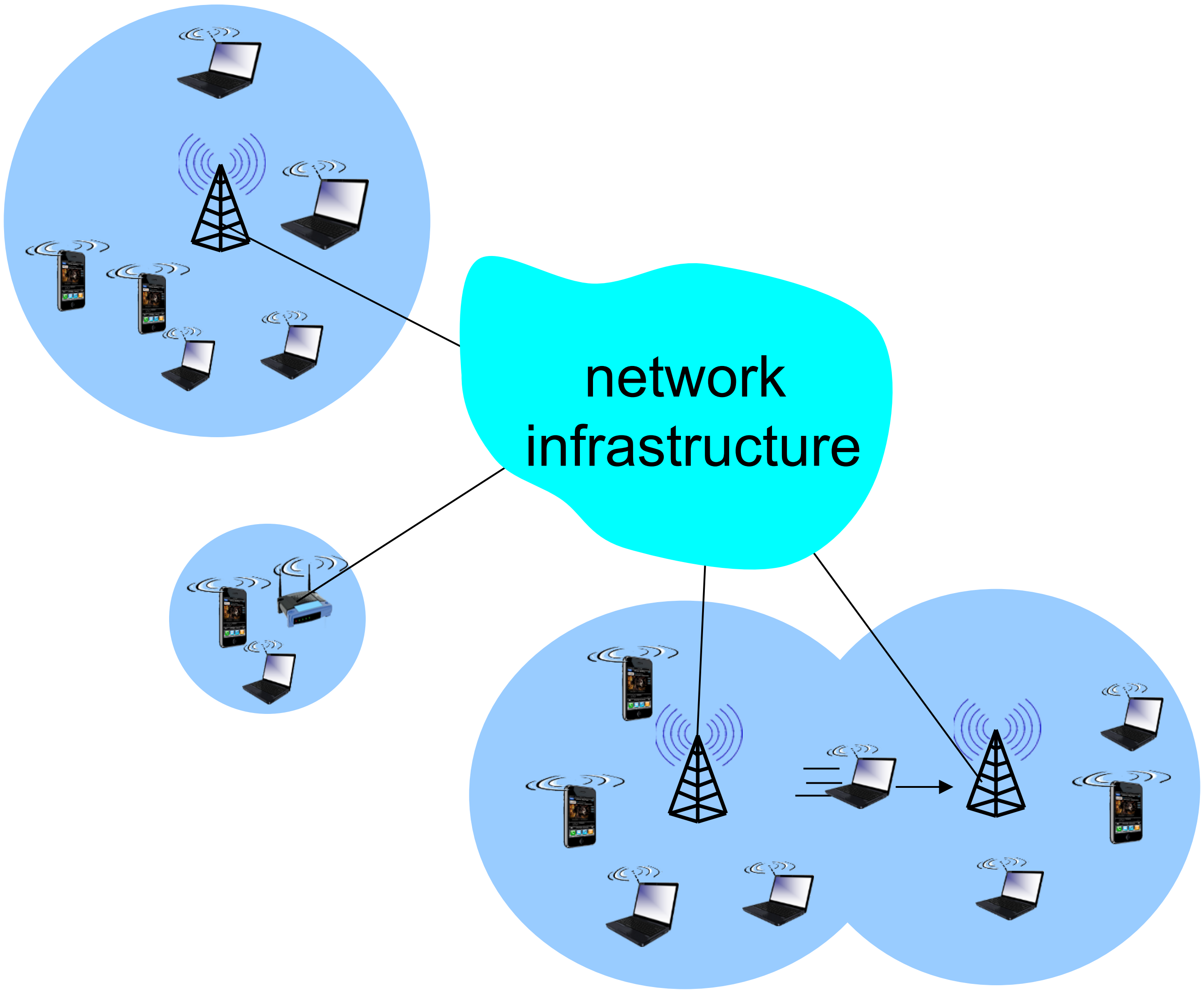
University of Duisburg-Essen
Networked Embedded Systems Group
Institute for Computer Science and
Business Information Systems (ICB)
Schützenbahn 70
D-45127 Essen, Germany

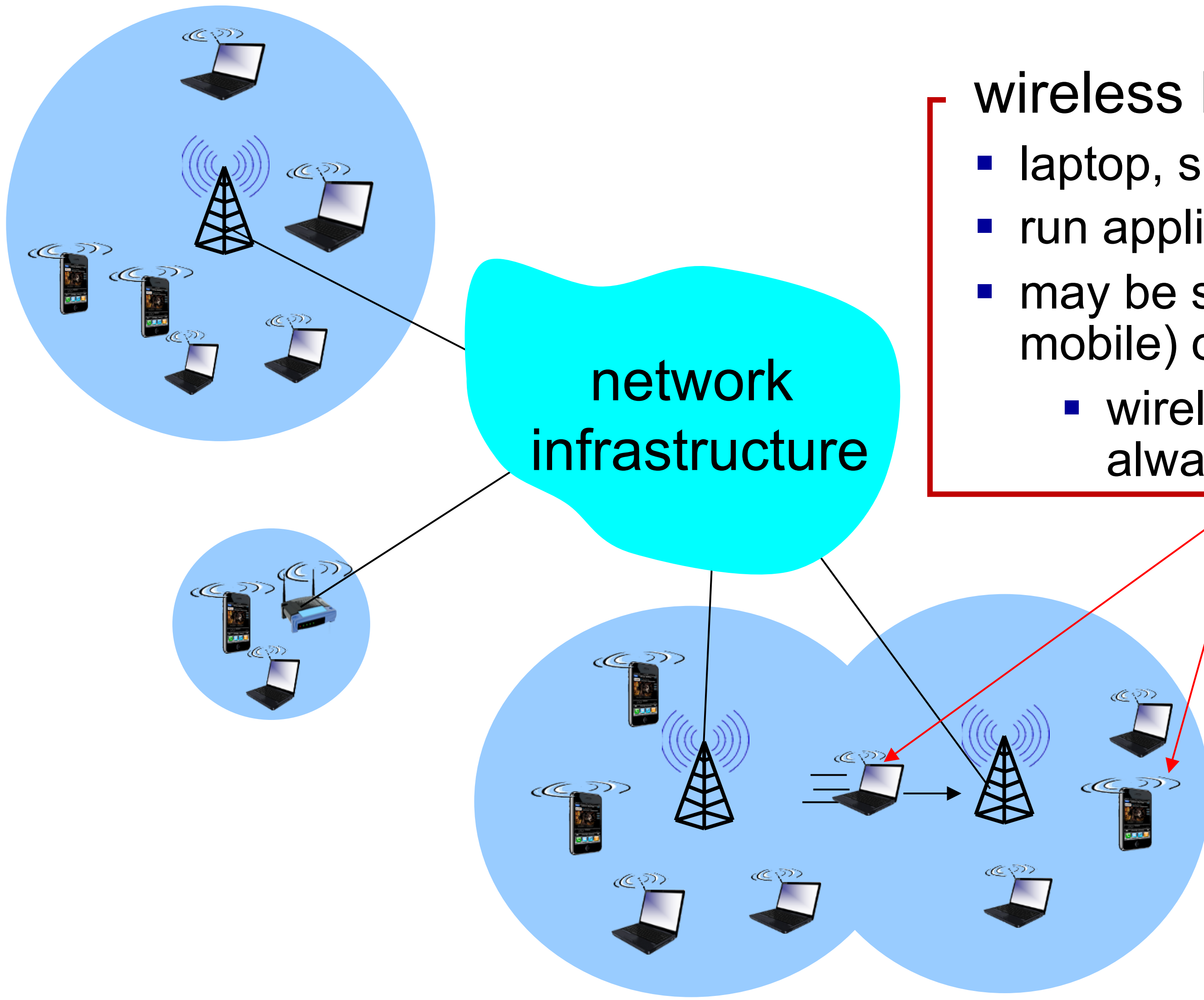
Kommunikationsnetze 2
8 – Wireless and Mobile Networks

Prof. Dr. Pedro José Marrón

Elements of a Wireless Network



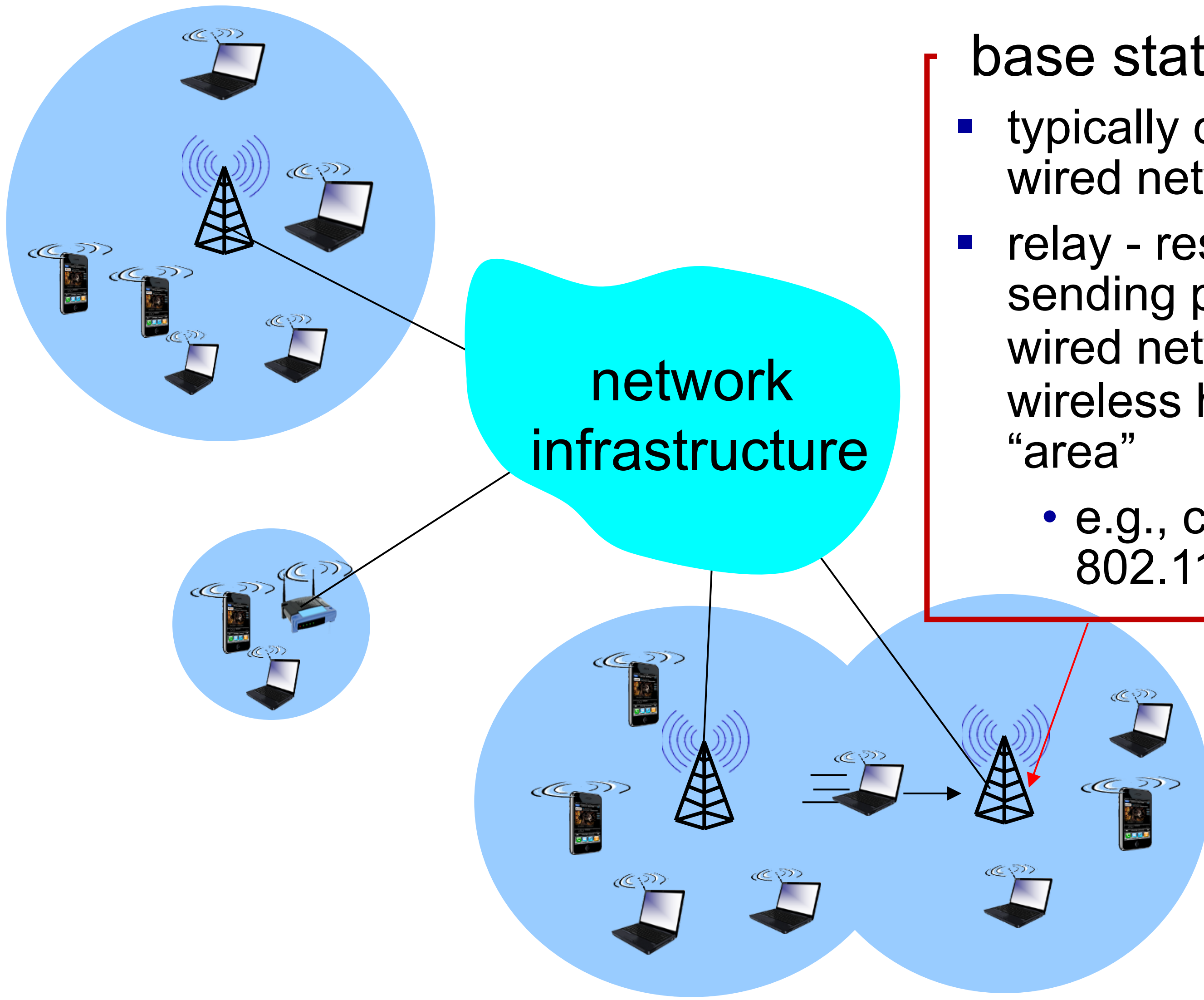
Elements of a Wireless Network



wireless hosts

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

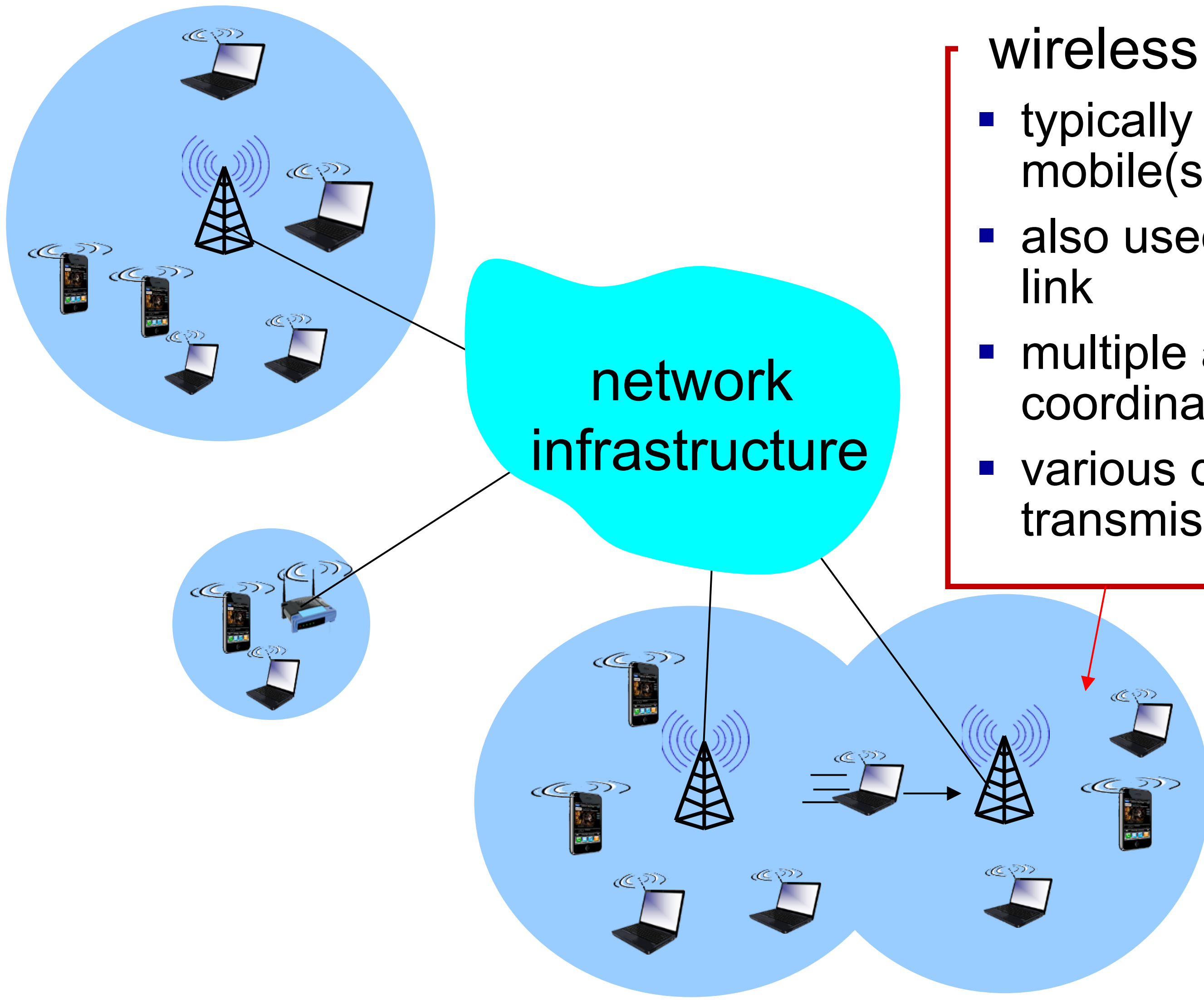
Elements of a Wireless Network



base stations

- 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

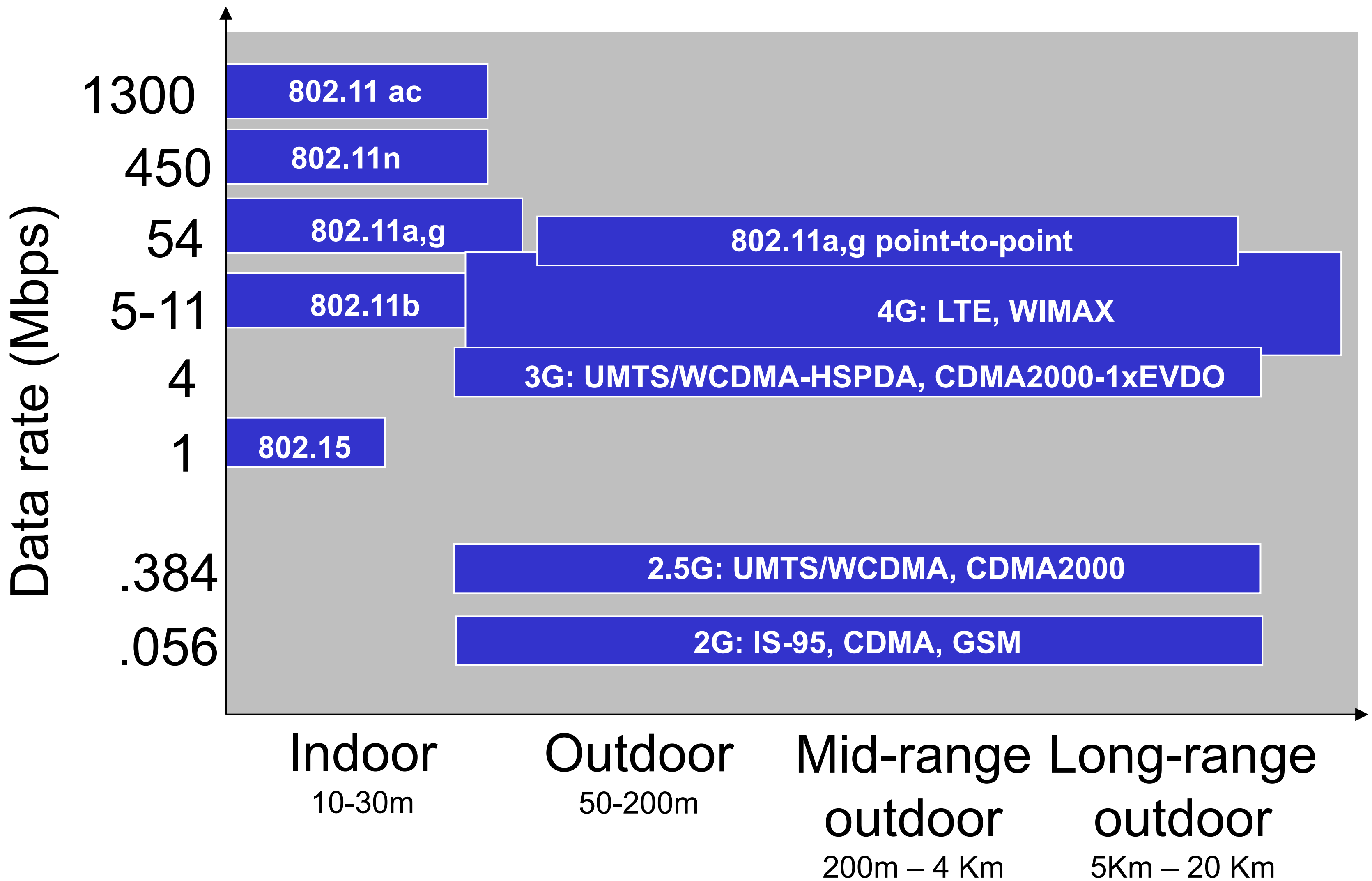
Elements of a Wireless Network



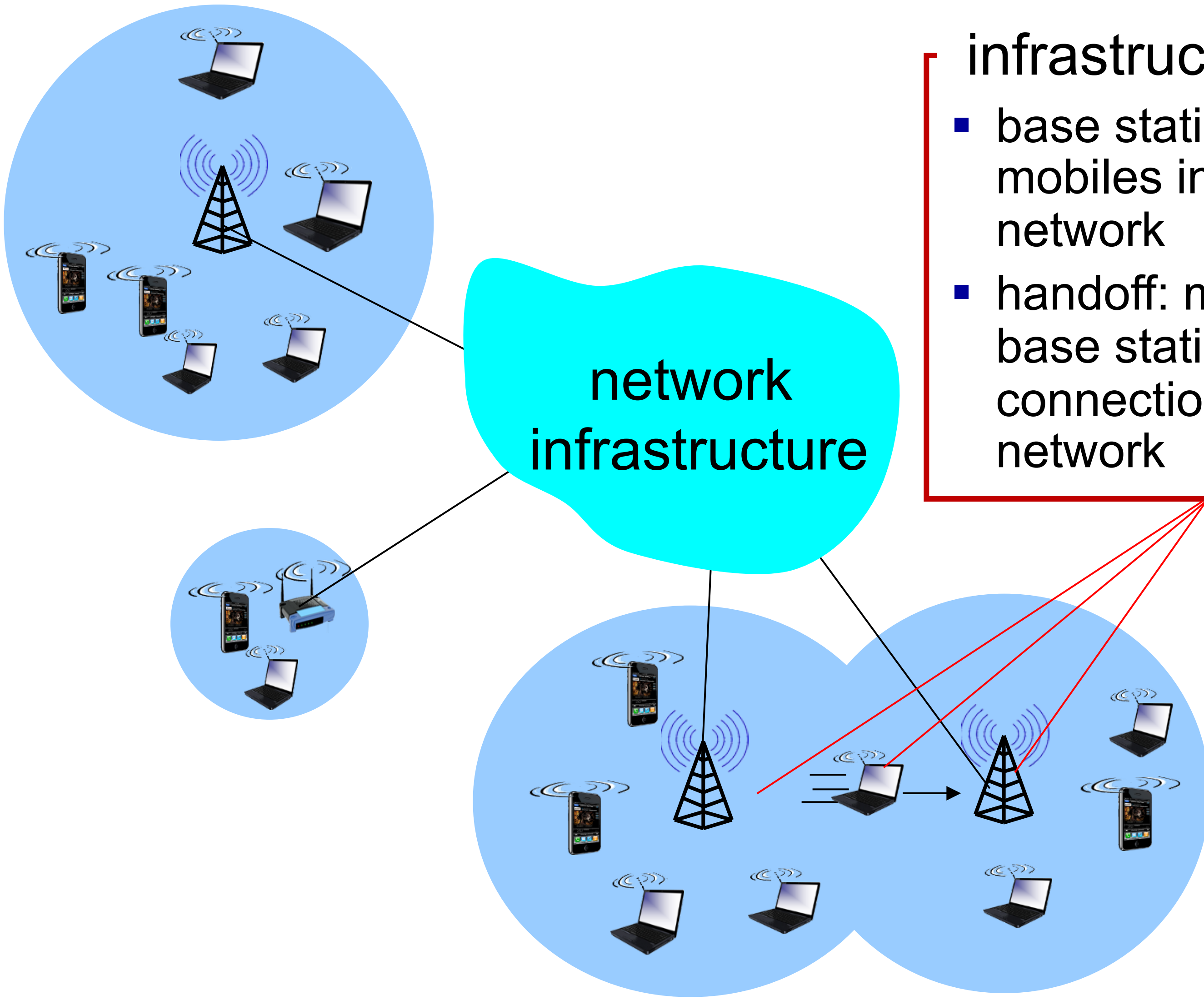
wireless link

- 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



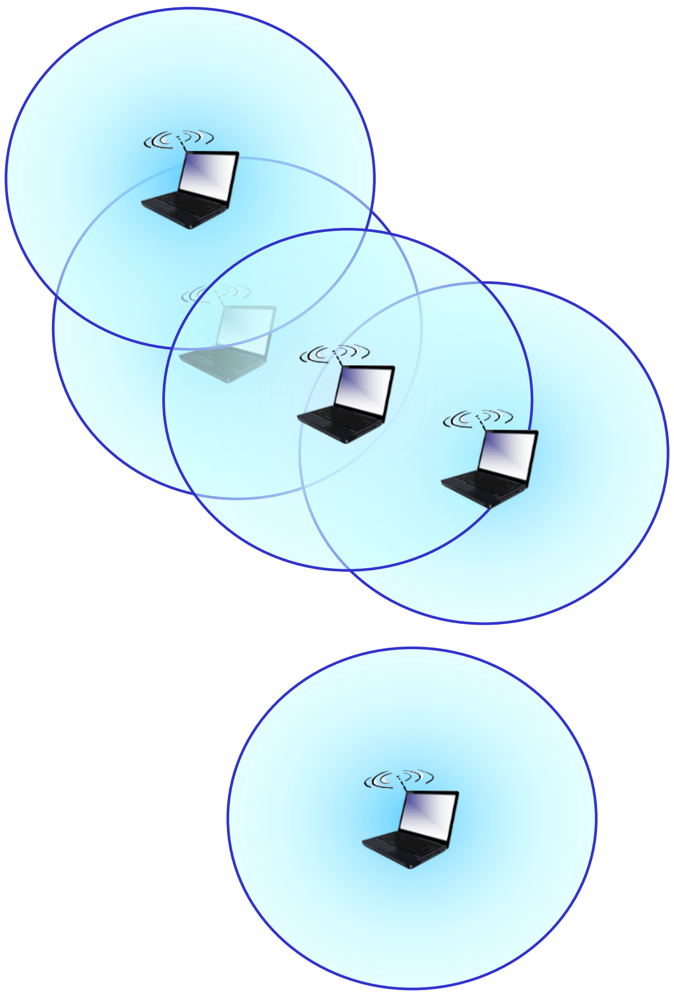
Elements of a Wireless Network



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

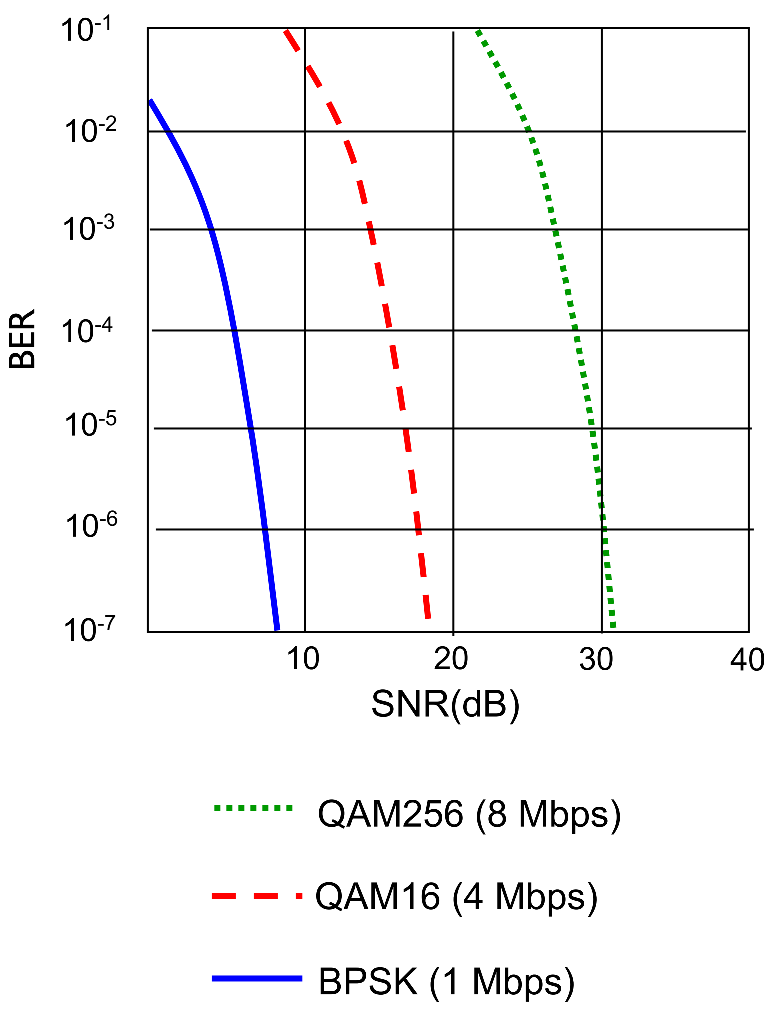
	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet (mesh net)
no infrastructure	no base station, no connection to larger Internet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

Wireless Link Characteristics (1)

- Important differences from wired link…
  - Decrease 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 are reflected by objects, ground, … arriving at destination at slightly different times
- Communication across wireless links is much more “challenging”

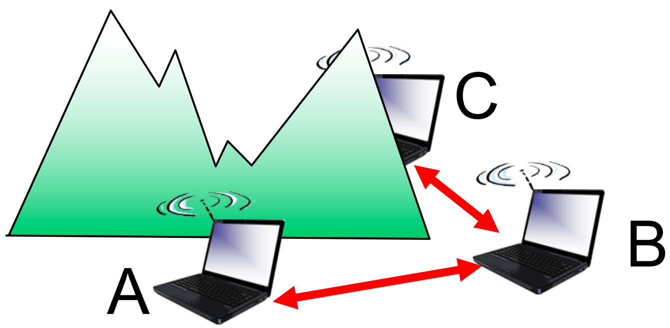
Wireless Link Characteristics (2)

- SNR: Signal-to-Noise Ratio
  - Larger SNR – easier to extract signal from noise
- SNR versus BER
  - 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)



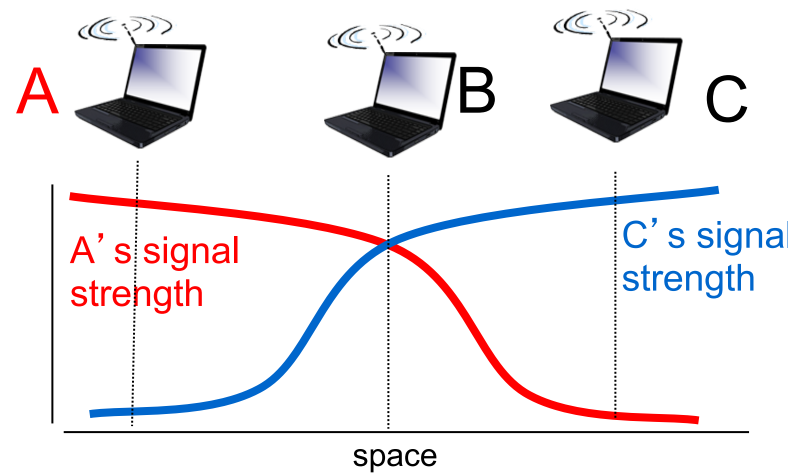
Wireless Network Characteristics

- Multiple wireless senders and receivers create additional problems



Hidden terminal problem

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



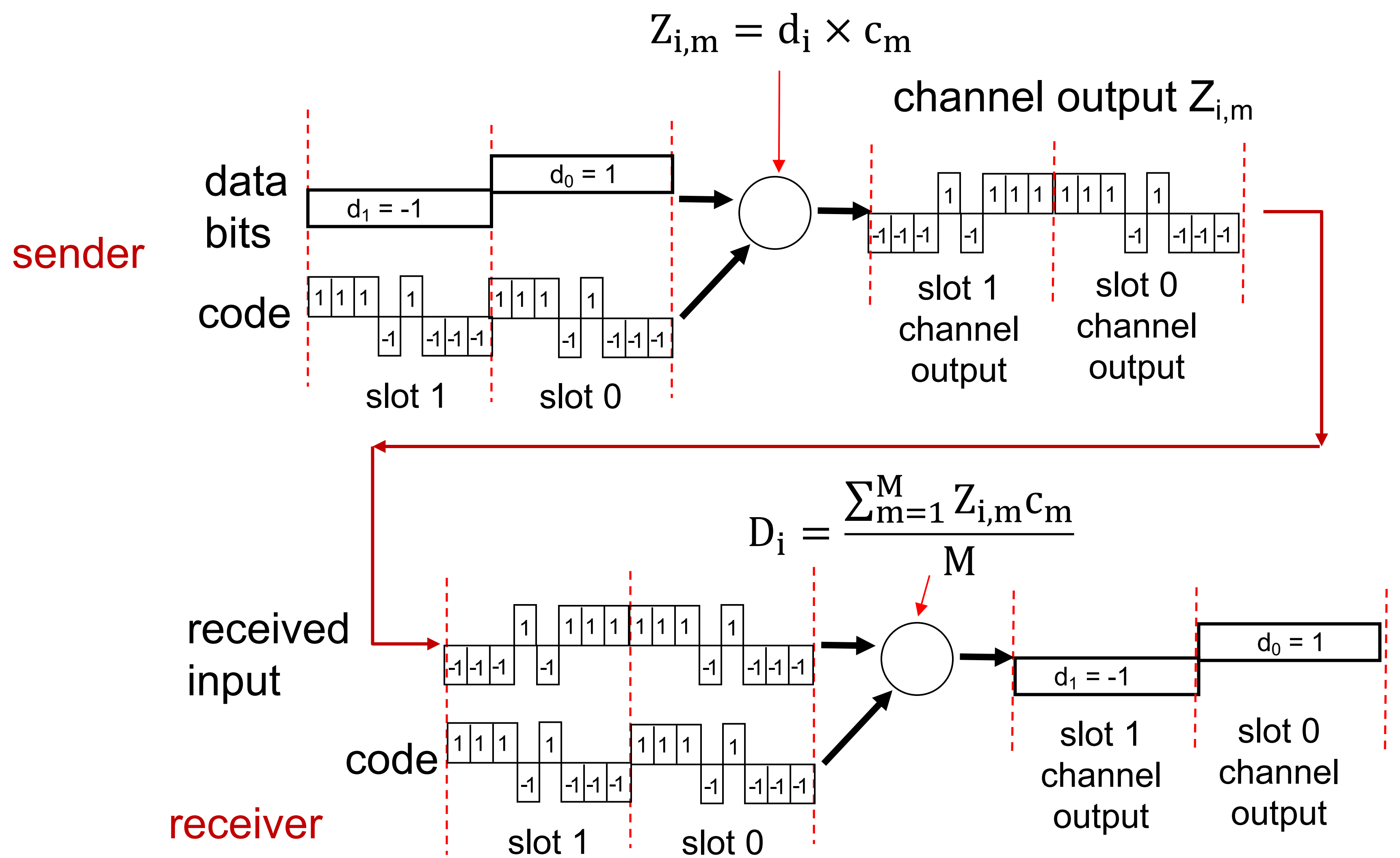
Signal attenuation

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

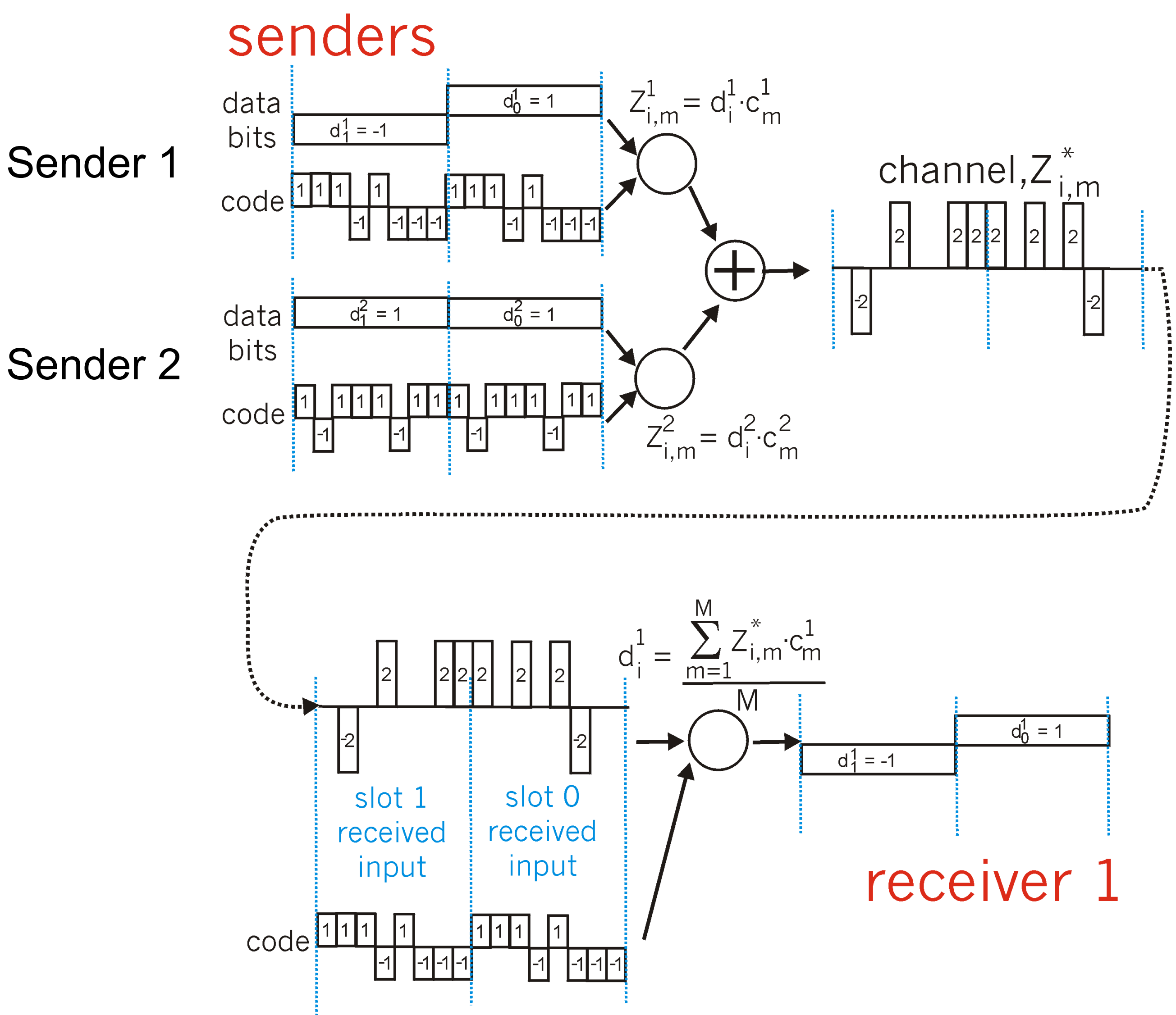
Code Division Multiple Access (CDMA)

- Unique “code” assigned to each host
  - 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



CDMA: Two-Sender Interference



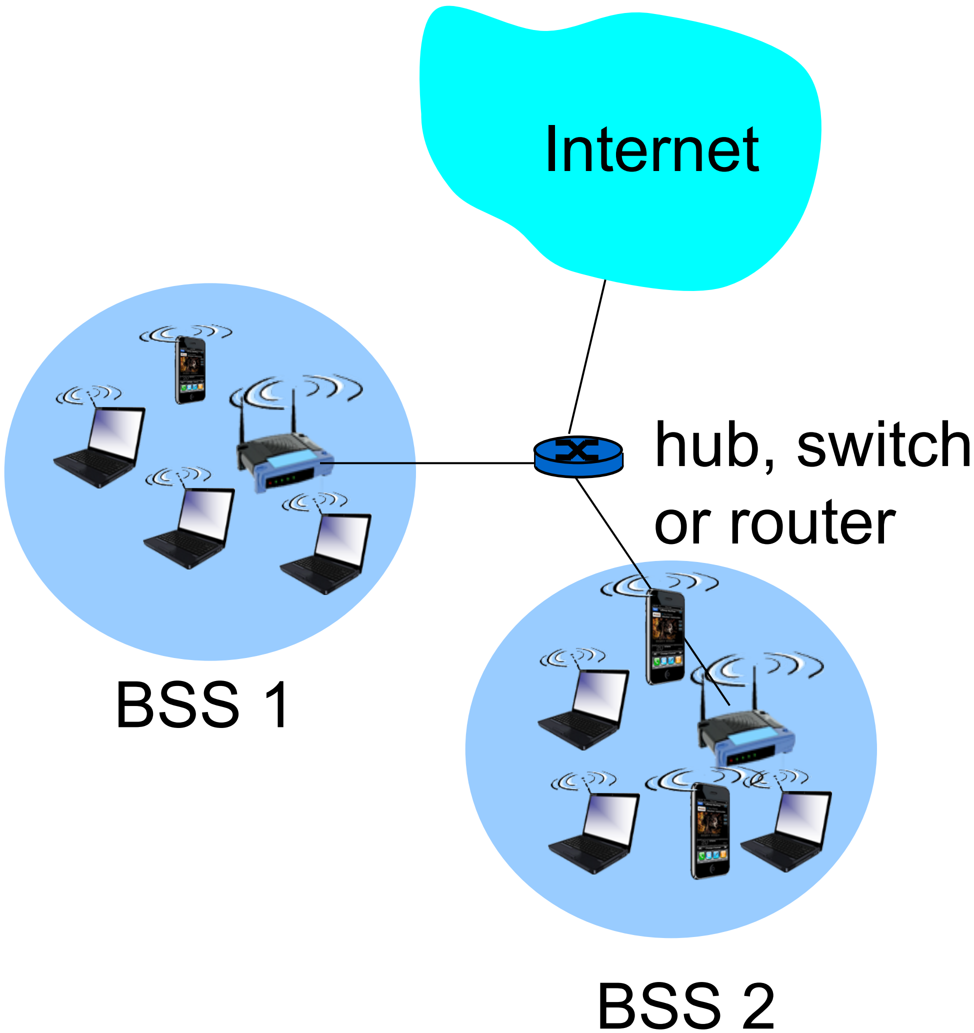
channel sums together transmissions by sender 1 and 2

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

IEEE 802.11 Wireless LAN

IEEE Standard	Year	Frequency	Max. Data Rate	Max. Range (Outdoor)
802.11a	1999	5 GHz	54 Mbps	120 m
802.11b	1999	2.4 GHz	11 Mbps	140 m
802.11g	2003	2.4 GHz	54 Mbps	140 m
802.11n	2009	2.4 GHz / 5 GHz	600 Mbps	250 m
802.11ac	2014	5 GHz	1 Gbps	250 m
802.11ad	2016	60 GHz	7 Gbps	5-10 m
802.11ax	2019	2.4 GHz / 5 GHz	10 Gbps	> 250 m

802.11 LAN Architecture

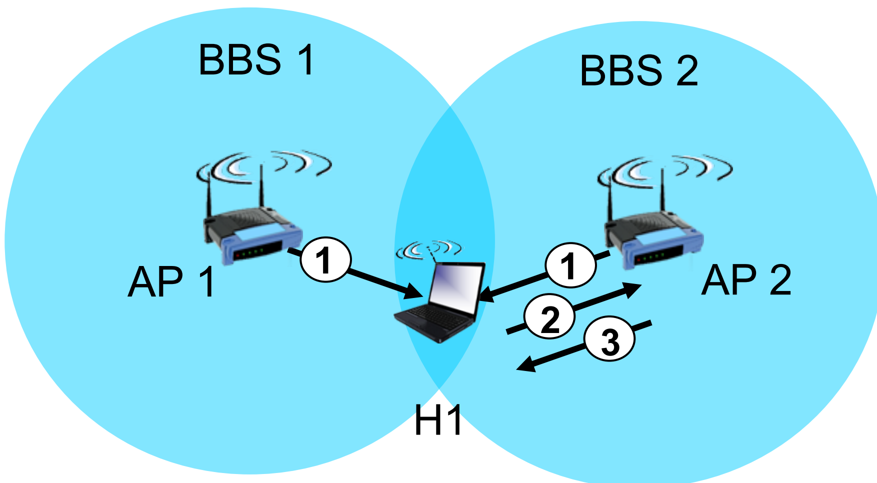


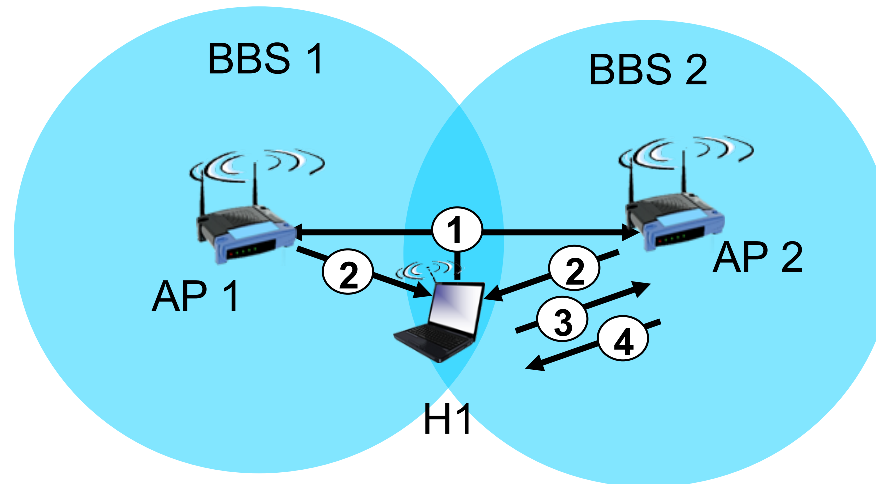
- Wireless host communicates with base station
  - Base station = access point (AP)
- Basic Service Set (BSS) (or "cell") in infrastructure more contains
  - Wireless hosts
  - Access point (AP)
- In ad hoc mode:
  - Only hosts

802.11: Channels, Association

- 802.11b: 2.4 GHz – 2.485 GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - Interference possible: channel can be same as that chosen by neighbouring 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 frame sent from Aps
  2. Association Request frame sent:
     - H1 to selected AP
  3. Association Response frame sent:
     - From selected AP to H1

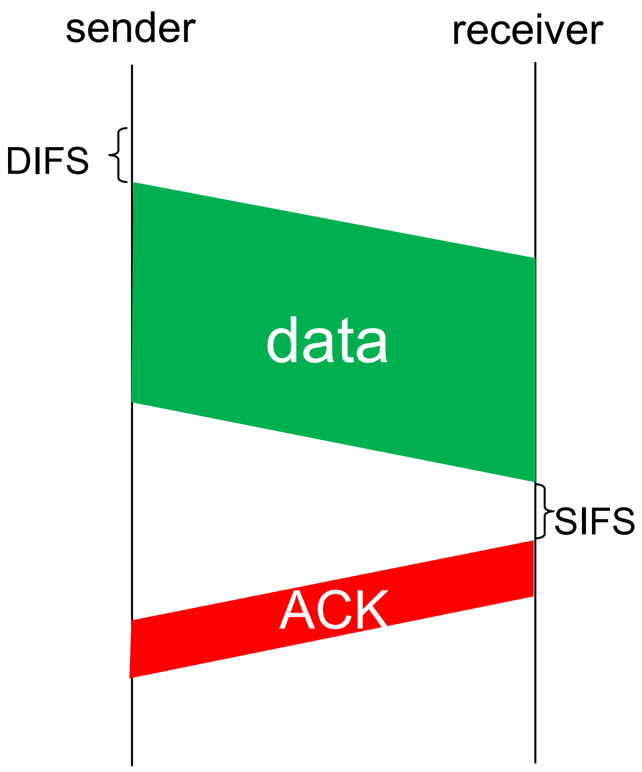
- Active scanning:
  1. Prove Request frame broadcast from H1
  2. Probe Response frames sent from APs
  3. Association Request frame sent:
     - H1 to selected AP
  4. Association Response frame sent:
     - From selected AP to H1

IEEE 802.11: Multiple Access

- Avoid collisions: 2+ nodes transmitting at the same time
- 802.11: CSMA – sense before transmitting
  - Do not collide with ongoing transmission by other node
- 802.11: no collision detection!
  - Difficult to receive (sense collisions) while transmitting due to weak received signals
  - Not possible to sense all collisions anyway, e.g., in case of hidden terminal
  - Need to 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 and transmit when timer expires
  3. If no ACK, increase random backoff interval and repeat 2.
- 802.11 receiver
  1. If frame received OK, return ACK after SIFS

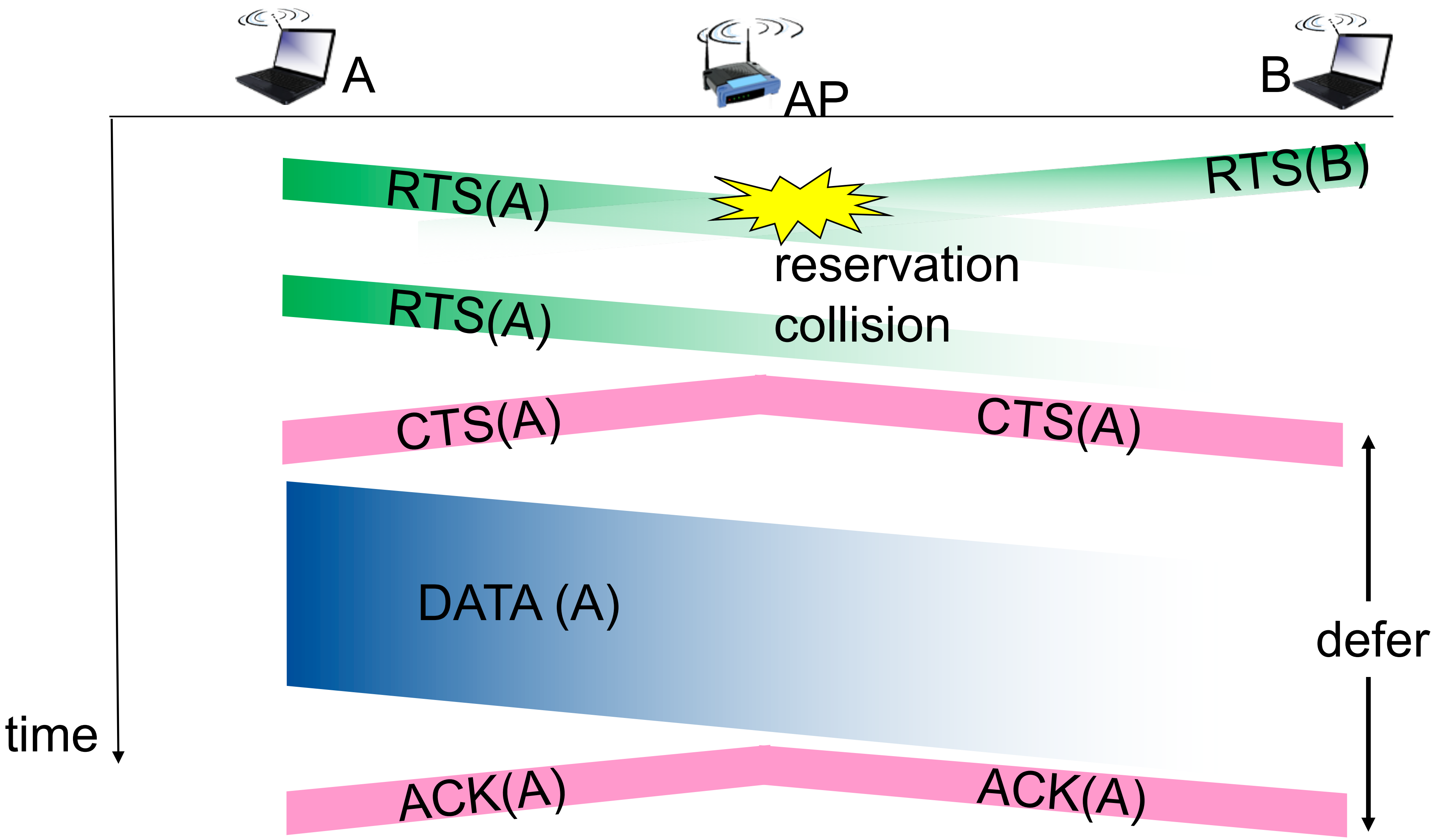


Avoiding Collisions (More)

- 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 AP using CSMA
    - RTSs may still collide with each other (but they are short)
  - AP 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

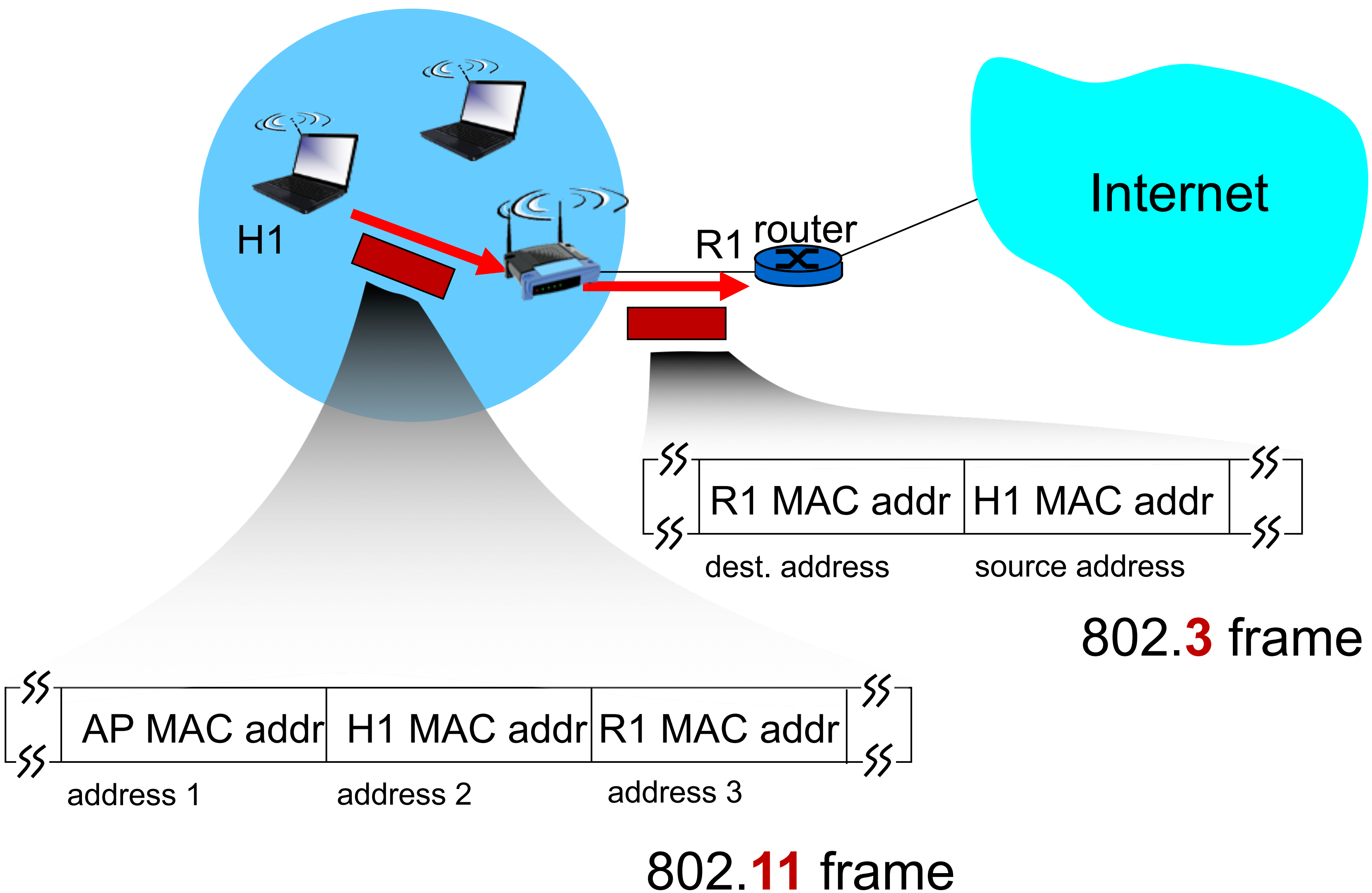
Address 4: used only in ad hoc mode

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

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

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

802.11 Frame: Addressing



802.11 Frame: More

duration of reserved transmission time (RTS/CTS)

frame seq # (for RDT)

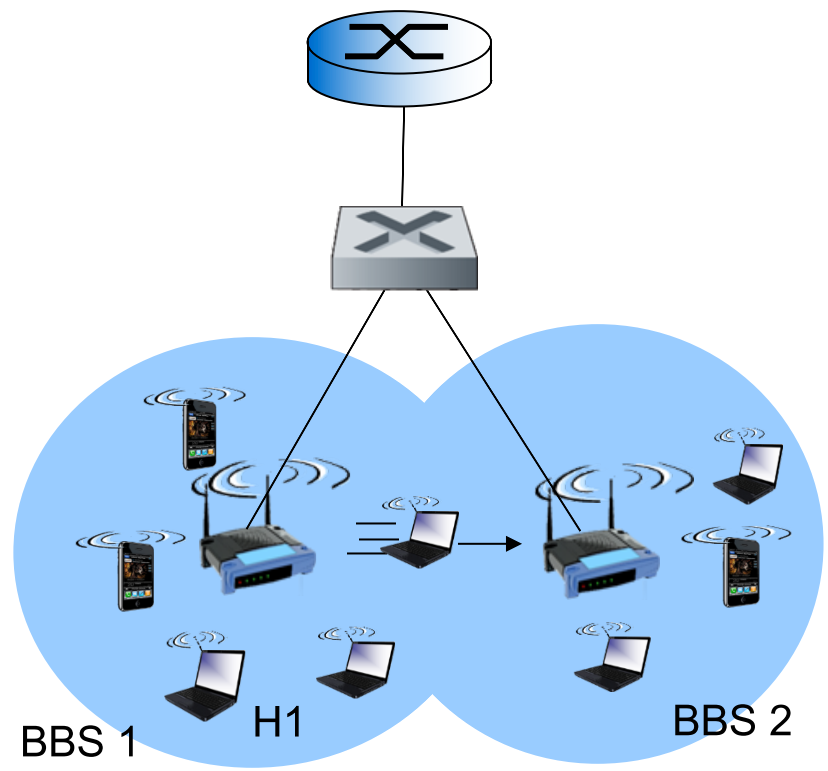
2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

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

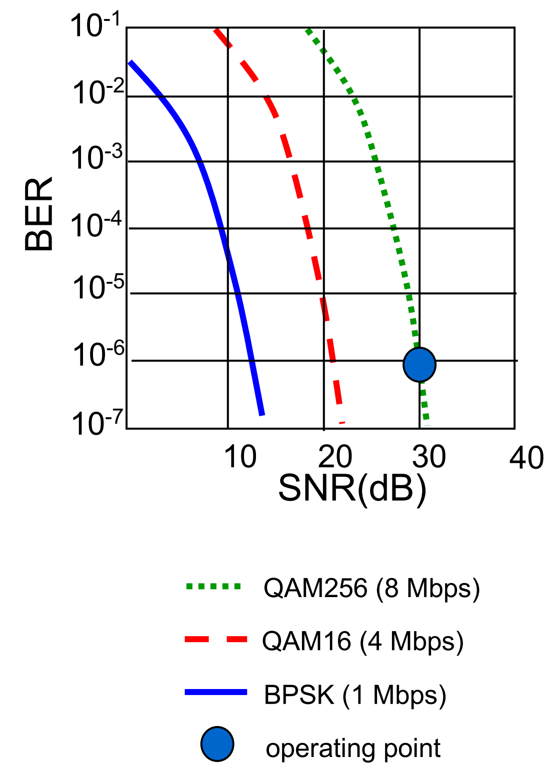
- H1 remains in same IP subnet
  - IP address can remain same
- Switch: which AP is associated with H1?
  - Self-learning: switch will see frame from H1 and "remember" which switch port can be used to reach H1



802.11: Advanced Capabilities

- Rate Adaptation
  - Base station and host dynamically change transmission rate (physical layer modulation technique) as host moves and SNR varies

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



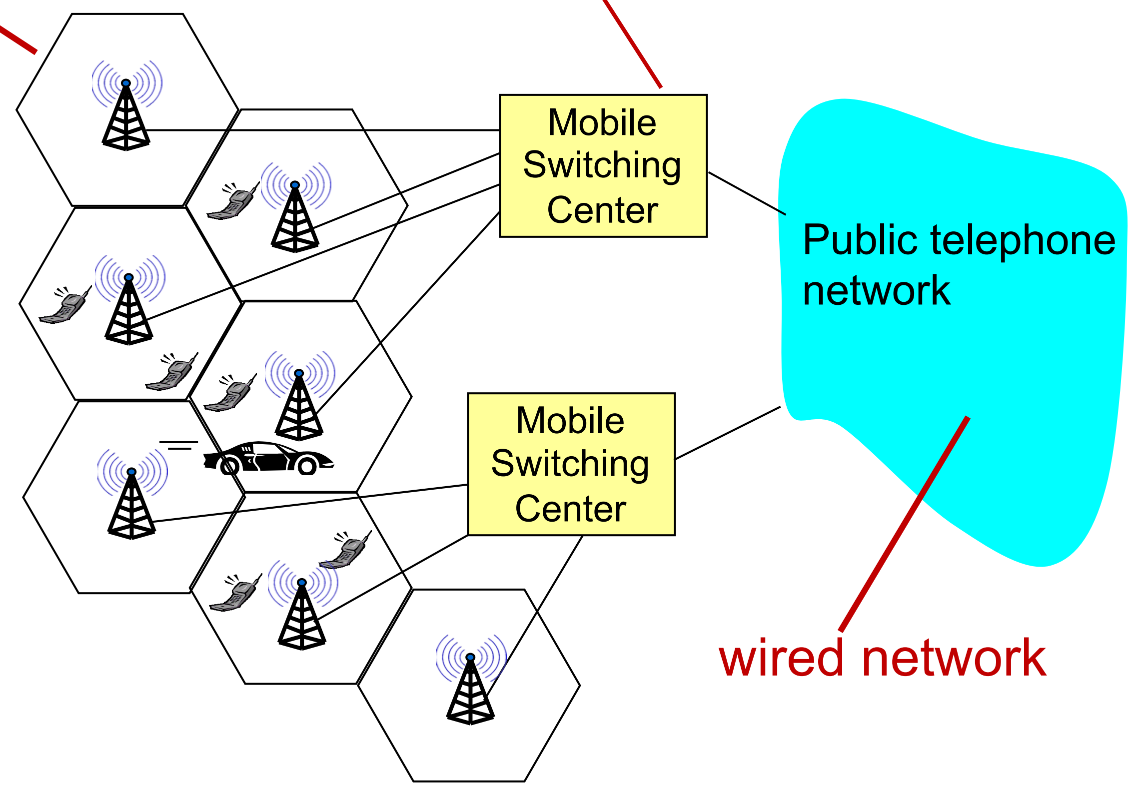
802.11: Advanced Capabilities

- Power Management
  - Host-to-AP: “I am going to sleep until next beacon frame”
    - AP knows not to transmit frames to this host
    - Host wakes up before next beacon frame
  - Beacon frame: contains list of hosts with AP-to-host frames waiting to be sent
    - Host will stay awake if AP-to-host frames to be received
    - Otherwise, sleep again until next beacon frame

Components of Cellular Network Architecture

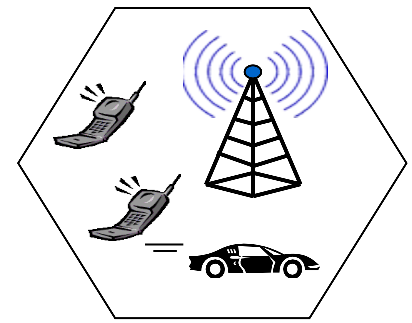
MSC
- connects cells to wired tel. net.
- manages call setup (more later!)
- handles mobility (more later!)

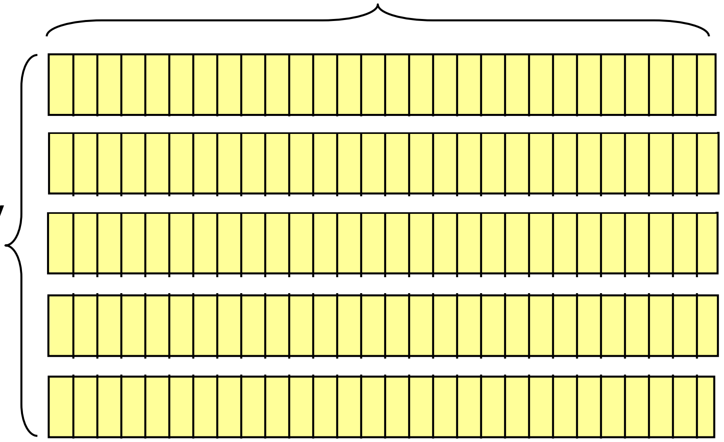
cell
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS



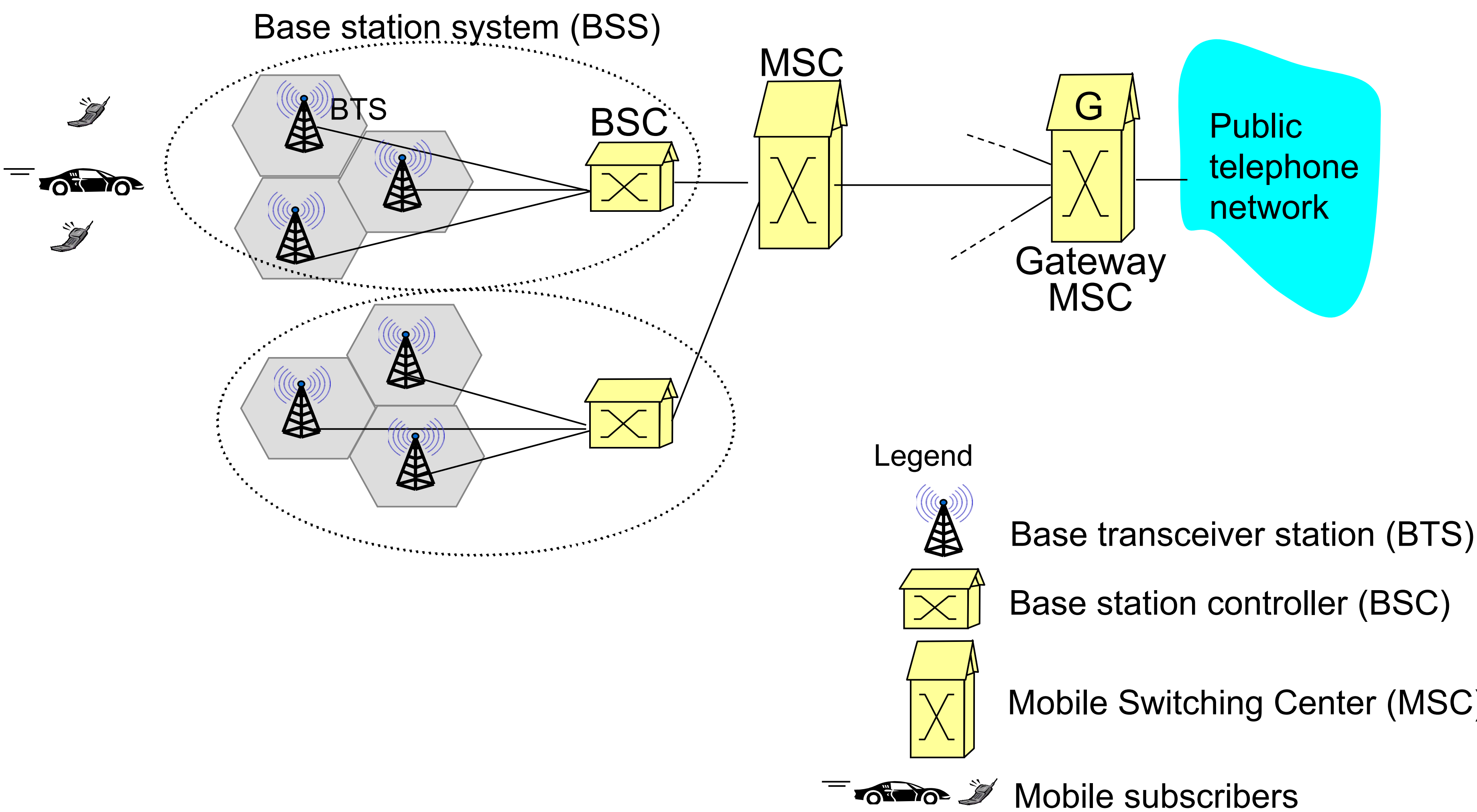
Cellular Networks: The First Hop

- 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

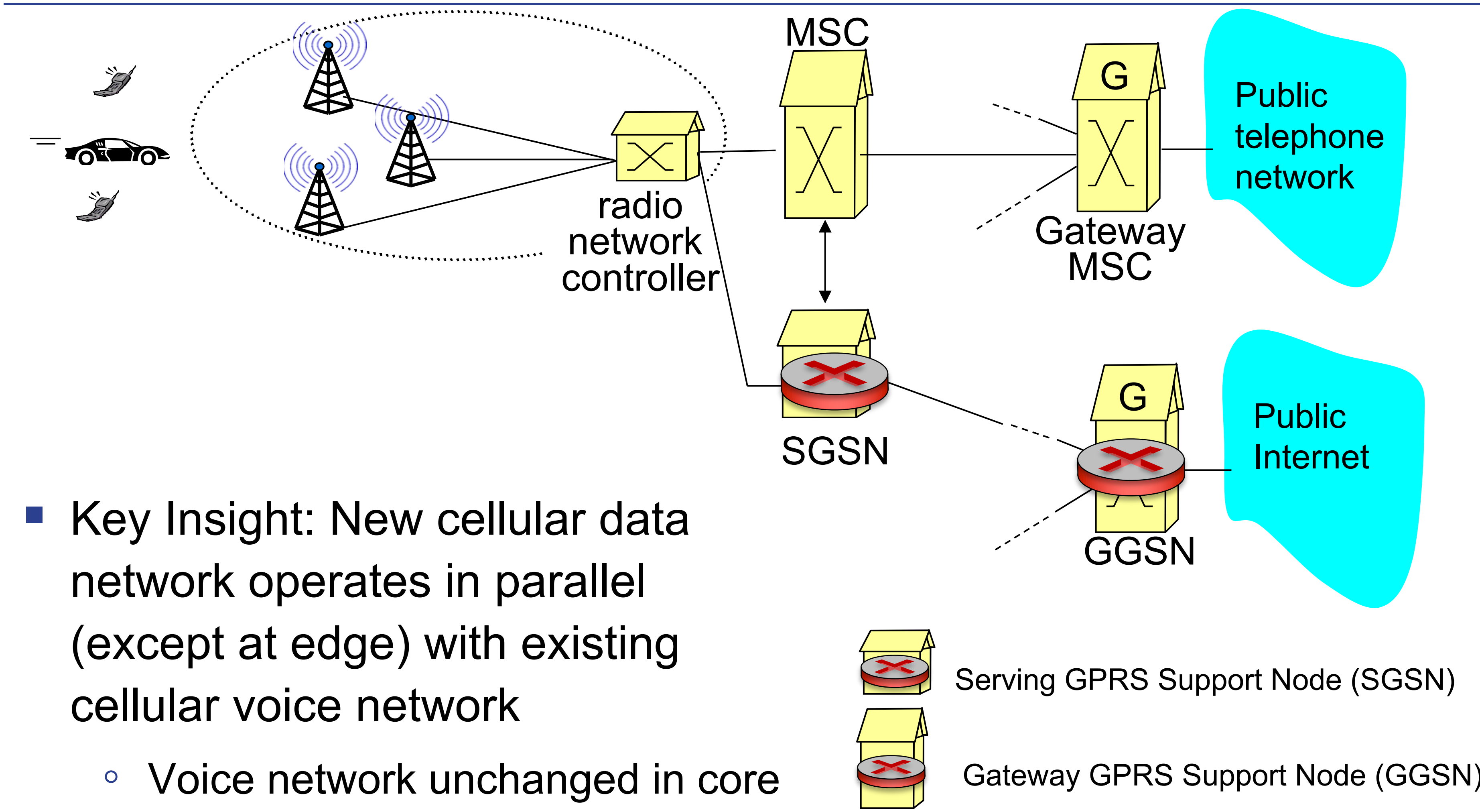




2G (Voice) Network Architecture

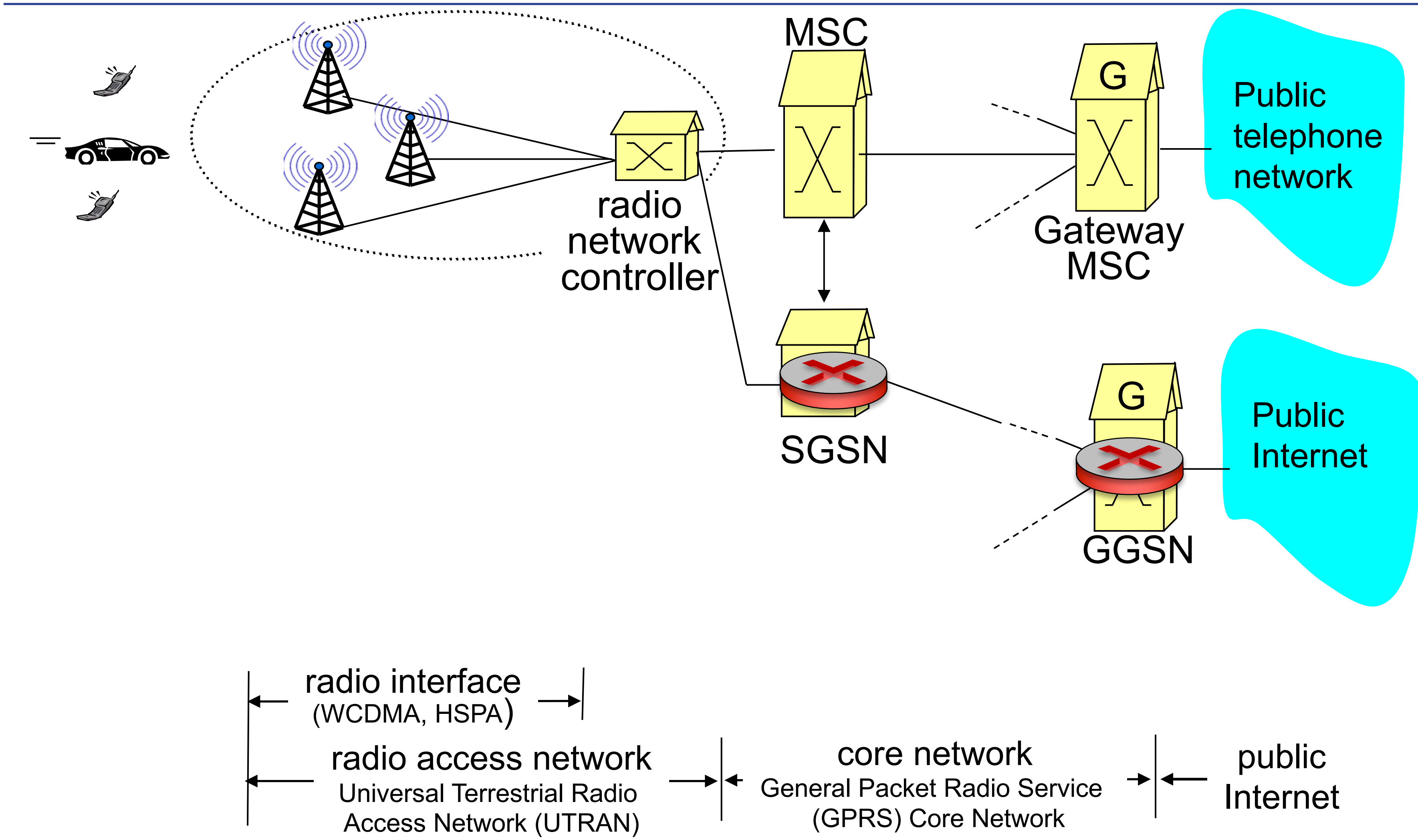


3G (Voice & Data) Network Architecture

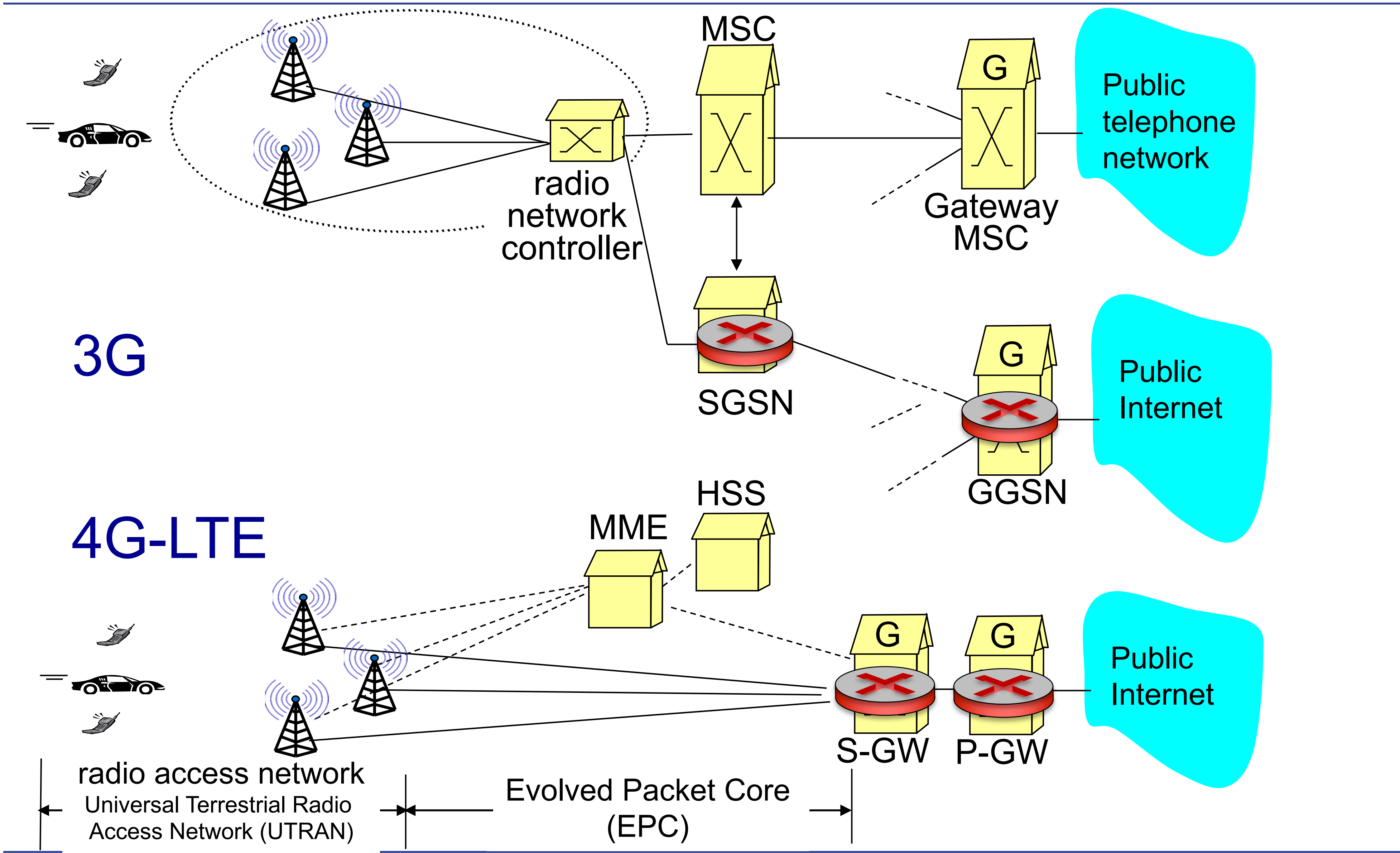


- Key Insight: New cellular data network operates in parallel (except at edge) with existing cellular voice network
  - Voice network unchanged in core
  - Data network operates in parallel

3G (Voice & Data) Network Architecture

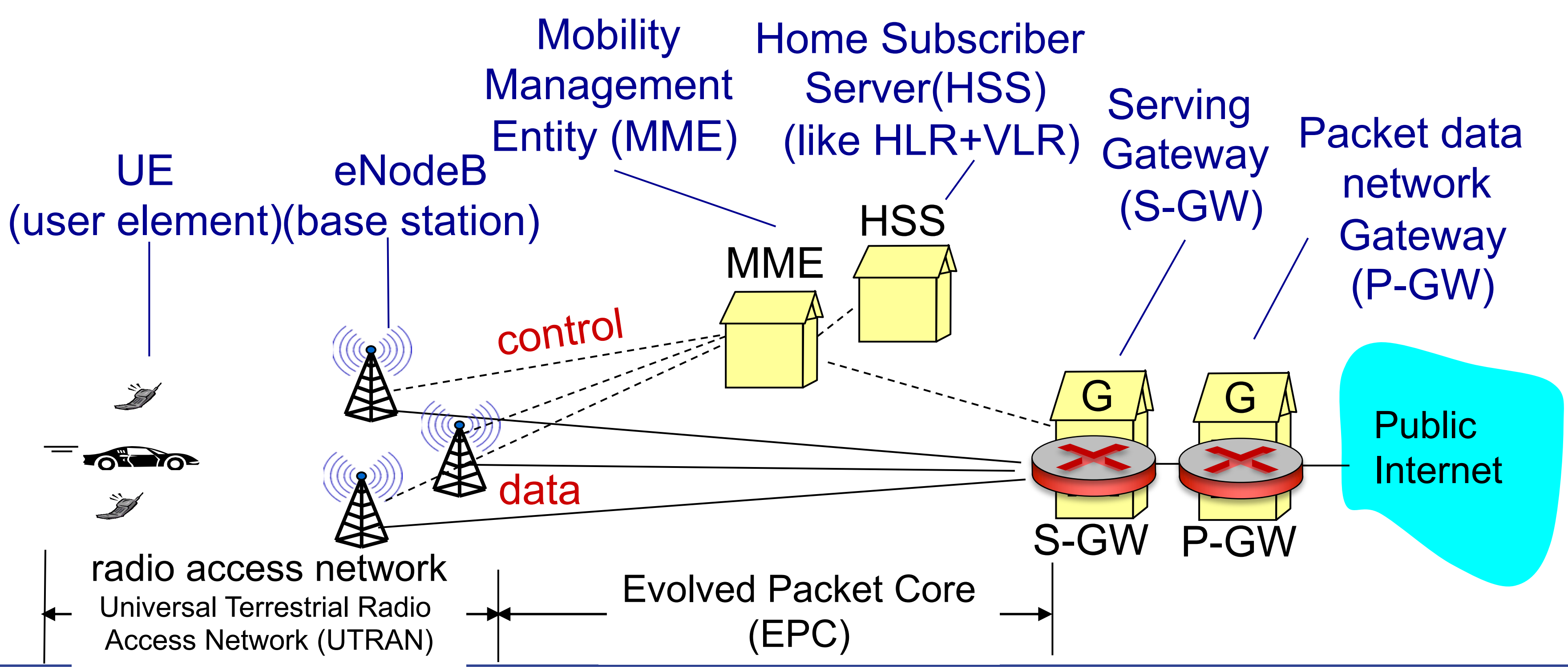


3G versus 4G LTE Network Architecture



4G: Differences from 3G

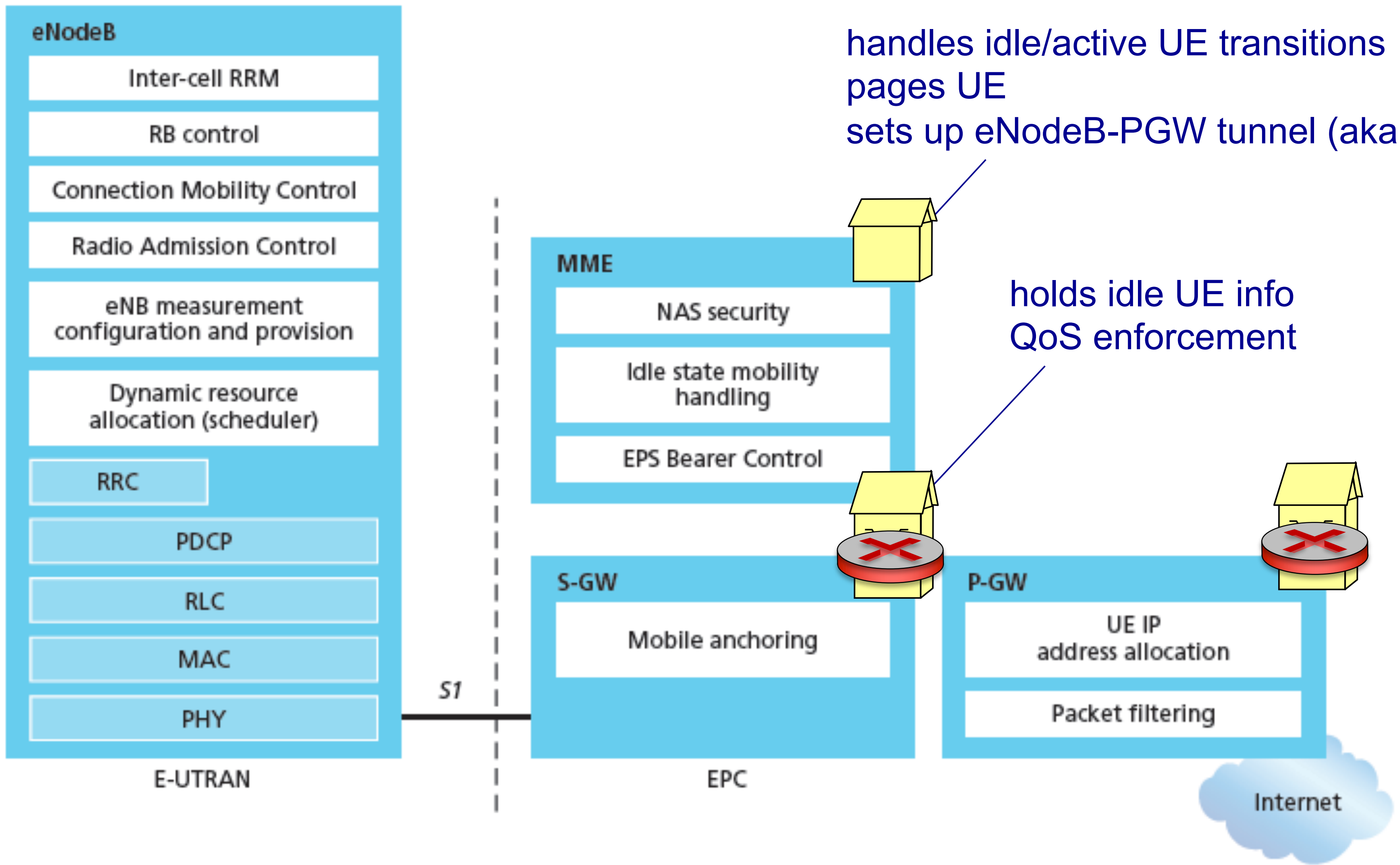
- All IP core: IP packets tunnelled (through core IP network) from base station to gateway
- No separation between voice and data – all traffic carried over IP core to gateway



Functional Split of Major LTE Components

handles idle/active UE transitions
pages UE
sets up eNodeB-PGW tunnel (aka bearer)

holds idle UE info
QoS enforcement



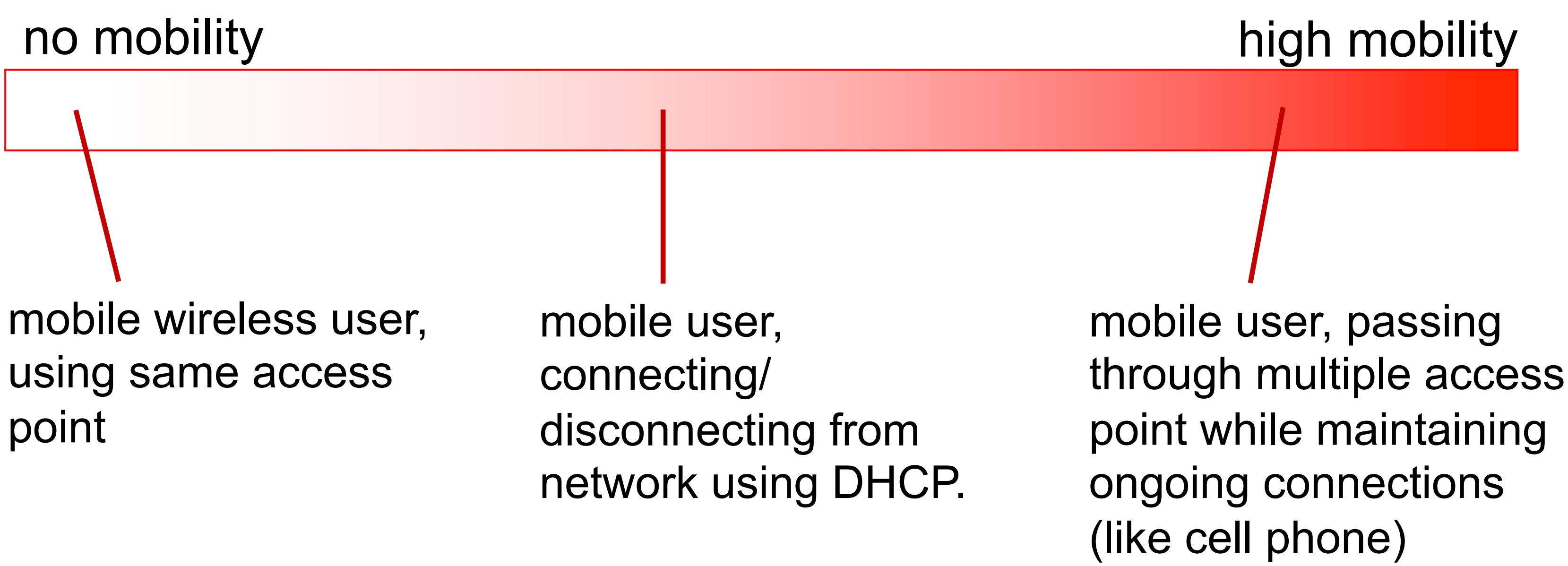
Quality of Service in LTE

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

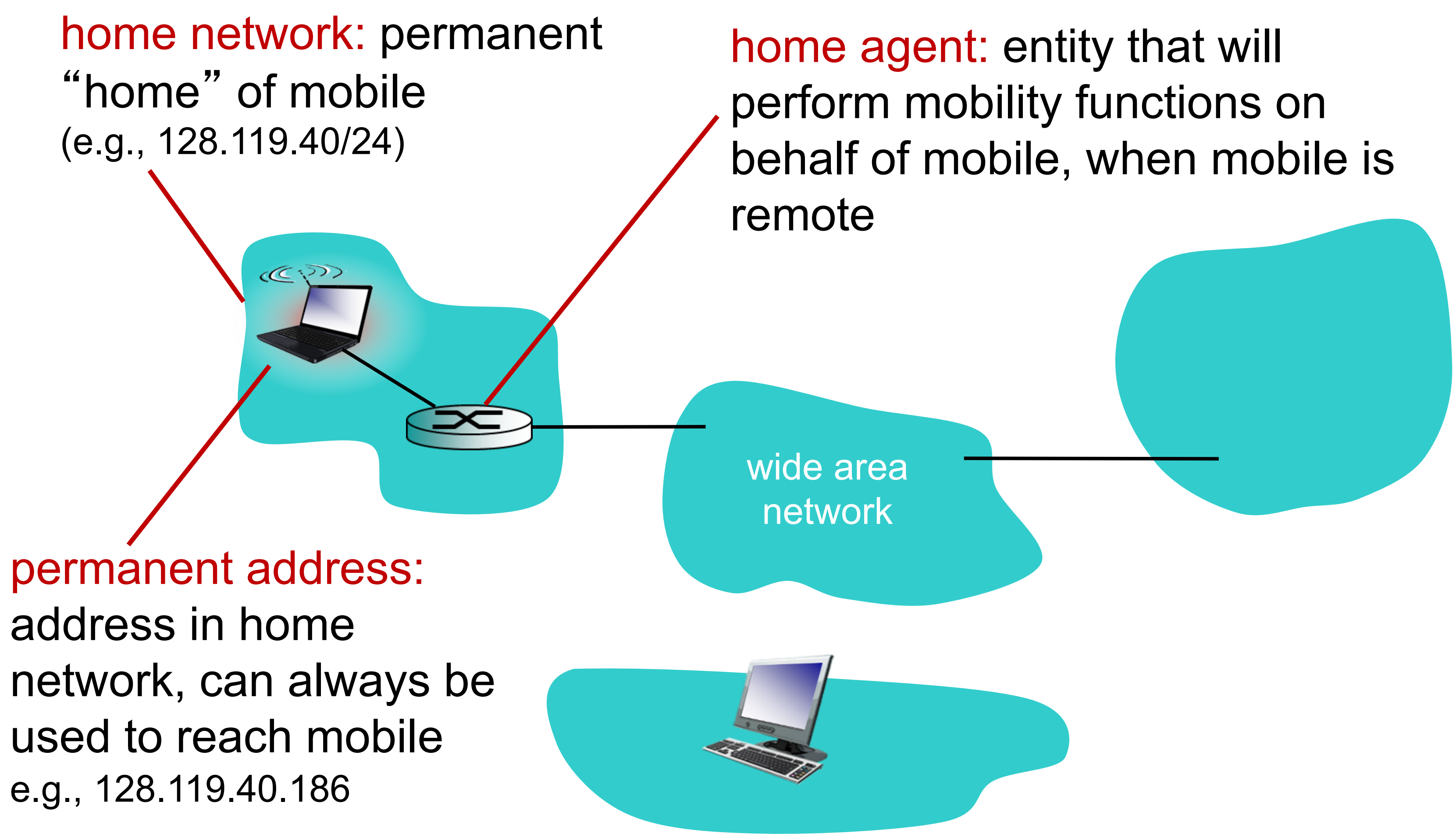
QCI	RESOURCE TYPE	PRIORITY	PACKET DELAY BUDGET (MS)	PACKET ERROR LOSS RATE	EXAMPLE SERVICES
1	GBR	2	100	10^{-2}	Conversational voice
2	GBR	4	150	10^{-3}	Conversational video (live streaming)
3	GBR	5	300	10^{-6}	Non-conversational video (buffered streaming)
4	GBR	3	50	10^{-3}	Real-time gaming
5	Non-GBR	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}	

What Is Mobility?

- Spectrum of mobility, from the network perspective



Mobility: Vocabulary

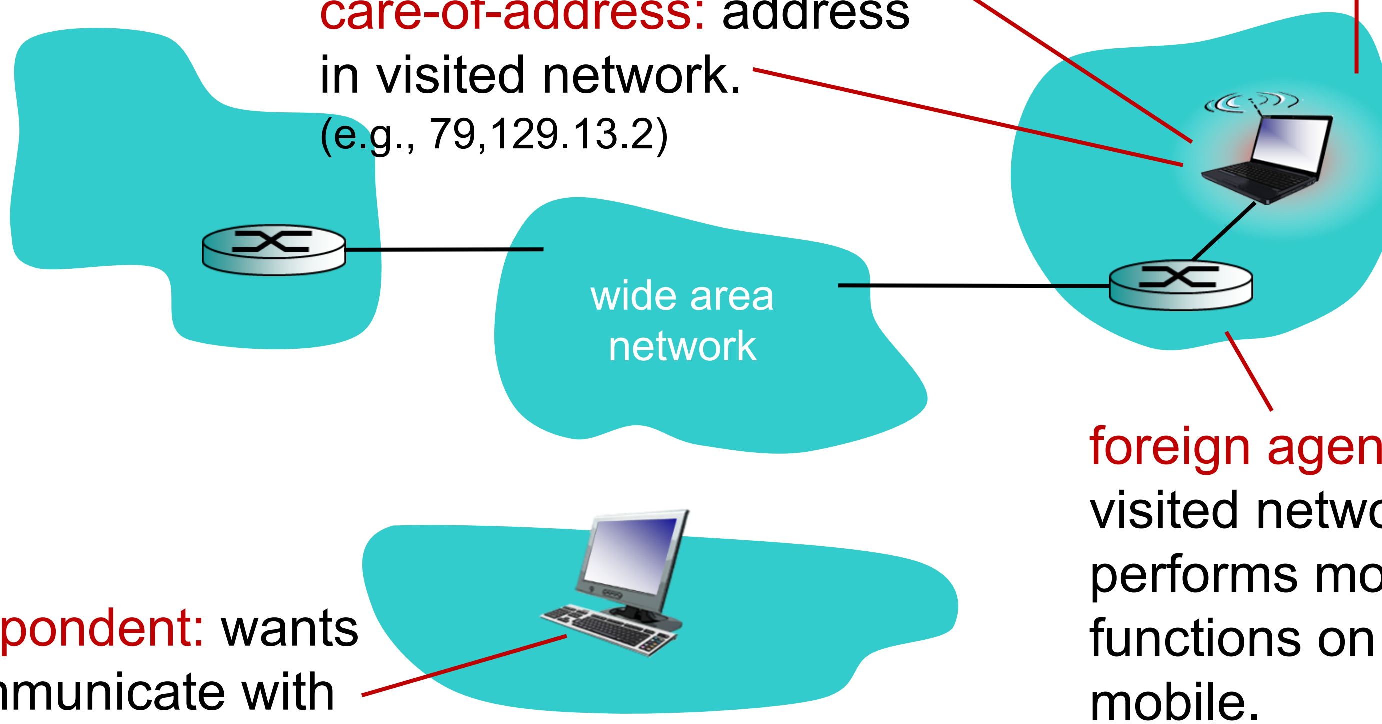


Mobility: (More) Vocabulary

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)

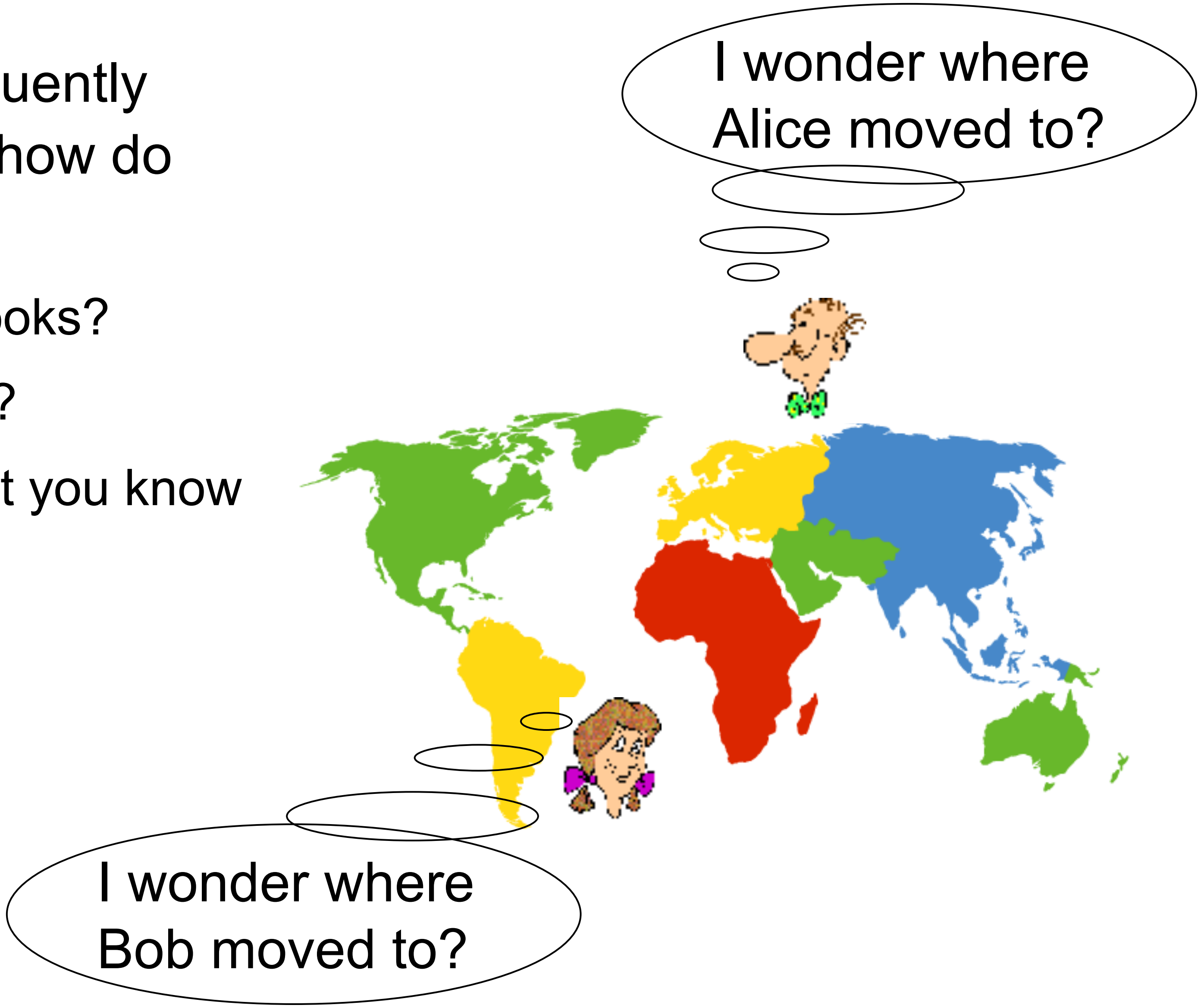


foreign agent: entity in visited network that performs mobility functions on behalf of mobile.

correspondent: wants to communicate with mobile

How Do You Contact a Mobile Friend?

- Consider a friend frequently changing addresses, how do you find him/her?
  - Search all phone books?
  - Call his/her parents?
  - Expect him/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

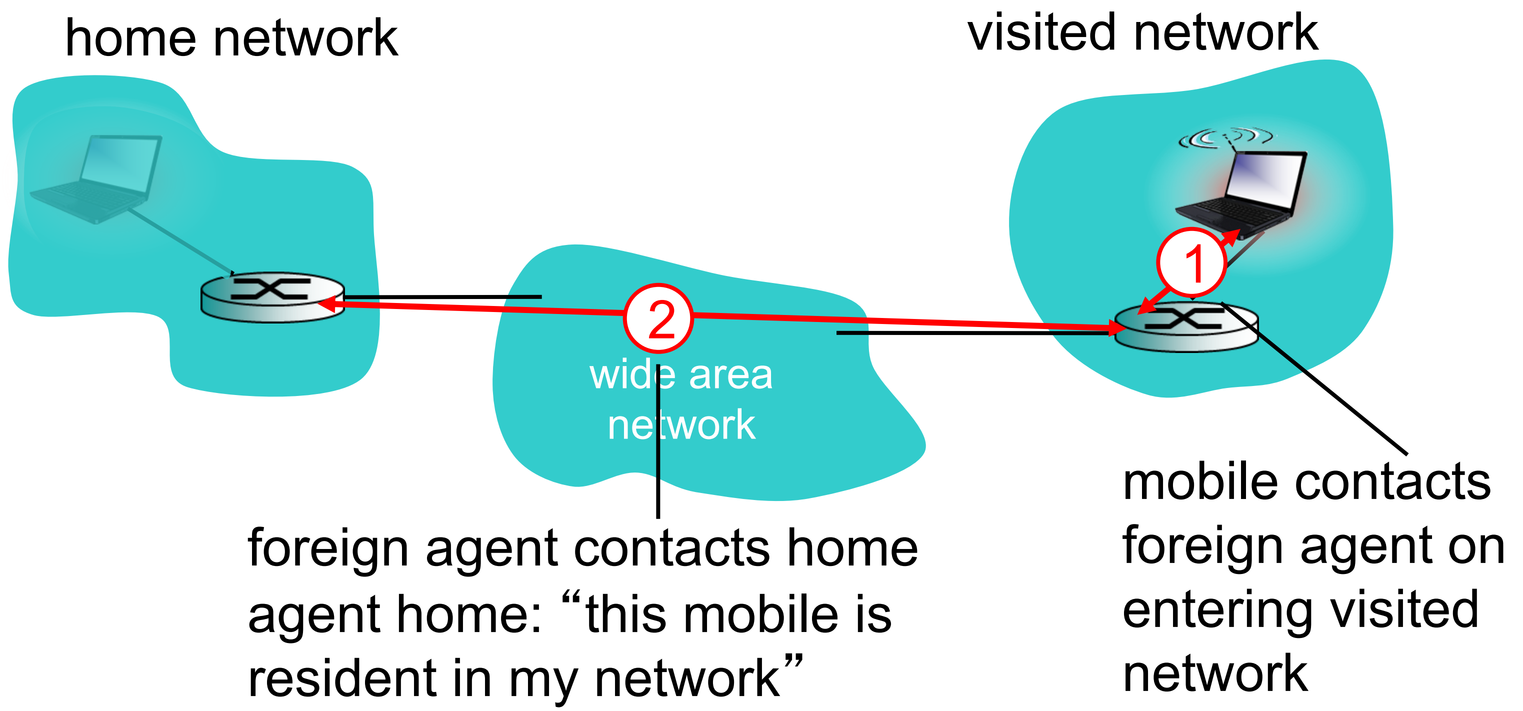
Mobility: Approaches

- Let routing handle it
  - Routers advertise perman… f mobile-nodes-in-residence via usual routing table exc…
    - Routing tables indicate w… le located
    - No changes to end-systems

not scalable

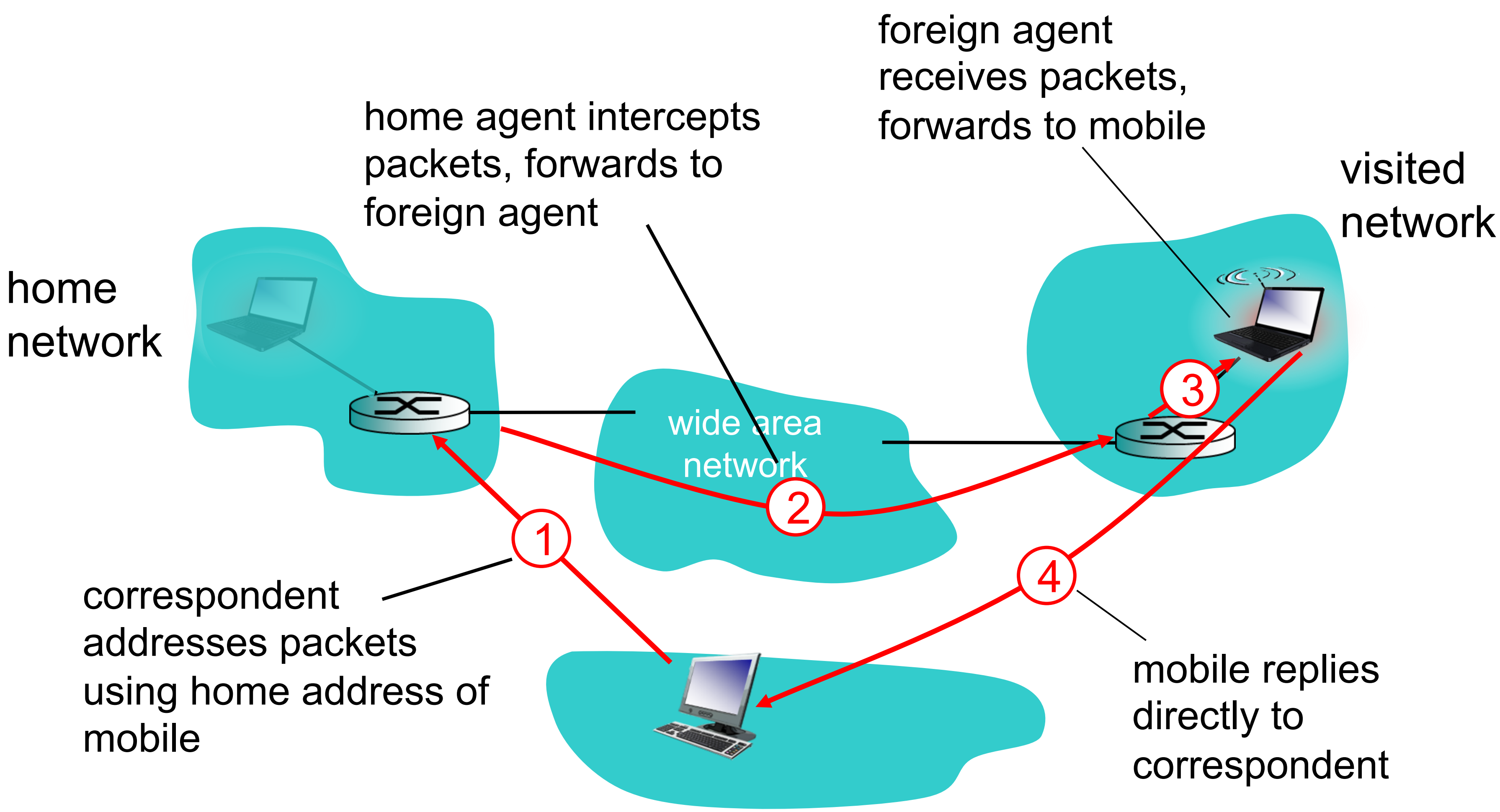
- Let end-systems handle it
  - Indirect routing: communication from correspondent to mobile goes through home agent, then forwarded to remote
  - Direct routing: correspondent gets foreign address of mobile, sends directly to mobile

Mobility: Registration



- End result:
  - Foreign agent knows about mobile
  - Home agent knows location of mobile

Mobility via Indirect Routing



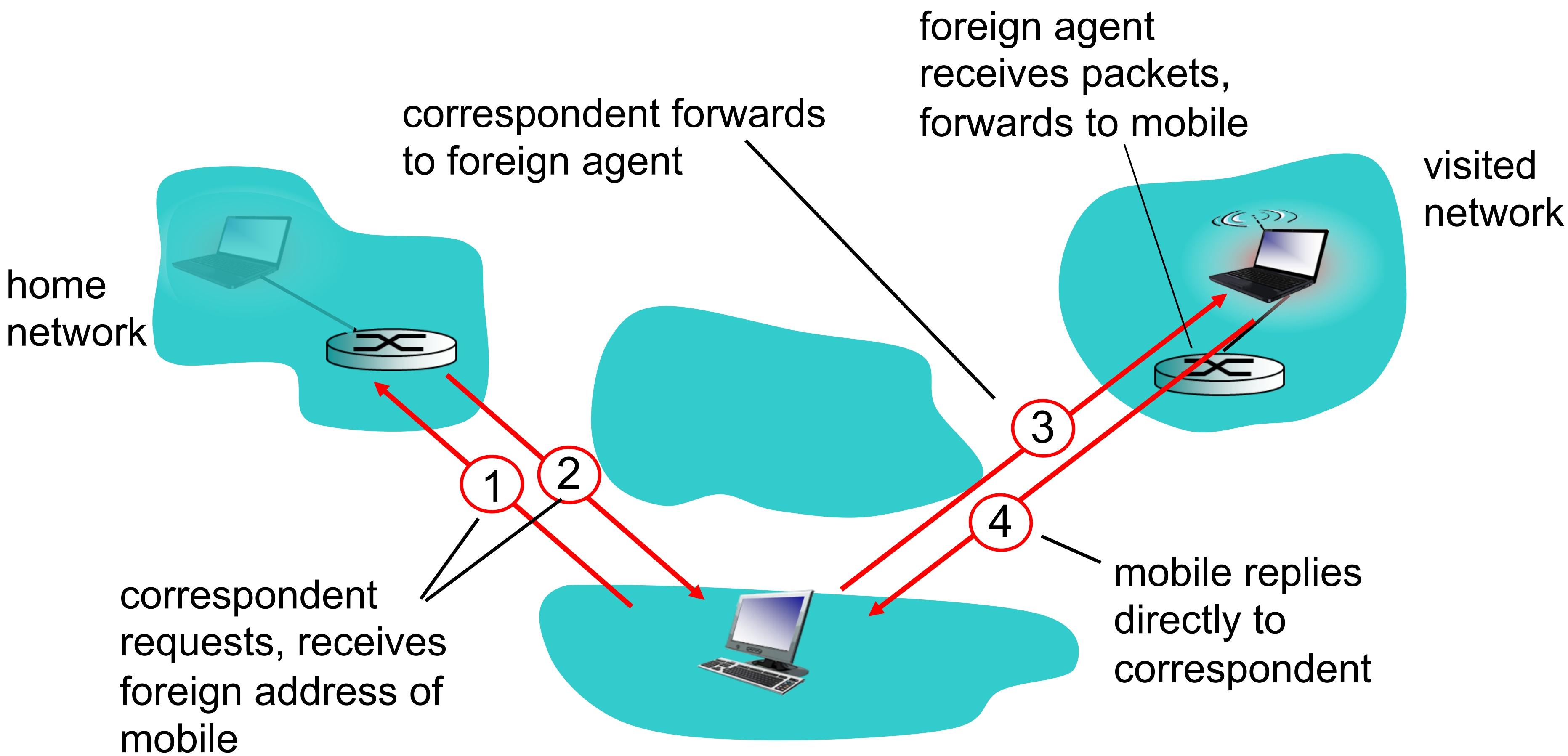
Indirect Routing: Discussion

- 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 and 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)
- Changing foreign networks is transparent
  - Ongoing connections can be maintained!

Mobility via Direct Routing

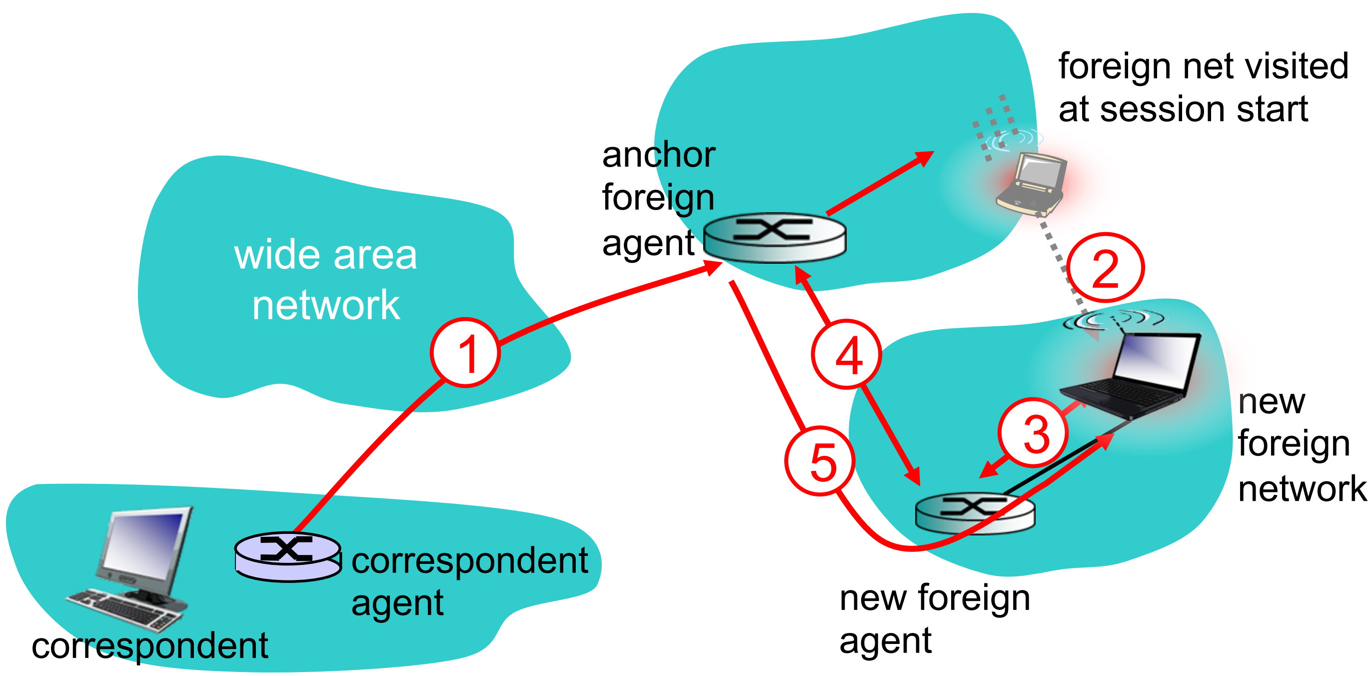


Mobility via Direct Routing: Discussion

- 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

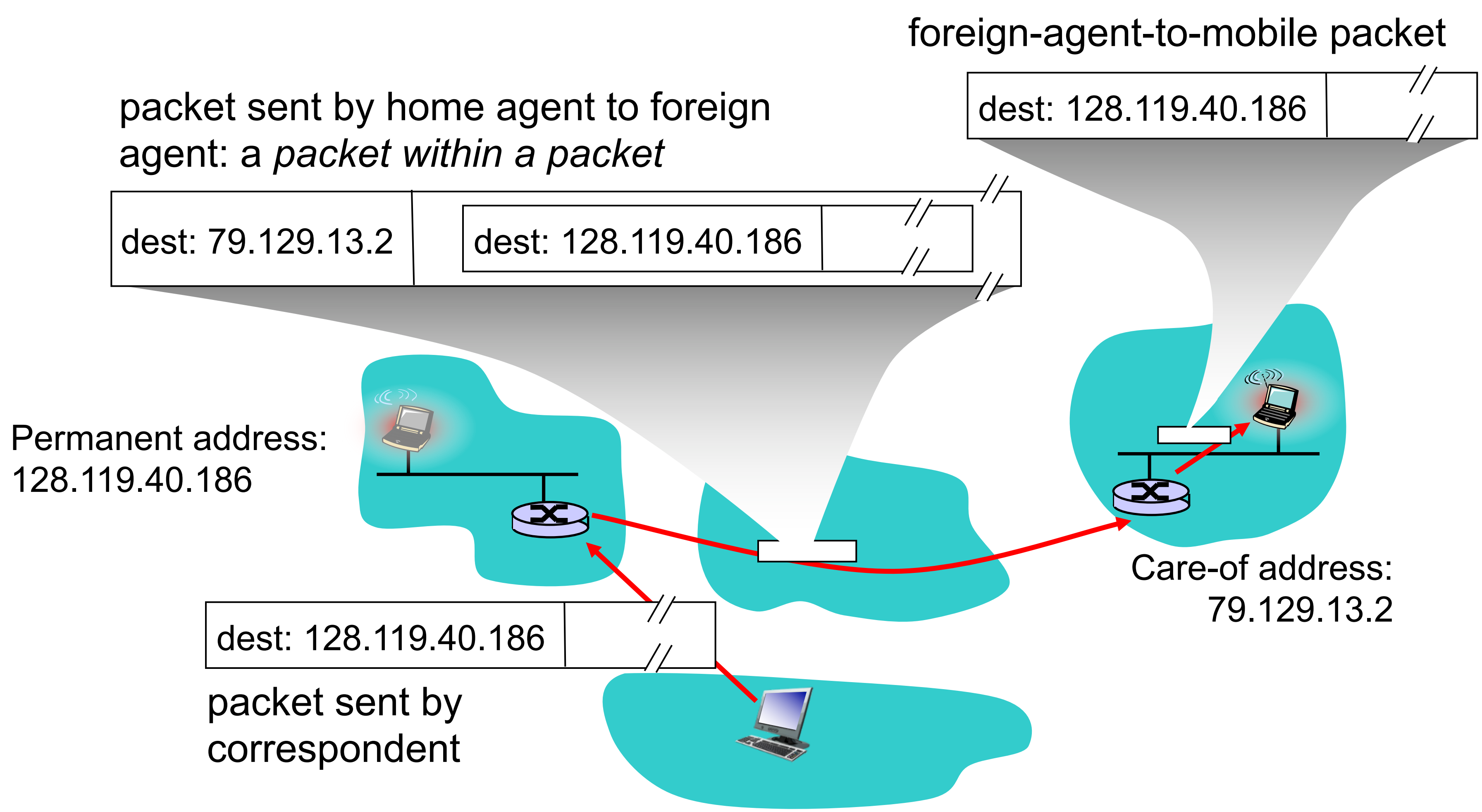
- Anchor foreign agent: FA in first visited network
- Data always routed first to anchor FA
- When mobile moves: new FA arranges to have data forwarded from old FA (chaining)



Mobile IP

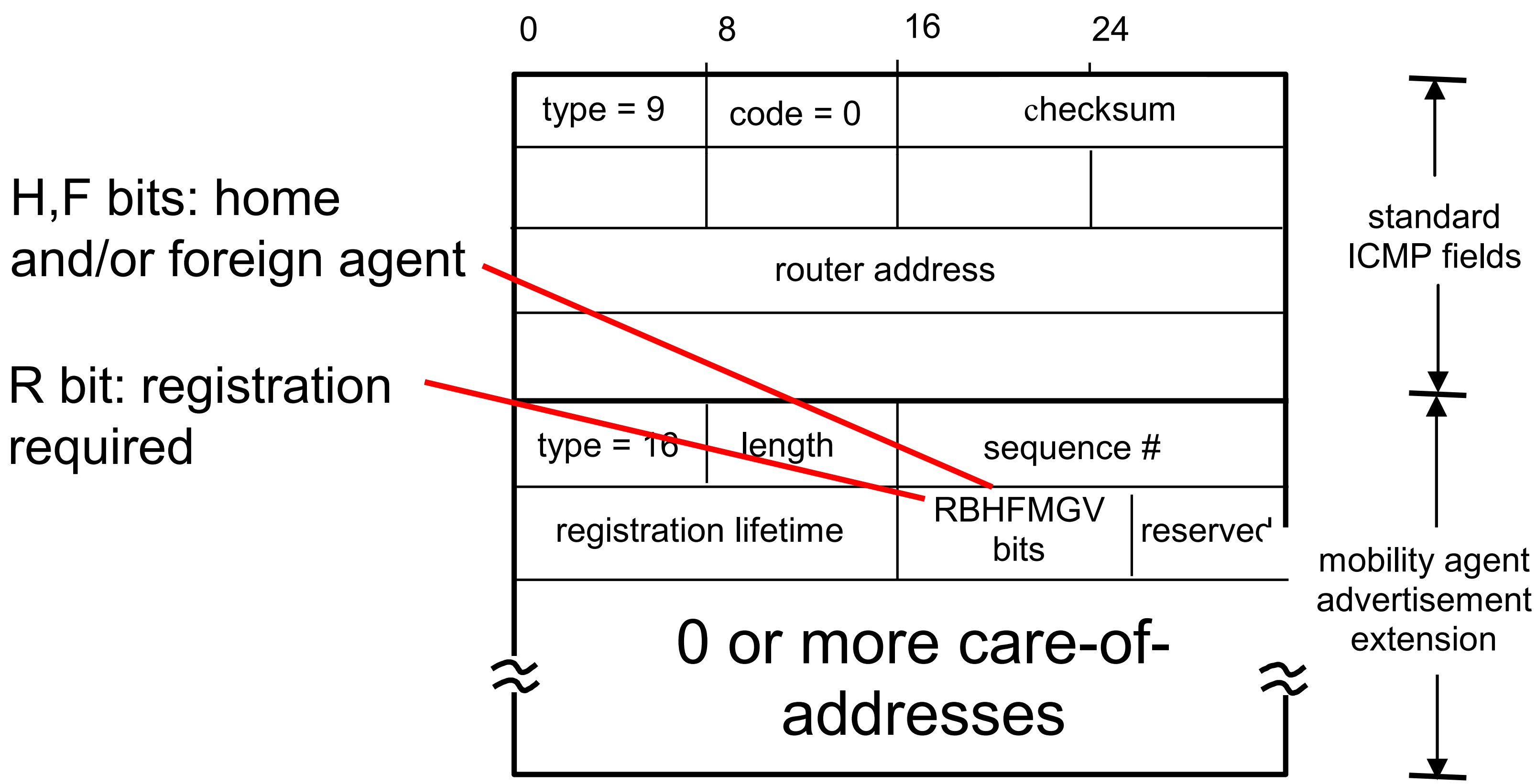
- RFC 3344
- Has many features we have seen
  - Home agents, foreign agents, foreign-agent registration, care-of-address, encapsulation (packet-within-a-packet)
- Three components to standard
  - Indirect routing of datagrams
  - Agent discovery
  - Registration with home agent

Mobile IP: Indirect Routing

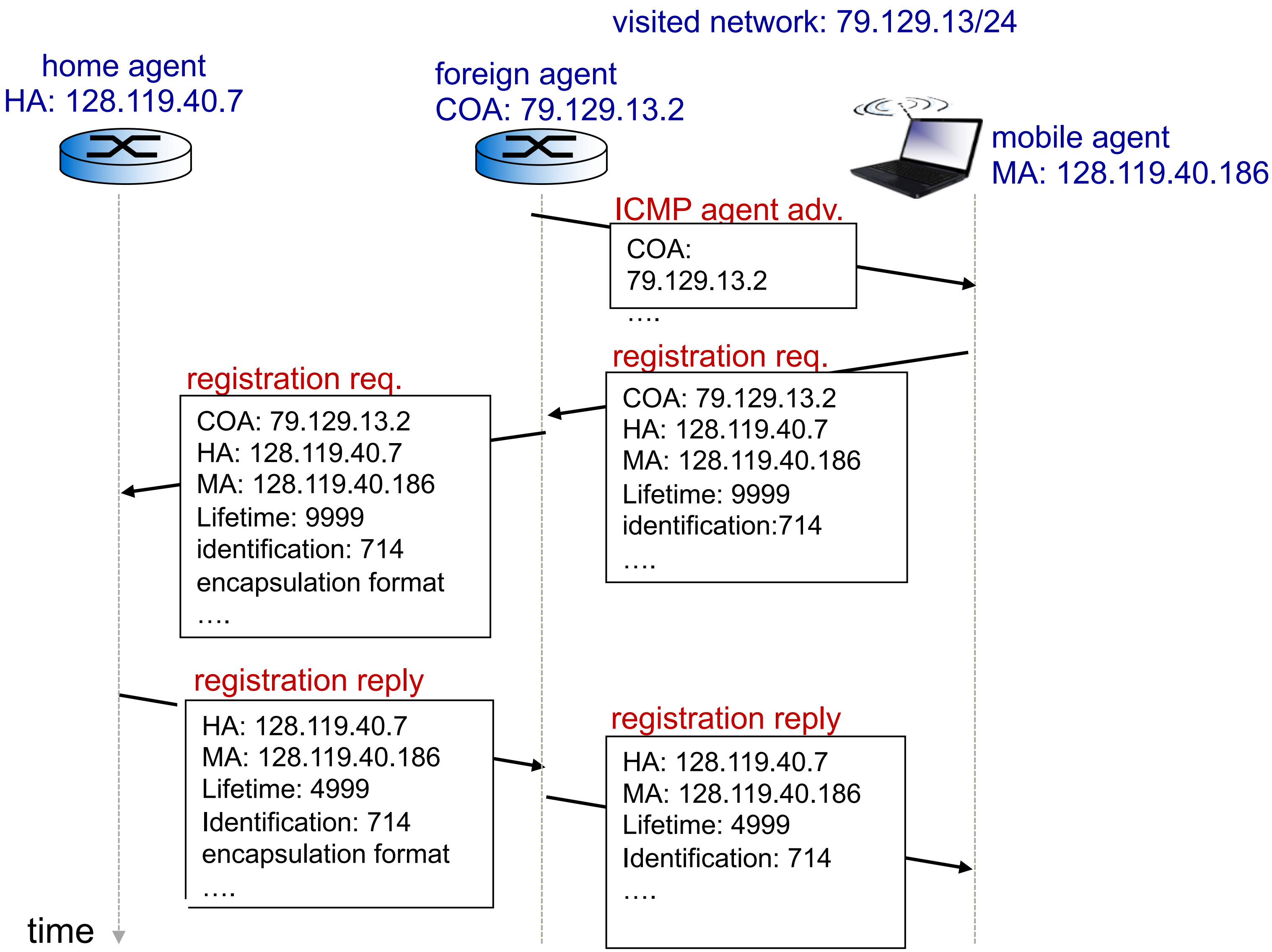


Mobile IP: Agent Discovery

- Agent Advertisement: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)

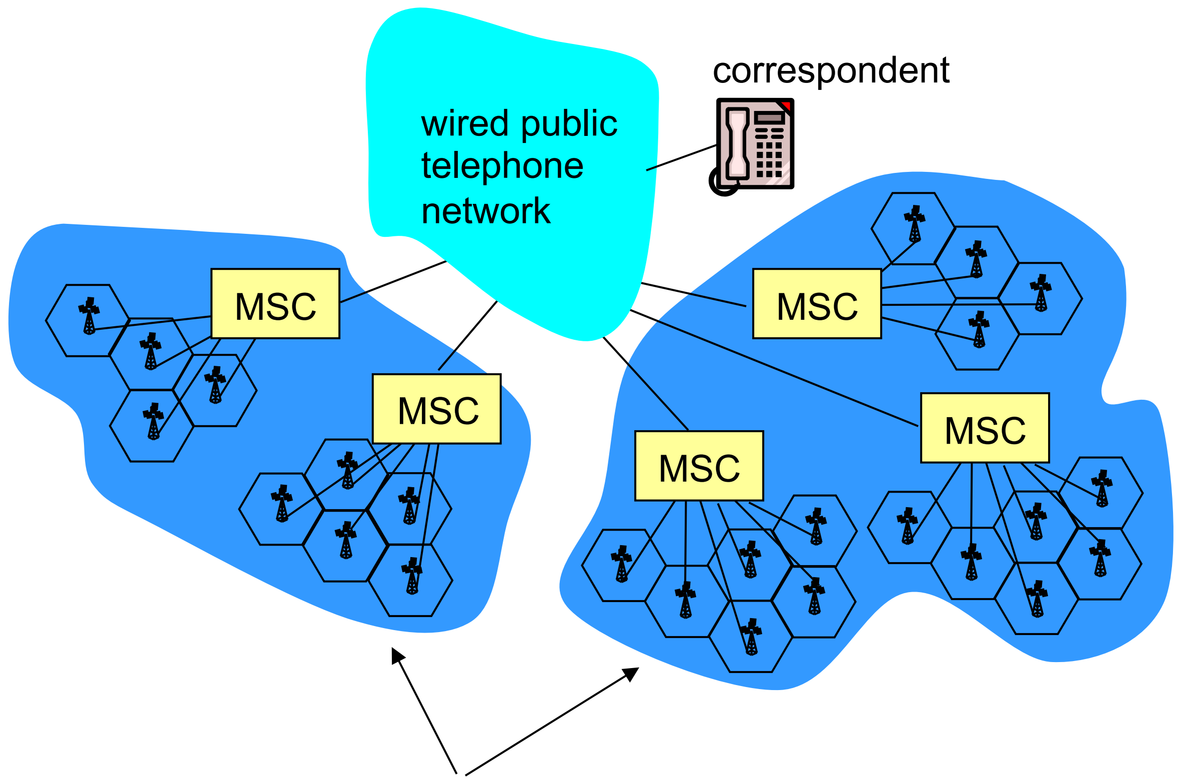


Mobile IP: Registration Example



Components of Cellular Network Architecture

- Recall:



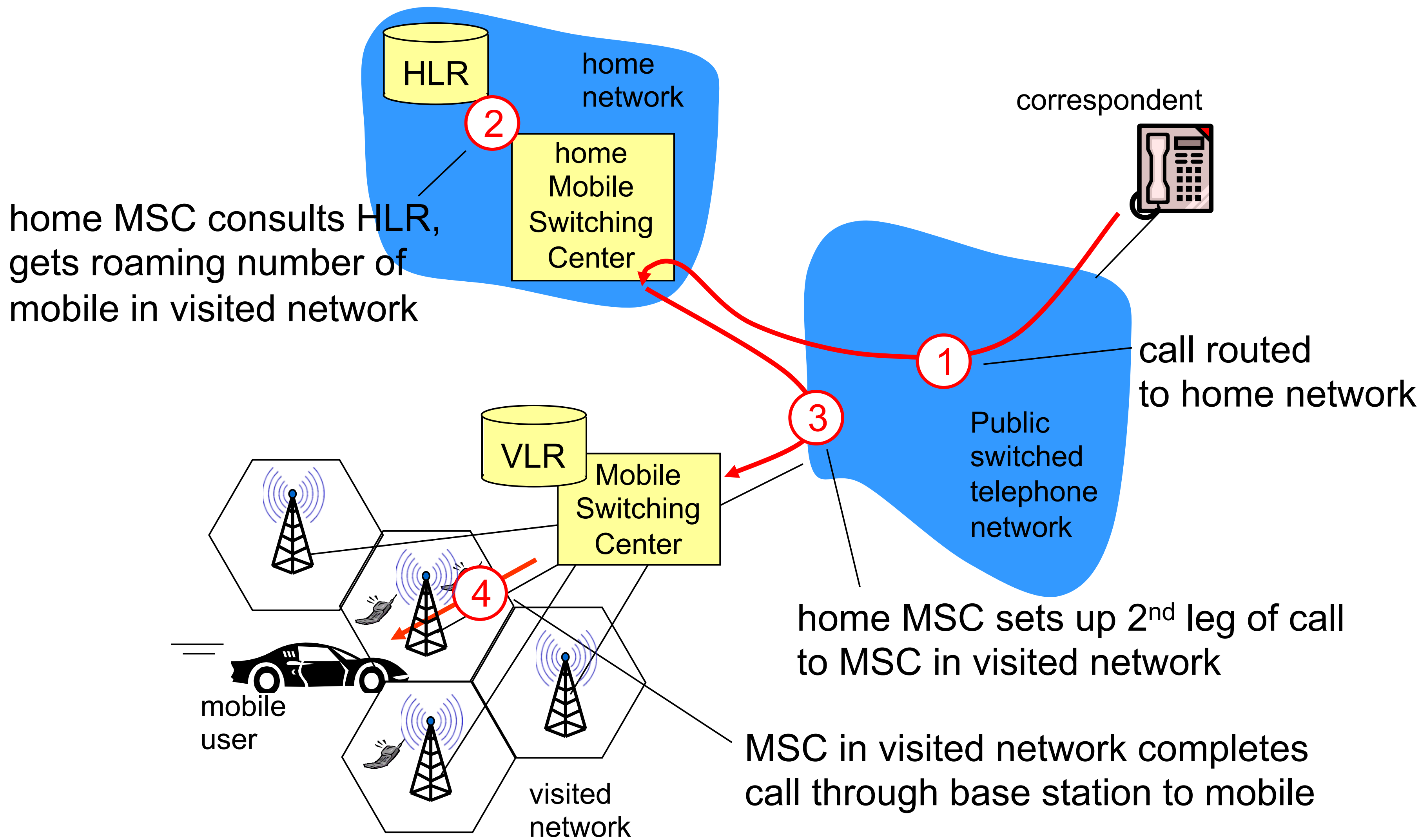
different cellular networks,
operated by different providers

Handling Mobility in Cellular Networks

- Home Network: network of cellular provider you subscribe to
  - 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)

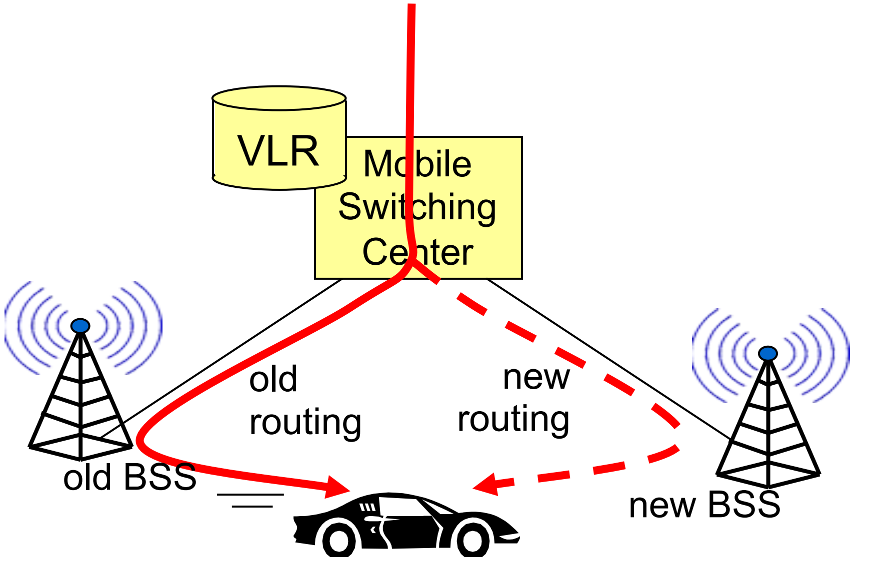
- Visited Network: network in which mobile currently resides
  - Visitor Location Register (VLR)
    - Database with entry for each user currently in network
    - Could be home network

GSM: Indirect Routing to Mobile



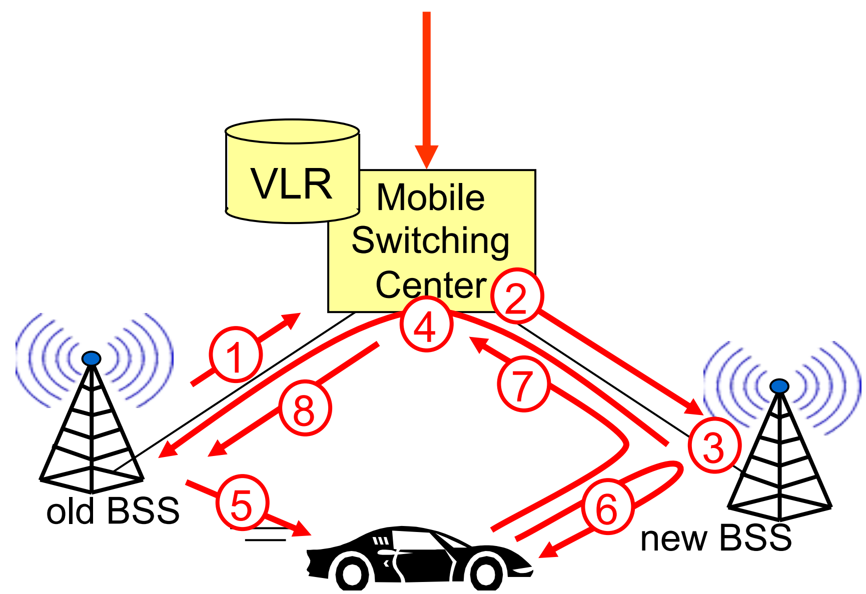
GSM: Handoff with Common MSC

- 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 does not mandate why to perform handoff (policy), only how (mechanism)
- Handoff initiated by old BSS



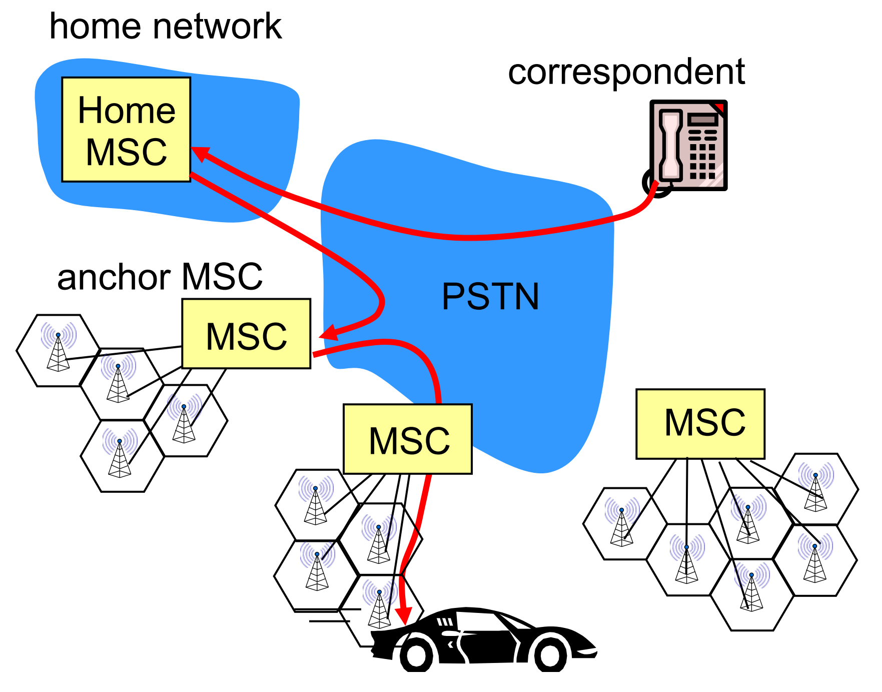
GSM: Handoff with Common MSC

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 and old BSS when ready
5. Old BSS tells mobile to perform handoff to new BSS
6. Mobile signals new BSS to activate new channel
7. Mobile signals via new BSS to MSC that the handoff is complete; MSC reroutes the call
8. Old BSS resources released



GSM: Handoff between MSCs

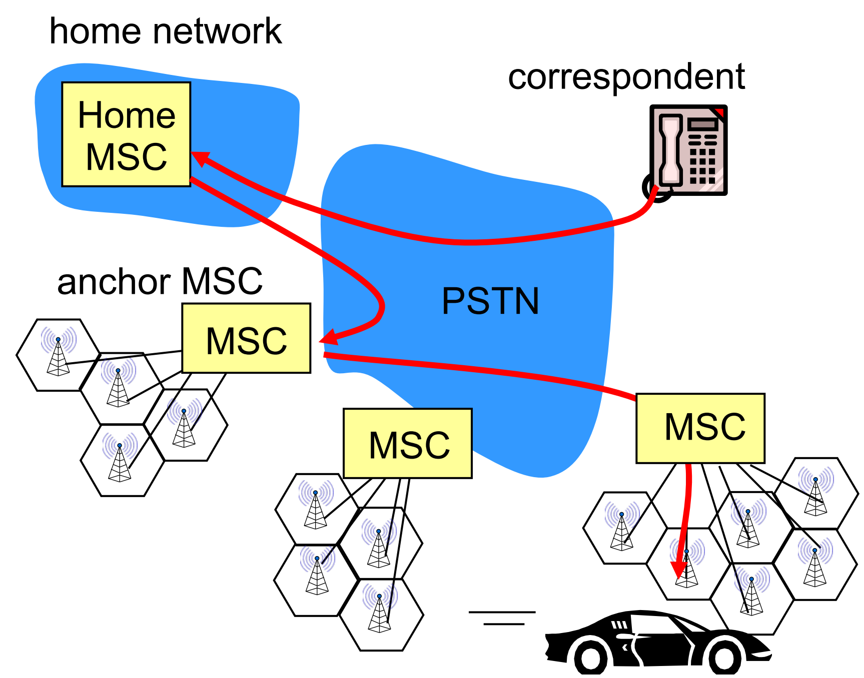
- Anchor MSC: first MSC visited during call
  - Call remains routed through anchor MSC
- New MSCs added to end of MSC chain as mobile moves to new MSC
- Optional path minimization step to shorten multi-MSC chain



(a) before handoff

GSM: Handoff between MSCs

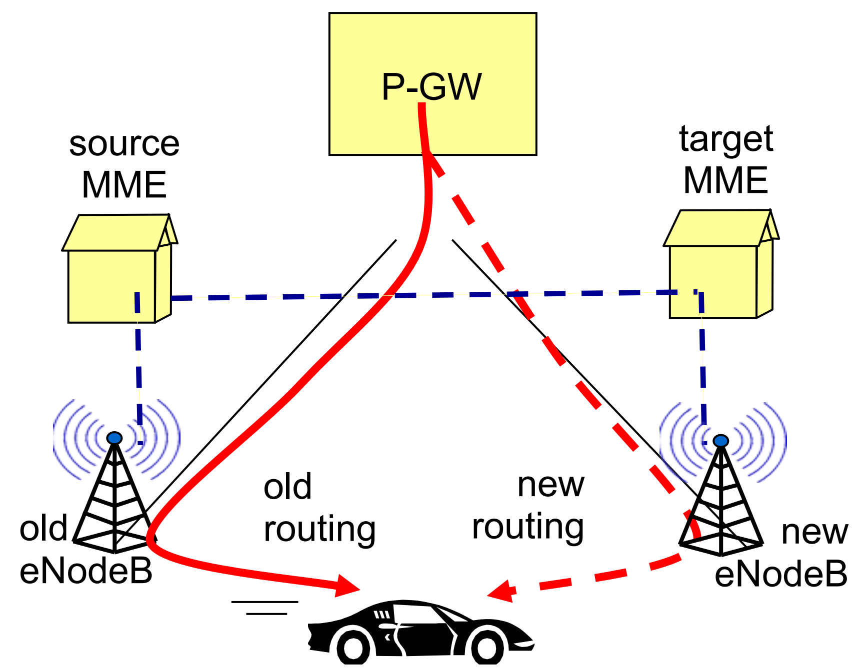
- Anchor MSC: first MSC visited during call
  - Call remains routed through anchor MSC
- New MSCs added to end of MSC chain as mobile moves to new MSC
- Optional path minimization step to shorten multi-MSC chain



(b) after handoff

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 broadcasted 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
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 mobile wireless links
- … 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