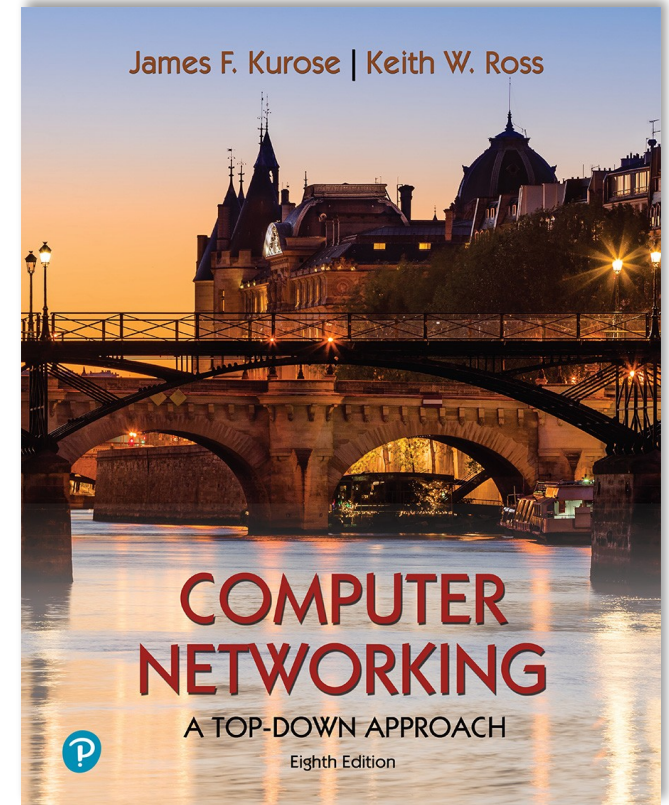


Chapter 7 Wireless and Mobile Networks



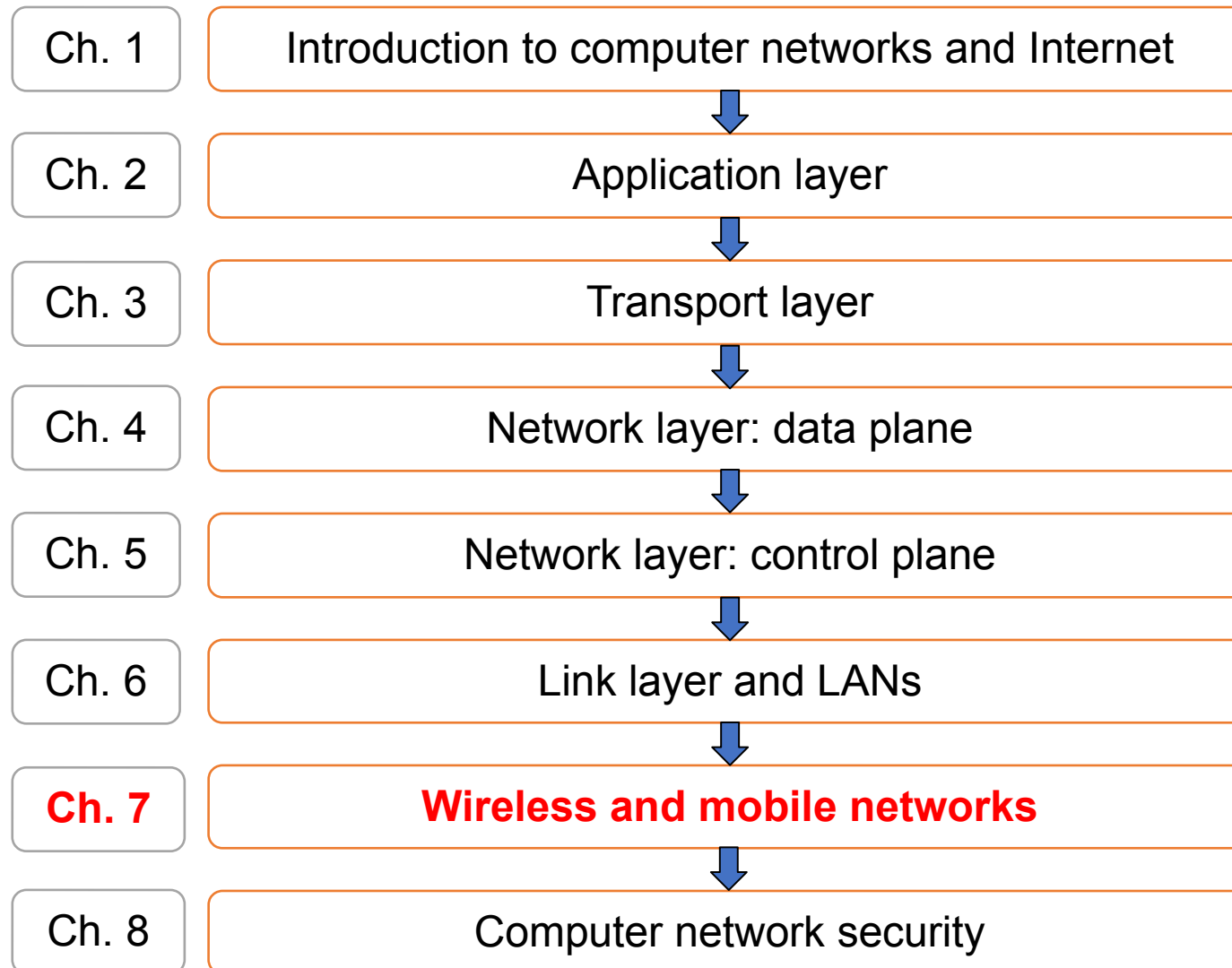
Computer Networking: A Top-Down Approach

8th edition

Jim Kurose, Keith Ross

Pearson, 2020

Course Roadmap



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 (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

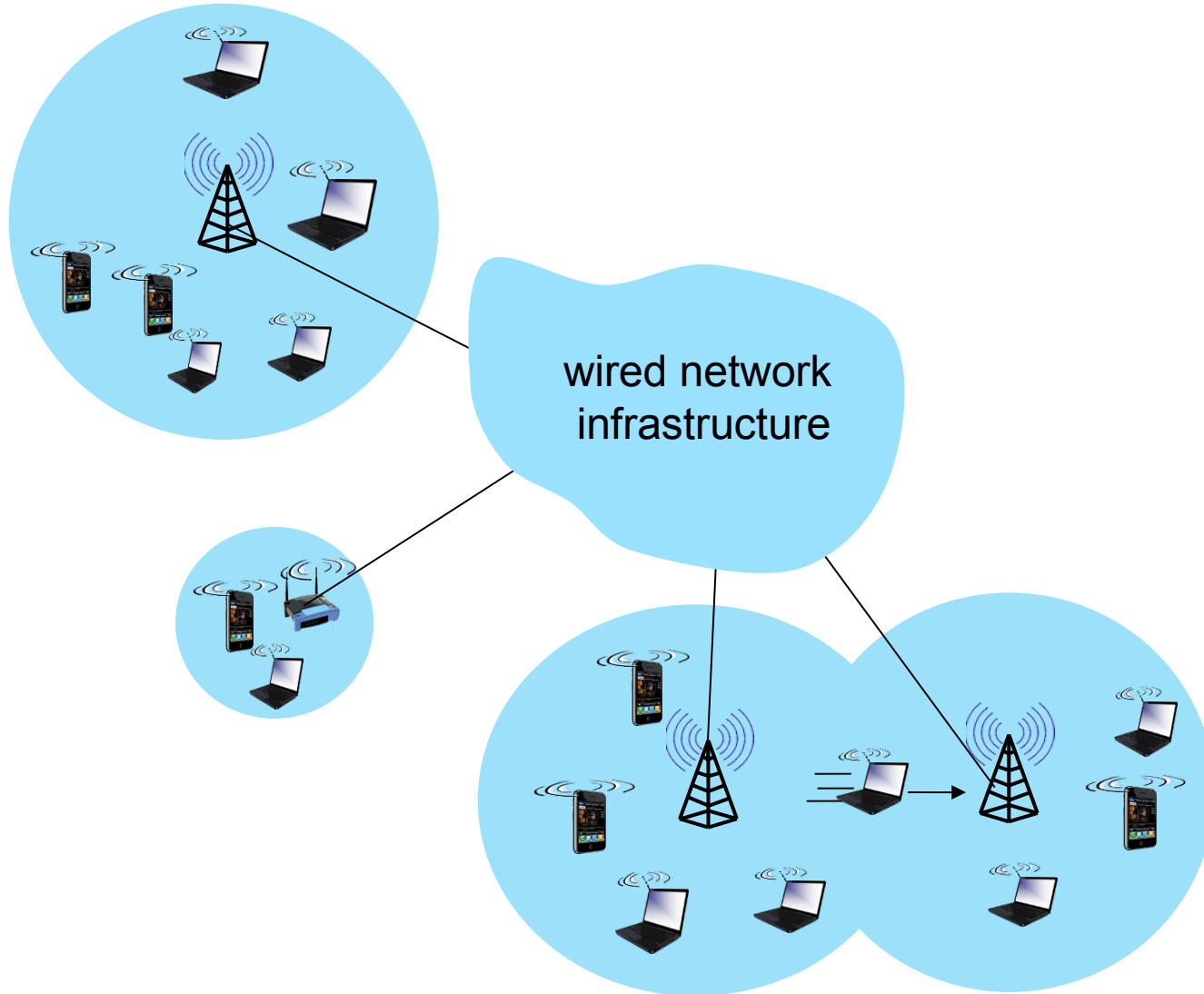
- Introduction

Wireless

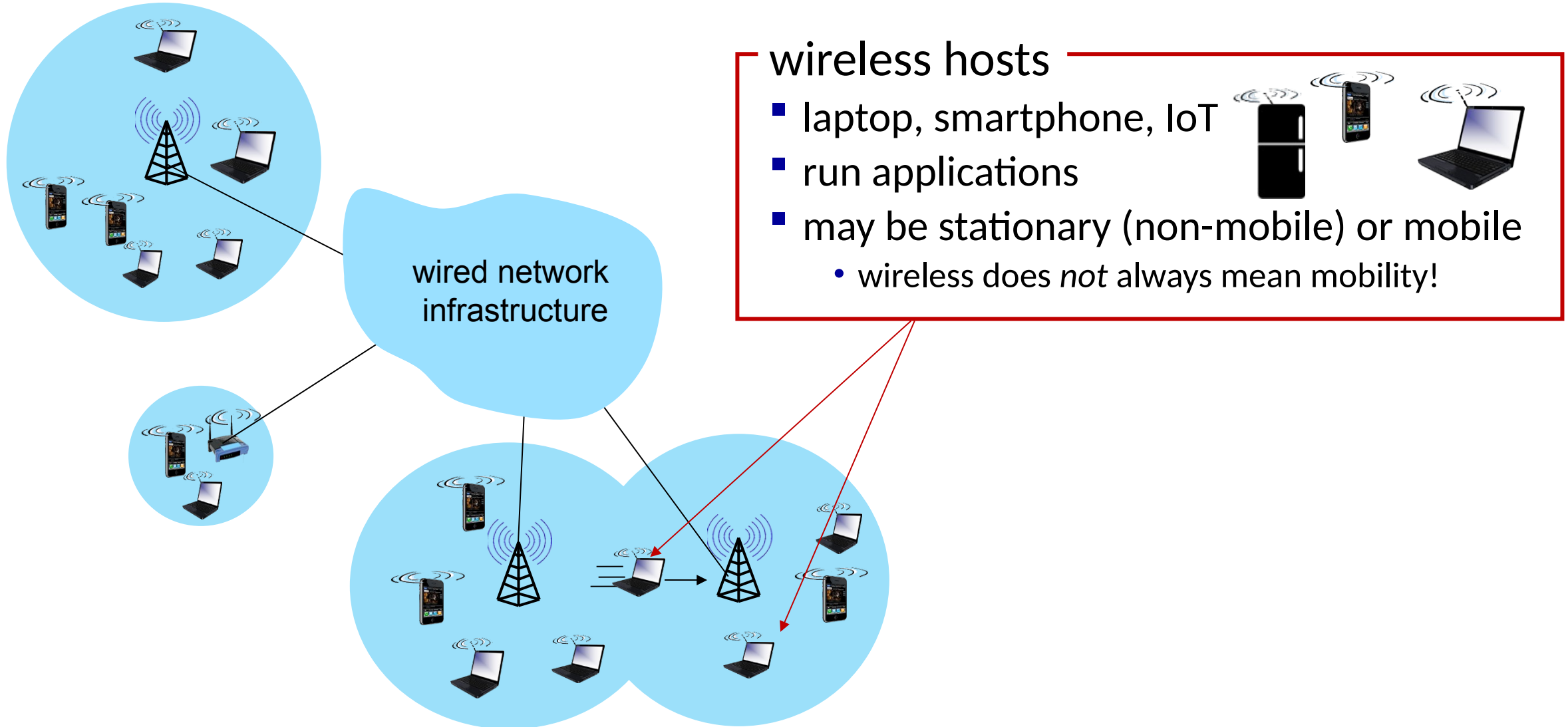
- Wireless Links and network characteristics
- WiFi: 802.11 wireless LANs
- Cellular networks: 4G and 5G



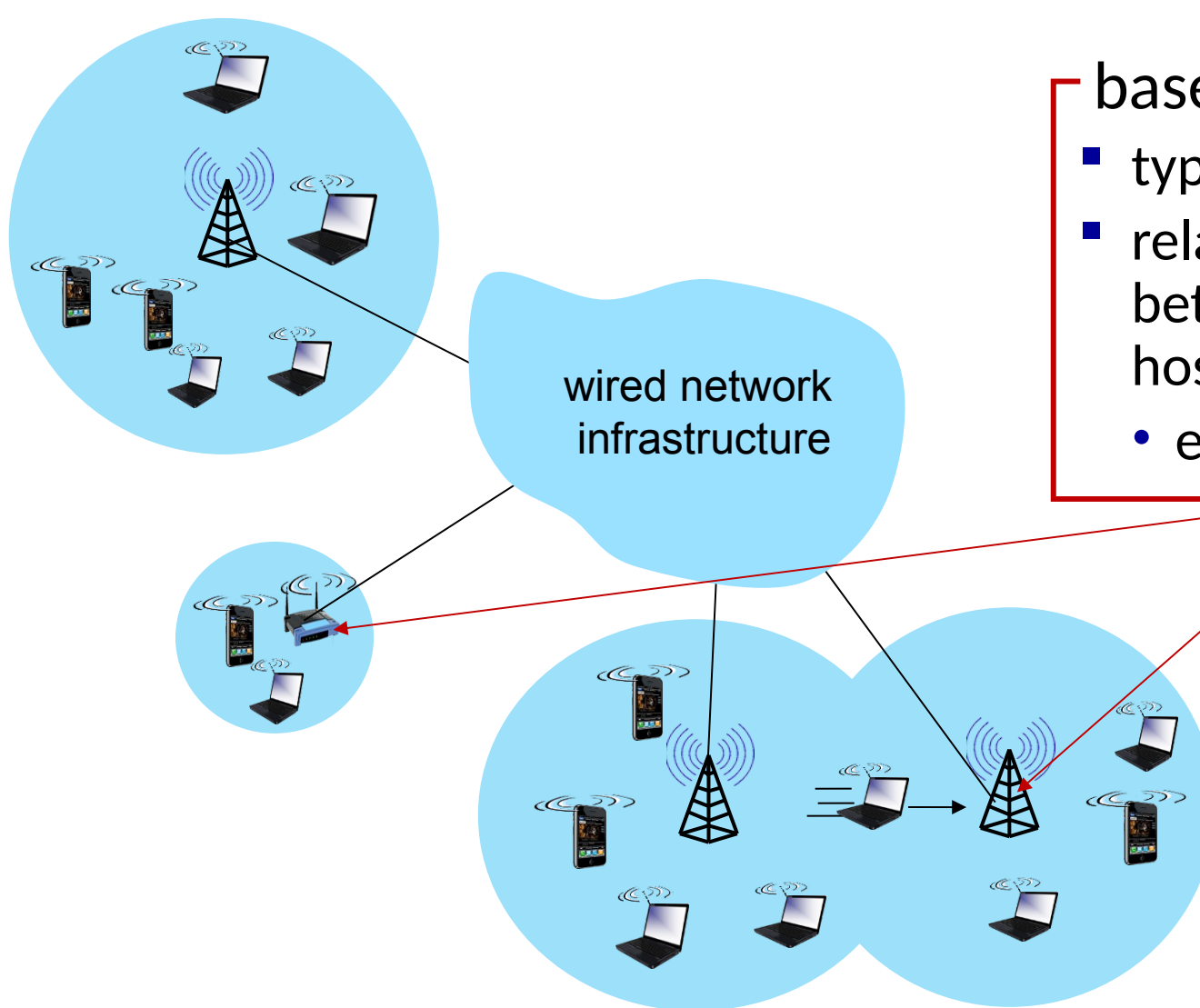
Elements of a wireless network



Elements of a wireless network



Elements of a wireless network

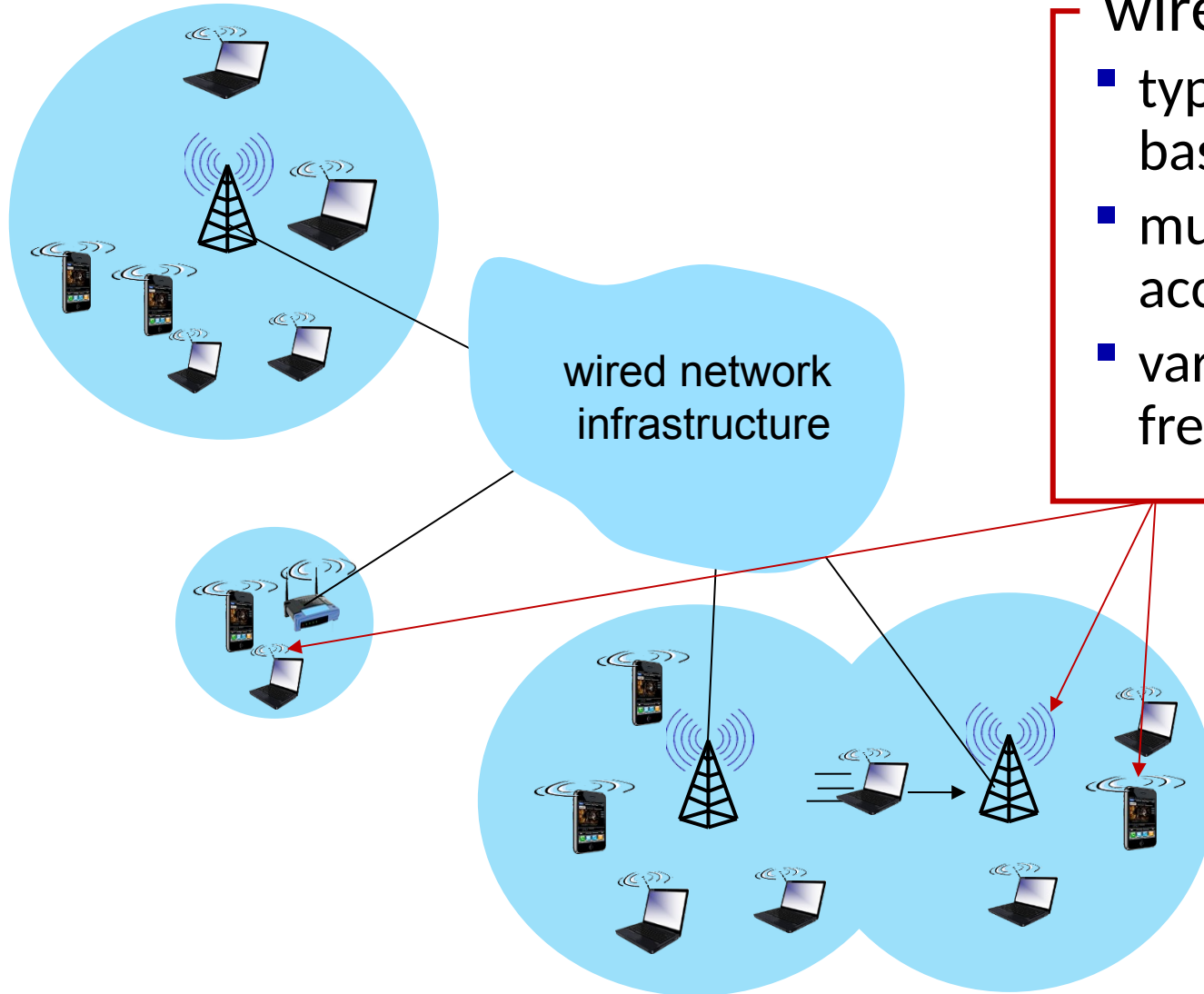


base station



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

Elements of a wireless network

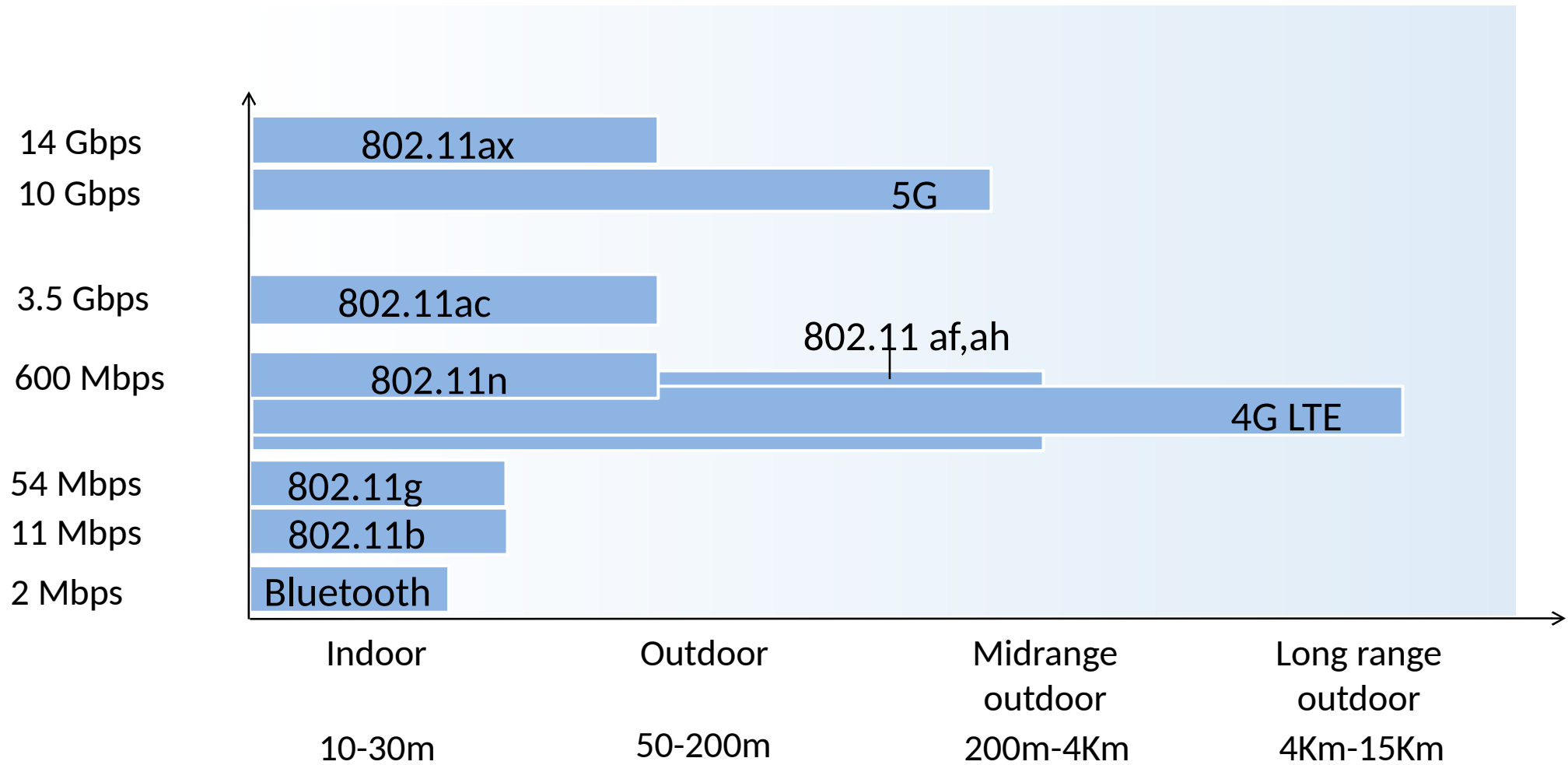


wireless link

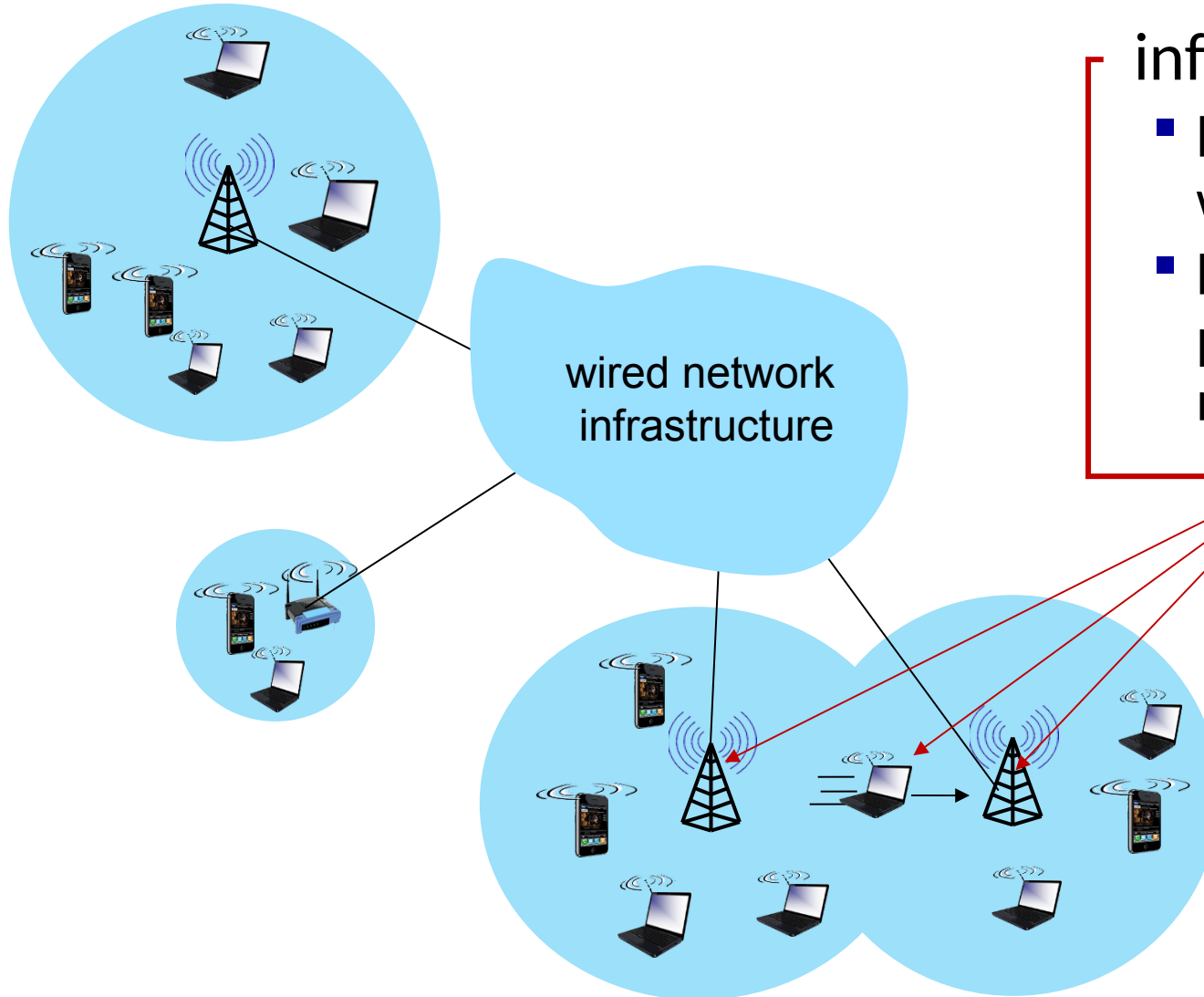


- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

Characteristics of selected wireless links



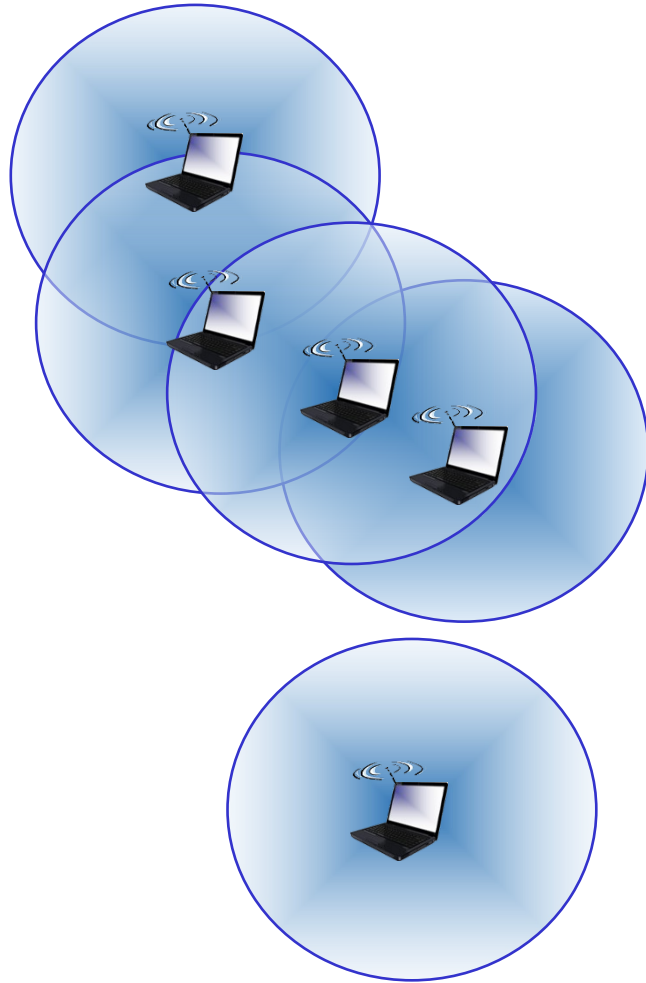
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: <i>mesh net</i>
<i>no infrastructure</i>	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Chapter 7 outline

- Introduction

Wireless

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

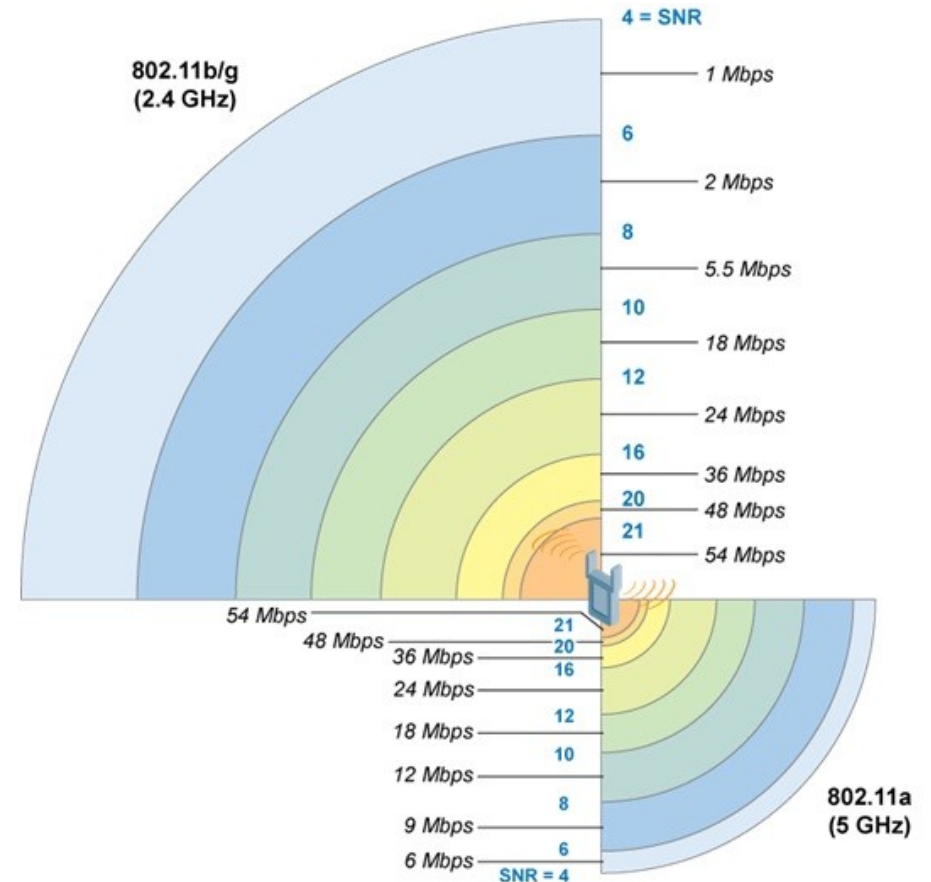
- **decreased signal strength:** radio signal attenuates as it propagates through matter (path loss)
- **interference from other sources:** wireless network frequencies (e.g., 2.4 GHz) shared by many devices (e.g., WiFi, cellular, motors): interference
- **multipath propagation:** radio signal reflects 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)

- SNR: signal-to-noise ratio
 - larger SNR – easier to extract signal from noise (a “good thing”)
- SNR and data rate
 - *given physical layer*: increase power -> increase SNR->increase data rate
 - *given SNR*: choose a modulation scheme that gives you the highest possible data rate for that SNR



<https://community.arubanetworks.com/browse/articles/blogviewer?blogkey=8659c839-8482-4388-a9e1-4589d8873eee>

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



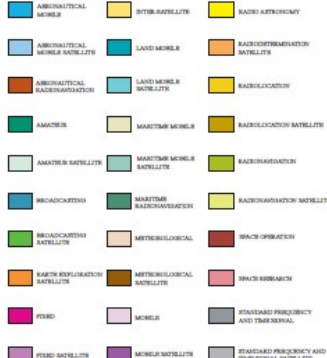
< 20KHz ?

Radio spectrum

UNITED
STATES
FREQUENCY
ALLOCATIONS

THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND



ACTIVITY CODE


 GOVERNMENT PRINTING OFFICE

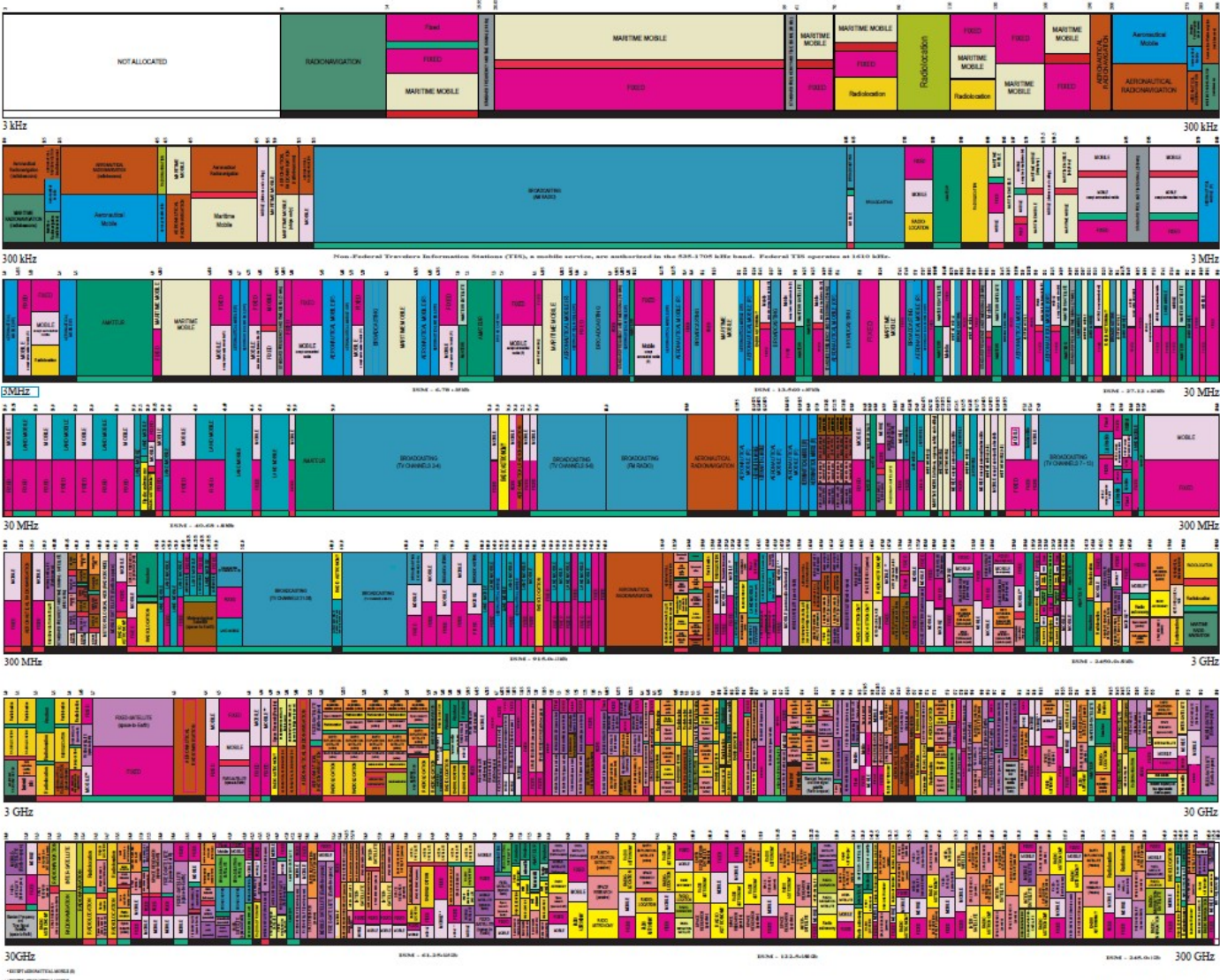
GOVERNMENT OF GOVERNMENT STAFF

ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FEED	Capital Letters
Secondary	FEED	Capital Letters

This chart is a graphic depiction in line pattern of the Table of Frequency Allocations used by the FCC. It is not intended to constitute a legal document. It does not constitute a contract and does not create any legal rights or obligations. It is not intended to constitute a legal document. It does not constitute a contract and does not create any legal rights or obligations.

 U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management
August 2011



Radio frequency spectrum: 3 KHz to 300 GHz

https://www.ntia.doc.gov/files/ntia/publications/spectrum_wall_chart_aug2011.pdf 6-17

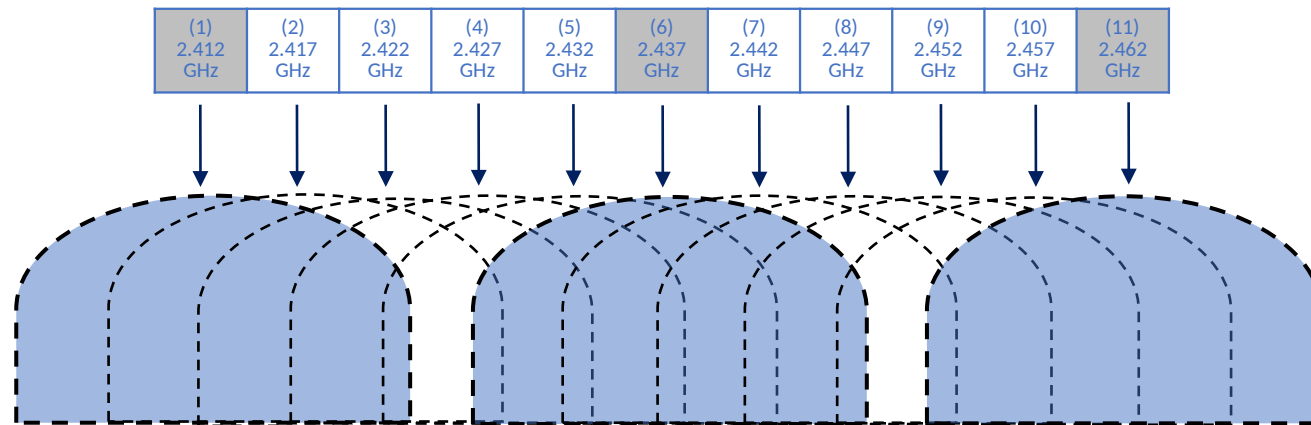
IEEE 802.11 Wireless LAN

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	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

Non-overlapping channels

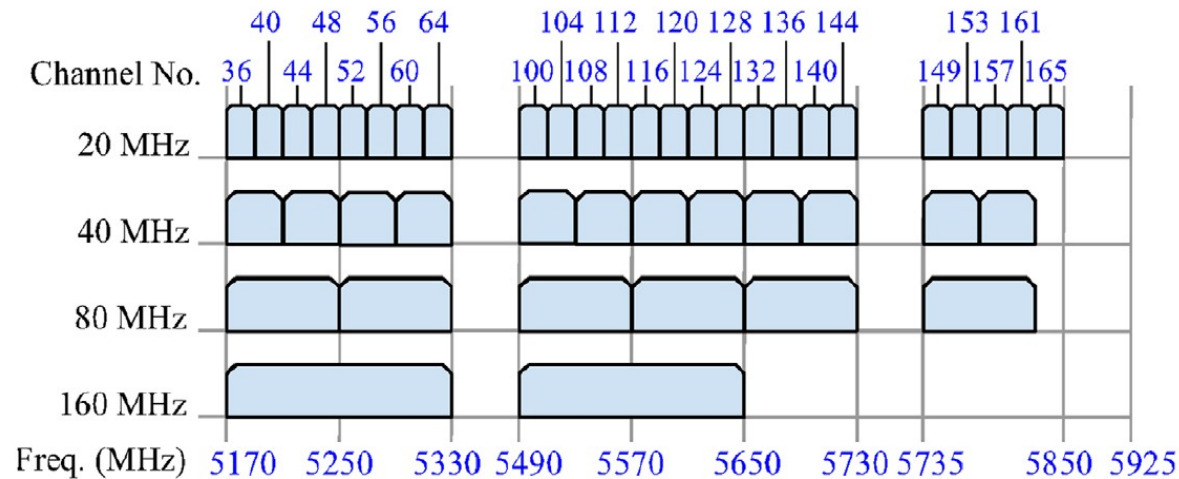
- 2.4 GHz ISM band
 - 11 channels of ~20 MHz bandwidth
 - 3 non overlapping channels (1, 6, 11)
 - 802.11 b/g/n



Non-overlapping channels

■ 5 GHz ISM band

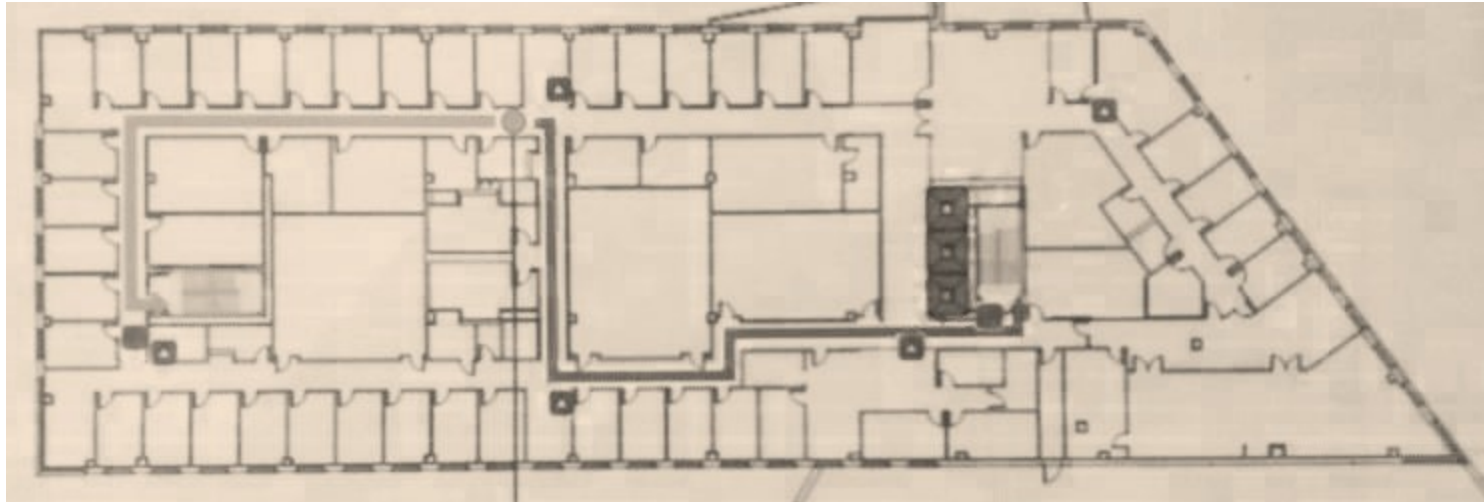
- 20 MHz bandwidth channels for 802.11a/n/ac
- 40 MHz bandwidth channels for 802.11n/ac
- 80 and 160 MHz bandwidth channels for 802.11ac



Non-overlapping channels	
20 MHz	25
40 MHz	12
80 MHz	6
160 MHz	2

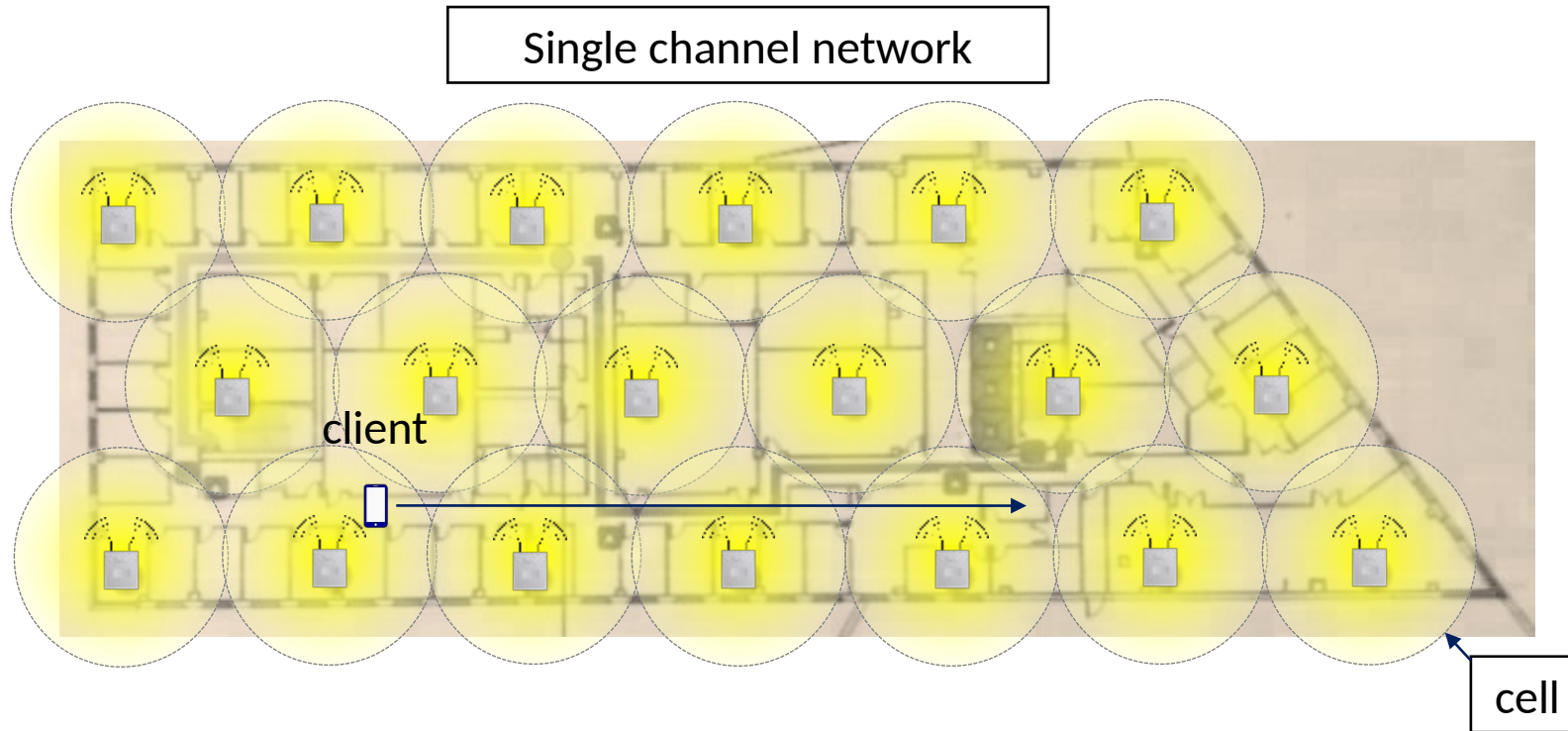
Frequency reuse and interference

- Deploy a WiFi network in the Engineering building



Frequency reuse and interference

- Deploy a WiFi network in the Engineering building

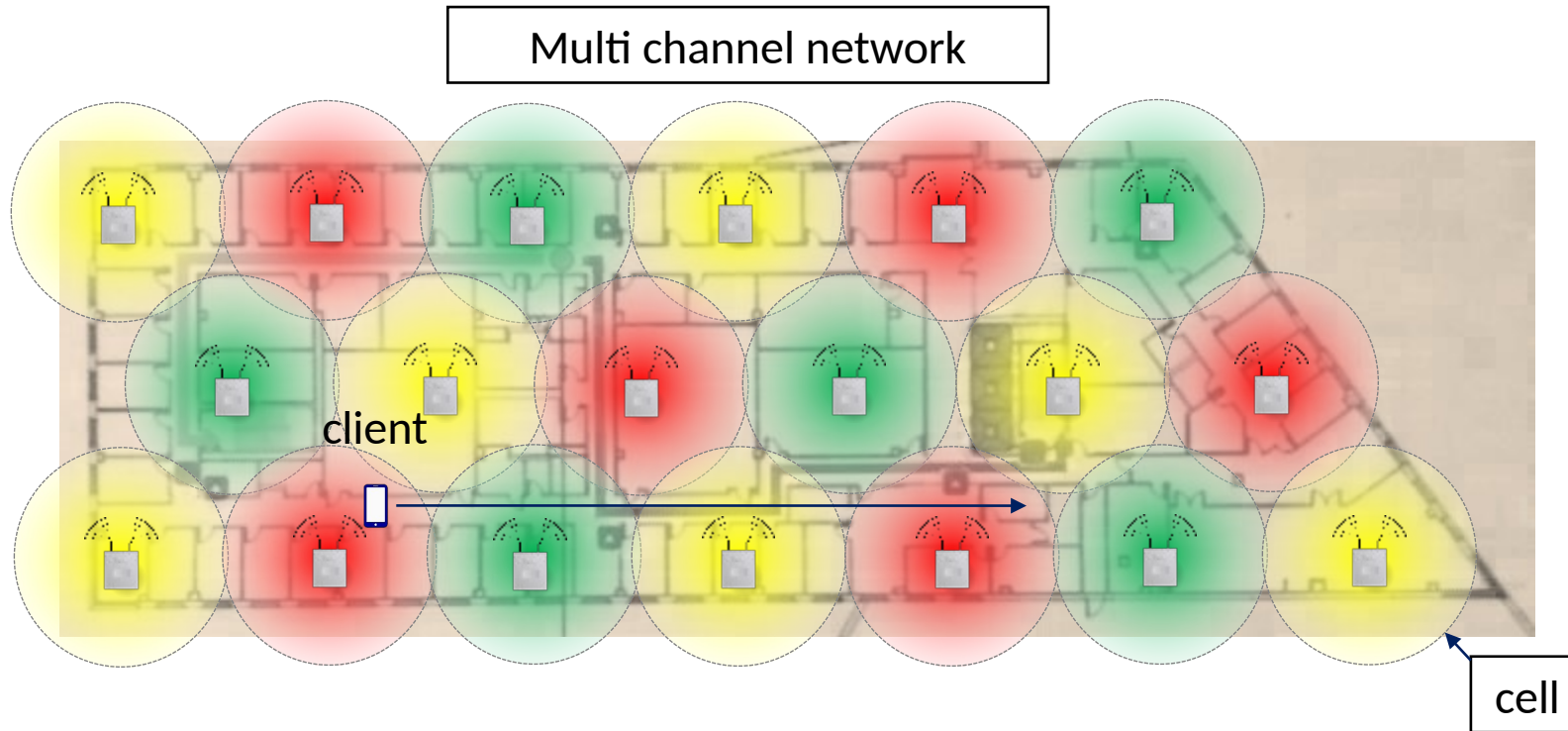


Use one channel from (1,6,11)

- Cons: Interference between adjacent cells
- Pros: Seamless mobility for clients roaming around different cells

Frequency reuse and interference

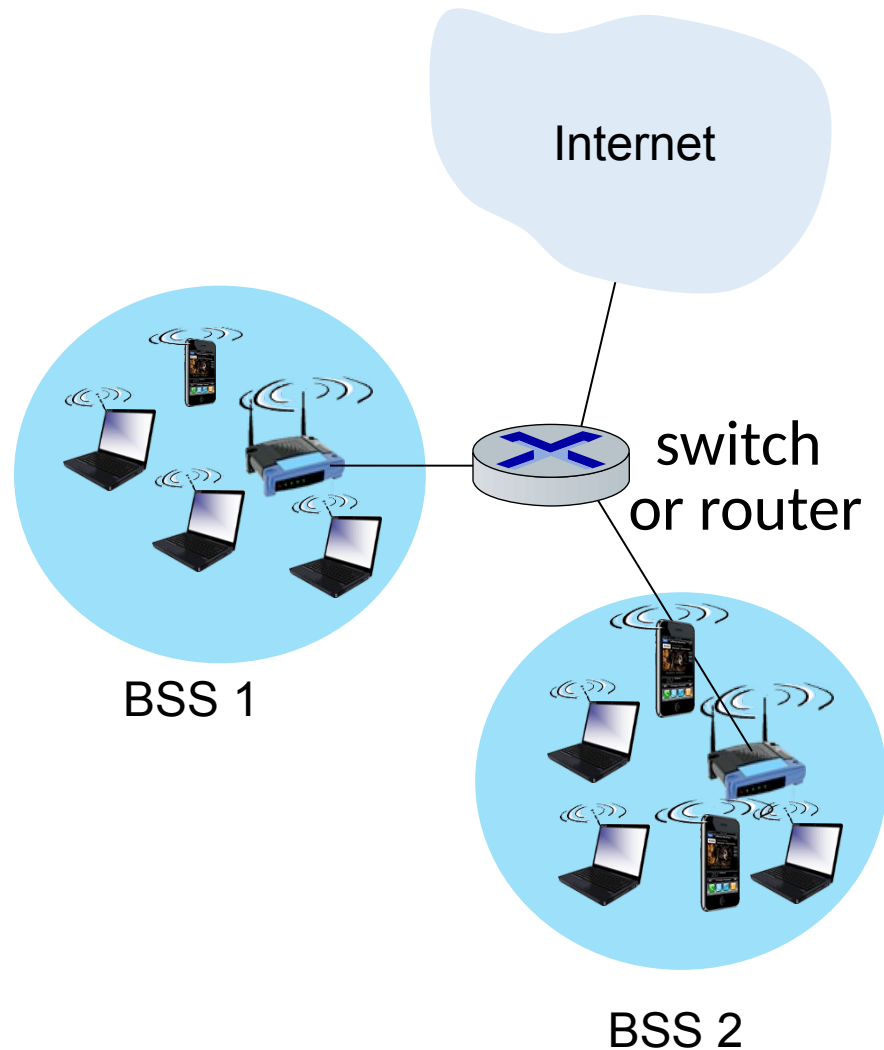
- Deploy a WiFi network in the Engineering building



Use three channels (1,6,11)

- Pros: lower interference between cells – higher data rates
- Cons: client mobility between cells is challenging

802.11 LAN architecture



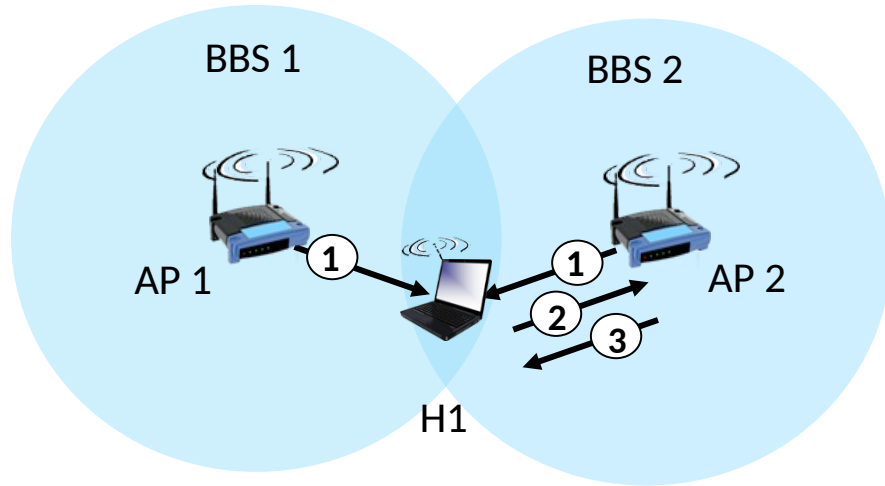
- wireless host communicates with base station
 - base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
 - wireless hosts
 - access point (AP): base station
 - ad hoc mode: hosts only

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

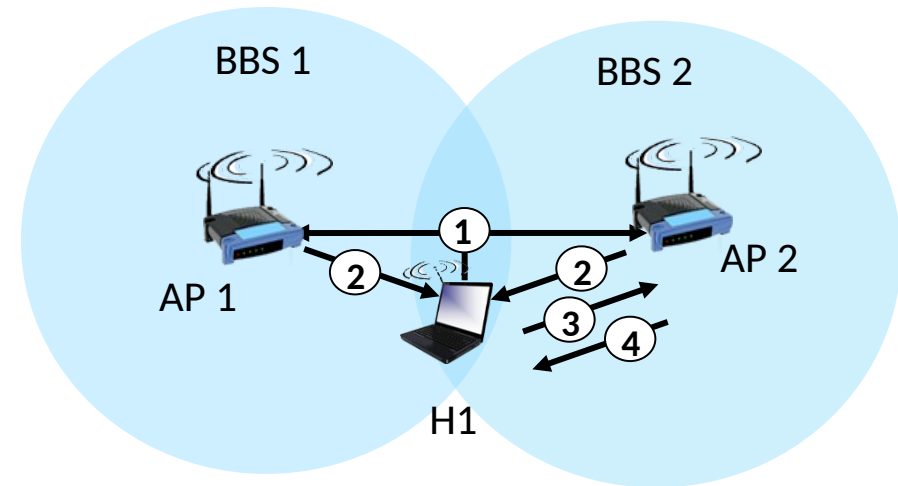


802.11: passive/active scanning



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

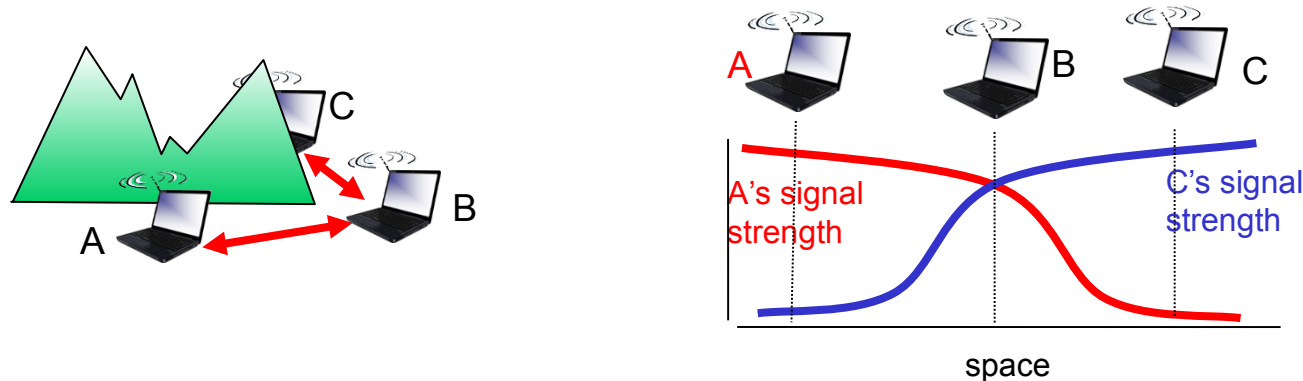


active scanning:

- (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

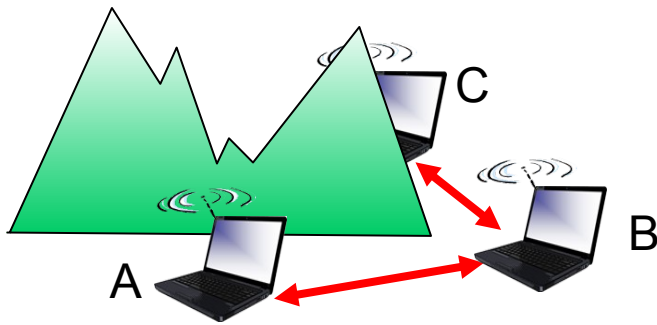
IEEE 802.11: multiple access

- 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/CollisionAvoidance



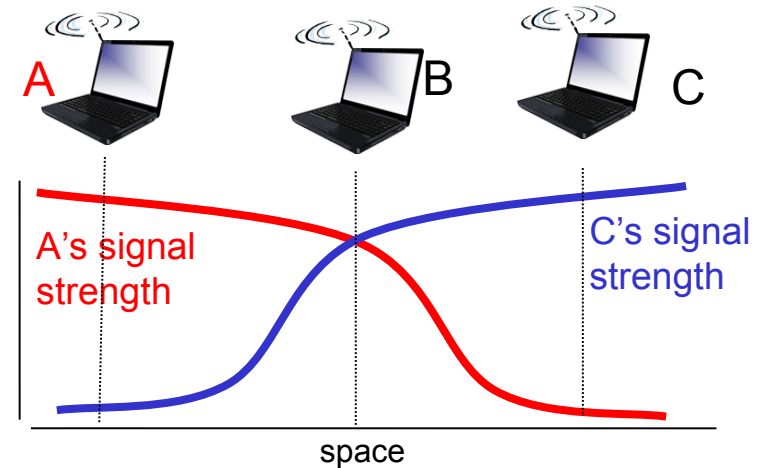
Wireless link characteristics (3)

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

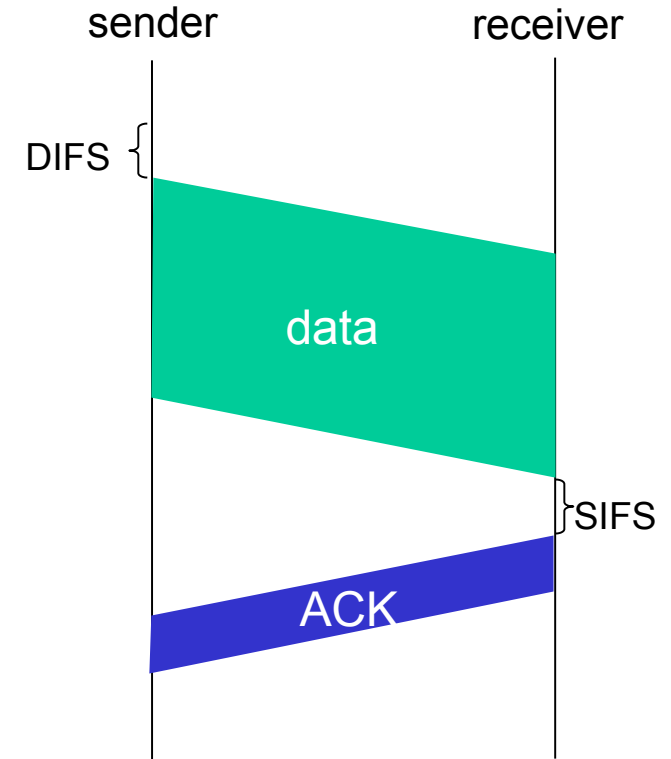
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

- 1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)
- 2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval, repeat 2

802.11 receiver

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



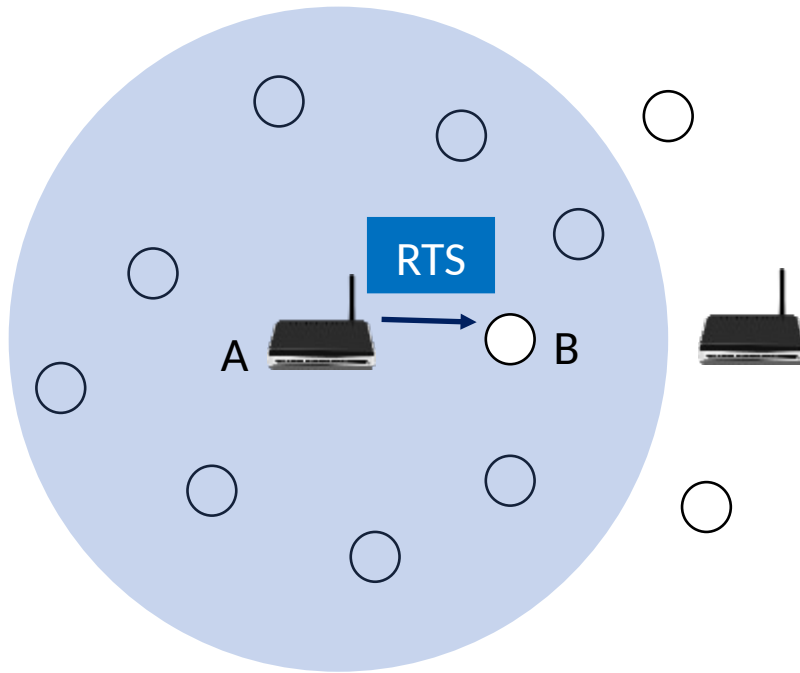
Avoiding collisions (more)

idea: sender “reserves” channel use for data frames using small reservation packets

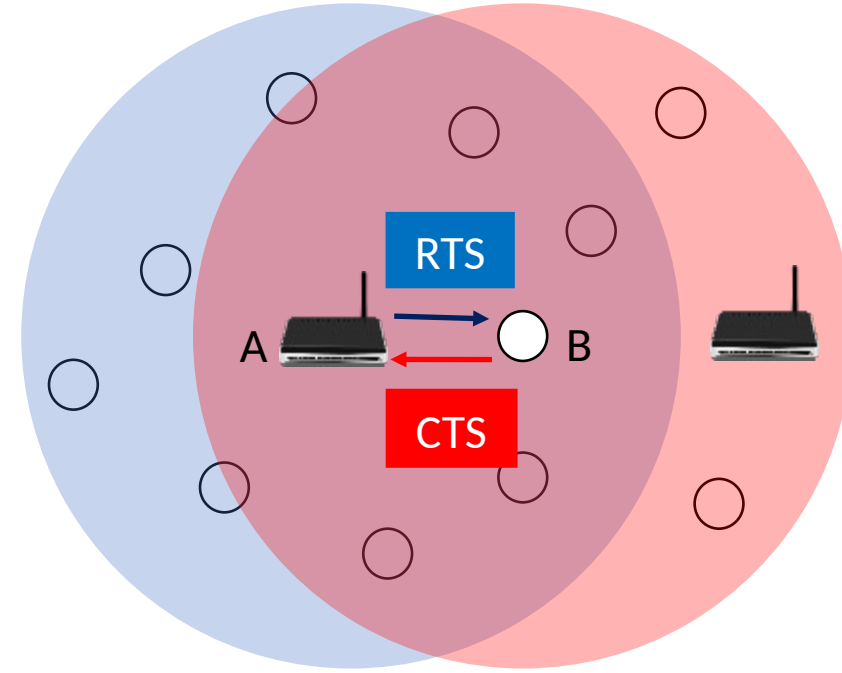
- sender first transmits *small* request-to-send (RTS) packet to BS using CSMA
 - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
 - sender transmits data frame
 - other stations defer transmissions

How to deal with hidden terminal problem?

- IEEE 802.11 suggests using explicit control frames
 - RTS – Request To Send
 - CTS – Clear To Send
- CSMA/CA – CSMA with Collision Avoidance
 - Nodes receiving RTS and CTS defer their transmissions

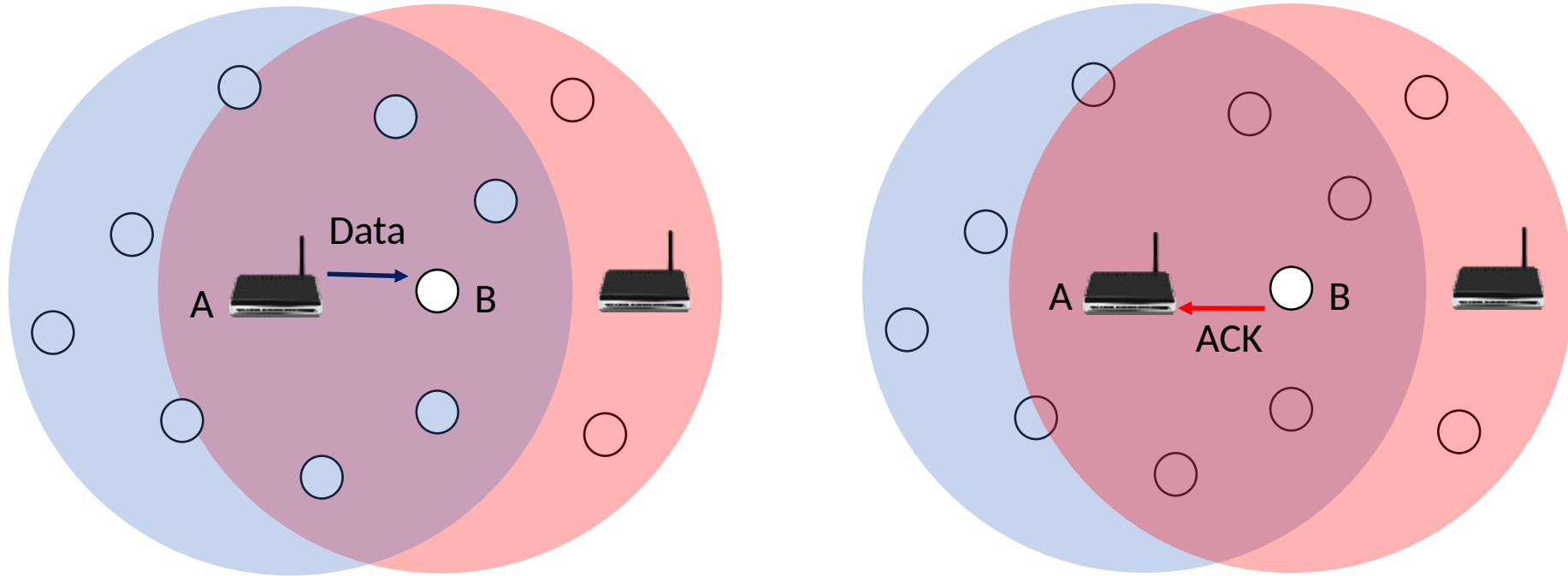


Node A sends RTS to B, all neighboring nodes receiving RTS defer their transmission



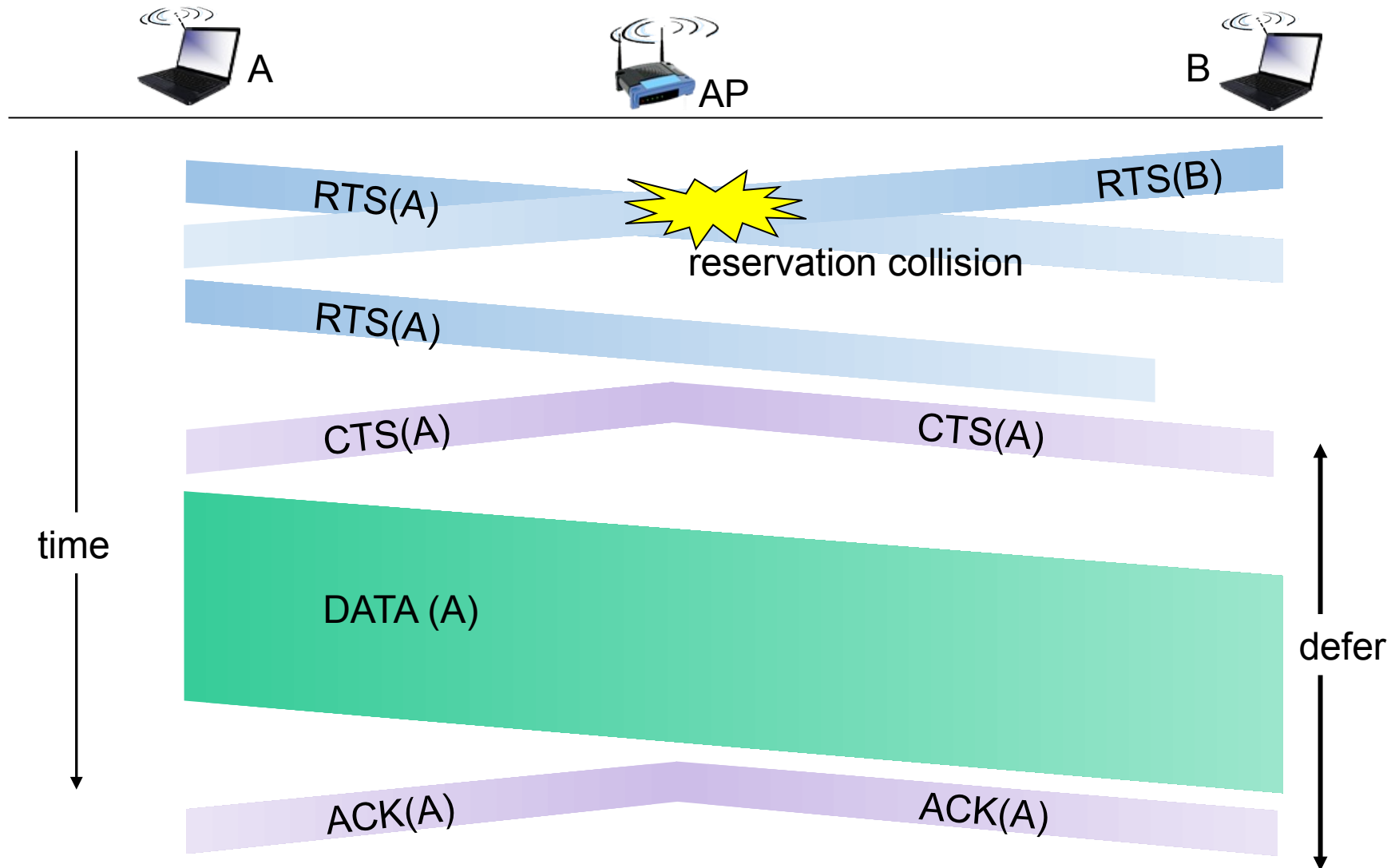
Node B sends CTS to A, all neighboring nodes receiving CTS defer their transmission

CSMA/CA

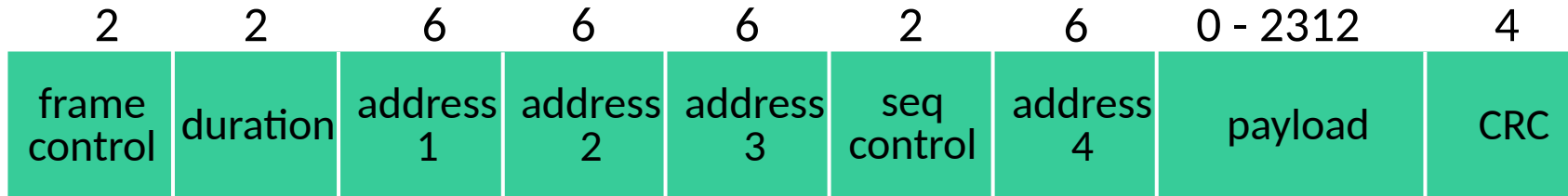


- How much neighboring nodes should wait?
 - RTS packet includes a time duration value which indicates the total time required for CTS return, data transmission and ACK return
 - Neighboring nodes set their Net Allocation Vector (NAV) to this duration and wait

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing



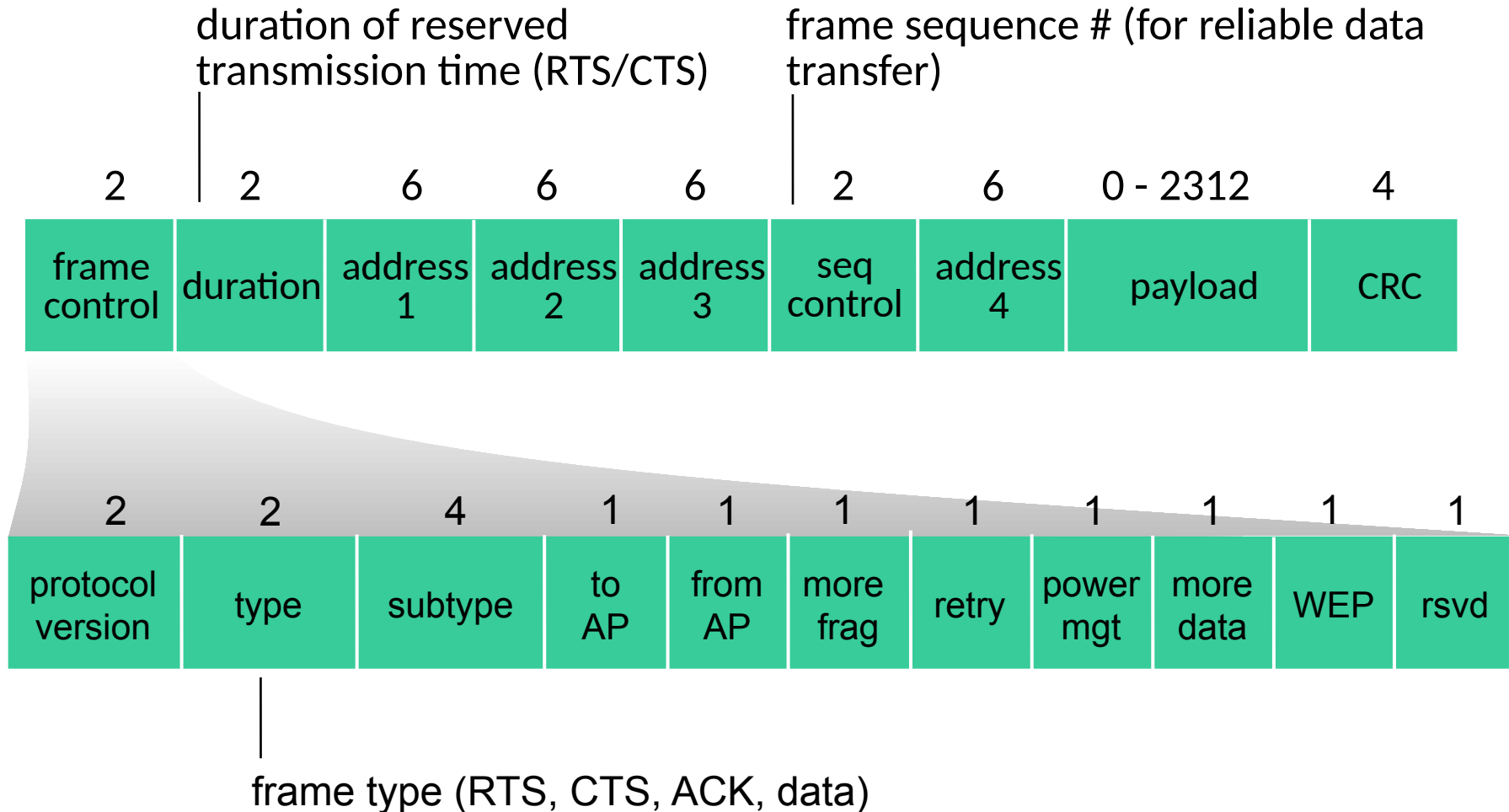
Address 1: MAC address of wireless host or AP to receive this frame

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

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

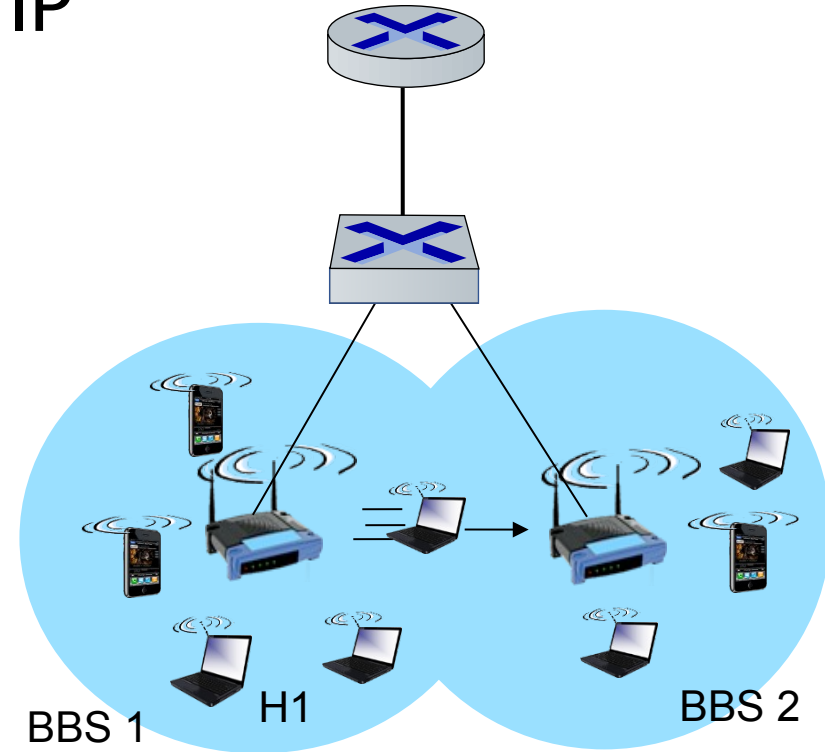
Address 4: used only in ad hoc mode

802.11 frame: addressing



802.11: mobility within same subnet

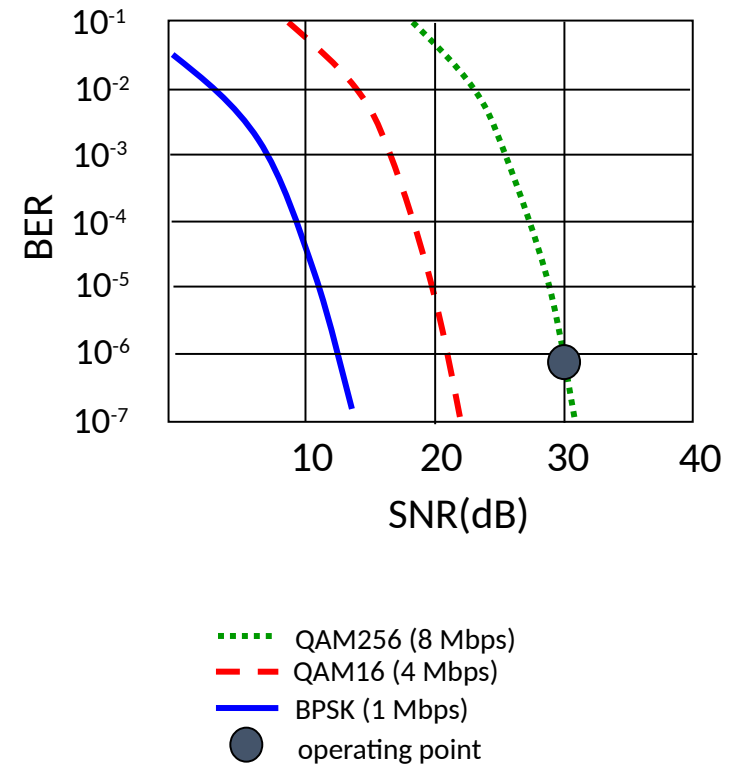
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
 - self-learning (Ch. 6): switch will see frame from H1 and “remember” which switch port can be used to reach H1



802.11: advanced capabilities

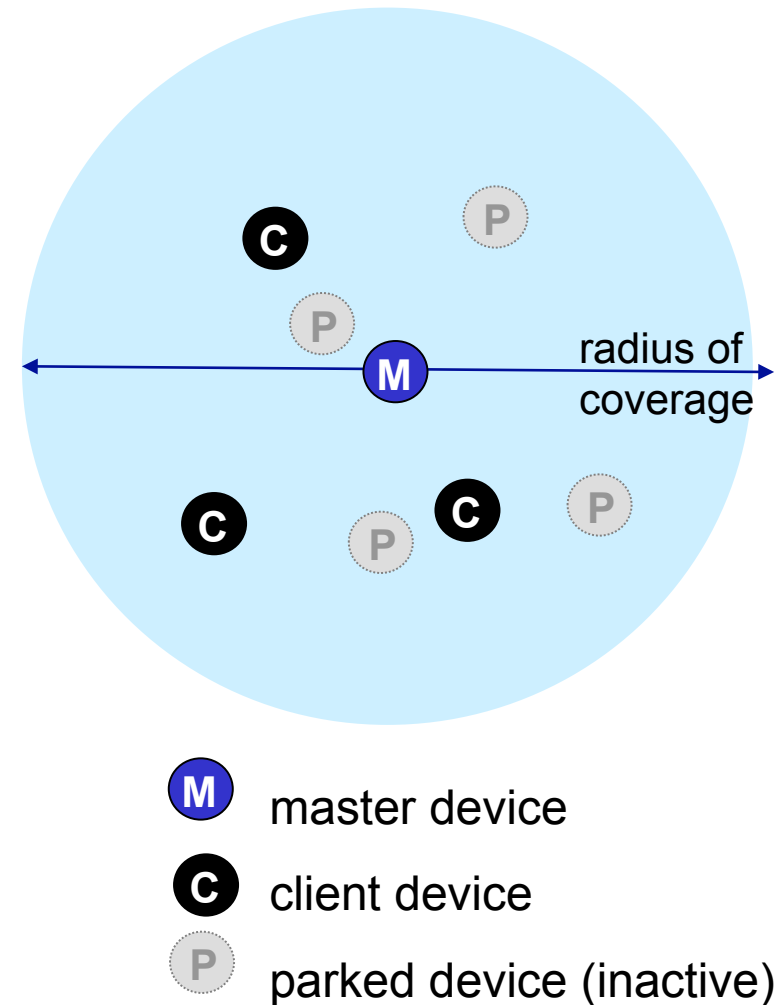
Rate adaptation

- 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



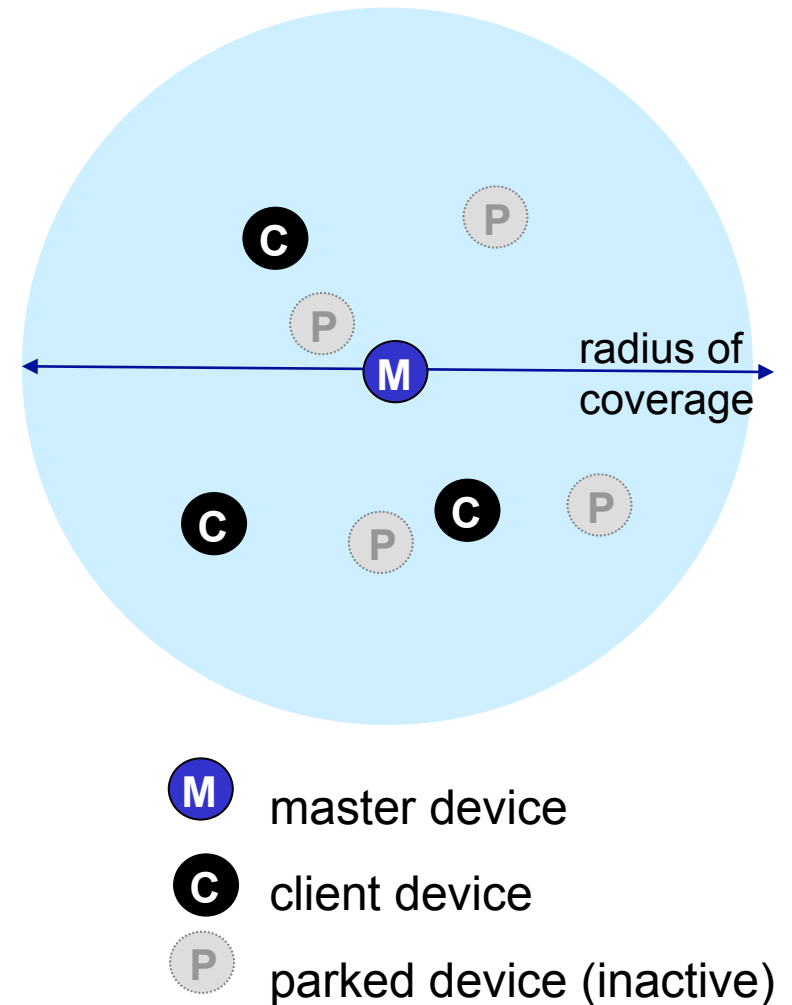
Personal area networks: Bluetooth

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- 2.4-2.5 GHz ISM radio band, up to 3 Mbps
- master controller / clients devices:
 - master polls clients, grants requests for client transmissions



Personal area networks: Bluetooth

- TDM, 625 μ sec sec. slot
- FDM: sender uses 79 frequency channels in known, pseudo-random order slot-to-slot (spread spectrum)
 - other devices/equipment not in piconet only interfere in some slots
- **parked mode:** clients can “go to sleep” (park) and later wakeup (to preserve battery)
- **bootstrapping:** nodes self-assemble (plug and play) into piconet



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



4G/5G cellular networks

- *the* solution for wide-area mobile Internet
- widespread deployment/use:
 - more mobile-broadband-connected devices than fixed-broadband-connected devices (5-1 in 2019)!
 - 4G availability: 97% of time in Korea (90% in US)
- transmission rates up to 100's Mbps
- technical standards: 3rd Generation Partnership Project (3GPP)
 - www.3gpp.org
 - 4G: Long-Term Evolution (LTE) standard

4G/5G cellular networks

similarities to wired Internet

- edge/core distinction, but both below to same carrier
- global cellular network: a network of networks
- widespread use of protocols we've studied: HTTP, DNS, TCP, UDP, IP, NAT, separation of data/control planes, SDN, Ethernet, tunneling
- interconnected to wired Internet

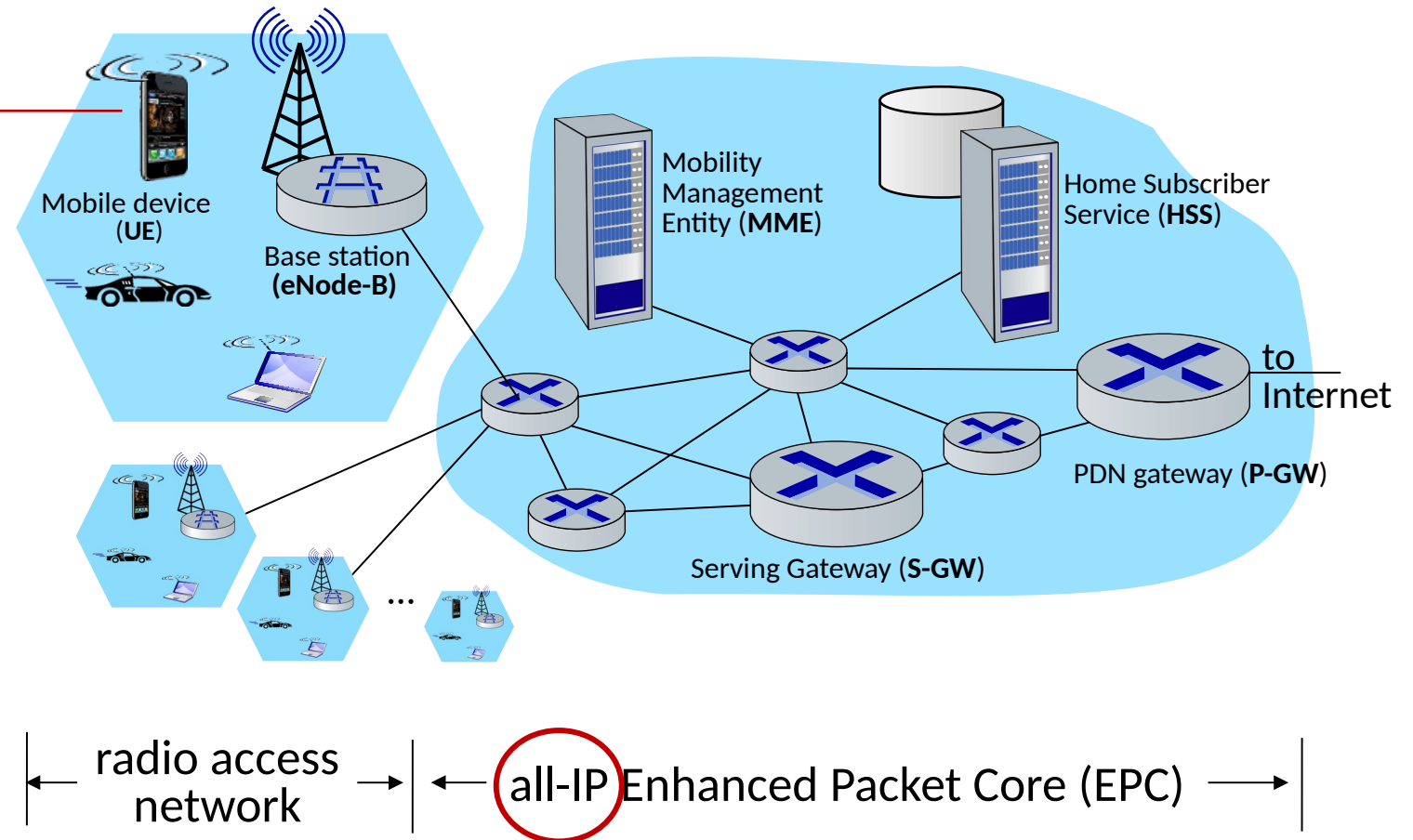
differences from wired Internet

- different wireless link layer
- mobility as a 1st class service
- user “identity” (via SIM card)
- business model: users subscribe to a cellular provider
 - strong notion of “home network” versus roaming on visited nets
 - global access, with authentication infrastructure, and inter-carrier settlements

Elements of 4G LTE architecture

Mobile device:

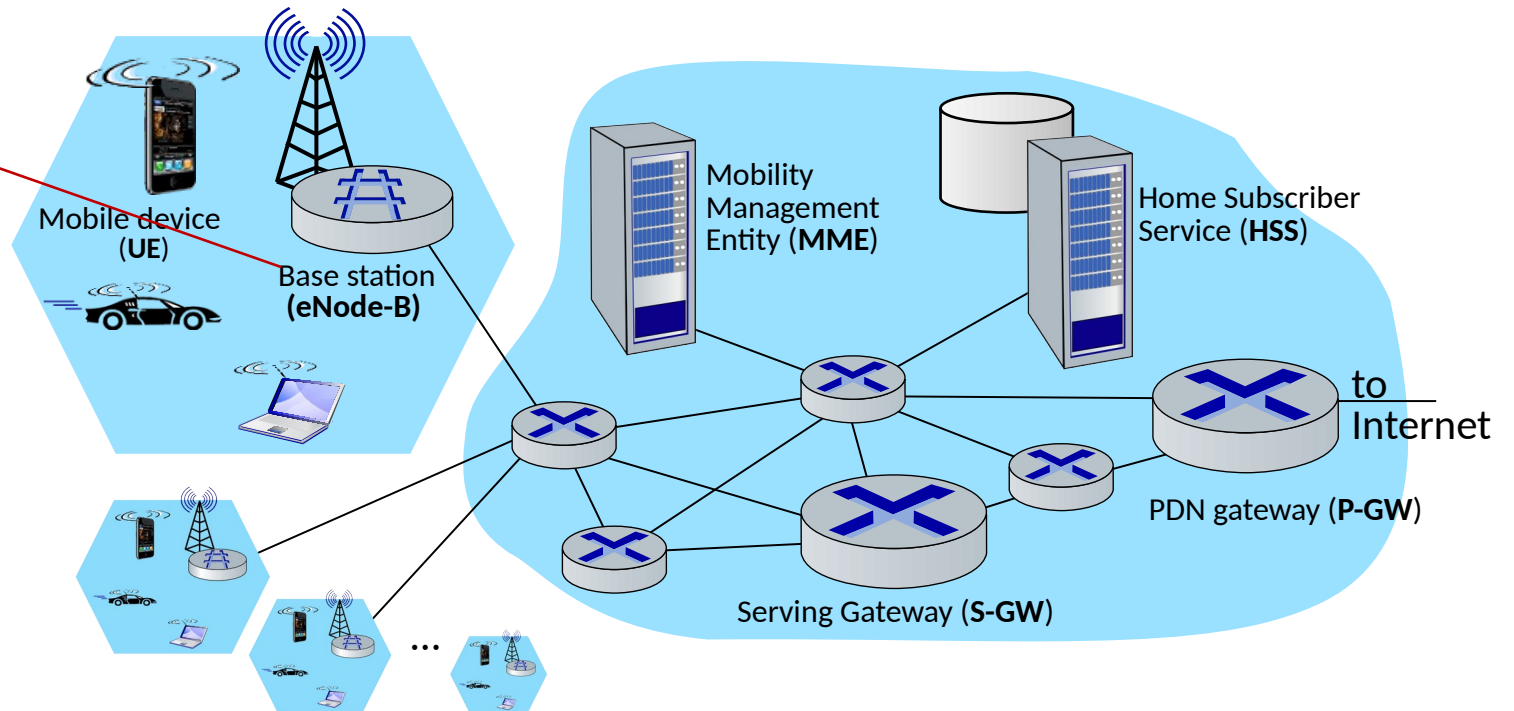
- smartphone, tablet, laptop, IoT, ... with 4G LTE radio
- 64-bit International Mobile Subscriber Identity (IMSI), stored on SIM (Subscriber Identity Module) card
- LTE jargon: User Equipment (UE)



Elements of 4G LTE architecture

Base station:

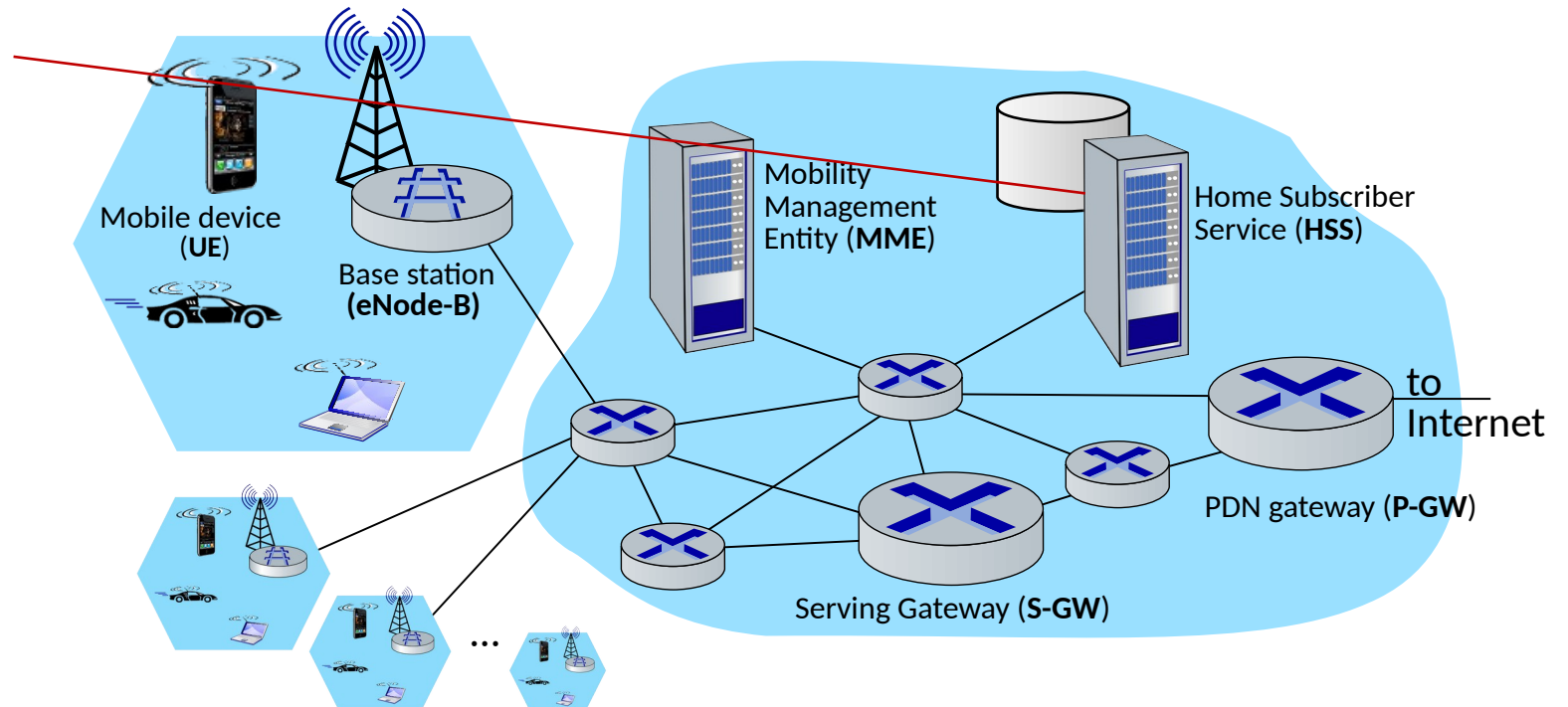
- at “edge” of carrier’s network
- manages wireless radio resources, mobile devices in its coverage area (“cell”)
- coordinates device authentication with other elements
- similar to WiFi AP but:
 - active role in user mobility
 - coordinates with nearby base stations to optimize radio use
- LTE jargon: eNode-B



Elements of 4G LTE architecture

Home Subscriber Service

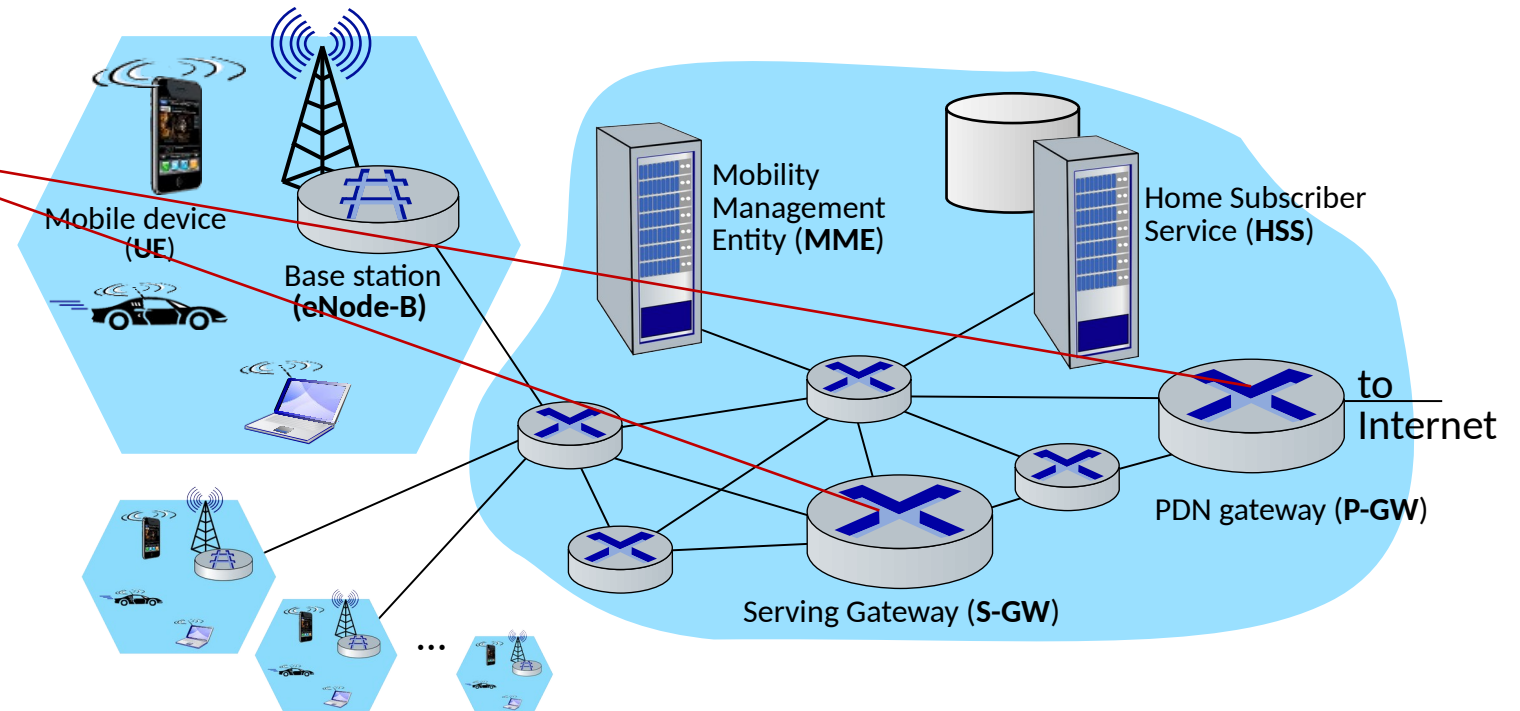
- stores info about mobile devices for which the HSS's network is their “home network”
- works with MME in device authentication



Elements of 4G LTE architecture

Serving Gateway (S-GW), PDN Gateway (P-GW)

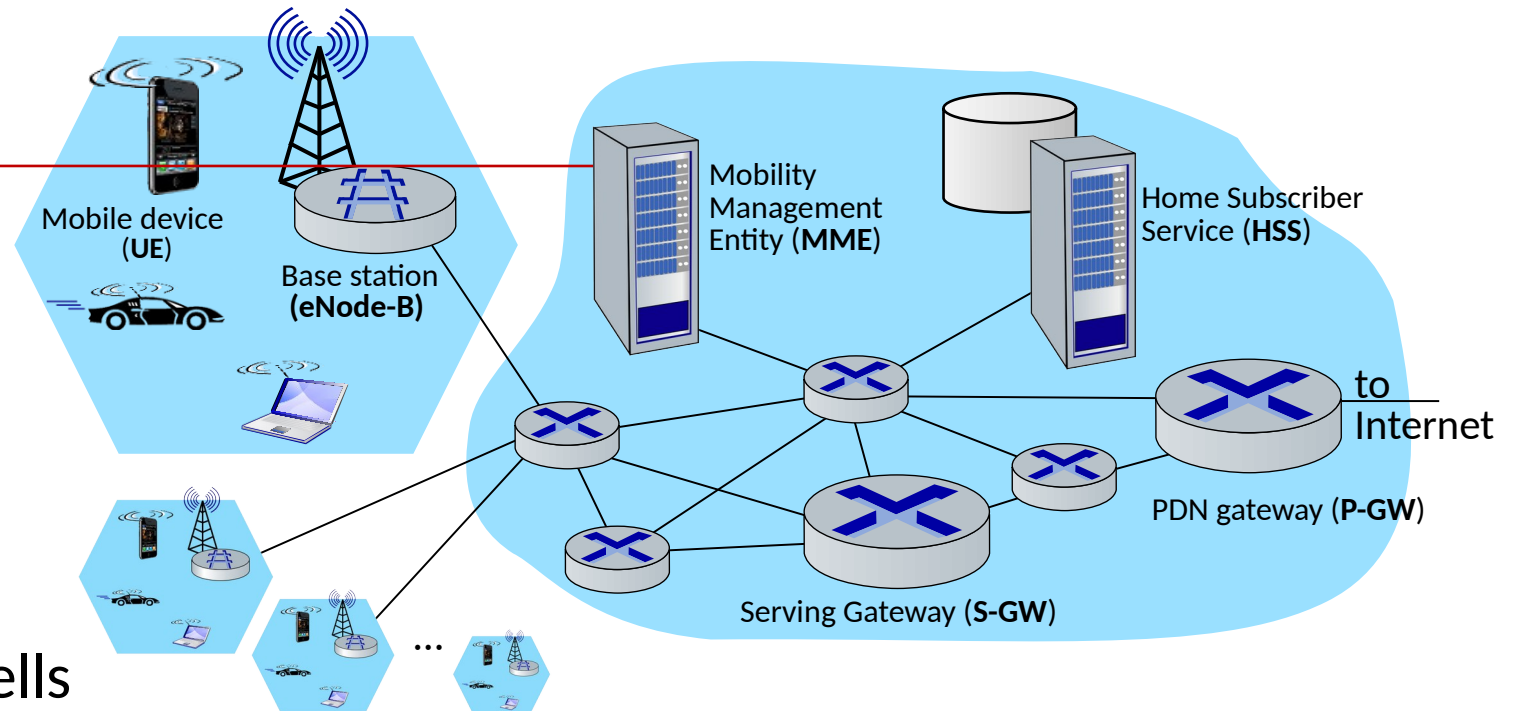
- lie on data path from mobile to/from Internet
- P-GW
 - gateway to mobile cellular network
 - Looks like any other internet gateway router
 - provides NAT services
- other routers:
 - extensive use of tunneling



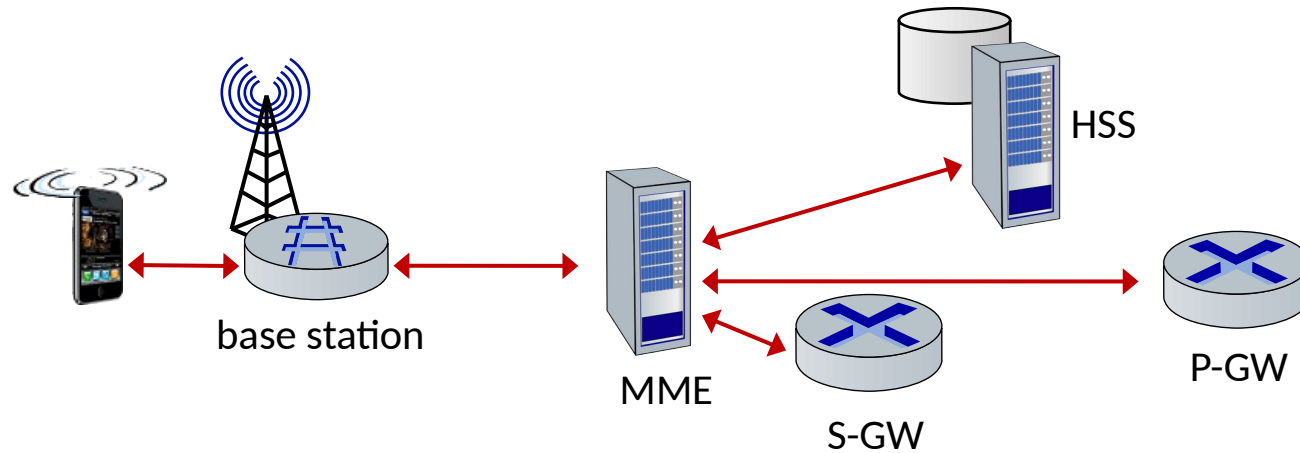
Elements of 4G LTE architecture

Mobility Management Entity

- device authentication (device-to-network, network-to-device) coordinated with mobile home network HSS
- mobile device management:
 - device handover between cells
 - tracking/paging device location
- path (tunneling) setup from mobile device to P-GW

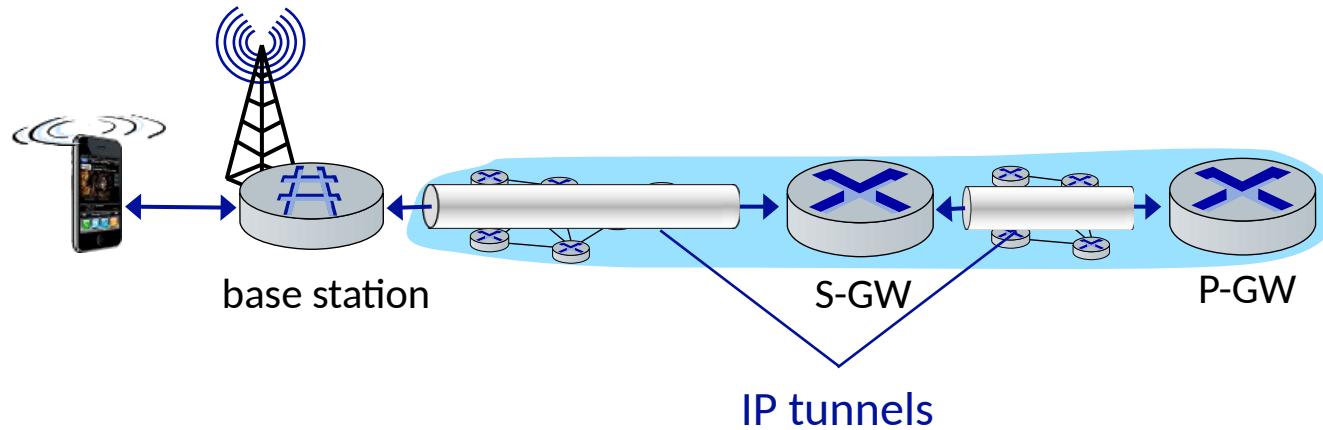


LTE: data plane control plane separation



control plane

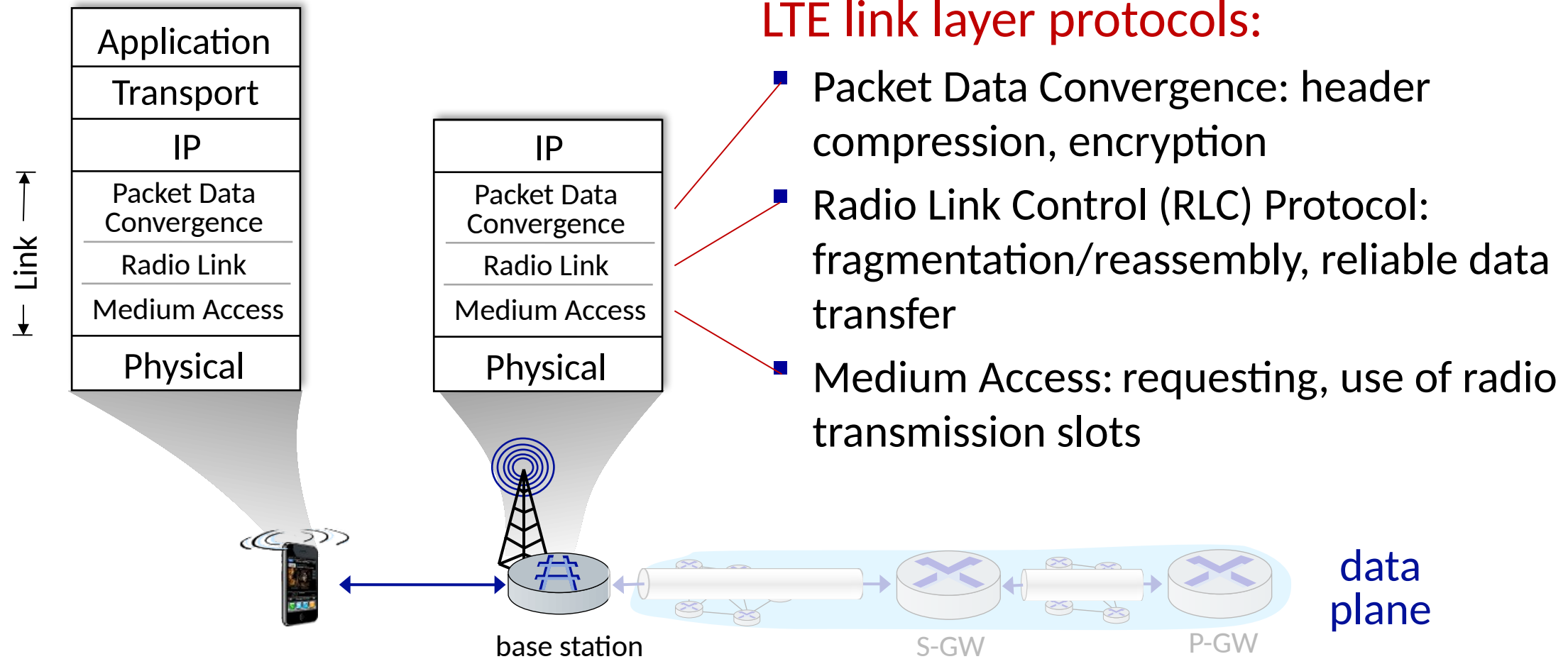
- new protocols for mobility management, security, authentication (later)



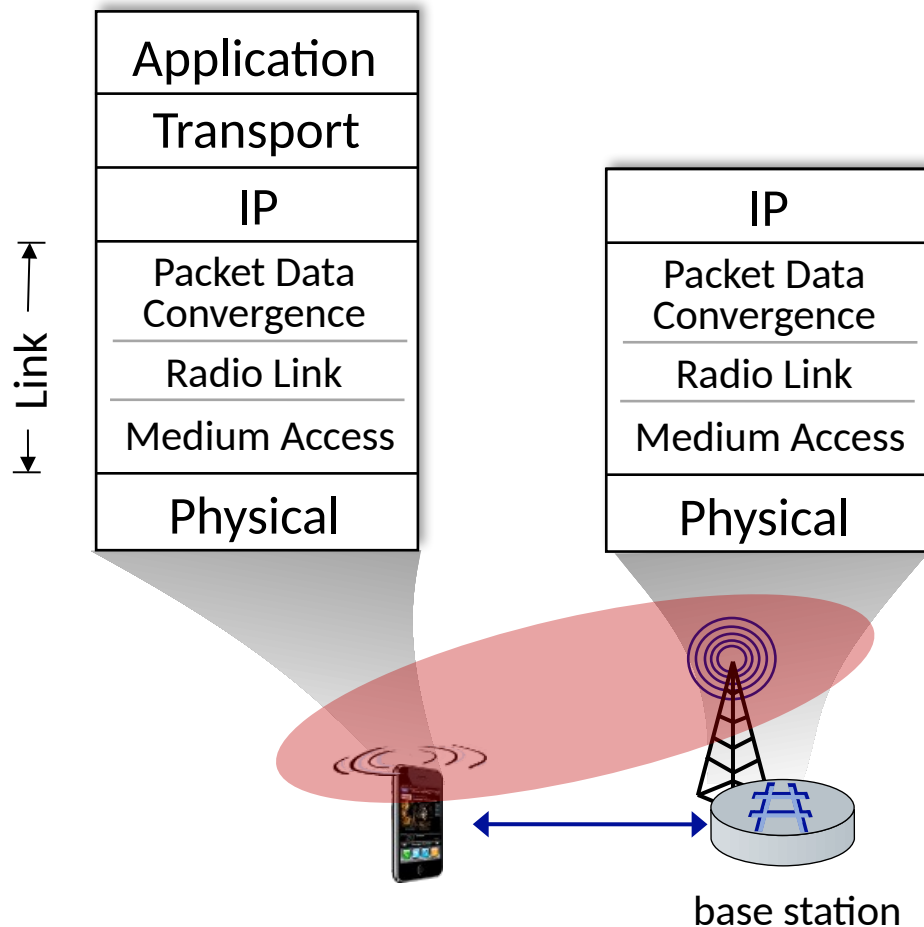
data plane

- new protocols at link, physical layers
- extensive use of tunneling to facilitate mobility

LTE data plane protocol stack: first hop



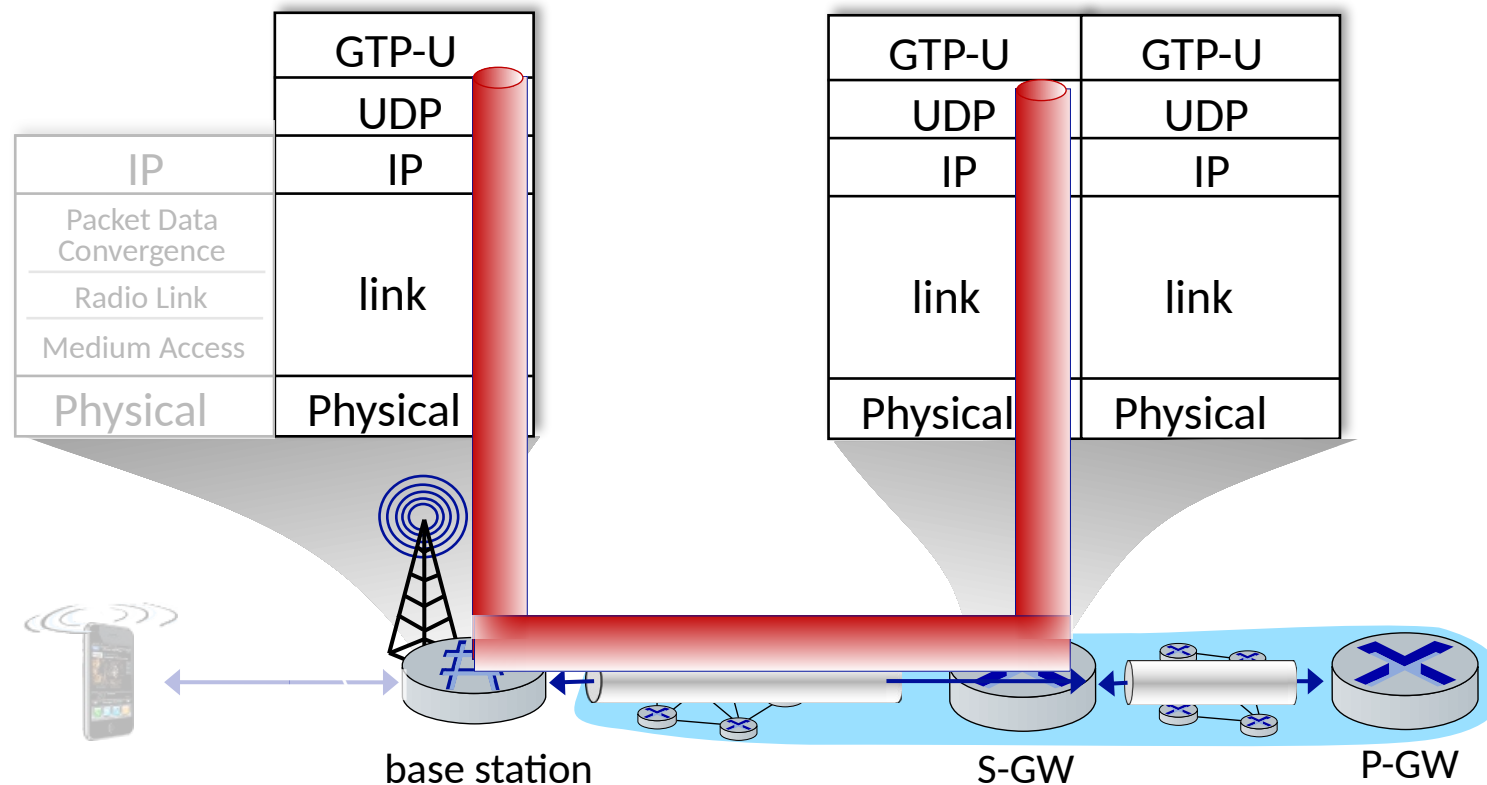
LTE data plane protocol stack: first hop



LTE radio access network:

- **downstream channel:** FDM, TDM within frequency channel (OFDM - orthogonal frequency division multiplexing)
 - “orthogonal”: minimal interference between channels
 - **upstream:** FDM, TDM similar to OFDM
- each active mobile device allocated two or more 0.5 ms time slots over 12 frequencies
 - scheduling algorithm not standardized – up to operator
 - 100's Mbps per device possible

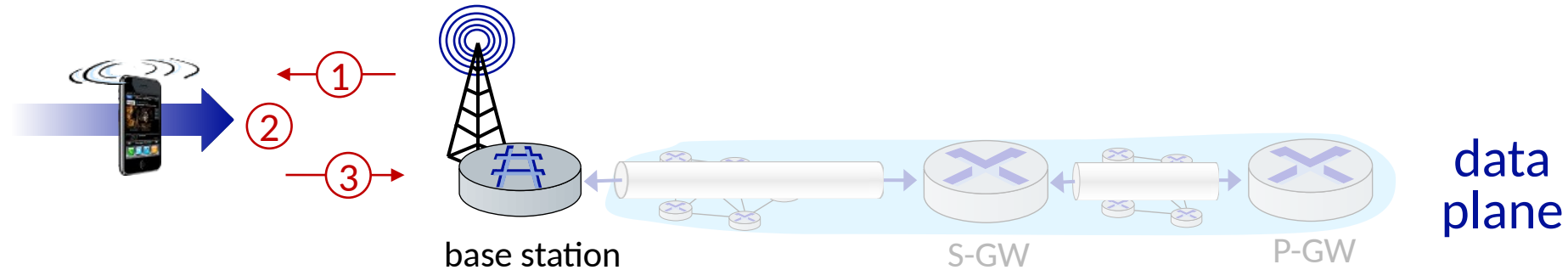
LTE data plane protocol stack: packet core



tunneling:

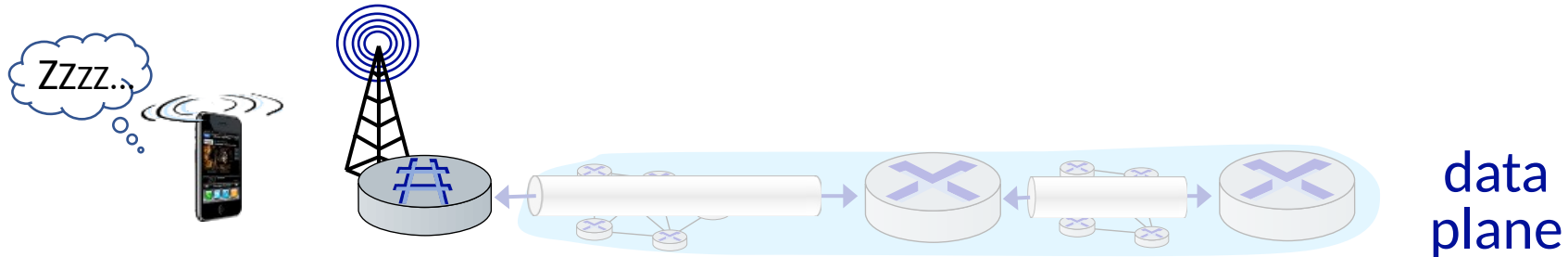
- mobile datagram encapsulated using GPRS Tunneling Protocol (GTP), sent inside UDP datagram to S-GW
- S-GW re-tunnels datagrams to P-GW
- supporting mobility: only tunneling endpoints change when mobile user moves

LTE data plane: associating with a BS



- ① BS broadcasts primary synch signal every 5 ms on all frequencies
 - BSs from multiple carriers may be broadcasting synch signals
- ② mobile finds a primary synch signal, then locates 2nd synch signal on this freq.
 - mobile then finds info broadcast by BS: channel bandwidth, configurations; BS's cellular carrier info
 - mobile may get info from multiple base stations, multiple cellular networks
- ③ mobile selects which BS to associate with (e.g., preference for home carrier)
- ④ more steps still needed to authenticate, establish state, set up data plane

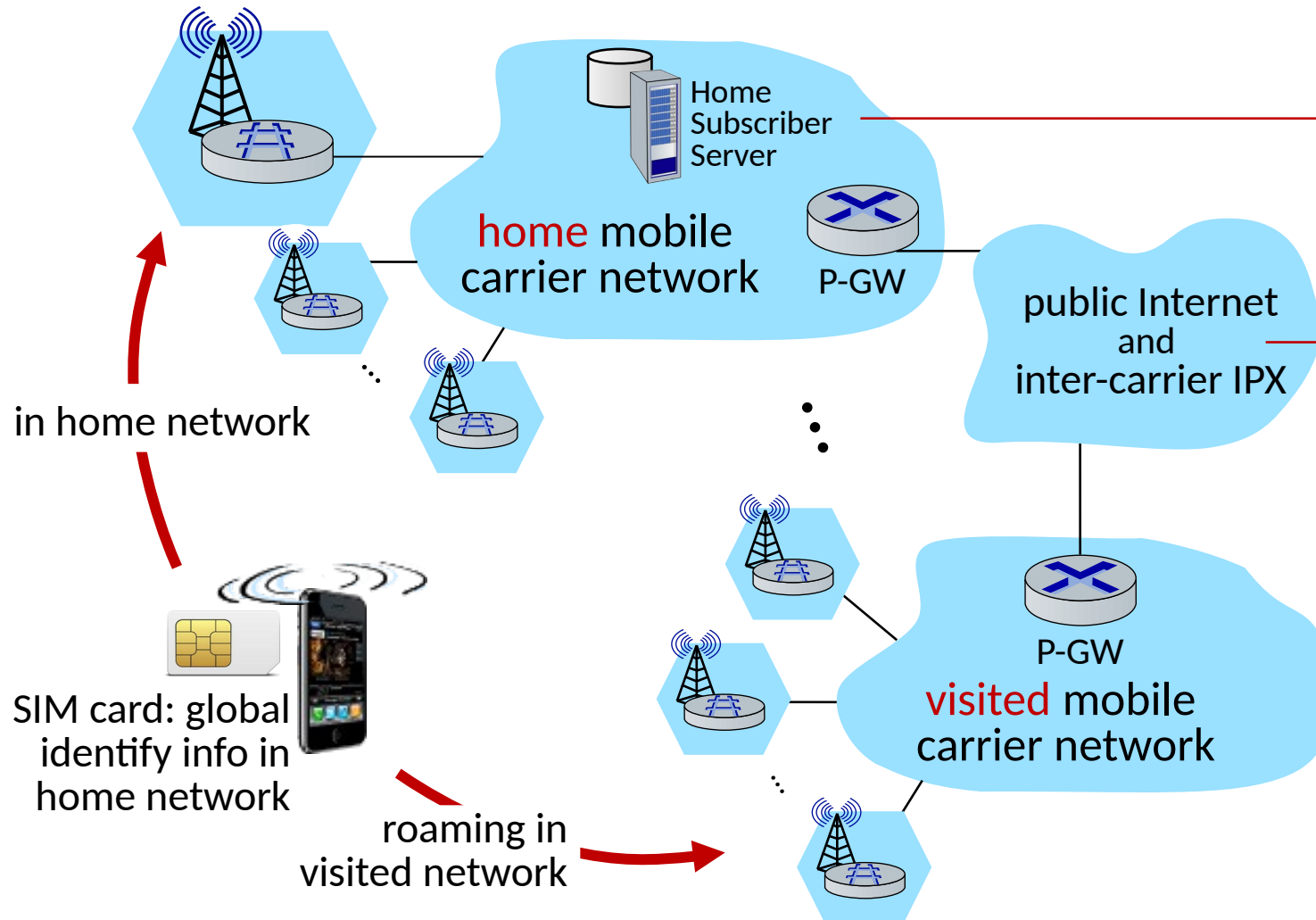
LTE mobiles: sleep modes



as in WiFi, Bluetooth: LTE mobile may put radio to “sleep” to conserve battery:

- **light sleep:** after 100's msec of inactivity
 - wake up periodically (100's msec) to check for downstream transmissions
- **deep sleep:** after 5-10 secs of inactivity
 - mobile may change cells while deep sleeping – need to re-establish association

Global cellular network: a network of IP networks



home network HSS:

- identify & services info, while in home network and roaming

all IP:

- carriers interconnect with each other, and public internet at exchange points
- legacy 2G, 3G: not all IP, handled otherwise

On to 5G!

- **goal:** 10x increase in peak bitrate, 10x decrease in latency, 100x increase in traffic capacity over 4G
- **5G NR (new radio):**
 - two frequency bands: FR1 (450 MHz–6 GHz) and FR2 (24 GHz–52 GHz): millimeter wave frequencies
 - not backwards-compatible with 4G
 - MIMO: multiple directional antennae
- **millimeter wave frequencies:** much higher data rates, but over shorter distances
 - pico-cells: cells diameters: 10-100 m
 - massive, dense deployment of new base stations required