CS 305: Computer Networks
Fall 2024

Week 15 Wireless and Mobile Networks

Tianyue Zheng

Department of Computer Science and Engineering
Southern University of Science and Technology (SUSTech)

Why we need MAC address?

- LAN is designed for arbitrary network layer protocol; not only IP and the Internet
- If use IP, IP needs to be stored at RAM and configured every time when moving
- [Independent building blocks: each layer has its own address]

Chapter 7 outline

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
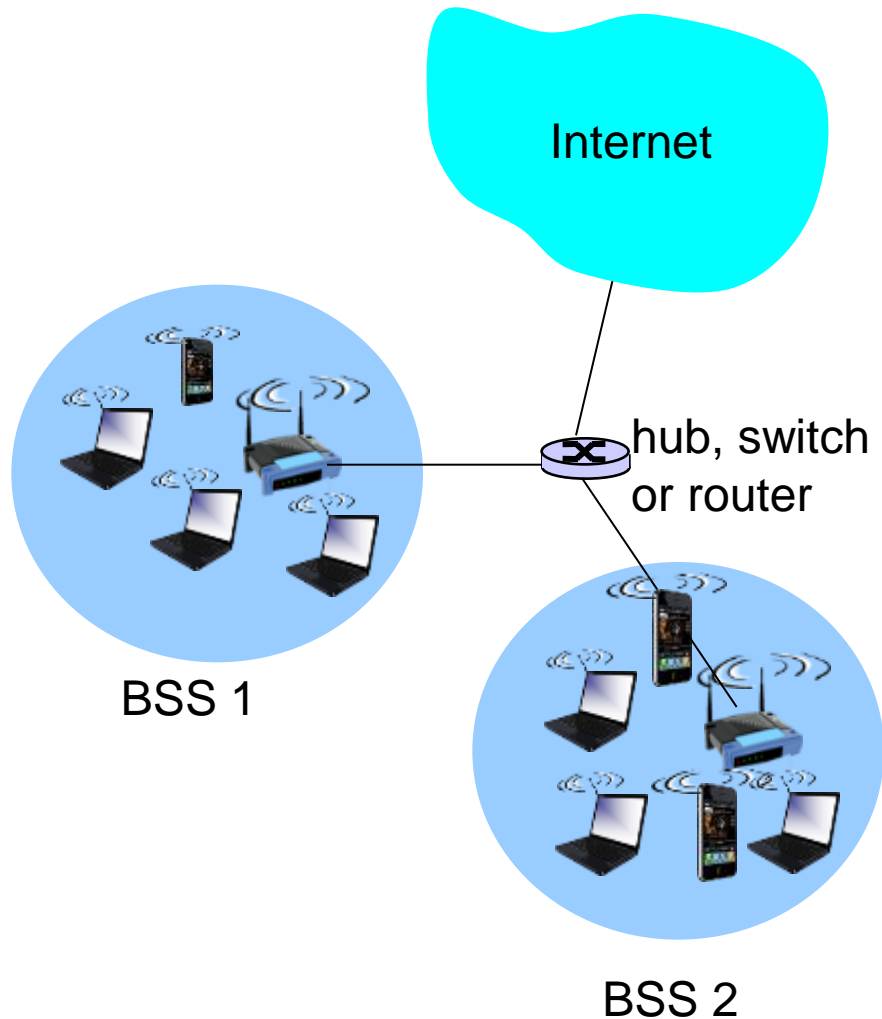
802.11g

- 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

Internet

hub, 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

- 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
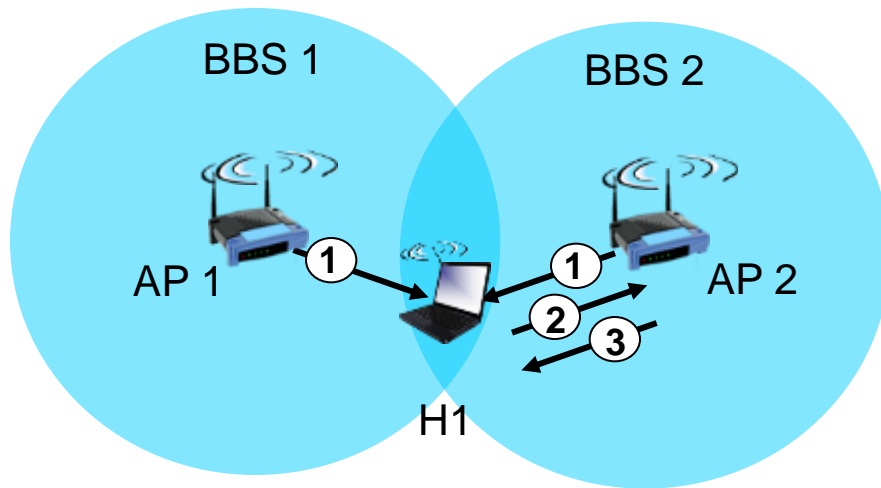
passive scanning:

(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
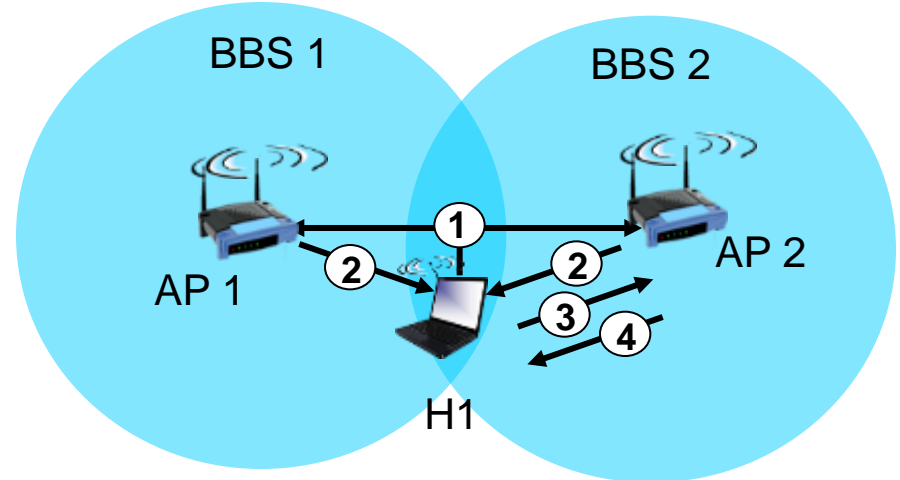
active scanning:

(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$^+$ 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)

C

B

A

A

B

C

A's signal strength

C's signal strength

space
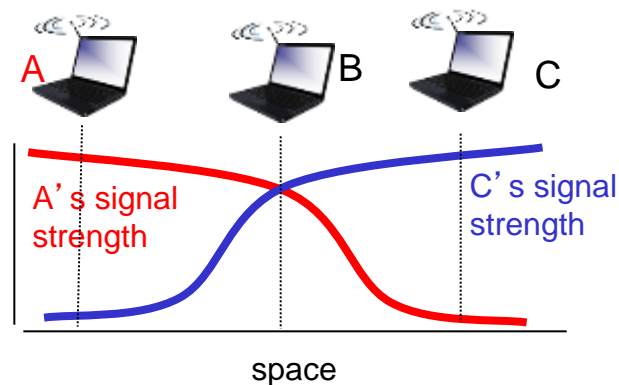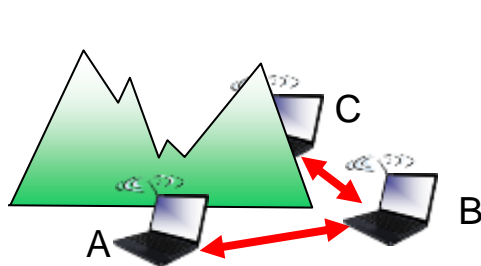
IEEE 802.11 MAC Protocol: CSMA/CA

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
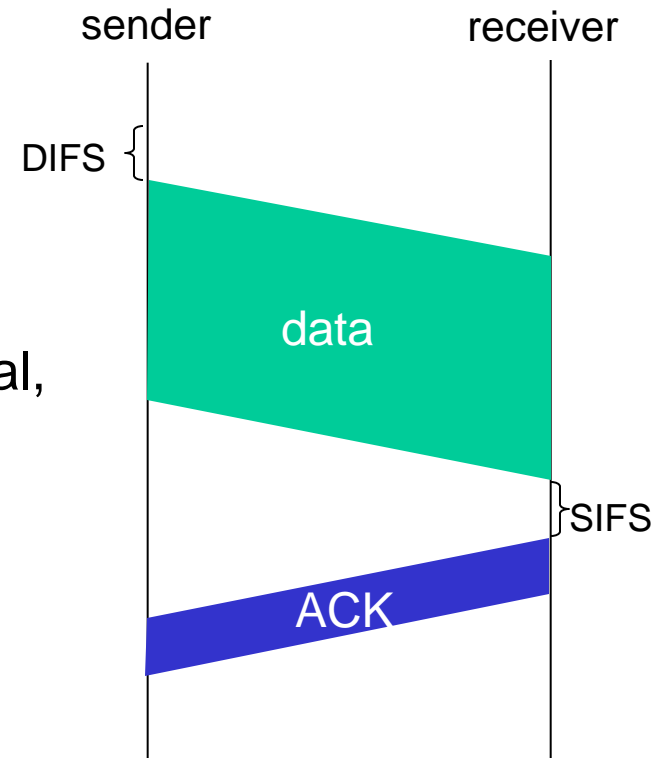
Avoiding collisions (more)

idea: 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!

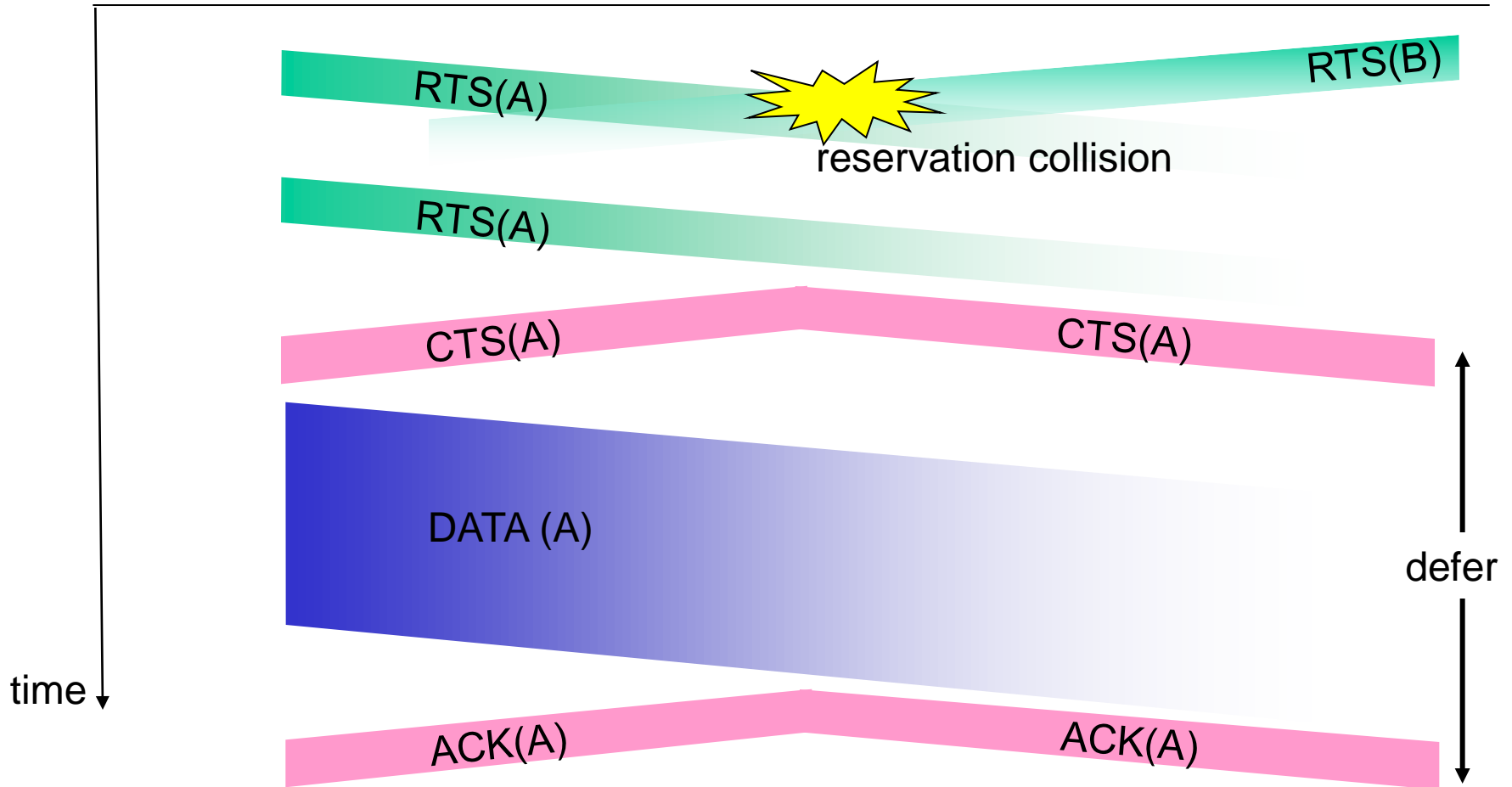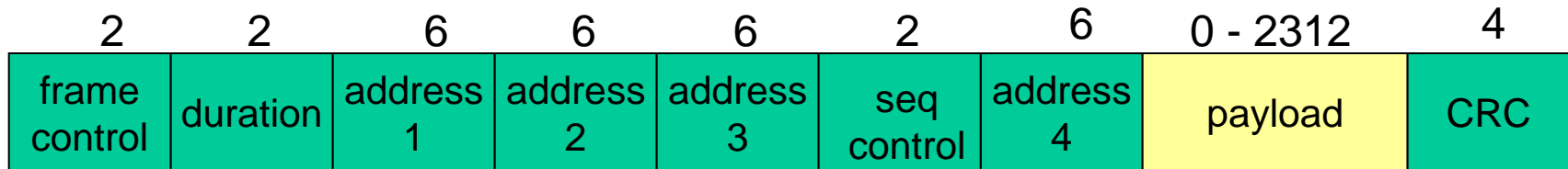# Collision Avoidance: RTS-CTS exchange

802.11 frame: addressing

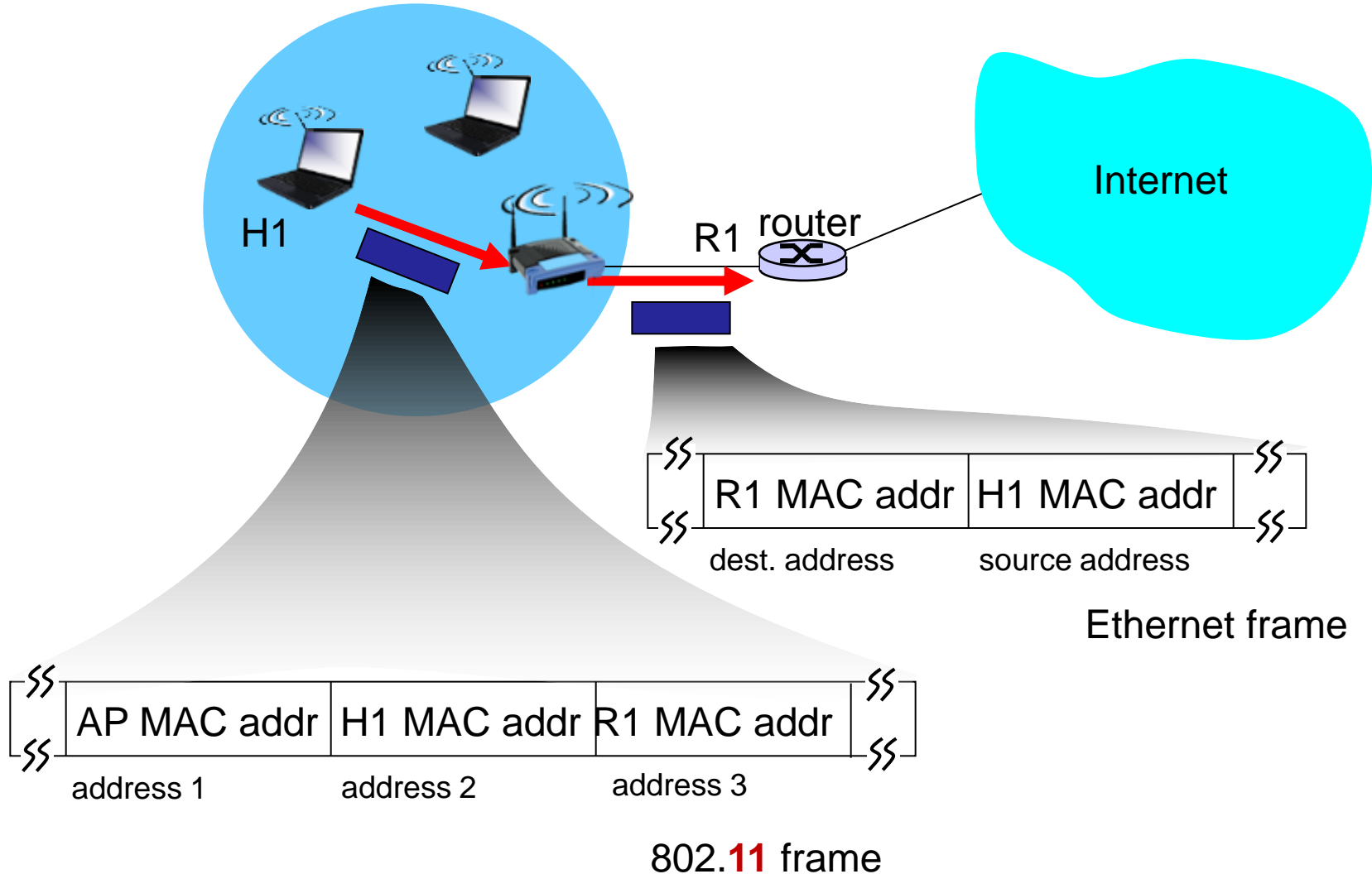| 2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

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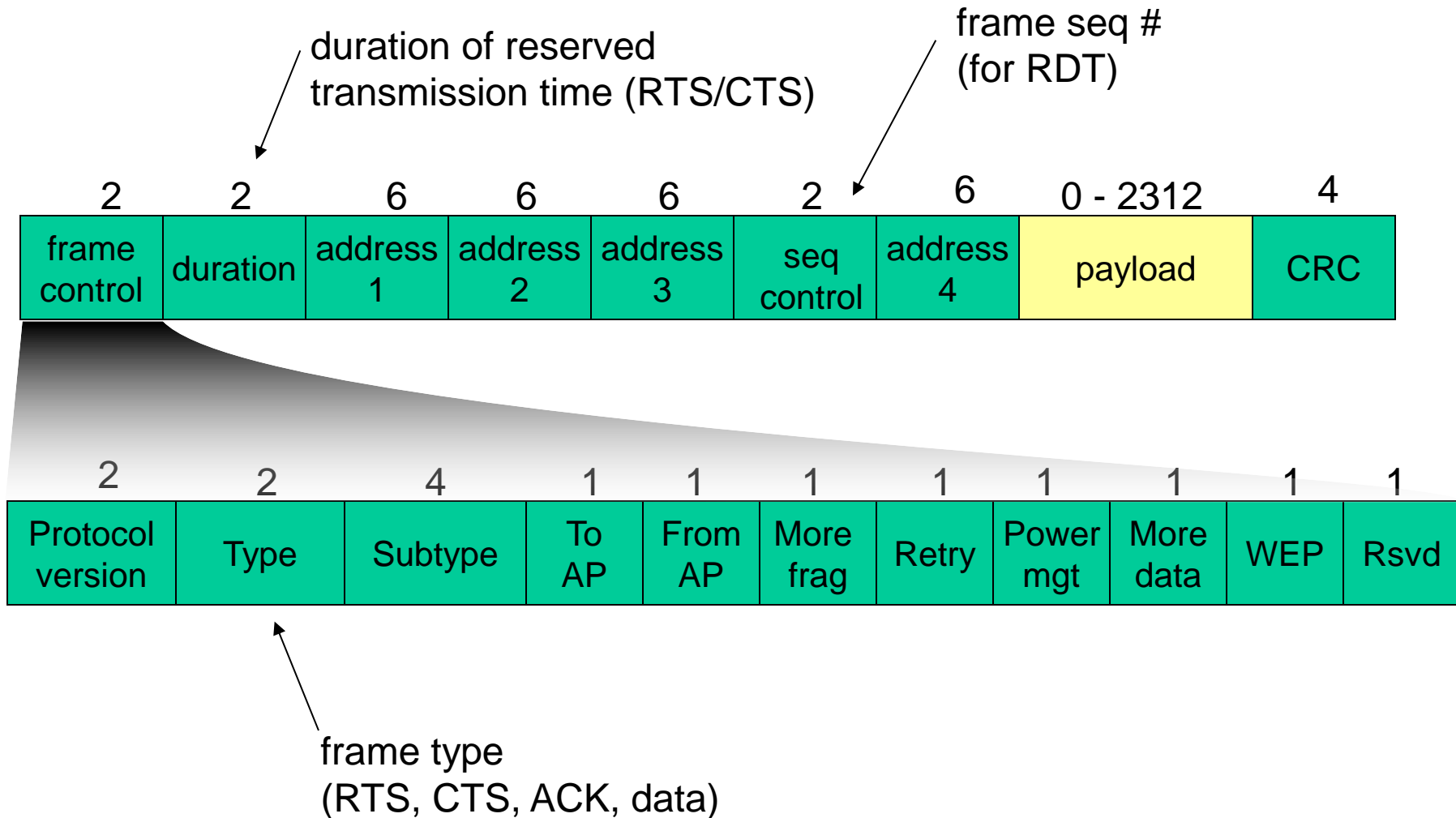
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing


Internet

H1

router

R1

R1 MAC addr	H1 MAC addr
dest. address	source address

Ethernet frame

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

802.**11** frame

802.11 frame: more

duration of reserved
transmission time (RTS/CTS)

frame seq #
(for RDT)

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)

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

BBS 1   H1   BBS 2
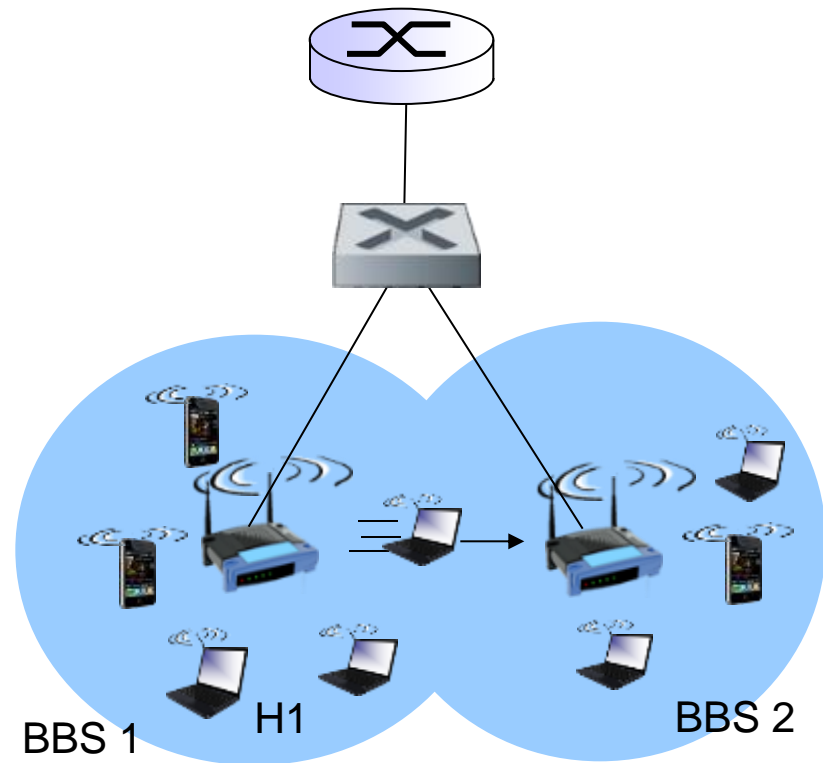
802.11: advanced capabilities

Rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies
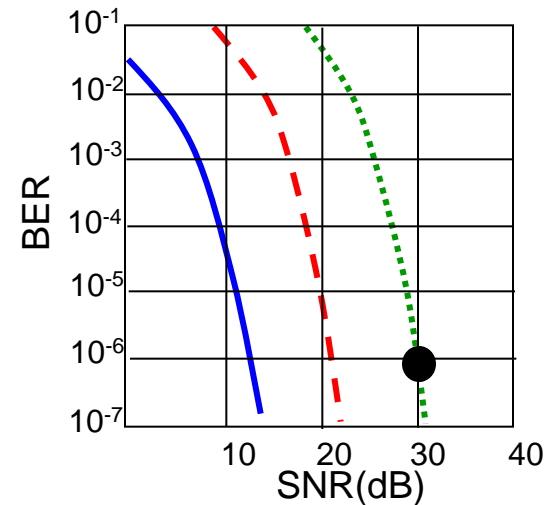
Legend:
- QAM256 (8 Mbps) — green dotted
- QAM16 (4 Mbps) — red dashed
- BPSK (1 Mbps) — blue solid
- ● operating point

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

radius of coverage
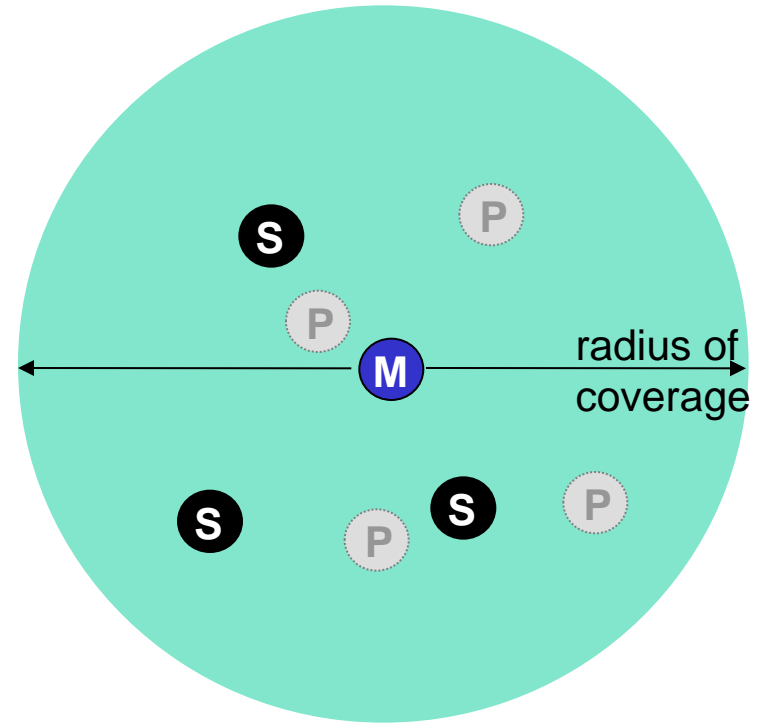
Ⓜ Master device

Ⓢ Slave device

Ⓟ Parked device (inactive)

Chapter 7 outline

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!)

Mobile Switching Center
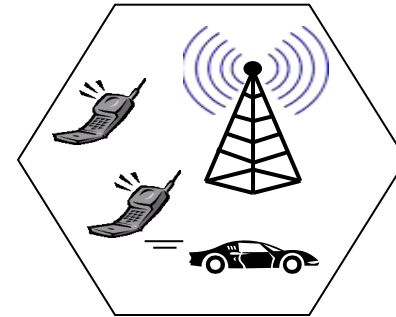
Mobile Switching Center

Public telephone network
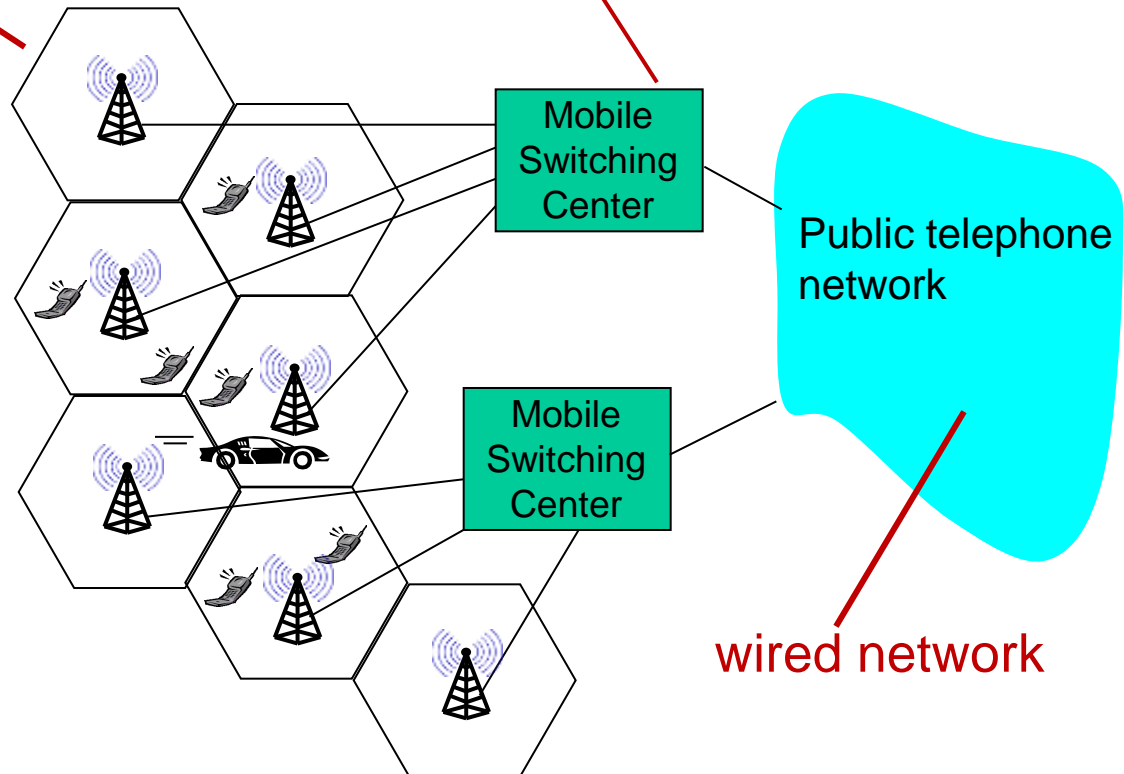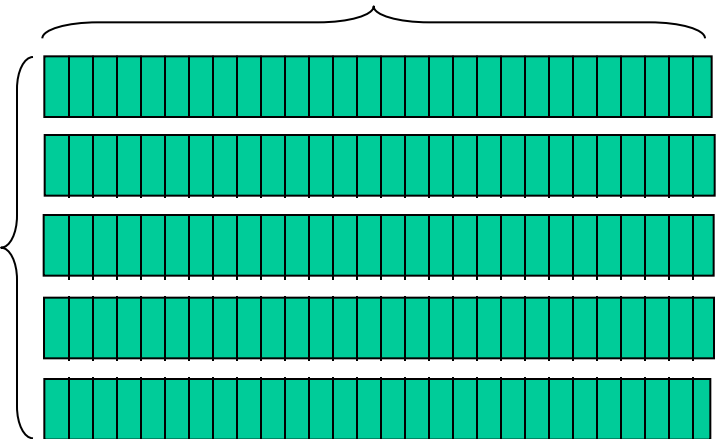
wired network

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
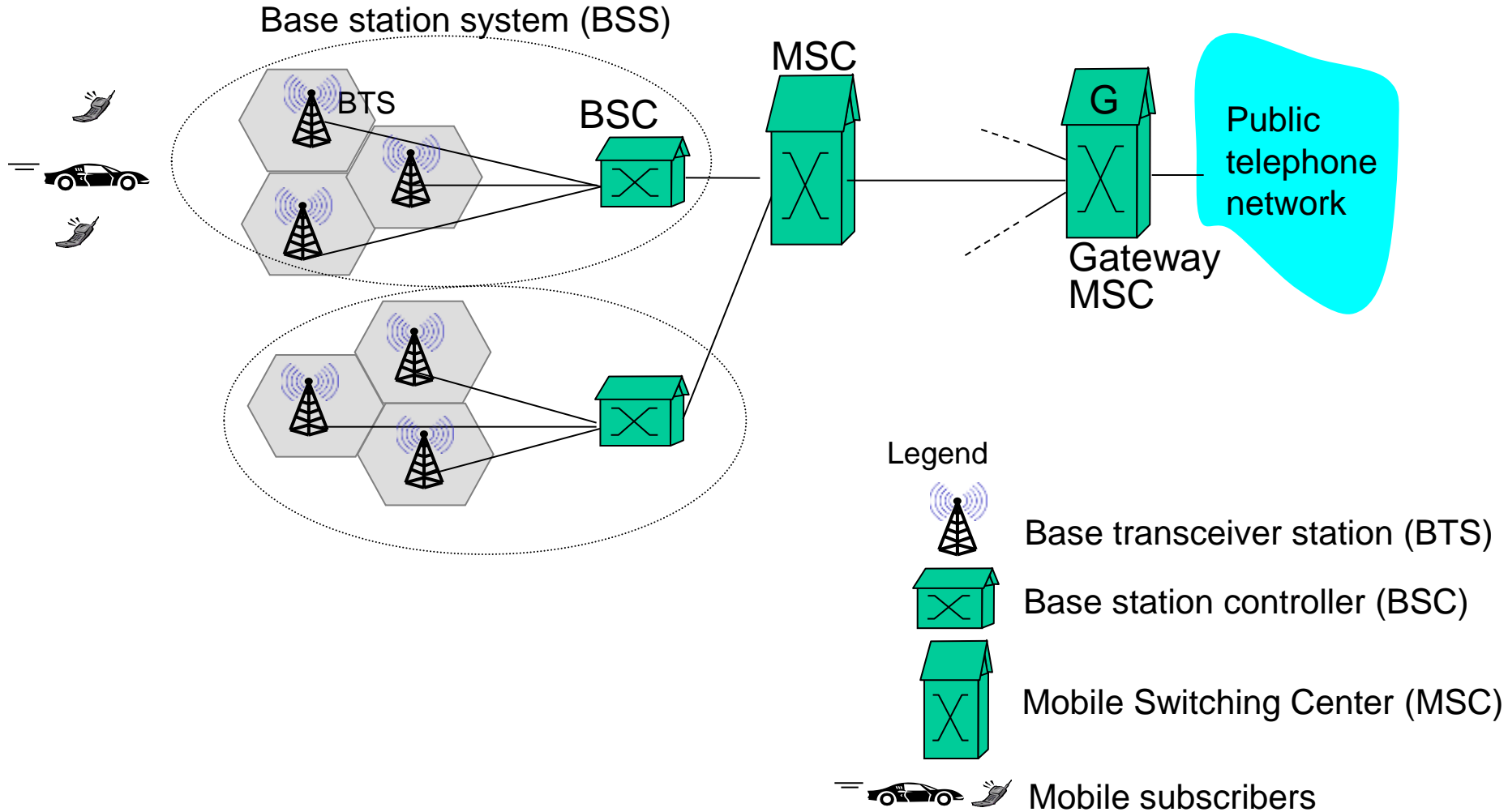
2G (voice) network architecture

Base station system (BSS)

BTS

BSC

MSC

G

Gateway
MSC

Public
telephone
network

Legend

Base transceiver station (BTS)

Base station controller (BSC)

Mobile Switching Center (MSC)

Mobile subscribers

3G (voice+data) network architecture

Key insight: new cellular data
network operates *in parallel*
(except at edge) with existing
cellular voice network

- voice network *unchanged* in core
- data network operates in parallel

Serving GPRS Support Node (SGSN)

Gateway GPRS Support Node (GGSN)

3G (voice+data) network architecture

MSC

G

Public telephone network

radio network controller

Gateway MSC

SGSN

G

Public Internet

GGSN

radio interface
(WCDMA, HSPA)

radio access network
Universal Terrestrial Radio
Access Network (UTRAN)

core network
General Packet Radio Service
(GPRS) Core Network

public Internet

3G versus 4G LTE network architecture

3G

MSC

radio network controller

Gateway MSC

Public telephone network

SGSN

GGSN

Public Internet

4G-LTE

HSS

MME

S-GW P-GW

G G

Public Internet

radio access network
Universal Terrestrial Radio
Access Network (UTRAN)

Evolved Packet Core
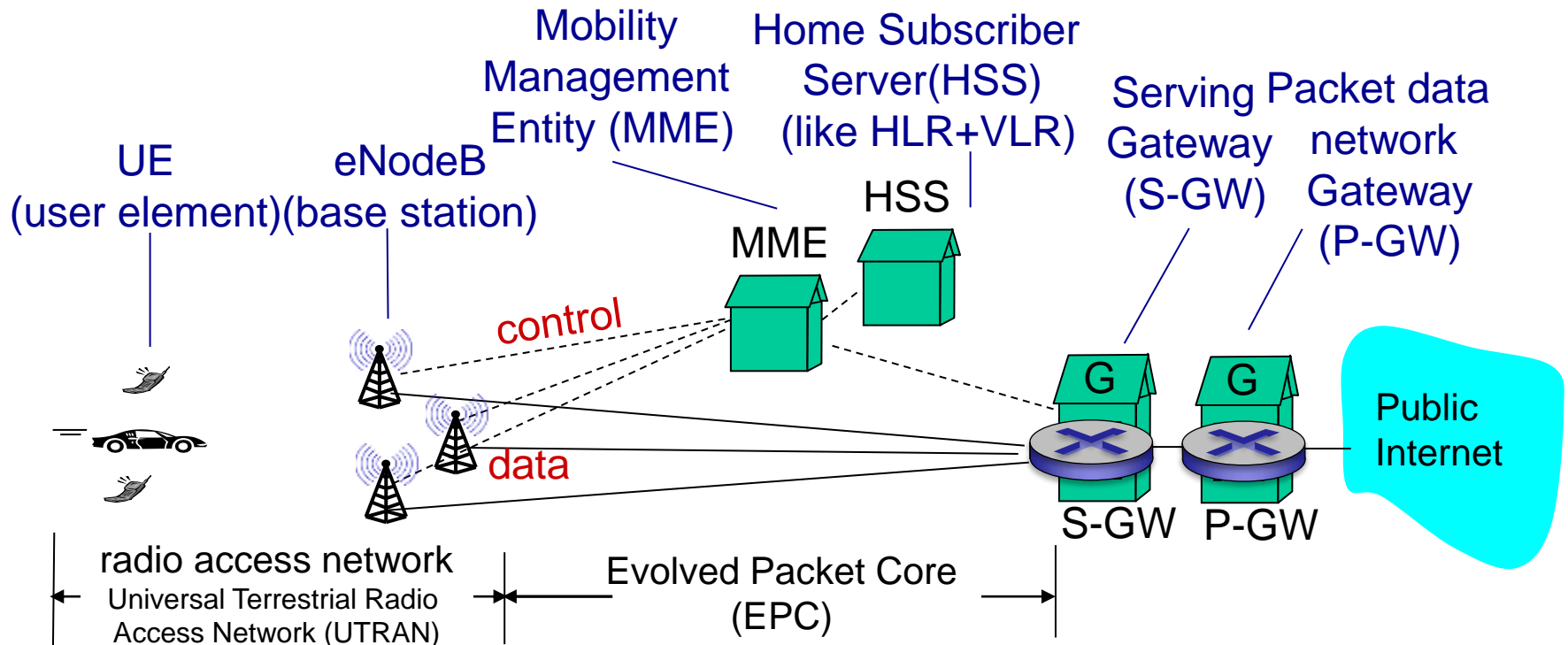(EPC)
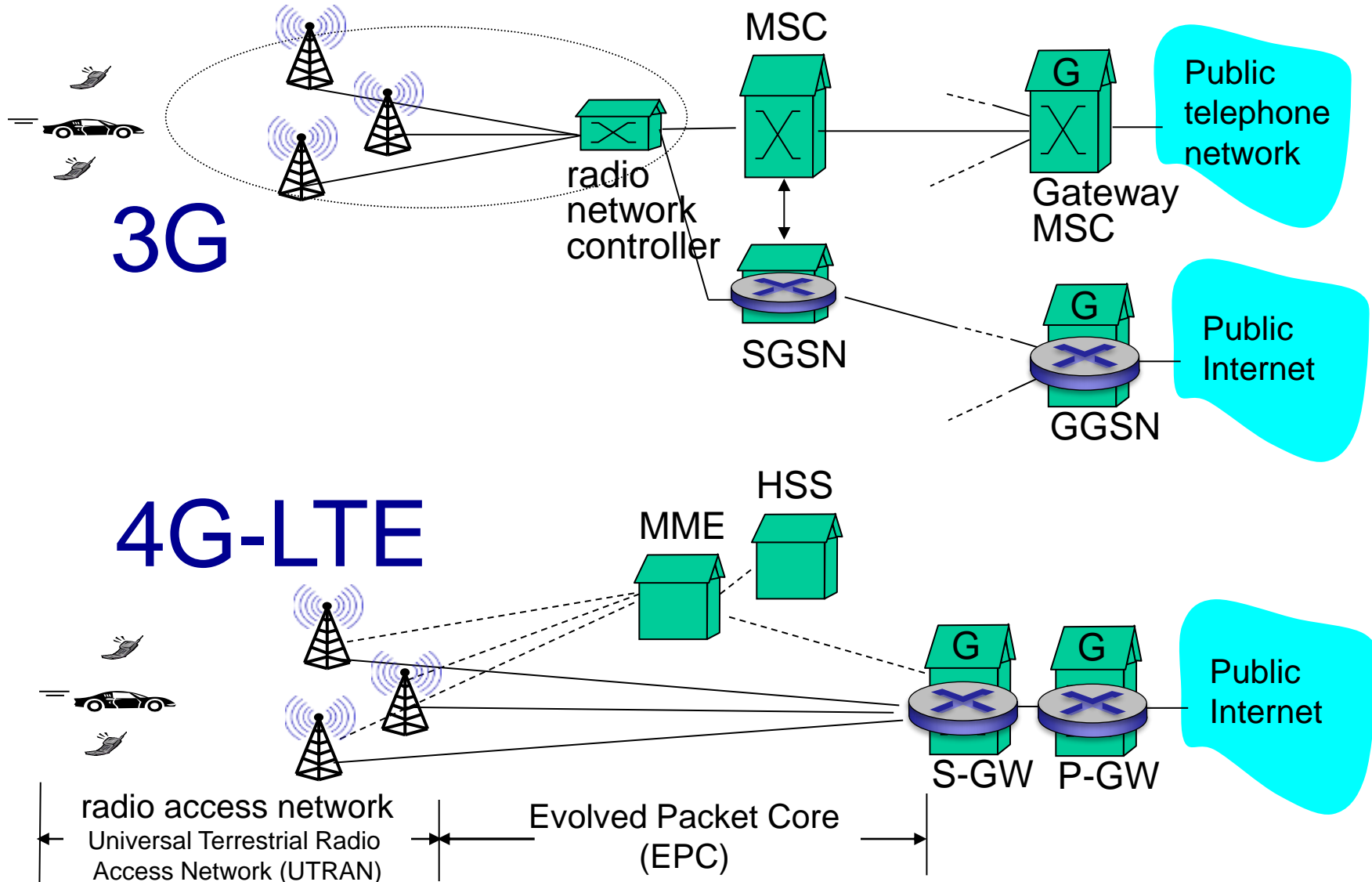
4G: differences from 3G

- 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

Chapter 7 outline

What is mobility?

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

no mobility   high mobility

mobile wireless user, using same access point

mobile user, connecting/ disconnecting from network using DHCP.

mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)
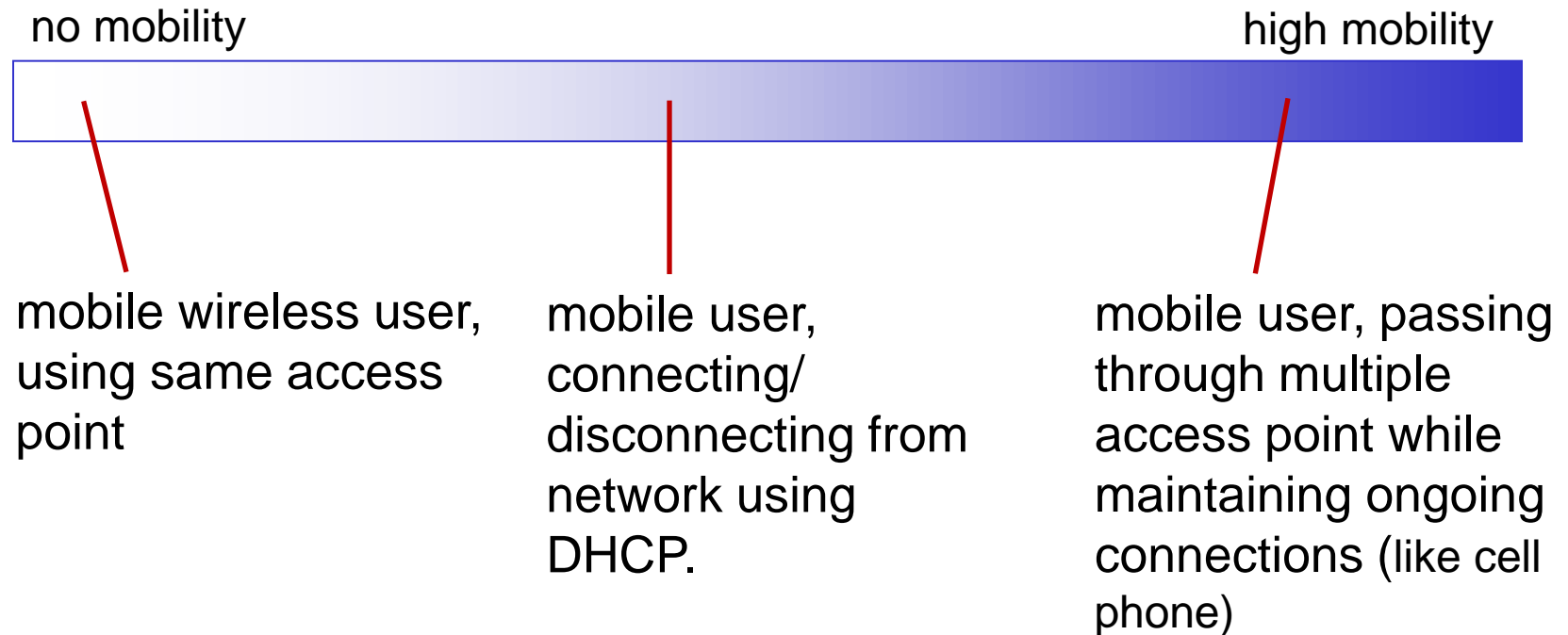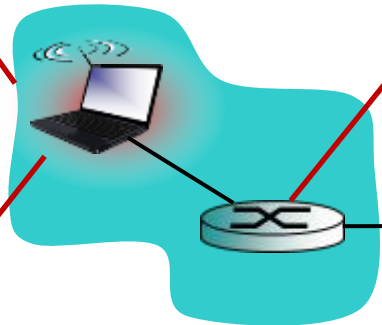
Mobility: vocabulary

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

wide area network

Mobility: more vocabulary

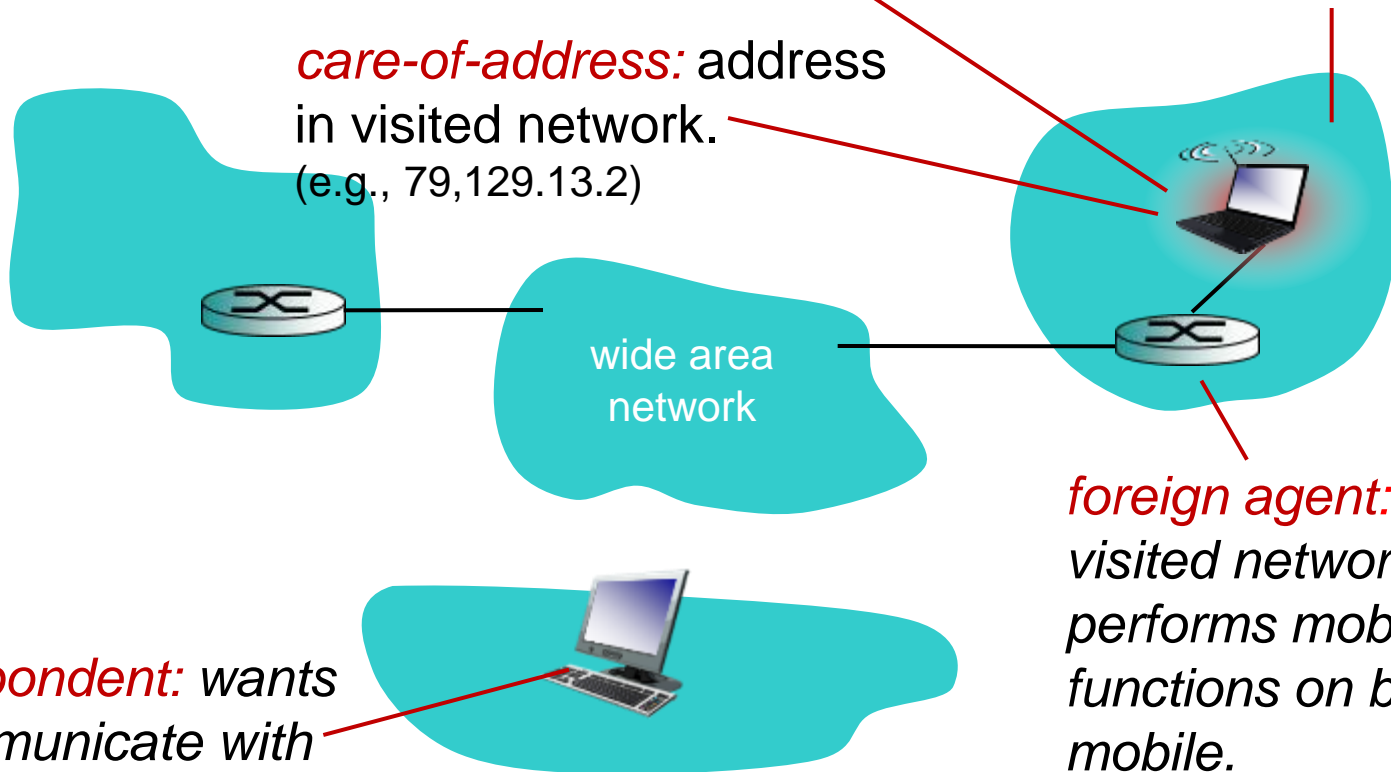**permanent address:** remains constant (e.g., 128.119.40.186)

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.
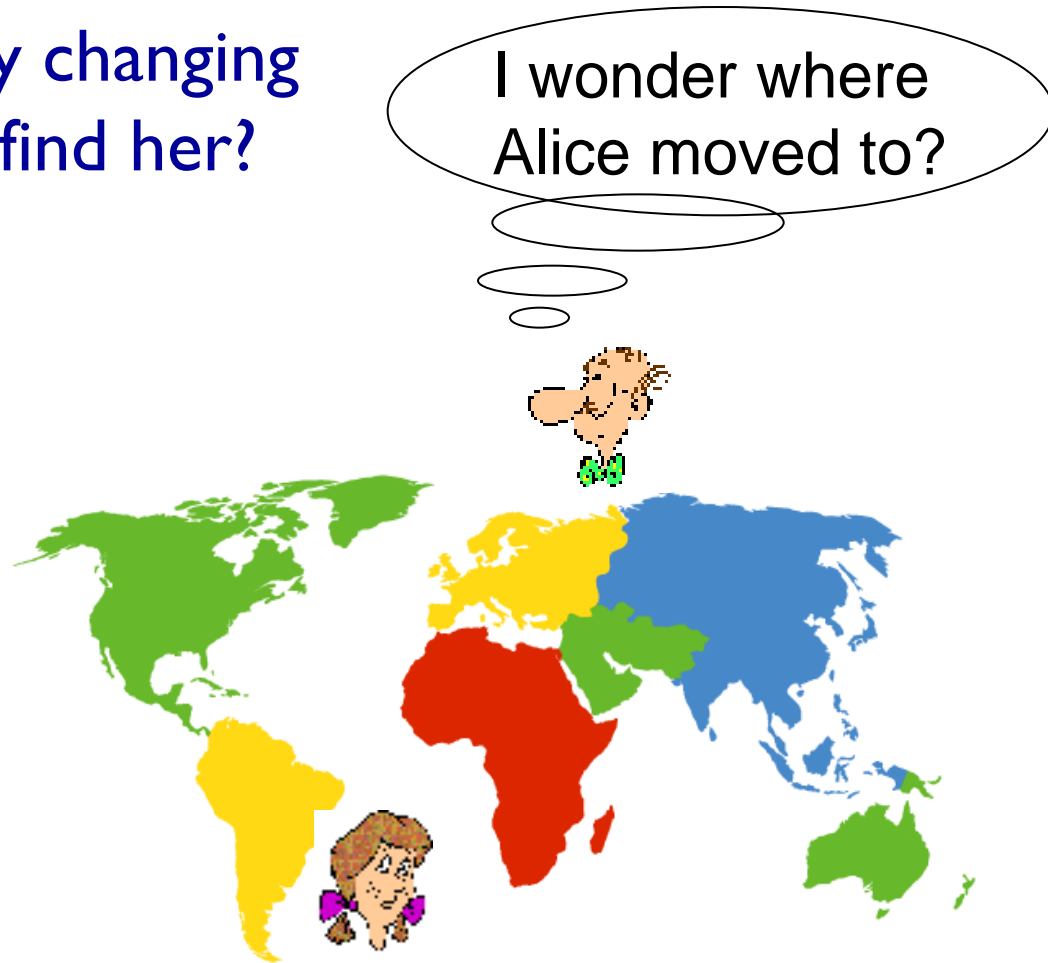
correspondent: wants to communicate with mobile

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!

I wonder where Alice moved to?
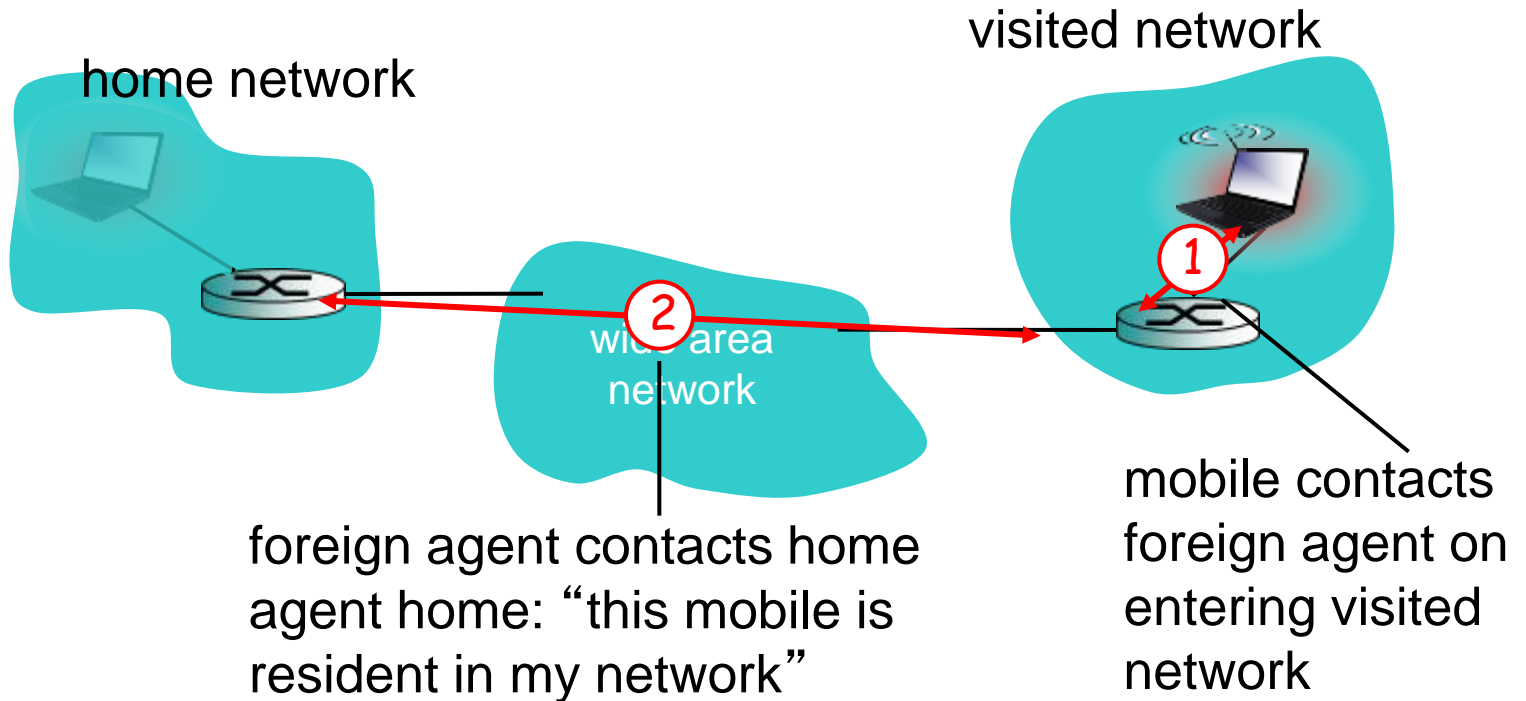
Mobility: approaches

- *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-node-in-residence via usual routing table ex
  - routing table ~~~~ere each mobile located
  - no changes to ~~~~ems

not scalable to millions of mobiles

- *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: registration

visited network

home network

(1)

(2)

wide area network

foreign agent contacts home agent home: "this mobile is resident in my network"

mobile contacts foreign agent on entering visited network
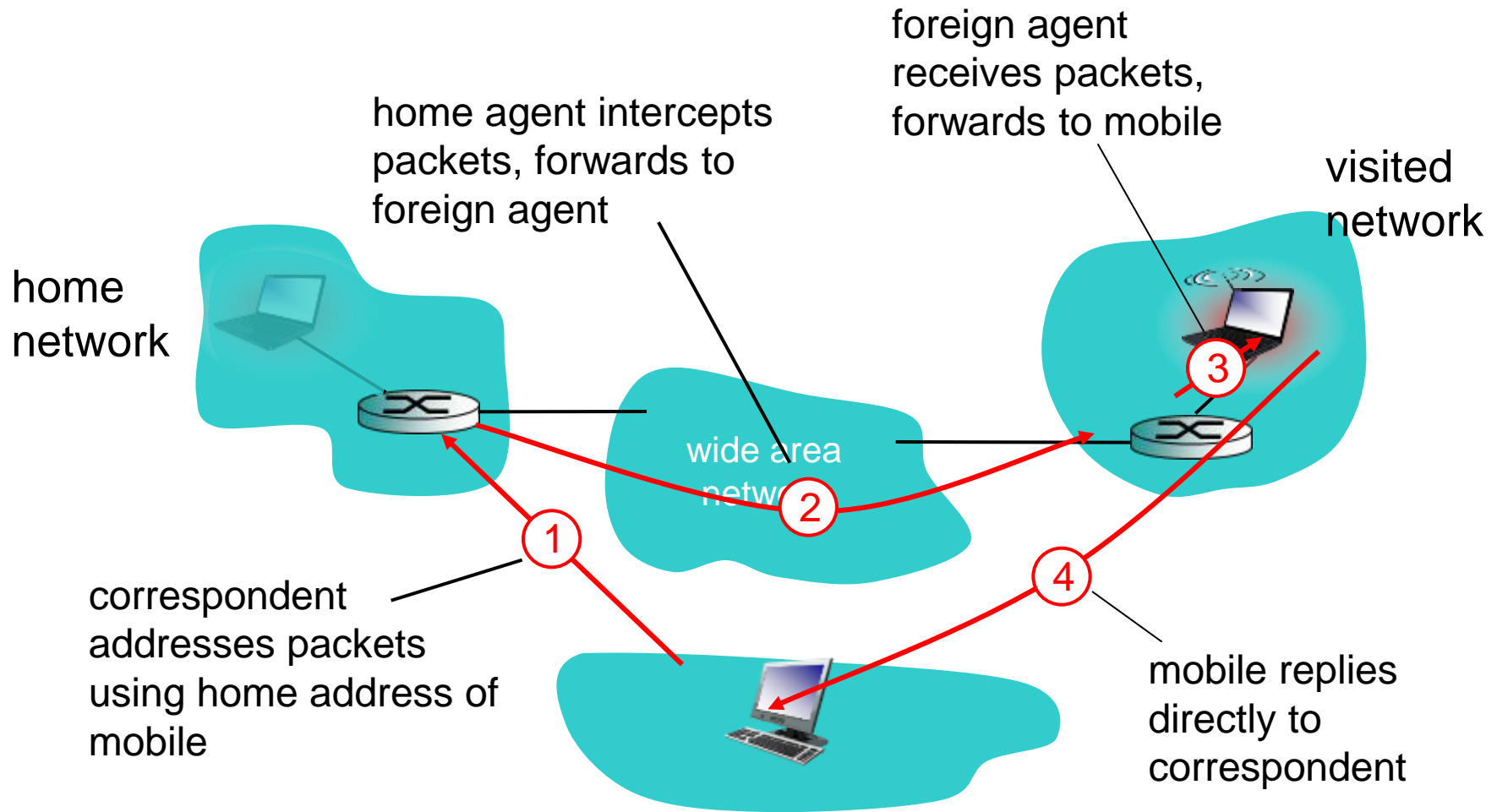
end result:
- foreign agent knows about mobile
- home agent knows location of mobile

Mobility via indirect routing

foreign agent
receives packets,
forwards to mobile

visited
network

home agent intercepts
packets, forwards to
foreign agent

home
network

wide area
network

correspondent
addresses packets
using home address of
mobile

mobile replies
directly to
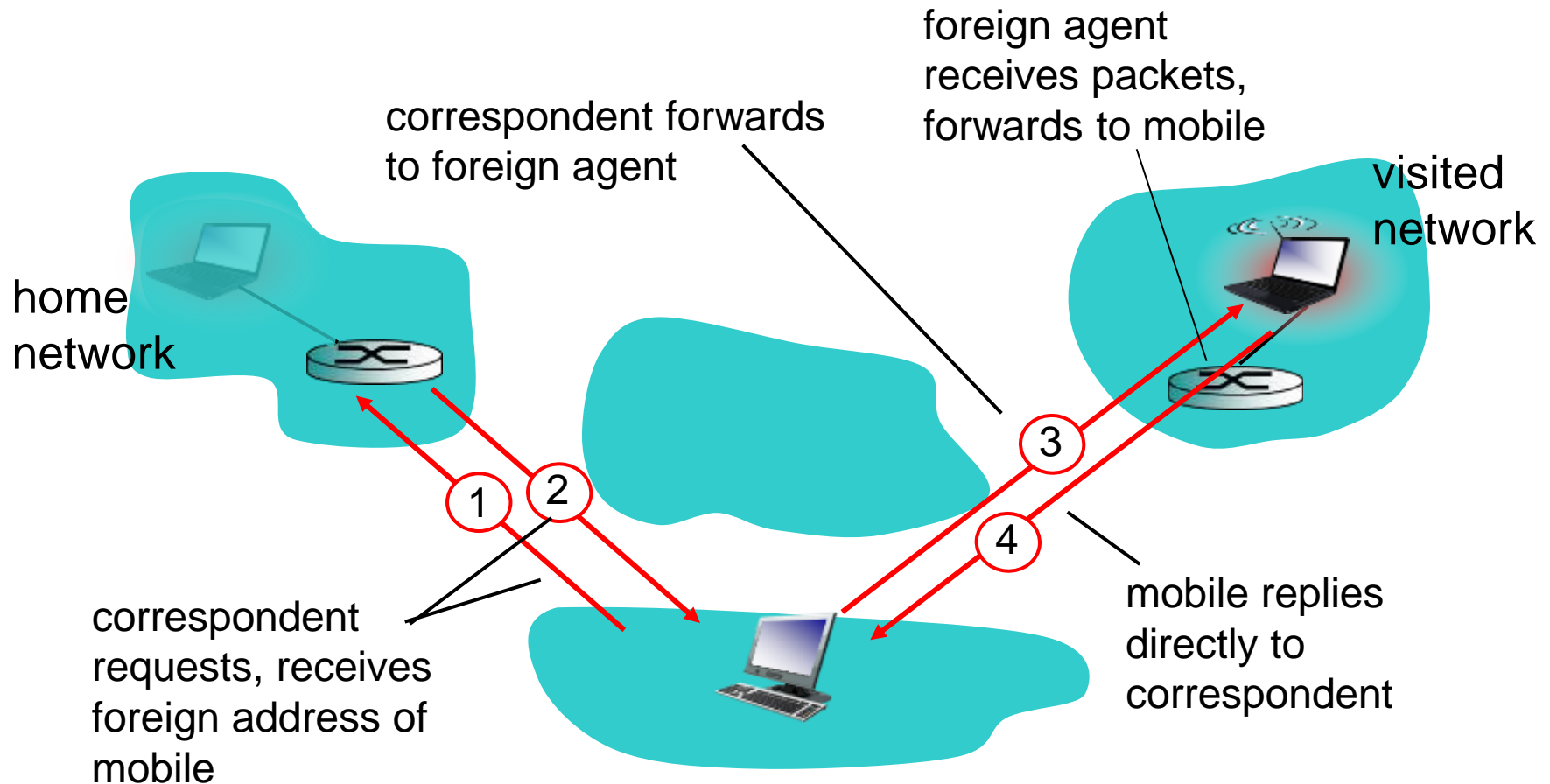correspondent

1

2

3

4

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
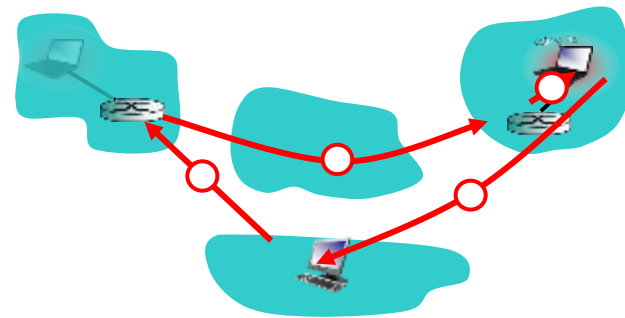
# Indirect routing: moving between networks

- 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

correspondent forwards to foreign agent

foreign agent receives packets, forwards to mobile

visited network

home network

1

2

3

4

correspondent requests, receives foreign address of mobile

mobile replies directly to correspondent

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?
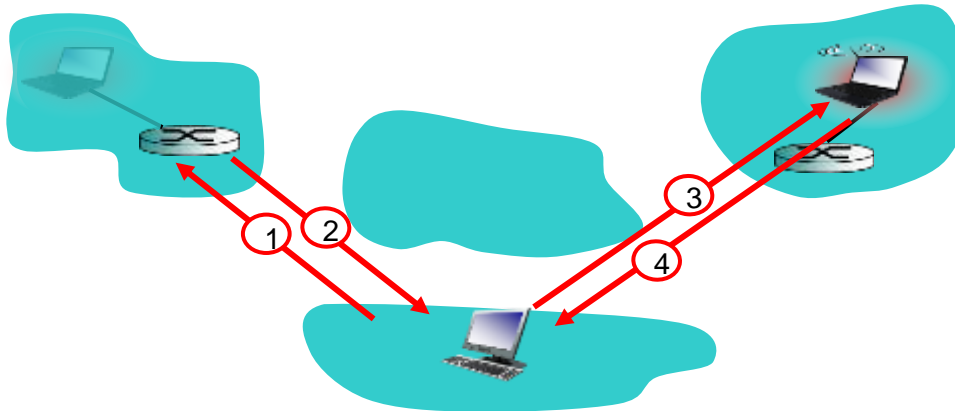
Accommodating mobility with direct routing

- 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)
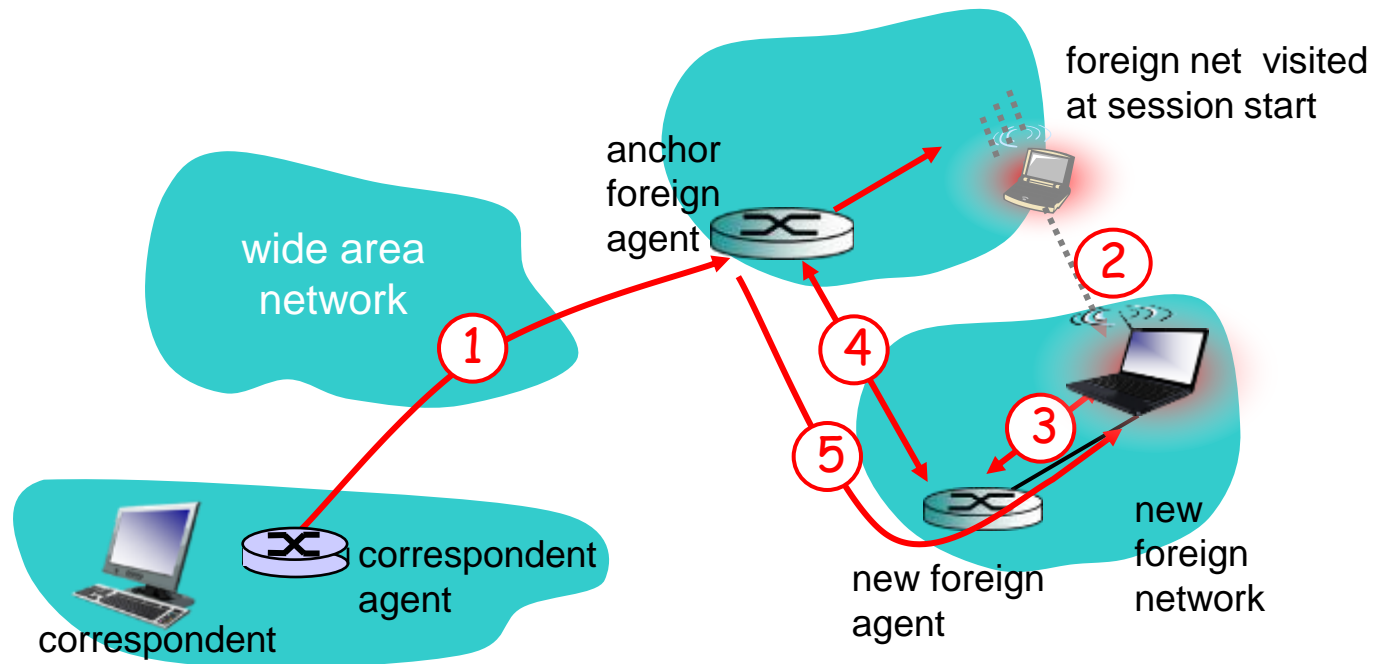
Chapter 7 summary

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