CSE 3231
Computer Networks

Mobile and Wireless Networks

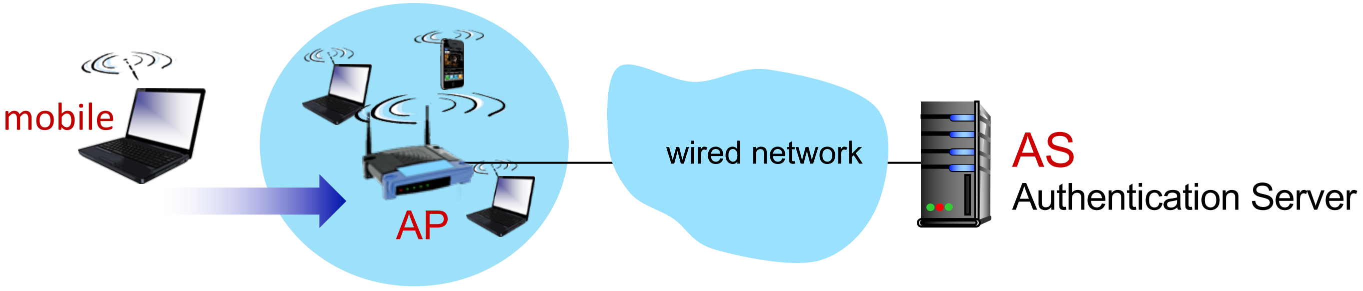
William Allen, PhD

Spring 2022

Mobile and Wireless Networks

- Smartphones combine aspects of mobile phones and mobile computers
  - Provide networked communications via cellular telephone system and local area networking
  - Support standard Internet protocols (TCP/IP, etc.)
  - Use computer-like Operating Systems and apps
- Wireless networks also communicate via radios, but are based on the IEEE 802.11 standard instead of cellular telephony standards
  - Thus, wireless networking and mobile computing are related but not identical

802.11: authentication, encryption

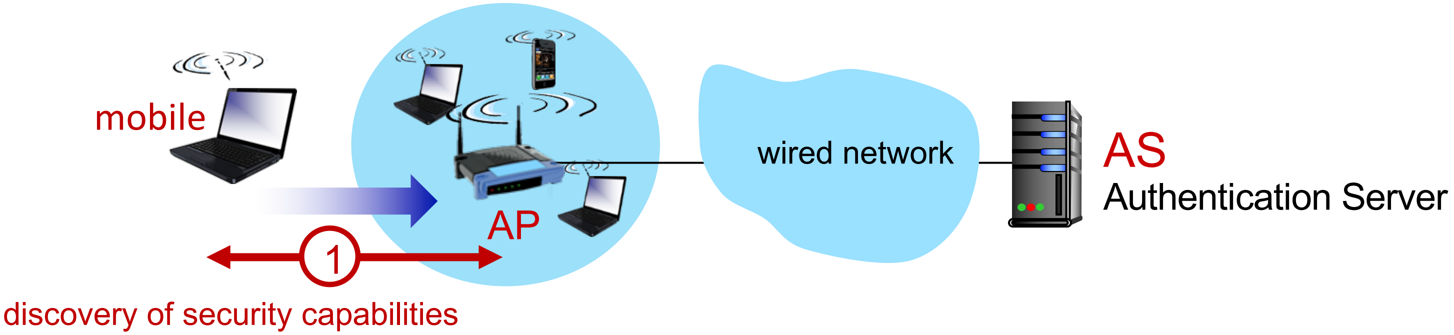


Arriving mobile device must:

- associate with an access point to establish communication over wireless link
- *optionally*: authenticate to the network

There are several steps in the process

802.11: authentication, encryption

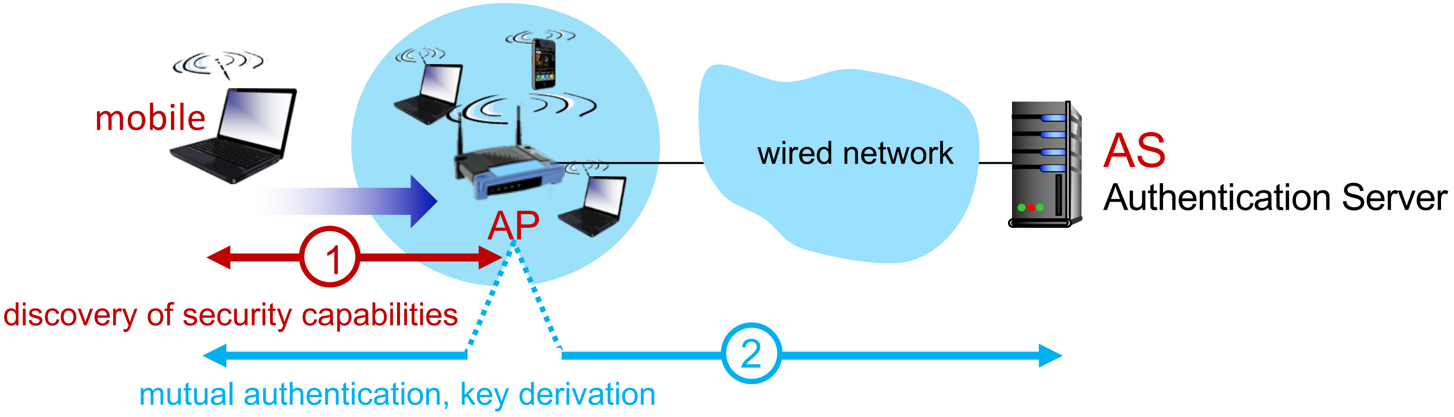


① Discovery of security capabilities:

- AP advertises its presence, notifies mobile device of the forms of authentication and encryption that are supported by the AP
- device requests specific authentication & encryption methods

Although mobile device and AP are already exchanging messages, mobile device is not yet authenticated and does not have encryption keys

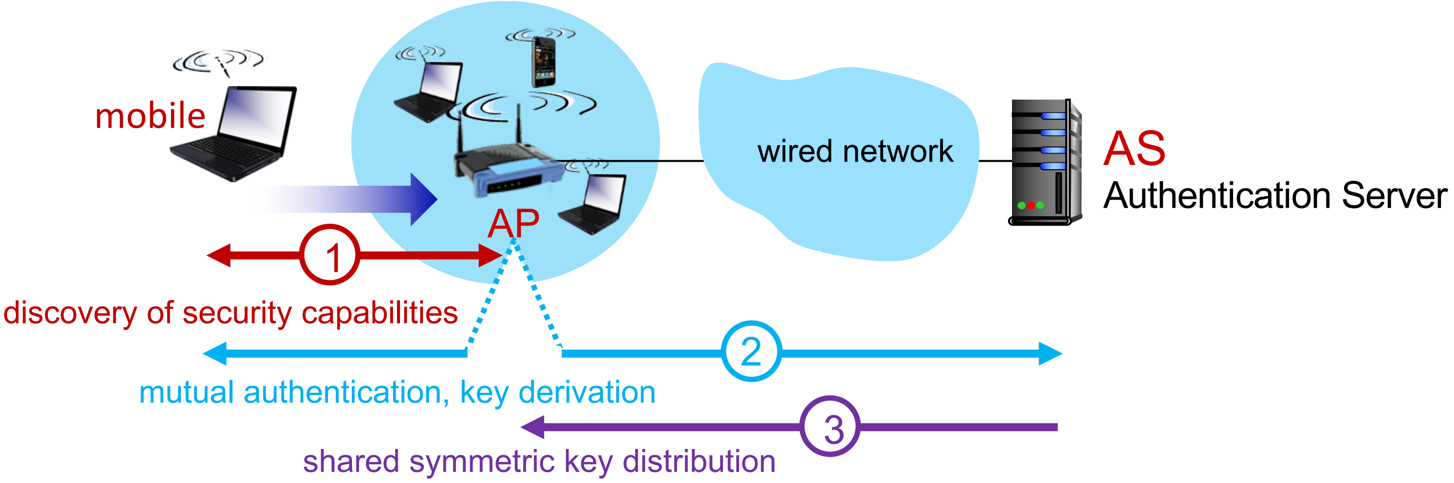
802.11: authentication, encryption


mobile
AP
wired network
AS
Authentication Server
1
discovery of security capabilities
2
mutual authentication, key derivation

② Mutual authentication and derivation of shared symmetric key

- AS and mobile already have a shared secret (e.g., password)
- AS, mobile use shared secret, nonces (prevent relay attacks), and cryptographic hashing to authenticating each other
- AS and mobile separately derive the symmetric session key (the AP does not participate in this exchange)

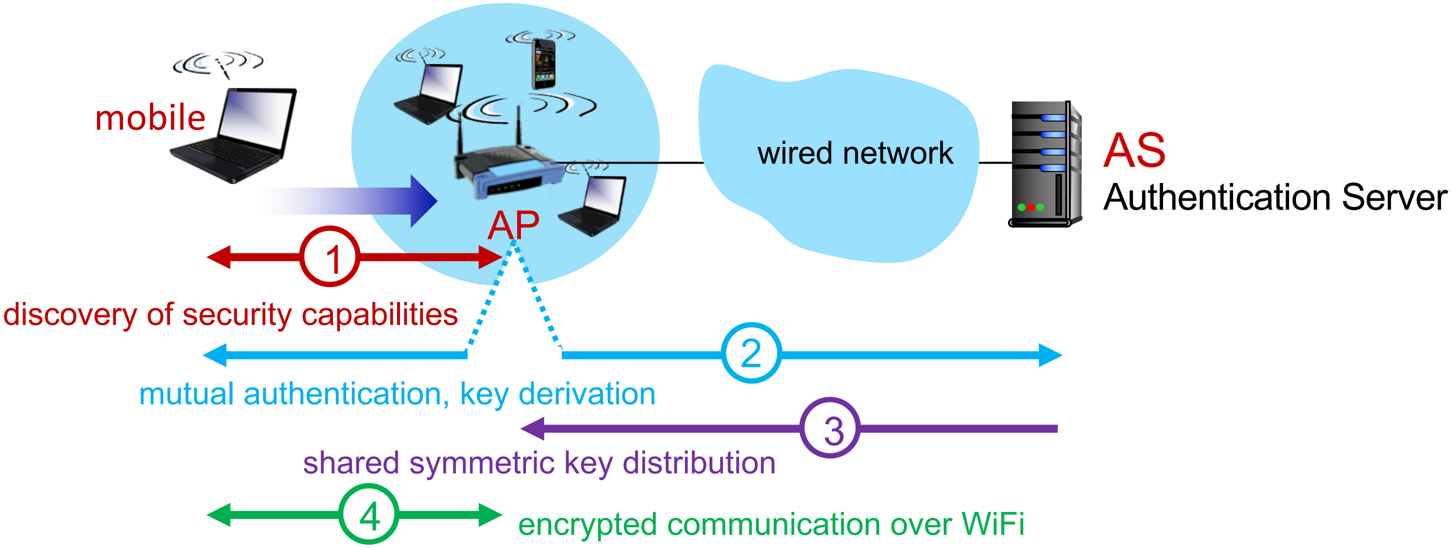
802.11: authentication, encryption


mobile
AP
wired network
AS
Authentication Server
1
discovery of security capabilities
2
mutual authentication, key derivation
3
shared symmetric key distribution

③ Distribution of shared symmetric session key

- (e.g., for AES encryption)
- same session key was derived at mobile and AS
- AS informs AP of the shared symmetric session key

802.11: authentication, encryption



mobile

AP

wired network

AS

Authentication Server

1 discovery of security capabilities

2 mutual authentication, key derivation

3 shared symmetric key distribution

4 encrypted communication over WiFi

④ Begin encrypted communication between mobile and remote host via AP

- uses the shared symmetric session key so that traffic from mobile to AP is encrypted

WiFi Security Issues

- Wireless networks are vulnerable to most of the attacks against wired networks, but they are also susceptible to additional attacks due to the open nature of radio transmission
  - attackers can more easily monitor traffic and discover MAC addresses which they can later spoof
  - denial of service attacks are easier because attackers can send interfering signals or corrupted packets
  - wireless access points can be attacked by sending false routing or network management packets
  - neighboring wireless networks can interfere because they also use the same radio channels

Wireless Privacy

- An obvious concern is that data transmitted over radio networks can be *monitored* by anyone with the correct type of receiver, which any WiFi device already has
  - As we have seen, unencrypted data can contain logins, passwords and other private information
- Due to the range of WiFi networks, they can often be monitored from outside of the view of the users connected to the network
  - WiFi signals can be received from cars in the street or from buildings near the network’s location

Jamming – a Simple DoS Attack

- Jamming - a simple way to prevent WiFi nodes from communicating
  - transmit random data on the WiFi frequency and 802.11 will detect that traffic as a collision and stop transmitting new frames
  - the attacker's transmitter will not follow the Collision Avoidance protocol and continues to transmit frames, preventing other nodes from sending
- However, jamming is easily detected and it violates U.S. law
  - *47 U.S. Code § 333, Communications Act of 1934*
  - "it is illegal to interfere with radio signals"

WiFi Deauthentication

- The 802.11 protocol includes a way to "*block a rogue node from re-connecting to the network*"
  - This uses a "*deauthentication frame*", a management message from the network's base station to a specific node that tells it to *drop the connection* immediately
- However, an attacker can *spoof* the address of the base station and send a deauthentication frame to a node to stop a legitimate connection
  - this can cause a denial-of-service or can be used to force a node to connect to a malicious base station
    - the IEEE 802.11w protocol update uses cryptography to create management frames that cannot be spoofed

Man-In-the-Middle Attacks

- Since anyone can buy a wireless access point, an attacker can set up an unauthorized AP
  - the attacker can then trick users into using this AP instead of authorized access points and either monitor or intercept and modify their traffic
- This kind of attack won’t benefit from link-level encryption between the device and the AP
  - packet data is decrypted when it arrives at the AP
- However, a secure tunnel or end-to-end encryption will protect the data in the traffic
  - thus, SSL/TLS or a VPN is recommended for WiFi

Mobile and Wireless Networks

- M-commerce (mobile-commerce) uses mobile phones
- NFC (Near Field Communication) allows mobile device to act as an RFID smartcard and interact with a nearby reader for payment
- Sensor networks use nodes for gathering and relaying information about the physical state of the world
  - Nodes may be small, separate devices
    - Examples: cameras or phones
  - Or, nodes may be embedded in familiar devices
    - Examples: cars, appliances, wireless parking meters

Electromagnetic Communications

- Radio transmission
  - Omnidirectional waves, easy to generate, travel long distances, penetrate buildings
- Microwave transmission
  - Directional waves requiring focused antennas and repeaters, do not penetrate very far into buildings
- Infrared transmission
  - Unguided waves for short-range communication, cheap, easy to build, does not penetrate solid walls

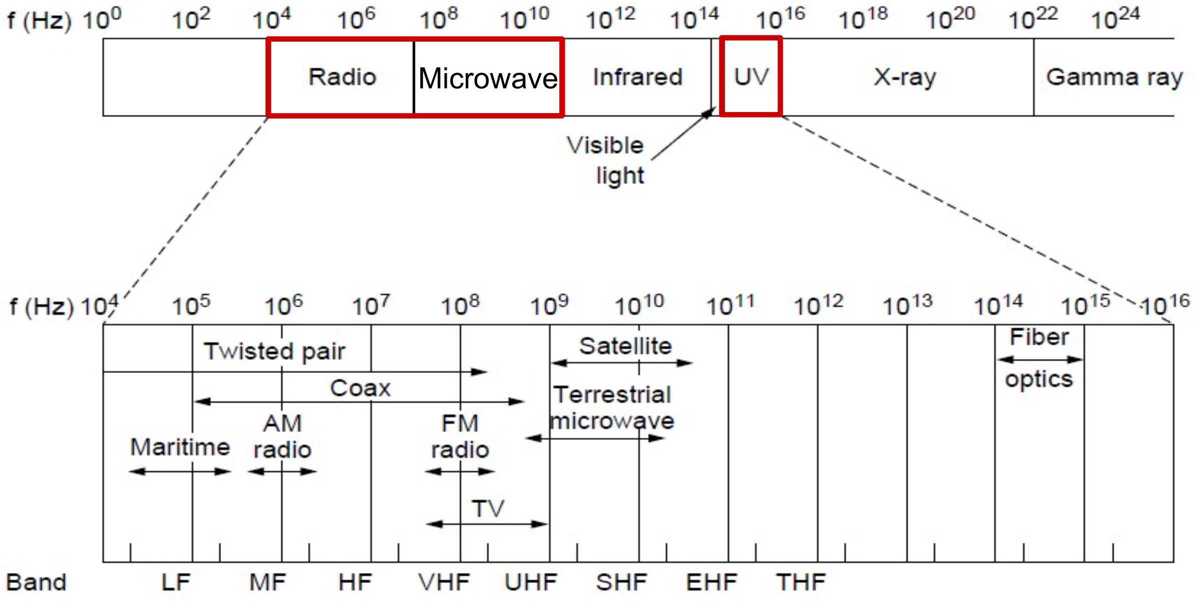
Radio Transmission Techniques

- The electromagnetic spectrum
  - Modulate wave amplitude, frequency, or phase
- Frequency hopping spread spectrum
  - Transmitter hops from frequency to frequency hundreds of times per second
- Direct sequence spread spectrum
  - Code sequence spreads data signal over wider frequency band
- Ultra-wideband communication
  - Sends a series of low-energy rapid pulses, varying their carrier frequencies to communicate information

Electromagnetic Spectrum

Networks use a range of frequency bands:

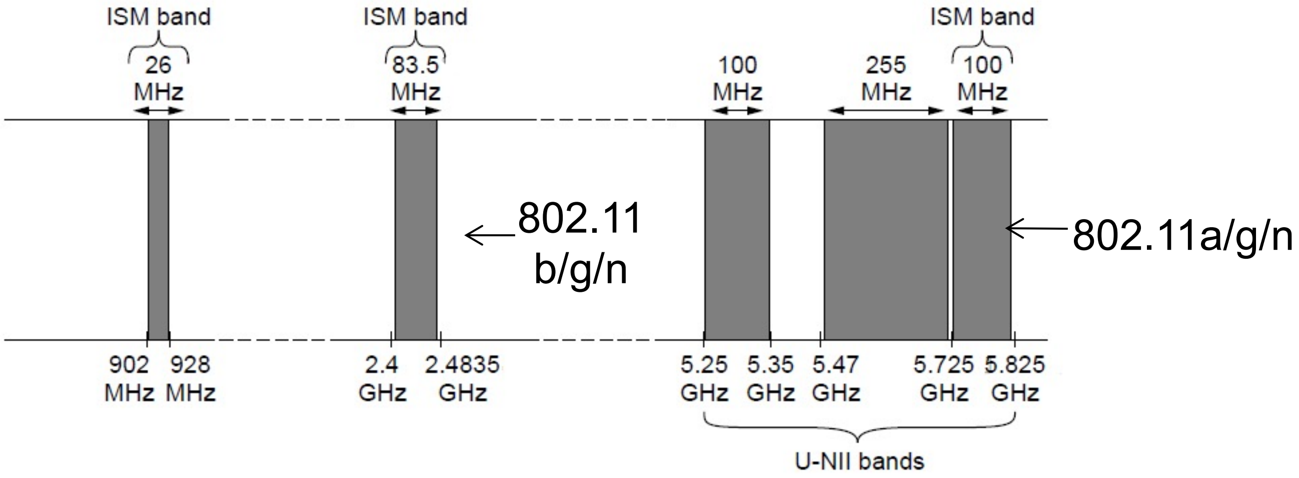
- Radio band: wide-area broadcast, RFID
- Microwave band: LANs and 3G/4G, IoT devices
- Fiber Optic often uses light in the UV-range


f (Hz) 10^0 10^2 10^4 10^6 10^8 10^10 10^12 10^14 10^16 10^18 10^20 10^22 10^24
Radio
Microwave
Infrared
UV
X-ray
Gamma ray
Visible light
f (Hz) 10^4 10^5 10^6 10^7 10^8 10^9 10^10 10^11 10^12 10^13 10^14 10^15 10^16
Twisted pair
Coax
Satellite
Terrestrial microwave
Fiber optics
Maritime
AM radio
FM radio
TV
Band LF MF HF VHF UHF SHF EHF THF

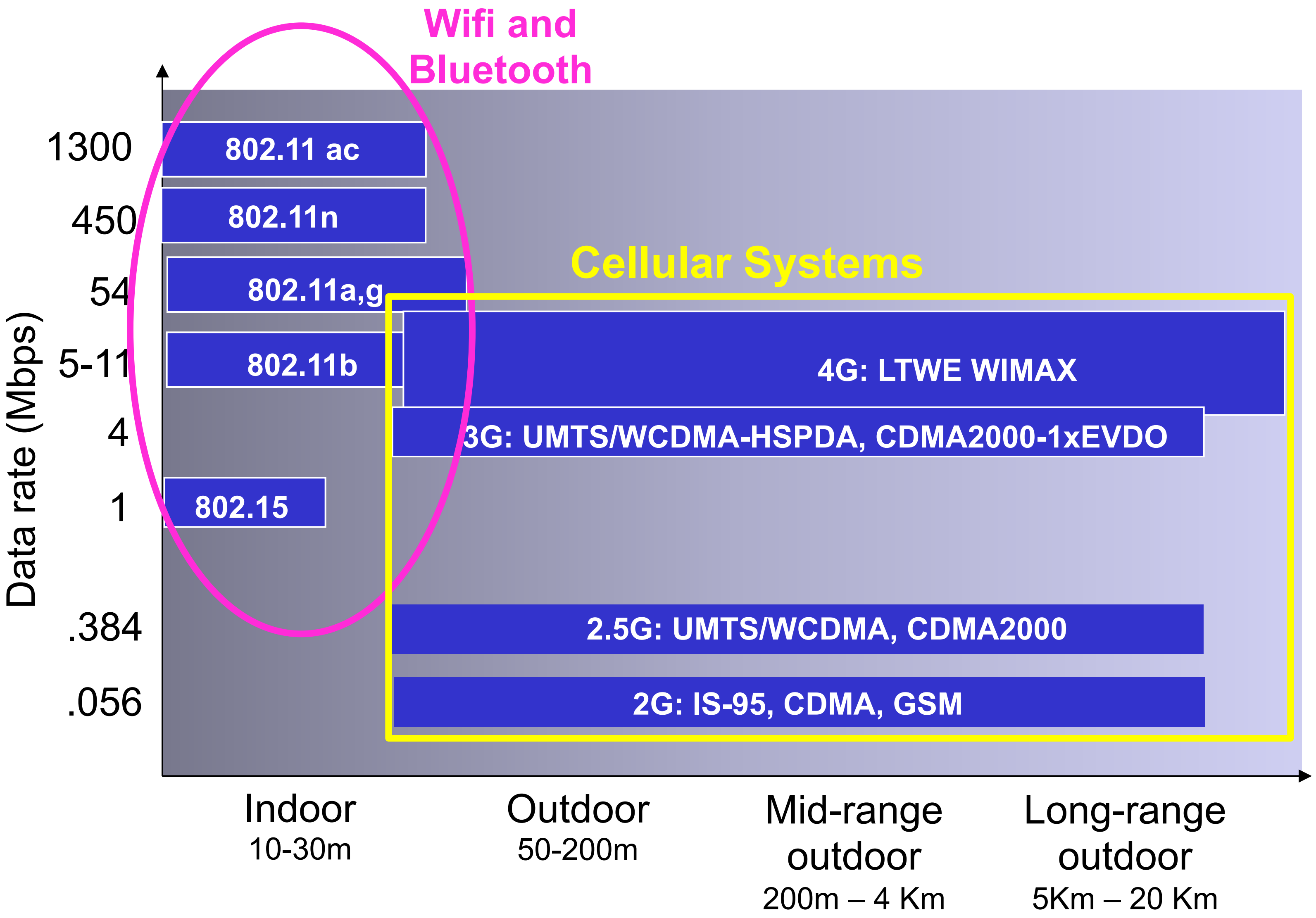
Electromagnetic Spectrum

There are special frequency bands for *Industrial, Scientific, Medical* (ISM) communications:

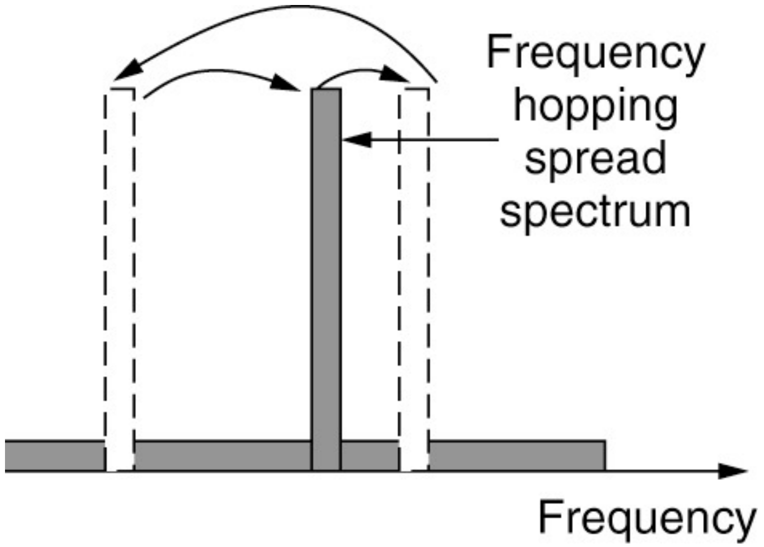
- No license required for use at low power
- Widely used for home/business networking
  - WiFi, Bluetooth, Zigbee, Z-wave, etc.



Characteristics of selected wireless links

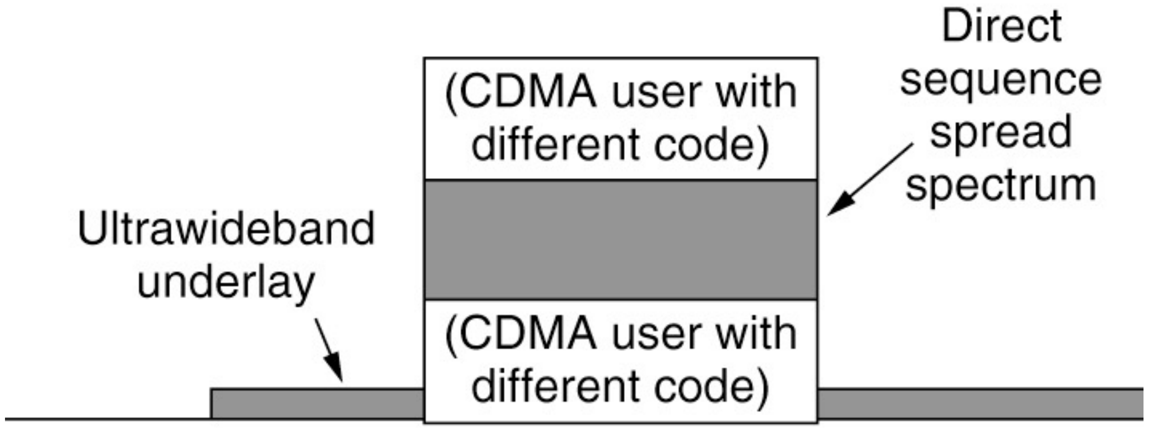


Frequency Hopping Spread Spectrum



Frequency hopping spread spectrum changes frequency along a pre-determined sequence to avoid interference. The sender and receiver follow the same sequence.

Direct Sequence Spread Spectrum


Direct sequence spread spectrum
(CDMA user with different code)
Ultrawideband underlay
(CDMA user with different code)

Direct sequence spread spectrum uses a code sequence to spread the data signal over a wider frequency band.

Mobile Networks

- Early systems used circuit switching because they were derived from the telephone system
  - Connection-oriented networks
  - Caller must dial the called party’s number and wait for a connection before talking or sending data
  - Route maintained until call is terminated
- Modern systems moved to packet switching
  - Connectionless networks
  - Every packet is routed independently
  - If some routers go down during a session, the system can dynamically reconfigure itself

Mobile Networks

- First-generation mobile phone systems
  - Transmitted voice calls as continuously varying (analog) signals
- Second-generation (2G) mobile phone systems
  - Transmitted voice calls in digital form to increase capacity, improve security, and offer text messaging
- Third generation (3G) offered both digital voice and broadband digital data services
- 4G: e.g., LTE (Long Term Evolution) technology offers faster speeds than 3G
- 5G technologies have even faster speeds, up to 10 Gbps
  - Main distinction between 4G & 5G: frequency spectrum they use

First-Generation (1G) Technology: Analog Voice

- 1946 push-to-talk systems (e.g., CB radio, walkie-talkie)
- 1960 IMTS (Improved Mobile Telephone System)
  - Two frequencies: one for sending, one for receiving
- 1983 AMPS (Advanced Mobile Phone System)
  - Analog mobile phone system
  - Cells are typically 10 to 20 km across
  - Uses FDM to separate channels
  - 832 full-duplex channels that each consist of a pair of simplex channels (Frequency Division Duplex)
  - Each simplex channel is 30 kHz wide
  - AMPS divides them into *paging* channels and *access* channels

Call Management

- Outgoing calls
  - Phone switched on, number entered, CALL button hit
  - Phone transmits called number and its own identity on the access channel
  - Base Station informs the Mobile Switching Center (MSC) and it looks for an available channel for the call
- Incoming calls
  - Idle phones continuously listen to the paging channel to detect messages directed at them
  - Caller's connection request packet is sent to base station in the current cell by broadcasting on the paging channel
  - The called phone detects the request and responds
  - Called phone switches to the access channel and starts ringing

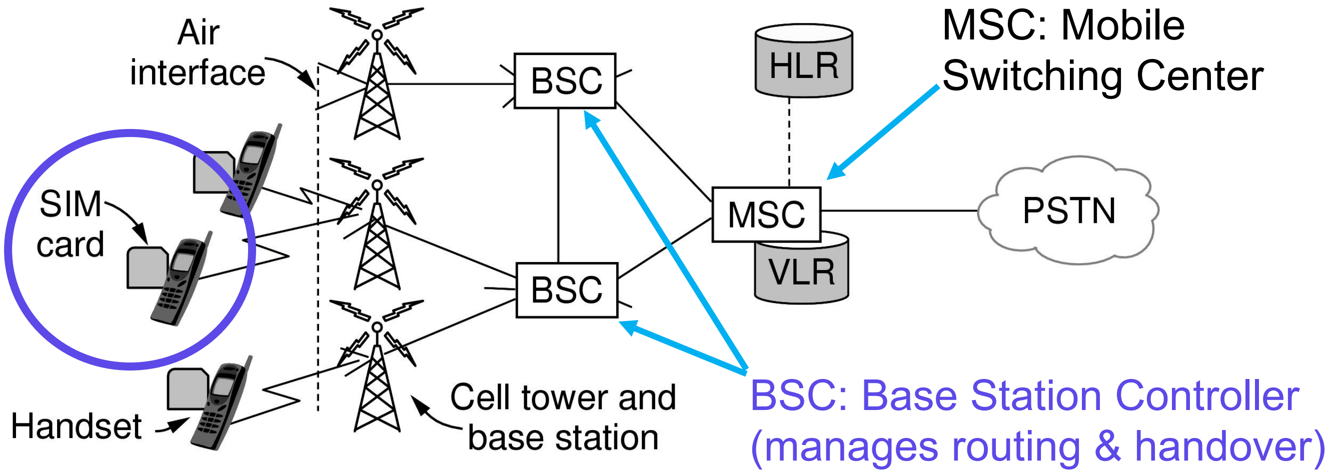
Second-Generation (2G) Technology: Digital Voice

- Digital advantages
  - Provided capacity gains by allowing voice signals to be digitized and compressed
  - Improved security by allowing voice and control signals to be encrypted
  - Deterred fraud and eavesdropping, whether from intentional scanning or echoes of other calls due to RF propagation
  - Enabled new services such as text messaging
- Three main systems were developed
  - D-AMPS (Digital Advanced Mobile Phone System)
  - GSM (Global System for Mobile communications)
  - CDMA (Code Division Multiple Access)

GSM: Global System for Mobile Communications

Mobile contains a Subscriber Identity Module (SIM card) where user credentials are stored

- Also stores the mobiles’ last known location in the HLR (Home Location Register) for call routing
- Base Station Controllers keep track of visiting mobiles in the VLR (Visitor Location Register)



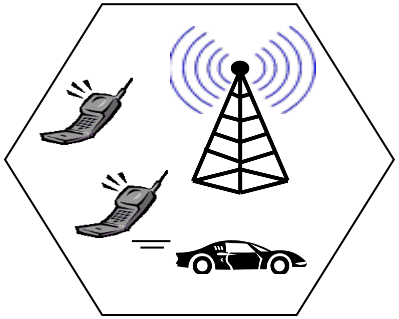
MSC: Mobile Switching Center

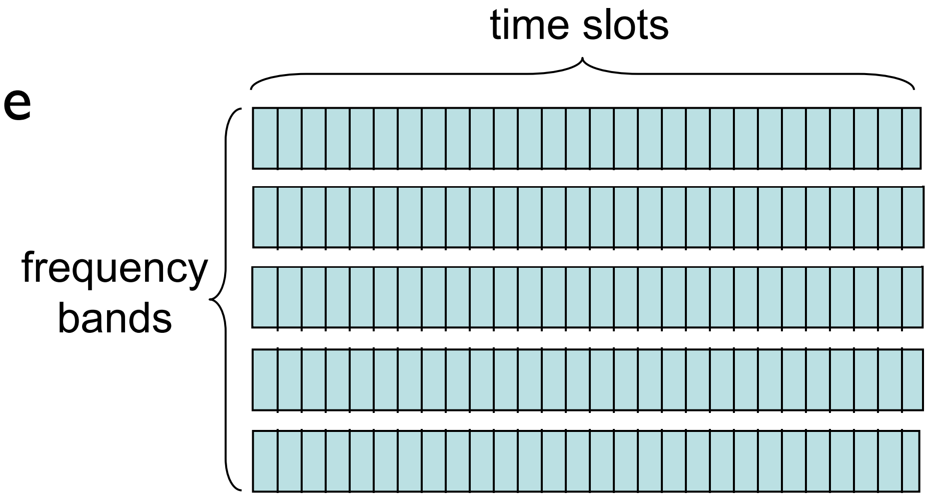
BSC: Base Station Controller (manages routing & handover)

Cellular networks: the first hop

Two techniques for sharing mobile-to-BaseStation radio spectrum

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

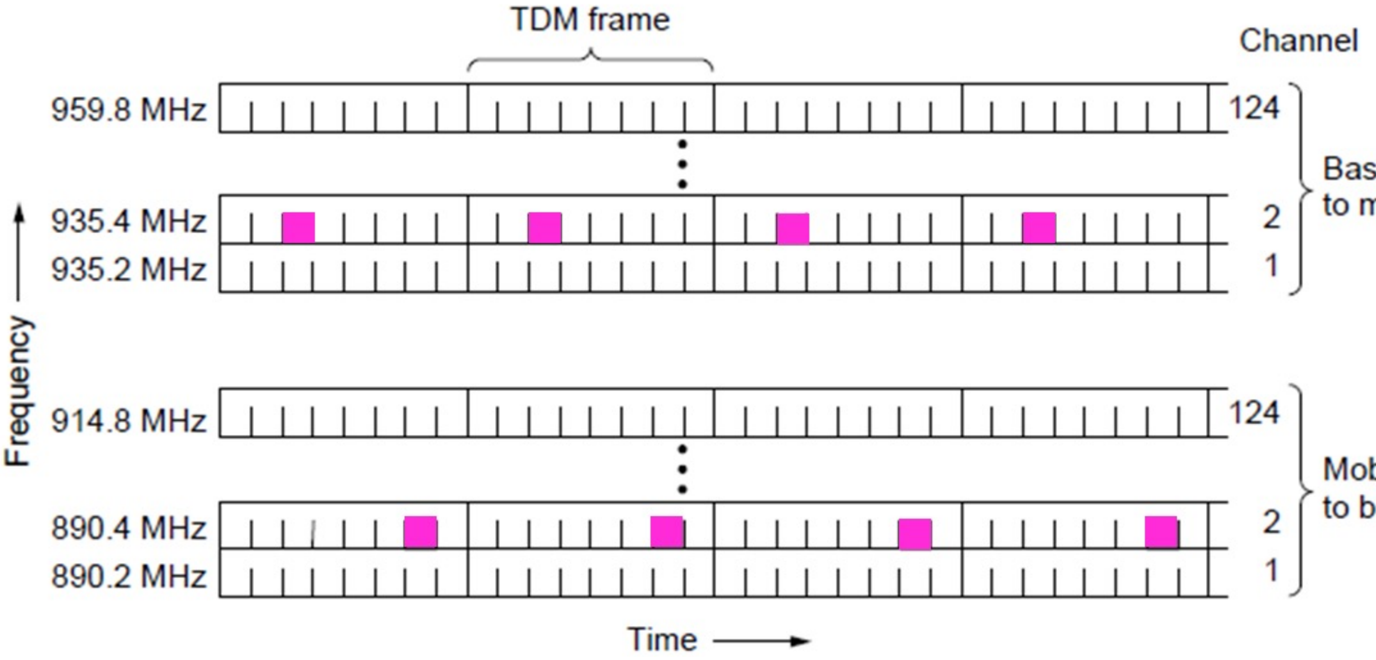




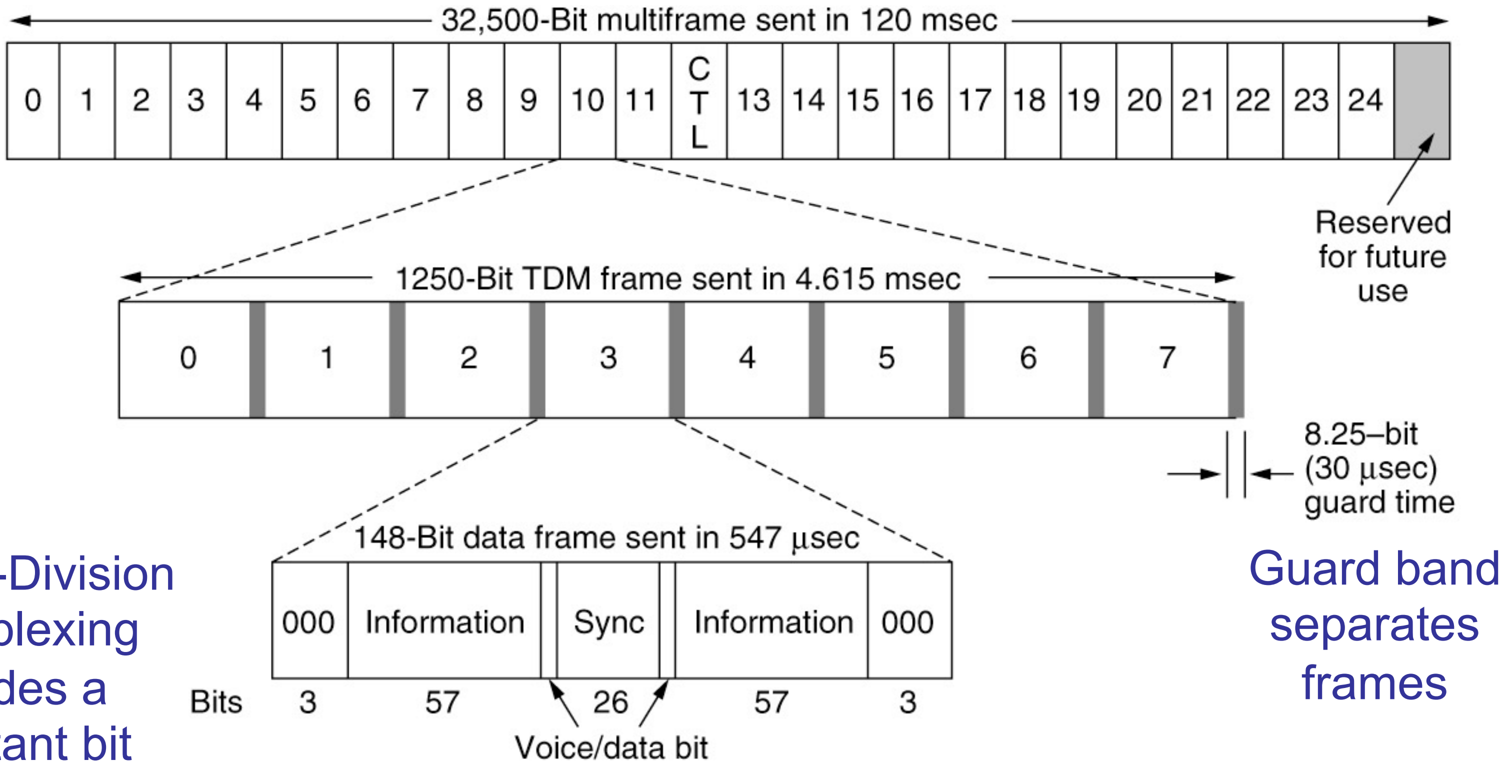
GSM: Global System for Mobile Communications

Air interface uses 200 KHz FDM channels with an eight-slot TDM frame every 4.615 ms

- Mobile is assigned up- and down-stream slots to use
- Each slot is 148 bits long, data rate is 27.4 kbps



GSM: Global System for Mobile Communications


32,500-Bit multiframe sent in 120 msec
0
1
2
3
4
5
6
7
8
9
10
11
C T L
13
14
15
16
17
18
19
20
21
22
23
24
Reserved for future use
1250-Bit TDM frame sent in 4.615 msec
0
1
2
3
4
5
6
7
8.25–bit (30 µsec) guard time
148-Bit data frame sent in 547 µsec
000
Information
Sync
Information
000
Bits
3
57
26
57
3
Voice/data bit

Time-Division Multiplexing provides a constant bit rate for voice and data

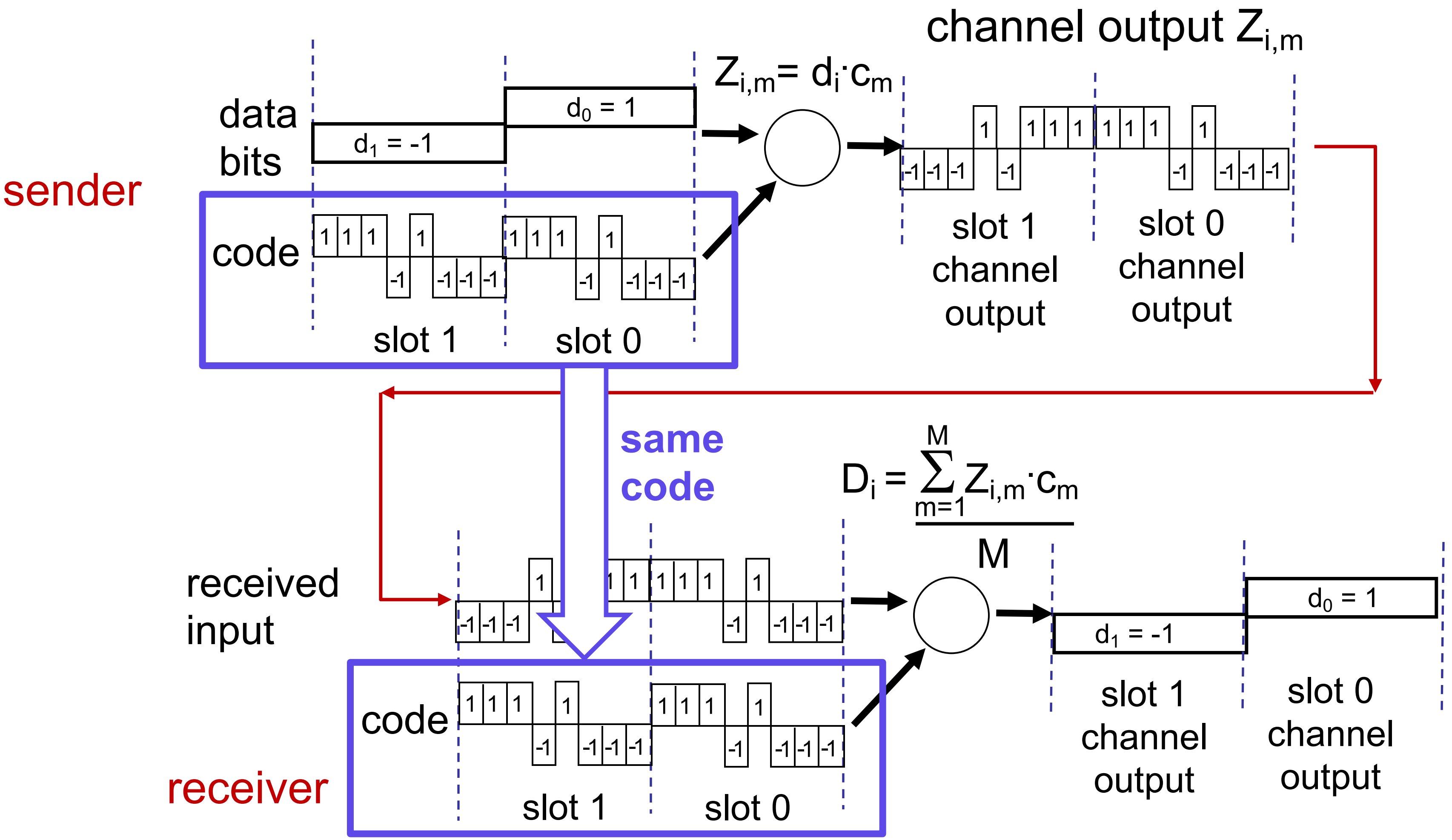
Guard band separates frames

A portion of the GSM framing structure.

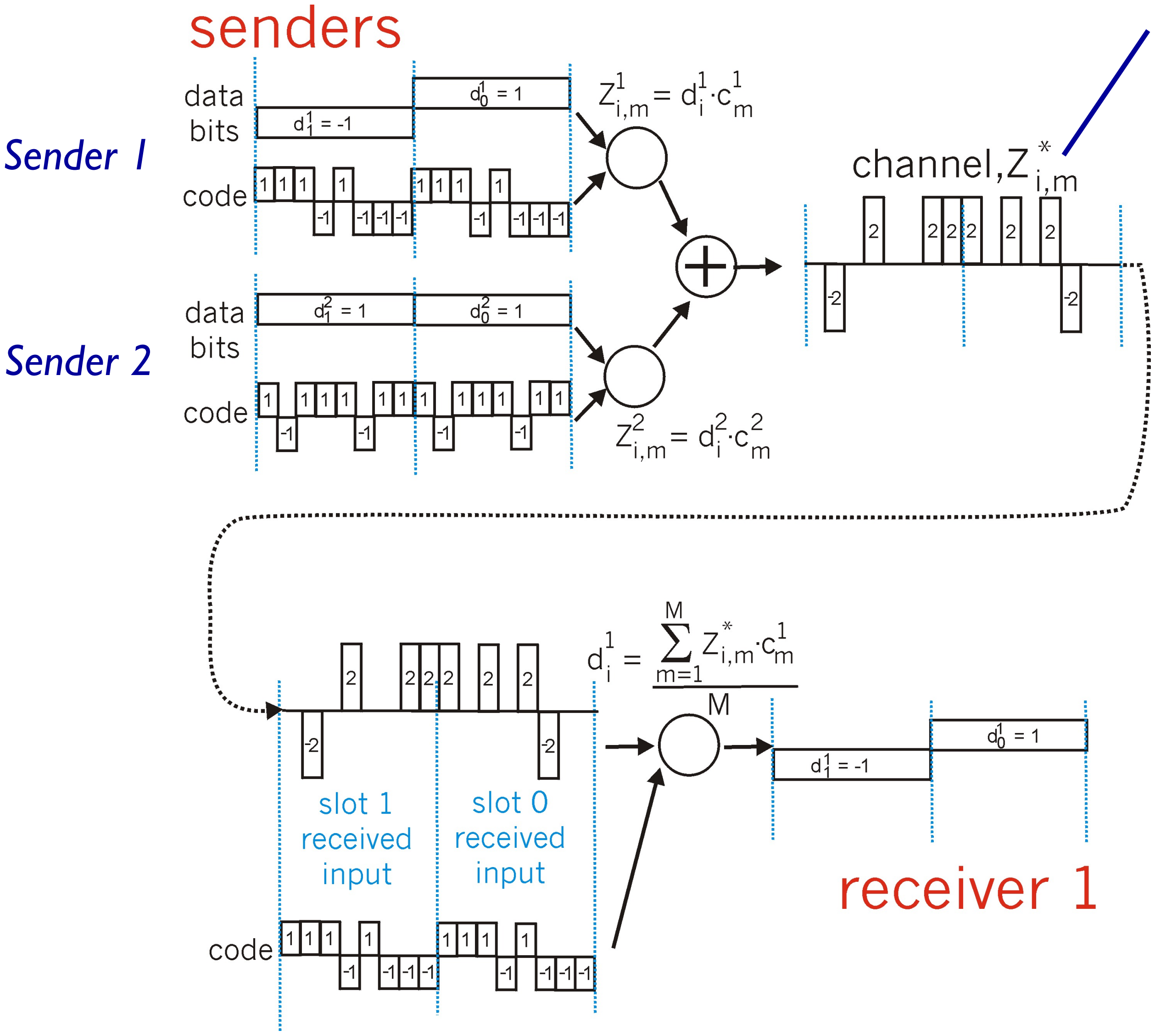
Code Division Multiple Access (CDMA)

- A unique “code” (i.e., *chipping sequence*) is assigned to each user
  - users share same frequency, each user has own “chipping” sequence to encode data
  - allows multiple users to “coexist” and they can each transmit simultaneously with minimal interference (if the 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 sender 2

using same code as sender 1, receiver 1 can recover sender 1’s original data from summed channel data

Third-Generation (3G) Technology: Digital Voice+Data

- With packet switching of digitized voice, voice and data can both be transmitted simultaneously
  - Provided broadband access, initially around 100Kilobits/sec but evolved into the Megabit/sec range
  - Improved security for communications by authentication of the network the user is connecting to
  - Most 3G systems are being dropped in favor of 4G
    - Verizon in 2020, T-Mobile in 2021, AT&T in 2022
- Many systems were based on enhanced 2G technology
  - W-CDMA (Wideband CDMA)
  - HSPA (High-Speed Packet Access)
  - CDMA2000 (another updated version of CDMA)

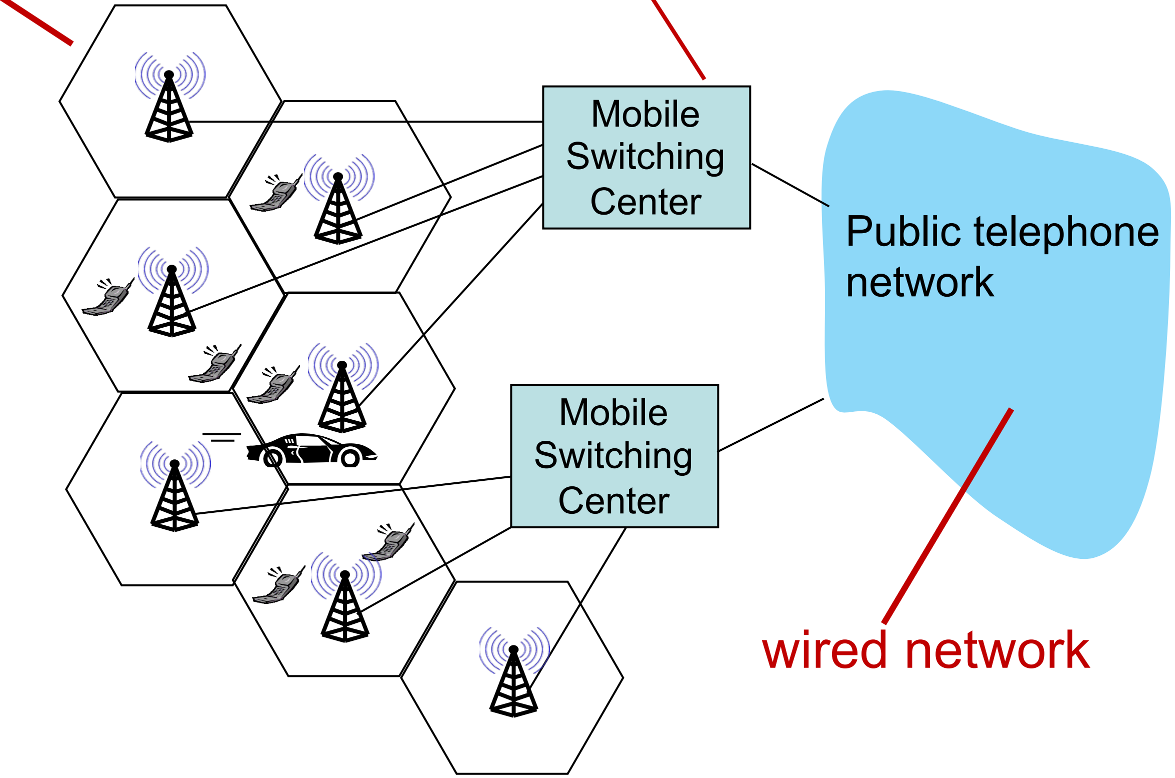
Architecture of a 3G cellular network

MSC

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

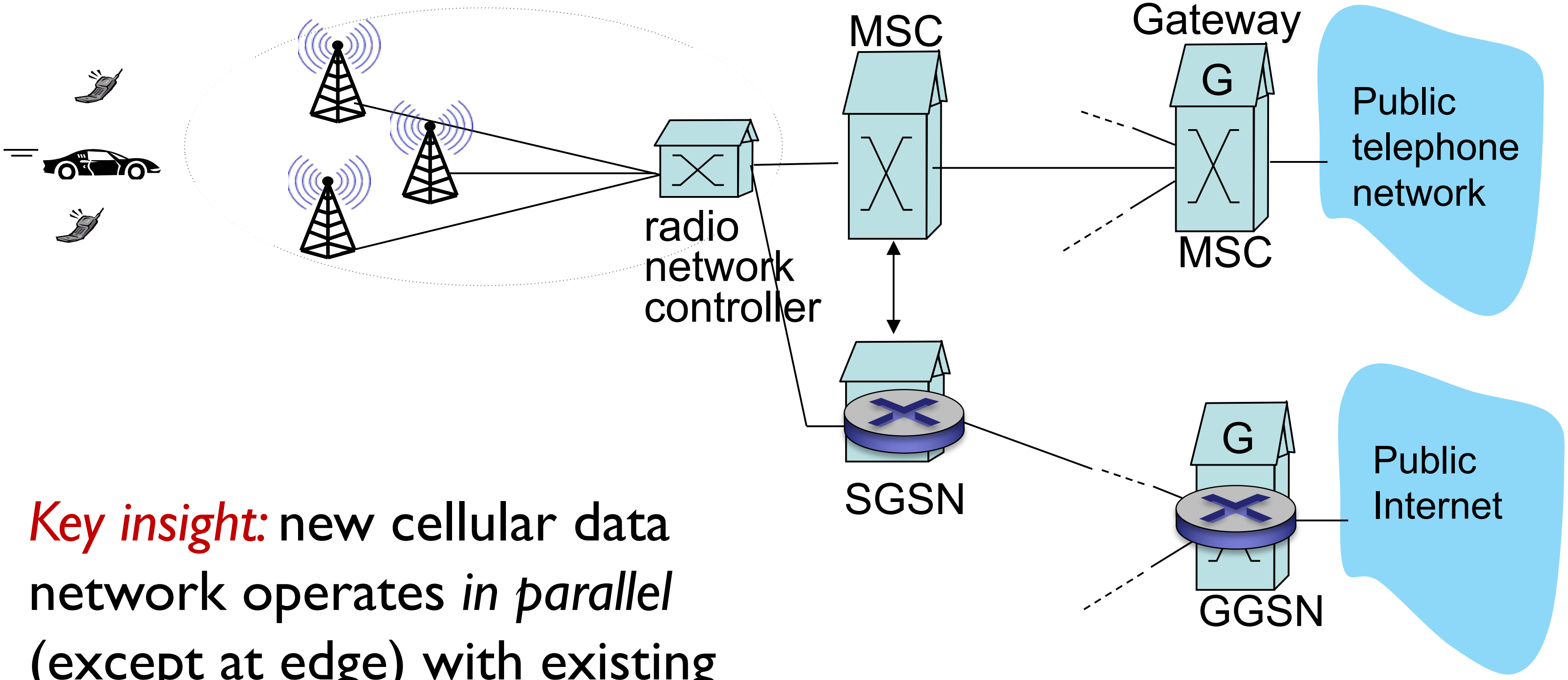
cell

- 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



wired network

3G (voice+data) network architecture

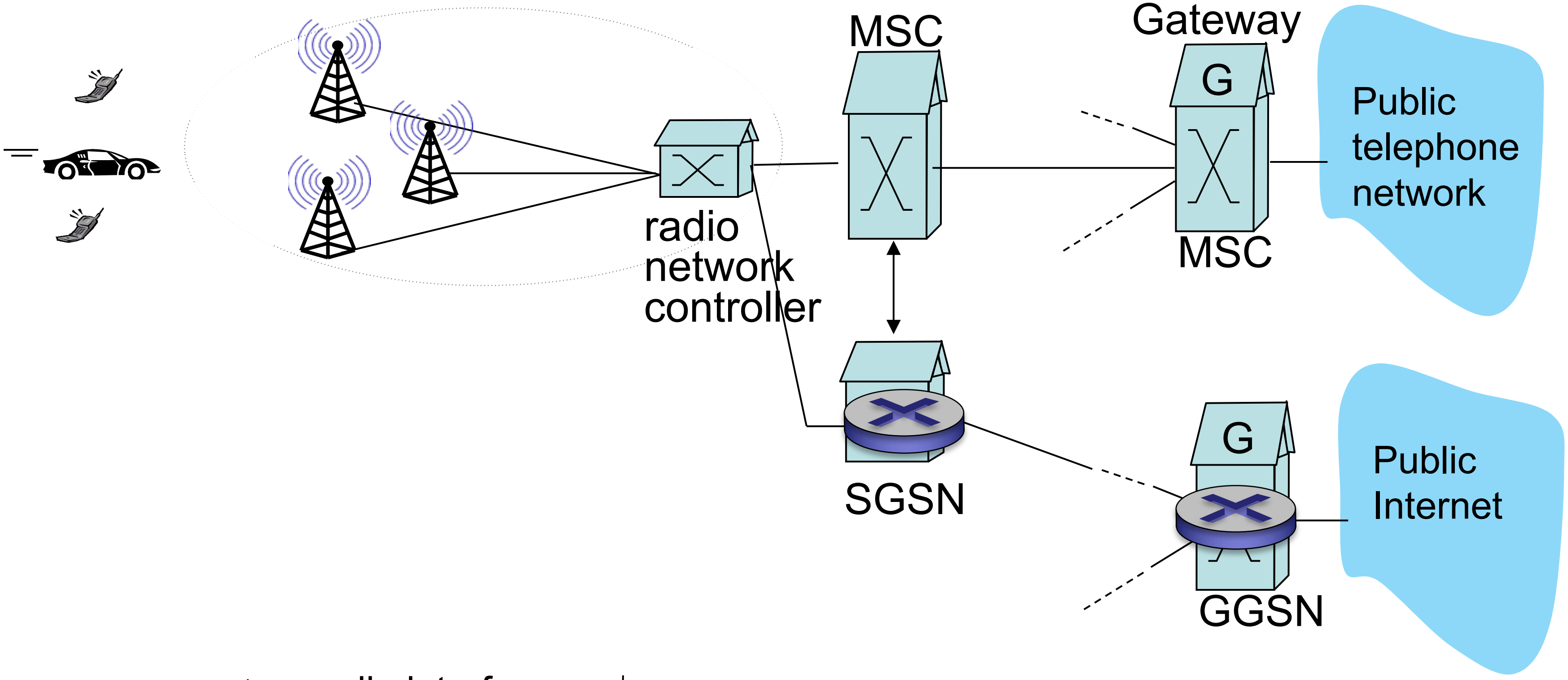


Serving GPRS Support Node (SGSN)
Gateway GPRS Support Node (GGSN)

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

3G (voice+data) network architecture



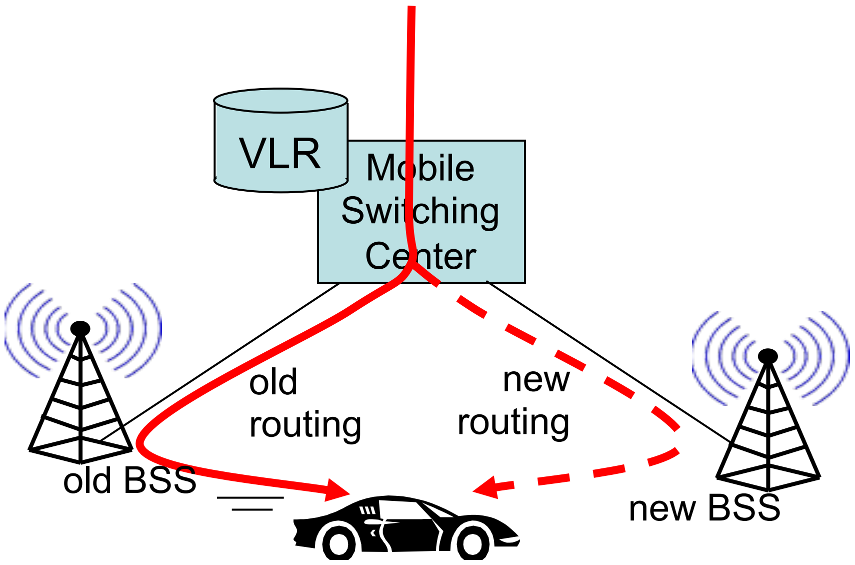
radio interface
(WCDMA, HSPA)

radio access network
Universal Terrestrial Radio
Access Network (UTRAN)

core network
General Packet Radio Service
(GPRS) Core Network

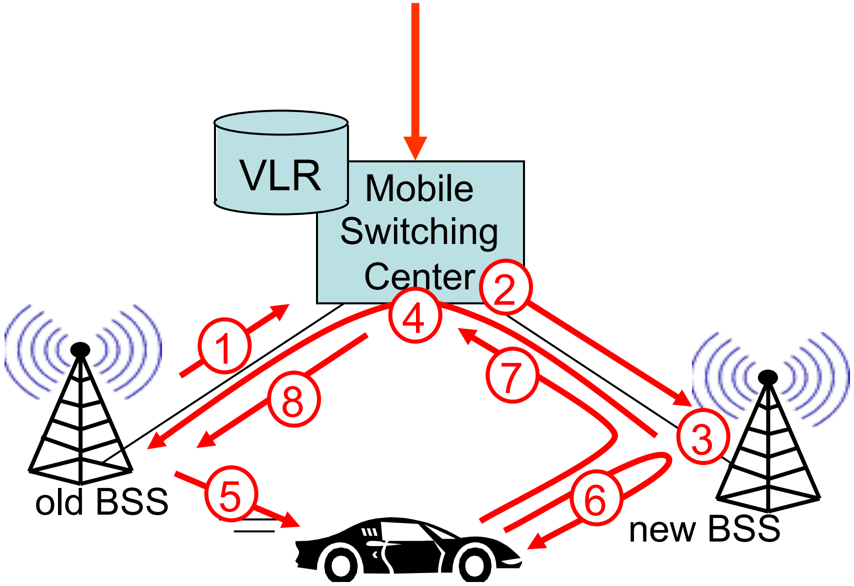
public
Internet

GSM: handoff with a common MSC



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

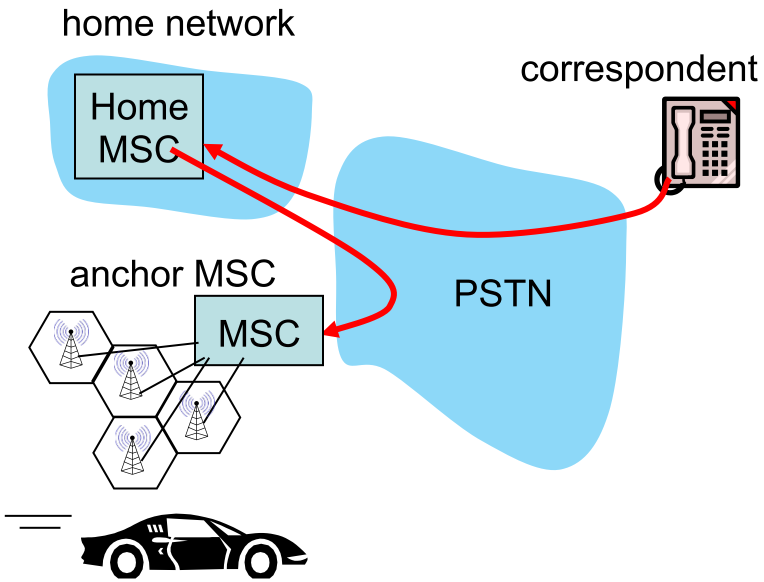
GSM: handoff with a common MSC



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 says it is ready to handoff
5. old BSS tells mobile to perform handoff to new BSS
6. mobile and new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call

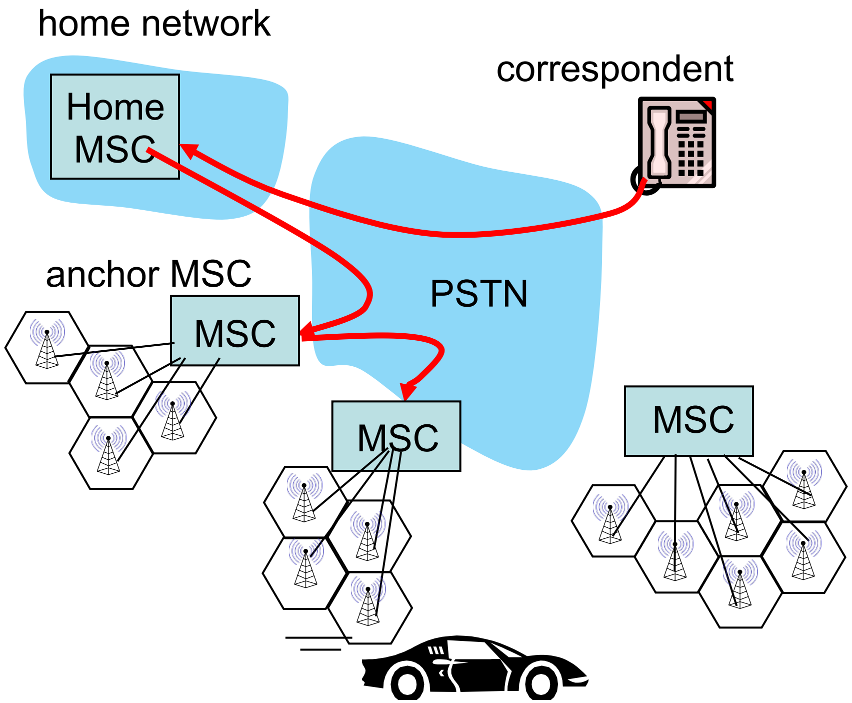
8 MSC-old-BSS resources released

GSM: handoff between MSCs



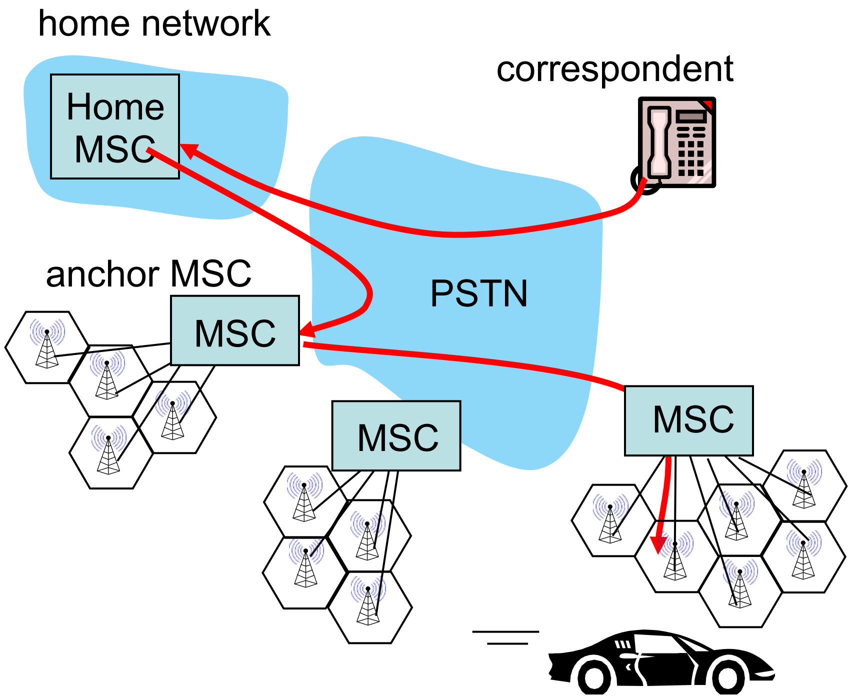
- *anchor MSC:* MSC where device is when call occurs
  - caller connects to home network, call is routed to the MSC nearest the called device

GSM: handoff between MSCs



- *anchor MSC:* MSC where device is when call occurs
  - when called device moves to a new cell, call is still routed through anchor MSC

GSM: handoff between MSCs



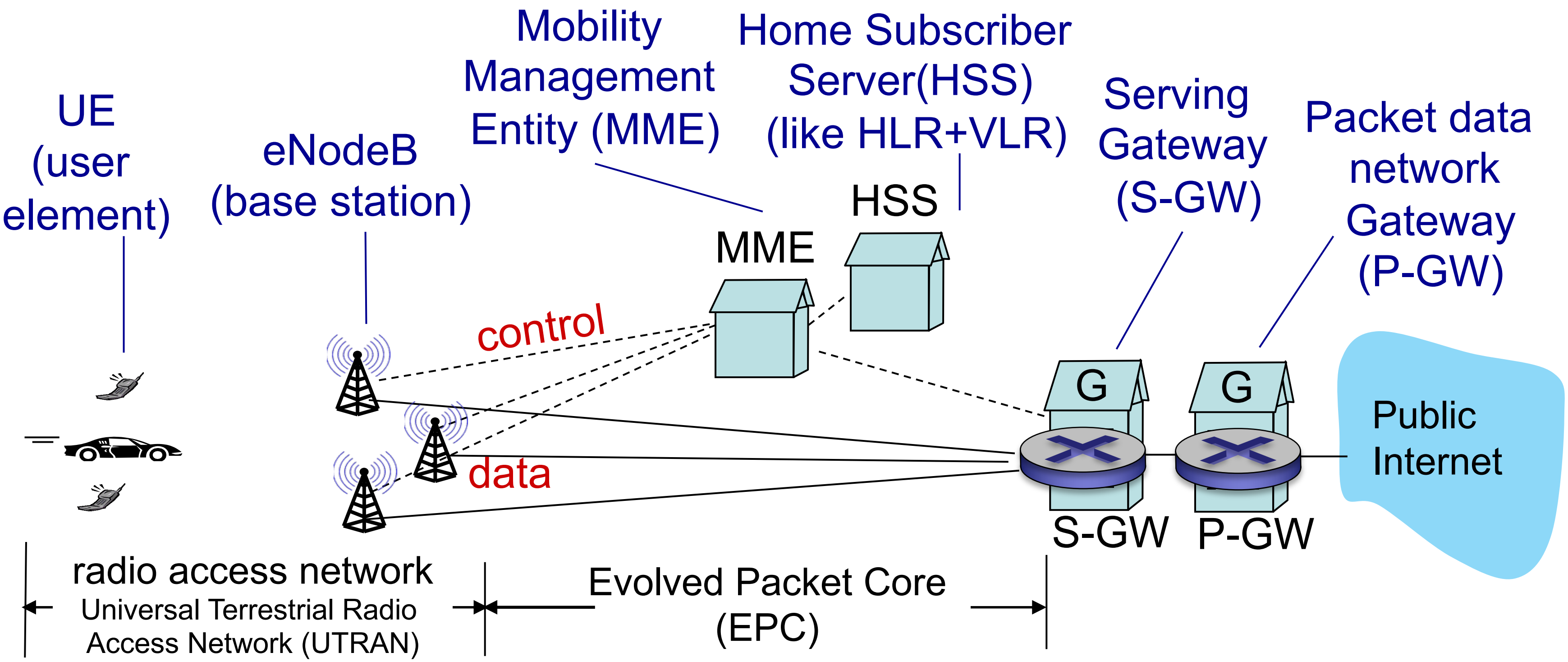
- *anchor MSC:* MSC where device is when call occurs
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- initially path gets longer, then optional path minimization step can be used to shorten multi-MSC chain

Fourth-Generation (4G) Technology: Packet Switching

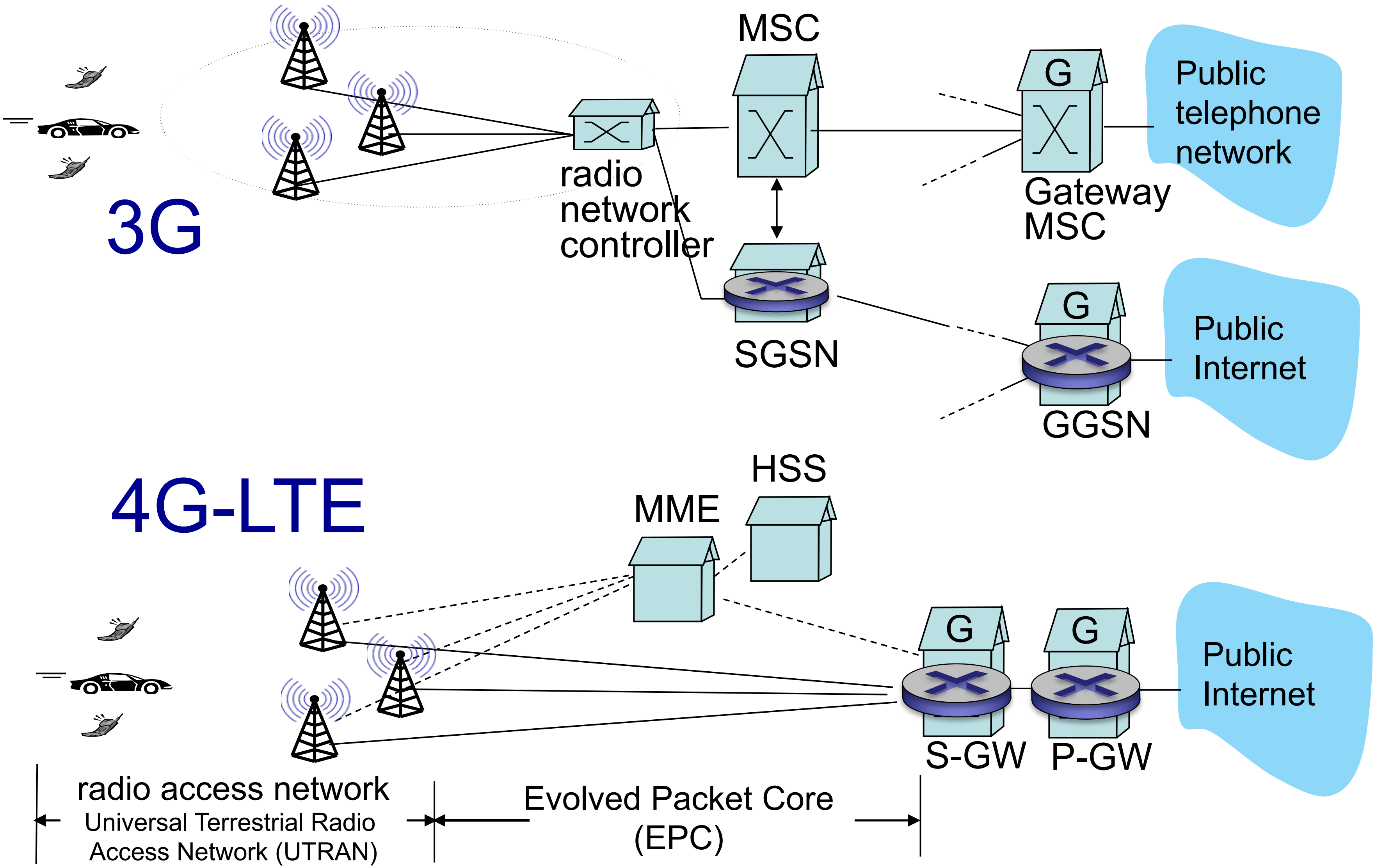
- Also called IMT Advanced
- Based on *packet-switched* technology
- EPC (Evolved Packet Core) allows packet switching
  - Simplified IP network separating voice traffic from the data network
    - Carries both voice and data in IP packets
  - *Voice over IP* (VoIP) network with resources allocated using the statistical multiplexing approaches
  - The EPC must manage resources in such a way that voice quality remains high in the face of network resources that are shared among many users

4G: differences from 3G

- all IP core: IP packets tunneled (through core IP network) from base station to gateway
- voice and data packets are both carried over the same IP network to the gateway



3G versus 4G LTE network architecture

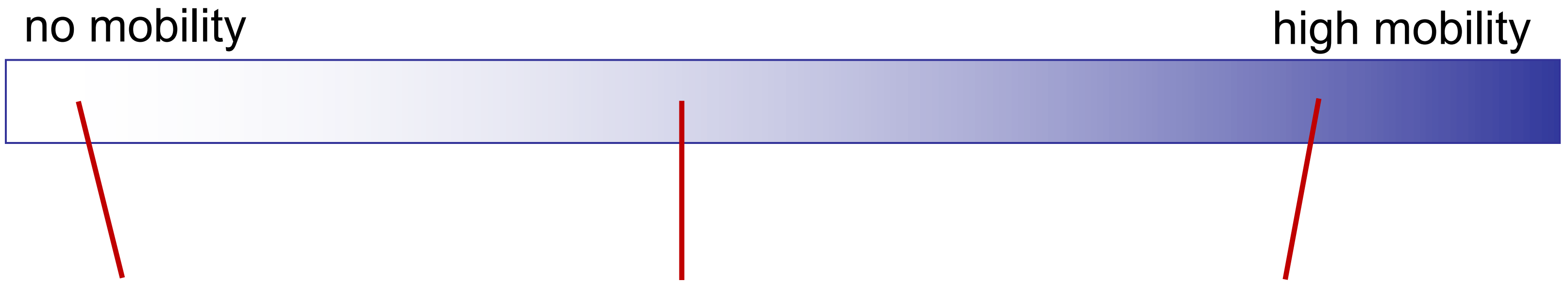


Fifth-Generation (5G) Technology

- Two main advantages:
  - *Higher data rates* and *lower latency* than 4G technologies
- Technology used to increase network capacity
  - Smaller cells using ultra-densification, faster offloading
  - *Increased bandwidth* with millimeter waves
  - *Increased spectral efficiency* through advances in massive MIMO (Multiple-Input Multiple-Output) technology
- Provides a network slicing feature
  - Cellular carriers can create *multiple virtual networks* on top of the same shared physical infrastructure
  - Can devote network portions to specific customer use cases

What is mobility?

- From the *network* perspective, there is a wide spectrum of mobility



no mobility

high mobility

mobile-capable, but non-moving wireless user, staying at the same access point

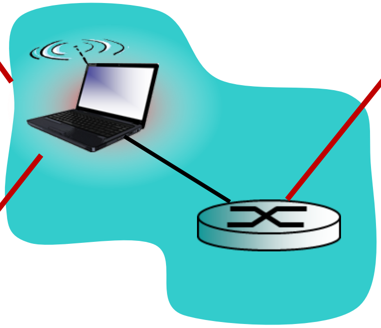
mobile user, connecting/ disconnecting from network using DHCP

mobile user, passing through multiple access points while maintaining ongoing connections (like a cell phone in a car)

Mobility: vocabulary

home network: permanent "home" of the mobile
(e.g., 128.119.40/24)

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



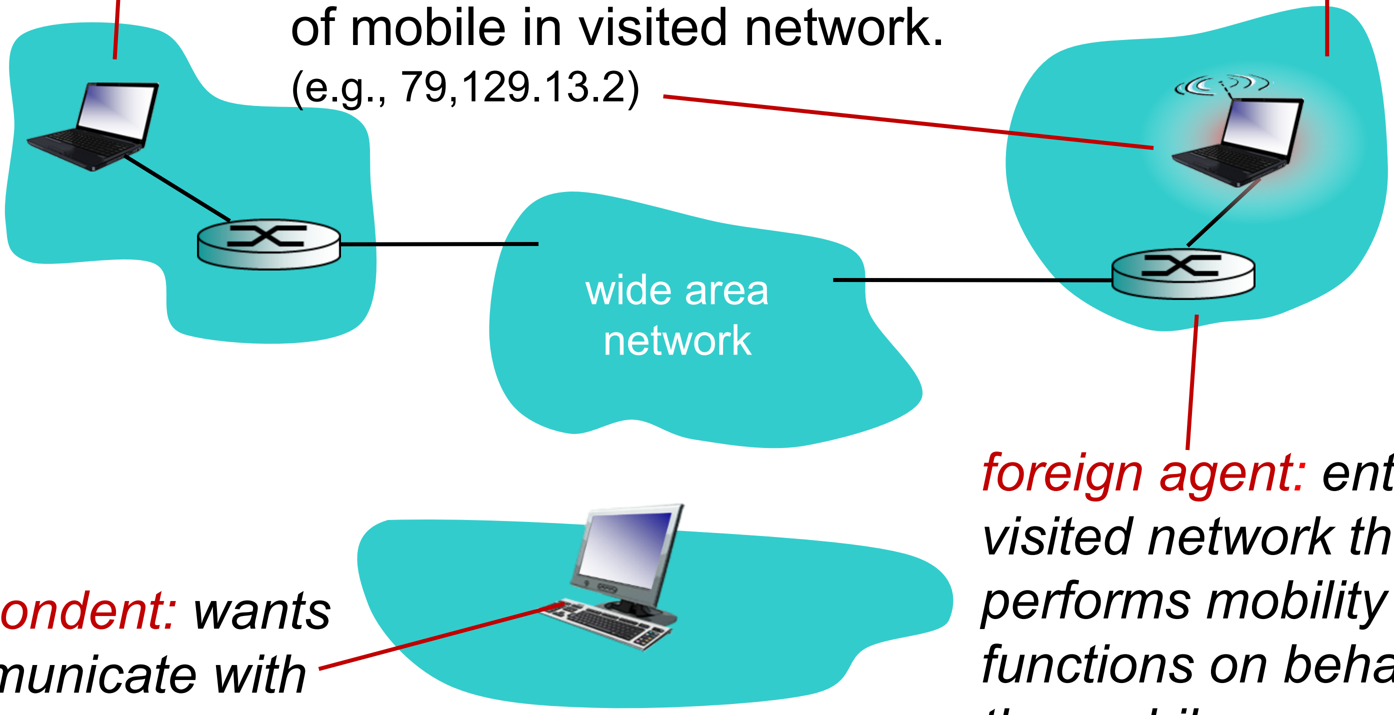
permanent address:
address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

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 of mobile in visited network. (e.g., 79,129.13.2)



correspondent: wants to communicate with the mobile

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

Mobility: two approaches

1. *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
2. *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

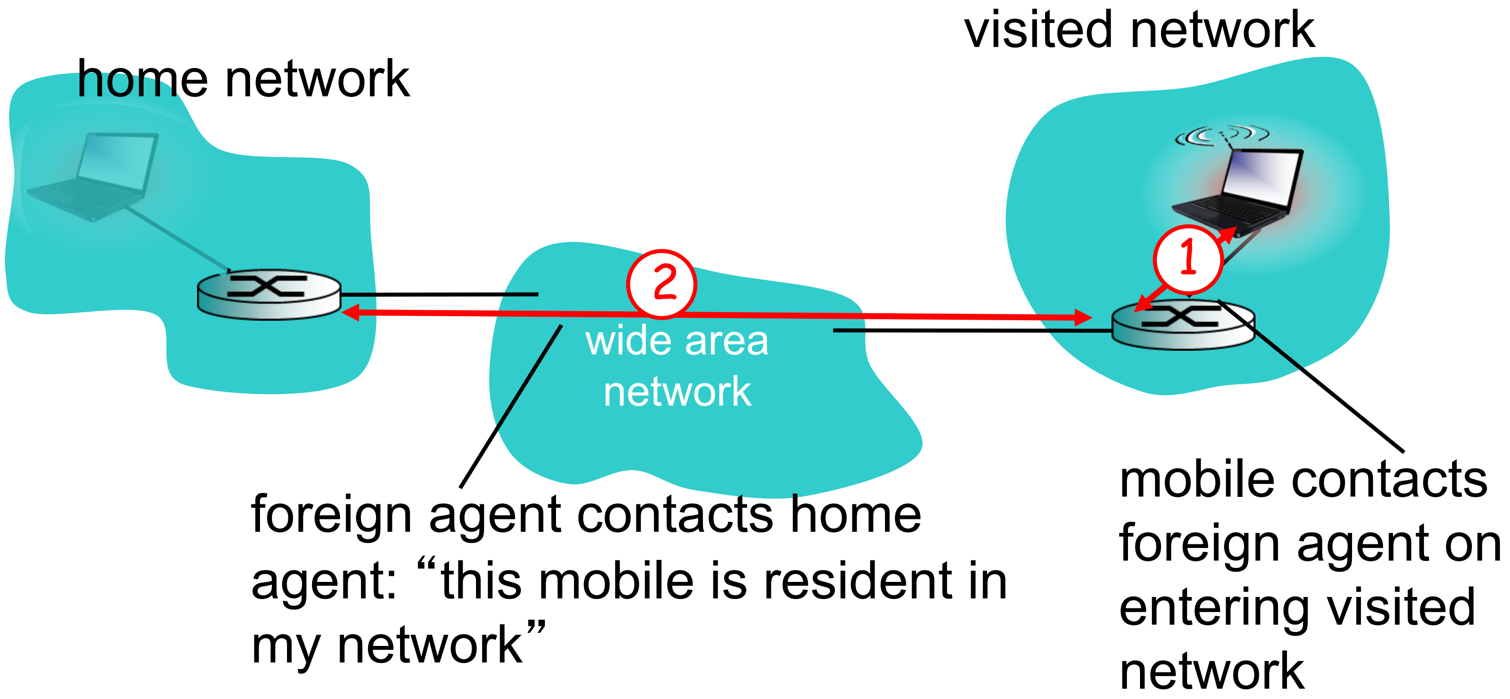
Mobility: two approaches

1. *let routing handle it:* routers advertise permanent ad mobile-nodes-in-residence vi ng table exchange.
   - routing tables here each mobile located
   - no changes to end-systems

not
scalable
to millions of
mobiles

2. *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



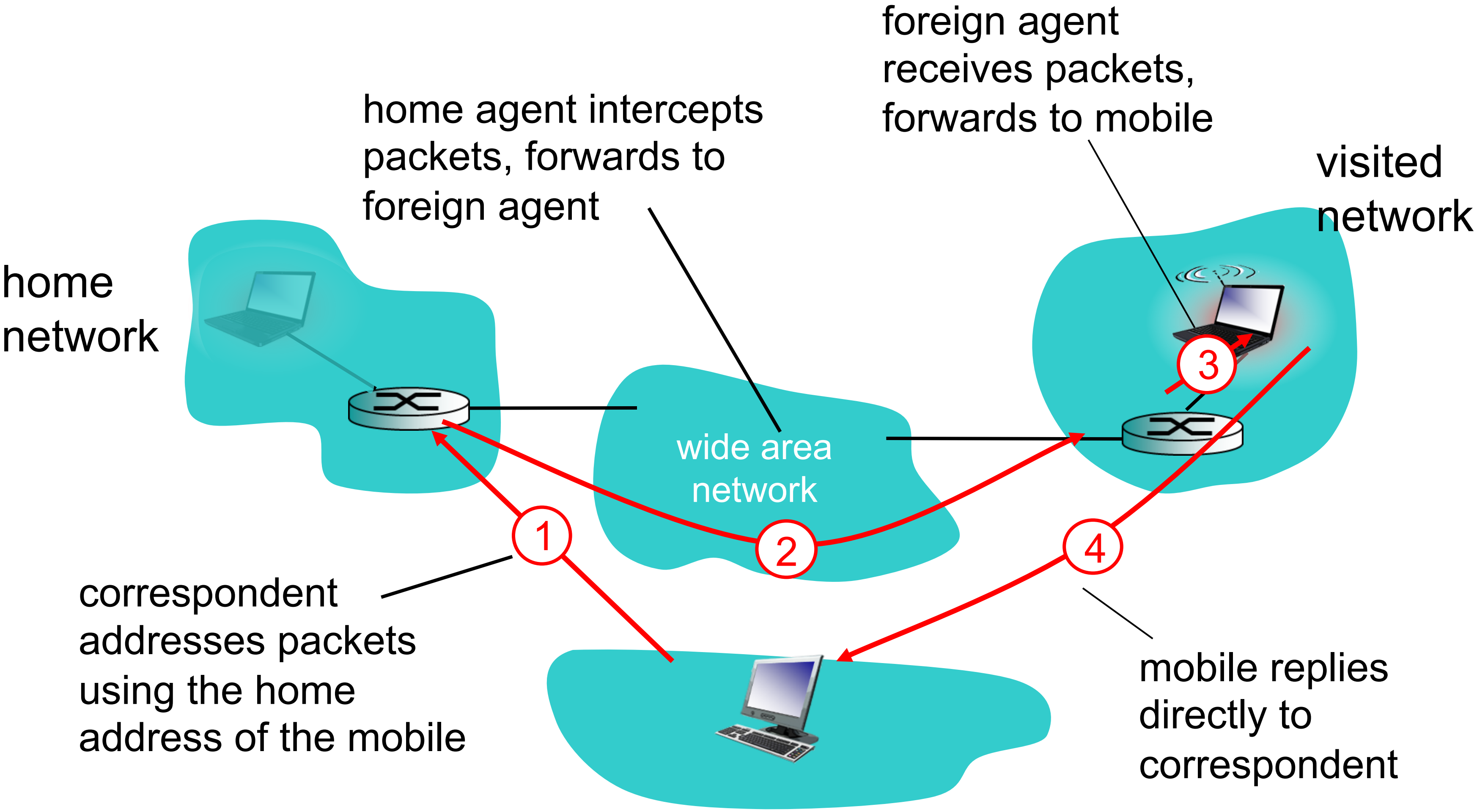
foreign agent contacts home agent: “this mobile is resident in my network”

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

correspondent addresses packets using the home address of the mobile

mobile replies directly to correspondent

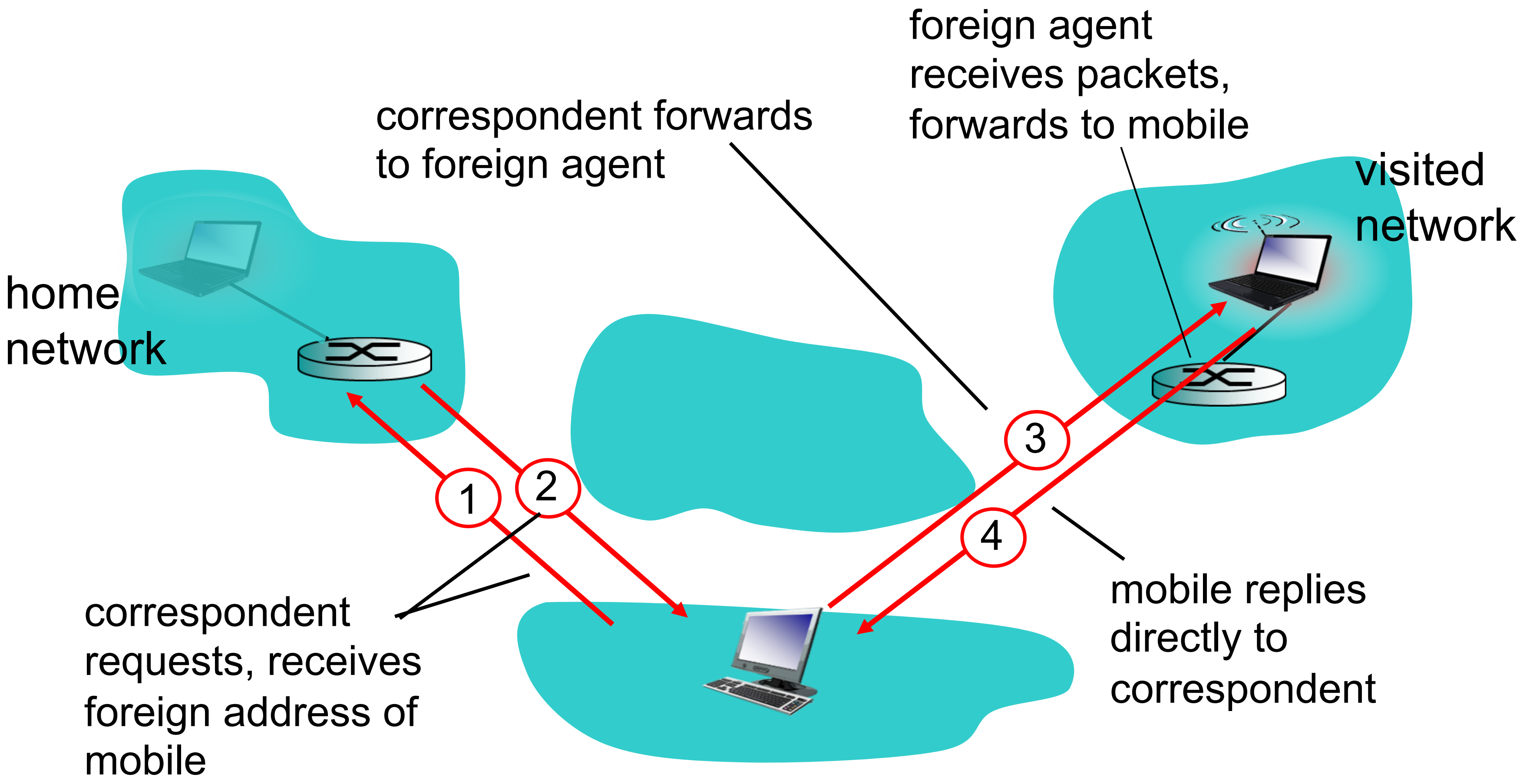
Indirect Routing: comments

- mobile device uses two addresses:
  - permanent address: correspondent connects to home address, doesn't need actual location
  - care-of-address: used by home agent to forward datagrams to mobile device
  - foreign agent functions may be done by the mobile itself
- causes triangle routing: packets flow from correspondent to home-network to mobile
  - inefficient when both are in the same network

Indirect routing: moving between networks

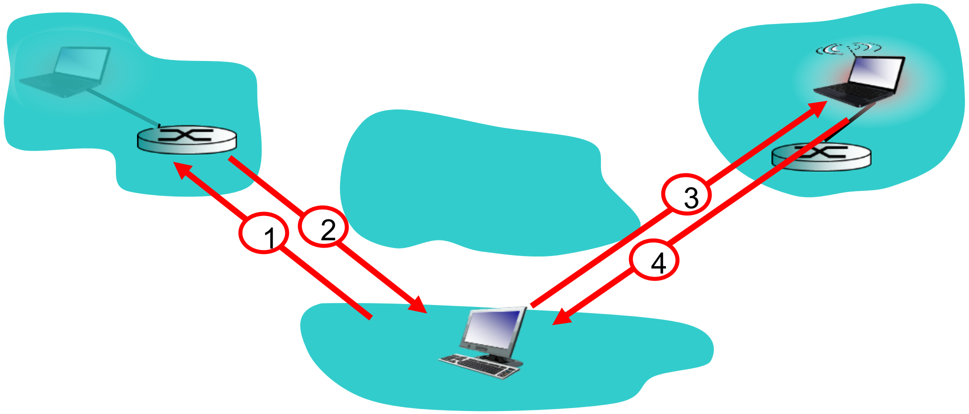
- suppose mobile user moves to another network
  - registers with new foreign agent and new foreign agent registers with home agent
  - home agent updates care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- transparent when changing foreign networks: *caller remains connected to home agent, home agent handles rerouting of packets to device*

Mobility via direct routing


foreign agent receives packets, forwards to mobile
correspondent forwards to foreign agent
visited network
home network
1
2
3
4
mobile replies directly to correspondent
correspondent requests, receives foreign address of mobile

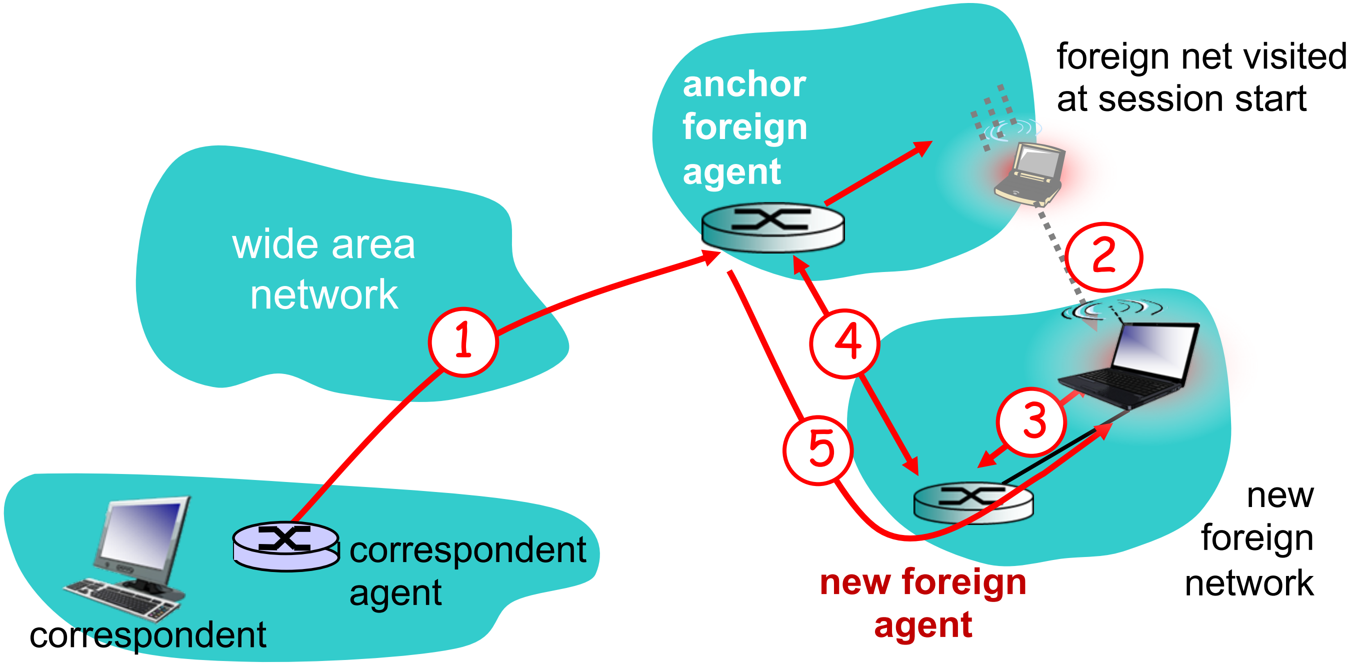
Mobility via direct routing: comments

- overcomes triangle routing problem
- *correspondent must reroute to new location:* each time device moves, correspondent must get a new care-of-address from home agent
  - what if mobile changes location again?



Accommodating mobility with direct routing

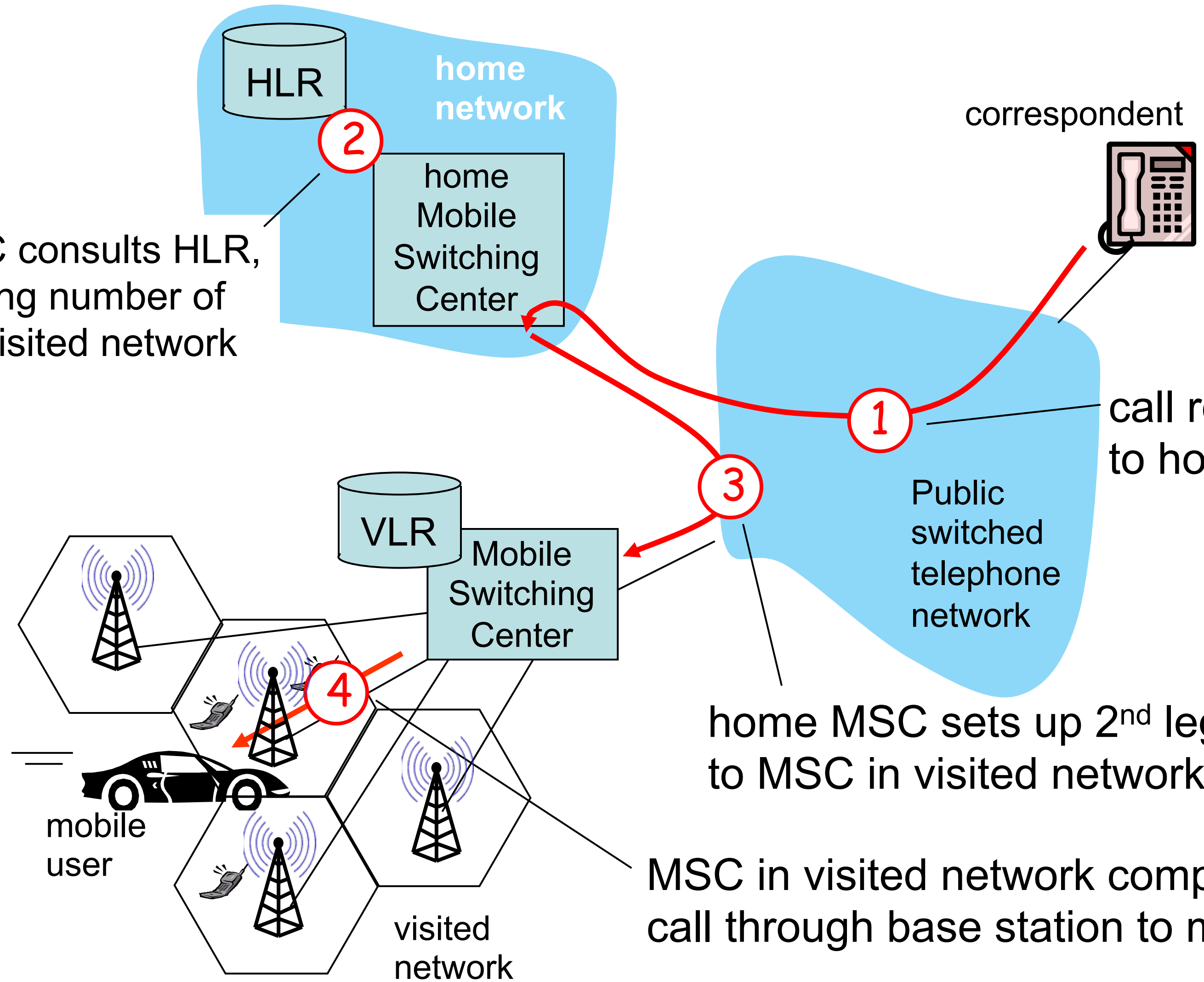
- Foreign agent (FA) is anchored in the first visited network
  - data always routed first to that anchor FA
  - when mobile moves: new FA arranges to have data forwarded from old FA (chaining the series of FA's)



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), and information about its current location
- *visited network:* network in which mobile currently resides
  - *visitor location register (VLR):* database with entry for each user currently in network
  - could be in its home network

Example: indirect routing in GSM



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

call routed to home network

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

MSC in visited network completes call through base station to mobile