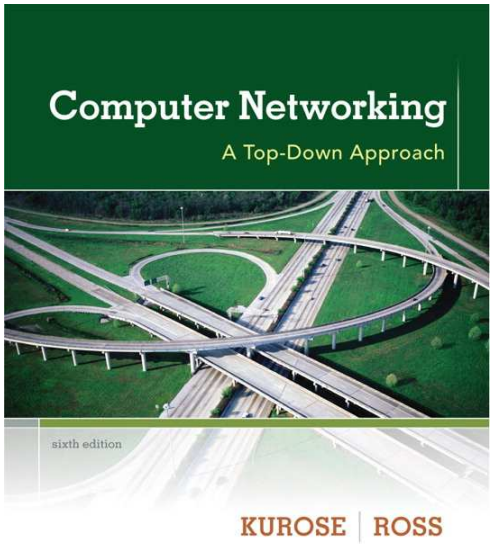
# Chapter 6
# Wireless and Mobile Networks




A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

NOTE:EDITED VERSION (UMinho, 2016)



*Computer Networking: A Top Down Approach*
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

# 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 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics

- CDMA

6.3 IEEE 802.11 wireless LANs ("Wi-Fi")

6.4 Cellular Internet Access

- architecture
- standards (e.g., GSM)

Mobility

6.5 Principles: addressing and routing to mobile users

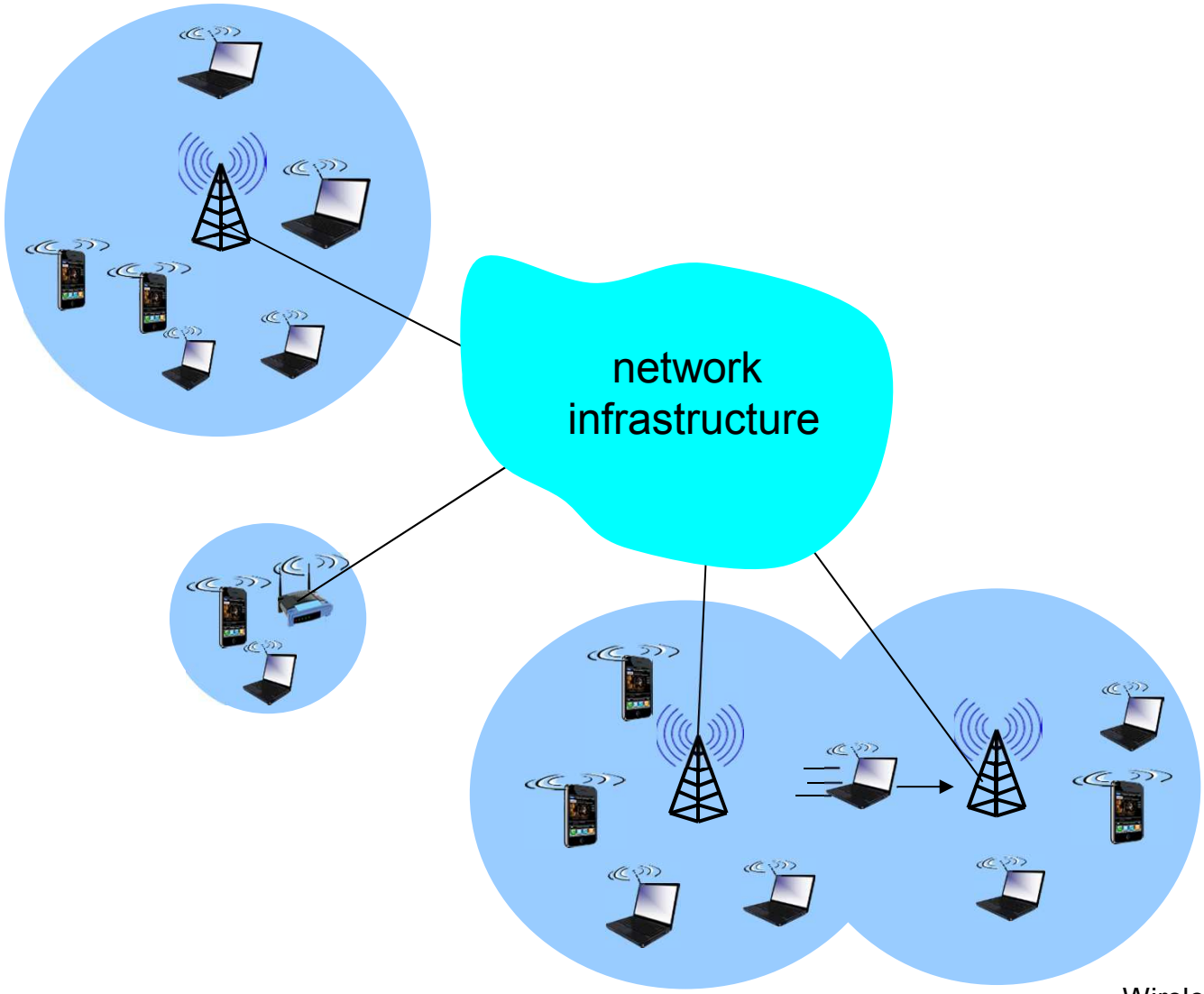
6.6 Mobile IP

6.7 Handling mobility in cellular networks

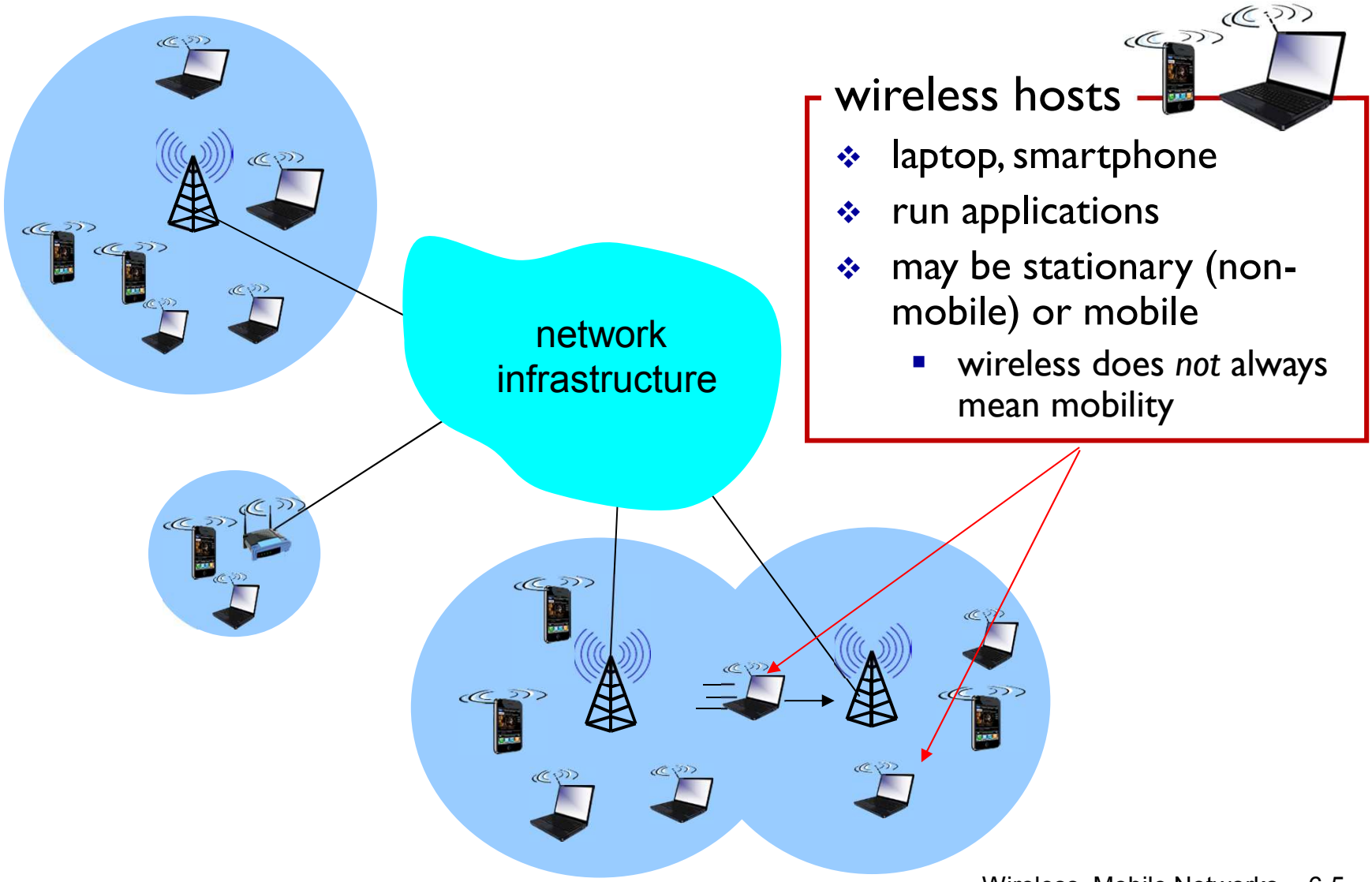
6.8 Mobility and higher-layer protocols

6.9 Summary

# Elements of a wireless network



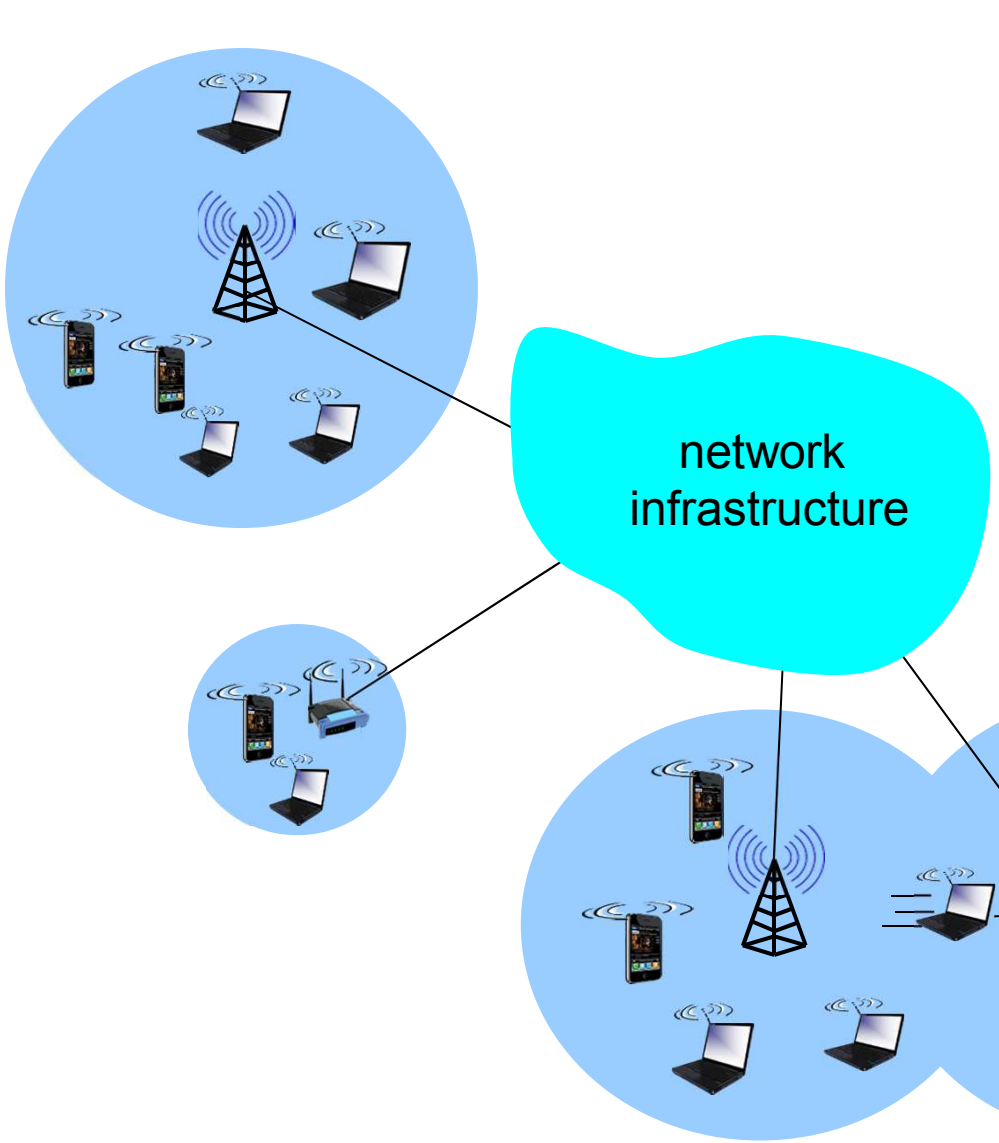
# Elements of a wireless network




wireless hosts

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

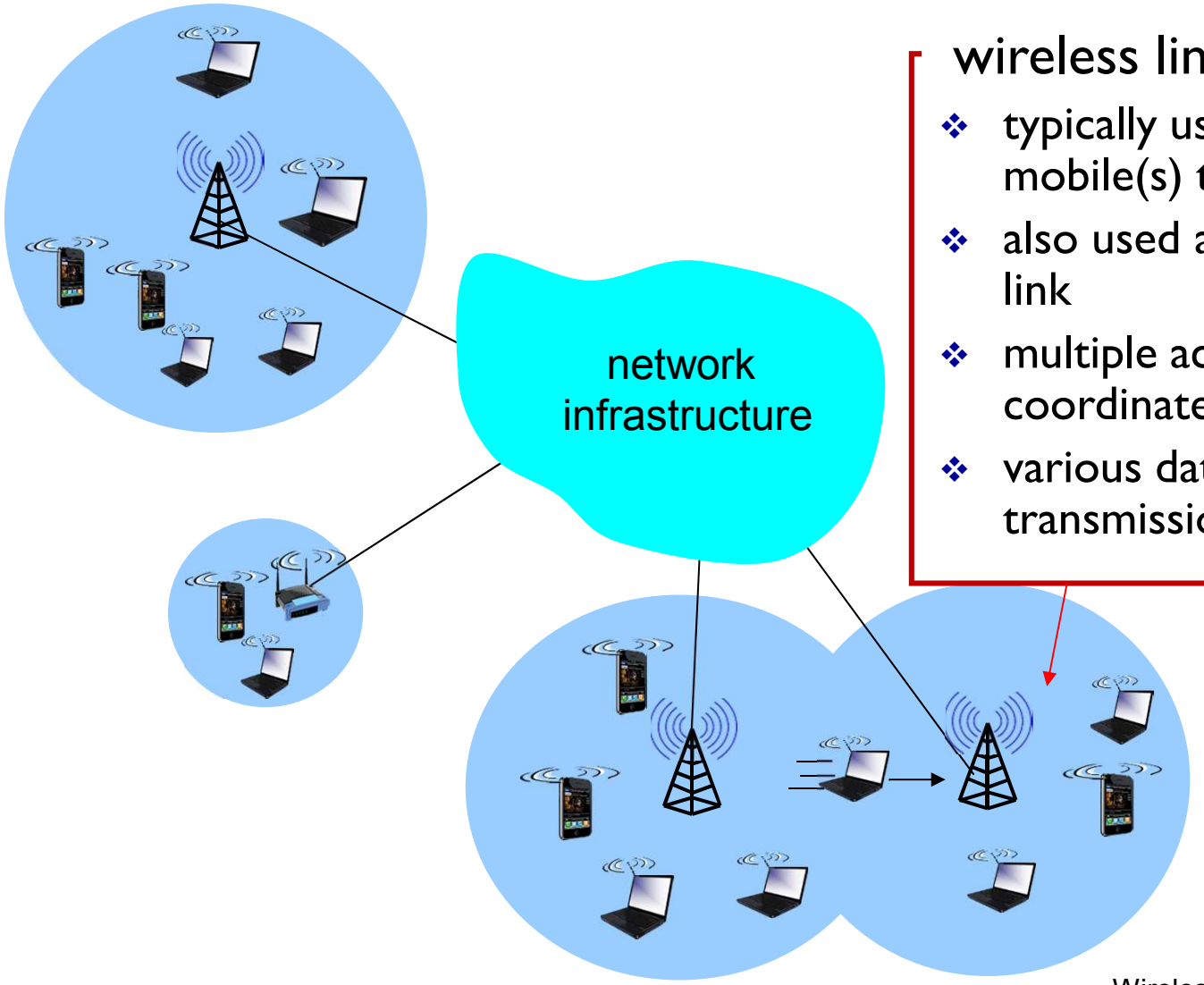
# Elements of a wireless network




**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

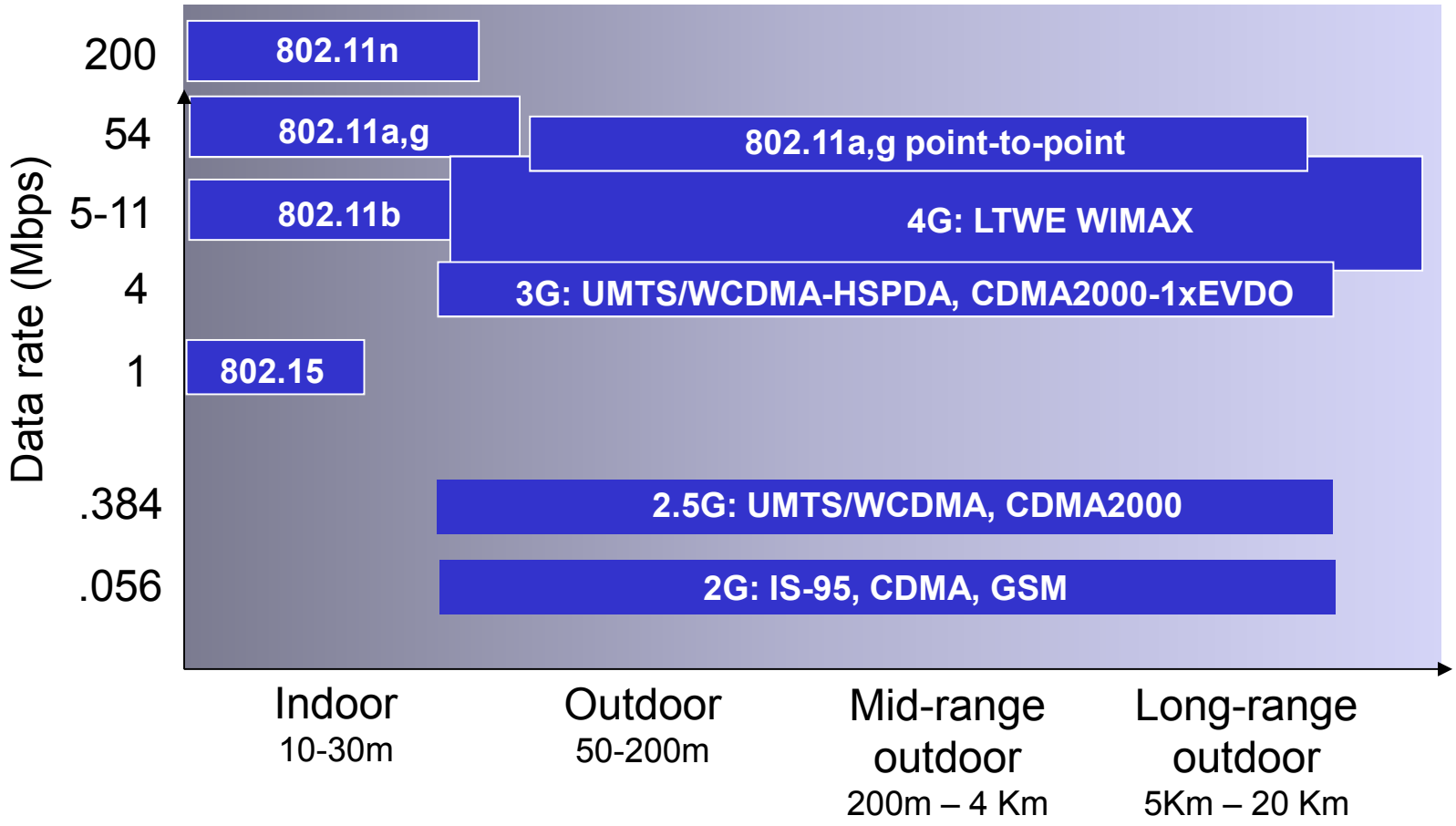
# Elements of a wireless network



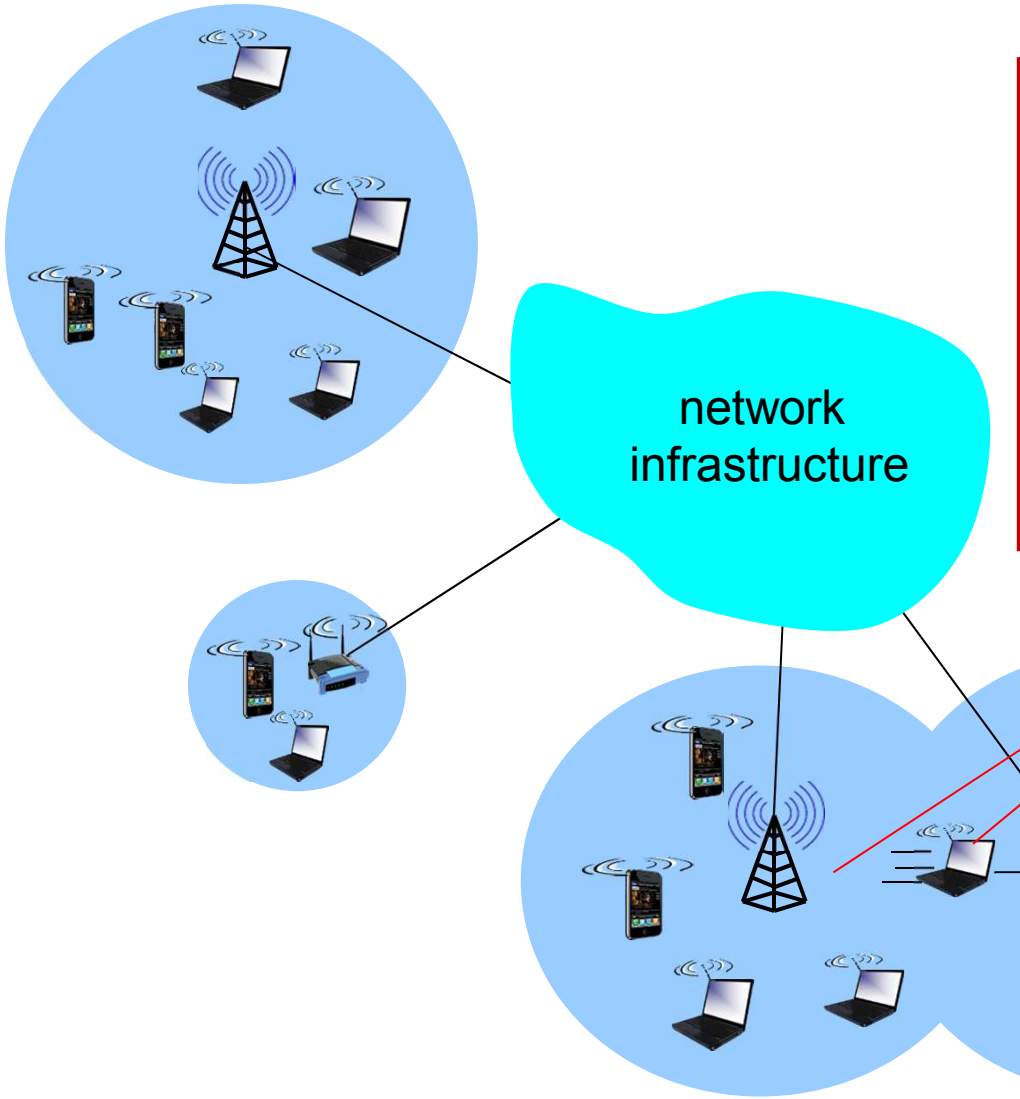

wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

# Characteristics of selected wireless links



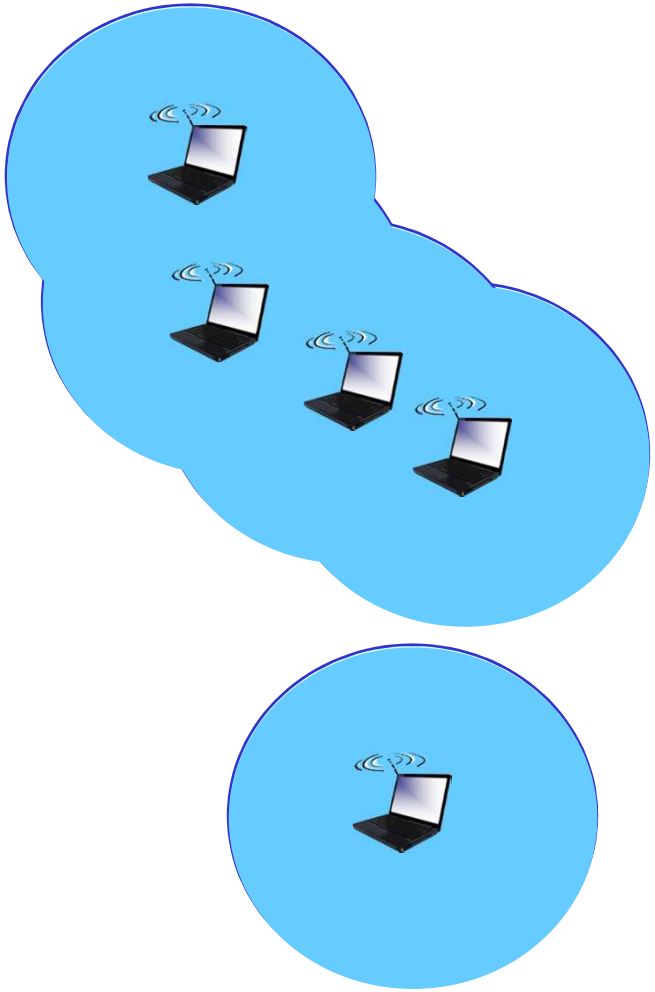
# Elements of a wireless network




infrastructure mode

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

# 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: *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 given wireless node MANET, VANET |

# Wireless Link Characteristics (1)

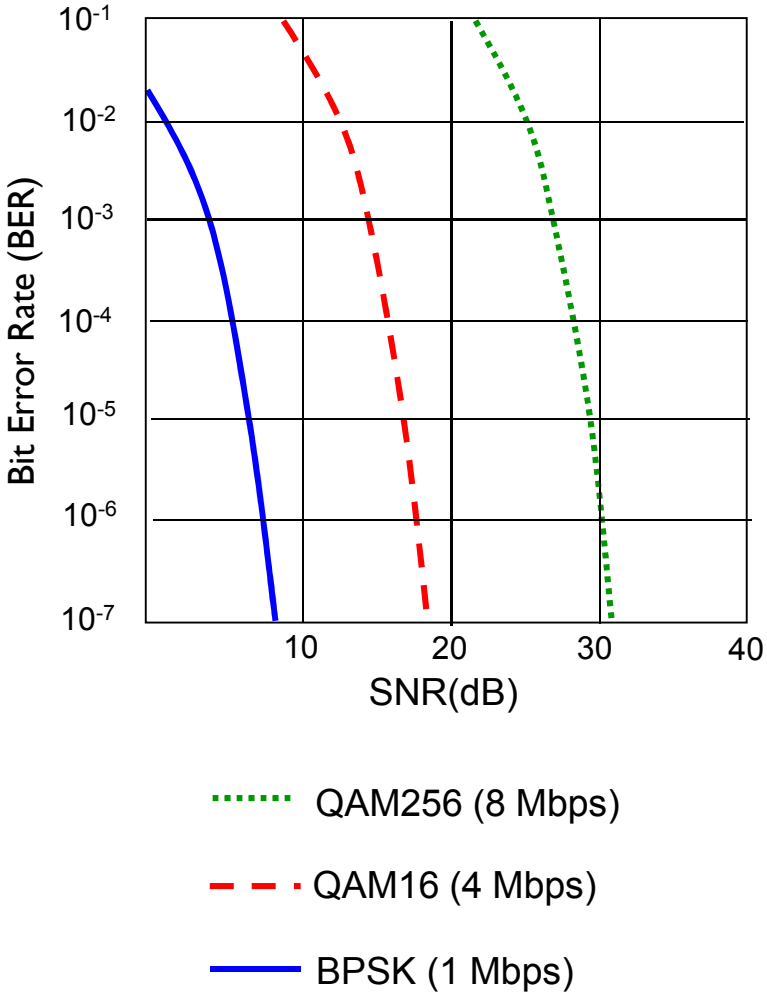
*important* differences from wired link ….

- *decreased signal strength:* radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources:* 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"

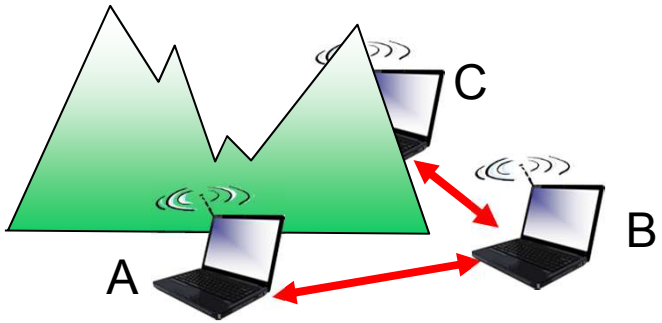
# Wireless Link Characteristics (2)

- 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 -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



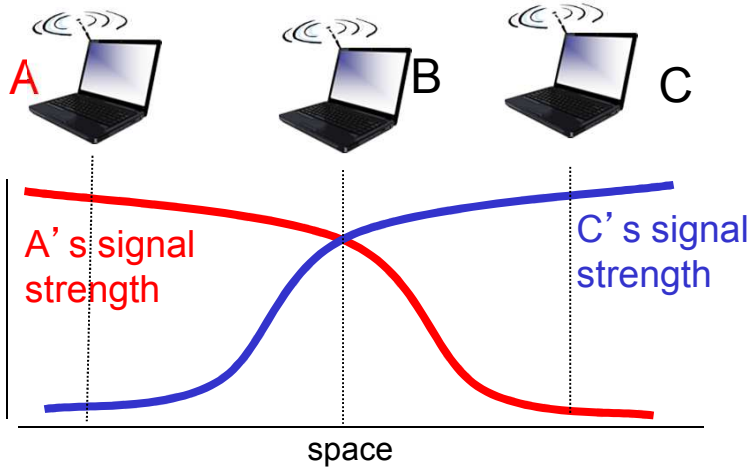
# Wireless network characteristics

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

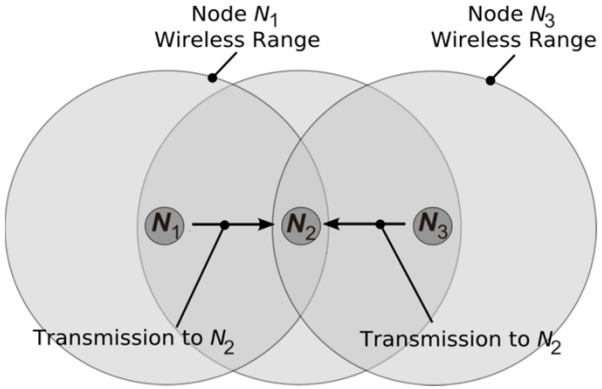



*Signal attenuation:*

- B, A hear each other
- B, C hear each other
- A, C cannot hear each other interfering at B

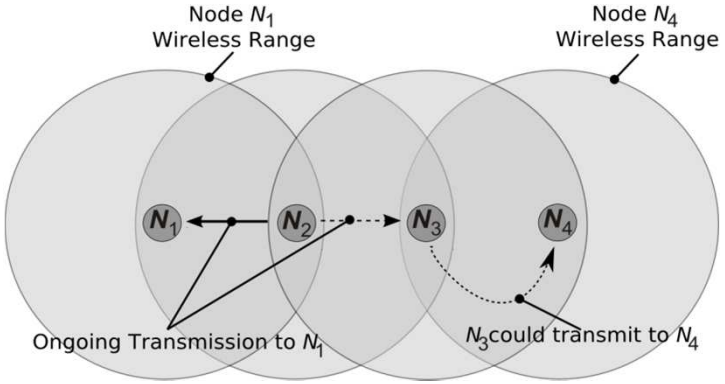
# Wireless network characteristics

*Sentir o canal no transmissor não fornece informação acerca do canal no receptor*




## Hidden node problem

N1 e N3 não se escutam mutuamente devido a obstáculos ou atenuação: os seus pacotes colidem em N2




## Exposed node problem

N1 e N4 poderiam ser receptores simultâneos mas os respectivos emissores N2 e N3 estão em zona de alcance

**Dois principais problemas**

Problema menos grave que o anterior
→reduz a utilização
→menos estudado

# 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

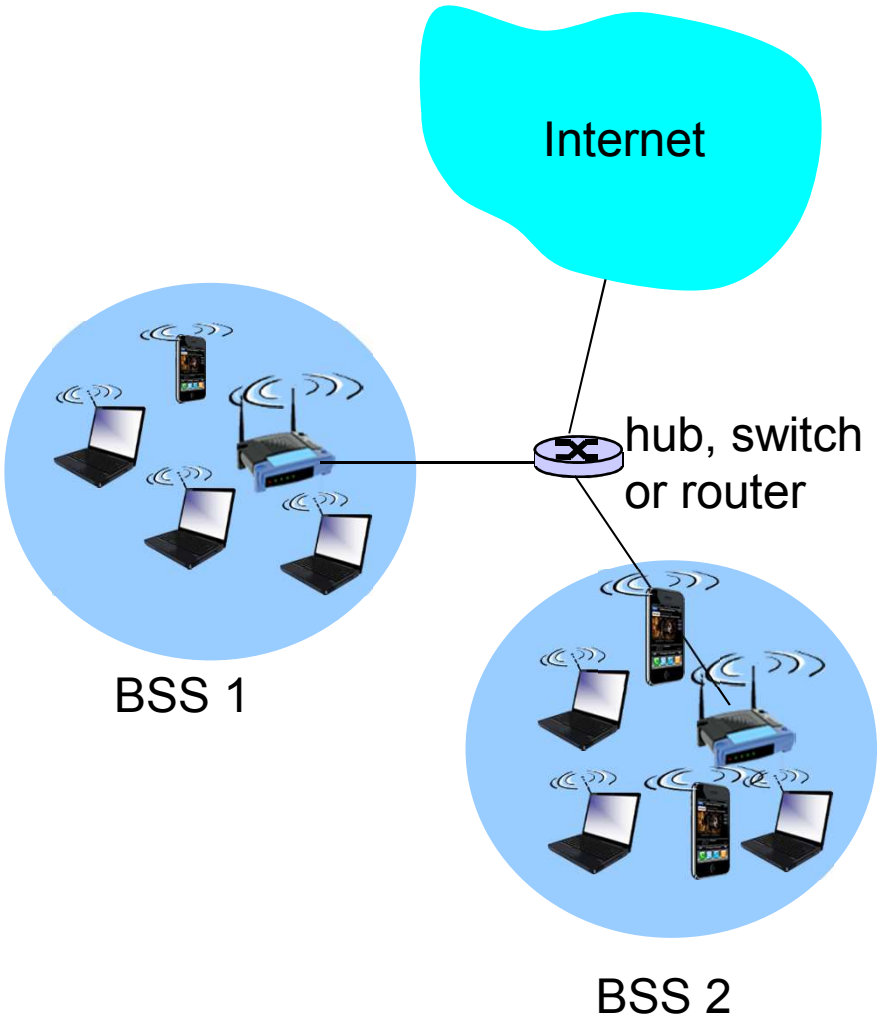
- 2.4-5 GHz range
- up to 54 Mbps

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

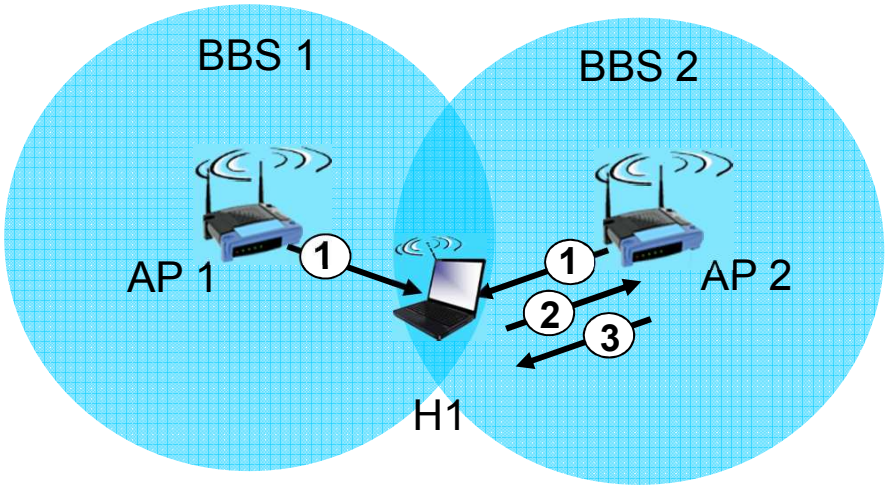


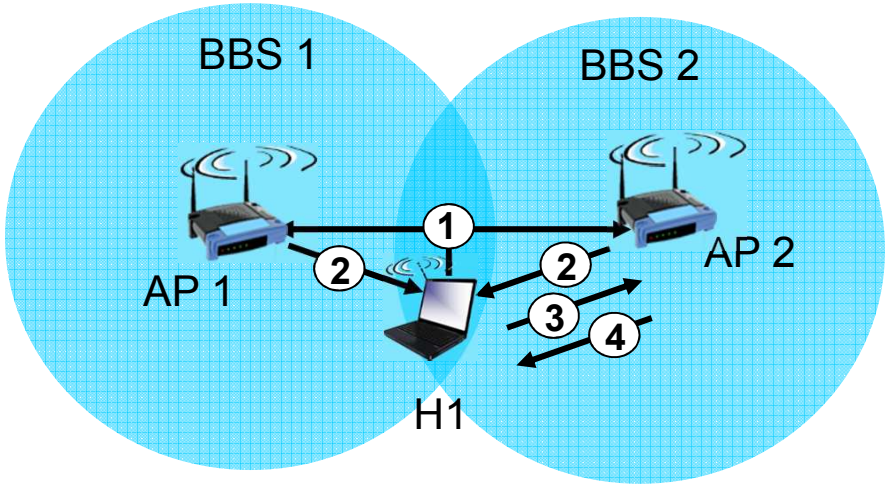

- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

# 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
  - will typically run DHCP to get IP address in AP's subnet

# 802.11: passive/active scanning




*passive scanning:*

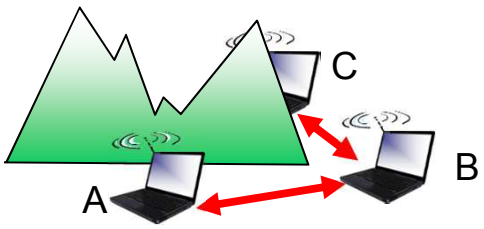
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

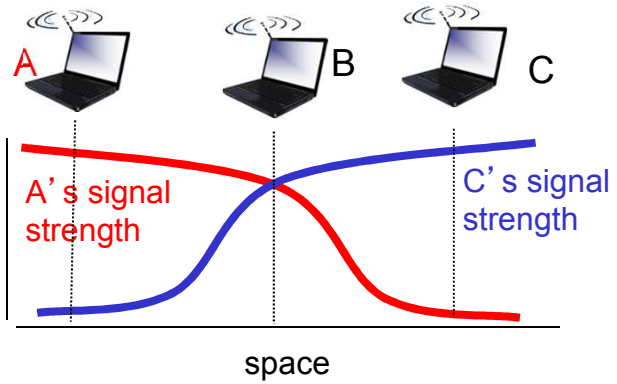
*active scanning:*

(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)



# IEEE 802.11 MAC Protocol: CSMA/CA

**DIFS**: **DCF** (Distributed Coordination Function) Inter-Frame Sequence
**SIFS**: Short Inter-Frame Sequence

## *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

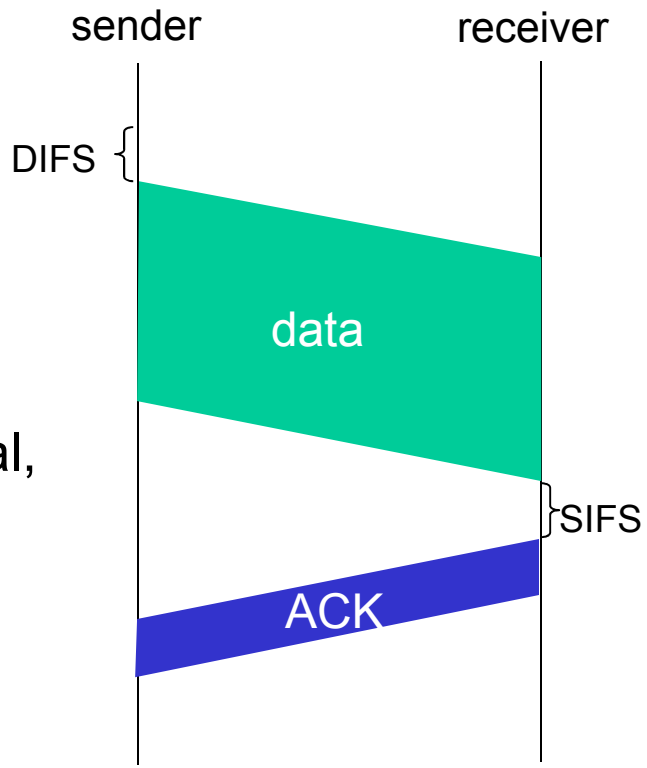
transmit when timer expires

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)



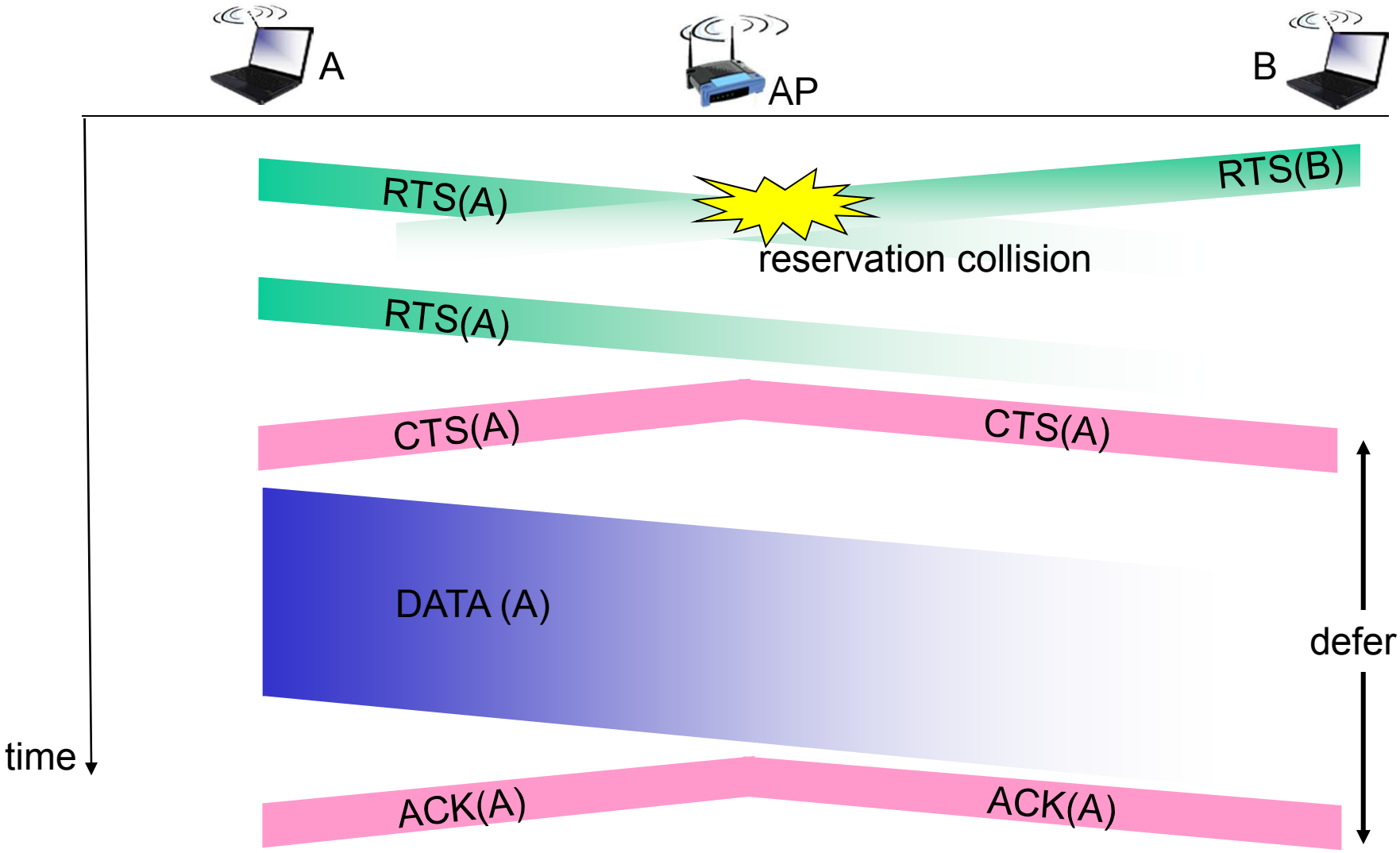
# Avoiding collisions (more)

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

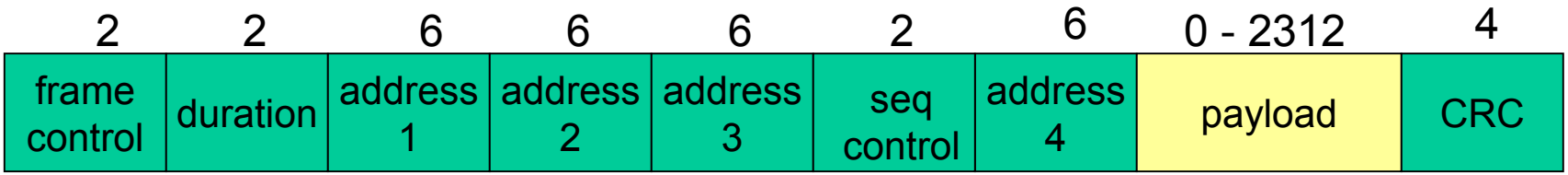
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

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

# Collision Avoidance: RTS-CTS exchange



# 802.11 frame: addressing



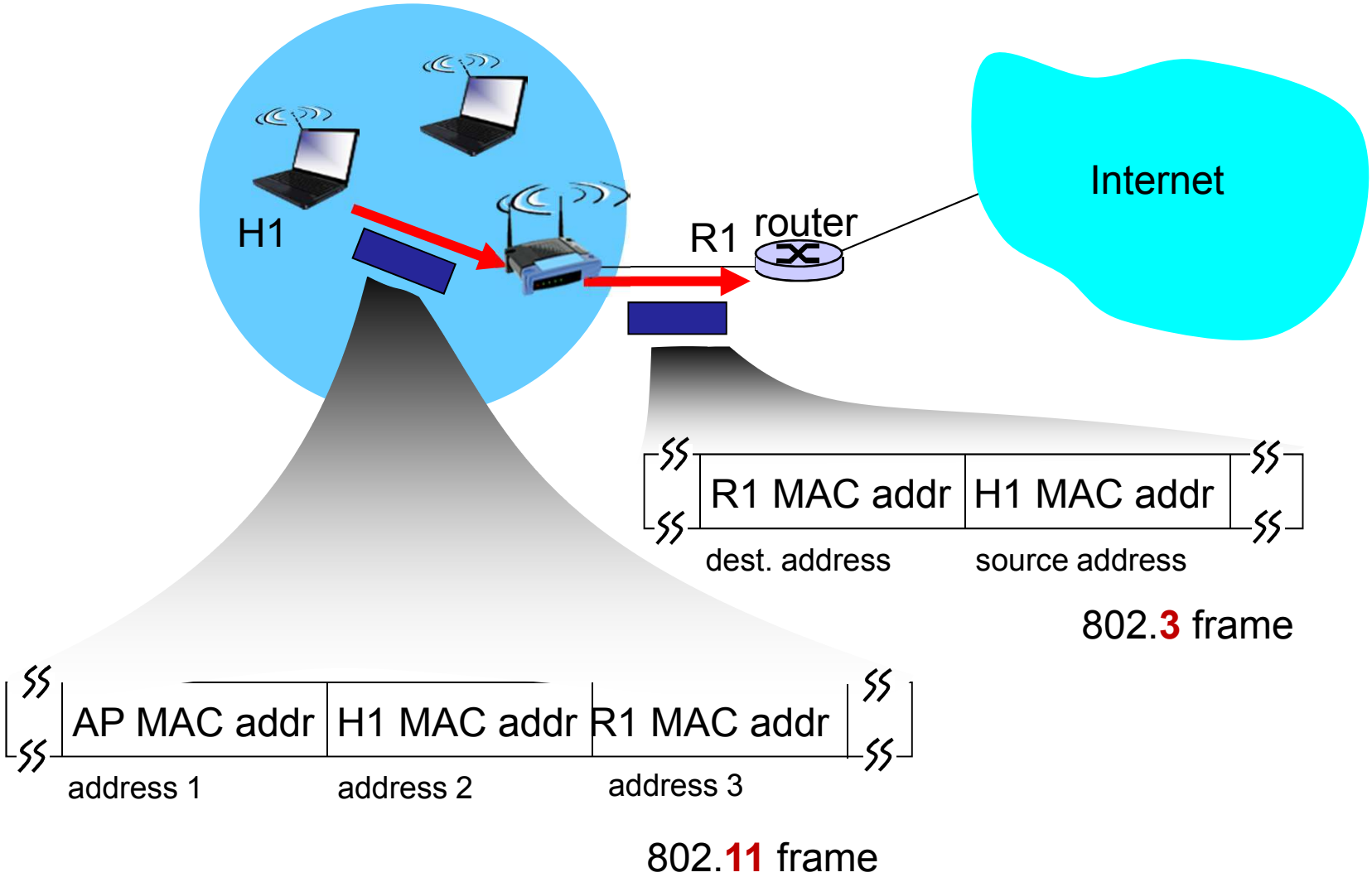

Address 1: MAC address of wireless host or AP to receive this frame

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



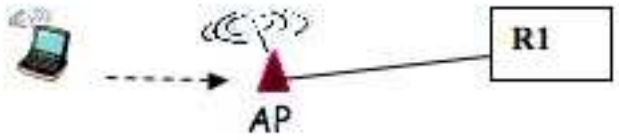
# 802.11 frame: addressing

- The addresses semantics depends on the frame type and directionality
- addr1 – MAC address of the receiver (varies);
- addr2 – MAC address of the sender

DS: Distribution System

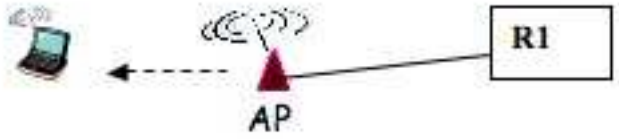
| toDS | fromDS | addr1 | addr2 | addr3 | addr4 | obs. |
|---|---|---|---|---|---|---|
| 0 | 0 | DA | SA | BSSID | - | ad hoc |
| 0 | 1 | DA | BSSID | SA | - | do AP |
| 1 | 0 | BSSID | SA | DA | - | para AP |
| 1 | 1 | RA | TA | DA | SA | dentro DS |

# 802.11 frame: addressing



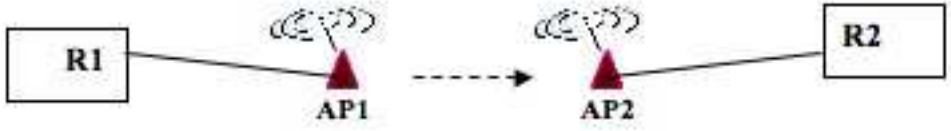

**toDS=1, fromDS=0**

A1 (RA) = BSSID = MAC AP
A2 (TA) = SA = MAC STA
A3 (DA) = MAC R1




**toDS=0, fromDS=1**

A1 (RA) = DA = MAC STA
A2 (TA) = BSSID = MAC AP
A3 (SA) = MAC R1

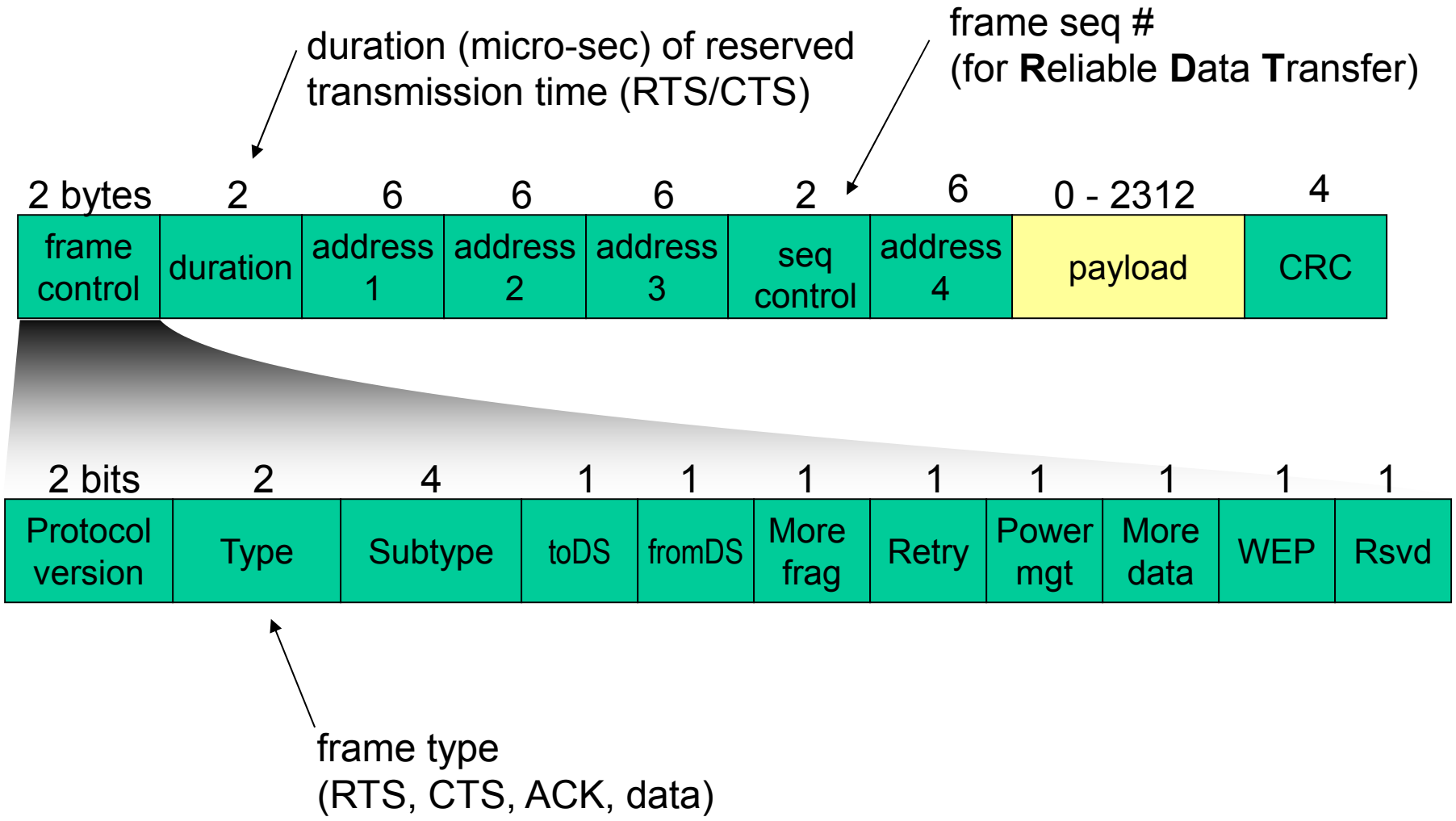



**toDS=1, fromDS=1**

A1 (RA) = MAC AP2
A2 (TA) = MAC AP1
A3 (DA) = MAC R2
A4 (SA) = MAC R1

DA - Destination Address - receptor final
SA - Source Address - origem da transmissão
RA - Receiver Address - estação wireless que deve processar a trama
wireless STA -> RA=DA
wired node -> RA=MAC AP; DA=router
TA - Transmitter Address - interface wireless que transmitiu a trama
BSSID - MAC da interface wireless do AP (Infrastructure networks);
aleatório BSSID (Ad-hoc networks)

# 802.11 frame: more



# 802.11 frame types and subtypes



Type 00 – Management frames
e.g. Beacon, Association request, Probe request, etc.

Type 01 – Control frames
e.g. RTS, CTS, ACK, etc.

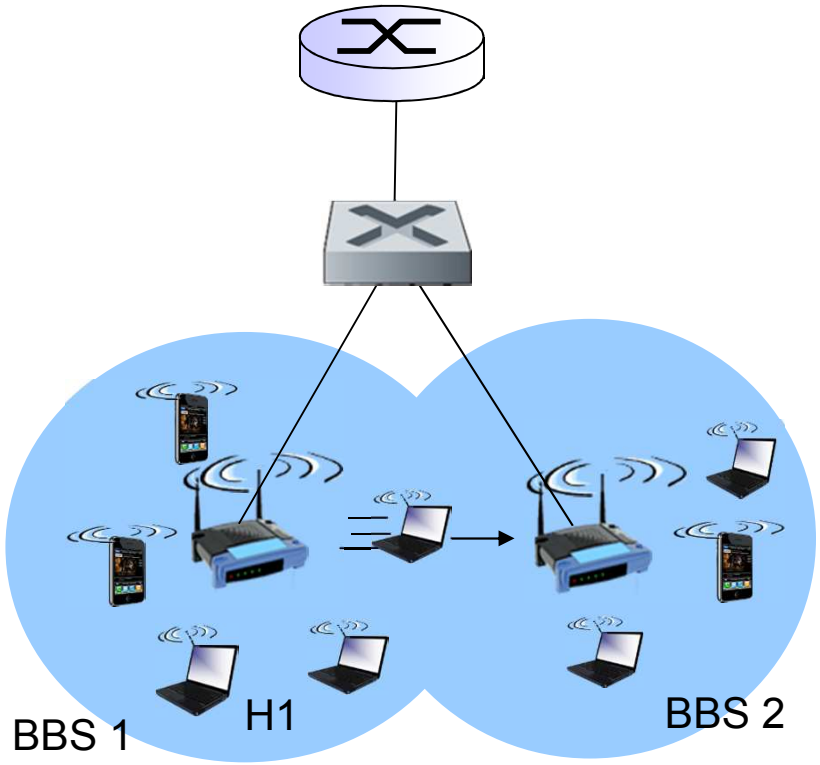
Type 10 – Data frames
e.g. Data

**Table 1—Valid type and subtype combinations**

| Type value b3 b2 | Type description | Subtype value b7 b6 b5 b4 | Subtype description |
|---|---|---|---|
| 00 | Management | 0000 | Association request |
| 00 | Management | 0001 | Association response |
| 00 | Management | 0010 | Reassociation request |
| 00 | Management | 0011 | Reassociation response |
| 00 | Management | 0100 | Probe request |
| 00 | Management | 0101 | Probe response |
| 00 | Management | 0110–0111 | Reserved |
| 00 | Management | 1000 | Beacon |
| 00 | Management | 1001 | Announcement traffic indication message (ATIM) |
| 00 | Management | 1010 | Disassociation |
| 00 | Management | 1011 | Authentication |
| 00 | Management | 1100 | Deauthentication |
| 00 | Management | 1101–1111 | Reserved |
| 01 | Control | 0000–1001 | Reserved |
| 01 | Control | 1010 | Power Save (PS)-Poll |
| 01 | Control | 1011 | Request To Send (RTS) |
| 01 | Control | 1100 | Clear To Send (CTS) |
| 01 | Control | 1101 | Acknowledgment (ACK) |
| 01 | Control | 1110 | Contention-Free (CF)-End |
| 01 | Control | 1111 | CF-End + CF-Ack |
| 10 | Data | 0000 | Data |
| 10 | Data | 0001 | Data + CF-Ack |
| 10 | Data | 0010 | Data + CF-Poll |
| 10 | Data | 0011 | Data + CF-Ack + CF-Poll |
| 10 | Data | 0100 | Null function (no data) |
| 10 | Data | 0101 | CF-Ack (no data) |
| 10 | Data | 0110 | CF-Poll (no data) |
| 10 | Data | 0111 | CF-Ack + CF-Poll (no data) |
| 10 | Data | 1000–1111 | Reserved |
| 11 | Reserved | 0000–1111 | Reserved |

# 802.11: mobility within same subnet

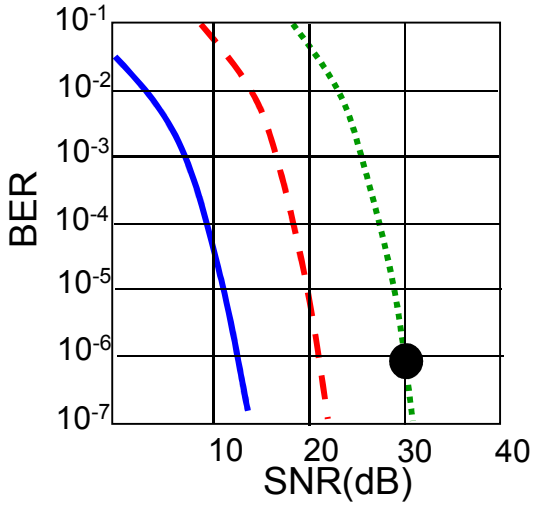
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1



# 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

# Chapter 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics

- CDMA

6.3 IEEE 802.11 wireless LANs ("Wi-Fi")

6.4 Cellular Internet access

- architecture
- standards (e.g., GSM)

Mobility

6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

6.7 Handling mobility in cellular networks

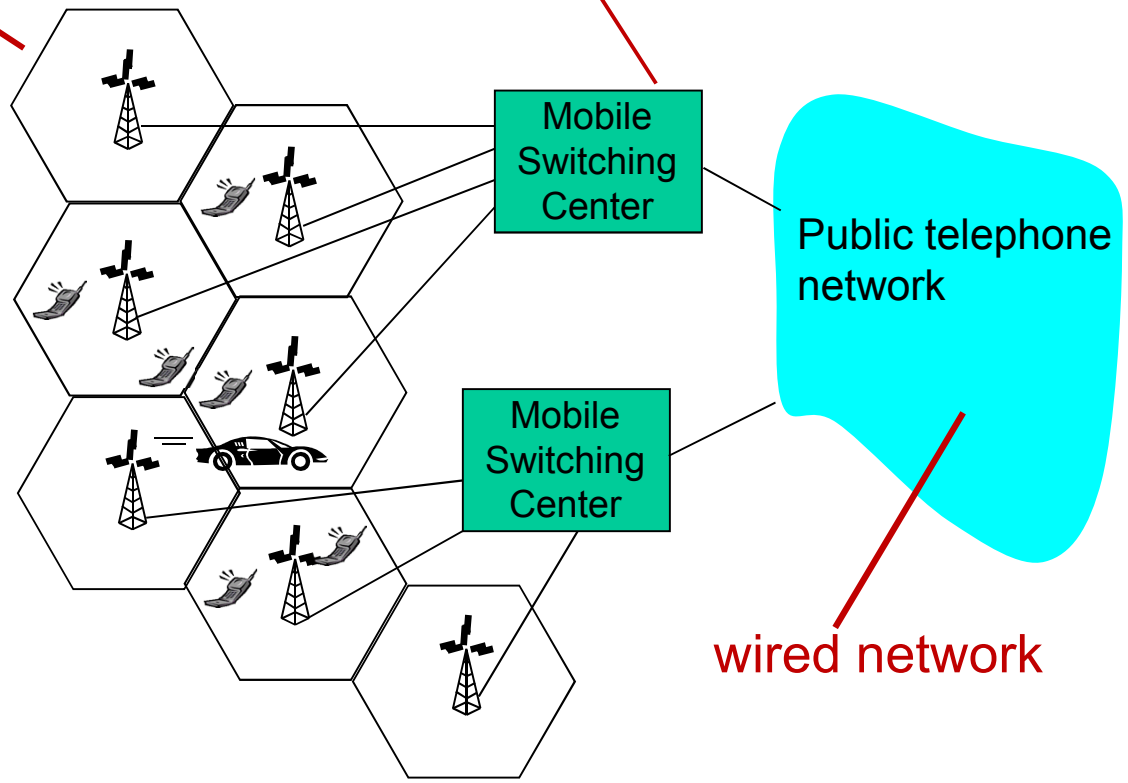
6.8 Mobility and higher-layer protocols

6.9 Summary

# Components of cellular network architecture

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

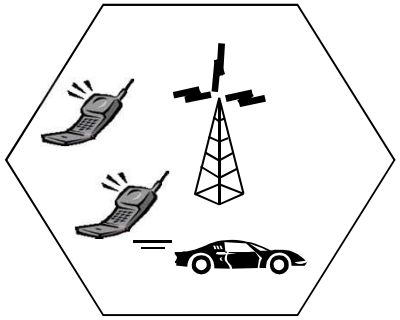
**cell**
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS

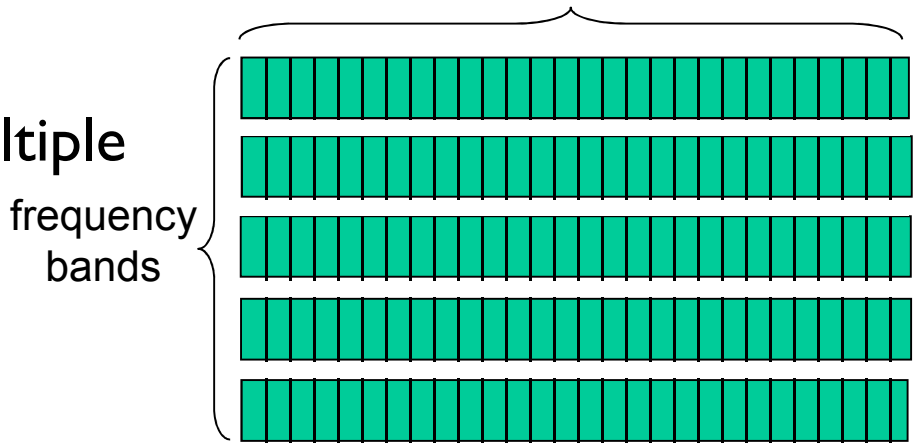


# Cellular networks: the first hop

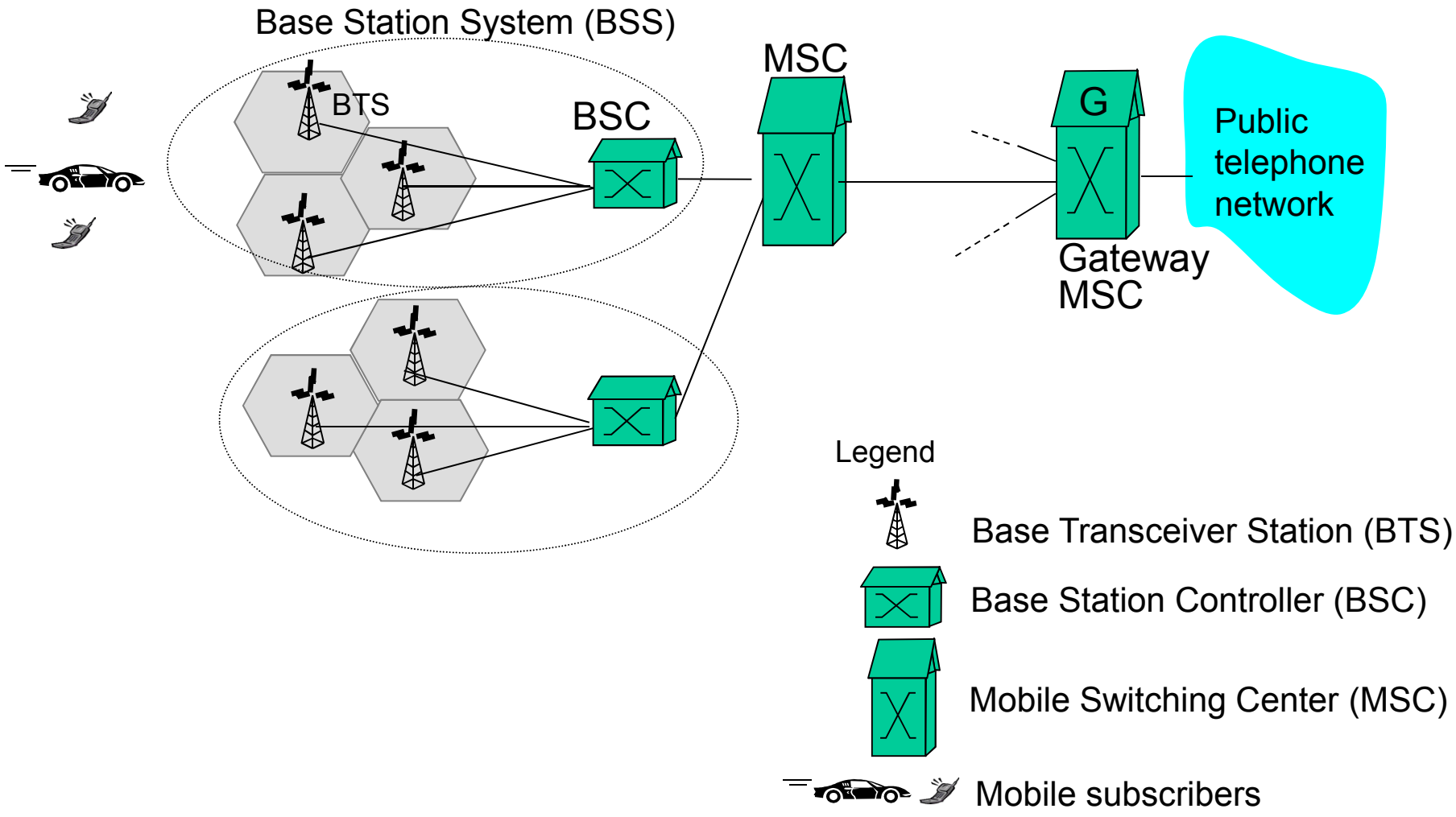
Two techniques for sharing mobile-to-BS radio spectrum

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

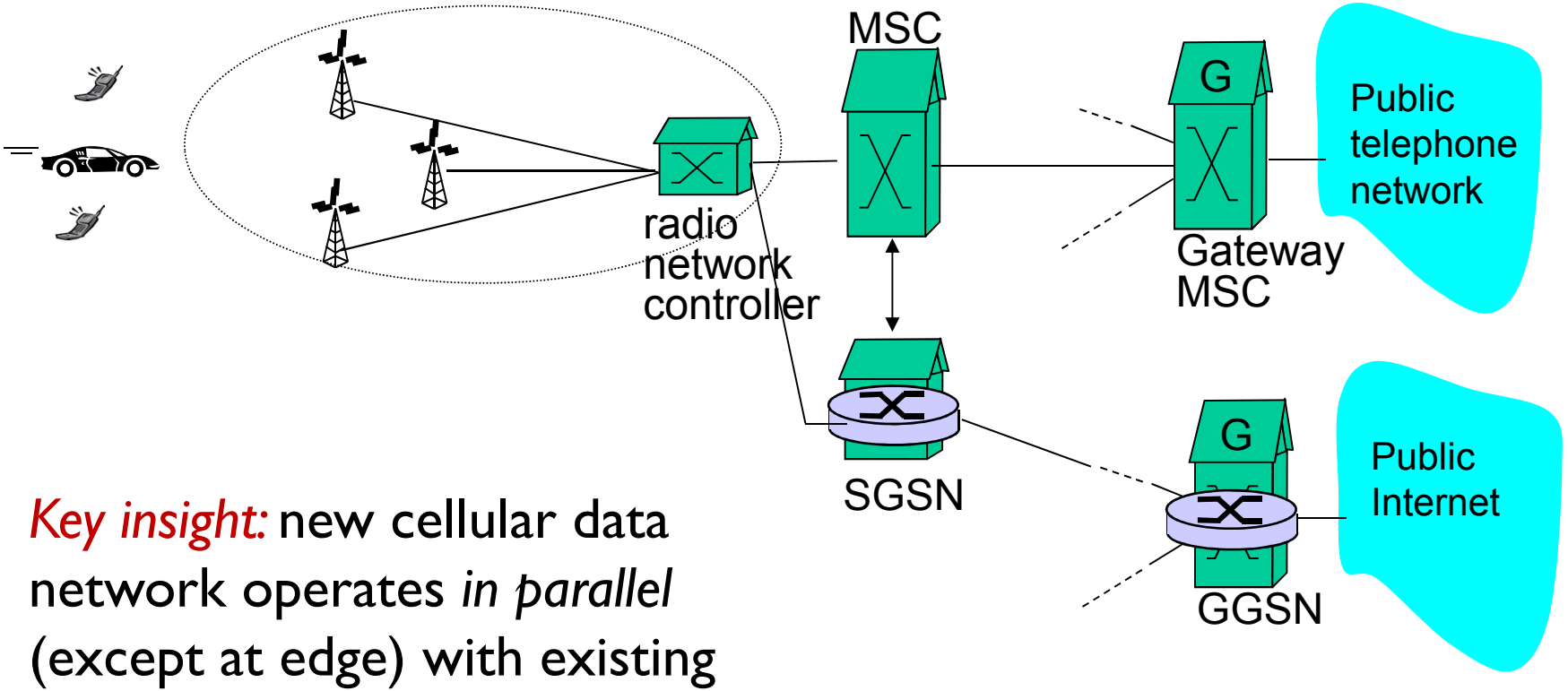




# 2G (voice) network architecture



# 3G (voice+data) network architecture



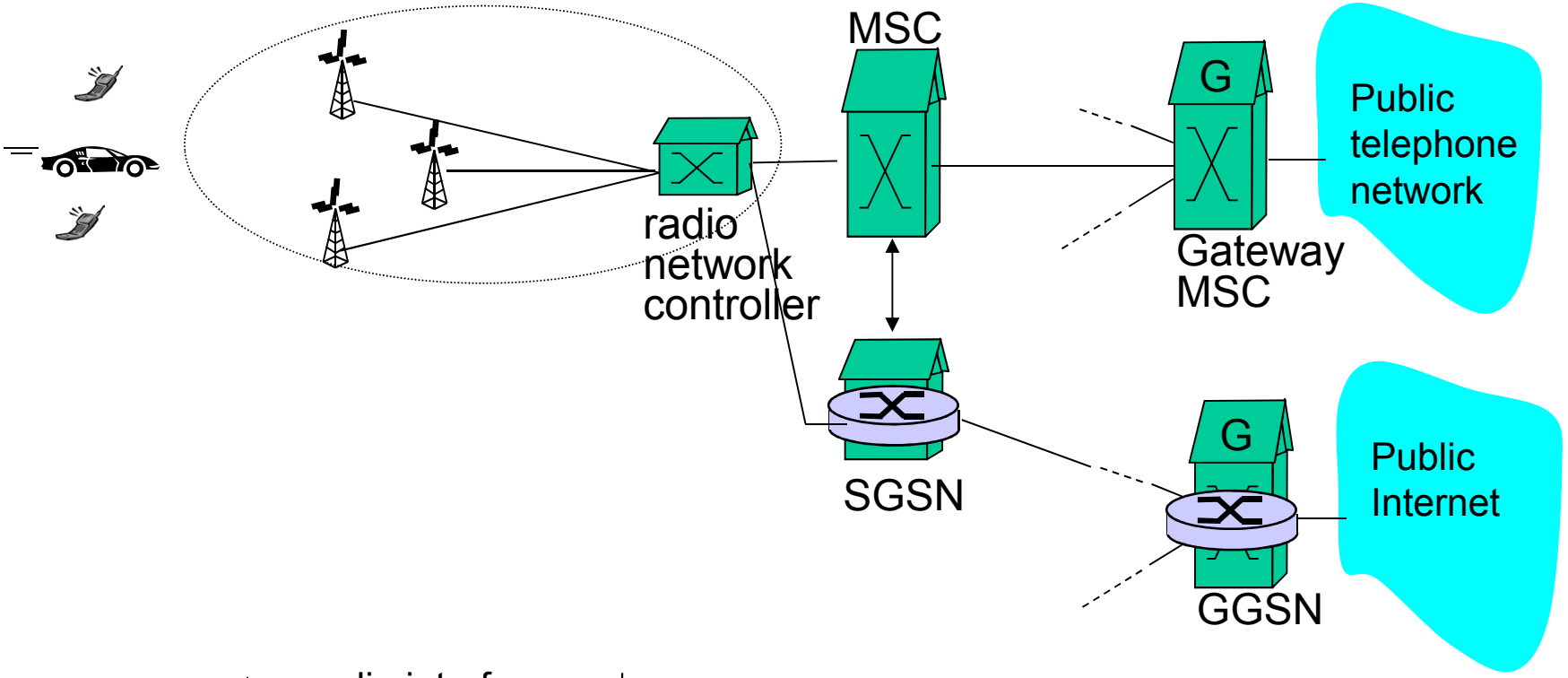

*Key insight:* new cellular data network operates *in parallel* (except at edge) with existing cellular voice network

- 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



# Chapter 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics
- CDMA

6.3 IEEE 802.11 wireless LANs ("Wi-Fi")

6.4 Cellular Internet Access
- architecture
- standards (e.g., GSM)

Mobility

6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

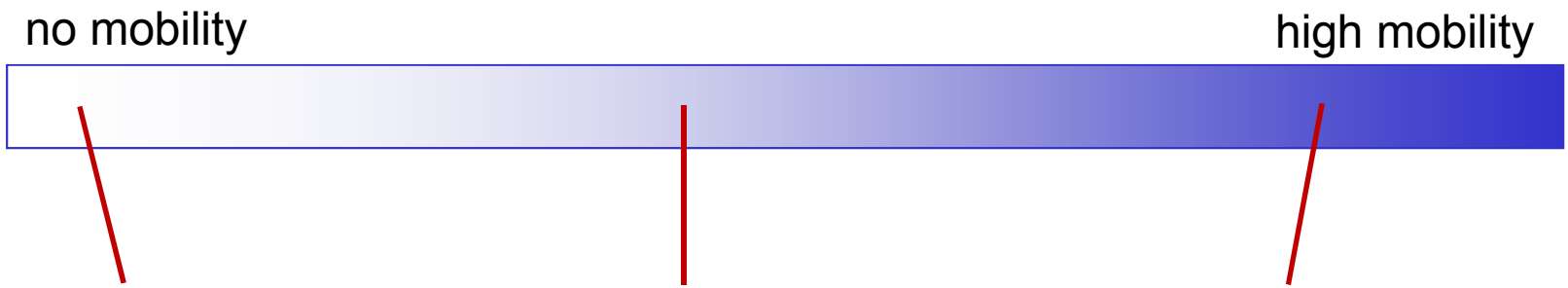
6.7 Handling mobility in cellular networks

6.8 Mobility and higher-layer protocols

6.9 Summary

# What is mobility?

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




mobile wireless user, using same access point

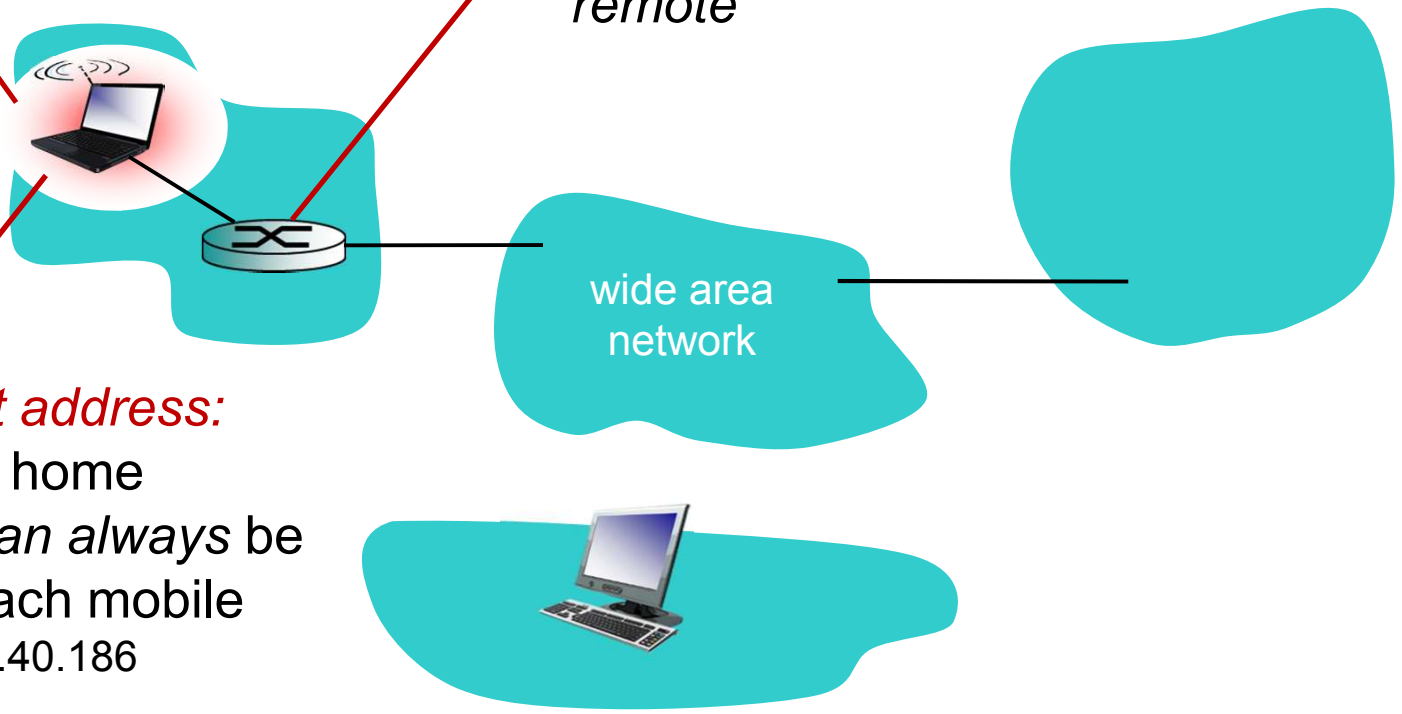
mobile user, connecting/ disconnecting from network using DHCP.

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*



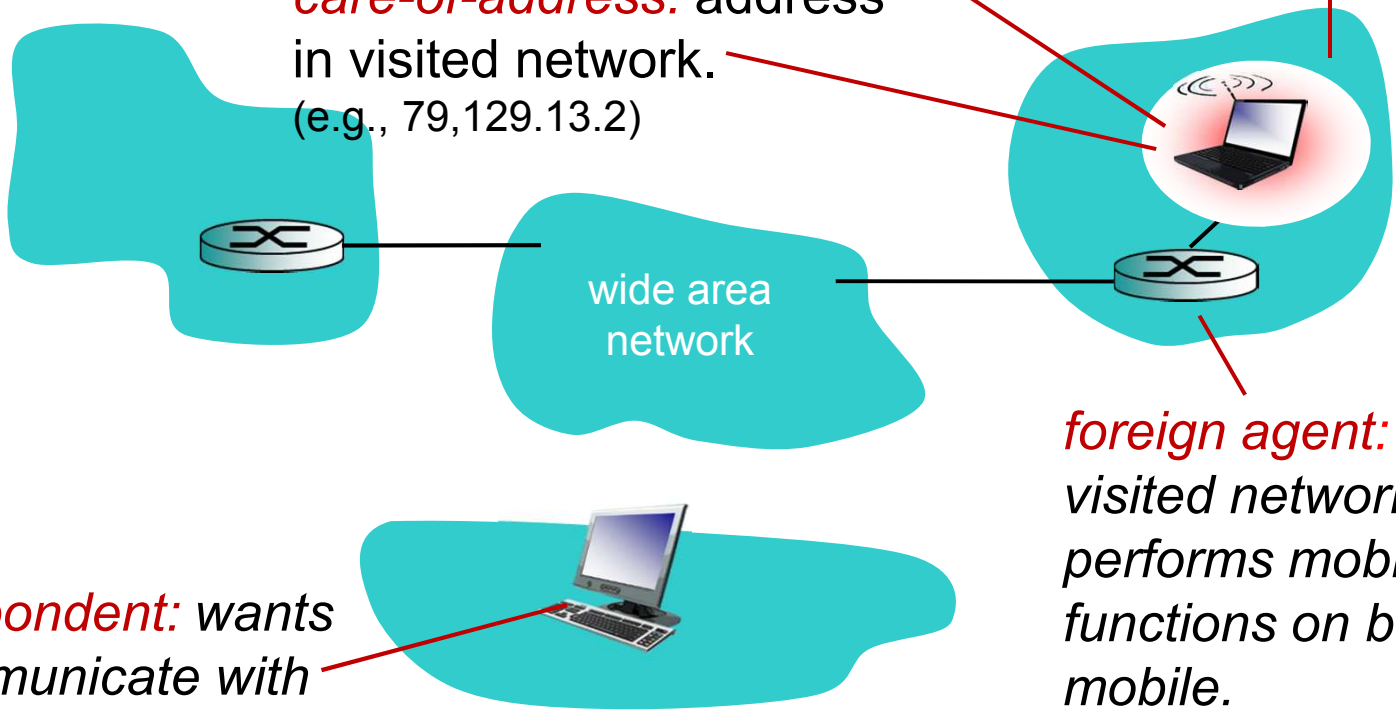

*permanent address:*
address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

# 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)



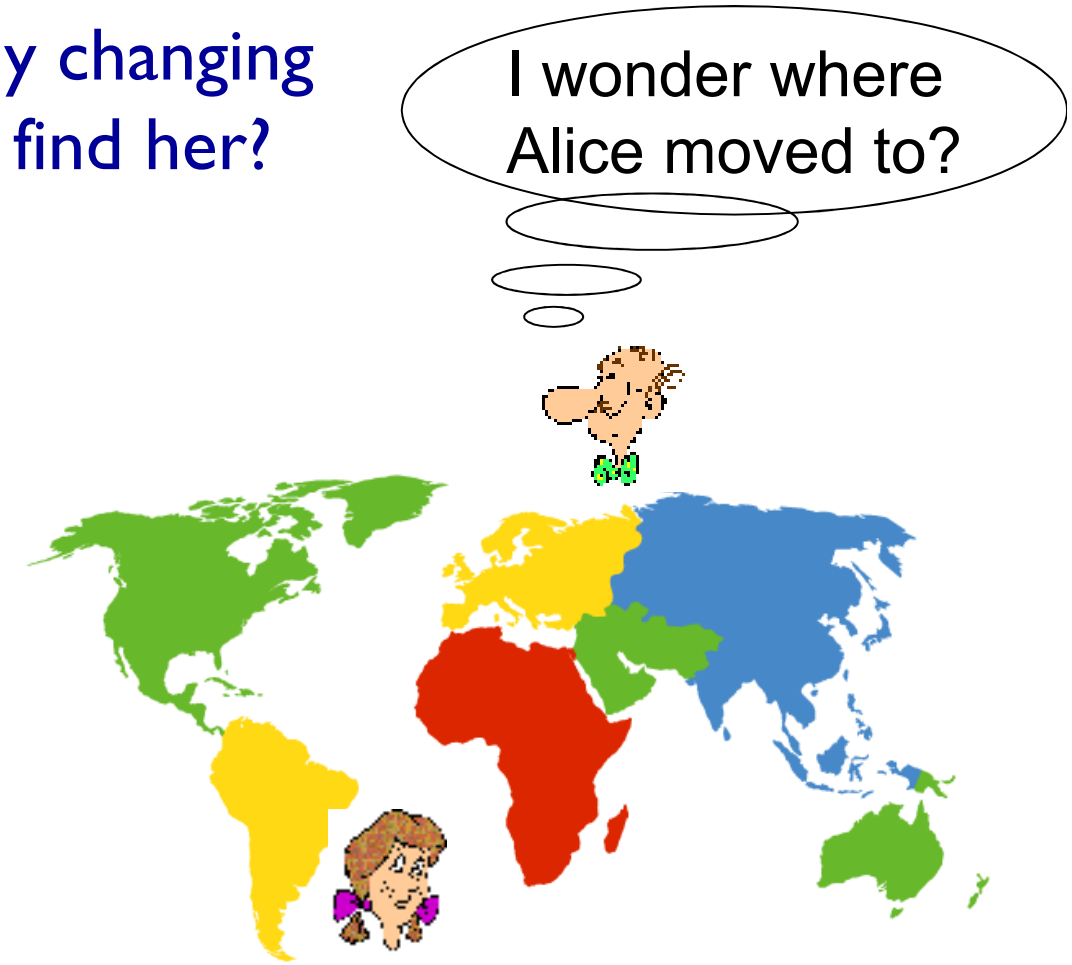

*foreign agent:* *entity in visited network that performs mobility functions on behalf of mobile.*

*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?

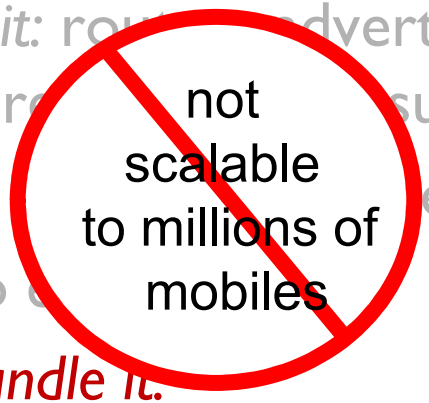


# Mobility: approaches

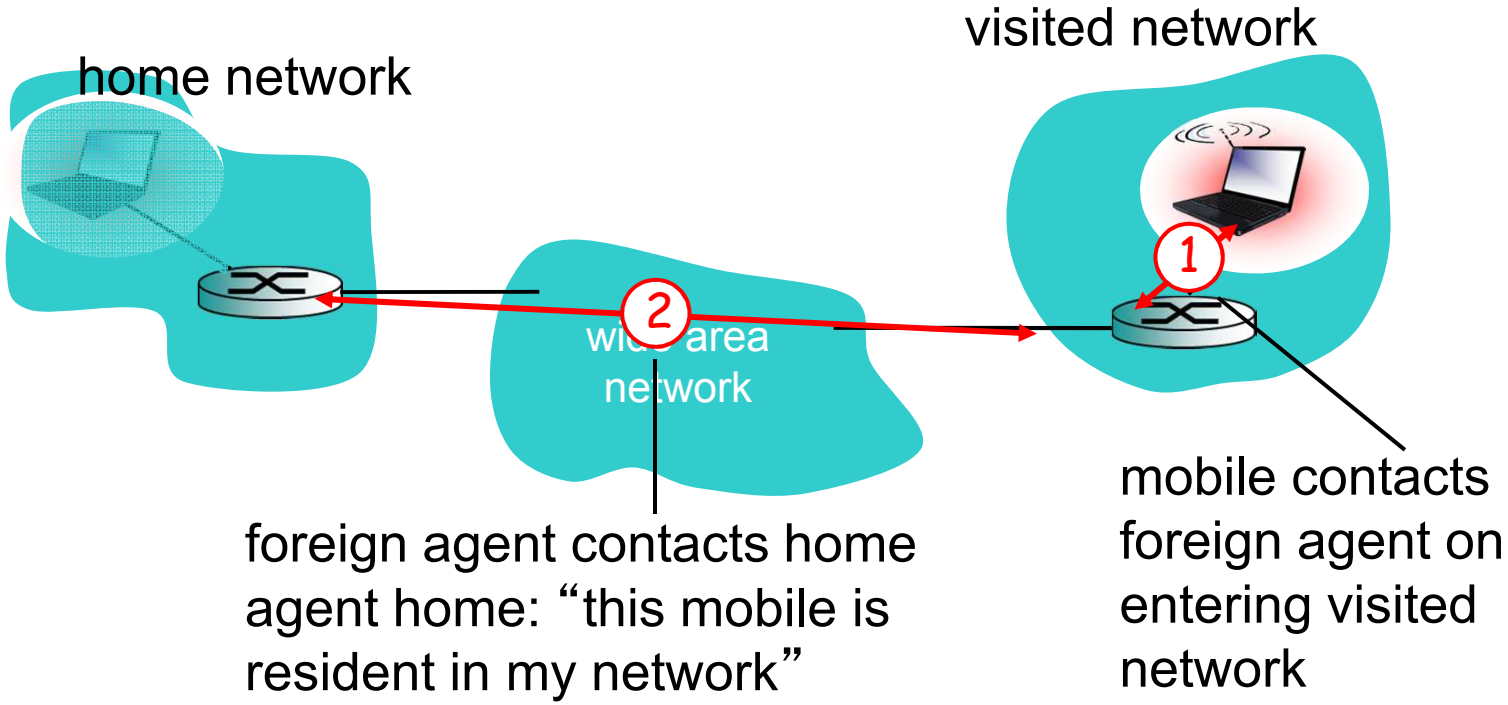
- *let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to 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 location of 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



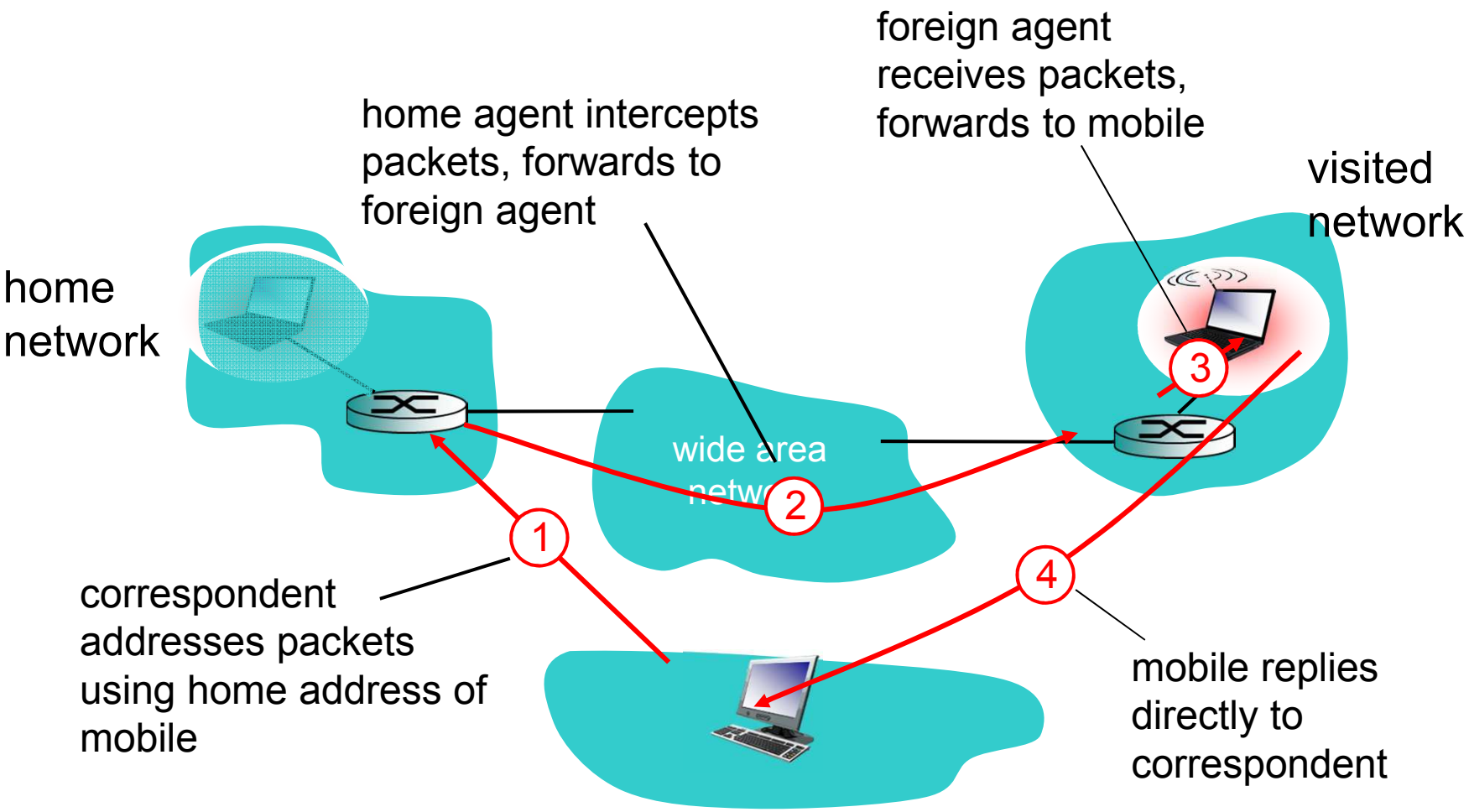
# Mobility: registration




end result:

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

# Mobility via indirect routing



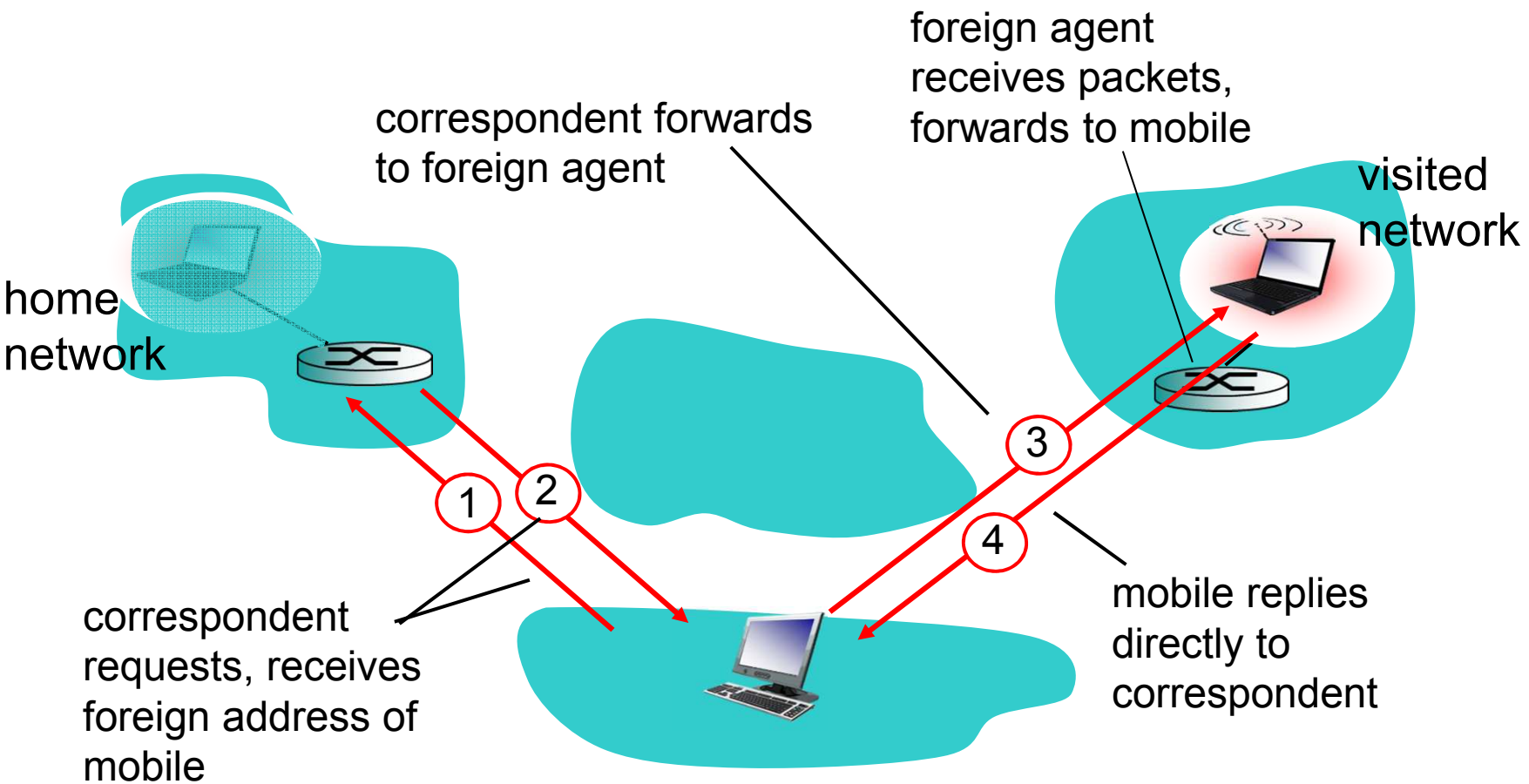
# Indirect Routing: comments

- 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

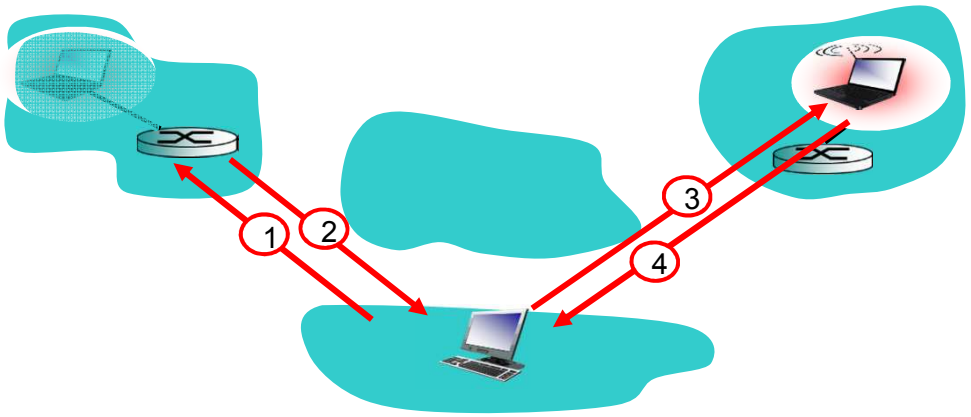
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: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

# Mobility via direct routing



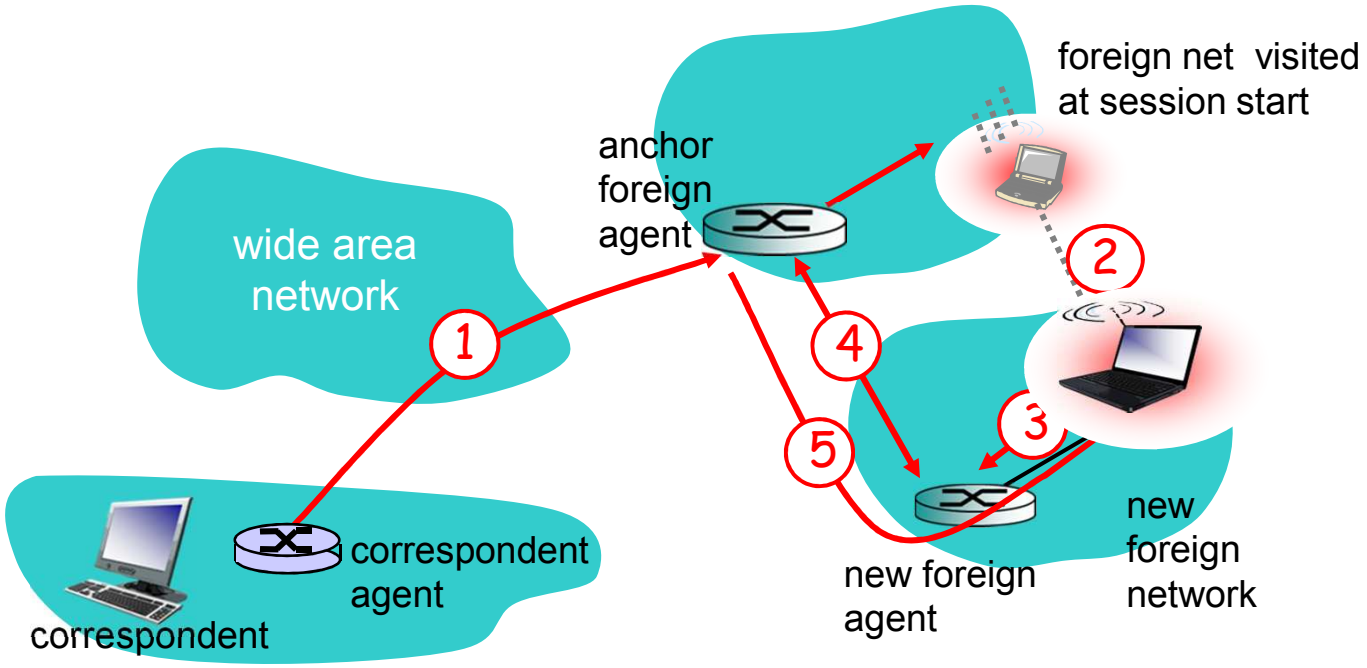
# Mobility via direct routing: comments

- 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 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics
- CDMA

6.3 IEEE 802.11 wireless LANs ("Wi-Fi")

6.4 Cellular Internet Access
- architecture
- standards (e.g., GSM)

Mobility

6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

6.7 Handling mobility in cellular networks

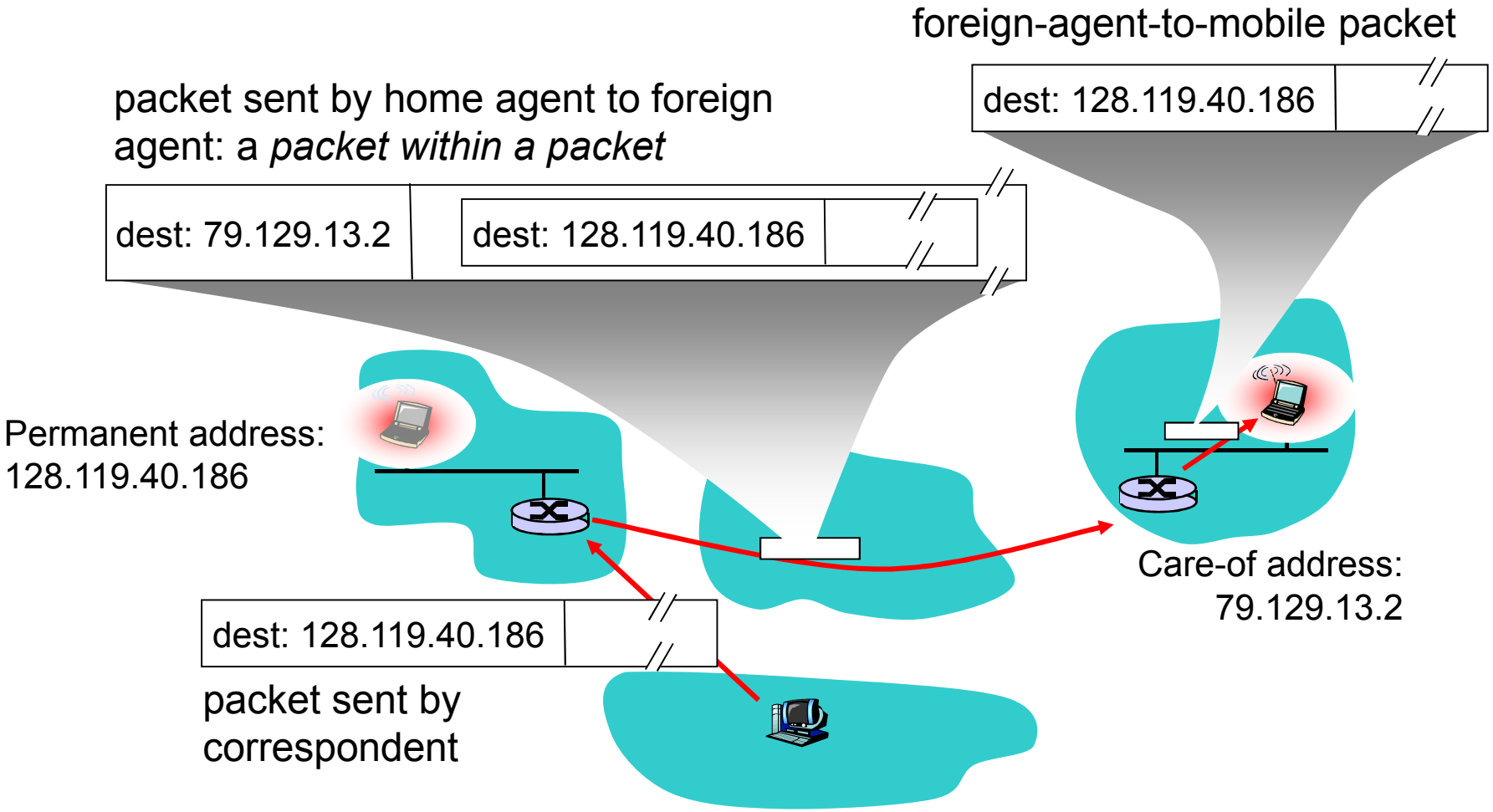
6.8 Mobility and higher-layer protocols

6.9 Summary

# 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

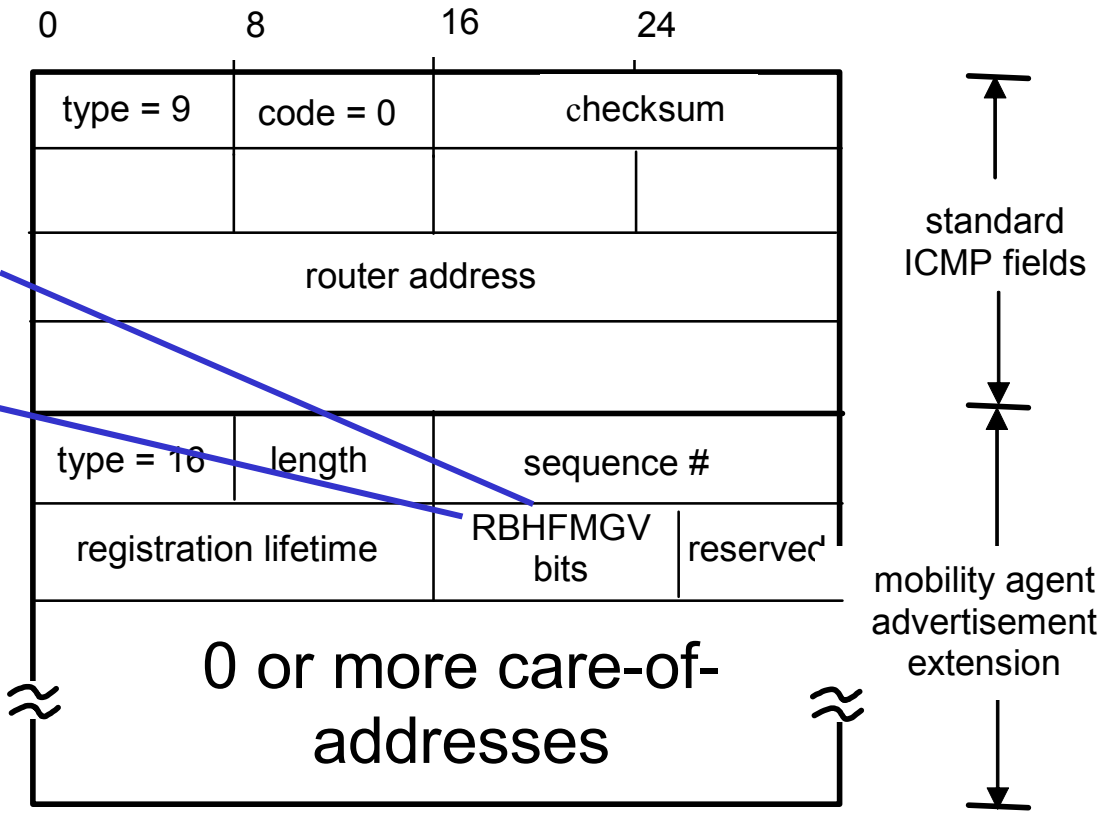


# Mobile IP: agent discovery

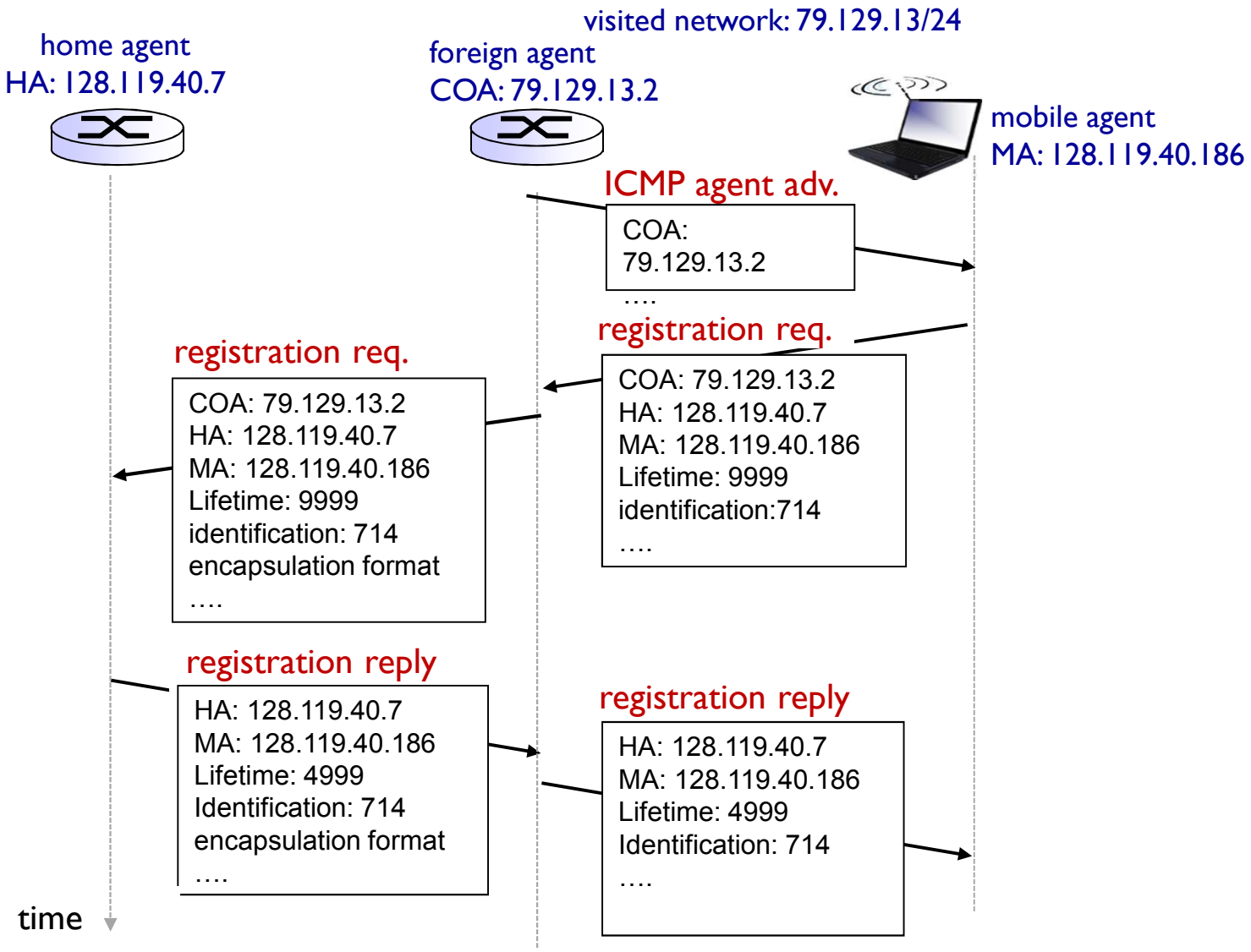
- *agent advertisement:* foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)

H,F bits: home and/or foreign agent

R bit: registration required

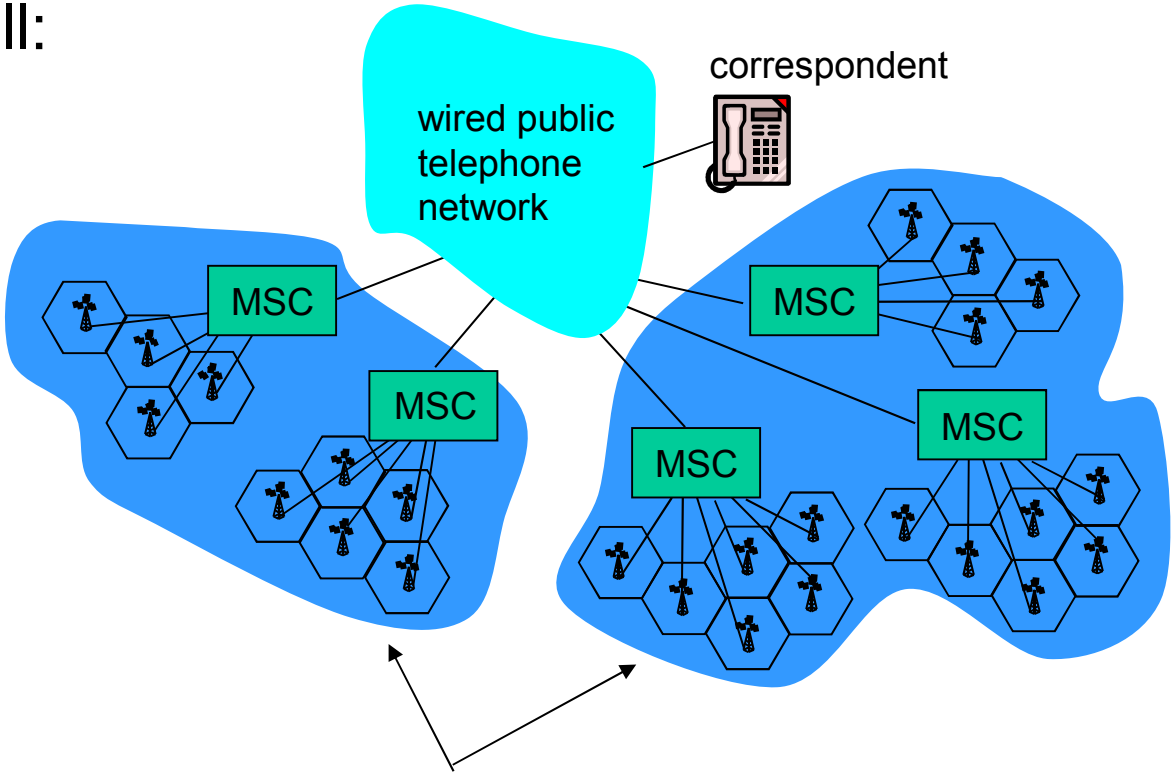


# Mobile IP: registration example



# Components of cellular network architecture

recall:

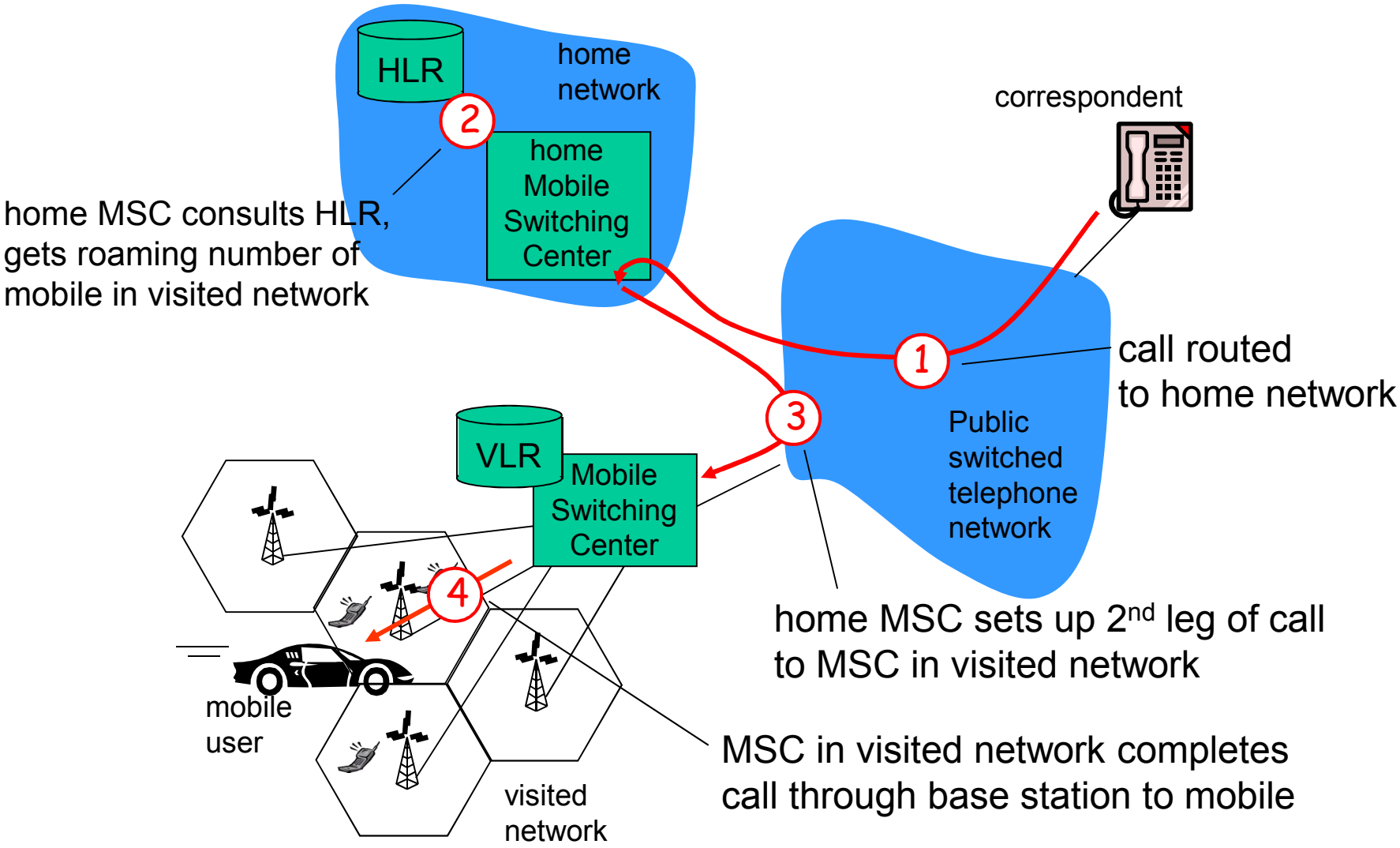



different cellular networks,
operated by different providers

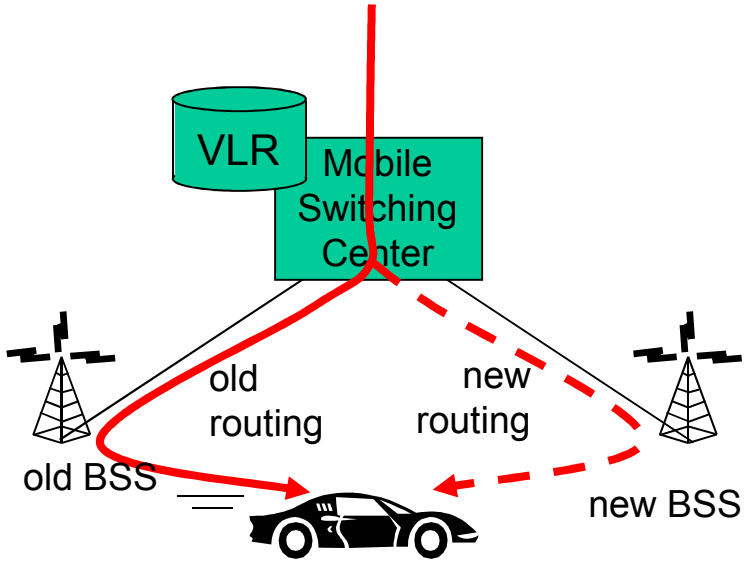
# Handling mobility in cellular networks

- *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

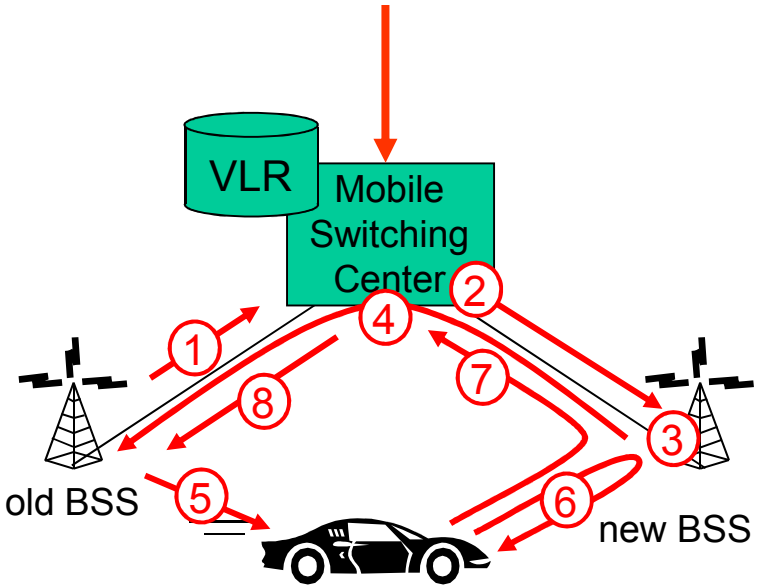


# GSM: handoff with common MSC




- *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 doesnt mandate why to perform handoff (policy), only how (mechanism)
- handoff initiated by old BSS

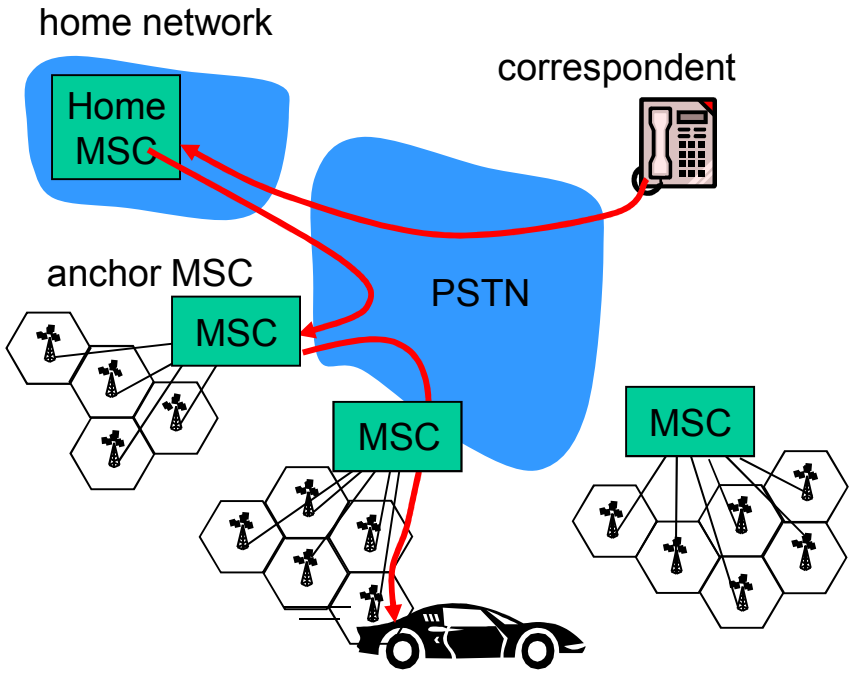
# GSM: handoff with common MSC




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

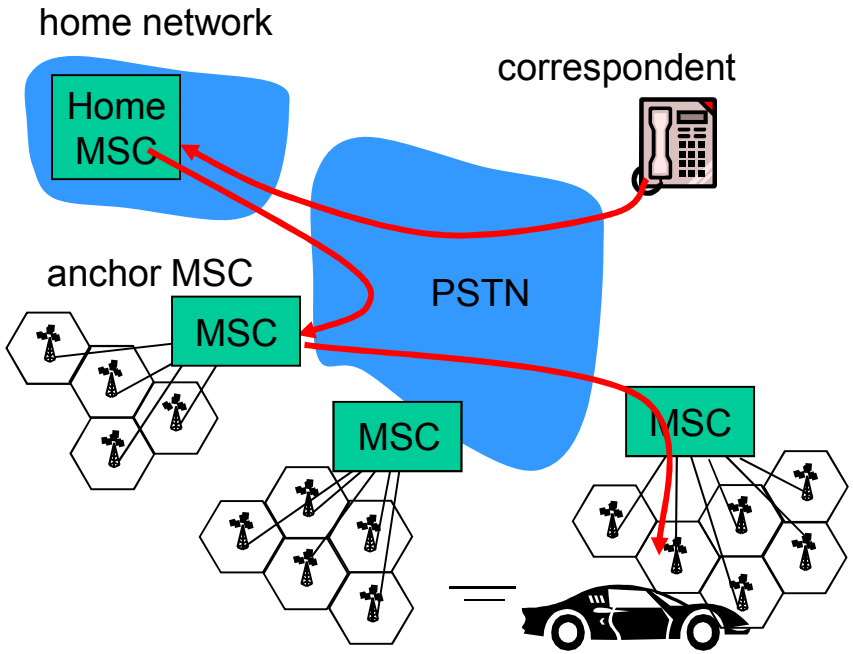
# GSM: handoff between MSCs




(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




(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