


# Chapter 7

## Wireless and Mobile Networks



# Ch. 6: Wireless and Mobile Networks

## Background:

- # wireless (mobile) phone subscribers now exceeds # wired phone subscribers (5-to-1)!
- # wireless Internet-connected devices equals # wireline Internet-connected devices
  - laptops, Internet-enabled phones promise anytime untethered Internet access
- 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

## 7.1 Introduction

### Wireless

#### 7.2 Wireless links, characteristics

- CDMA

#### 6.73 IEEE 802.11 wireless LANs (“Wi-Fi”)

#### 67.4 Cellular Internet Access

- architecture
- standards (e.g., 3G, LTE)

### Mobility

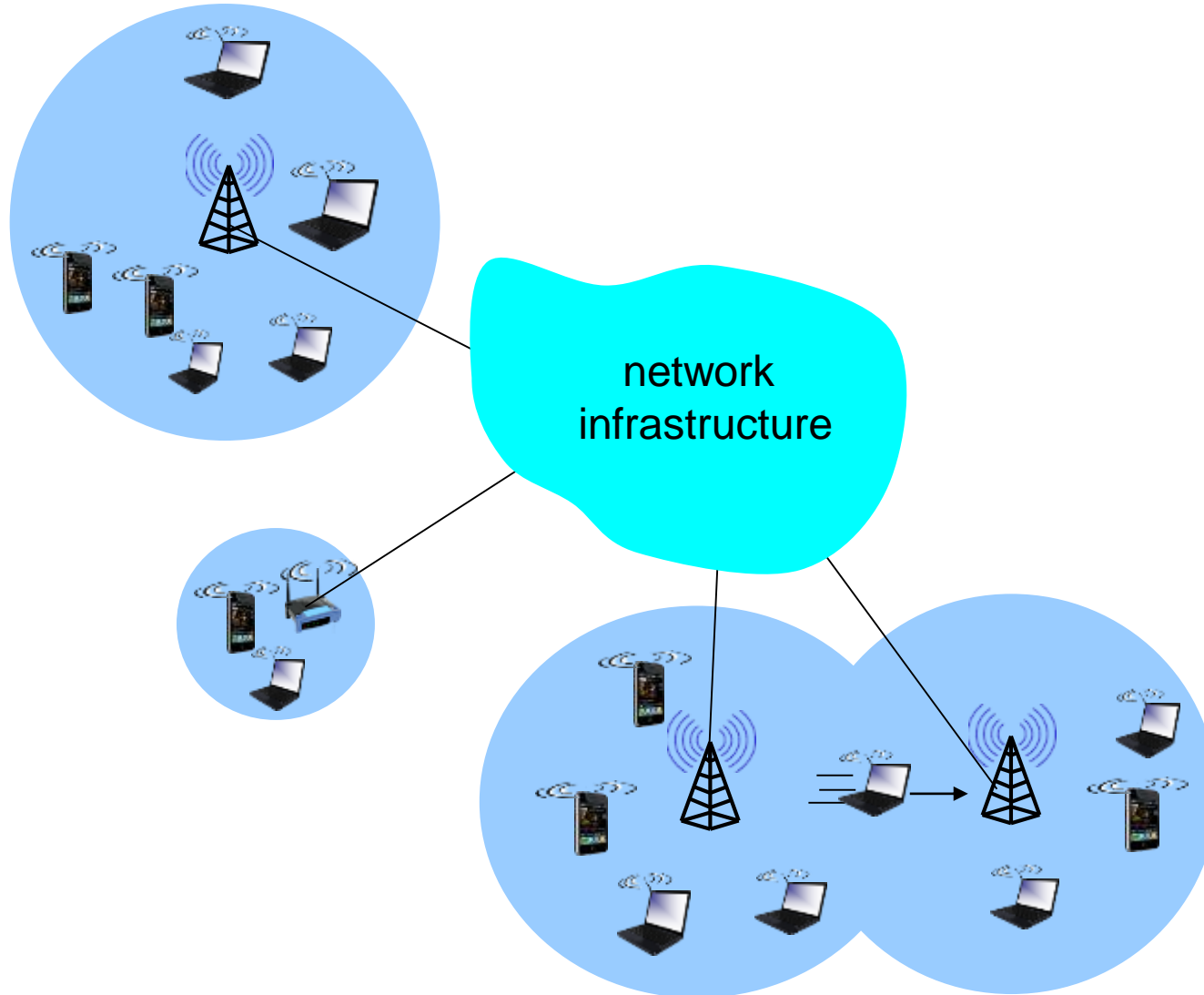
#### 7.5 Principles: addressing and routing to mobile users

#### 7.6 Mobile IP

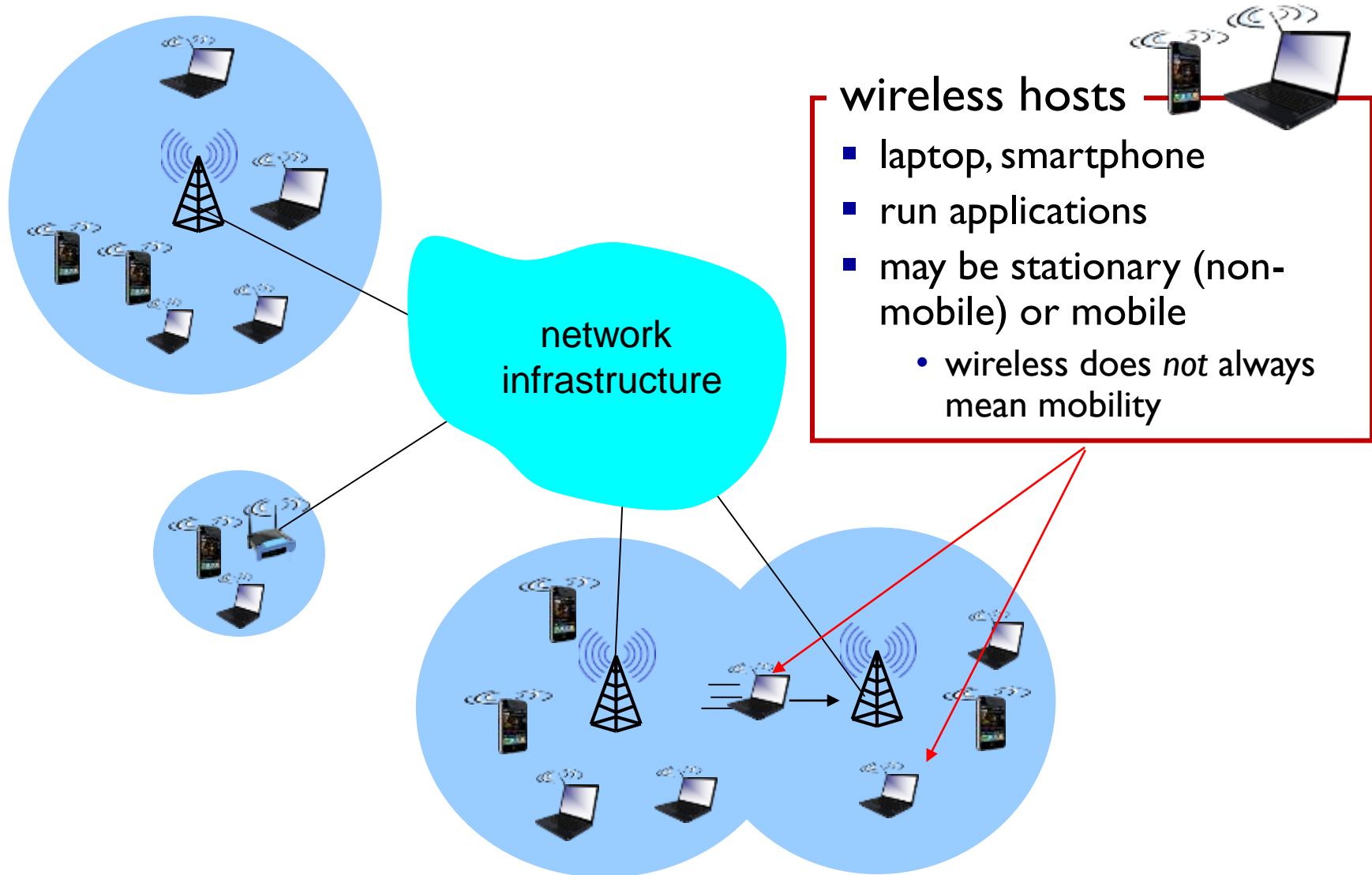
#### 7.7 Handling mobility in cellular networks

#### 7.8 Mobility and higher-layer protocols

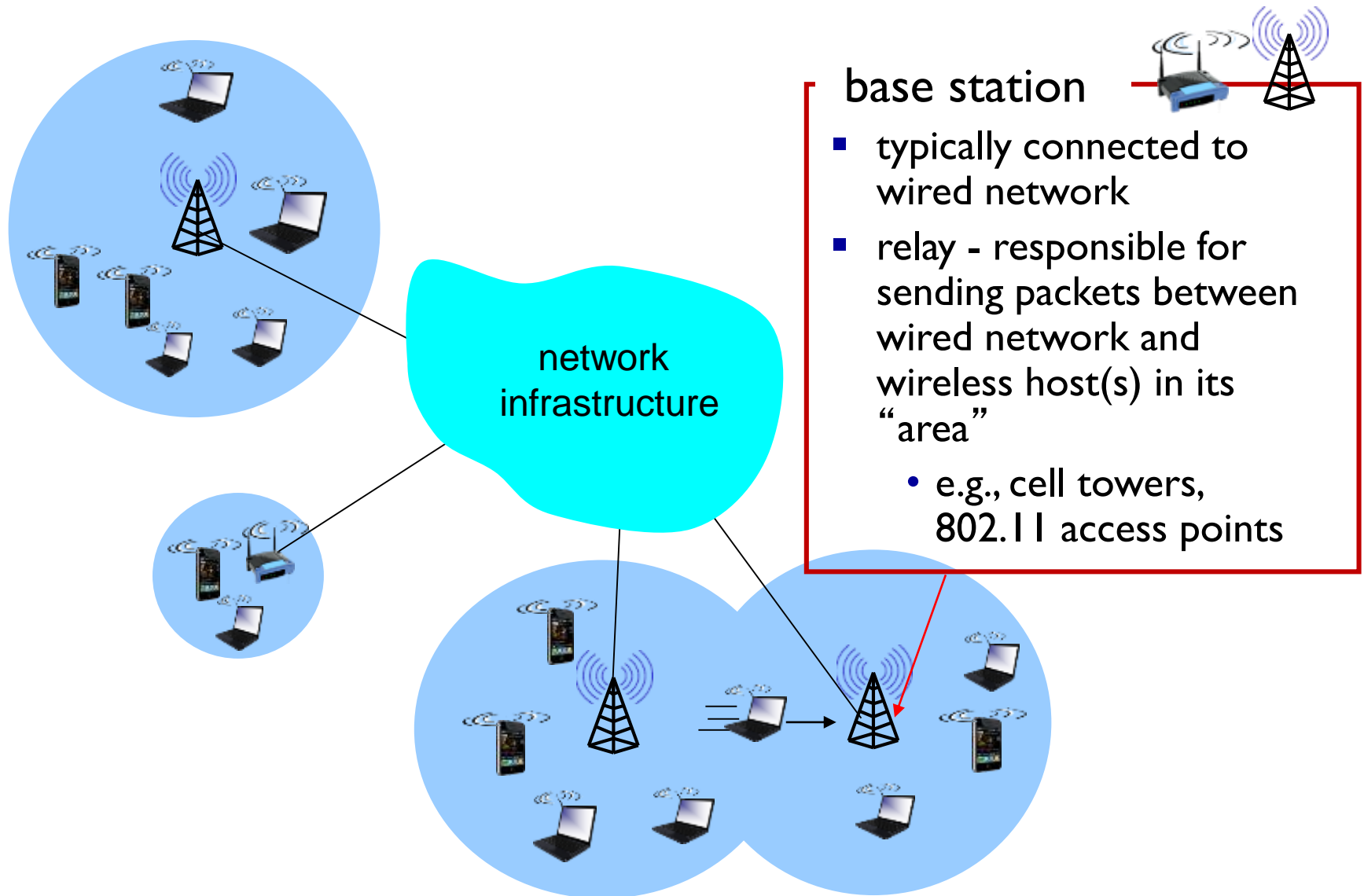
# Elements of a wireless network



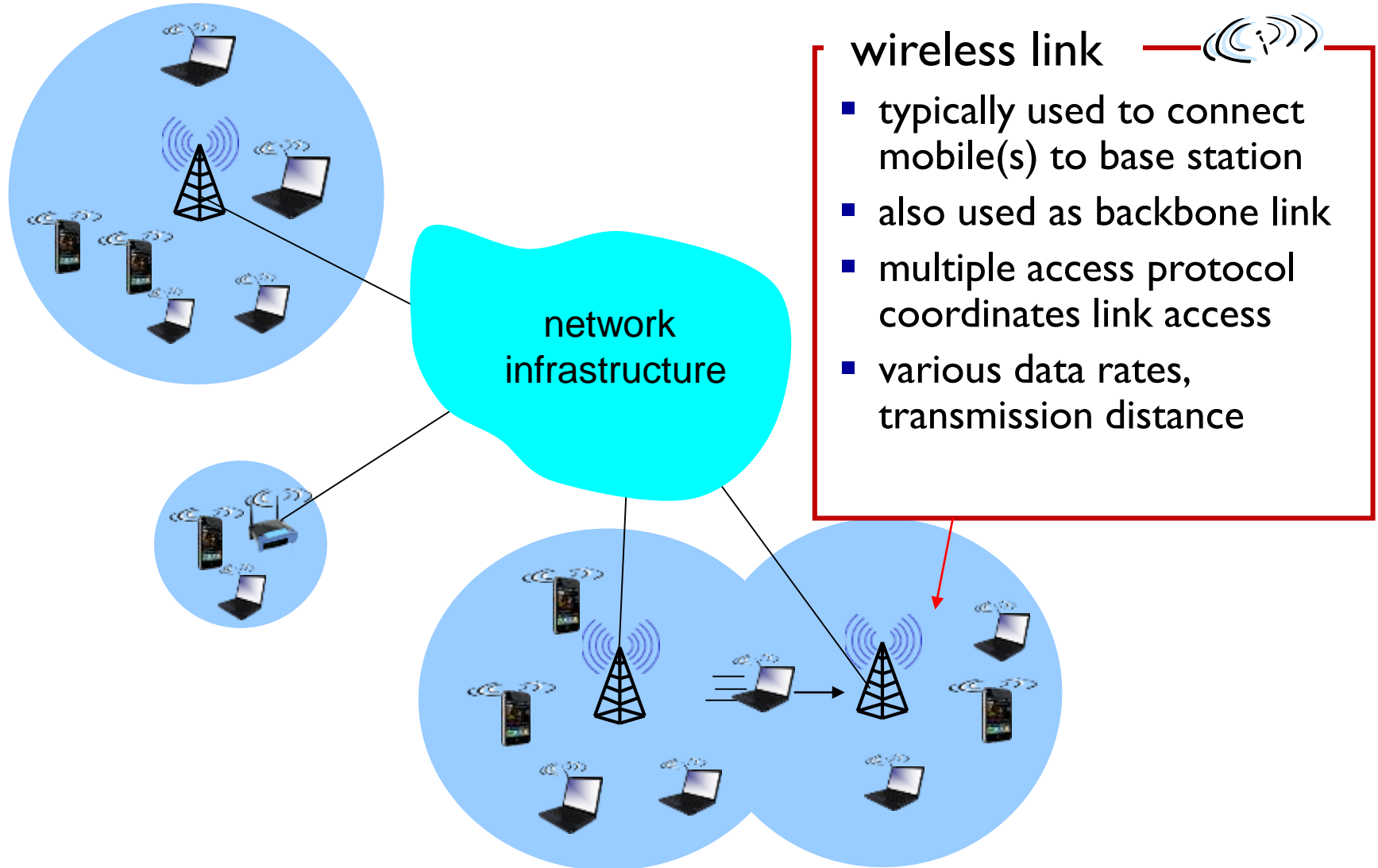
# Elements of a wireless network



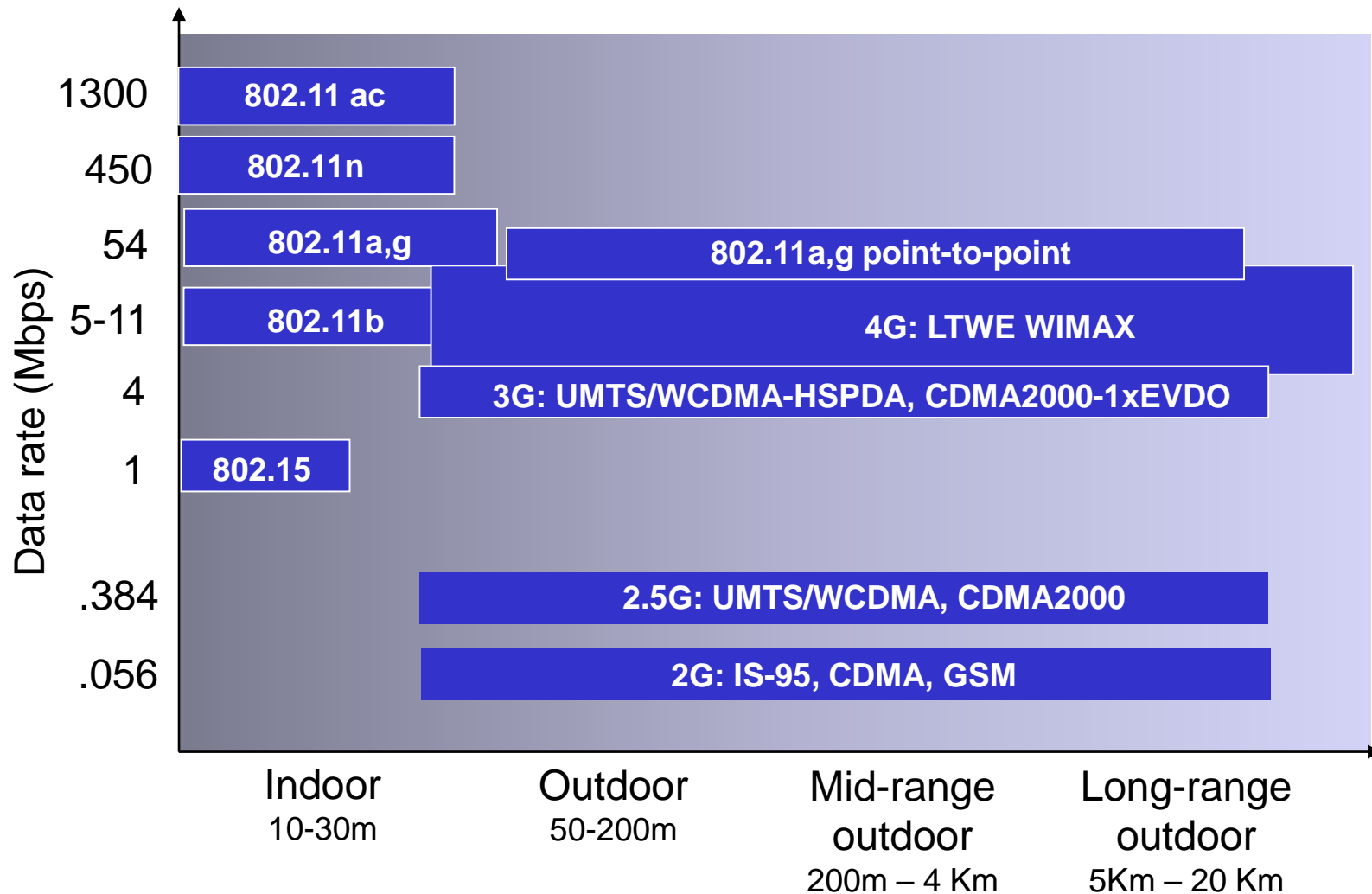
# Elements of a wireless network



# Elements of a wireless network

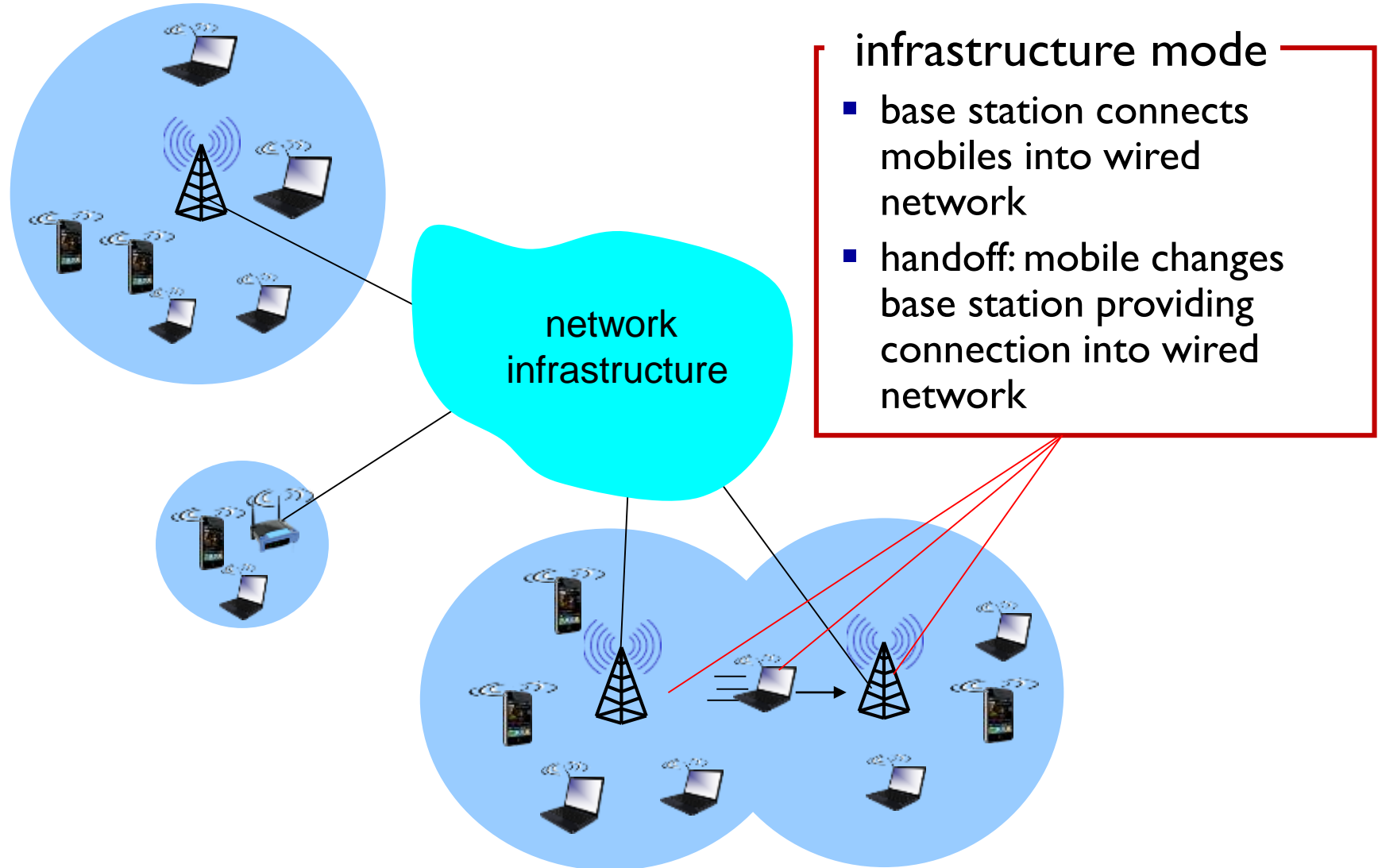


# Characteristics of selected wireless links

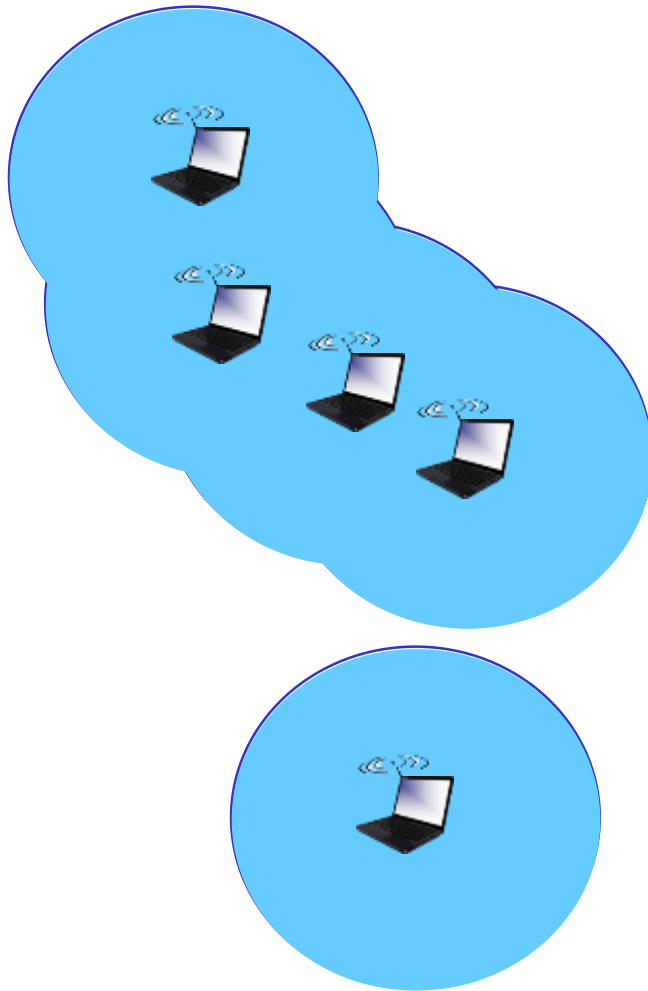




# Elements of a wireless network



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

# Chapter 7 outline

## 7.1 Introduction

## Wireless

### 7.2 Wireless links, characteristics

- CDMA

### 7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

### 7.4 Cellular Internet Access

- architecture
- standards (e.g., 3G, LTE)

## Mobility

### 7.5 Principles: addressing and routing to mobile users

### 7.6 Mobile IP

### 7.7 Handling mobility in cellular networks

### 7.8 Mobility and higher-layer protocols

# Wireless Link Characteristics (I)

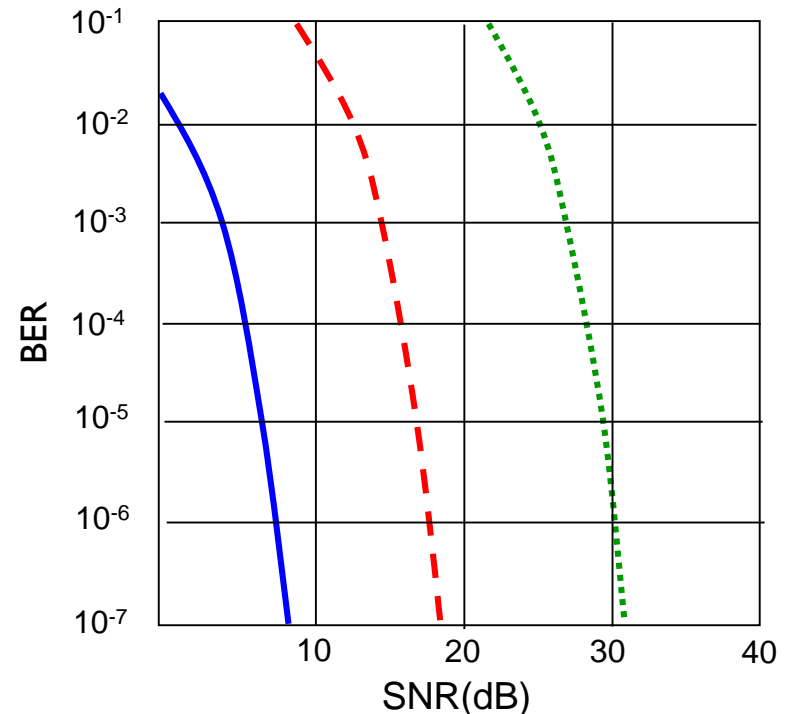
*important* differences from wired link ....

- *decreased signal strength*: radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources*: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- *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  $\rightarrow$  increase SNR  $\rightarrow$  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)



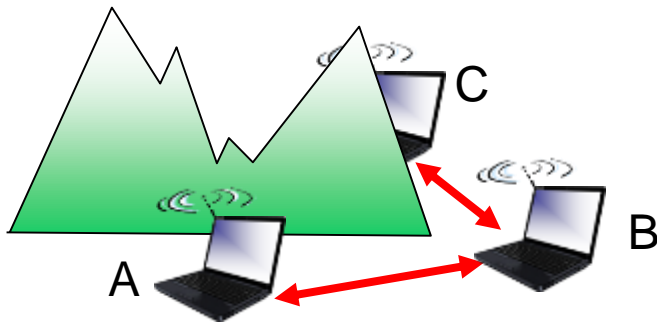
..... QAM256 (8 Mbps)

- - - QAM16 (4 Mbps)

— BPSK (1 Mbps)

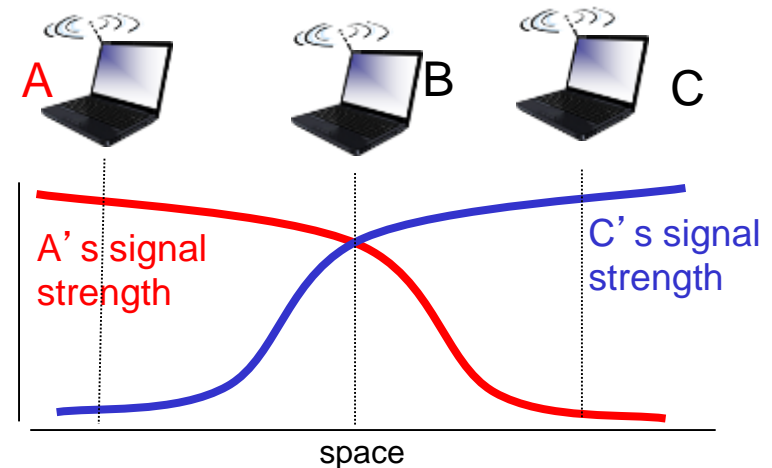
# Wireless network characteristics

Multiple wireless senders and 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:*

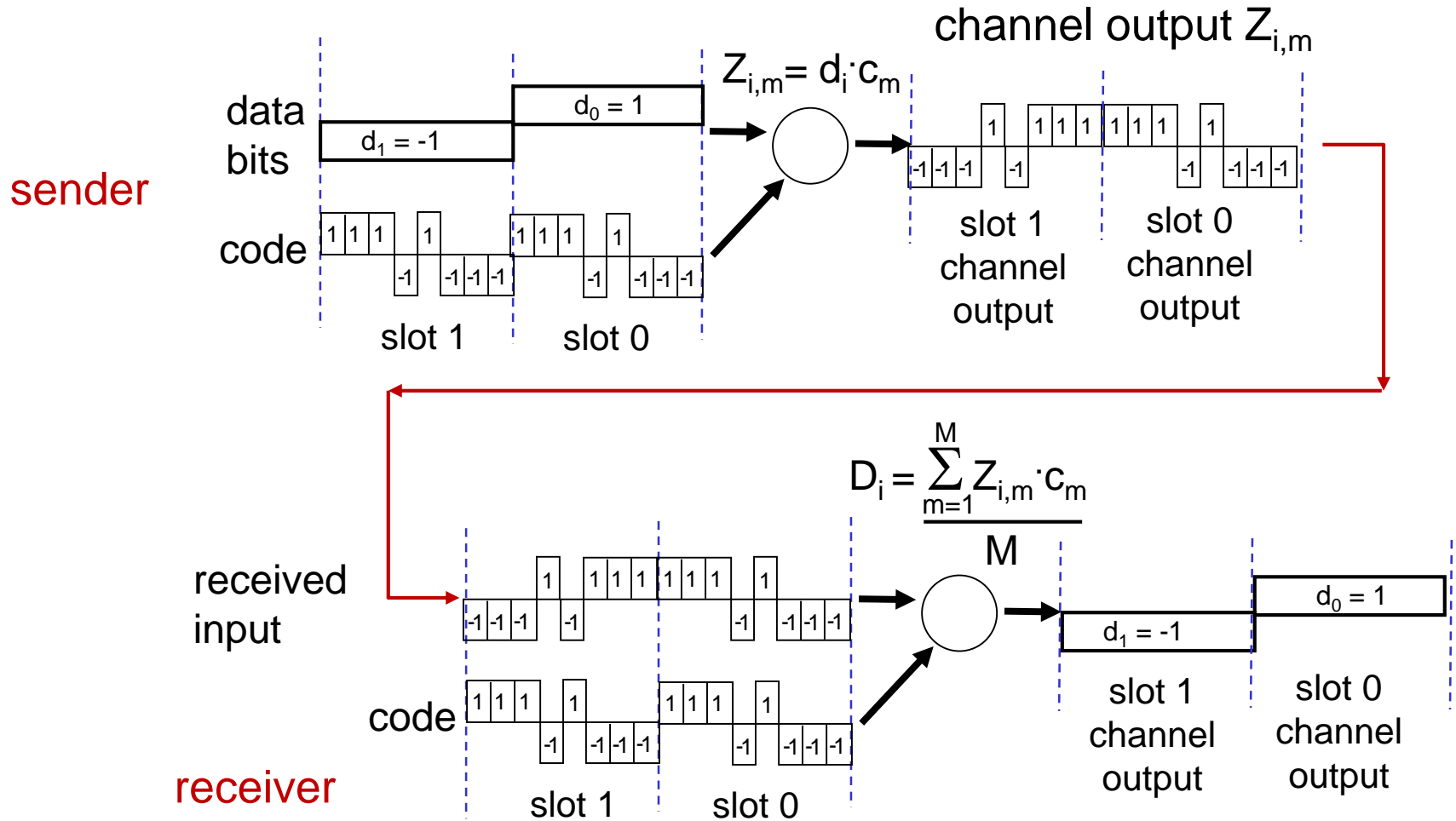
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

# Code Division Multiple Access (CDMA)

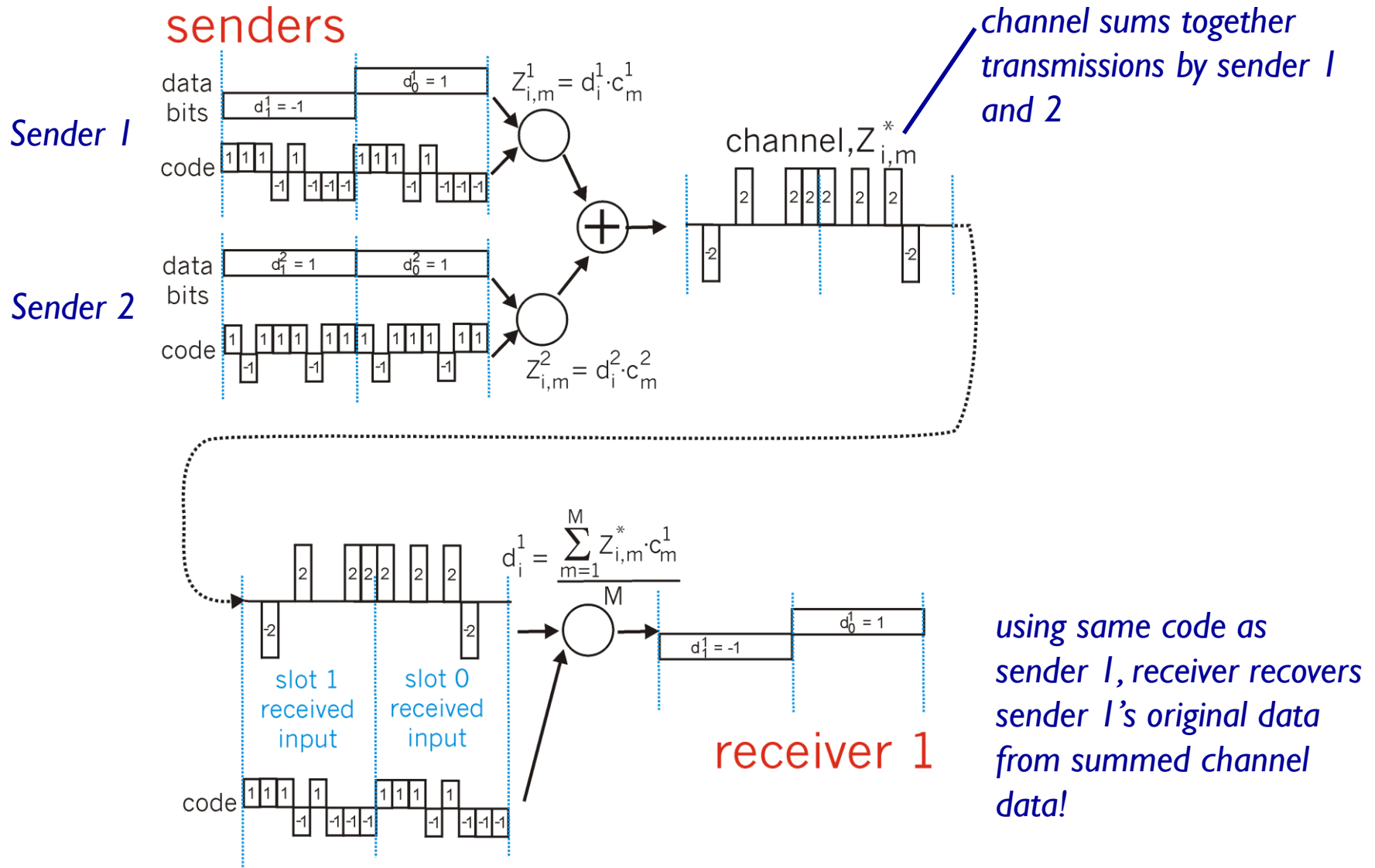
- unique “code” assigned to each user; i.e., code set partitioning
  - all users share same frequency, but each user has own “chipping” sequence (i.e., code) to encode data
  - allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)
- *encoded signal* = (original data)  $\times$  (chipping sequence)
- *decoding*: inner-product of encoded signal and chipping sequence



# CDMA encode/decode



# CDMA: two-sender interference



# Chapter 7 outline

## 7.1 Introduction

## Wireless

### 7.2 Wireless links, characteristics

- CDMA

### 7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

### 7.4 Cellular Internet Access

- architecture
- standards (e.g., 3G, LTE)

## Mobility

### 7.5 Principles: addressing and routing to mobile users

### 7.6 Mobile IP

### 7.7 Handling mobility in cellular networks

### 7.8 Mobility and higher-layer protocols

# IEEE 802.11 Wireless LAN

## 802.11b

- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer
  - all hosts use same chipping code

## 802.11a

- 5-6 GHz range
- up to 54 Mbps

## 802.11g

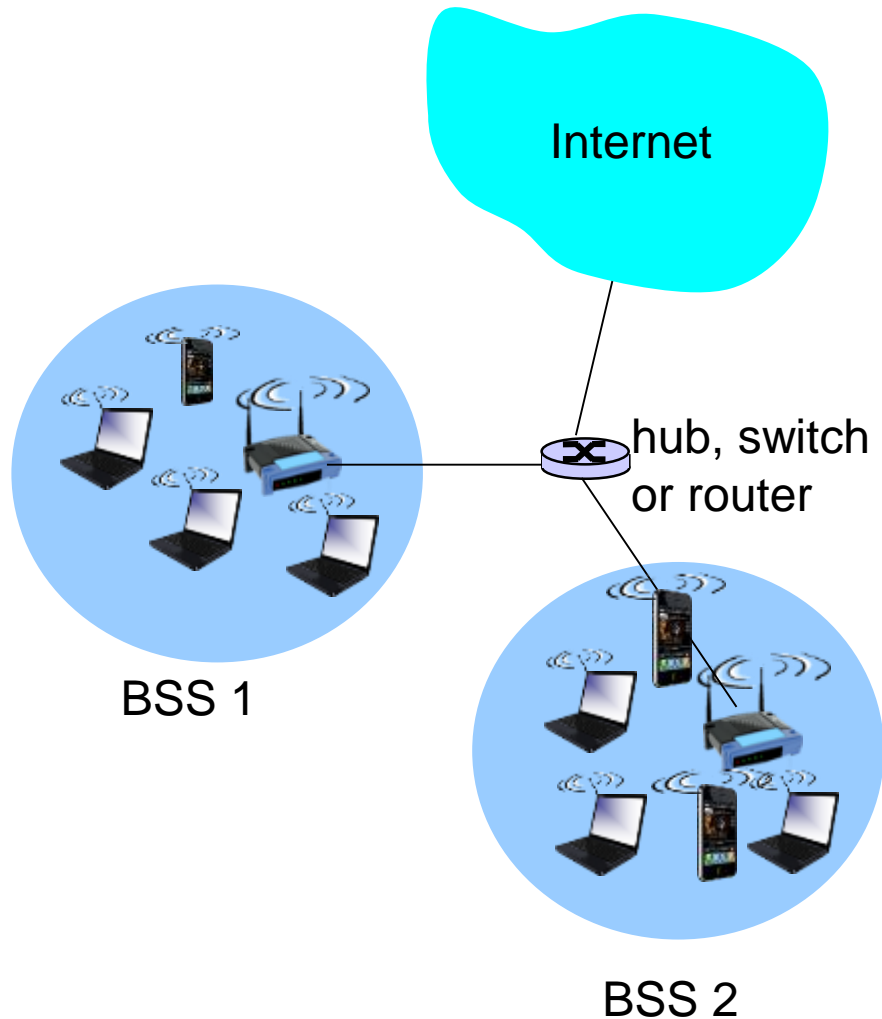
- 2.4-5 GHz range
- up to 54 Mbps

## 802.11n: multiple antennae

- 2.4-5 GHz range
- up to 200 Mbps

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

# 802.11 LAN architecture

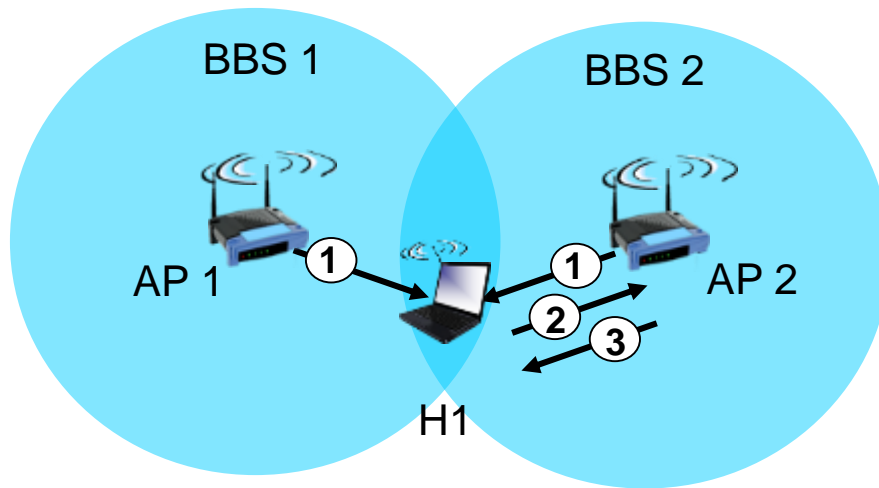


- wireless host communicates with base station
  - **base station = access point (AP)**
- **Basic Service Set (BSS)** (aka “cell”) in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

# 802.11: Channels, association

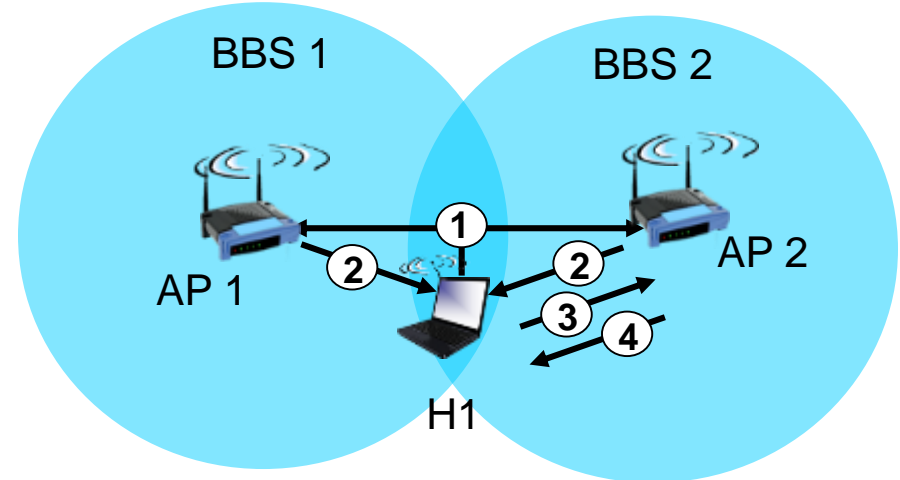
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication [Chapter 8]
  - will 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

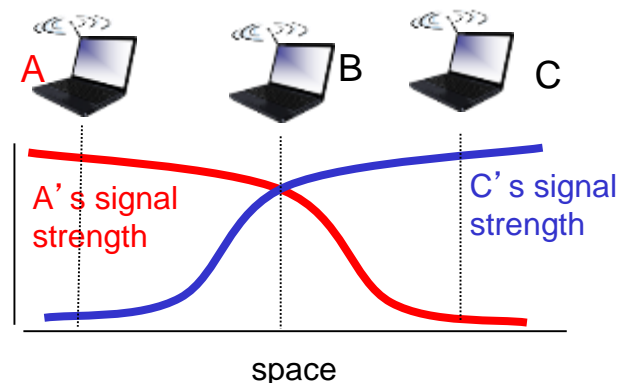
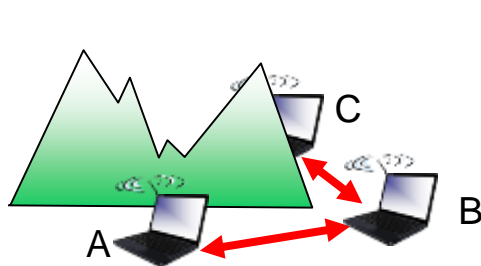


## active scanning:

- (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<sup>+</sup> nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions*: CSMA/C(ollision)A(voidance)





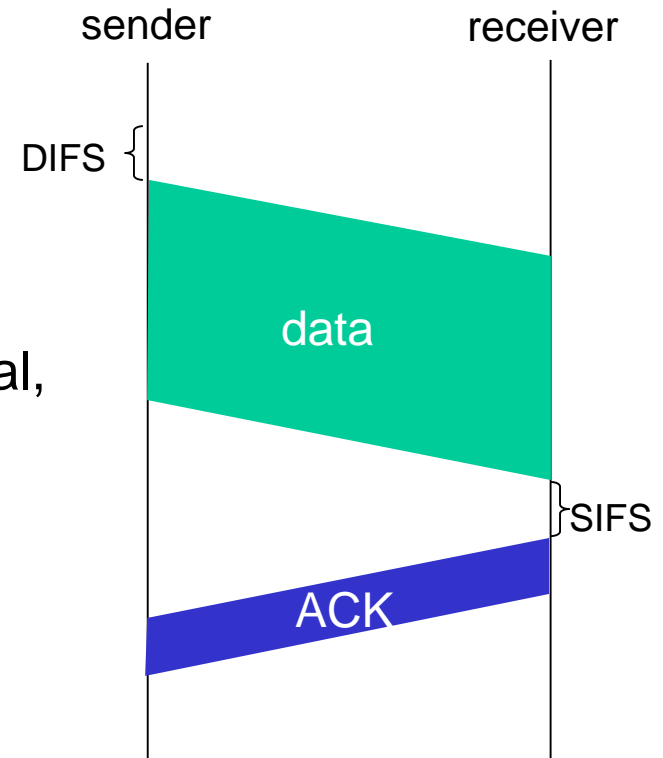
# IEEE 802.11 MAC Protocol: CSMA/CA

## 802.11 sender

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

## 802.11 receiver

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



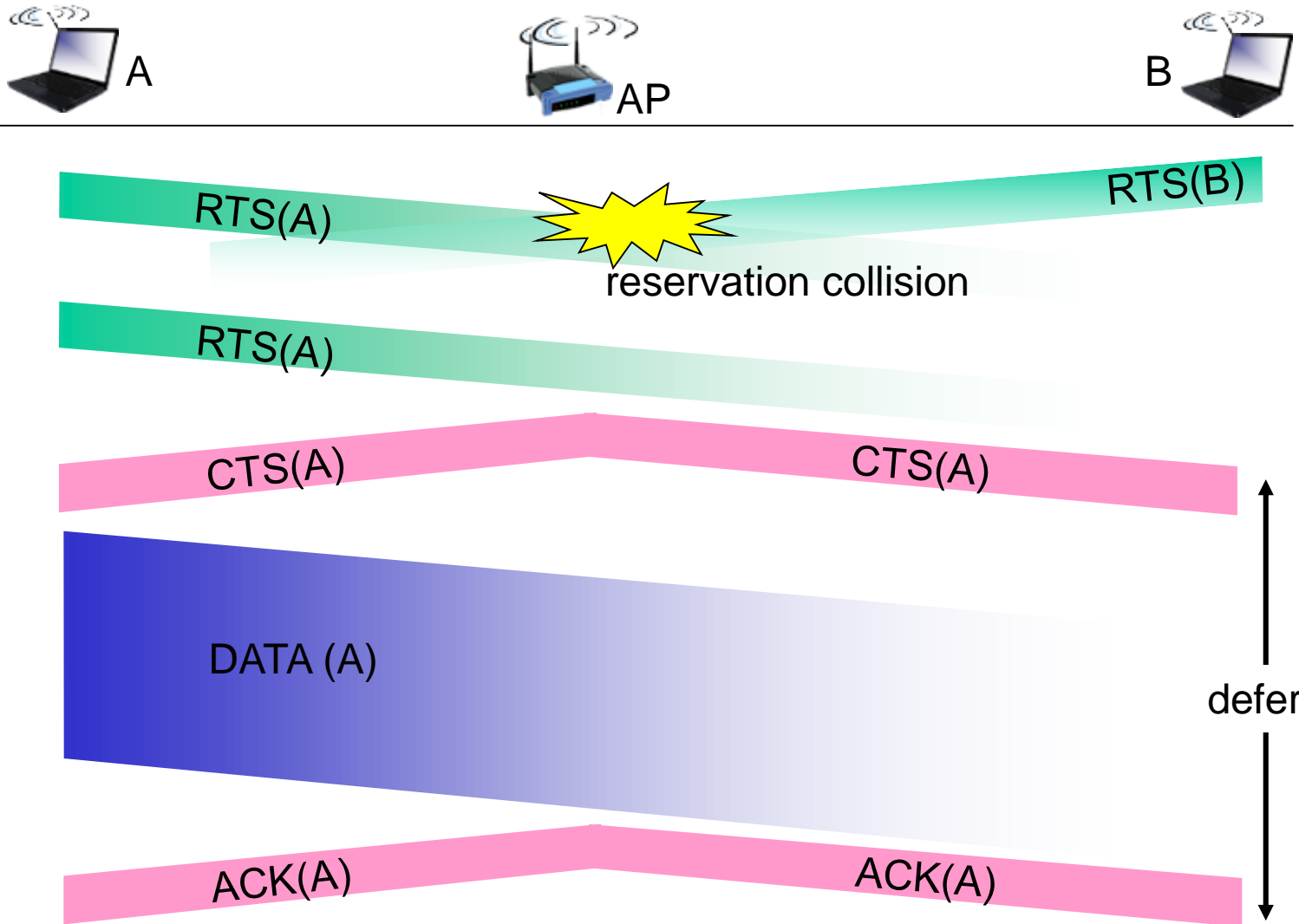
# Avoiding collisions (more)

*idea:* allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

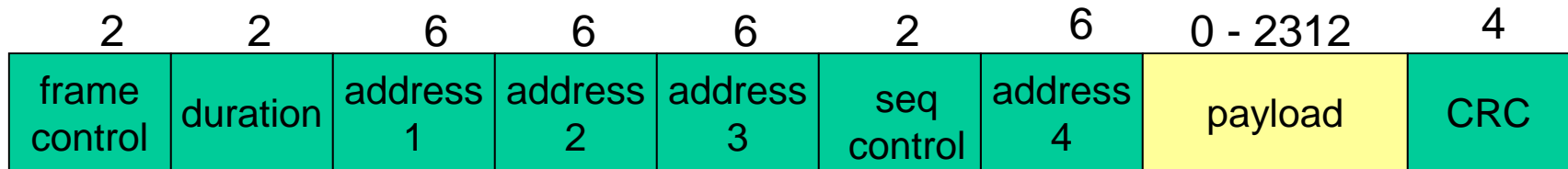
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

*avoid data frame collisions completely  
using small reservation packets!*

# Collision Avoidance: RTS-CTS exchange



# 802.11 frame: addressing



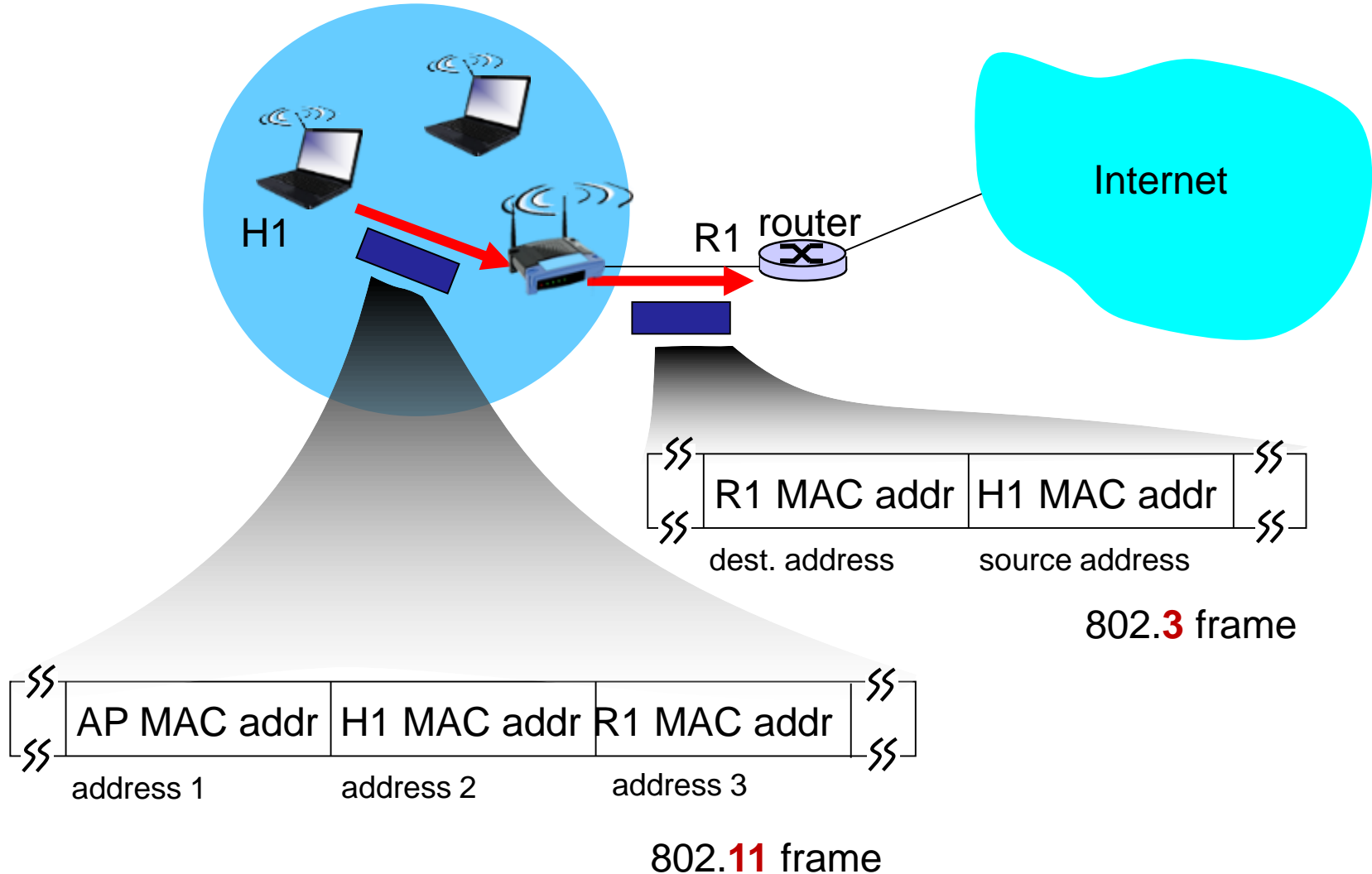
**Address 1:** MAC address of wireless host or AP to receive this frame

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

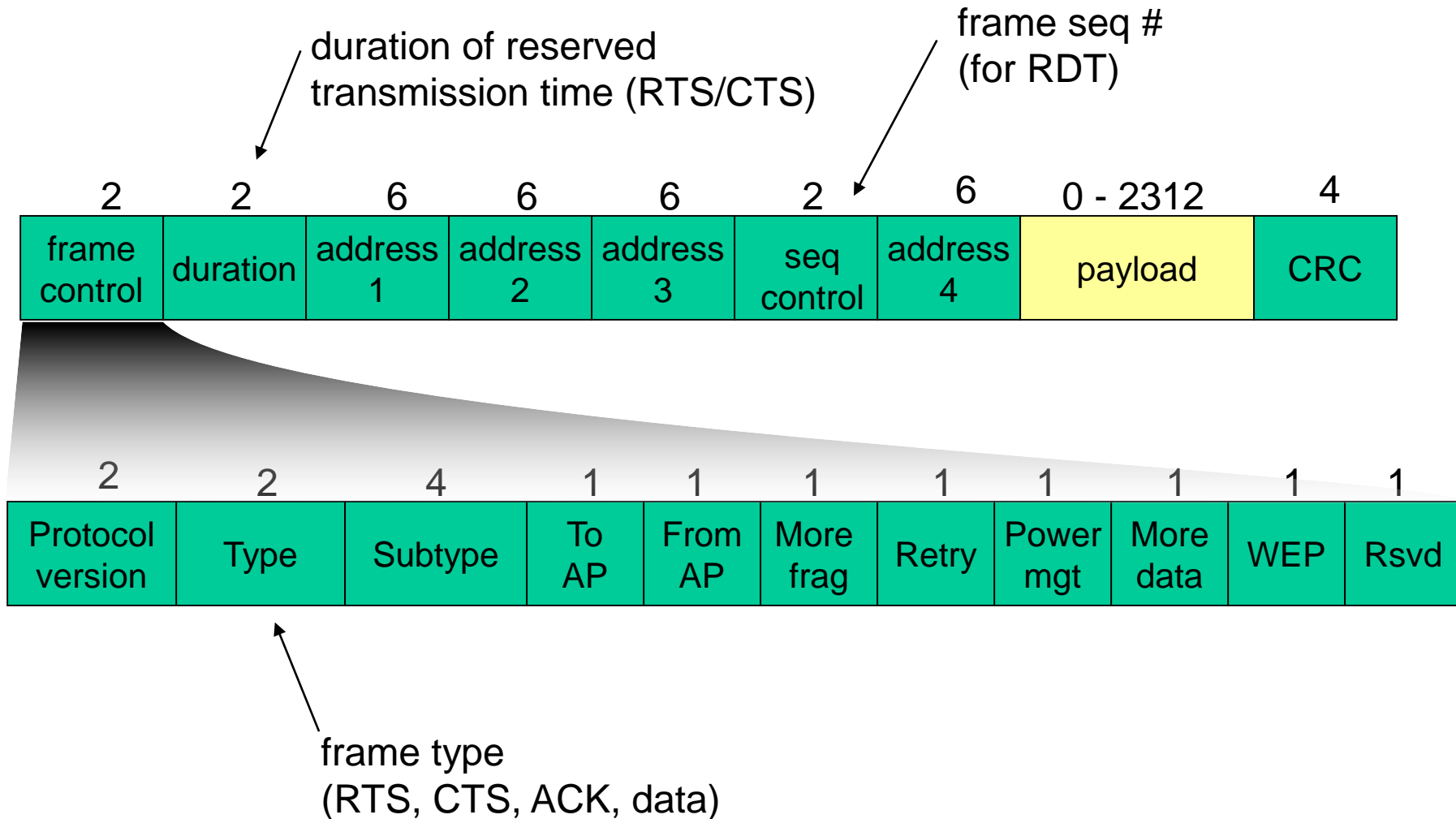
**Address 3:** MAC address of router interface to which AP is attached

**Address 4:** used only in ad hoc mode

# 802.11 frame: addressing

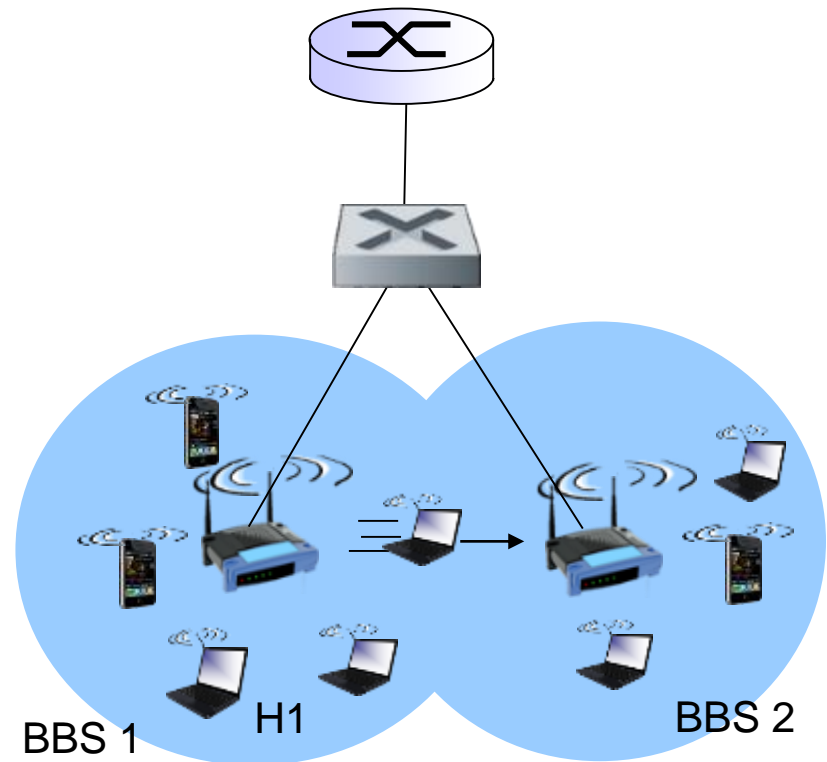


# 802.11 frame: more



# 802.11: mobility within same subnet

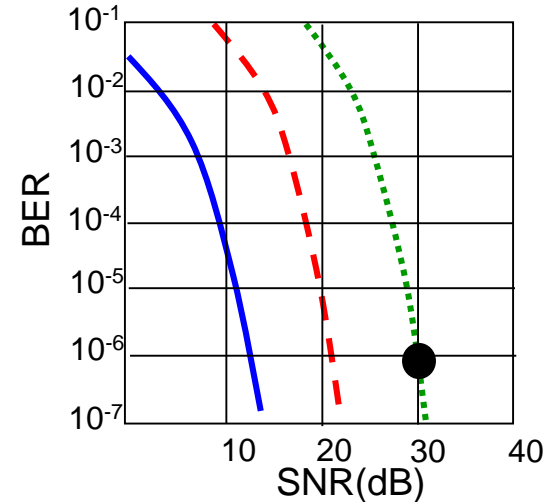
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and “remember” which switch port can be used to reach H1



# 802.11: advanced capabilities

## *Rate adaptation*

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



- ..... QAM256 (8 Mbps)
- - - QAM16 (4 Mbps)
- BPSK (1 Mbps)
- operating point

1. SNR decreases, BER increase as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but with lower BER



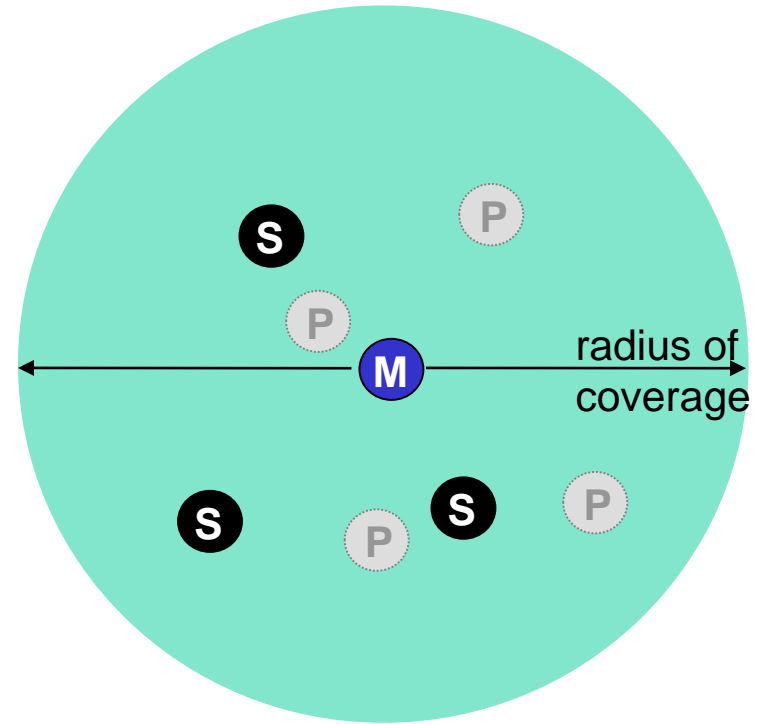
# 802.11: advanced capabilities

## *power management*

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

# 802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps



- M** Master device
- S** Slave device
- P** Parked device (inactive)

# Chapter 7 outline

## 7.1 Introduction

## Wireless

### 7.2 Wireless links, characteristics

- CDMA

### 7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

### 7.4 Cellular Internet access

- architecture
- standards (e.g., 3G, LTE)

## Mobility

### 7.5 Principles: addressing and routing to mobile users

### 7.6 Mobile IP

### 7.7 Handling mobility in cellular networks

### 7.8 Mobility and higher-layer protocols

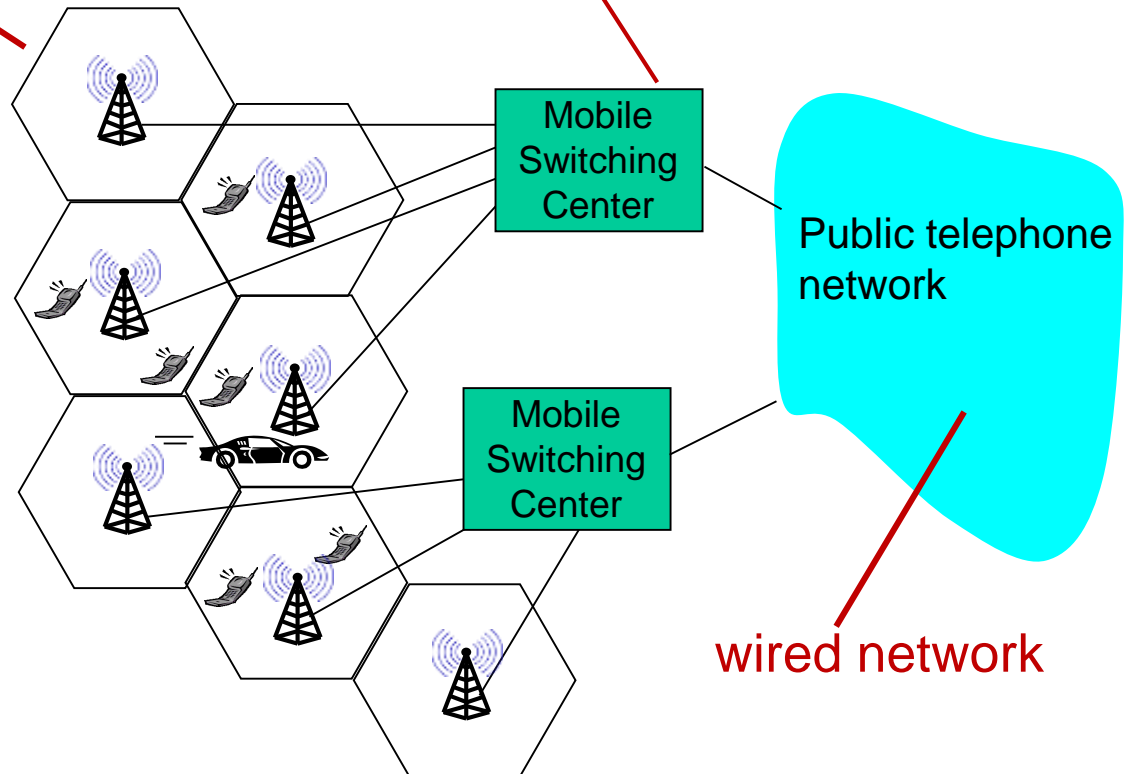
# Components of cellular network architecture

## cell

- ❖ covers geographical region
- ❖ *base station* (BS)  
analogous to 802.11 AP
- ❖ *mobile users* attach to network through BS
- ❖ *air-interface*: physical and link layer protocol between mobile and BS

## MSC

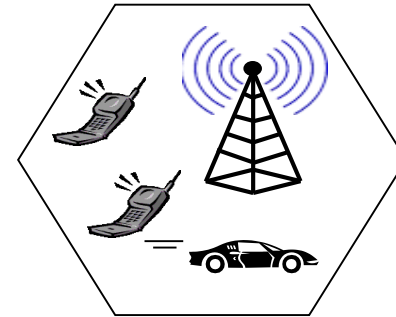
- ❖ connects cells to wired tel. net.
- ❖ manages call setup (more later!)
- ❖ handles mobility (more later!)



# Cellular networks: the first hop

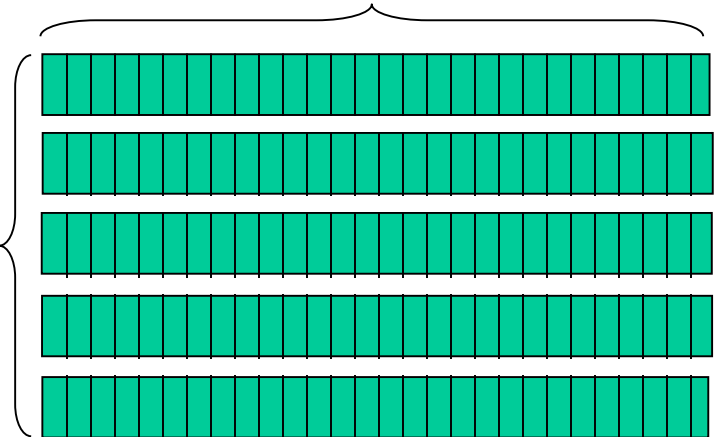
Two techniques for sharing mobile-to-BS radio spectrum

- **combined FDMA/TDMA:** divide spectrum in frequency channels, divide each channel into time slots
- **CDMA:** code division multiple access

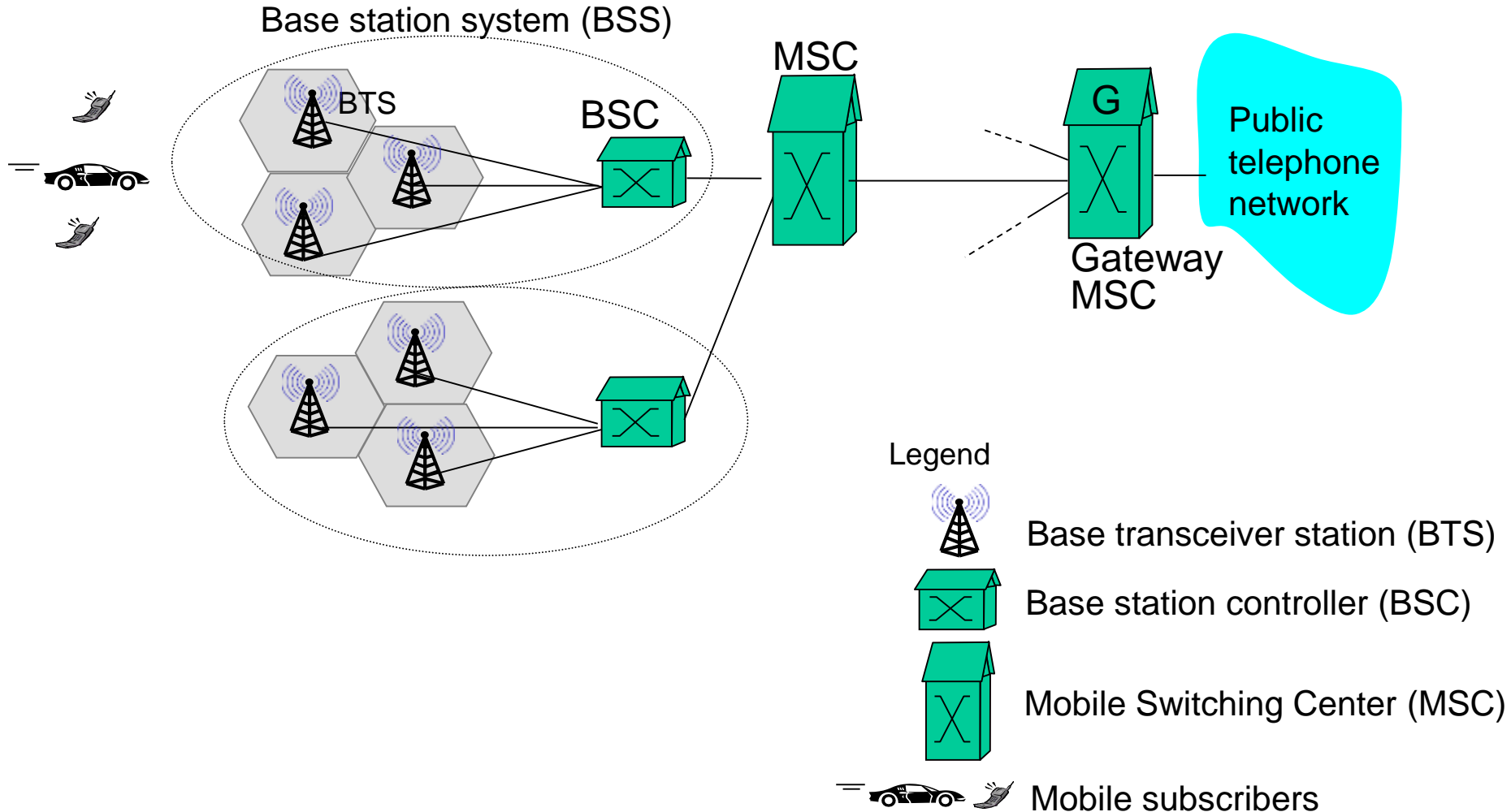


time slots

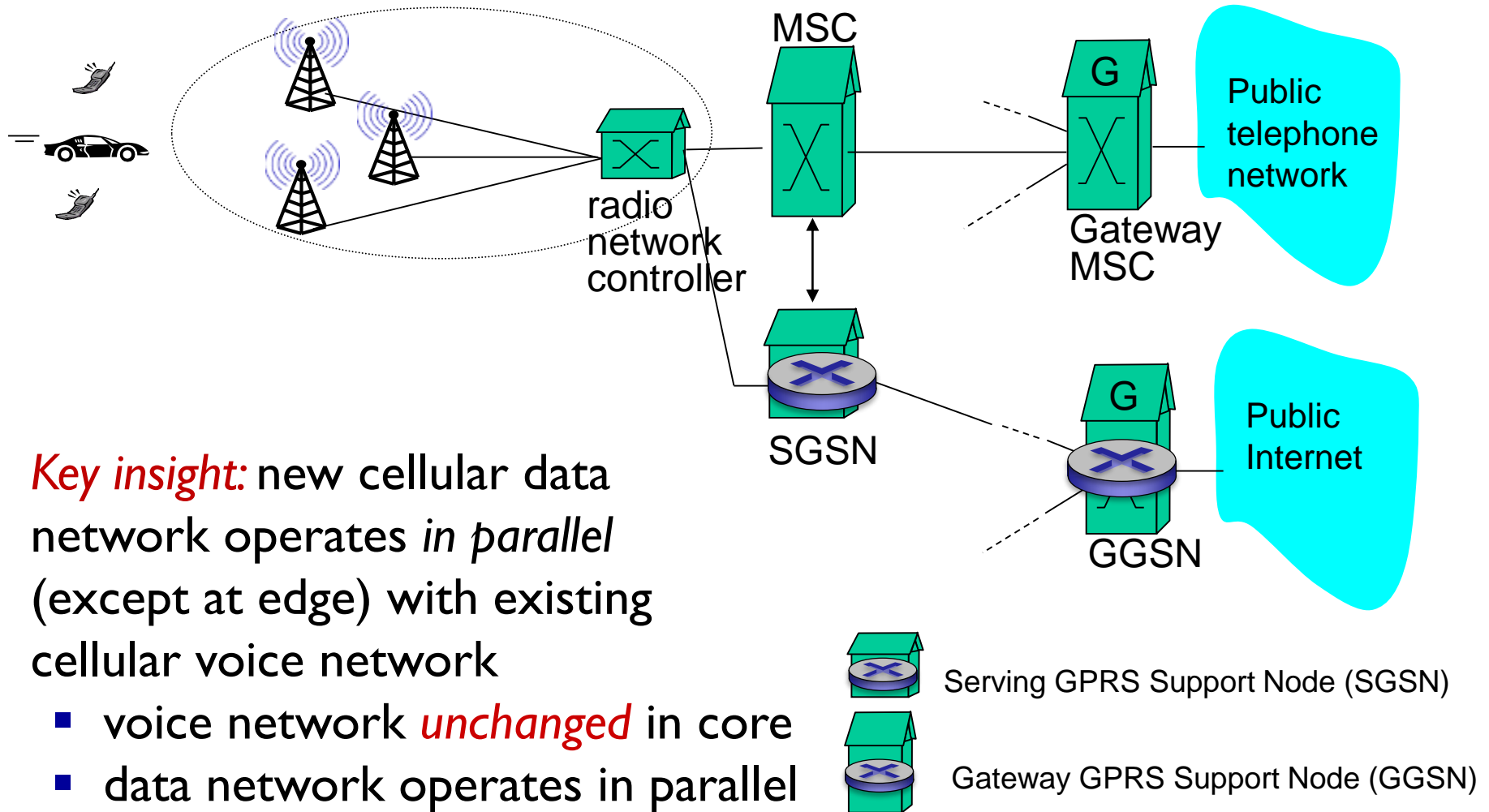
frequency bands



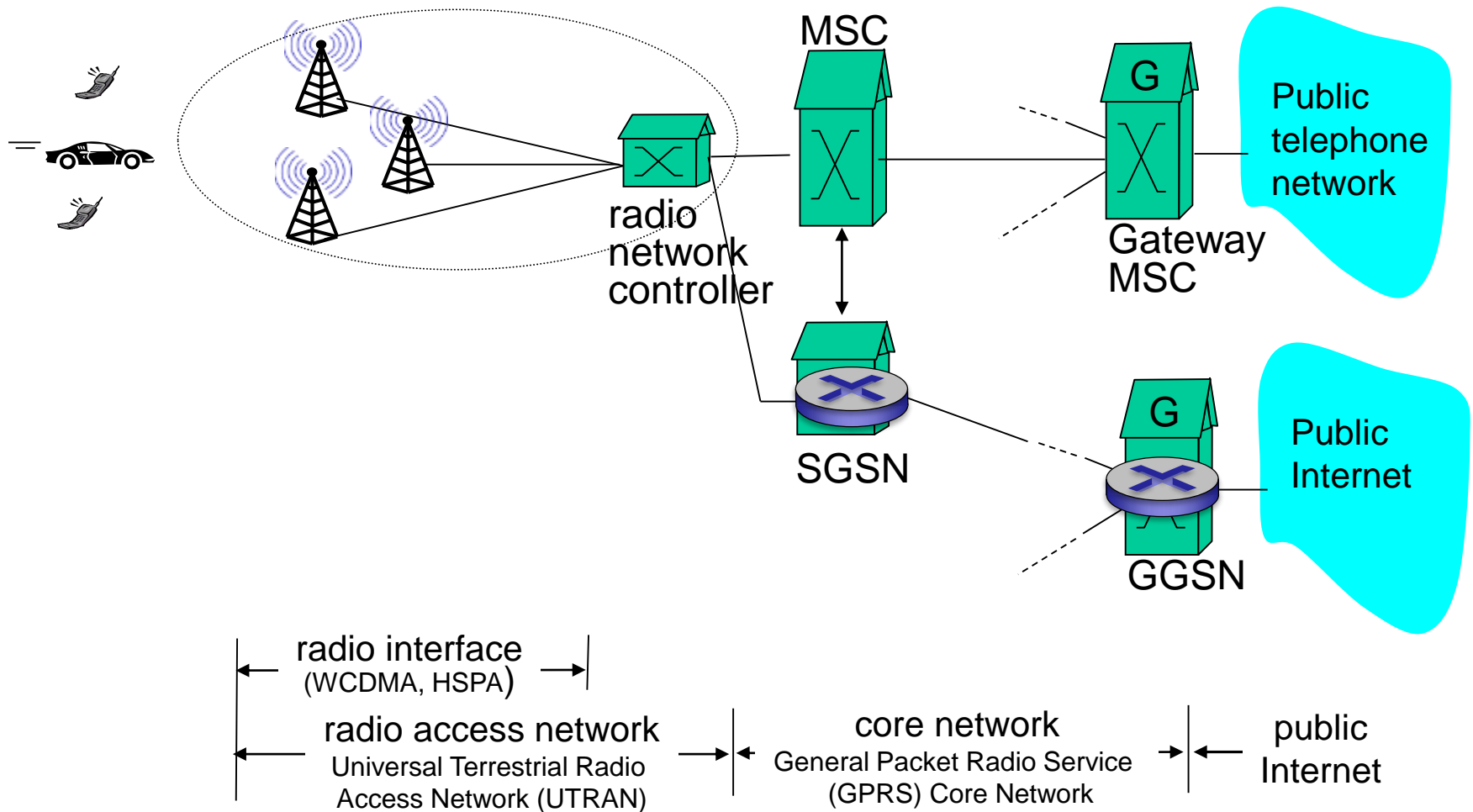
# 2G (voice) network architecture



# 3G (voice+data) network architecture

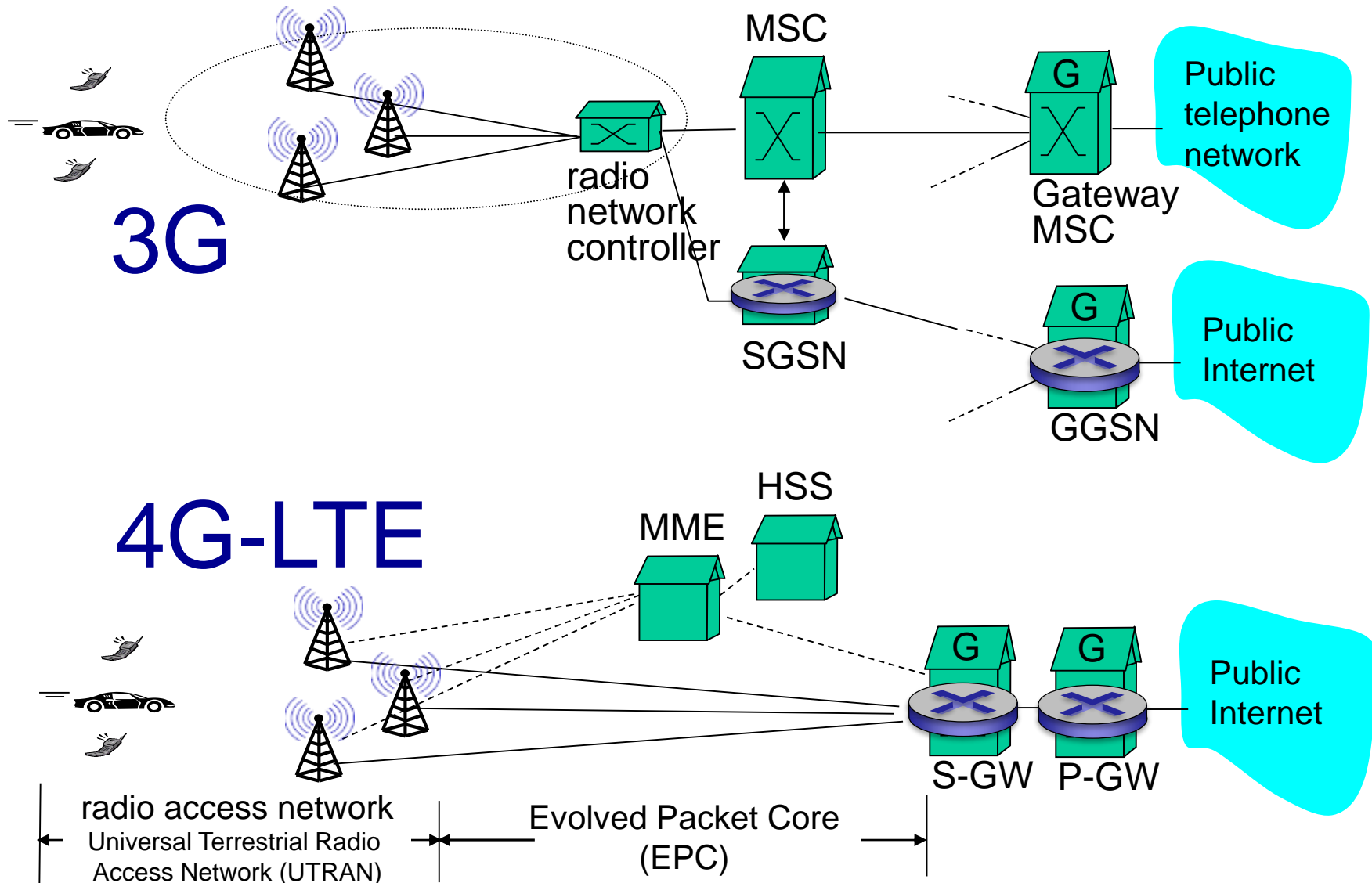


# 3G (voice+data) network architecture



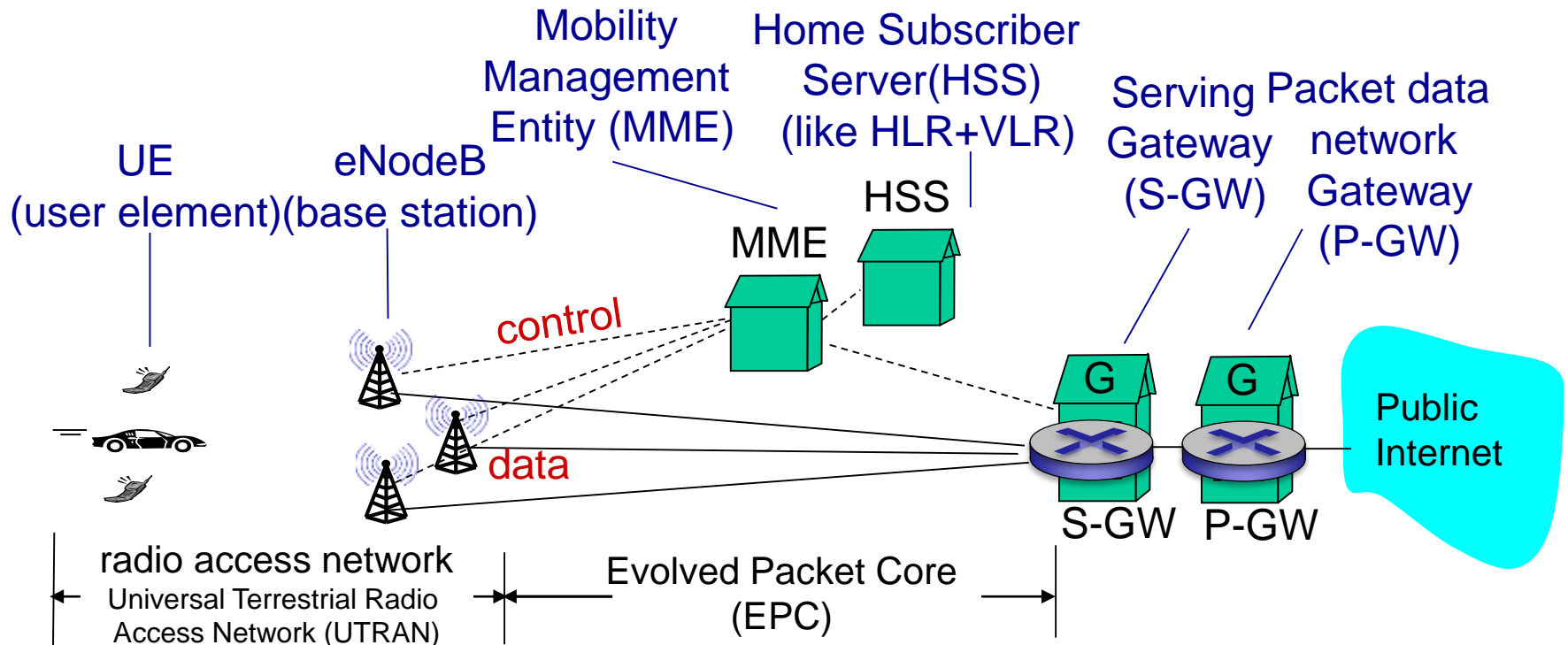


# 3G versus 4G LTE network architecture

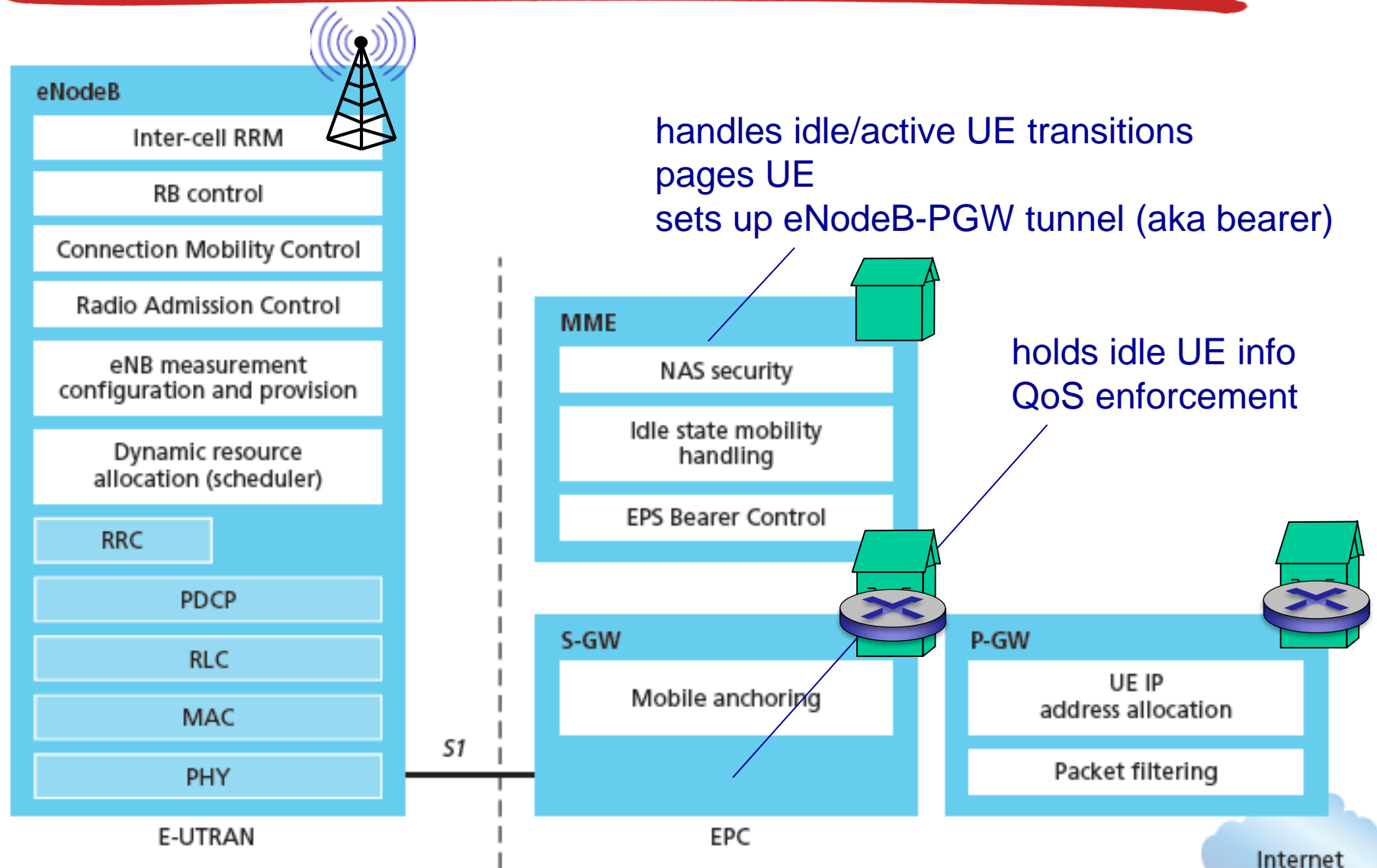


# 4G: differences from 3G

- all IP core: IP packets tunneled (through core IP network) from base station to gateway
- no separation between voice and data – all traffic carried over IP core to gateway



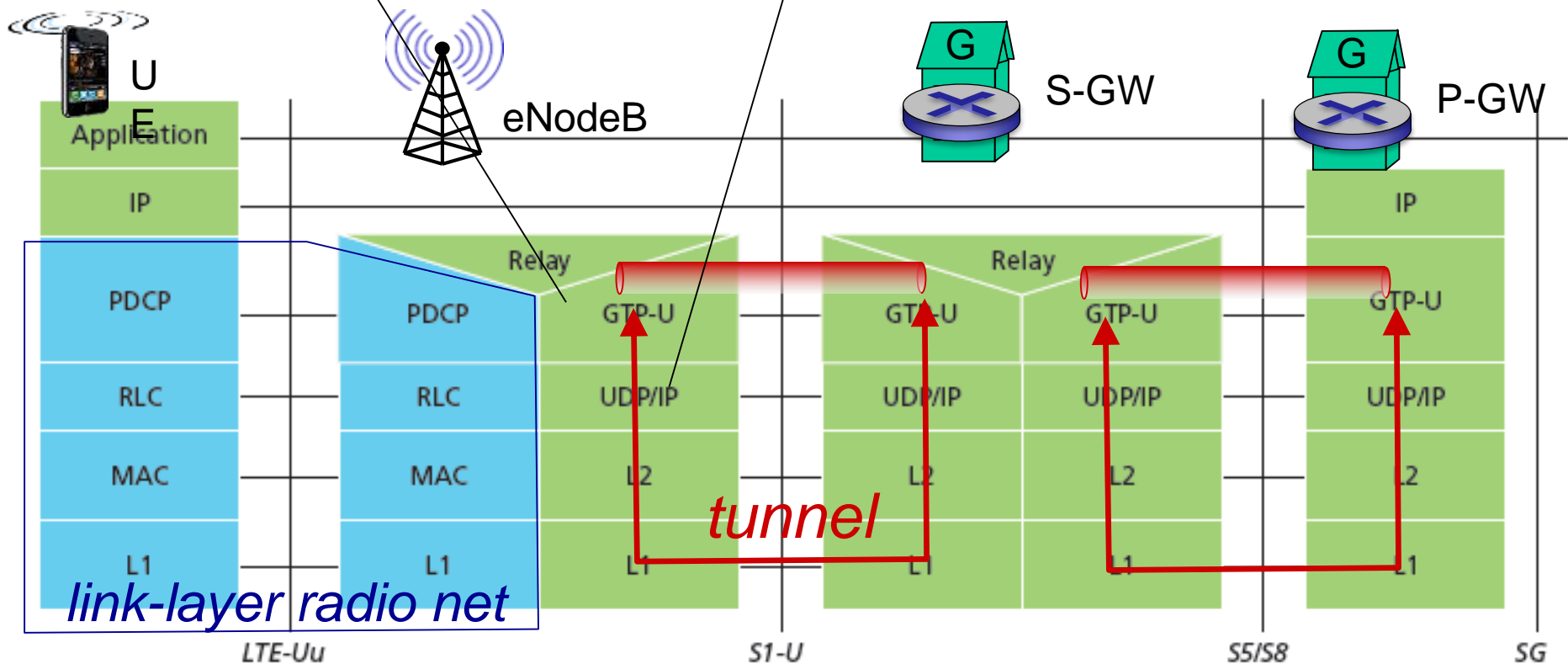
# Functional split of major LTE components



# Radio+Tunneling: UE – eNodeB – PGW

IP packet from UE encapsulated in GPRS Tunneling Protocol (GTP) message at ENodeB

GTP message encapsulated in UDP, then encapsulated in IP. large IP packet addressed to SGW



# Quality of Service in LTE

- QoS from eNodeB to SGW: min and max guaranteed bit rate
- QoS in radio access network: one of 12 QCI values

QCI	RESOURCE TYPE	PRIORITY	PACKET DELAY BUDGET (MS)	PACKET ERROR LOSS RATE	EXAMPLE SERVICES
1	GBR	2	100	$10^{-2}$	Conversational voice
2	GBR	4	150	$10^{-3}$	Conversational video (live streaming)
3	GBR	5	300	$10^{-6}$	Non-conversational video (buffered streaming)
4	GBR	3	50	$10^{-3}$	Real-time gaming
5	Non-GBR	1	100	$10^{-6}$	IMS signaling
6	Non-GBR	7	100	$10^{-3}$	Voice, video (live streaming), interactive gaming
7	Non-GBR	6	300	$10^{-6}$	Video (buffered streaming)
8	Non-GBR	8	300	$10^{-6}$	TCP-based (for example, WWW, e-mail), chat, FTP, p2p file sharing, progressive video and others
9	Non-GBR	9	300	$10^{-6}$	

# Chapter 7 outline

## 7.1 Introduction

## Wireless

## 7.2 Wireless links, characteristics

- CDMA

## 7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

## 7.4 Cellular Internet Access

- architecture
- standards (e.g., 3G, LTE)

## Mobility

## 7.5 Principles: addressing and routing to mobile users

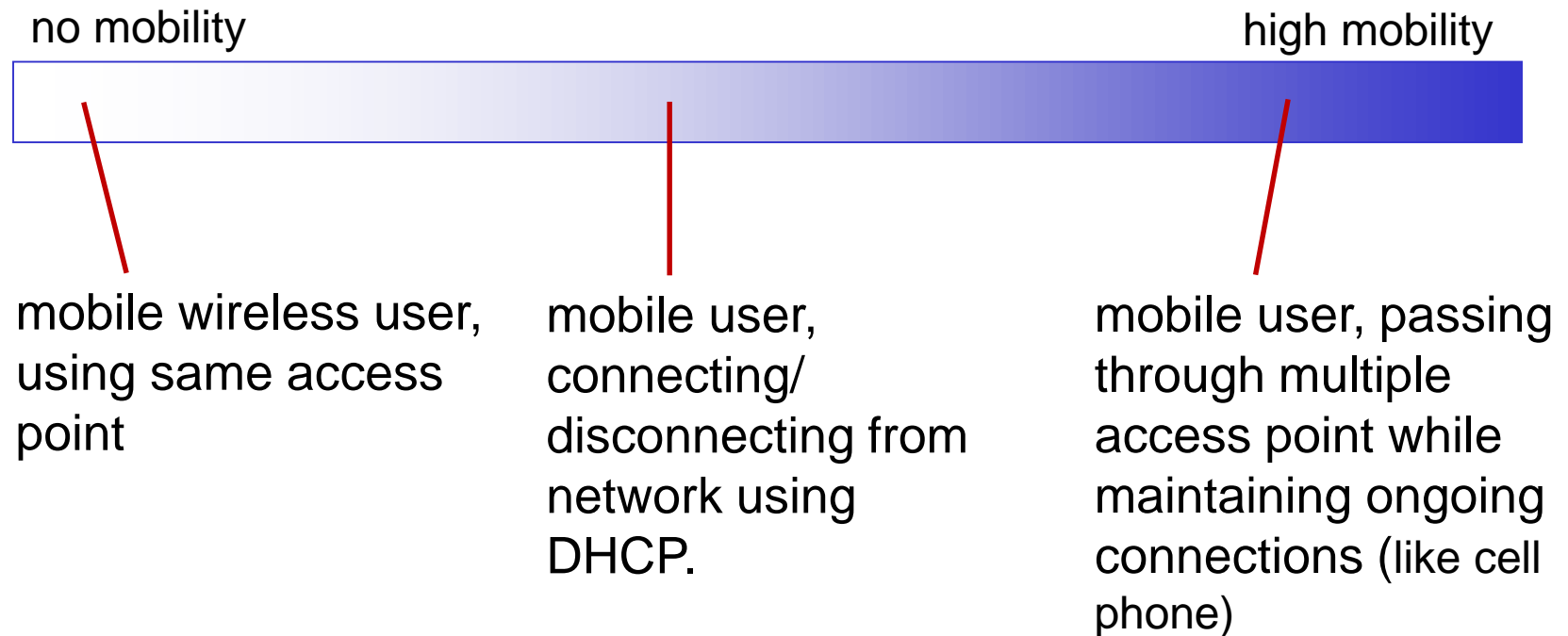
## 7.6 Mobile IP

## 7.7 Handling mobility in cellular networks

## 7.8 Mobility and higher-layer protocols

# What is mobility?

- spectrum of mobility, from the *network* perspective:

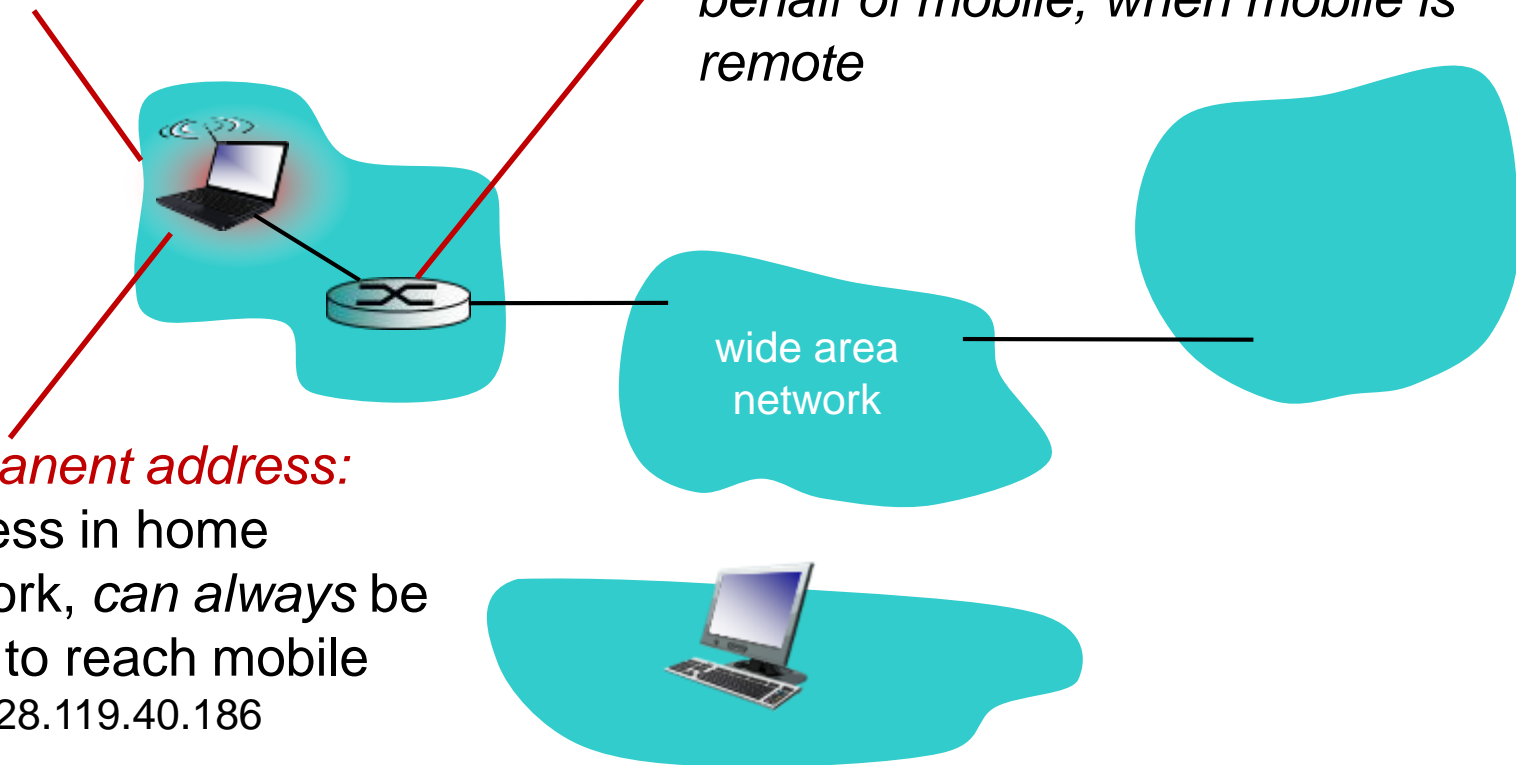


# Mobility: vocabulary

*home network:* permanent  
“home” of mobile  
(e.g., 128.119.40/24)

*home agent:* entity that will  
perform mobility functions on  
behalf of mobile, when mobile is  
remote

*permanent address:*  
address in home  
network, *can always* be  
used to reach mobile  
e.g., 128.119.40.186





# Mobility: more vocabulary

*permanent address*: remains constant (e.g., 128.119.40.186)

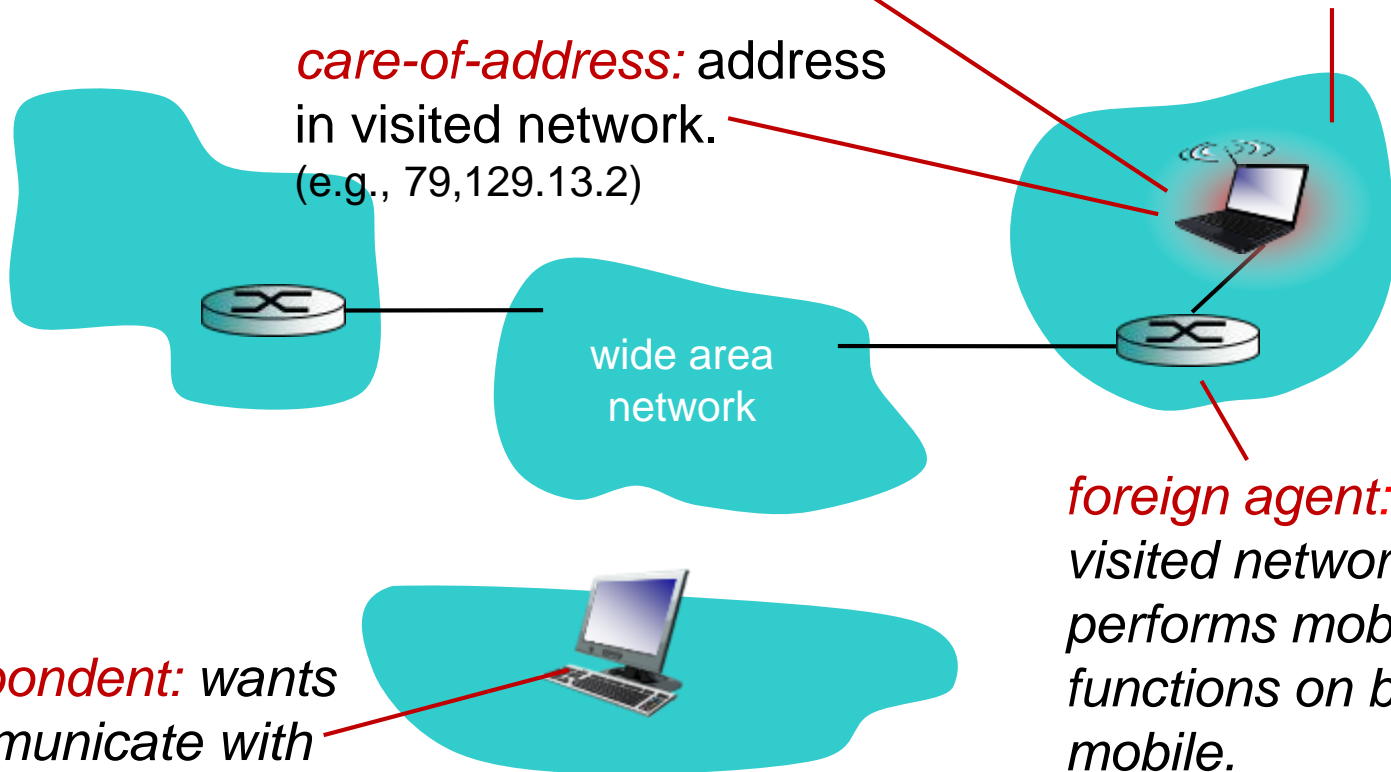
*visited network*: network in which mobile currently resides (e.g., 79.129.13/24)

*care-of-address*: address in visited network. (e.g., 79.129.13.2)

wide area network

*foreign agent*: entity in visited network that performs mobility functions on behalf of mobile.

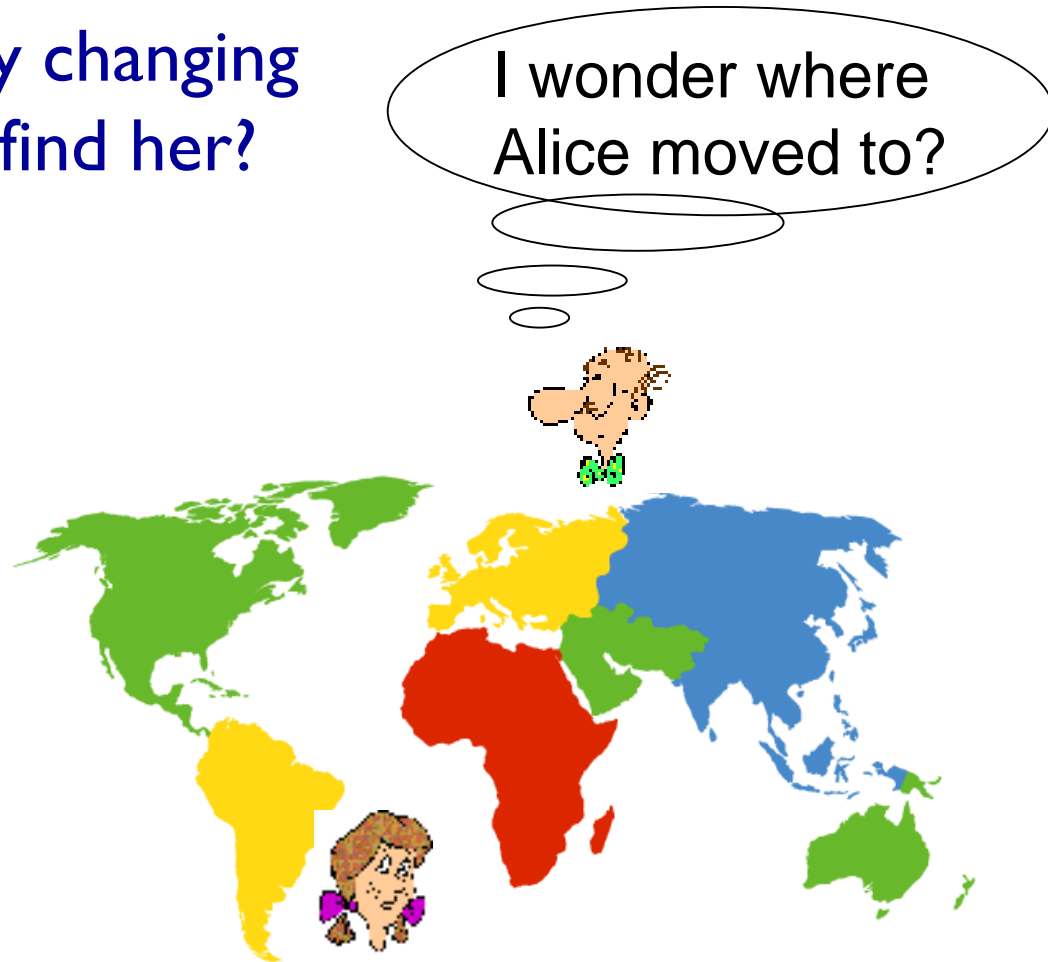
*correspondent*: wants to communicate with mobile



# How do *you* contact a mobile friend:

Consider friend frequently changing addresses, how do you find her?

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



# Mobility: approaches

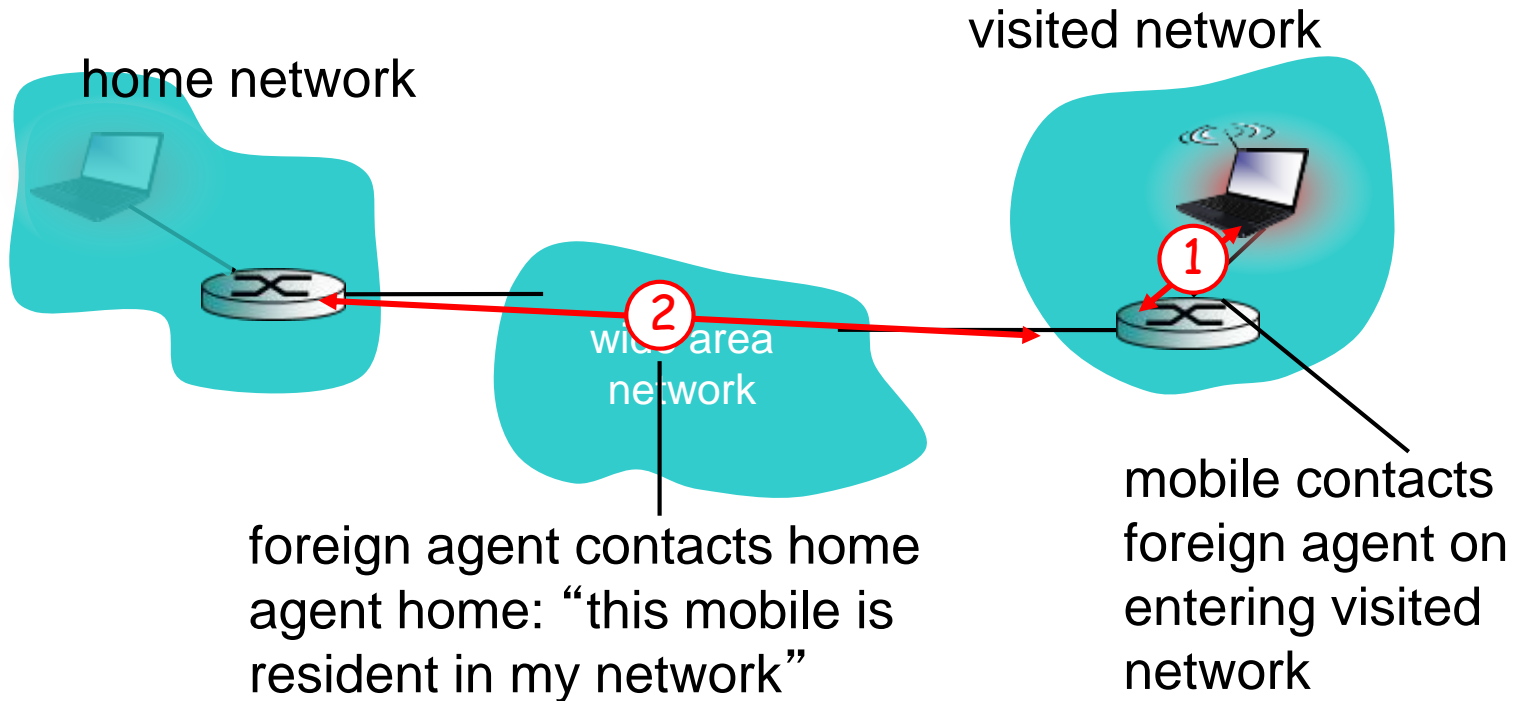
- *let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

# Mobility: approaches

- *let routing handle it:* routers advertise permanent address of mobile, mobile's residence via usual routing table exchange
  - routing table entry for each mobile location
  - no changes to routing tables
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

not  
scalable  
to millions of  
mobiles

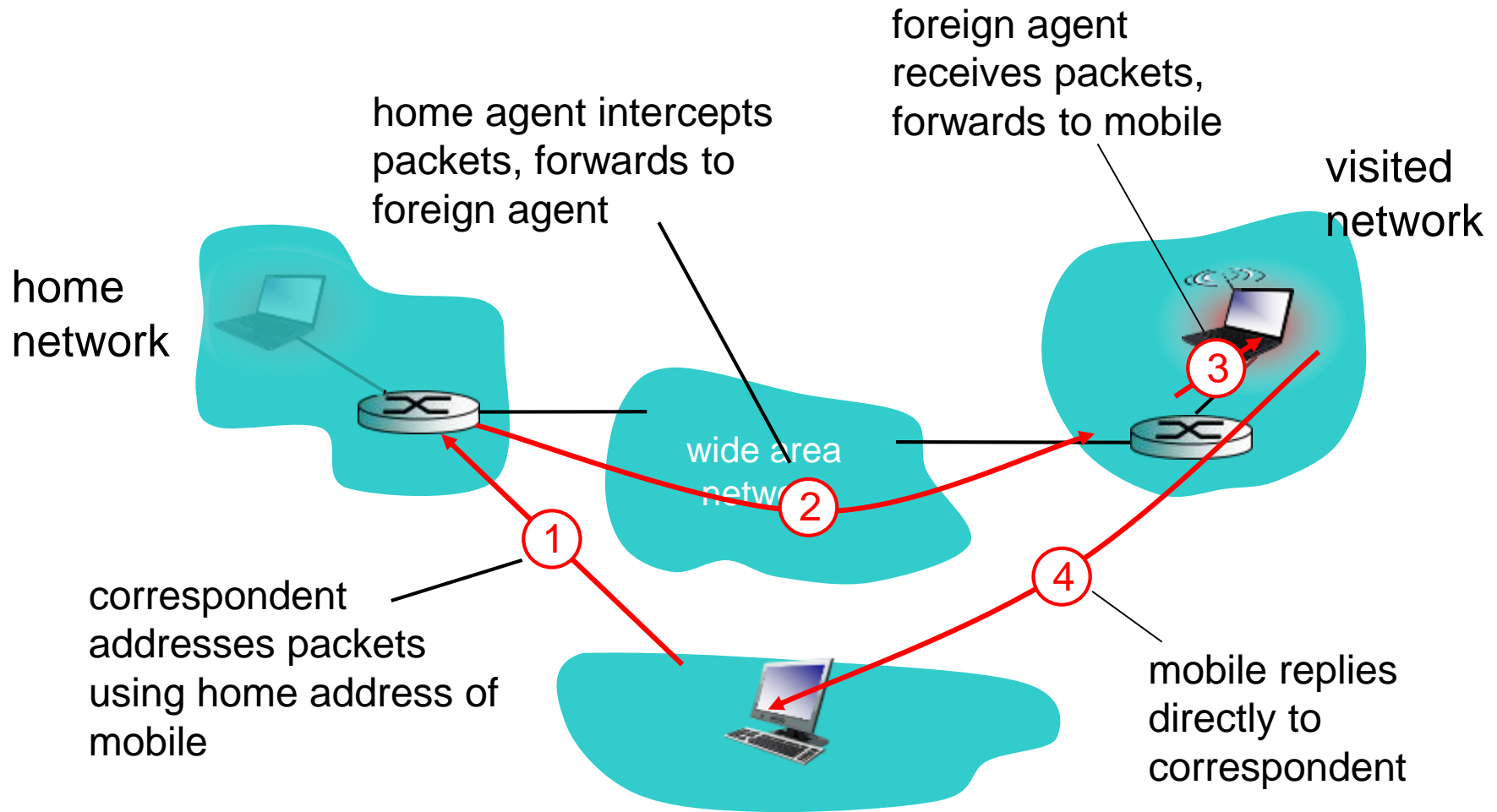
# Mobility: registration



end result:

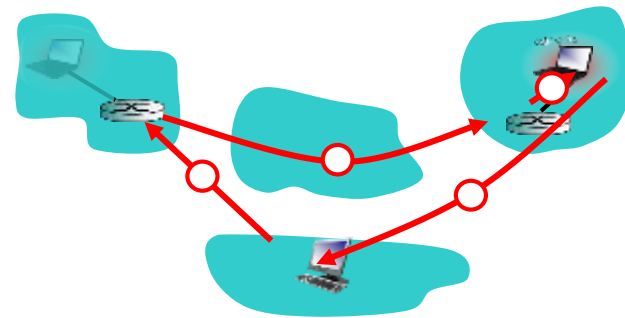
- foreign agent knows about mobile
- home agent knows location of mobile

# Mobility via indirect routing



# Indirect Routing: comments

- mobile uses two addresses:
  - **permanent address**: used by correspondent (hence mobile location is *transparent* to correspondent)
  - **care-of-address**: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- **triangle routing**: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network

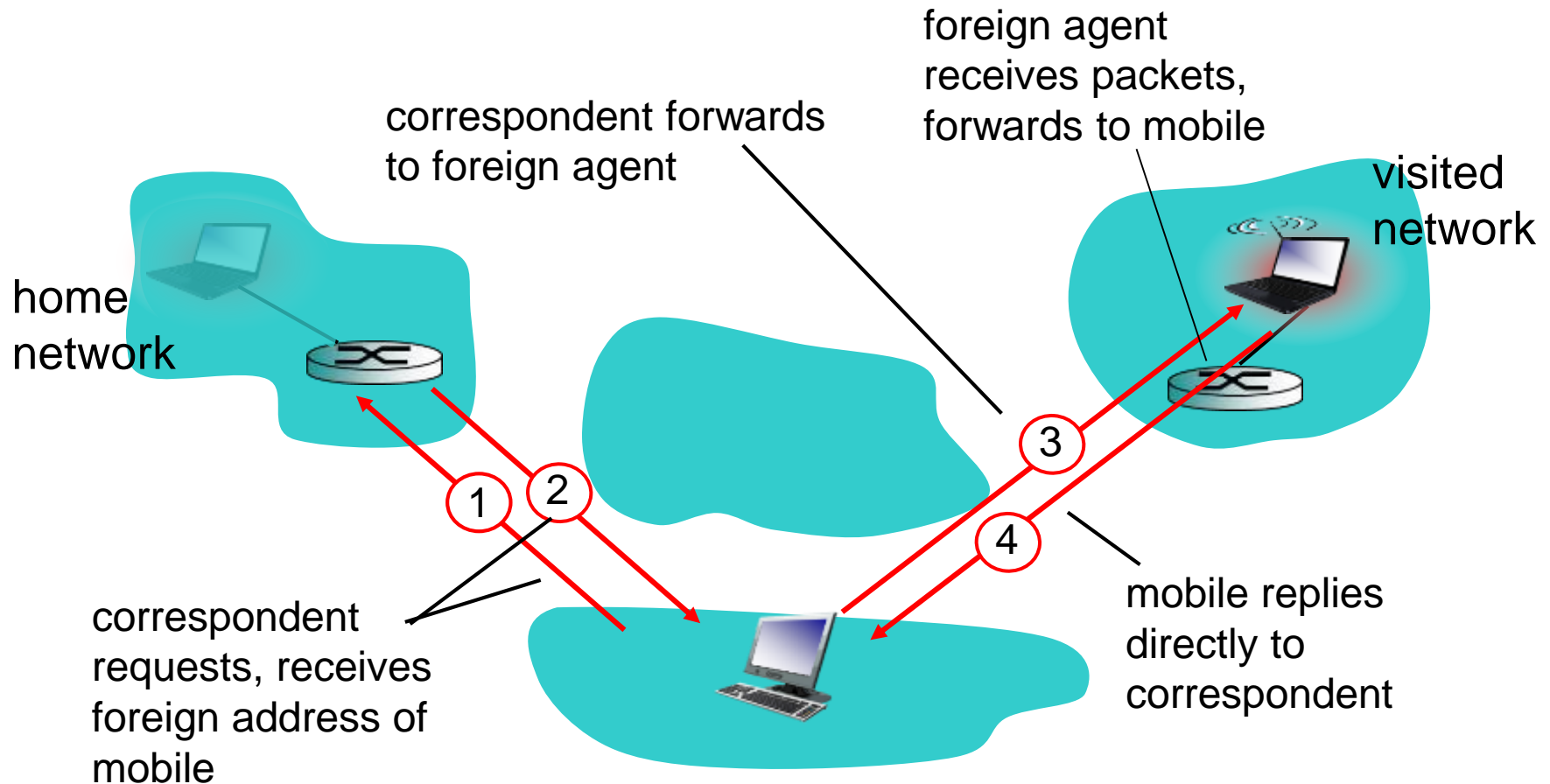


# Indirect routing: moving between networks

- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: *on going connections can be maintained!*

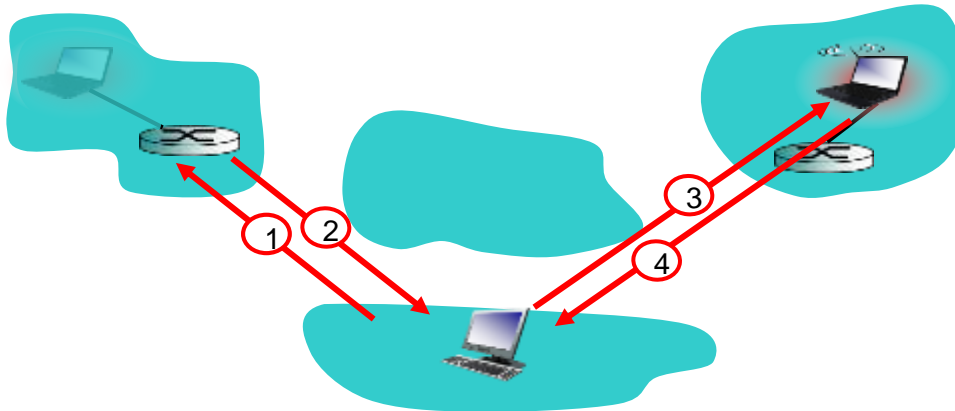


# Mobility via direct routing



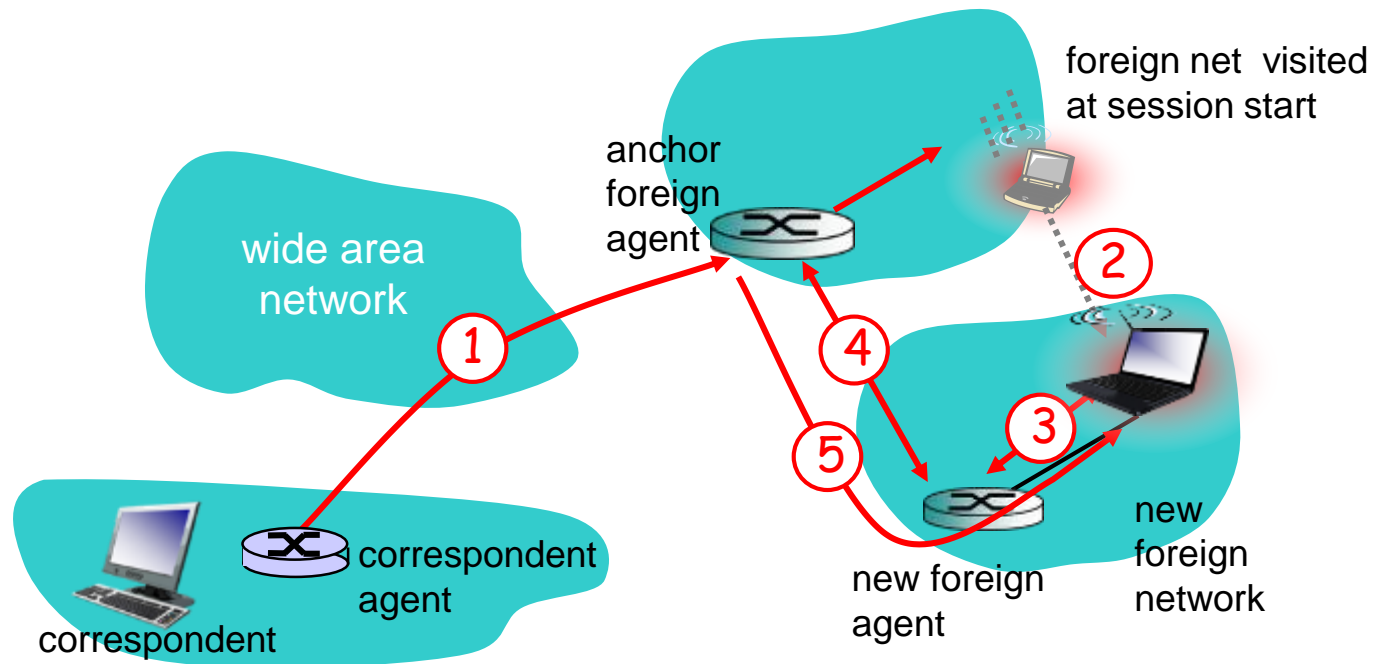
# Mobility via direct routing: comments

- overcome triangle routing problem
- *non-transparent to correspondent*: correspondent must get care-of-address from home agent
  - what if mobile changes visited network?



# Accommodating mobility with direct routing

- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



# Chapter 7 outline

## 7.1 Introduction

## Wireless

## 7.2 Wireless links, characteristics

- CDMA

## 7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

## 7.4 Cellular Internet Access

- architecture
- standards (e.g., 3G, LTE)

## Mobility

## 7.5 Principles: addressing and routing to mobile users

## 7.6 Mobile IP

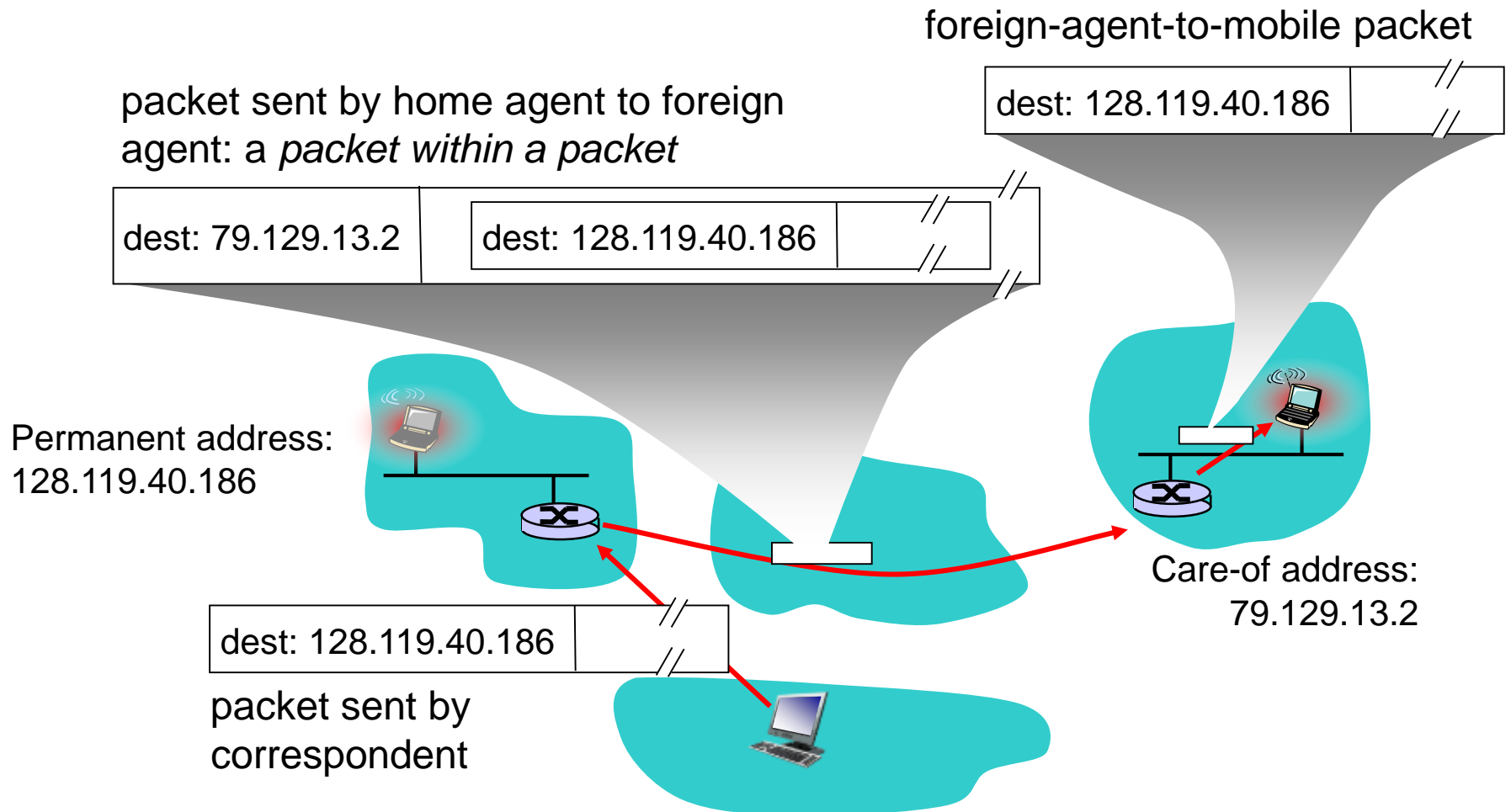
## 7.7 Handling mobility in cellular networks

## 7.8 Mobility and higher-layer protocols

# Mobile IP

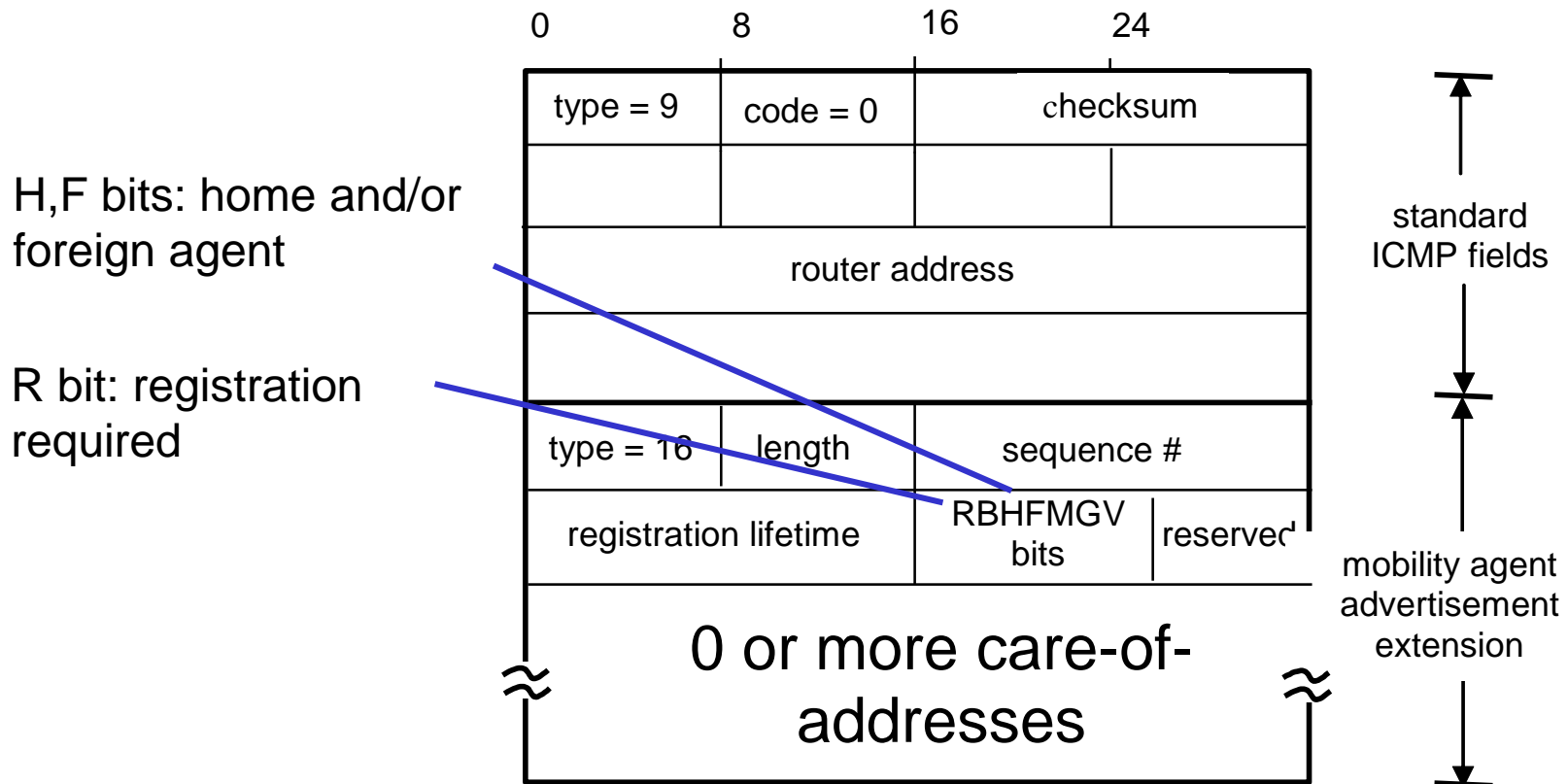
- RFC 3344
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

# Mobile IP: indirect routing

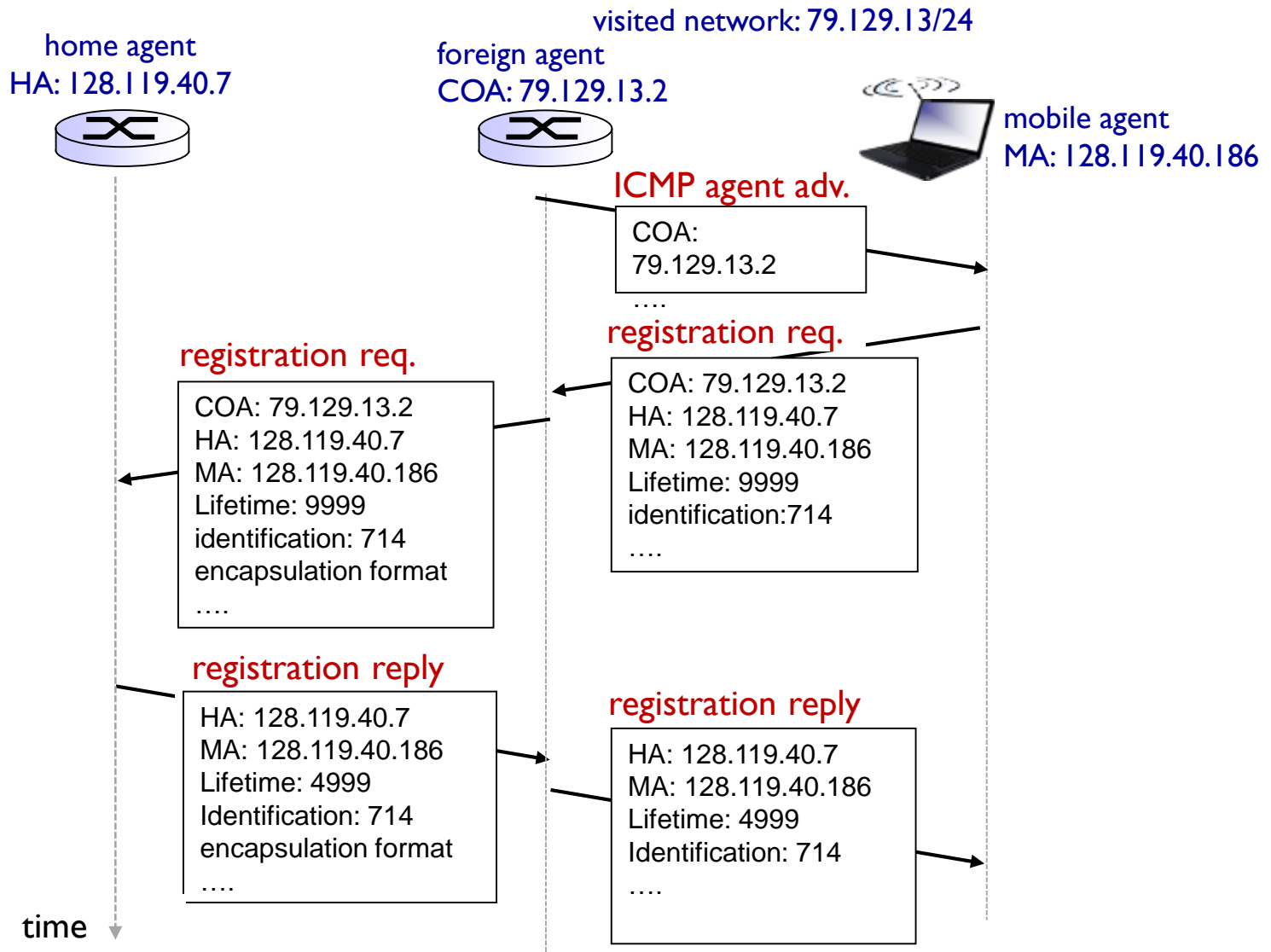


# Mobile IP: agent discovery

- *agent advertisement*: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)



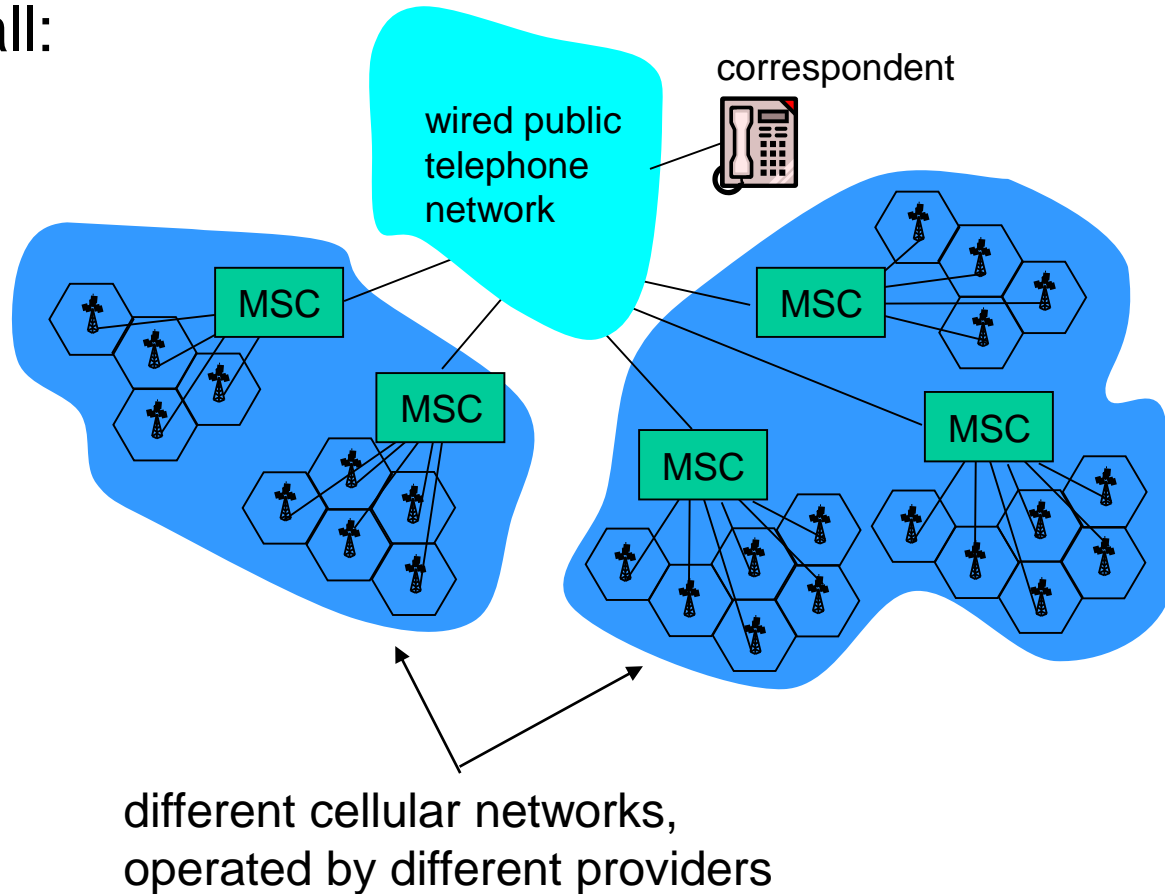
# Mobile IP: registration example





# Components of cellular network architecture

recall:

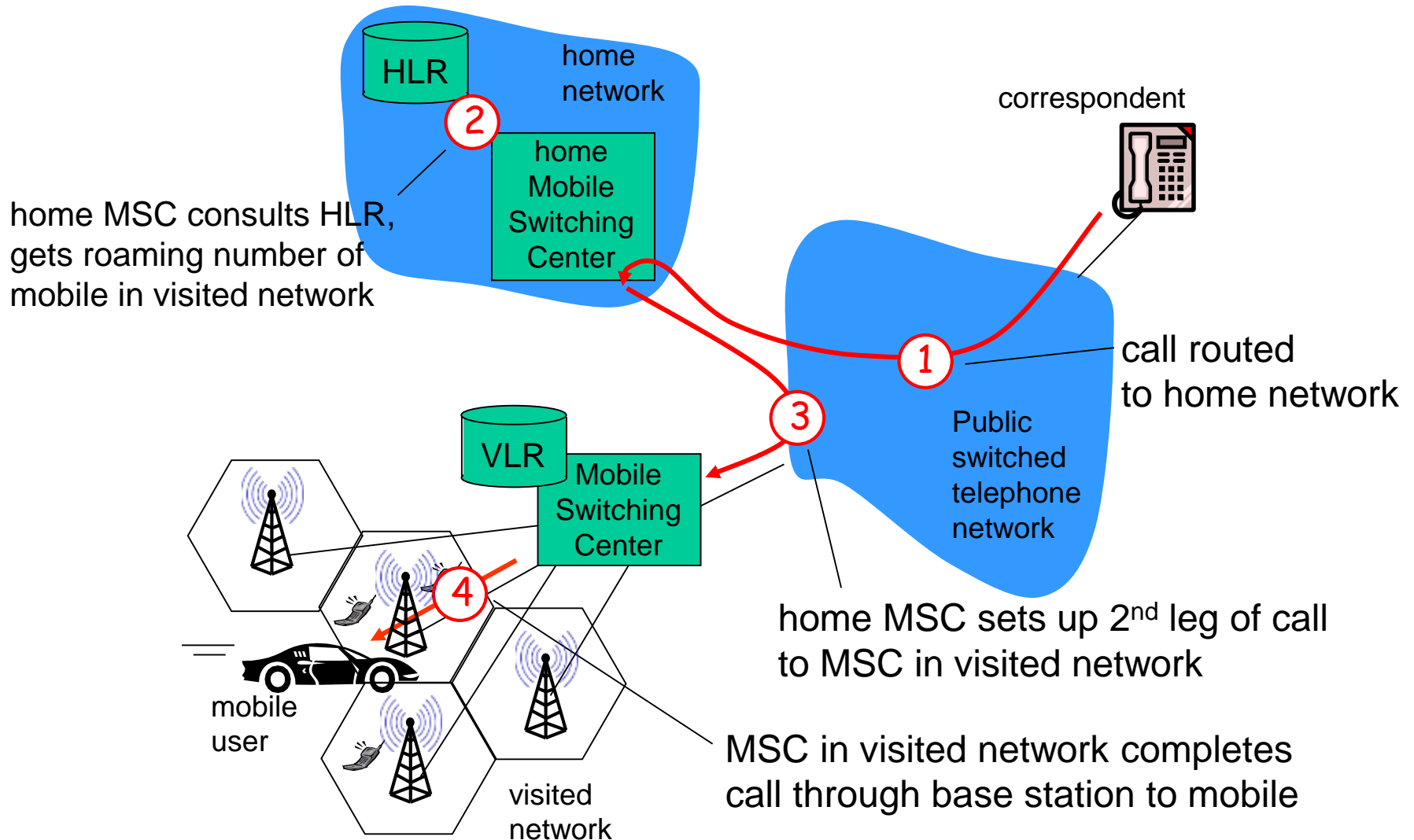


# Handling mobility in cellular networks

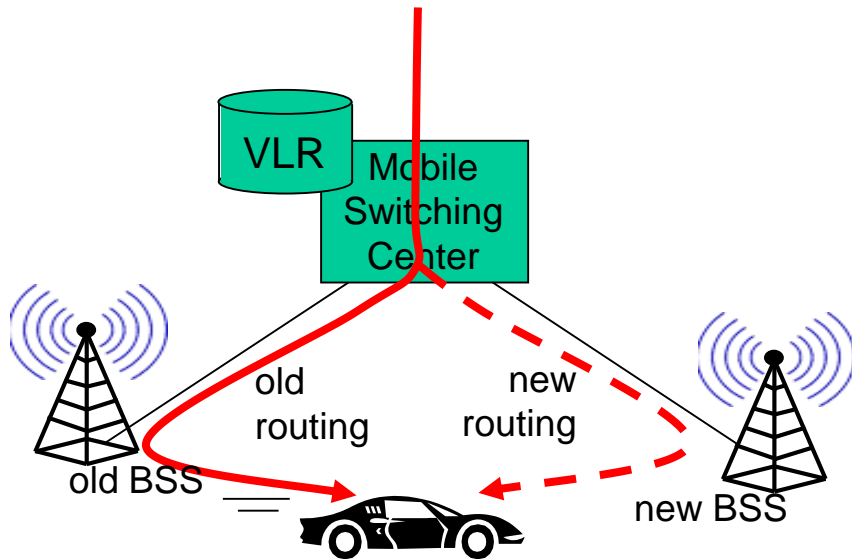
---

- *home network*: network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - *home location register (HLR)*: database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- *visited network*: network in which mobile currently resides
  - *visitor location register (VLR)*: database with entry for each user currently in network
  - could be home network

# GSM: indirect routing to mobile

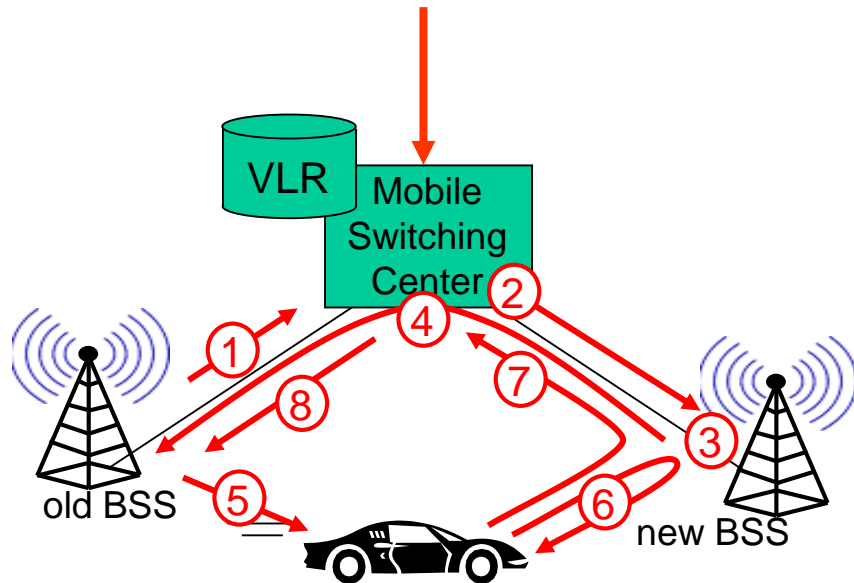


# GSM: handoff with common MSC



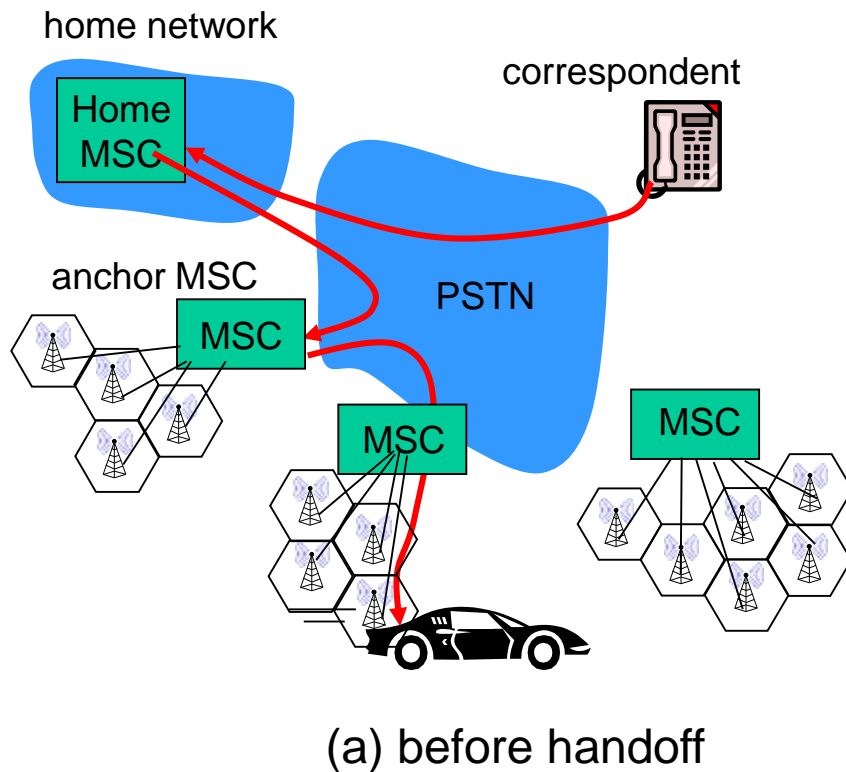
- *handoff goal*: route call via new base station (without interruption)
- reasons for handoff:
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - GSM doesn't mandate why to perform handoff (policy), only how (mechanism)
- handoff initiated by old BSS

# GSM: handoff with common MSC



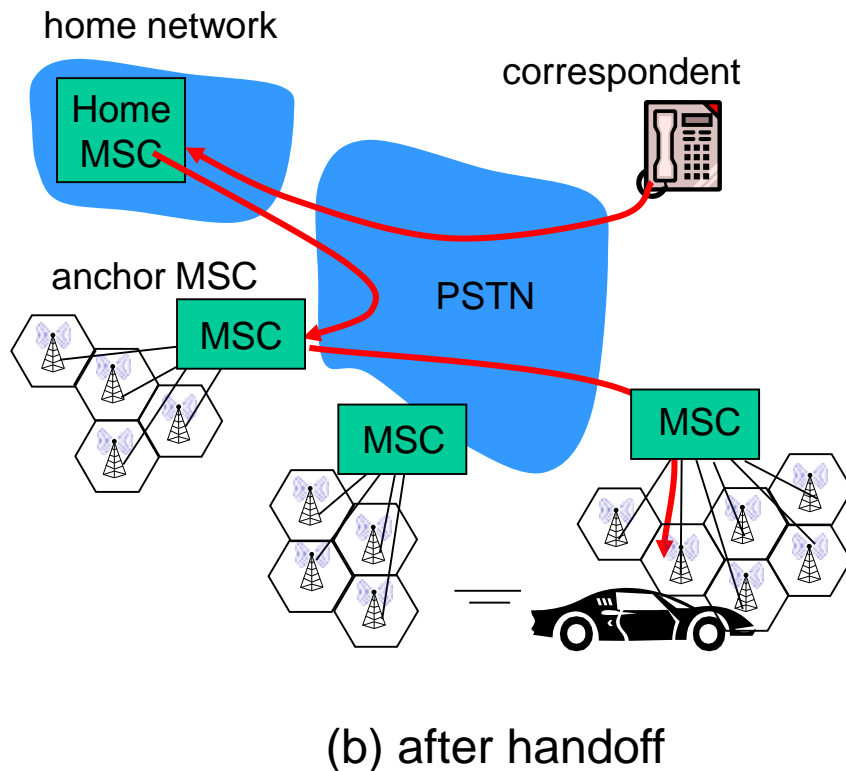
1. old BSS informs MSC of impending handoff, provides list of 1+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call
8. MSC-old-BSS resources released

# GSM: handoff between MSCs



- *anchor MSC*: first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- optional path minimization step to shorten multi-MSC chain

# GSM: handoff between MSCs



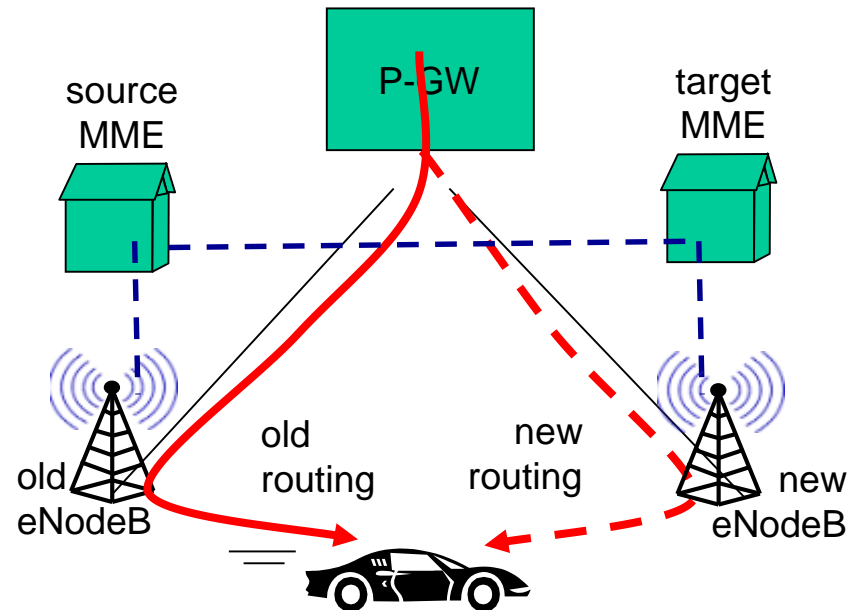
- *anchor MSC*: first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- optional path minimization step to shorten multi-MSC chain

# Handling Mobility in LTE

- Paging: idle UE may move from cell to cell: network does not know where the idle UE is resident
  - paging message from MME broadcast by all eNodeB to locate UE

- handoff: similar to 3G:

- preparation phase
- execution phase
- completion phase





# Mobility: cellular versus Mobile IP

cellular element	Comment on cellular element	Mobile IP element
<b>Home system</b>	Network to which mobile user's permanent phone number belongs	<b>Home network</b>
<b>Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)</b>	Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information	<b>Home agent</b>
<b>Visited System</b>	Network other than home system where mobile user is currently residing	<b>Visited network</b>
<b>Visited Mobile services Switching Center. Visitor Location Record (VLR)</b>	Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user	<b>Foreign agent</b>
<b>Mobile Station Roaming Number (MSRN), or "roaming number"</b>	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	<b>Care-of-address</b>

# 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 handoff
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - limited bandwidth of wireless links

# Chapter 7 summary

## *Wireless*

- wireless links:
  - capacity, distance
  - channel impairments
  - CDMA
- IEEE 802.11 (“Wi-Fi”)
  - CSMA/CA reflects wireless channel characteristics
- cellular access
  - architecture
  - standards (e.g., 3G, 4G LTE)

## *Mobility*

- principles: addressing, routing to mobile users
  - home, visited networks
  - direct, indirect routing
  - care-of-addresses
- case studies
  - mobile IP
  - mobility in GSM, LTE
- impact on higher-layer protocols