Logistics
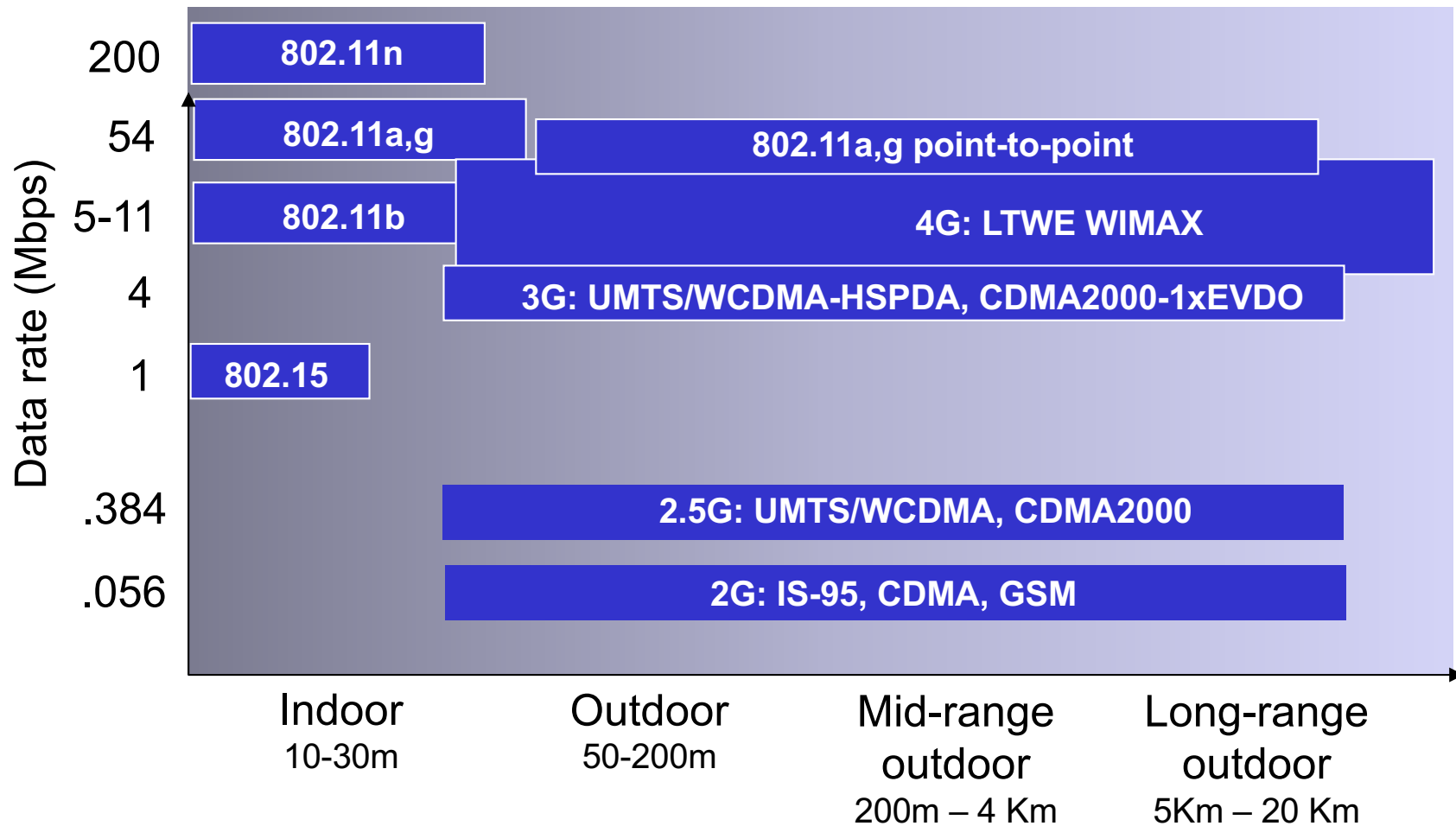
❖ Reading: Chapter on Wireless Networks

  ▪ Homework coming Weds

  ▪ Programming assignment Weds

❖ Wireshark Labs due!

❖ Today:

  ▪ Wireless -> Security

Characteristics of selected wireless links

Data rate (Mbps)

200	802.11n		
54	802.11a,g	802.11a,g point-to-point	
5-11	802.11b	4G: LTWE WIMAX	
4	3G: UMTS/WCDMA-HSPDA, CDMA2000-1xEVDO		
1	802.15		
.384	2.5G: UMTS/WCDMA, CDMA2000		
.056	2G: IS-95, CDMA, GSM		

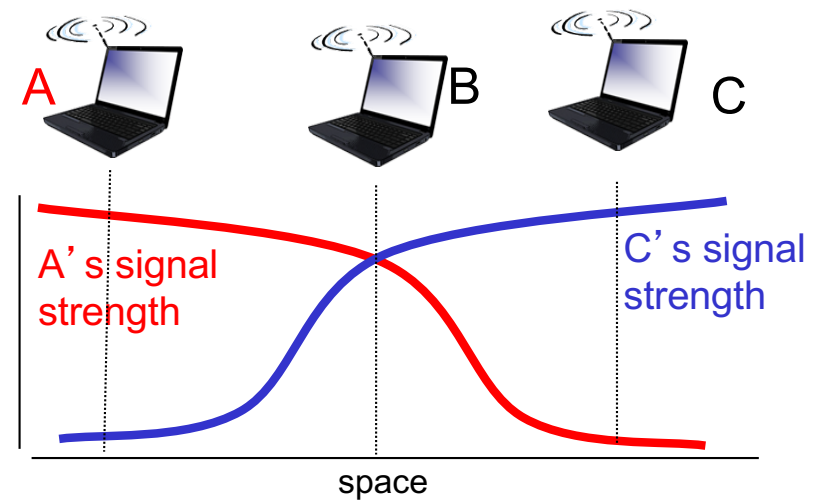| Indoor	Outdoor	Mid-range outdoor	Long-range outdoor
10-30m	50-200m	200m – 4 Km	5Km – 20 Km

Wireless network characteristics

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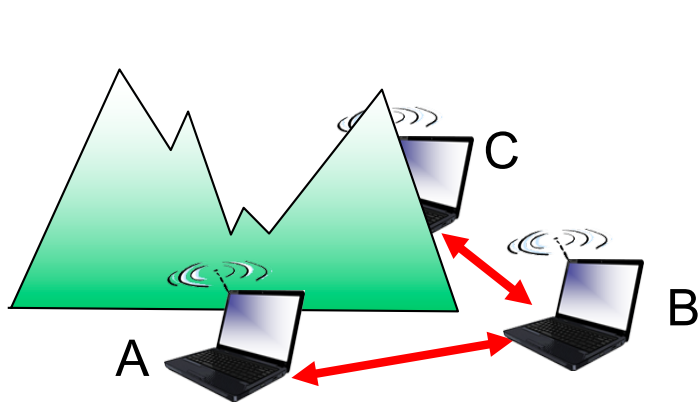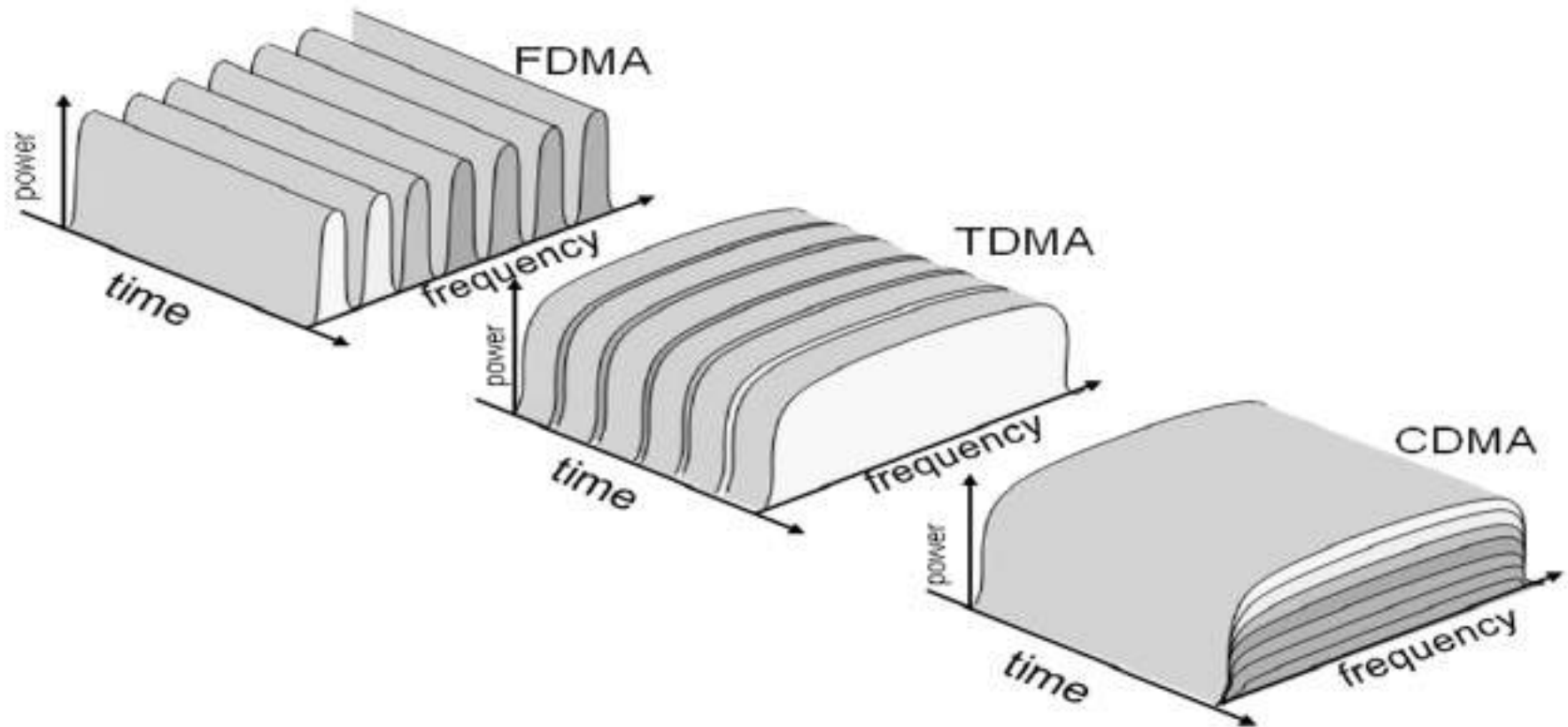

Hidden terminal problem

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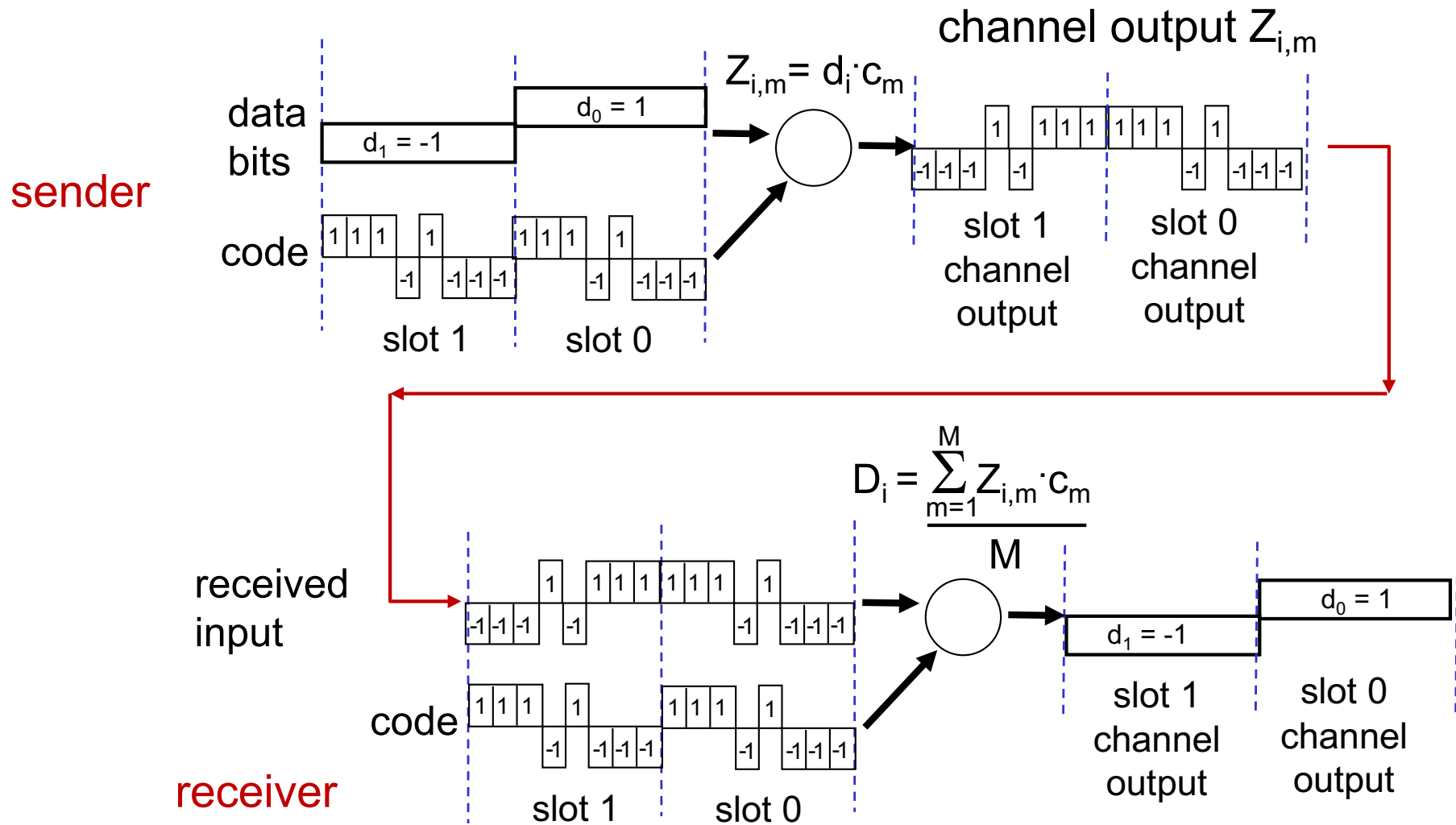- ❖ A, C can not hear each other interfering at B

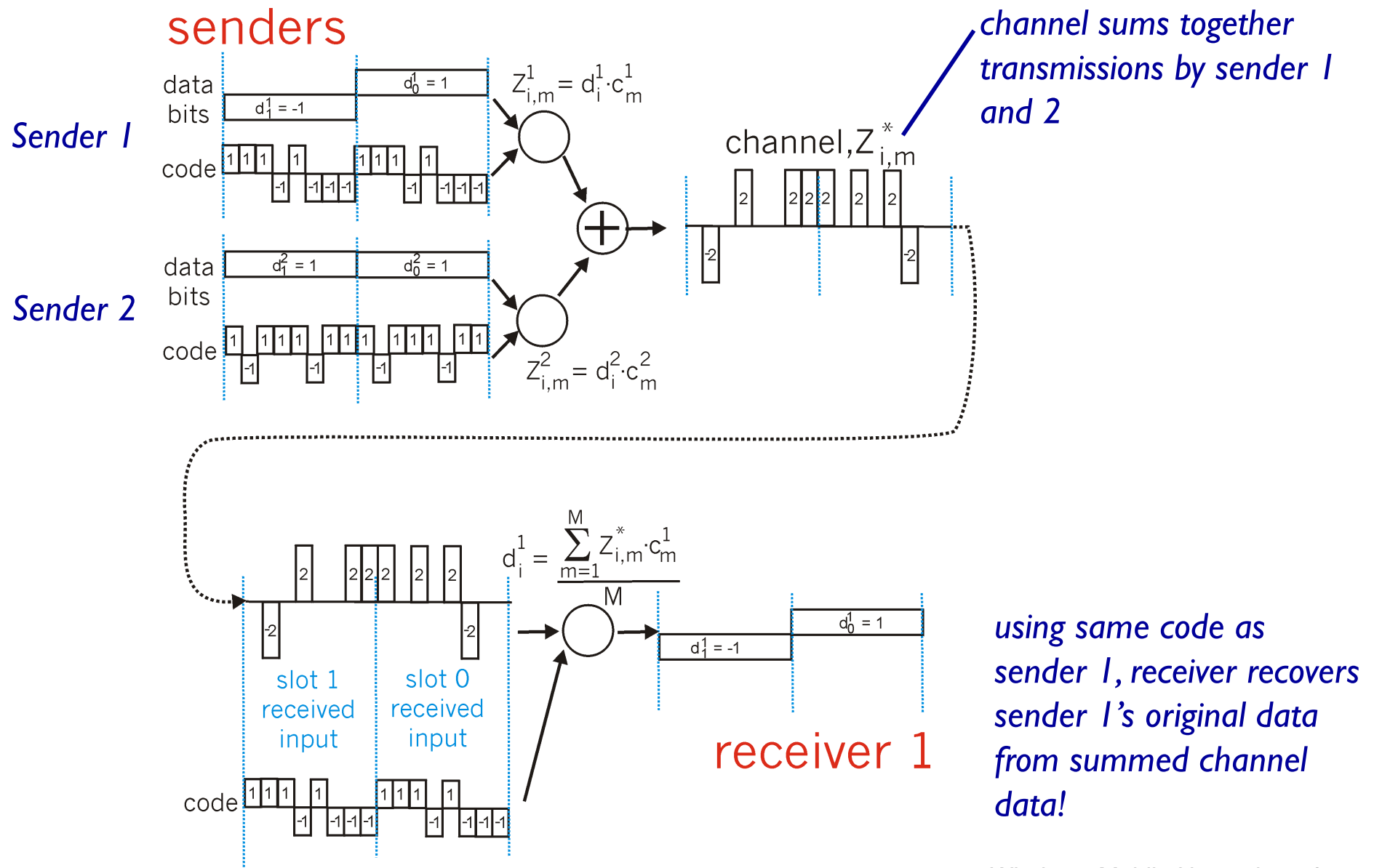# Code Division Multiple Access (CDMA)

Code Division Multiple Access (CDMA)

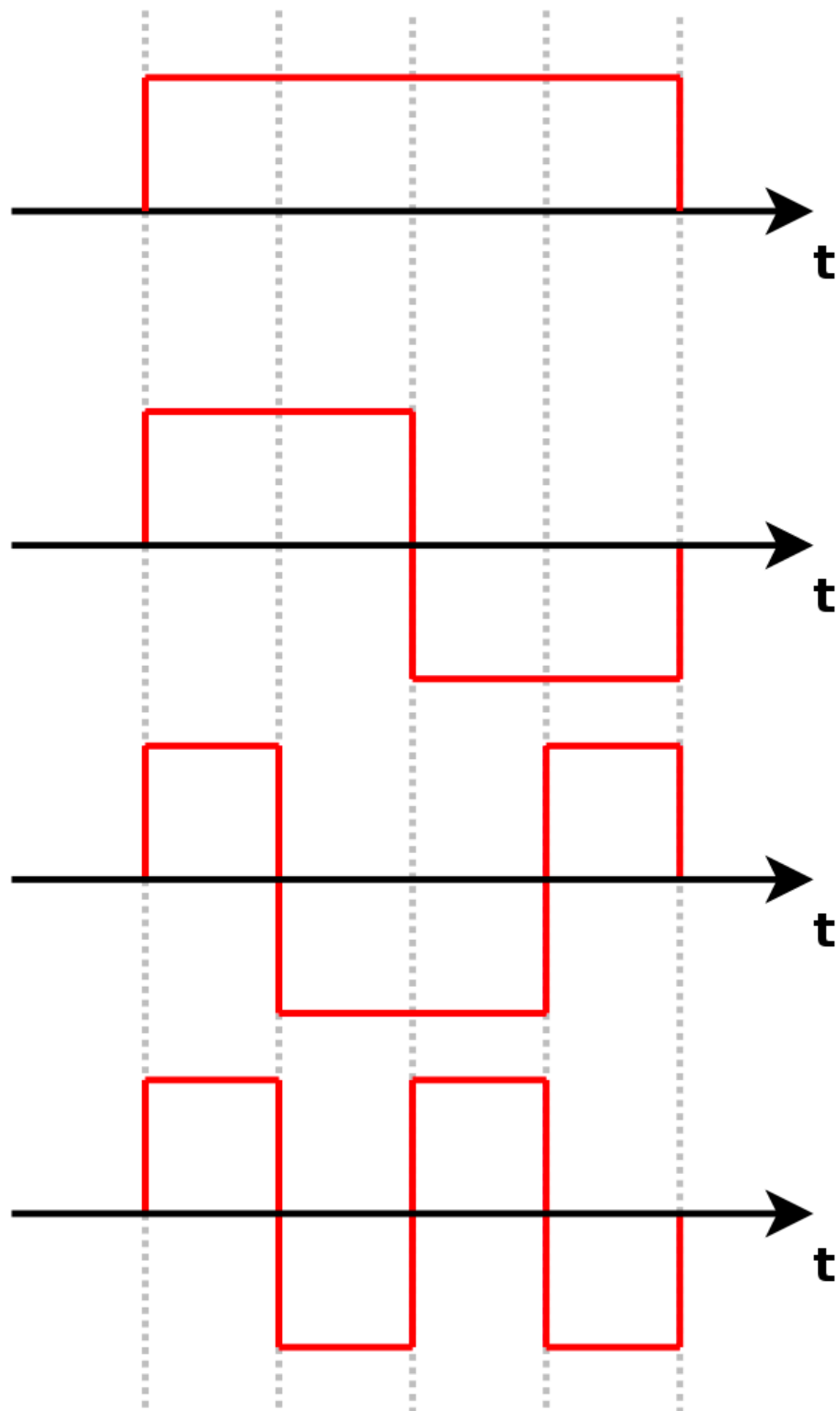❖ unique "code" assigned to each user; i.e., code set partitioning
  ▪ all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data
  ▪ allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")

❖ *encoded signal* = (original data) X (chipping sequence)

❖ *decoding:* inner-product of encoded signal and chipping sequence

CDMA encode/decode

channel output $Z_{i,m}$

sender

data bits

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

$d_0 = 1$

$d_1 = -1$

code

1	1	1		1				1	1	1		1
			-1		-1	-1	-1				-1	

slot 1   slot 0

slot 1 channel output   slot 0 channel output

receiver

received input

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

code

slot 1   slot 0

$d_0 = 1$

$d_1 = -1$

slot 1 channel output   slot 0 channel output

CDMA: two-sender interference

senders

Sender 1

data bits $d_1^1 = -1$ $d_0^1 = 1$

$Z_{i,m}^1 = d_i^1 \cdot c_m^1$

code

Sender 2

data bits $d_1^2 = 1$ $d_0^2 = 1$

code

$Z_{i,m}^2 = d_i^2 \cdot c_m^2$

channel, $Z_{i,m}^*$

channel sums together transmissions by sender 1 and 2

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

slot 1 received input

slot 0 received input

$d_1^1 = -1$ $d_0^1 = 1$

receiver 1

code

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

Chapter 6 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
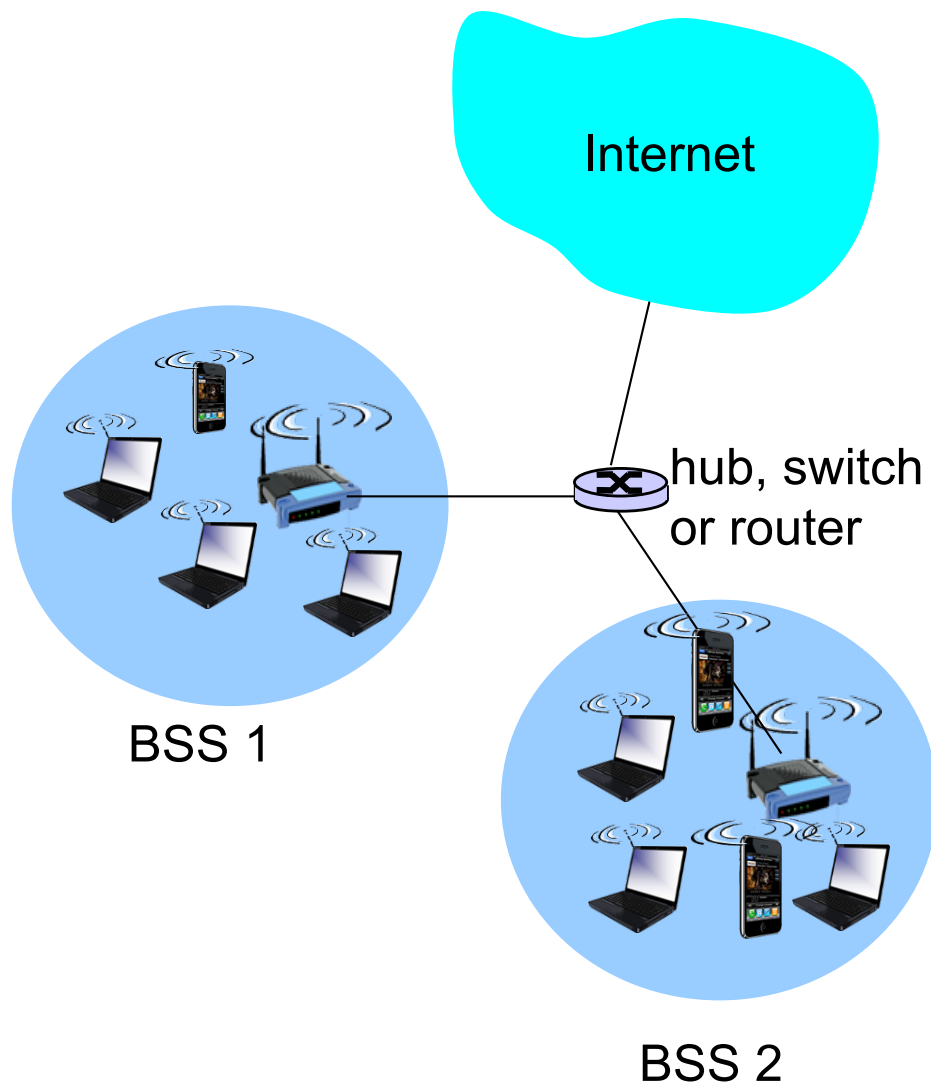
- ▪ 5-6 GHz range
- ▪ up to 54 Mbps

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
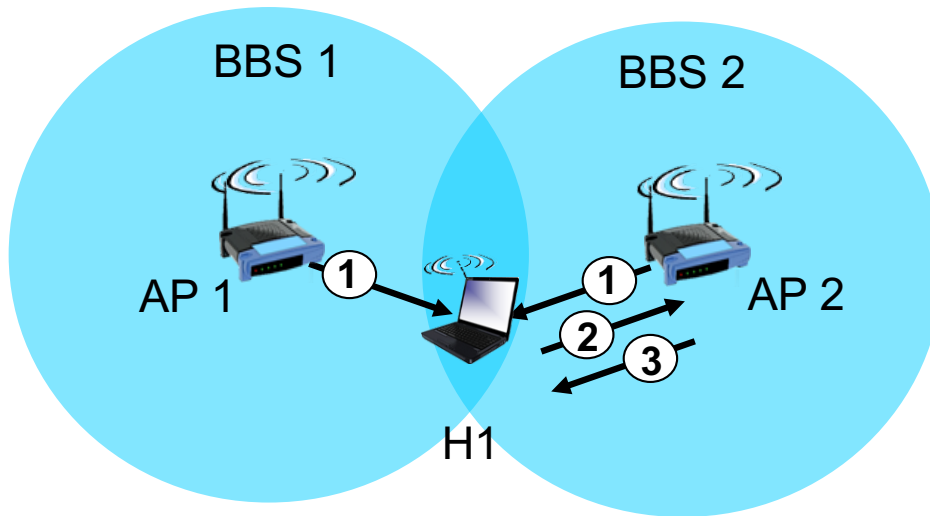
passive scanning:

(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
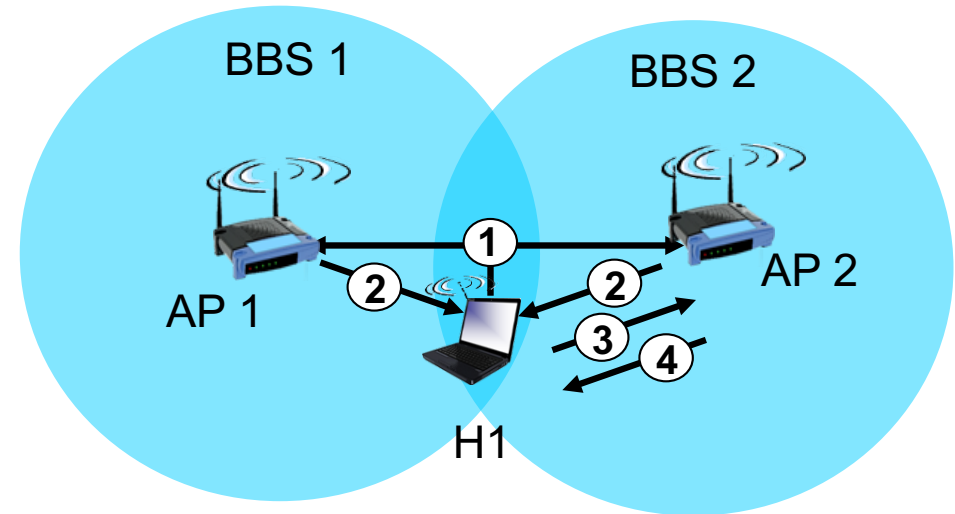
active scanning:

(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)

A's signal strength

C's signal strength

space
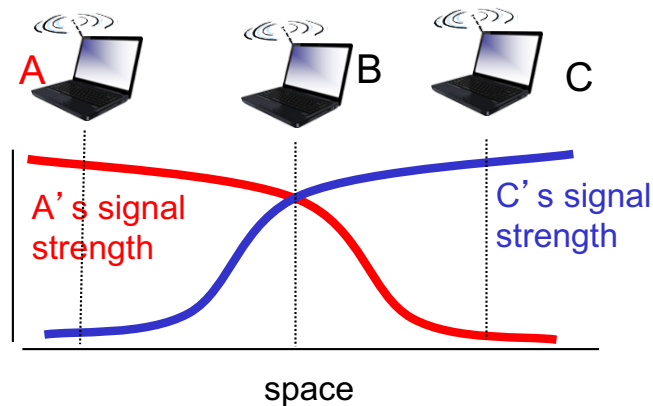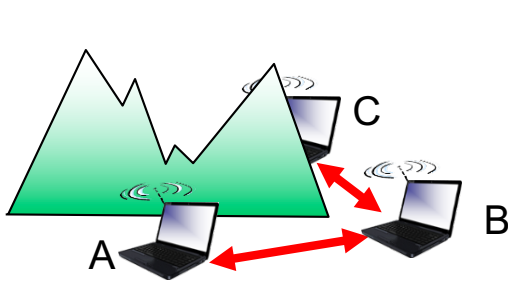
IEEE 802.11 MAC Protocol: CSMA/CA

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
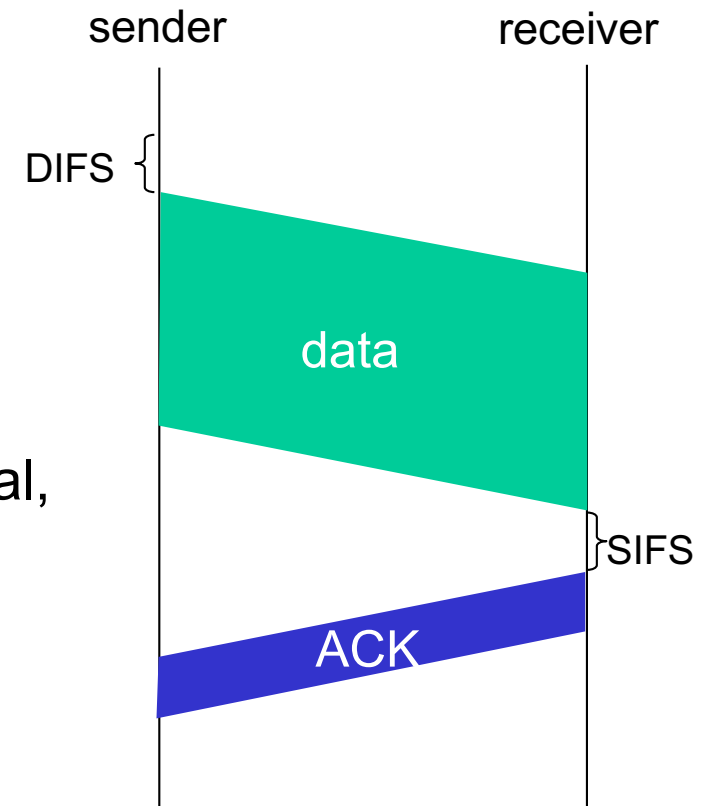
Avoiding collisions (more)

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

A   AP   B

RTS(A)   reservation collision   RTS(B)

RTS(A)

CTS(A)   CTS(A)

DATA (A)   defer

time

ACK(A)   ACK(A)

802.11 frame: addressing

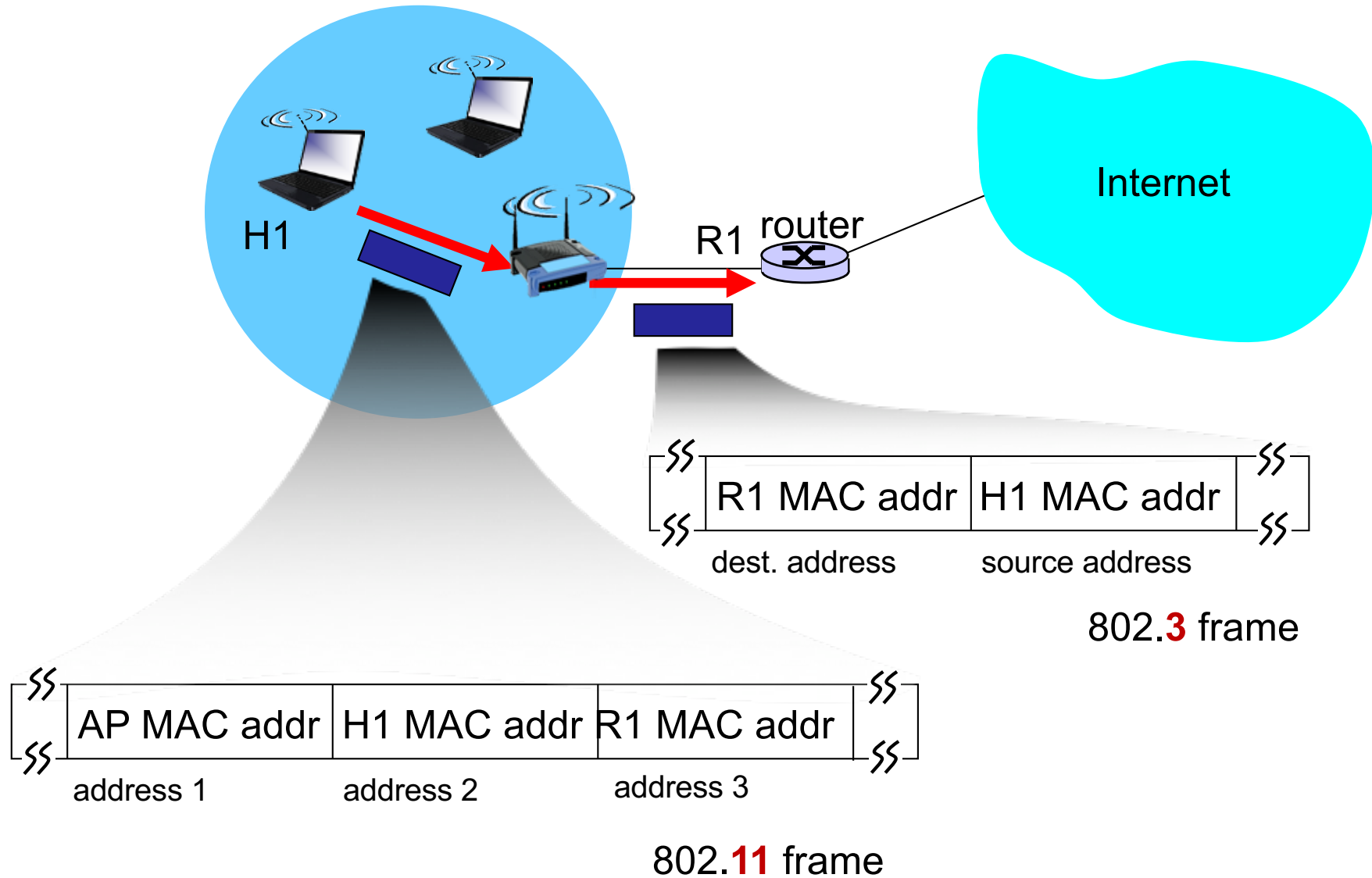| 2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC
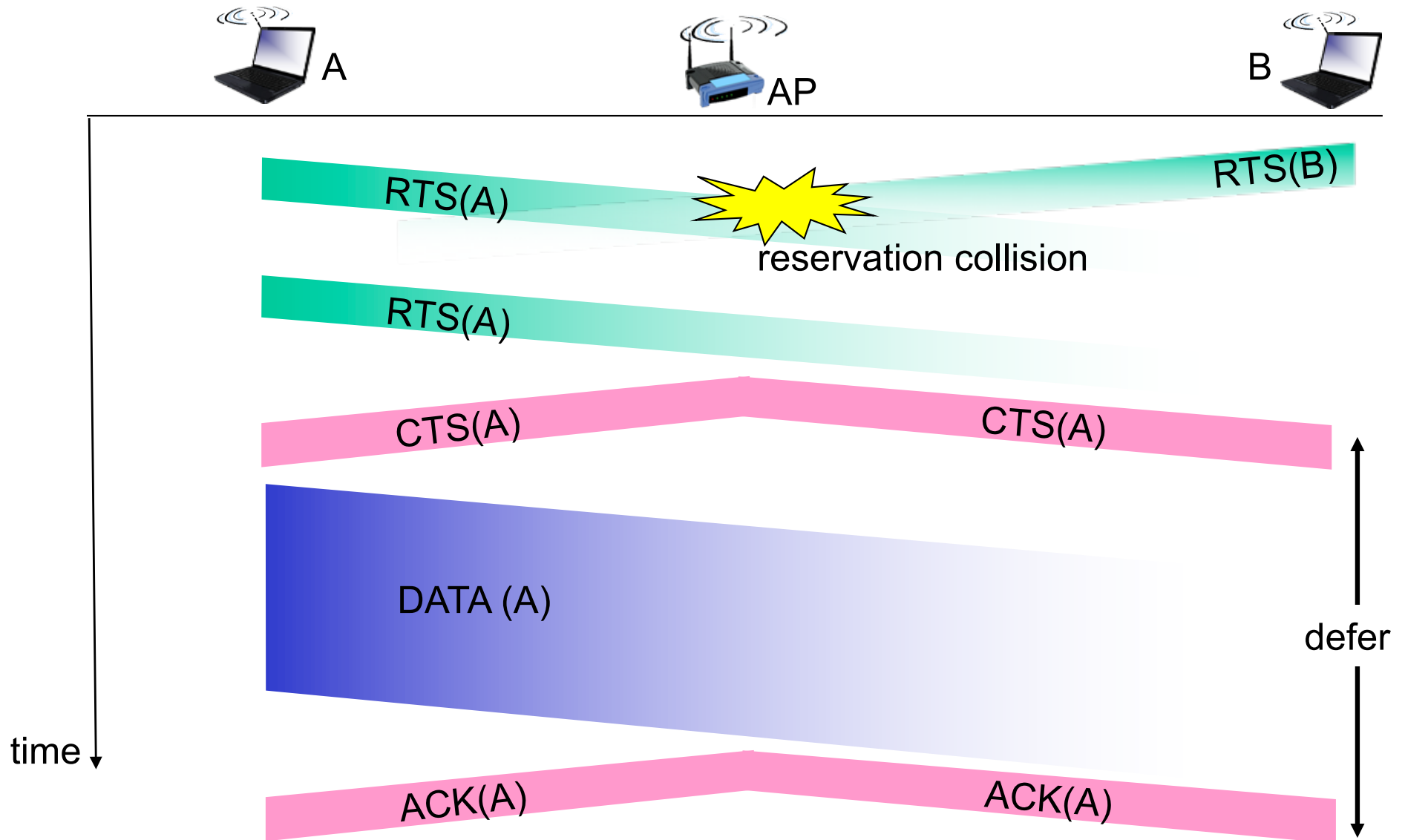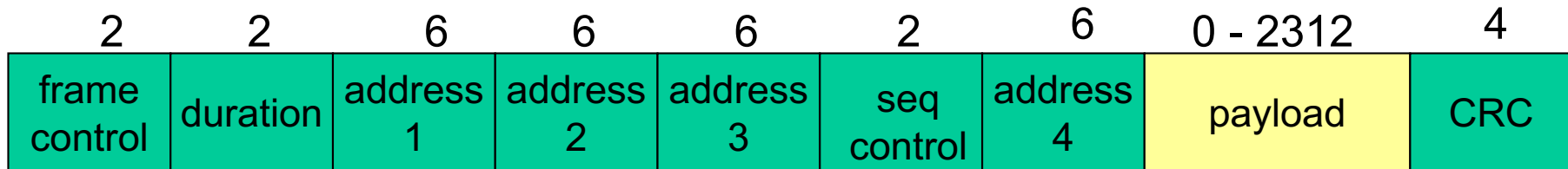
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame
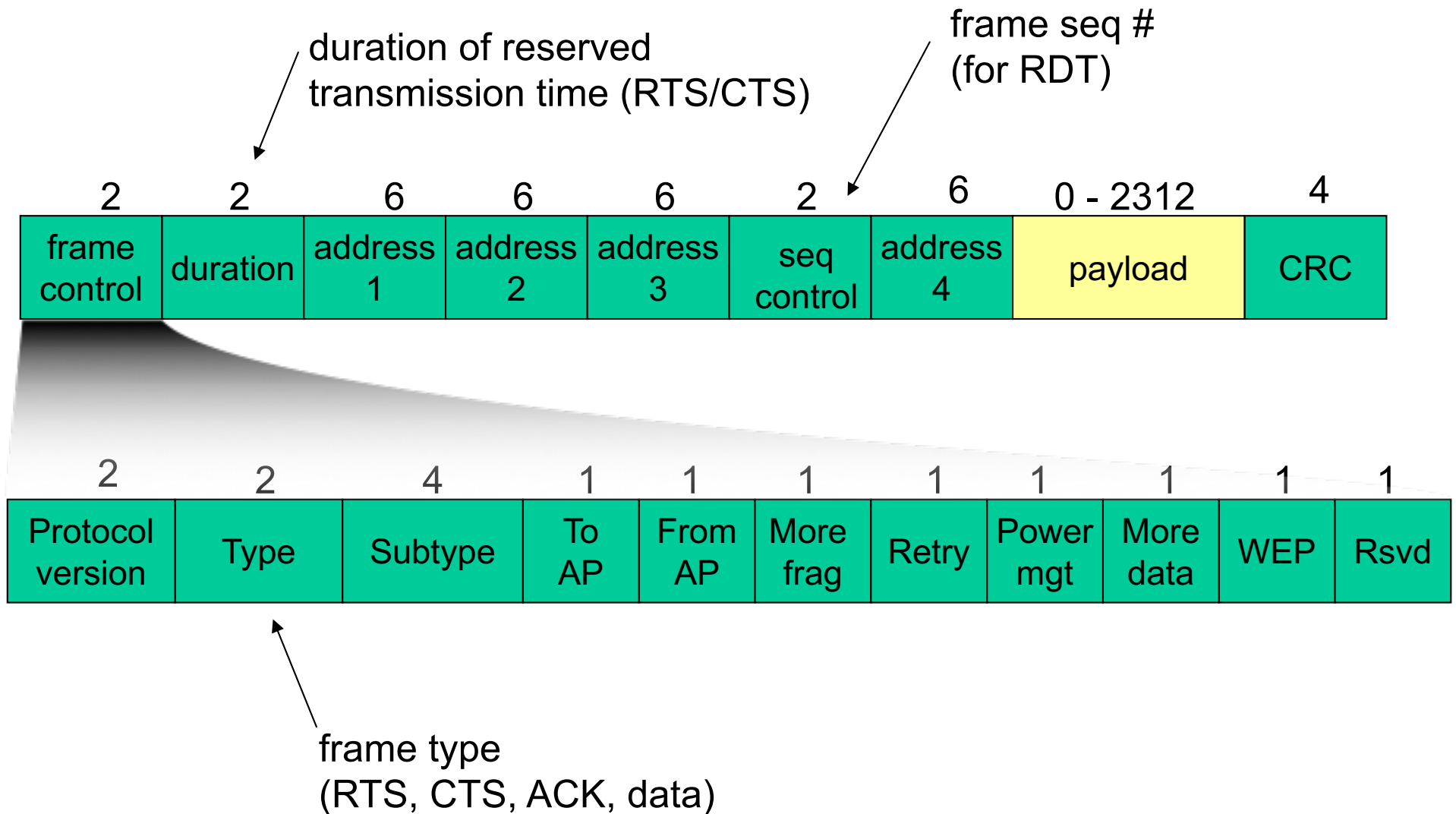
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing

Internet

H1

R1   router

R1 MAC addr	H1 MAC addr
dest. address	source address

802.**3** 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)
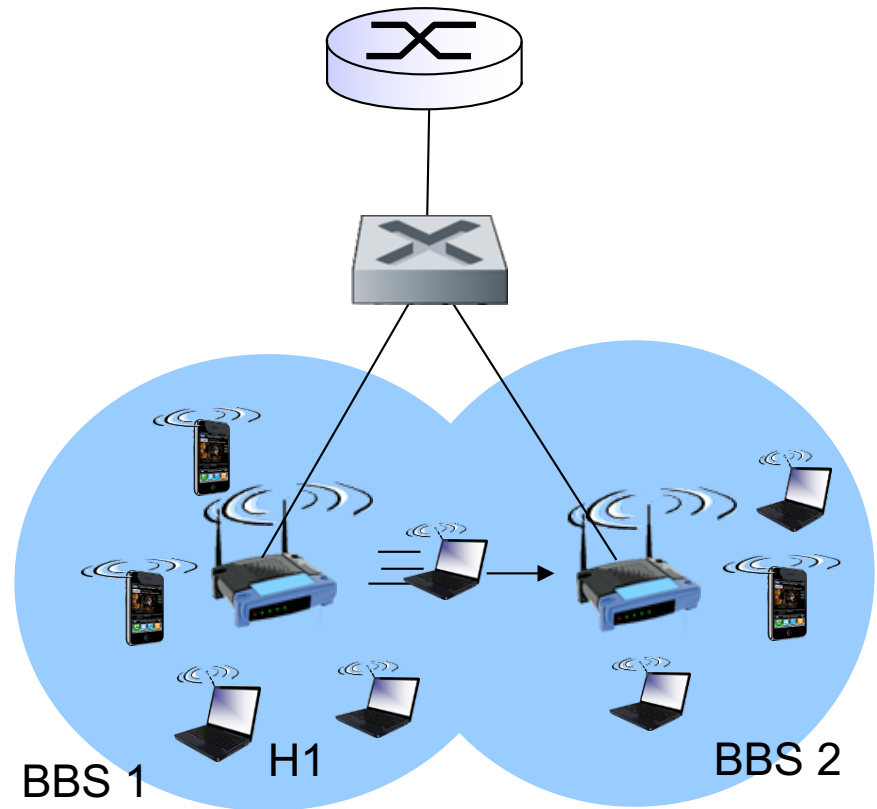
802.11: mobility within same subnet

❖ 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


```
········· QAM256 (8 Mbps)
— — —  QAM16 (4 Mbps)
————   BPSK (1 Mbps)
●        operating point
```
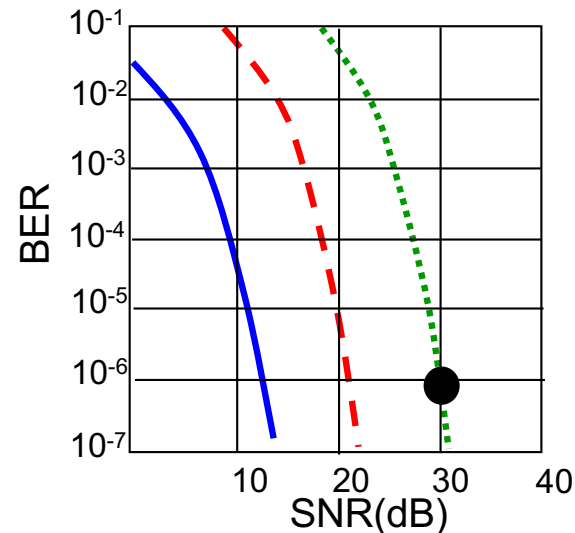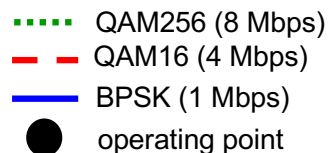
1. SNR decreases, BER increase as node moves away from base station

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

radius of coverage
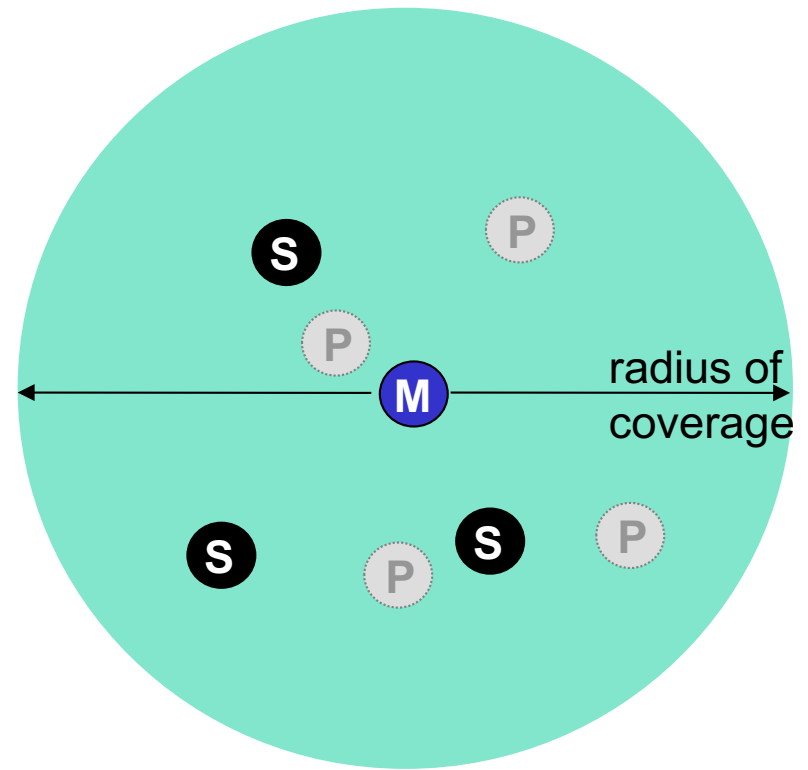
Ⓜ Master device

Ⓢ Slave device

Ⓟ Parked device (inactive)

Chapter 6 outline

Components of cellular network architecture

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

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

Mobile Switching Center

Mobile Switching Center

Public telephone network

wired network
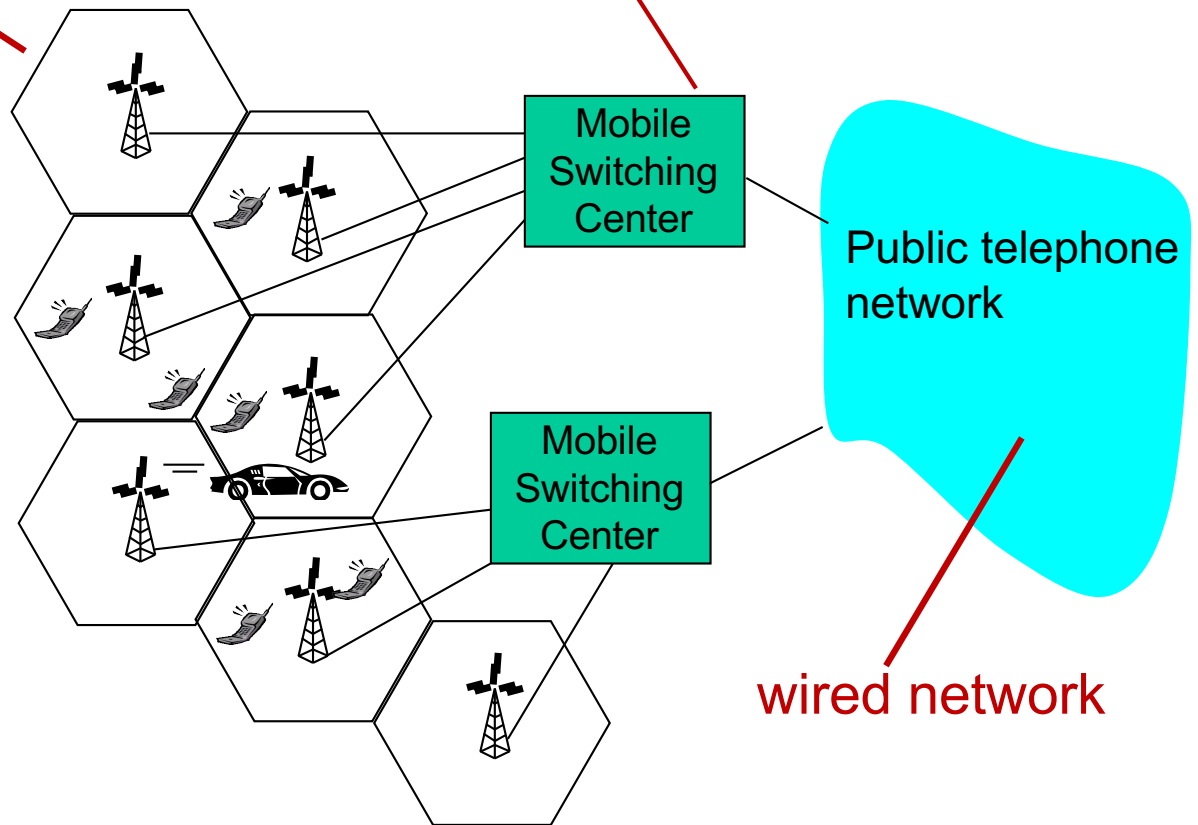
Cellular networks: the first hop

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
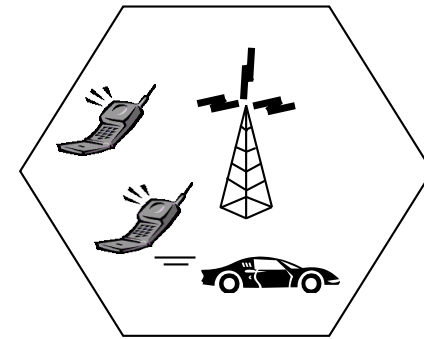
time slots

frequency bands
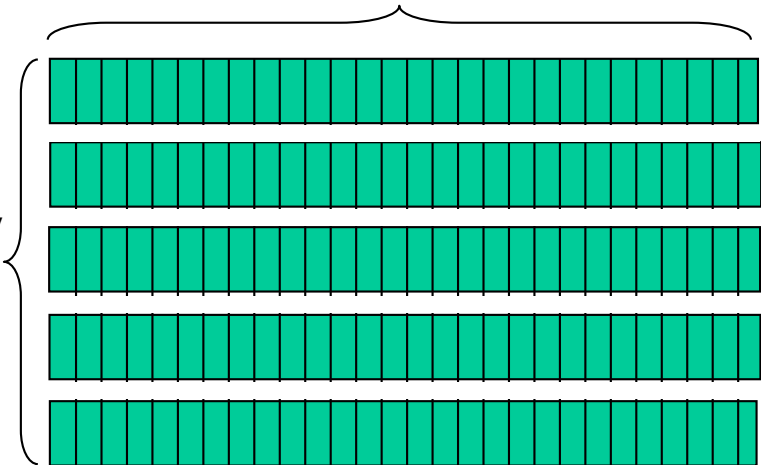
2G (voice) network architecture
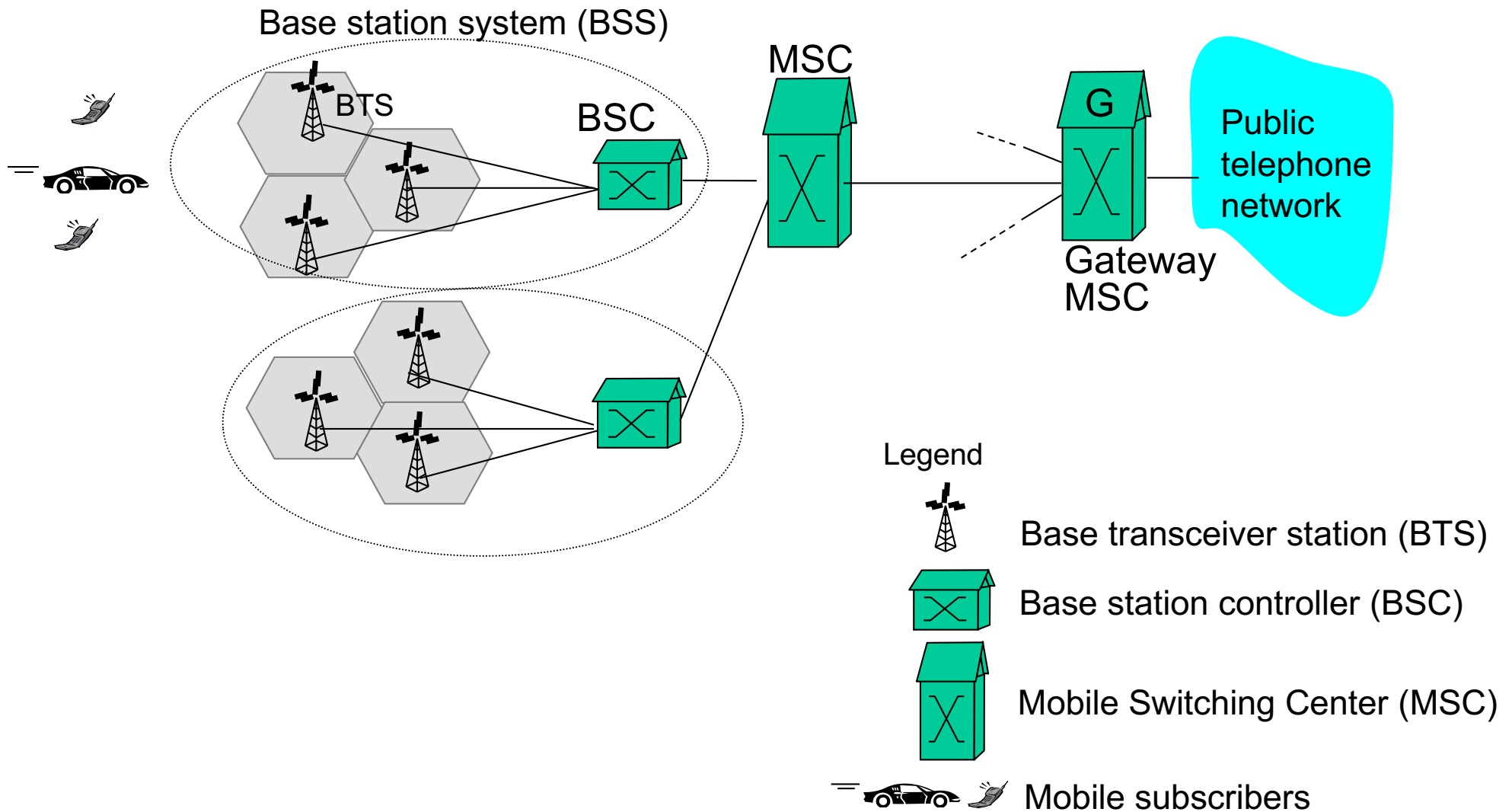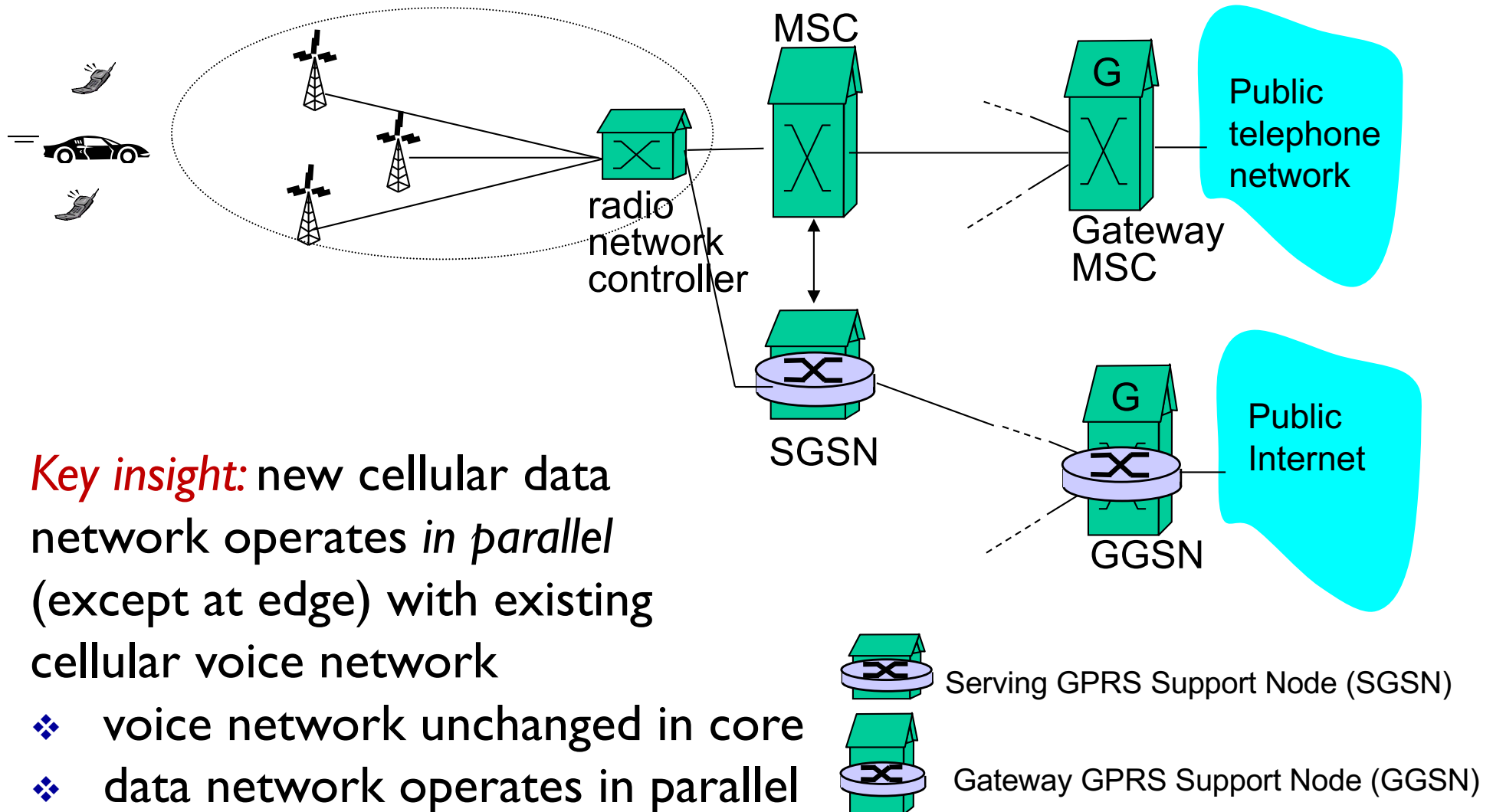
Base station system (BSS)

MSC

BTS

BSC

G

Public telephone network

Gateway MSC

Legend

Base transceiver station (BTS)

Base station controller (BSC)

Mobile Switching Center (MSC)

Mobile subscribers

3G (voice+data) network architecture

MSC

G

Public telephone network

radio network controller

Gateway MSC

SGSN

G

Public Internet

GGSN

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
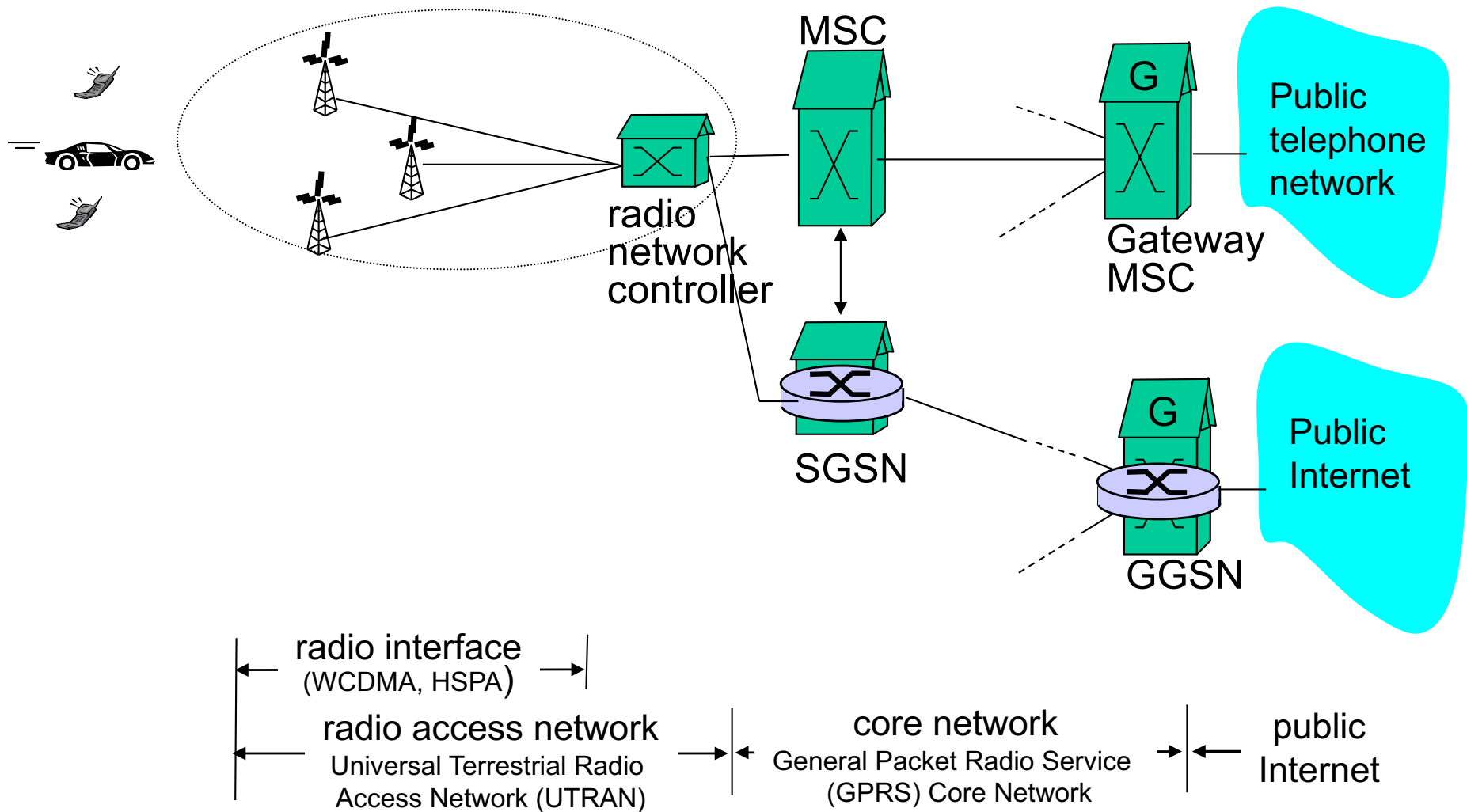
Chapter 6 outline

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)
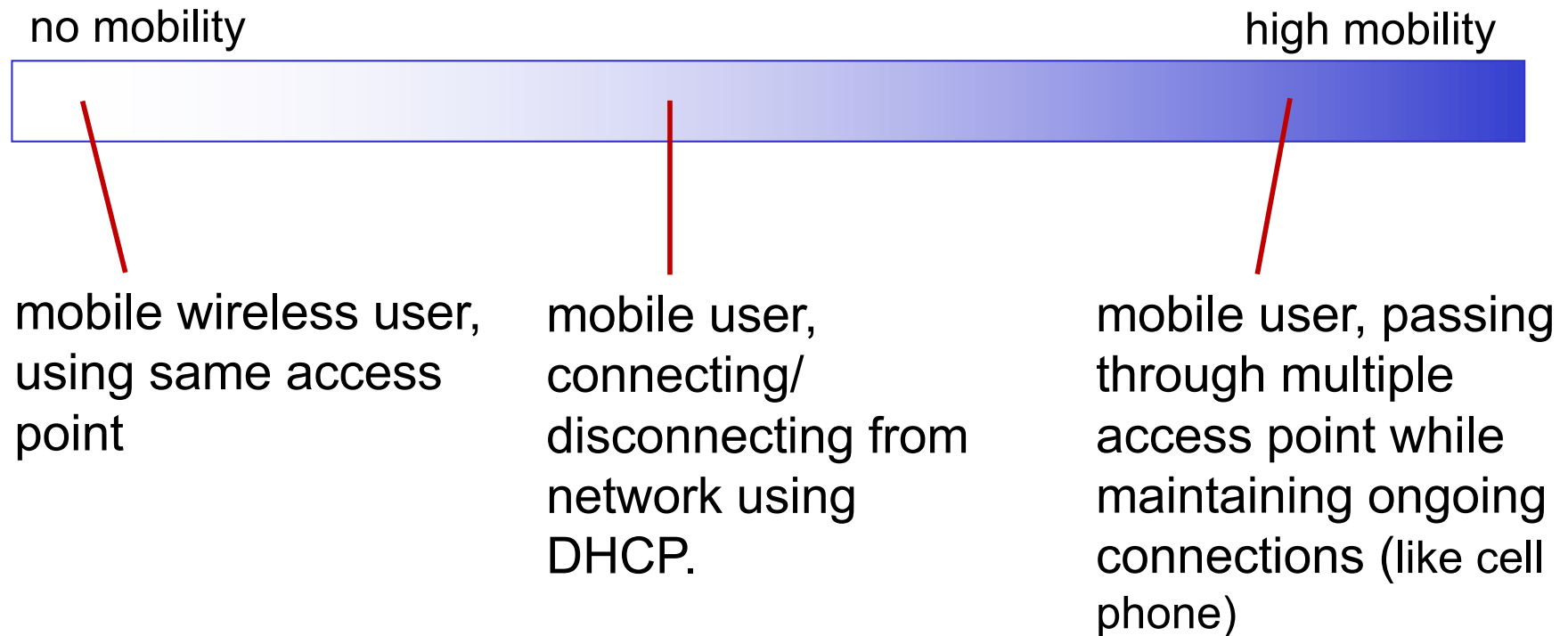
Mobility: vocabulary

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

wide area network

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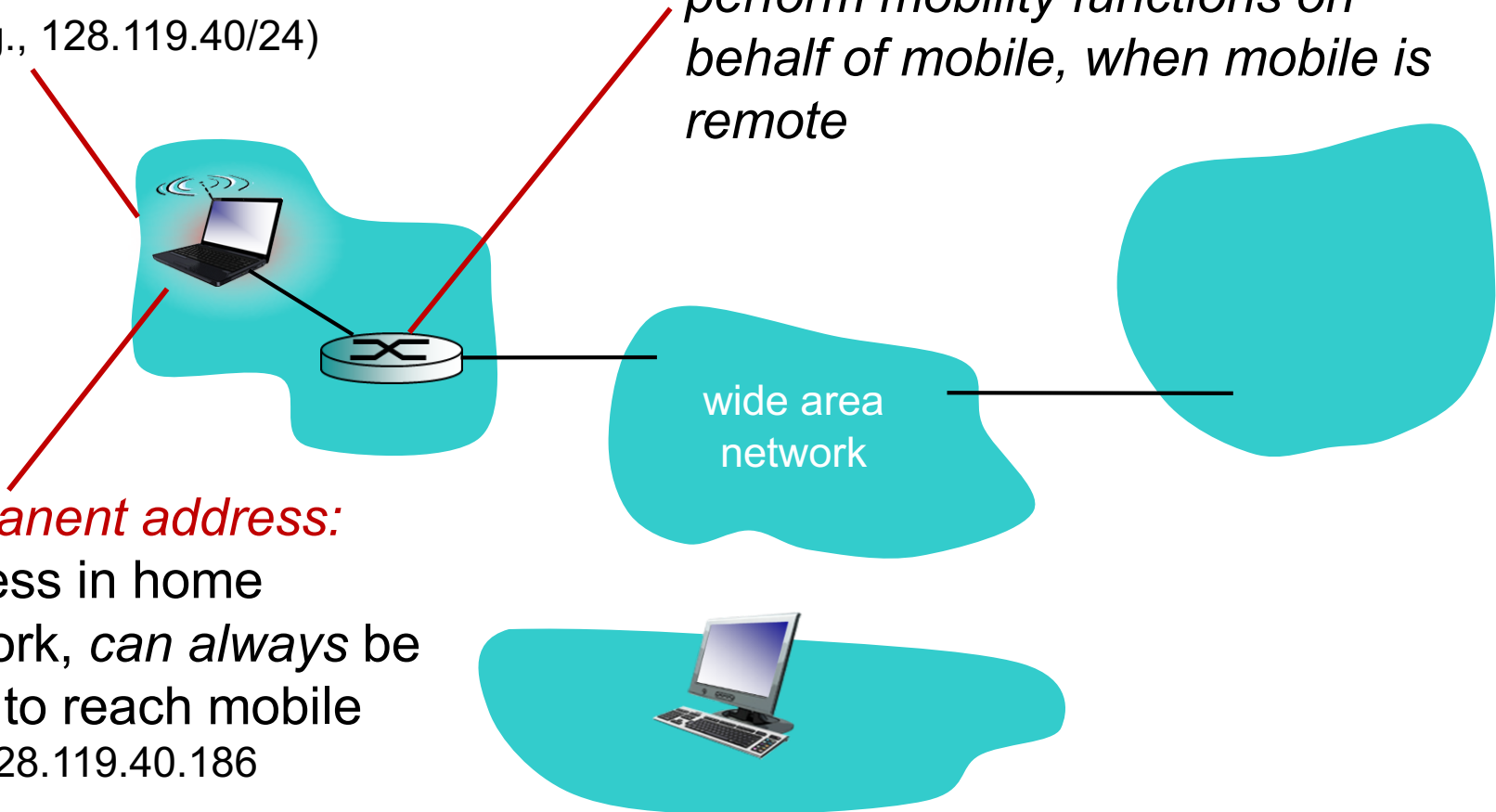
Mobility: more vocabulary

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
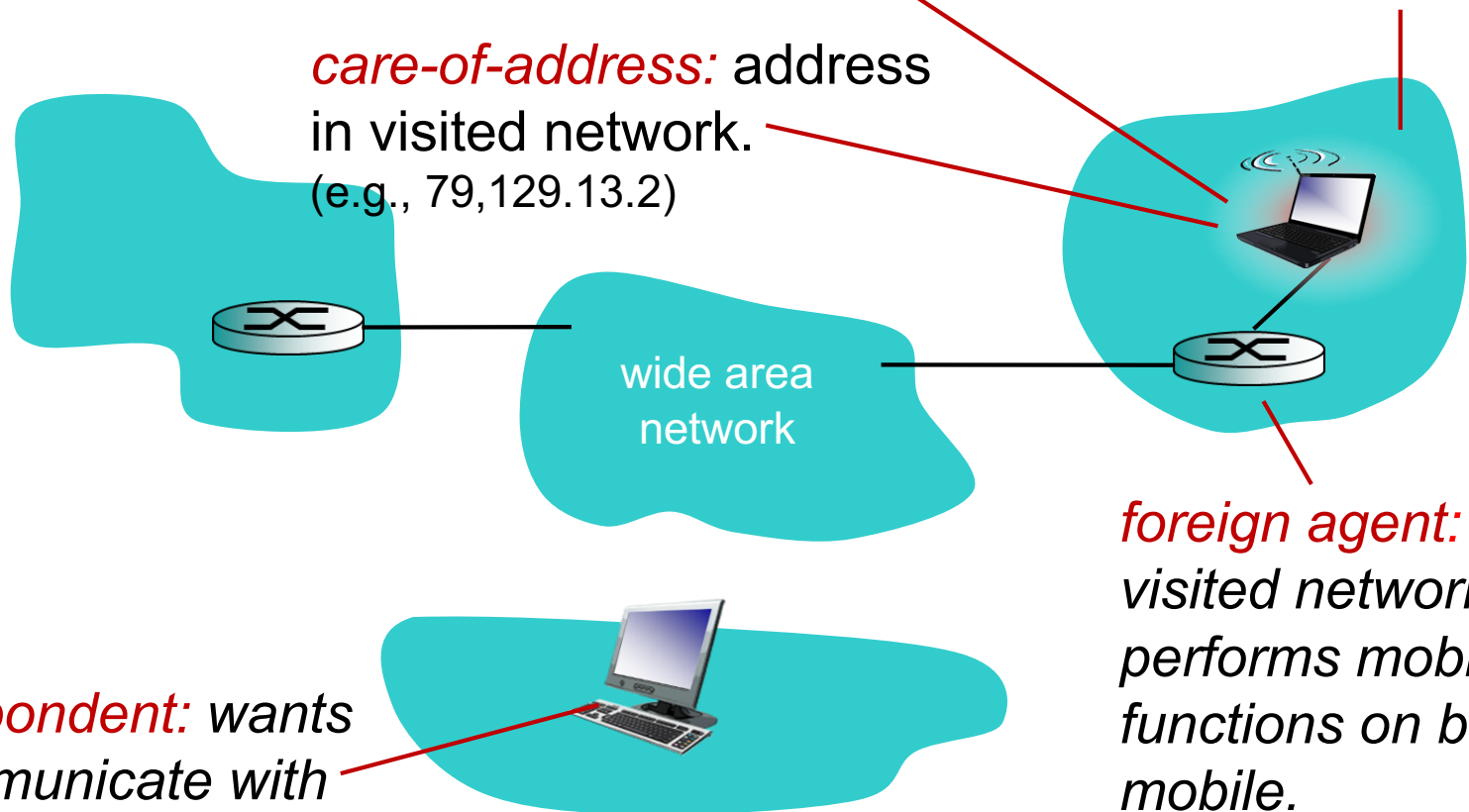
How do *you* contact a mobile friend:

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?
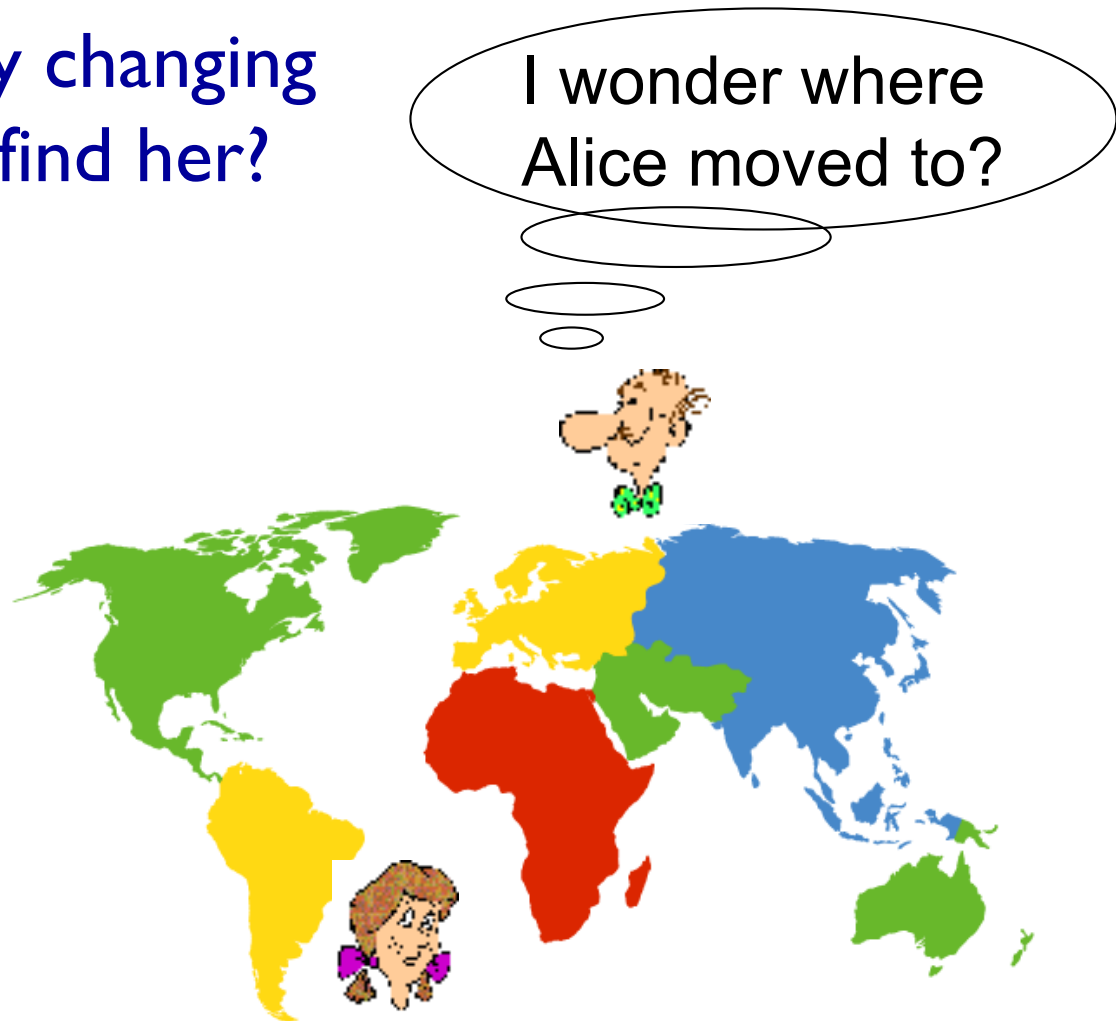
I wonder where Alice moved to?

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-nodes-in-residence via usual routing table exchange.
- routing tables indicate where each mobile located
- no changes to end-systems

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

home network

visited network

②

wide area
network

①

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

mobile contacts
foreign agent on
entering visited
network
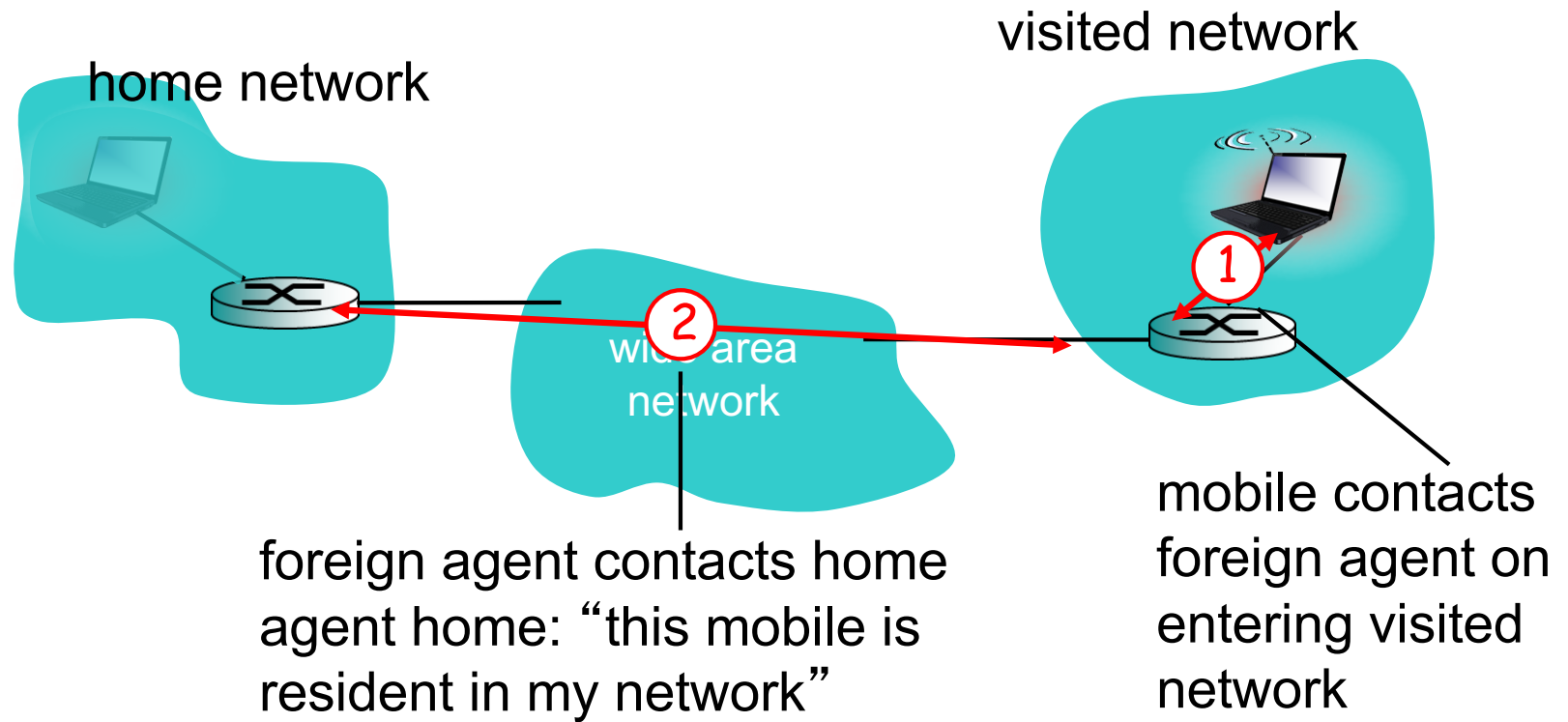
end result:

❖ foreign agent knows about mobile

❖ home agent knows location of mobile

Mobility via indirect routing

home agent intercepts packets, forwards to foreign agent

foreign agent receives packets, forwards to mobile

visited network

home network

wide area network

correspondent addresses packets using home address of mobile

mobile replies directly to correspondent

1

2

3

4
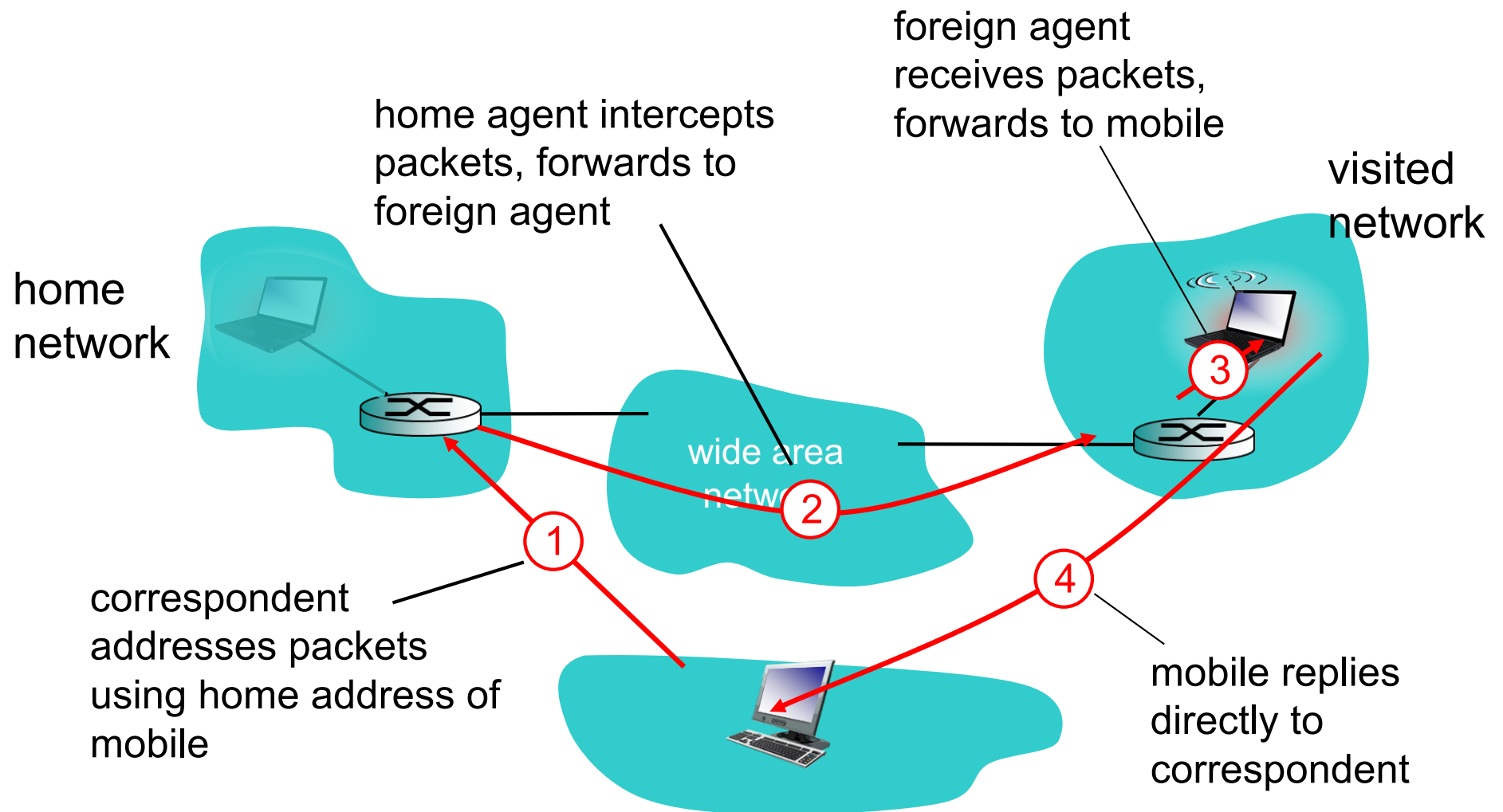
Indirect Routing: comments

❖ **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
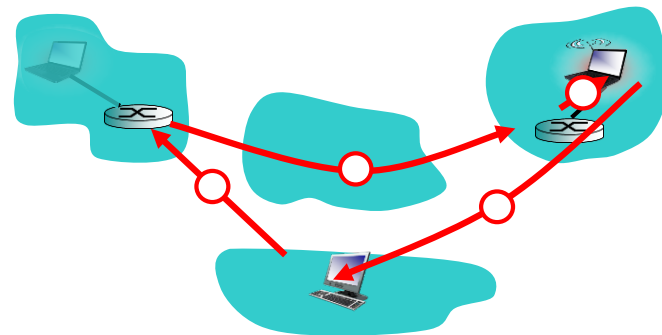
Indirect routing: moving between networks

❖ 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

foreign agent
receives packets,
forwards to mobile

correspondent forwards
to foreign agent

visited
network

home
network

3

1 2

4

correspondent
requests, receives
foreign address of
mobile

mobile replies
directly to
correspondent
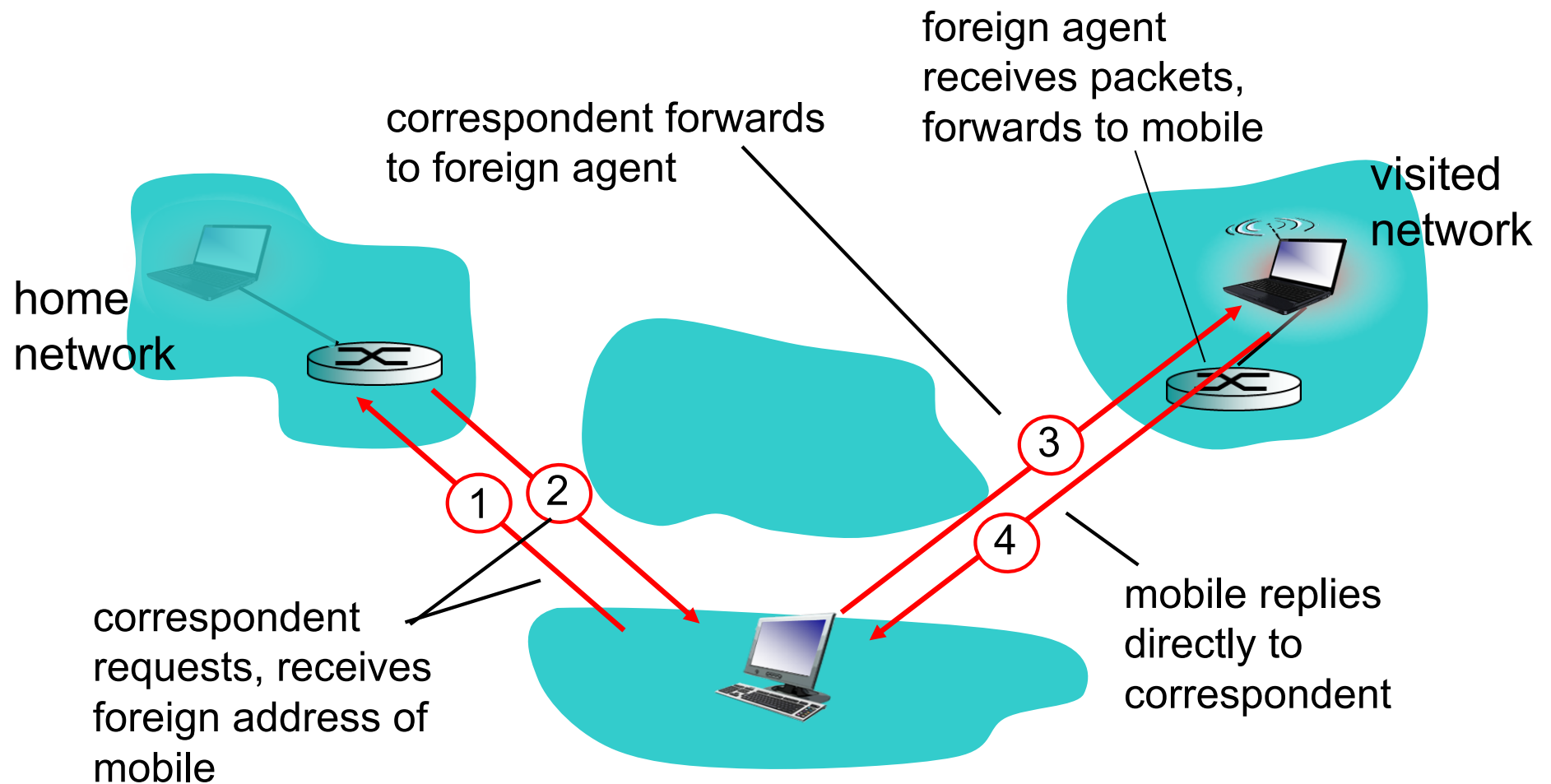
Mobility via direct routing: comments

❖ overcome triangle routing problem

❖ *non-transparent to correspondent:* correspondent must get care-of-address from home agent

 ▪ what if mobile changes visited network?
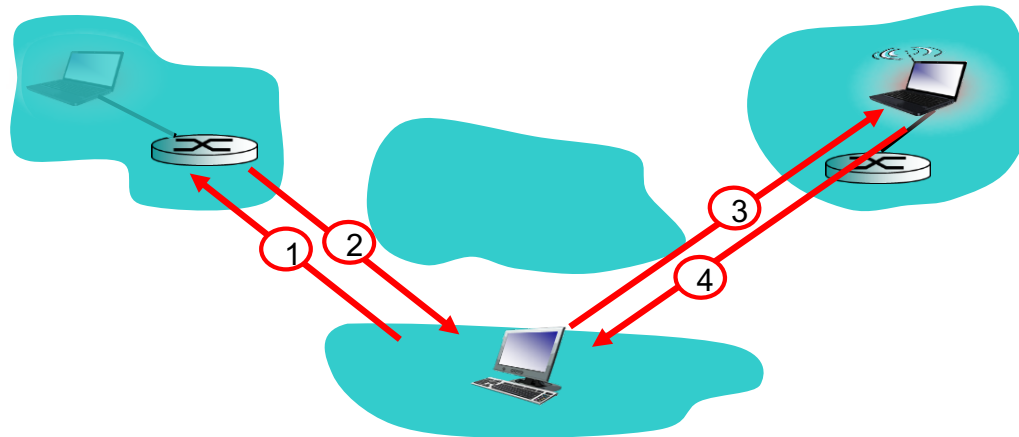
Accommodating mobility with direct routing

❖ 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)
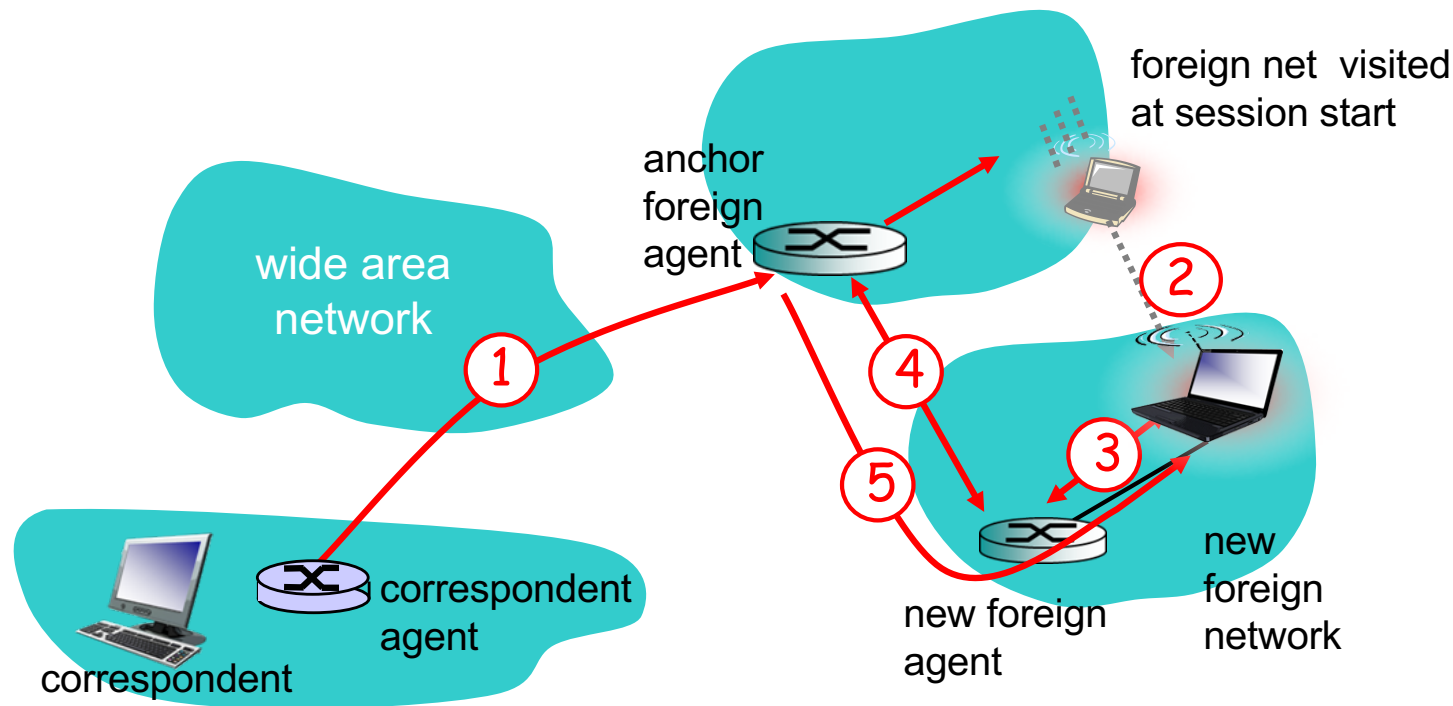
Chapter 6 outline

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

foreign-agent-to-mobile packet

| dest: 128.119.40.186 | // |
| | // |

packet sent by home agent to foreign agent: a *packet within a packet*

| dest: 79.129.13.2 | dest: 128.119.40.186 | // |
| | | // |

Permanent address:
128.119.40.186

Care-of address:
79.129.13.2

| dest: 128.119.40.186 | // |
| | // |

packet sent by
correspondent
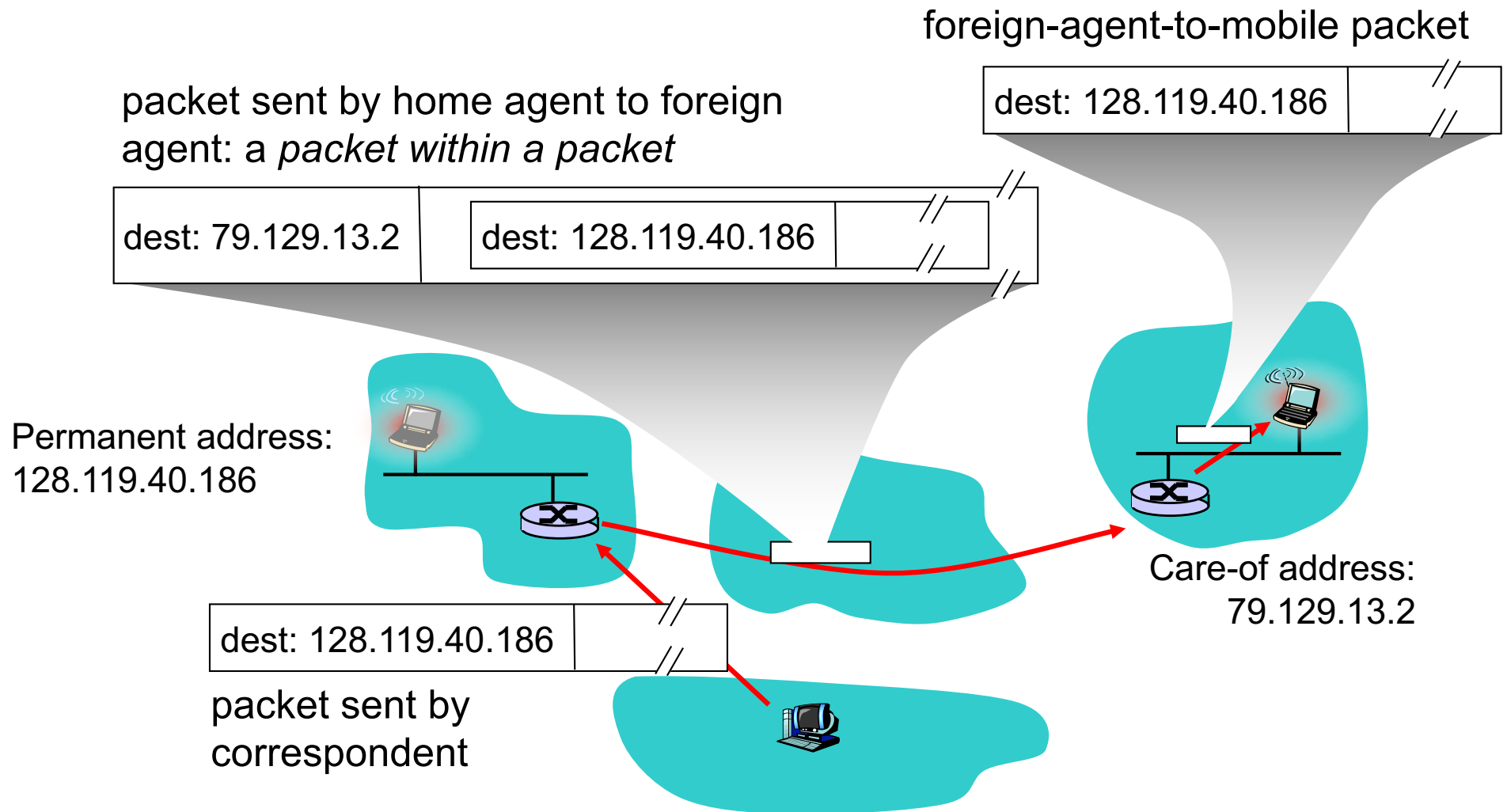
Mobile IP: agent discovery

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

H,F bits: home and/or foreign agent

R bit: registration required

```
              0          8          16         24
          ┌──────────┬──────────┬─────────────────┐  ┬
          │ type = 9 │ code = 0 │    checksum     │  │
          ├──────────┴──────────┼────────┬────────┤  │  standard
          │                     │        │        │  │  ICMP fields
          ├─────────────────────┴────────┴────────┤  │
          │            router address             │  │
          ├───────────────────────────────────────┤  ┴
          │                                       │
          ├──────────┬──────────┬─────────────────┤
          │ type = 16│  length  │    sequence #   │
          ├──────────┴─────┬─────┴──────┬──────────┤
          │ registration   │  RBHFMGV   │ reserved │  mobility agent
          │ lifetime       │   bits     │          │  advertisement
          ├────────────────┴────────────┴──────────┤  extension
          │         0 or more care-of-             │
          │            addresses                   │
          └───────────────────────────────────────┘
```
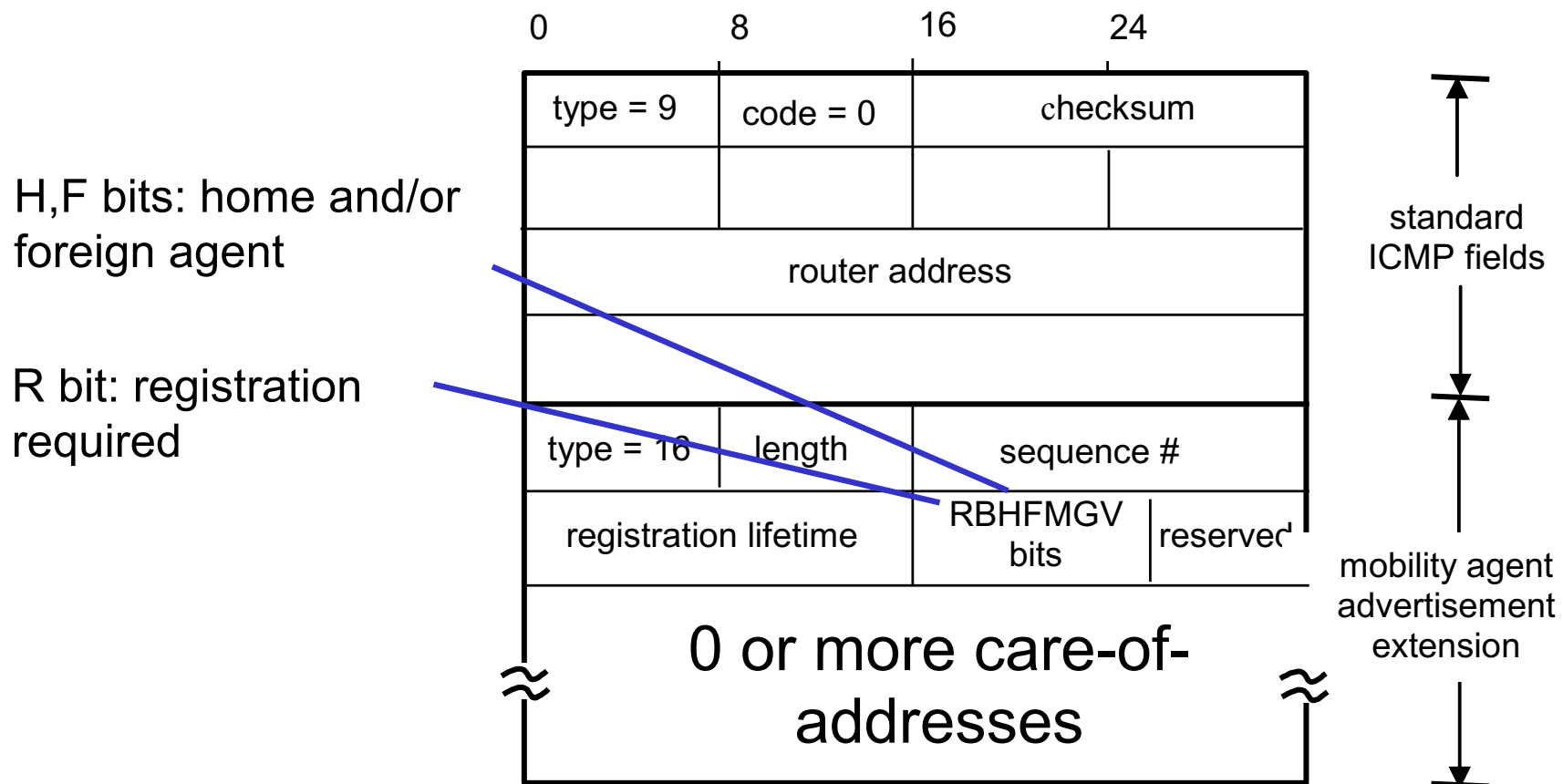
Mobile IP: registration example

visited network: 79.129.13/24

home agent
HA: 128.119.40.7

foreign agent
COA: 79.129.13.2

mobile agent
MA: 128.119.40.186

ICMP agent adv.

COA:
79.129.13.2
….

registration req.

COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification:714
….

registration req.

COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification: 714
encapsulation format
….

registration reply

HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
….

registration reply

HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
….

time

Components of cellular network architecture

recall:

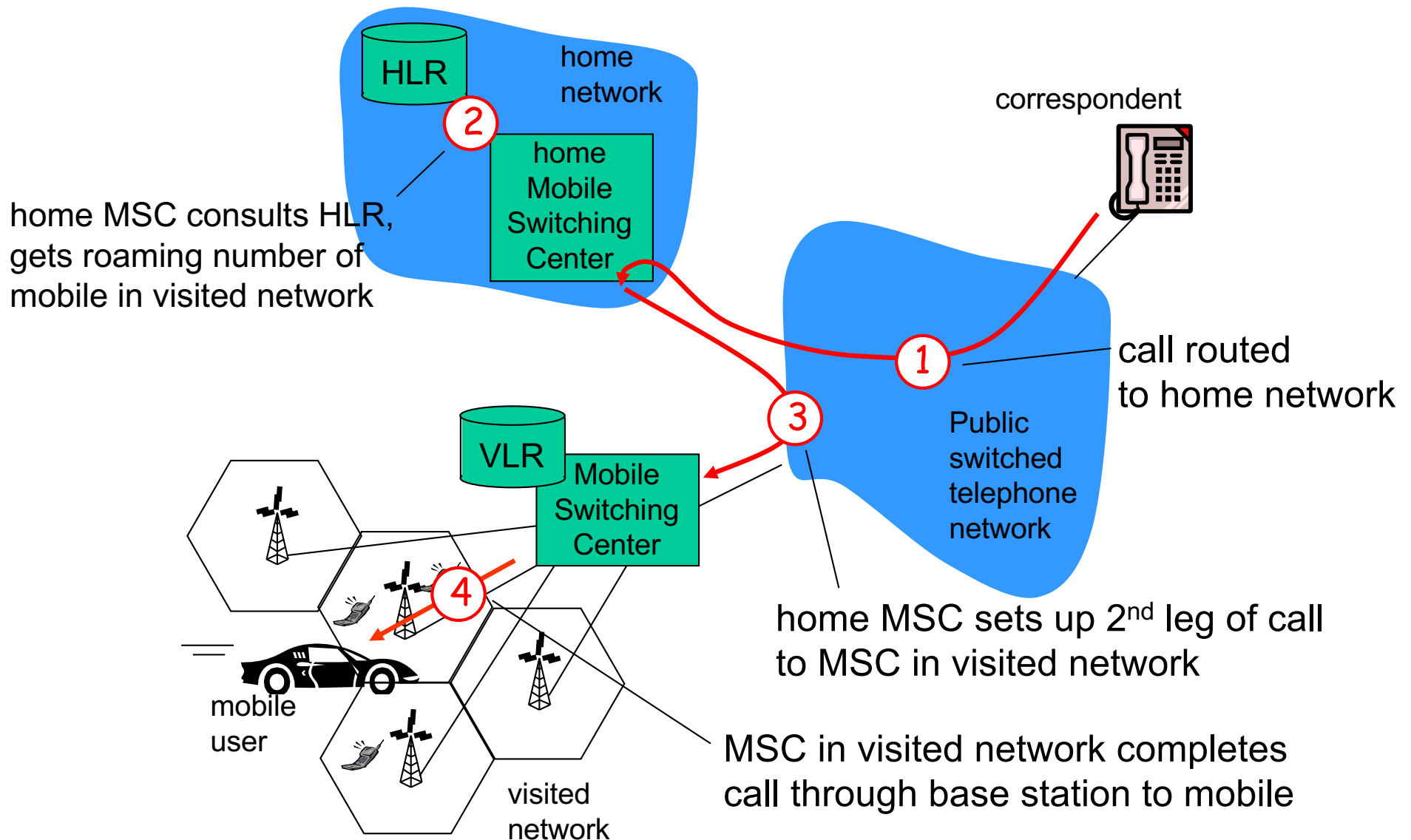
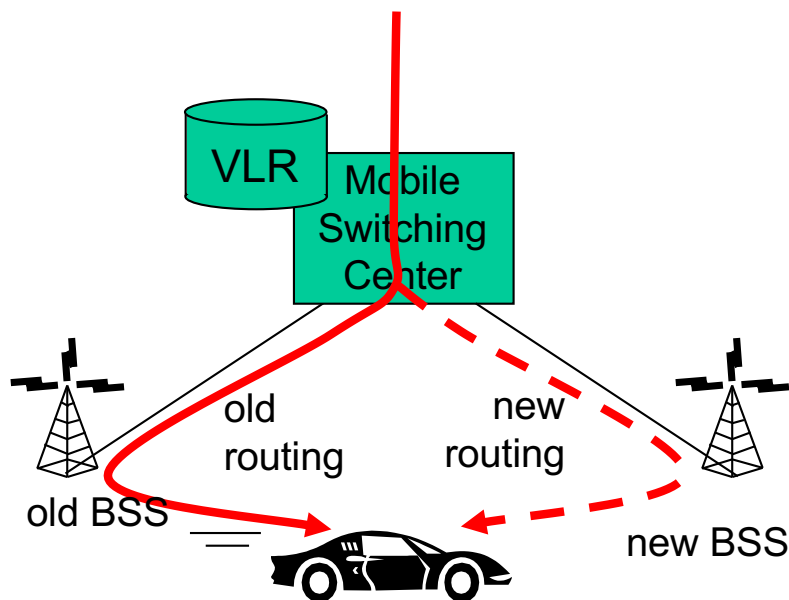different cellular networks,
operated by different providers
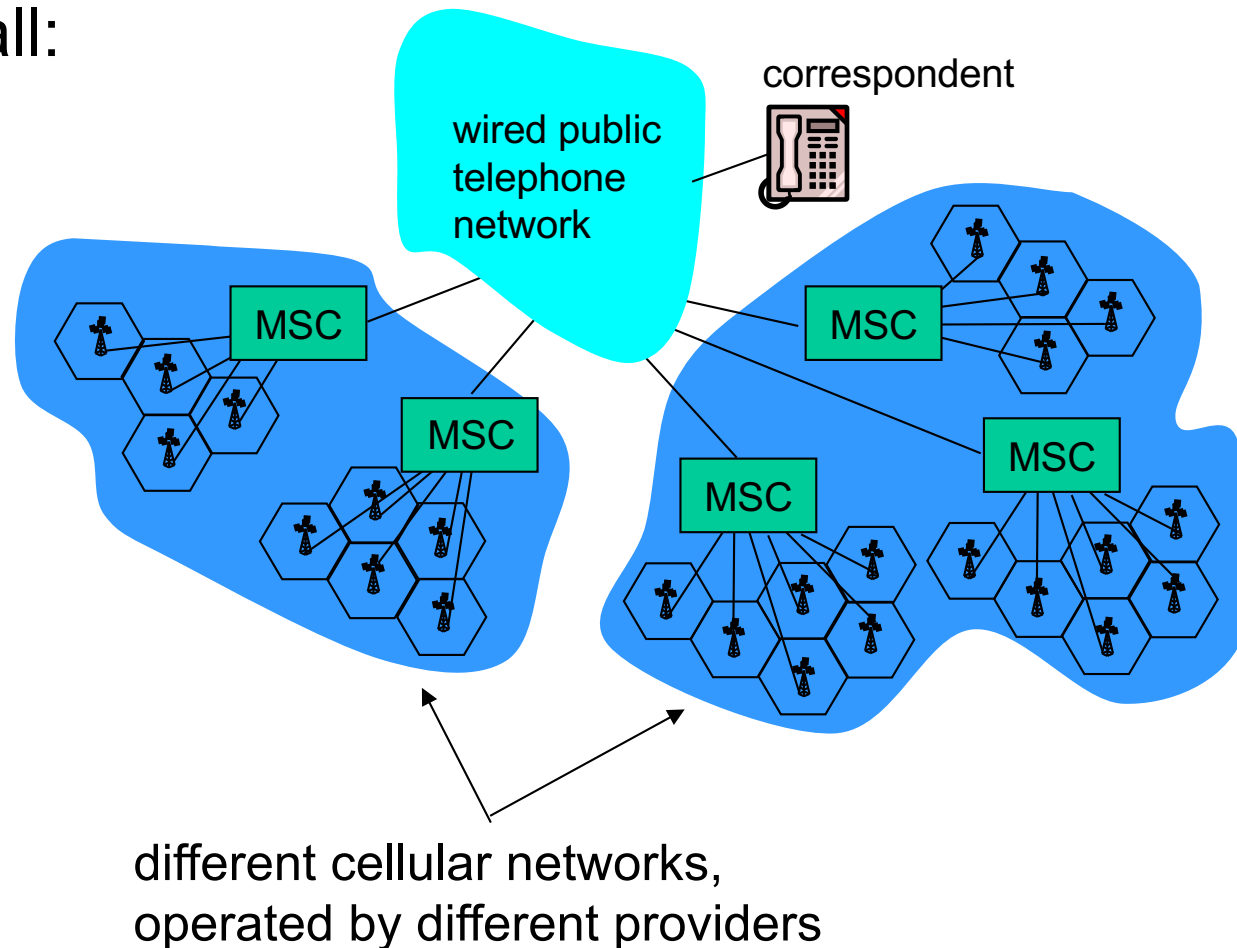
Handling mobility in cellular networks

❖ *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

HLR

home network

2

home Mobile Switching Center

home MSC consults HLR, gets roaming number of mobile in visited network

correspondent

1

call routed to home network

3

VLR

Mobile Switching Center

Public switched telephone network

4

home MSC sets up 2nd leg of call to MSC in visited network

mobile user

MSC in visited network completes call through base station to mobile

visited network

GSM: handoff with common MSC


VLR

Mobile Switching Center

old routing

new routing

old BSS

new BSS

❖ *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 doesnt mandate why to perform handoff (policy), only how (mechanism)

❖ handoff initiated by old BSS

GSM: handoff with common MSC
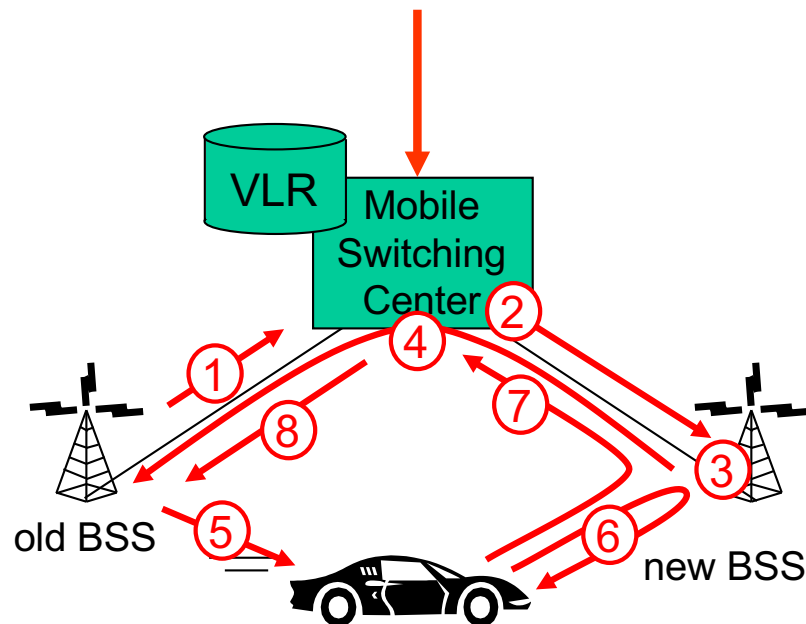
1. old BSS informs MSC of impending handoff, provides list of 1+ new BSSs

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
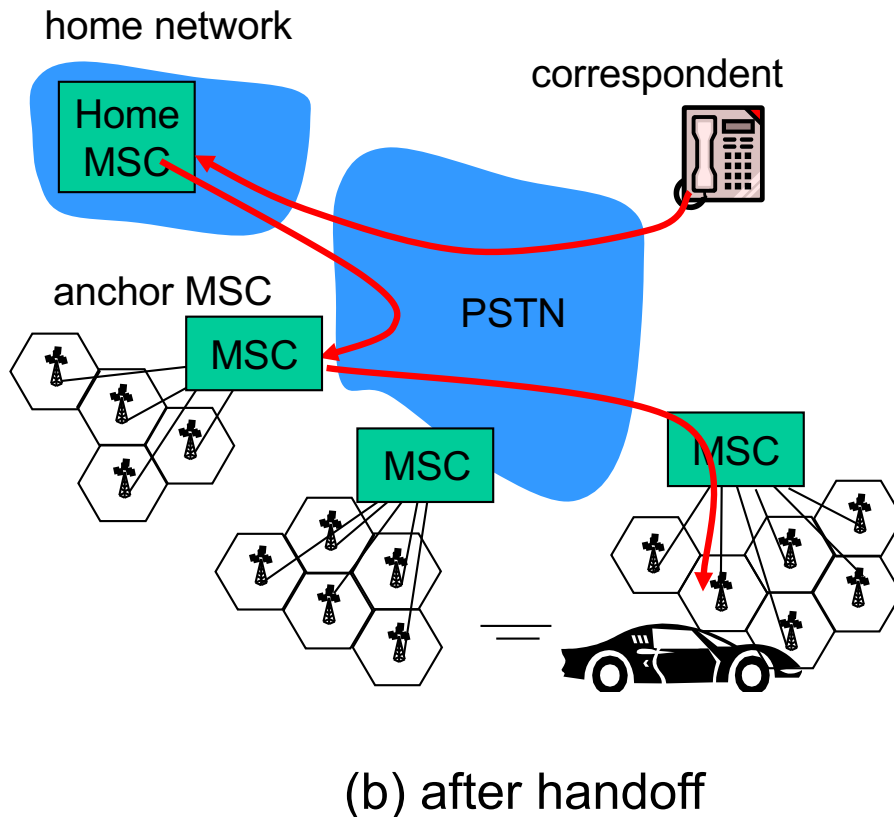
GSM: handoff between MSCs

(a) before handoff

❖ *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

home network

correspondent

Home MSC

anchor MSC

PSTN

MSC

MSC

MSC

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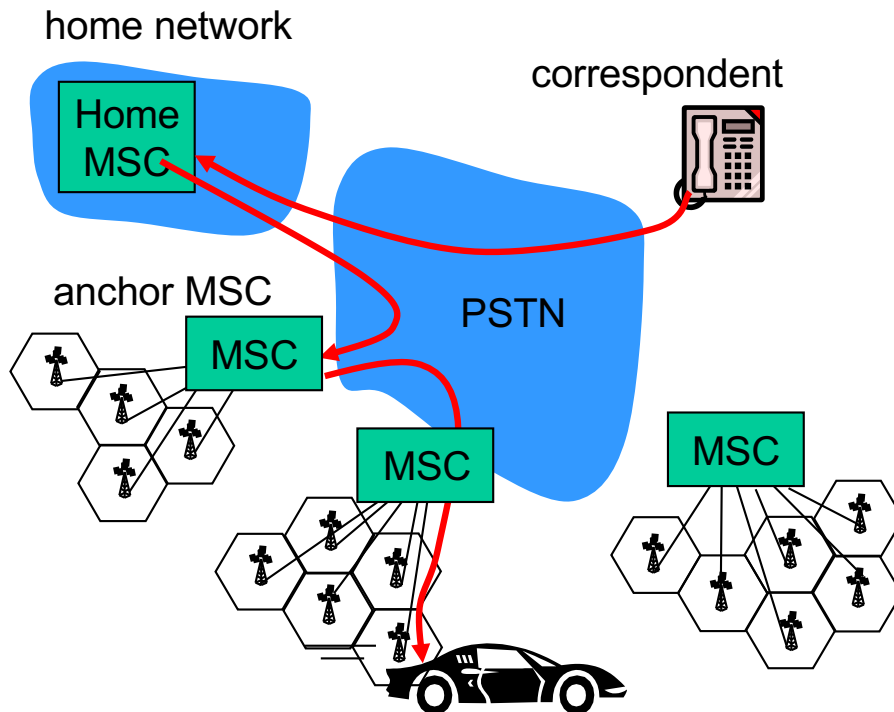
- ❖ *anchor MSC:* first MSC visited during call
  - ■ call remains routed through anchor MSC
- ❖ new MSCs add on to end of MSC chain as mobile moves to new MSC
- ❖ optional path minimization step to shorten multi-MSC chain

Mobility: GSM versus Mobile IP

GSM element	Comment on GSM element	Mobile IP element
Home system	Network to which mobile user's permanent phone number belongs	**Home network**
Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	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	**Home agent**
Visited System	Network other than home system where mobile user is currently residing	**Visited network**
Visited Mobile services Switching Center. Visitor Location Record (VLR)	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	**Foreign agent**
Mobile Station Roaming Number (MSRN), or "roaming number"	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	**Care-of-address**

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 6 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., GSM, 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

❖ impact on higher-layer protocols