Wireless and Mobile Networks

Wireless and Mobile Networks: context

- more wireless (mobile) phone subscribers than fixed (wired) phone subscribers (10-to-1 in 2019)!

- more mobile-broadband-connected devices than fixed-broadband-connected devices devices (5-1 in 2019)!
  - 4G/5G cellular networks now embracing Internet protocol stack, including SDN

- two important (but different) challenges
  - wireless: communication over wireless link
  - mobility: handling the mobile user who changes point of attachment to network
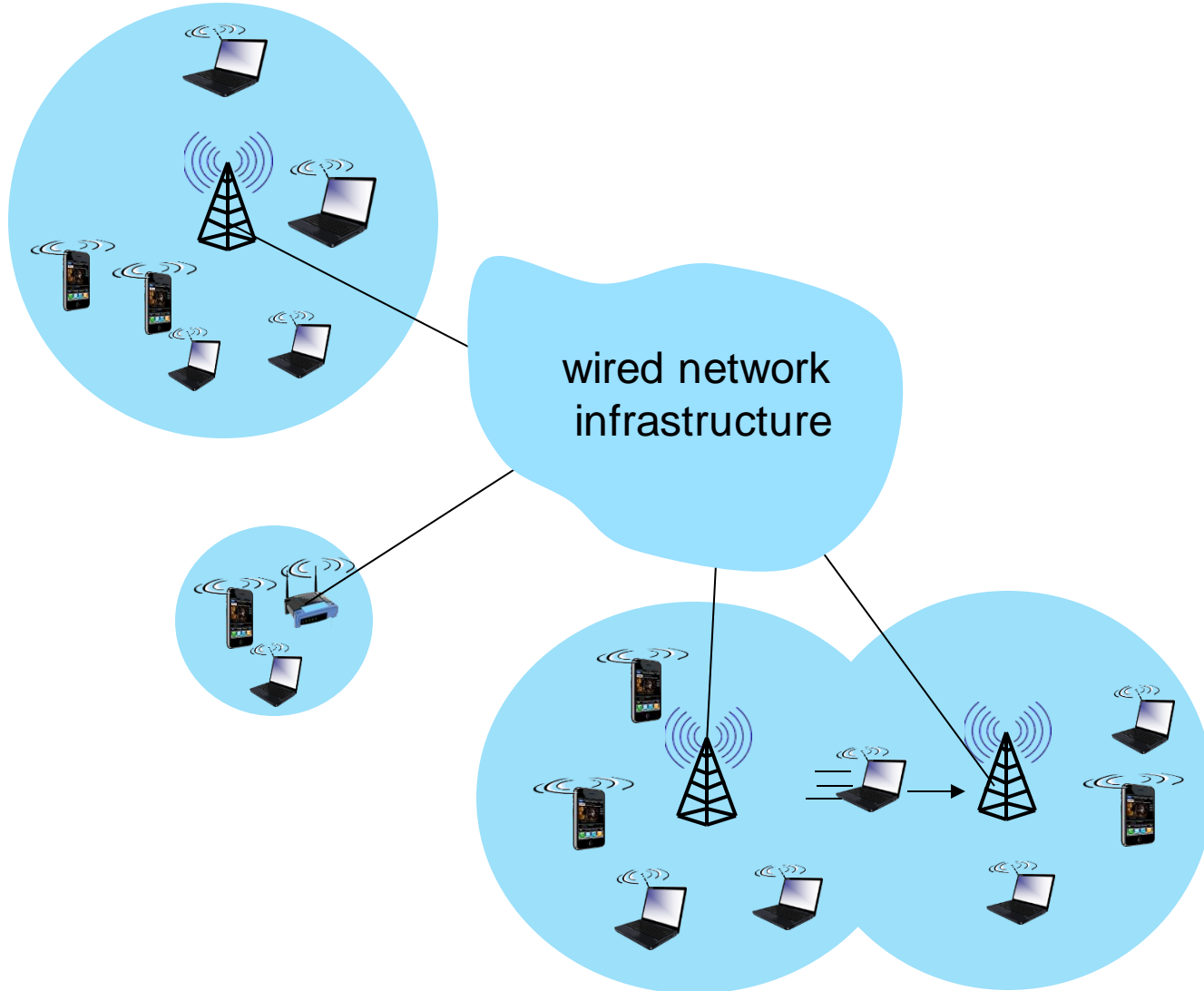
Outline

- **Introduction**

Wireless

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

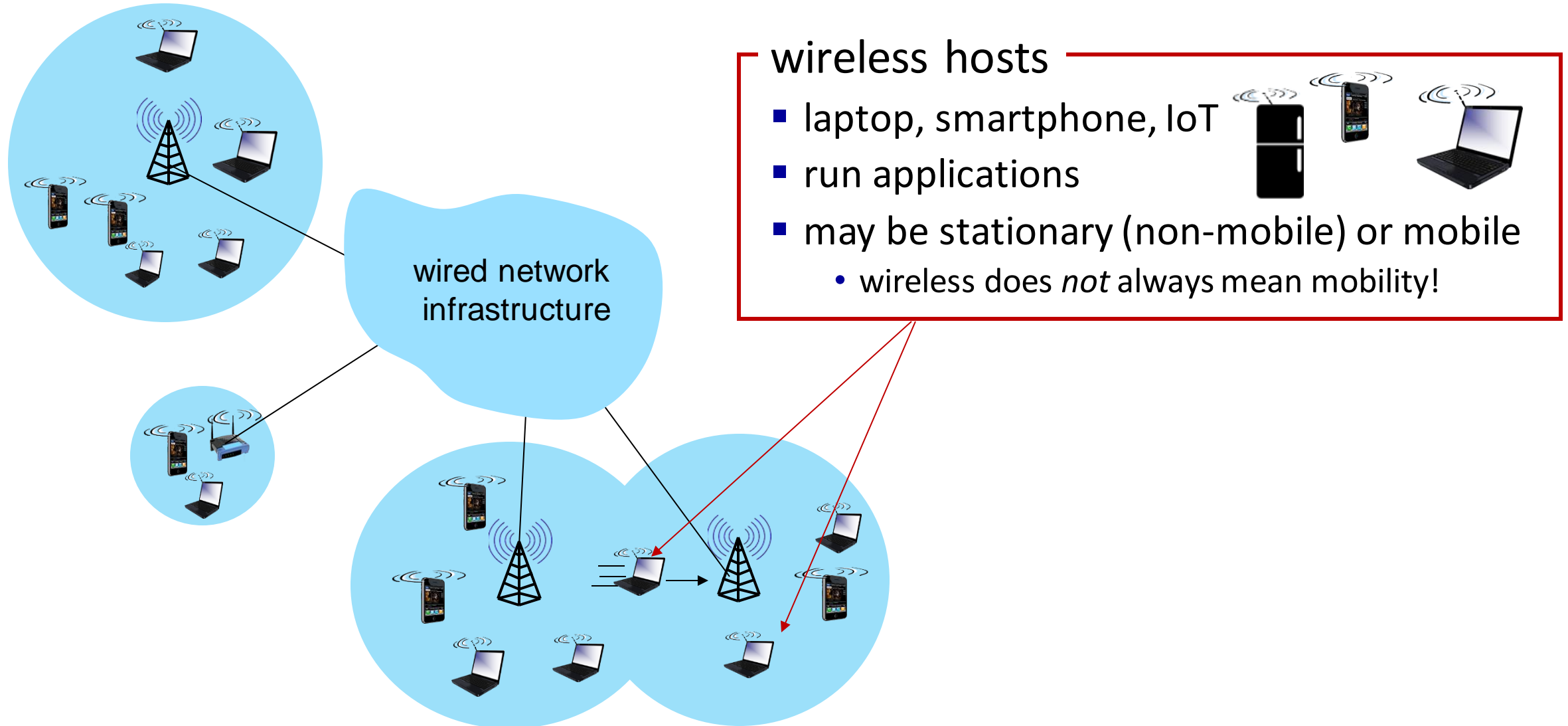## Mobility

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

Elements of a wireless network

wired network infrastructure

Elements of a wireless network

wired network
infrastructure

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

Elements of a wireless network

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

wired network infrastructure
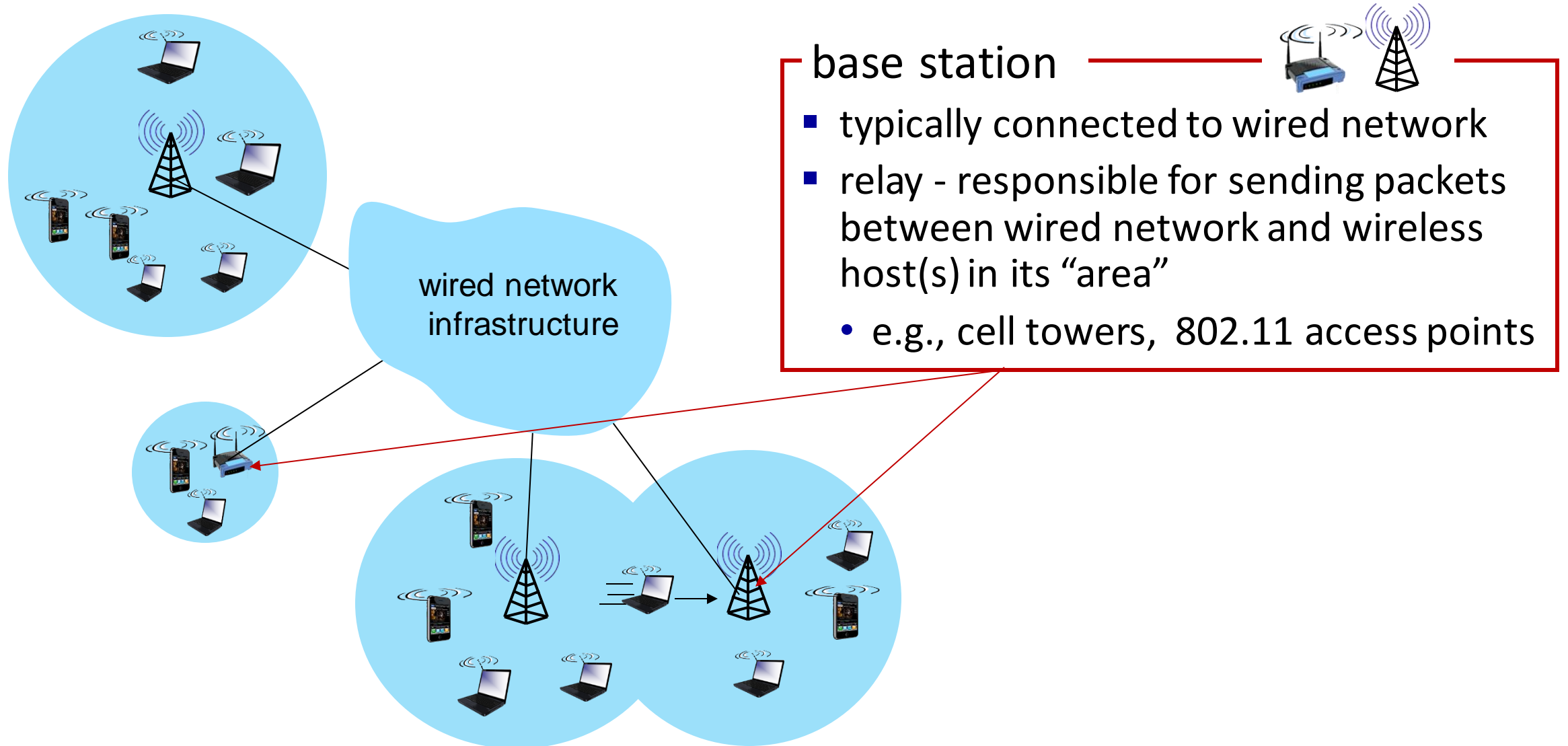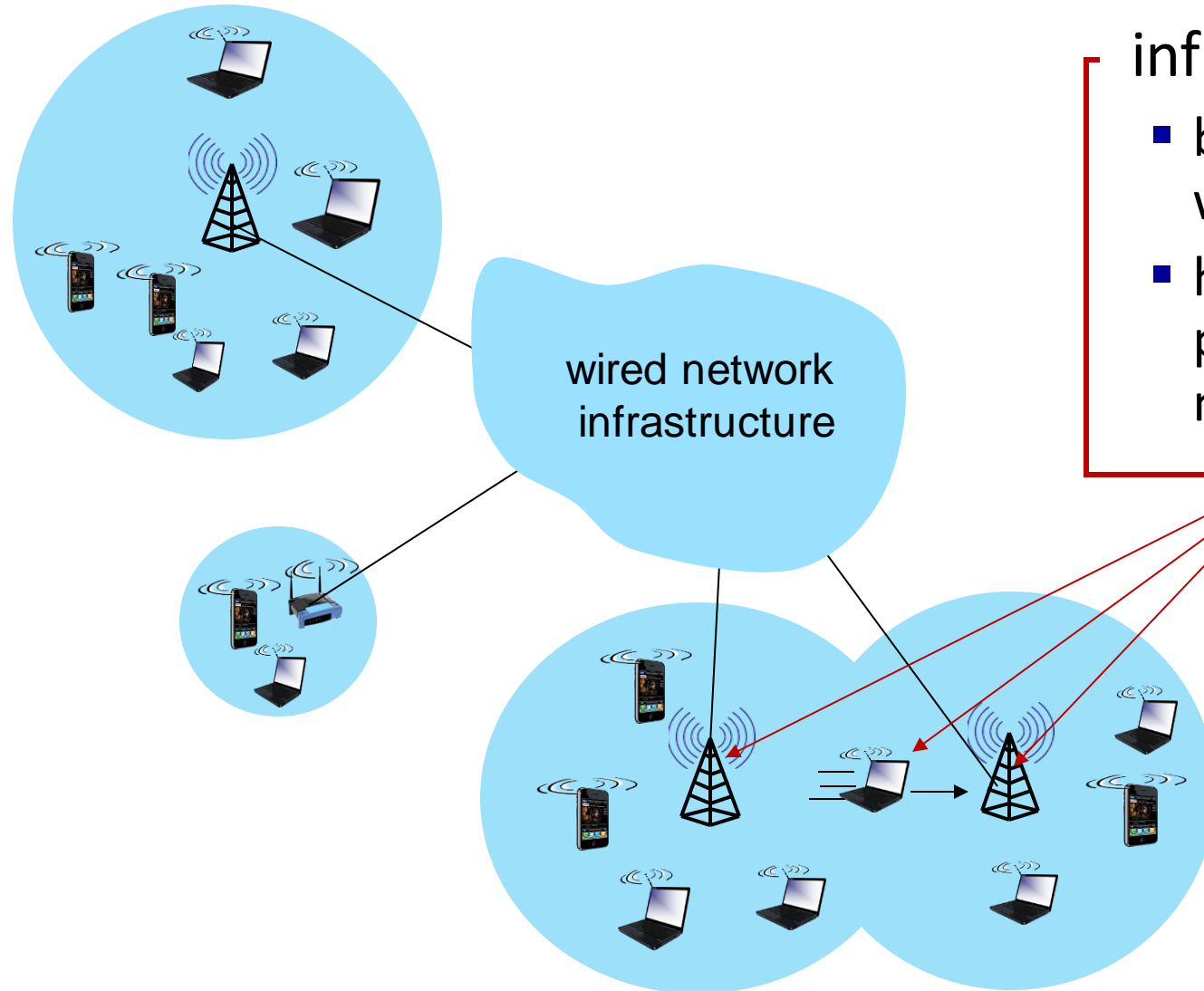
Elements of a wireless network
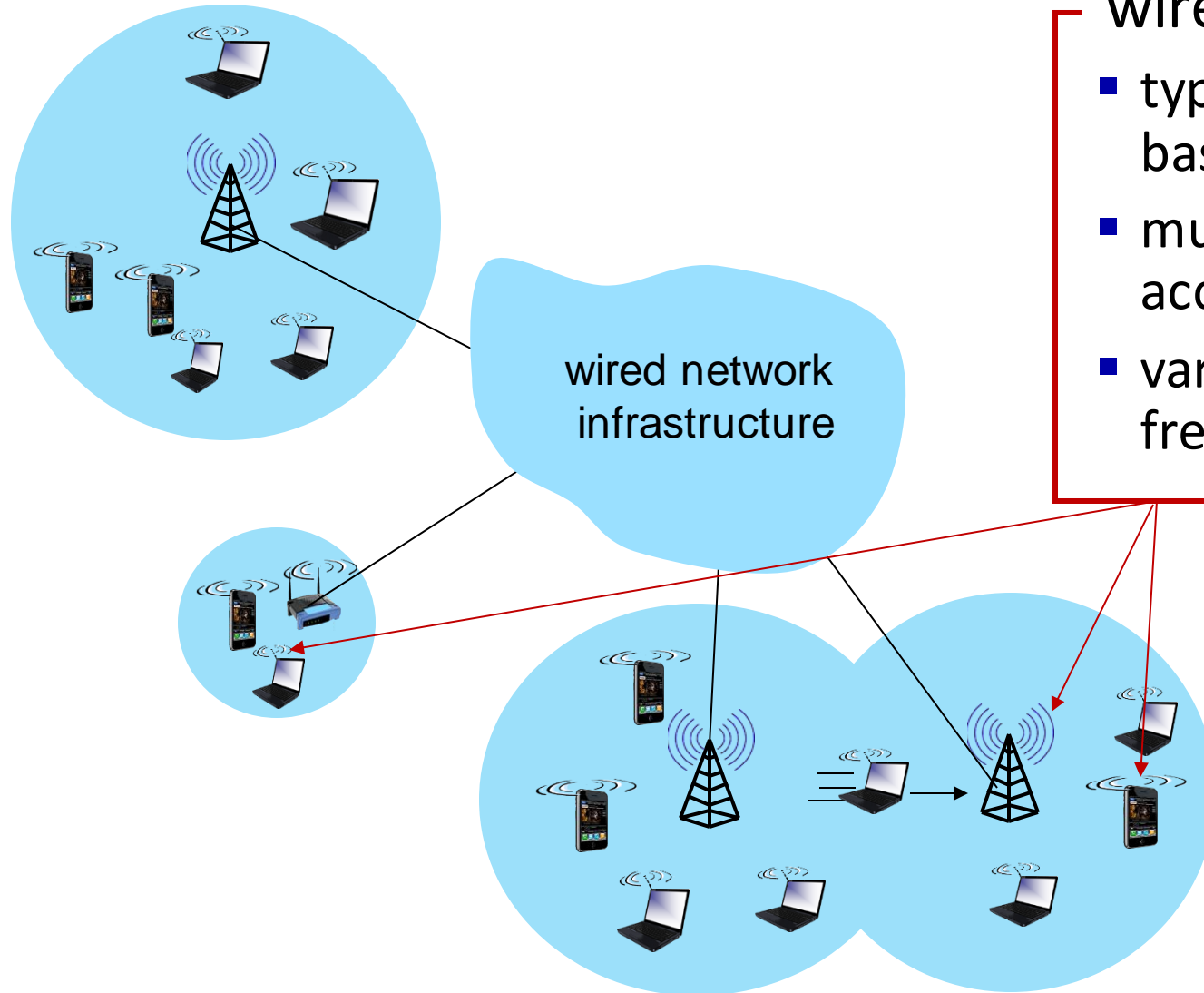
wireless link

- 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

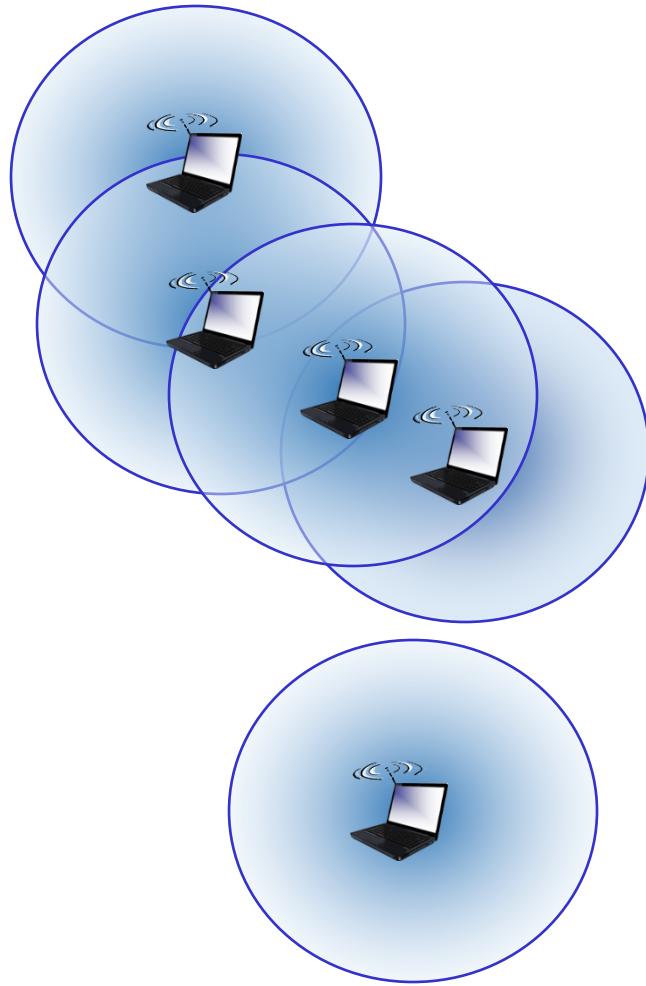wired network infrastructure

Elements of a wireless network

infrastructure mode

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

wired network infrastructure

Elements of a wireless network

ad hoc mode

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

Wireless network taxonomy

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

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"
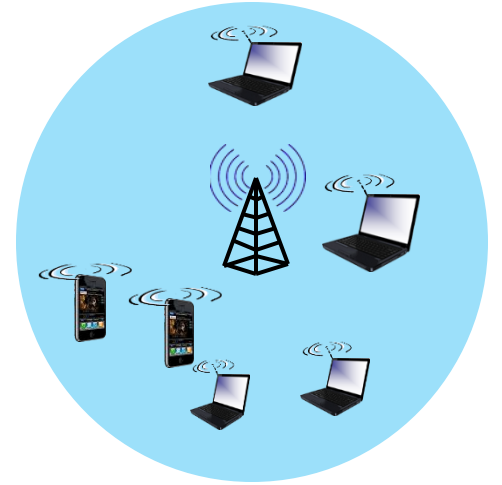
Wireless link characteristics (2)

- **SNR: signal-to-noise ratio**
  - larger SNR – easier to extract signal from noise (a "good thing")

- **SNR versus BER 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)

······· QAM256 (8 Mbps)

- - - QAM16 (4 Mbps)

——— BPSK (1 Mbps)
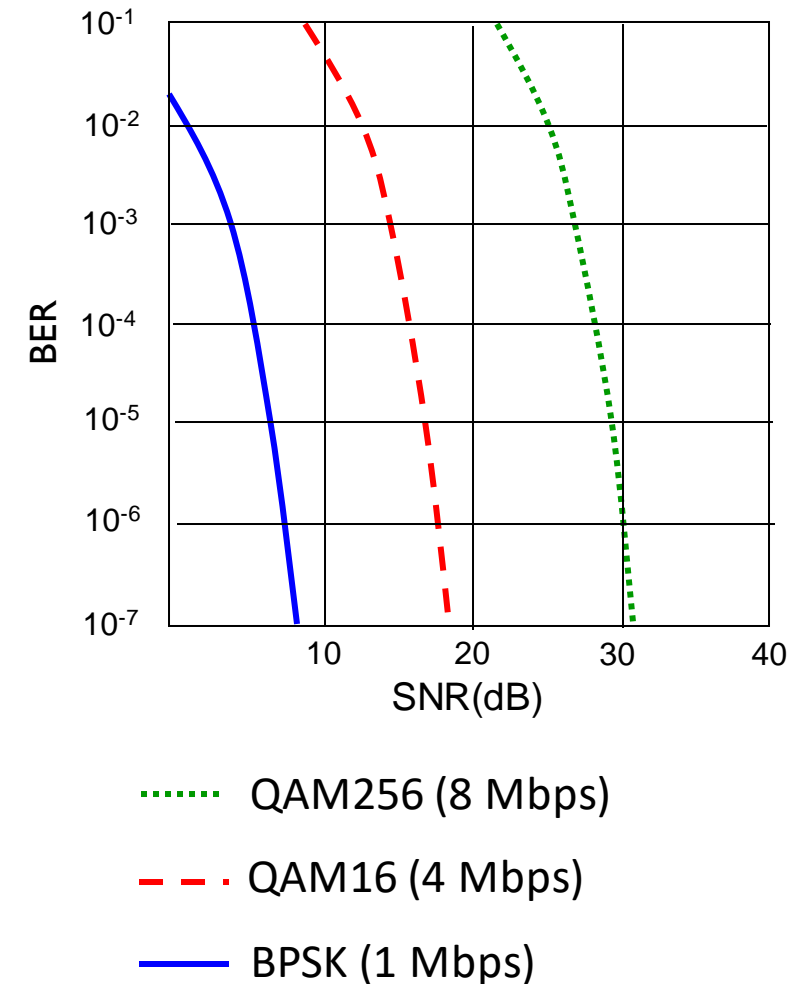
Wireless link characteristics (3)

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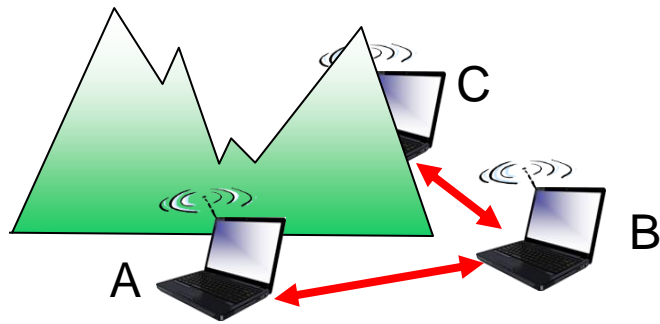
Hidden terminal problem

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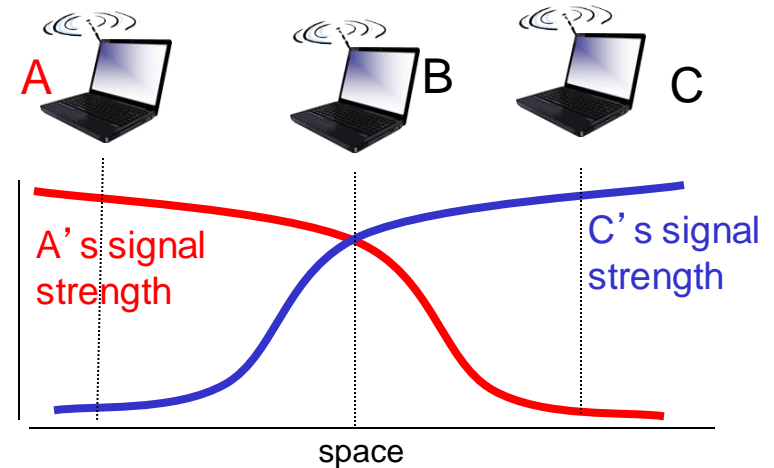- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B

Signal attenuation:

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

Code Division Multiple Access (CDMA)

- unique "code" assigned to each user; i.e., code set partitioning
  - all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data
  - allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")

- encoding: inner product: (original data) X (chipping sequence)

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

CDMA encode/decode

channel output $Z_{i,m}$

$Z_{i,m} = d_i \cdot c_m$

sender

data bits

$d_1 = -1$ $d_0 = 1$

code

slot 1   slot 0

slot 1 channel output   slot 0 channel output

receiver

received input

$$D_i = \frac{\sum_{m=1}^{M} Z_{i,m} \cdot c_m}{M}$$

code

slot 1   slot 0

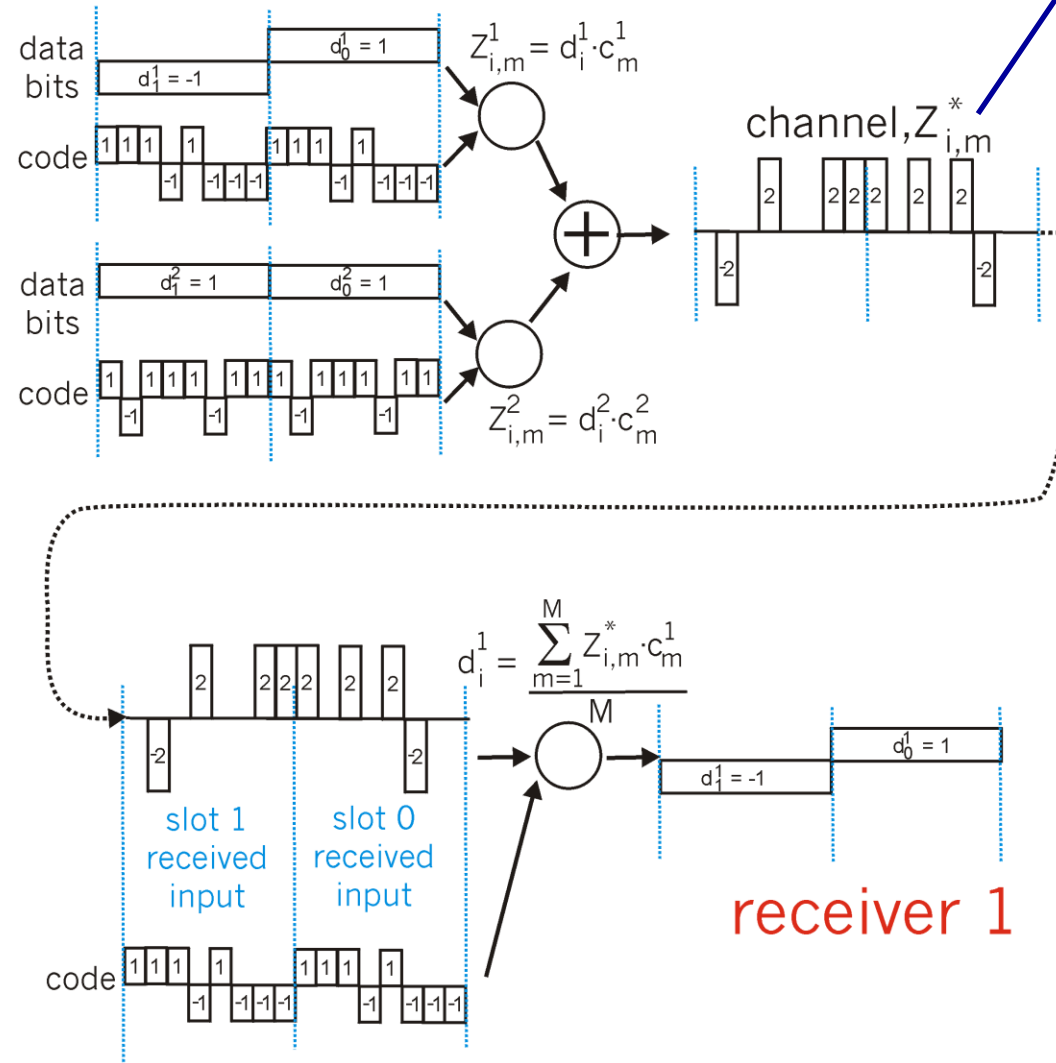$d_1 = -1$ $d_0 = 1$

slot 1 channel output   slot 0 channel output
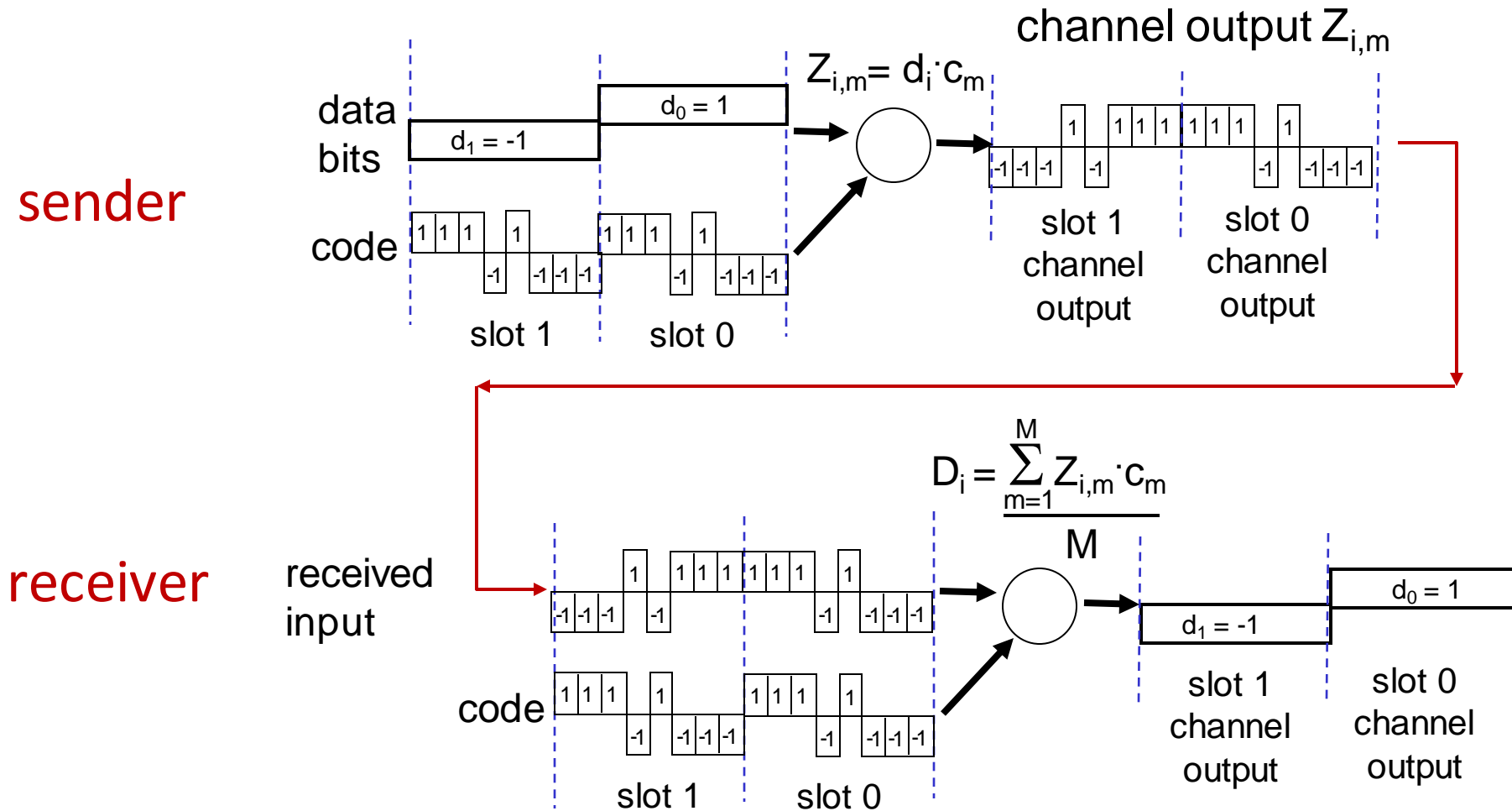
… but this isn't really useful yet!

CDMA: two-sender interference

channel sums together transmissions by sender 1 and 2

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

... now *that's* useful!

Outline

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

Internet

switch or router

BSS 1

BSS 2
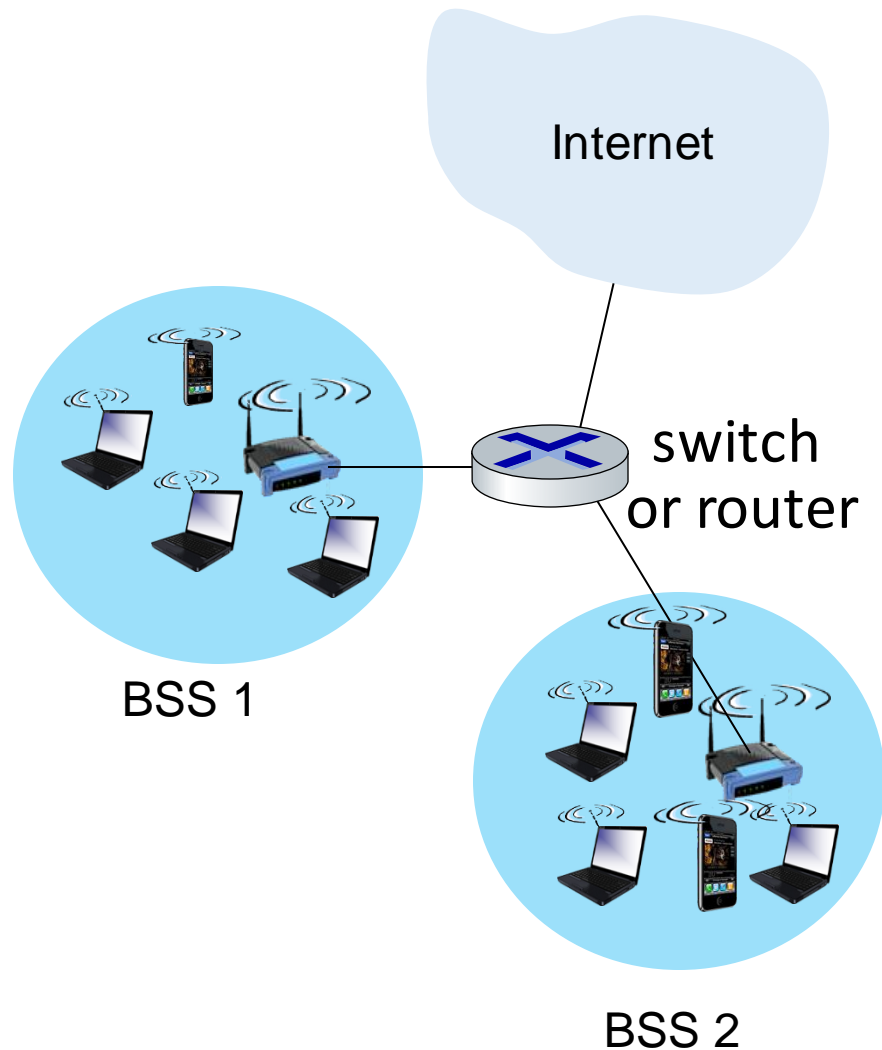
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

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

BSS

802.11: passive/active scanning
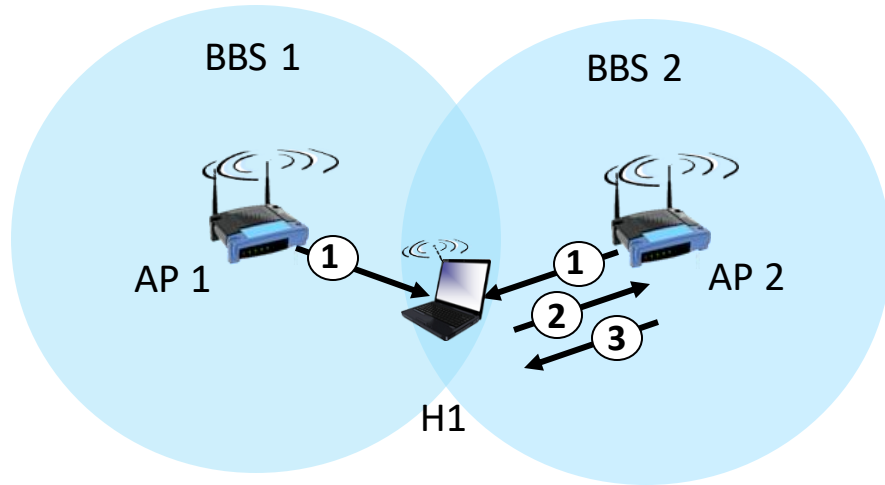
passive scanning:
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1
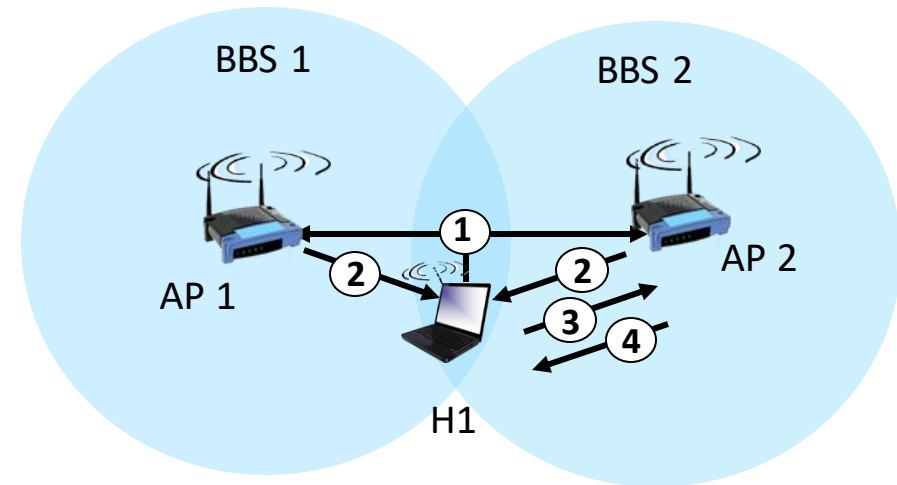
active scanning:
(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

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

A' s signal strength

C' s signal strength

space
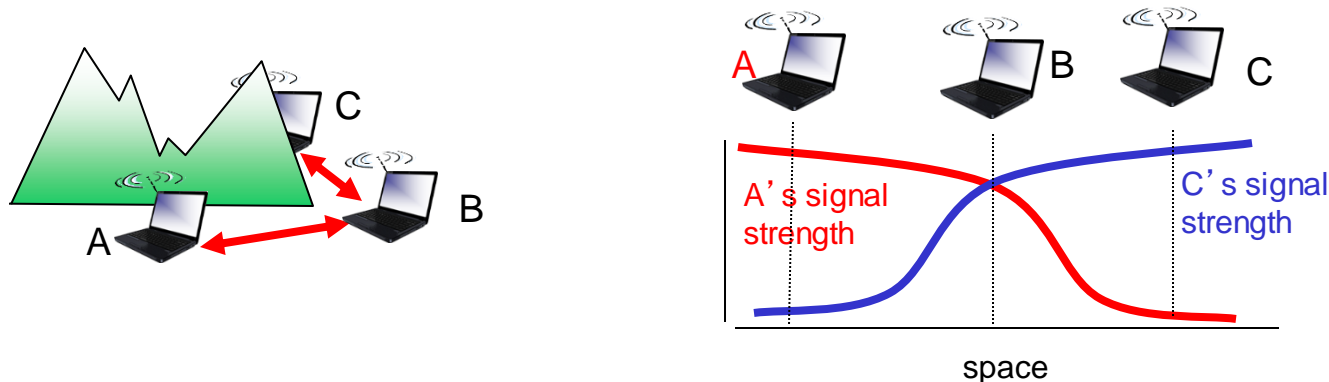
IEEE 802.11 MAC Protocol: CSMA/CA

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)

sender   receiver

DIFS {

data

SIFS

ACK
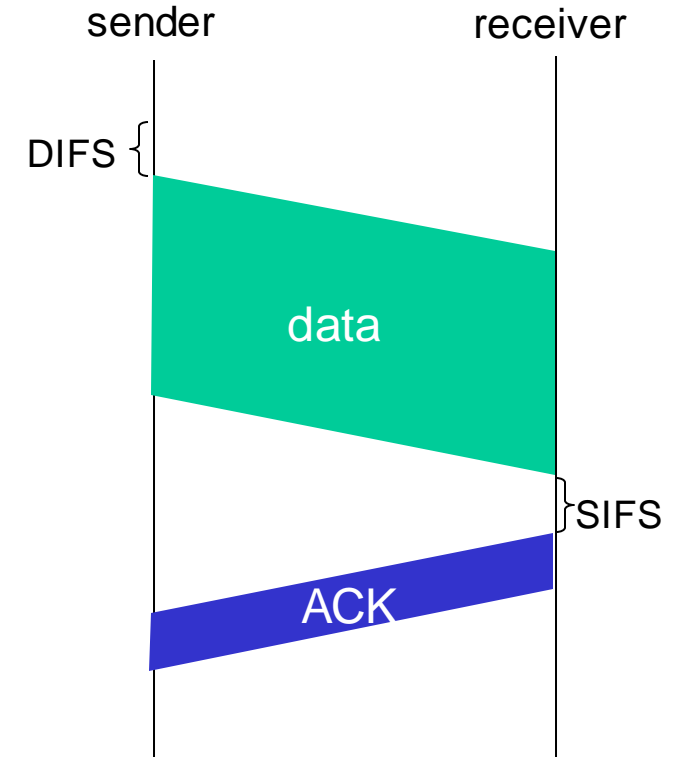
Avoiding collisions (more)

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

A

AP

B

RTS(A)

RTS(B)

reservation collision

RTS(A)

CTS(A)

CTS(A)

time

DATA (A)

defer

ACK(A)

ACK(A)

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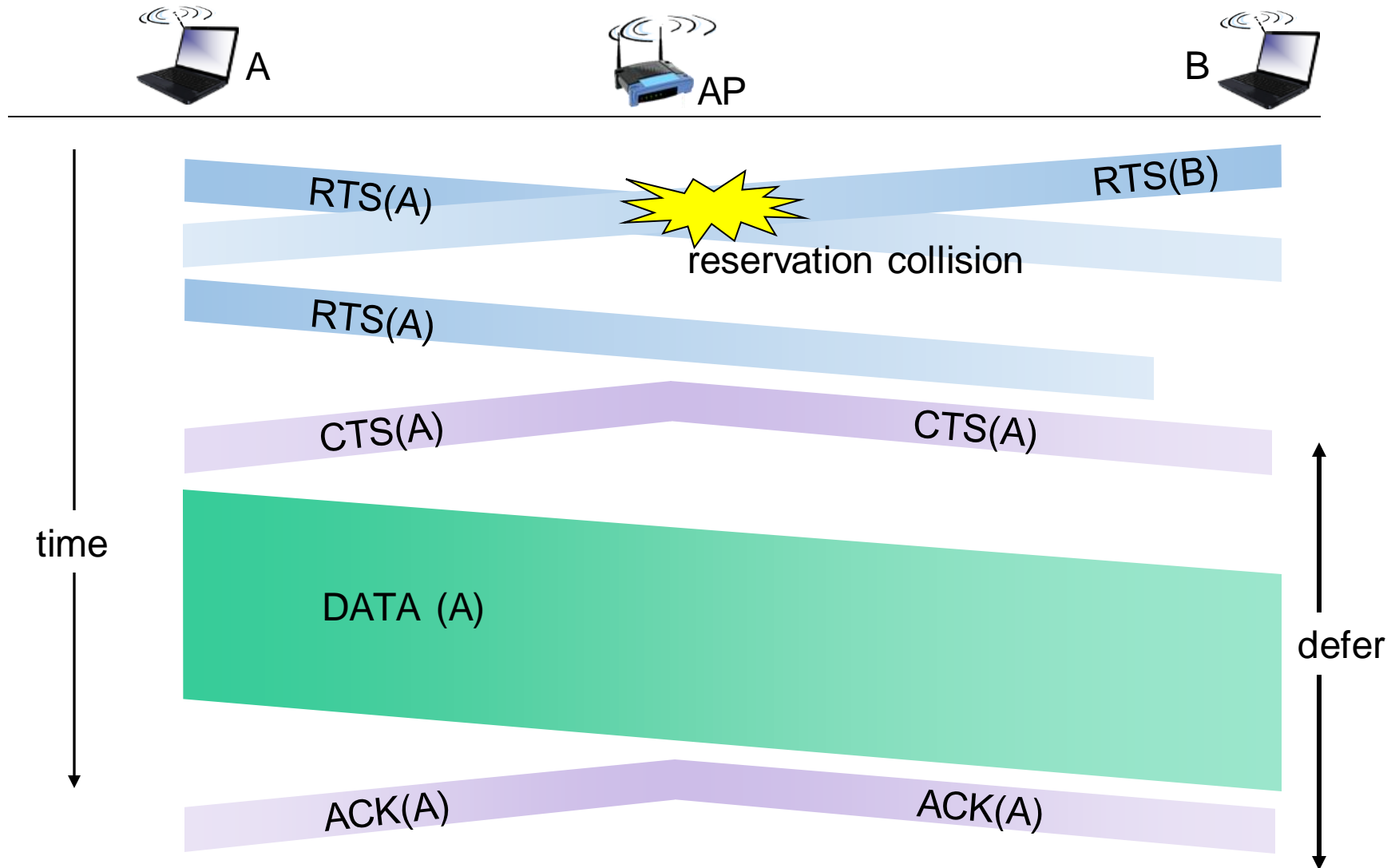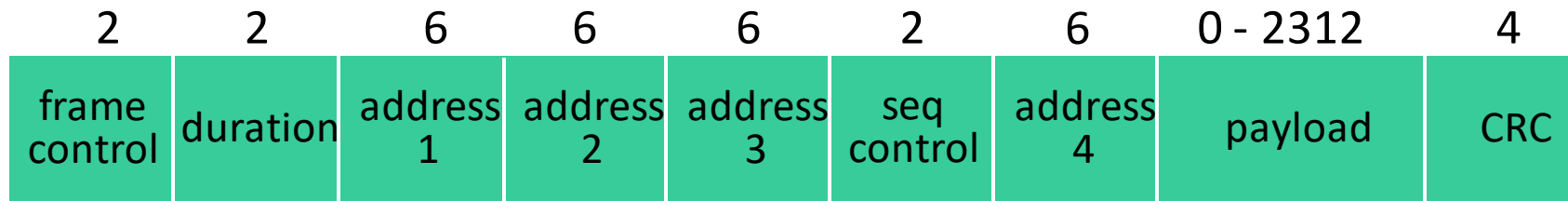
Address 1: MAC address of wireless host or AP to receive this frame

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

Internet

H1

R1

802.3 Ethernet frame

R1 MAC addr	H2 MAC addr
MAC dest addr	MAC source addr

AP MAC addr	H1 MAC addr	R1 MAC addr
address 1	address 2	address 3

802.11 WiFi frame

802.11 frame: addressing

duration of reserved
transmission time (RTS/CTS)

frame sequence # (for reliable data
transfer)

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

frame type (RTS, CTS, ACK, data)

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

radius of coverage

M master device

C client device

P parked device (inactive)
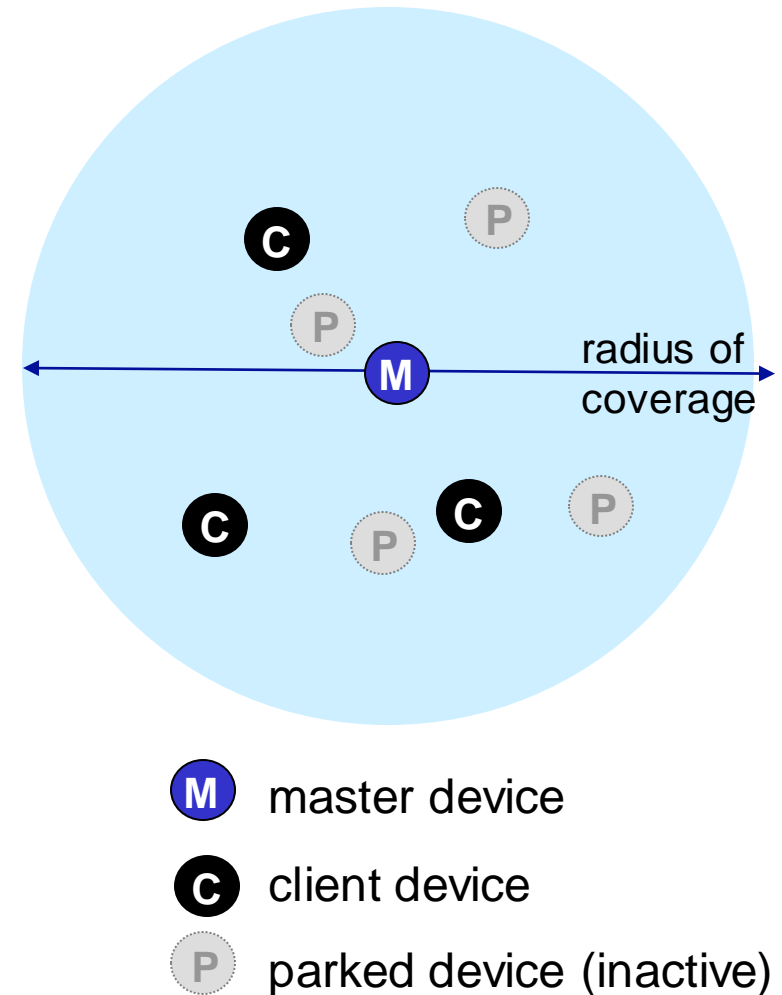
Personal area networks: Bluetooth

- TDM, 625 μsec 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
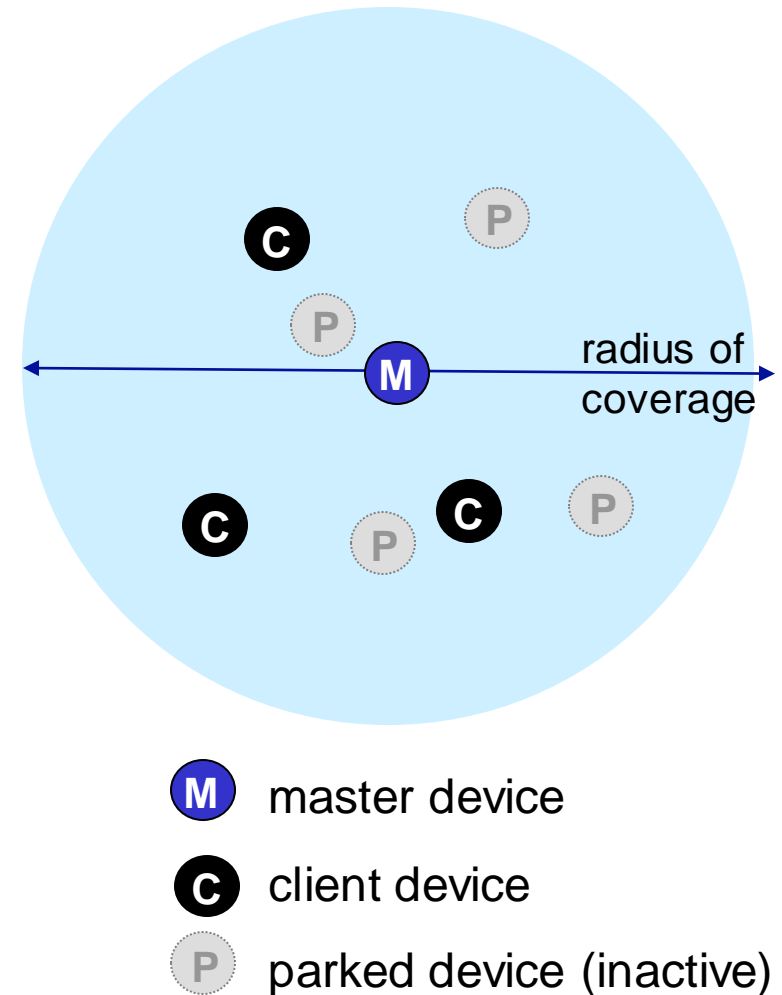
radius of coverage

M master device

C client device

P parked device (inactive)

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

cellular networks

- *the* solution for wide-area mobile Internet

- widespread deployment/use:

  - more mobile-broadband-connected devices than fixed-broadband-connected devices 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)

  - wwww.3gpp.org

  - 4G: Long-Term Evolution (LTE)standard

cellular networks

similarities to wired Internet

- edge/core distinction, but both belong 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)

Mobile device (**UE**)

Base station (**eNode-B**)

Mobility Management Entity (**MME**)

Home Subscriber Service (**HSS**)

to Internet

PDN gateway (**P-GW**)

Serving Gateway (**S-GW**)

radio access network

all-IP Enhanced Packet Core (EPC)
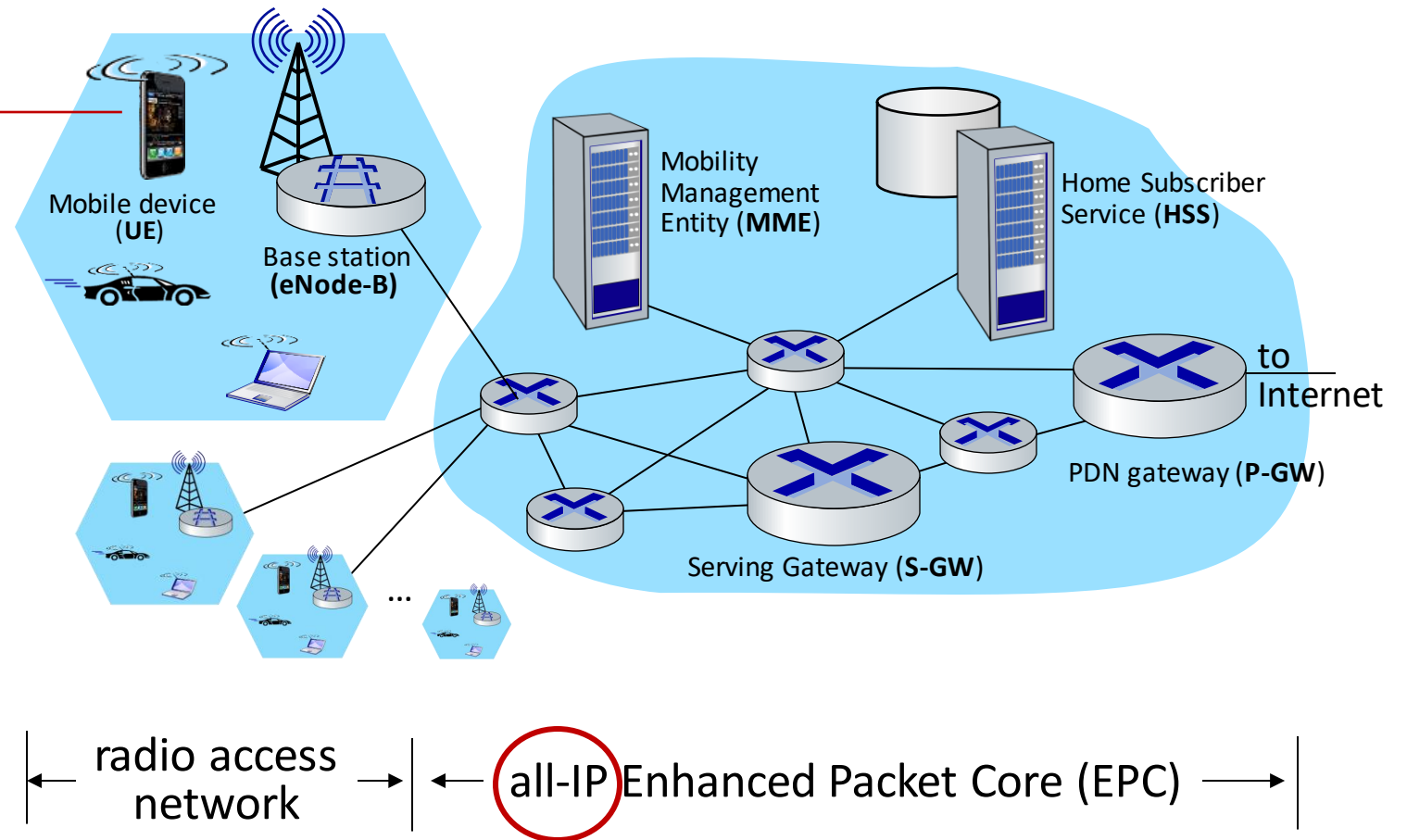
Elements of 4G LTE architecture

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 nearly base stations to optimize radio use

- LTE jargon: eNode-B

Mobile device (**UE**)

Base station (**eNode-B**)

Mobility Management Entity (**MME**)

Home Subscriber Service (**HSS**)

to Internet

PDN gateway (**P-GW**)

Serving Gateway (**S-GW**)

...
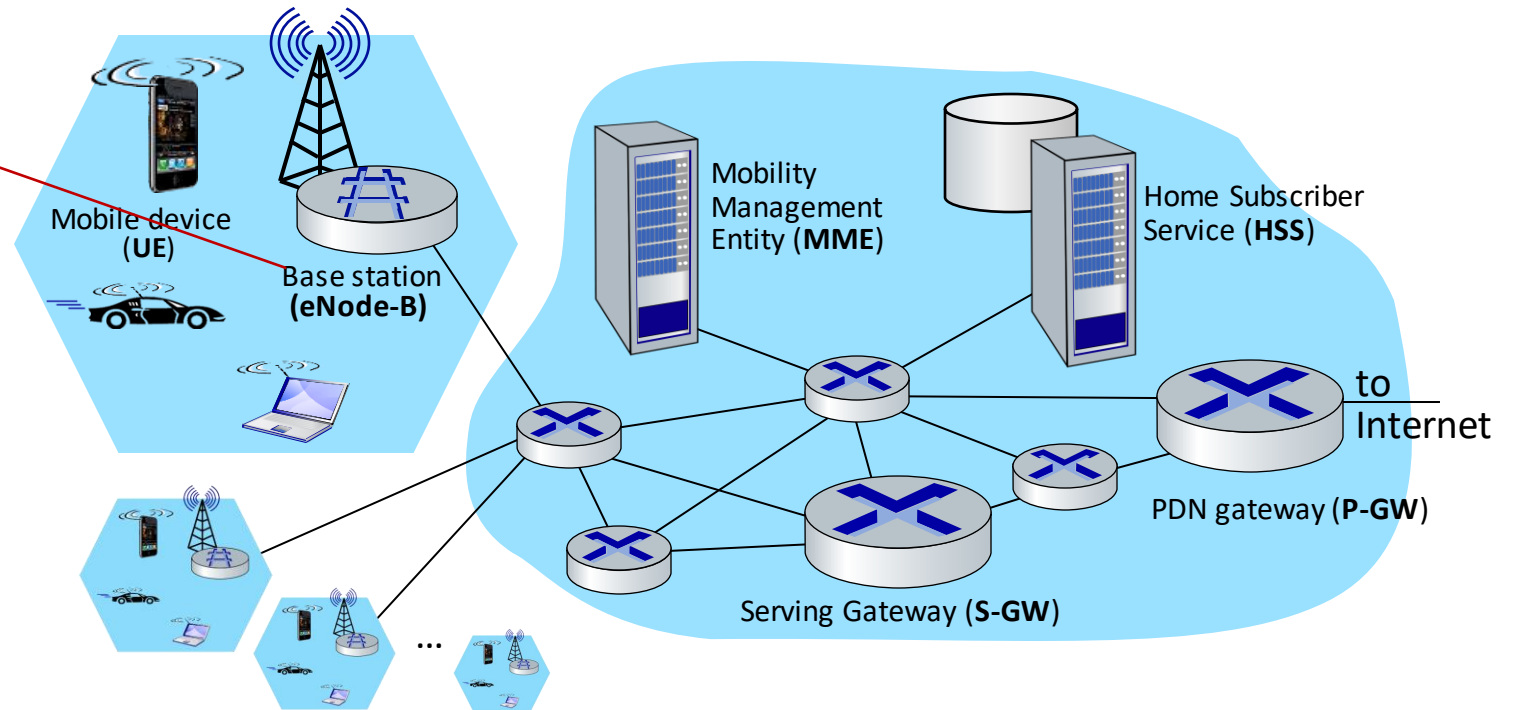
Elements of 4G LTE architecture

Home Subscriber Service

- stores info about mobile devices for which the HSS's network is their "home network"

- works with MME in device authentication

Mobile device (**UE**)

Base station (**eNode-B**)

Mobility Management Entity (**MME**)

Home Subscriber Service (**HSS**)

to Internet

PDN gateway (**P-GW**)

Serving Gateway (**S-GW**)

...
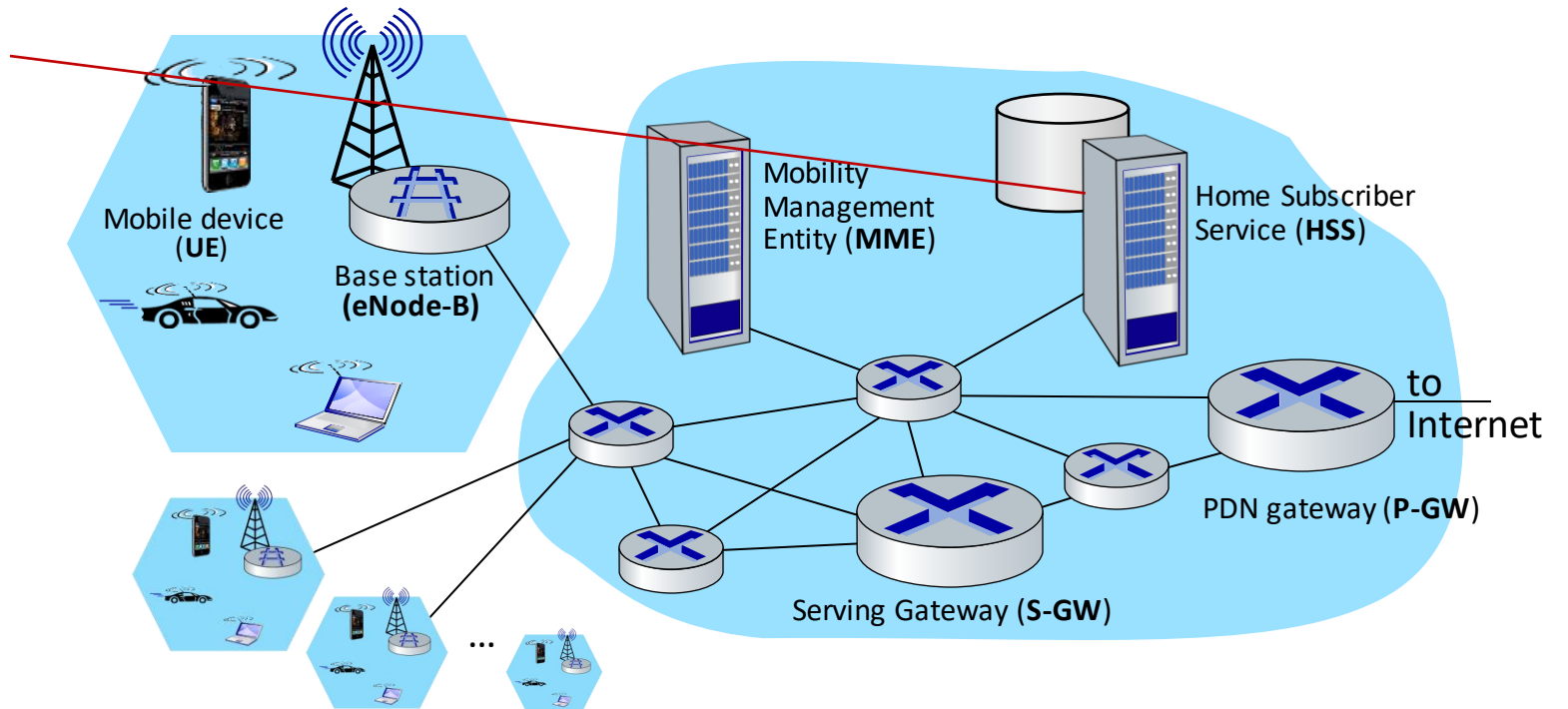
Elements of 4G LTE architecture

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

Mobile device (**UE**)

Base station (**eNode-B**)

Mobility Management Entity (**MME**)

Home Subscriber Service (**HSS**)

to Internet

PDN gateway (**P-GW**)

Serving Gateway (**S-GW**)

...
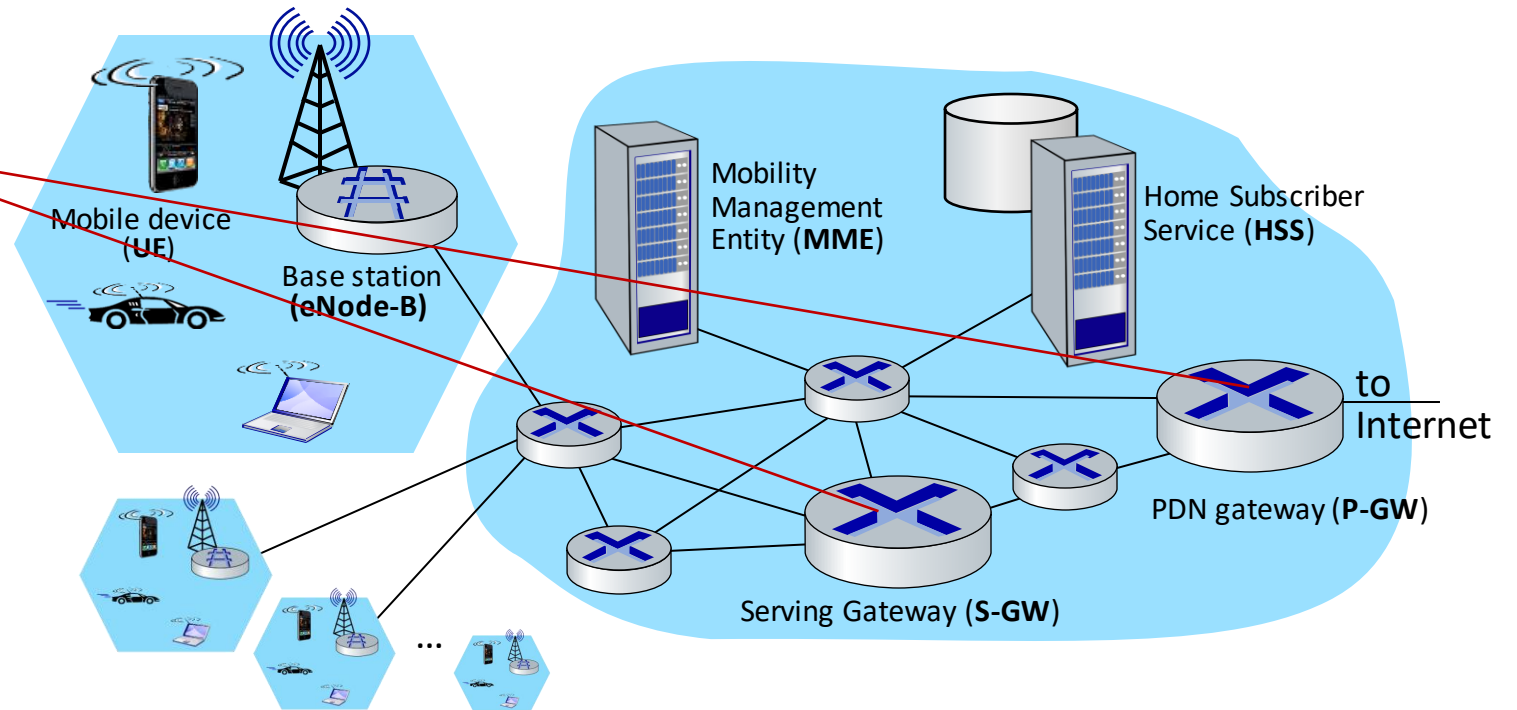
Elements of 4G LTE architecture

Mobility Management Entity

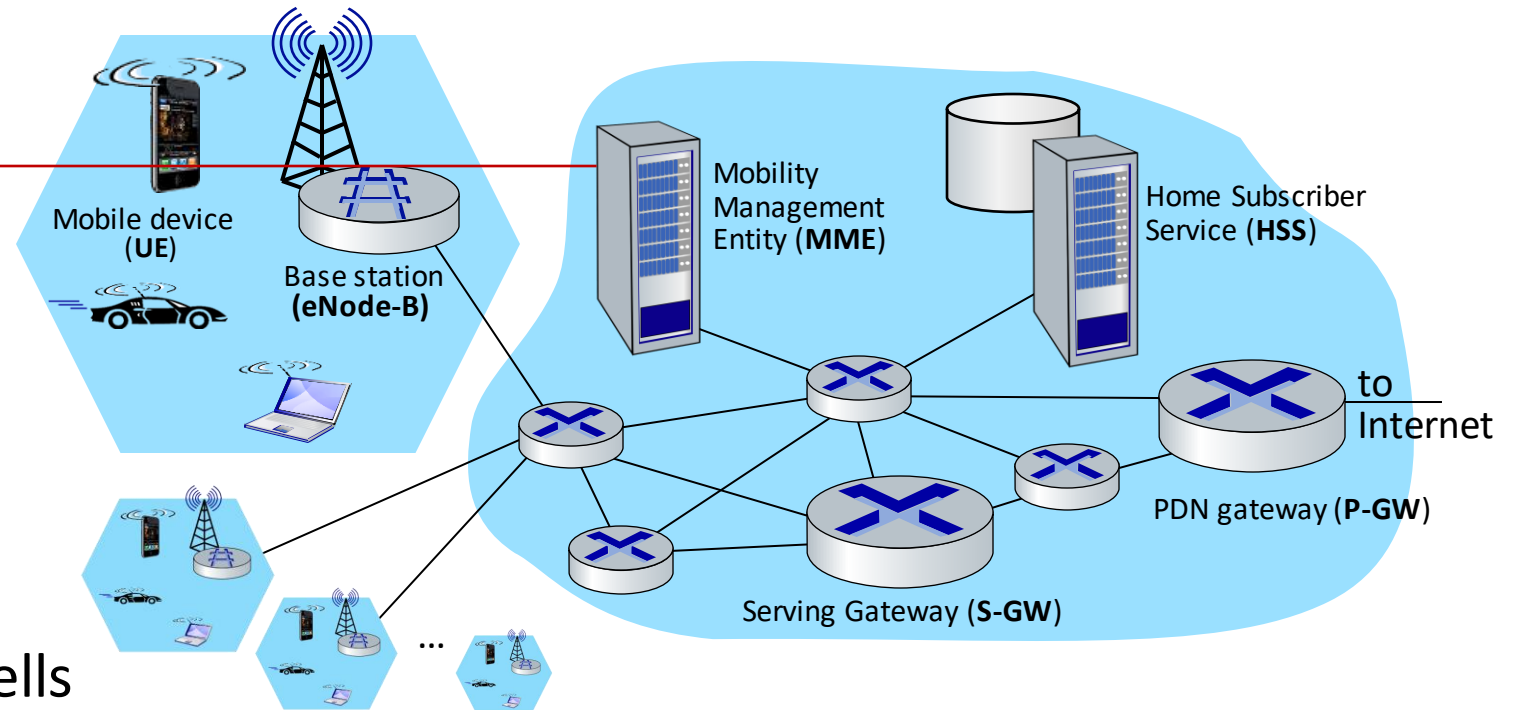- device authentication (device-to-network, network-to-device) coordinated with mobile home network HSS

- mobile device management:
  - device handover between cells
  - tracking/paging device location

- path (tunneling) setup from mobile device to P-GW

Mobile device (**UE**)

Base station (**eNode-B**)

Mobility Management Entity (**MME**)

Home Subscriber Service (**HSS**)

to Internet

PDN gateway (**P-GW**)

Serving Gateway (**S-GW**)

...

LTE: data plane control plane separation

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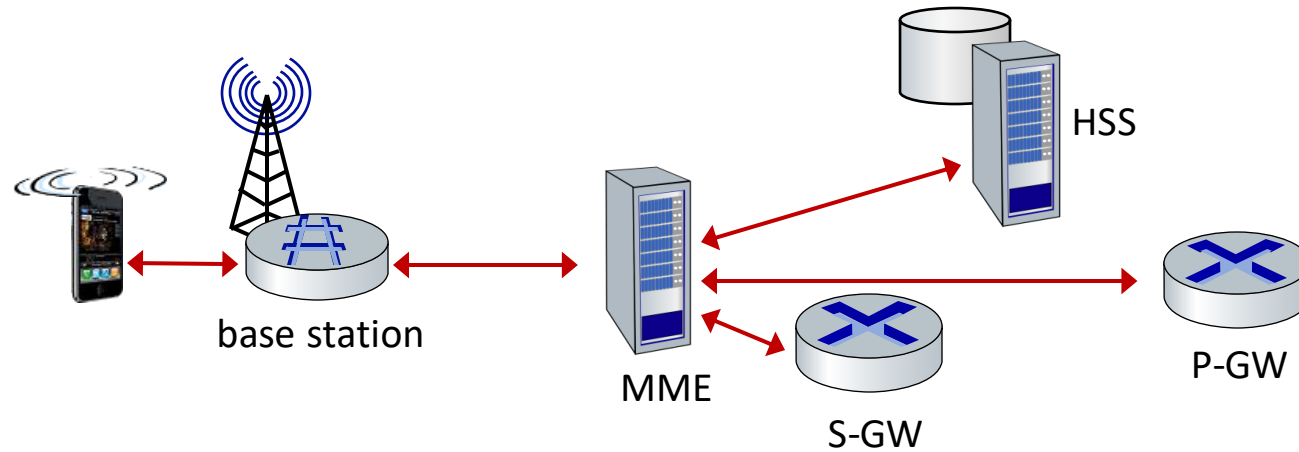
control plane
- new protocols for mobility management , security, authentication (later)

base station

MME

S-GW

P-GW

base station

S-GW

P-GW

data plane
- new protocols at link, physical layers
- extensive use of tunneling to facilitate mobility
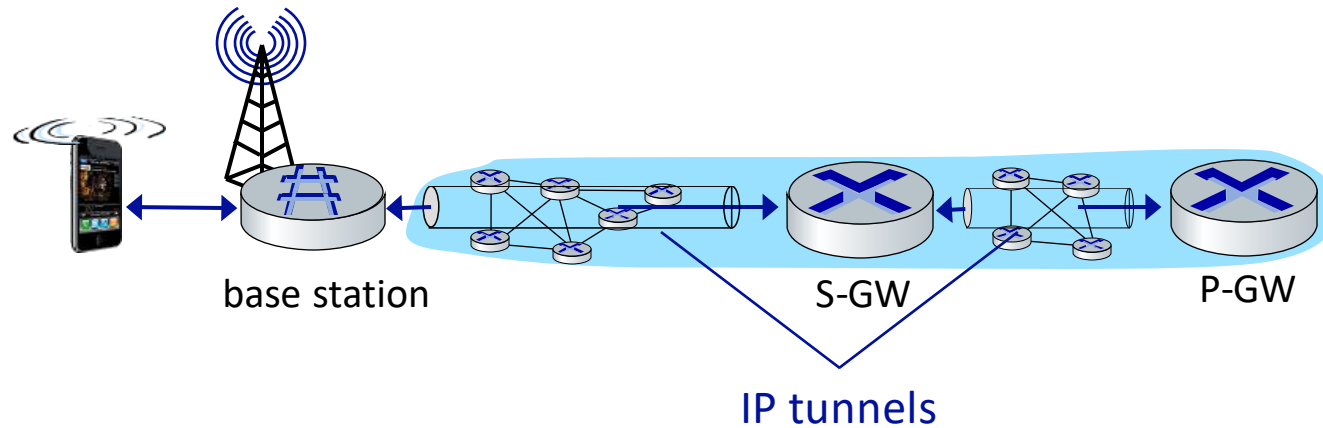
IP tunnels

LTE data plane protocol stack: first hop

Application
Transport
IP
Packet Data Convergence
Radio Link
Medium Access
Physical

Link

IP
Packet Data Convergence
Radio Link
Medium Access
Physical

LTE link layer protocols:

- Packet Data Convergence: header compression, encryption

- Radio Link Control (RLC) Protocol: fragmentation/reassembly, reliable data transfer

- Medium Access: requesting, use of radio transmission slots

base station

S-GW

P-GW

data plane

LTE data plane protocol stack: first hop

Application
Transport
IP
Packet Data Convergence
Radio Link
Medium Access
Physical

Link

IP
Packet Data Convergence
Radio Link
Medium Access
Physical

base station

LTE radio access network:

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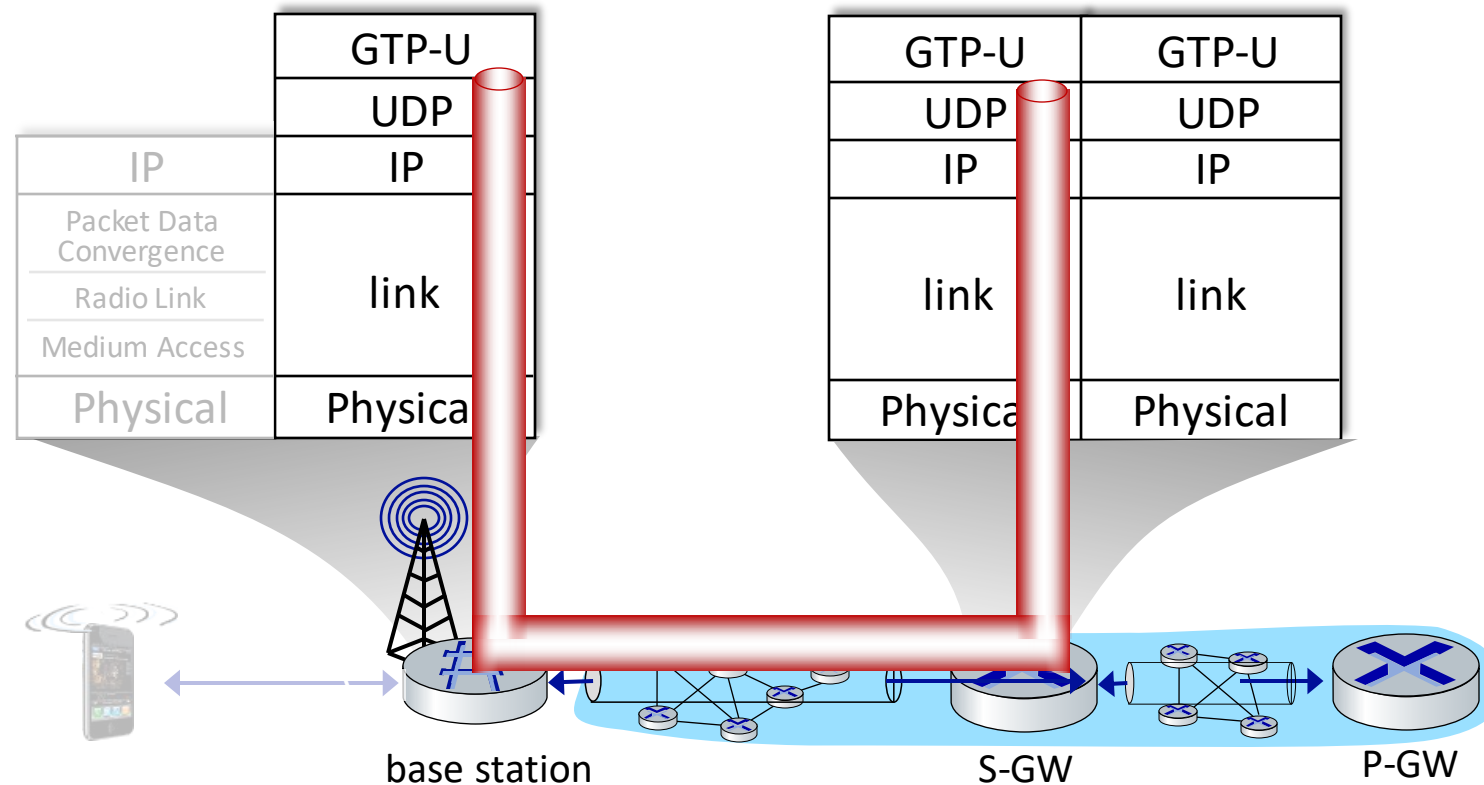 - "orthogonal": minimal interference between channels
  - **upstream:** FDM, TDM similar to OFDM
- each active mobile device allocated two or more 0.5 ms time slots over 12 frequencies
  - scheduling algorithm not standardized – up to operator
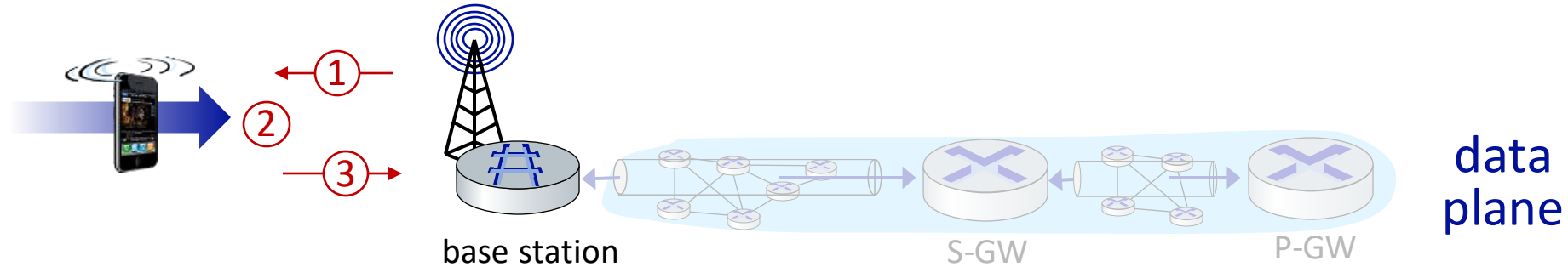 - 100's Mbps per device possible

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

base station   S-GW   P-GW   data plane

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

data plane
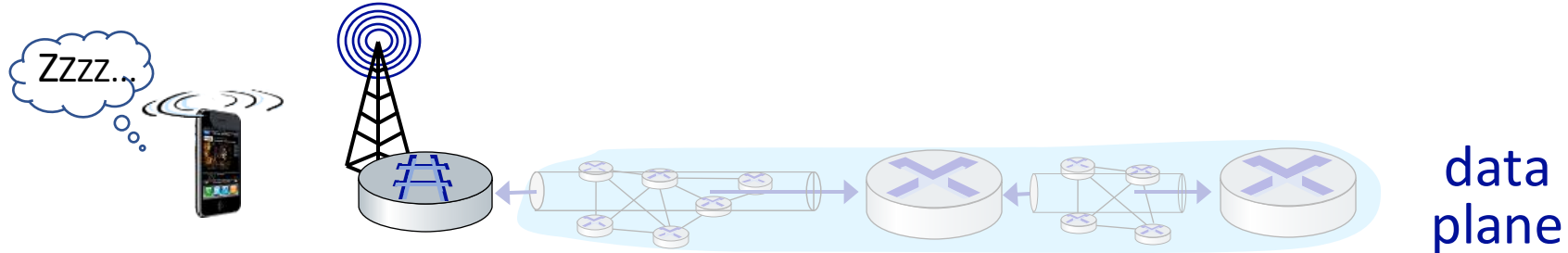
as in WiFi, Bluetooth: LTE mobile may put radio to "sleep" to conserve battery:

- 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
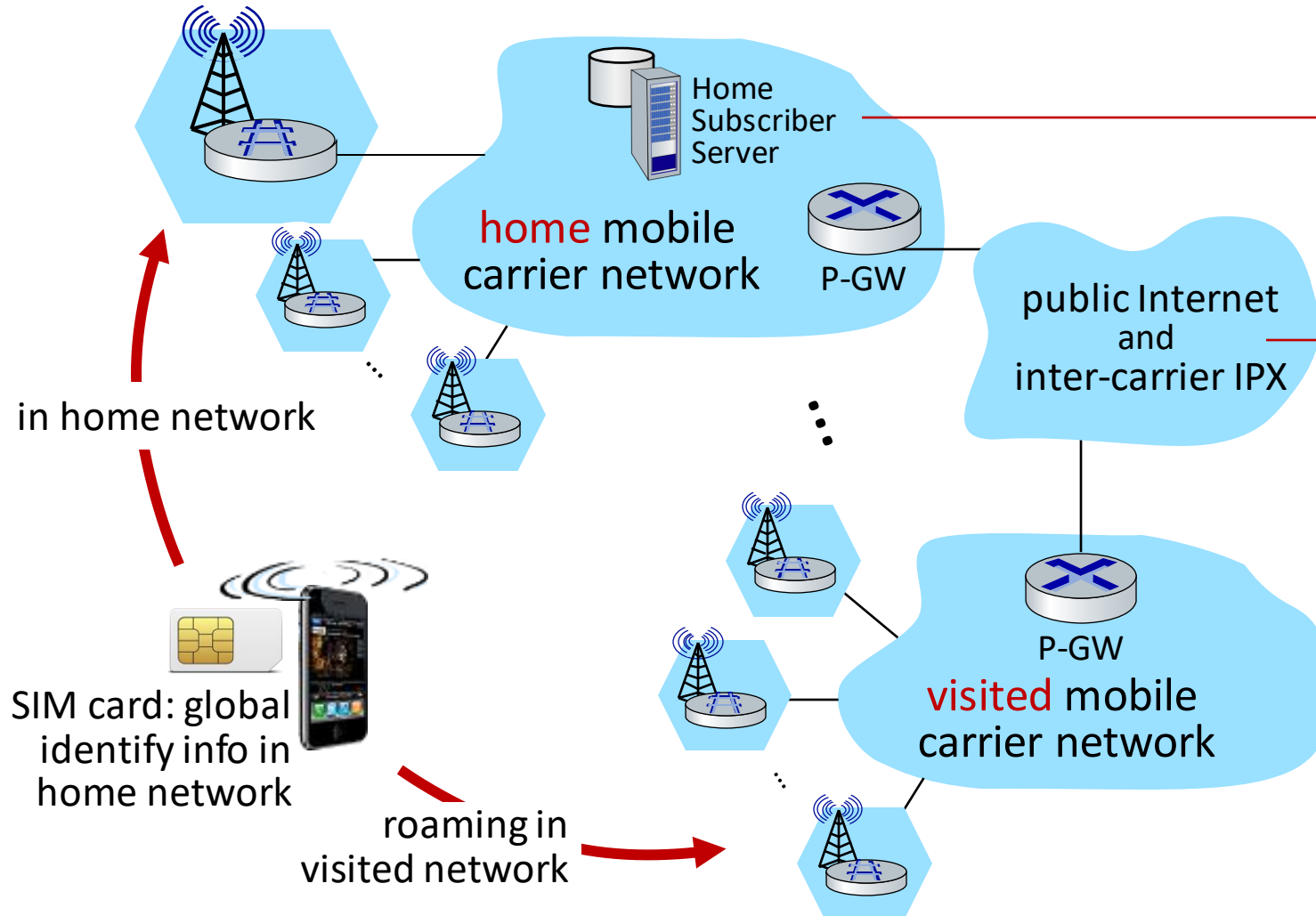
home network HSS:

- 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

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

What is mobility?

- spectrum of mobility, from the network perspective:

no mobility   high mobility

| device moves between networks, but powers down while moving | device moves within same AP in one provider network | device moves among APs in one provider network | device moves among multiple provider networks, while maintaining ongoing connections |

We're interested in these!

Mobility approaches

- **let network (routers) handle it:**
  - routers advertise well-known name, address (e.g., permanent 32-bit IP address), or number (e.g., cell #) of visiting mobile node via usual routing table exchange
  - Internet routing could do this already *with no* changes! Routing tables indicate where each mobile located via longest prefix match!

Mobility approaches

- let network (routers) handle it:
  - routers advertise well-kn~~~~~~ address (e.g., permanent 32-bit IP address), or numb~~~~~~) of visiting mobile node via usual routing table exch~~~~~~

    not scalable to billions of mobiles

  - Internet routing could do t~~~~~~dy *with no* changes! Routing tables indicate where each mobile located via longest prefix match!

- **let end-systems handle it:** functionality at the "edge"
  - *indirect routing:* communication from correspondent to mobile goes through home network, then forwarded to remote mobile
  - *direct routing:* correspondent gets foreign address of mobile, send directly to mobile

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

I wonder where Alice moved to?

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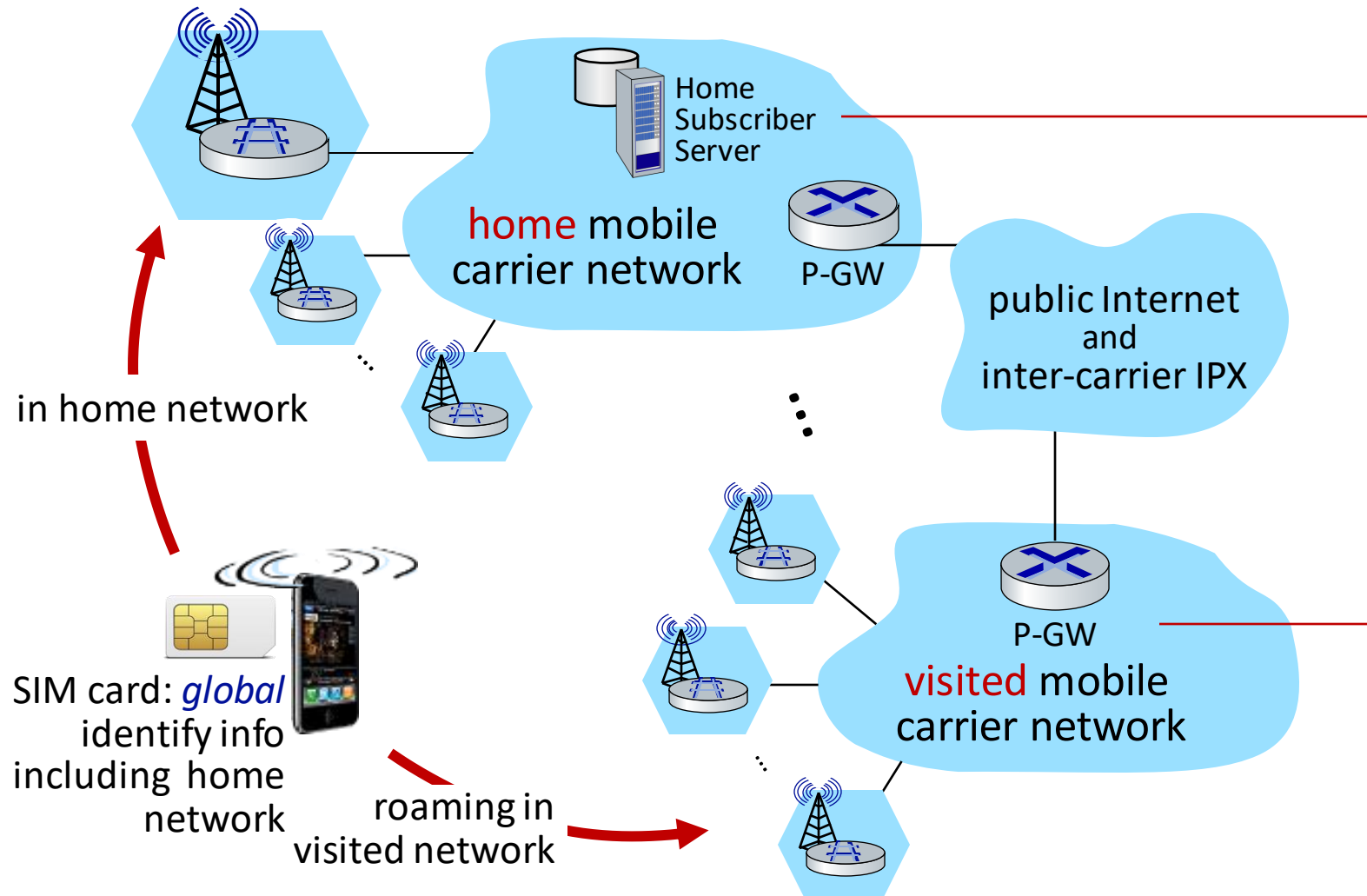
home network:

- (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
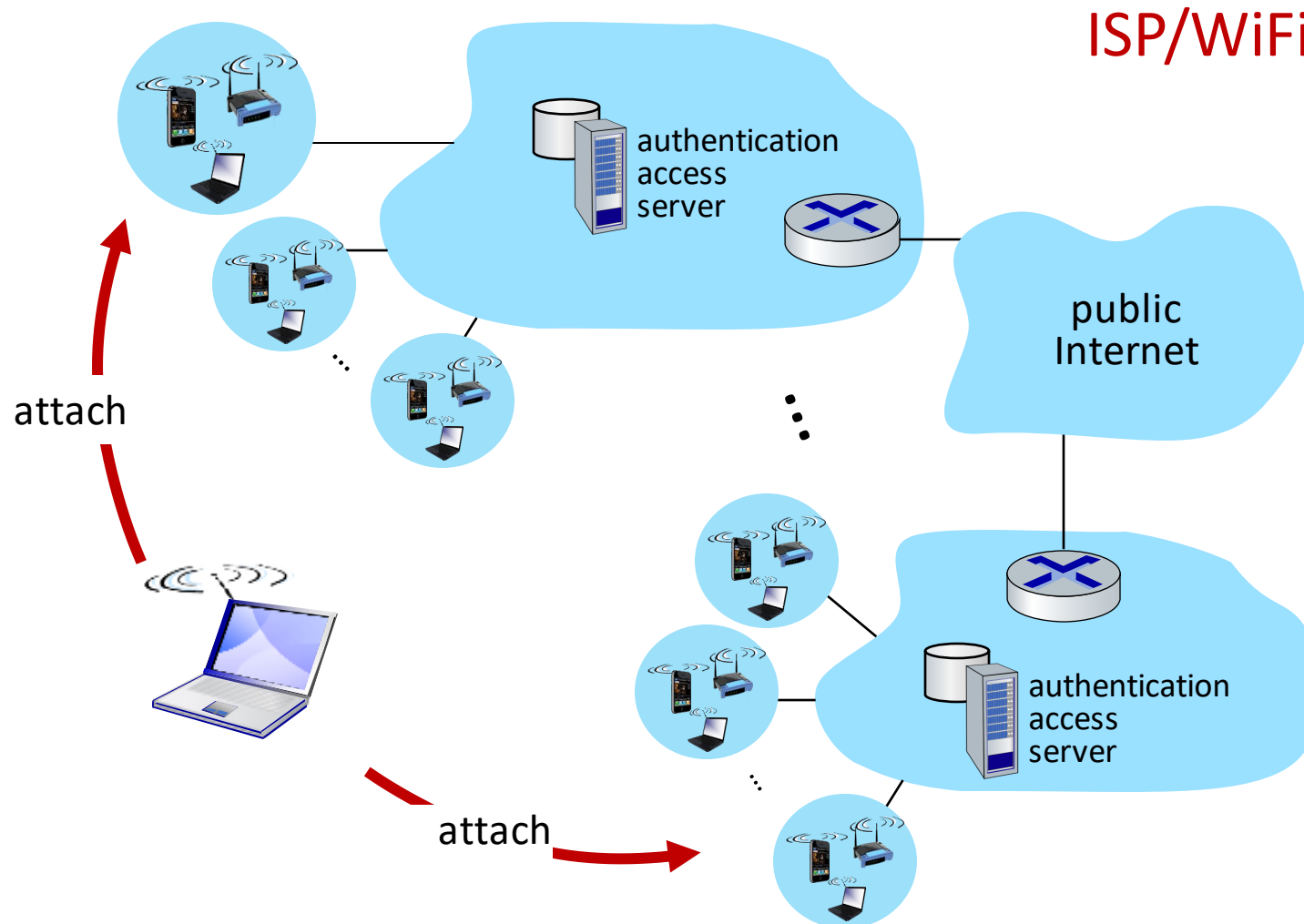
ISP/WiFi: no notion of global "home"

- 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

Permanent IP:
128.119.40.186
IMSI
78:4f:43:98:d9:27

Home Subscriber Server

Mobility manager

Home network gateway

Visited Network
e.g.,: 79.129/16

NAT IP:
10.0.0.99
IMSI
78:4f:43:98:d9:27
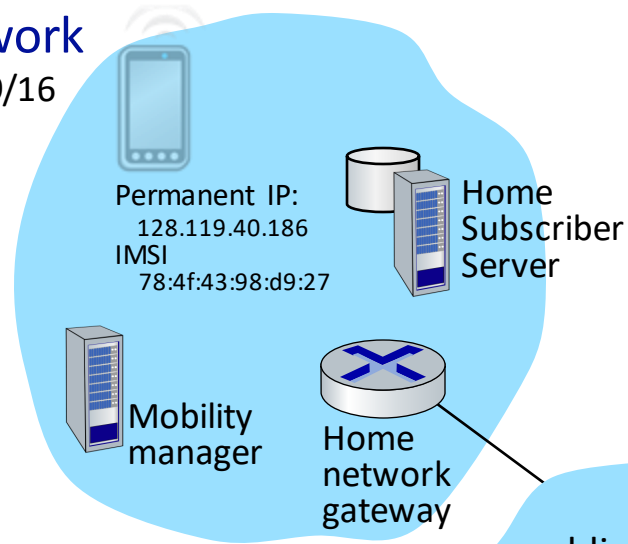
Mobility manager

Visited network gateway
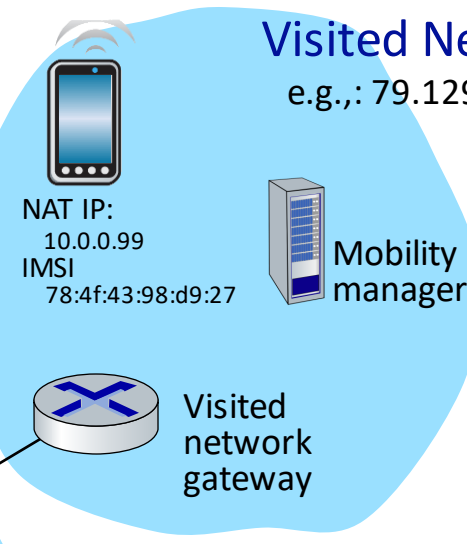
public or private Internet

Correspondent

Registration: home needs to know where you are!

Home Network
e.g.,: 128.119/16

Permanent IP:
128.119.40.186
IMSI
78:4f:43:98:d9:27

Home Subscriber Server

Mobility manager

Home network gateway

public or private Internet

Visited Network
e.g.,: 79.129/16

① mobile *associates* with visited mobility manager

NAT IP: 10.0.0.99
IMSI 78:4f:43:98:d9:27

Mobility manager

② visited mobility manager *registers* mobile's location with home HSS

Visited network gateway

end result:

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

Mobility with indirect routing

Home Network
e.g.,: 128.119/16

Permanent IP:
128.119.40.186
IMSI
78:4f:43:98:d9:27

Home Subscriber Server

Mobility manager

Home network gateway

Visited Network
e.g.,: 79.129/16

NAT IP:
10.0.0.99
IMSI
78:4f:43:98:d9:27

③

Mobility manager

Visited network gateway

②

④a

public or private Internet

①

④b

Correspondent

visited gateway router forwards to mobile

home gateway receives datagram, forwards (tunnels) to remote gateway

correspondent uses *home* address as datagram destination address

visited gateway router forwards reply to correspondent via home network (4a) or directly (4b)

Mobility with indirect routing: comments

- triangle routing:
  - inefficient when correspondent and mobile are in same network

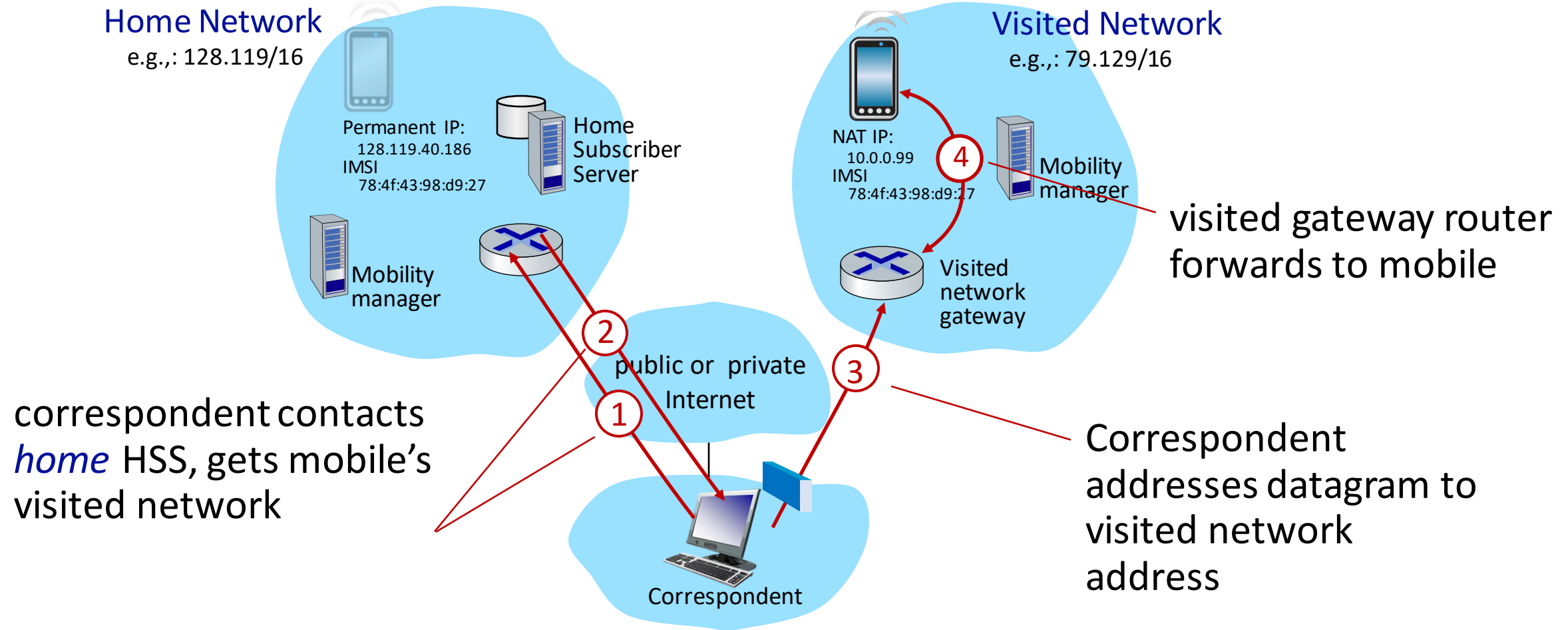- mobile moves among visited networks: transparent to correspondent!
  - registers in new visited network
  - new visited network registers with home HSS
  - datagrams continue to be forwarded from home network to mobile in new network
  - *on-going (e.g., TCP) connections between correspondent and mobile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

Mobility with direct routing

Home Network
e.g.,: 128.119/16

Permanent IP:
128.119.40.186
IMSI
78:4f:43:98:d9:27

Home Subscriber Server

Mobility manager

Visited Network
e.g.,: 79.129/16

NAT IP:
10.0.0.99
IMSI
78:4f:43:98:d9:27

④

Mobility manager

visited gateway router forwards to mobile

Visited network gateway

public or private Internet

②

③

①

correspondent contacts *home* HSS, gets mobile's visited network

Correspondent addresses datagram to visited network address

Correspondent

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
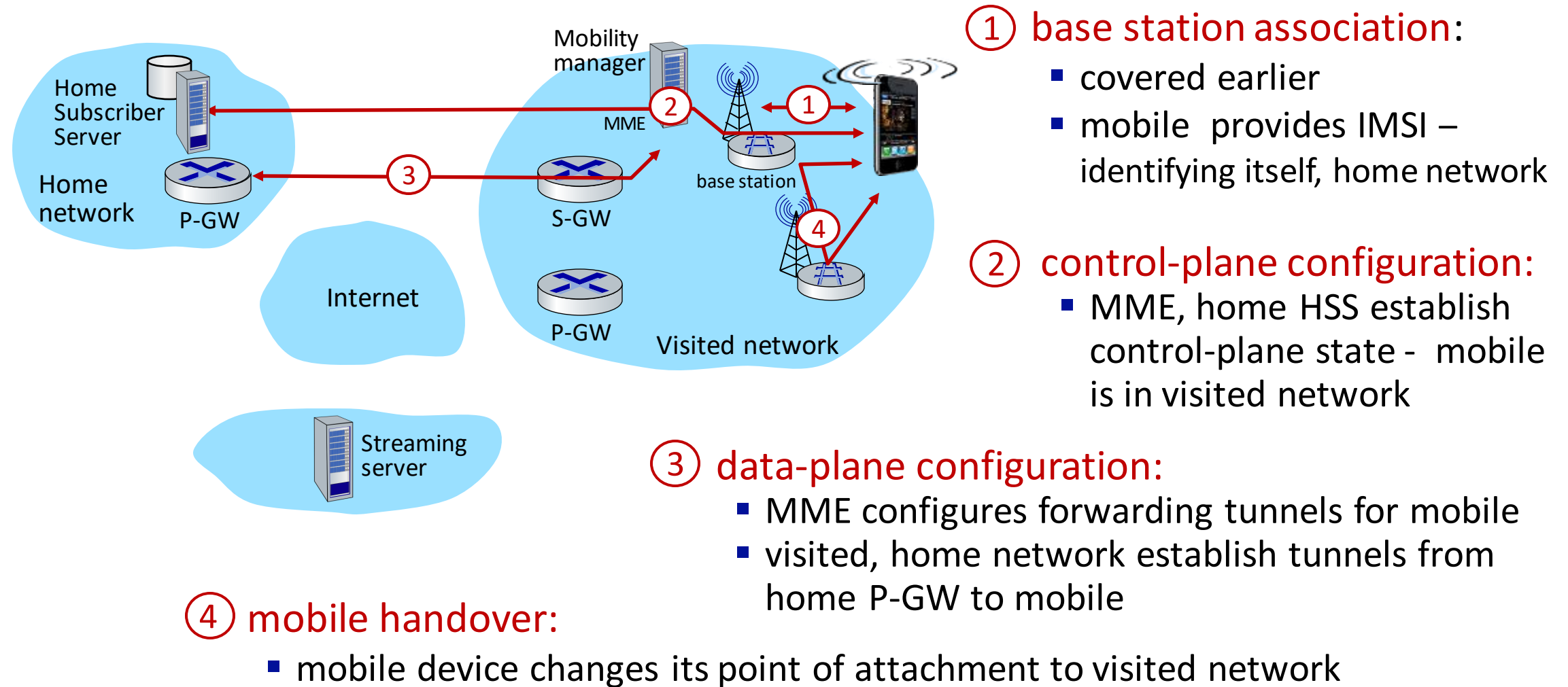
Outline

- Introduction

Wireless

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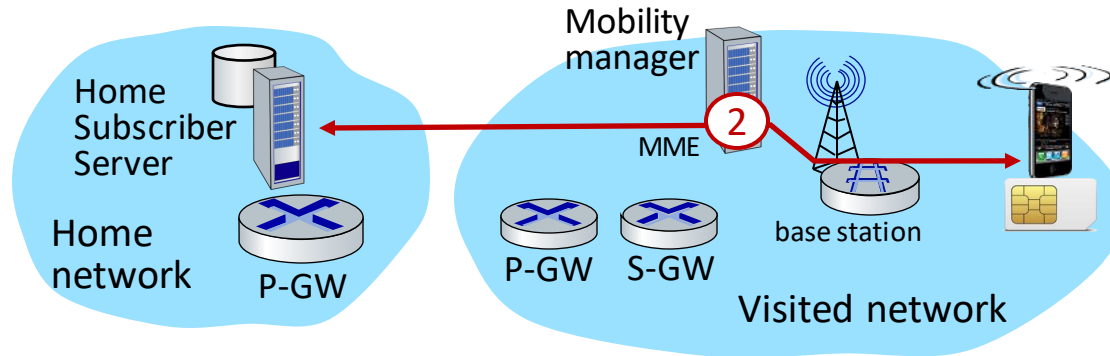- Cellular networks: 4G and 5G

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

Home Subscriber Server

Home network

P-GW

Internet

Streaming server

Mobility manager

MME

S-GW

P-GW

base station

Visited network

① **base station association:**
  - covered earlier
  - mobile provides IMSI – identifying itself, home network

② **control-plane configuration:**
  - MME, home HSS establish control-plane state - mobile is in visited network

③ **data-plane configuration:**
  - MME configures forwarding tunnels for mobile
  - visited, home network establish tunnels from home P-GW to mobile

④ **mobile handover:**
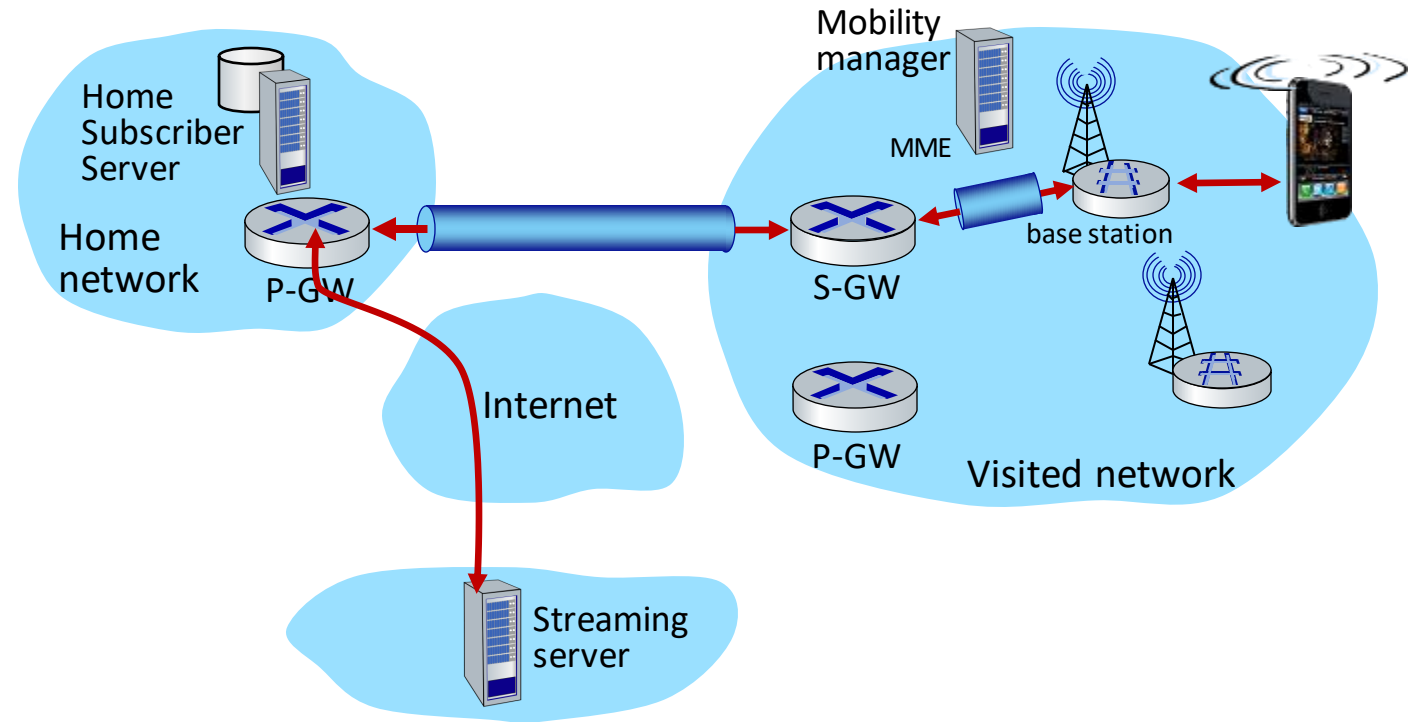 - mobile device changes its point of attachment to visited network

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 HHS 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

data path *before* handover

data path *after* handover

source BS

S-GW

P-GW

MME
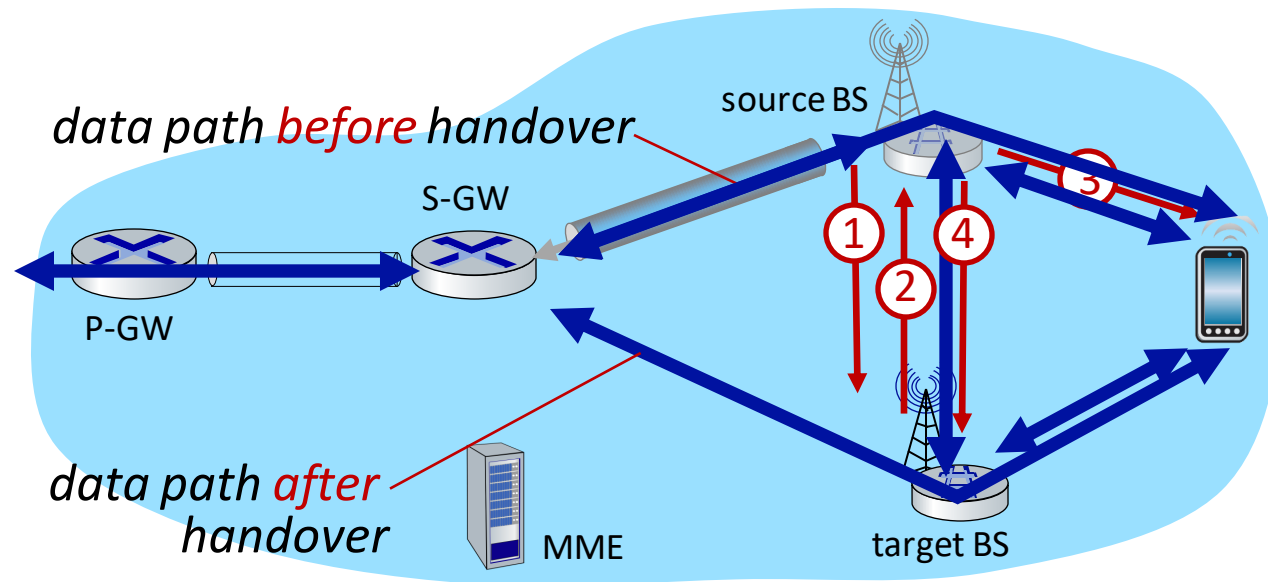
target BS

① current (source) BS selects target BS, sends *Handover Request message* to target BS
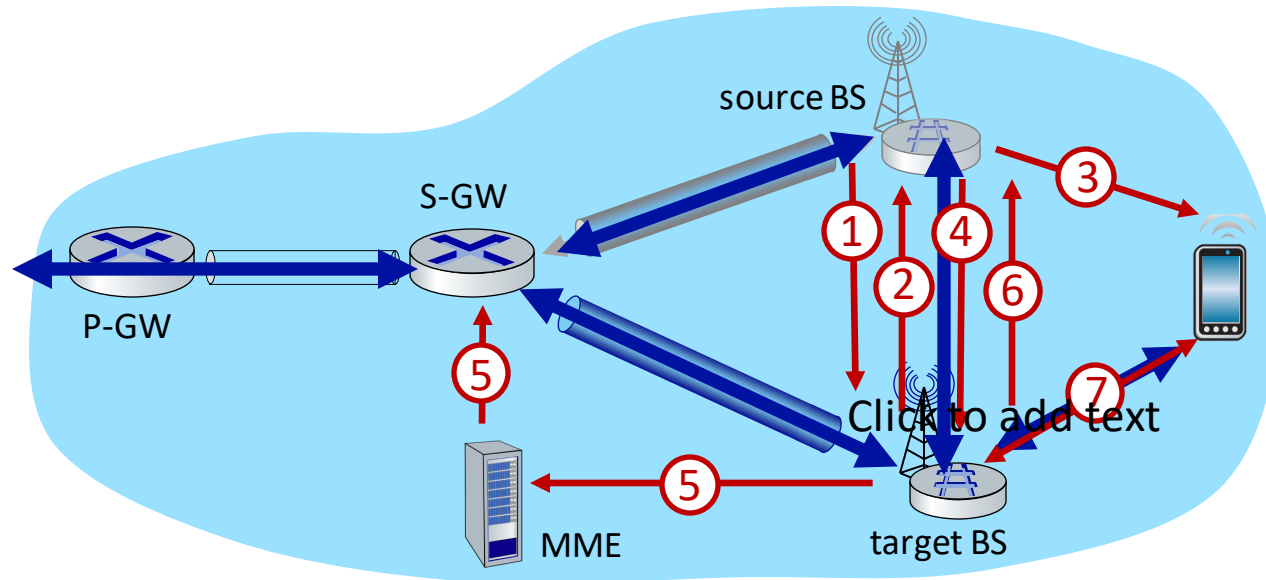
② target BS pre-allocates radio time slots, responds with HR ACK with info for mobile

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

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 un-necessarily
  - delay impairments for real-time traffic
  - bandwidth a scare resource for wireless links