Chapter 7 Wireless and Mobile Networks

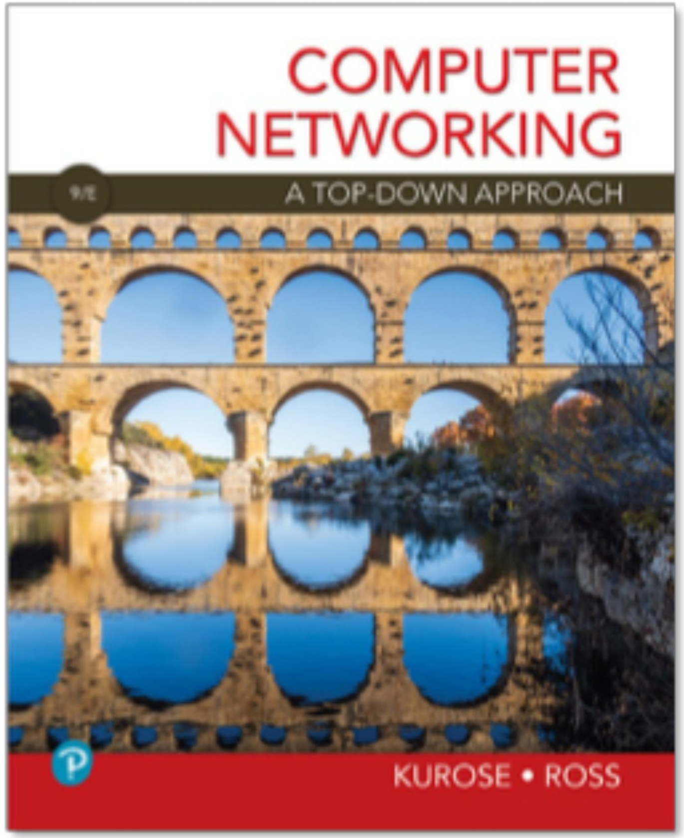
A note on the use of these PowerPoint slides:

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
9th edition
Jim Kurose, Keith Ross
Pearson, 2025

Wireless and mobile networks: overview

Chapter goals:

- understand principles of wireless networks:
  - physical layer: radio, influence on higher layers
  - access network: link-layer challenges/solutions in any wireless networks
  - core network: the "network" layer in a wireless network
  - user/device mobility: among access networks
  - application-specific wireless networks: Bluetooth, satellite, IoT
- wireless networks in practice:
  - WiFi
  - 5G (with a bit of 4G)
  - Bluetooth, satellite, IoT

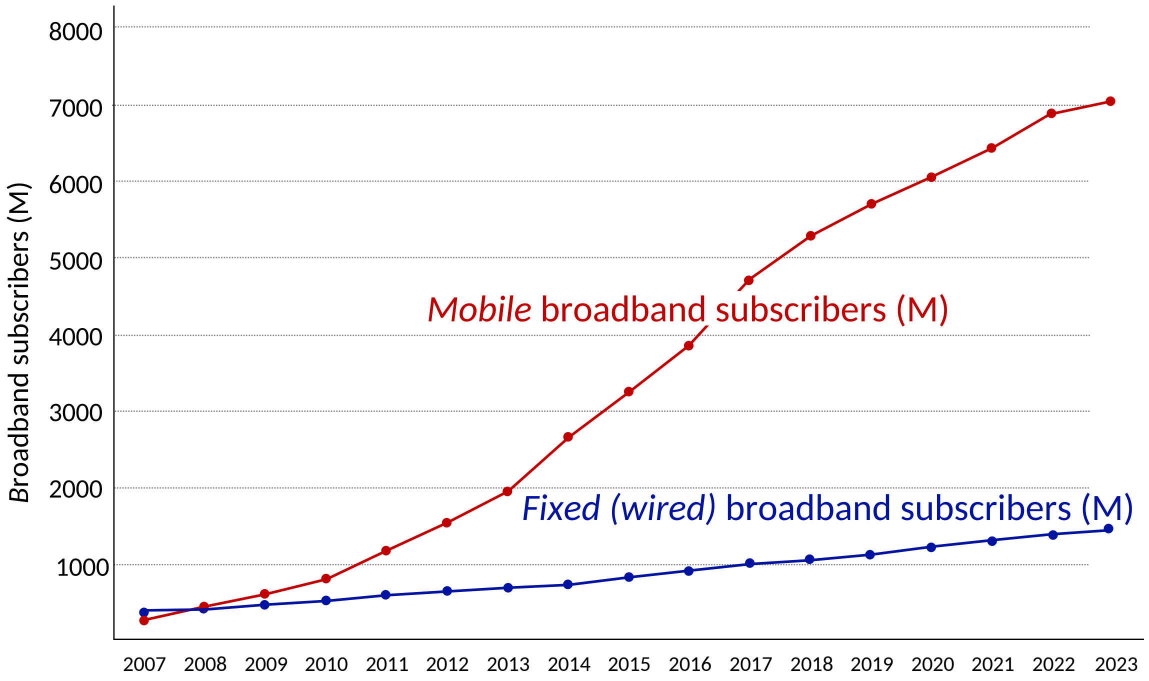
For a more extensive treatment of wireless and mobile networks visit: https://gaia.cs.umass.edu/wireless_and_mobile_networks

Chapter 7 outline

- introduction
- radio: the physical layer
- the wireless *access* network
  - principles, WiFi, 5G
- the wireless core network
  - principles, 5G
- mobility
- Bluetooth, satellite, IoT wireless networks

Wireless and Mobile Networks: context

- more mobile-broadband-connected (cellular) devices than fixed-broadband-connected devices devices (5-1 in 2019)!
  - wireless connectivity even great when WiFi users considered (80% of broadband homes use WiFi)
  - 60% of Internet traffic from major web sites destinated to mobile device



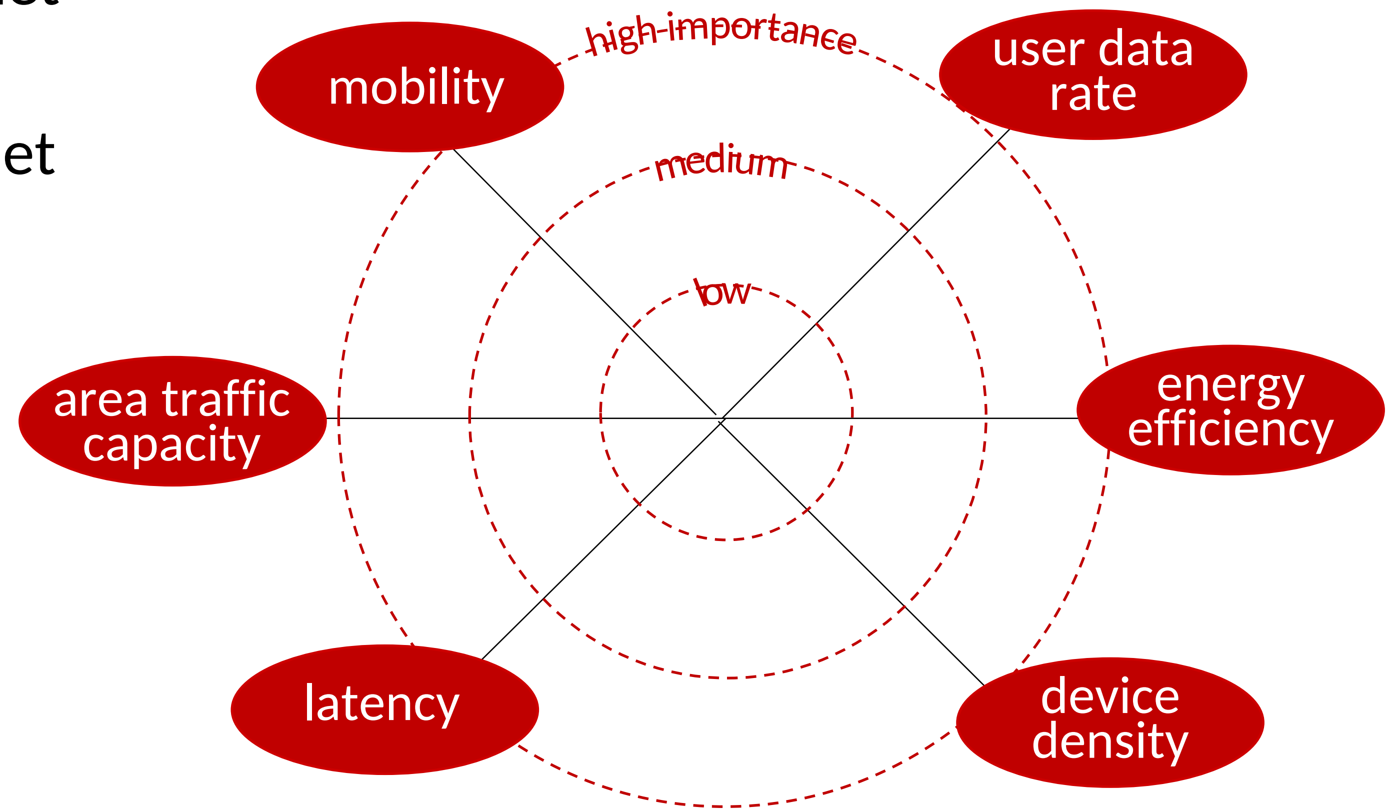
Data source: www.statista.com (1/25)

Wireless applications their needs

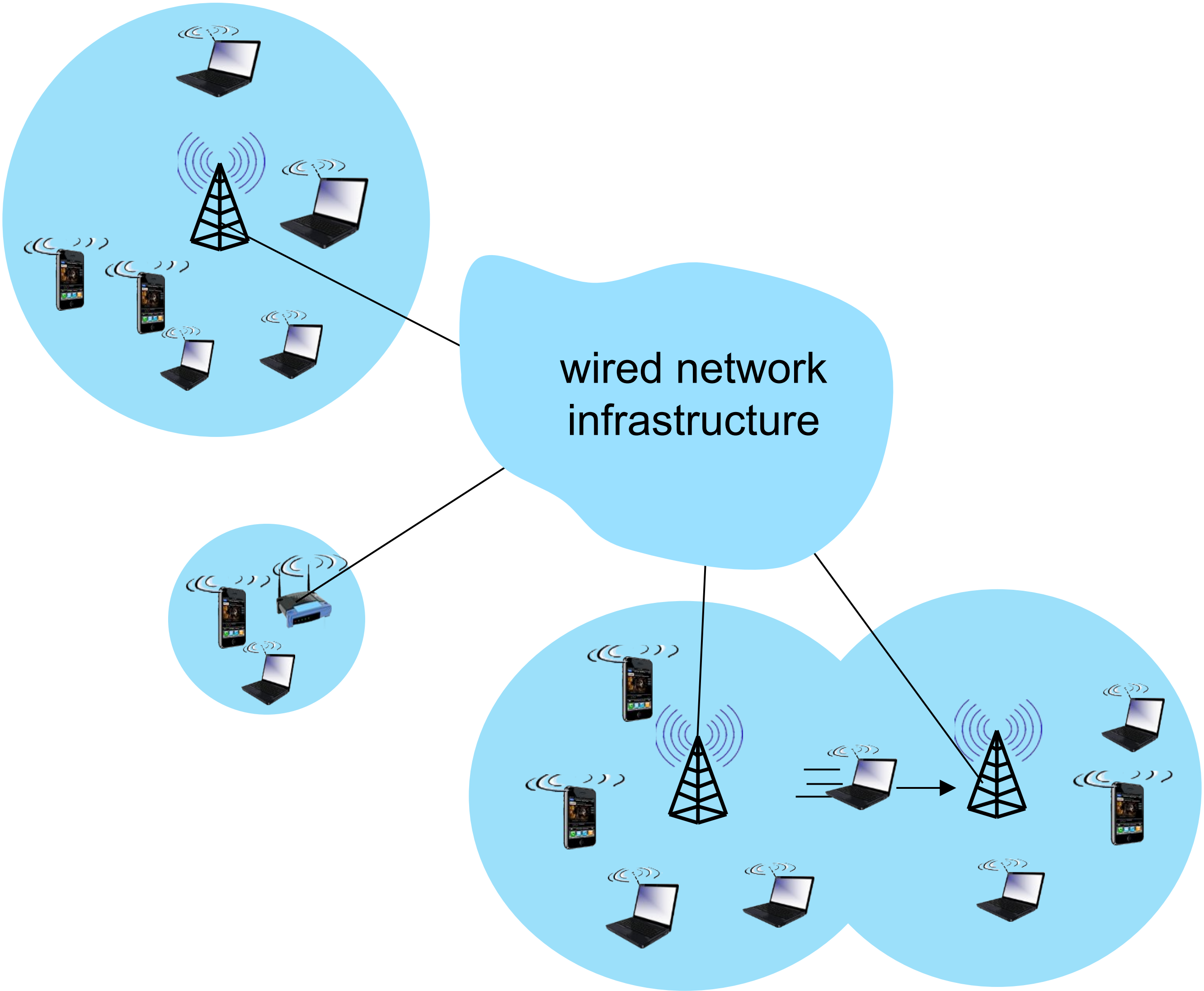
Six application areas :

- Wide-area Mobile Wireless Internet Access
- Local-area Mobile Wireless Internet Access
- Fixed Wireless Internet Access
- Satellite Networks for Internet Access and Sensing
- Cable replacement
- Internet of Things (IoT)

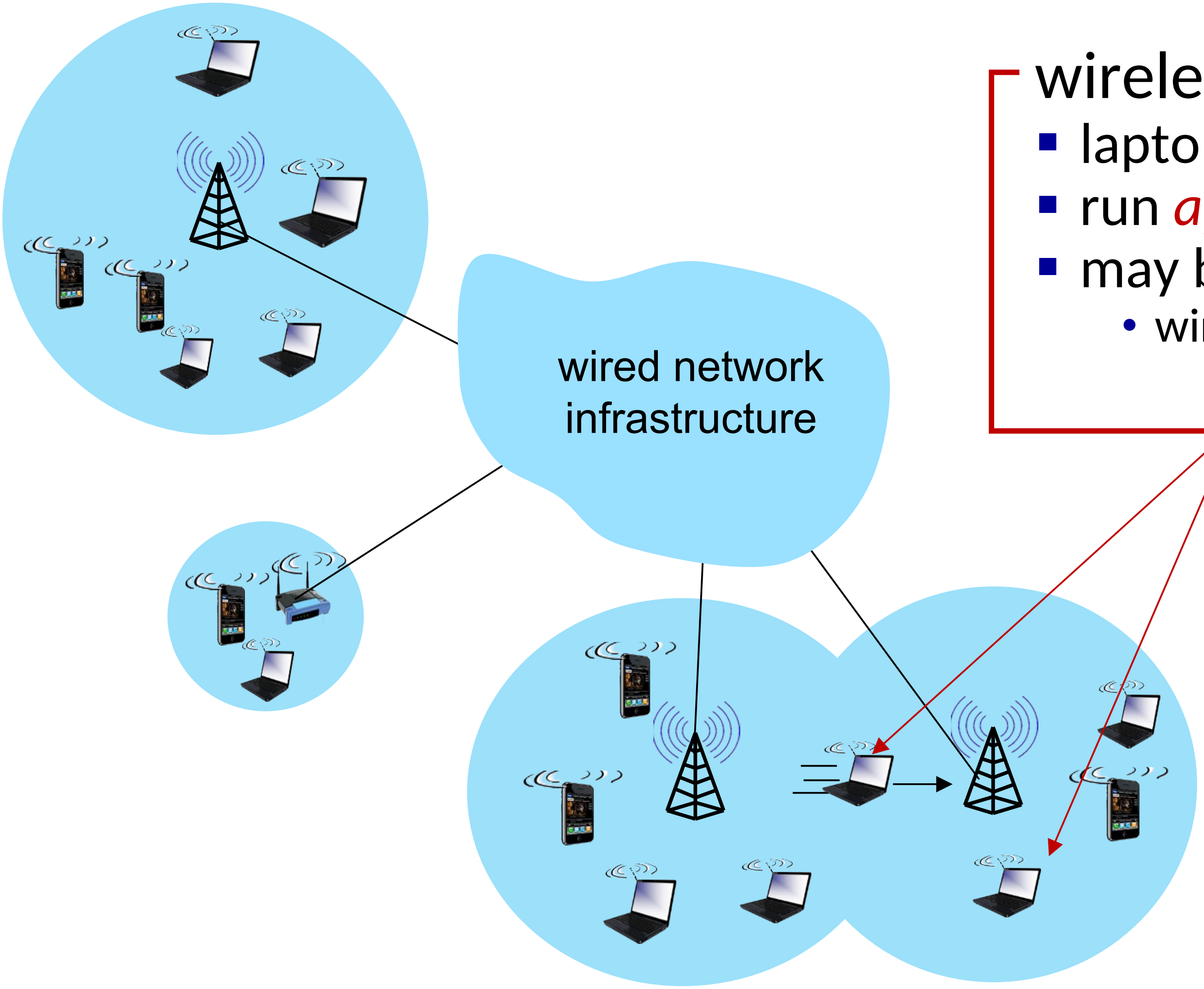
Application needs:



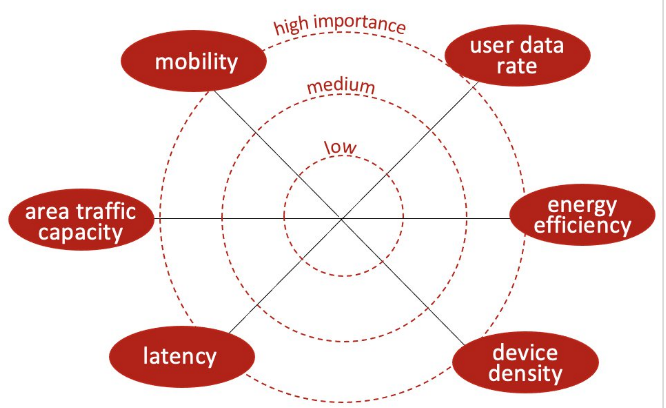
Elements of a wireless network



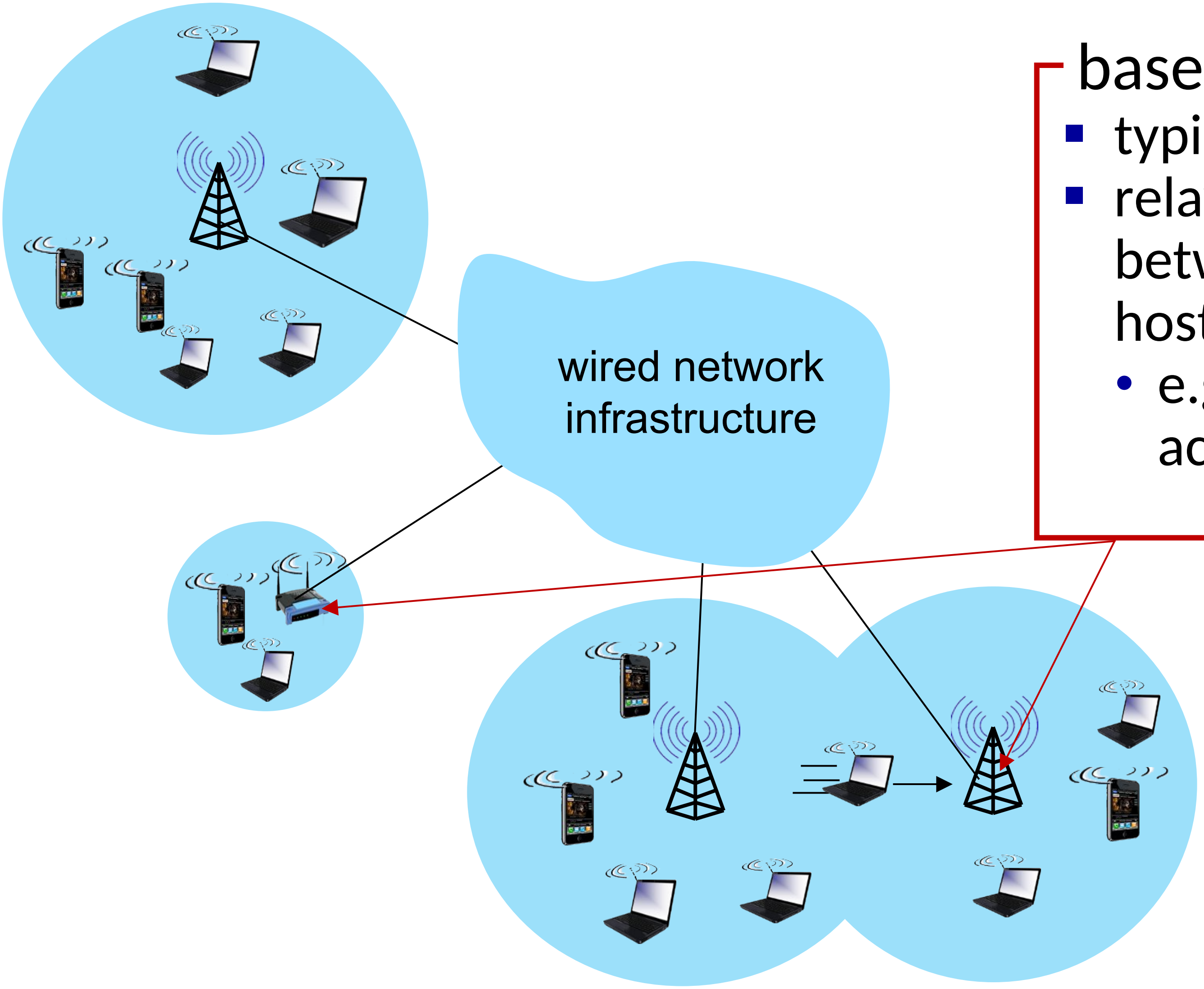
Elements of a wireless network



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



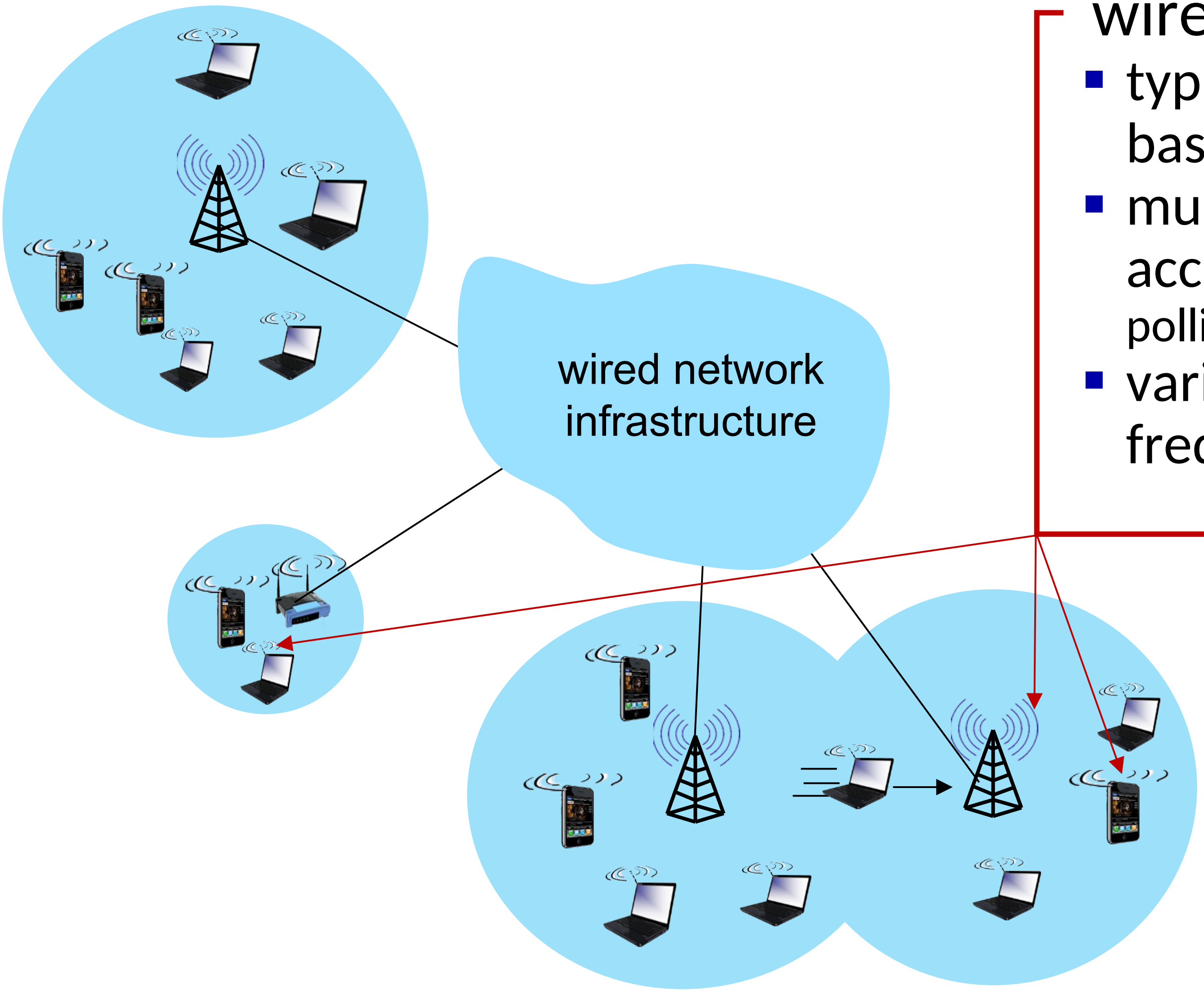
Elements of a wireless network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., 4G/5G cell towers, 802.11 (WiFi) access points (APs)

Elements of a wireless network

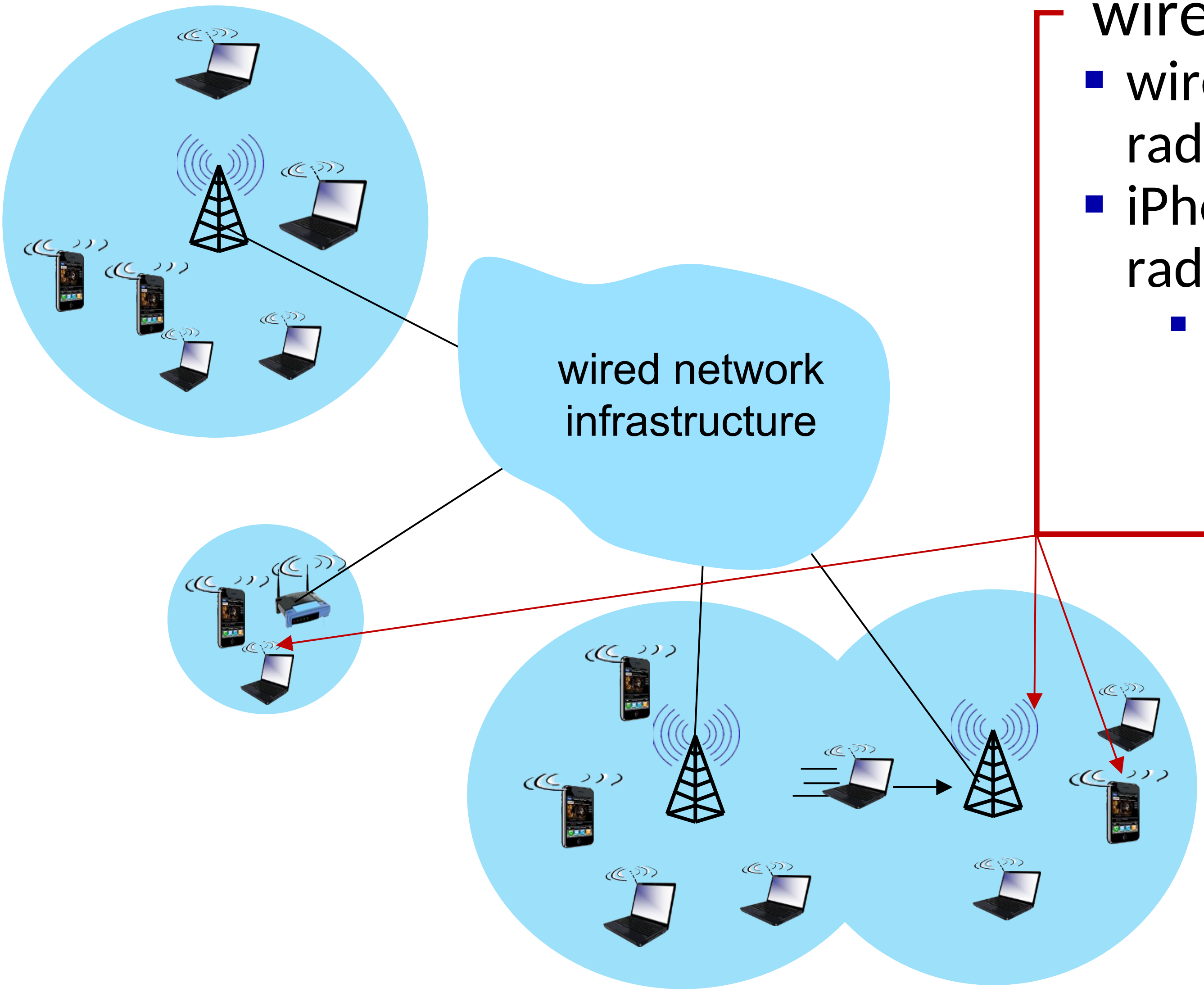


wireless link

- typically used to connect device(s) to base station, also used as backbone link
- multiple access protocol coordinates link access (random access, FDMA, TDMA, CDMA, polling)
- various transmission rates and distances, frequency bands

Ad hoc networks: not all wireless networks are connected into a larger network

Elements of a wireless network

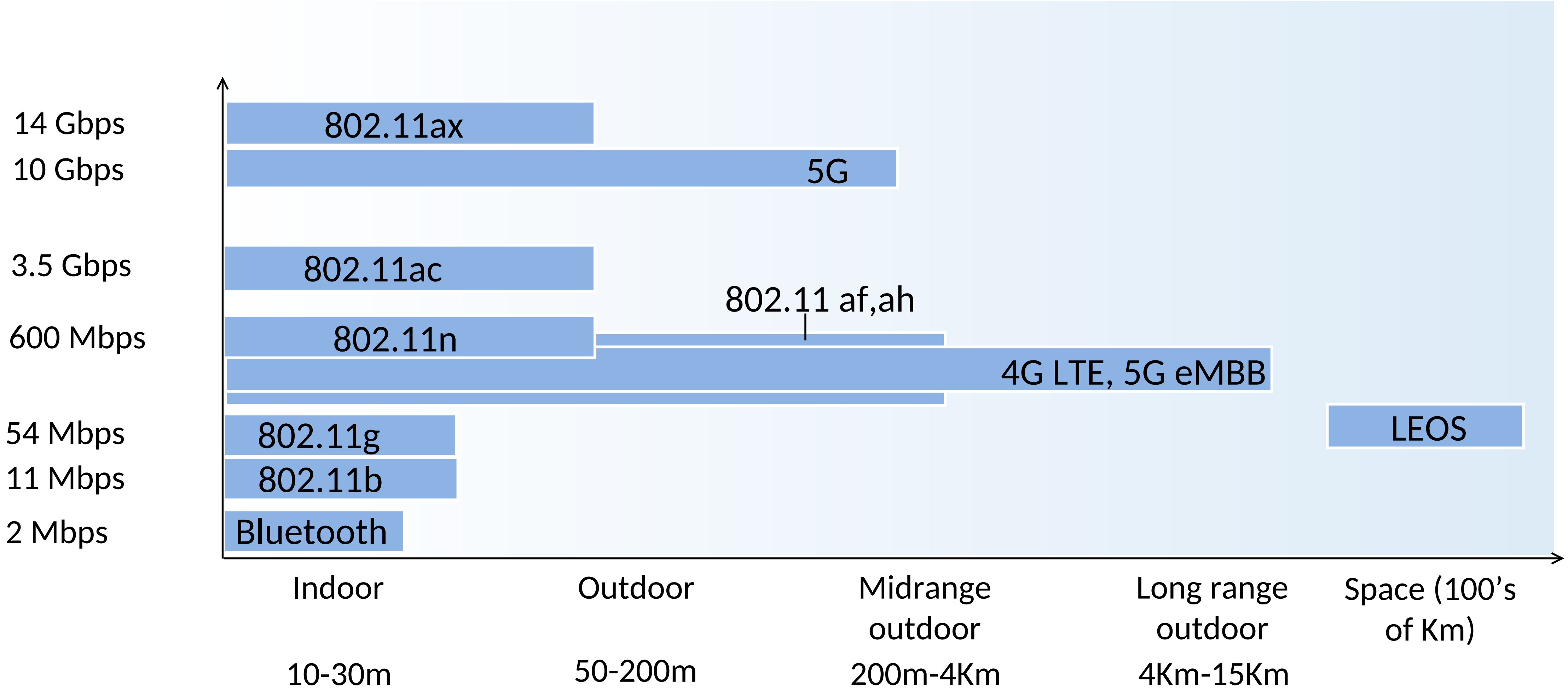


wireless device radio

- wireless device has different radios for different networks
- iPhone16: has ~11 different radios, many antennae
  - 5 different cellular radios, WiFi, Bluetooth, UWB, satellite NFC, GPS

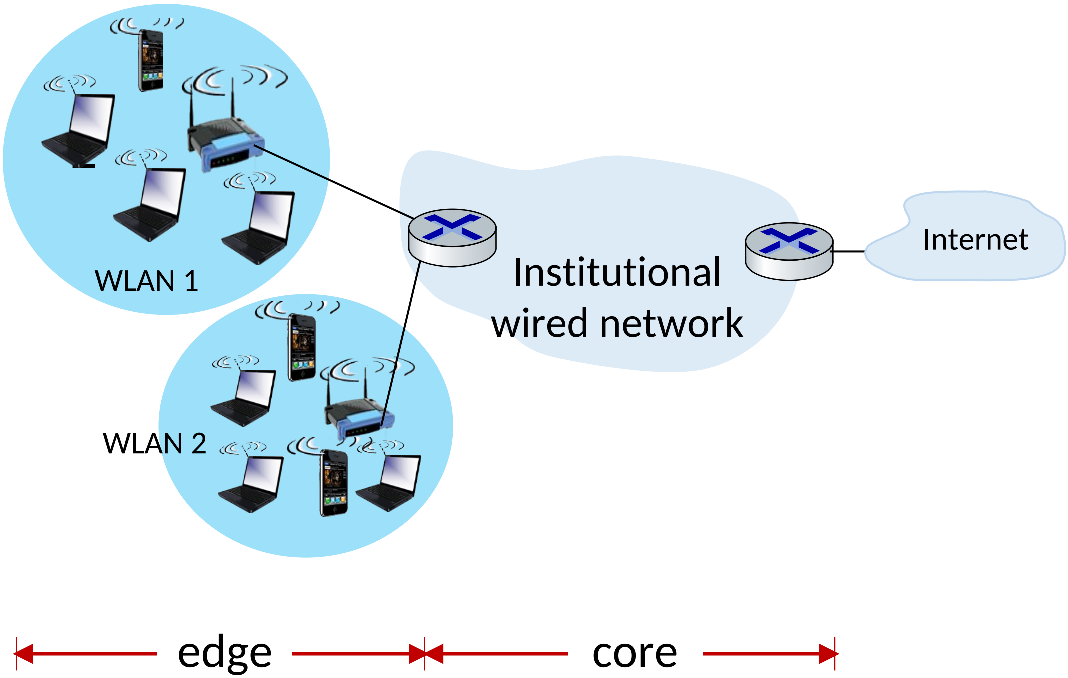
Ad hoc networks: not all wireless networks are connected into a larger network

Characteristics of selected wireless links

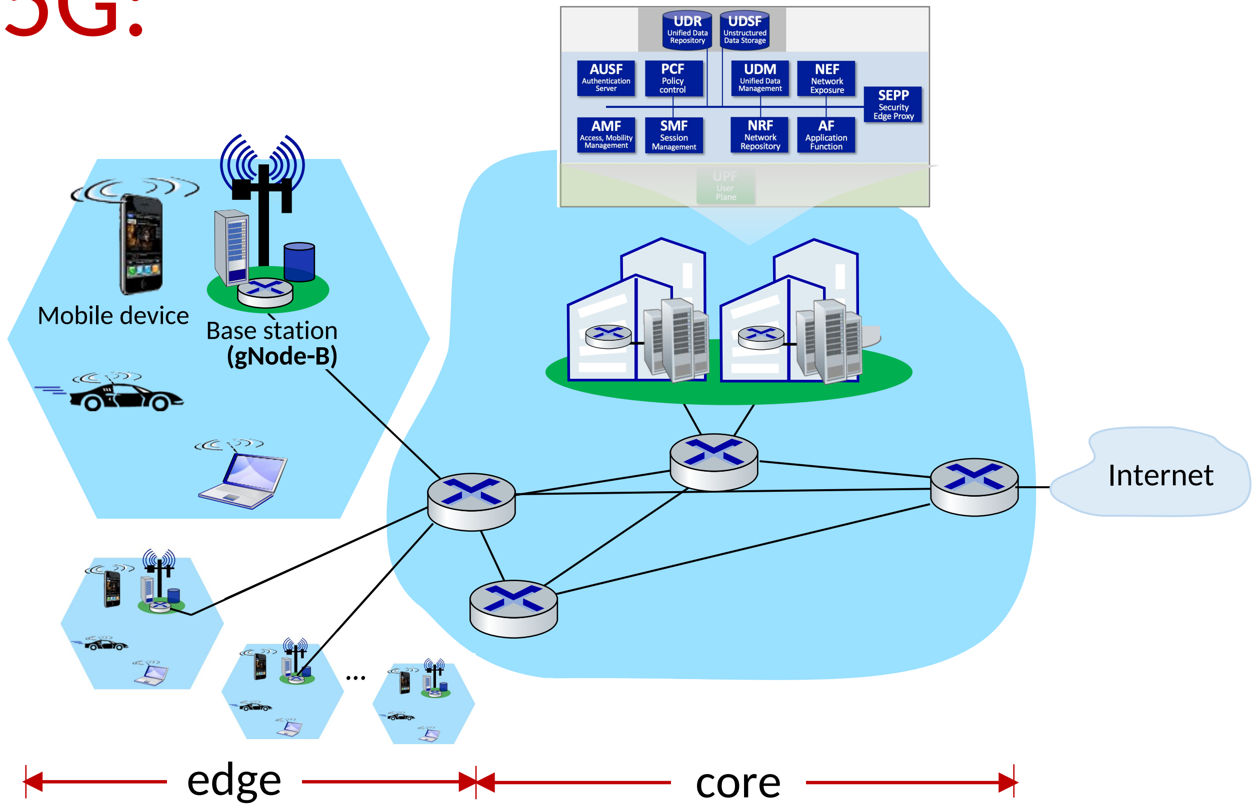


Wireless networks: edge and core networks

WiFi:



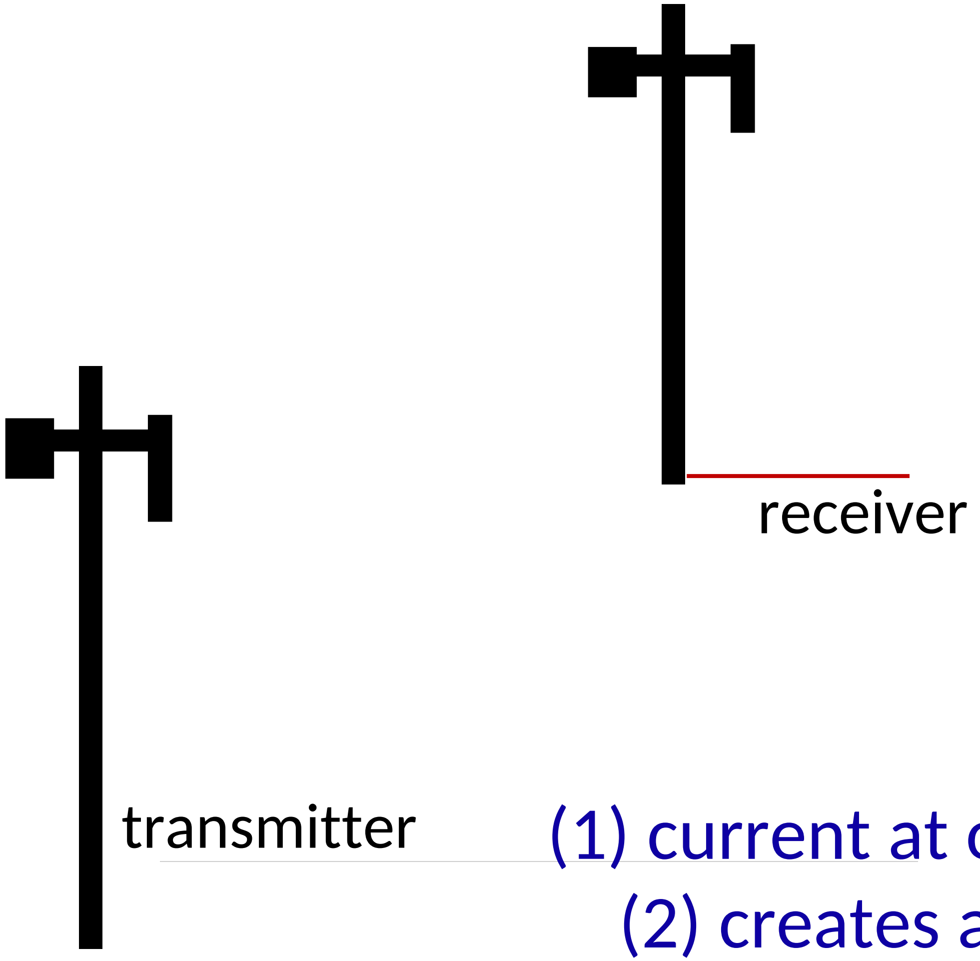
5G:



Chapter 7 outline

- introduction
- radio: the physical layer
  - radio principles
  - radio channels
  - antennas: MIMO
  - radio spectrum
  - coding and modulation
- the wireless *access* network
- the wireless core network
- mobility
- Bluetooth, satellite, IoT wireless

Electromagnetics: enabling communication

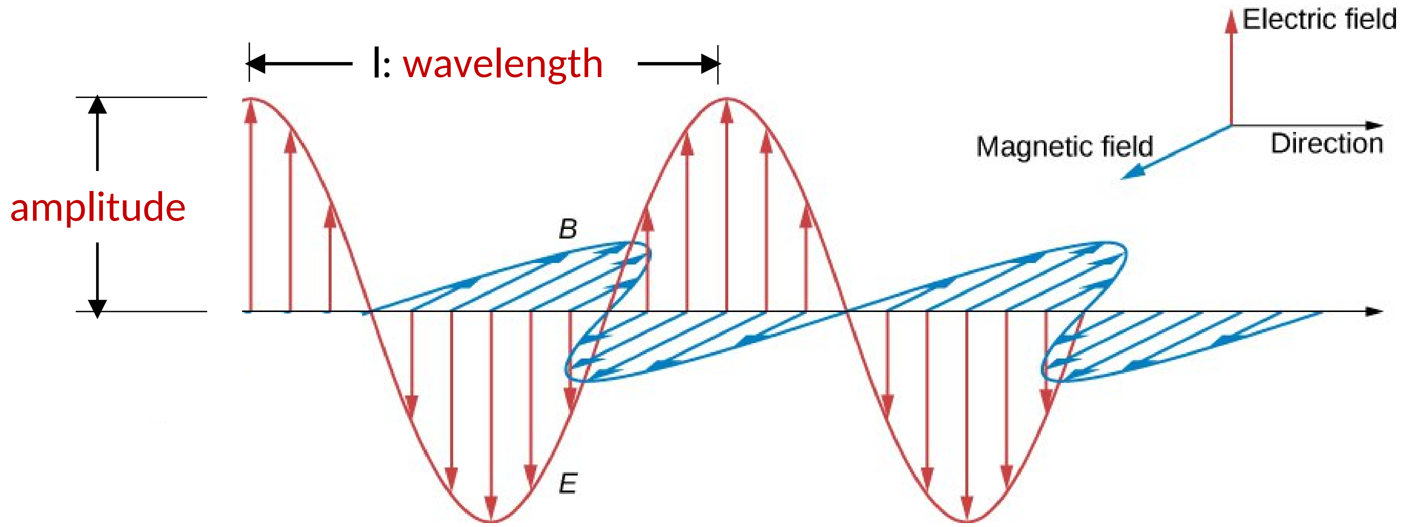


(1) current at one location (transmitter) ….

(2) creates an EM field in space ….

(3) induces a current at remote location (receiver)….

Radio basics: electromagnetic waves



wave propagation:

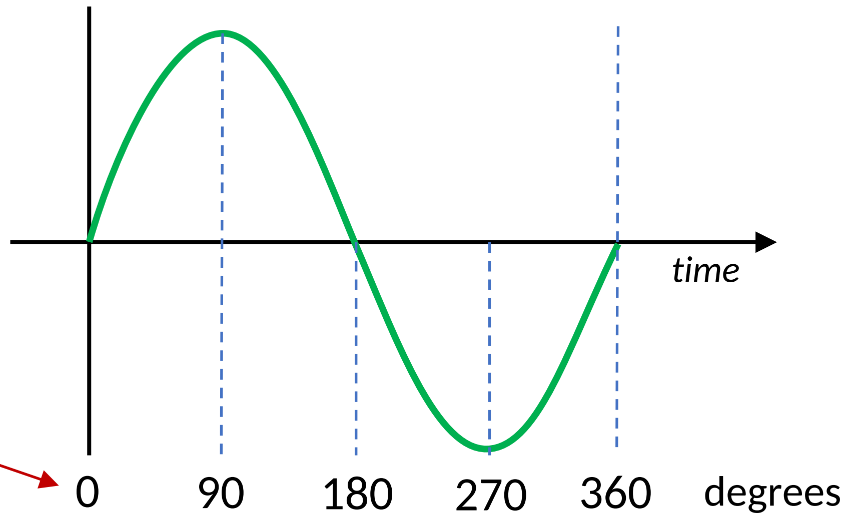
Electromagnetic wave has:

- wavelength (l)
- frequency: speed of light / wavelength = c/l
- directionality (of propagation)
- time-varying amplitude

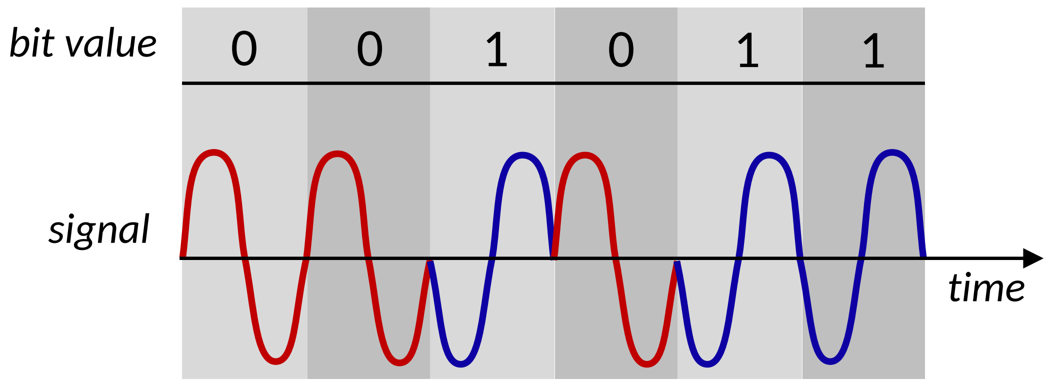
Radio basics: phase

The phase of a periodic signal, represents the fraction of the period covered up until time t

- often measured in angular units (0 to 360)



we can code information into signal by changing signal's phase (keeping frequency the same!)



Radio signal characteristics

Power: antenna receive/transmit energy per unit time

- linear: measured in watts (or milliwatts)
- logarithmic: measured in decibels (db)

$$P_{dBm} = 10 \cdot \log_{10}\left(\frac{P_{mW}}{1mW}\right)$$

- example:

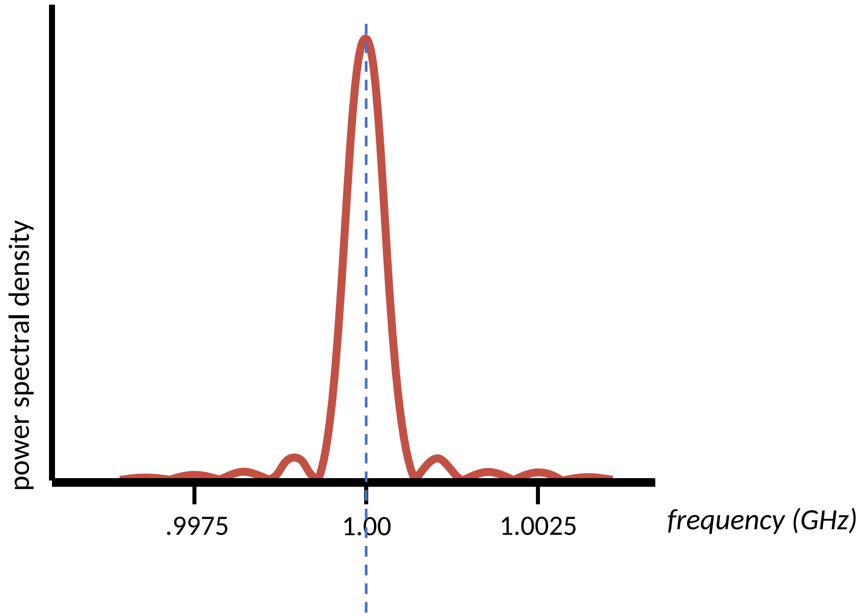
P_{mW} = 250 mW (typical max mobile transmit power)

$$P_{dBm} = 10 \cdot \log_{10}\left(\frac{250mW}{1mW}\right)$$

$= 24$ dBm

Power spectral density:

- power present in signal as a function of frequency



carrier (center) frequency

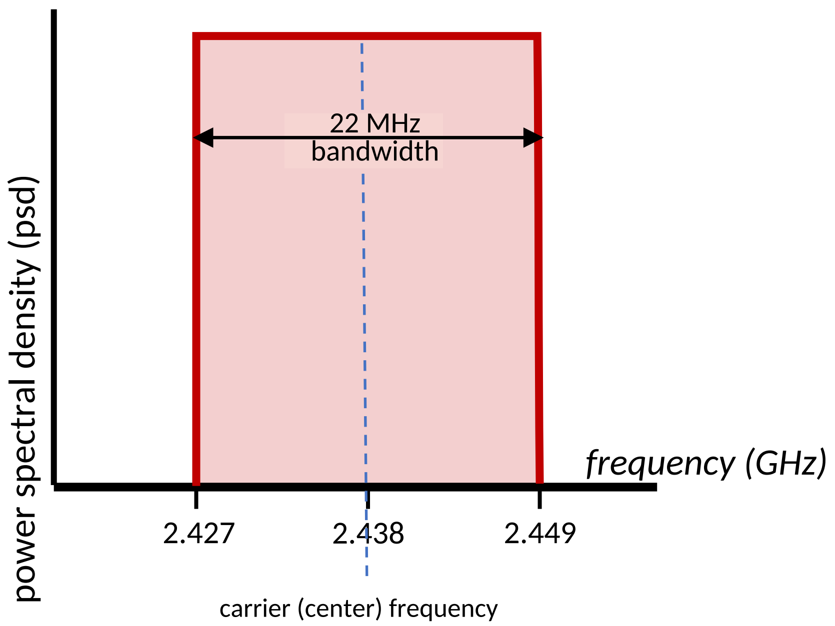
Radio signal characteristics

Bandwidth: width (measured in Hz) of range of frequencies use by radio signal

- radio frequency usage characterized by power spectral density (psd of zero means no signal power at that frequency)
- bandwidth = “band” + “width” (width of frequency band used)

two meanings/usage of “bandwidth”

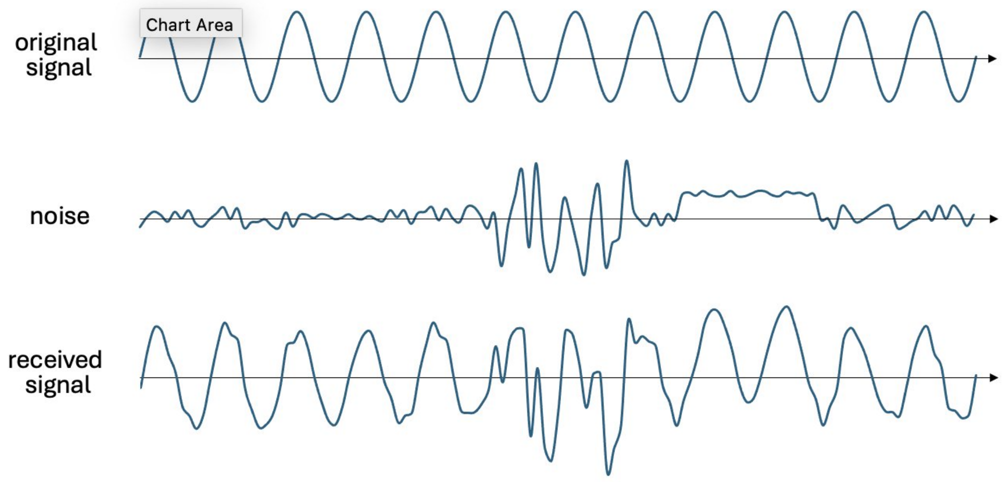
Radio signal “bandwidth” different from link “bandwidth” (maximum transmission rate) term used by network engineers!



Radio signal with 22 MHz bandwidth, evenly spread between 2.427, 2.429 GHz. This 22 MHz bandwidth channel corresponds to channel 6 in WiFi network)

Signals and Noise

- interference: other transmitters/EM radiaters in same frequency band
  - hundreds of consumer devices operate in unlicensed 2.4 GHz band (aka: Industrial, Scientific, and Medical band): WiFi, Bluetooth, Zigbee, satellite TV, microwave ovens, garage-door openers, baby monitors, cordless phones, wireless mics/speakers, radio-controlled drones and toys, amateur radio, …
- thermal and electronic noise in receiver:
  - natural thermal variations, imperfections in electronics



Original signal, noise, and noisy received signal

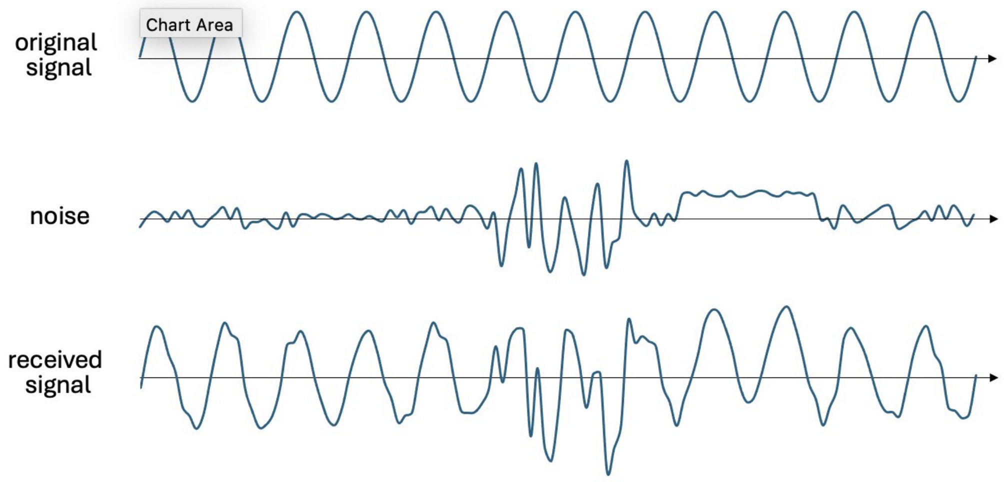
Signal to Noise Ratio (SNR)

SNR: ratio of signal power to noise power (often measured in dB)

- fundamental measure of channel "quality"

  $$\text{SNR (dB)} = 10 \cdot \log_{10}\left(\frac{\text{received signal power}}{\text{noise power}}\right)$$

- SNR of 0 implies equal signal and noise
- high (or low) SNR: easy (or hard) to extract signal from signal+noise
- Typical ranges for current radios:
  - lower limit for cellular: -10 to -6 dB
  - lower limit for WiFi: 20dB



Original signal, noise, and noisy received signal

Channel Capacity

Shannon capacity (of a communication channel): maximum rate at which data can be transmitted, given bandwidth, SNR constraints

$$C = B \cdot \log_2\left(1 + \frac{\text{received signal power}}{\text{noise power}}\right)$$

where:

- C is capacity (bits/sec)
- B is bandwidth (in Hz)
- power measured linearly (e.g., in mW)

Observations:

- C scales linearly with B (for constant SNR)
- high SNR: C scales logarithmically: *little value in increasing SNR beyond a certain point*
- Shannon: classic 1948 paper

Wireless link characteristics: path loss

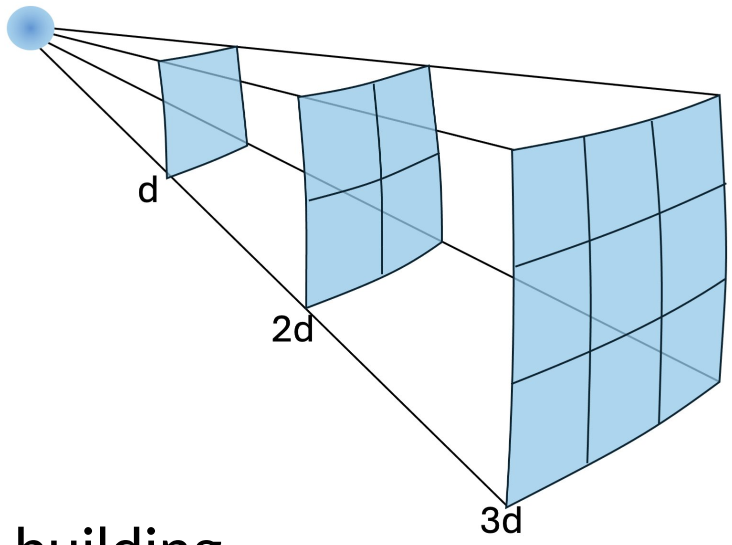
Wireless radio signal attenuates (loses power) as it propagates

path loss

(aka *fading*) reduction in power density (attenuation) of an electromagnetic wave as it propagates from transmitter to receiver

$$\frac{P_{received}}{P_{transmitted}} \sim \frac{1}{(fd)^2}$$

f: frequency
d: distance

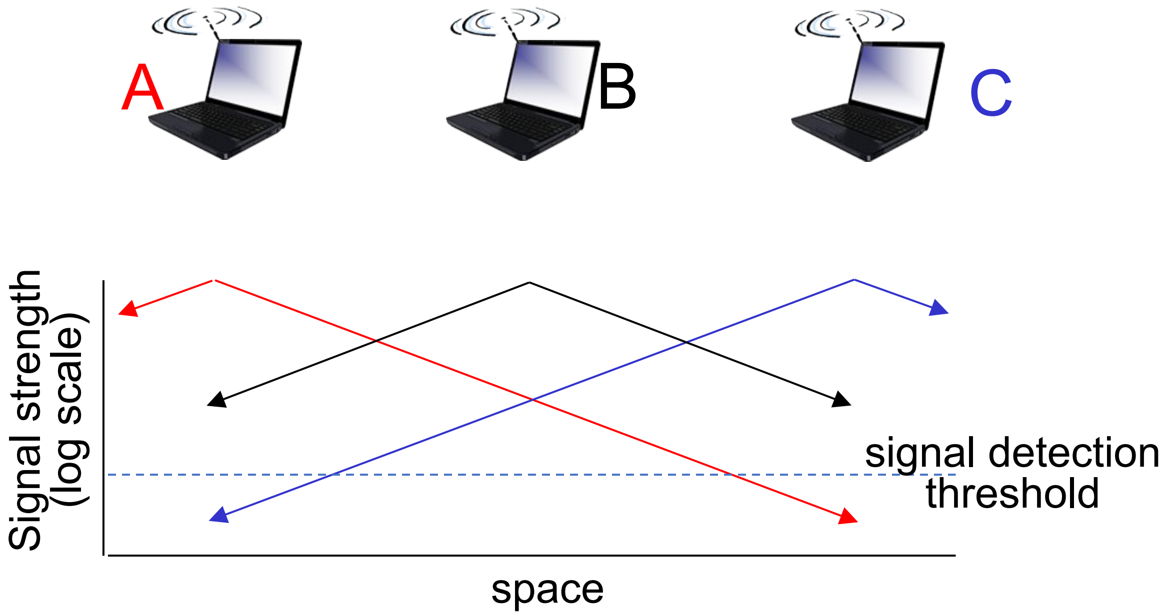


Generalized path loss ~ $(fd)^n$:

- n=2 (free space), n=(2.7,3.5) urban, n= (3,6) in building

“Hidden terminal problem” recalling ~ $(fd)^2$ path loss

Signal fading with~ $(d)^2$ path loss, causes a “hidden terminal” problem:

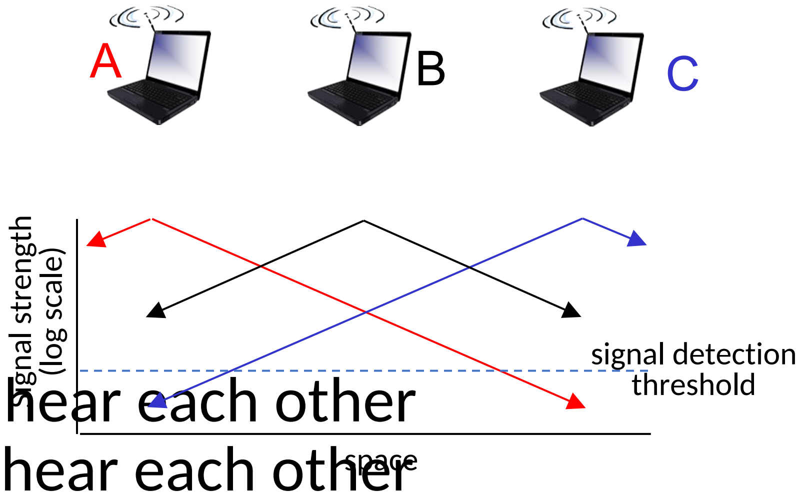


hidden terminals: A and B can hear each other, B and C can hear each other, but A and C can not hear each other

- complicates wireless channel sharing among A, B, C

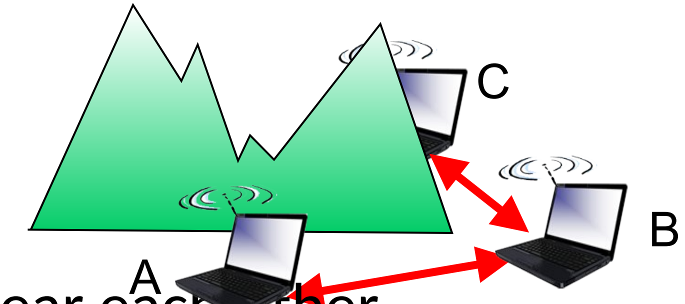
Wireless link characteristics: hidden terminals

Path loss causes “hidden terminals”



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

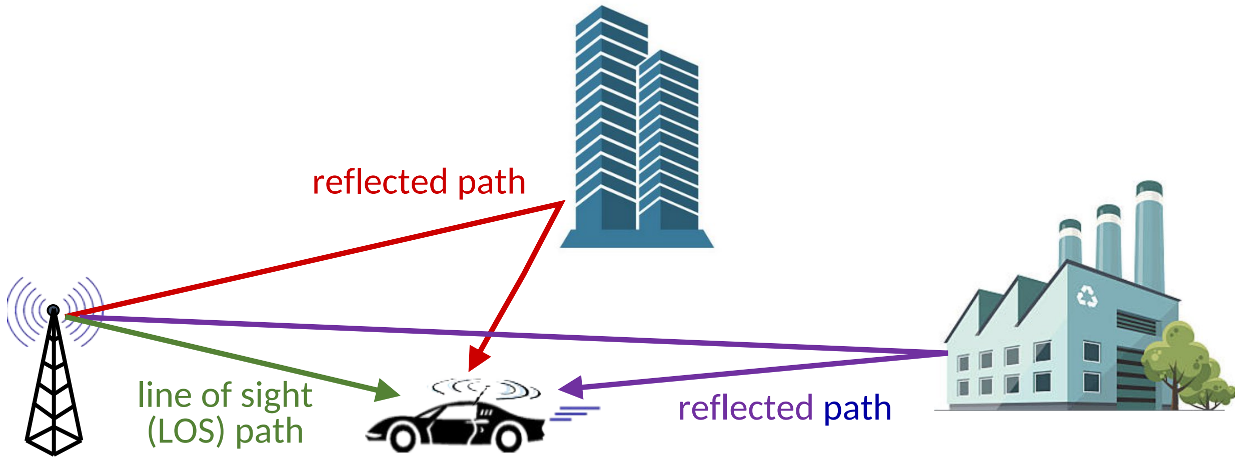
Objects cause ”hidden terminals”



- 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

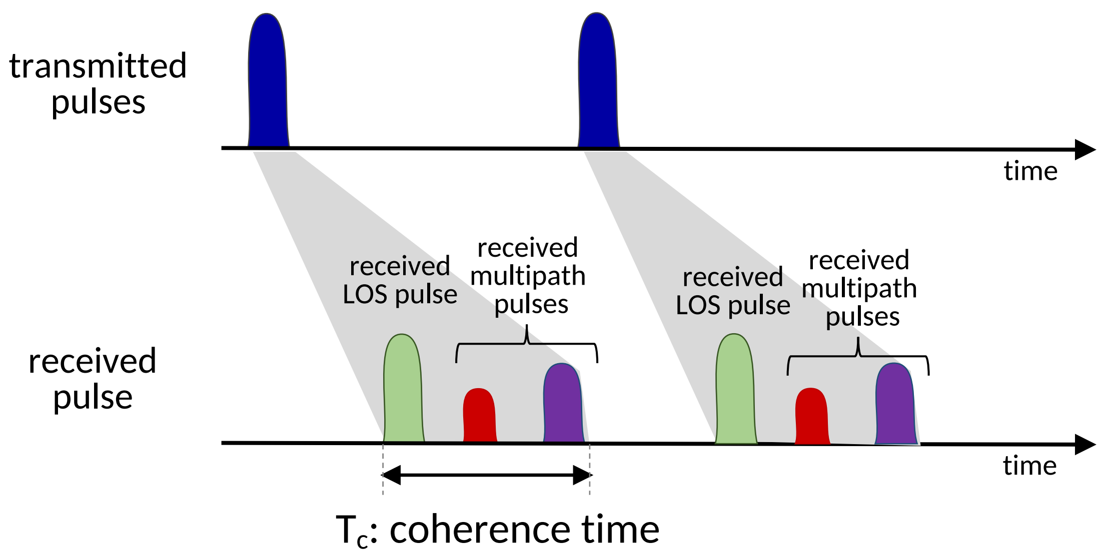
Wireless link characteristics: multipath

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

Antennas

MIMO: Multiple input multiple output antenna

Antennas both transmit and receive radio waves

single antenna: old school

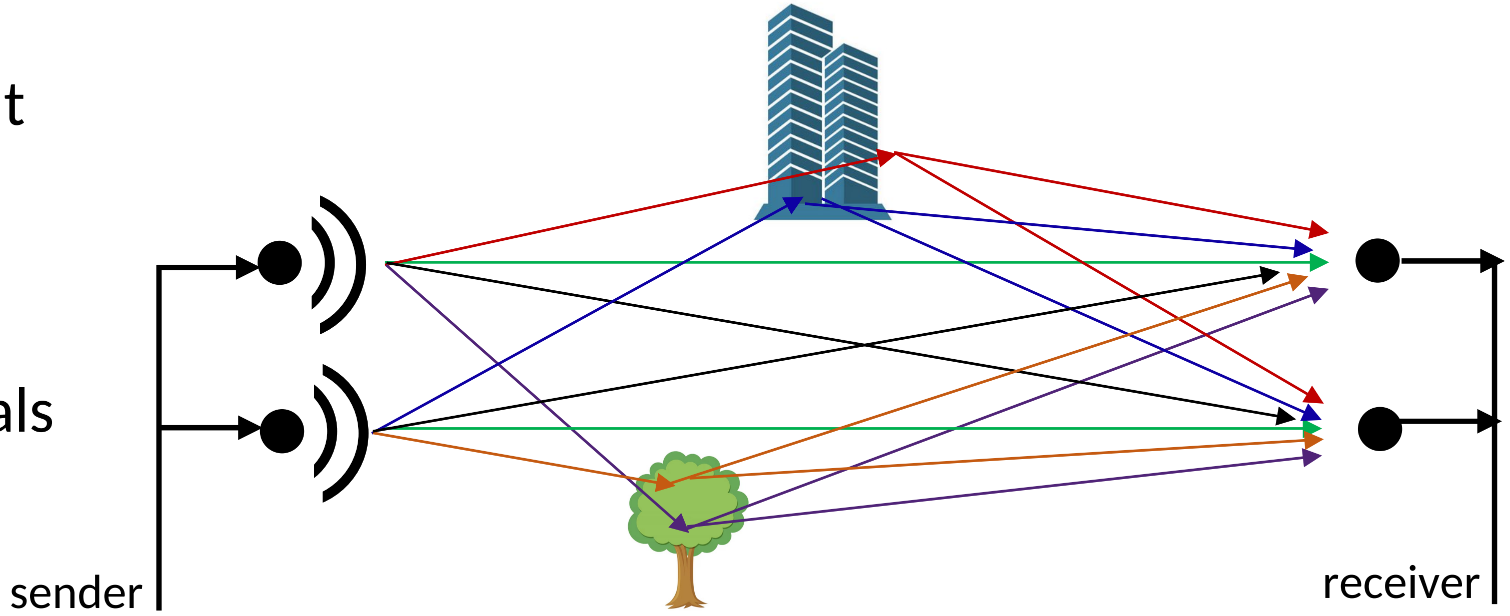
multiple antenna: common now in wireless networks

- Gigabit LTE with 4x4 MIMO
- Wi-Fi 6 (802.11ax) with 2x2 MIMO

MIMO transmission: single user

Single User MIMO: spatial *diversity*

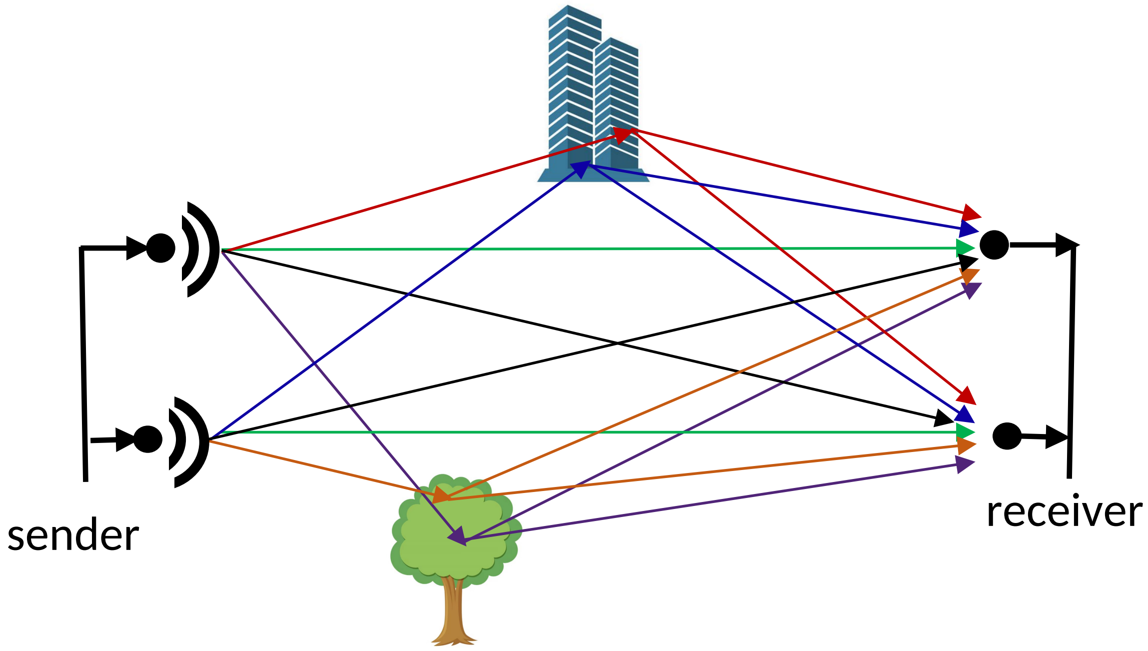
- multiple transmit/receive antenna to/at one user at same time
- *exploit multipath:* use multiple antennas to increase number of paths for transmitted signal between transmitter and receiver
  - multipath: signals arriving at receiver not the same (e.g., some at higher quality)
  - antenna gain: increase SNR by combining multiple signals



12 signal paths from one sender (with two antennae) to one receiver (with two antennae)

MIMO: spatial *diversity*

- increase reliability, range by sending / receiving *redundant streams of information in parallel* along different spatial paths between transmit and receive antennas



- *improved reliability:* unlikely that all paths degraded at same time
- *improved range*: multiple antennas gather more signal at receiver

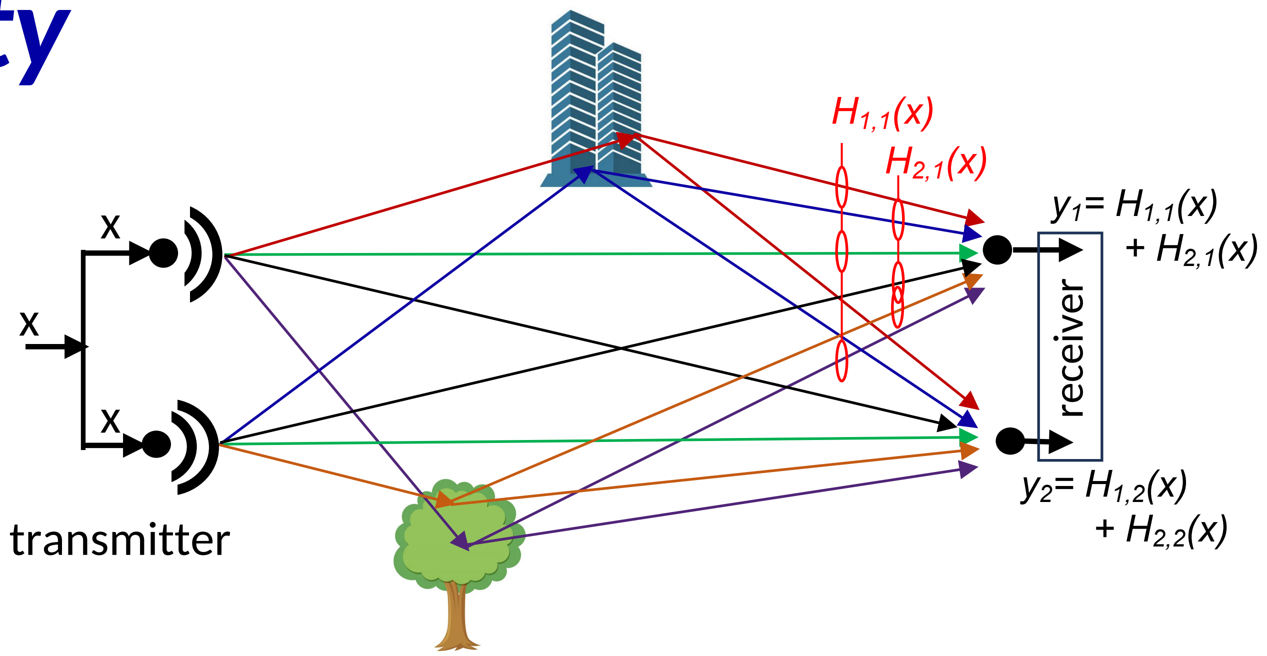
MIMO: spatial *diversity*

x: signal transmitted

y_j: signal received at antenna *j*

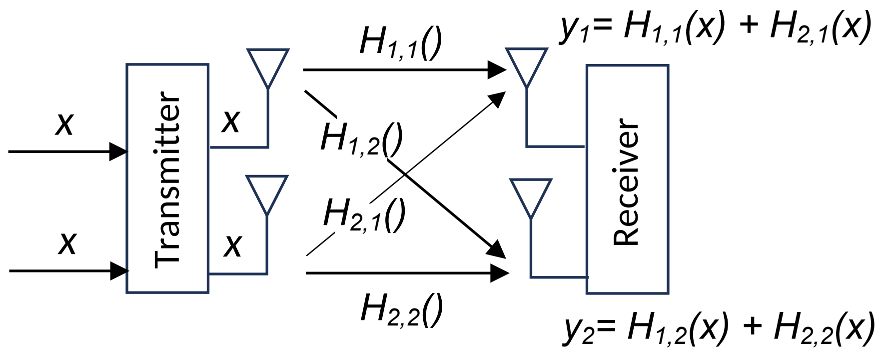
$H_{i,j}(x)$: transformation of signal *x* from transmitter antenna *i* to receiver antenna *j*

- estimated by receiver (perhaps with sender's help)



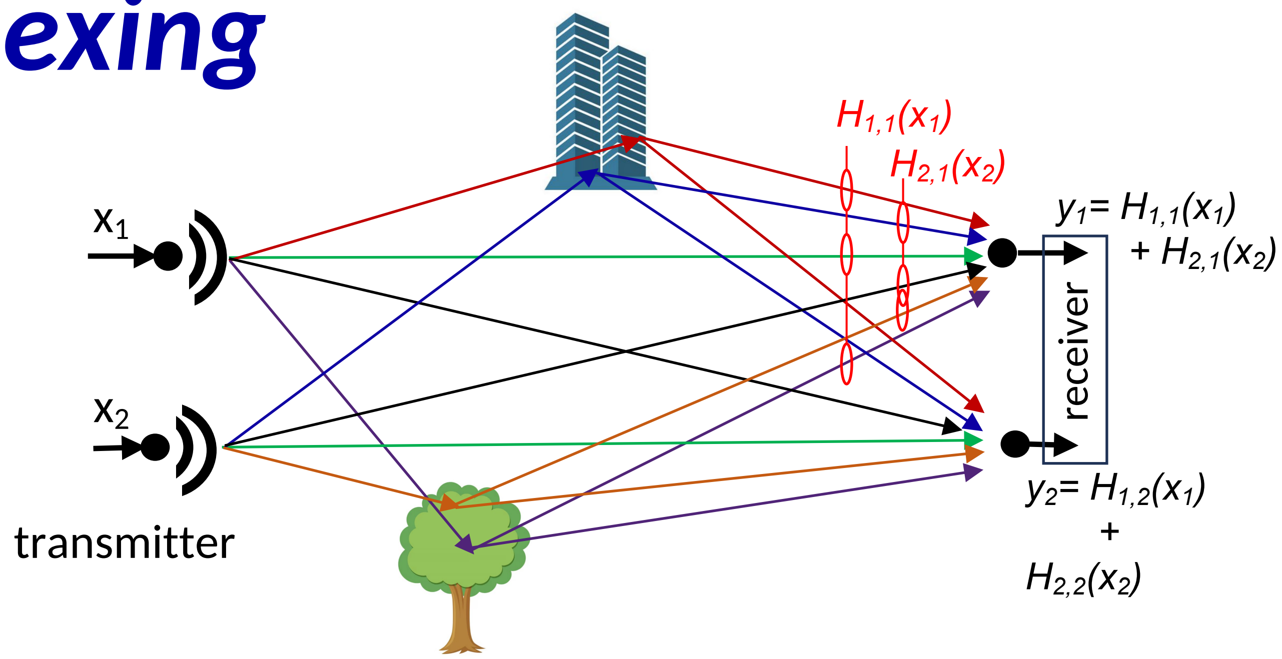
Signal processing at receiver?

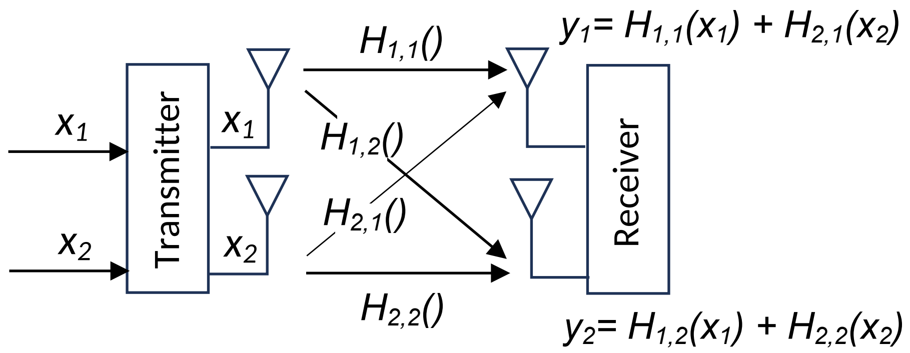
- don't want to just add y1, y2
- take stronger or smaller SNR of y1, y2?
- re-align phases, coherently add?



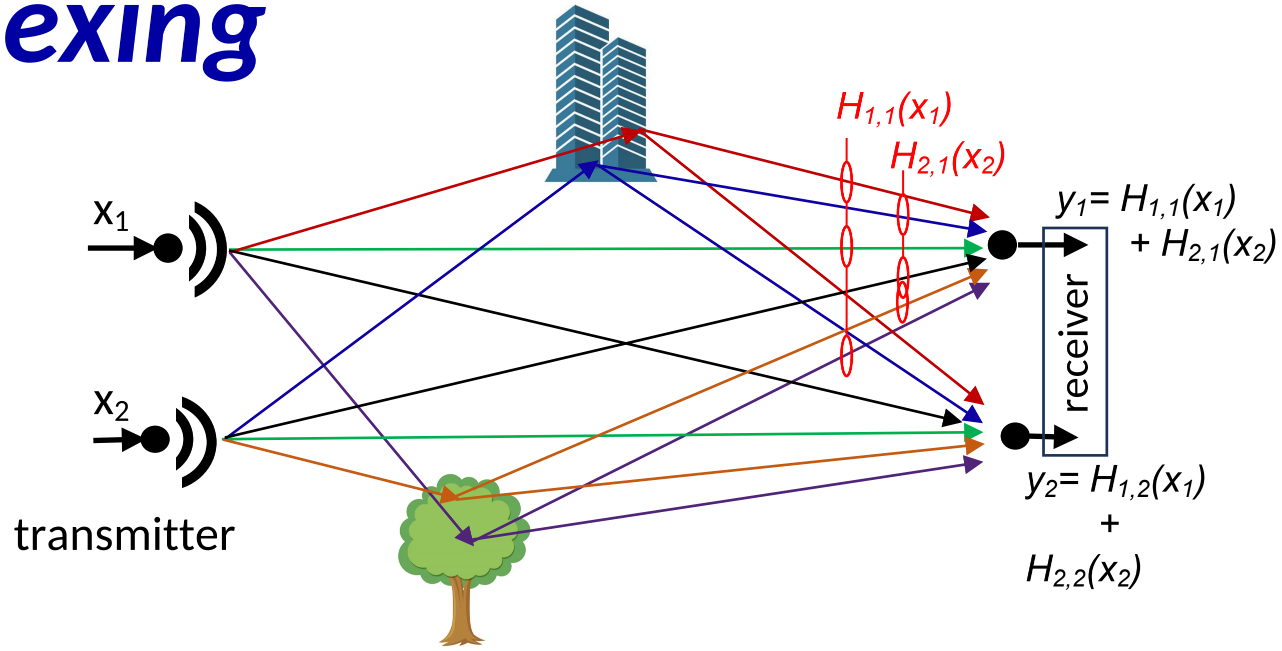
MIMO: spatial *multiplexing*

- send two *different streams of information*, x_1 and x_2 in parallel along different spatial paths from transmitter to receiver
- spatial *multiplexing* differs from spatial *diversity*





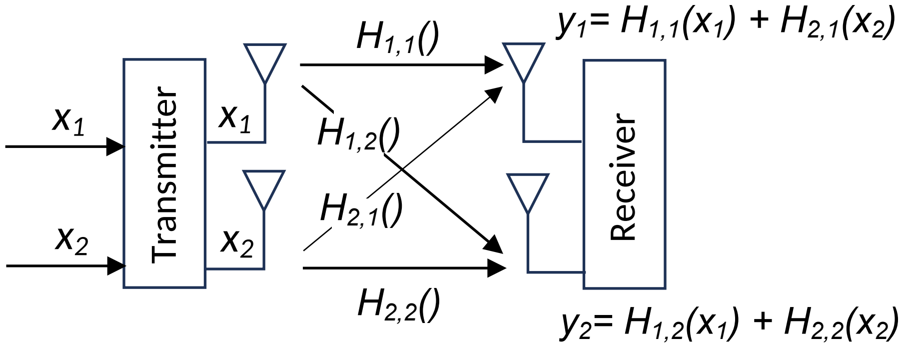
MIMO: spatial *multiplexing*



$$y_1 = H_{1,1}(x_1) + H_{2,1}(x_2)$$
$$y_2 = H_{1,2}(x_1) + H_{2,2}(x_2)$$

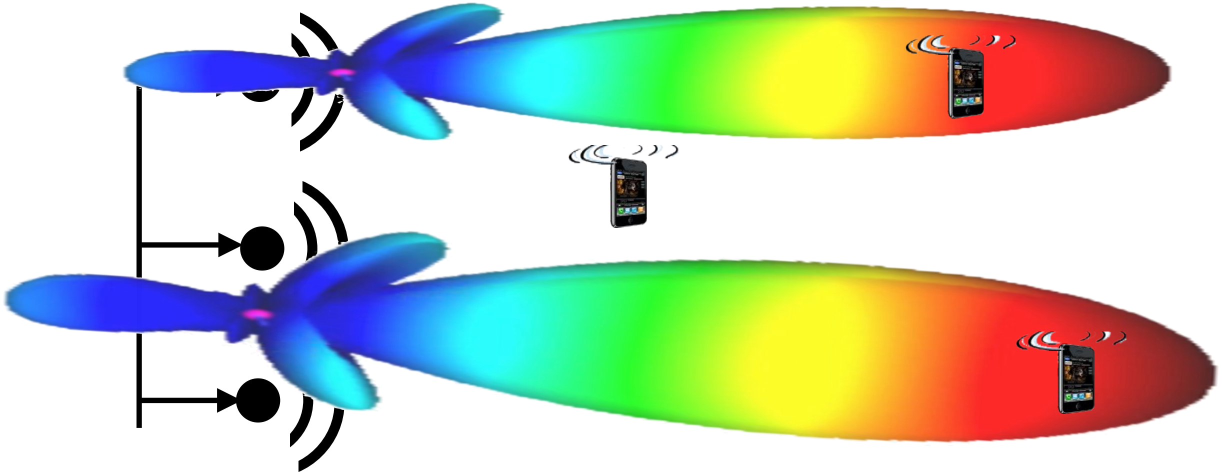
Two equations in two unknowns

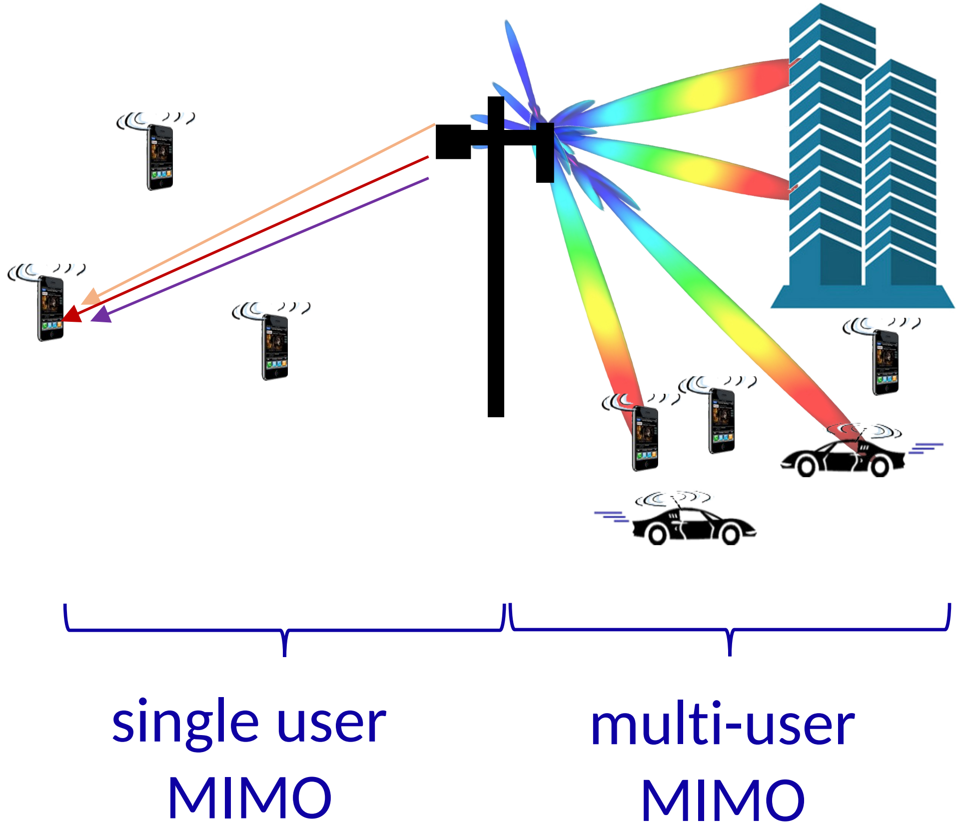
- but $H_{i,j}(x_i)$ are time-varying stochastic quantities



Multi-user MIMO

- multiple transmit antenna send to *different* users at same time
  - "spatial multiplexing"
- *exploit directional antenna:* send to geographically separated users at same time via beamforming





Wireless radio spectrum:

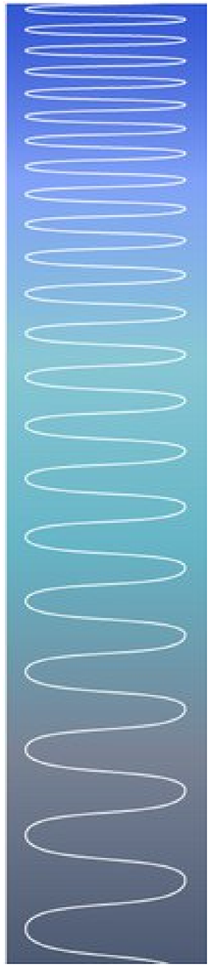
- radio spectrum: national asset, owned by the nation
- national government determine how spectrum is used "locally"
- different spectrum use types:

licensed:
- dedicated use, typically by one "owner" (e.g., cellular carrier such as AT&T, Verizon)
- often allocated by spectrum auction

shared:
- spectrum dynamically shared among users
- "incumbent" may get preferential access, others "back off"

unlicensed:
- open (free) for anyone to use, conforming to rules (e.g., power transmission levels)
- 2.4GHz and 5 Ghz WiFi
- 3.5GHz "Private 5G" (aka CBRS)

WiFi spectrum bands



6 GHz range
- most recently added
- more than 250 configurable/selectable WiFi channels of different transmission rates

802.11
ax/be

5 GHz range
- more than 150(configurable/selectable WiFi channels) of different transmission rates

802.11
a/h/n/ac/ax

2.4 GHz
- Divided into 11-14 channels, depending on country

802.11
b/g/n/ax

- other 802.11 WiFi spectrum bands, but not in widespread use

5G spectrum: three spectrum bands*

* No single, well-accepted ranges for “low”, “mid” and “high”

High band frequencies: 25–66 GHz range (aka mmwave)

- 26 GHz, 40 GHz, 50 GHz, 66 GHz bands popular
- short distances (< mile), high speeds (<3 Gbps)
- line of sight transmission: poor penetration of trees, buildings, …

5G

Mid-band frequencies: 1 - 6 GHz ranges

- balance distances (~5 miles ?) and transmission rates (100–900 Mbps)
- 1.8, 3.3 GHz to 3.8 GHz, 6 GHz bands popular

3.4 - 6 GHz: 5G 4G

1-2.6 GHz: 5G 4G 3G 2G

Low band frequencies: (< 1 GHz range)

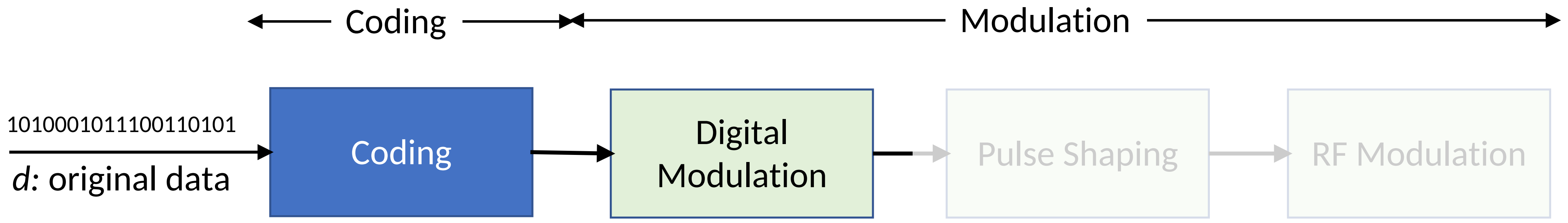
- covers longer distances (10’s of miles), but at lower speeds (50–250 Mbps)

5G 4G 3G 2G

Chapter 7 outline

- introduction
- radio: the physical layer
  - radio principles
  - radio channels
  - antennas: MIMO
  - radio spectrum
  - coding and modulation
- the wireless *access* network
- the wireless core network
- mobility
- Bluetooth, satellite, IoT wireless networks

Physical Layer: coding and modulation



Add error detection, correction bits at physical layer

Choose digital modulation technique that maximizes number of reliably transmitted bits/sec based on observed channel impairments e.g., in family of Quadrature amplitude modulation (QAM)

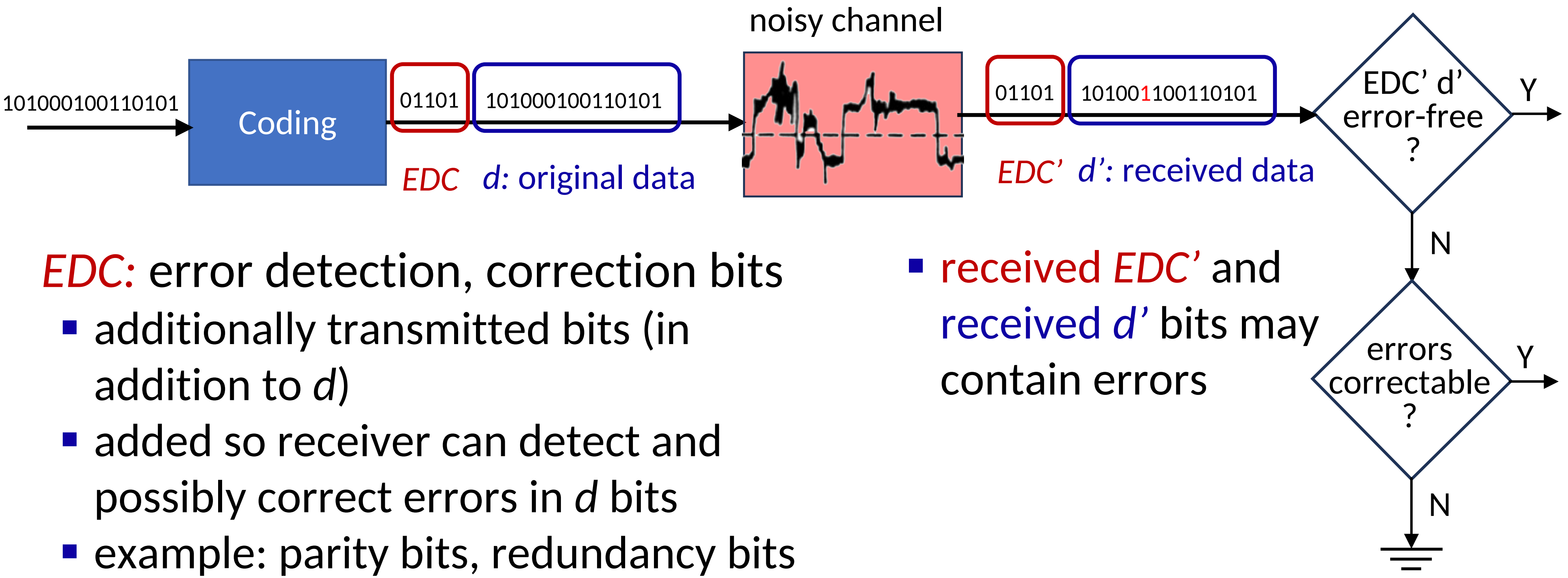
match transmission bandwidth to channel bandwidth using pulse shaping

transmit signal as an electromagnetic wave over assigned *carrier frequency*

We won't cover this (look at ECE for courses)

Carrier: waveform at a given frequency, f_c (carrier frequency), modified (modulated) with an information-bearing signal

Physical Layer: Error detection, correction coding



EDC: error detection, correction bits

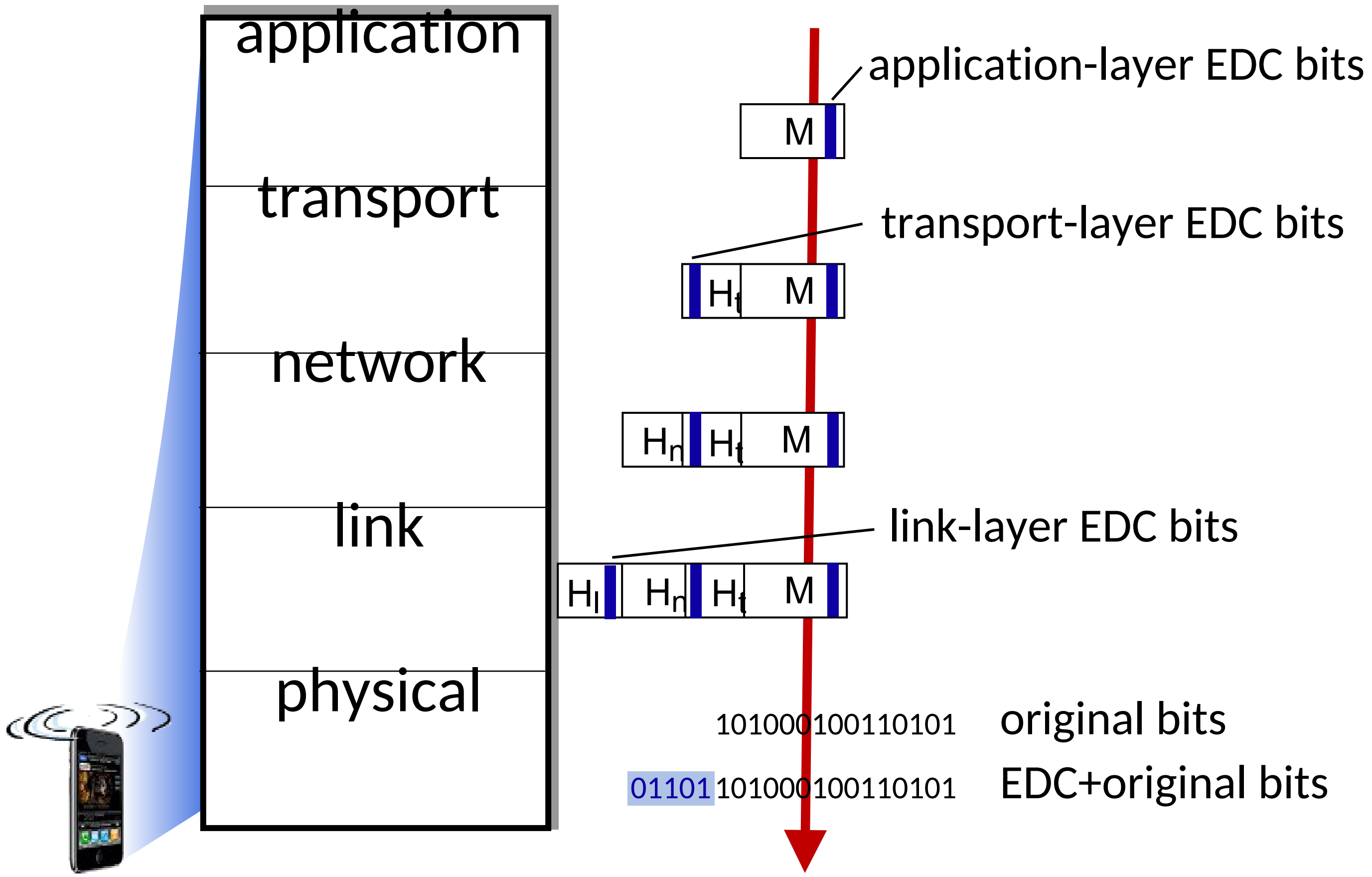
- additionally transmitted bits (in addition to *d*)
- added so receiver can detect and possibly correct errors in *d* bits
- example: parity bits, redundancy bits

- received *EDC'* and received *d'* bits may contain errors

EDC used at many layers: channel (physical), link, network, transport, application layers

Physical Layer: Error detection, correction coding

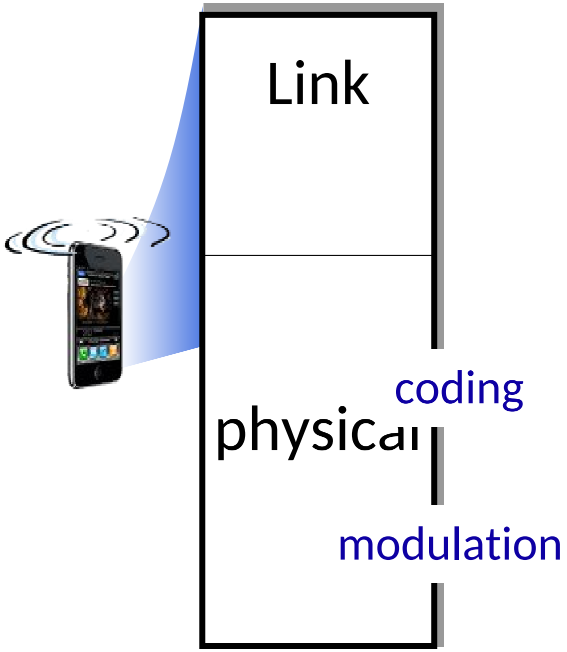
Wireless *physical layer* may add EDC bits, into addition to:



adding physical-layer EDC makes sense!

- detect/recover locally, rather than wait for end-end
- physical layer techniques adapted to local radio error characteristics

Physical Layer: EDC shuffling example



A burst of noise in this interval causing 3 bits to be unintelligible , with no shuffling, would mean receiver can not determine d_4

$d_1\, d_2\, d_3\, d_4\, d_5\, d_6\, d_7\, d_8$ original bits from link layer, including EDC

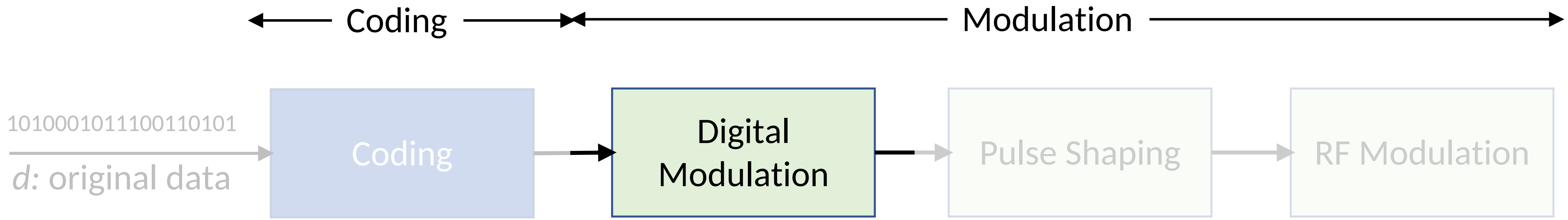
$d_1\, d_1'\, d_2\, d_2'\, d_3\, d_3'\, \boxed{d_4\, d_4'\, d_5}\, d_5'\, d_6\, d_6'\, d_7\, d_7'\, d_8\, d_8'$ *add* EDC duplicate bits in PHY

$d_1\, d_5'\, d_2\, d_6'\, d_3\, d_7'\, \boxed{d_4\, d_8'\, d_5}\, d_1'\, d_6\, d_2'\, d_7\, d_3'\, d_8\, d_4'$ *shuffle* for resistance to burst errors

modulation: from bits to symbols to waveforms

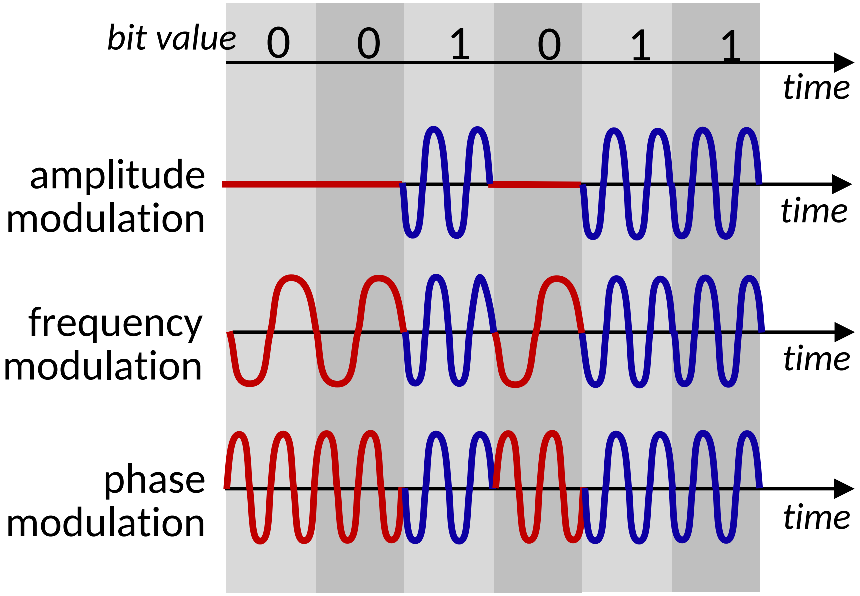
A burst of noise in this interval, causing 3 bits to be unintelligible still allows receiver to determine all original bits

Modulation



digital modulation

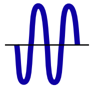
encoding bits (1's, 0's) into analog RF carrier signal by changing ("**modulating**") a characteristic of the RF carrier signal: *amplitude*, *frequency*, *or phase*.



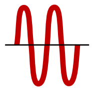
Modulation schemes: ASK, PSK

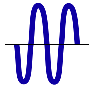
Amplitude shift keying (ASK):
signal's *amplitude* encodes bits

0: —

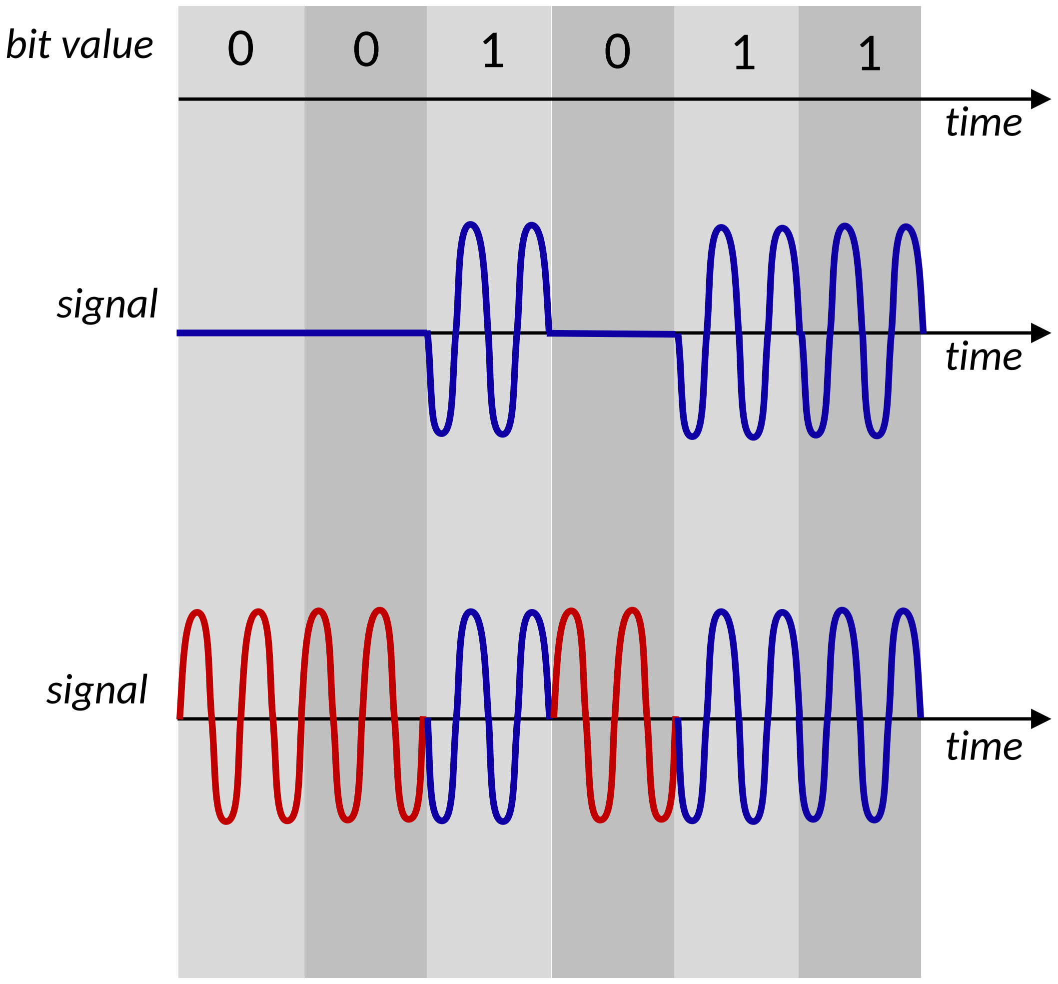
1: 

Binary Phase shift keying (BPSK): signal's *phase* encode bits

0: 

1: 

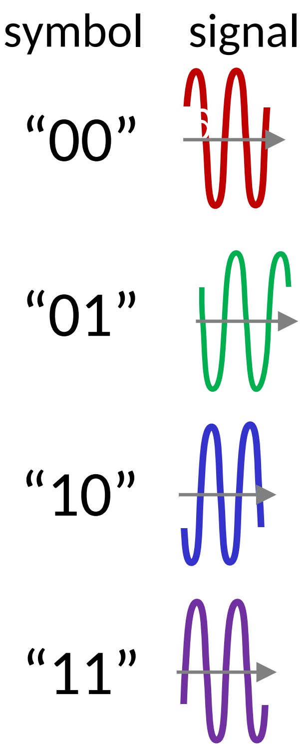
PSK: 0 and 1 signals *out of phase* by 180°, but at same carrier frequency

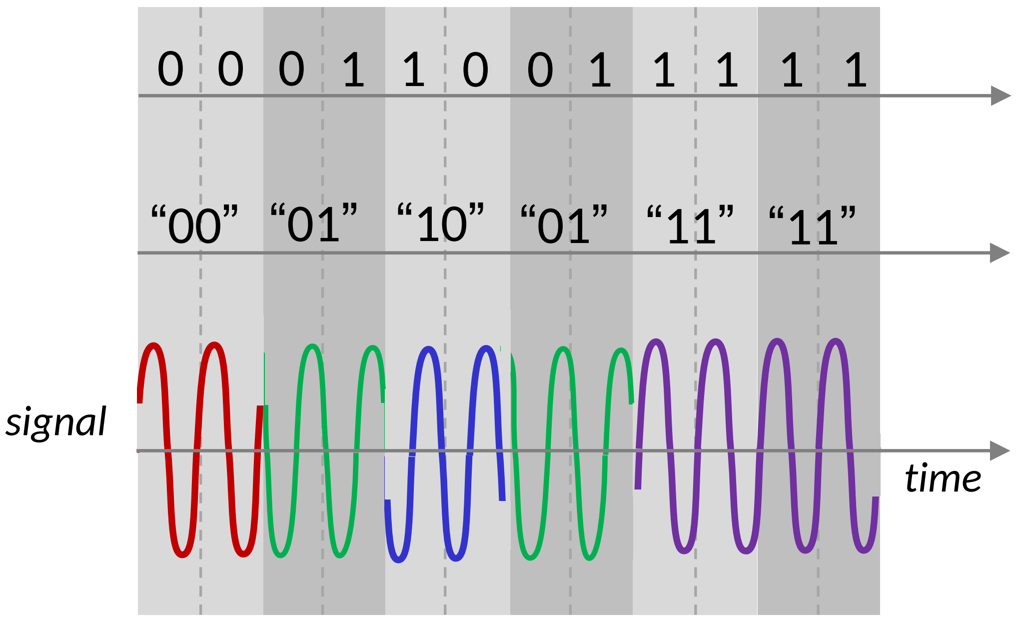


Modulation schemes: QPSK

Why stop at just two phases?

- two bits grouped to become one "symbol" (2 bits -> 4 symbols)
- *QPSK: Quadrature Phase Shift Keying:* 4 symbols encoded using 4 phases



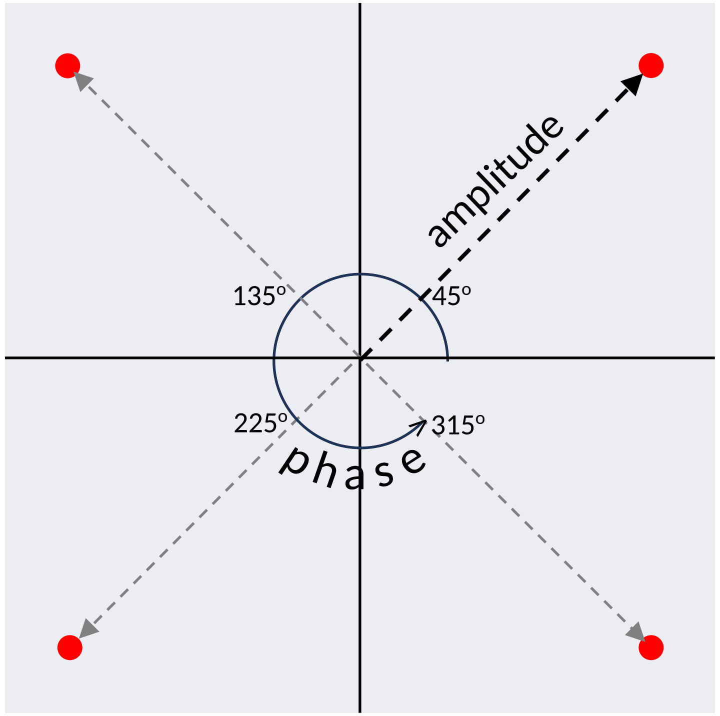


QPSK frequency same as BPSK, but twice the data rate!

Fun interactive QPSK tool: https://www.geogebra.org/m/enkymjtg

Constellation diagrams

graphical characterization of modulation: amplitude, phase of symbols



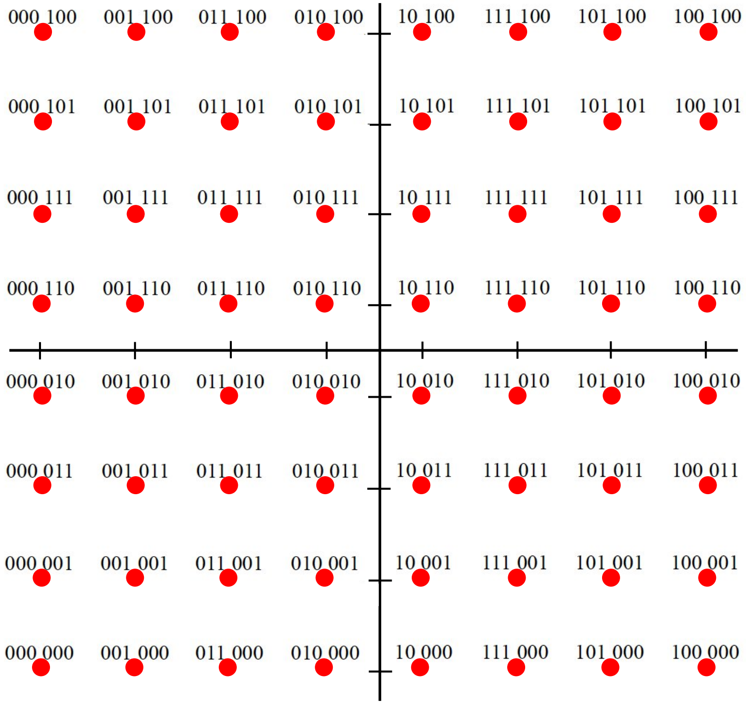
QPSK constellation diagram

- point in constellation diagram depicts symbol's phase (degrees counterclockwise from east) and amplitude (distance from origin)
- QPSK constellation diagram: four symbols represented by four signal waveforms:
  - four different *phases*
  - identical *amplitude*

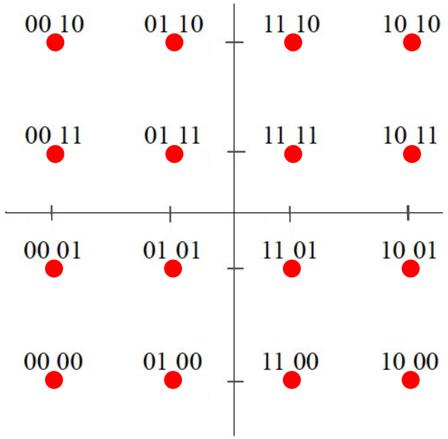
QAM: Quadrature Amplitude Modulation

- generalizing QPSK
- *m*-QAM: using *m* different amplitude/phase values to encode log2(m) bits

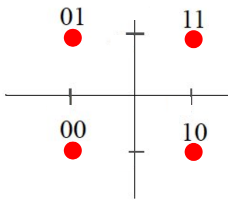
64-QAM $b_0b_1b_2b_3b_4b_5$



16-QAM



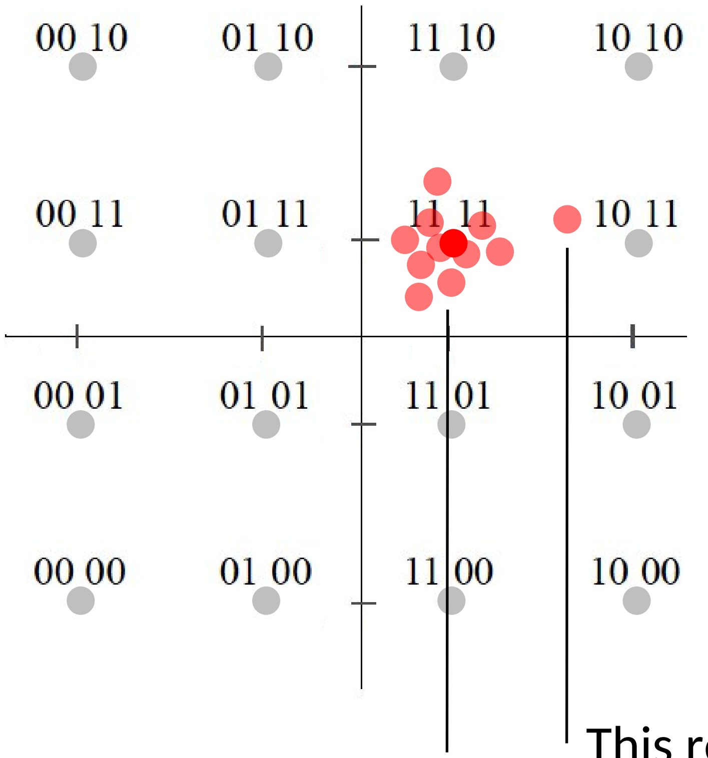
4-QAM b_0b_1



bit encodings for 4-QAM, 16-QAM, 64-QAM (for WiFi)

Constellation diagrams: how bit errors occur

16-QAM $b_0b_1b_2b_3$



These received signals correctly classified as 1111 (received amplitude, phases closest to 1111)

This received signal, is misclassified as 1011 since its amplitude, phases are closer to 1011 than 1111

Transmitter transmits waveforms for 12 1111 symbols, sequentially

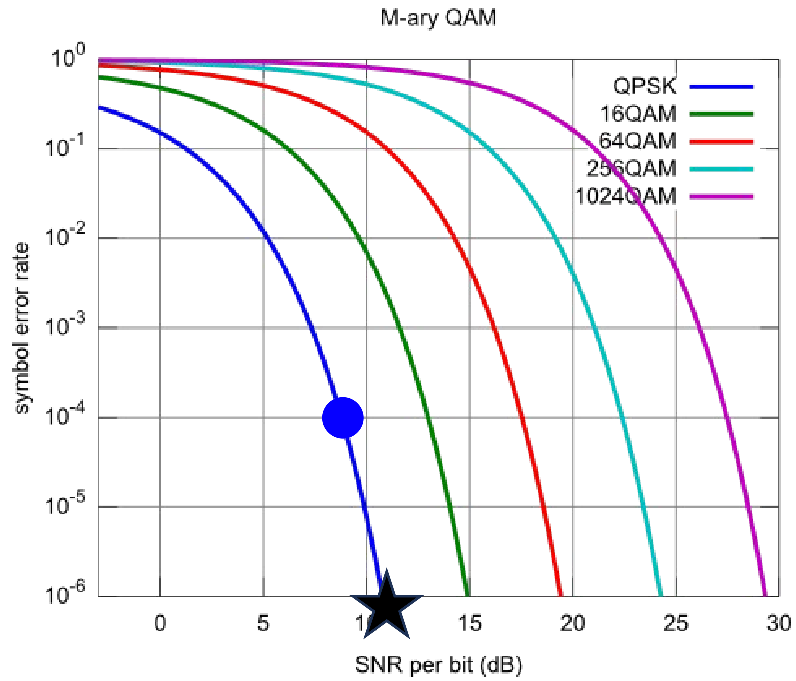
- phase/amplitude of transmitted signal
- phase/amplitude of received signals

- receiver measures amplitude, phase of received signal
- receiver classifies symbol as bit pattern with amplitude, phase closest to received signal amplitude, phase

Adaptive modulation

given modulation scheme :

- has nominal data rate (assuming no errors)
- SNR can increase/decrease:
  - changing interference
  - sender transmitter power
- move along SNR vs BER tradeoff curve



Idea: change modulation scheme, power on the fly, getting highest data rate possible (at acceptable BER, acceptable energy expenditure), as SNR changes

Max data rate:

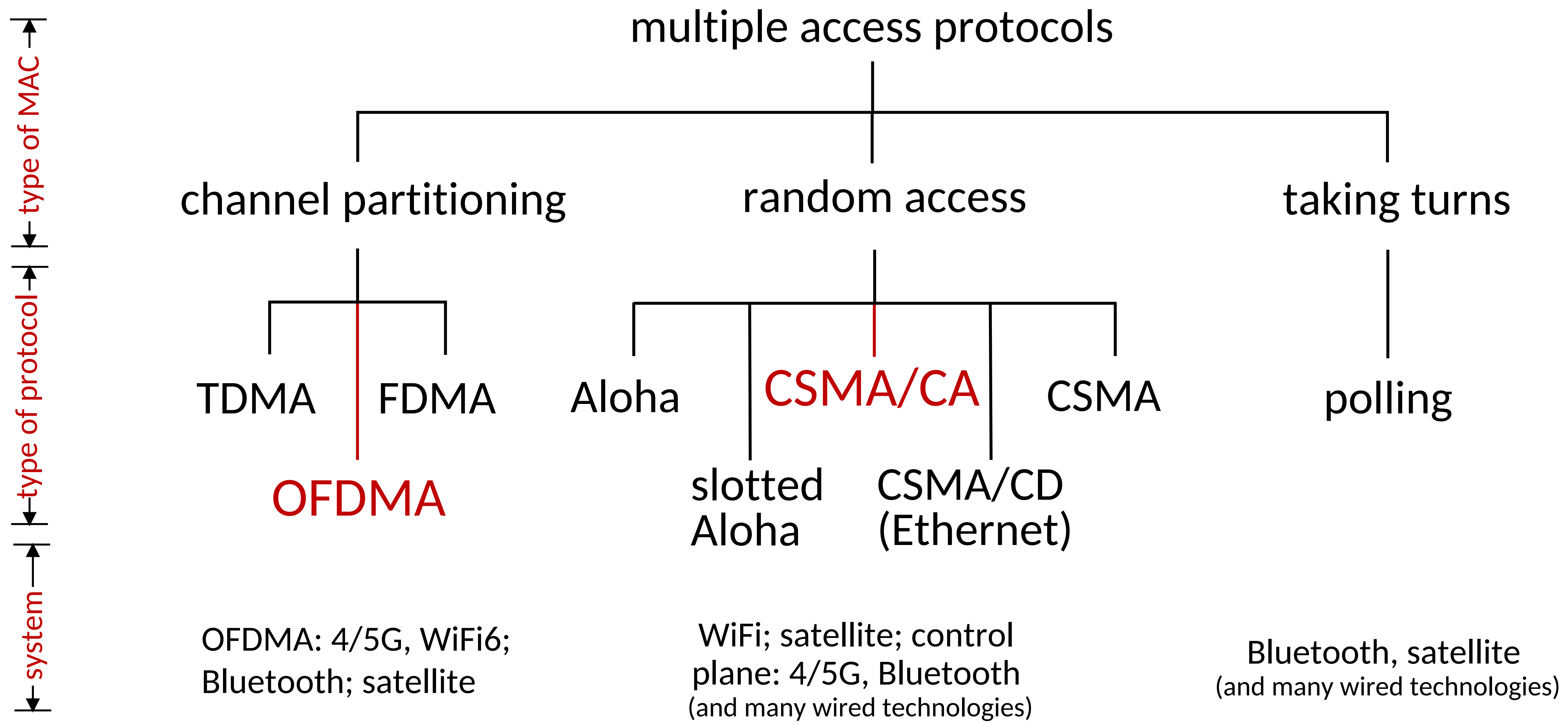
16 QAM: 11.5 Mbps

64 QAM: 26.9 Mbps

Chapter 7 outline

- introduction
- radio: the physical layer
- the wireless *access* network
  - sharing a wireless access channel: OFDMA, CSMA/CA
  - WiFi wireless LAN
  - 5G radio access network
- the wireless core network
  - principles, 5G
- mobility
- Bluetooth, satellite, IoT wireless networks

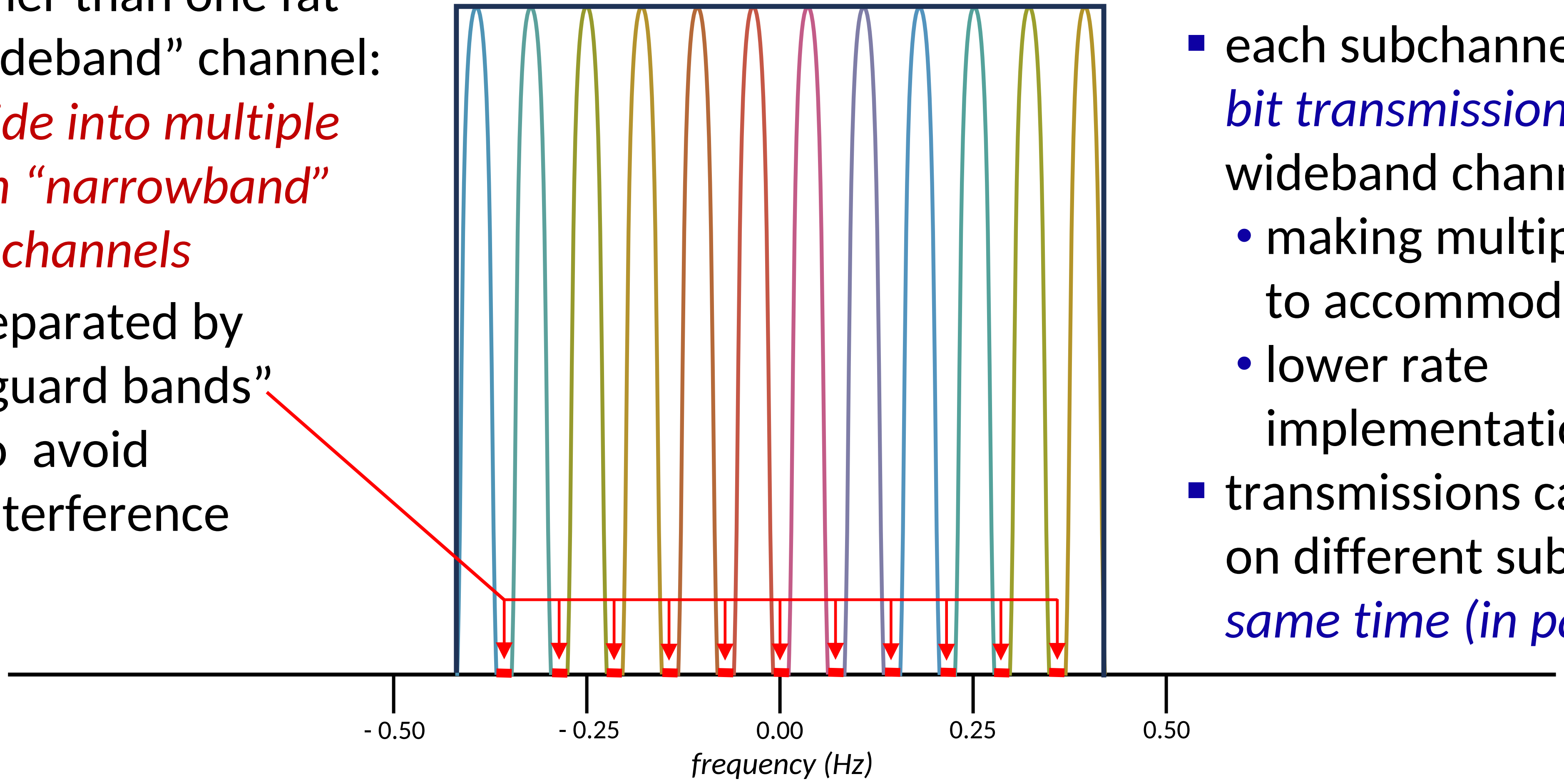
Recall: MAC protocols



FDM: Frequency Division Multiplexing

rather than one fat "wideband" channel: *divide into multiple thin "narrowband" subchannels*

- separated by "guard bands" to avoid interference

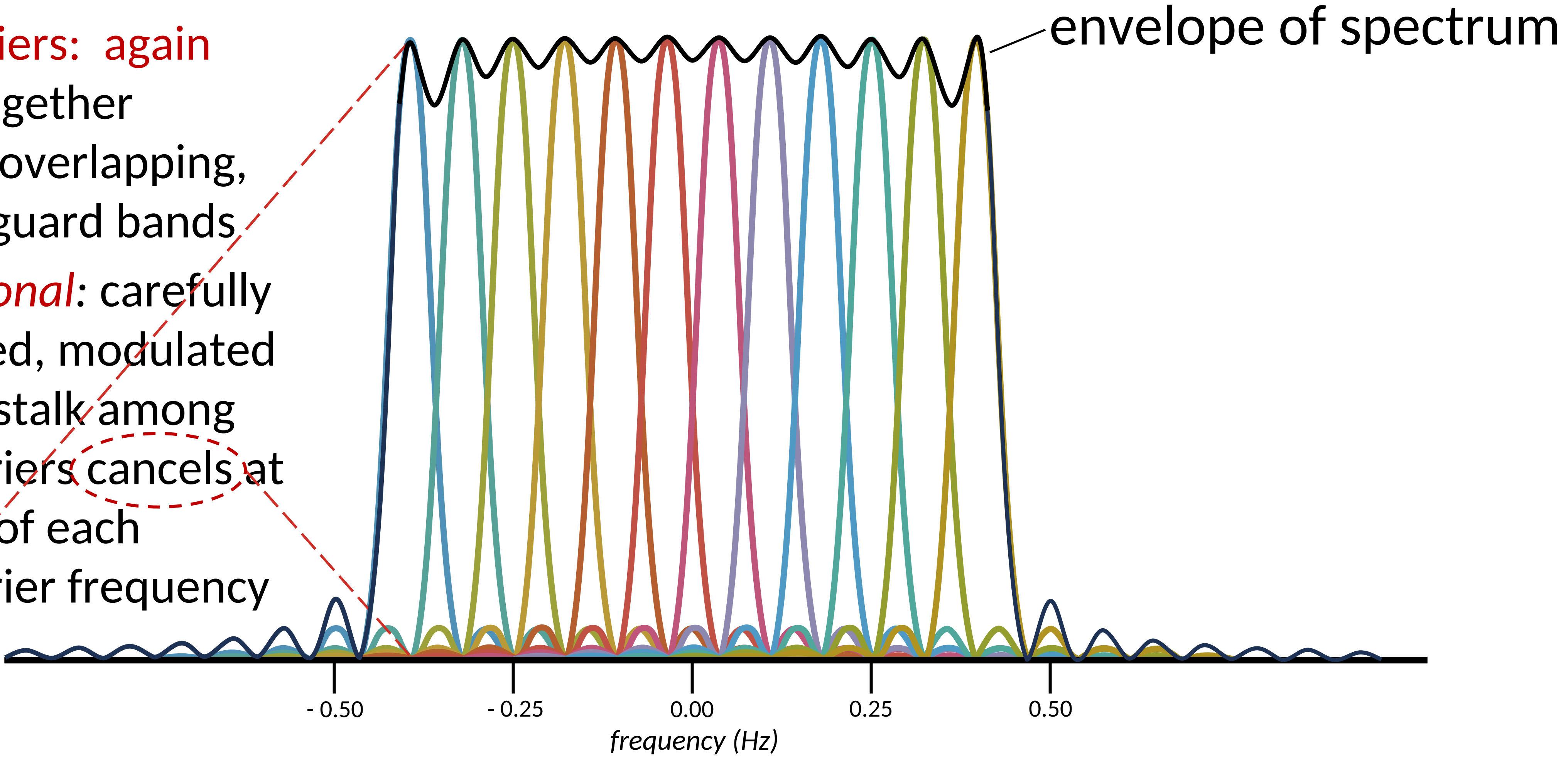


Narrowband channels:

- each subchannel has *lower bit transmission rate* than wideband channel:
  - making multipath easier to accommodate
  - lower rate implementations easier
- transmissions can happen on different subchannels at *same time (in parallel)*

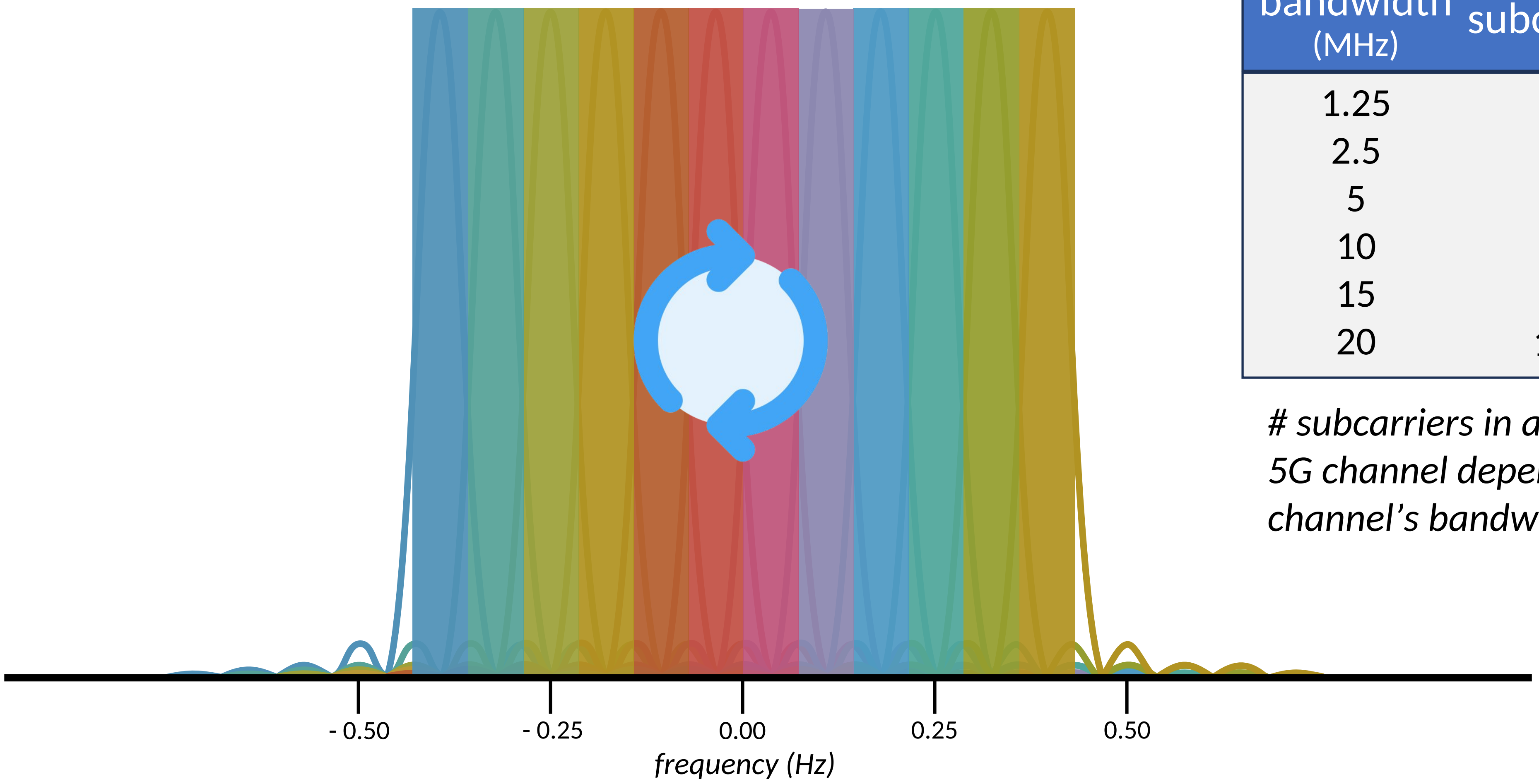
OFDM: *Orthogonal* FDM

- subcarriers: again close together
- slightly overlapping, but no guard bands
- *orthogonal*: carefully designed, modulated so crosstalk among subcarriers cancels at center of each subcarrier frequency



OFDM: Subcarriers

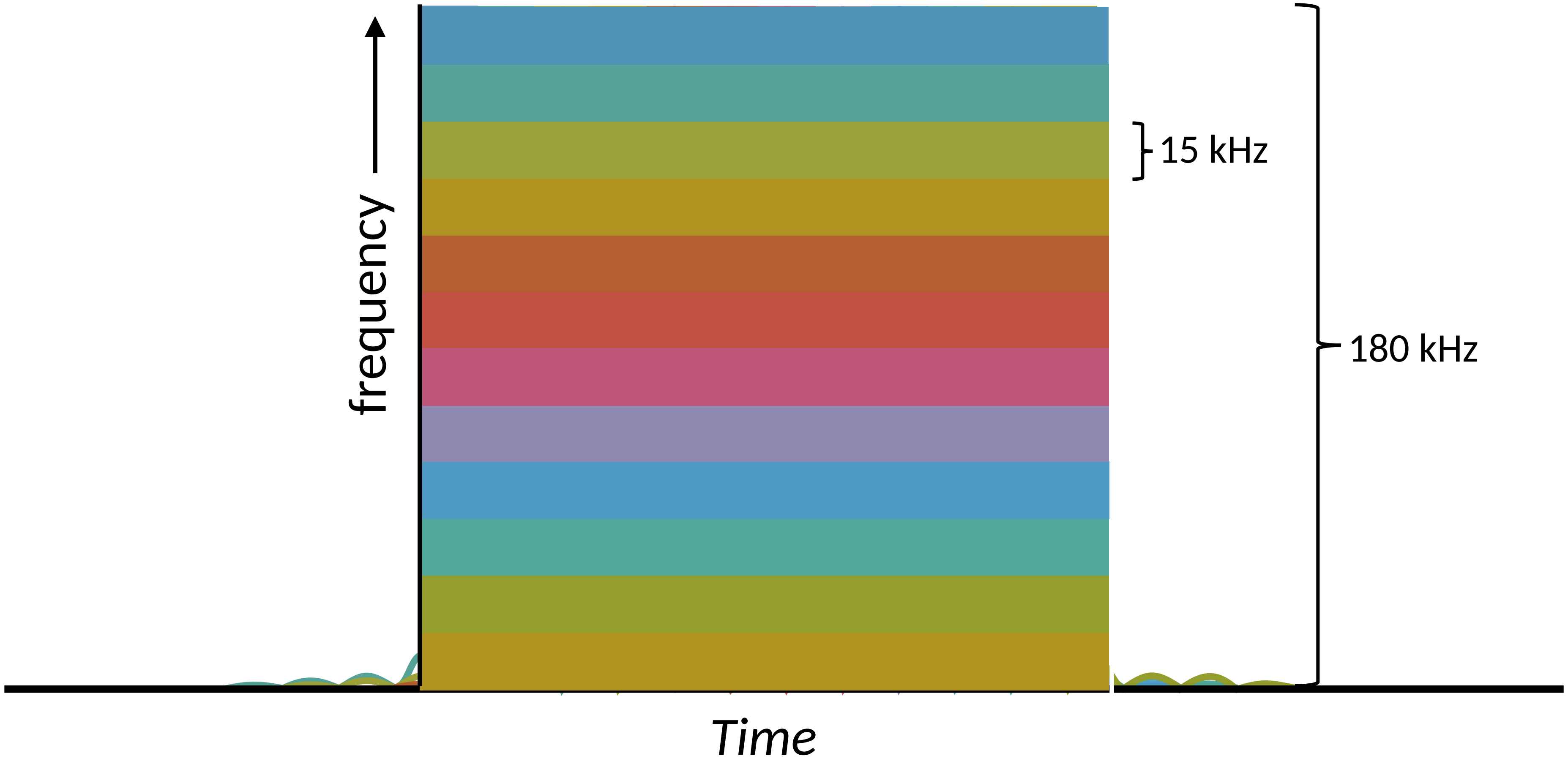
Wireless Jargon:
"carrier" ~ "channel"
"subcarrier" ~ "subchannel"



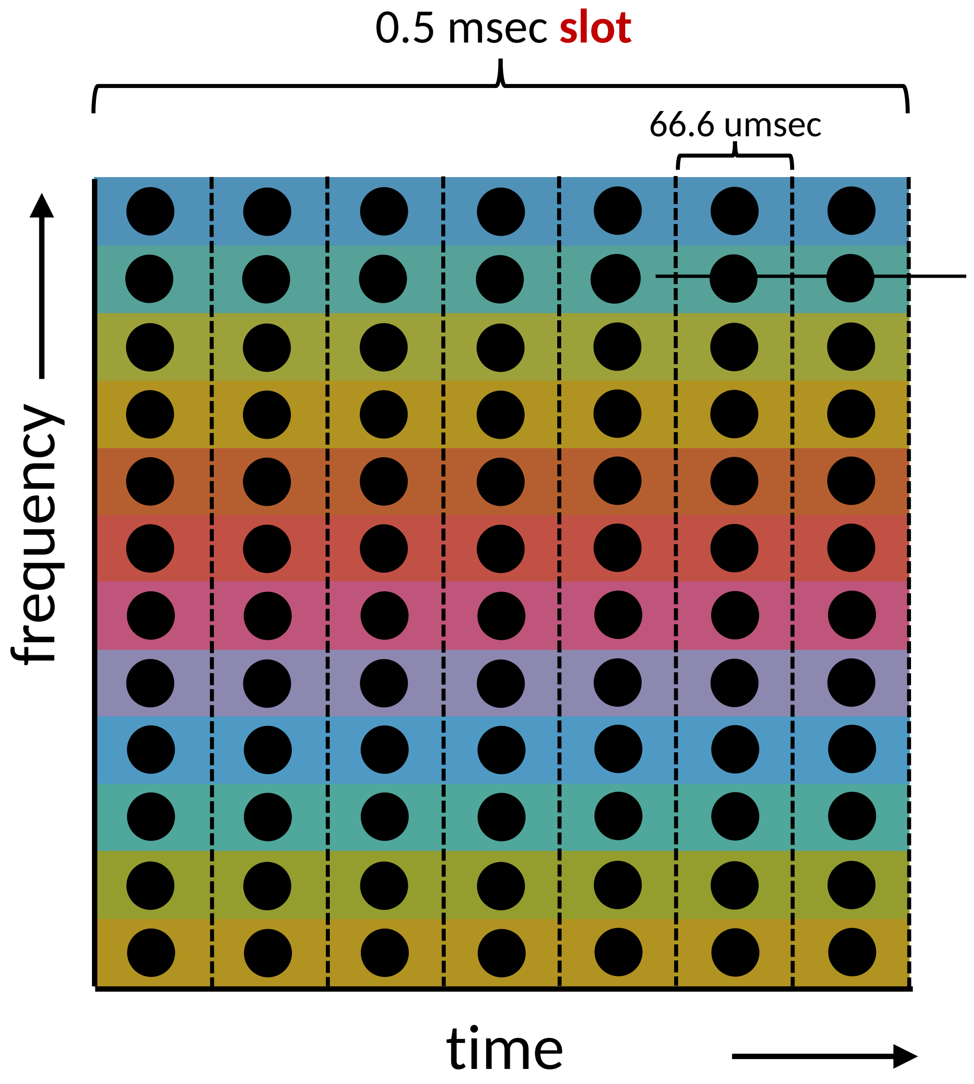
Channel bandwidth (MHz)	Number of subcarriers
1.25	76
2.5	150
5	300
10	600
15	900
20	1200

 # subcarriers in an 4G / 5G channel depends on channel's bandwidth

OFDMA: subcarriers, time



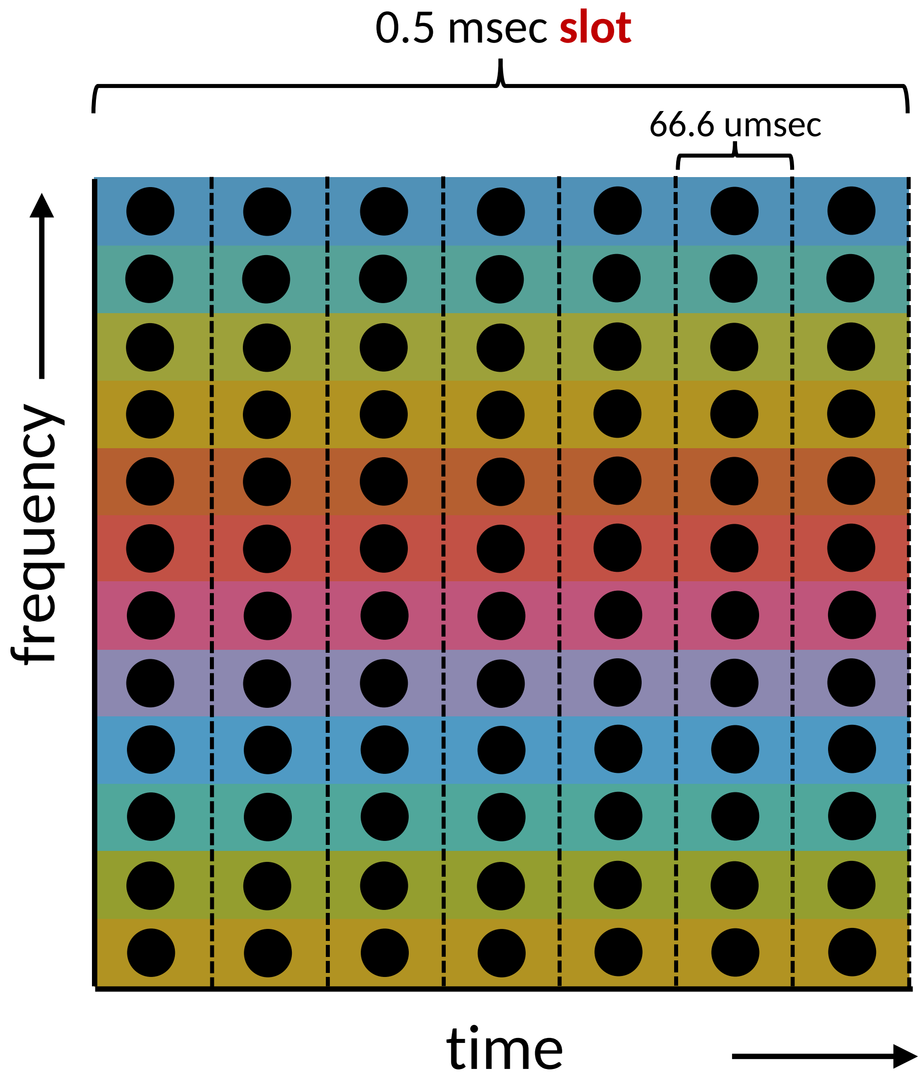
OFDMA: symbols



one "symbol" can be transmitted per 66.6 usec (4G) at given subcarrier frequency

- *number of bits (between 2-8) in symbol depends on modulation technique* chosen (which depends on channel quality)

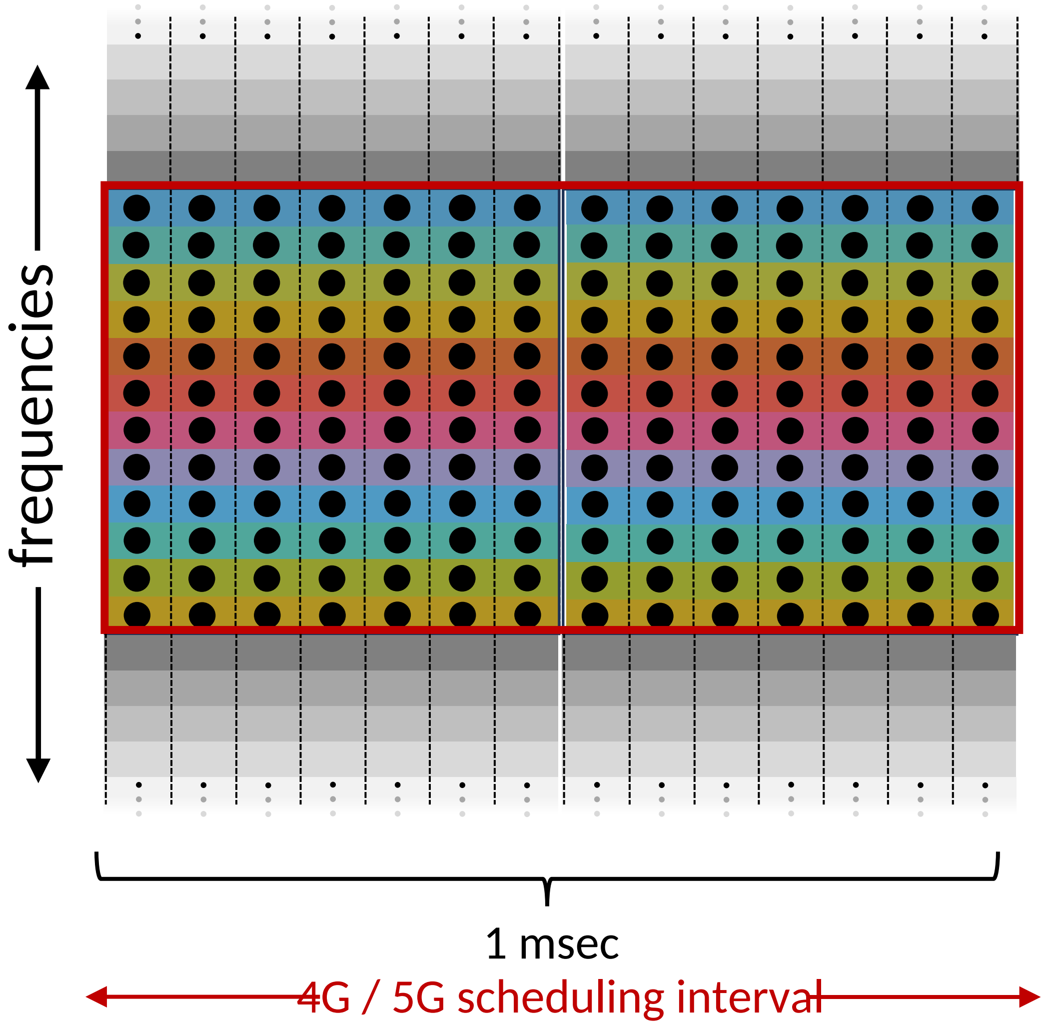
OFDMA: resource blocks



resource block (RB):

- symbols grouped into resource blocks
- 84 symbols (7 symbols/slot over 12 subcarriers) in 4G
- *smallest unit of data that can be sent to (assigned to) a user*

OFDMA: resource blocks



Base station decides which RBs get assigned (over all frequencies) to which devices at 1 msec intervals

From 4G LTE to 5G New Radio (NR)

Commonalities, differences:

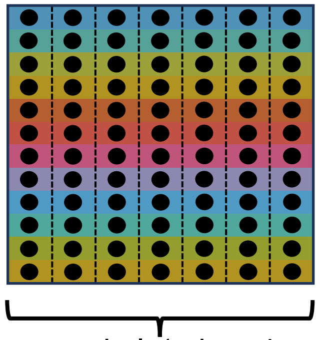
4G, 5G both use OFDMA

- Subcarrier bandwidths:
  - 4G: 15 kHz
  - 5G: 15, 30, 60, 120 kHz
- Max carrier bandwidth:
  - 4G: 20 MHz
  - 5G: 100 MHz

4G, 5G: resource blocks (RB)

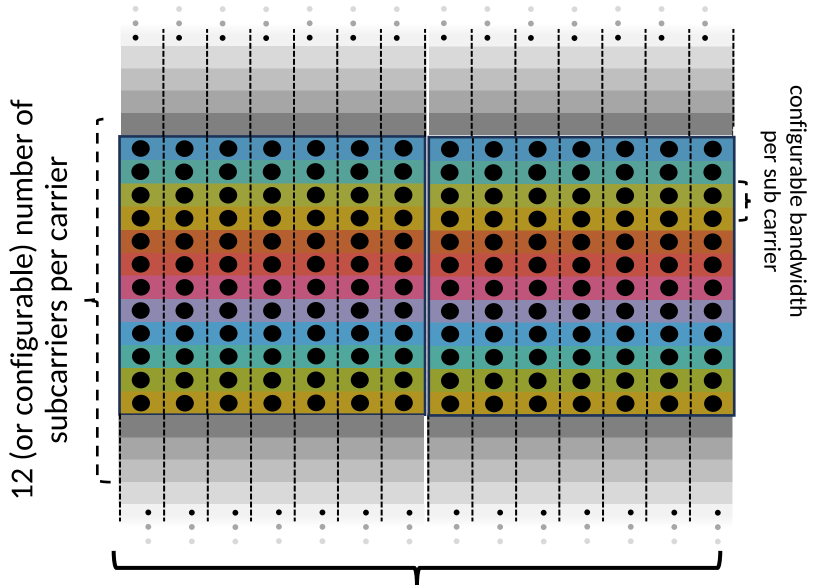
- smallest scheduling unit of transmission to device

4G



7 symbols/subcarrier
0.5 msec
1 LTE PRB

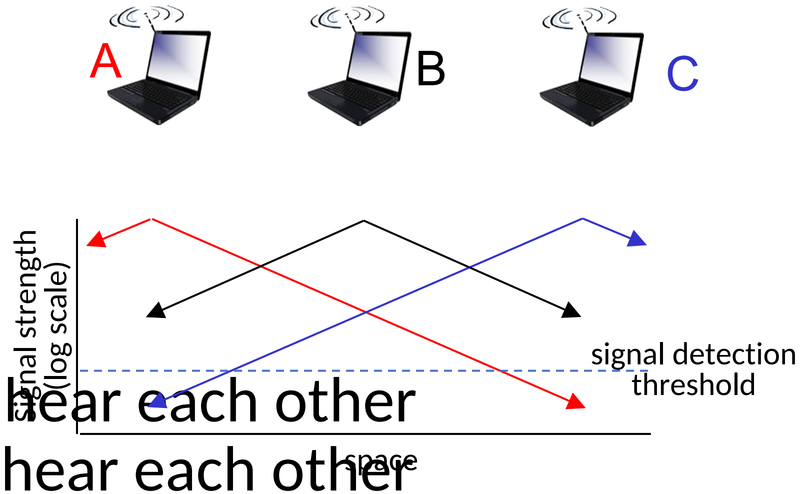
5G



14 symbols/subcarrier
1 msec
1 5G NR PRB

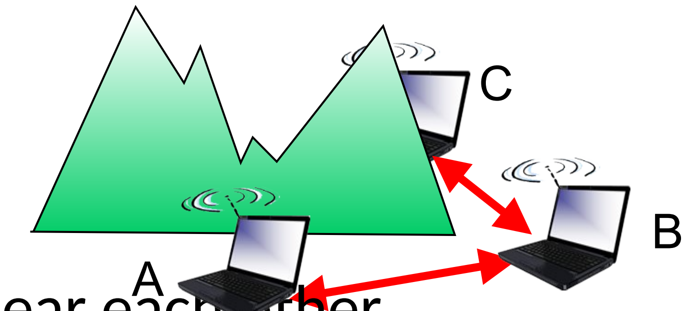
CSMA/CA: addressing the “hidden terminals” problem

Path loss causes “hidden terminals”



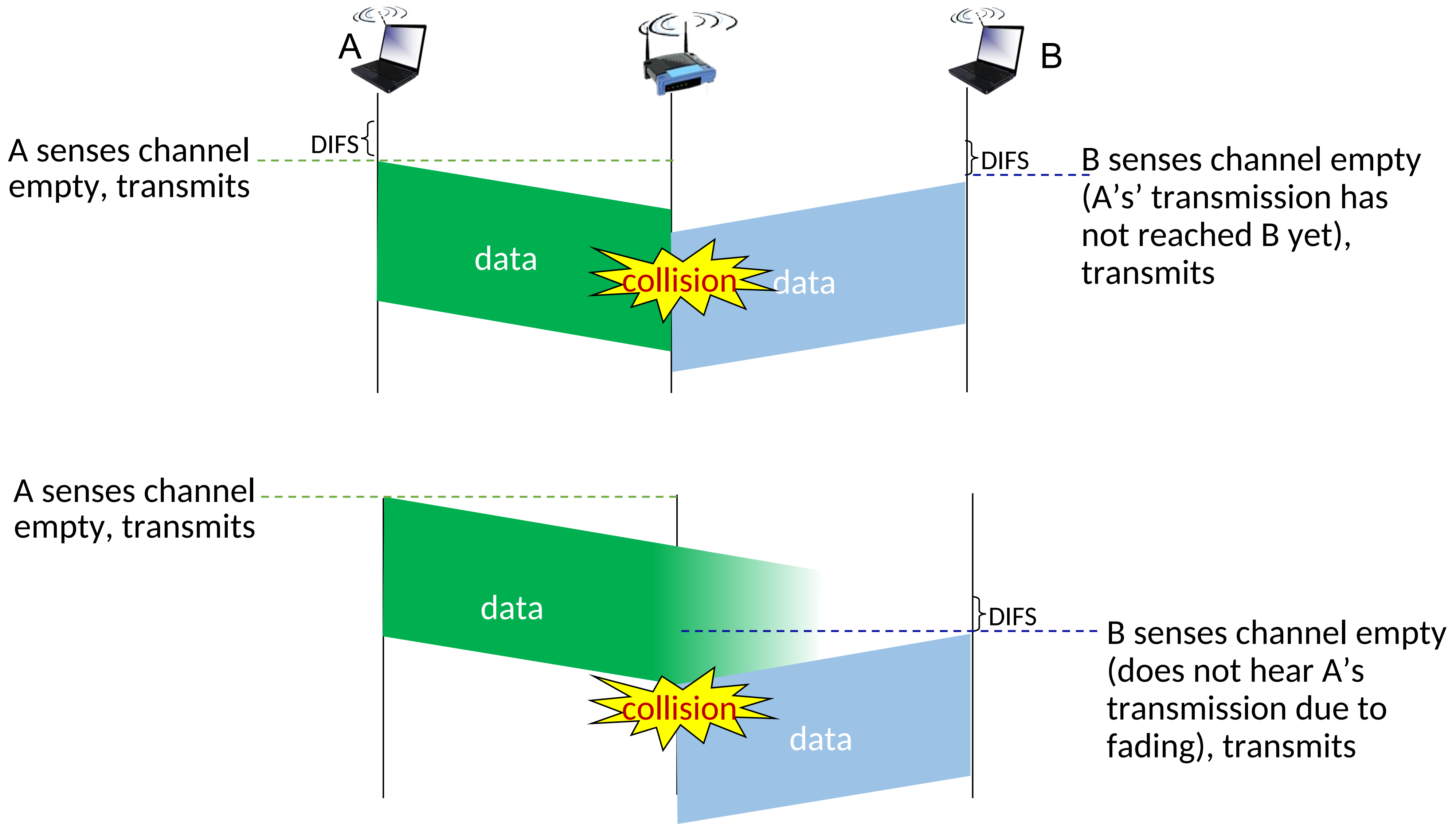
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Objects cause ”hidden terminals”



- 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

CSMA/CA: collisions happen



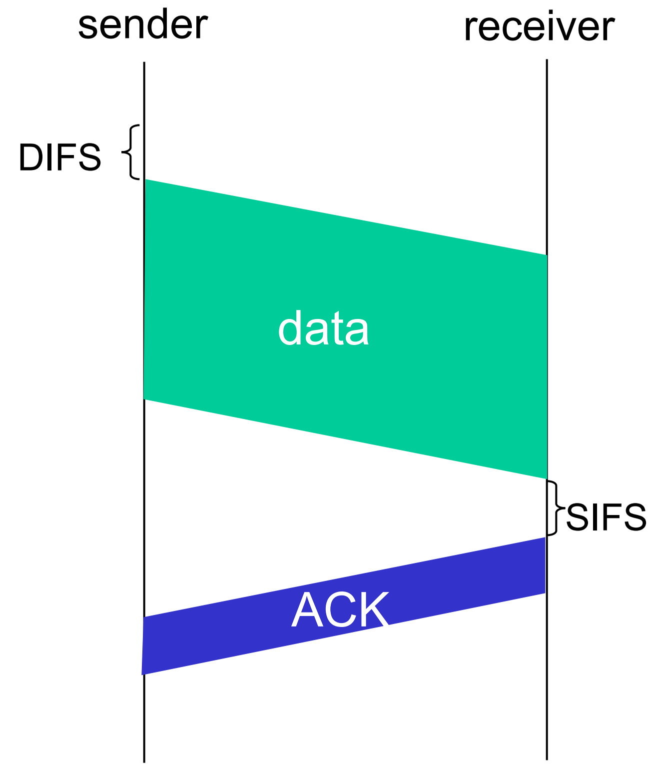
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then
transmit *entire* frame (no collision detection)

2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires

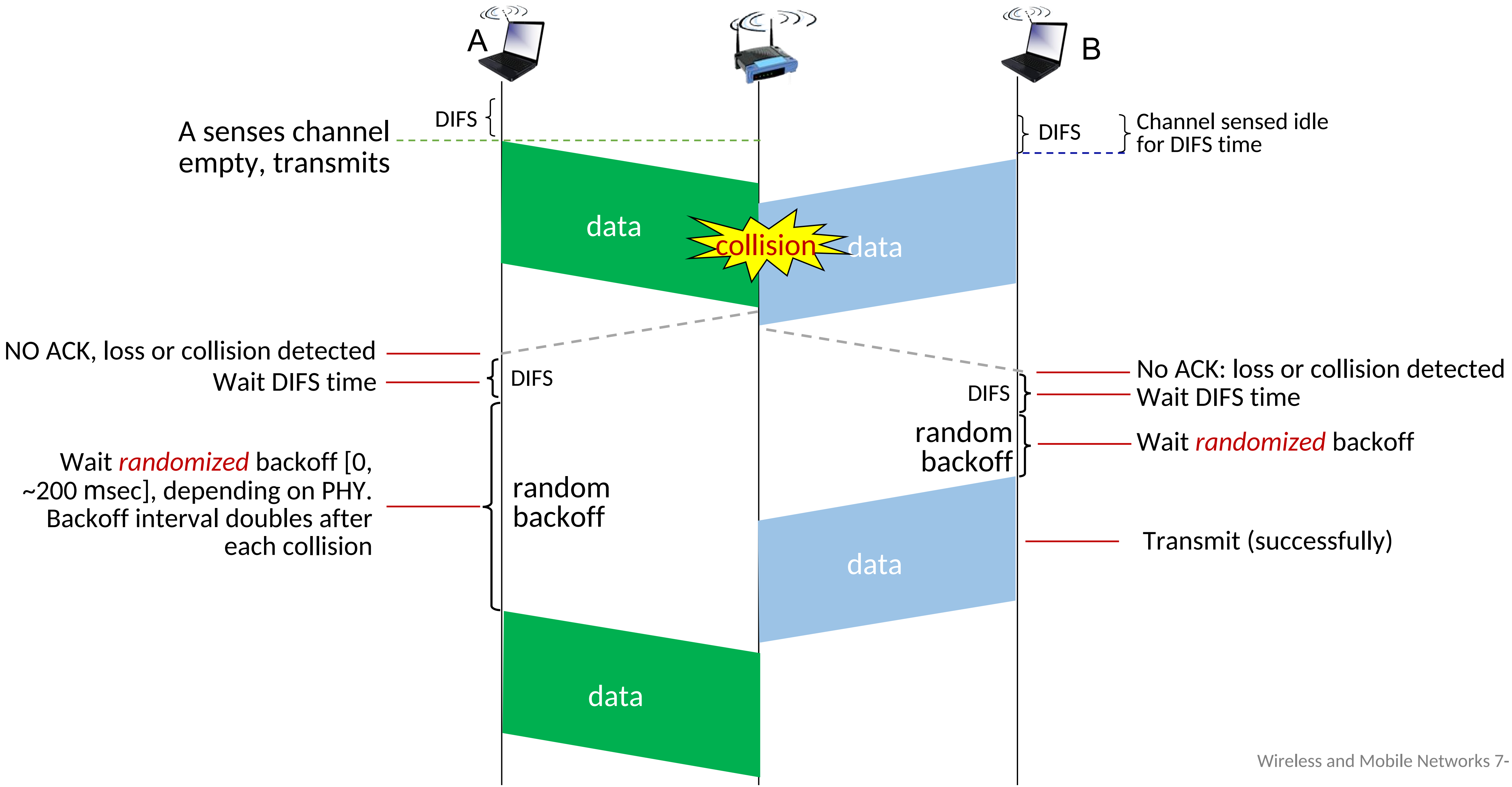
3. if no ACK, increase random backoff interval,
repeat 2 (see next slide)



802.11 receiver

if frame received OK
return ACK after **SIFS** (ACK needed due to hidden terminal problem)

CSMA/CA: randomization after collision

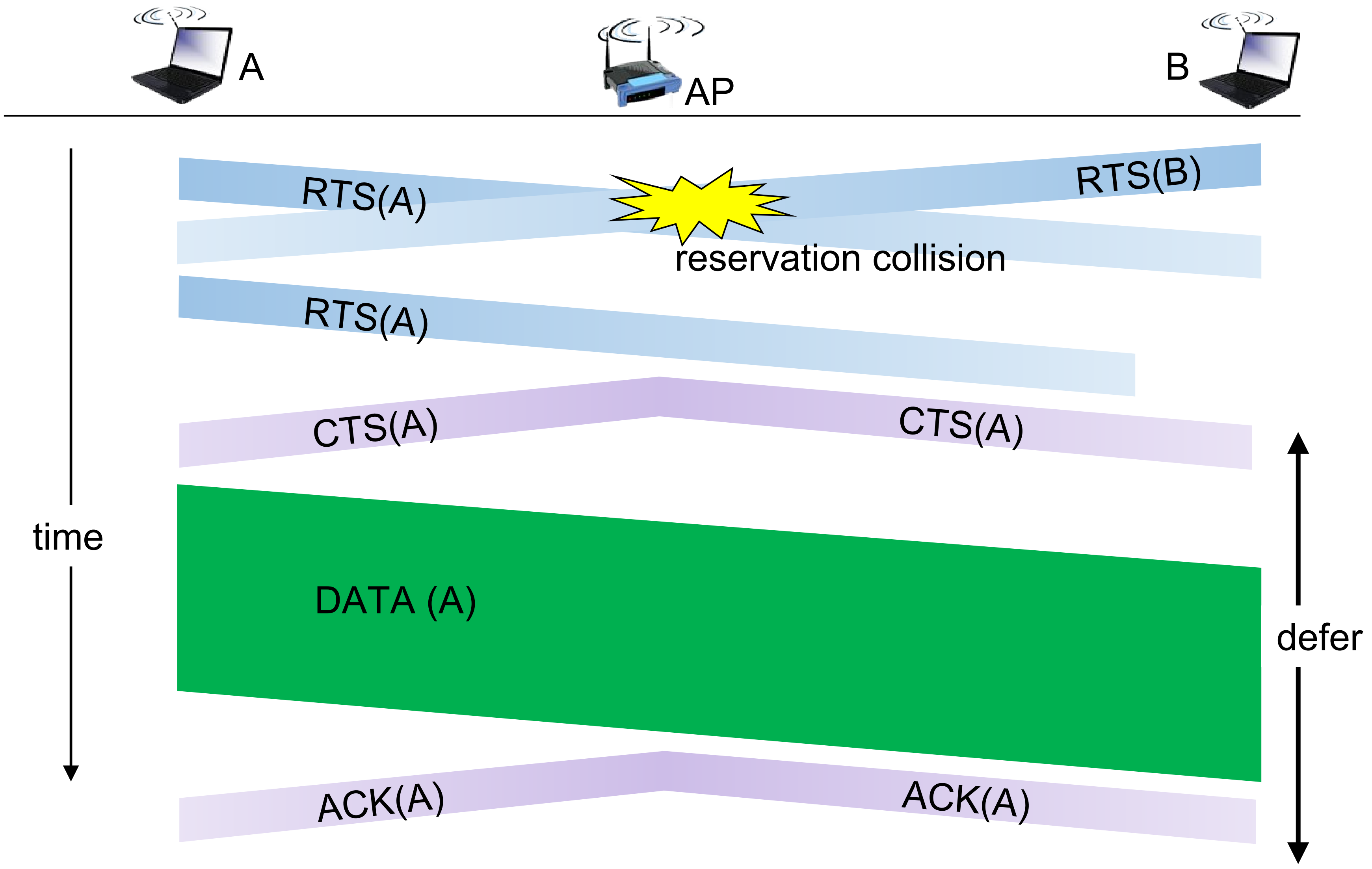


Avoiding collisions: using RTS/CTS

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)
  - contains duration for following data transmission
- BS broadcasts clear-to-send (CTS) packet in response to RTS
  - contains duration for following data transmission
- RTS and/or CTS heard by all nodes
  - All nodes except transmitter defer transmissions
  - transmits data frame

Collision Avoidance: RTS-CTS exchange



Backwards compatibility: challenging

IEEE standard	WiFi gen	Year	Max data rate (theoretical)	Frequency (GHz)	Bandwidth	PHY
802.11b		1999	11 Mbps	2.4	22	spread spectrum
802.11g		2003	54 Mbps	2.4	20	OFDM
802.11n	WiFi 4	2009	600 Mbps	2.4, 5	20, 40	OFDM
802.11ac	WiFi 5	2013	6.9 Gbps	5	20, 40, 80,160	OFDM, MIMO
802.11ax	WiFi 6	2020	9.5 Gbps	2.4, 5	20, 40, 80,160	OFDM, OFDMA, MIMO
802.11be	WiFi 7	2024	30+ Gbps	2.4, 5, 6	20, 40, 80,160, 320	OFDM, OFDMA, MIMO

Challenge: WiFi 6/7 APs support OFDM (FDMA) and OFDMA (FDMA+TDMA)

- How can a WiFi 6/7 AP do *both* FDMA and TDMA at the same time?
- How can WiFi 6/7 AP support user device radios that only do FDMA?

Extending RTS/CTS: Multiuser RTS

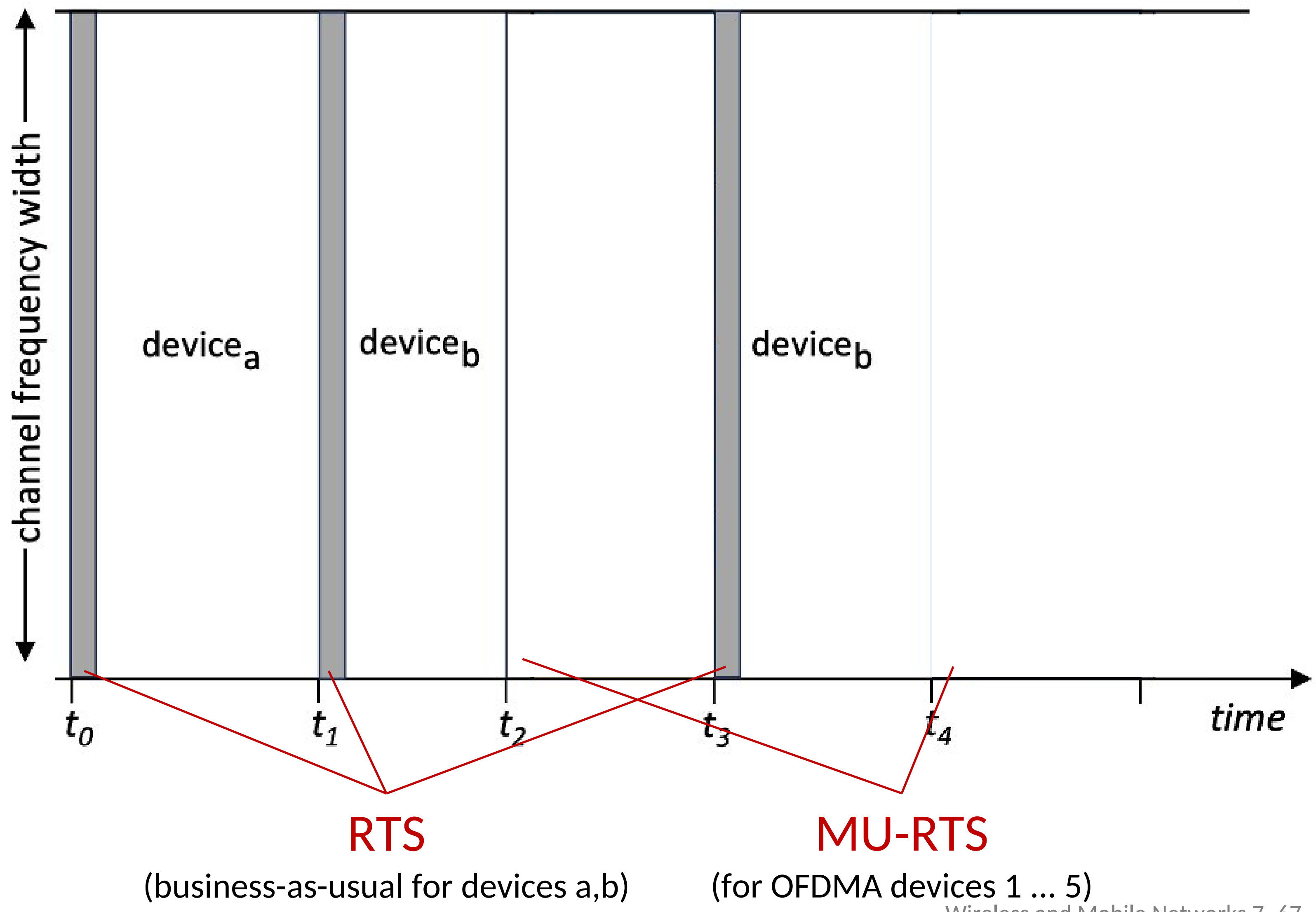
idea: create new type of RTS message Multiuser RTS (MU-RTS)

- transmitter must use MU-RTS before OFDMA transmissions
- transmit MU-RTS using full FDMA channel, with duration info (as usual)
  - heard by all 802.11* devices (both OFDM- and OFDMA-capable)
  - contains additional OFDMA assignment info for receivers (so receivers will know which OFDMA RUs to listen to)
- receivers respond with CTS, sent on assigned OFDMA subchannel
- transmitter sends resource blocks to OFDMA receivers, according to assignment

Extending RTS/CTS: Multiuser RTS

Example scenario:

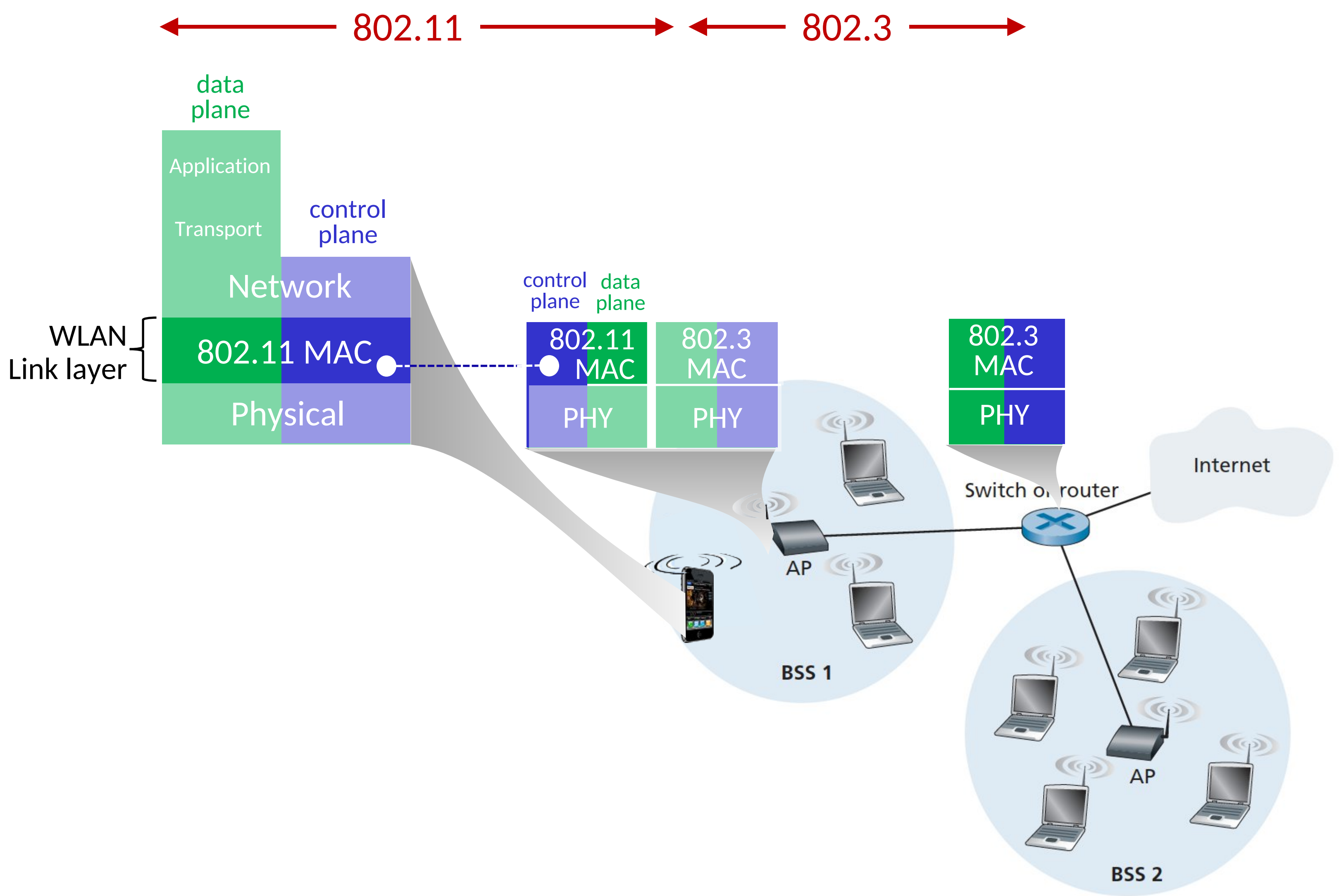
- AP wants to send to seven devices
- two legacy devices a, b (OFDM only)
- five OFDMA-capable devices 1, … 5



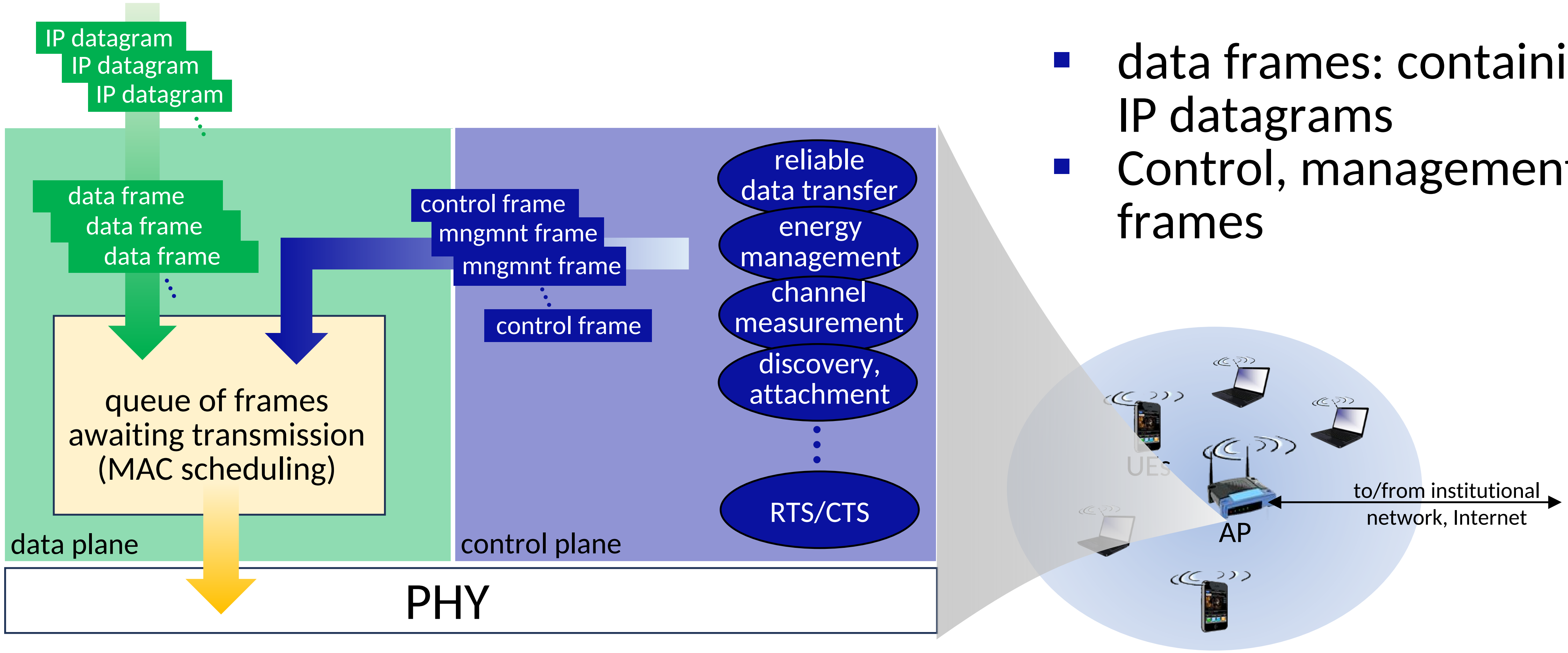
Chapter 7 outline

- introduction
- radio: the physical layer
- the wireless *access* network
  - sharing a wireless access channel: OFDMA, CSMA/CA
  - WiFi wireless LAN
  - 5G radio access network
- the wireless core network
  - principles, 5G
- mobility
- Bluetooth, satellite, IoT wireless networks

802.11 wireless link layer



802.11 downlink (AP-to-device) frame flow



- data frames: containing IP datagrams
- Control, management frames

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

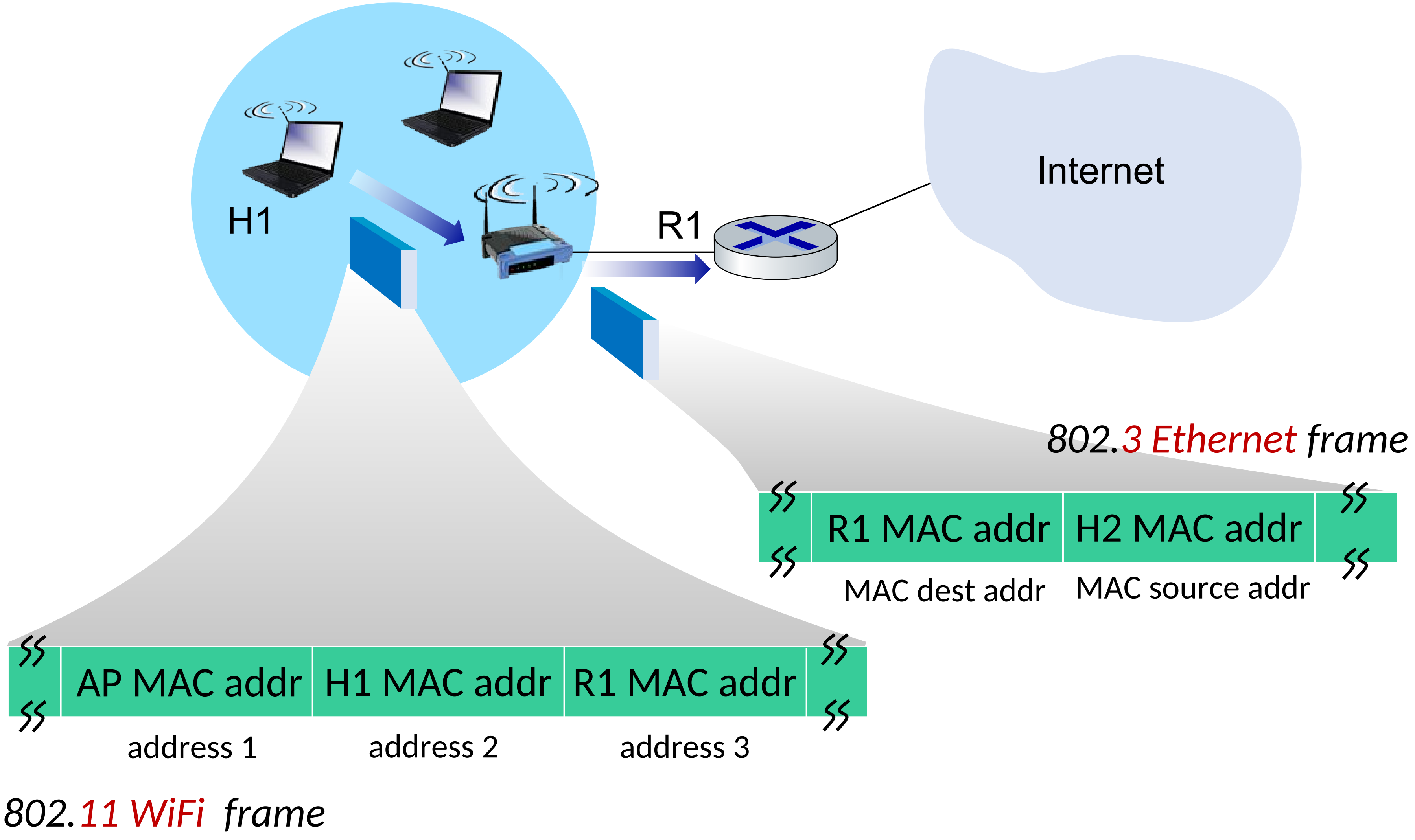
Address 1: MAC address of wireless host or AP to receive this frame

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

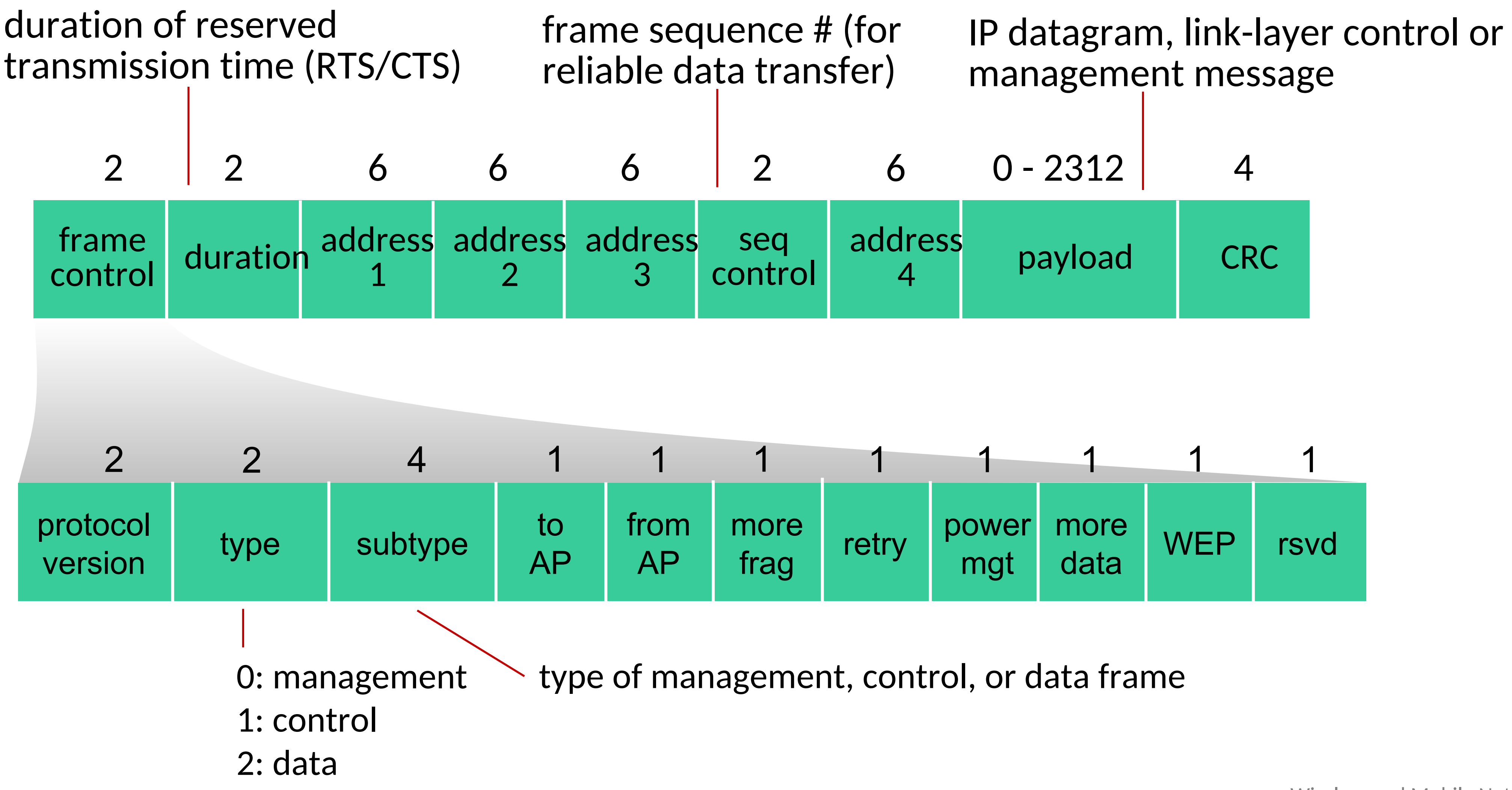
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

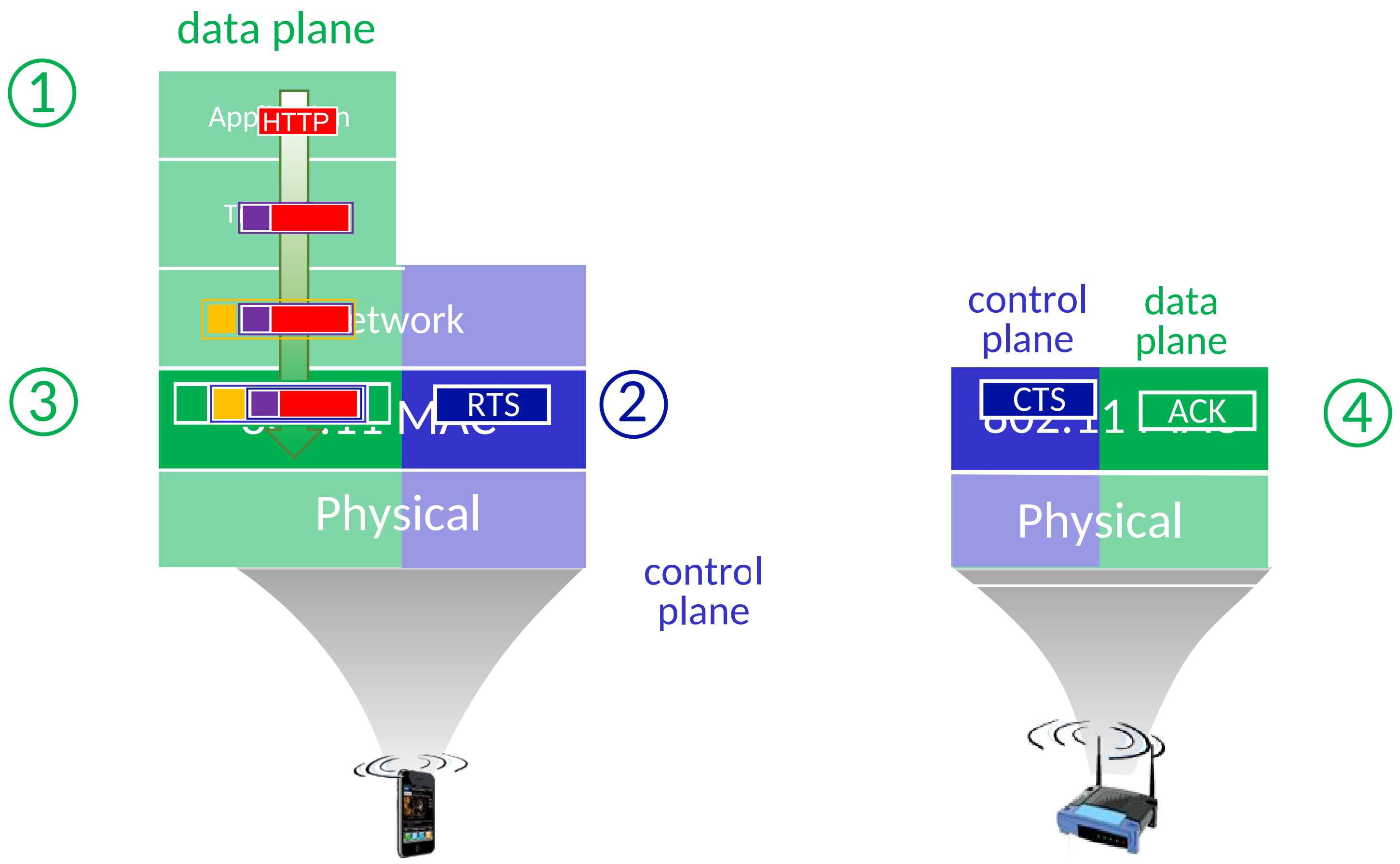
802.11 frame: addressing



802.11 frame


duration of reserved transmission time (RTS/CTS)
frame sequence # (for reliable data transfer)
IP datagram, link-layer control or management message
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
2
2
4
1
1
1
1
1
1
1
1
protocol version
type
subtype
to AP
from AP
more frag
retry
power mgt
more data
WEP
rsvd
0: management
1: control
2: data
type of management, control, or data frame

Retrospective: "A day in the life"* (WiFi)



1. HTTP/3 request in UDP segment, in IP datagram, into 802.11 frame. Enter, wait, MAC frame scheduling queue
2. Device sends RTS control frame (using CSMA/CA); AP responds with CTS.
3. Device sends DATA frame to AP. Buffers DATA frame
4. AP responds with ACK, device removes transmitted frame

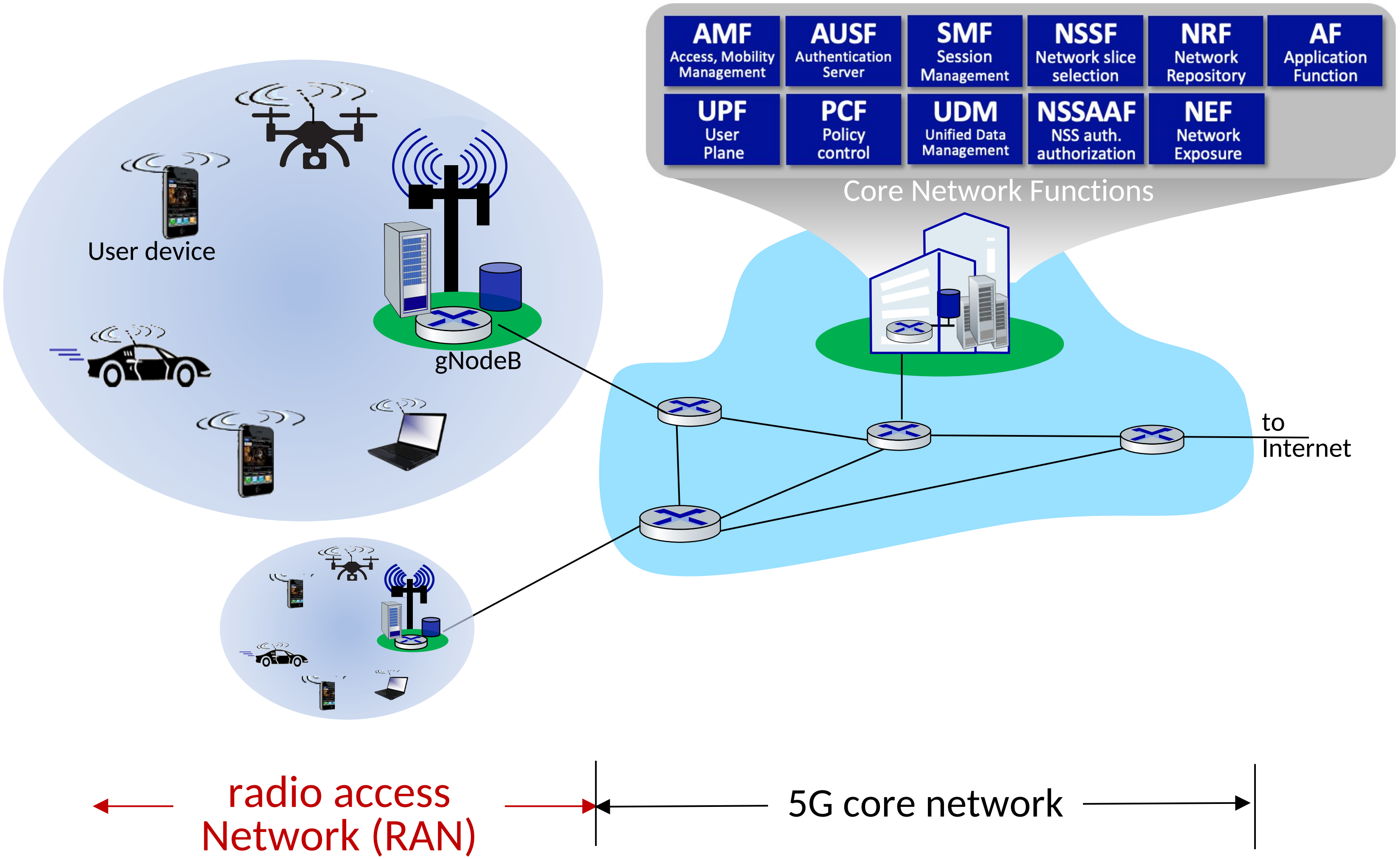
AP can now forward frame to router

*https://gaia.cs.umass.edu/kurose_ross/videos/6/

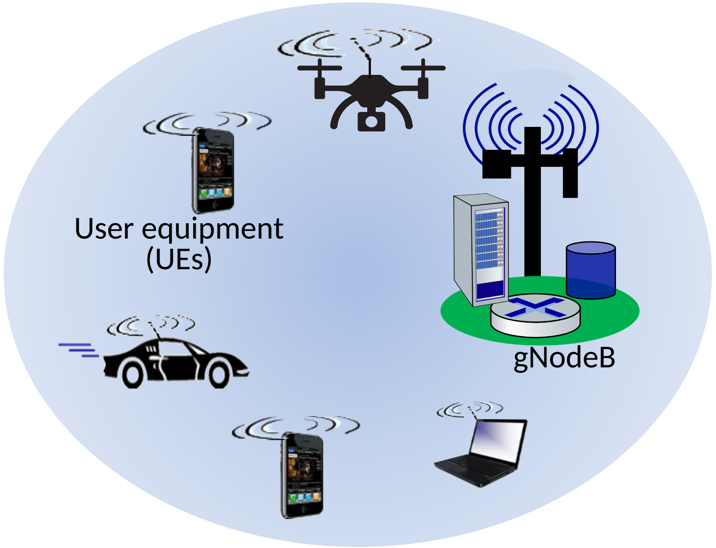
Chapter 7 outline

- introduction
- radio: the physical layer
- the wireless *access* network
  - sharing a wireless access channel: OFDMA, CSMA/CA
  - WiFi wireless LAN
  - 5G radio access network (RAN)
- the wireless core network
  - principles, 5G
- mobility
- Bluetooth, satellite, IoT wireless networks

Architectural Elements of 5G



5G Radio Access Network (RAN)

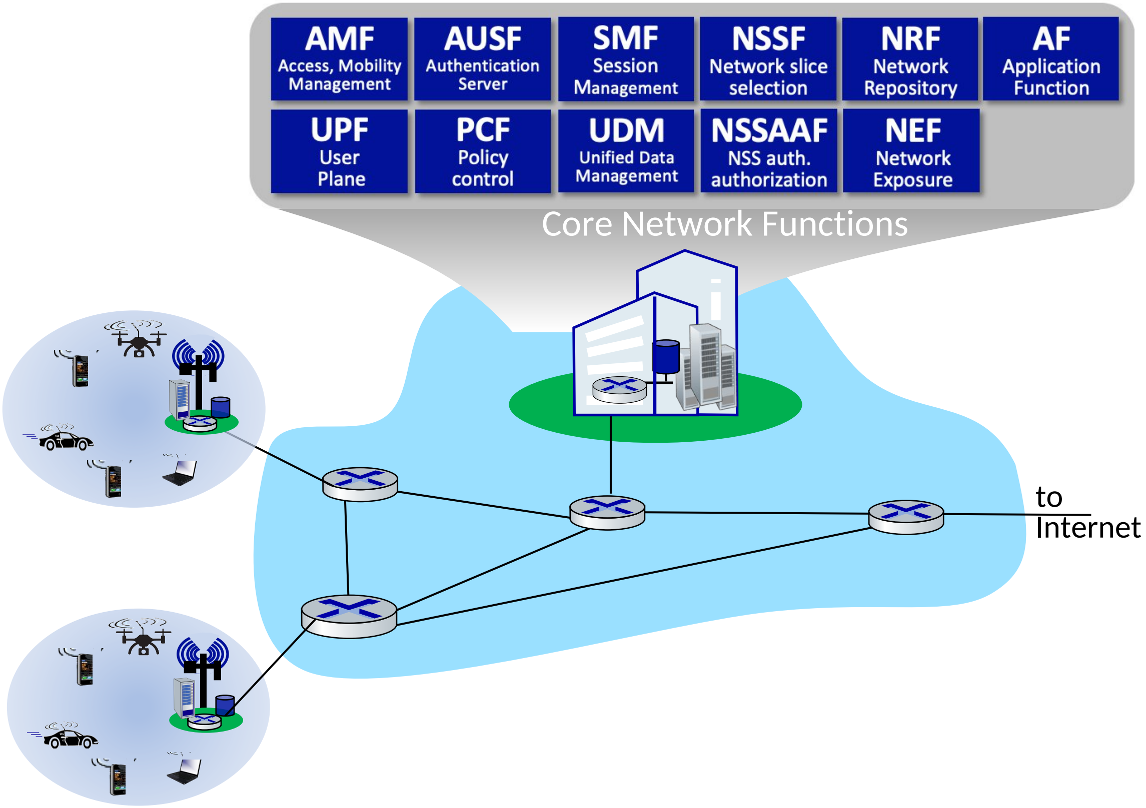


5G RAN: edge network connecting devices to base station

- provides link-layer service, as first hop between devices and larger network
- limited geographic scope
- under control of a single service provider
- somewhat analogous to WiFi LAN
- RAN components:
  - many devices (User Equipment: UE)
  - radio channel (New Radio: NR)
  - one base station (Next Generation Node B: gNodeB, gNB)

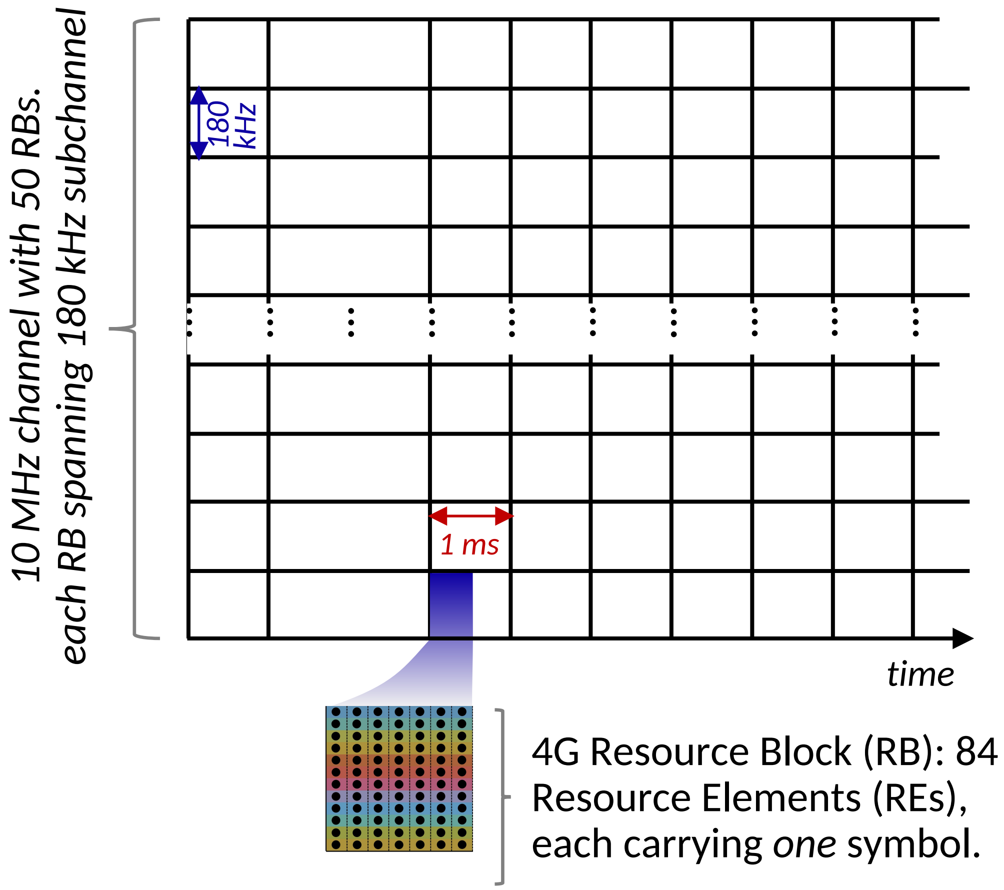
5G Core Network

- Core situated between RAN and other endpoints (Core, larger Internet)
  - single Core; multiple RANs
- consist of links, routers, servers, providing services to devices and base stations
  - "all IP" Core, but very different services than traditional Internet apps
- clear logical separation between control-plane, user plane:
  - *CUPS:* Control-Plane and User-Plane Separation

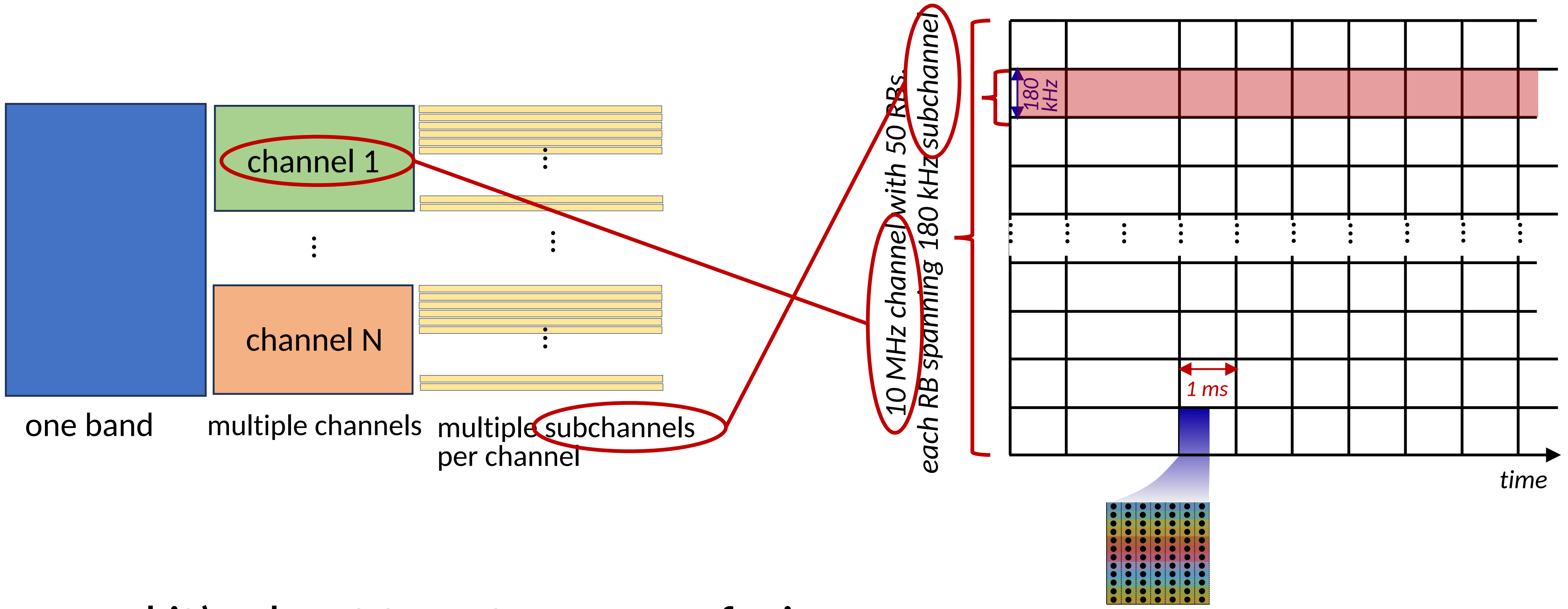


Resource Blocks (RB)

- Resource Element (RE): holds one transmitted OFDMA symbol, in one time minislot on one subcarrier frequency
- Resource Block (RB): bundle of neighboring (time, frequency) Resource Elements
  - 4G: 84 symbols (12 neighboring subcarriers, 7 consecutive minislots)
  - 5G: multiple bundlings possible
  - *RB is smallest unit of transmission scheduling: all symbols in RB have same source, destination*

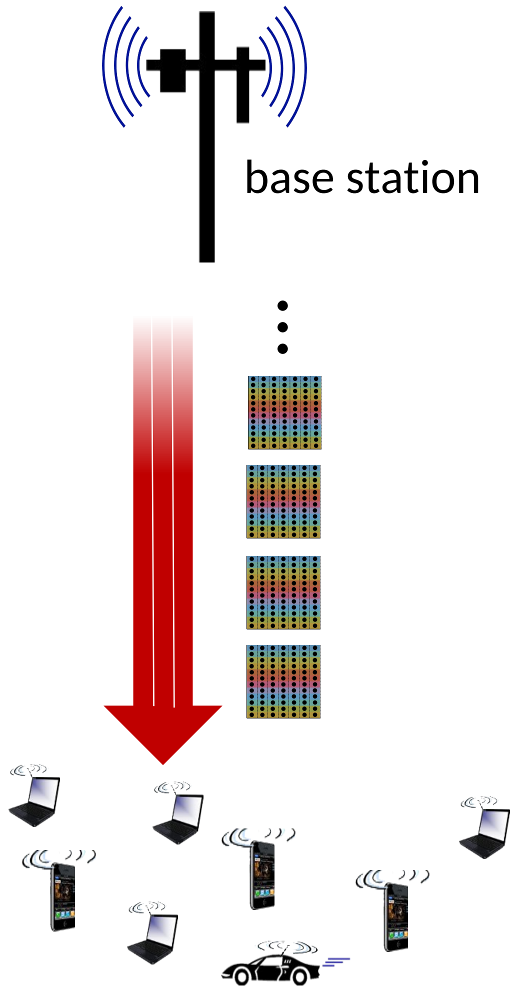


5G Bands, Channels, Subchannels: it confusing!



… and it's about to get *more* confusing

Downlink physical channels

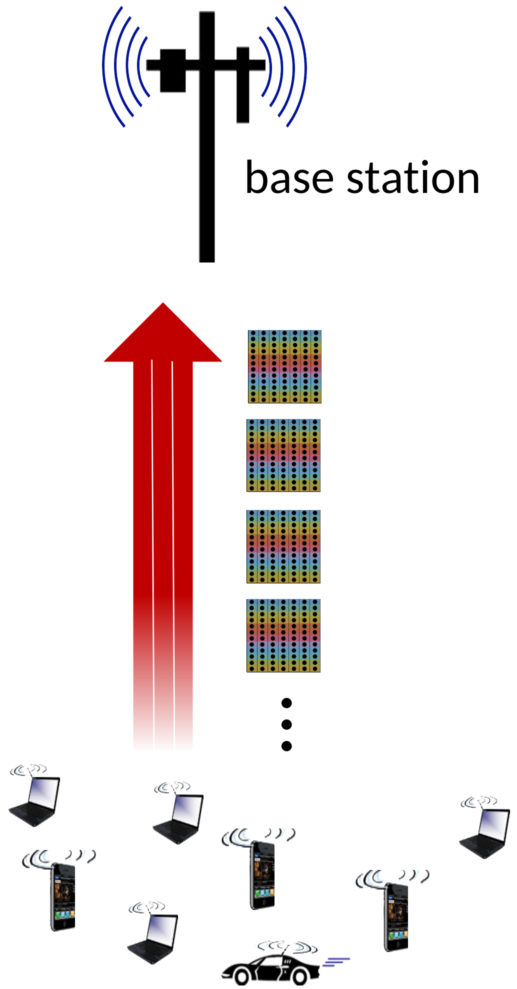


Physical channel

set of Resource Blocks (RBs) carrying similar type of data (channel information RBs, user and control RBs, RB allocation information)

- downlink RBs transmitted from base station to devices
- three 5G downlink physical channels:
  - Physical Downlink Shared Channel (PDSCH)
  - Physical Downlink Control Channel (PDCCH)
  - Physical Broadcast Channel (PBCH)

Uplink physical channels

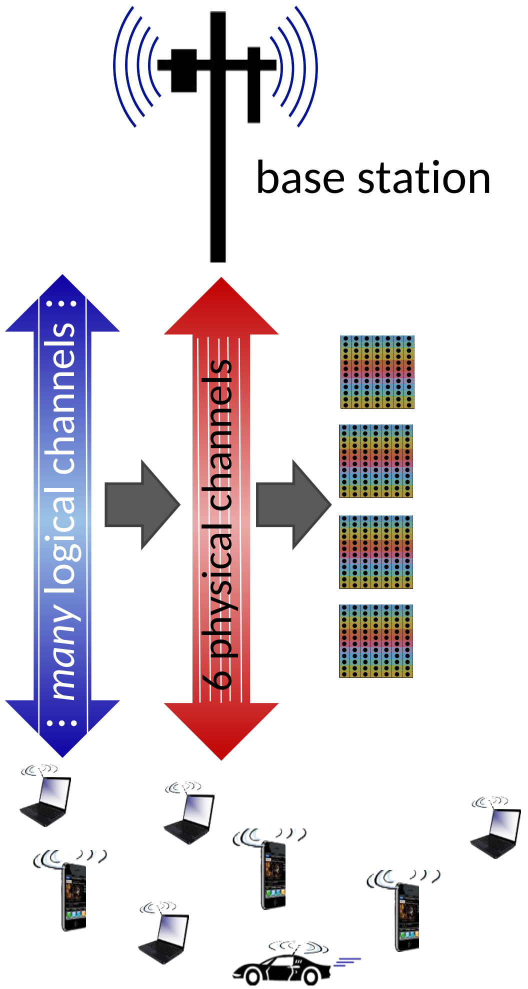


Physical channel

set of Resource Blocks (RBs) carrying similar type of data (radio channel information RBs, user and control RBs, RB allocation information)

- uplink RBs transmitted from devices to base station
- three 5G uplink physical channels:
  - Physical Uplink Shared Channel (PUSCH)
  - Physical Random-Access Channel (PRACH)
  - Physical Uplink Control Channel (PUCCH)

Uplink/downlink *logical* channels

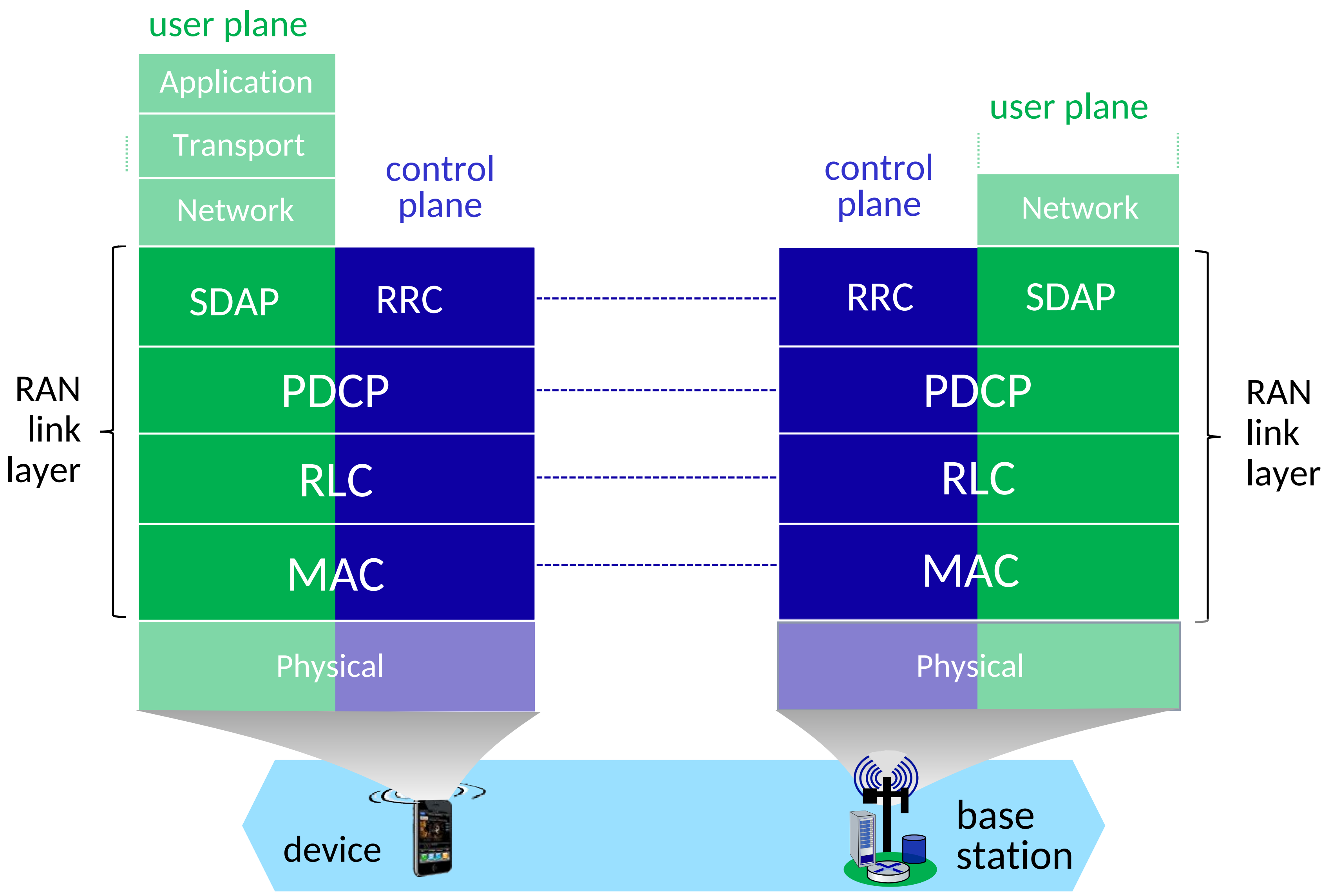


logical channel

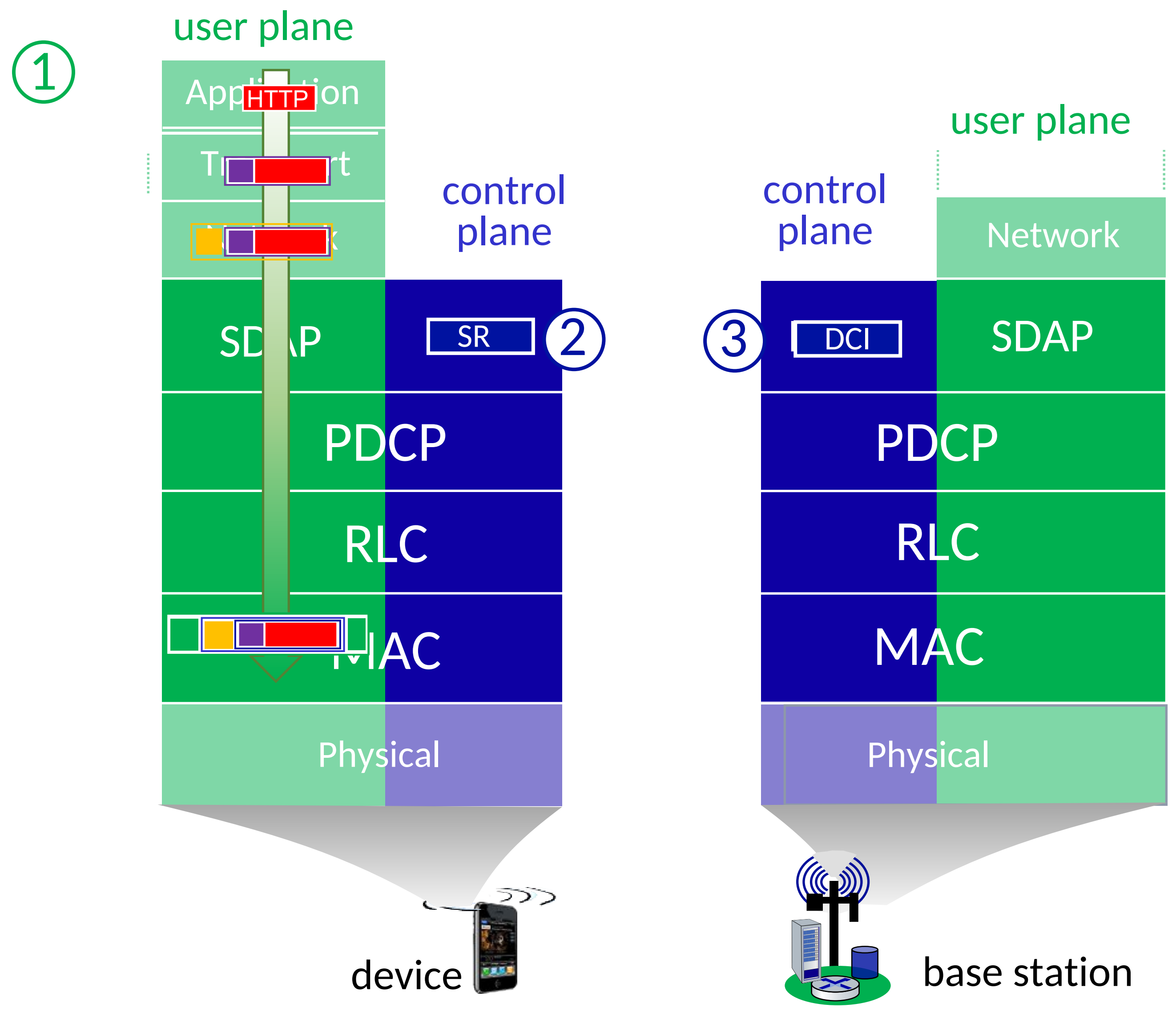
Set of Resource Blocks (RBs) carrying similar type of data. Logical channels are mapped onto physical channels, with one or more logical channel mapped to same physical channel

- individual, per-device logical channels, as well as shared logical channels among devices

RAN protocol stack (at device, base station)



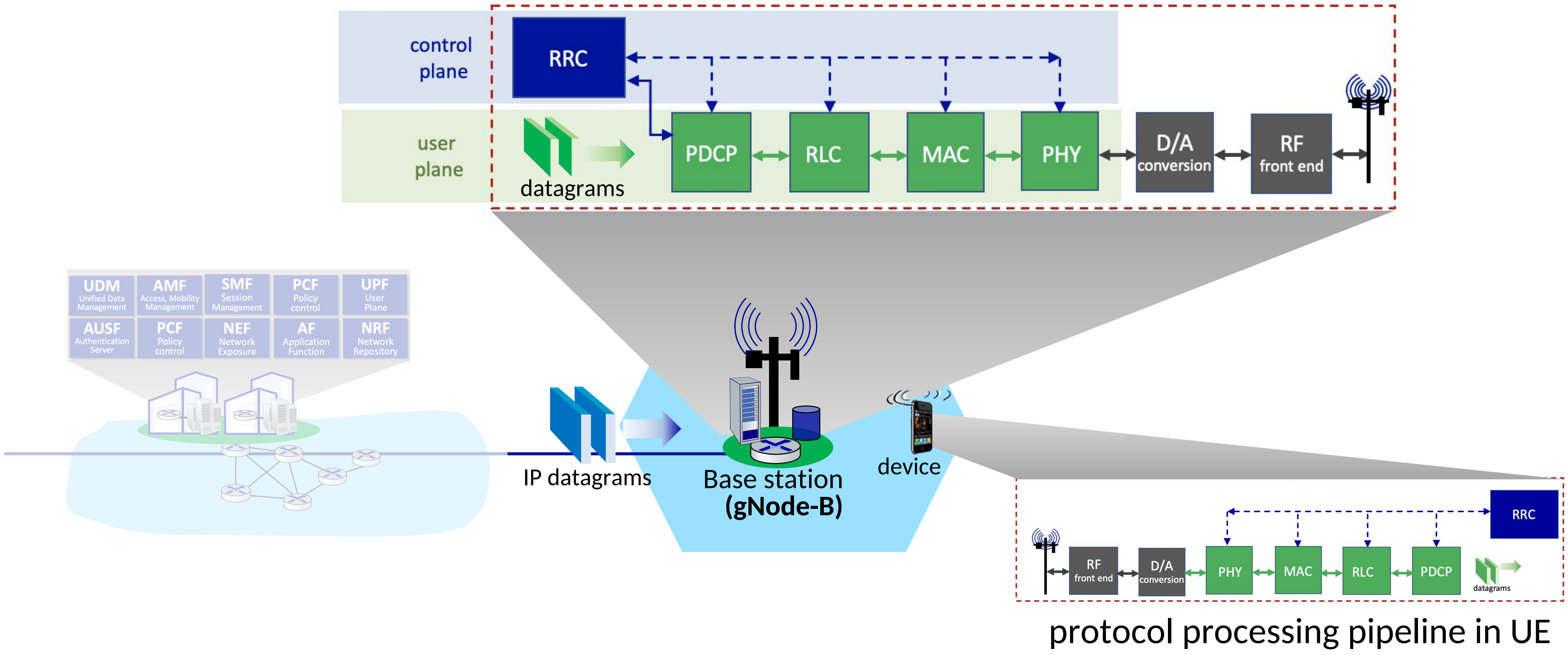
Retrospective: "A day in the life"* (5G RAN)



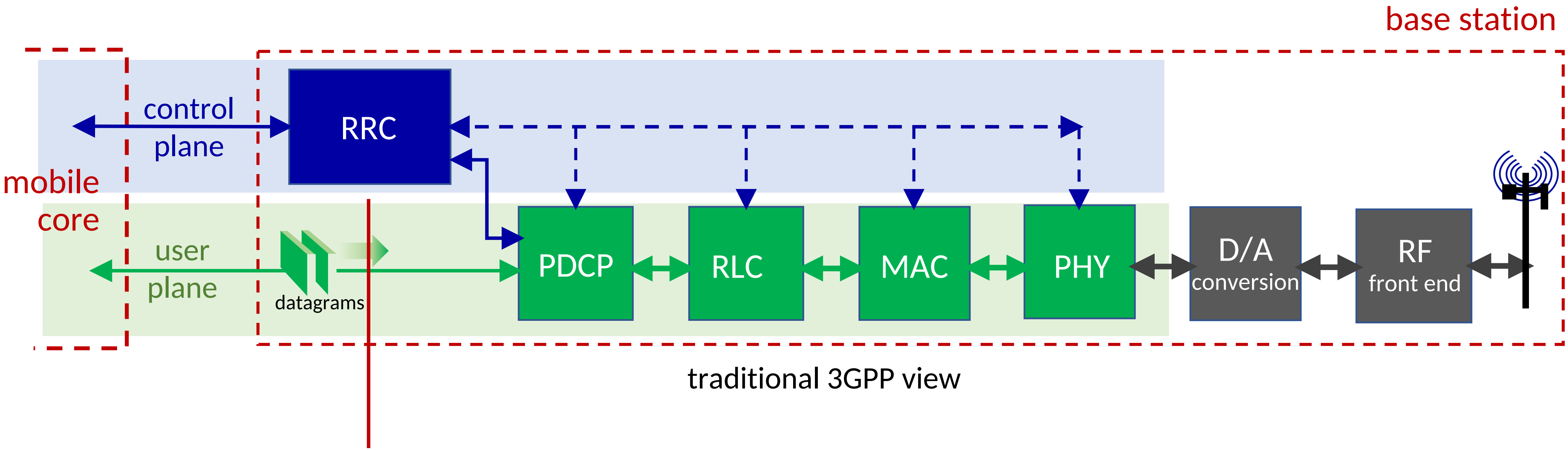
1. HTTP/3 request in UDP segment, in IP datagram, into 5G frame. Enter, wait, 5G MAC frame scheduling queue
2. device's control plane sends SR Scheduling Req) on Physical Uplink Control Channel (PUCCH) to base station
3. base station control plane send DCI message Physical Downlink Control Channel (PDCCH) granting upstream RBs
4. device sends frame in allocated RBs

RAN packet processing pipeline: context

RAN: transfers datagrams between mobile core and devices



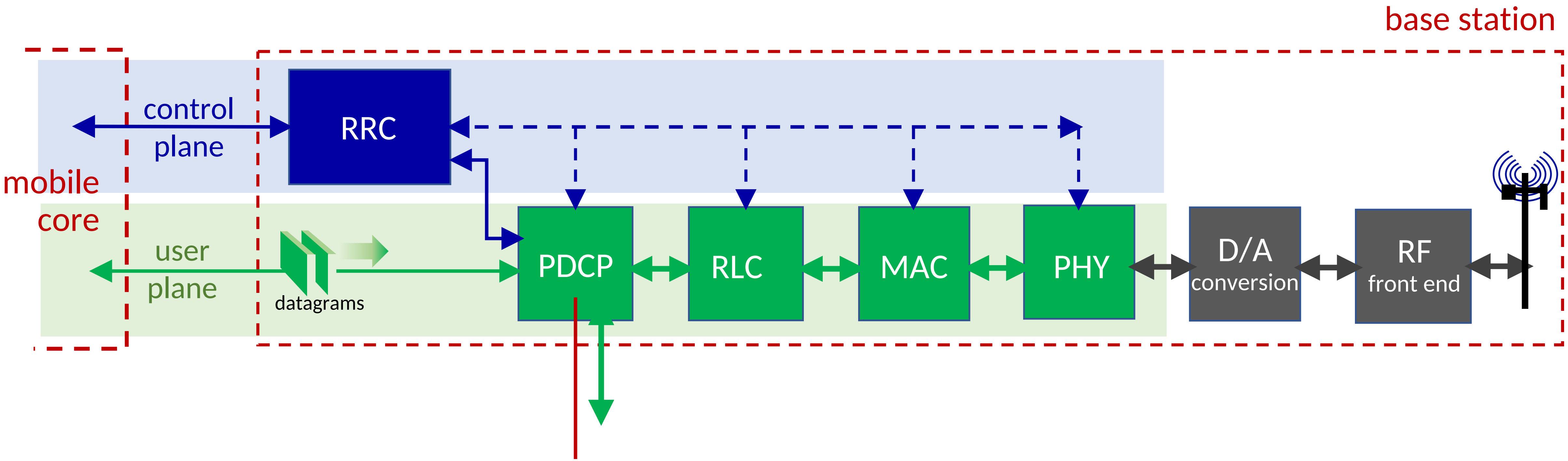
RAN packet processing pipeline



RRC (Radio Resource Control)

- configures coarse-grained, policy-related aspects of pipeline (e.g., scheduling prioritization, security)
- this implements the RAN's control plane
- does not process user plane packets

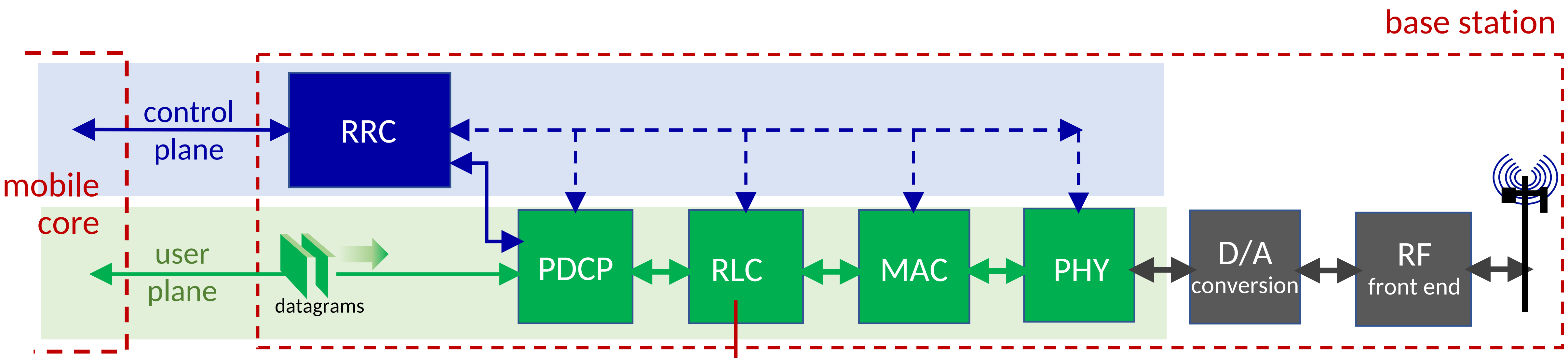
RAN packet processing pipeline



PDCP (Packet Data Convergence Protocol)

- compress/decompress IP headers
- ciphering, integrity protection

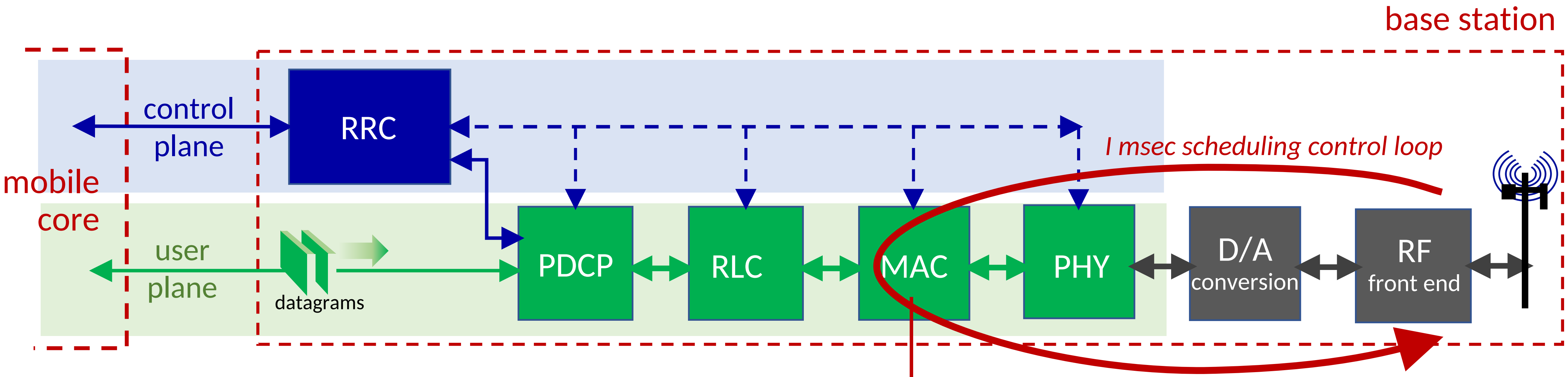
RAN packet processing pipeline

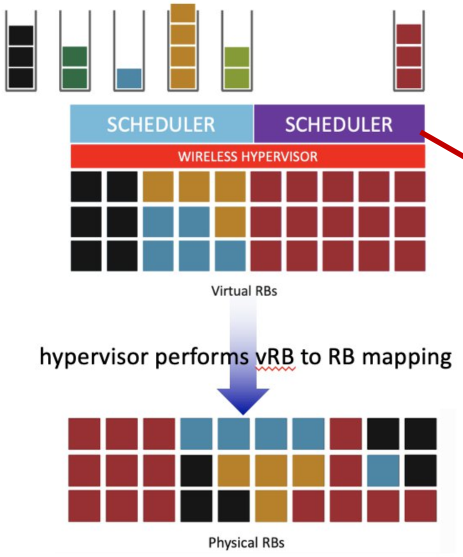


RLC (radio link control)

- link-layer frame segmentation/reassembly
- reliable data transfer (ARQ)

RAN packet processing pipeline

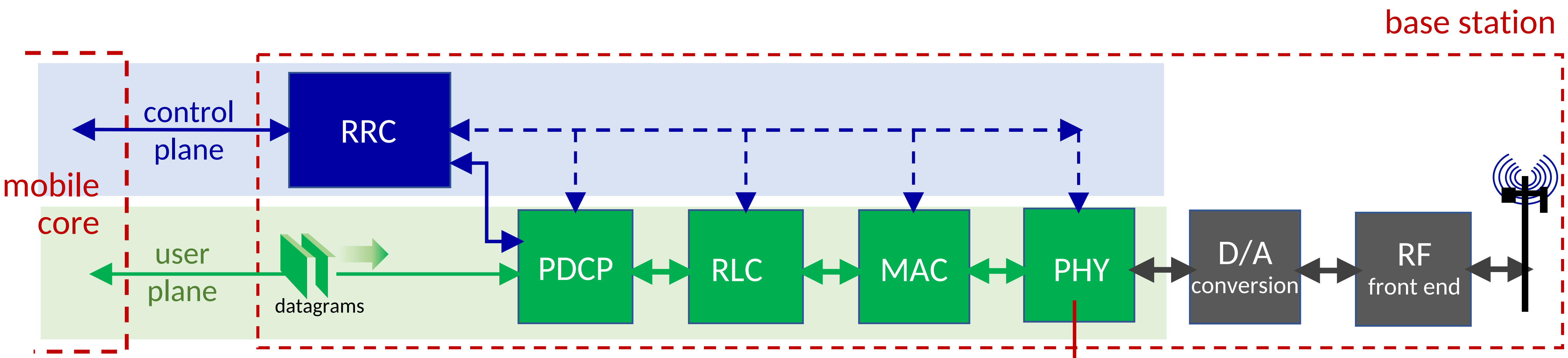




MAC (Media Access Control)

- buffering, multiplexing/demultiplexing frames
- scheduling: real-time scheduling frame decisions

RAN packet processing pipeline

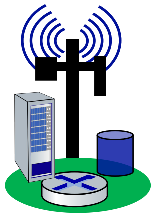


PHY (Physical Layer)

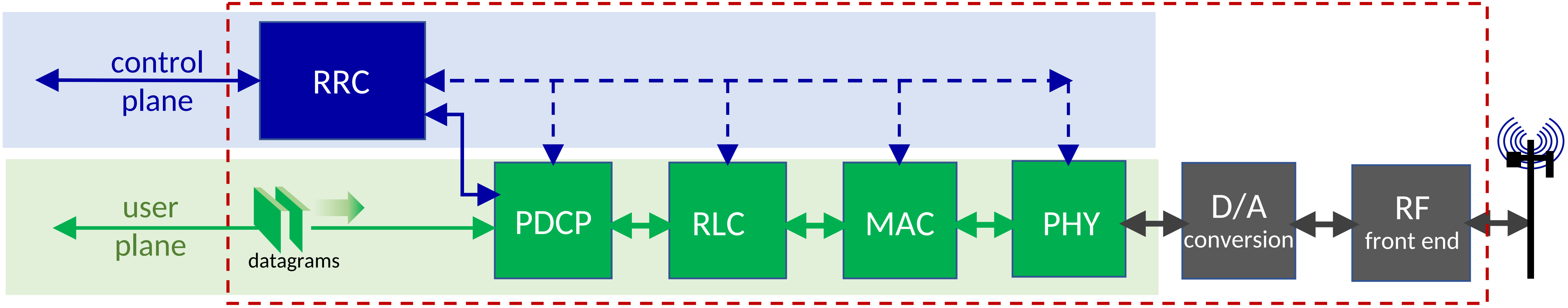
- modulation, coding

Split RAN

- Q: how is RAN *functionality* partitioned between physical elements (i.e.,., "split" across centralized and distributed locations)?
  - historically: no split - implemented in base station

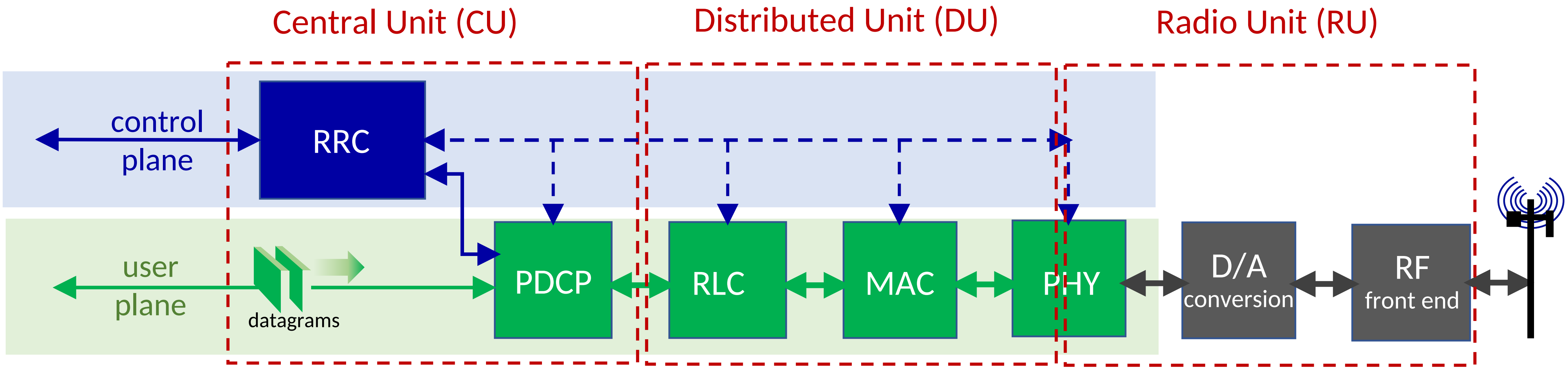


Monolithic base station



Split RAN

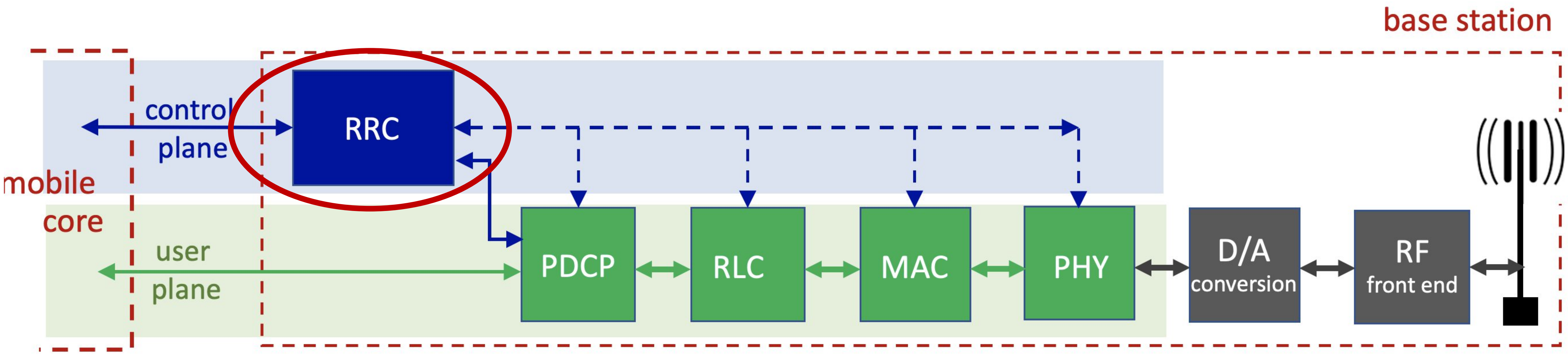
- Q: how is RAN *functionality* partitioned between physical elements (i.e,., “split” across centralized and distributed locations)?
  - historically: no split - implemented in base station
  - O-RAN: three “units” - *where* units are implemented is an *implementation* choice



Software-defined RAN

Recall our earlier description of traditional RAN base station (below)

- tightly coupled control and data planes
- let's focus on control / management: RRC *implementation*

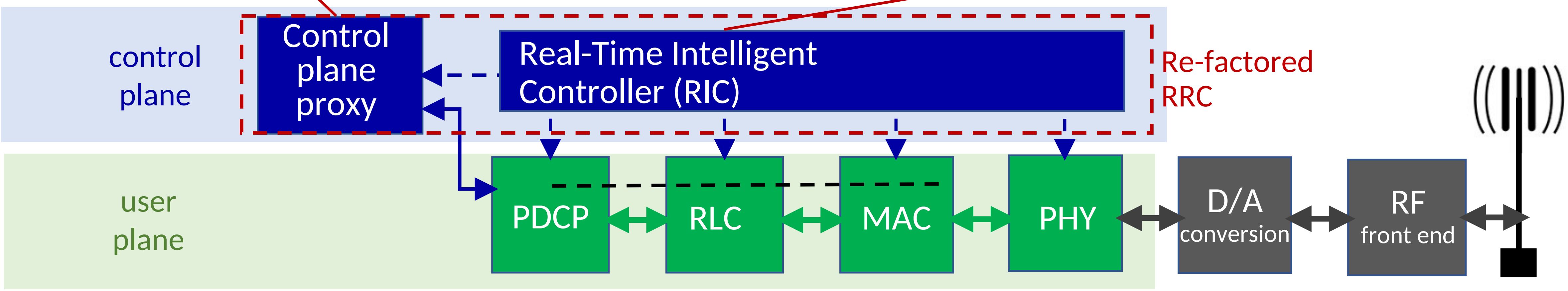


Software-defined RAN

- *SD-RAN:* implementing RAN using SDN approach

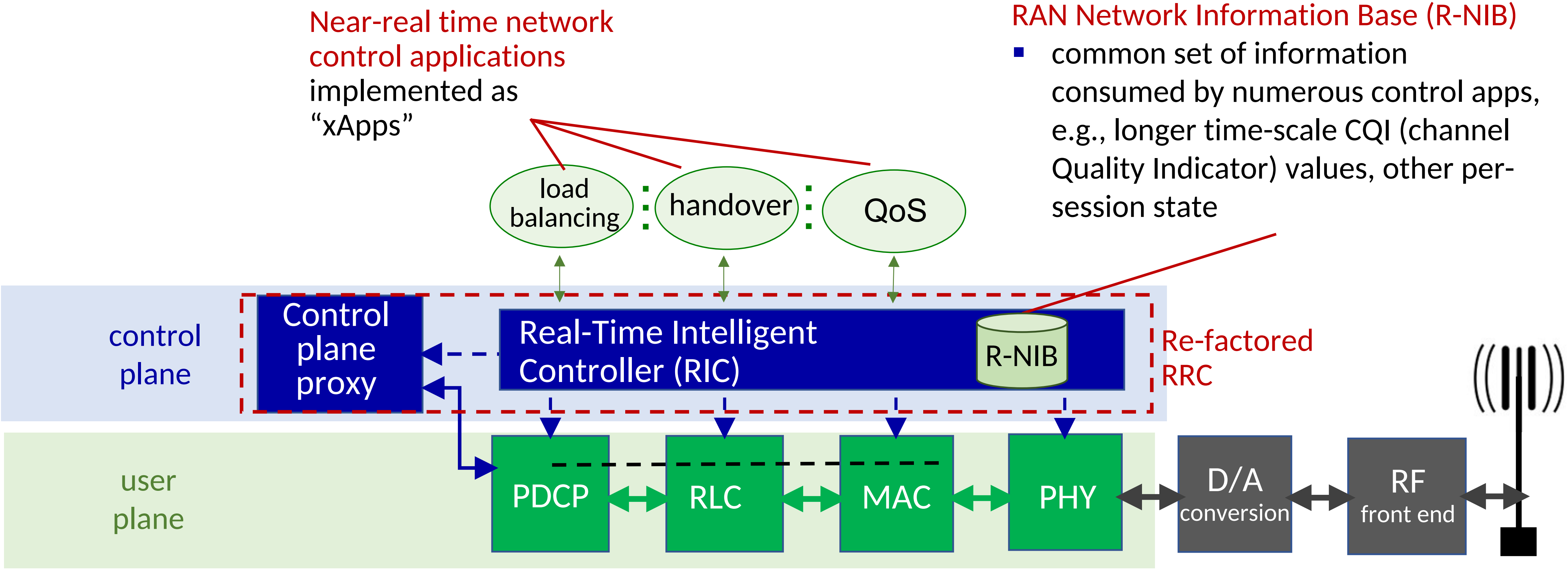
3GPP-compliant interface between RAN and Mobile Core control plane

New programmatic API for exerting software-based control over pipeline that implements RAN user plane



Software-defined RAN

- *SD-RAN:* implementing RAN using SDN approach



RAN: operator's "secret sauce"

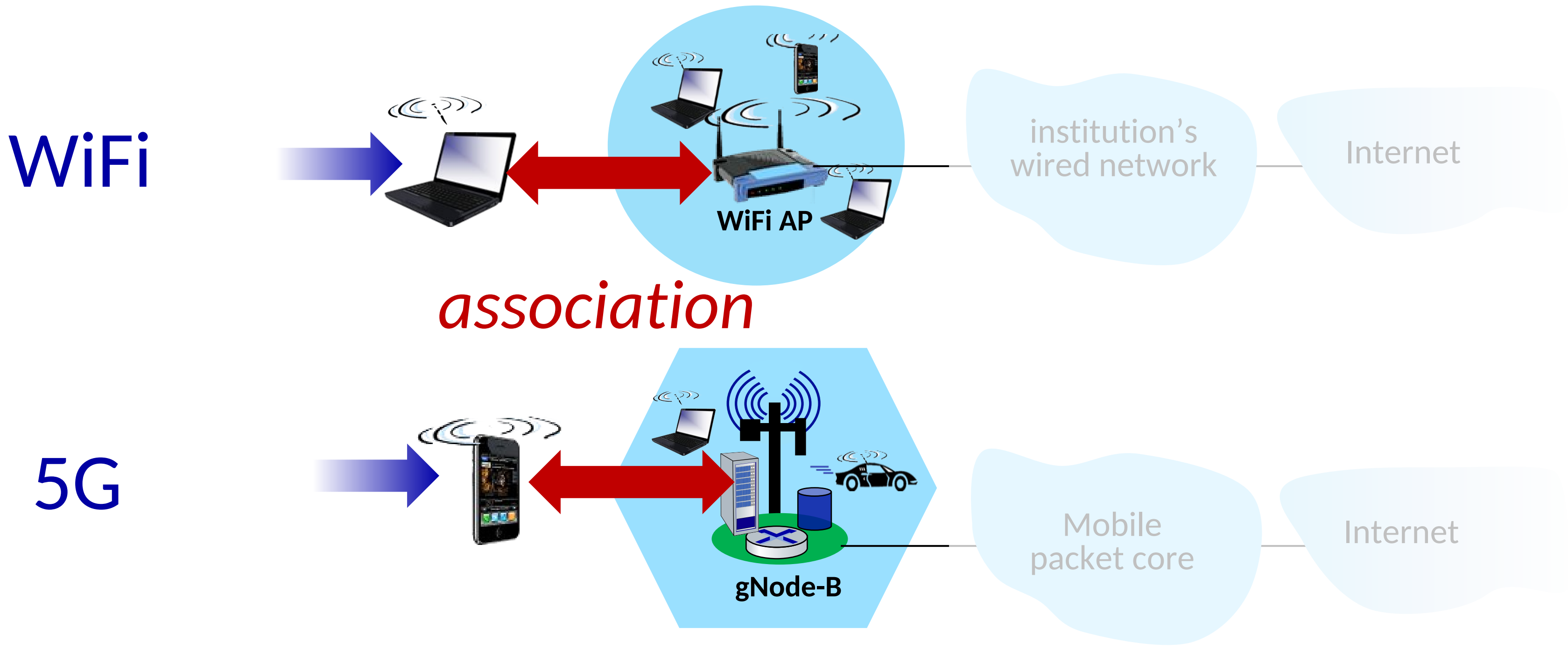
- combination of standardized specifications + implementation strategies:
  - interfaces, high-level functions standardized
  - implementation of some functions, e.g., RB assignment to channels, frame scheduling, not standardized – up to the network operator.
  - *implementation choices are the technical "secret sauces"*

Chapter 7 outline

- introduction
- radio: the physical layer
- the wireless *access* network
  - sharing a wireless access channel
  - WiFi wireless LAN
  - 5G radio access network
  - common challenges: network discovery, frame scheduling, energy
- the wireless core network
  - principles, 5G
- mobility
- Bluetooth, satellite, IoT wireless

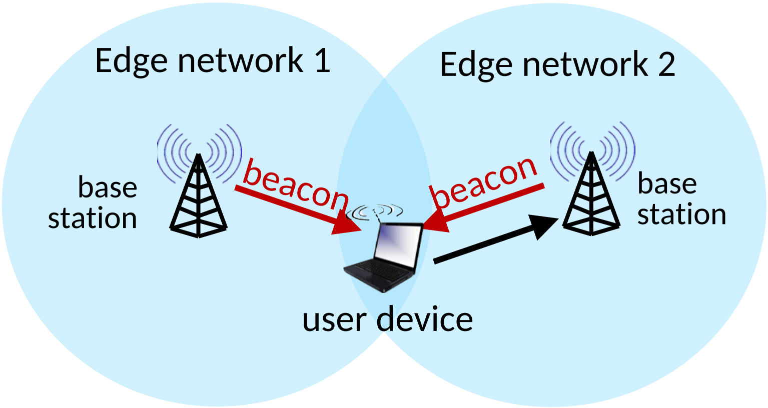
Joining the edge wireless network

- *arriving device:* must establish initial connection with node (WiFi AP, 4G/5G base station) at *wireless edge* of network
  - initial connection then used for authentication, DHCP, gain full network access
  - "bootstrapping" connectivity: *initial connection is just with edge node*

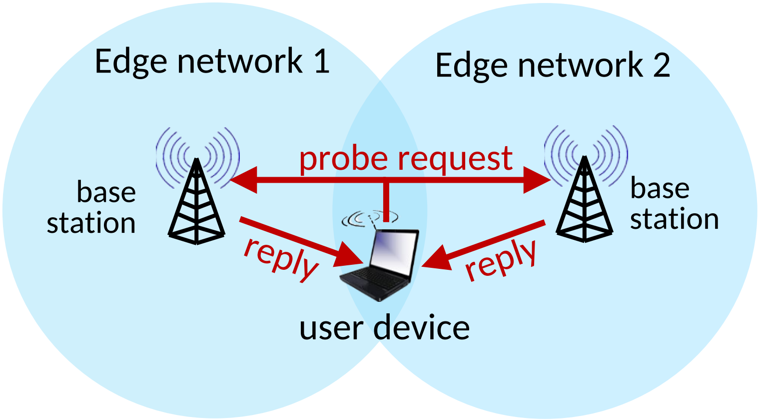


Association: two approaches

Beaconing: mobile listens to wireless channels for "beacons" advertising existence of wireless network node(s)



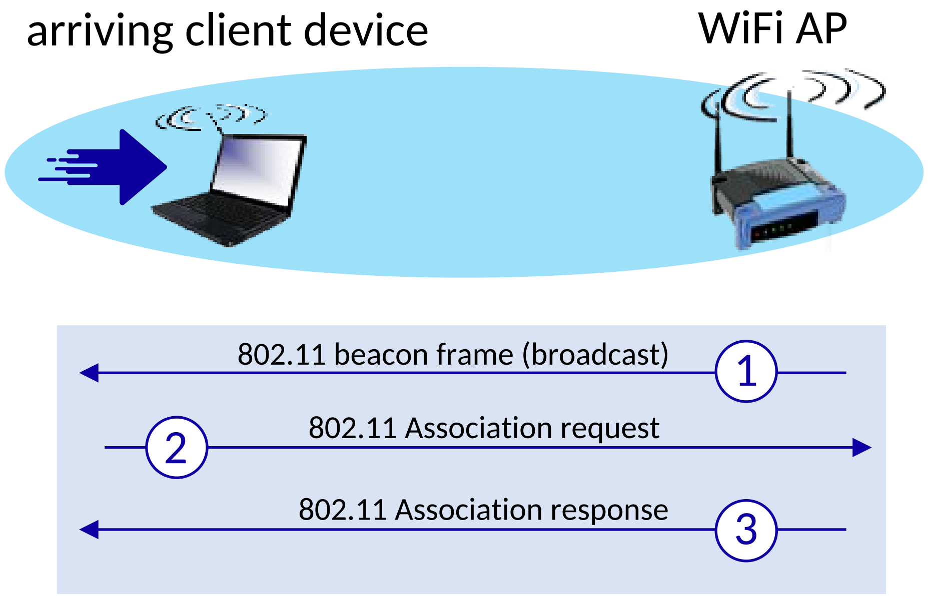
Probing: mobile actively transmits probe messages, waits for wireless network node(s) to reply



Either (or both) approaches used in practice in an edge network

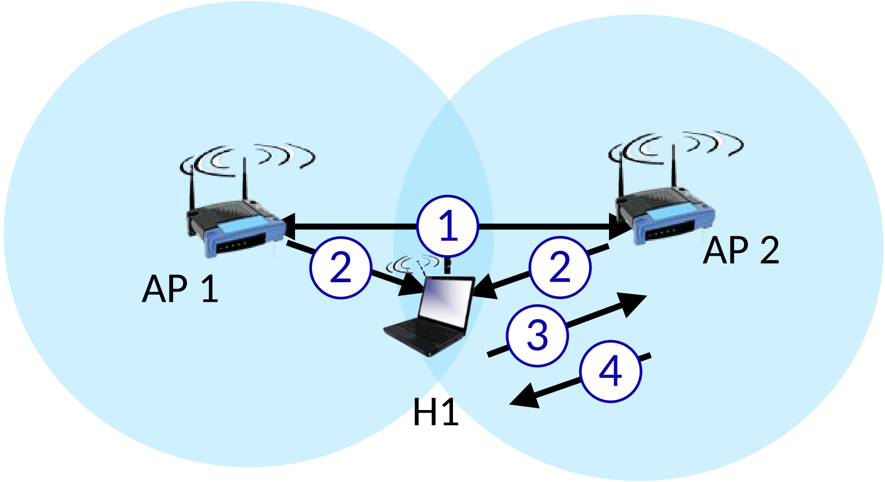
802.11: beaconing and probing

Beaconing:



... device will next authenticate to network

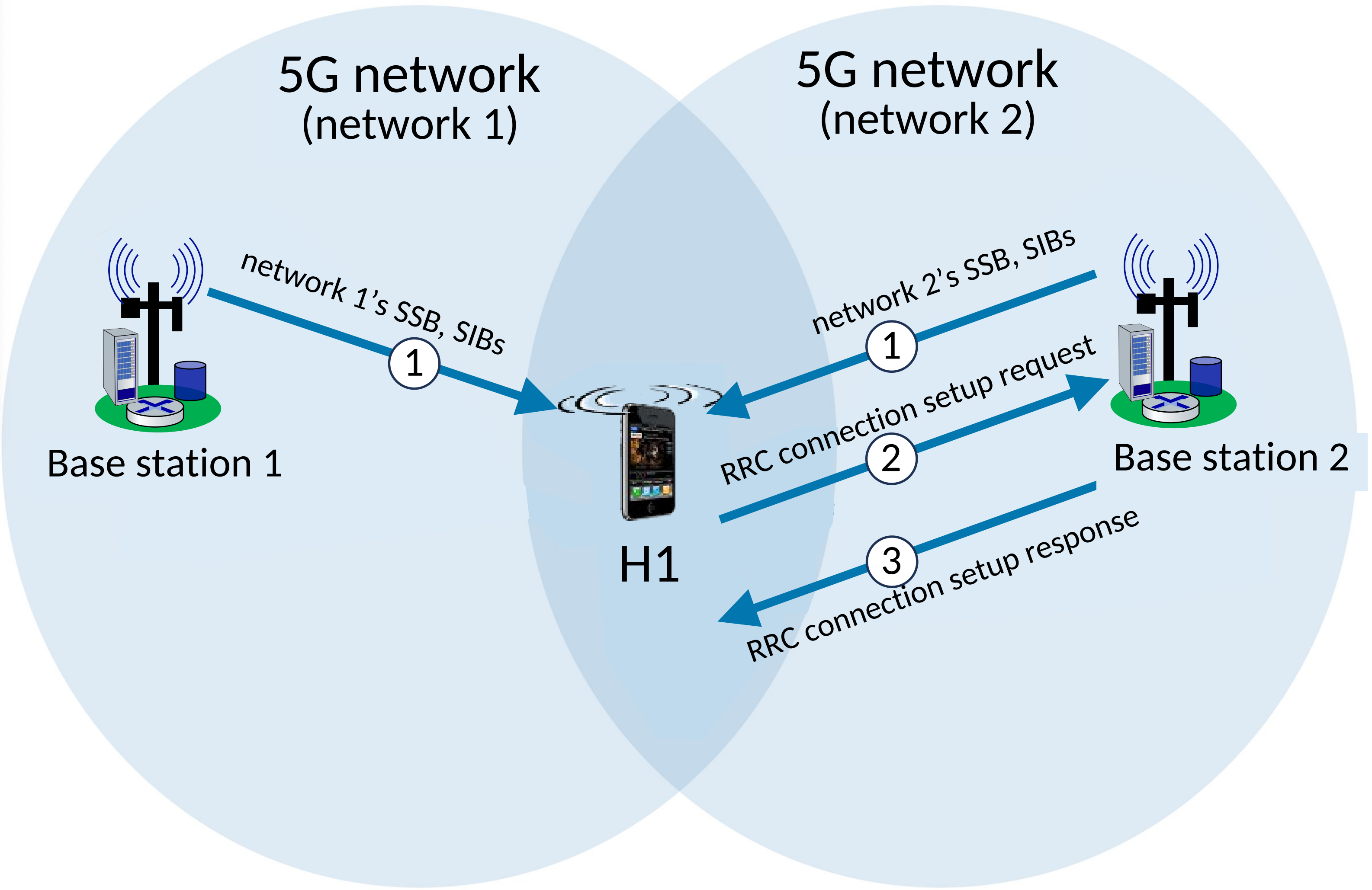
Probing:



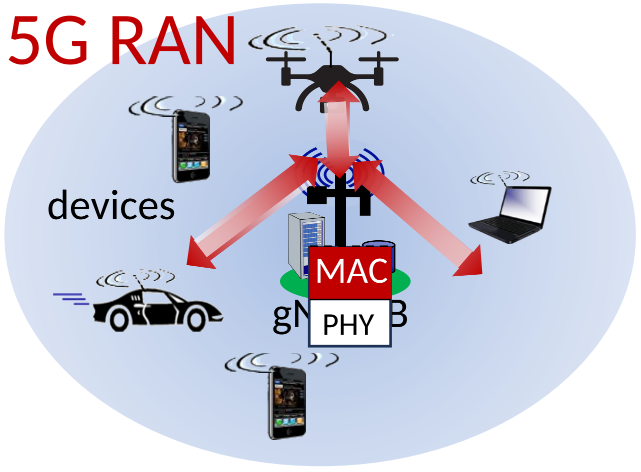
1. Probe Request frame broadcast from H1
2. Probe Response frames sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent from selected AP to H1

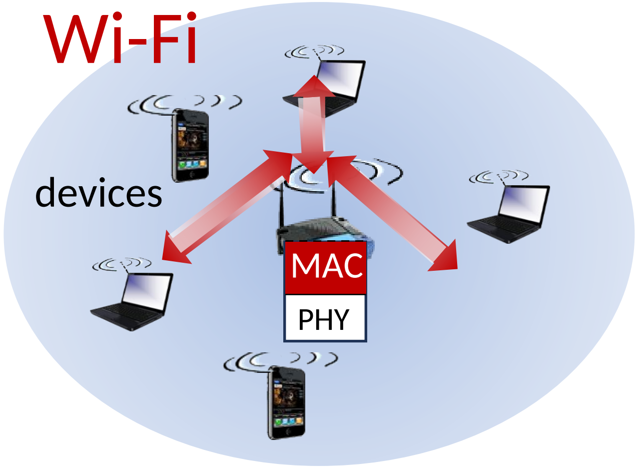
No exchange of identity, credentials (yet)! Just "Can we talk?"

Connecting to the 5G edge



RAN/WLAN scheduling: the "big picture"





All packets to/from all devices in edge network must pass through base station

- 4G/5G and WiFi 6/7: OFDMA RB scheduling
- *downlink MAC scheduler:* which frames to send from base station to which devices in which order in which RBs (if OFDMA)?
- *uplink MAC scheduler:* which devices send which frames in which order in which RBs to base station (if OFDMA)

Wireless MAC scheduling: considerations

Channel aware or channel unaware?

- does scheduler consider quality of channel between base station and device?

QoS aware or QoS unaware?

- does scheduler consider QoS (quality of service) needed by (or guaranteed to) device?

Priorities, Fair scheduling?

- Does scheduler provide priority among different types of traffic (user, control, real-time)?
- does scheduler consider *fairness* among UEs?
- fairness: no standard definition

"We are all equally important"

MAC scheduling considerations

Channel aware or channel unaware?

- does scheduler consider quality of channel between base station and device?

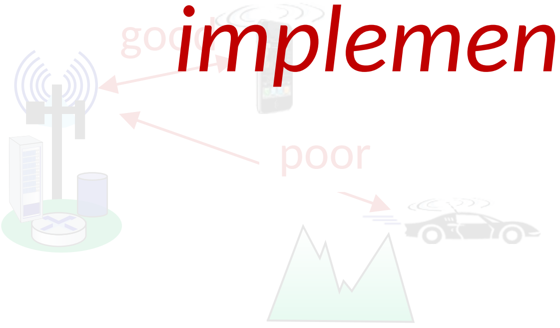
QoS aware or QoS unaware?

- does scheduler consider QoS (quality of service) needed by [illegible] device?

Priorities, Fair scheduling?

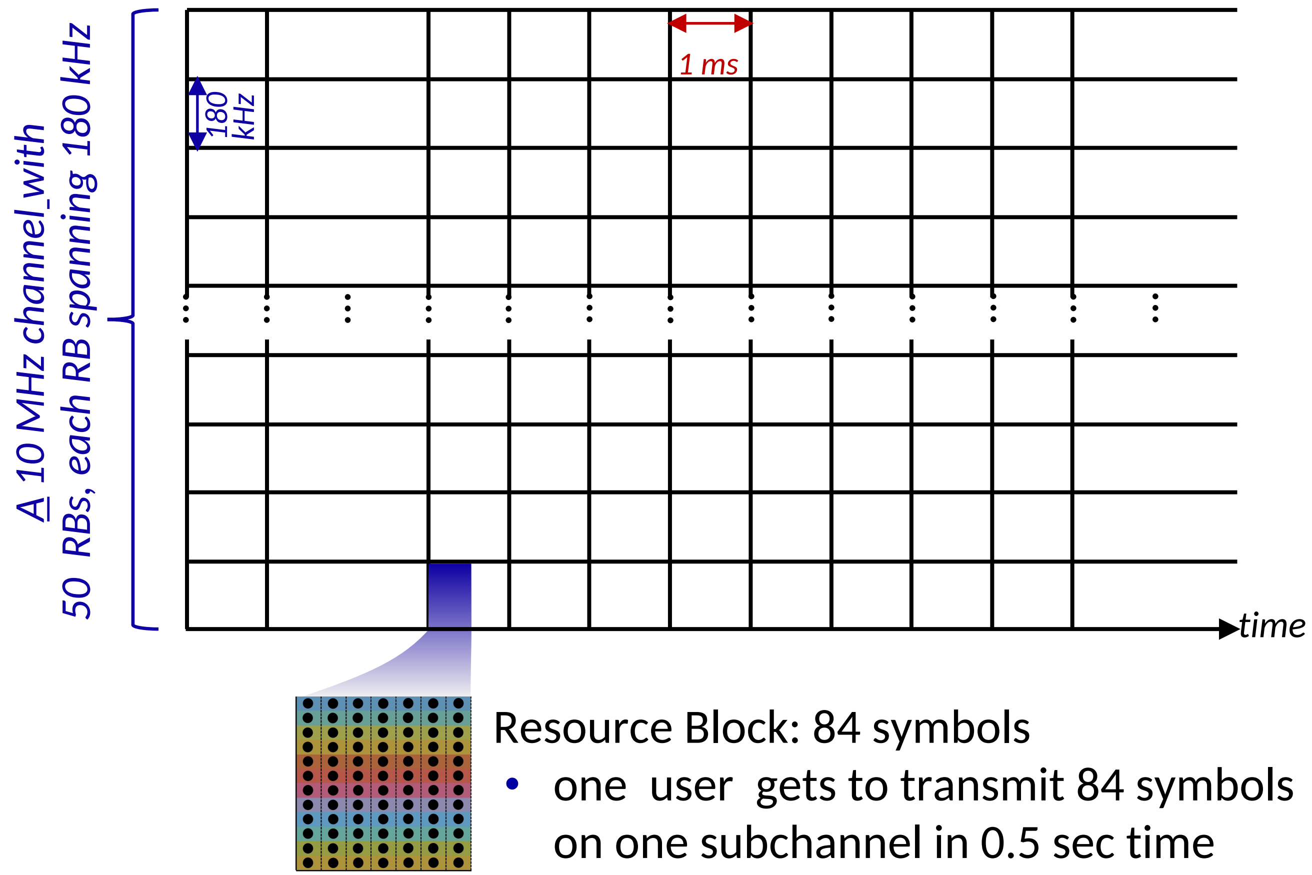
- Does scheduler provide priority among different types of traffic (user, control, real-time)?
- does scheduler consider fairness among UEs?
- fairness: no standard definition

- *Standards do not dictate answers to these questions!*
- *Scheduling algorithms, parameters up to network implementers, operators: their "secret sauce"*



"We are all equally important"

RAN scheduling: Resource Blocks



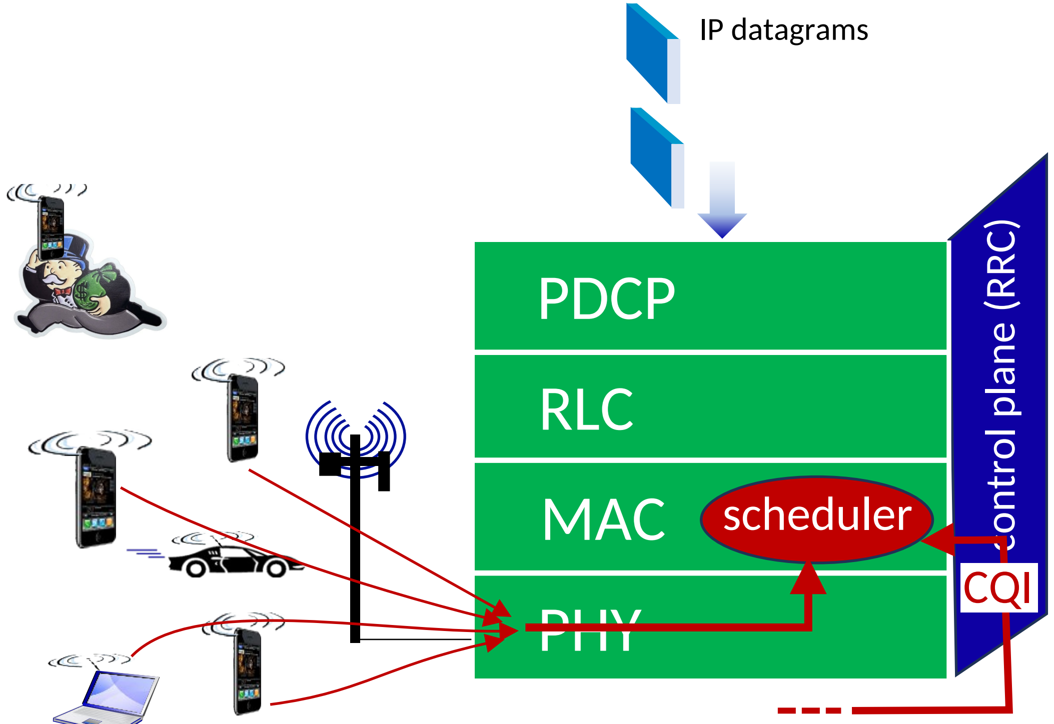
Resource Block: 84 symbols

- one user gets to transmit 84 symbols on one subchannel in 0.5 sec time interval
- 50 subchannels per 10MHz channel

Scheduling:

- Base station decides which frames/packets get assigned to which RBs for transmission to user
- scheduling interval: 1 msec
- scheduling complexity:
  - 50 subchannels per 10MHz channel
  - 100’s (?) active user

RAN scheduling: Channel Quality Indicator

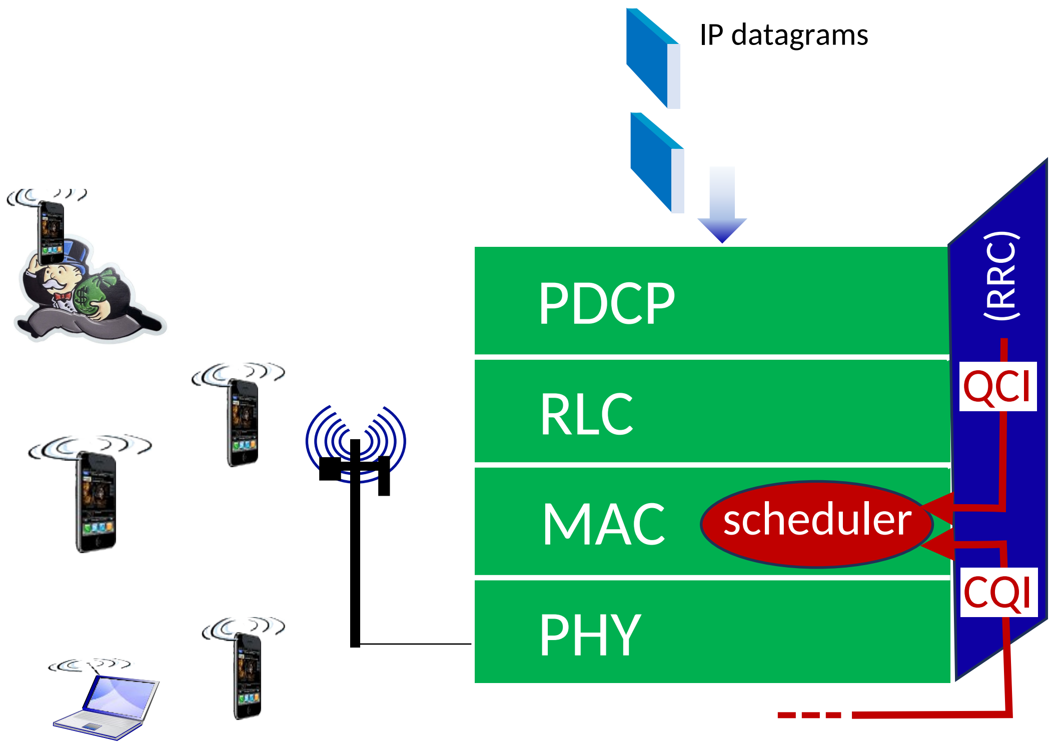


RAN packet-processing stack (3GPP)

Channel Quality Indicator (CQI):

- user measures quality of received reference signals (embedded in RBs), reports quality back to base station
- 4-bit CQI value maps to modulation scheme to use (e.g., which QAM?) and expected throughput

RAN scheduling: QoS Class Indicator



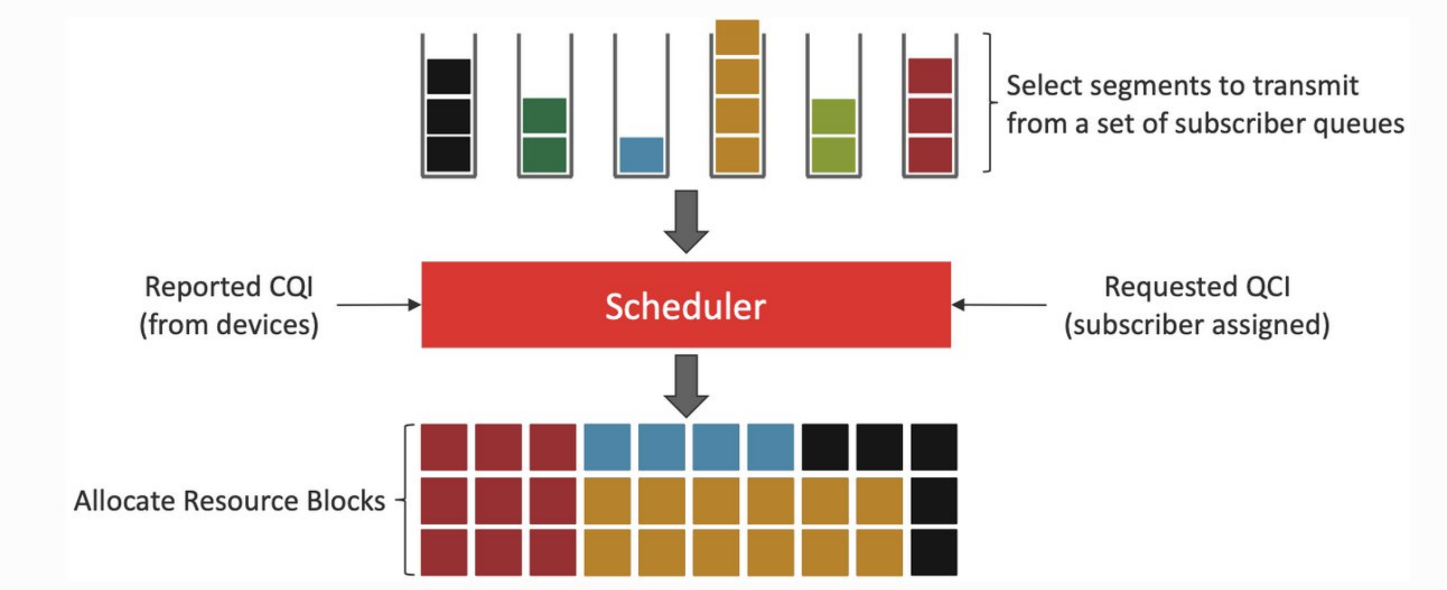
RAN packet-processing stack (3GPP)

QCI: QoS Class Indicator

- *QoS* network wants to provide to a particular device (e.g., delay, guaranteed bit rate QoS guarantees)
- scheduler determines allocation of available radio spectrum to ensure all UEs meet their QoS requirements

Priority	QCI	Max delay	Max loss	Application
2	1	100ms	.01	Voice
3	4	50 ms	.001	Real-time gaming
6	7	300 ms	.000001	Streaming video
8	8	600	.000001	Web browsing, TCP

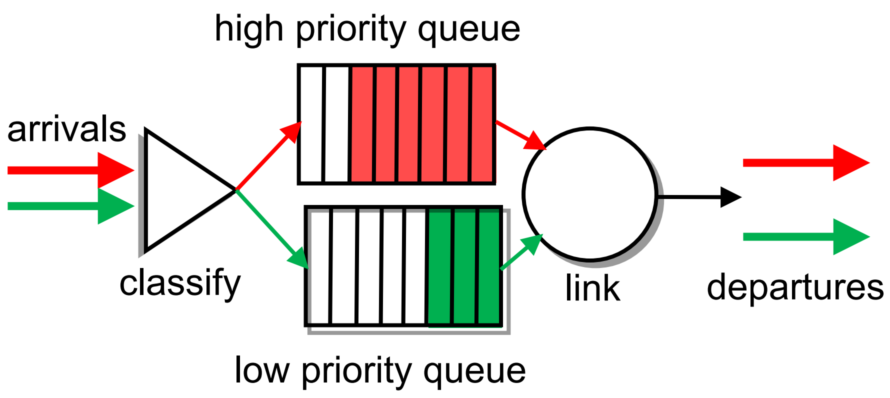
4G/5G scheduling: abstraction

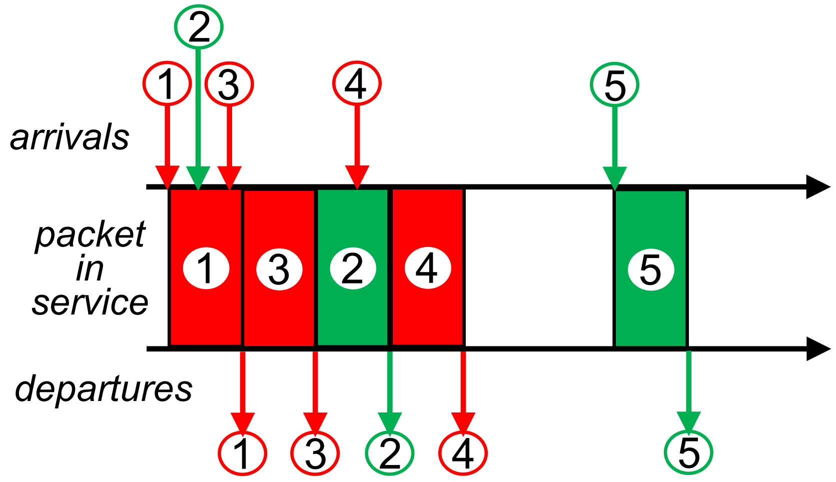


Scheduling policies: priority

Priority scheduling:

- arriving traffic *classified*, queued by class
  - any header fields can be used for classification, e.g., control versus user data
- send packet from highest priority queue that has buffered packets
  - scheduling within priority class could be another scheduling discipline

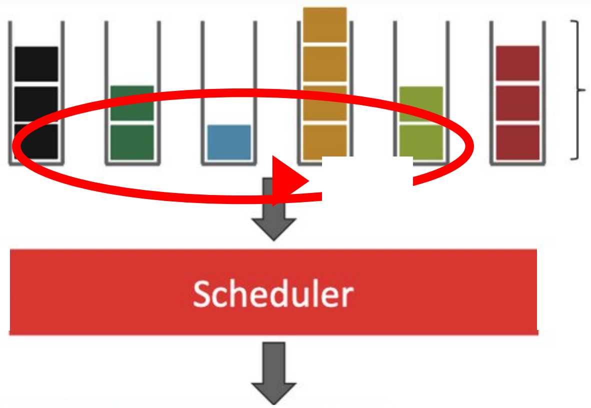




Round Robin scheduling (per UE)

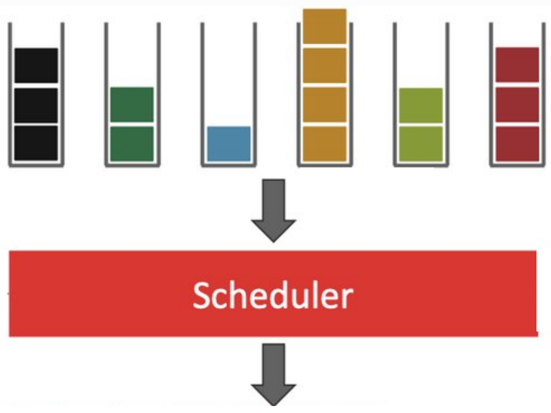
- scheduler cyclically scans device queues, mapping packets/frame from each device (if available) to an RB in turn
- channel unaware, QoS unaware
- fair (by turns) but not necessarily throughput-fair since different devices may have different channel quality

Each device has its own queue



Maximum Throughput (MT) scheduling

- find device (UE) i, with highest quality channel over all RBs, k:
  - $d^i_k(t)$: expected data rate for UE^i using kth RB at time t (e.g., based on CQI)
  - at t: select $\max_{i,k} \{d^i_k(t)\}$, *assign* UE^i frame to RB_k
- maximizes overall immediate throughput
- channel aware, QoS unaware, throughput unfair



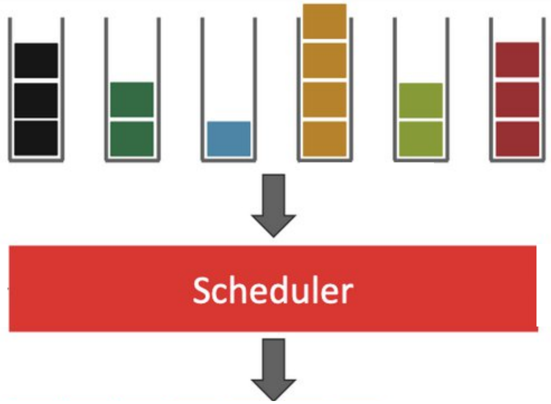
Blind Equal Throughput (BET) scheduling (per device)

- scheduler maintains exponentially-weighted-moving-average of data rate received at each UE^i at time t, $R^i(t)$:

$$R^i(t) = (1-b) \cdot r^i(t) + b \cdot R^i(t-1)$$

where $r^i(t)$ is data rate achieved in scheduling interval t

- at t: select $\min_i \{R^i(t-1)\}$: assign UE^i frame blindly (not know channel conditions) to (any) RB
  - assign RB to device with smallest data rate last round
- channel somewhat-aware, QoS unaware, blind throughput fair

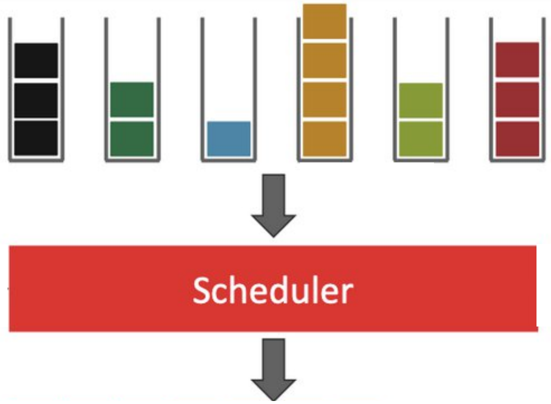


Proportional Fairness (PF) scheduling

- combine Blind Equal Throughput (BET) and Maximum Throughput (MT) scheduling

  $d^i_k(t)$: expected data rate for UE^i using kth RB at time t

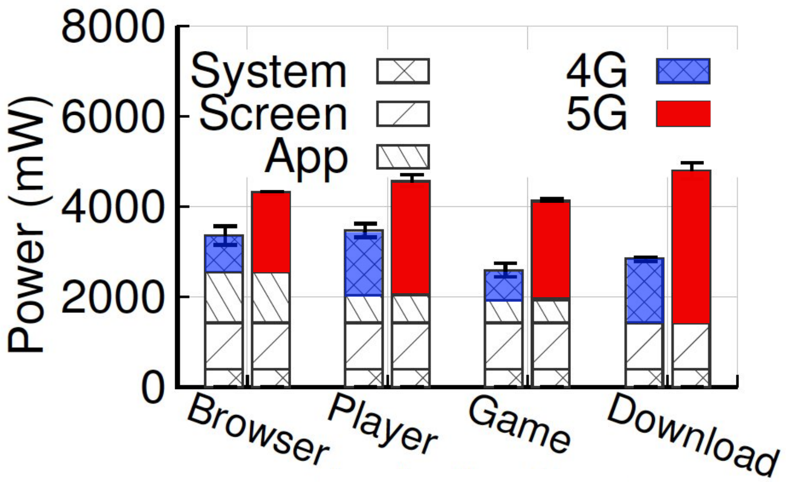
  $R^i(t\text{-}1)$: data rate achieved by UE^i at t
- at t: select $\max_{i,k} \{d^i_k(t) / R^i(t\text{-}1)\}$: assign UE^i



- balances high data rate with a measure of fairness
- channel aware, QoS unaware, fairness aware

Energy consumption in wireless devices

- battery/energy: a critical resource in wireless devices (phones, IoT)
- energy use by LTE radios[1]:
  - on: transmitting or receiving/waiting to receive: 1000 — 3500mW
  - off: < 15mW (~1% – 2 % of on-state energy use)



Power use in mobile phones:
app vs screen vs system vs network

- significant amount of device energy expended on communication, across applications
- 5G implementations currently expending more energy than 4G

Sources: 1: ATT, 2: “Understanding Operational 5G,” ACM SIGCOMM 2020

Cycles of sleep/activity: sleep

4G/5G, WiFi, Bluetooth radios turned off when not in use: conserve energy

Going to sleep is easier:

- device-driven: go to sleep if nothing to send, nothing being received
- sleep may (or may not) be coordinated with base station (4/5G), AP (WiFi) , controller (BT)
- may have deep-sleep (longer, more "turned off") versus light sleep (shorter, less "turned off")

Cycles of sleep/activity: awake

4G/5G, WiFi, Bluetooth radios turned off when not in use: conserve energy

Waking up is harder:

- base station (4/5G), AP (WiFi) , controller (BT) needs to signal to “wake up” device when there are packets to be sent to it
  - network context (4/5G) may need to be re-created
  - *data frames containing IP datagram (e.g., from remote hosts) need to be buffered at base station until device is awake*

Cycles of sleep/activity: tradeoff/challenges

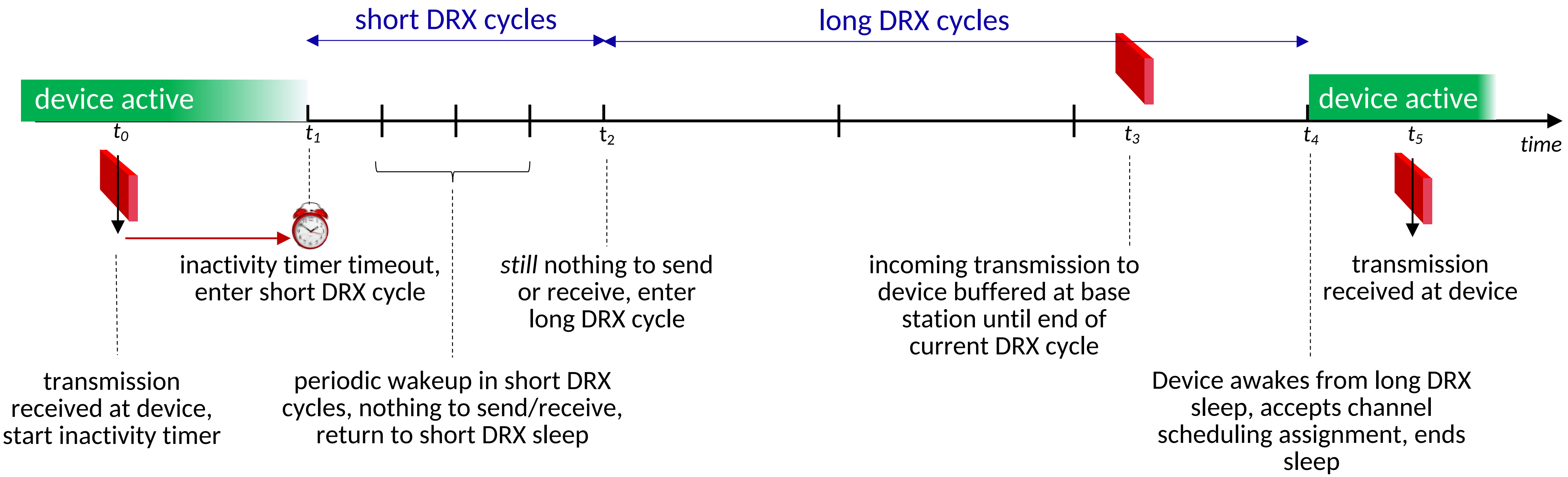
How long to sleep?

- longer: save more energy but greater latency
  - effects on high-layer protocols: e.g., TCP
- shorter: less energy savings, and more signaling overhead with short sleep cycles

How long to stay awake?

- time since last activity (before going to sleep)
  - data transmission typically "bursty"
  - burst should be over before going to sleep: how long to wait?

Coordinated wake/sleep in 5G

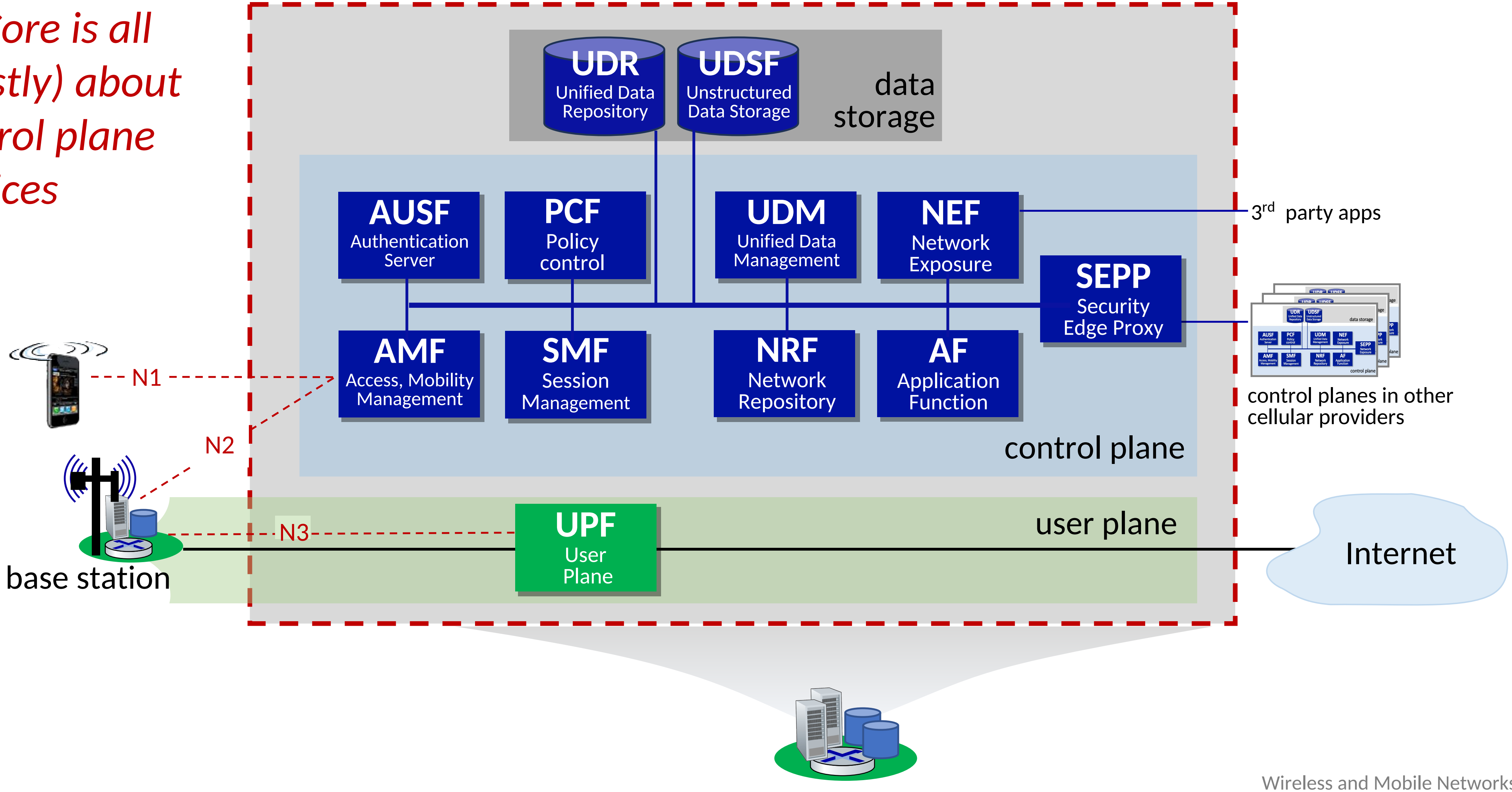


Chapter 7 outline

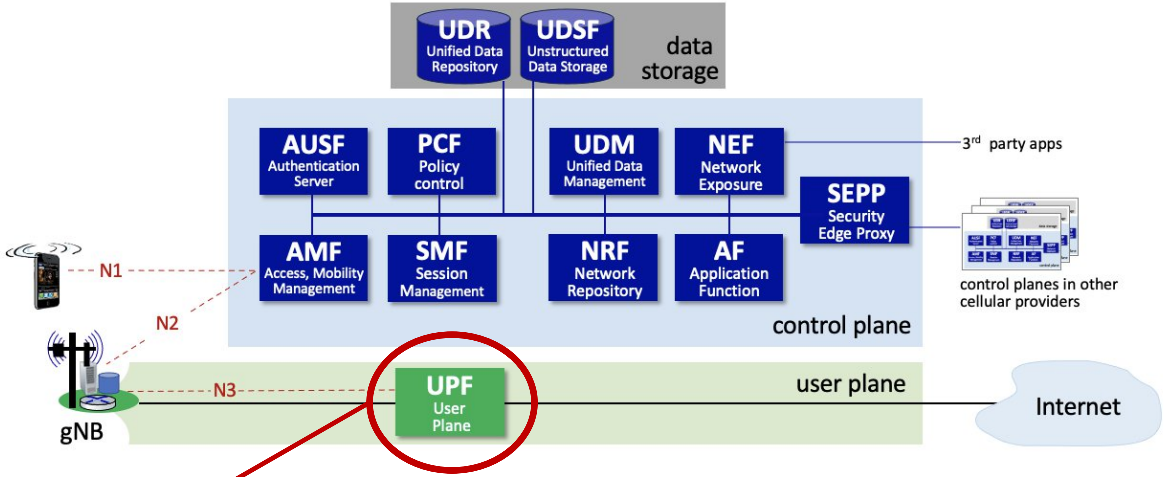
- introduction
- radio: the physical layer
- the wireless *access* network
  - principles, WiFi, 5G
- the wireless core network
  - principles, 5G
- mobility
- Bluetooth, satellite, IoT wireless networks

5G Core Functional Components

5G Core is all (mostly) about control plane services



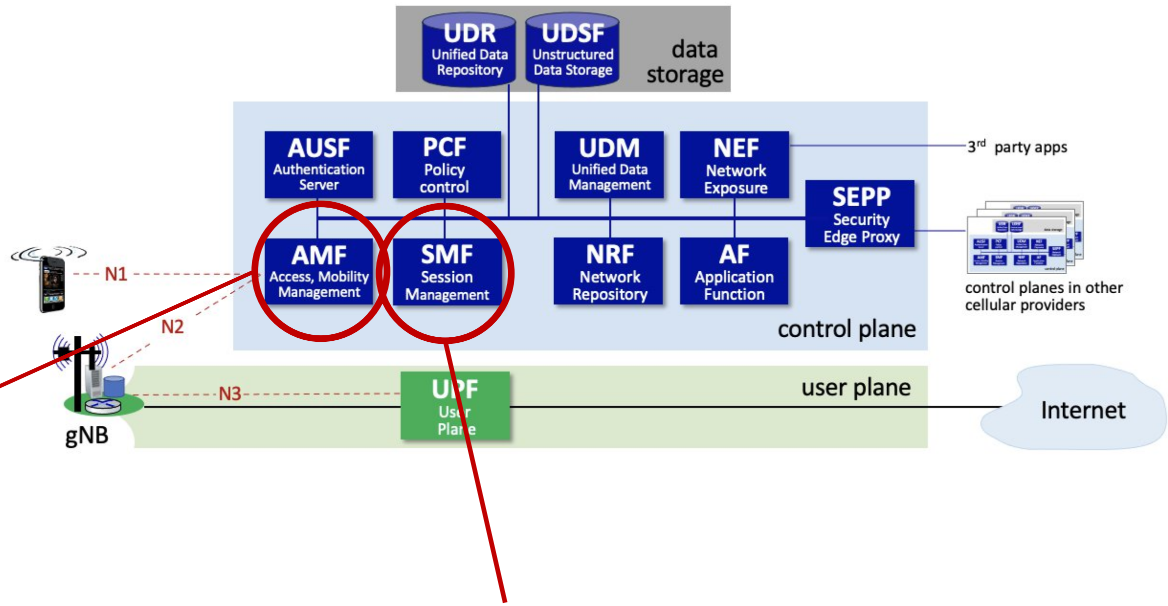
5G Core Functional Components



UPF (User Plane Function)

- each device is assigned to a UPF, which acts as relay, forwarding traffic between UE, Internet
- UPF responsible for policy enforcement, lawful intercept, traffic usage measurement, QoS policing
- responsible for tunneling (i.e., encapsulating, decapsulating) traffic to/from base station over N3 interface

5G Core Functional Components



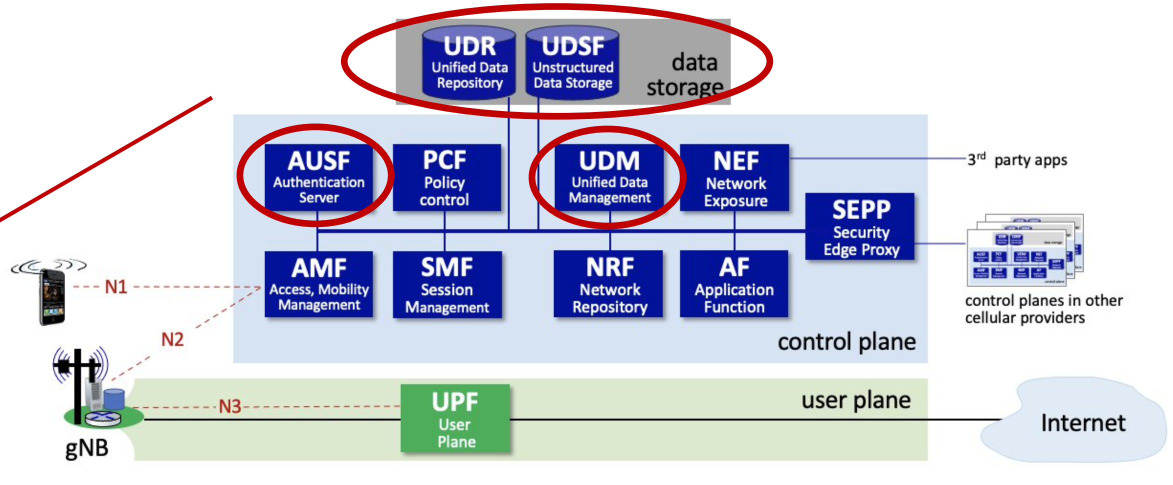
AMF (Access, Mobility Management Function)

- connection, reachability management; mobility management; access authorization; and location services

SMF (Session Management Function)

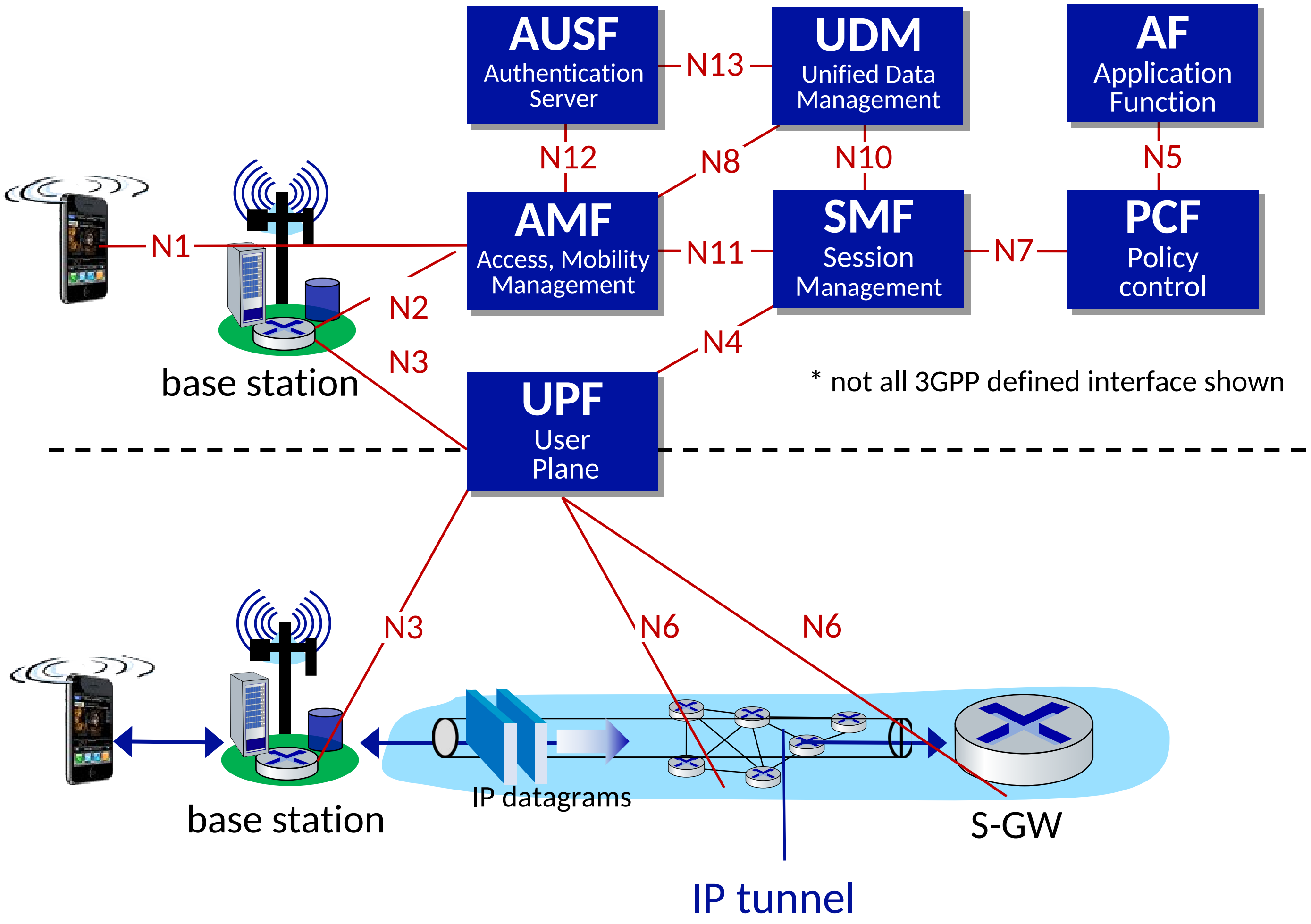
- manages each UE session, including IP address allocation, selection of associated UP function, QoS control, control aspects of UP routing

5G Core Functional Components



- *AUSF (Authentication Server Function):* Authenticates devices.
- *UDM (Unified Data Management):* Manages user identity, including the generation of authentication credentials.
- *UDR (Unified Data Repository):* Manages user static subscriber-related information.
- *UDSF (Unstructured Data Storage Network Function):* Used to store unstructured data, and so is similar to a *Key/Value Store*.

5G interfaces*, control/user -plane separation (CUPS)



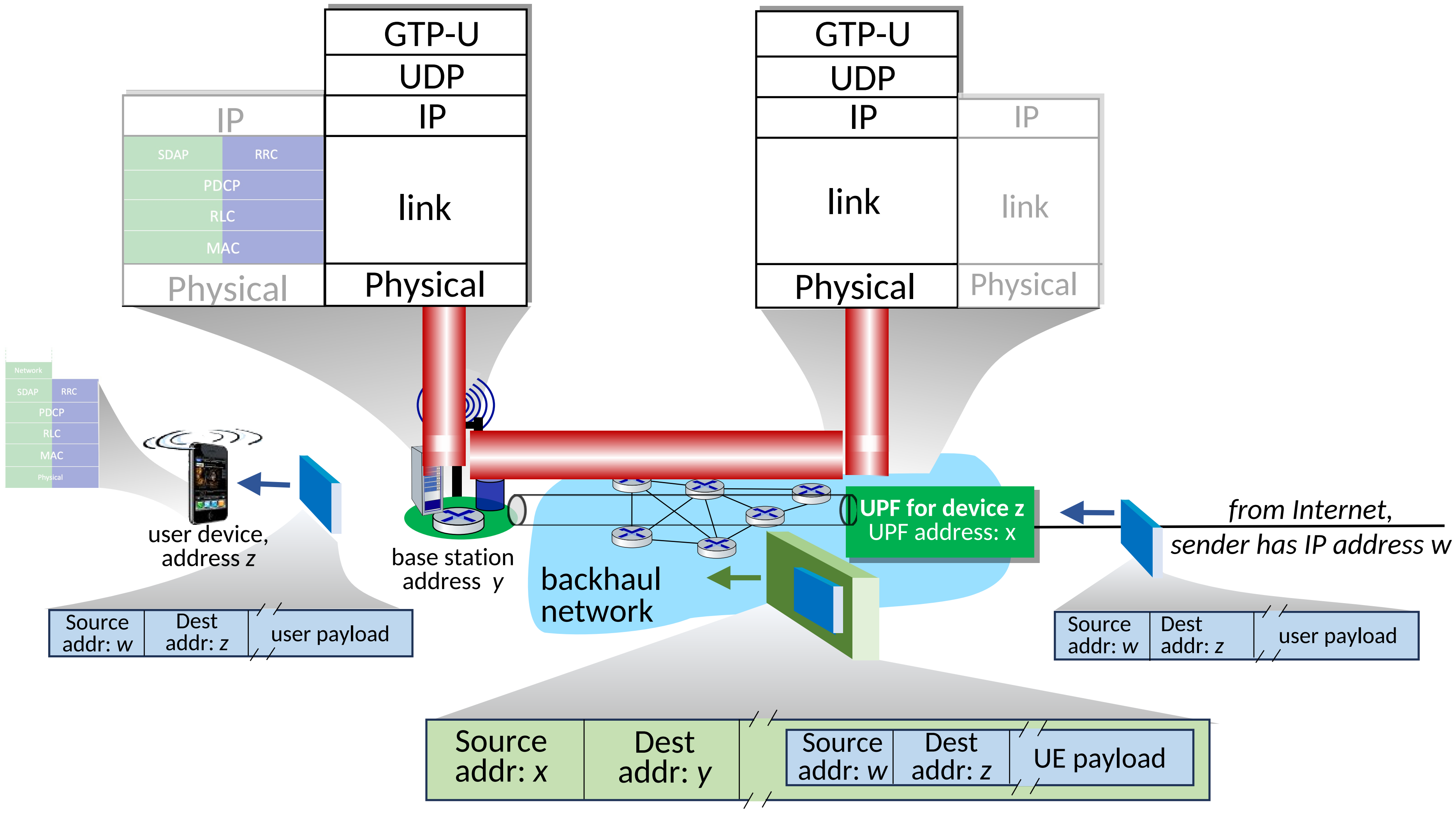
control plane

- emphasis on functions and services
- well-defined interfaces defines between services

data plane

- 5-layer Internet data plane
- extensive use of tunneling

5G Core: User plane tunnels



Identity: who are you?

4G/5G:

- You're a customer to a wireless service provider, with a home cellular network (who you pay)
- you have a SIM (Subscriber Identity Module) card or vSIM
  - identifies you, your home network to all cellular networks globally
  - has cryptographic key info also known to your home network

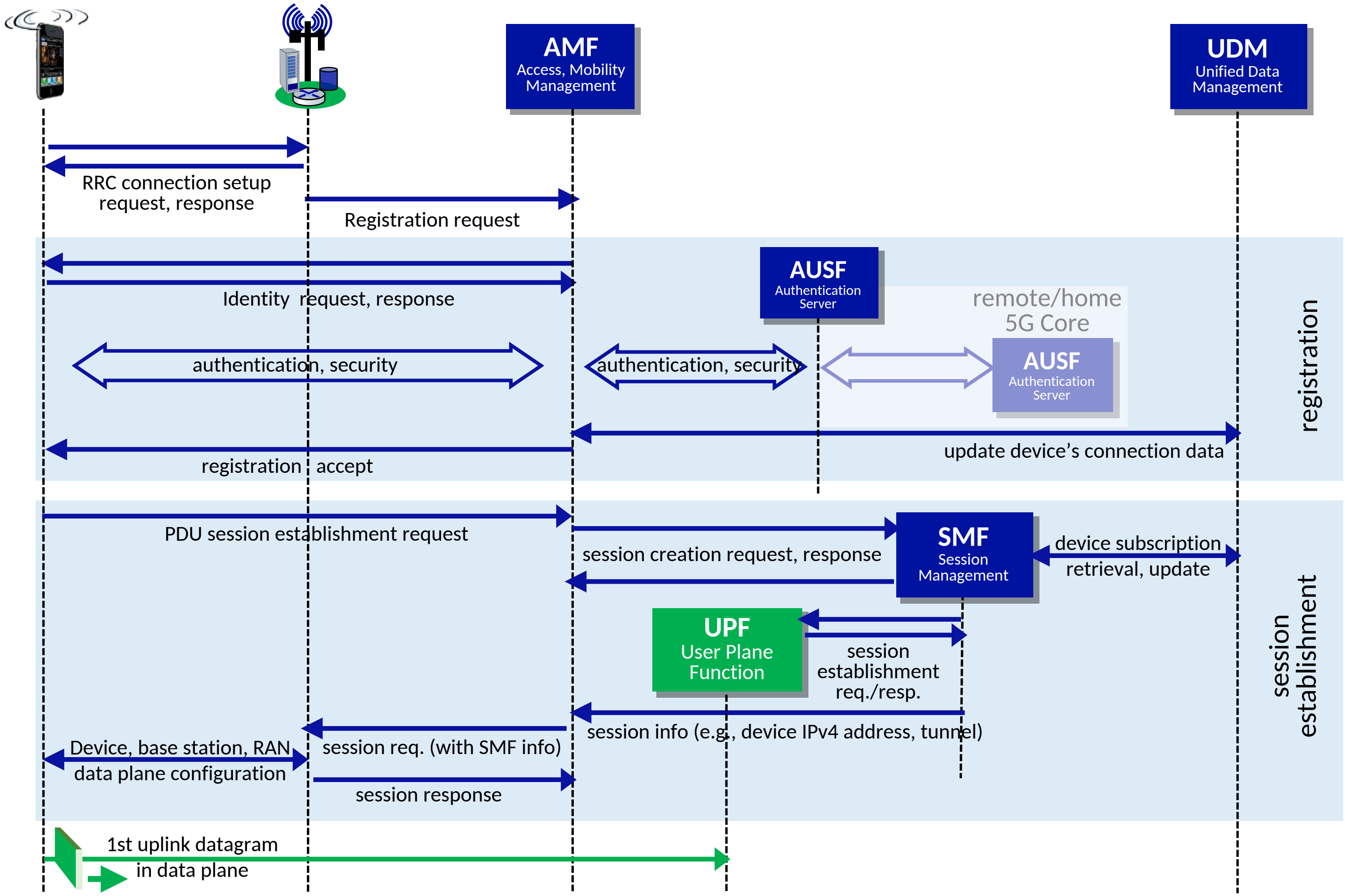
Internet approaches:

- You're a name, password
  - different names, password for different applications, services
- You're a name, public key certificate
  - servers often have public keys, users not so much (yet)

Joining a 5G network

- Two major phases:
  - *Registration:* device identifies, authenticates itself to network, and *vice versa*
  - *PDU Session establishment:* Core network functions allocate IP address to device, create data-plane path between device and device's UPF
    - PDU: protocol data unit, aka, "packet"
- *Access and Mobility Management Function (AMF)* plays key role in joining arriving device into network

Joining a 5G network: steps

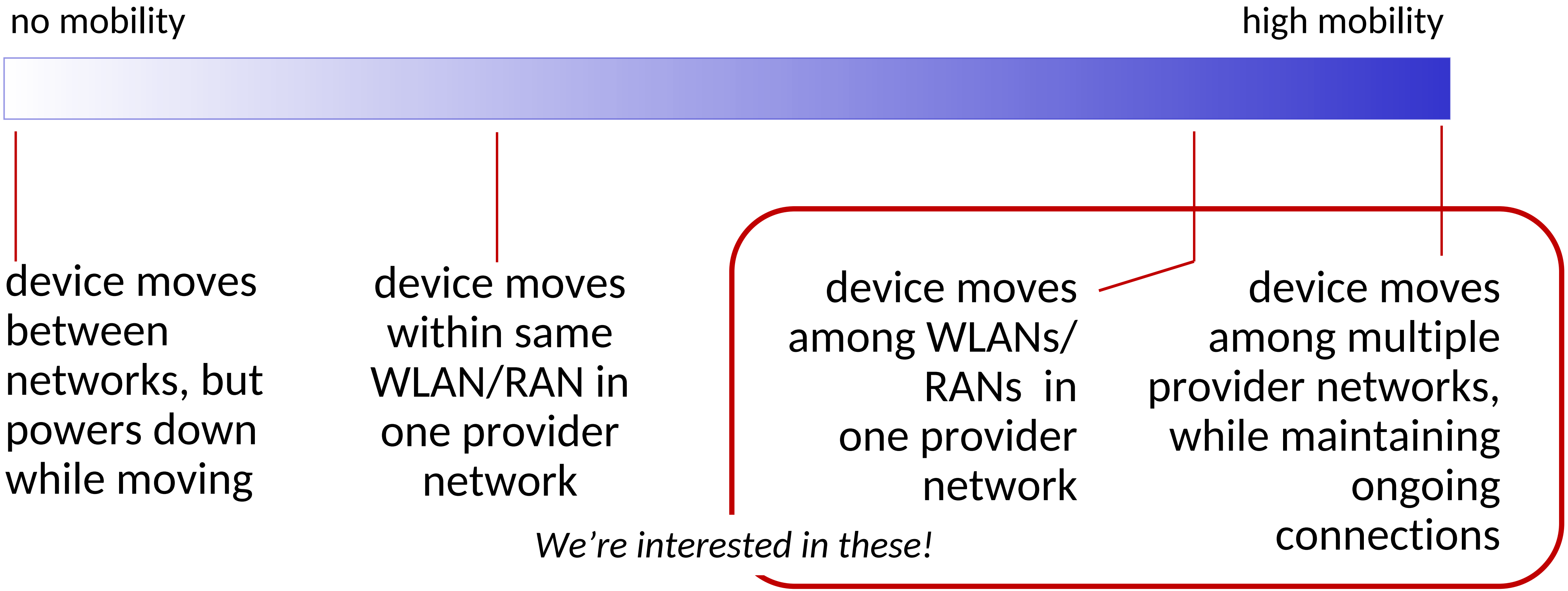


Chapter 7 outline

- introduction
- radio: the physical layer
- the wireless *access* network
  - principles, WiFi, 5G
- the wireless core network
  - principles, 5G
- mobility
- Bluetooth, satellite, IoT wireless networks

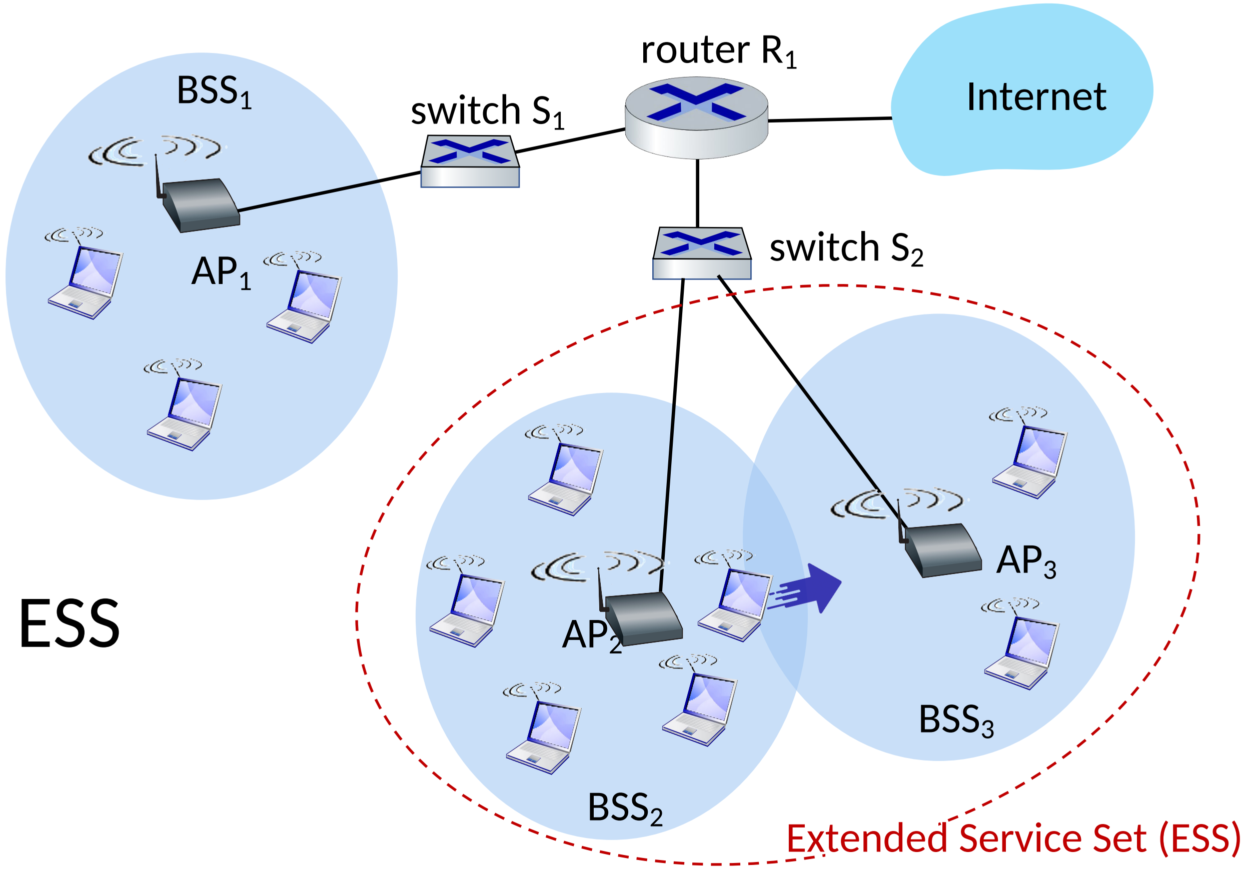
What is mobility?

- spectrum of mobility, from the network perspective:

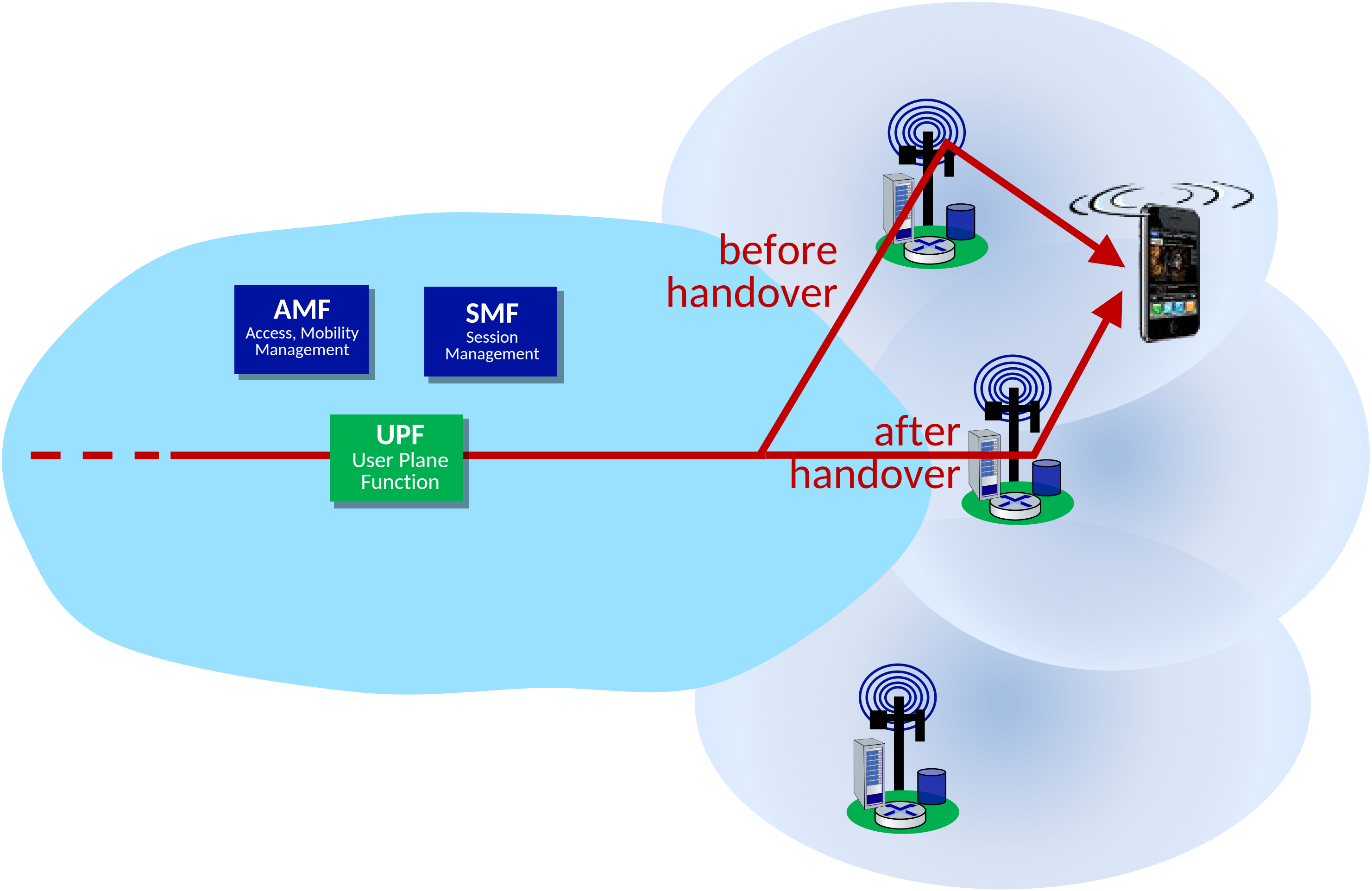


Mobility in a WiFi network

- 802.11: a link-layer standard, takes a link-layer approach towards mobility
- Extended Service Set (ESS): multiple BSS's, in same layer-3 subnet, each with same SSID
- mobility between BSSs in same ESS
  - Fast re-authentication
  - AP can suggest new APs to device
- proprietary (vendor) solutions for enhanced mobility



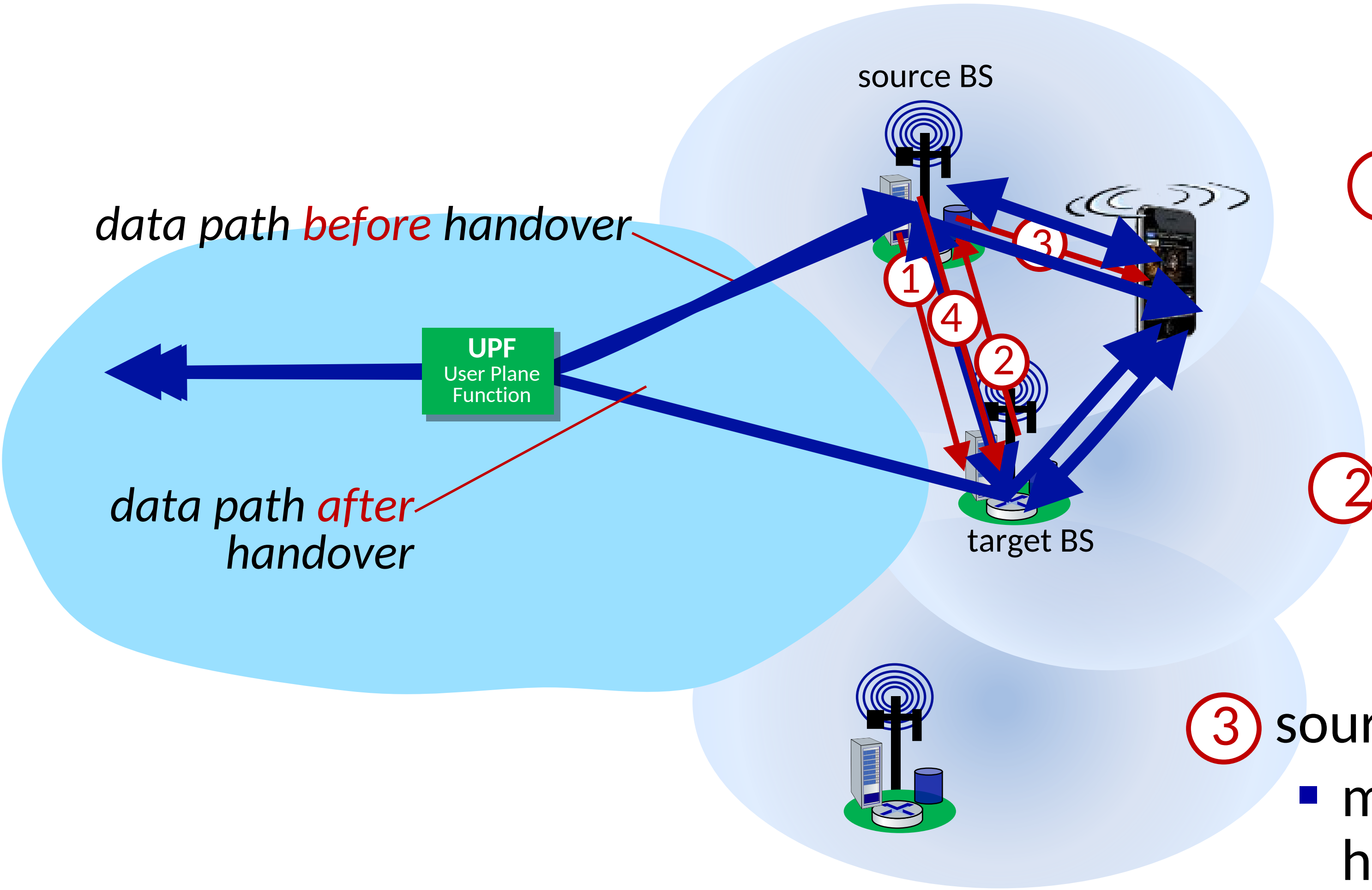
Mobility in 5G networks: handover



Handover:
- mobile device changes is point of attachment to the network
- data flow to device changes from *source* base station to *target* base station

Why perform handover?
- stronger signal from target base station
- target base station has less devices, less traffic

Mobility in 5G networks: handover



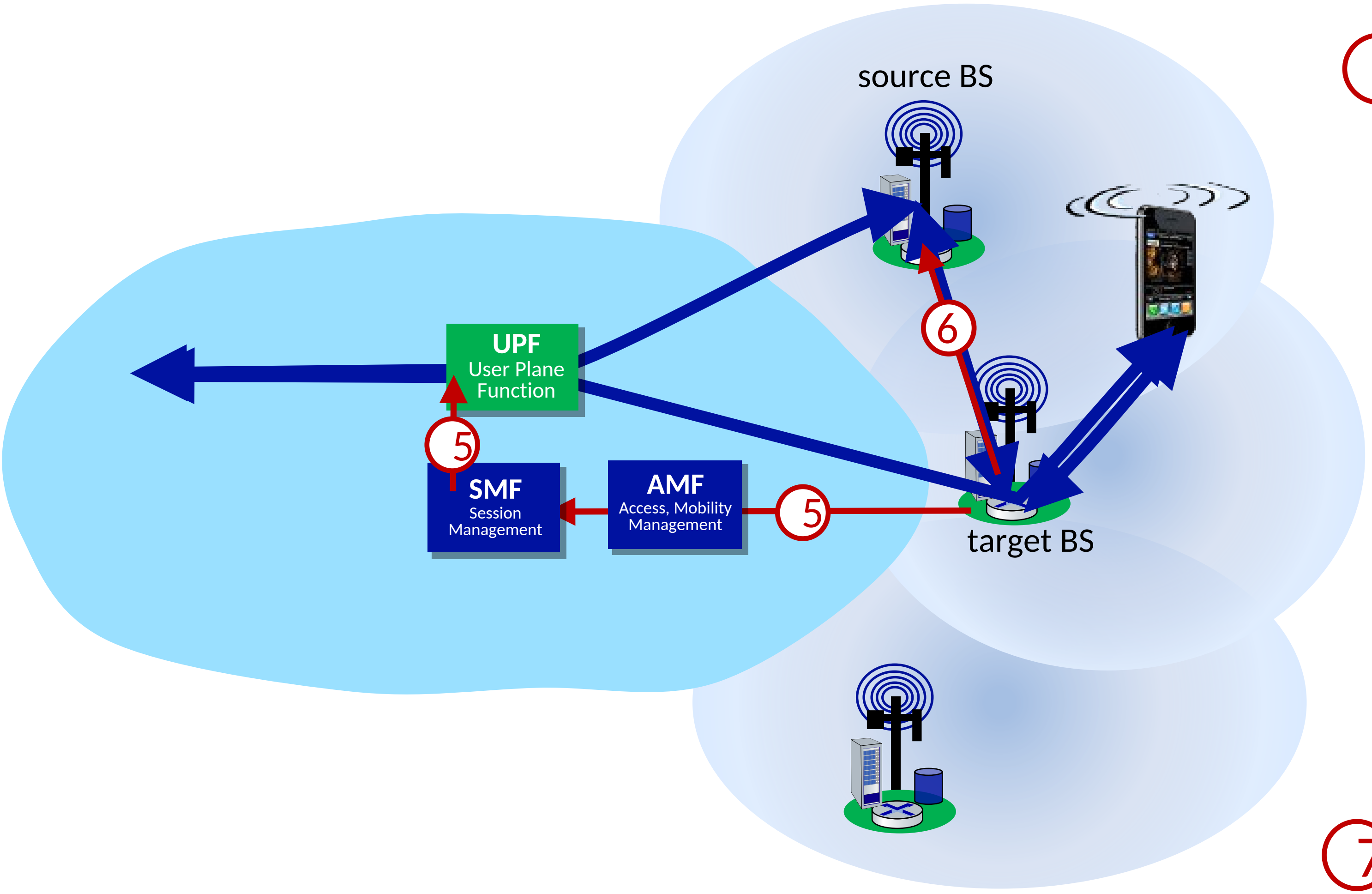
1. current (source) BS selects target BS, sends *Handover Request message* to target BS

2. target BS pre-allocates radio time slots, responds with HR ACK with info for mobile

3. source BS informs mobile of new BS
   - mobile can now send via new BS - handover *looks* complete to mobile

4. source BS stops sending datagrams to mobile, instead forwards to new BS (who forwards to mobile over radio channel)

Mobility in 5G networks: handover



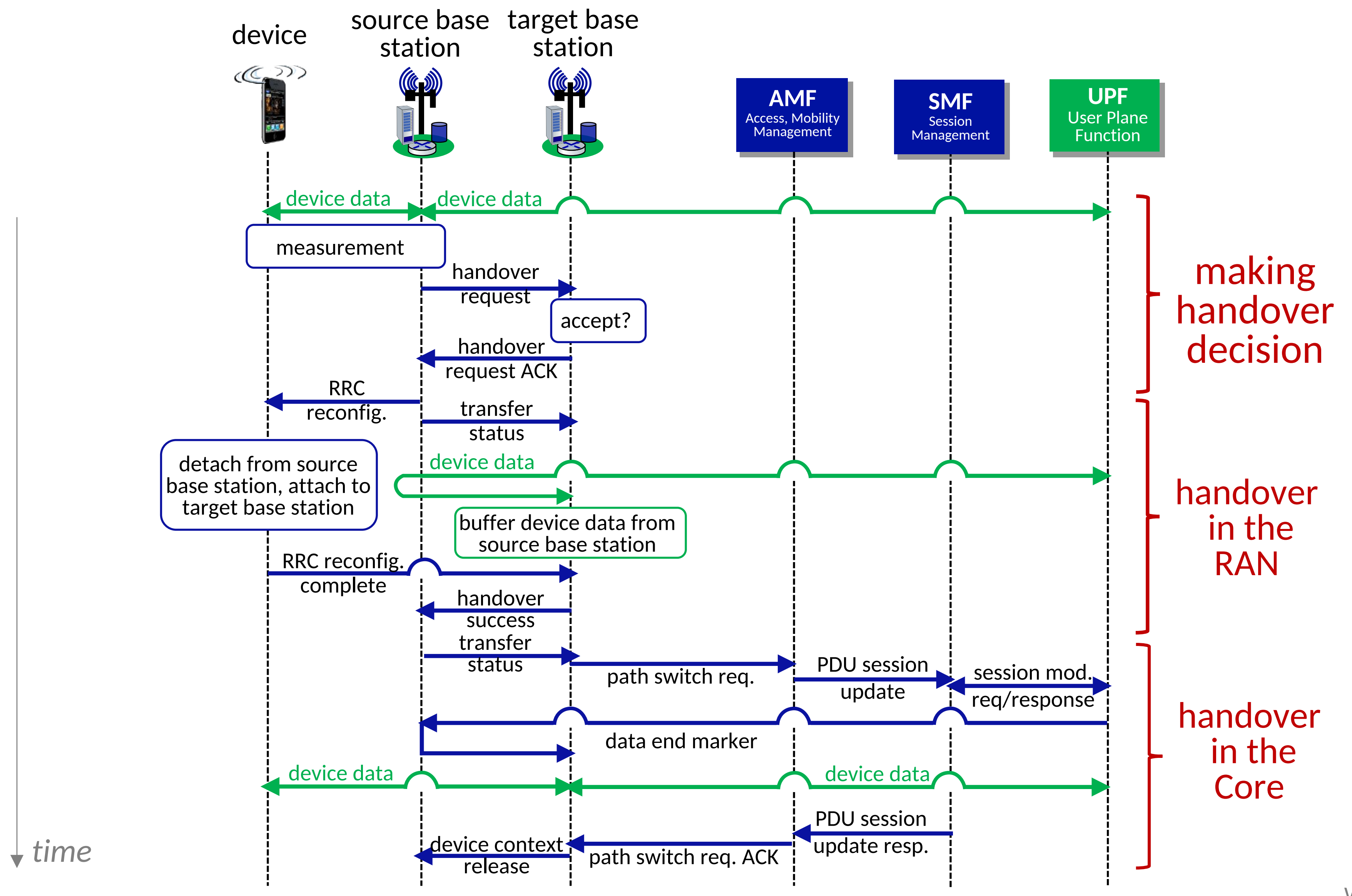
5 target BS informs AMF, SMF that it is new BS for mobile

- SMF instructs UPF to change tunnel endpoint to be (new) target BS

6 target BS ACKs back to source BS: handover complete, source BS can release resources

7 mobile's datagrams now flow through new tunnel from target BS to UPF

Handover: timeline, signaling



Chapter 7 outline

- introduction
- radio: the physical layer
- the wireless *access* network
  - principles, WiFi, 5G
- the wireless core network
  - principles, 5G
- mobility
- Bluetooth, satellite, IoT wireless networks

Bluetooth (BT) overview

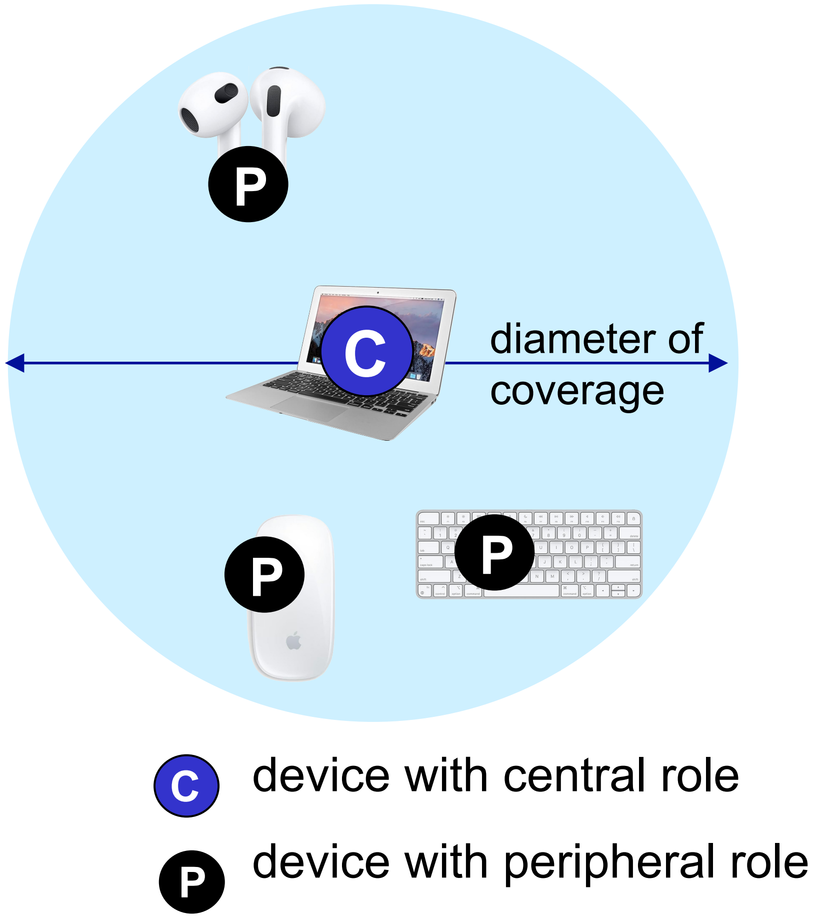
example of *wireless ad hoc network*: devices have no “infrastructure” (e.g., access point, base station) to connect to

- BT devices must find other BT devices, *organize themselves* into a network from scratch!
  - connect devices at link layer, providing channel allocation
  - addressing assignment
  - service discovery
  - application-to-application communication over Bluetooth network
  - security

An entirely new architecture and protocol stack (different from Internet) is needed!

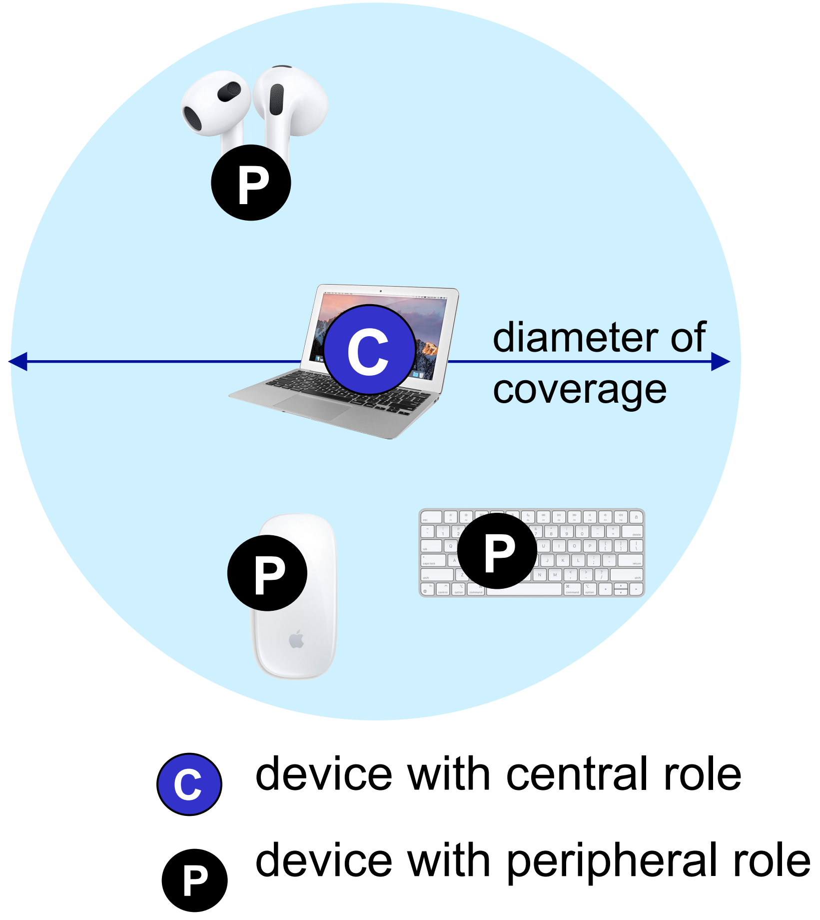
Bluetooth: overview

- Bluetooth network: piconet
- coverage: generally <10 m diameter
- no more than 8 devices per piconet
  - device initially forming network: *central* role
  - up to 7 more devices: *peripheral* role
- *communication only between central and peripheral node*
  - no direct peripheral-to-peripheral communication
- BT device has unique 48-bit address
- Operate in unlicensed ISM band: 2.4 GHz



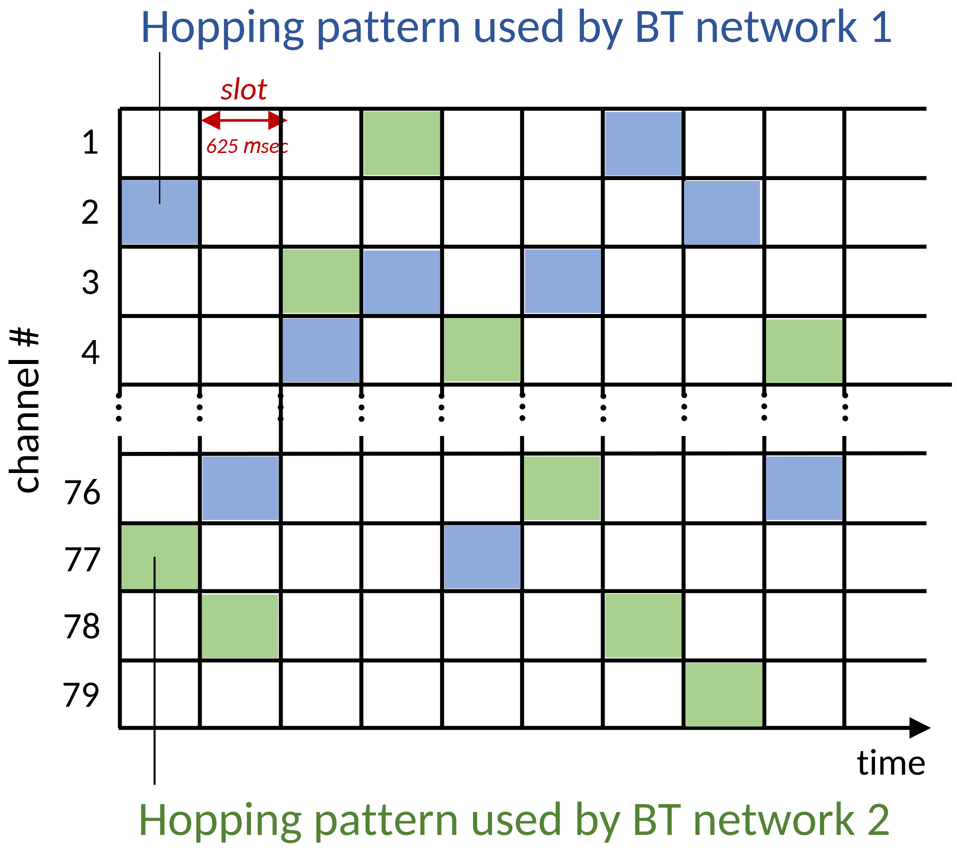
Bluetooth basics: wireless channel

- operates in 2.4-2.5 GHz ISM radio band
  - Classic BT: 1 MHz bandwidth/channel, 79 channels, 2.1 Mbit network max rate
  - BLE: 2 MHz bandwidth/channel, 40 channels. 3 advertising, 37 data channels
- BT channel: TDM, 625 msec slot length
- channel access via polling: central device advertises, grants channel access to peripherals in its BT network
- uses frequency hopping (form of "spread spectrum") transmissions



Bluetooth channel: frequency hopping

- senders in BT network "hop" among 79 frequencies/channels
  - transmit on different frequency after each slot
  - hopping pattern known by all BT devices in same piconet
- different BT piconets (with different hop patterns) can exist in same space

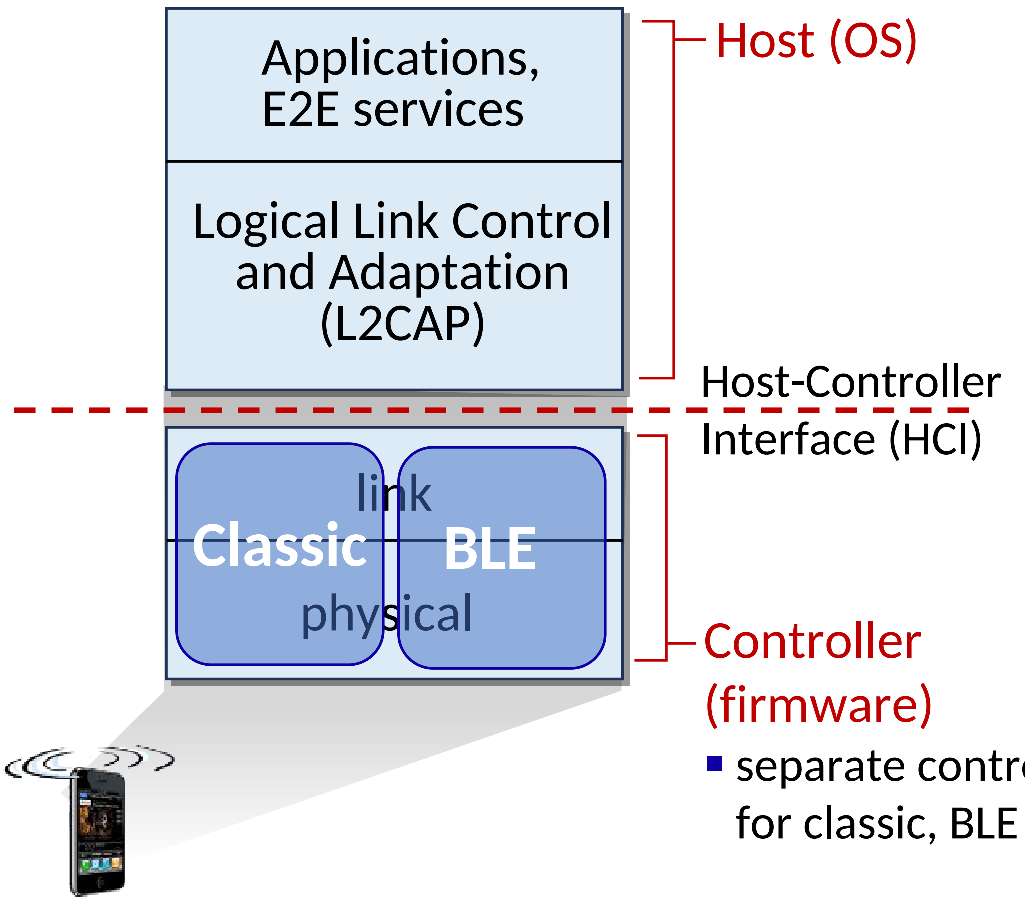


Q: Why hop?

A: minimize effects of interference:

- potentially many interfering transmitters in ISM
- If interfering device uses channel *x*, *x* occurs only occasionally in sequence
- BT frame sent on *x* (not received at receive due to interference), retransmitted on different frequency in next slot

Bluetooth architecture, protocol stack (simplified)

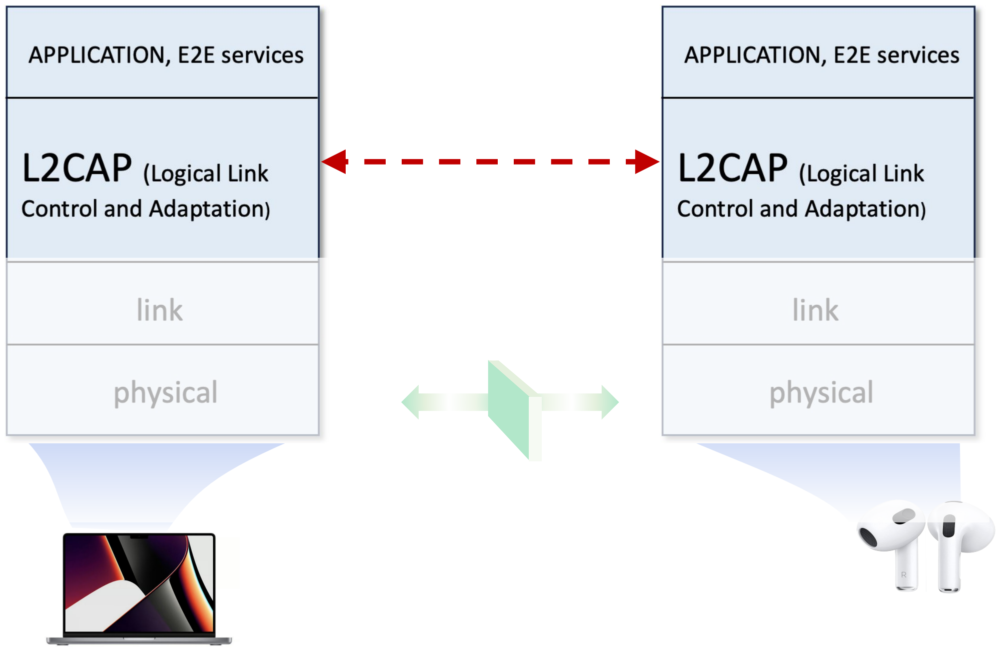


- separate controllers for classic, BLE

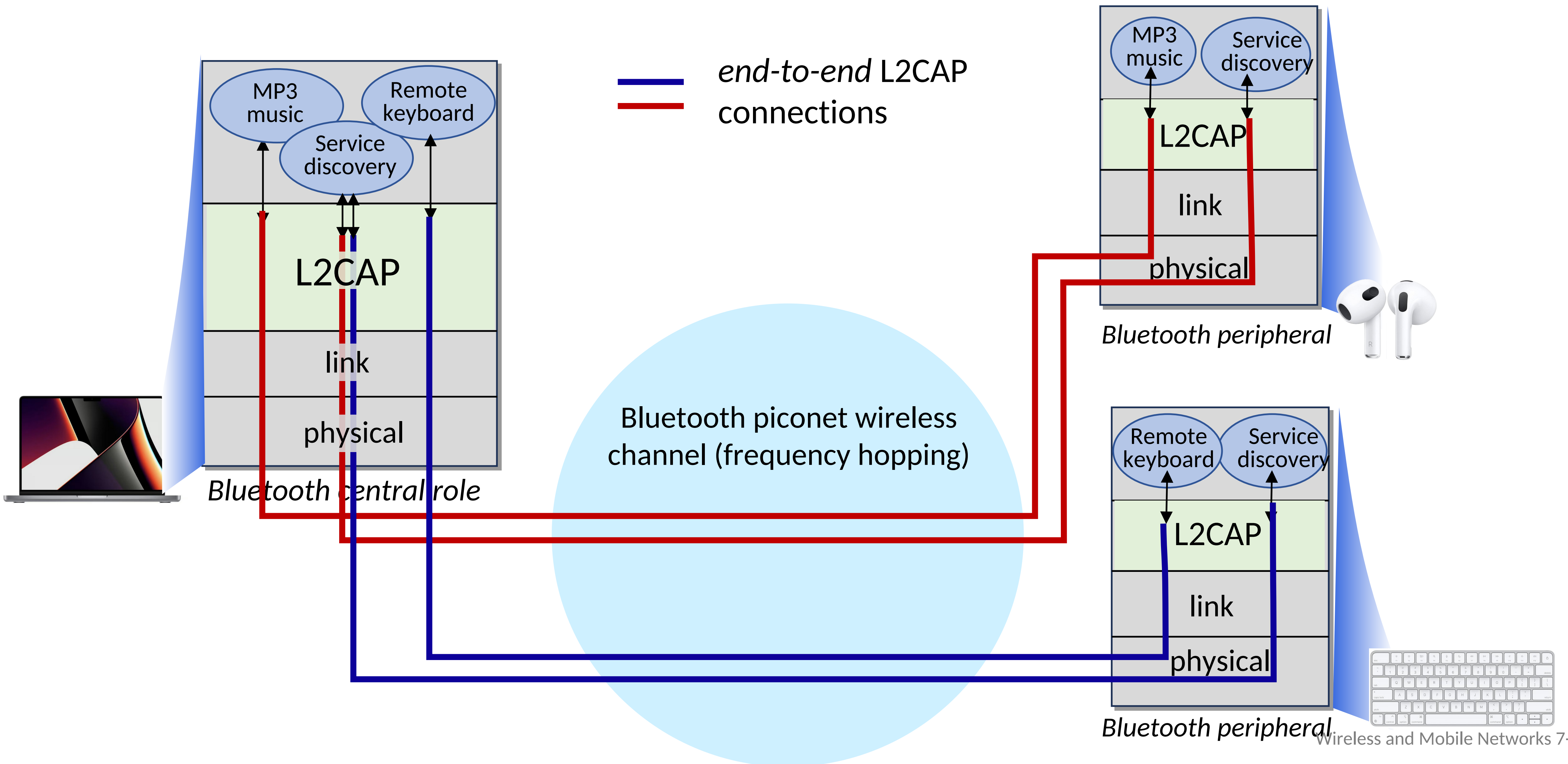
- Bluetooth stack *completely* different from Internet stack!
  - differences reflect BT's special purpose
- no "network," "transport" layer!
  - no routing in Classic BT (BLE adds managed flooding)
- layers not as conceptually well-defined as in Internet, 5G
- host, controller structure deeply embedded in architecture

Logical Link Control, Adaptation (L2CAP) layer

- creation, management of end-end L2CAP channels *between two devices*
  - channels for E2E application/user data, or higher-level services
  - reliability, flow control, segmentation
- L2CAP channels types:
  - connection-oriented, asynchronous (ACL)
  - connectionless, asynchronous (ACL)
  - synchronous (eSCO), e.g., for periodic audio app)



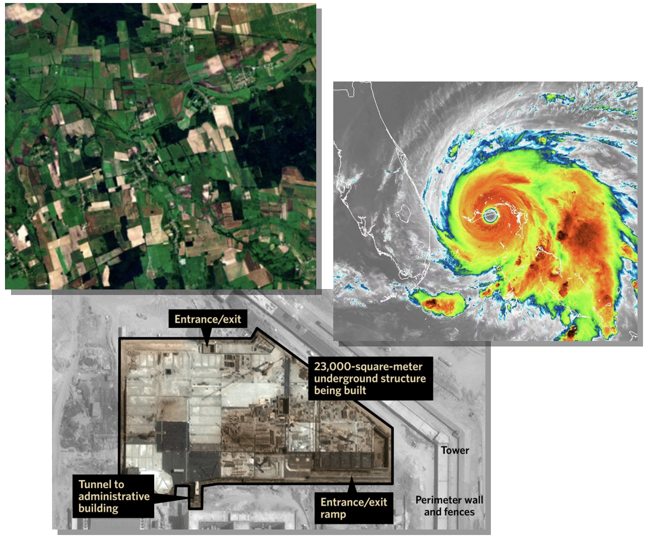
Bluetooth piconet and L2CAP connections



Satellite applications

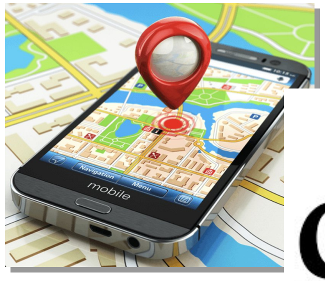
Sensing:

- environment: weather, land use, various human activity
- resolution: ~m/pixel



Broadcast:

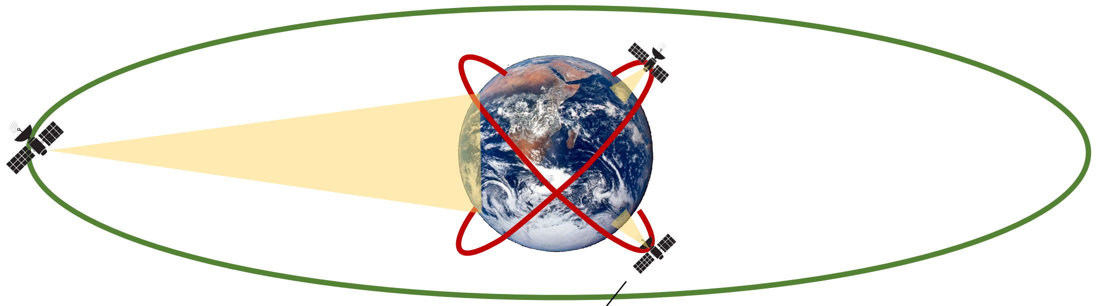
- consumer: Direct to Home TV/video, radio (Dish, SiriusXM)
- business: content to many cable head ends
- GPS
- leverage broadcast: one send reaches many users



Internet:

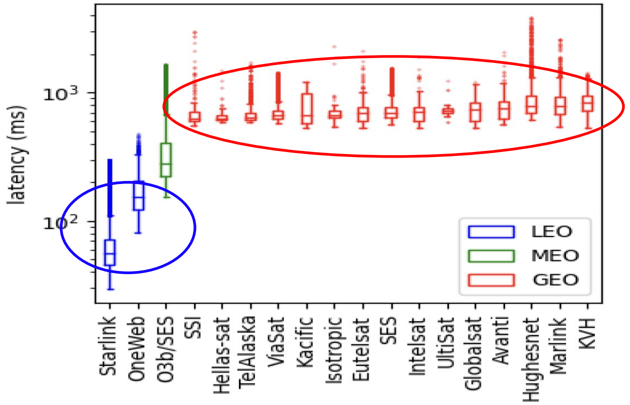
- connectivity to unserved regions, alternative to wired Internet
- low latency over long distances
- access in airplanes

GEO and LEO satellites



GEO:

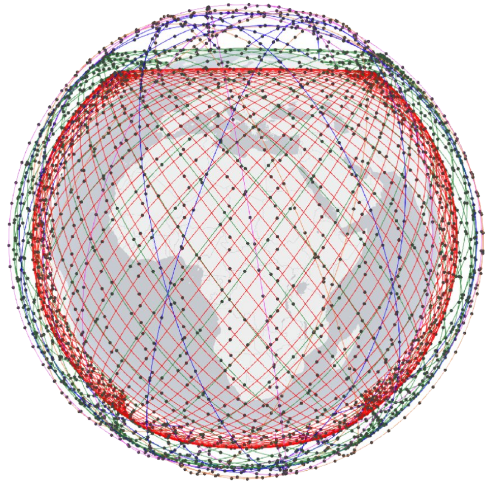
- *geosynchonous:* stationary with respect to ground
- 35,768 km above earth
- ~800 msec RTT
- wide area coverage / satellite



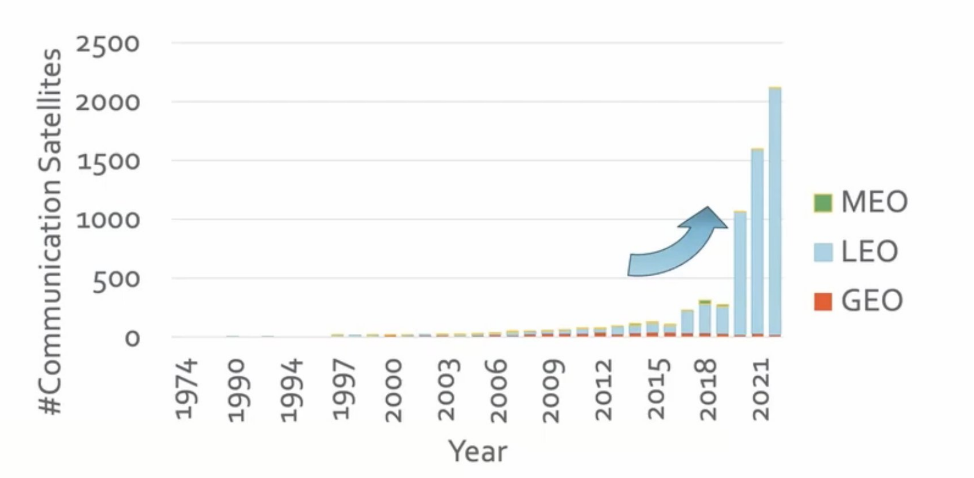
LEO:

- *Low Earth Orbit:* satellite moves with respect to ground: 27,000 km/hour
  - within line of sight (LOS) of ground station for 5-15 mins
- 550 - 1200 km above earth
- ~30 msec RTT in practice
- smaller area coverage / satellite
  - constellation (network) of multiple LEO satellites to cover wide area
  - inter-satellite links (ISL)

Satellites: why all the fuss?



Lots of (LEOS) satellites being launched

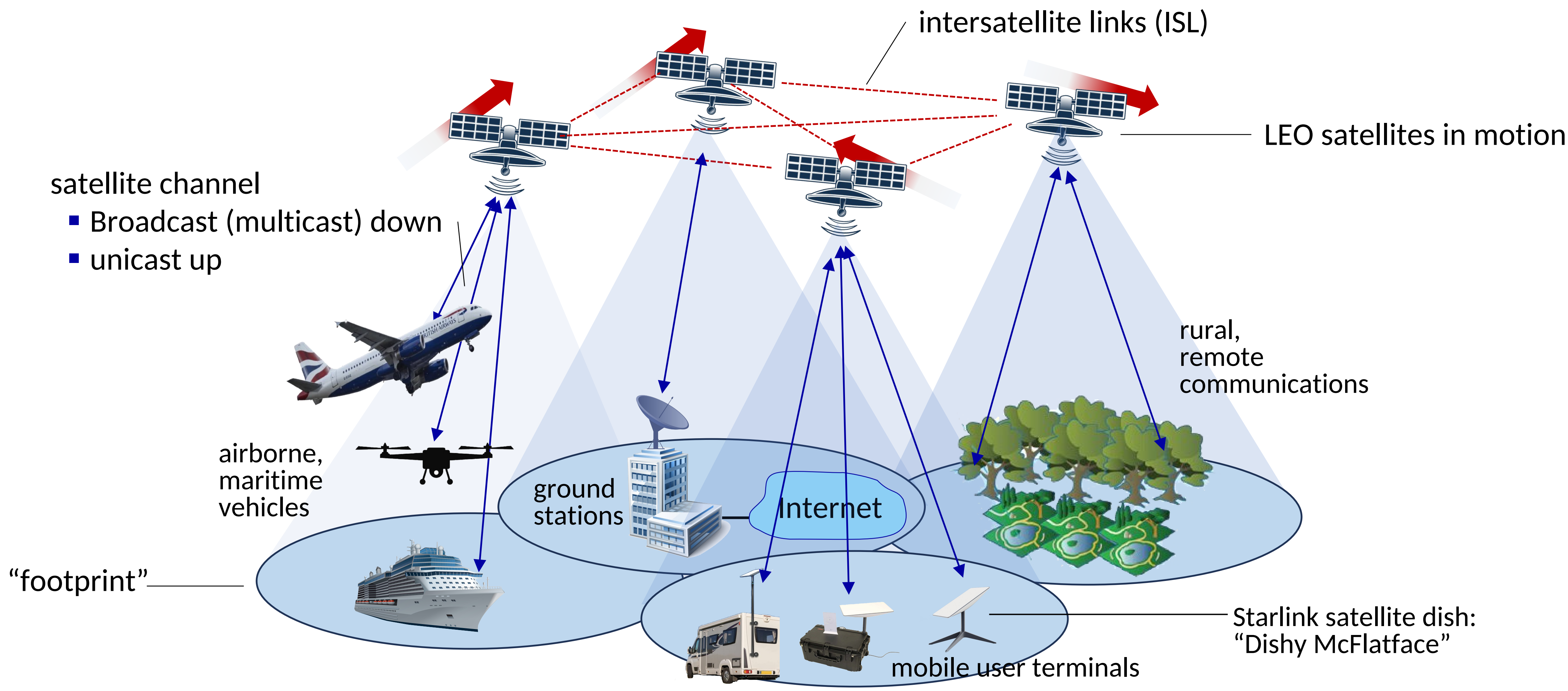


LEOS constellations

	# deployed (2025)	# planned	ISL planned?
Starlink	7,239	12,000 - 42,000	Yes
EutelSat Oneweb	648	716 – 6,372	No
Kuipers (Amazon)	27	3,236	?
Telesat	1	298 - 1671	Yes

Sources: A. Raman, LEO Satellite Mega Constellations, networkingchannel.eu;
N.Pachler et al., An Updated Comparison of Four Low Earth Orbit Satellite Constellation Systems to Provide Global Broadband; company literature

Components of a LEO satellite network

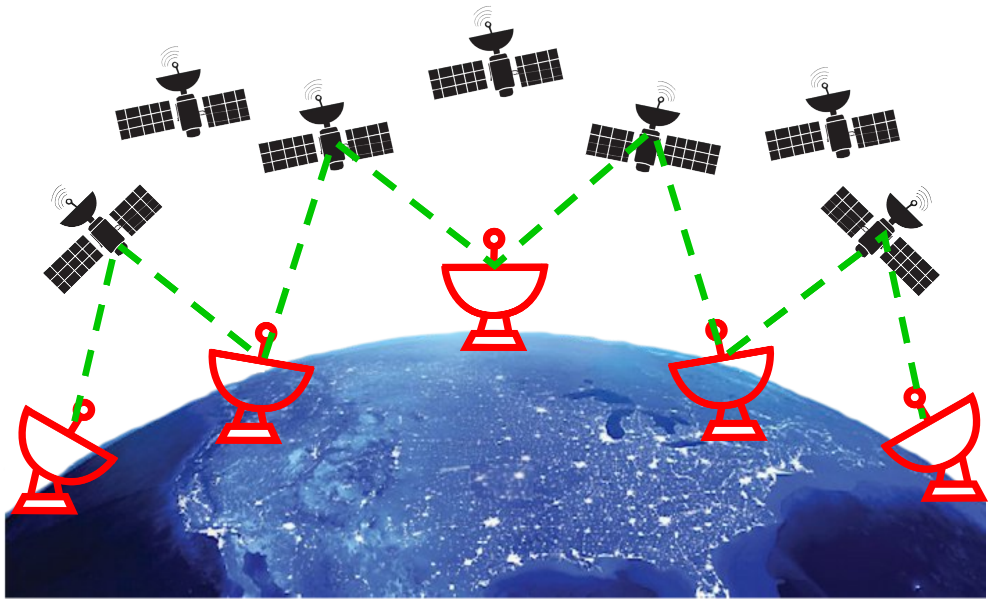


satellite channel

- Broadcast (multicast) down
- unicast up

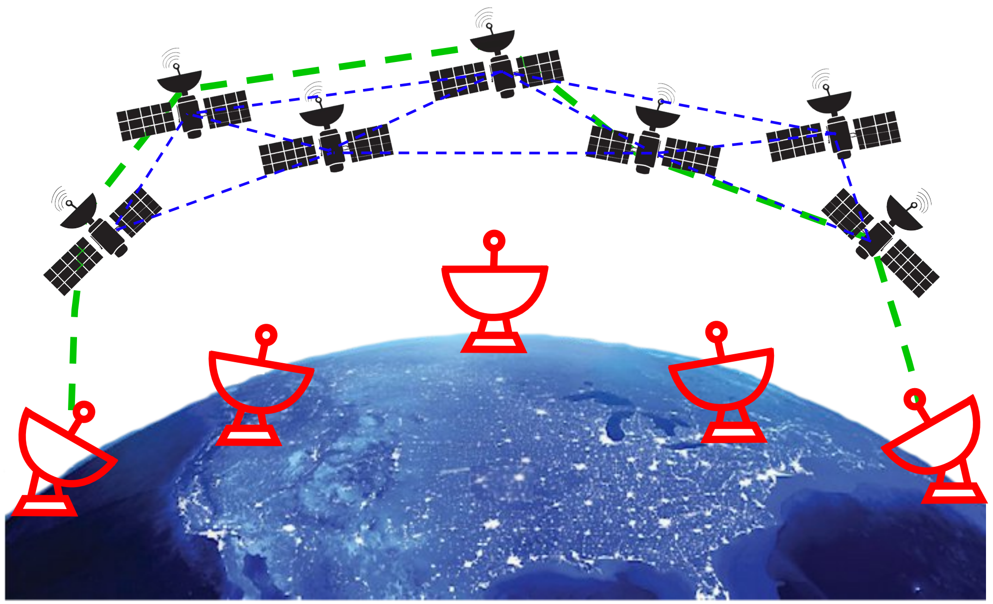
Satellite networking: a *link* or a *network*?

links in the sky



- single satellite hop between base stations
- AKA “bent pipe” architecture

network in the sky:



- multiple satellite hops between base stations
- routing among satellites

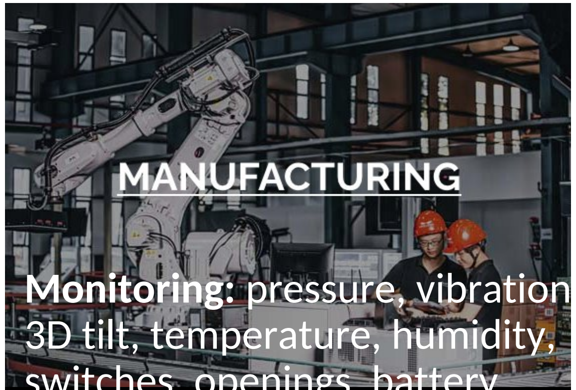
Starlink

- April 2025: ~7,239 operational LEO satellites (planned: 12K, requesetd:30K)
  - first launches: 2019
  - three low-Earth-orbit orbital shells, at 525, 530, 535 km
  - satellites: 500 – 2700 lbs

60 Starlink satellites stacked together before deployment on 24 May 2019

- services:
  - Internet service: 4M subscribers in Sept 2024 (residential US: $120/mo)
  - service in Ukraine (terrestrial networks damaged)
  - 2024: testing direct-to-smartphone tests would use cellular spectrum from SpaceX’s U.S. mobile partner T-Mobile

IoT: many, many use cases!



MANUFACTURING

Monitoring: pressure, vibration, 3D tilt, temperature, humidity, switches, openings, battery charge, voltage, leaks, cracks, strain gauges, fill levels …

SUPPLY CHAIN & LOGISTICS

Asset geolocation, tracking warehouse security, monitoring transport conditions, e.g., for food safety …

SMART CITIES

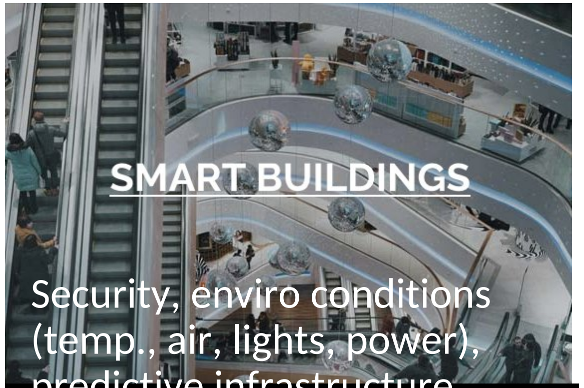
Monitoring: sound, air, water, weather, lighting, traffic, crowds, infrastrcuture; sharing (bikes) …

UTILITIES & ENERGY

Smart metering, service (de)activation , efficiency monitoring, remote diagnosis, asset surveillance, quality monitoring …

AGRICULTURE

rainfall, temperature, wind, humidity, animal tracking and health, soil condition, infrastructure monitoring …

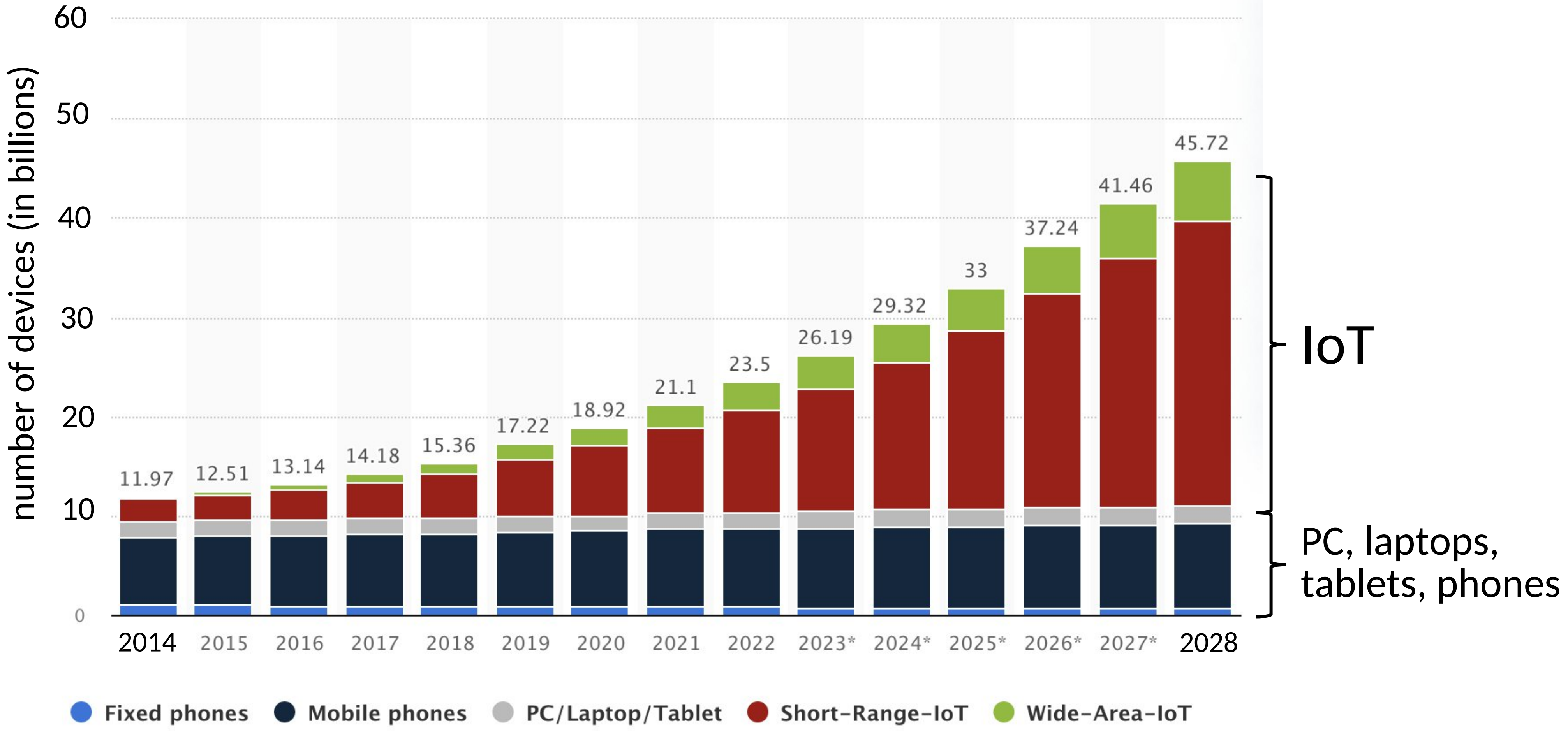


SMART BUILDINGS

Security, enviro conditions (temp., air, lights, power), predictive infrastructure monitoring, …

…. and there's many more!

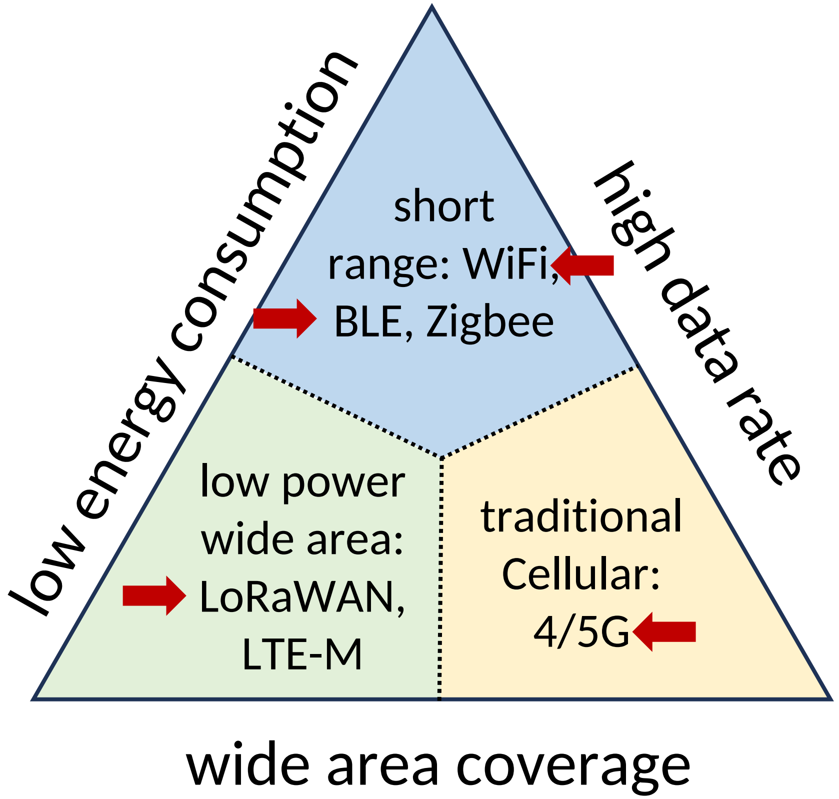
Lots of connected IoT devices, and more soon!



https://www.statista.com/statistics/512650/worldwide-connected-devices-amount/

IoT communication requirements

- wireless
- distance: from meters to kilometers
- data rate: 100’s bps when active (metering) to ~1 Mbps (video surveillance)
- energy: always a consideration
  - up ~10 years without external power
  - local energy harvesting



IoT technical tradeoffs

Wireless and mobile networks: Summary

- The physical layer: radio
- The wireless *access* network
  - principles, WiFi, 5G
- The wireless core network
  - principles, 5G
- Mobility
- Bluetooth, satellite, IoT wireless networks

For a more extensive treatment of wireless and mobile networks visit: https://gaia.cs.umass.edu/wireless_and_mobile_networks