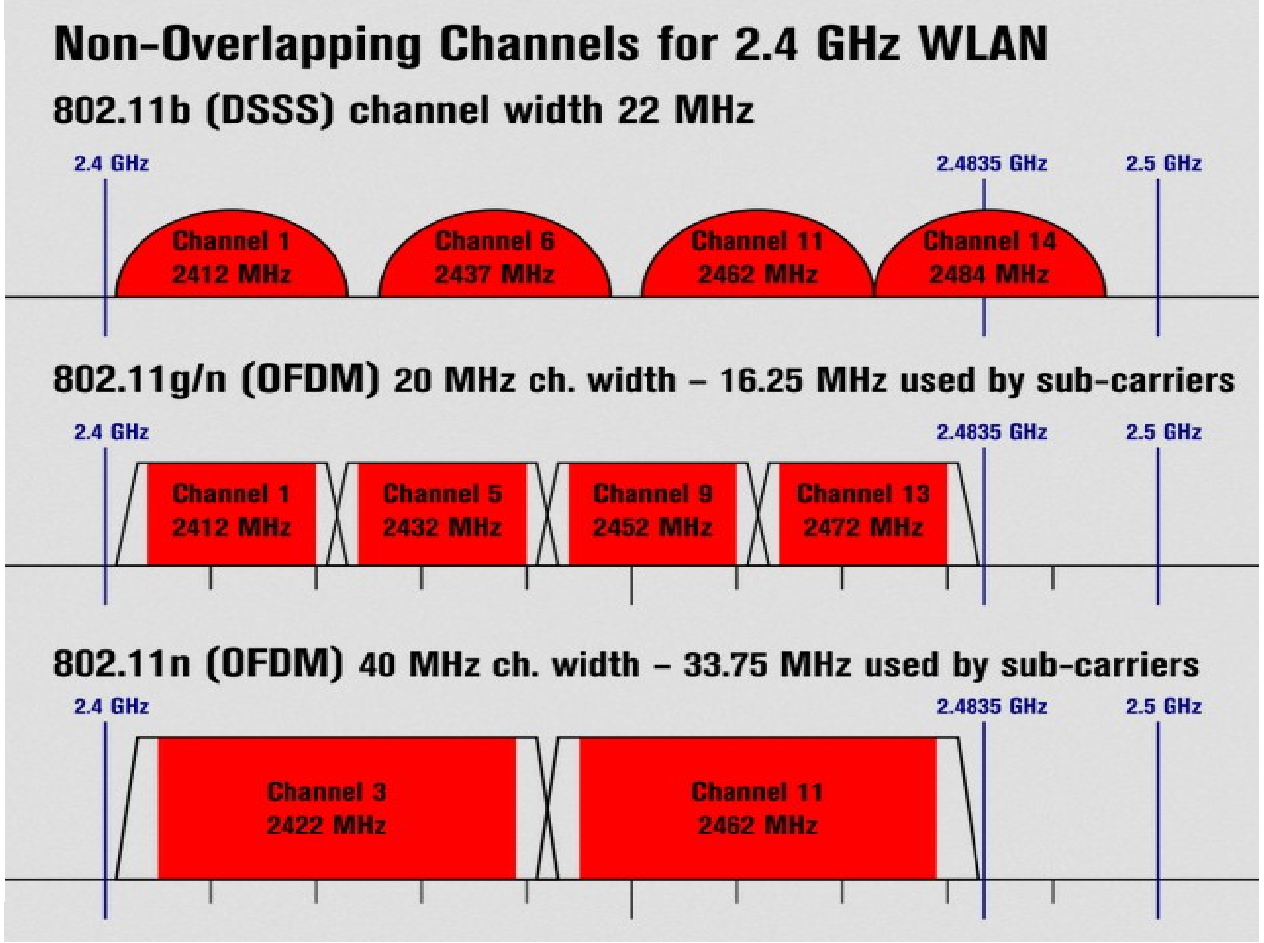
- spectrum divided into channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!

- 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



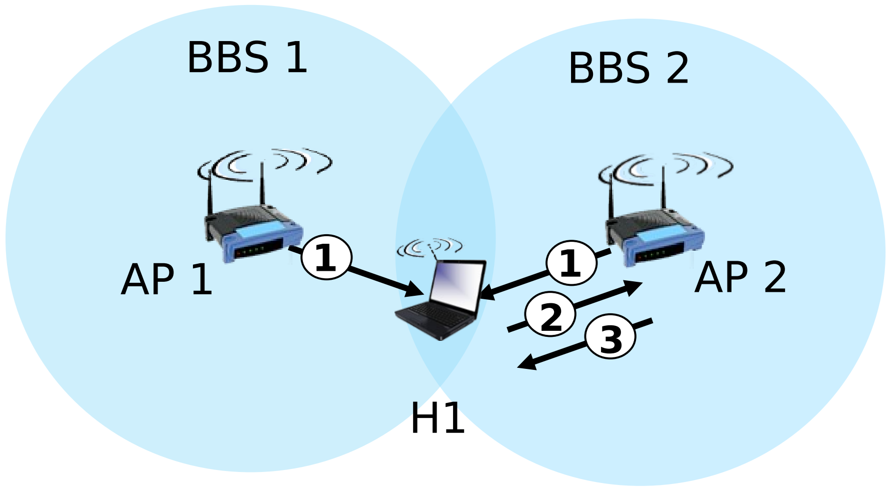
802.11: Channels, association(2)

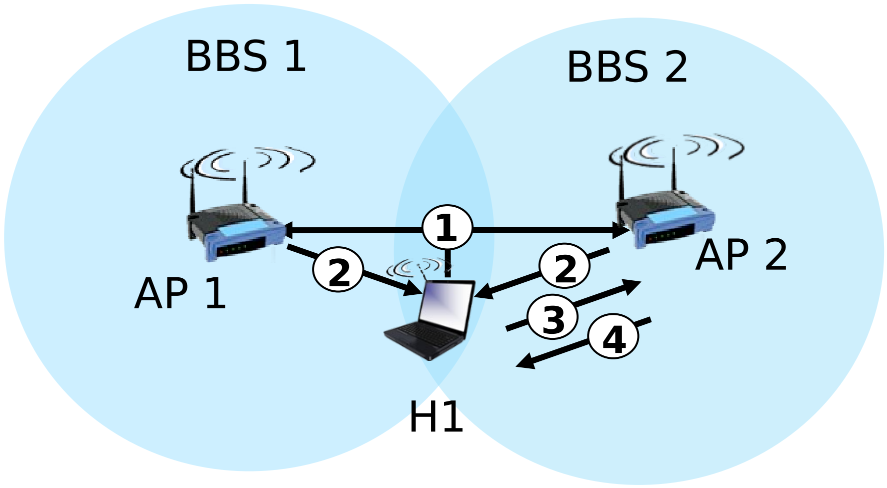
Channel	Frequency (MHz)	North America [6]	Japan[6]	Most of world [6][7][8][9][10][11][12]
1	2412	Yes	Yes	Yes
2	2417	Yes	Yes	Yes
3	2422	Yes	Yes	Yes
4	2427	Yes	Yes	Yes
5	2432	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9	2452	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No[B]	Yes	Yes
13	2472	No[B]	Yes	Yes
14	2484	No	11b only[C]	No



Source: **https://en.wikipedia.org/wiki/List_of_WLAN_channels**

802.11: passive/active scanning





passive scanning:

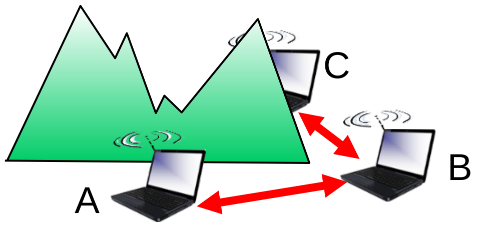
1) beacon frames sent from APs
2) association Request frame sent: H1 to selected AP
3) association Response frame sent from selected AP to H1

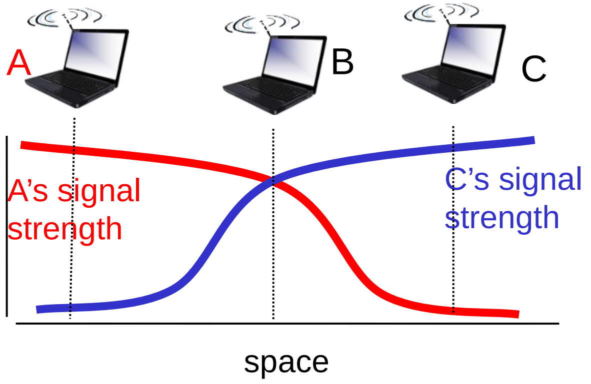
active scanning:

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 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/<u>C</u>ollision<u>A</u>voidance



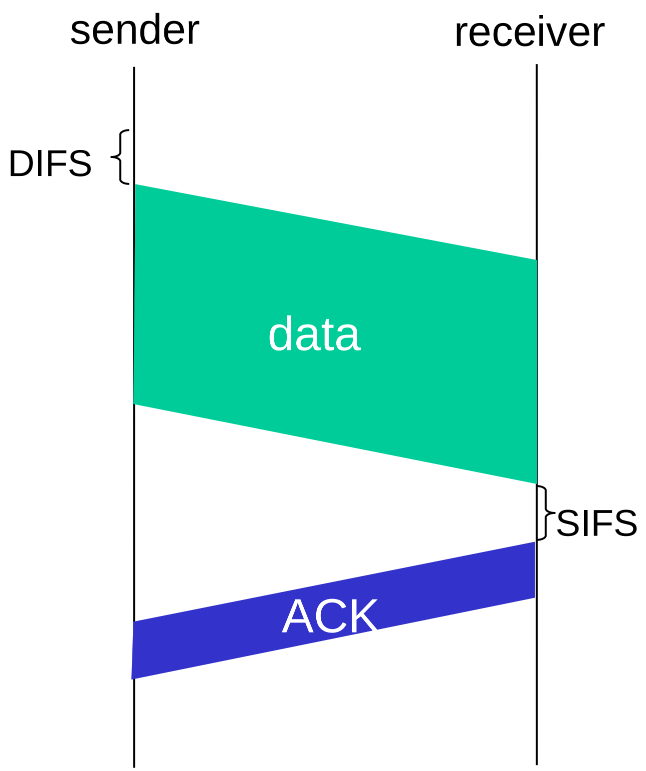


IEEE 802.11 MAC Protocol: CSMA/CA

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)

802.11: CSMA/CA behavior

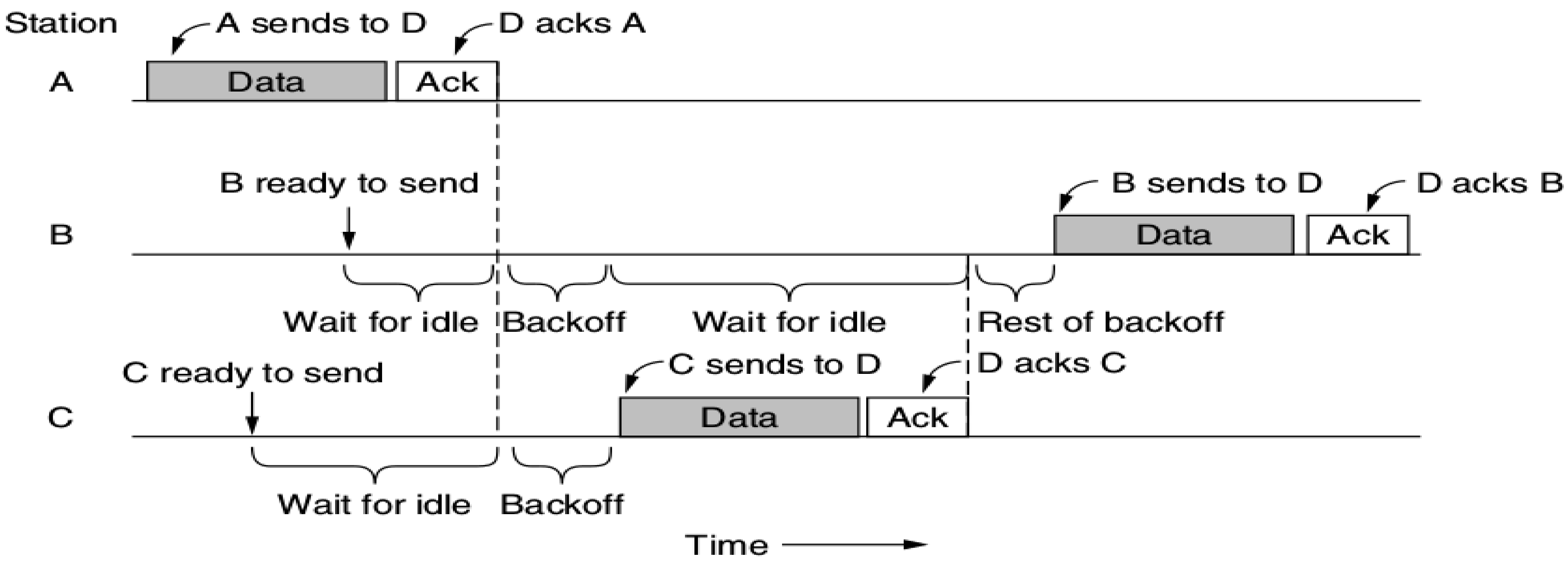


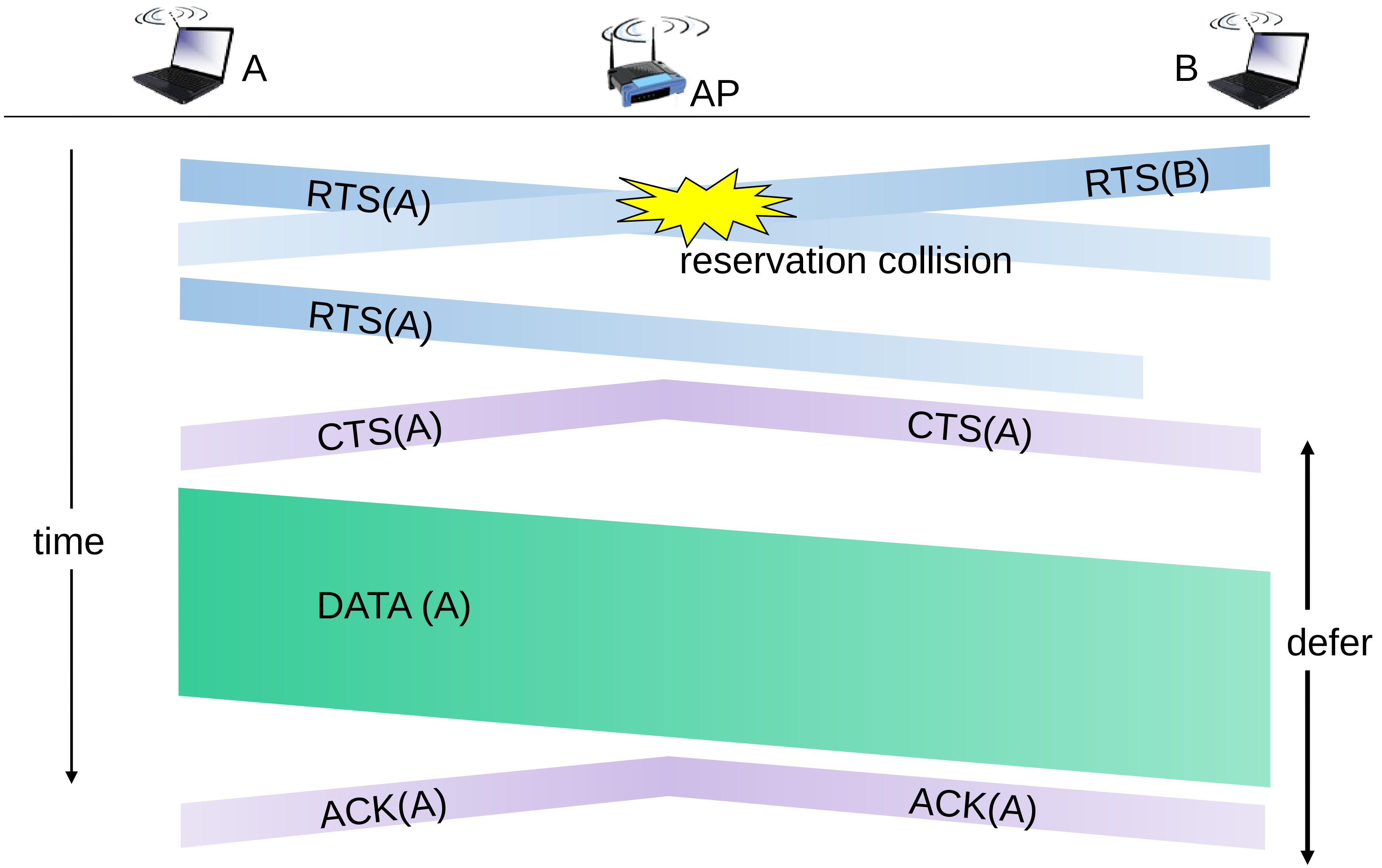
Figure 4-25. Sending a frame with CSMA/CA.

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

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

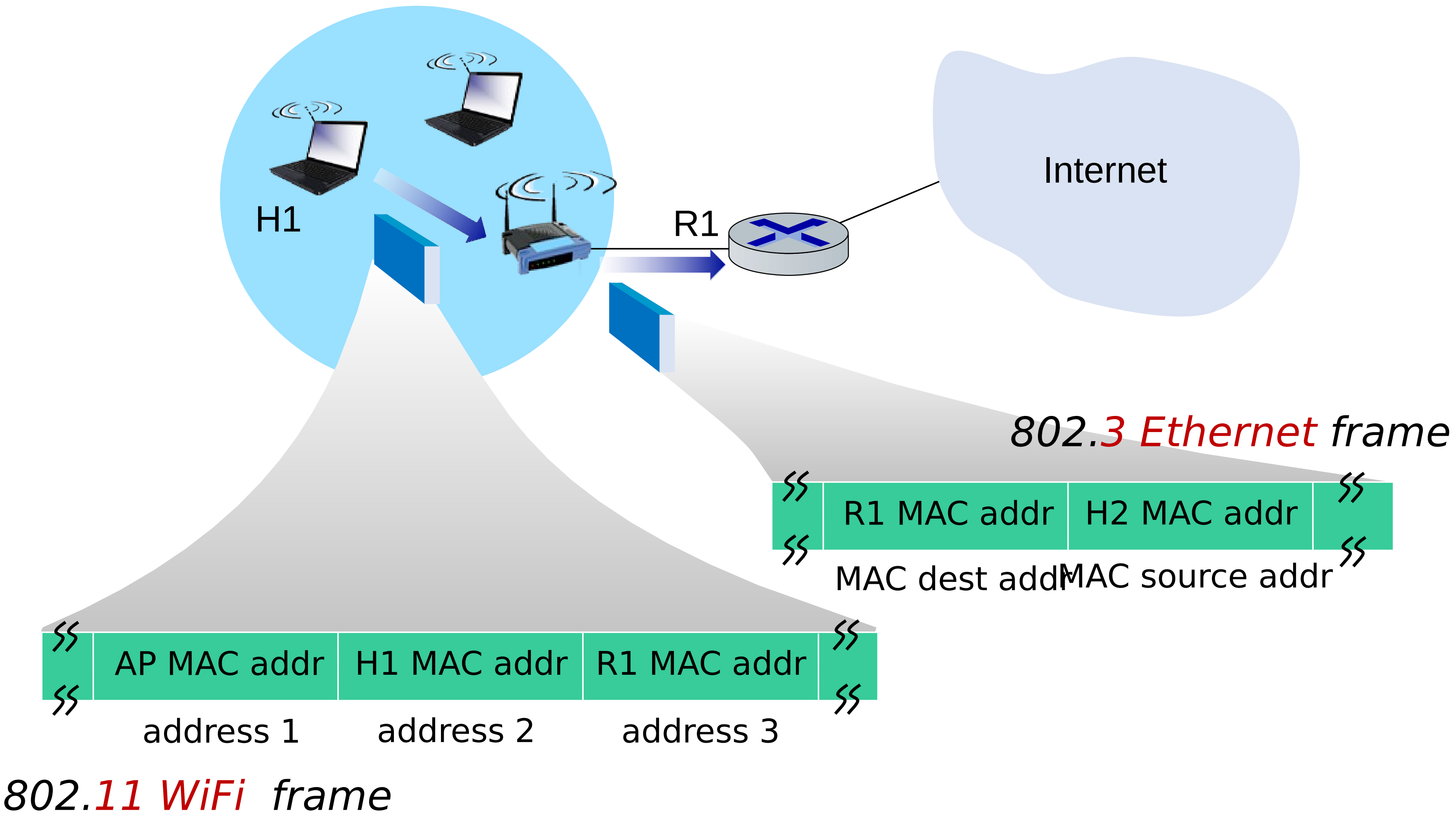
Address 1: MAC address of wireless host or AP to receive this frame

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

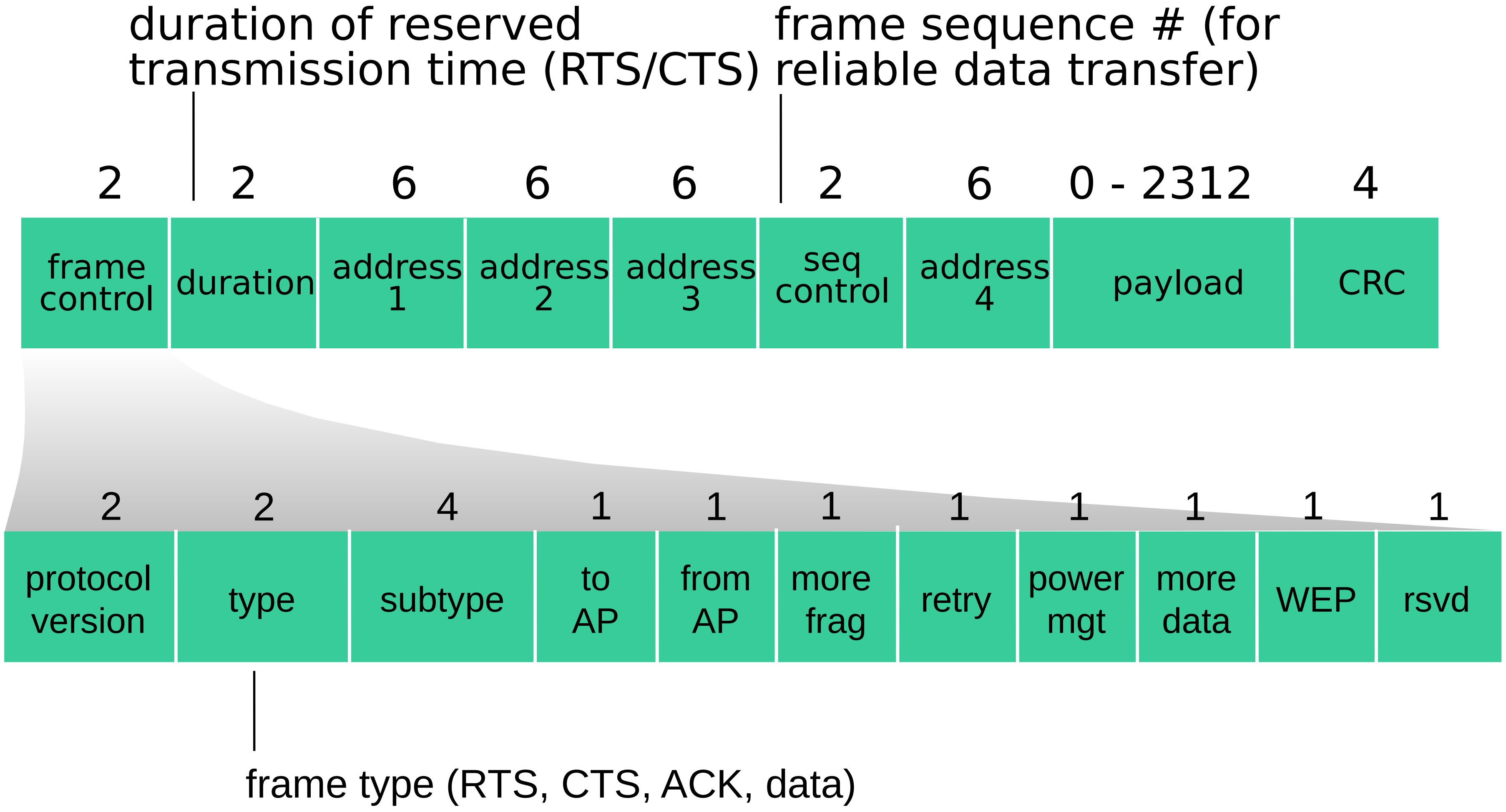
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing

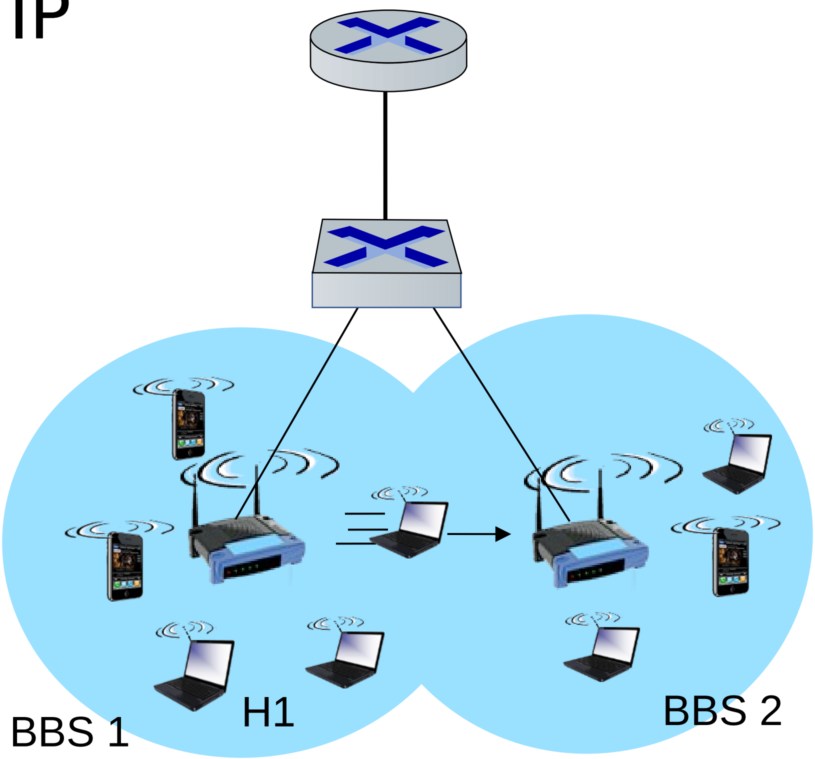


802.11 frame: addressing



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



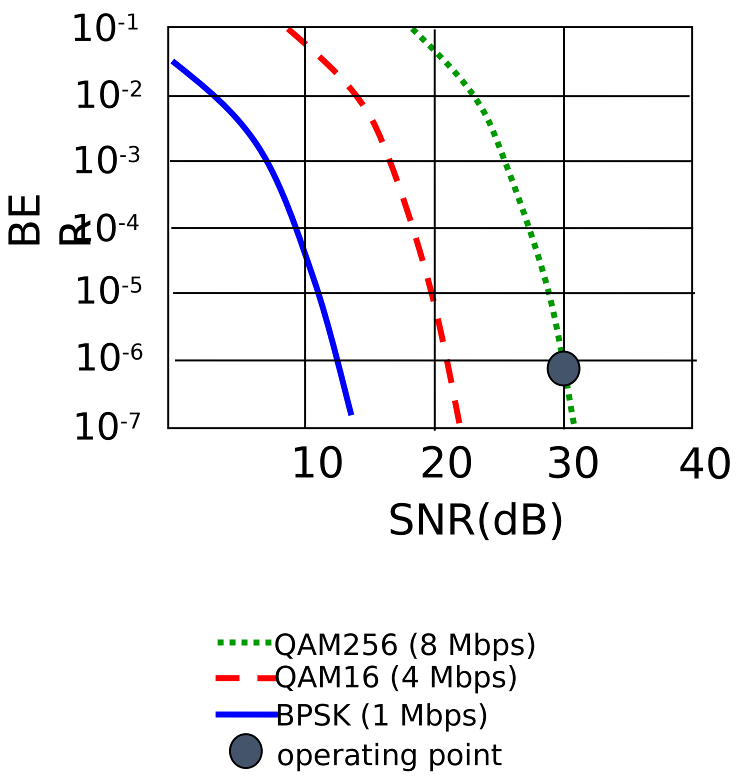
802.11: advanced capabilities

Rate adaptation

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



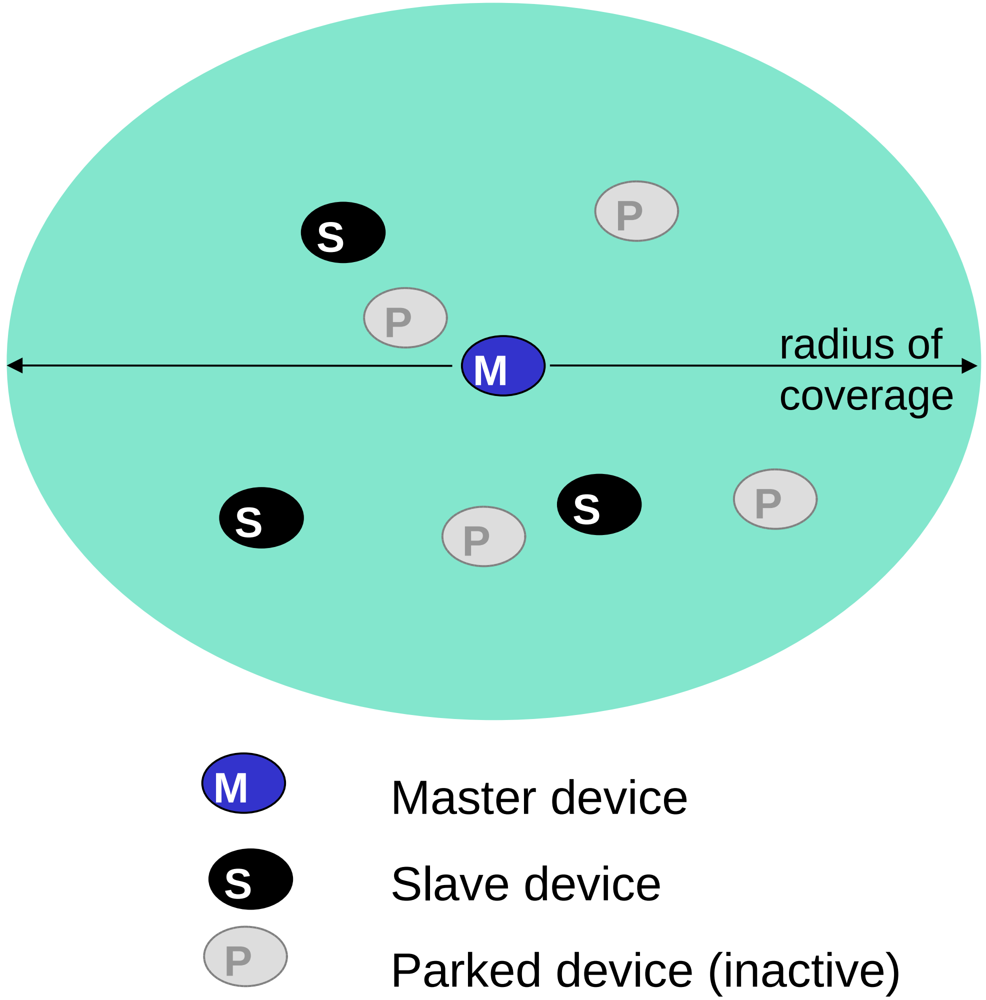
802.11: advanced capabilities

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

802.15: personal area network

- less than 20 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



Bluetooth 802.15.1

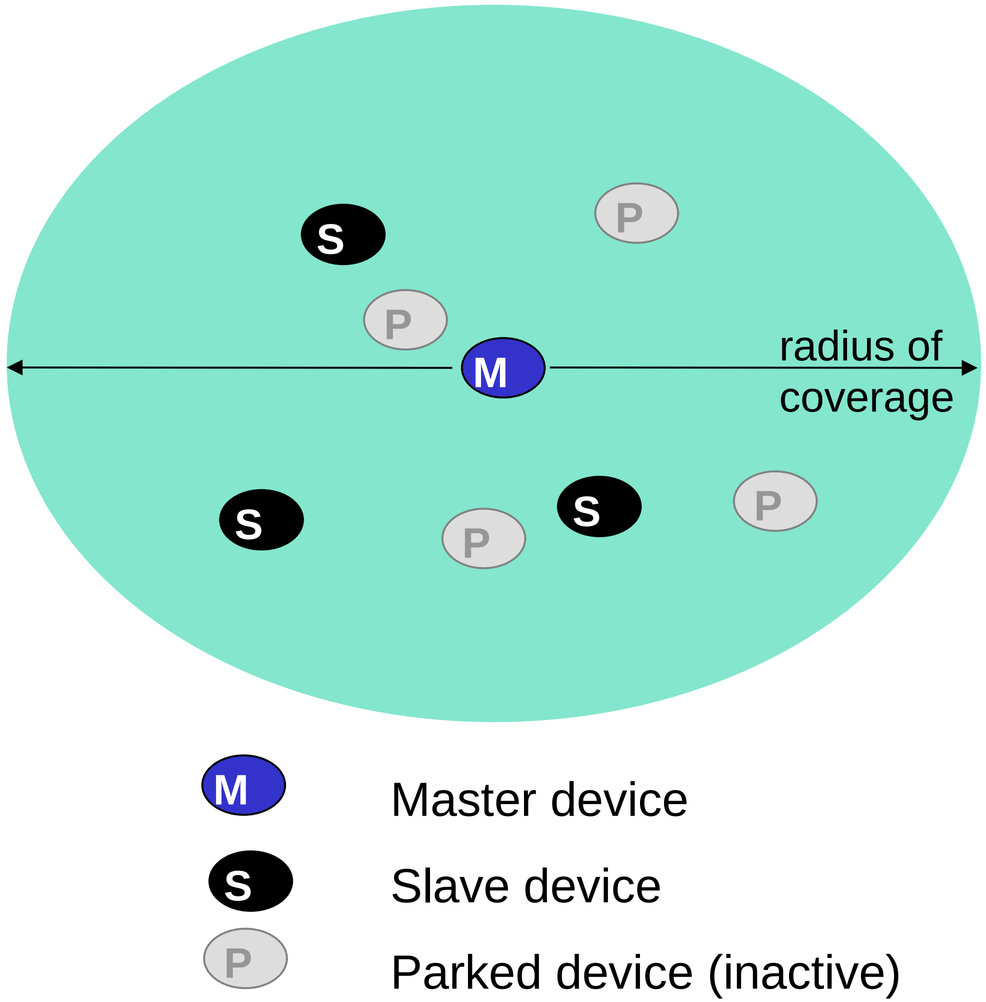
- Its development starts in 1994 by Ericsson company

- Replacement for cables
  - Connecting mouse, keyboard, headphones, …
  - Short range, low-power inexpensive wireless radios

- Ad hoc: no infrastructure

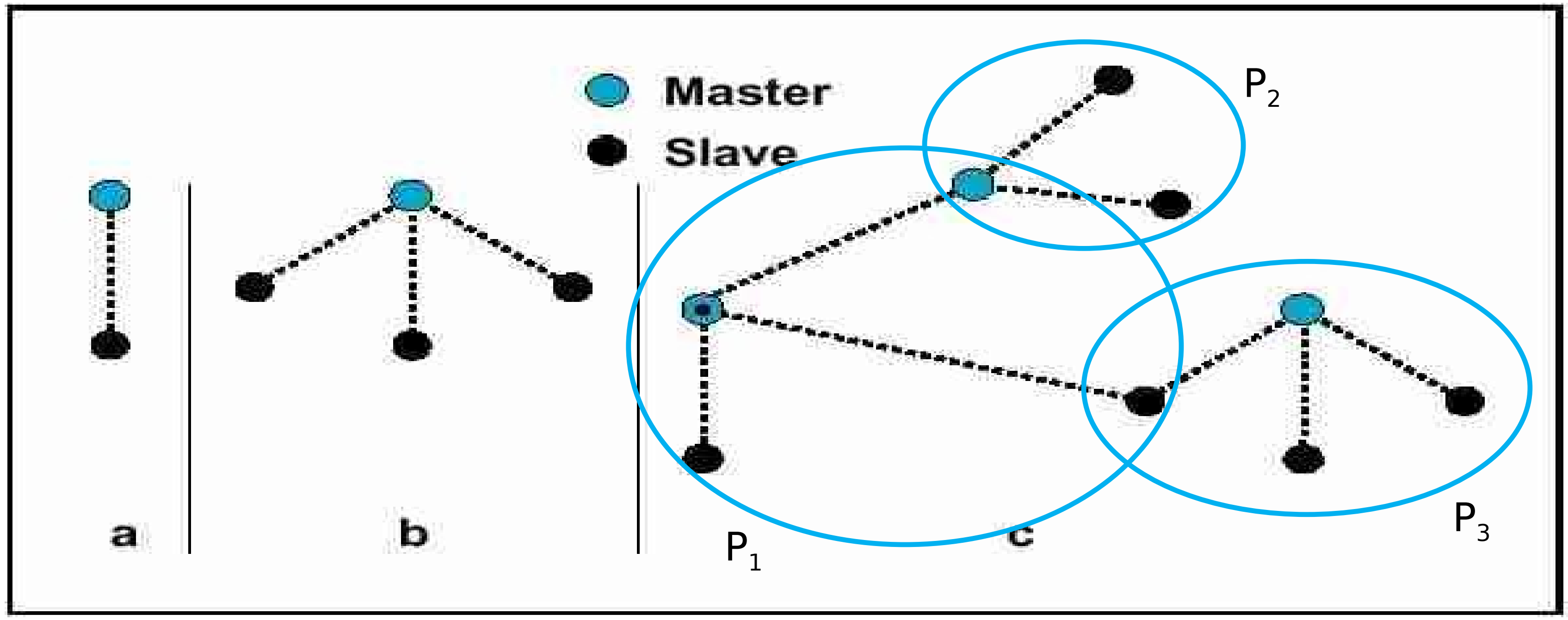
Bluetooth piconet

- Basic topology up to 8 active devices
  - One master
  - Up to 7 slaves
  - Max 200 “parked” devices
- Slave
  - Stay in sync with master
  - request permission to send (to master)
- Master
  - grants requests
  - activates parked devices
- Parked devices
  - Don’t communicate
  - Stay in sync with master



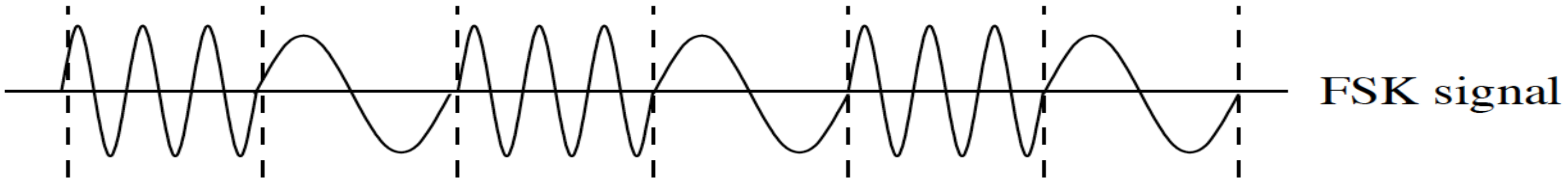
Bluetooth scatternet

- Any device may be at the same time in more piconets
- The result is called scatternet



Bluetooth communication

- Bandwidth 2.4 GHz (same of 802.11)
- Modulation with 2 frequency 2-FSK



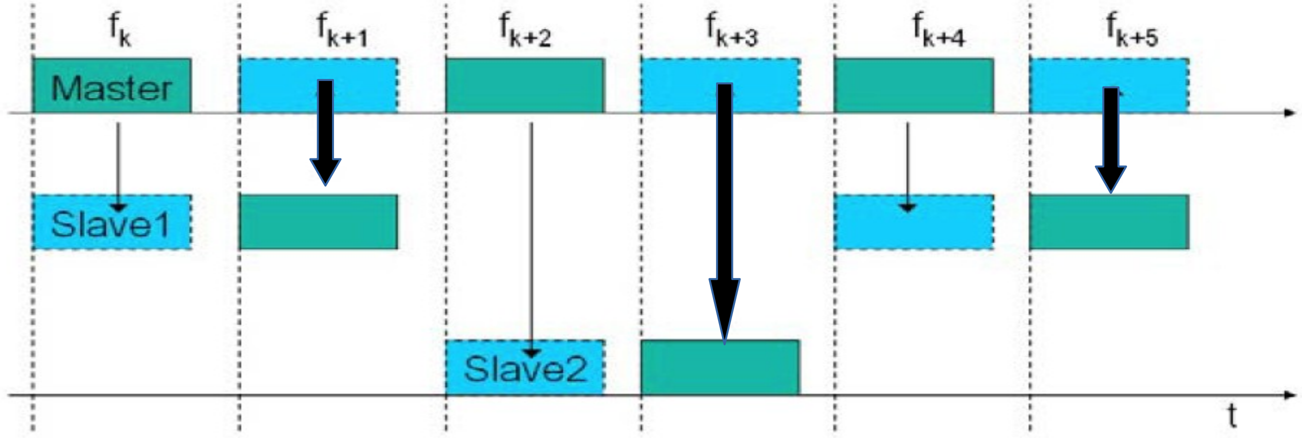
- and *frequency hopping spread spectrum* (FHSS)

Bluetooth FHSS

- Objective:
  - Minimize interferences
- Bandwidth partitioned in 79 channels
- Devices change transmission channel (1600 ch/sec)
  - Same channel for all members of piconet
  - Channels transitions according to pseudo-random schema
    - Seed chosen by master, slaves synch with him

Bluetooth: Medium Access Control

- Time division multiplexing
  - Master defines slot 625 μsec
- Slot partition:
  - Even: master; odd: slaves
- Single slave communication
  - Receiver slave in previous slot can answer in the current one



Bluetooth connection

- Inquiry
  - When two device don’t known each other
  - One send a request…
  - The other answer with its address
- Pairing (connecting)
  - After inquire phase two device can activate a connection state communication
- Connection
  - *Active mode*: active communication
  - *Sniff mode*: sleep and periodically wake-up to listen master
  - *Hold mode*: sleep during a fixed interval decided by master
  - *Park mode*: sleep until master wake-up it. Periodically sync and listen master

Bluetooth evolution

- Bluetooth 1.0 released in 1999
  - Up to 720 Kbit/s
  - FHSS
- Bluetooth 2.0+EDR in 2004
  - Introduces EDR to achieve up to 3 Mbit/s
  - EDR: combination of two modulation techniques GFSK and PSK
- Bluetooth 3.0 in 2009
  - Used in combination with 802.11 for high-throughput data transfer
- Bluetooth 4.0+LE (2009) includes:
  - Bluetooth “classic”
  - Bluetooth Low Energy (Bluetooth LE, BLE, Bluetooth Smart)
    - no backward-compatible with “classic” versions
    - extends battery life-time lowering data rate (0.27 Mbps)

ZigBee (802.15.4)

- Actually the only open standard (low power)
- Frequency 2.4G
- Last version ZigBee RF4CE
- Supported by the ZigBee Alliance:

ZigBee: topology

- Mesh topology
  - Multiple redundant path
  - Scalability
  - Cover wide area (WPAN) with low-power devices

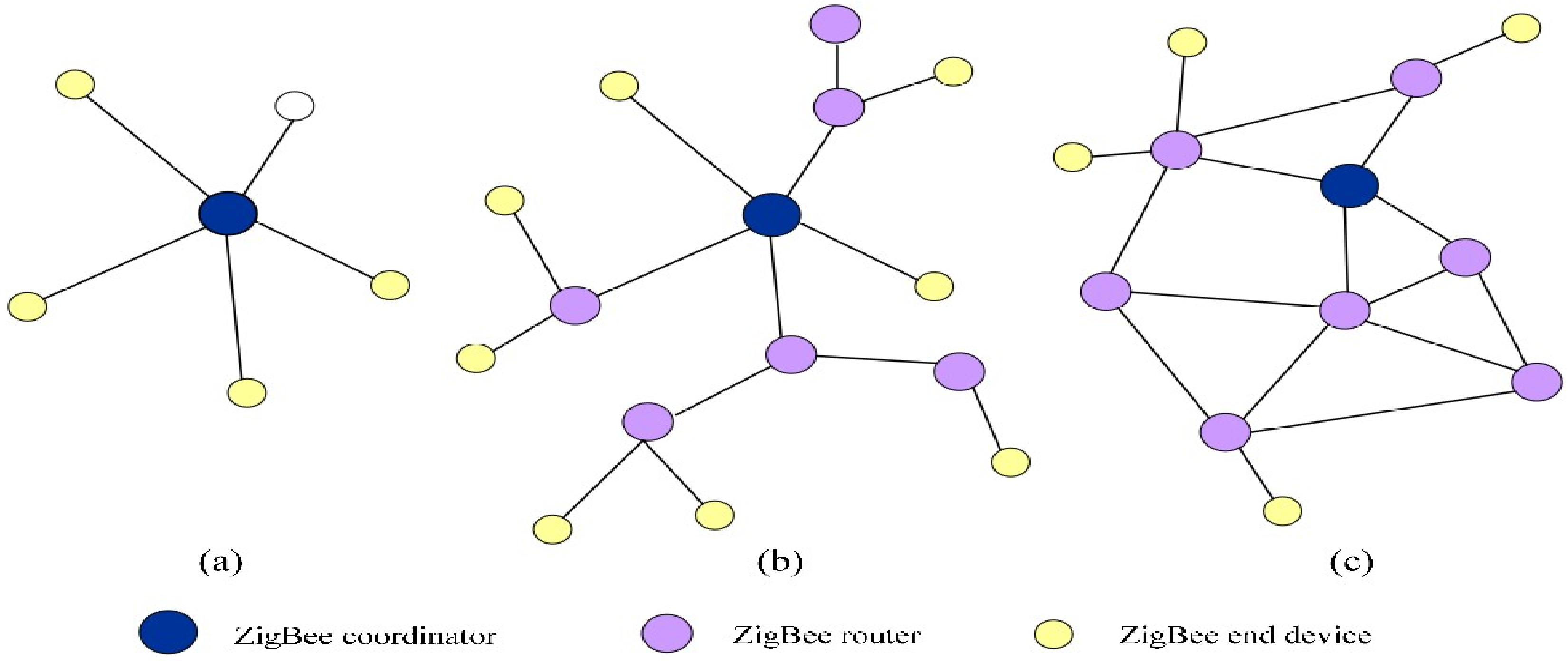


Fig. x. 8. Zigbee network topologies: (a) star, (b) tree, and (c) mesh.

ZigBee: architecture (1)

- Two address types
  - 64 bit: univocally identifies each device folllowing the standard
  - 16 bit: dynamically assigned when a device associates to a WPAN
    - Identify the service (like TCP/IP ports)
- ZigBee stack:
  - Low level defined by 802.15.4
  - Higher defined by ZigBee

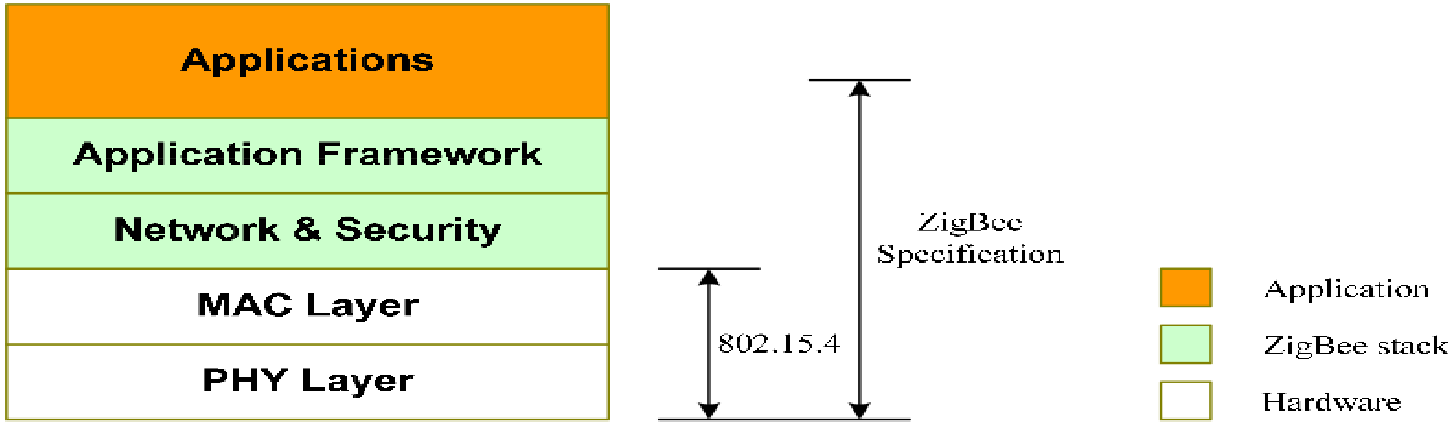


Fig. x.1. The ZigBee/IEEE 802.15.4 protocol stack.

ZigBee: architecture (2)

- Three node types:
  - *PAN Coordinator* – maintain the net, discover devices and configure them
  - *Full funtion devices* (FFDs) – can work as a router
  - *Reduced function devices* (RFDs) – just work as end-point

- PAN Coordinator enquires to discover nodes that can join the net
  - Assign the 16 bit ID and the communication channel

Channels in 2.4GHz

- 27 channels operating at 868 MHz, 915 MHz, 2.4 GHz
  - Channel 0 – BPSK at 20 Kbps
  - Channels 1 – BPSK at 40 Kbps
  - Channels 2 – OQPSK at 250 Kbps

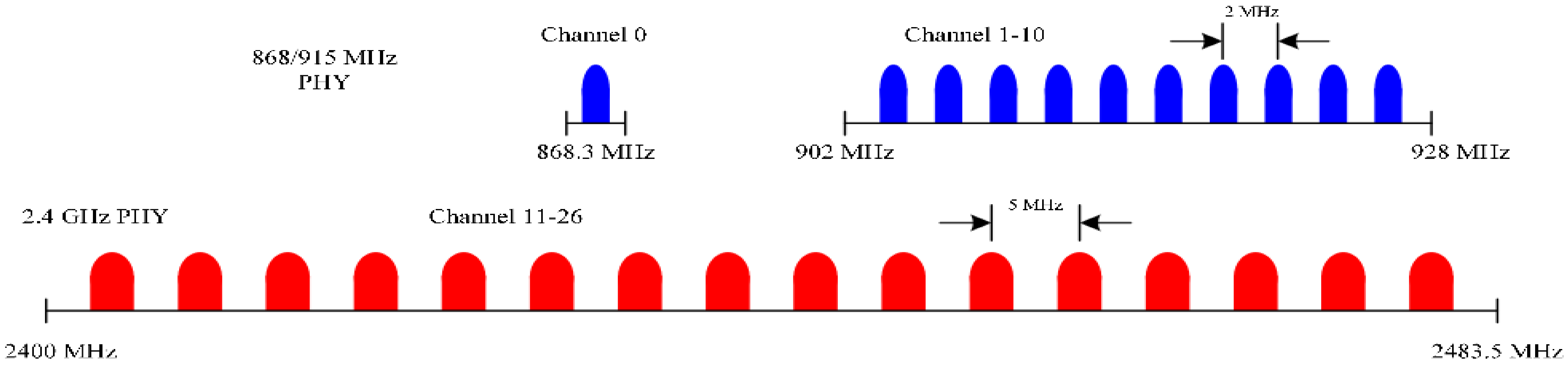


Fig. x.2. Arrangement of channels in IEEE 802.15.4.

Physical and communication layer

Property Description	Prescribed Values	
	915 MHz	2.4 GHz
Raw data bit rate	40 kbps	250 kbps
Transmitter output power	1 mW = 0 dBm	
Receiver sensitivity (<1% packet error rate)	-92 dBm	-85 dBm
Transmission range	Indoors: up to 30 m; Outdoors: up to 100 m	
Latency	15 ms	
Channels	10 channels	16 channels
Channel numbering	1 to 10	11 to 26
Channel access	CSMA-CA and slotted CSMA-CA	
Modulation scheme	BPSK	O-QPSK

Medium access control

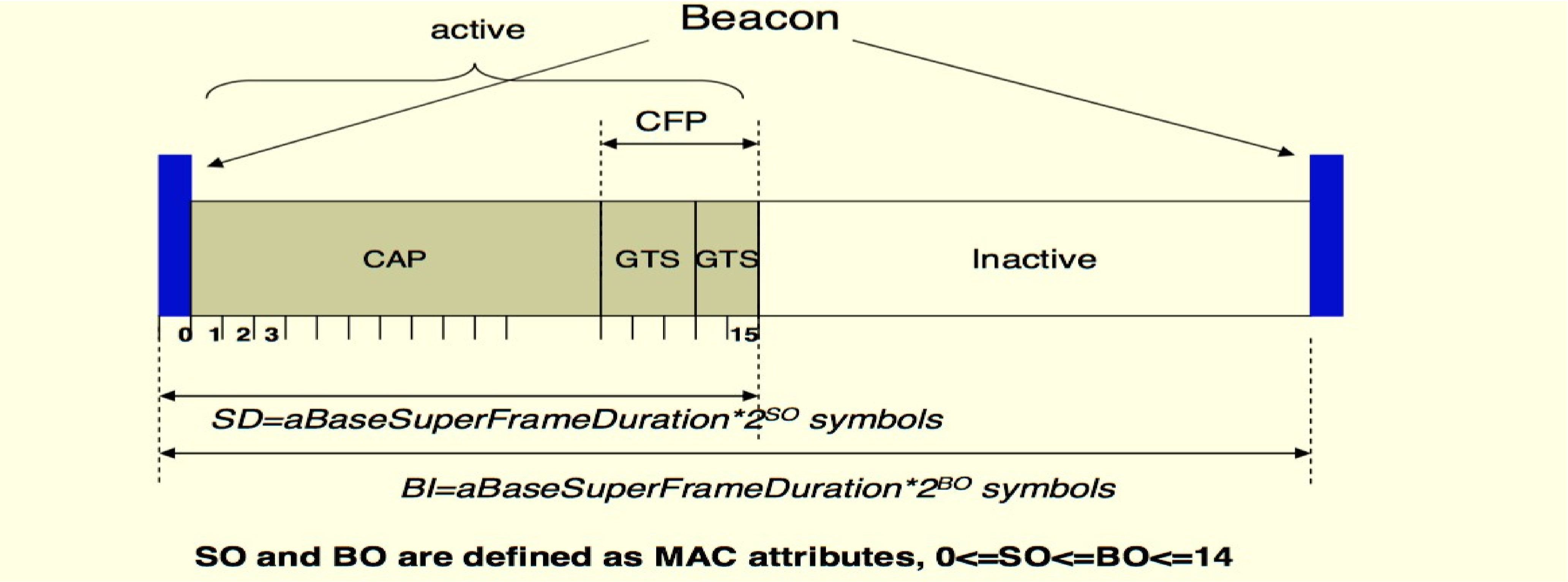
- MAC layer
  - Manages superframes, control channel access
  - Validate frames, sends acks

- Slotted CSMA/CA:
  - Directed by PAN coordinator using super-frame

- CSMA/CA
  - Nodes communicate directly (as in ad-Hoc WI-FI)

Superframe: Slotted CSMA/CA

- During Contention Period access by slotted CSMA/CA
- In Contention Free Period slots are reserved



Frames

- Frames of 4 types
  - Beacon Frame – used by coordinator to send beacons
  - Data Frame – used for data transfer
  - Ack Frame
  - MAC command Frame – used to manage MAC interfaces

Z-Wave

- Proprietary protocol
  - Based on a mesh network topology
    - each (non-battery) device becomes a signal repeater
- Devices can communicate point-to-point for up to 35 meters on their own
- Z-Wave networks can be linked together
- Each network can support up to 232 devices
- In Europe, it works on the 868,42 MHz

Command classes

- Z-Wave device messages are called “commands”
  - even if they are just info reports
- Commands are organized into command classes
  - i.e., groups of related functionality
- Some devices list which command classes they support in their manuals
- • They enable interoperability
  - if one device controls a command class and another device support the same command class then these devices are able to communicate

Listening and sleepy devices

- Devices that are plugged into power are called listening devices
  - they keep their receiver on all the time
- Listening devices act as repeaters and therefore extend the Z-Wave mesh network
- Battery powered devices (such as sensors) are sleepy
  - they turn off their receivers to save energy, so you can't send them commands at any time
  - however, they wake up at a regular interval and send a notification to alert other devices that they will be listening for incoming commands for the next few seconds