

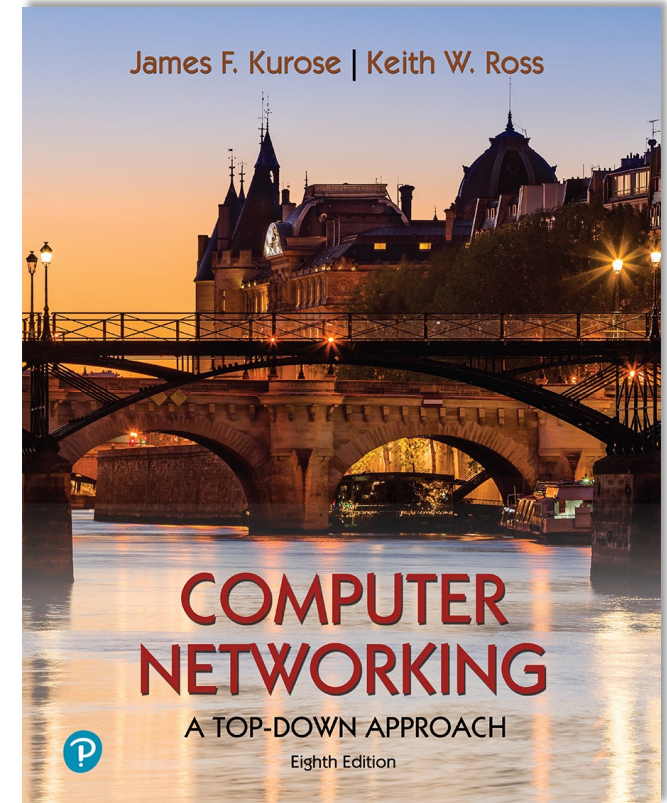
# Chapter 7

# Wireless and Mobile Networks

Yaxiong Xie

Department of Computer Science and Engineering  
University at Buffalo, SUNY

Adapted from the slides of the book's authors



*Computer Networking: A  
Top-Down Approach*

8<sup>th</sup> edition

Jim Kurose, Keith Ross  
Pearson, 2020

# Wireless and Mobile Networks: context

- more wireless (mobile) phone subscribers than fixed (wired) phone subscribers (10-to-1 in 2019)!
- more mobile-broadband-connected devices than fixed-broadband-connected devices (5-1 in 2019)!
  - 4G/5G cellular networks now embracing Internet protocol stack, including SDN
- two important (but different) challenges
  - **wireless**: communication over wireless link
  - **mobility**: handling the mobile user who changes point of attachment to network

# Chapter 7 outline

## ■ Introduction

### Wireless

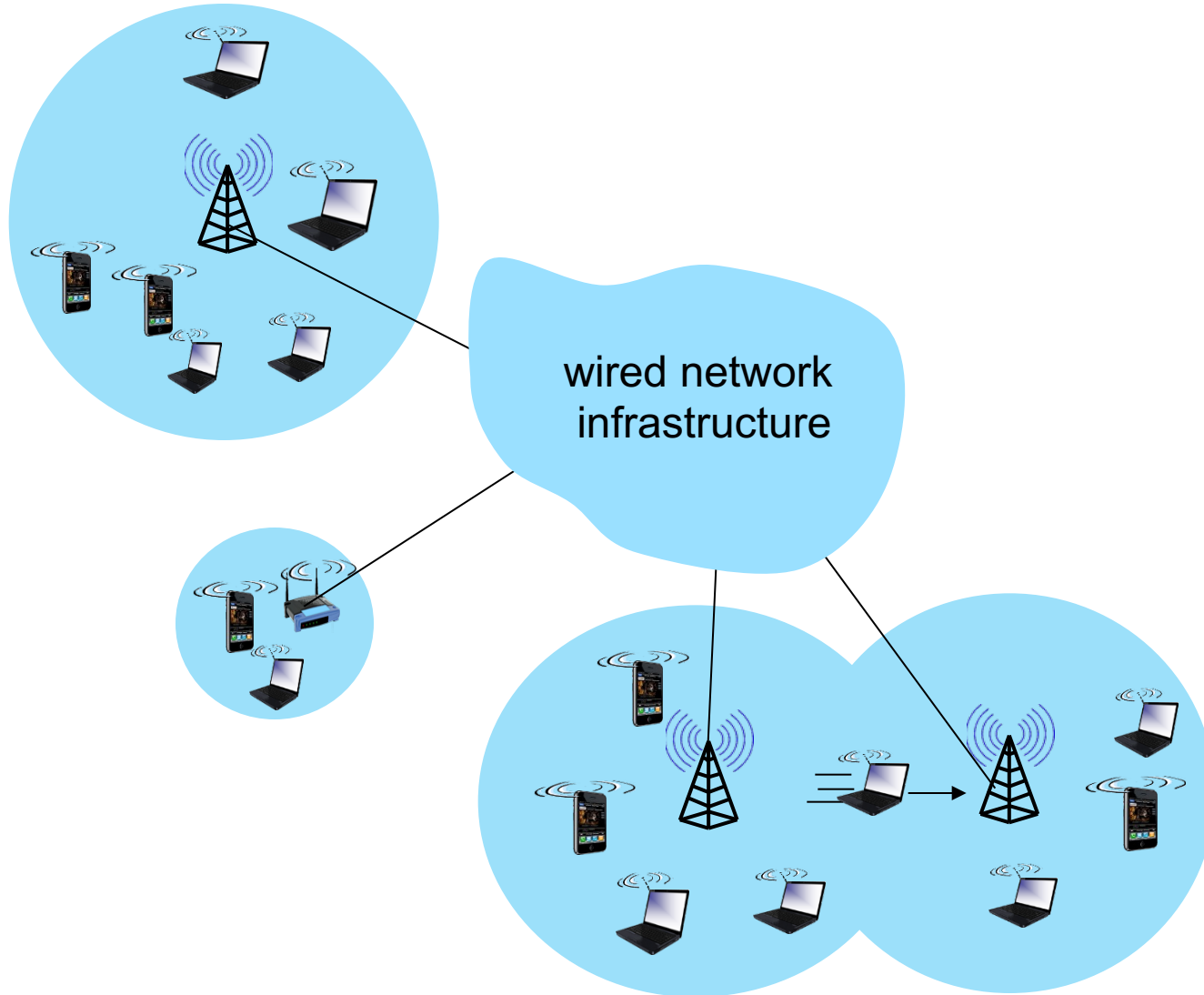
- Wireless Links and network characteristics
- WiFi: 802.11 wireless LANs
- Cellular networks: 4G and 5G

### Mobility

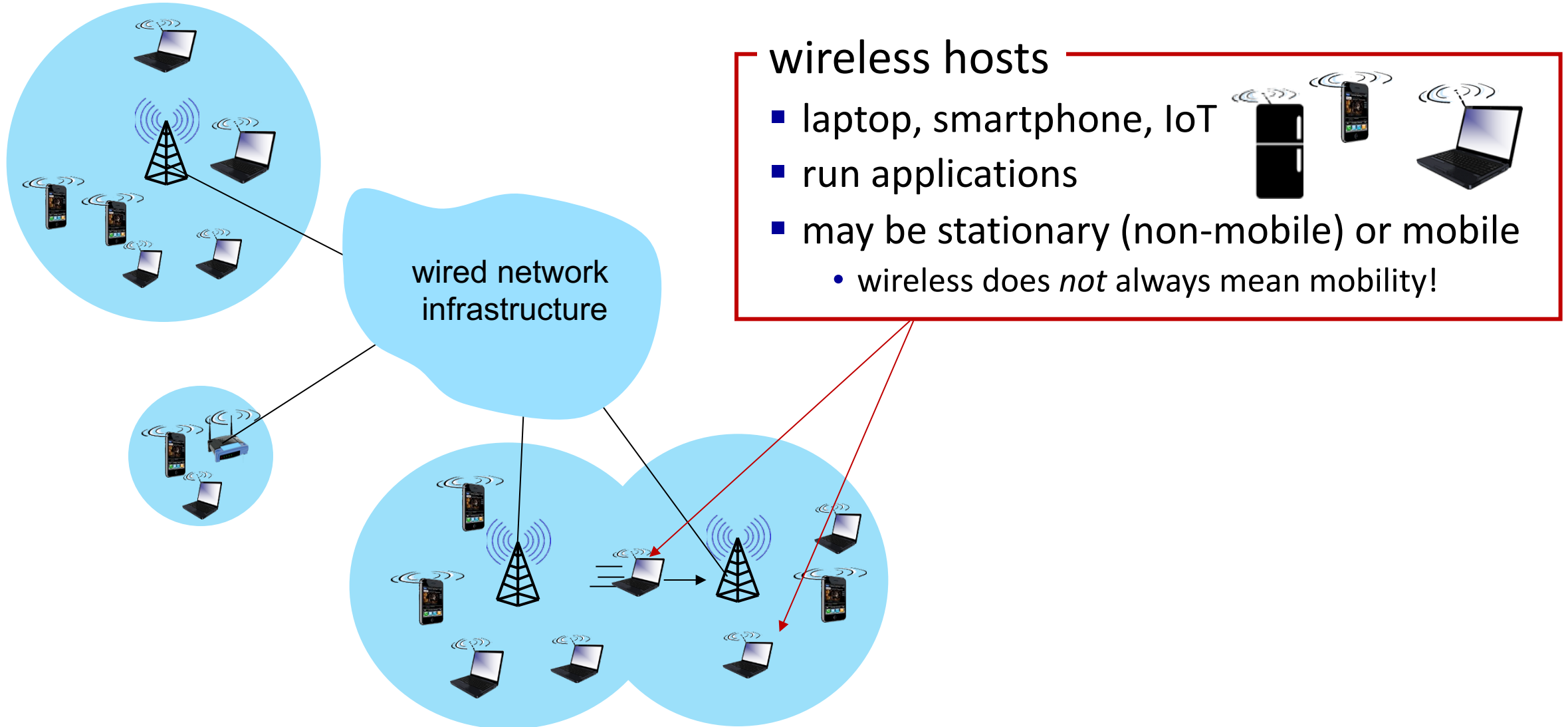
- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols



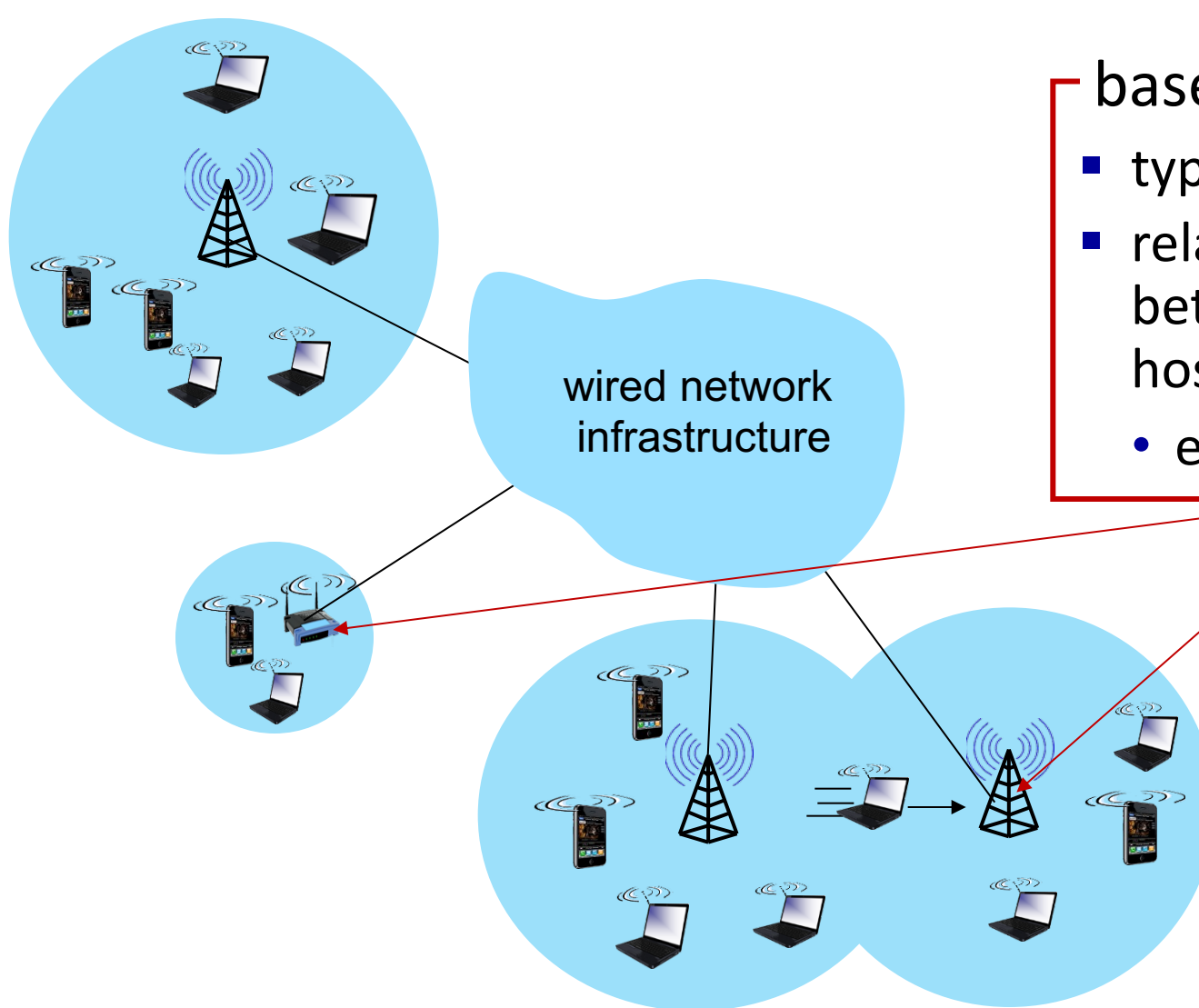
# Elements of a wireless network



# Elements of a wireless network



# Elements of a wireless network

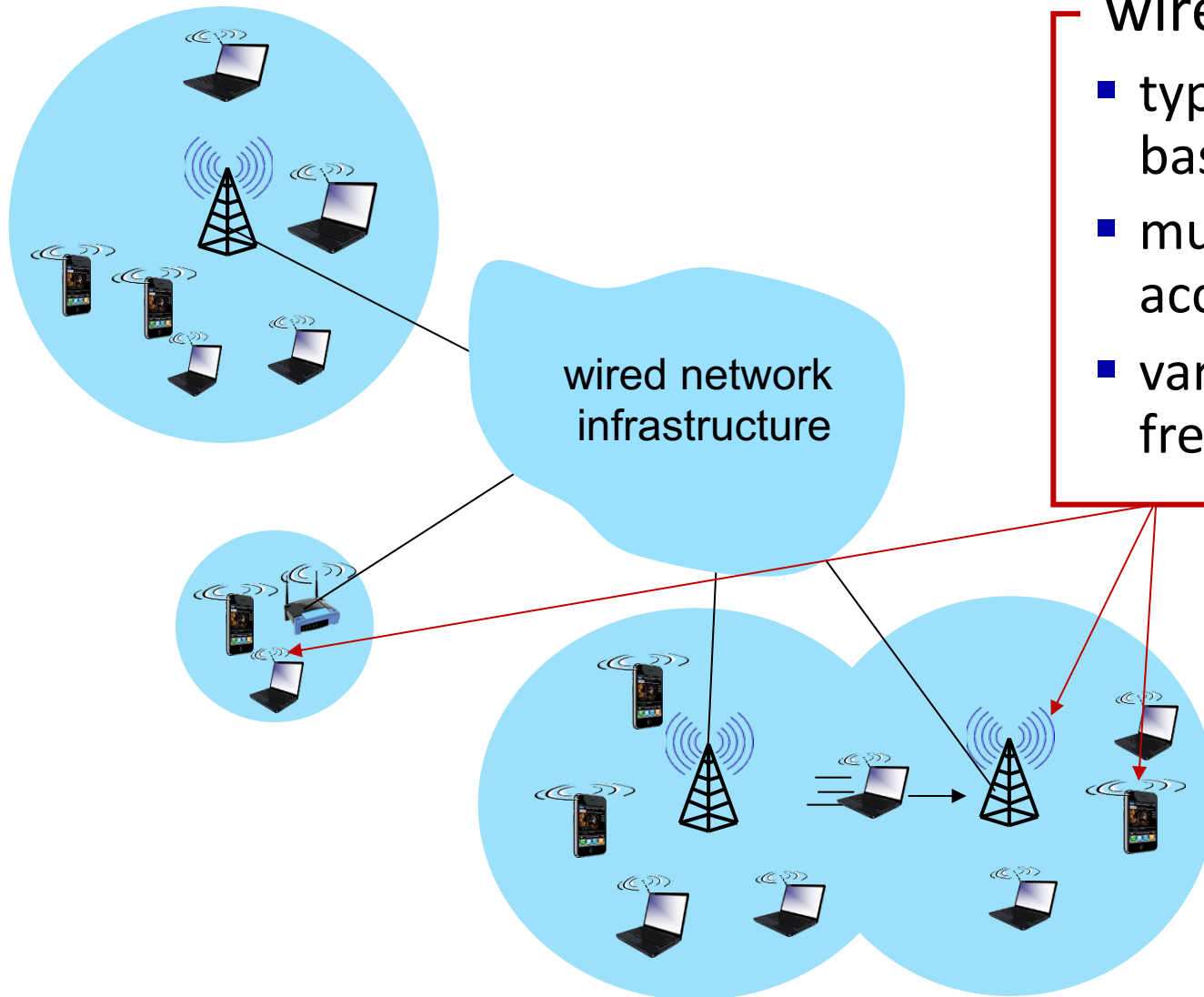


base station



- 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

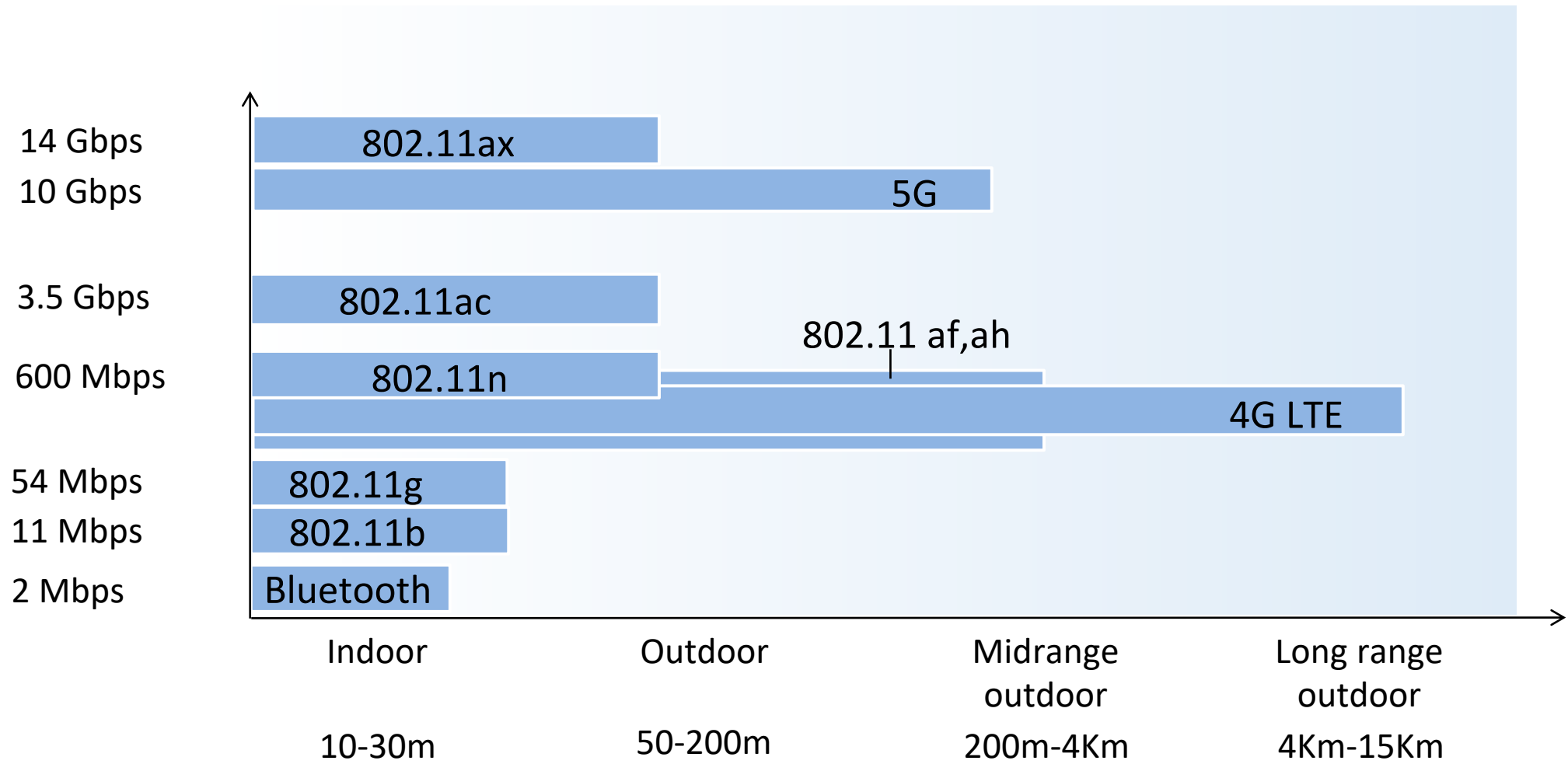


wireless link



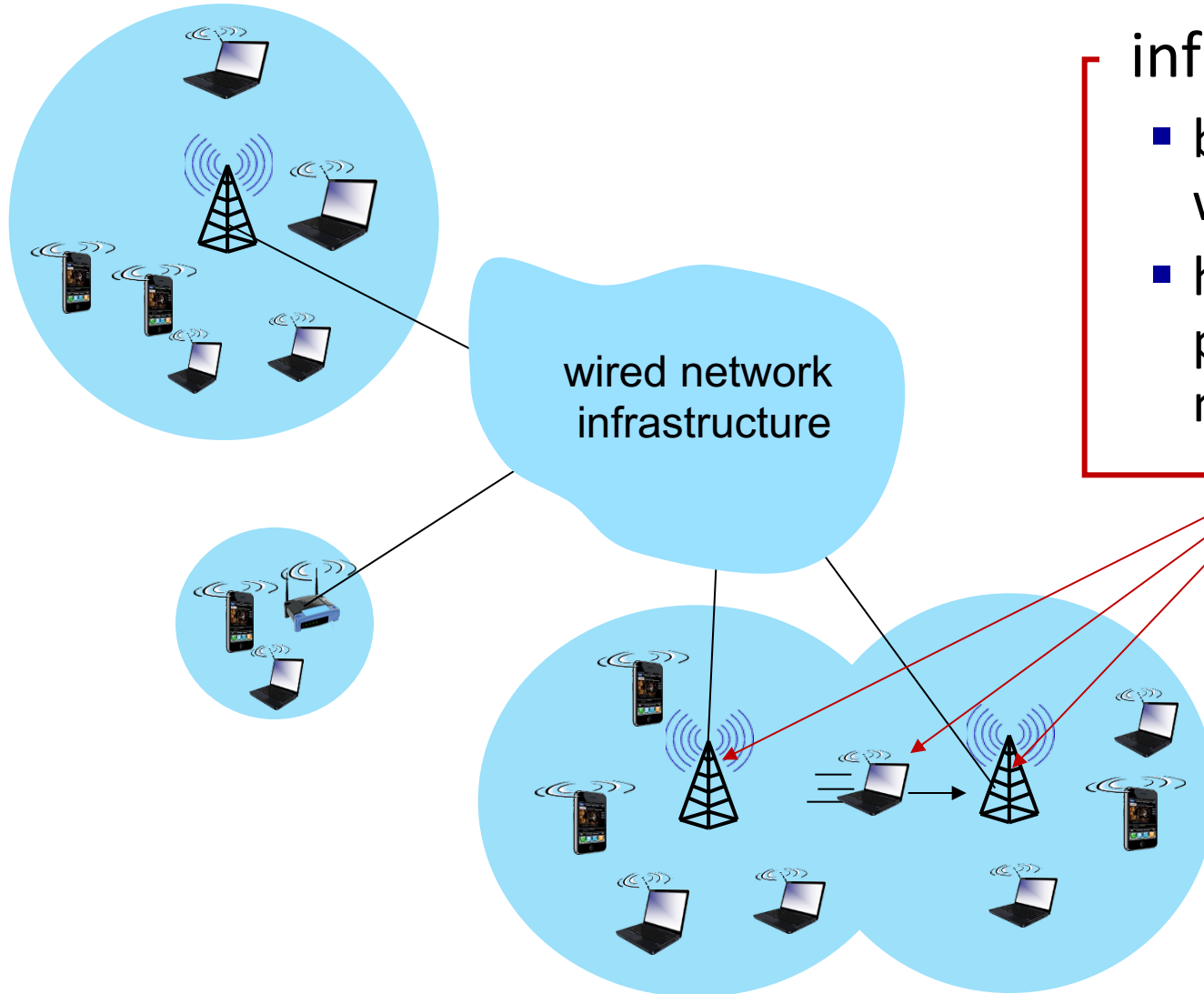
- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

# 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

# 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 ....

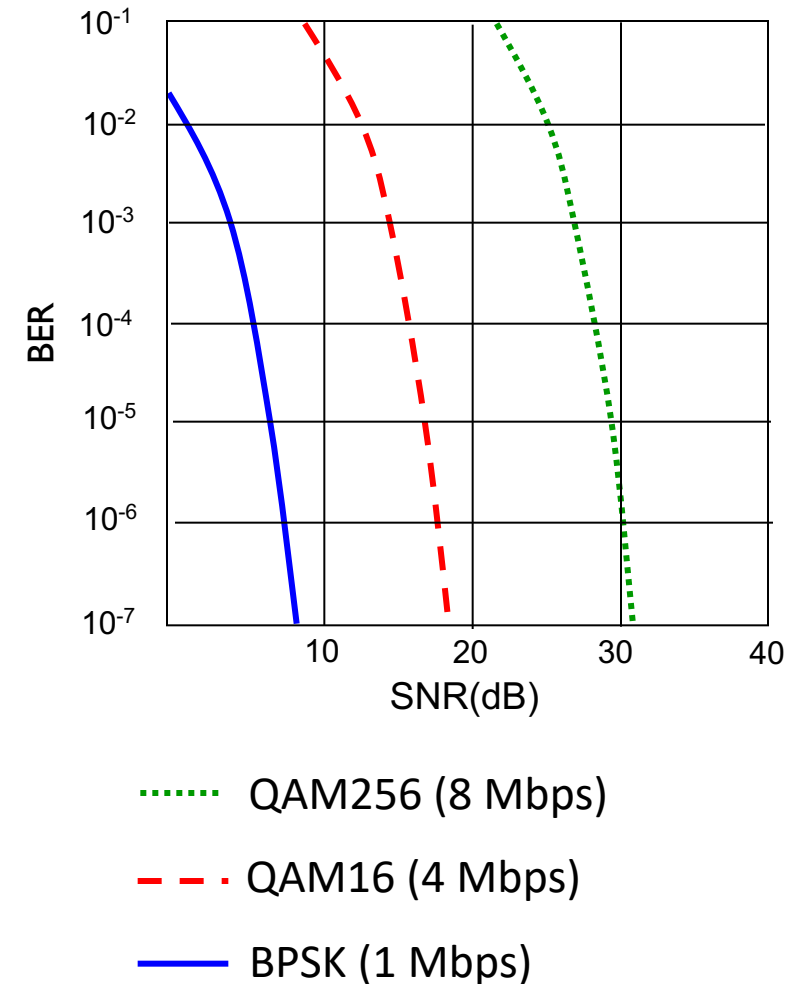
- **decreased signal strength:** radio signal attenuates as it propagates through matter (path loss)
- **interference from other sources:** wireless network frequencies (e.g., 2.4 GHz) shared by many devices (e.g., WiFi, cellular, motors): interference
- **multipath propagation:** radio signal reflects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

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



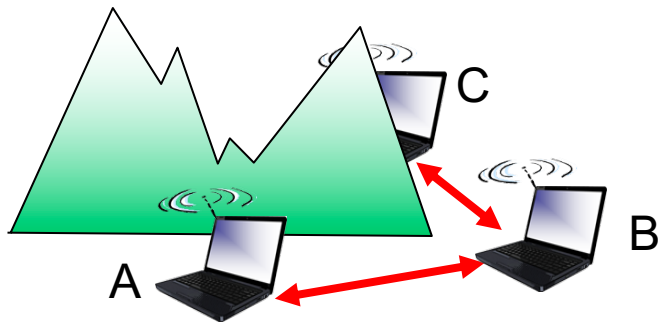
# Wireless link characteristics (2)

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



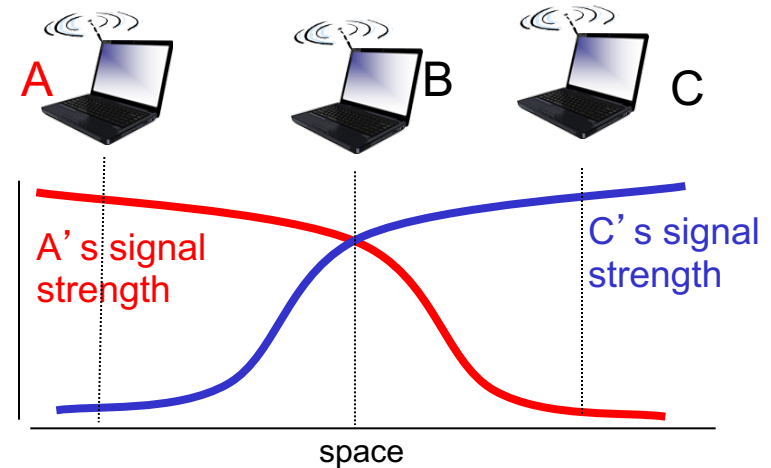
# Wireless link characteristics (3)

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



## Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B

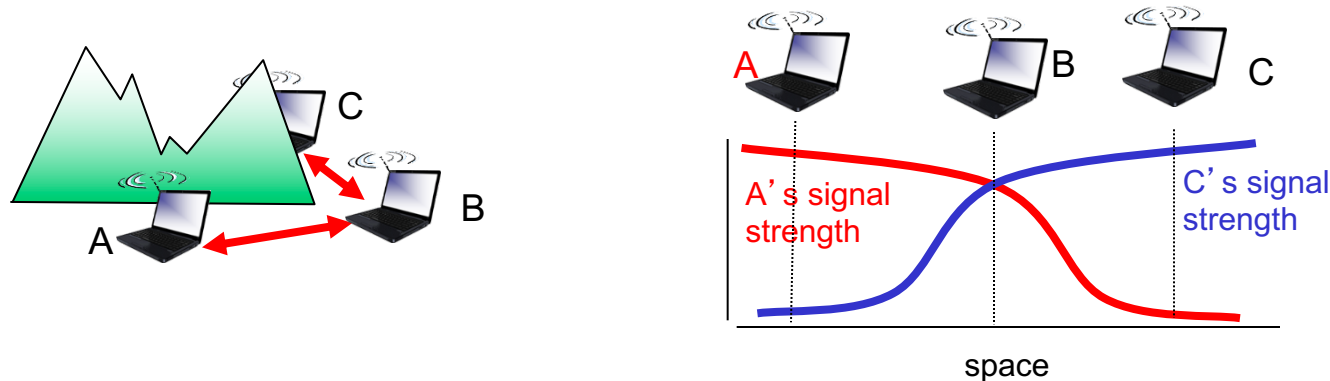


## Signal attenuation:

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

# IEEE 802.11: multiple access

- avoid collisions: 2<sup>+</sup> 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



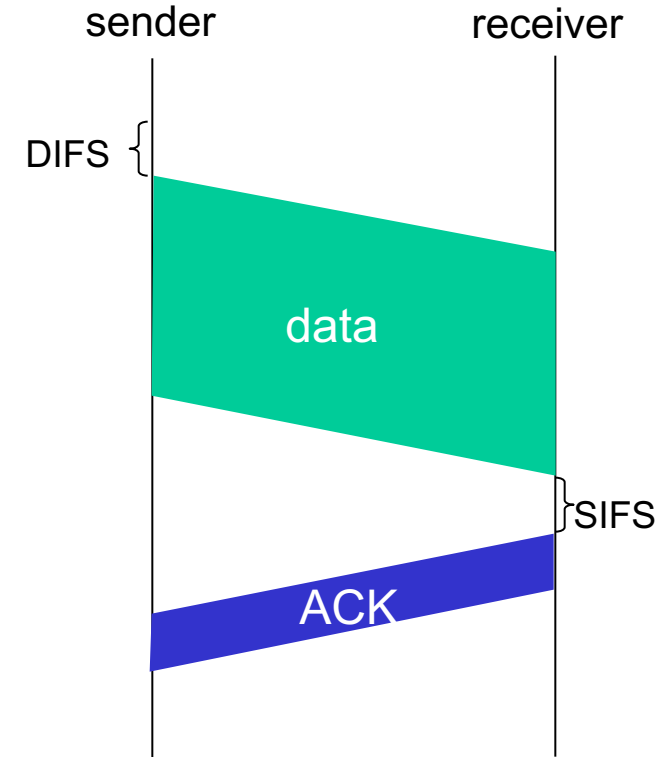
# IEEE 802.11 MAC Protocol: CSMA/CA

## 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)



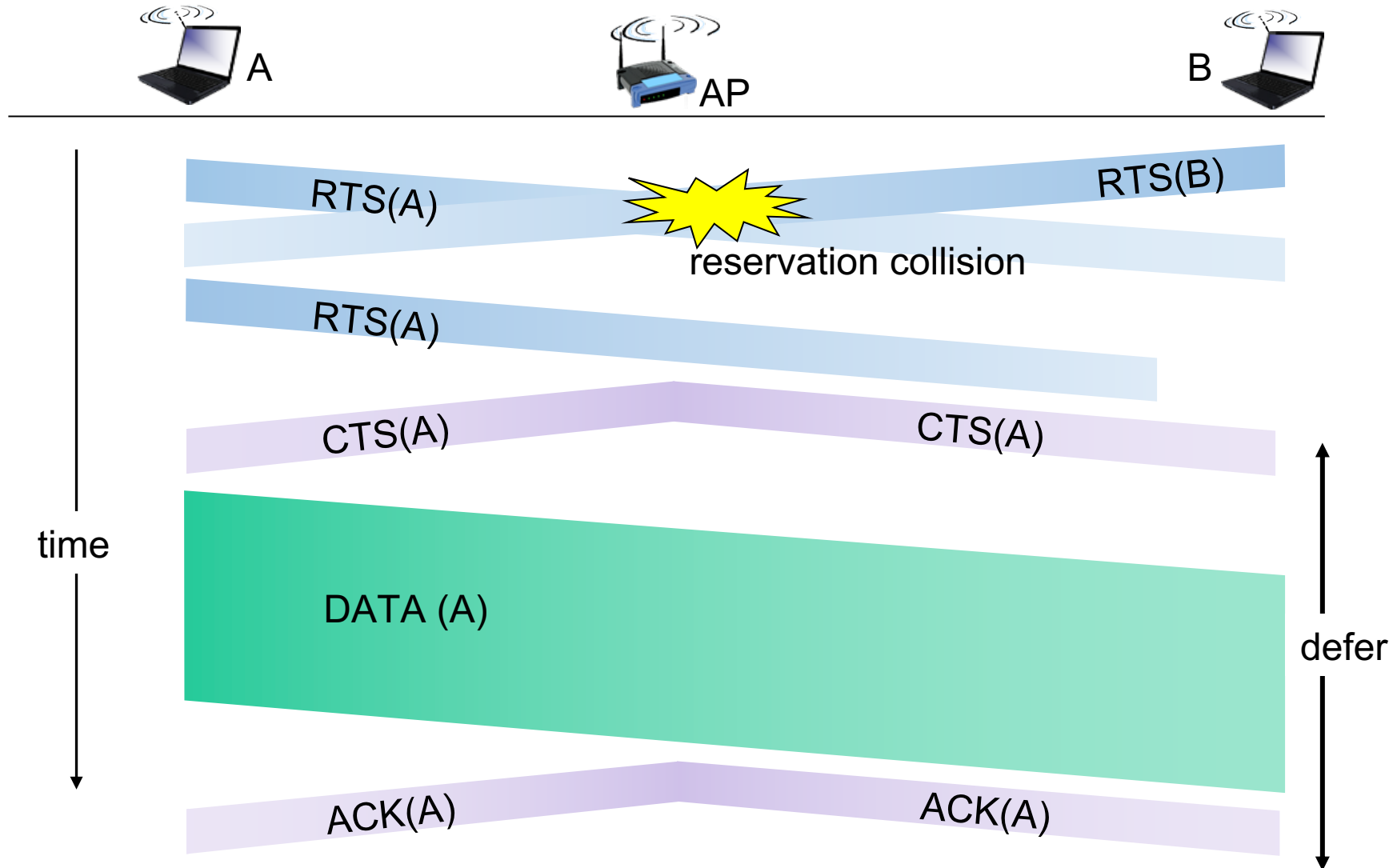
# Avoiding collisions (more)

**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



# Collision Avoidance: RTS-CTS exchange



# Chapter 7 outline

- Introduction

## Wireless

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

## Mobility

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

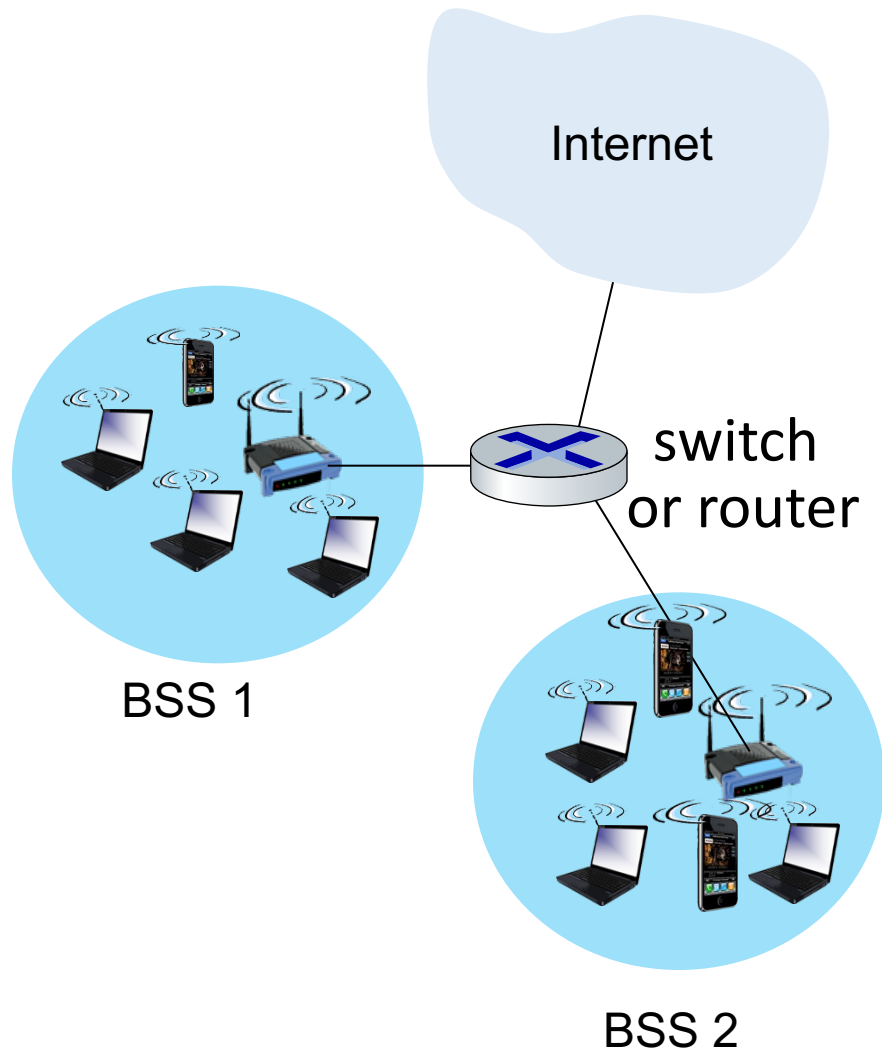


# IEEE 802.11 Wireless LAN

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

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

# 802.11 LAN architecture



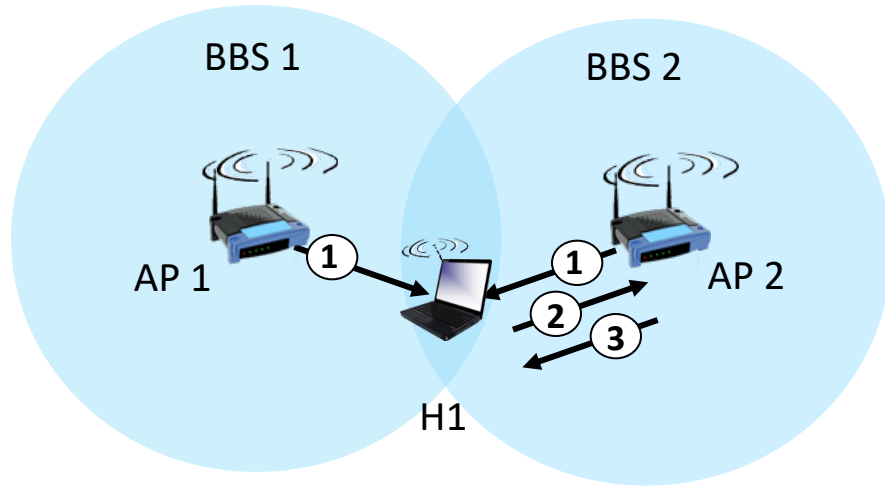
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

# 802.11: Channels, association

- spectrum divided into channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- arriving host: must **associate** with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - then may perform authentication [Chapter 8]
  - then typically run DHCP to get IP address in AP's subnet

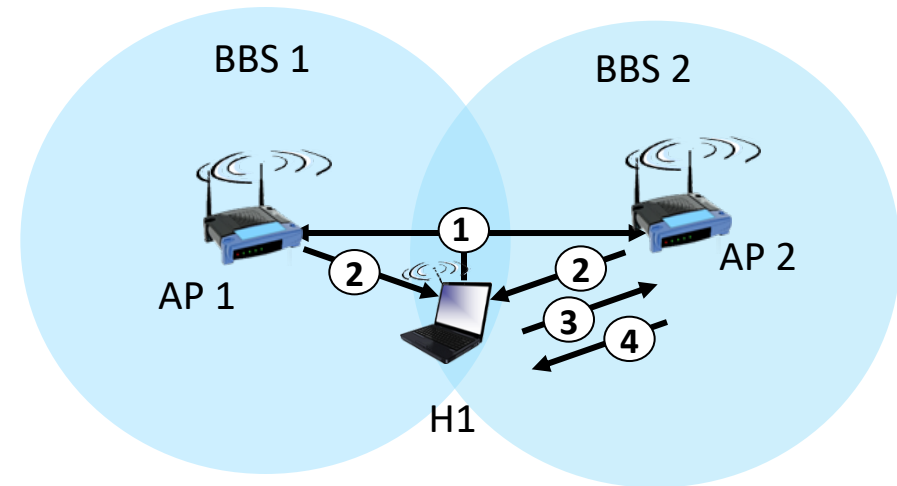


# 802.11: passive/active scanning



## 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

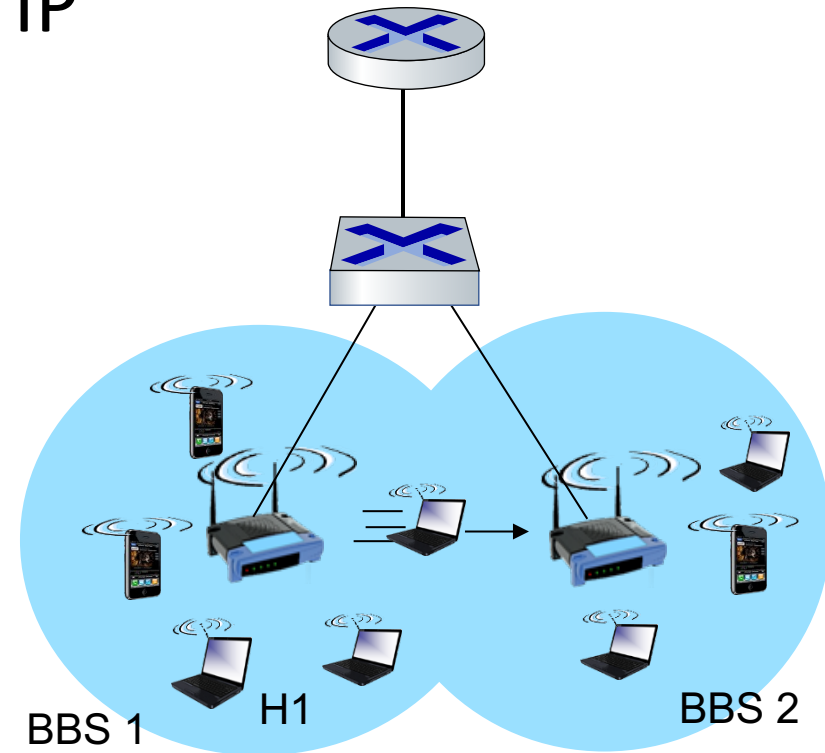


## active scanning:

- (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

# 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

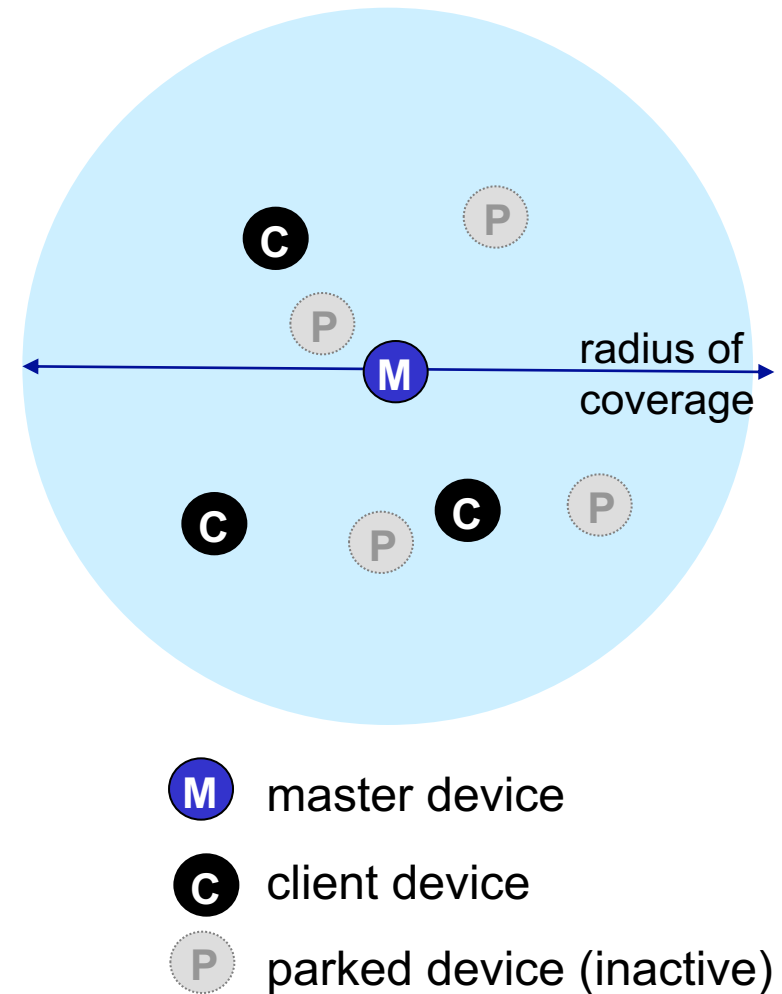
## power management

- node-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame



# 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



# 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

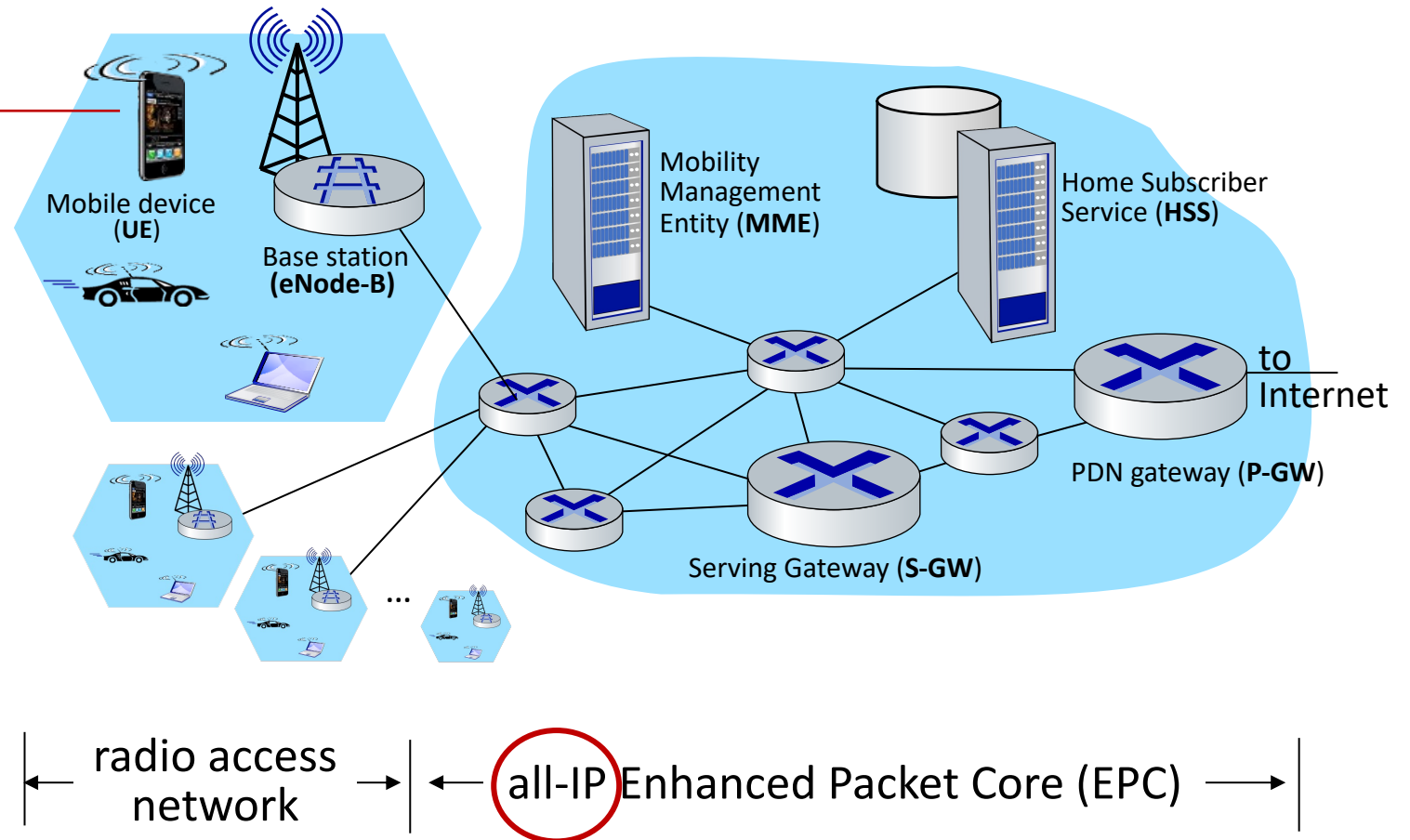
# 4G/5G cellular networks

- *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](http://www.3gpp.org)
  - 4G: Long-Term Evolution (LTE) standard

# Elements of 4G LTE architecture

## Mobile device:

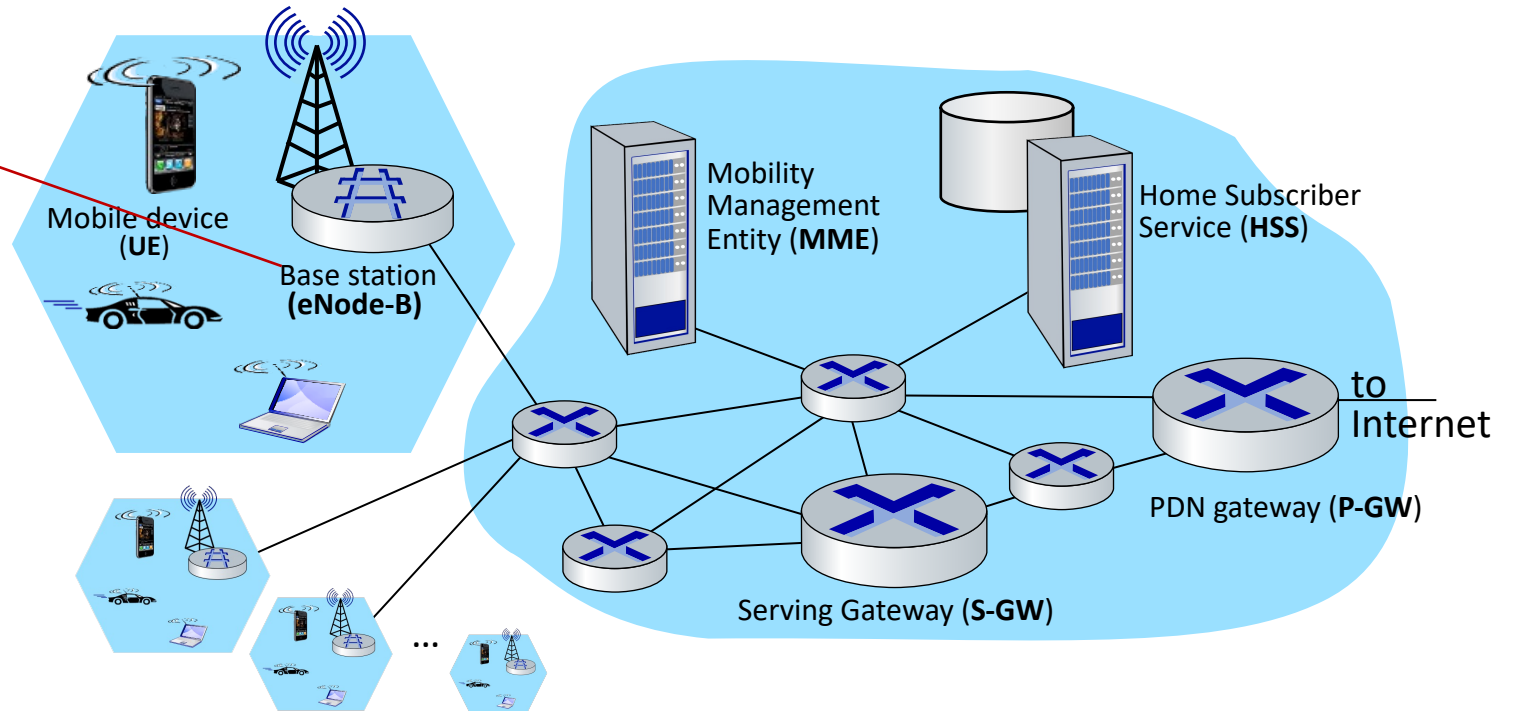
- smartphone, tablet, laptop, IoT, ... with 4G LTE radio
- 64-bit International Mobile Subscriber Identity (IMSI), stored on SIM (Subscriber Identity Module) card
- LTE jargon: User Equipment (UE)



# Elements of 4G LTE architecture

## Base station:

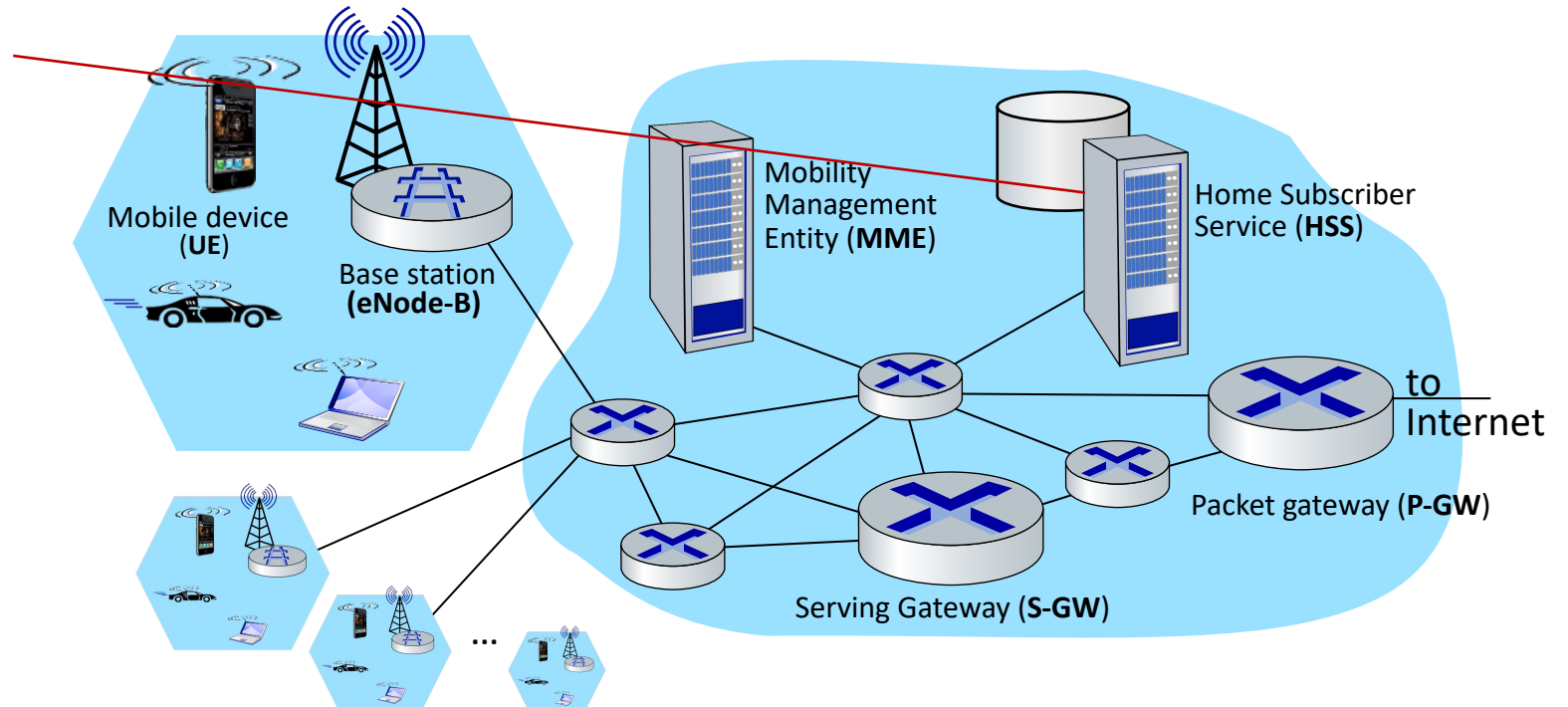
- at “edge” of carrier’s network
- manages wireless radio resources, mobile devices in its coverage area (“cell”)
- coordinates device authentication with other elements
- similar to WiFi AP but:
  - active role in user mobility
  - coordinates with nearby base stations to optimize radio use
- LTE jargon: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



# Elements of 4G LTE architecture

## Home Subscriber Service

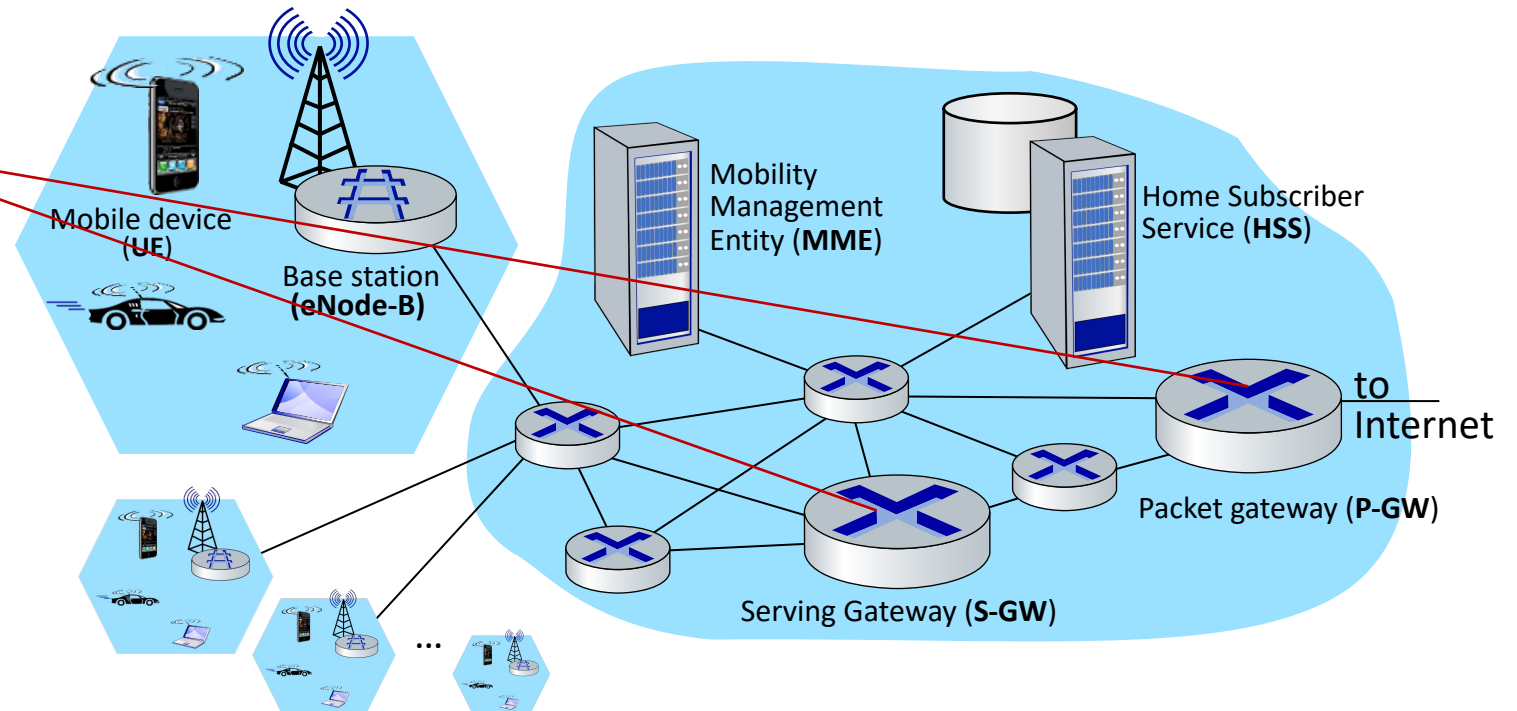
- stores info about mobile devices for which the HSS's network is their “home network”
- works with MME in device authentication



# Elements of 4G LTE architecture

## Serving Gateway (S-GW), Packet Gateway (P-GW)

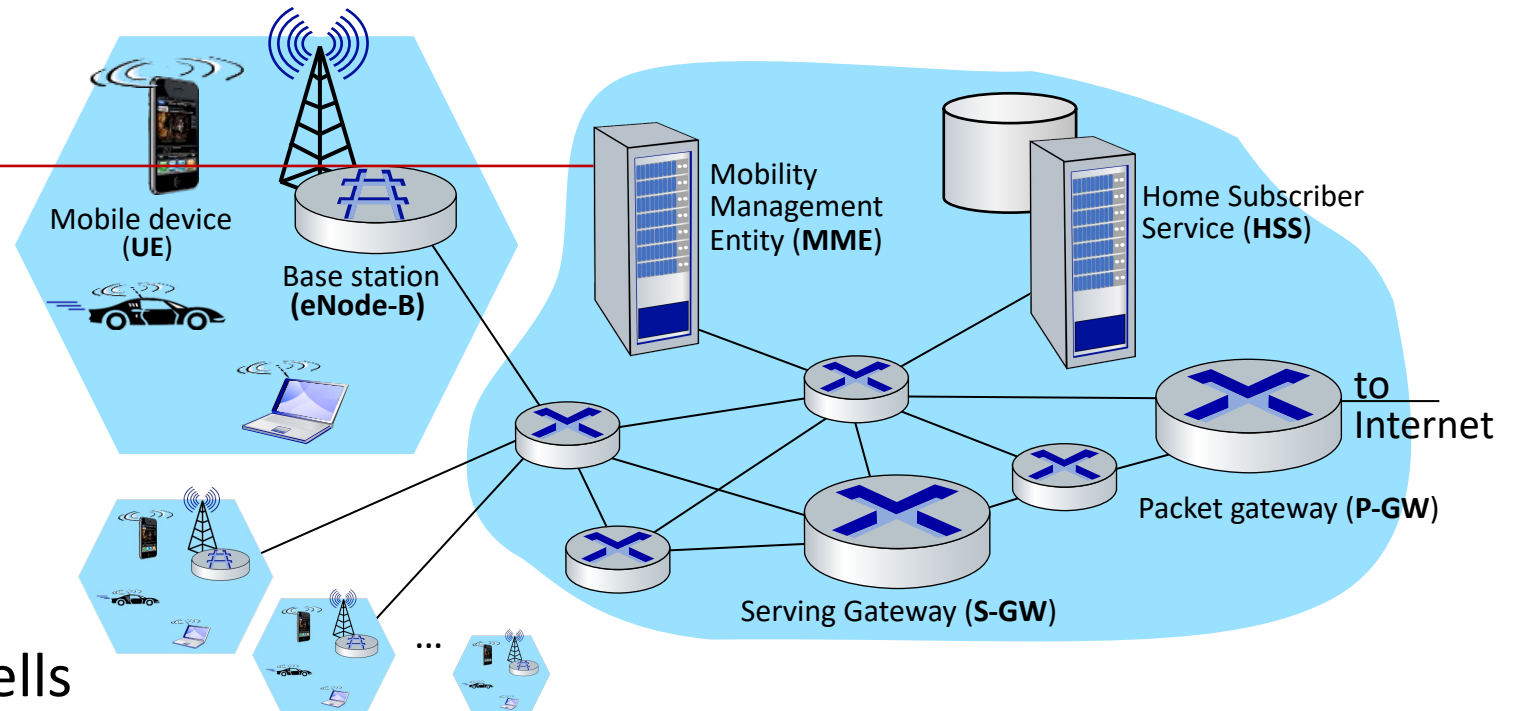
- lie on data path from mobile to/from Internet
- P-GW
  - gateway to mobile cellular network
  - Looks like any other internet gateway router
  - provides NAT services
- other routers:
  - extensive use of tunneling



# Elements of 4G LTE architecture

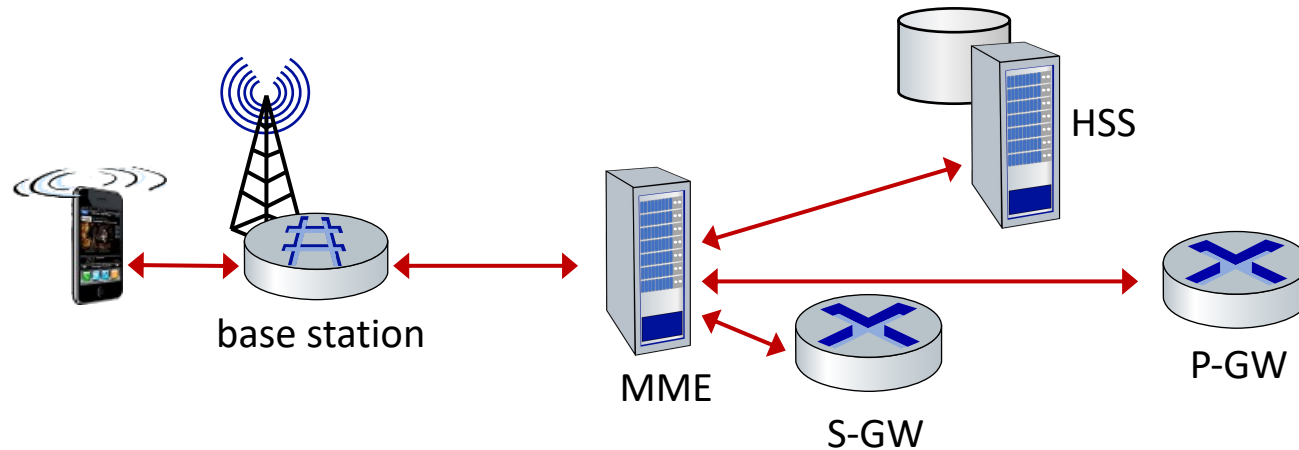
## Mobility Management Entity

- 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



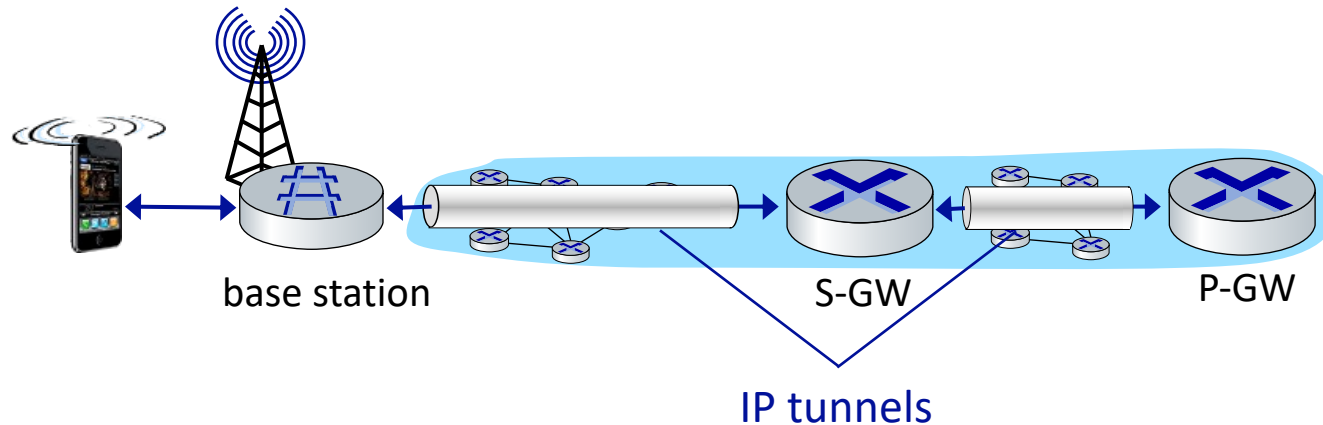


# LTE: data plane control plane separation



## control plane

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

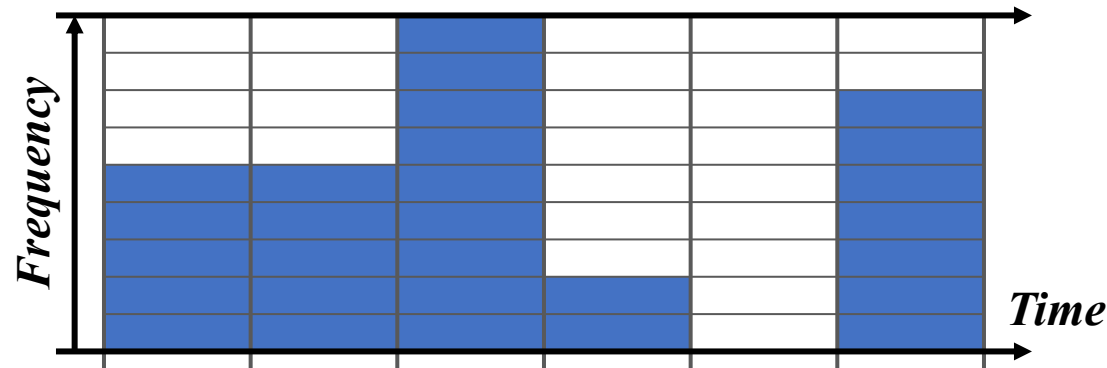


## data plane

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

# LTE data plane protocol stack: first hop

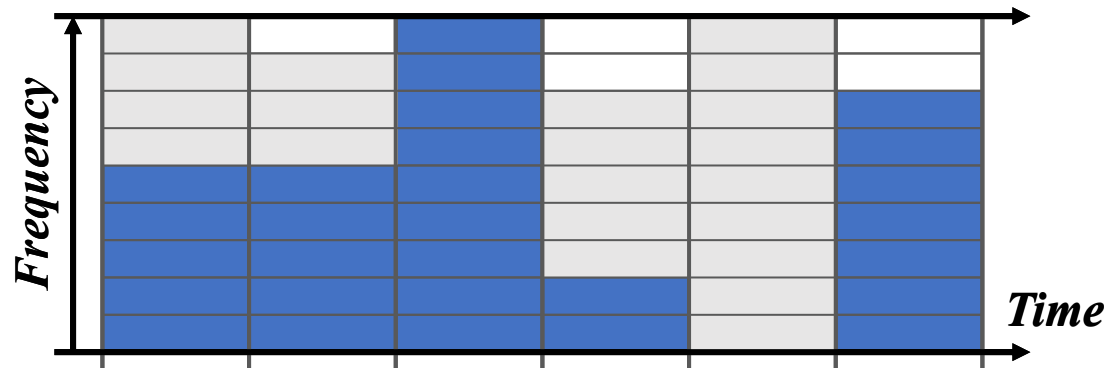
LTE radio access network (RA)



UE 1

# LTE data plane protocol stack: first hop

LTE radio access network (RA)

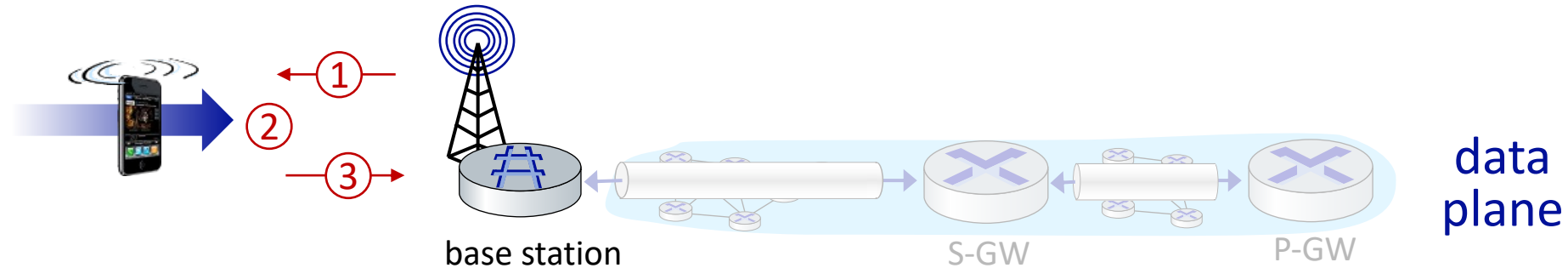


UE 1



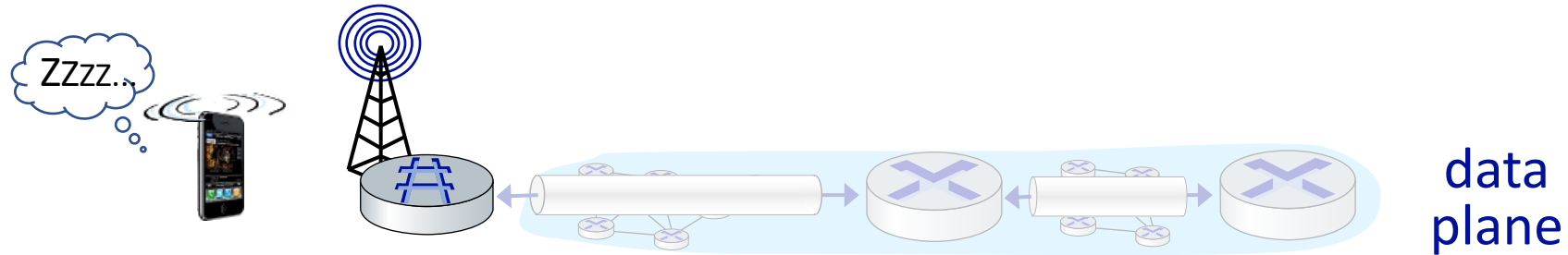
UE 2

# 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 2<sup>nd</sup> 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

# 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

# Contacting a mobile friend:

Consider friend frequently changing locations, how do you find him/her?

- search all phone books?
- expect her to let you know where he/she is?

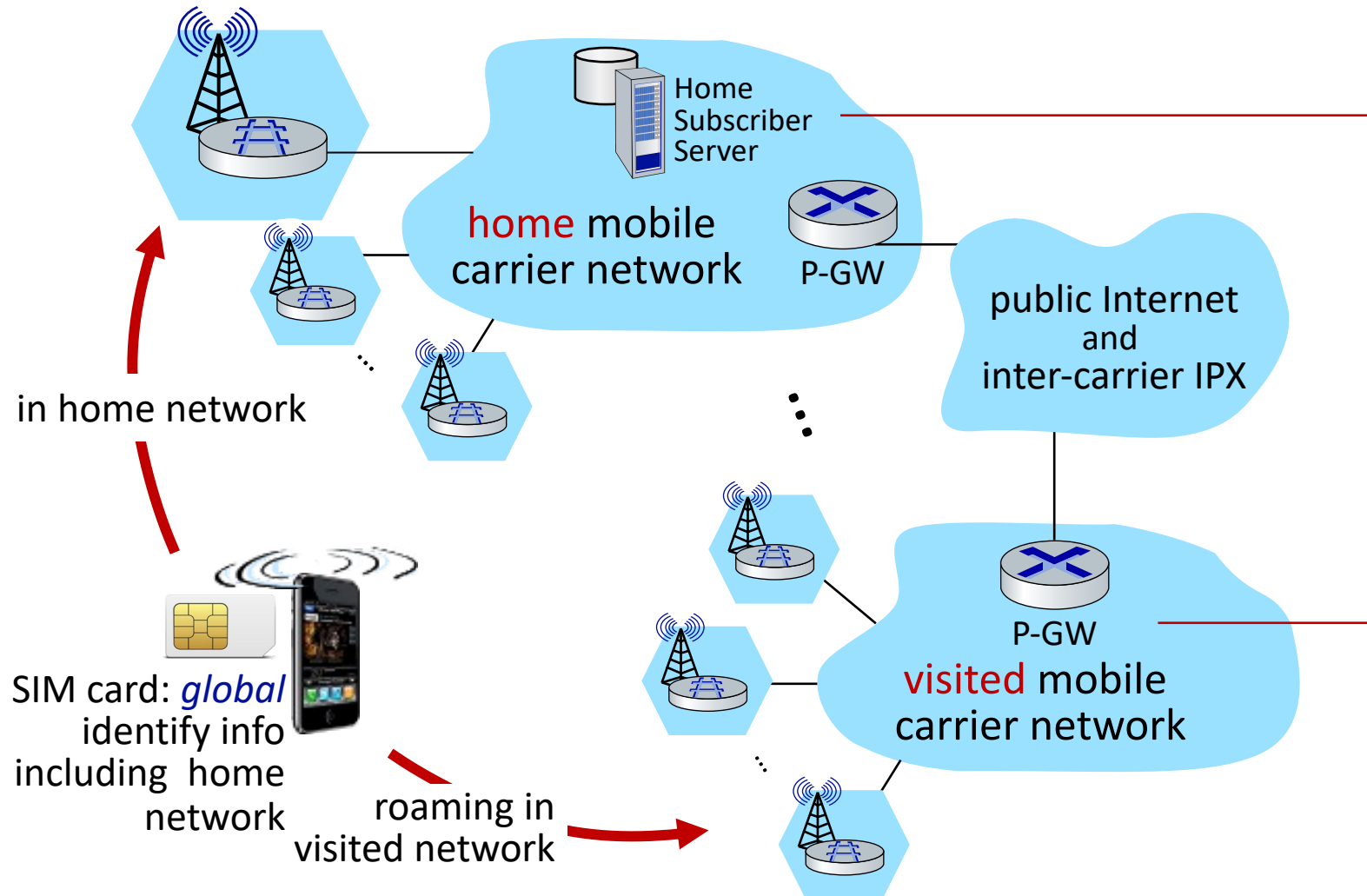
- call his/her parents?
- Facebook!

The importance of having a “home”:

- a definitive source of information about you
- a place where people can find out where you are



# Home network, visited network: 4G/5G



## home network:

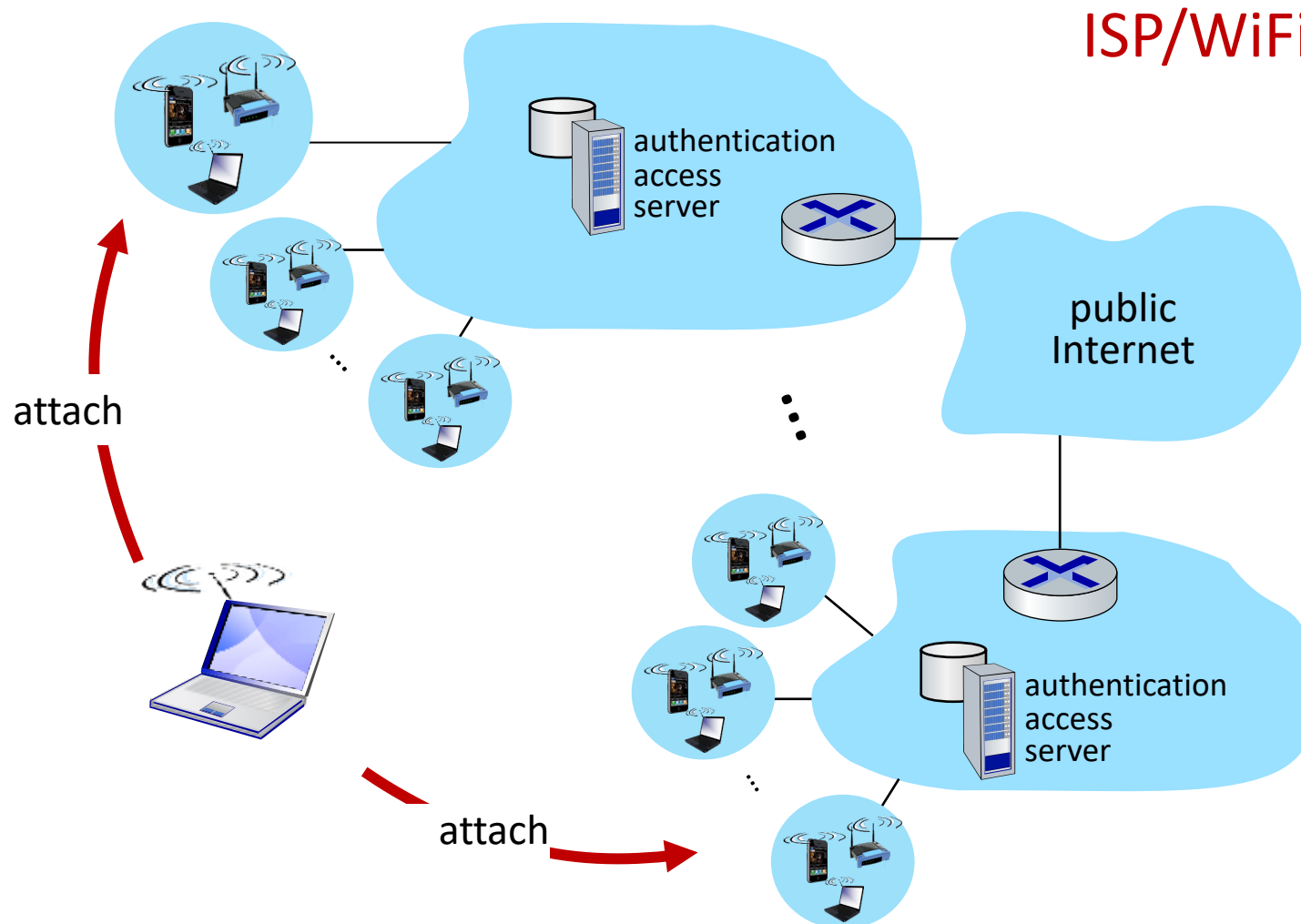
- (paid) service plan with cellular provider, e.g., Verizon, Orange
- home network HSS stores identify & services info

## visited network:

- any network other than your home network
- service agreement with other networks: to provide access to visiting mobile



# Home network, visited network: ISP/WiFi



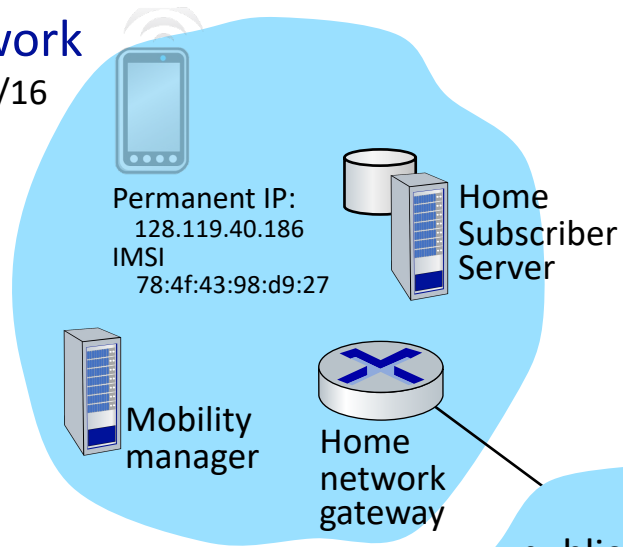
ISP/WiFi: no notion of global “home”

- credentials from ISP (e.g., username, password) stored on device or with user
- ISPs may have national, international presence
- different networks: different credentials
  - some exceptions (e.g., eduroam)
  - architectures exist (mobile IP) for 4G-like mobility, but not used

# Home network, visited network: generic

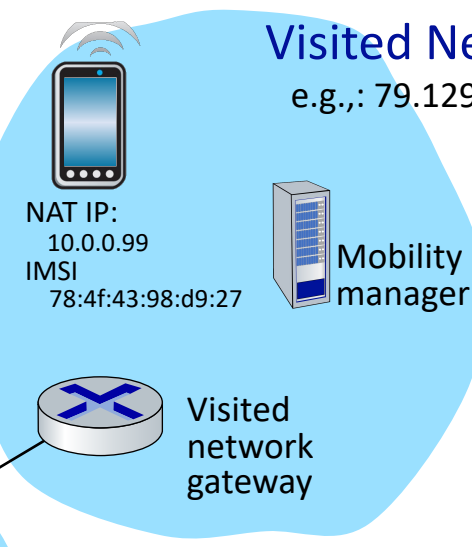
## Home Network

e.g.,: 128.119/16



## Visited Network

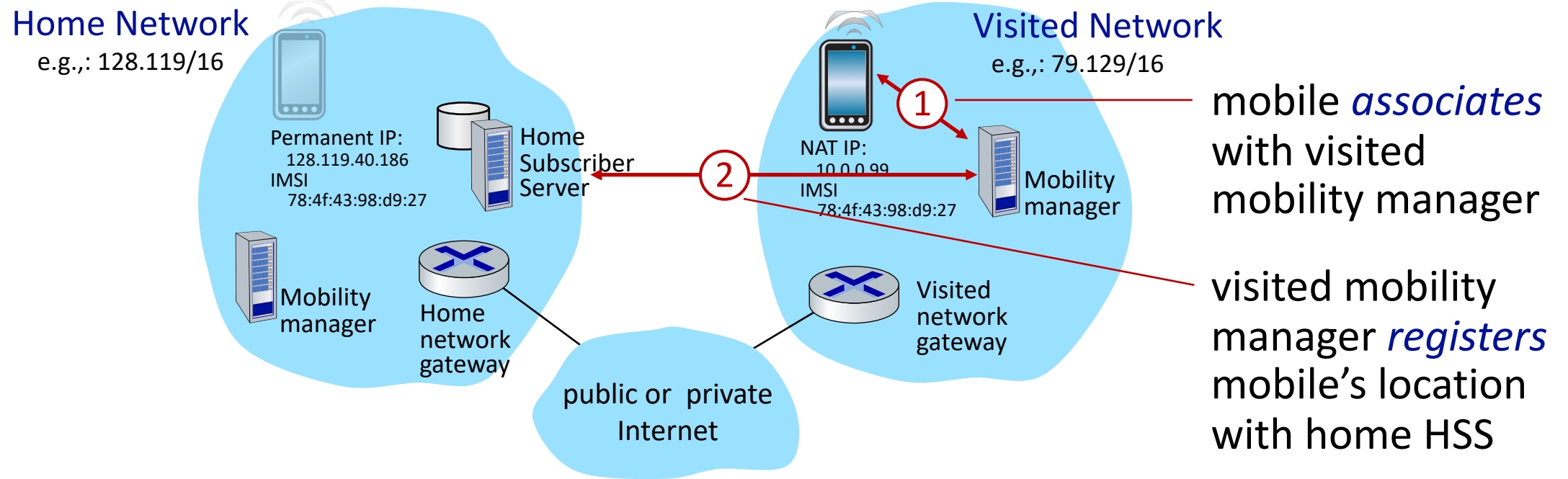
e.g.,: 79.129/16



public or private  
Internet

Correspondent

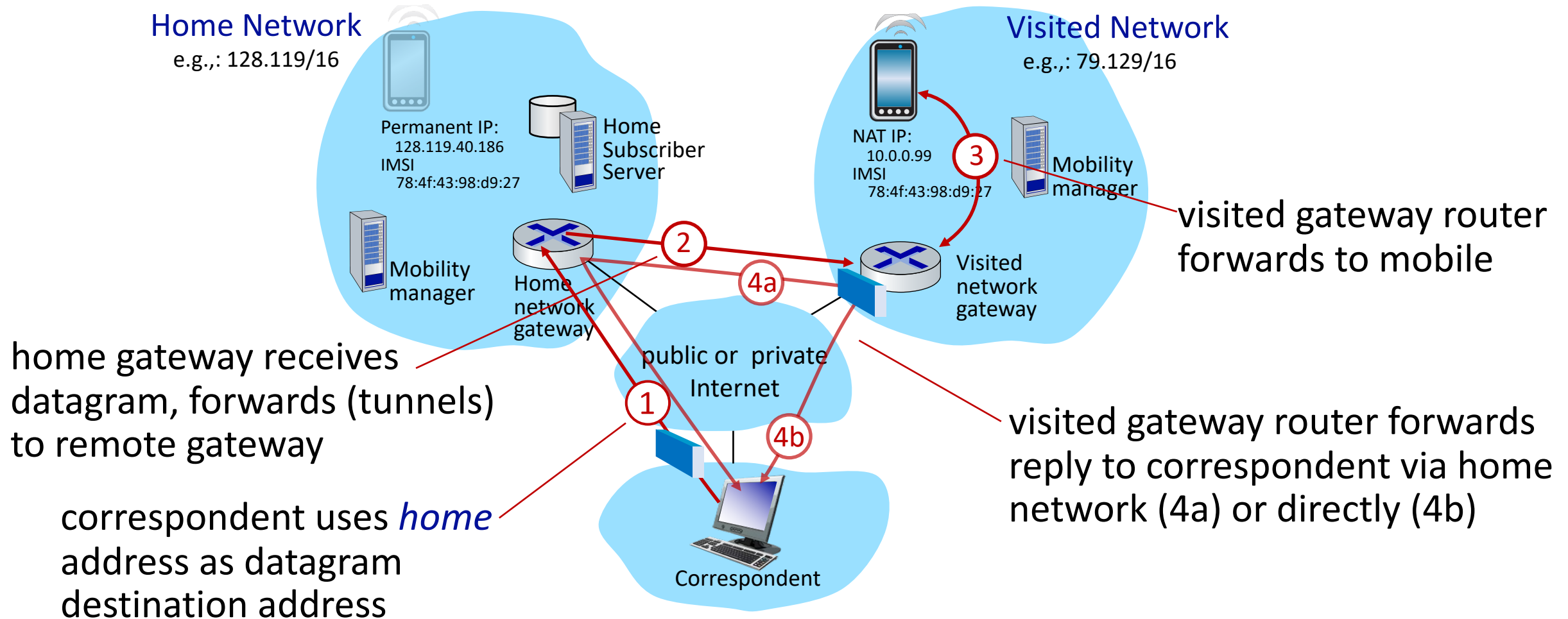
# Registration: home needs to know where you are!



end result:

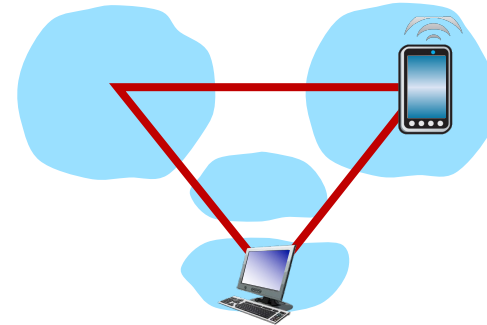
- visited mobility manager knows about mobile
- home HSS knows location of mobile

# Mobility with indirect routing

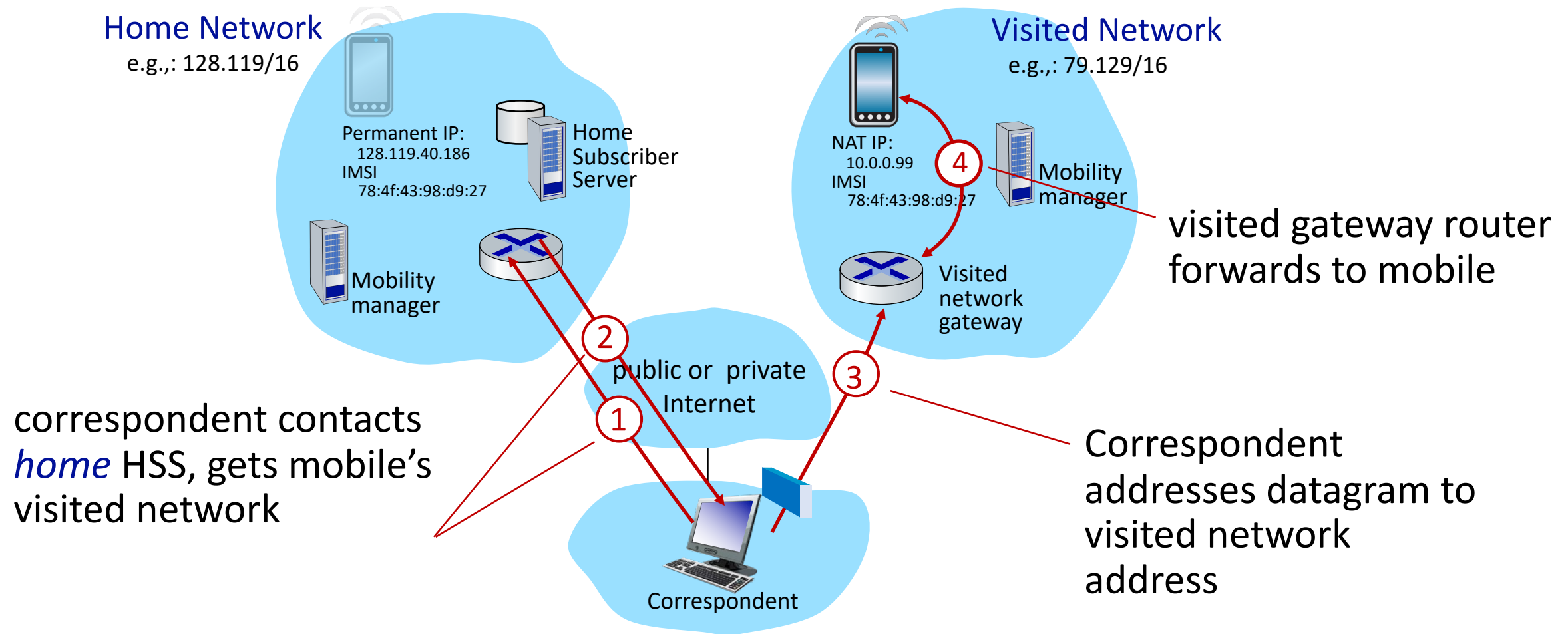


# Mobility with indirect routing: comments

- triangle routing:
  - inefficient when correspondent and mobile are in same network
- mobile moves among visited networks: transparent to correspondent!
  - registers in new visited network
  - new visited network registers with home HSS
  - datagrams continue to be forwarded from home network to mobile in new network
  - *on-going (e.g., TCP) connections between correspondent and mobile can be maintained!*



# Mobility with direct routing



# Mobility with direct routing: comments

- overcomes triangle routing inefficiencies
- *non-transparent to correspondent*: correspondent must get care-of-address from home agent
- what if mobile changes visited network?
  - can be handled, but with additional complexity

# Chapter 7 outline

- Introduction

## Wireless

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

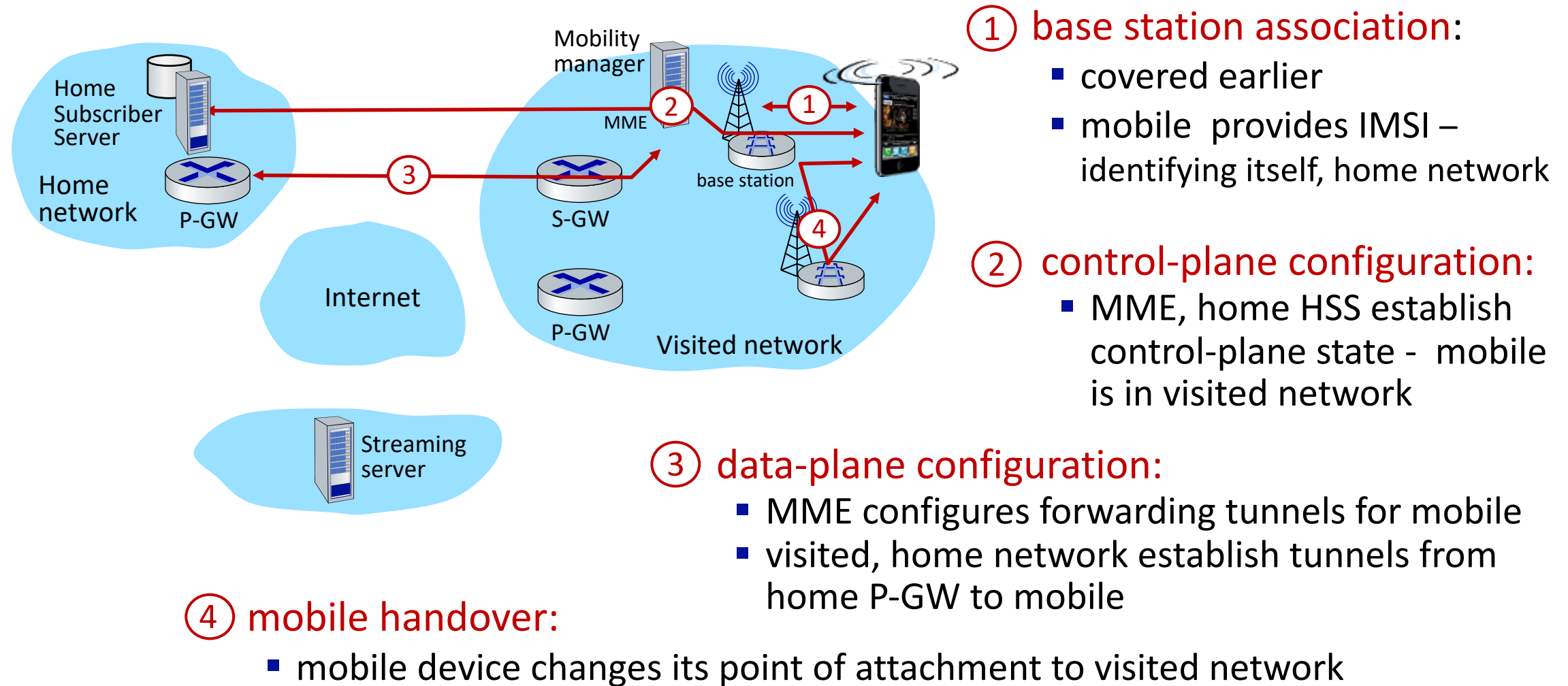


## Mobility

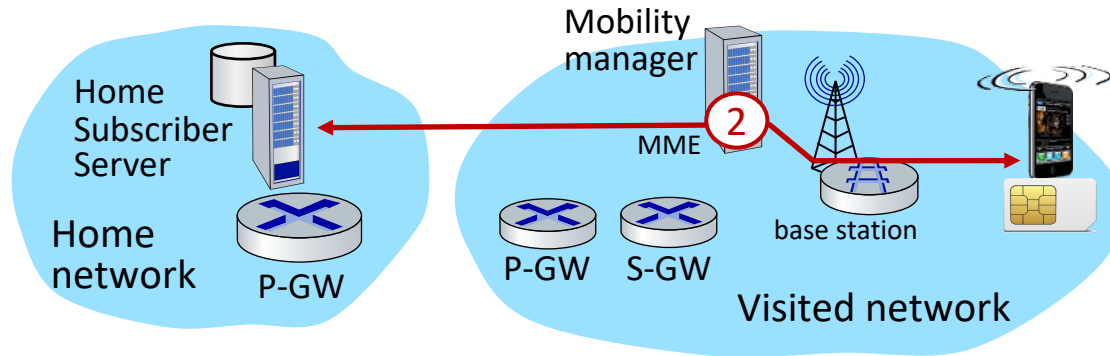
- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols



# Mobility in 4G networks: major mobility tasks



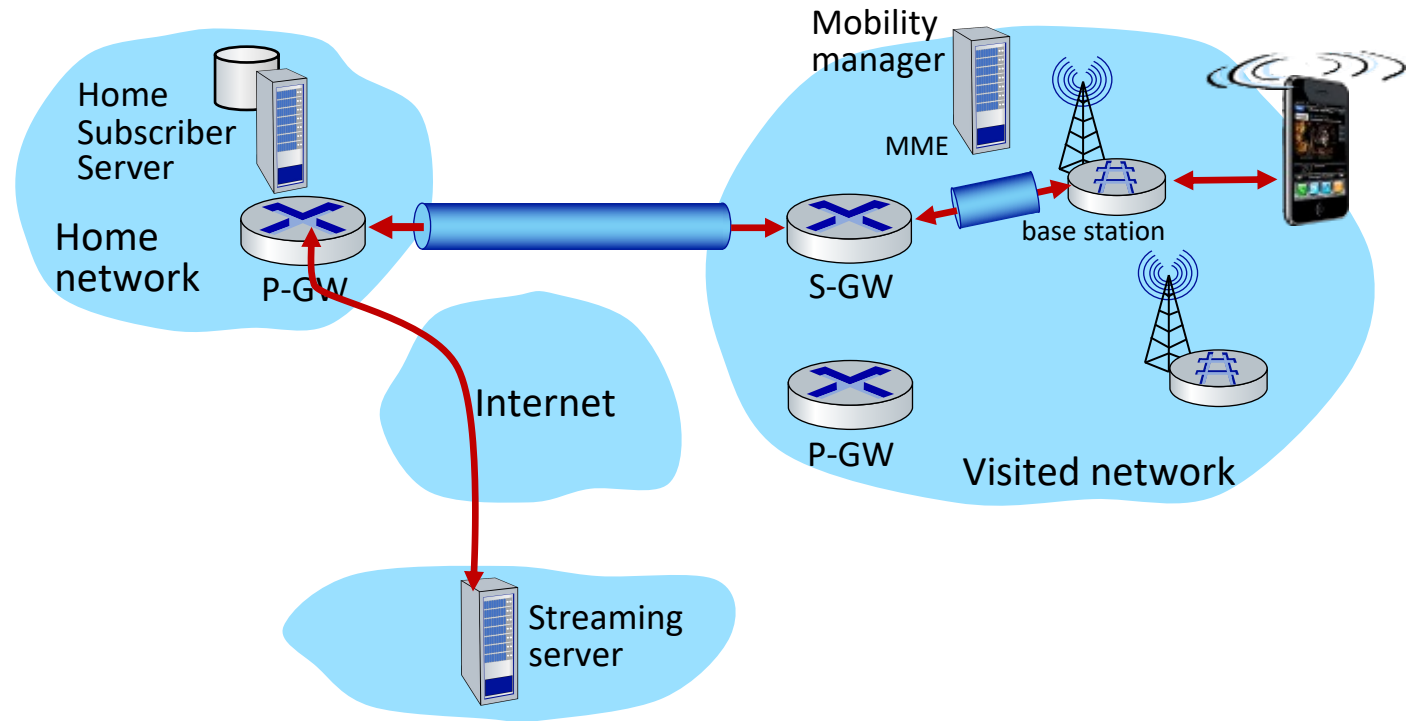
# Configuring LTE control-plane elements



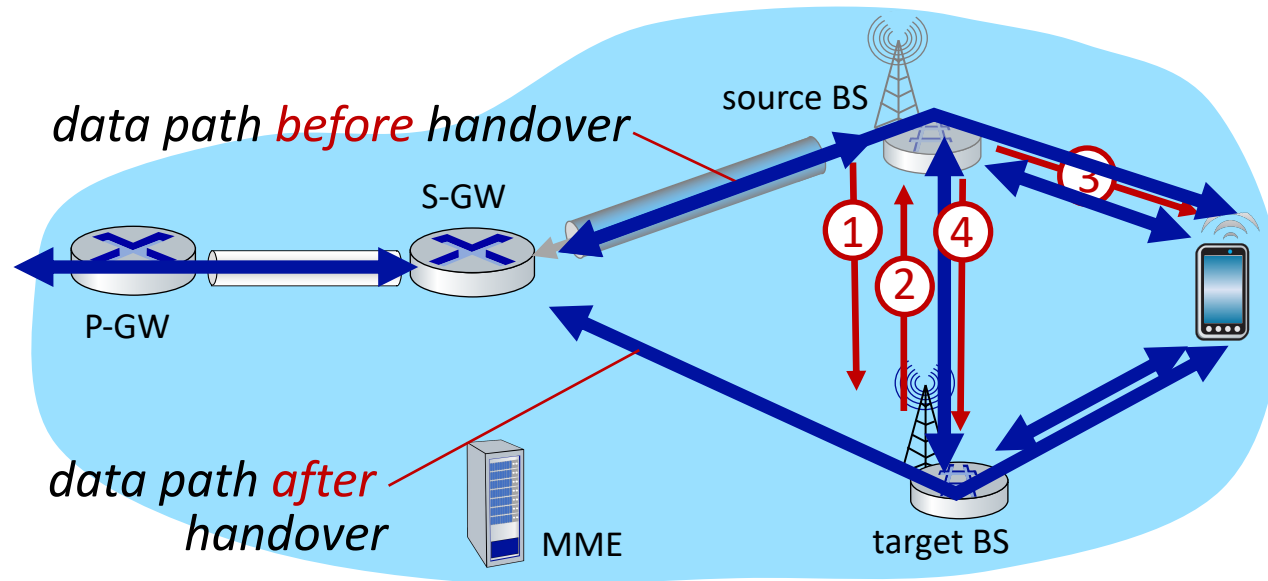
- Mobile communicates with local MME via BS control-plane channel
- MME uses mobile's IMSI info to contact mobile's home HSS
  - retrieve authentication, encryption, network service information
  - home HSS knows mobile now resident in visited network
- BS, mobile select parameters for BS-mobile data-plane radio channel

# Configuring data-plane tunnels for mobile

- **S-GW to BS tunnel:** when mobile changes base stations, simply change endpoint IP address of tunnel
- **S-GW to home P-GW tunnel:** implementation of indirect routing
- **tunneling via GTP** (GPRS tunneling protocol): mobile's datagram to streaming server encapsulated using GTP inside UDP, inside datagram

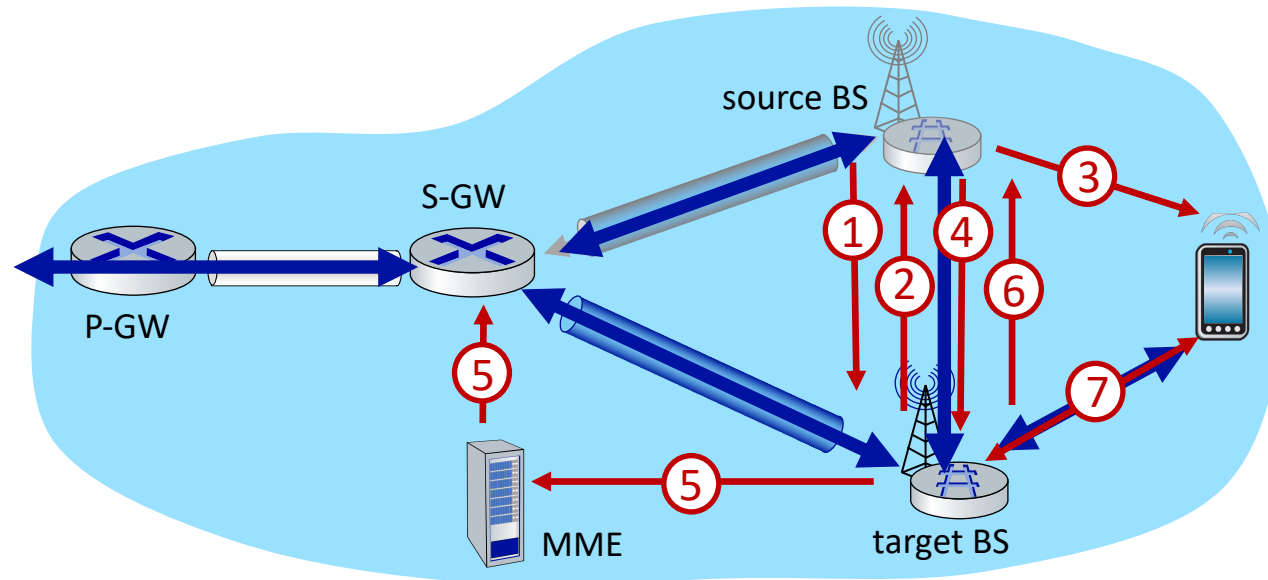


# Handover between BSs in same cellular network



- 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)

# Handover between BSs in same cellular network



- ⑤ target BS informs MME that it is new BS for mobile
- MME instructs S-GW 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 S-GW

# Mobile IP

- mobile IP architecture standardized ~20 years ago [RFC 5944]
  - long before ubiquitous smartphones, 4G support for Internet protocols
  - did not see wide deployment/use
  - perhaps WiFi for Internet, and 2G/3G phones for voice were “good enough” at the time
- mobile IP architecture:
  - indirect routing to node (via home network) using tunnels
  - mobile IP home agent: combined roles of 4G HSS and home P-GW
  - mobile IP foreign agent: combined roles of 4G MME and S-GW
  - protocols for agent discovery in visited network, registration of visited location in home network via ICMP extensions

# Wireless, mobility: impact on higher layer protocols

- logically, impact *should* be minimal ...
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- ... but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handover loss
  - TCP interprets loss as congestion, will decrease congestion window unnecessarily
  - delay impairments for real-time traffic
  - bandwidth a scarce resource for wireless links

# Chapter 7 summary

## 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

