Wireless and Cellular Networks

Tecnologie e Servizi di Rete

Computer Network Technologies and Services

Mario Baldi, Claudio Casetti, Guido Marchetto, Fulvio Valenza

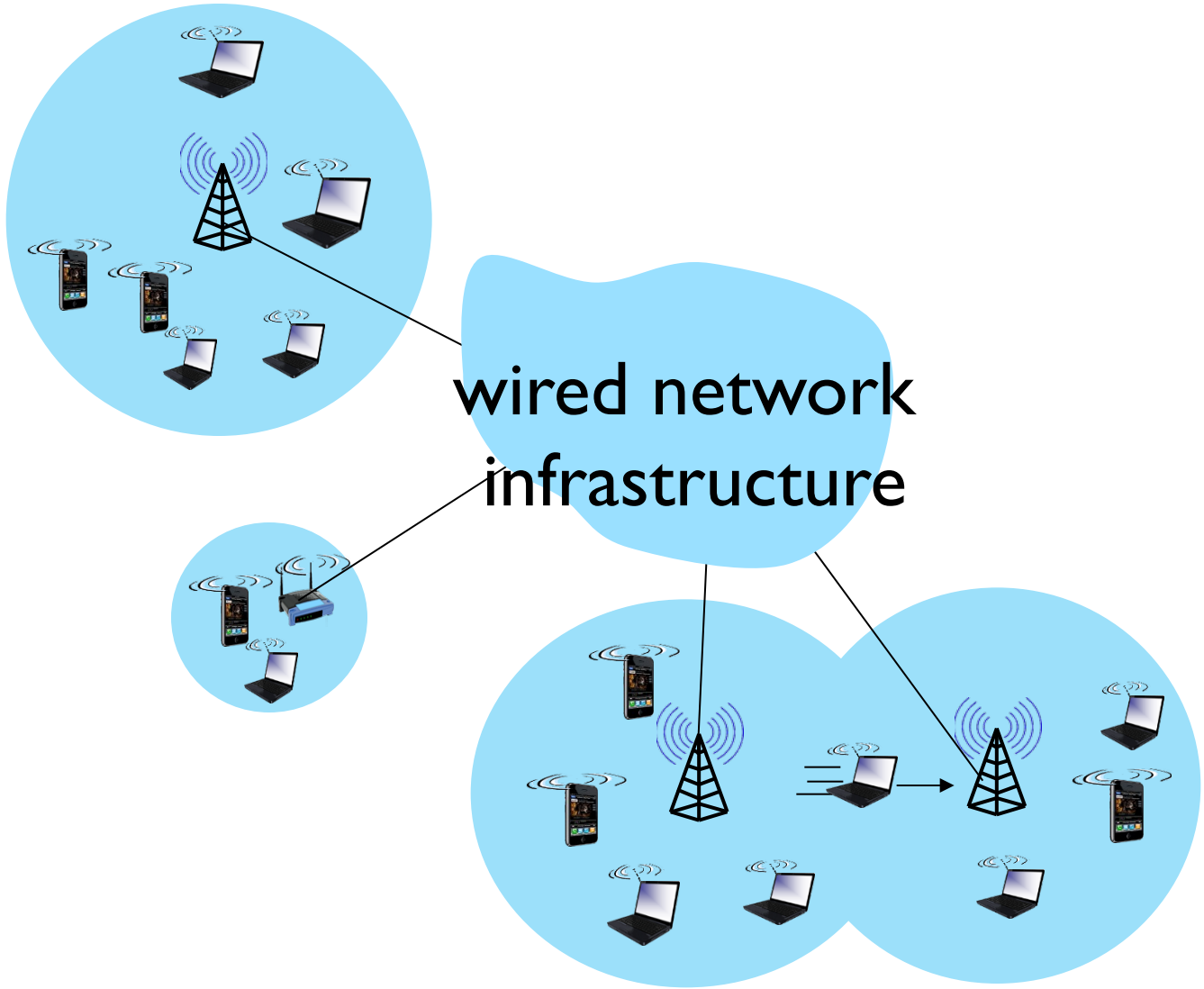
*part of the slides adapted from material by Carla Fabiana Chiasserini, Jim Kurose, Keith Ross

Copyright Notice

Wireless and Mobile Networks: context

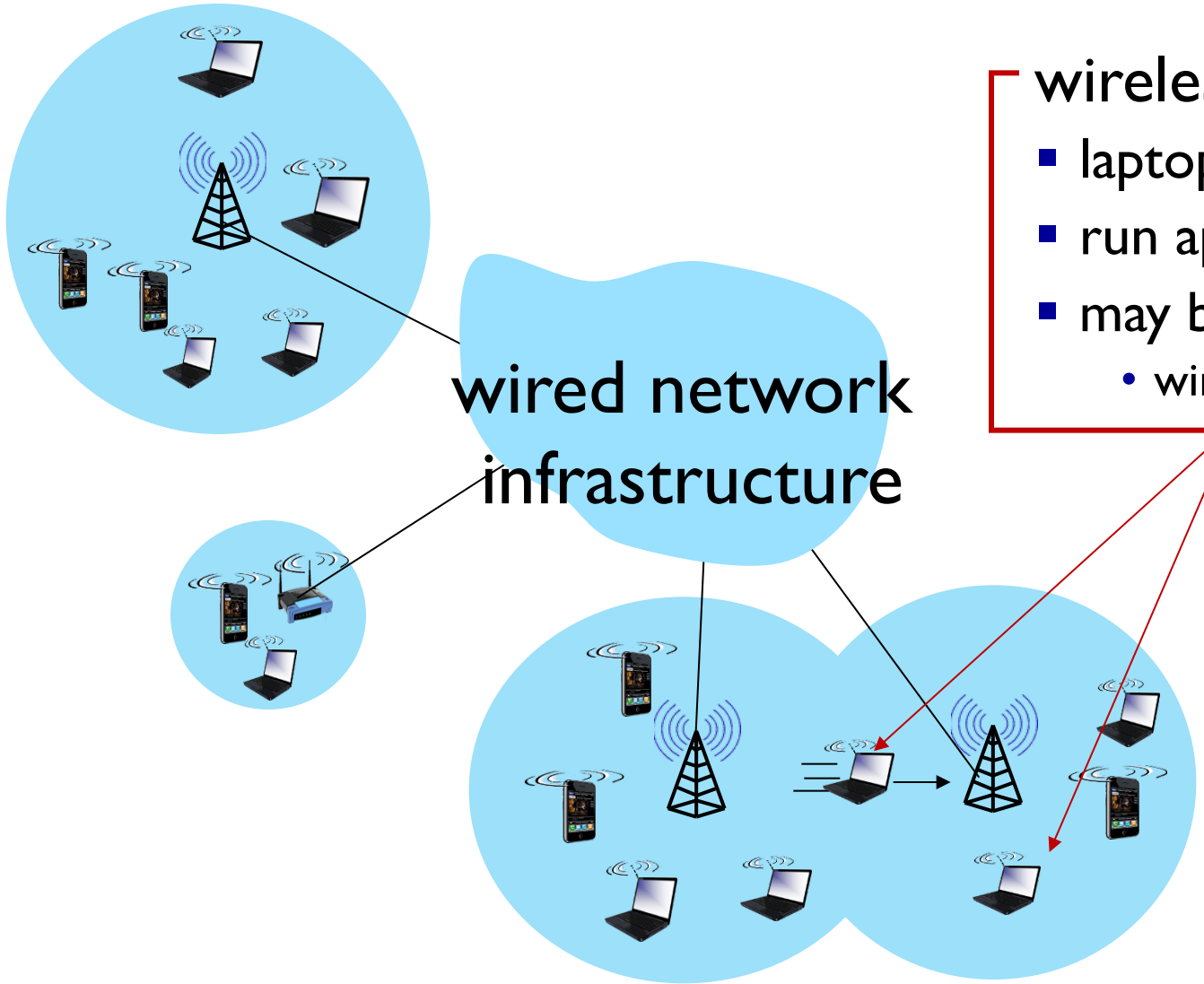
- more wireless (mobile) phone subscribers than fixed (wired) phone subscribers (10-to-1 in 2019)!
- more mobile-broadband-connected devices than fixed-broadband-connected devices devices (5-1 in 2019)!
  - 4G/5G cellular networks now embracing Internet protocol stack, including SDN
- two important (but different) challenges
  - wireless: communication over wireless link
  - mobility: handling the mobile user who changes point of attachment to network

Elements of a wireless network



ANTENNA DI FORNISCE RETE WIRELESS

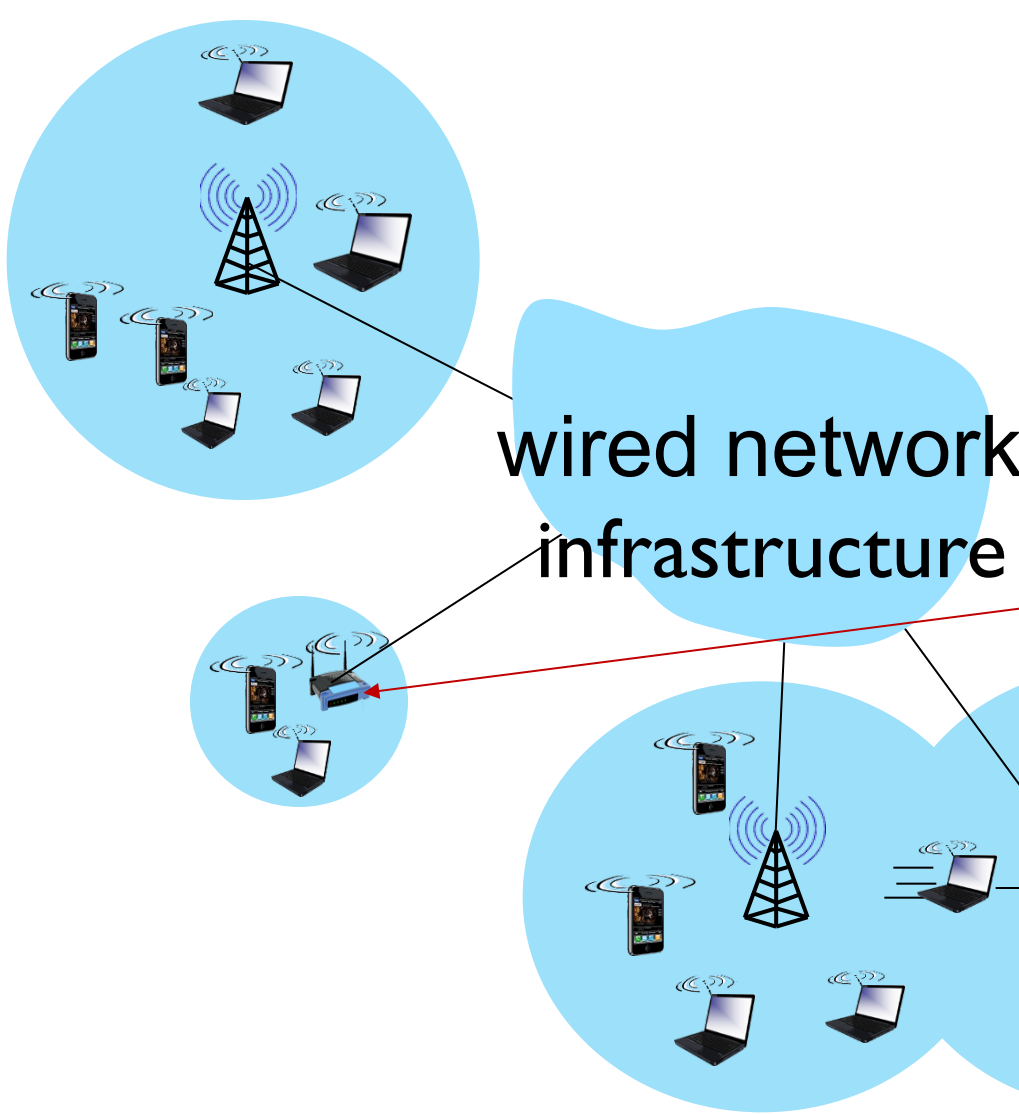
Elements of a wireless network



wireless hosts

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

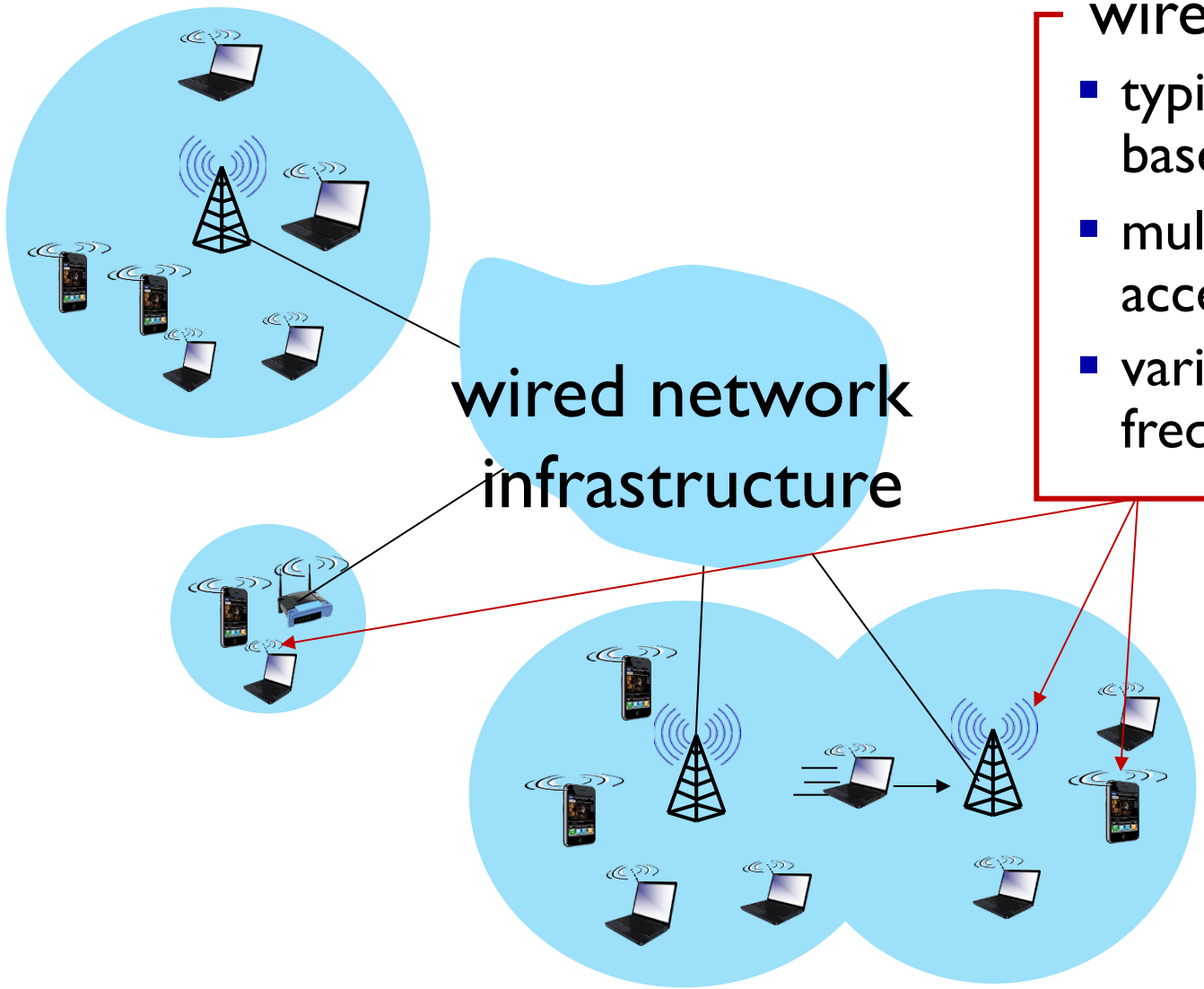
Elements of a wireless network



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

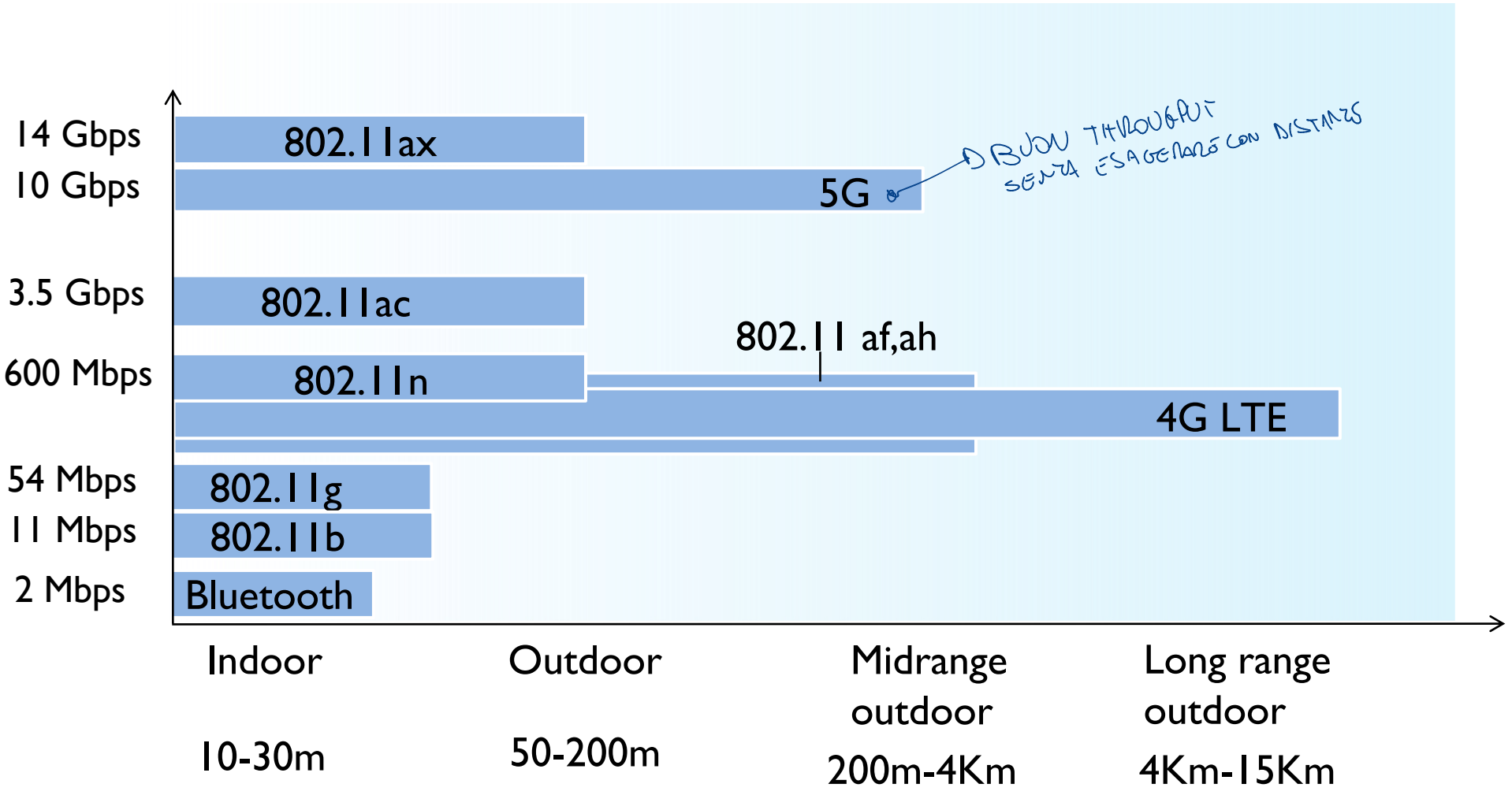
Elements of a wireless network



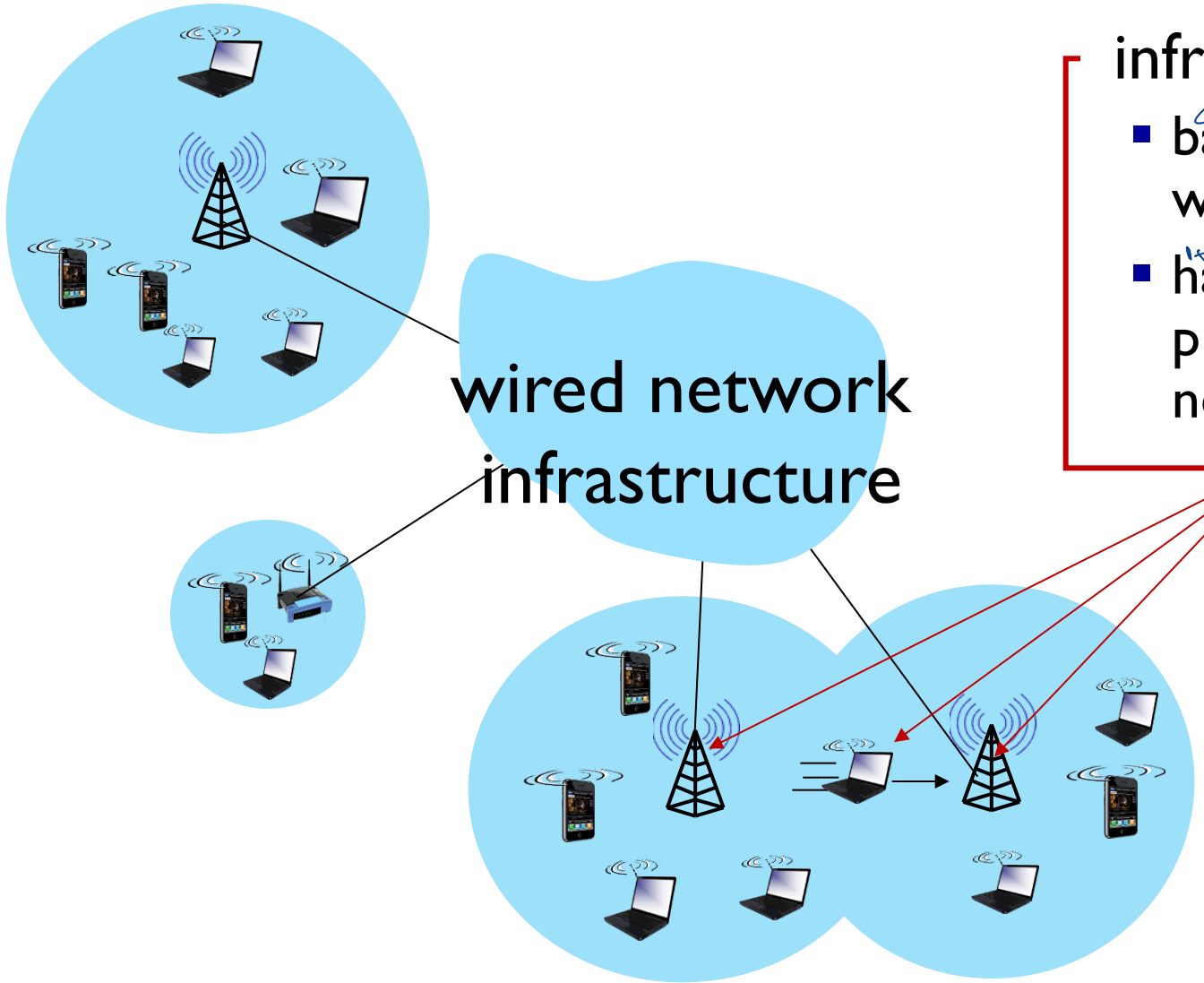
wireless link

- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

Characteristics of selected wireless links



Elements of a wireless network

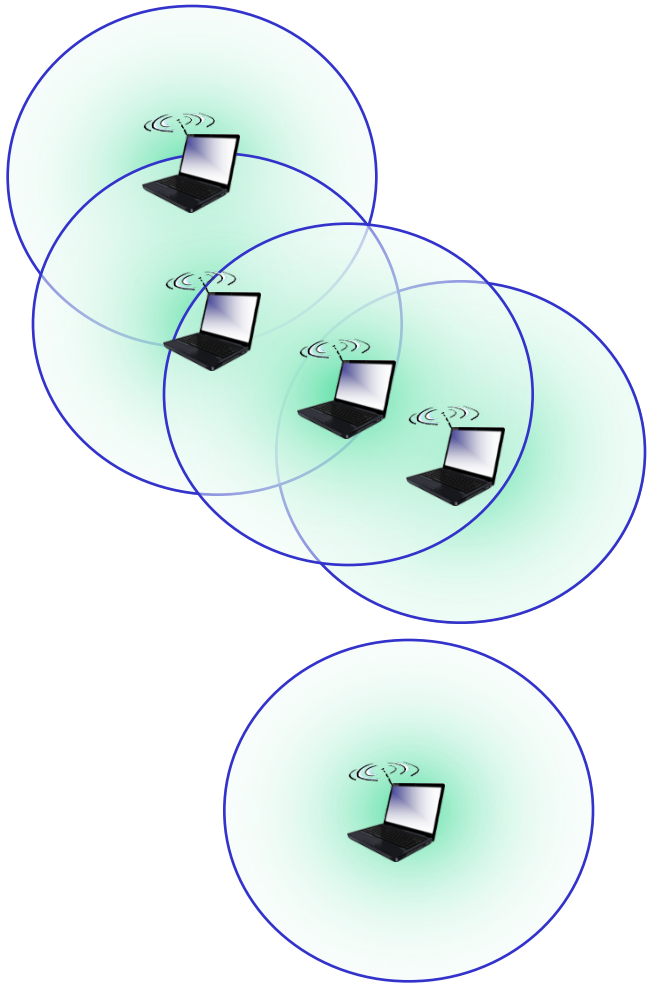


infrastructure mode

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

Elements of a wireless network

POCO USATA



ad hoc mode

SENZA INF RASTRUTTURE

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

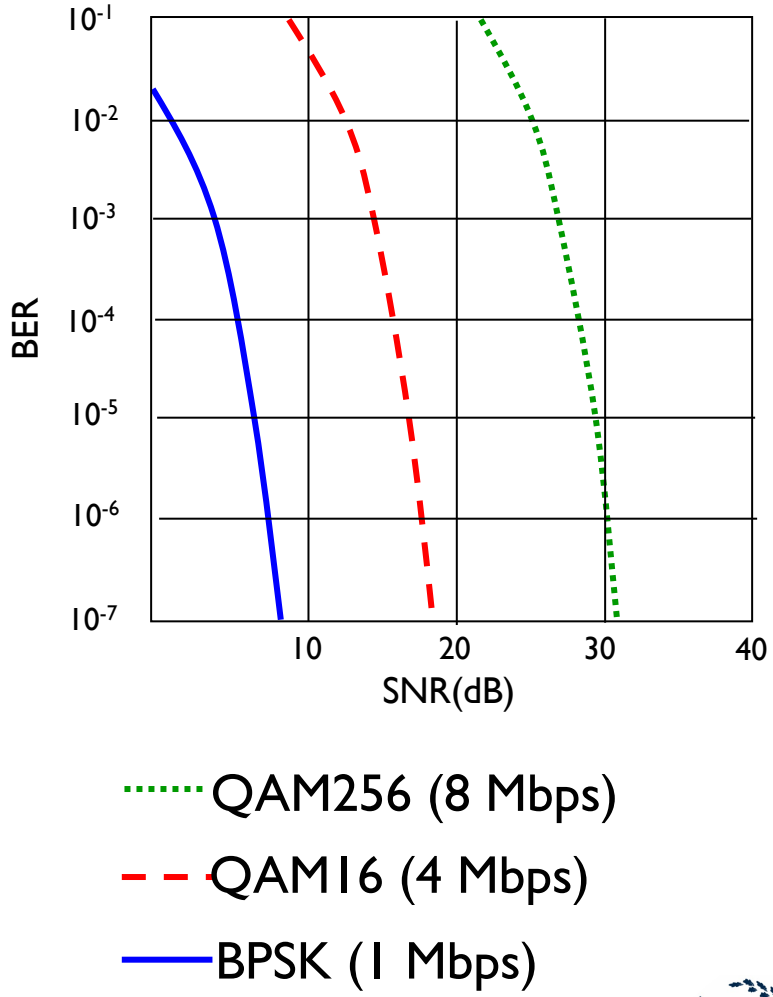
NODI SI SCAMBIANO I DATI DIRETTAMENTE TRA LORO AL LIV. 2

Wireless link characteristics (1)

- *important* differences from wired link ….
  - decreased signal strength: radio signal attenuates as it propagates through matter (path loss) DEGRADO SENSIBILE
  - interference from other sources: wireless network frequencies (e.g., 2.4 GHz) shared by many devices (e.g., WiFi, cellular, motors): interference
  - multipath propagation: radio signal reflects off objects ground, arriving at destination at slightly different times COPIE DI SEGNALI COMPLETAMENTE SFASATE TRA LORO → FADING
- …. make communication across (even a point to point) wireless link much more "difficult"

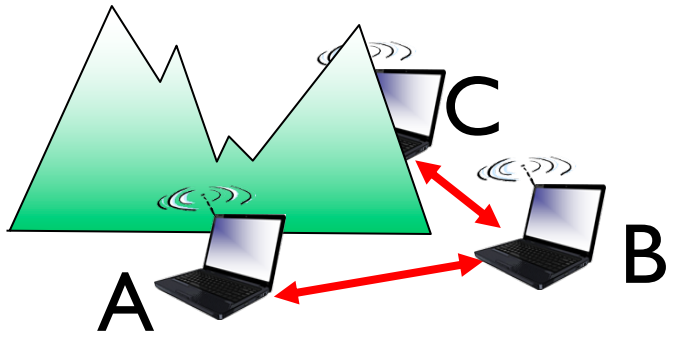
Wireless link characteristics (11)

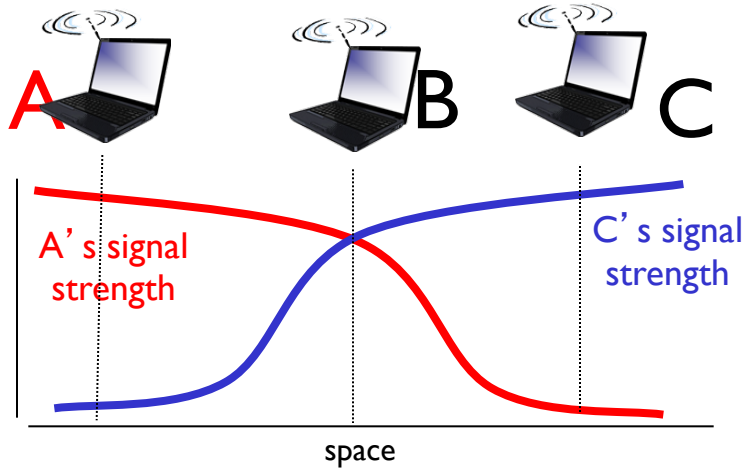
- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- SNR versus BER tradeoffs
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



Wireless link characteristics (III)

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





Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B

Signal attenuation:

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

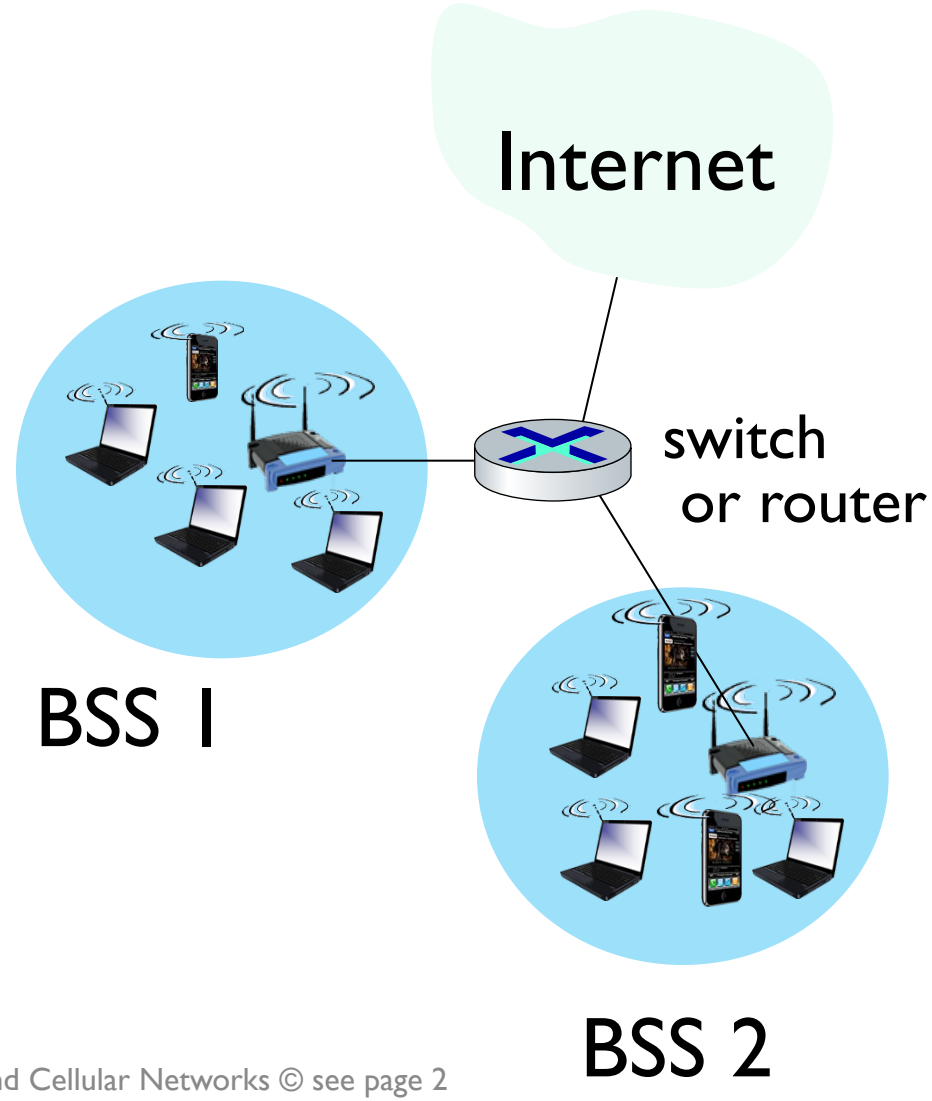
Wireless LANs

IEEE 802.11 Wireless LAN

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2021	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

- all use CSMA/CA for multiple access, and have base-station and ad-hoc network versions

802.11 LAN architecture



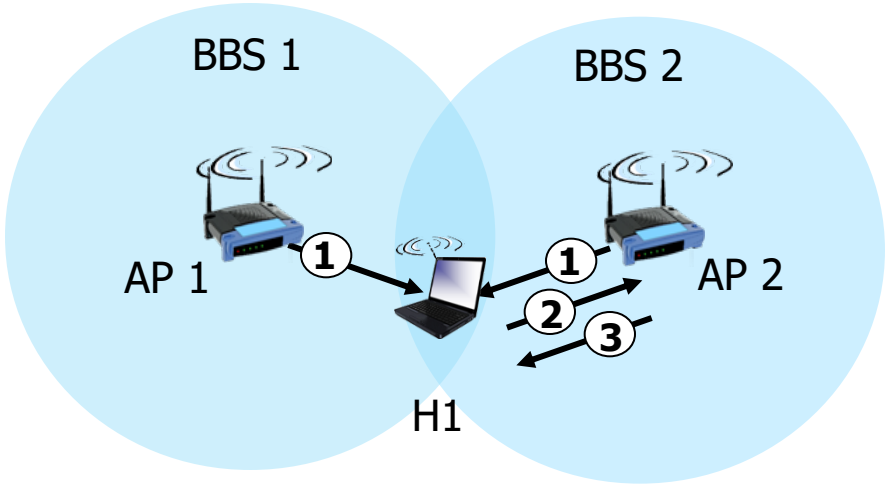
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

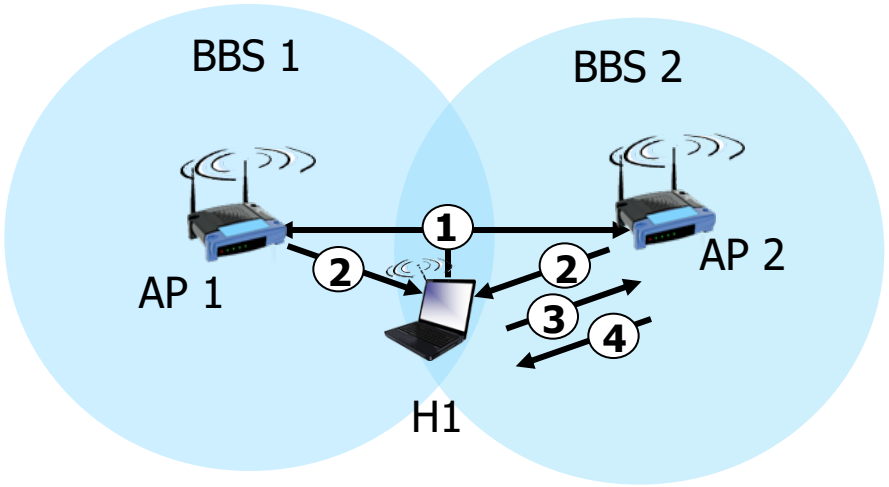
802.11: Channels, association

- spectrum divided into channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- arriving 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
  - then may perform authentication [Chapter 8]
  - then typically run DHCP to get IP address in AP's subnet

BSS

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

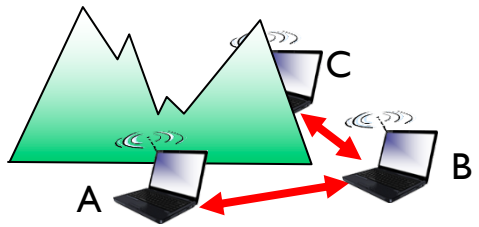
active scanning:

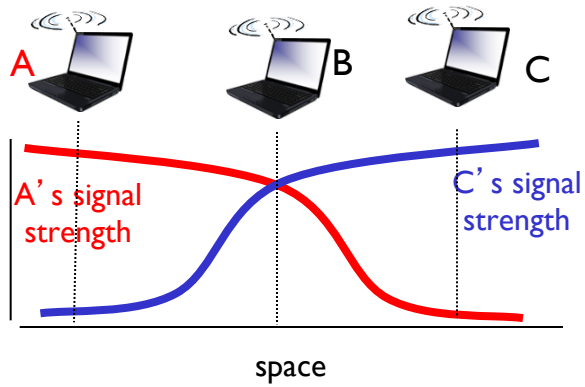
HOST FA RICHIESTA BROADCAST

(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 : SI CERCA DI ELIMINARE LE COLLISIONI
  - don't collide with detected ongoing transmission by another node
- 802.11: *no* collision detection!
  - difficult to sense collisions: high transmitting signal, weak received signal due to fading
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/CollisionAvoidance





IEEE 802.11 MAC Protocol: CSMA/CA

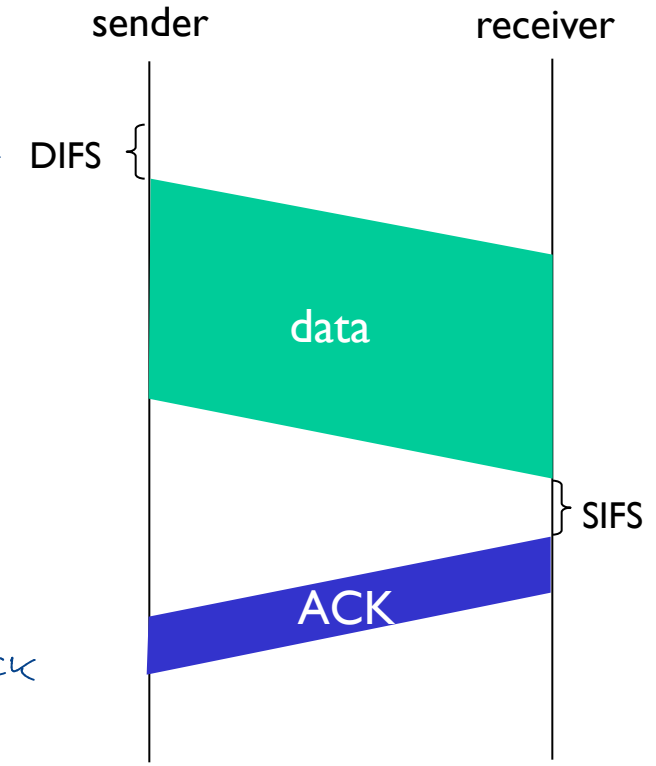
802.11 sender

1 if sense channel idle for **DIFS** then
    transmit entire frame (no CD)

2 if sense channel busy then
    start random backoff time
    timer counts down while channel idle
    transmit when timer expires
    if no ACK, increase random backoff interval, repeat 2

802.11 receiver

if frame received OK
    return ACK after **SIFS** (ACK needed due to hidden terminal problem)



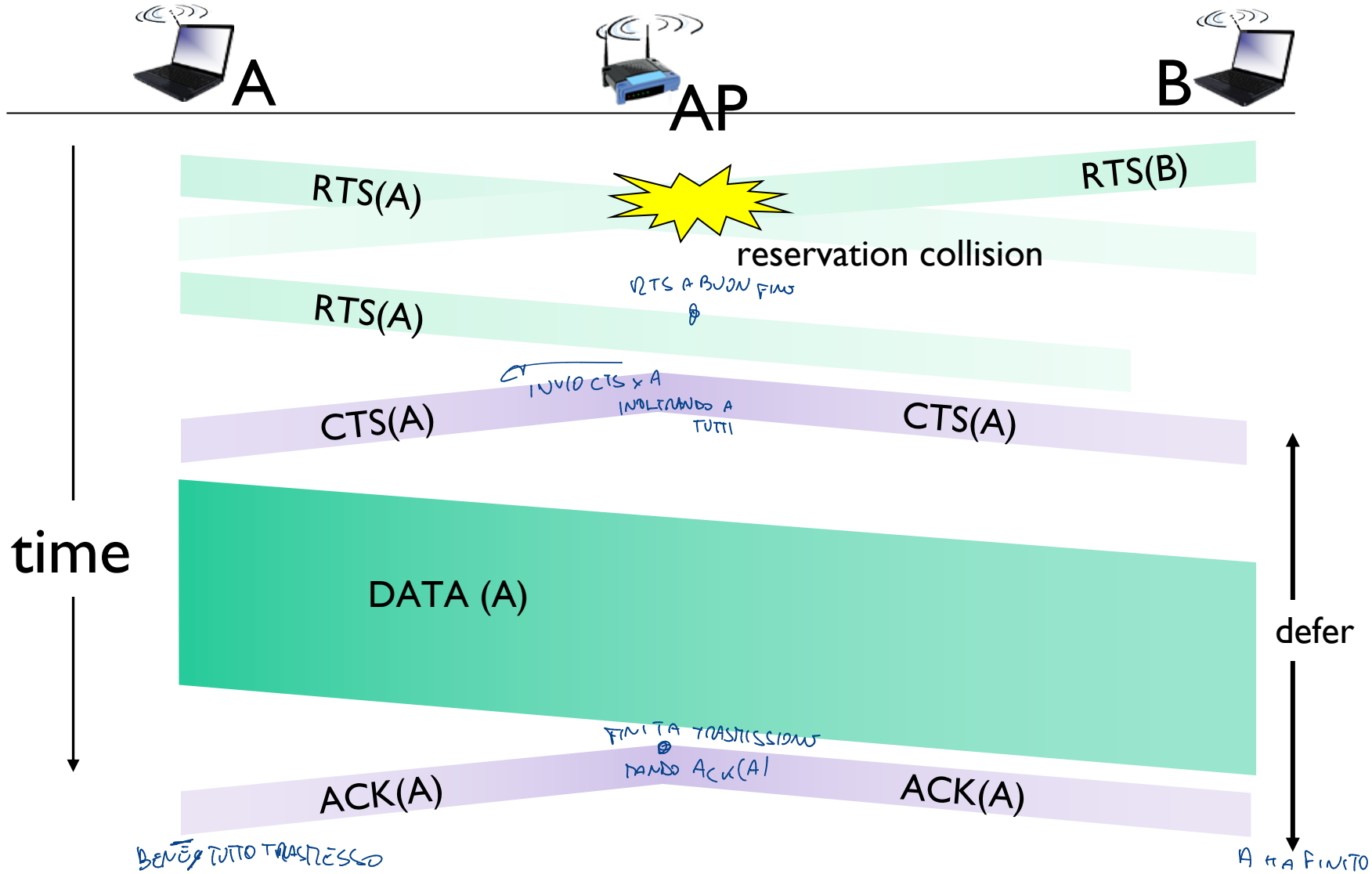
Avoiding collisions (more)

RICHIEDO L'USO DEL CANALE PRIMA DI MANDARE LA TRAMA

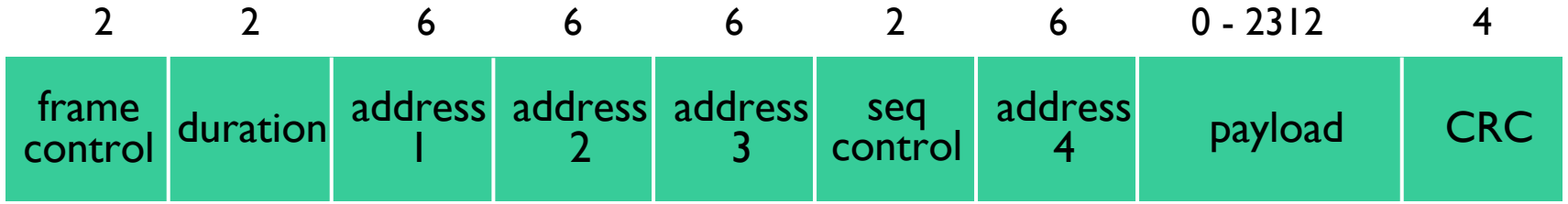
idea: sender "reserves" channel use for data frames using small reservation packets

- sender first transmits *small* request-to-send (RTS) packet 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

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing



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

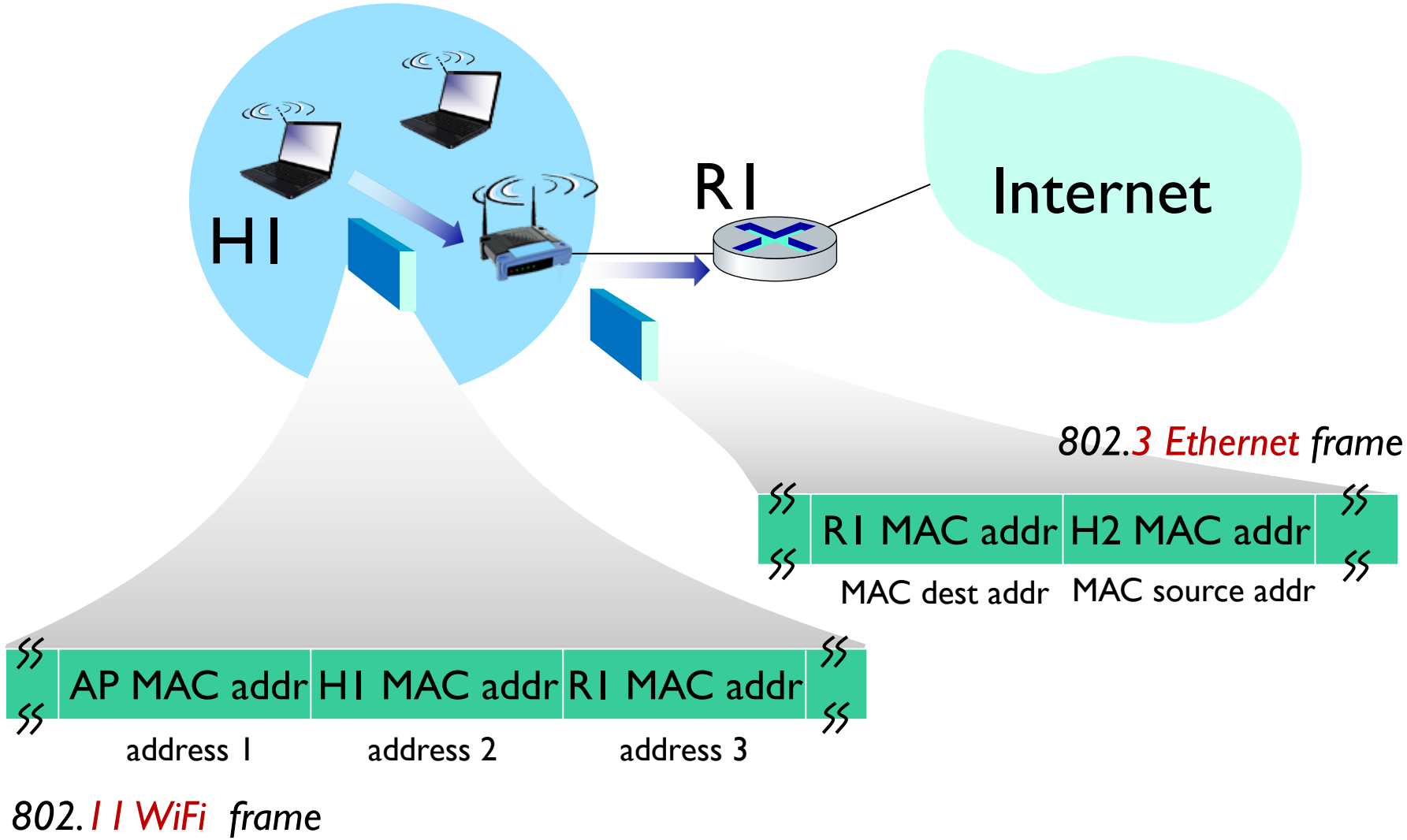
Address 2: MAC address of wireless host or AP transmitting this frame

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

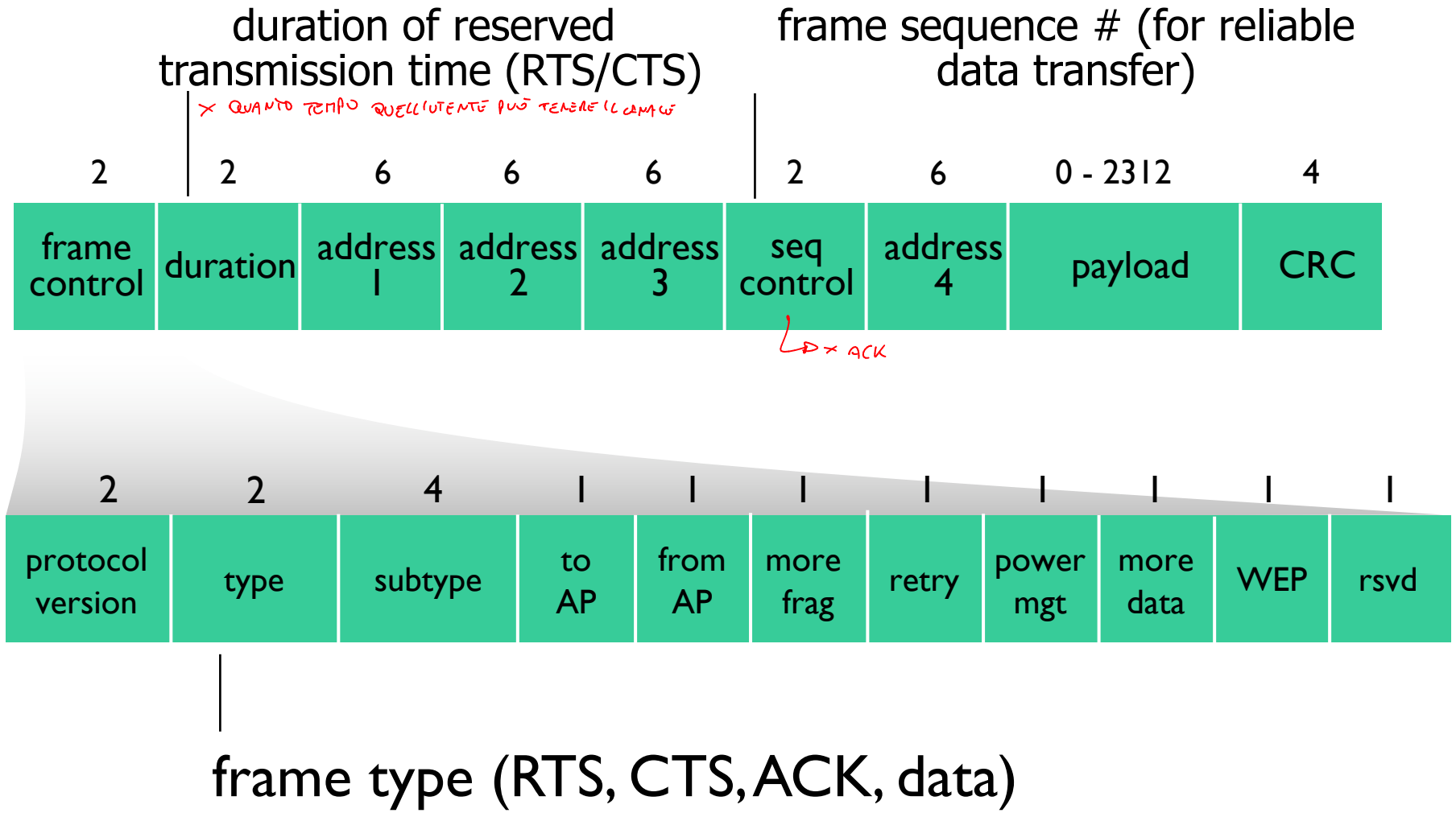
INDIRIZZO DEL ROUTER DEFAULT GATEWAY

Address 4: used only in ad hoc mode

802.11 frame: addressing



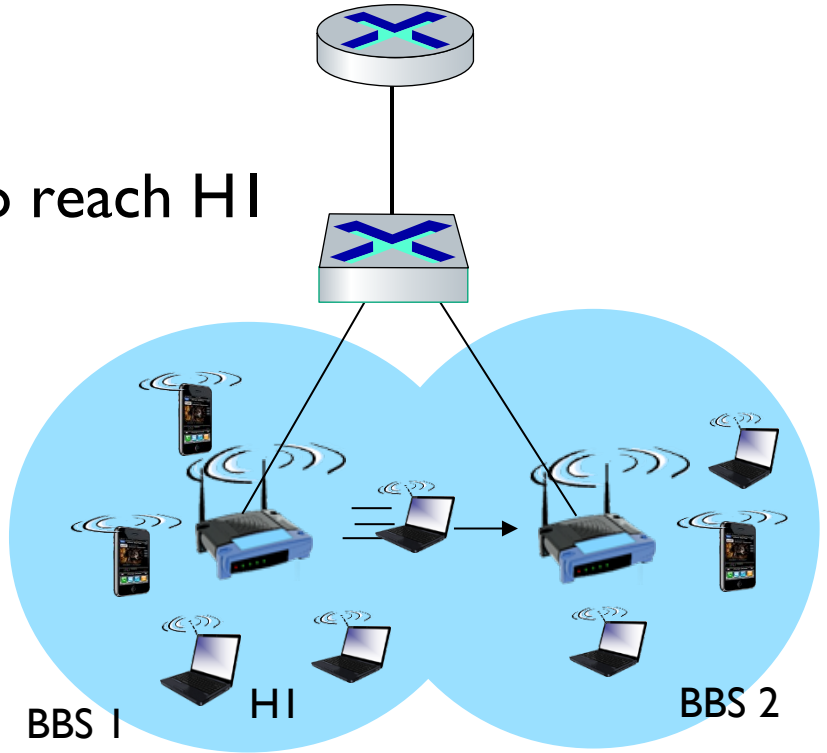
802.11 frame: addressing



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

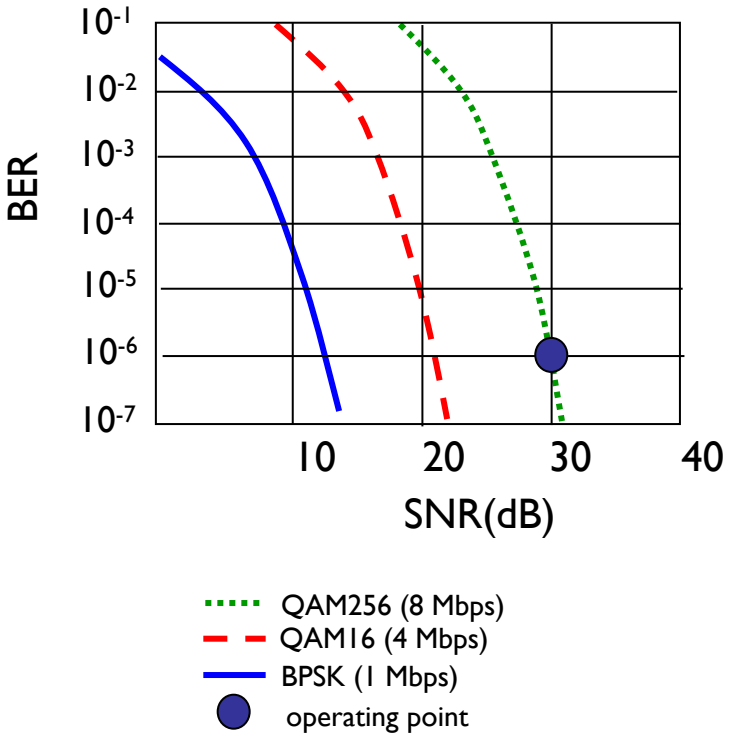
HO PIÙ SWITCH → gestiscono LE mobilità FACENDO in modo che
LO switch sappia che il nodo è raggiungibile da
una determinata porta. → SWITCH AGGIORNA LE PROPRIE TABELLE



802.11: advanced capabilities

Rate adaptation → SAPER CAMBIARE LA MODULAZIONE IN BASE ALLO STATO DEL CANALE

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, 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

→ nodi in grado di entrare in uno stato di "SLEEP"

- 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

QUANDO UN NODO RICEVE UN BEACON FRAME, SE NON HANNO NULLA DA TRASMETTERE VANNO IN SLEEP MODE FINO AL SEGUENTE BEACON FRAME.
→ AVVISA AP (Access Point) CHE È IN SLEEP

AccessPoint sa quali nodi sono in Sleep quindi non invia traffico ai nodi in Sleep. Quando arriva BeaconFrame → invia traffico in sospeso

Cellular Networks

Definitions

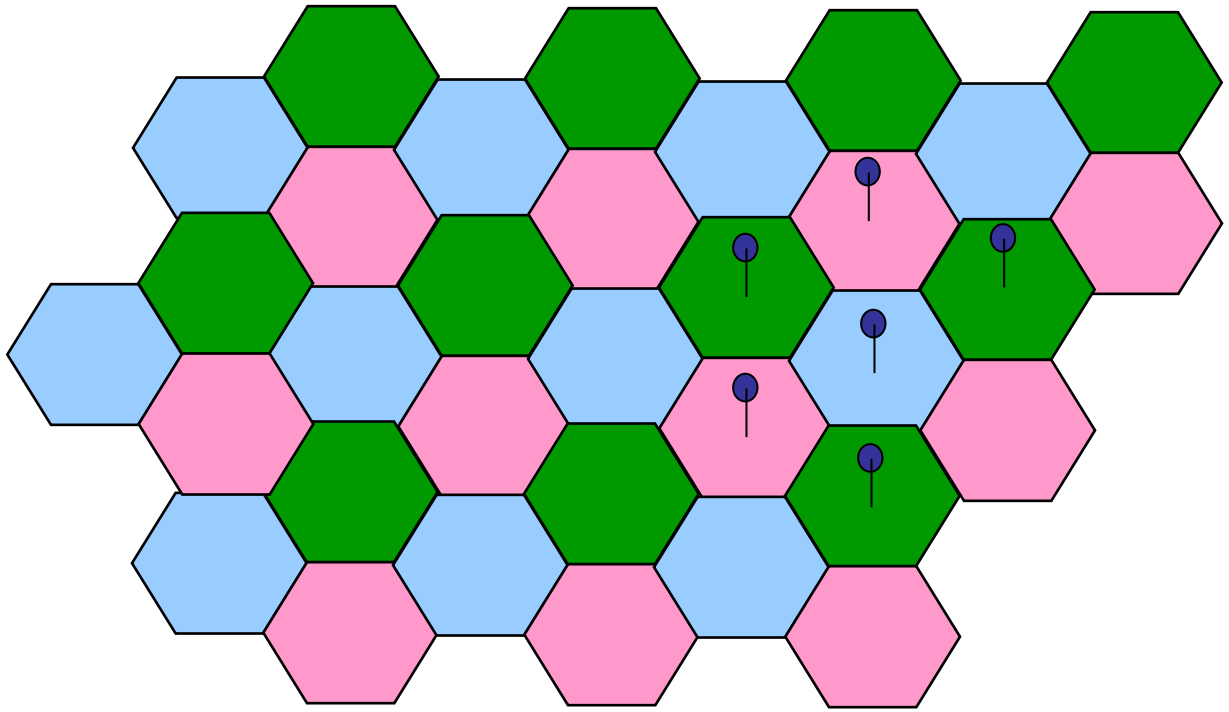
- Cellular network
  - Network where a geographical area is covered by tassellation through adjacent or overlapping areas, called *cells*
  - User terminals can move form one cell to another without communication disruption (*handover*)

Rete cellulare

Rete in cui un'area geografica è coperta da una tassellatura attraverso aree adiacenti o sovrapposte, chiamate celle.

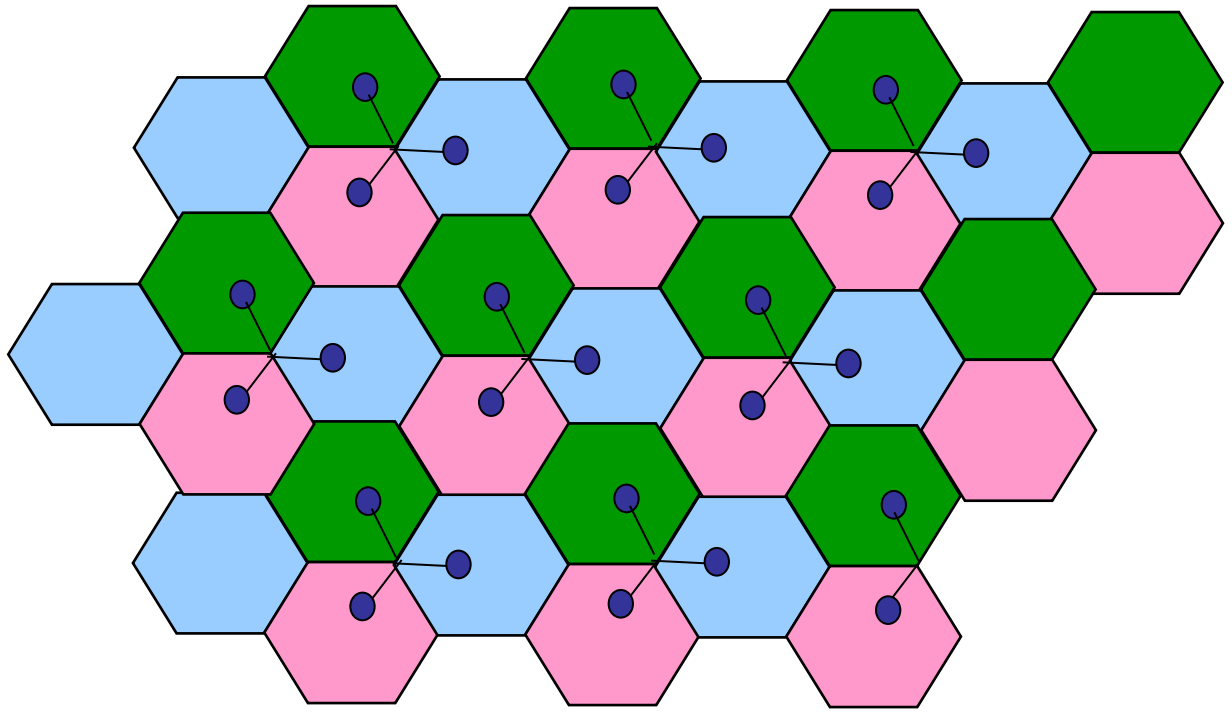
I terminali degli utenti possono spostarsi da una cella all'altra senza interruzioni nella comunicazione (handover).

Cellular coverage – In theory…



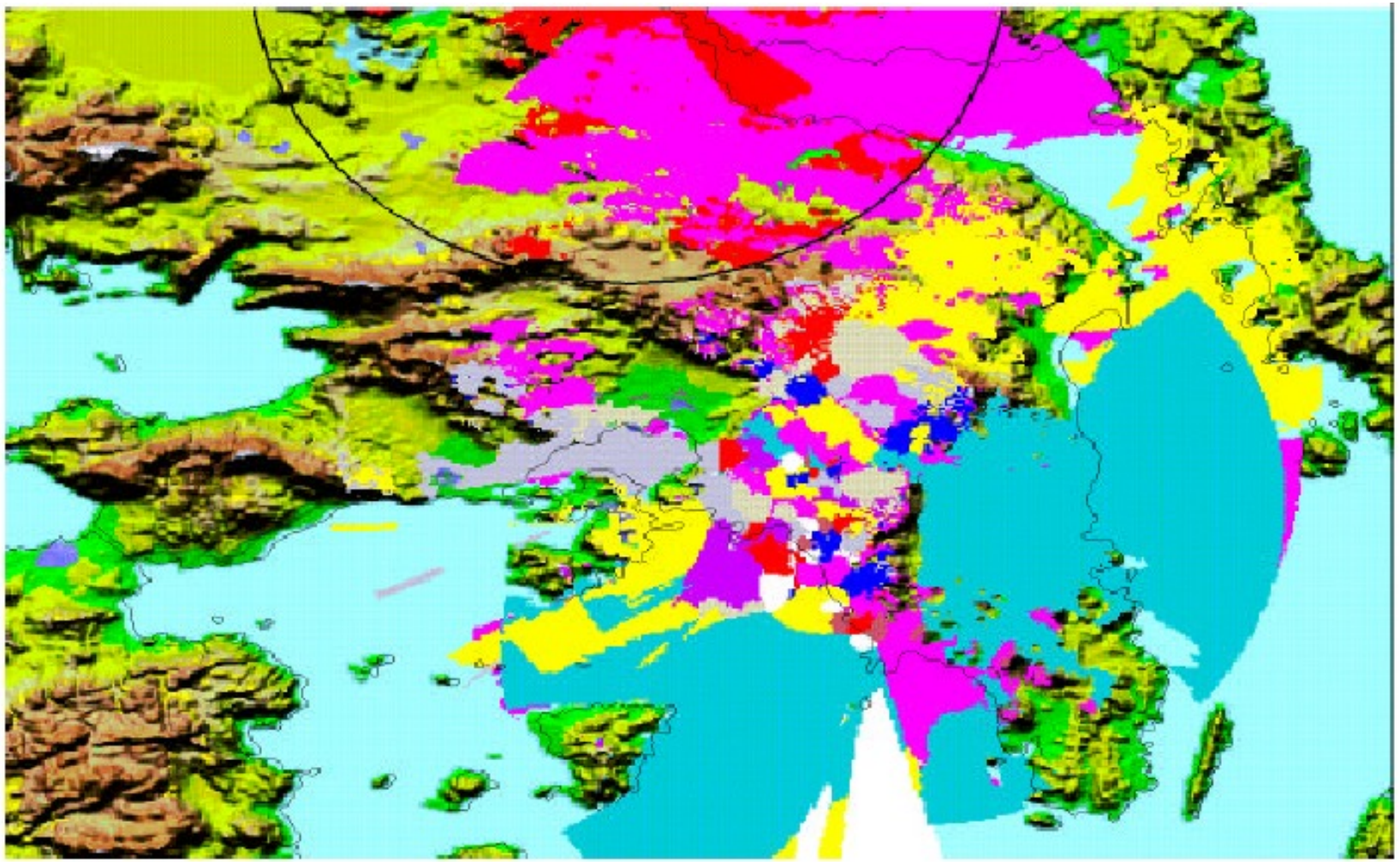
- Base station at the center of the cell, equipped with isotropic antenna
- Cells: regular exagonal shape

Cellular coverage – In theory…



- 3 directional antennas with a 120° opening, located at one extreme of each cell
- 3 co-located antennas

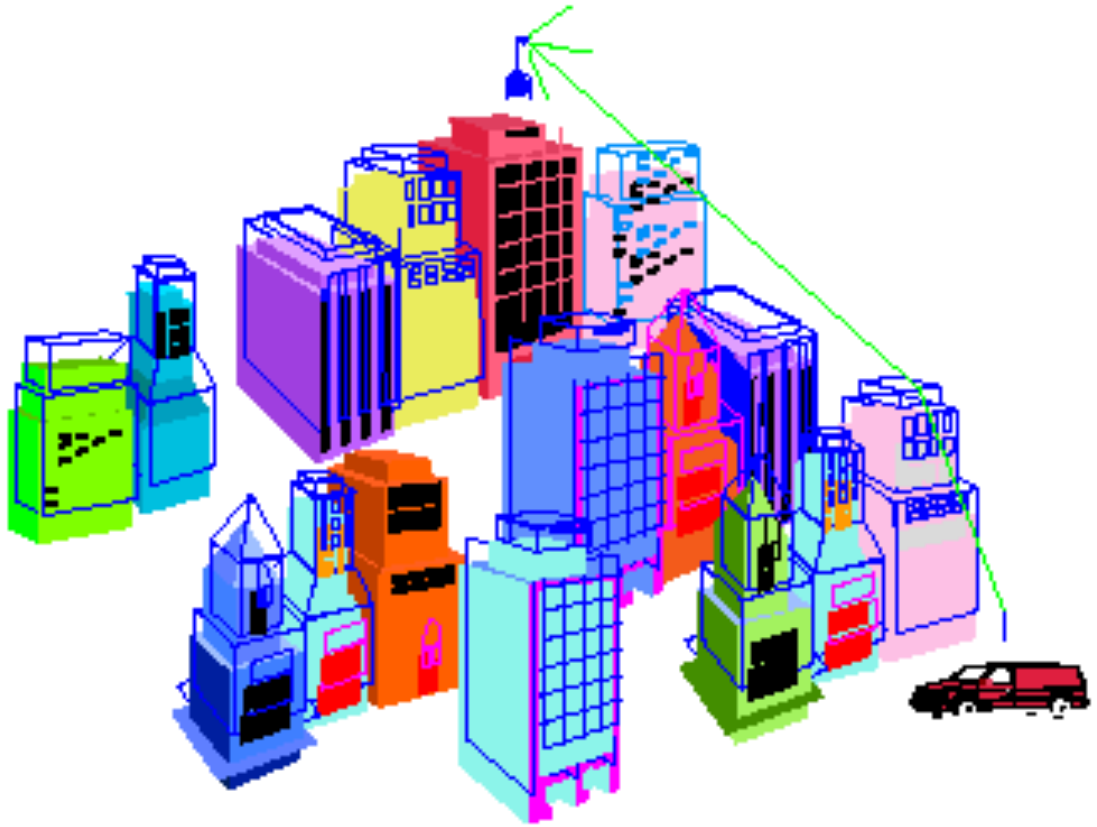
Cellular coverage – In practice… (Ce cells non sont propres et exagérés)



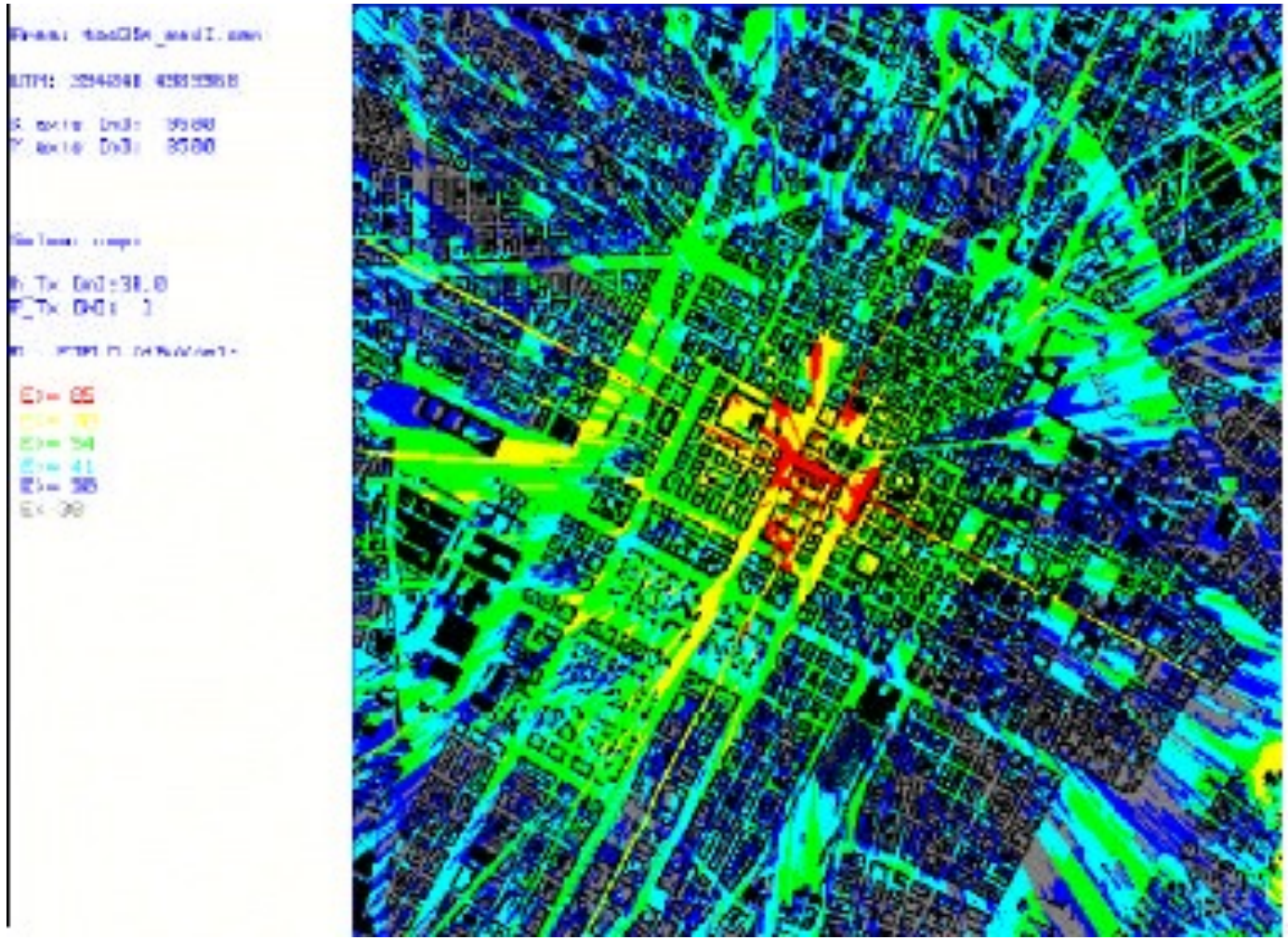
Cells

- Cells are not regular exagons and do not have same size
- Cell shape and size are determined by:
  - Power emitted at the antenna • POTENZA EMISSIVA
  - Antenna height
  - Antenna gain : capacità che un'antenna ha di trasmettere in una determinata direzione
  - Morphology of the geographical area (in urban areas: buildings height and shape)
    - Fading (multiple copies of the signal)
  - Propagation conditions
- Macrocells vs microcells
  - Different size, depending on the specific needs

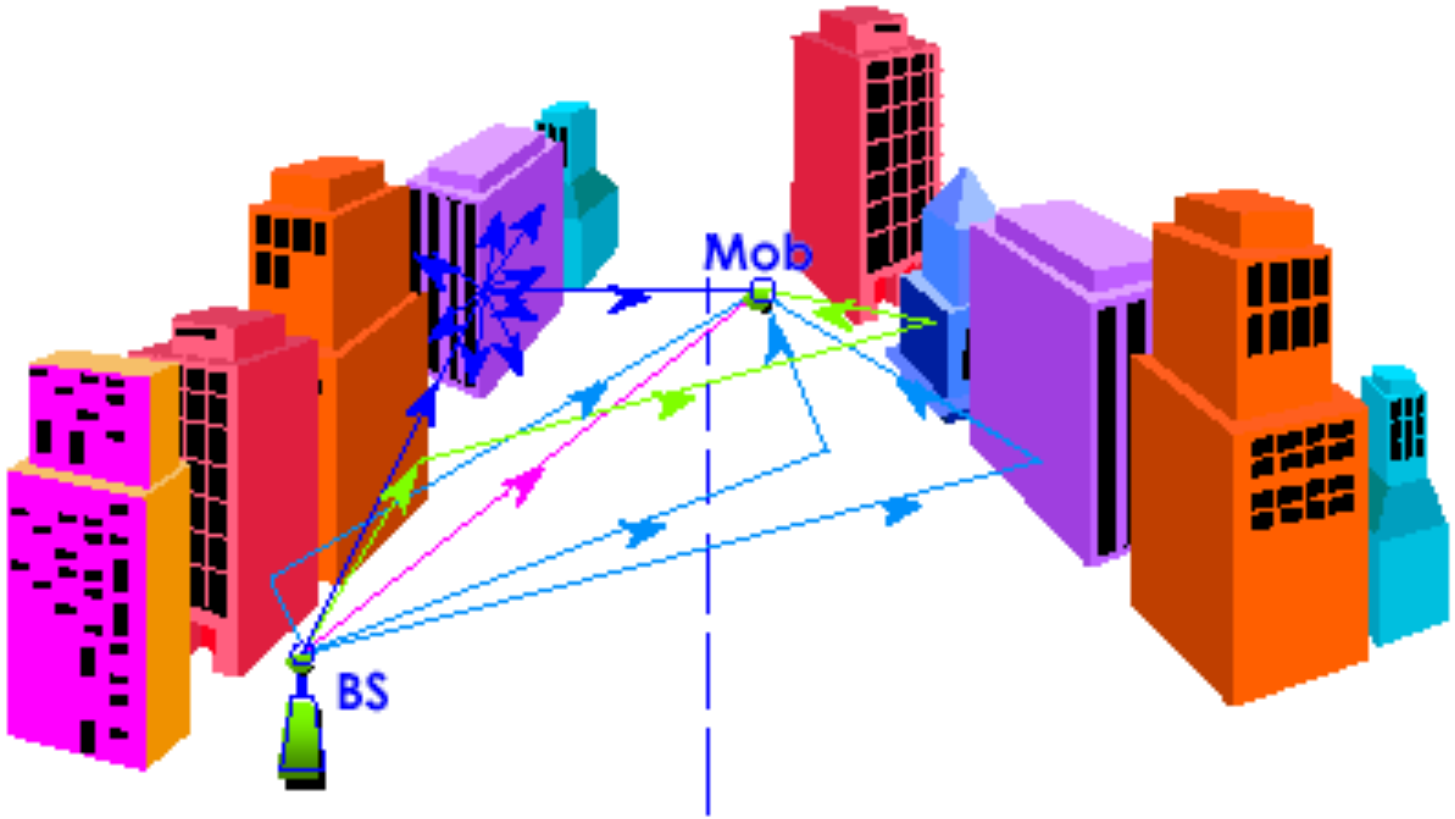
Example: macrocell



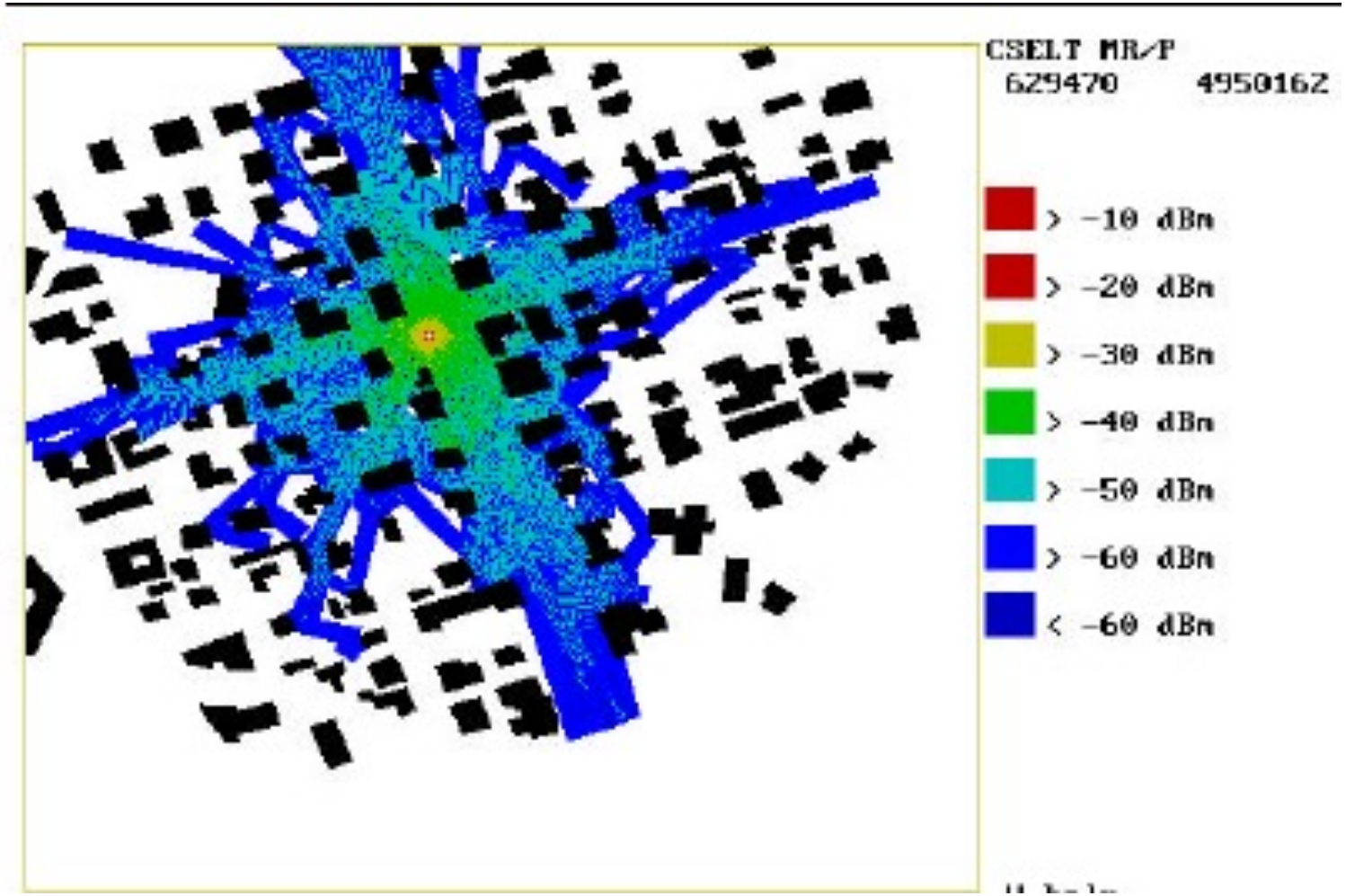
Macrocell: received power levels



Example: microcell

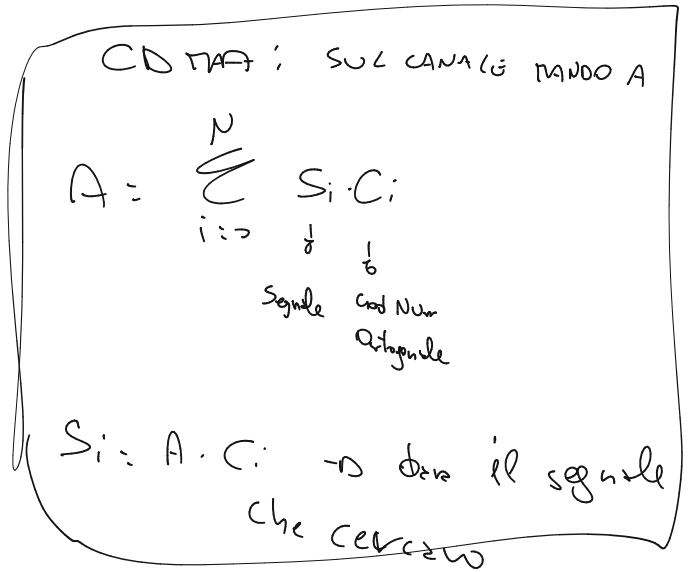


Microcell: received power levels



Channel access

- *Multiple user channel access*: wireless channel is a common resource that has to be shared among multiple users
- Possible techniques to share resources:
  - FDMA (Frequency Division Multiple Access)
  - TDMA (Time Division Multiple Access)
  - CDMA (Code Division Multiple Access)
  - SDMA (Space Division Multiple Access)



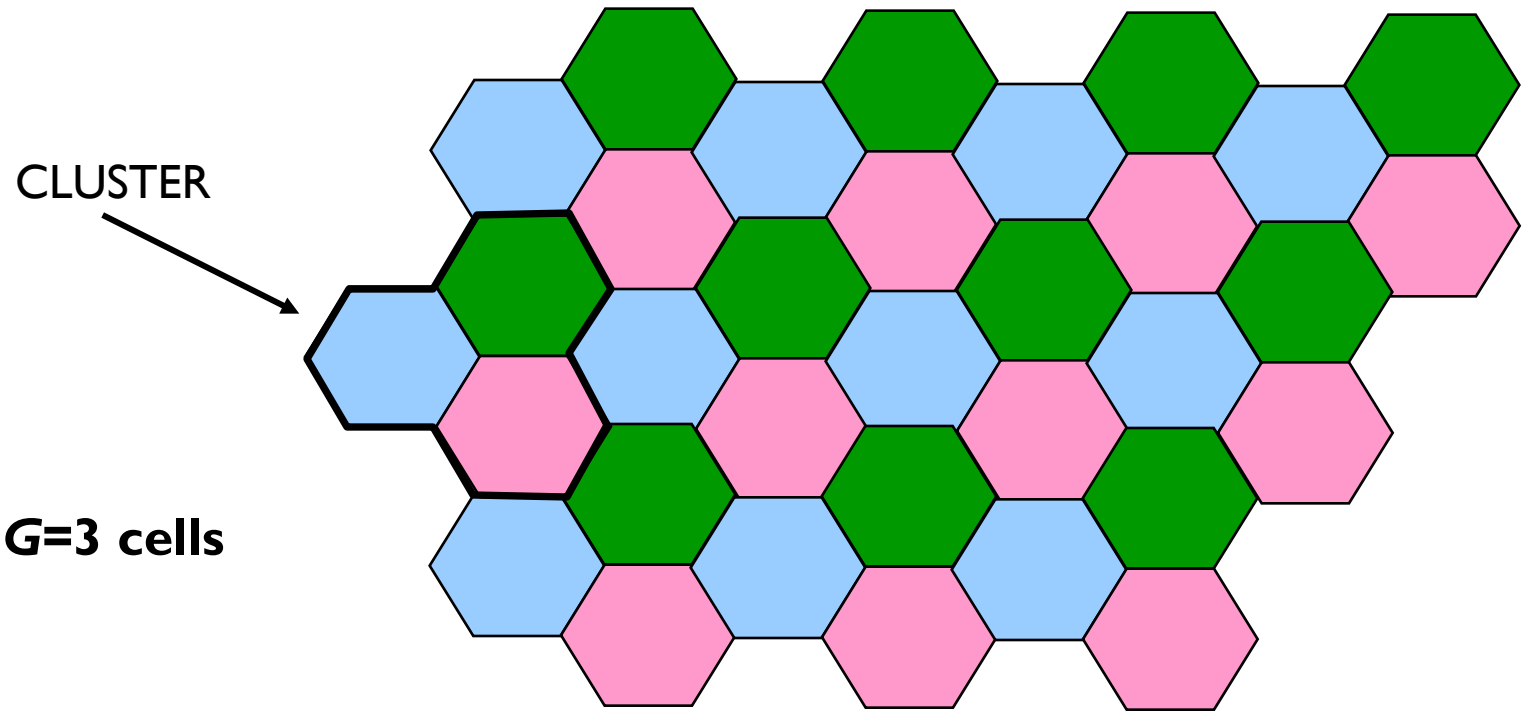
FDMA with frequency reuse

- Given the limited number of available resources, we need to:
  - Ensure coverage
  - Serve a high number of users

Reuse the same frequencies at different locations

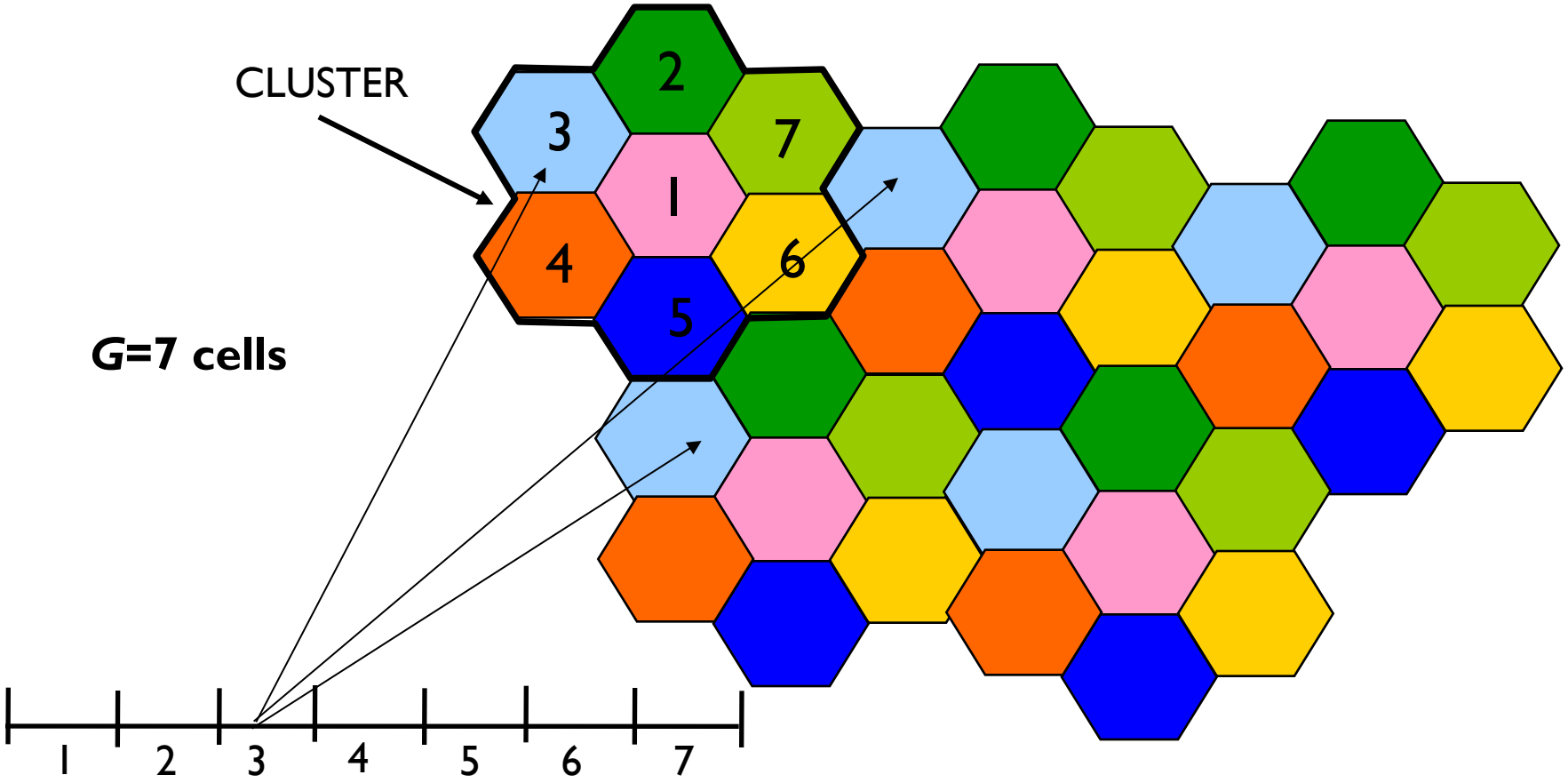
- We define as cluster the set of *G* adjacent cells that use all the frequencies available to one (dove non posso violtilizzare le frequenze)

3-Cell cluster (dove ho colori uguali, posso riutilizzare frequenze)

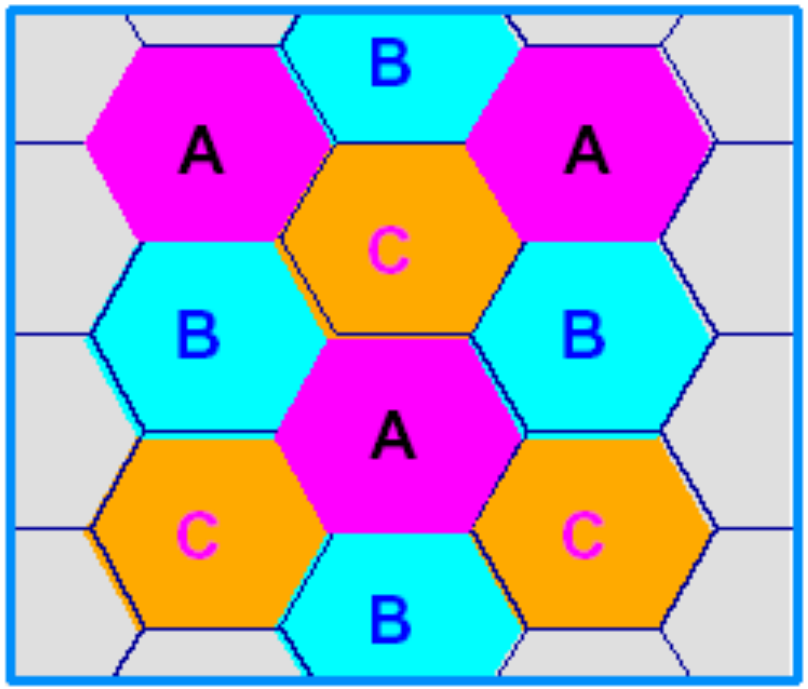


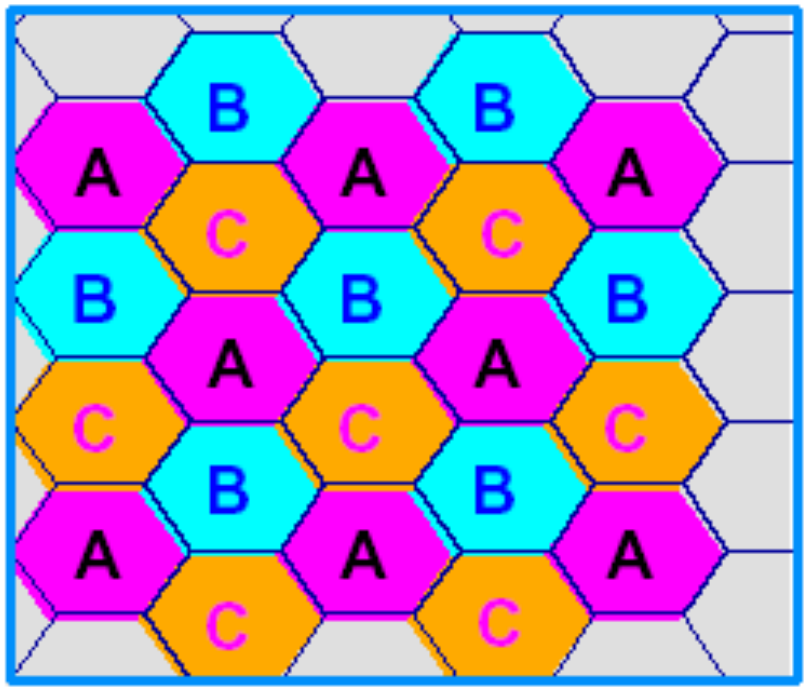
- Green, pink and light blue cells use disjoint sets of channels
- Cells of the same color are called "co-channel" cells → usano stesso canale

7-cell cluster



Fixing *G* and varying the cell size *R*





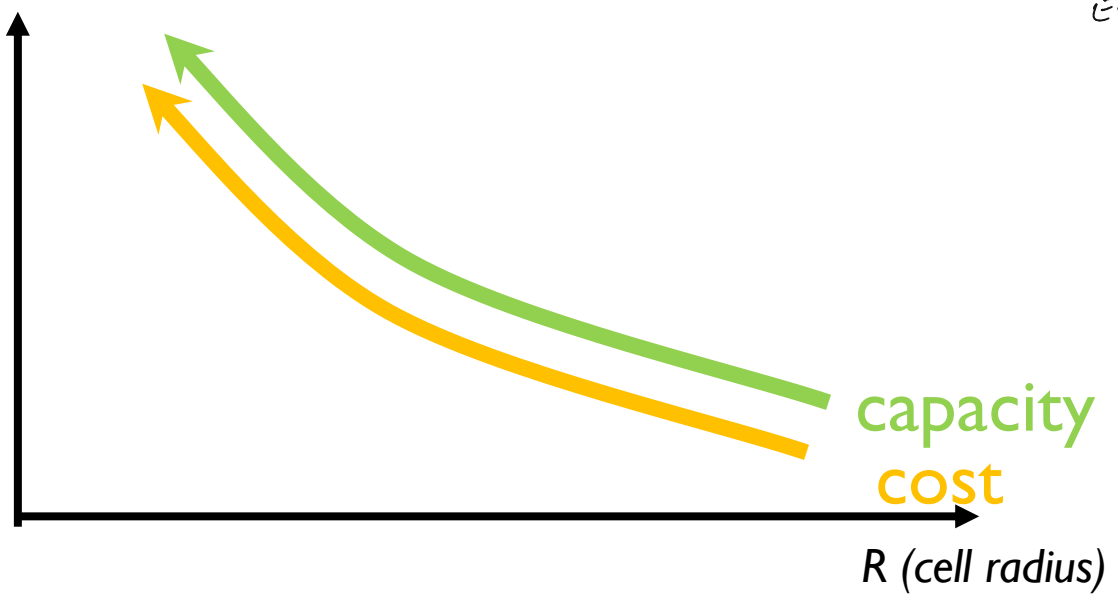
Given a cluster size, the *system capacity* increases as the cell radius (i.e., cell size) decreases

USARE MICROCELLS, AUMENTA I COSTI

AREE DENSAMENTE POPOLATE → DOVE MICROCELLS
APERTA CAMPAGNA → NON MICRO

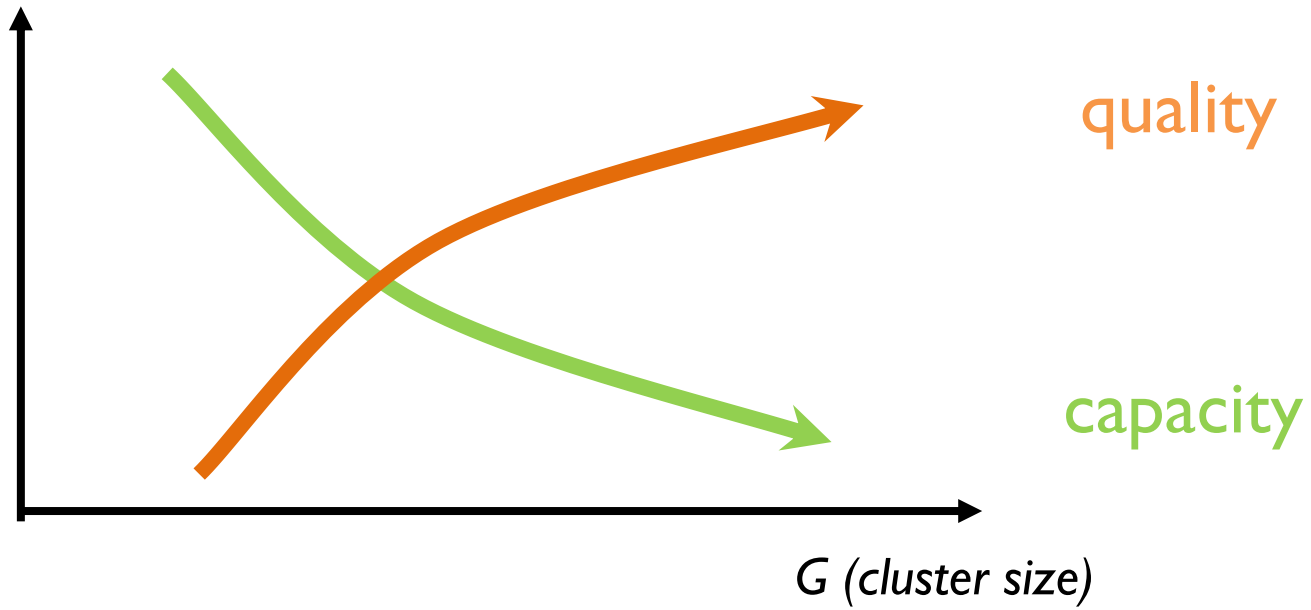
Fixing *G* and varying the cell size *R*

• INOLTRE IL RAGGIO NON DEVE ESSERE TROPPO PICCOLO × EVITARE INTERFERENZE



- Given *G*:
  - The smaller the *R*, the larger the capacity
  - The smaller the *R*, the larger the number of antennas needed to ensure same total coverage

Fixing *R* and varying the cluster size *G*



- Given *R* (i.e., given the cell size):
  - The larger the *G*, the smaller the number of channels per cell, the lower the system capacity (allo stesso modo xò allontano le celle co-channel → migliore qualità)
  - The larger the *G*, the larger *the distance between co-channel cells*, the less the interference, the better the quality

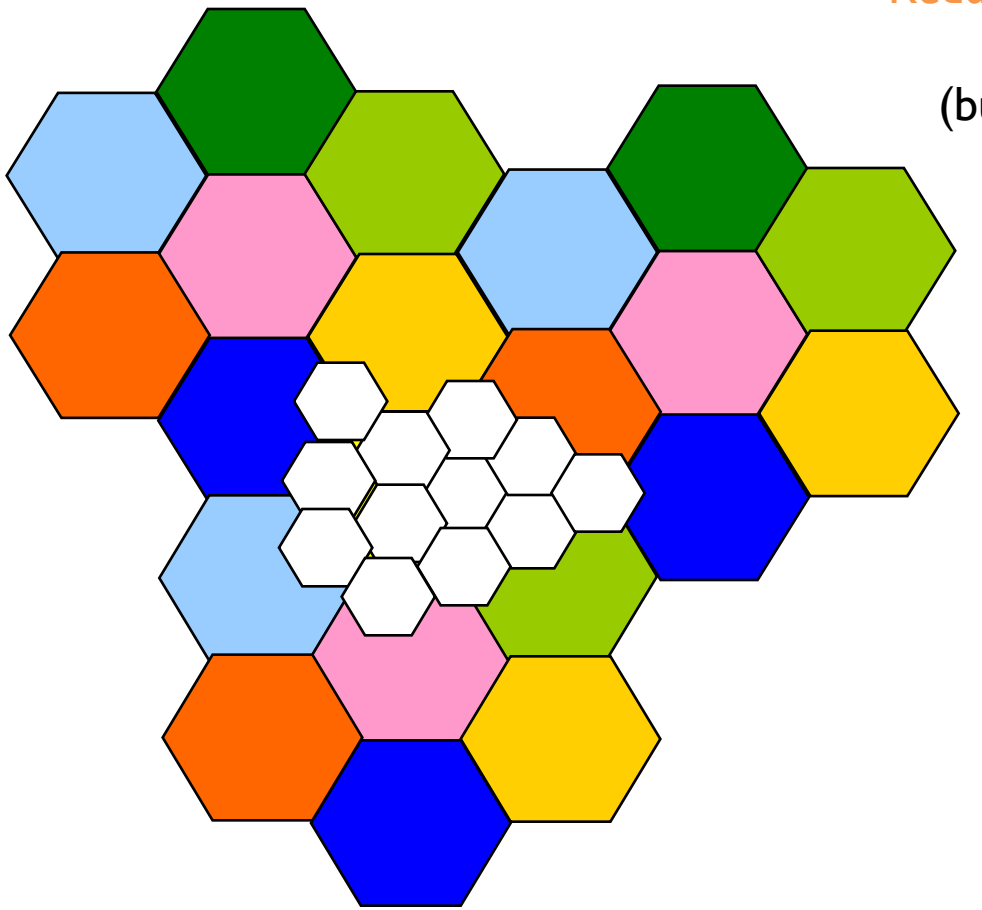
Frequency reuse

- Some techniques reduce interference and increase capacity
  - Splitting → usare celle sovrapposte
  - Sectoring → usare antenne ± direzionali in base al contesto in cui mi trovo
  - Tilting → non puntare l'antenna esattamente a 90° dal suolo
  - Creating femtocells → celle molto molto piccole che uso solo in determinati eventi, per un determinato tempo (es: in caso di un concerto molto grande)

Splitting

- Split large cells into a set of small cells
- Coexistence between
  - Microcells: small cells in highly populated areas with high traffic density (large cities). Transmit power at the base station ≈ 3 W
  - Macrocells: large cells in areas with low traffic density (rural areas). Transmit power at the base station ≈ 20-60 W

Splitting



Reducing R leads to capacity increase

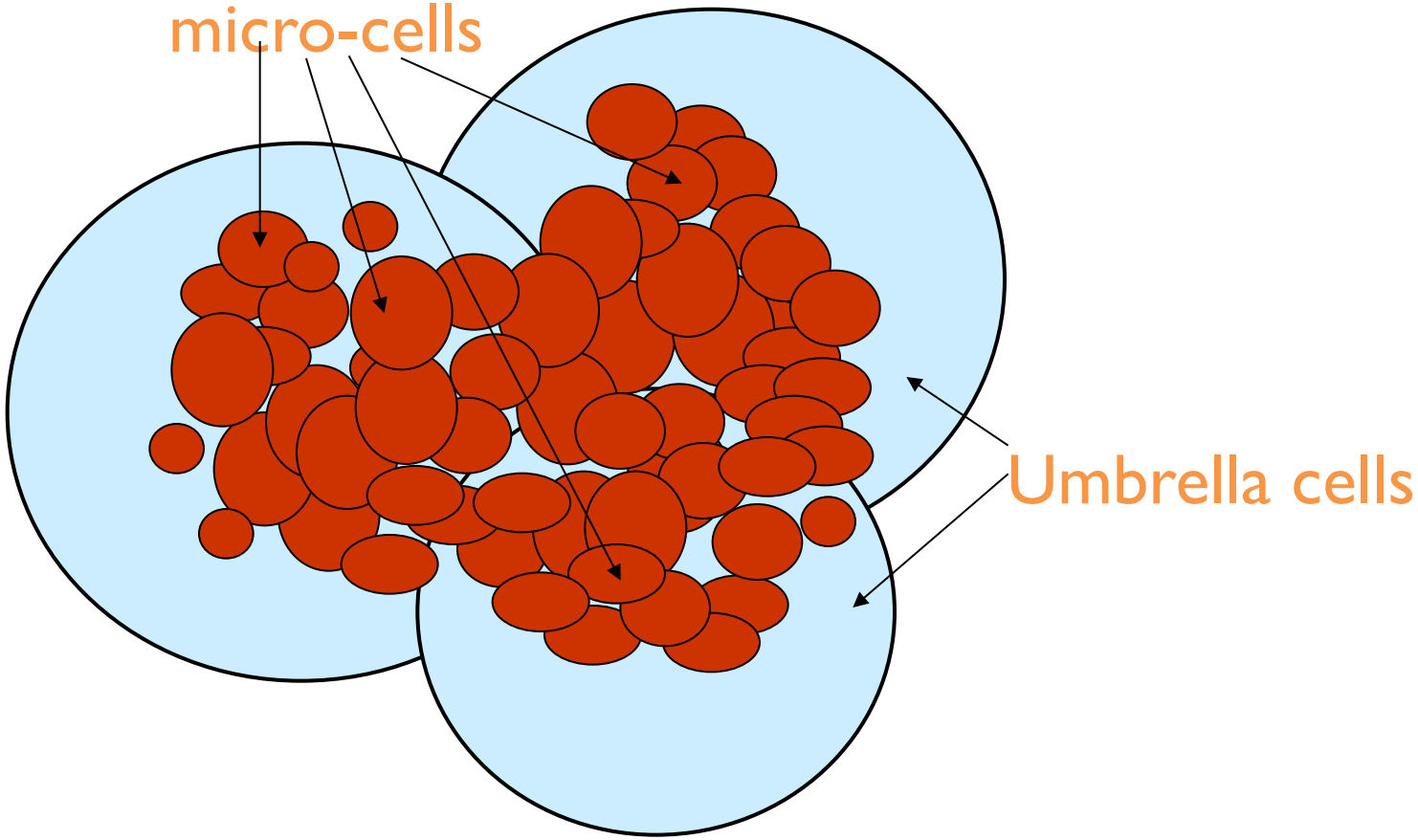
(but also cost increase)

- Each large cell is replaced by a group of small cells

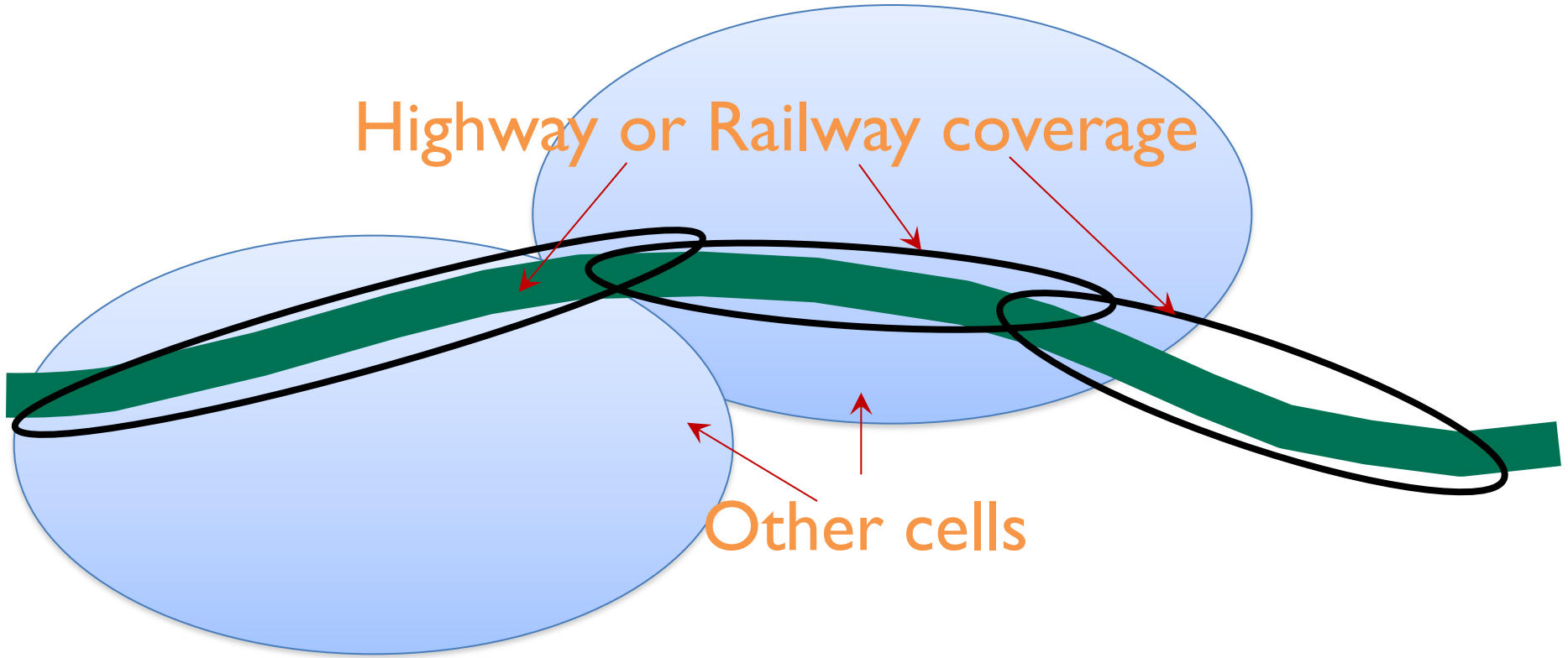
Cell shaping

- It is possible to use directional antennas to have cells with an ad-hoc size and shape
- It is possible to create multi-layer cell coverage (umbrella coverage)
- Microcells that follow the user as she moves

Cell shaping

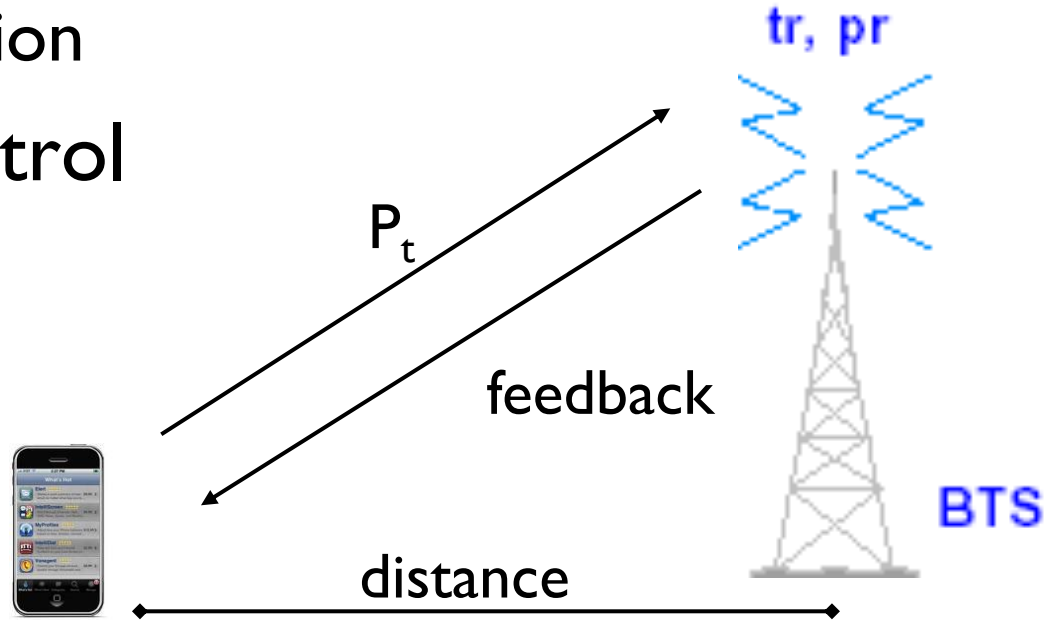


Cell shaping



Power control

- Needed to reduce:
  - Interference
  - Energy consumption
- Open/ closed control



Power control strategies

- In uplink:
  - Closed loop power control
  - Open loop power control
  - Outer loop power control
- In downlink:
  - Downlink power control

Power control: open loop (uplink)

- The user terminal controls itself
- 2-phase mechanism:
  - User measures the quality of the signal received from the BS (downlink signal)
  - The user employs an algorithm to set the transmit power to be used in uplink so that the estimated SINR is above a given threshold
- "Open Loop" since there is no feedback
- Not very accurate as uplink and downlink transmissions typically occur on different channels
  - Other techniques more accurate but more complex (e.g., closed loop)

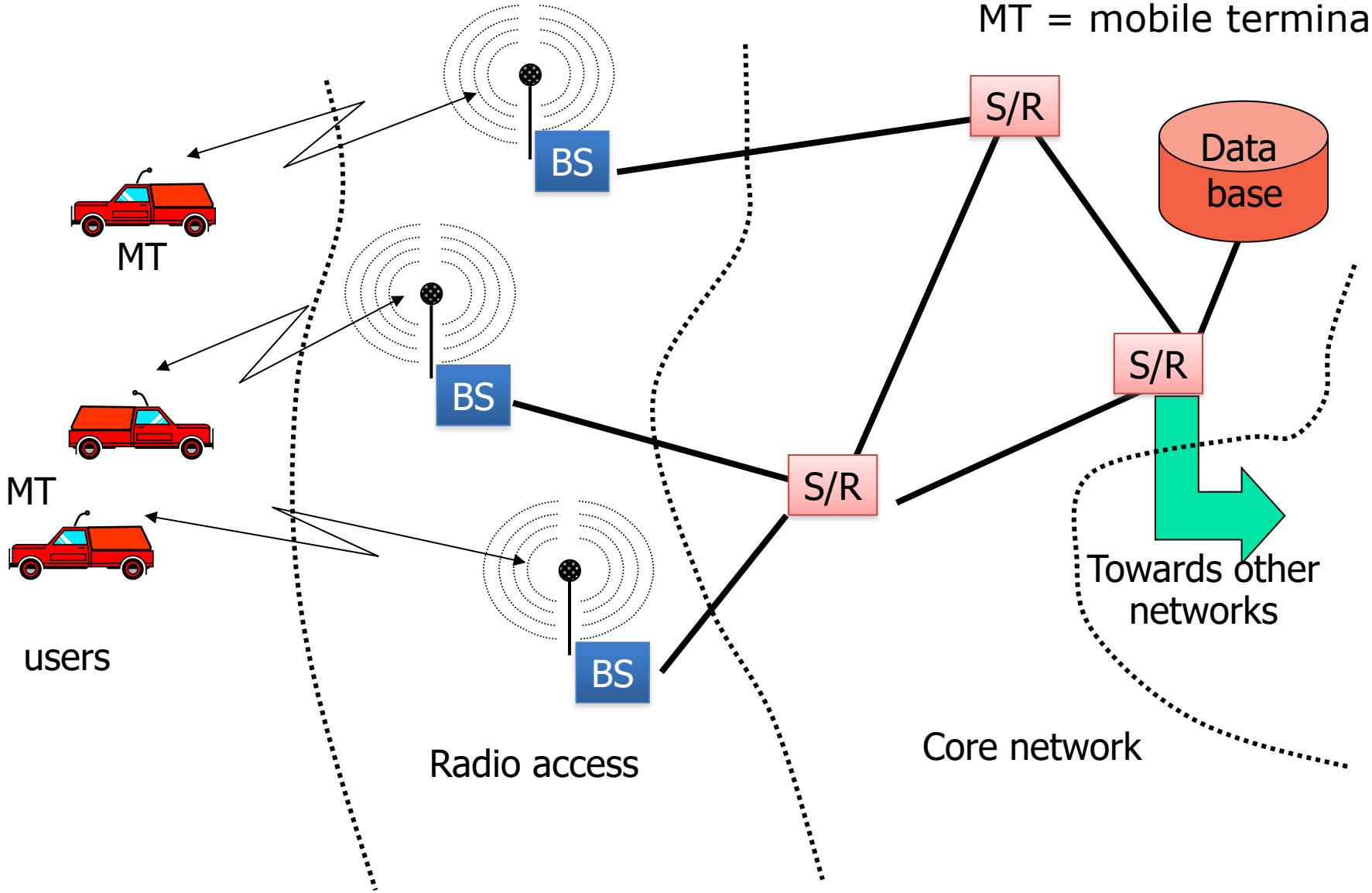
veli da 70 a 96

Frequency allocation

- Fixed Channel Allocation (FCA)
  - Based on the concept of cluster
  - Frequencies are assigned in a static way
  - Frequency plan is changed only rarely to improve performance and adapt to slow variations in user traffic
- Dynamic Channel Allocation (DCA)
  - Resources assigned to cells by a central controller when needed
  - Frequency plan changes over time to adapt to the system status
- Hybrid Channel allocation Scheme (HCS)
  - One portion is statically allocated (FCA)
  - One portion is dynamically allocated (DCA)

Network architecture

S/R = switch/router
BS = base station
MT = mobile terminal



Basic procedures: Registration

- It allows a mobile terminal:
  - to connect with the network
  - to identify and authenticate itself
- It is performed:
  - When a terminal is switched on and has to associate with the network
  - Whenever a user wants to access a service (es. start a call)
  - Periodically

Basic procedures: Mobility management

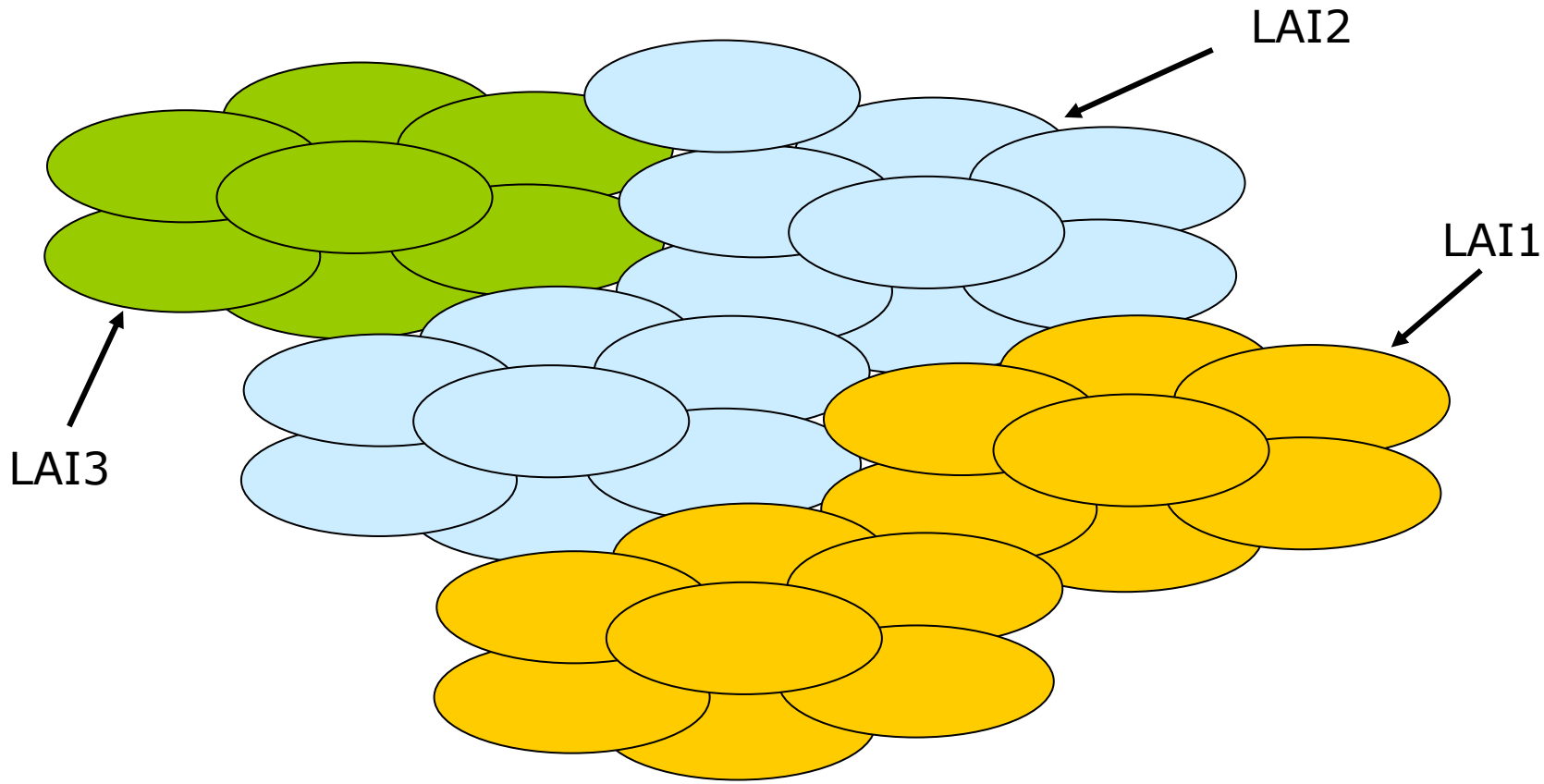
- Mobility support characterizes cellular networks
- We need procedures to handle mobility
  - Roaming
  - Location updating
  - Paging
  - Handover

Roaming

- The user position has to be *traceable* even if she moves over the network area
- The system has to store the user position in a database to locate users whenever needed
- To store user positions, the network area is divided into *location areas (LAs)*, i.e., groups of cells

Roaming

- Each location area has an ID: *location area identifier (LAI)*



Location updating

- Procedure through which the user position is updated
- A control channel is periodically broadcasted in each cell of an LA
- When the mobile terminal receives an LAI different from the one previously stored, the user starts a location updating procedure in order to update her position in the database

Paging

Si usa x raggiungere l'utente quando qualcuno vuole raggiungerlo

- Procedure through which the system notifies a mobile terminal about an incoming call/data delivery
- The system broadcasts a paging message within the LA where the user is

o informa che c'è del traffico in arrivo

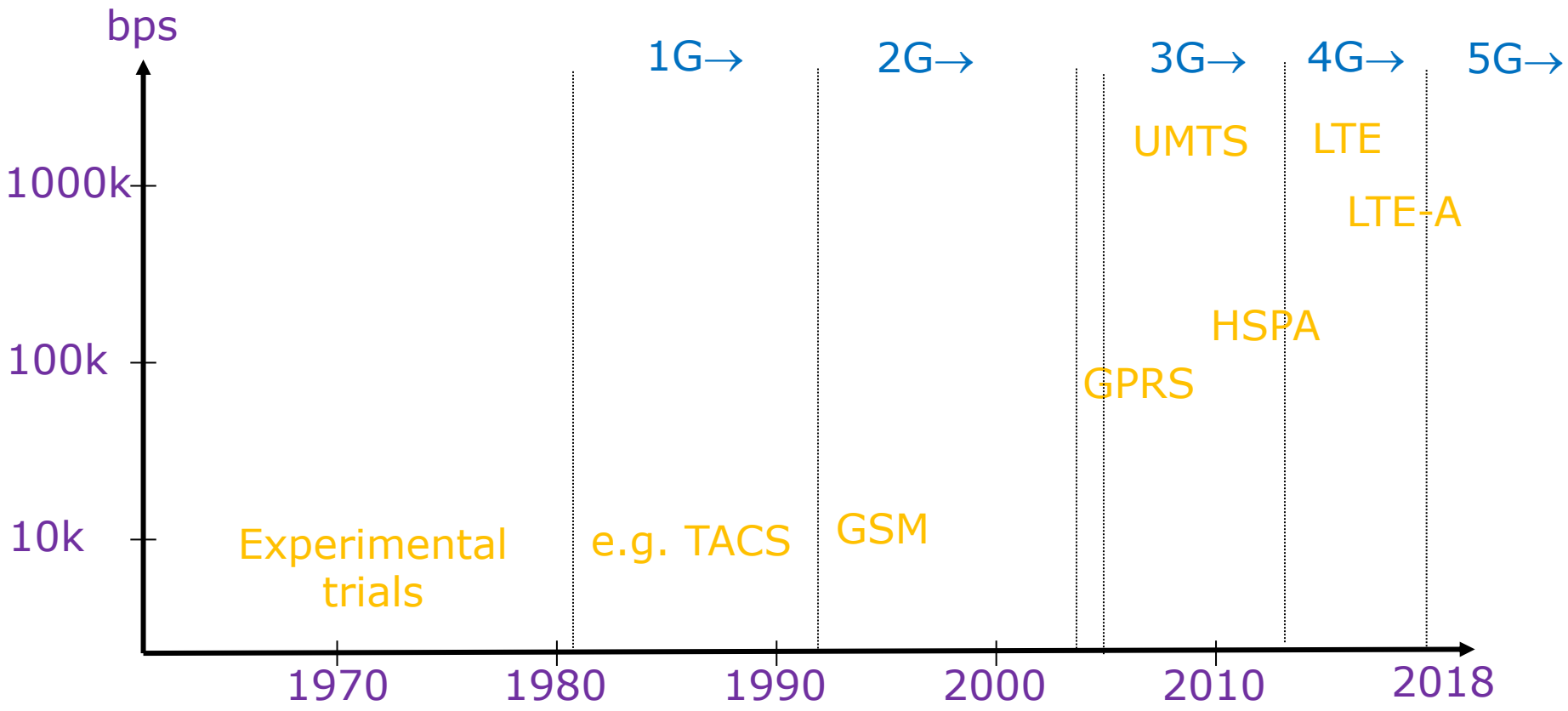
Handover (Quando mi muove nel bel mezzo della chiamata

- Procedure that enables the transfer of an active connection from one cell to another, while the mobile terminal moves over the network area
- Complex procedure that poses constraints on the network architecture, protocols and signaling

Handover classification

- Intra vs. Inter Cell
  - It indicates whether the handover is between frequencies within the same cell or different cells
- Soft vs. Hard
  - It indicates whether during handover both radio channels are active (soft) or only one at the time is active (hard)
- MT vs. BS initiated
  - It indicates whether the first control message to start a handover is sent by the mobile terminal (MT initiated) or by the BS (BS initiated), i.e., which entity performs measurements to understand where and when a handover has to be executed
- Backward vs. Forward
  - It indicates whether handover signaling occurs via the origin BS (backward) or the destination BS (forward)

Cellular network evolution



1G: First generation

- *Analog technology*
- FDMA
- Voice traffic only
- Low service quality
- Low efficiency in frequency reuse, and low network capacity
- TACS:
  - 900 MHz
  - Channel width=25 kHz
  - In Italy, service stopped (TIM) on 31/12/05

2G: Second generation

(usata x telefonate in qualche contesto)

- Main change: *from analog to digital*
- Advantages:
  - Integration of different services (e.g., SMS)
  - Cryptography
  - Advanced voice coding to reduce bandwidth requirements
- FDMA/TDMA in Europe, CDMA in the U.S.
- Frequency bands: 850, 900, 1800, 1900 MHz
- Active networks:
  - IS-95 in USA
  - GSM in Europe -> Slovenia
  - PDC in Japan

2.5G: Extended second generation

(PRIMA VOLTA PACCHETTI)

- GPRS/EDGE in Europe, IS-95B in USA
- Introduction of data service
  - Packet switched
  - 170 kb/s in GPRS, 384 kb/s in EDGE
  - Traffic-based instead of time-based billing

3G: Third generation (anche in Europa CDMA) (non + USATA)

- Improvement of data service (multimedia services)
- CDMA
- Exploit spatial diversity (simultaneous transmissions with multiple BSs) to improve quality
- High data rate (up to 2 Mb/s)
- Handover between different networks (2G-3G) is possible (vertical handover)
- Networks:
  - UMTS (Universal Mobile Telecommunication System) in Europe and Japan
  - CDMA2000 (IS-95C) in USA

3.5G: Extended third generation

- Evolution of UMTS
  - HSPA (High-Speed Packet Access), composed of HSDPA and HSUPA (downlink/uplink)
  - HSPA+ (Evolved High-Speed Packet Access)
- Mainly changes at the UMTS physical layer
- Data rates up to:
  - 56 Mb/s DL
  - 22 Mb/s UL

4G: Fourth generation (usa OFDMA)

- Known as LTE (Long Term Evolution)
- Data rate up to 250 Mb/s
- Uses MIMO and high-performance modulations
- All – IP
- Initially only data service (now also voice with *VoLTE*) → gestire QoS voce a pacchetto e non GSM
- Standardization
  - "4G" has to satisfy ITU requirements for "IMT Advanced" (high spectrum efficiency, minimum data rate of 1 Gb/s for fixed users and 100 Mb/s for mobile users)
  - LTE does not meet such constraints yet, the right name would be "3.9 G"
  - LTE-Advanced (standard since 2011) meets such requirements

5G: Fifth generation

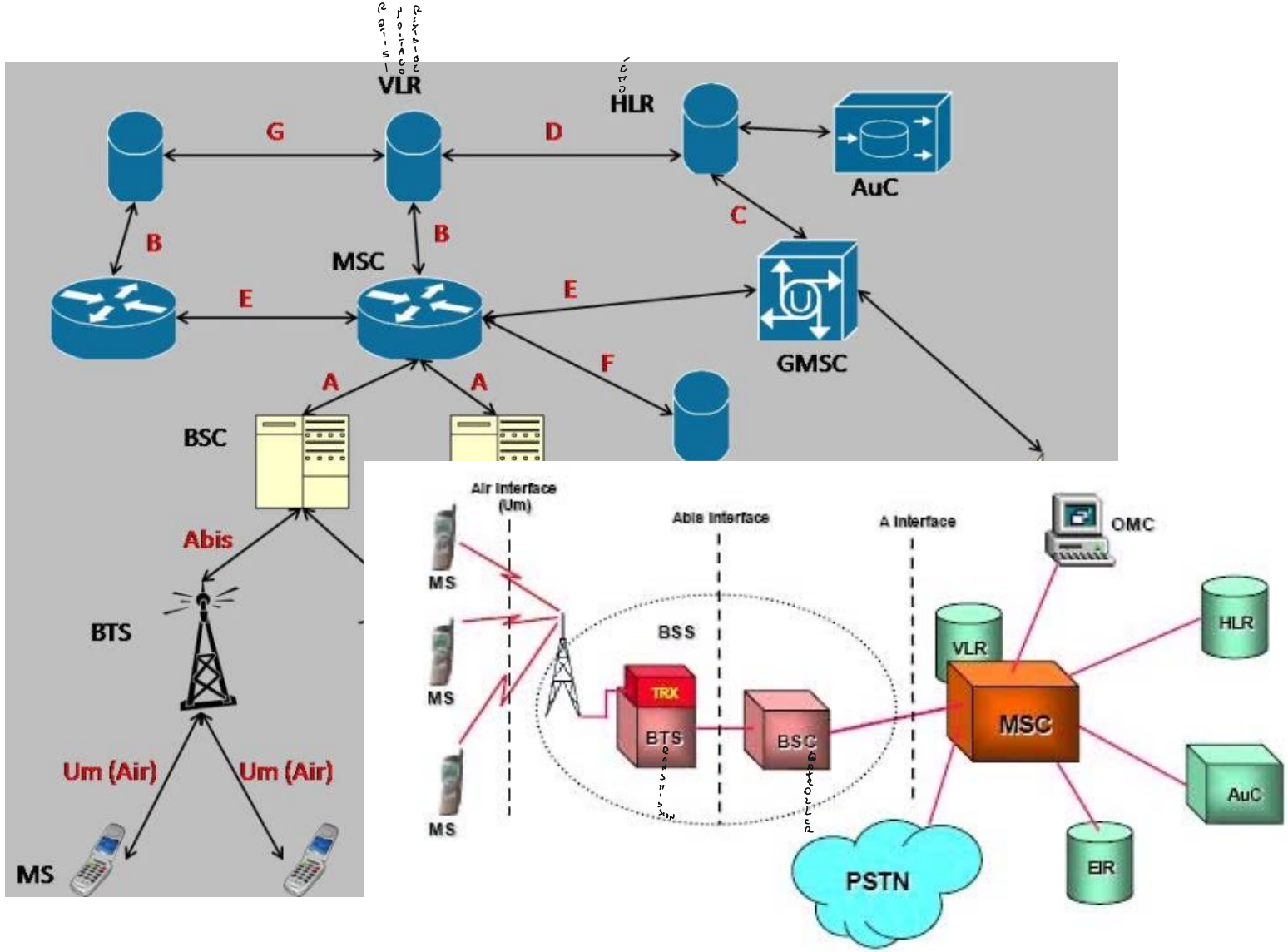
- Integrates different technology over the wireless segment (mainly, further evolution of LTE-A, WiFi and mmWave communications)
- Exploit the SDN (*Software defined Networking*) paradigm for network control and operation
  - Offrire un piano di controllo facilmente modificabile e flessibile (in quanto SW)
- Exploits the NFV (*Network Function Virtualization*) paradigm for service implementation
  - Fornire servizi di rete in maniera virtuale attraverso datacenter più o meno distribuiti

GSM: the 2nd Generation

Services offered by GSM

- Voice full rate (13 kbit/s), half rate (6.5 kbit/s)
- SMS
- Supplementary services (call forward, recall on busy tone,….)

GSM network architecture



Mobile Station (MS)

- User Equipment
- several types depending on the application, e.g.:
  - Mobile phones
  - Mobile devices (e.g., laptop, tablet, etc.)
  - Antennas on vehicles
- Different transmitted power at the antenna
  - Up to 2W for mobile phones
  - Up to 8W for mobile devices
  - Up to 20W for car antennas

Subscriber Identity Module (SIM)

- MS is “hardware” only, to connect to the network it needs a SIM

MT
(Mobile Terminal)

=

+

- SIM=Smart card with processor and memory (to be inserted in the SIM reader)
- SIM stores (encrypted) user information: phone no., accessible services, security parameters, ecc.

IMSI

TMSI

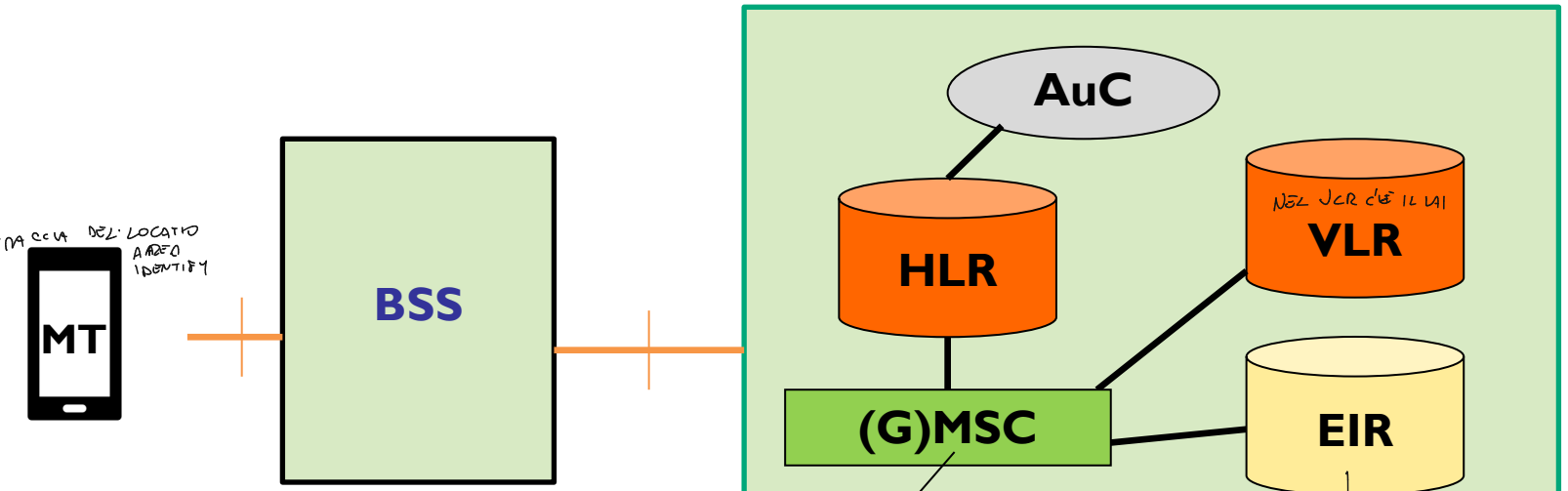
Base Station Subsystem (BSS) → ID CELLA

CELLA GESTITA DA:

- Base Station (BS)
  - Base Transceiver Station (BTS) (ANTENNA)
    - Physical interface in charge of transmission and reception
    - Point of access for the MT
    - Unlike other signal sources (e.g. radio, TV), BTSs transmit signal only towards users that are active
    - Up to 32 FDM channels per BTS (half uplink, half downlink)
  - Base Station Controller (BSC)
    - Resource control on the radio interface: BSCs and BTSs communicate over a wired link
    - A BSC controls a high number of BTSs: from *tens* to *hundreds*
    - Typically, BSCs are collocated with one MSC, instead of being located near the BTSs
    - BSC main functions:
      - Voice transcoding 13 kb/s ↔ 64 kb/s
      - Paging → BROADCAST NELLA LOCATION AREA
      - Radio resource control: dynamic frequency assignment to BTSs → GESTISCE ALLOCAZIONE DI RISORSE NELLA CELLA MA SI OCCUPA ANCHE DI ASSEGNARE UN CANALE FISICO AGLI UTENTI CHE NE HANNO BISOGNO
      - Signal quality measurement
      - Management of handover between BTSs controlled by the same BSC

Network and Switching Subsystem (NSS)

- Main functions:
  - Call handling
  - Service support
  - Mobility support
  - Authentication

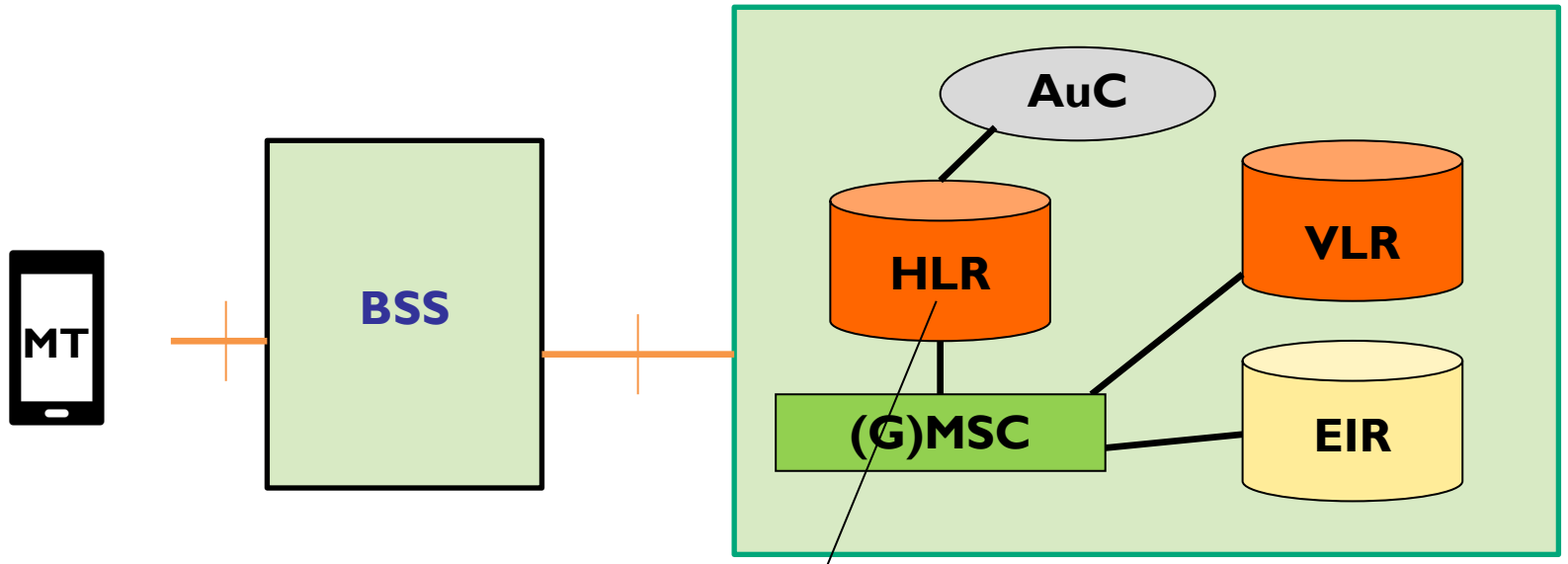


Mobile Switching Center

- Mobility support
- Call routing between MT
- GMSC: Interface between the GSM network and other networks

Network and Switching Subsystem (NSS)

- Main functions:
  - Call handling
  - Service support
  - Mobility support
  - Authentication

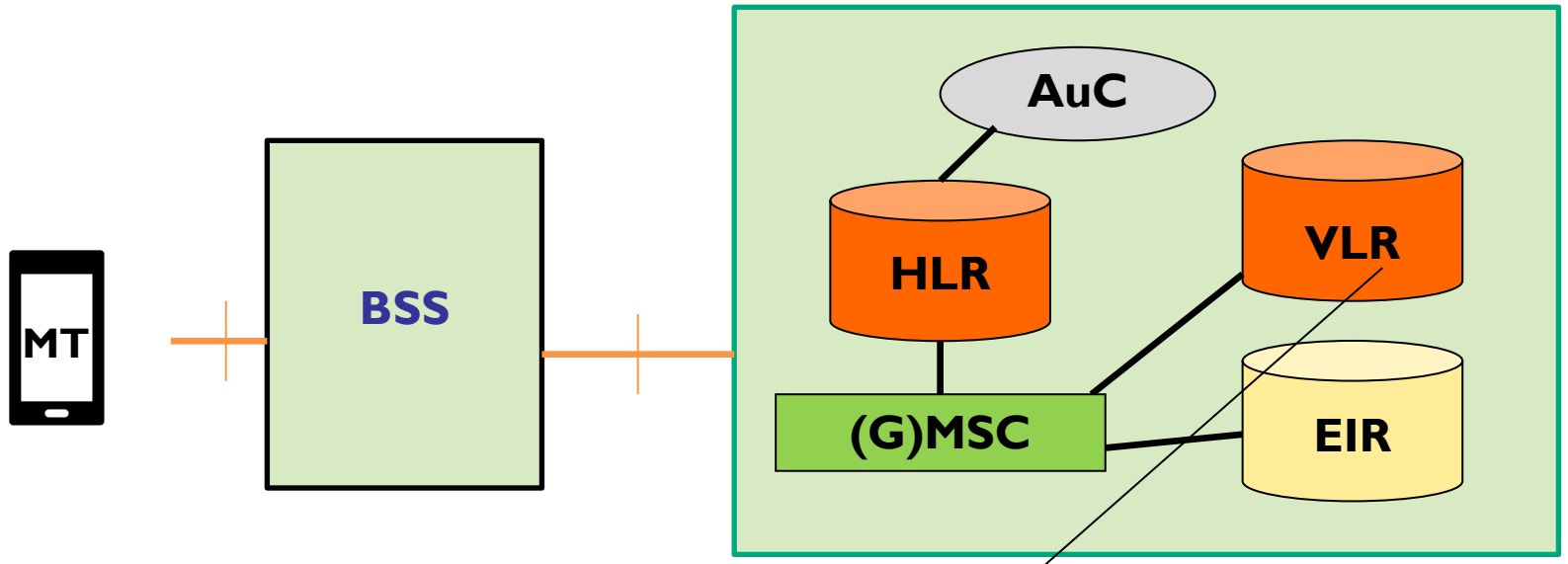


Home Location Register

Database storing:
- Permanent user data: id, enabled services, security parameters
- Dynamic data to handle user mobility (e.g., VLR identifier)

Network and Switching Subsystem (NSS)

- Main functions:
  - Call handling
  - Service support
  - Mobility support
  - Authentication



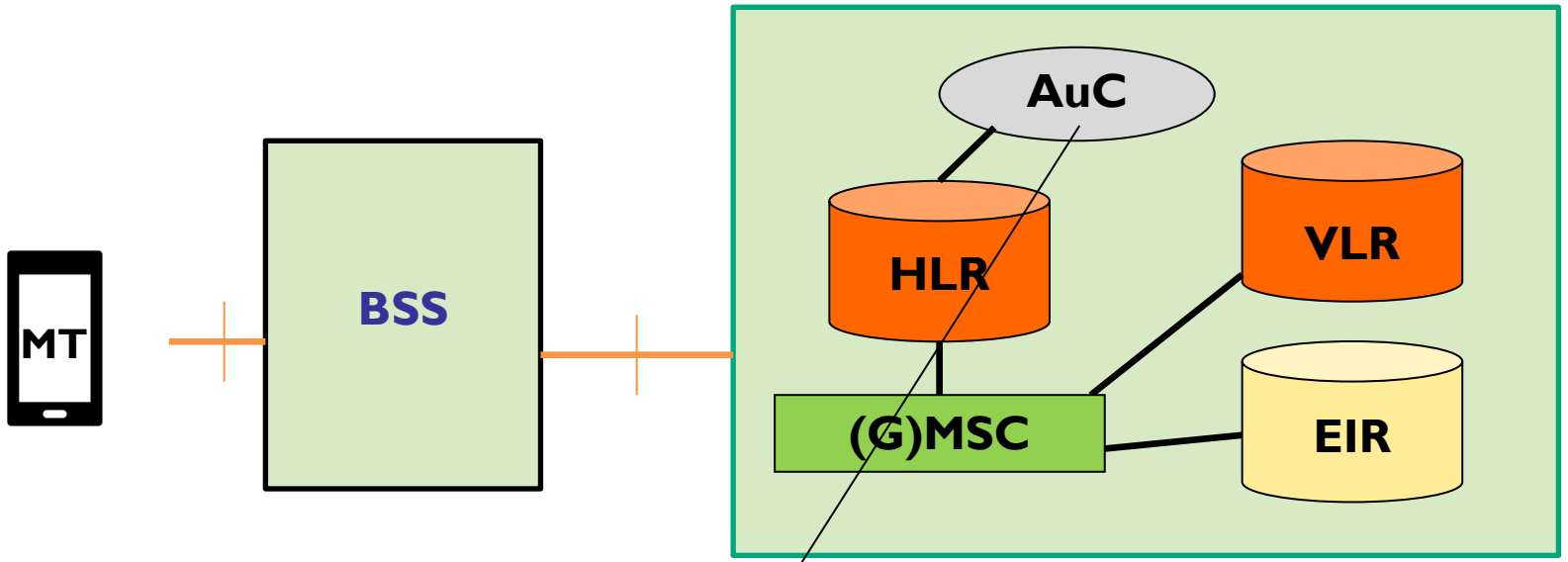
Visitor Location Register

Database storing:

- Information related to MTs currently in the area controlled by the MSC: IDs, on/off status, LAI, routing information, security

Network and Switching Subsystem (NSS)

- Main functions:
  - Call handling
  - Service support
  - Mobility support
  - Authentication

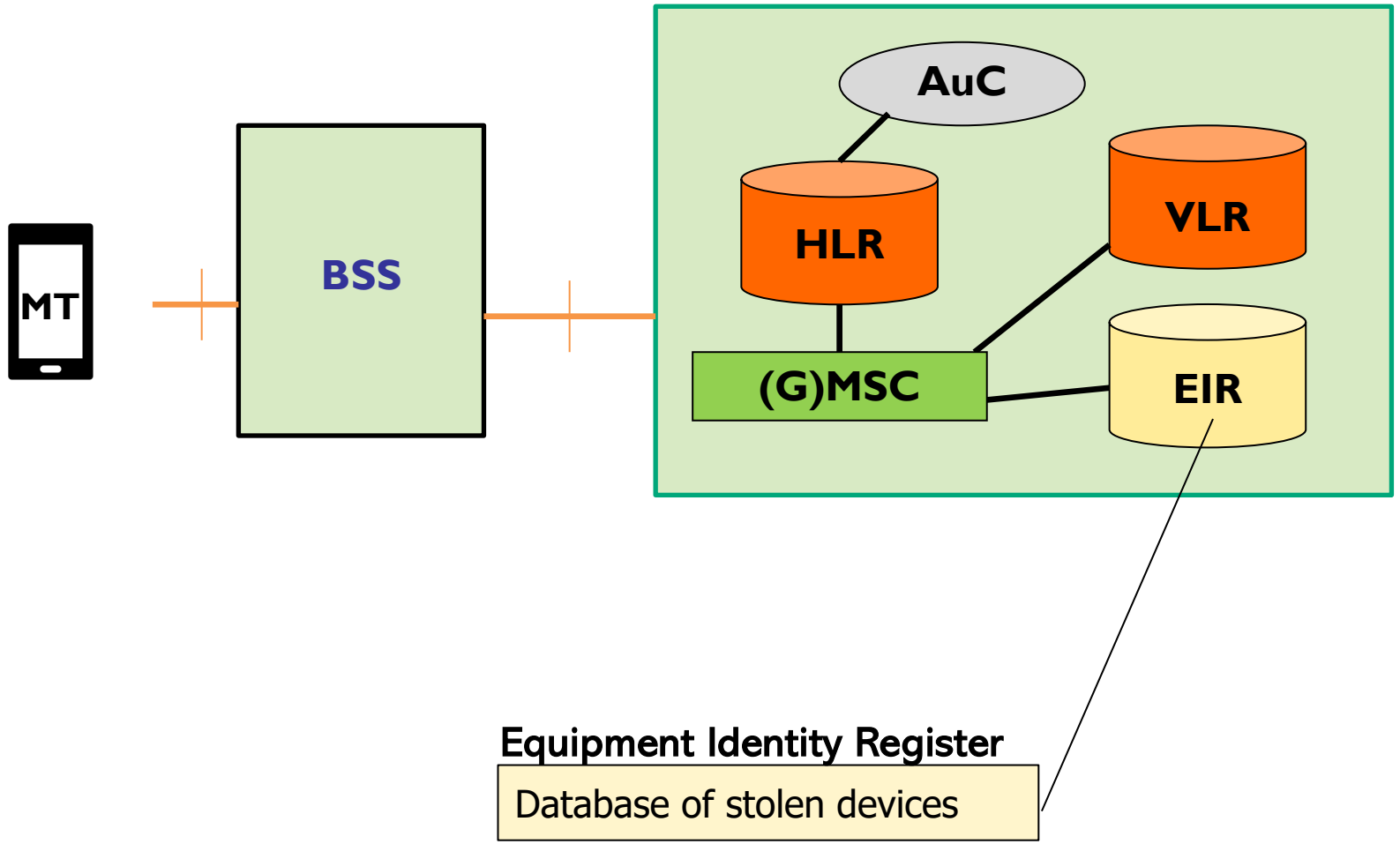


Authentication Center

Authentication based on challenge & response protocol
Generations of encryption keys for over-the-air communication

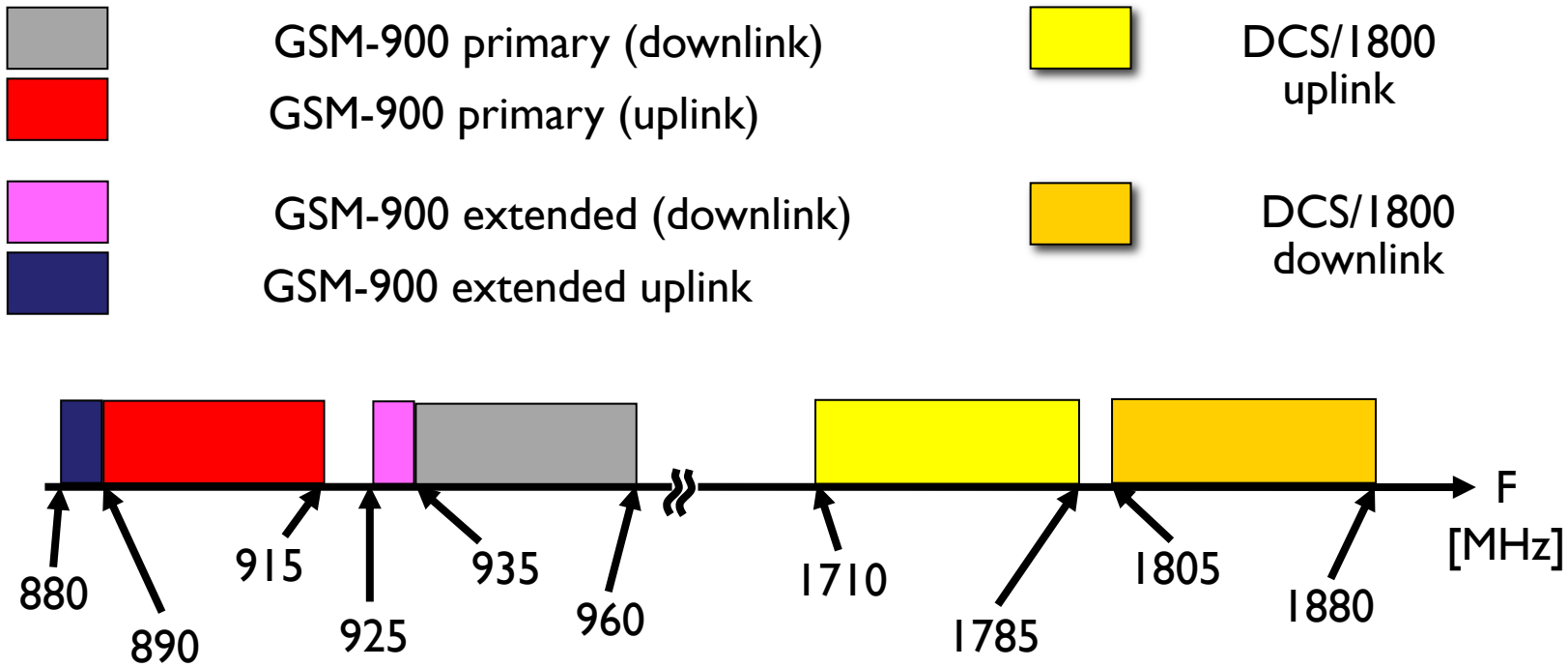
Network and Switching Subsystem (NSS)

- Main functions:
  - Call handling
  - Service support
  - Mobility support
  - Authentication



GSM frequencies (Europe)

- Allocated frequencies: 850, 900, 1800, 1900 MHz
- FDD (Frequency Division Duplex) system
  - different frequencies for UL and DL



GSM physical channels

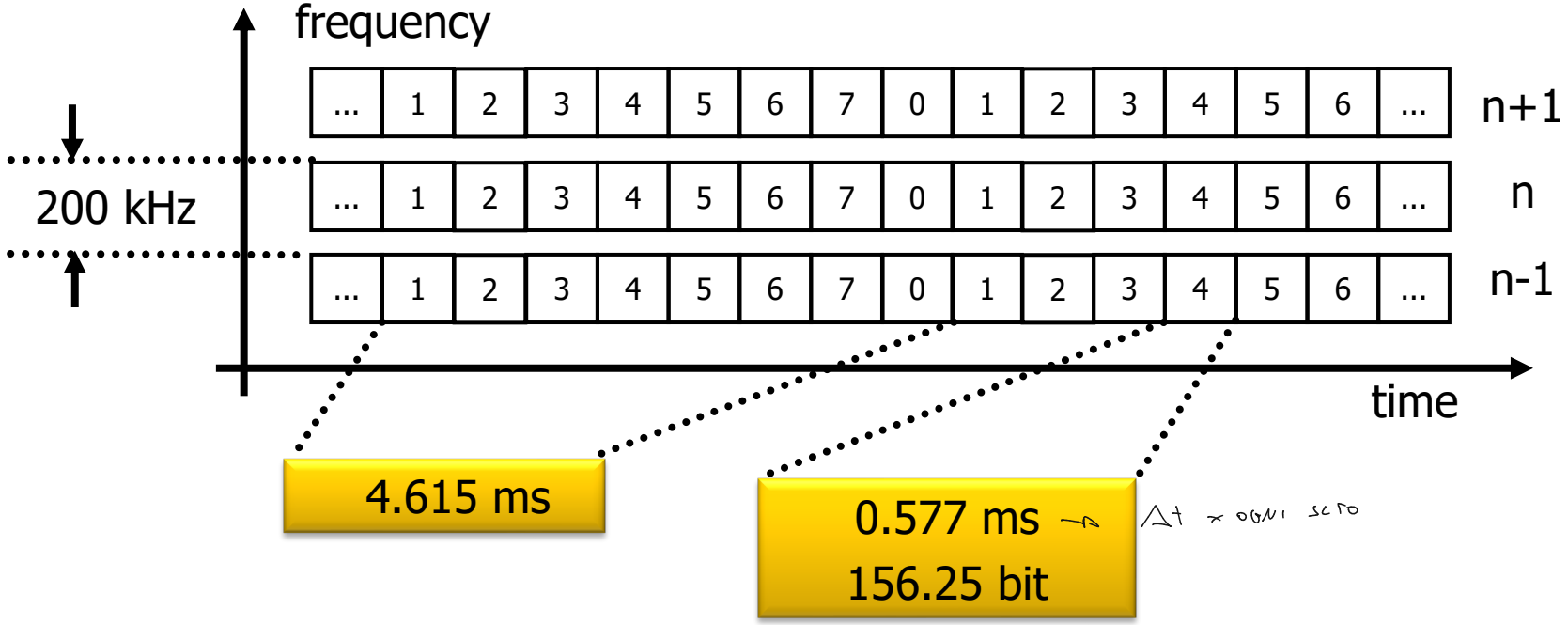
- Channel access: FDMA/TDMA
- Frequency spectrum divided into FDM channels, each 200 kHz wide
- Each FDM channel is divided into TDM frames
- Each TDM frame is divided into 8 slots

$\Rightarrow$ *Frequency* + *time slot* = *physical channel*

- Transmission organized into "bursts", i.e., blocks of data that are transmitted on a physical channel
  - Bursts are similar to packets…But it is still circuit switching!
- Transmission speed = 271 kbit/s

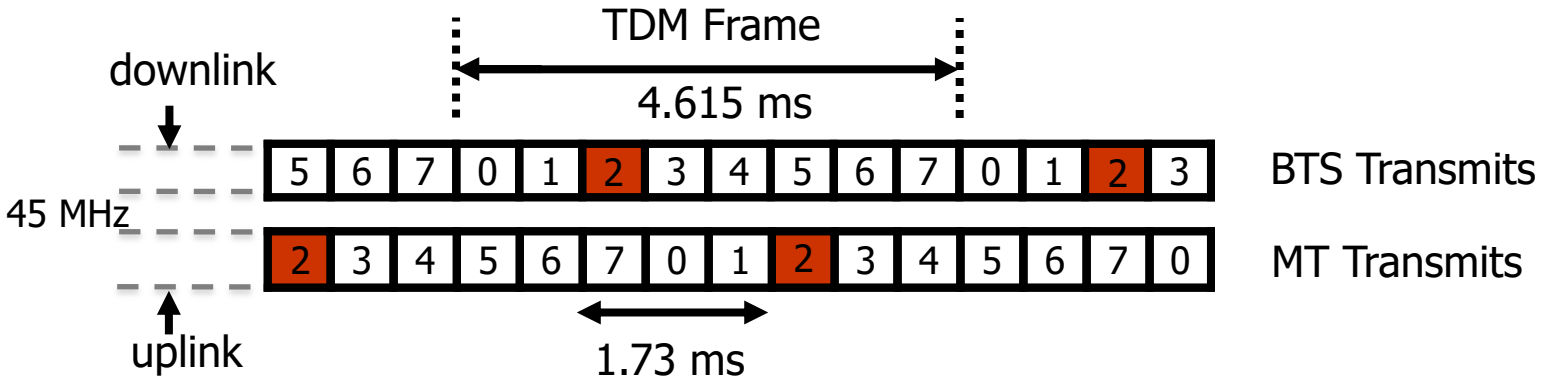
Channel access – Summary of FDM/TDM schema

- Slot time = 0.577 ms
  - 1 slot carries 156.25 bits (i.e., 0.577*271 kbps)
- Each time slot carries 1 transmission burst
- Slots are grouped into TDM frames, of 8 slots each
  - Frame = 4.615 ms



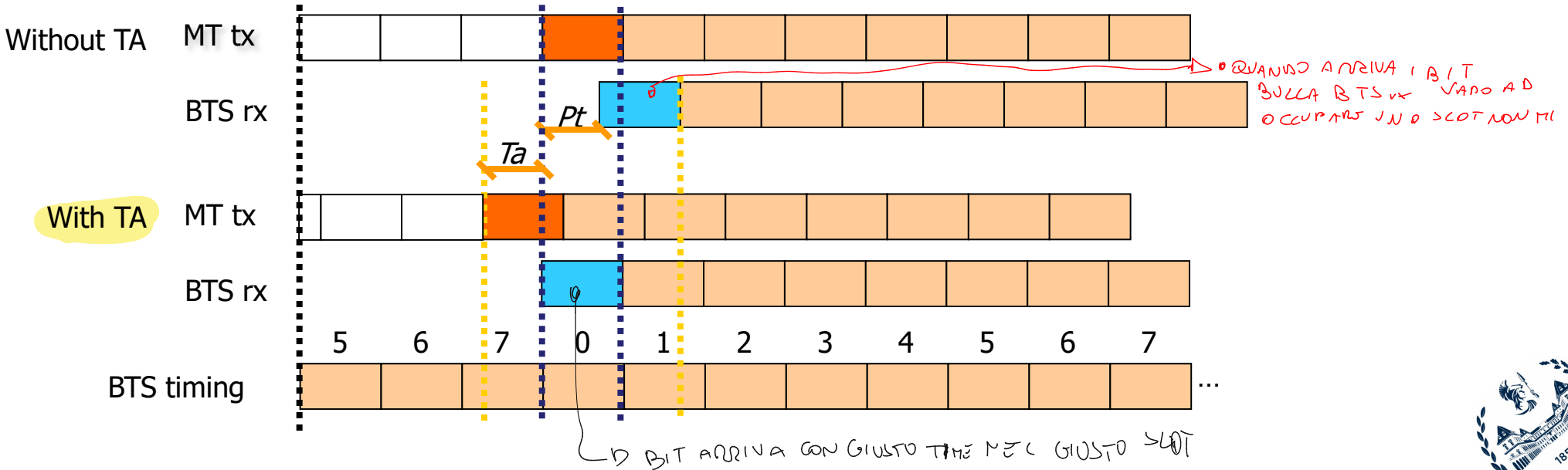
Channel access – GSM frame

- Circuit-switched network
  - Each call @full rate (13kb/s) is assigned 1 slot per frame in UL and 1 slot per frame in DL
- Each MT transmits on a carrier for one time slot, i.e., one burst of data, and remains silent during the other 7 slots
- Frames on UL and DL are synchronized on a time slot basis and shifted by 3 slots
- Separating UL/DL transmissions in frequency and time allows the use of one transceiver only

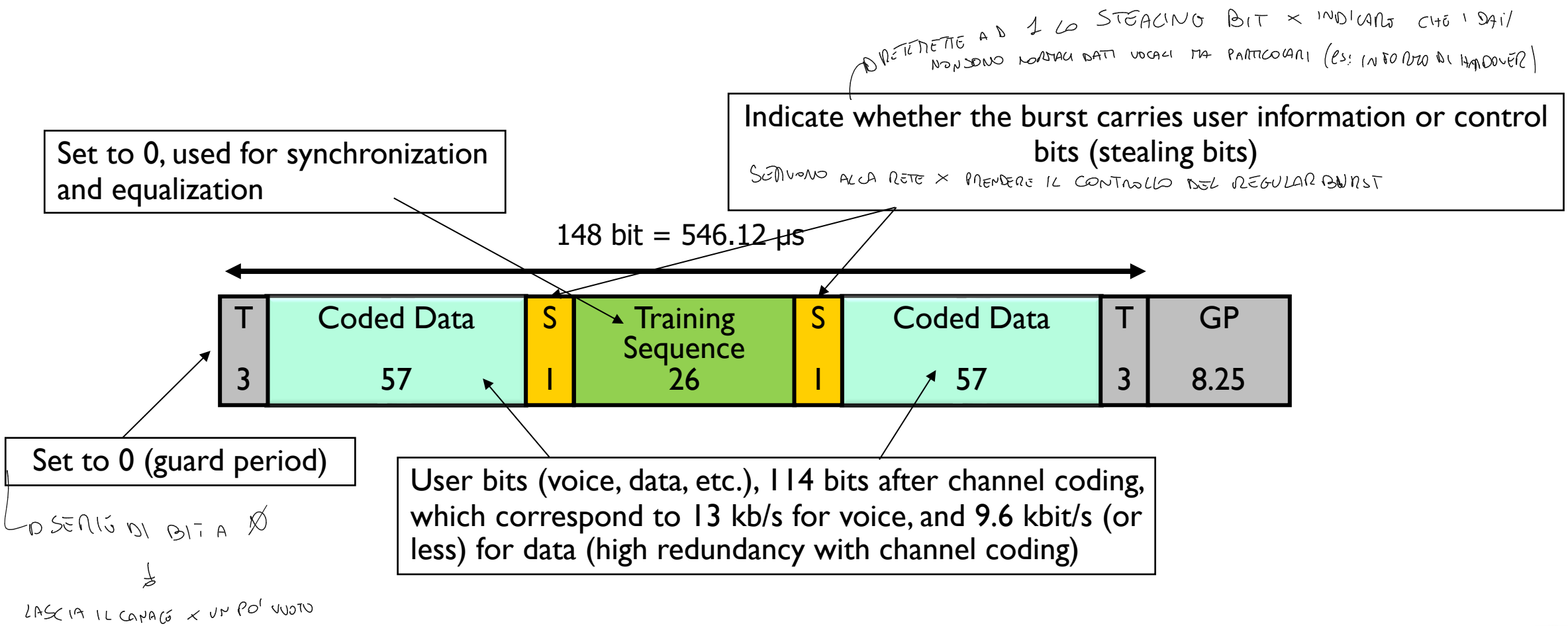


Channel access – Timing advance

- Non-zero propagation times
  - Bursts transmitted by MTs might arrive at the BTS when the slot is already finished
  - Possible collisions
- Solution: *timing advance*
  - Transmission at the MT starts *before* the real timeslot beginning



“Regular” burst structure



GSM Logical channels

SERVONO X SPECIFICARE COSA DEVE ESSERE TRASMESSO

- Physical channels (SPECIFICA COME DEVE ESSERE TRASMESSO)
  - Combination of timeslot and carrier
  - 8 physical channels per carrier: timeslots 0 - 7
- Logical channels
  - Carry useful information, i.e., specify "*what*" is transmitted
  - Mapped into physical channels according to proper criteria → I CANALI LOGICI VANNO MAPPATI SU CANALI FISICI
- Two types of logical channels (es: messaggi di paging)
  - *Control channels*
    - Carry control information (related to user or network)
  - *Traffic channels* (USATI DAI TERMINALI UTENTE X INVIARE CAMPIONI VOCALI)
    - Carry user information

Control channels

- **Network signaling** → PERMETTONO ALLA RETE DI COMUNICARE ALL'UTENTE:
  - SEGNALI RELATIVI ALLA CELLA (capire così se fare handover)
  - SINCRONIZZAZIONE SCOT
  - Cell parameters
  - Synchronization
  - Receiver tuning
- **User signaling** → MESSAGGI DI SEGNALE RELATIVI A CIASCUNA CHIAMATA
  - Call control (cellulare deve squillare, bisogna capire quando chiamata termina)
  - Signal quality control (measurement delivery)

→ SEGNALE DURANTE LA CHIAMATA

LTE: the 4th Generation

LTE

Si è passato da CDMA(3G) a FDMA(4G) xkè il rapporto costo/benefici non era ottimo e c'era anche un alto consumo di batteria sui dispositivi.

- First release by 3GPP as Release 8, known as LTE-Advanced since Rel. 10
- Speeds up to 300 Mb/s DL - 50 Mb/s UL with modulations up to 64 QAM
- 10-ms data latency
- Replaces WCDMA with OFDMA (DL) and SC-FDM (UL)
- Leverages high-order MIMO
- Up to 20 MHz channels
- Scalable frequency bands from 1.4MHz to 20 MHz
- "All-IP" HSDPA core network

A livello data link

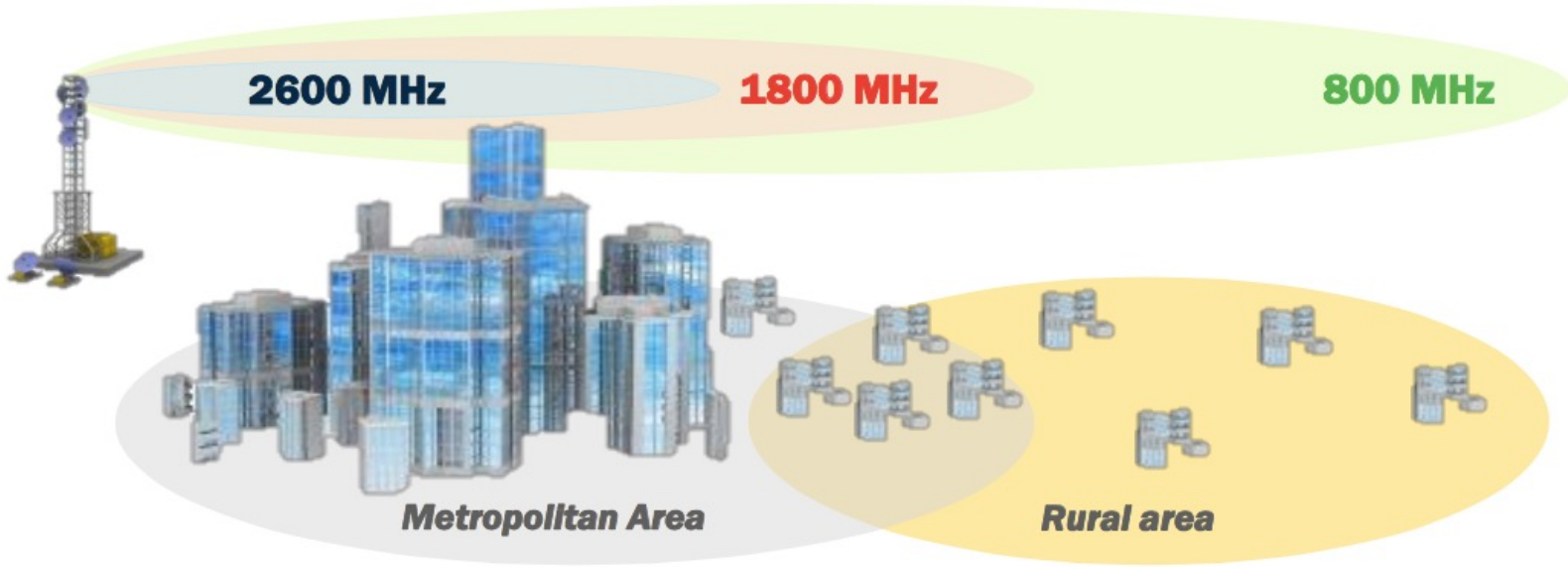
ortogonal → frequenze + vicine - ho più canali di trasmissione → aumenta throughput

→ antenne MIMO (+ performanti)

→ rete completamente a pacchetto e IP

	Release 8 LTE	
	Downlink	Uplink
Peak data rate	300 Mbps (4x4 MIMO) 150 Mbps (2x2 MIMO)	75 Mbps (1x2 SIMO)
Bandwidth	Up to 20 MHz	Up to 20 MHz
Peak Spectrum efficiency	≈ 16.3 bit/s/Hz	≈ 4.3 bit/s/Hz (1x2 SIMO)
Average Spectrum efficiency [bit/s/Hz/cell]	1.69 (2x2 MIMO) 1.87 (4x2 MIMO) 2.67 (4x4 MIMO)	0.74 (1x2 SIMO)
Latency	Data plane : 10 ms (round trip delay) Control plane : 100 ms (idle to active state)	

Usage of Frequency Bands



2600 MHz

*Used to **maximize capacity***

ALTO BITRATE

POCA COBERTURA

1800 MHz

*Band with **high capacity**, and **limited interference***

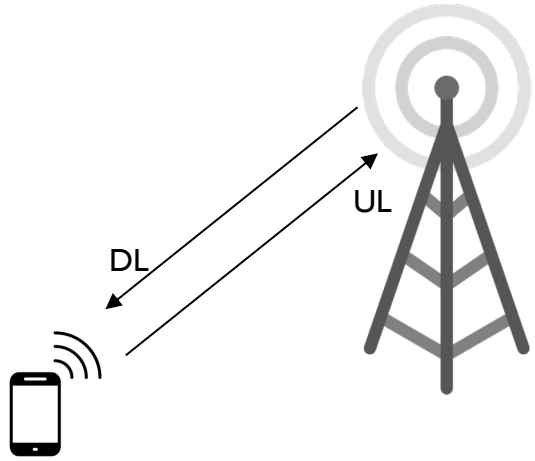
800 MHz

*Band with **high coverage** and interference*

MA MINOR BITRATE

LTE Terminology

- **Downlink** (DL): data going from the network to the user device
- **Uplink** (UL): data going from the user device to the network

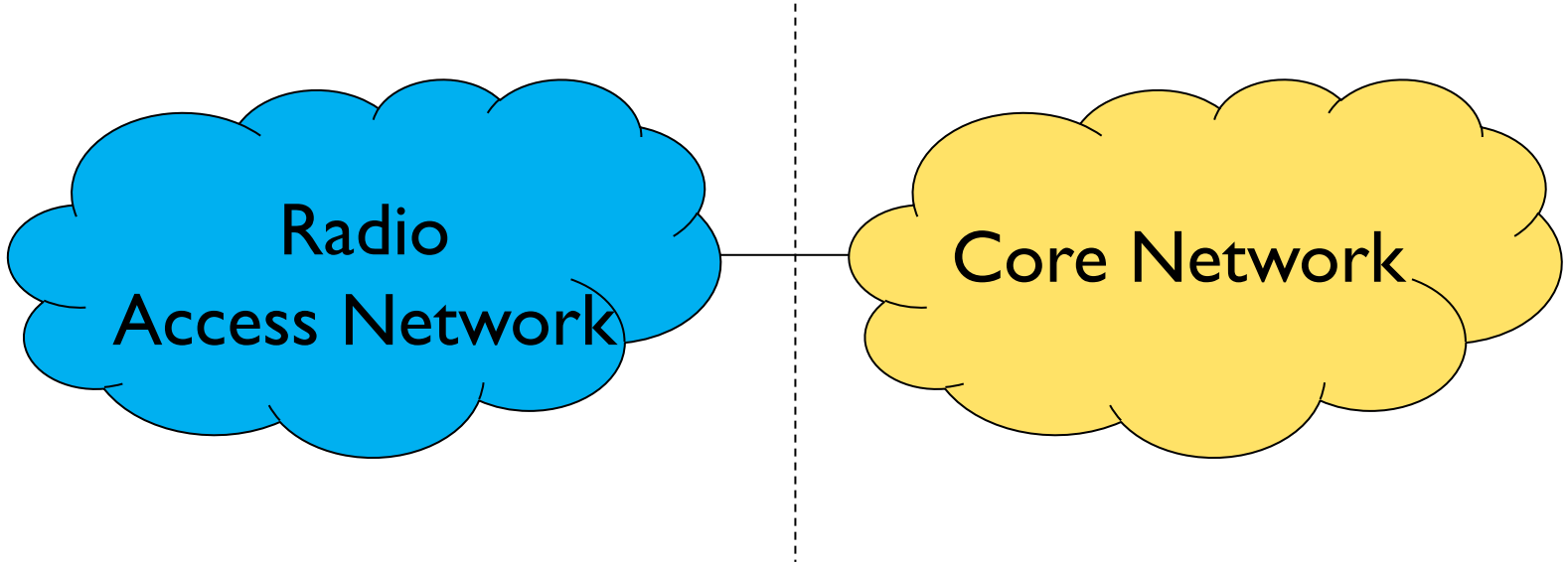


- **User plane**: all the operations related to the transport of user data in DL and UL
- **Control plane**: all operations related to the set-up, control and maintenance of communications between user and network

ACCESS STRATUM

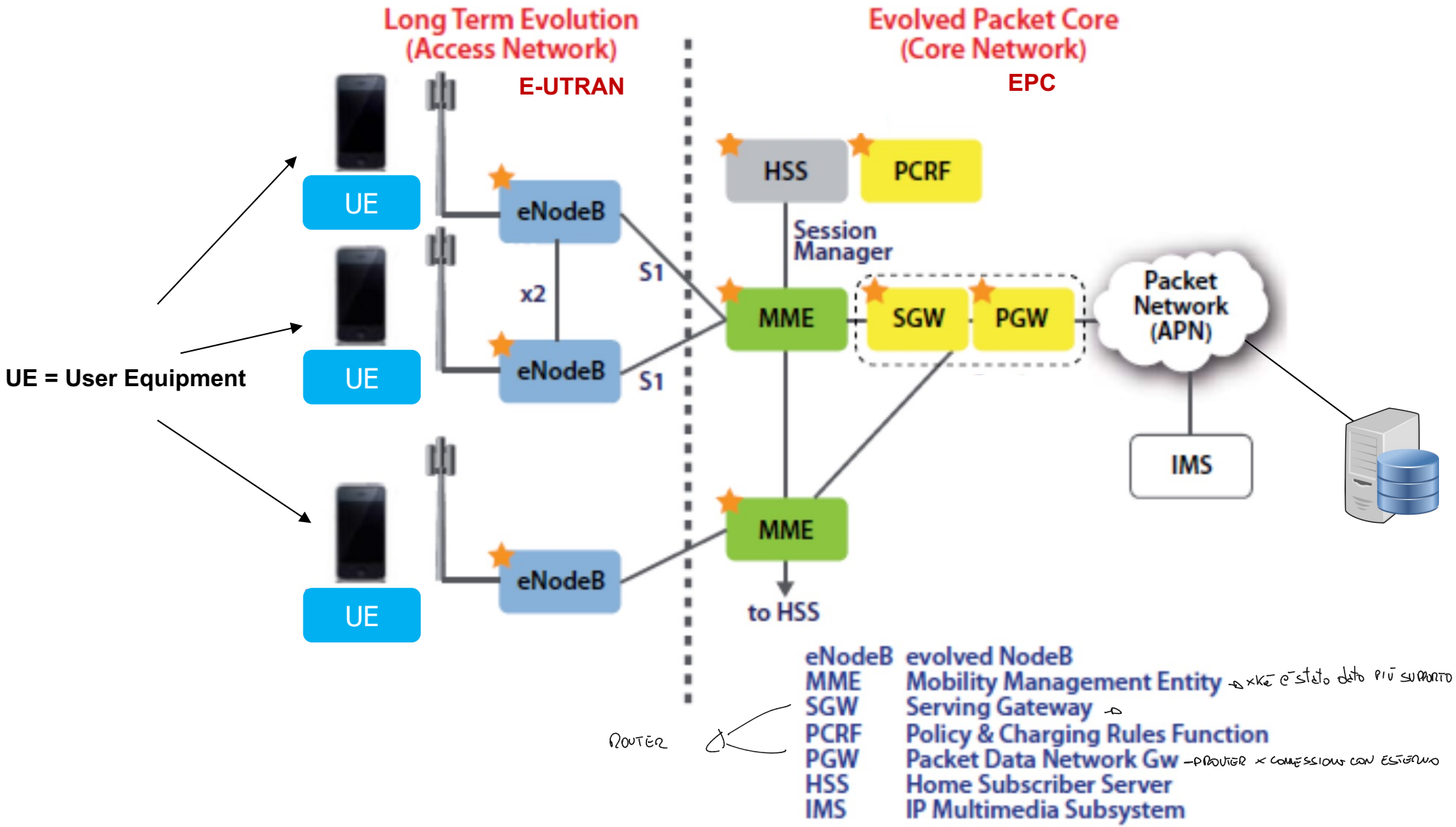
NON ACCESS STRATUM

LTE Architecture



- **Radio Access Network** (RAN): it includes all the devices involved with the direct interaction with user devices
  - In LTE, it is called the E-UTRAN
- **Core Network** (CN): it includes all the devices responsible for the transport of data to/from the Internet or toward other user devices
  - In LTE, it is called EPC

LTE Architecture



EPC – Design Principles

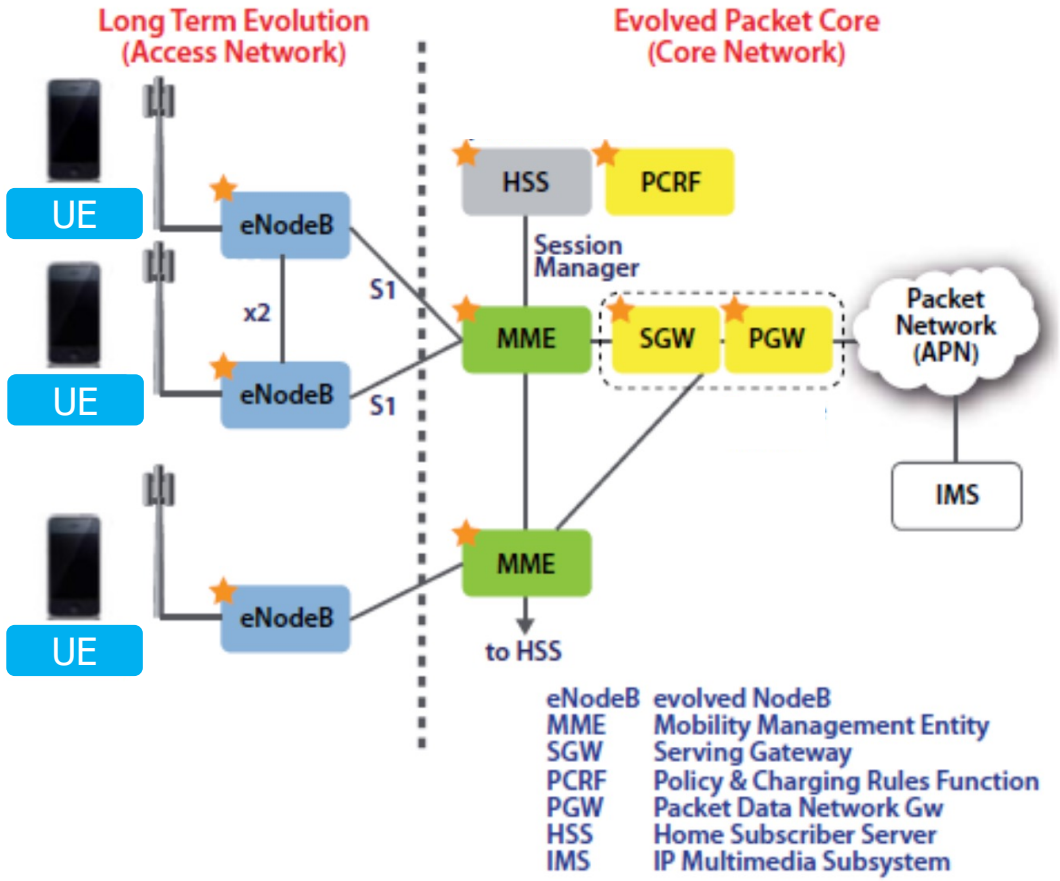
- Clean-slate design
- Packet-switched transport for traffic belonging to all QoS classes including conversational, streaming, real-time, non-real-time, and background
- Radio resource management for: end-to-end QoS, transport for higher layers, load sharing/balancing, policy management/enforcement across different radio access technologies
- Integration with existing 3GPP 2G and ~~3G~~ networks

EPC – Functions

- **Network access control**, including network selection, authentication, authorization, admission control, policy and charging enforcement, and lawful interception
- Packet **routing** and transfer
- **Security**, including ciphering, integrity protection, and network interface physical link protection
- **Mobility management** to keep track of the current location of the UE
- **Radio resource management** to assign, reassign, and release radio resources taking into account single and multi-cell aspects
- **Network management** to support operation and maintenance
- IP networking functions, connections of eNodeBs, E-UTRAN sharing, emergency session support, among others

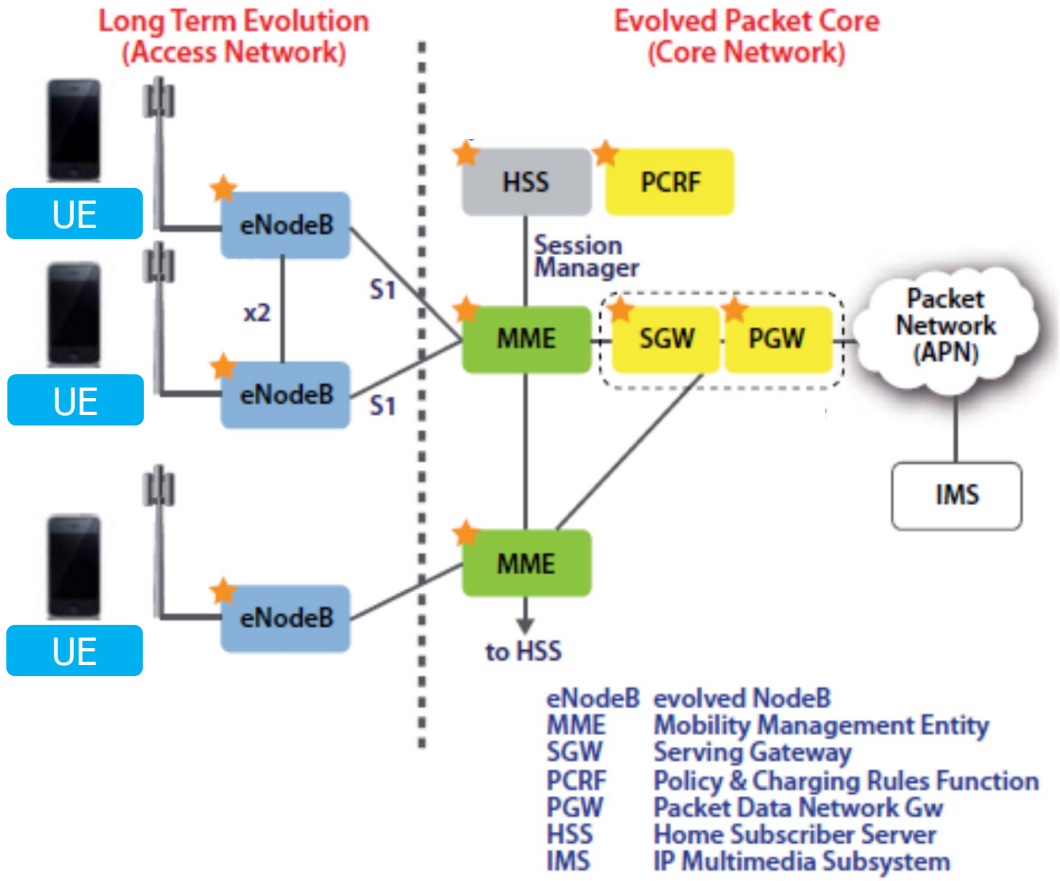
EPC - Components

- Mobility Management Entity (MME) SI OCCUPA DI GESTIRE LA MOBILITÀ
  - Resides in the Control Plane
  - Supports user equipment context, identity, authentication, and authorization
  - Mainly perform Non Access Stratum procedures, consisting of two main groups
    - Functions related to *bearer* management GESTIONE DEI BEARER
      - *Bearer can be seen as a logical communication tunnel*
    - Functions related to connection and mobility management



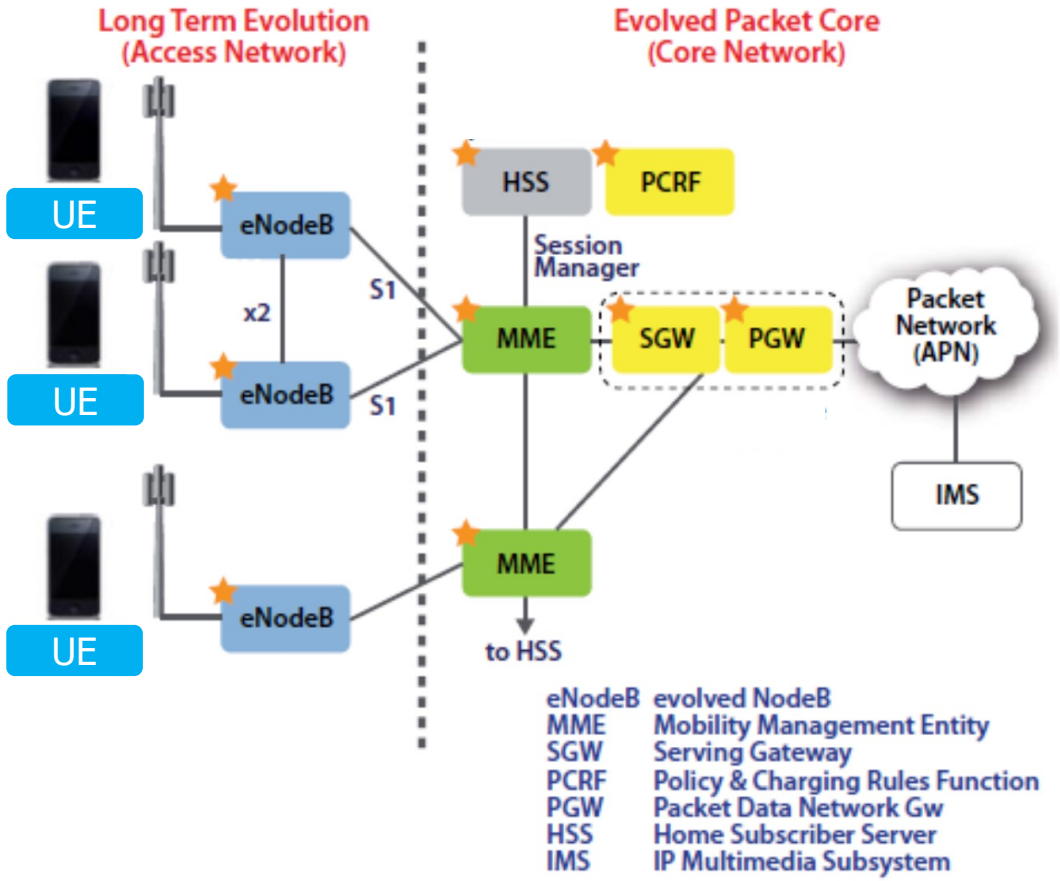
EPC - Components

- Serving Gateway (SGW)
  - Resides in the User Plane
  - Receives and sends packets between the eNodeB and the core network
  - Perform packet routing and forwarding within EPC
  - Anchor point for intra LTE-mobility
  - Lawful intercept



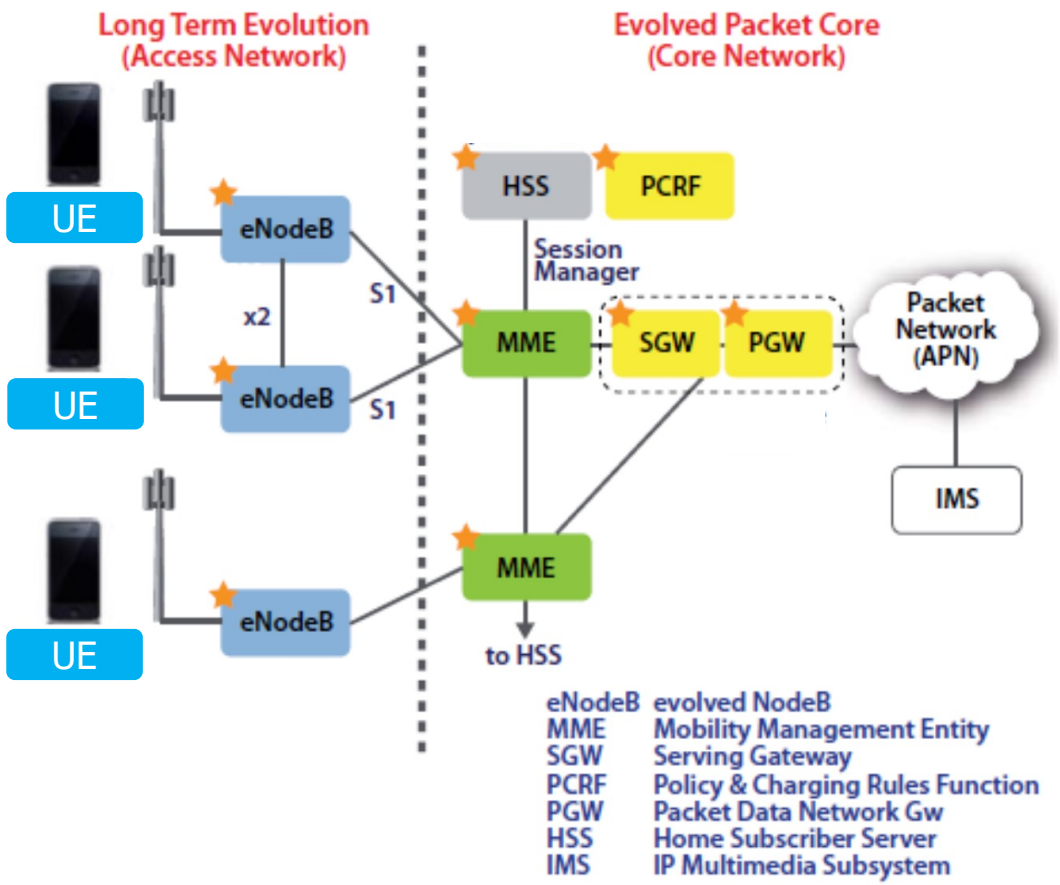
EPC - Components

- Packet Data Network Gateway (PGW)
  - Resides in the User Plane
  - Connects the EPC with external networks/Internet
  - Basically, a router that performs UE IP assignment, per user packet filtering and NAT services LARGE SCALE NAT
  - Anchor point for mobility with non-3GPP access network
  - Lawful intercept



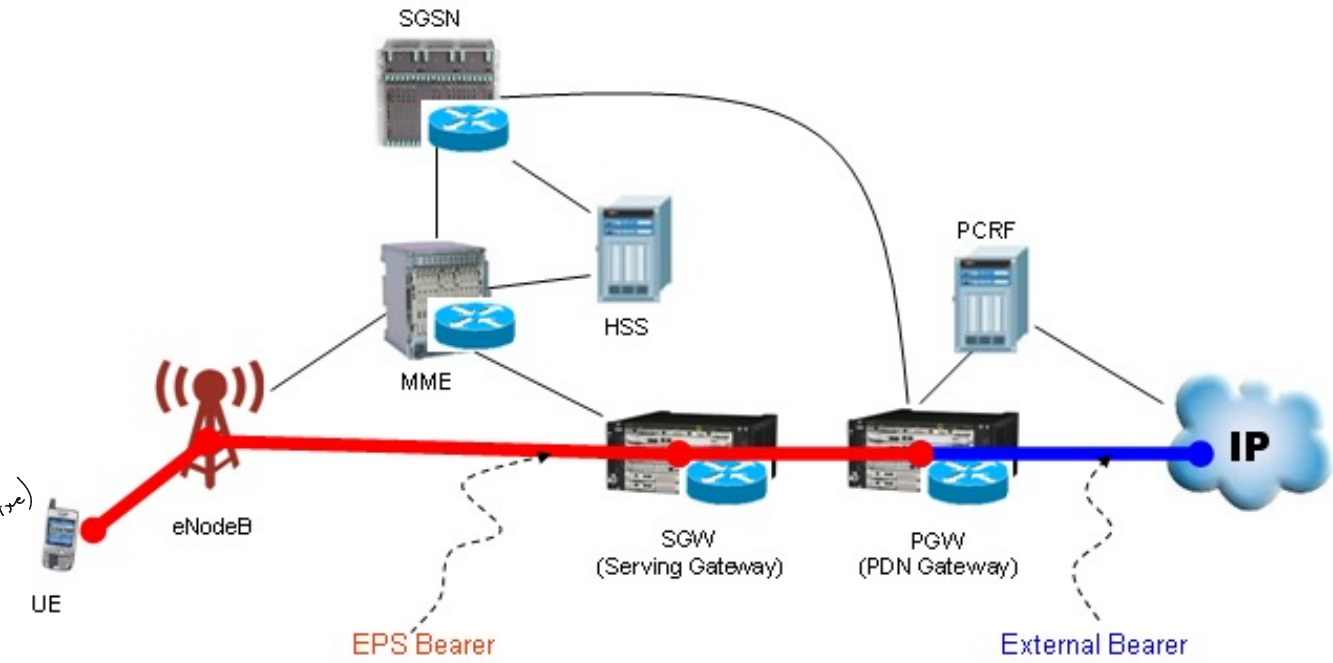
EPC - Components

- Home Subscriber Server (HSS)
  - Database of user-related and subscriber-related information
  - Used for authentication (together with MME) and authorization
  - Similar to HLR in GSM architecture



The LTE Bearers

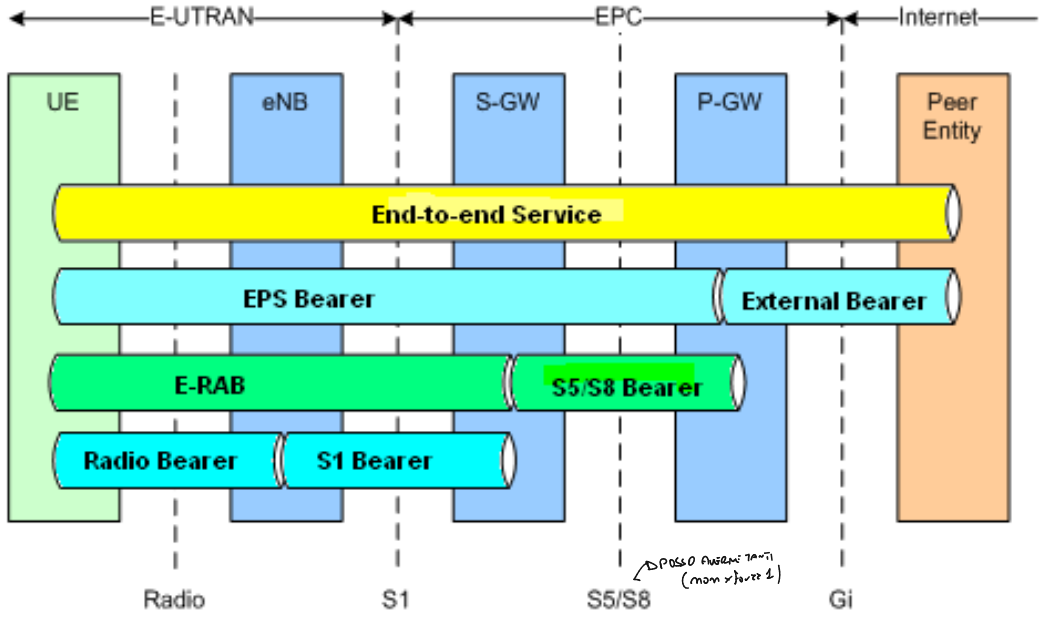
- Think of a *bearer* as a pipe (tunnel) that carries data from the UE to other elements of the LTE architecture (e.g., the P-GW)
- one *default bearer* is established to the P-GW whenever the UE is activated
- the UE can establish other *dedicated bearers* to other networks, based on quality-of-service (QoS) requirements
  - e.g., viewing a streaming video over the Internet can be done over a dedicated bearer
  - dedicated bearers can use a bandwidth guarantee (a guaranteed bit rate, or GBR) tunnel



The LTE Bearers

Se un nodo cambio eNB → devo spostare S1 e S5 bearer senza bisogno di cambiare configura tutto utente

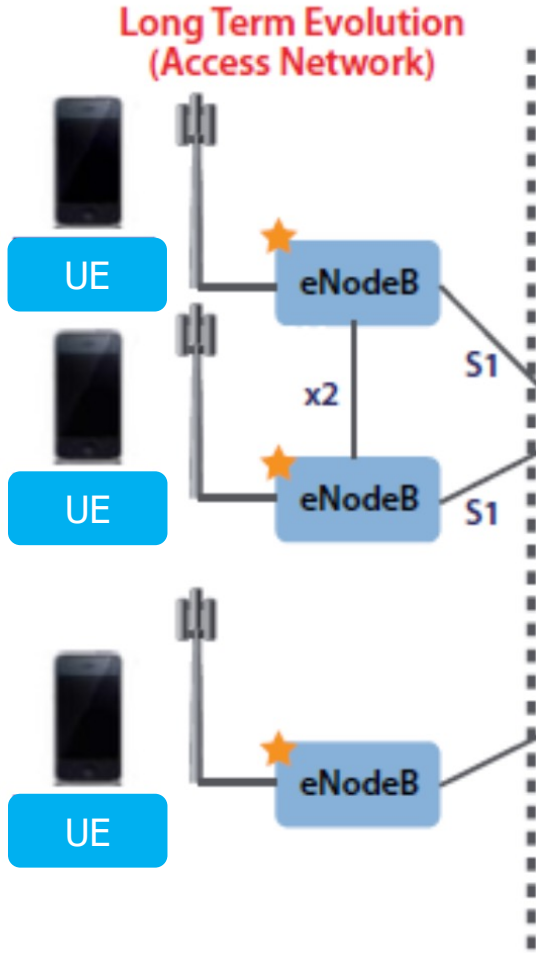
- The bearer is a concatenated tunnel consisting of three portions established in the following order:
  - **The S5 bearer** — connects the Serving Gateway (S-GW) to the P-GW. (The tunnel can extend from P-GW to the Internet)
  - **The S1 bearer**— connects the eNodeB with the S-GW. Handover establishes a new S1 bearer for end-to-end connectivity.
  - **The radio bearer**— connects the UE to the eNodeB. This bearer follows the mobile user under the direction of the MME as the radio network performs handovers when the user moves from one cell to another



E-UTRAN

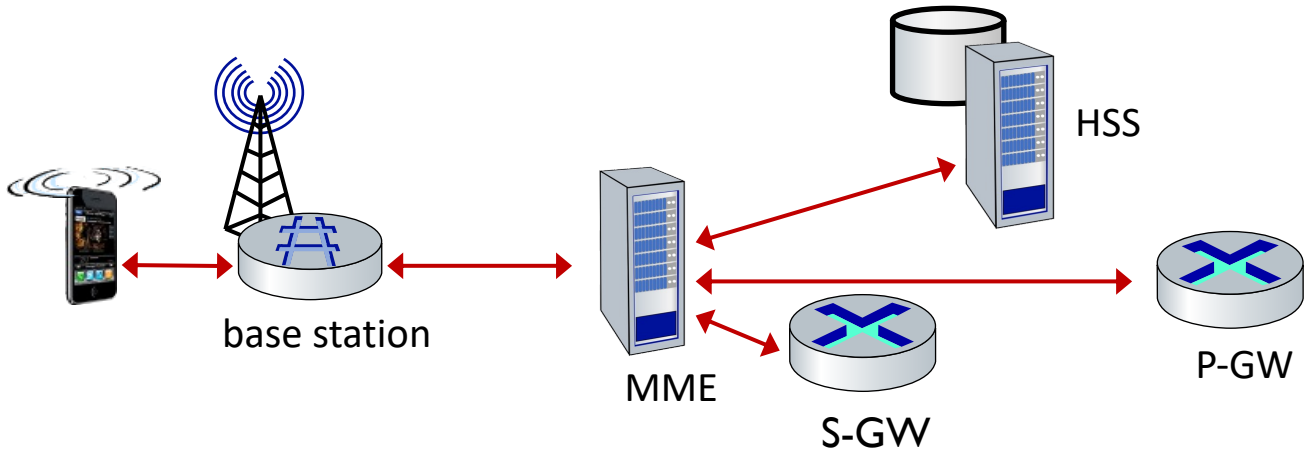
- Mainly consist of eNodeB

- An interface X2 interconnects between eNodeB
  - Consist of two type : X2 control and X2 user
- Main functions
  - Radio resource management: related to the radio bearer such as radio bearer control, radio mobility control, scheduling and dynamic allocation of radio resource at uplink and downlink
  - Header compression
  - Security
  - Connectivity to EPC



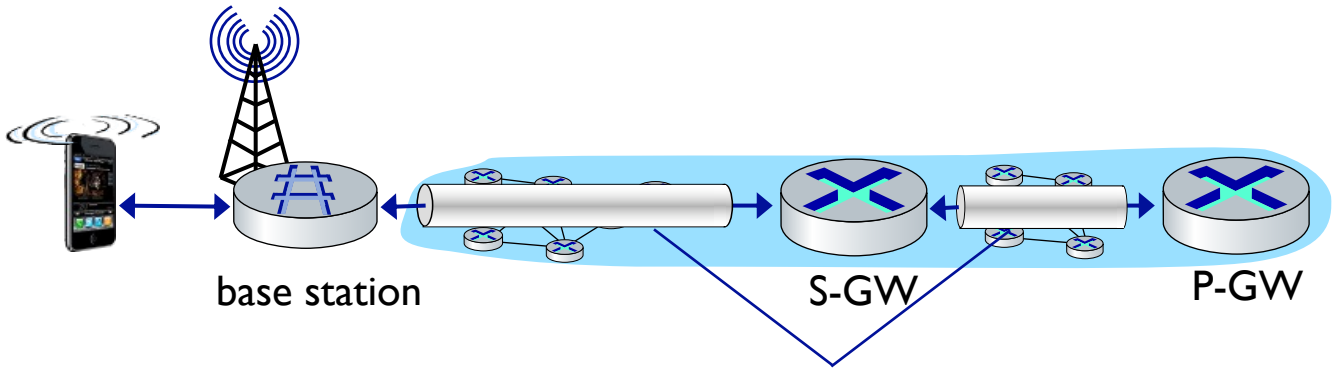
LTE Data Plane/Control Plane

LTE data plane control plane separation



control plane

- new protocols for mobility management , security, authentication (later)

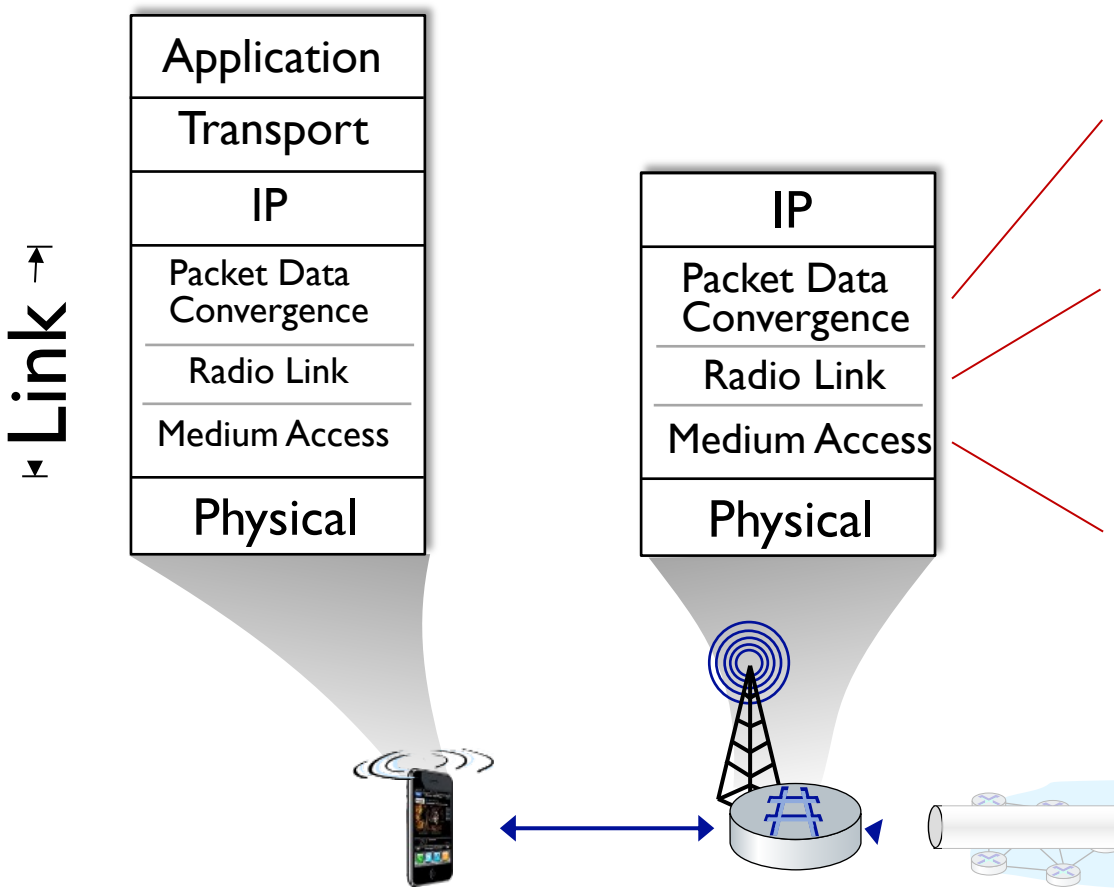


IP tunnels

data plane INSIEME DI TUNNEL CONCATENATI × CREANO UNA CATENA CHE SEMPLIFICA LA D:L CONTROL PLANE

- new protocols at link, physical layers
- extensive use of tunneling to facilitate mobility

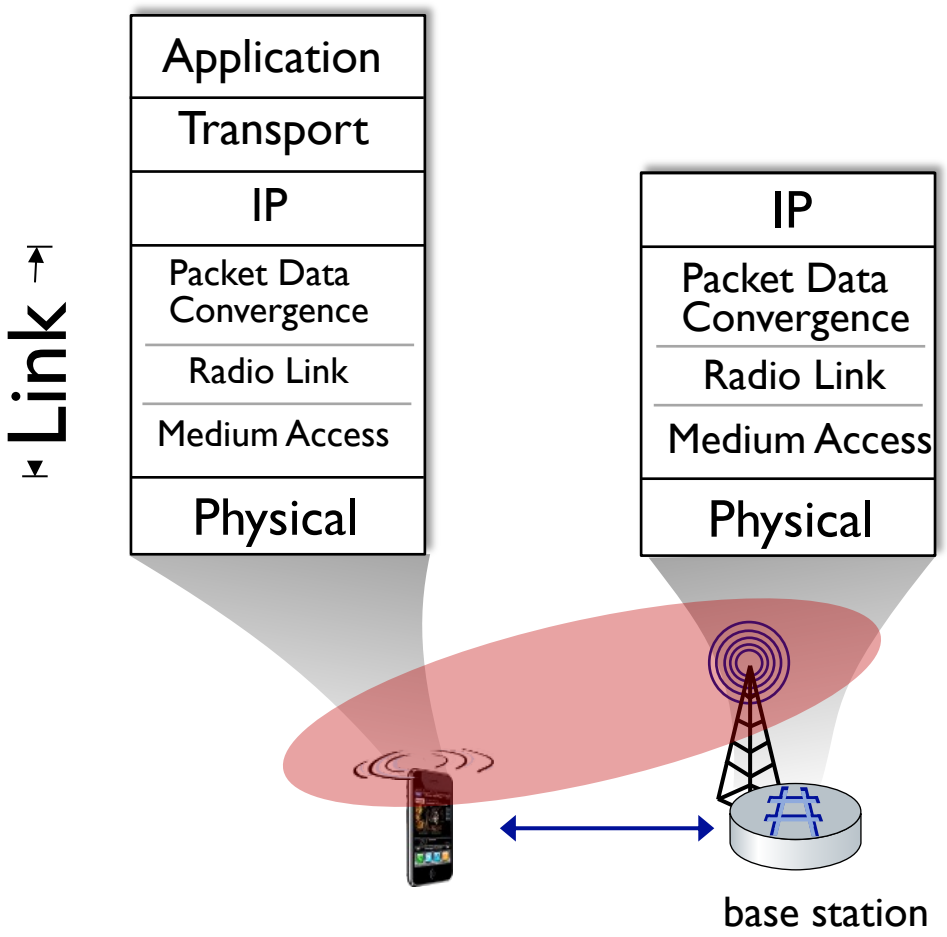
LTE data plane protocol stack: first hop



LTE link layer protocols:

- Packet Data Convergence: header compression, encryption
- Radio Link Control (RLC) Protocol: fragmentation/reassembly, reliable data transfer
- Medium Access: requesting, use of radio transmission slots

LTE data plane protocol stack: first hop



LTE radio access network:

- downstream channel: FDM, TDM within frequency channel (OFDM - orthogonal frequency division multiplexing)
  - "orthogonal": minimal interference between channels
  - upstream: FDM, TDM similar to OFDM
- each active mobile device allocated two or more 0.5 ms time slots over 12 frequencies
  - scheduling algorithm not standardized – up to operator
  - 100's Mbps per device possible

LTE data plane protocol stack: Physical Channels

- Transmitted bits fit into the frame structure according to predefined subdivisions called **Physical Channels**
- Each channel conveys specific information related to: user data, TX/RX parameters, eNB identity, network control etc., as well as to the format of the channel itself (i.e., FDD or TDD)
- Each physical channel is mapped into a portion of the LTE subframe

- Physical channels are divided into Downlink and Uplink Channels
  - Each U/D channel is further divided into Data and Control

LTE Physical Downlink Channels

- Physical Broadcast Channel (PBCH)
  - MIB (Master Information Block) and RACH parameters (Radio Access Channel)
- Physical Control Format Indicator Channel (PCFICH)
  - Details on PDCCH format (e.g., number of symbols used)
- Physical Hybrid ARQ Indicator Channel (PHICH)
  - Ack/Nack to uplink frame transmission
- Physical Downlink Control Channel (PDCCH)
  - Downlink resource scheduling
  - Uplink power control instructions
  - Uplink resource grant
  - Indication for paging or system information
- Physical Downlink Shared Channel (PDSCH)
  - User data and SIB (System Information Block) for cell information

control

data

LTE Physical Uplink Channels (control)

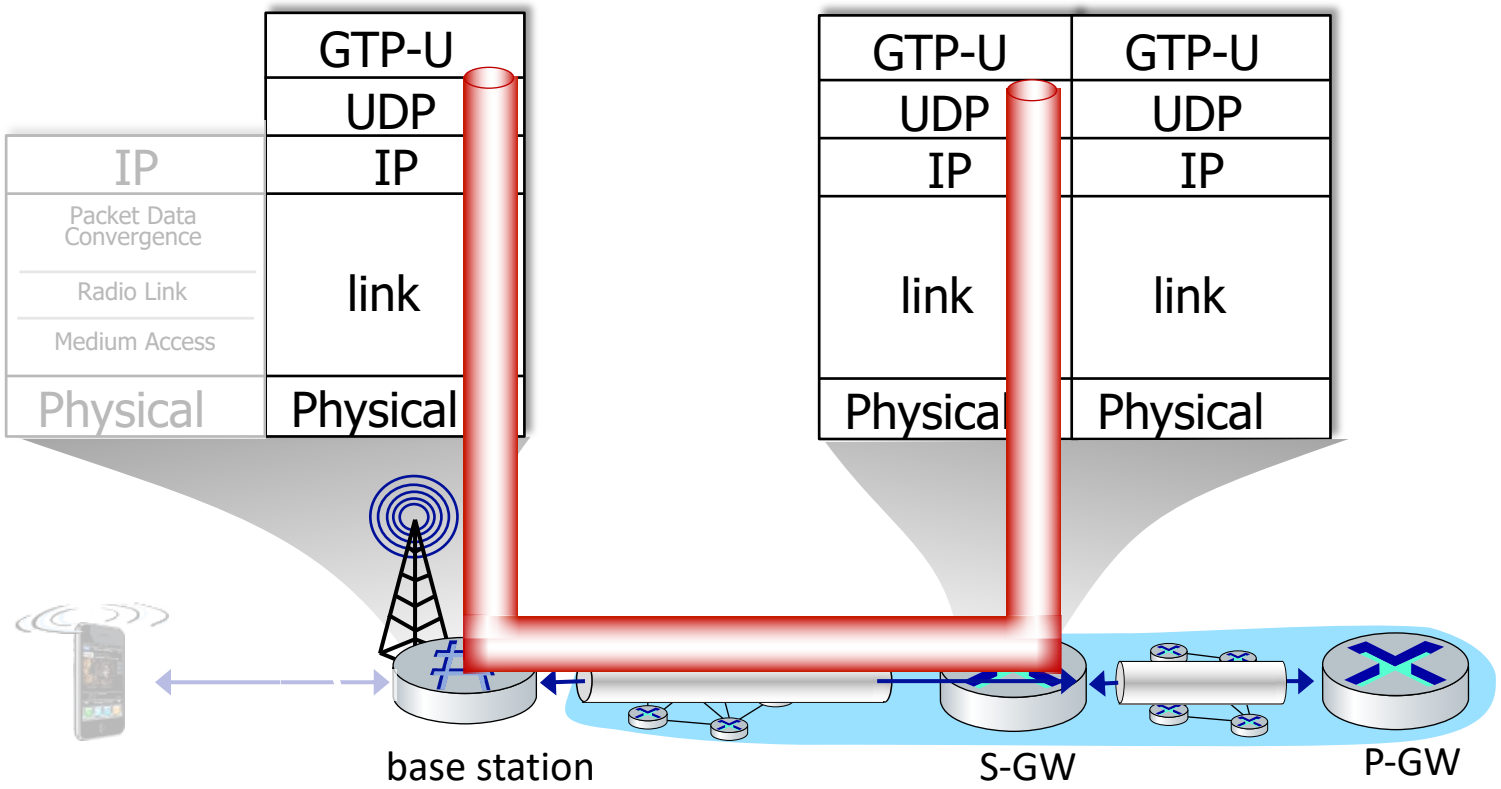
- Physical Random Access Channel (PRACH)
  - It carries the random access preamble a UE sends to access the network in non-synchronized mode
  - used to allow the UE to synchronize timing with the eNodeB

- Physical Uplink Control Channel (PUCCH)
  - Signaling includes HARQ ACK/NACK, channel quality indicators (CQI), MIMO feedback
    and scheduling requests for uplink transmission

LTE Physical Uplink Channels (data)

- Physical Uplink Shared Channel (PUSCH)
  - It carries user data
  - The uplink scheduling TTI is 1 ms; it is possible to 'bundle' a group of 4 TTIs to improve performance at cell edge and reduce higher-layer protocol overhead

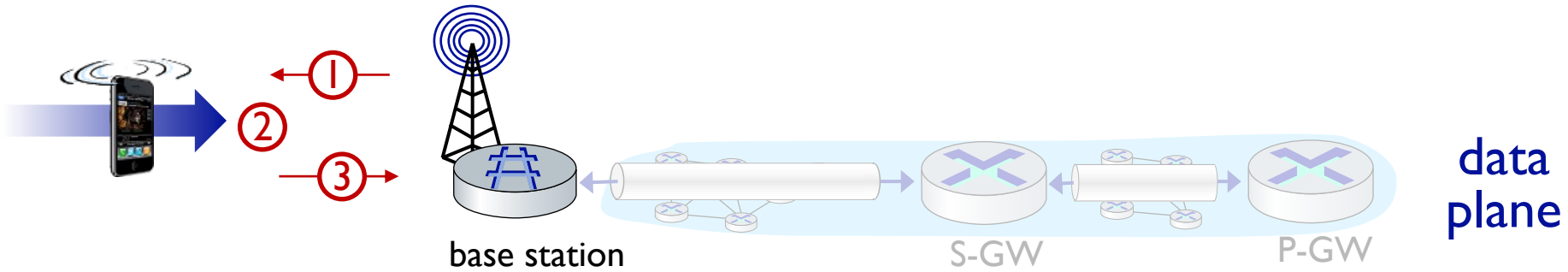
LTE data plane protocol stack: packet core



tunneling:

- mobile datagram encapsulated using GPRS Tunneling Protocol (GTP), sent inside UDP datagram to S-GW
- S-GW re-tunnels datagrams to P-GW
- supporting mobility: only tunneling endpoints change when mobile user moves

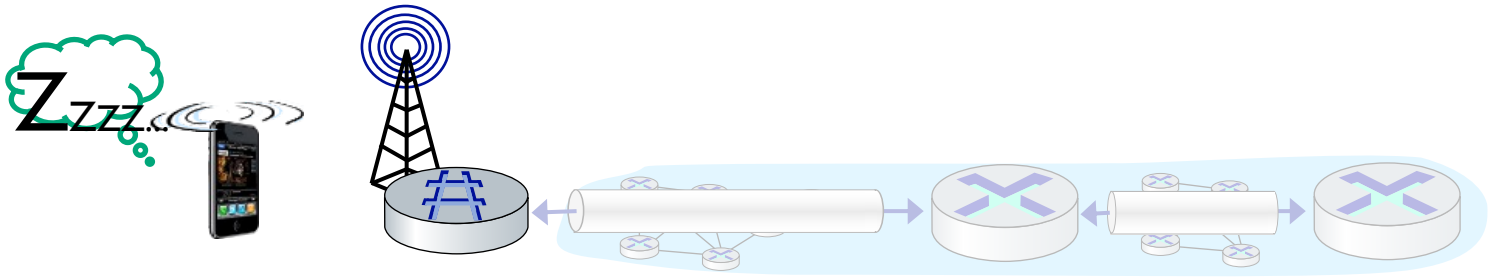
LTE data plane: associating with a BS



1. BS broadcasts primary synch signal every 5 ms on all frequencies (SERVE SOLO X AGGANCIO, NON CONTIENE INFORMAZIONI)
   - BSs from multiple carriers may be broadcasting synch signals
2. mobile finds a primary synch signal, then locates 2nd synch signal on this freq.
   - mobile then finds info broadcast by BS: channel bandwidth, configurations; BS's cellular carrier info
   - mobile may get info from multiple base stations, multiple cellular networks
3. mobile selects which BS to associate with (e.g., preference for home carrier)
4. more steps still needed to authenticate, establish state, set up data plane

BISOGNA INTERAGIRE CON HSS PER AUTENTICARSI

LTE mobiles: sleep modes



as in WiFi, Bluetooth: LTE mobile may put radio to "sleep" to conserve battery:

- light sleep: after 100's msec of inactivity
  - wake up periodically (100's msec) to check for downstream transmissions
- deep sleep: after 5-10 secs of inactivity
  - mobile may change cells while deep sleeping – need to re-establish association

5G Networks

5G objectives

- 5G will meet the requirements of a highly mobile, fully connected society.
  - proliferation of connected objects and devices
  - wide range of new services and associated business models
  - automation in various industry sectors and vertical markets (e.g. energy, e-health, smart city, connected cars, industrial manufacturing, etc.).
  - more pervasive human centric applications, e.g., virtual and augmented reality augmentation, 4k video streaming, etc.
- 5G networks will support the coexistence of
  - human-centric
  - machine type applications
- 5G networks will have to support very diverse functional and KPI/performance requirements

5G Key Requirement

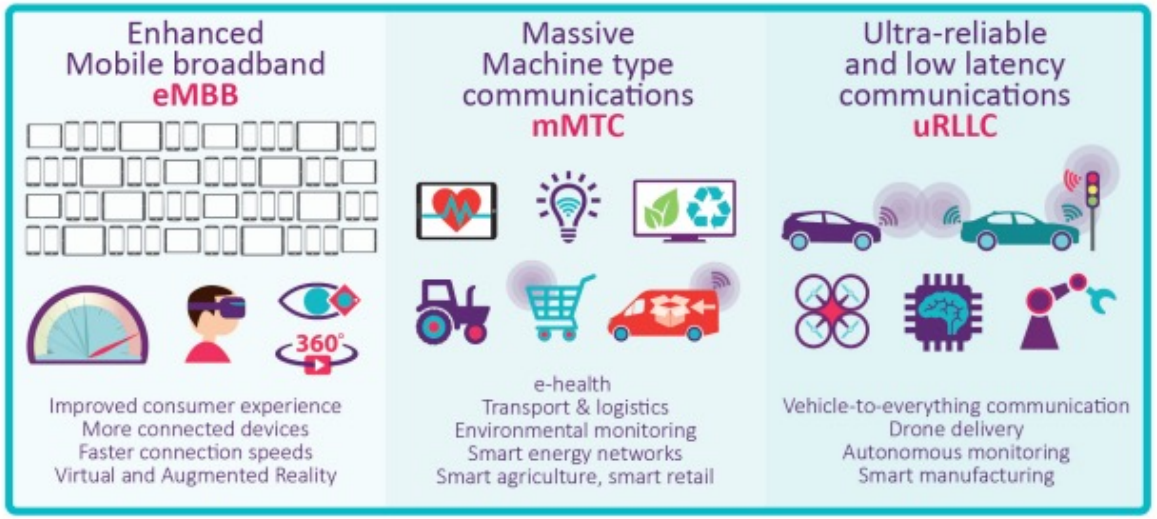
Unlike previous generations of mobile networks, 5G will require not only improved networking solutions but also a sophisticated integration of massive computing and storage infrastructures.

5G Ecosystem

- Operators will have to deploy **orchestrator functions** that will allocate appropriate computing and logical network resources to services
- These logical networks, called **network slices**, will contain specialized networking and computing functions that meet the desired performance of the service providers
- 5G networks will support **cross-domain orchestration** of services and resources over multiple administrative domains (multiple operators) allowing flexible sharing schemes
- The implementation of these schemes will also require interworking among operators in the network function layer as well (e.g., setting up SDN rules).

5G use cases

- Enhanced Mobile Broadband (eMBB)
- Massive Machine Type Communication (mMTC)
- Ultra-Reliable Low-Latency Communication (URLLC)



5G technologies in the Radio Access

Advanced waveforms

- Alternatives to pure OFDM such as RBF-OFDM, FBMC, GFDM, and UFMC

Advanced MIMO

- Both co- located and distributed architectures are envisaged, with co-located massive MIMO particularly appealing to high frequency bands

Millimeter Wave

- Millimeter Wave spectrum (20-80GHz) offers large chunks (up to 2GHz) of contiguous bandwidth, for ultra-high throughput and low latency scenarios.

5G technologies in the Core Network

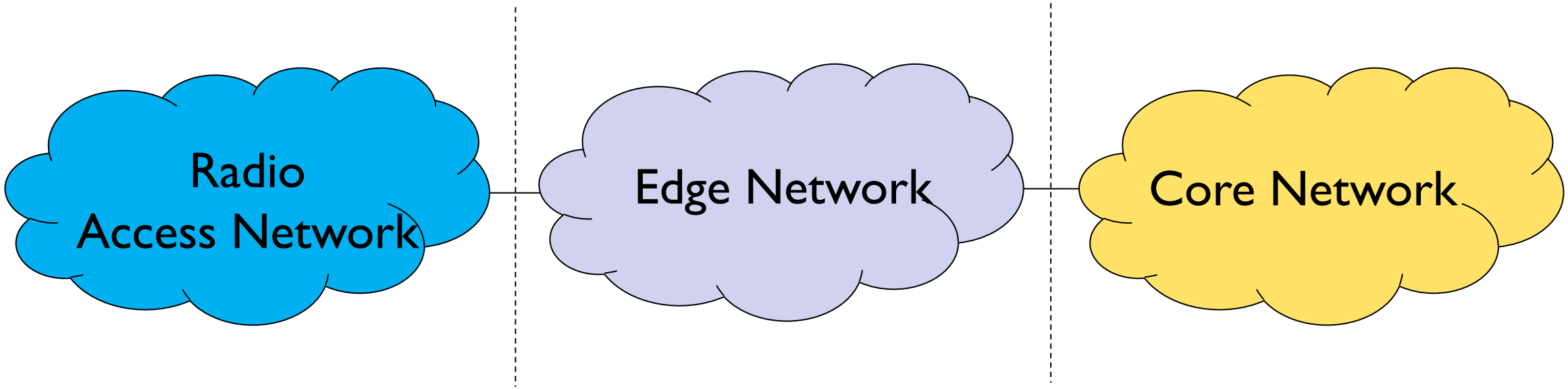
Software Defined Networking

Network Function Virtualization

SDN/NFV Orchestration

- SDN is an approach to networking in which routing control is *centralized* and decoupled from the physical infrastructure (data plane), which is *distributed*.
- NFV moves network services (firewall, load balancing, access control) from hardware to software, creating *virtual building blocks* that can be easily connected (NFV chaining)
- Aka. the new *network operating system*: it manages function lifecycle, resources, policies and it provides system analytics

5G Architecture



- **Radio Access Network** (RAN): it includes all the devices involved with the direct interaction with user devices
  - In 5G, base stations are called gNodeB
- **Edge Network** (MEC): it hosts computing and storage elements for local services
- **Core Network** (CN): it includes all the devices responsible for the transport of data to/from the Internet or toward other user devices

Main differences between 4G and 5G networks

- Nomenclature
  - Radio Interface E-UTRA –> New Radio (NR)
  - Radio access network: E-UTRAN –> 5G-RAN
  - Core Network: EPC -> 5GC

- Data and Control Plane split
  - LTE -> have a bit mixed CP and UP functions between different network nodes;
  - In 5G -> full CP/UP split

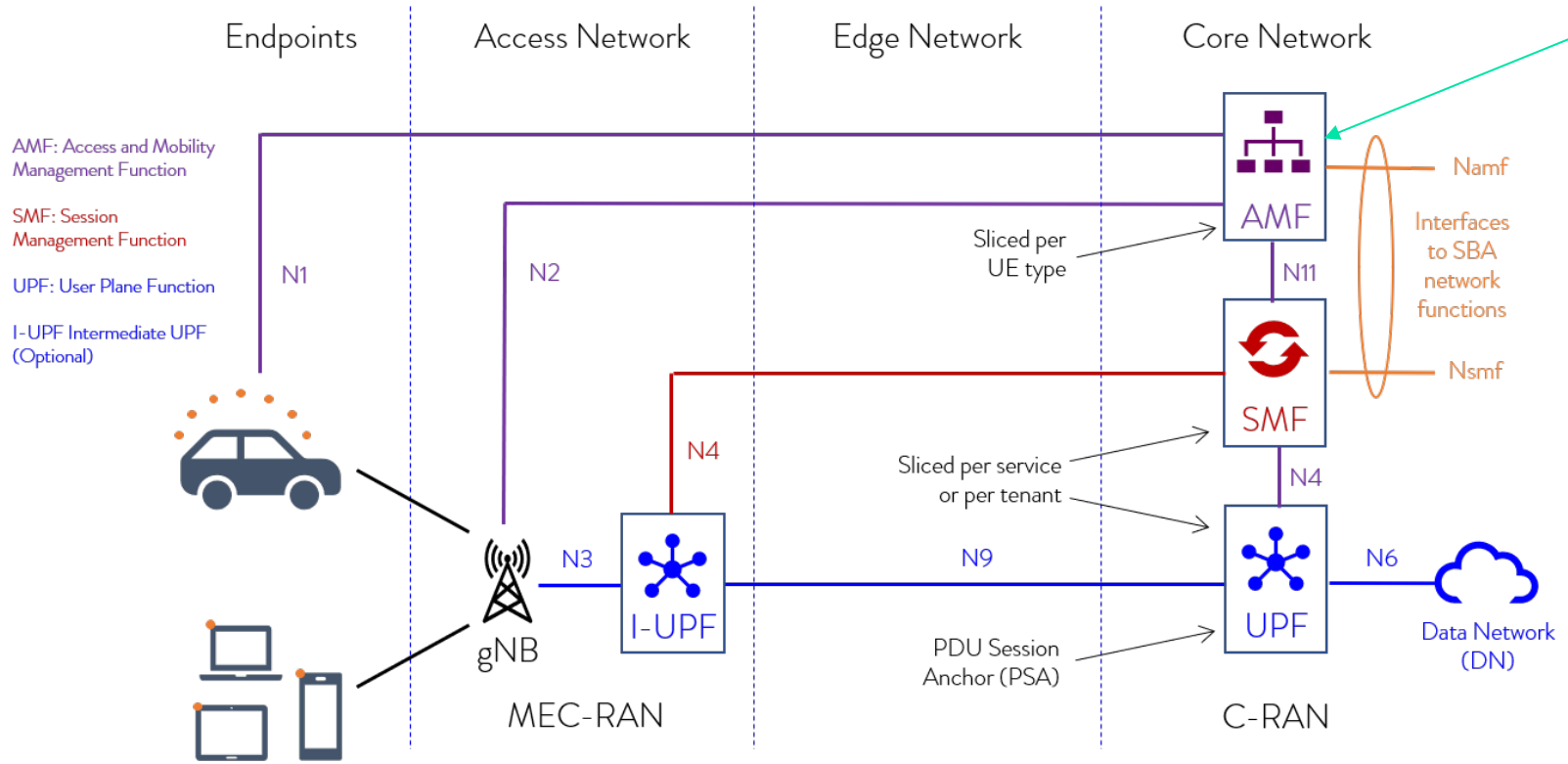
- Brand-new functionalities
  - network slicing implying different configurations of RAN
  - new QoS framework with flows instead of end-to-end bearers
  - new approach to 5GC using Service Based Architecture (SBA) concept

5G CORE NETWORK

5G Service Based Architecture (SBA)

AMF=Access & mobility Management Function

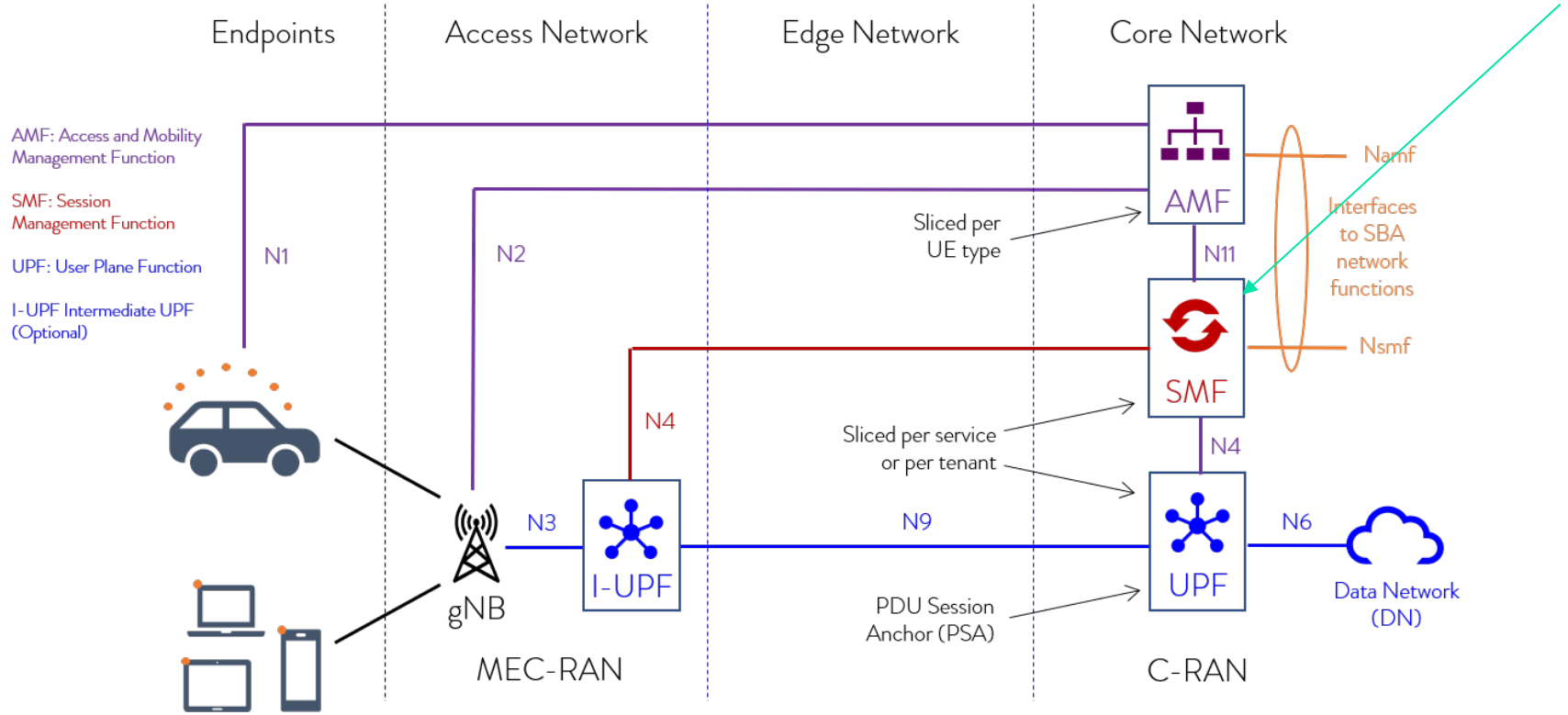
5G evolution of MME



5G Service Based Architecture (SBA)

SMF=Session Management Function

5G evolution of control plane of SGW and PGW

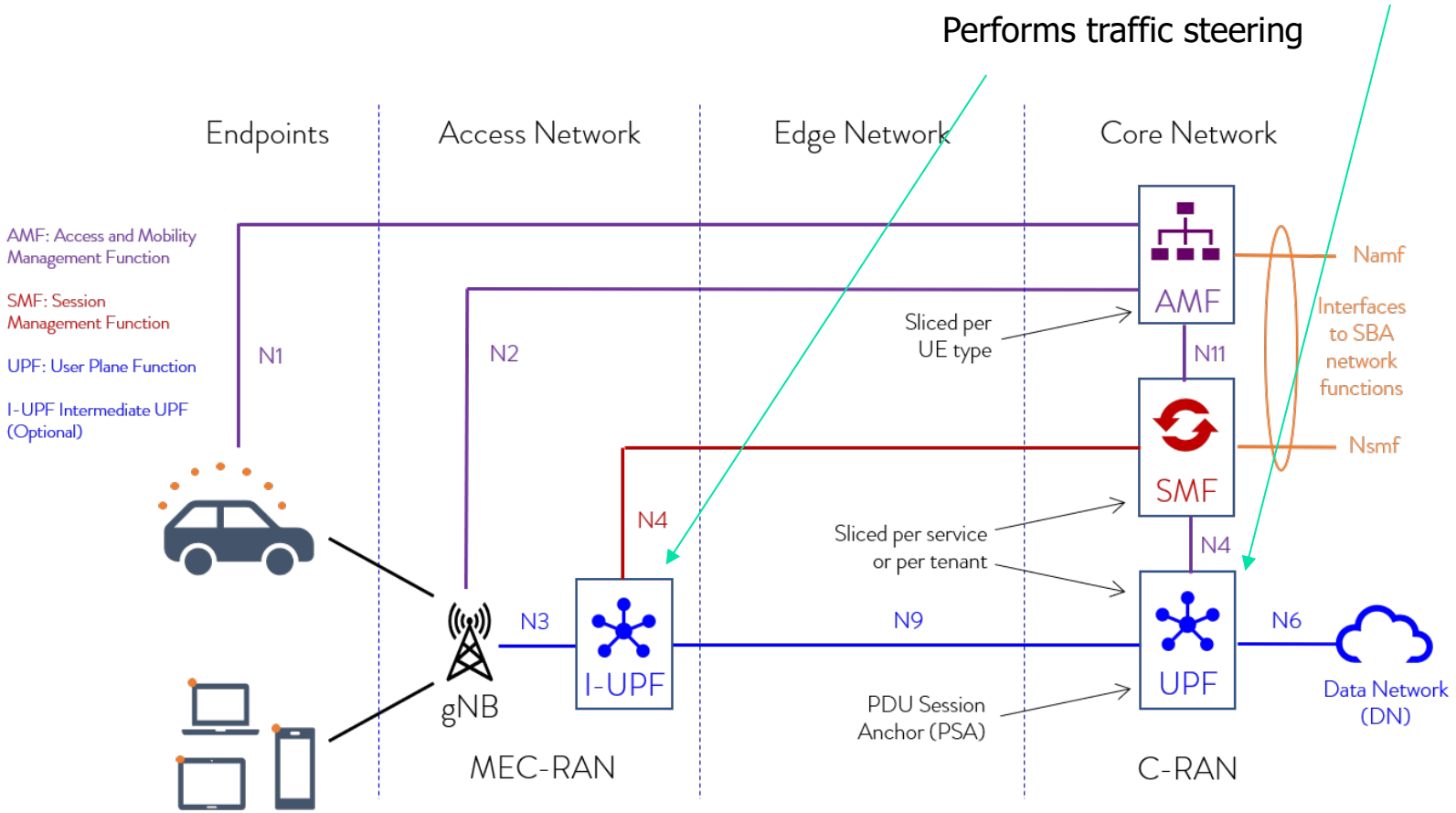


5G Service Based Architecture (SBA)

UPF=User Plane Function

5G evolution of data plane

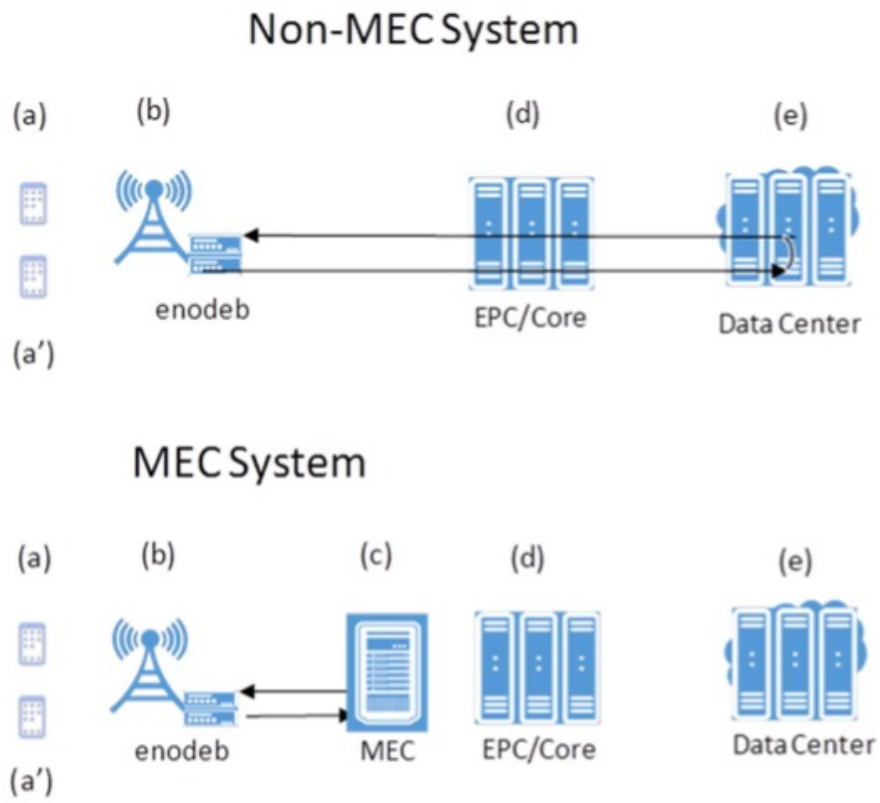
Performs traffic steering



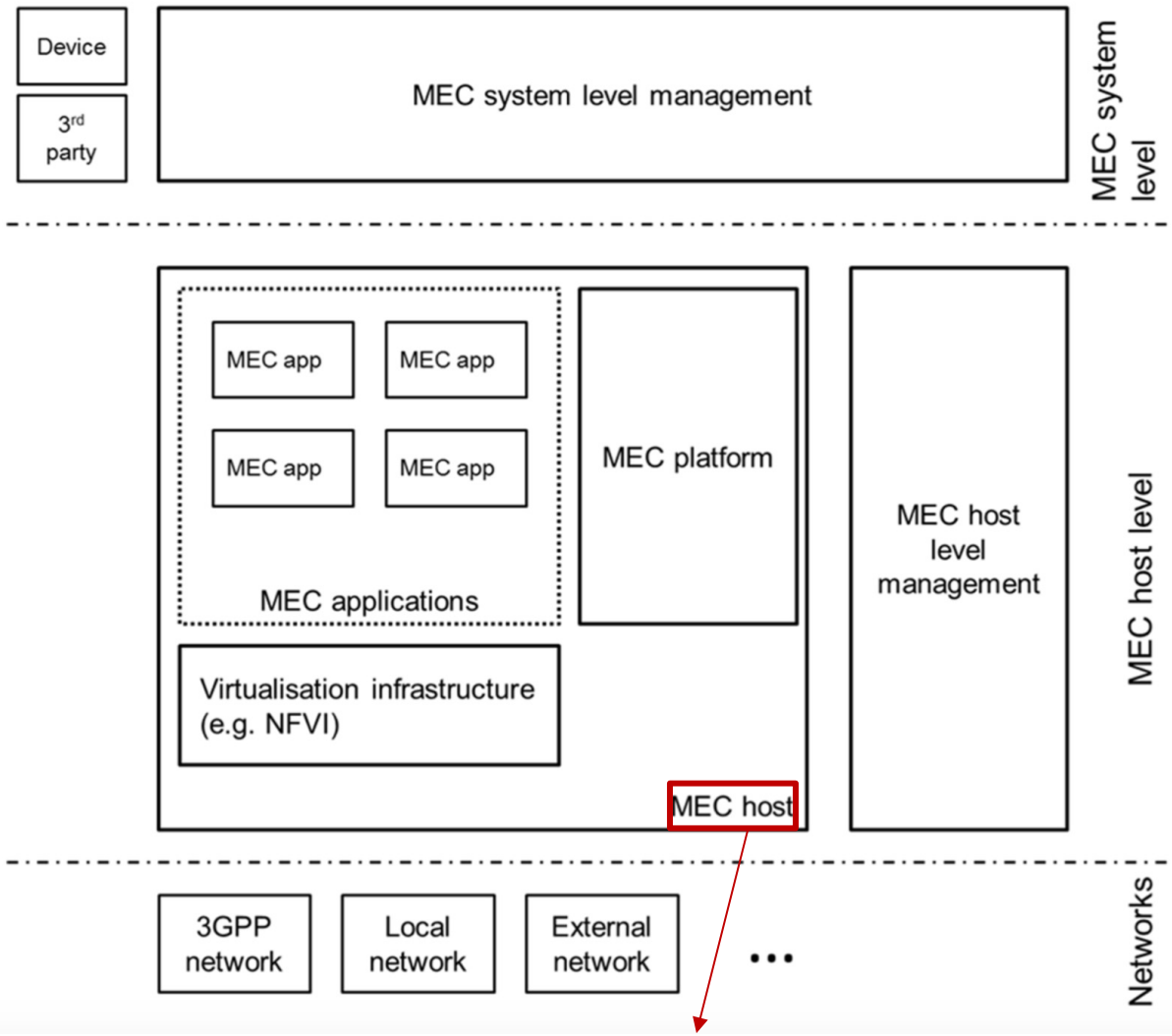
5G EDGE NETWORK

Multiaccess Edge Computing

- Edge Network infrastructure providing IT service environment and cloud-computing capabilities at the edge of the mobile network, in close proximity to mobile subscribers
- Standardization begun in 2014 («Mobile Edge Computing»)
  - First set of specifications published in 2017
- Expected benefits:
  - ultra-low latency
  - high bandwidth
  - real-time access to radio network
  - contextual information
  - location awareness
  - flexible and extendable framework for services

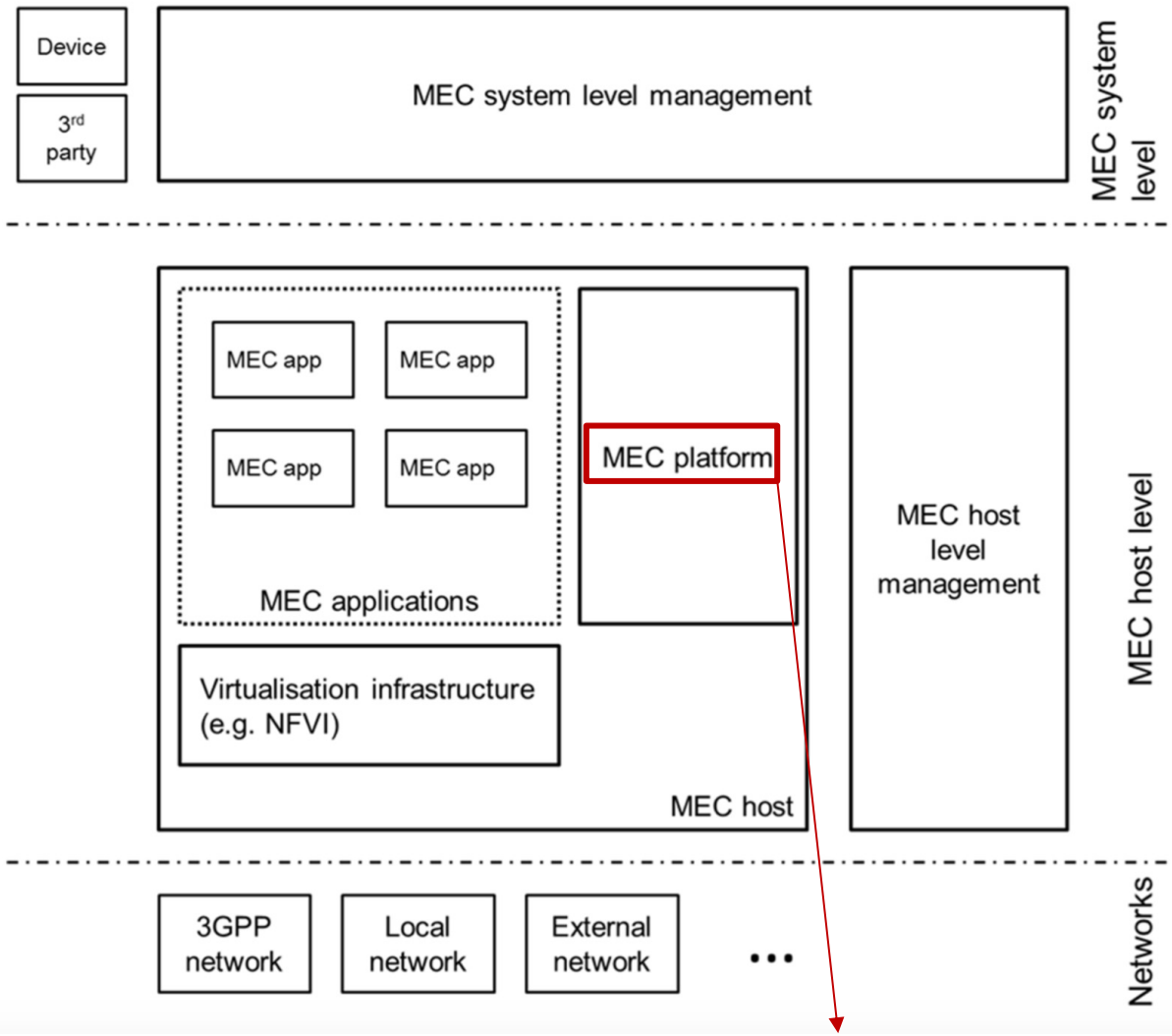


MEC Architecture



MAC host contains the MEC platform and a virtualization infrastructure which provides compute, storage, and network resources for the MEC applications.

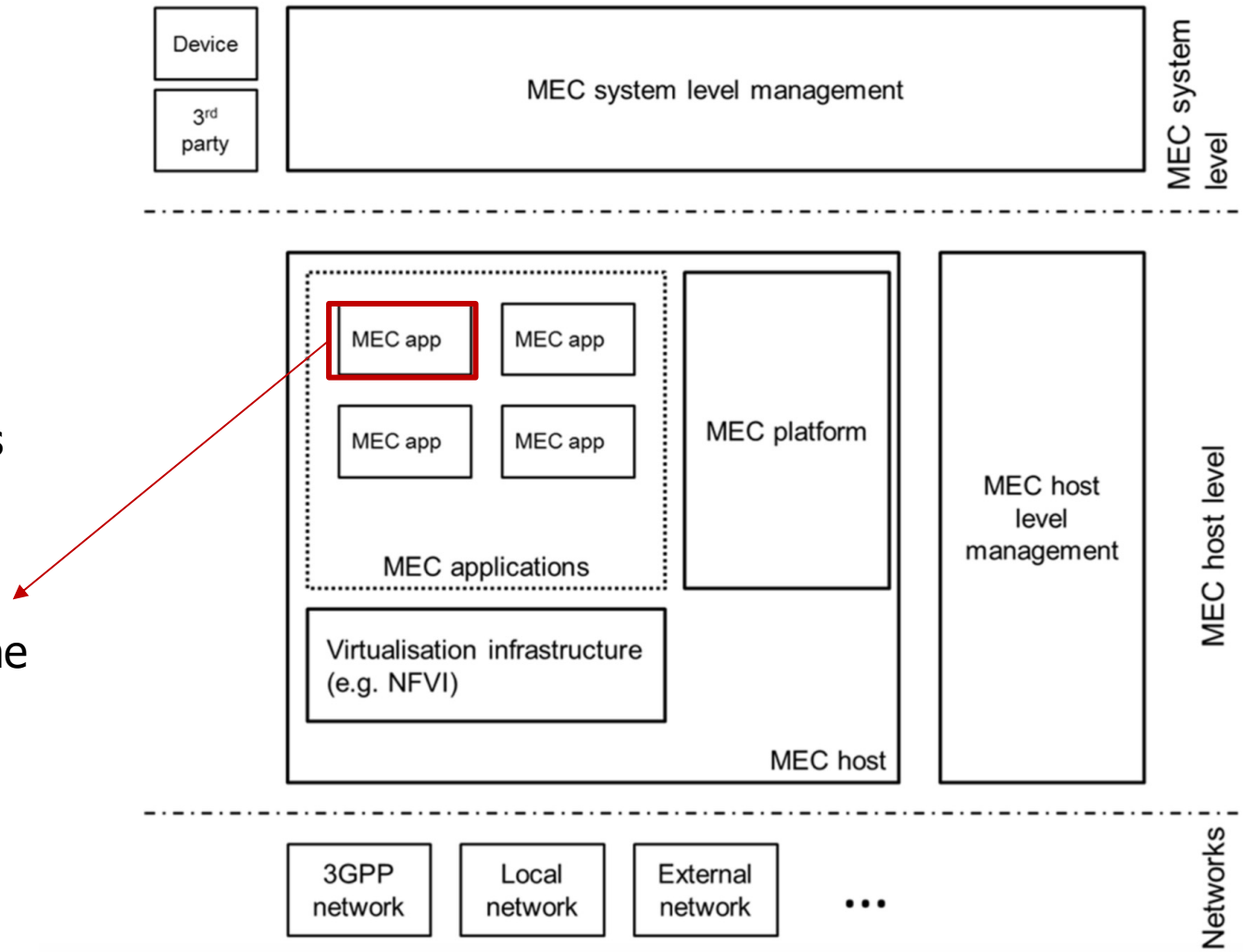
MEC Architecture



The MAC platform offers an environment where the MEC applications can discover, advertise, consume and offer MEC services

MEC Architecture

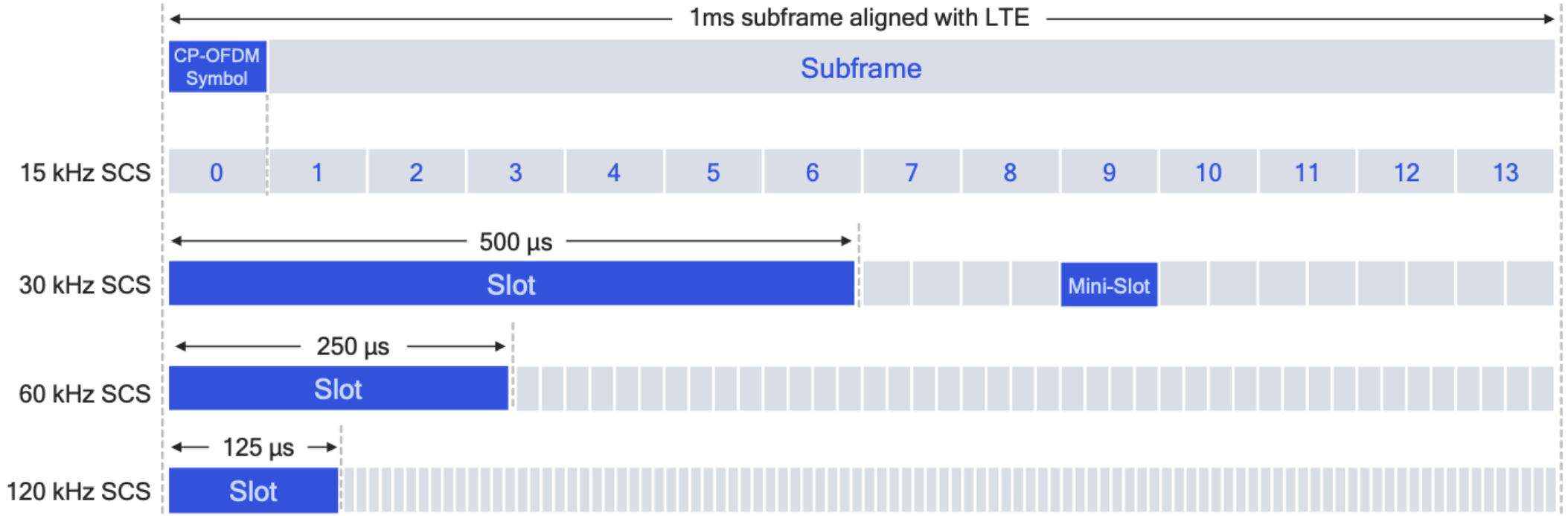
MEC applications are running as virtual machines (VM) on top of the virtualization infrastructure provided by the MEC host, and can interact with the MEC platform to consume and provide MEC services



5G RADIO ACCESS NETWORK

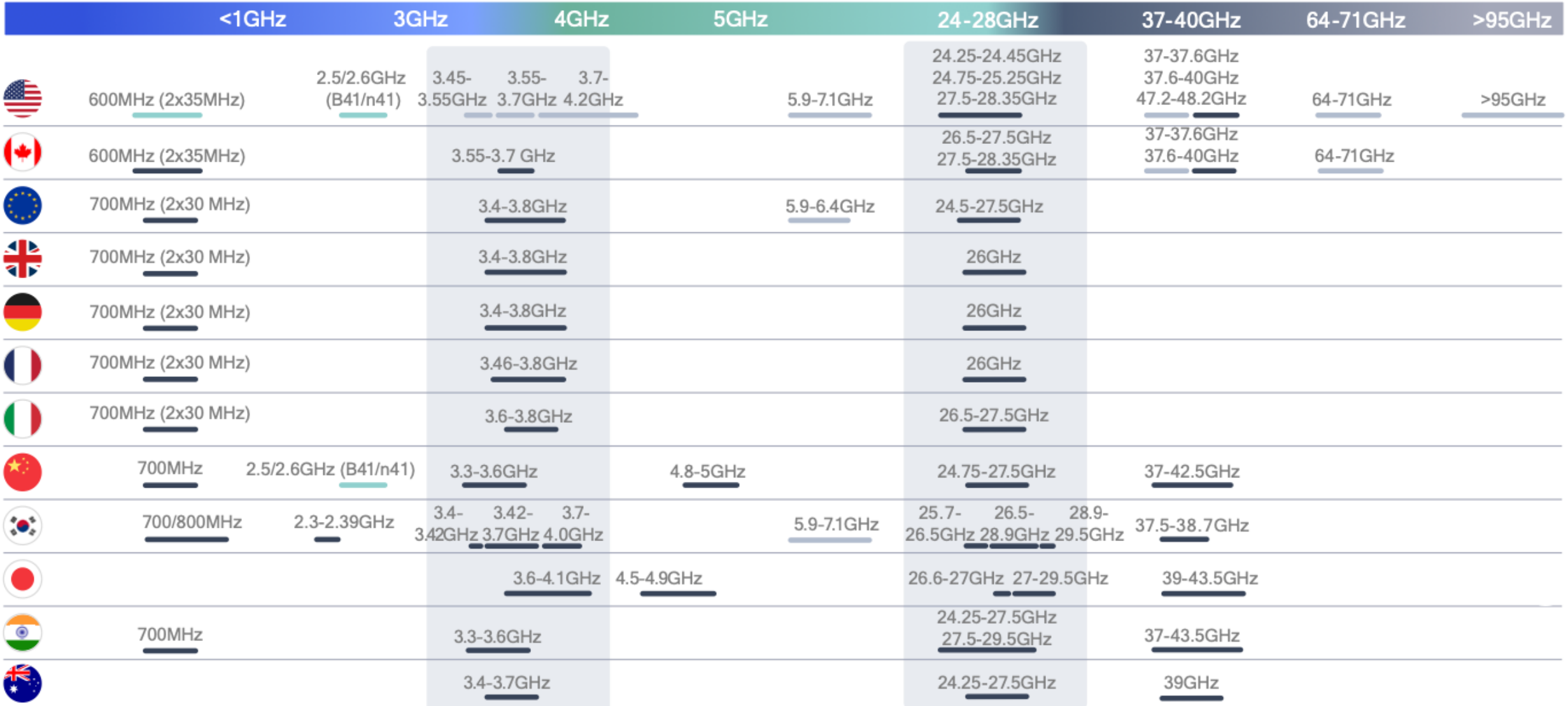
5G New Radio - Overview

- Flexible slot-based framework
  - Variable number of slots per subframe
  - Transmissions can start in any part of the slot
- Different subcarrier spacing ("numerology"): shorter slots for higher spacing
- Supports slot aggregation for data-heavy transmissions



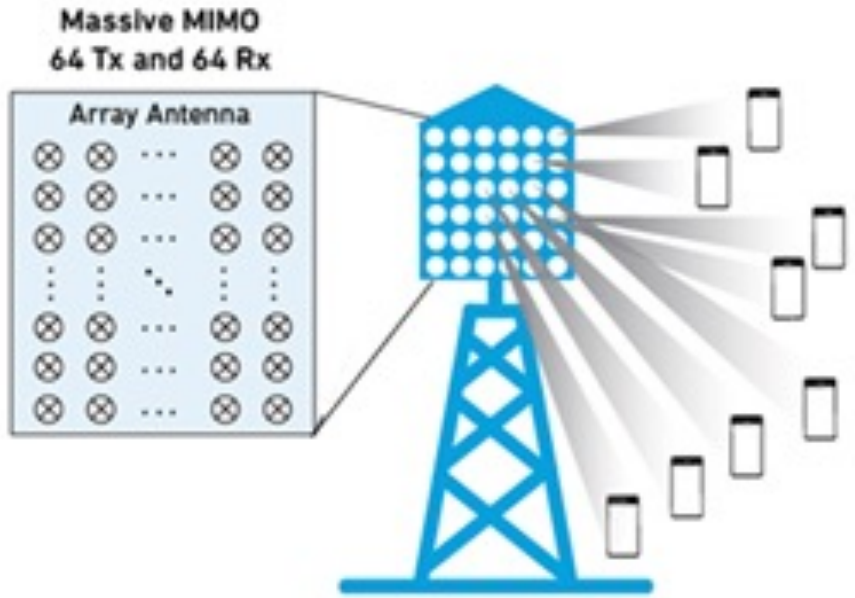
Source: Qualcomm

5G New Radio – Frequency bands



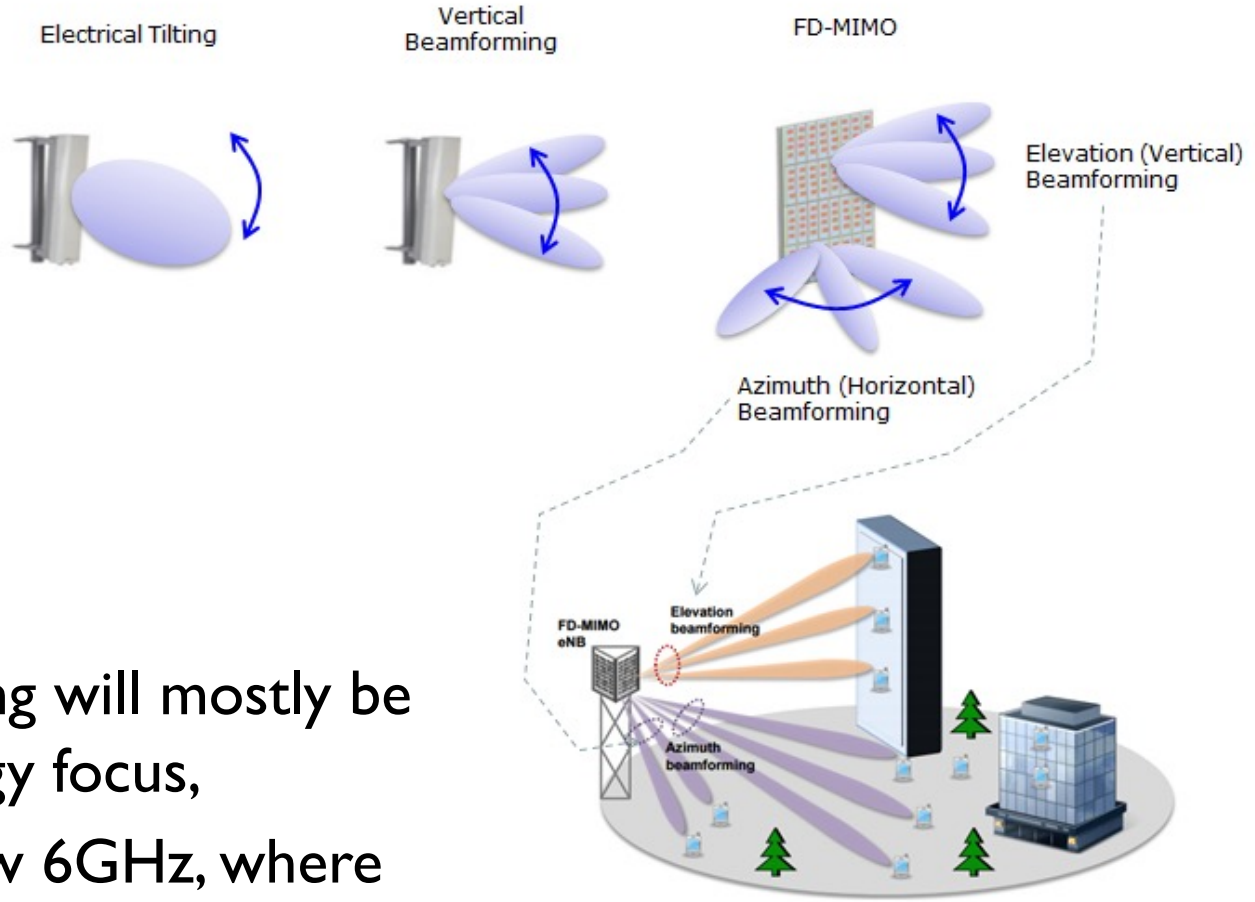
5G New Radio – Massive MIMO

- MIMO (Multiple Input Multiple Output): both the base station and UE have multiple antenna ports and antennas, and multiple data streams are transmitted simultaneously to the UE using same time/frequency resources, doubling (2×2 MIMO), or quadrupling (4×4 MIMO) the peak throughput of a single user
- Massive MIMO (mMIMO) is a system where the number of antennas exceeds the number of users
- Although not part of the first release, 5G NR will support distributed-MIMO, where a user can receive different parts of the same data stream from multiple sites.



5G New Radio - Beamforming

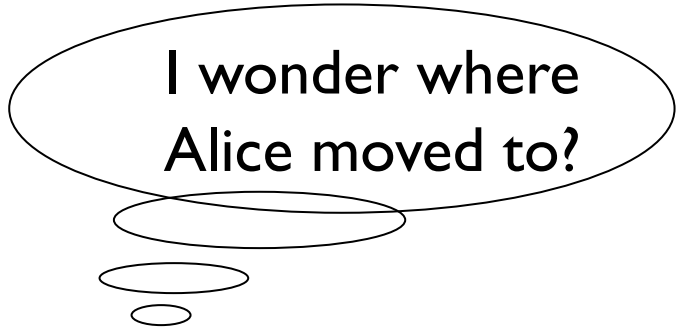
- Beamforming is the manipulation of the signals fed to and received from complex antennas to create beams in space that focus power in a particular direction
- LTE applies it only to data, 5G also to control
- At high frequencies beamforming will mostly be used to increase range by energy focus,
- At the mid and low bands below 6GHz, where attenuation is less of a problem, beamforming will be a key part of MIMO



Mobility

Contacting a mobile friend:

CHIEDO ALL'HSS DELL'UTENTE, DOVE SI TROVA L'UTENTE



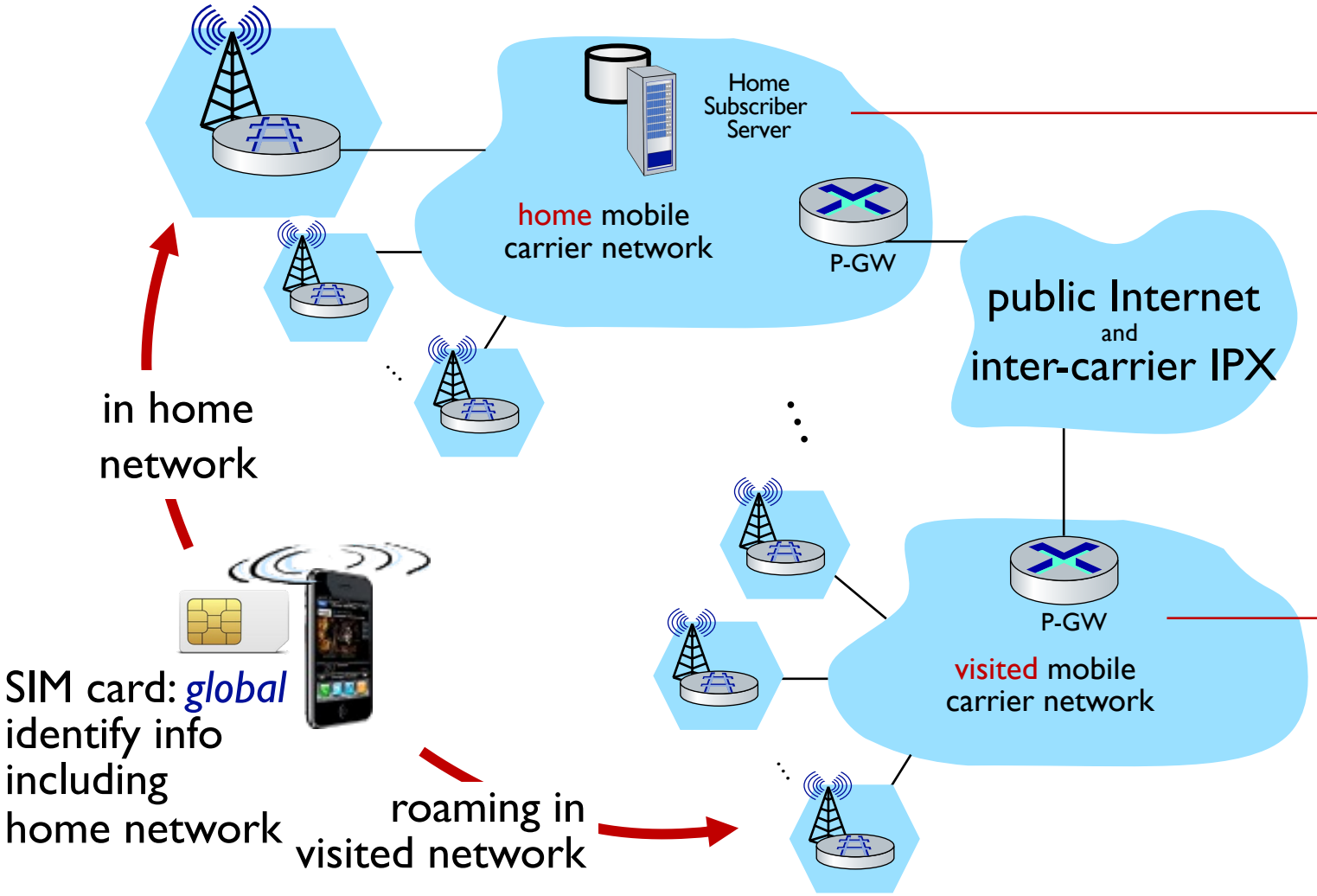
Consider friend frequently changing locations, how do you find him/her?

- search all phone books?
- expect her to let you know where he/she is?
- call his/her parents?
- Facebook!

The importance of having a "home":

- a definitive source of information about you
- a place where people can find out where you are

Home network, visited network: 4G/5G



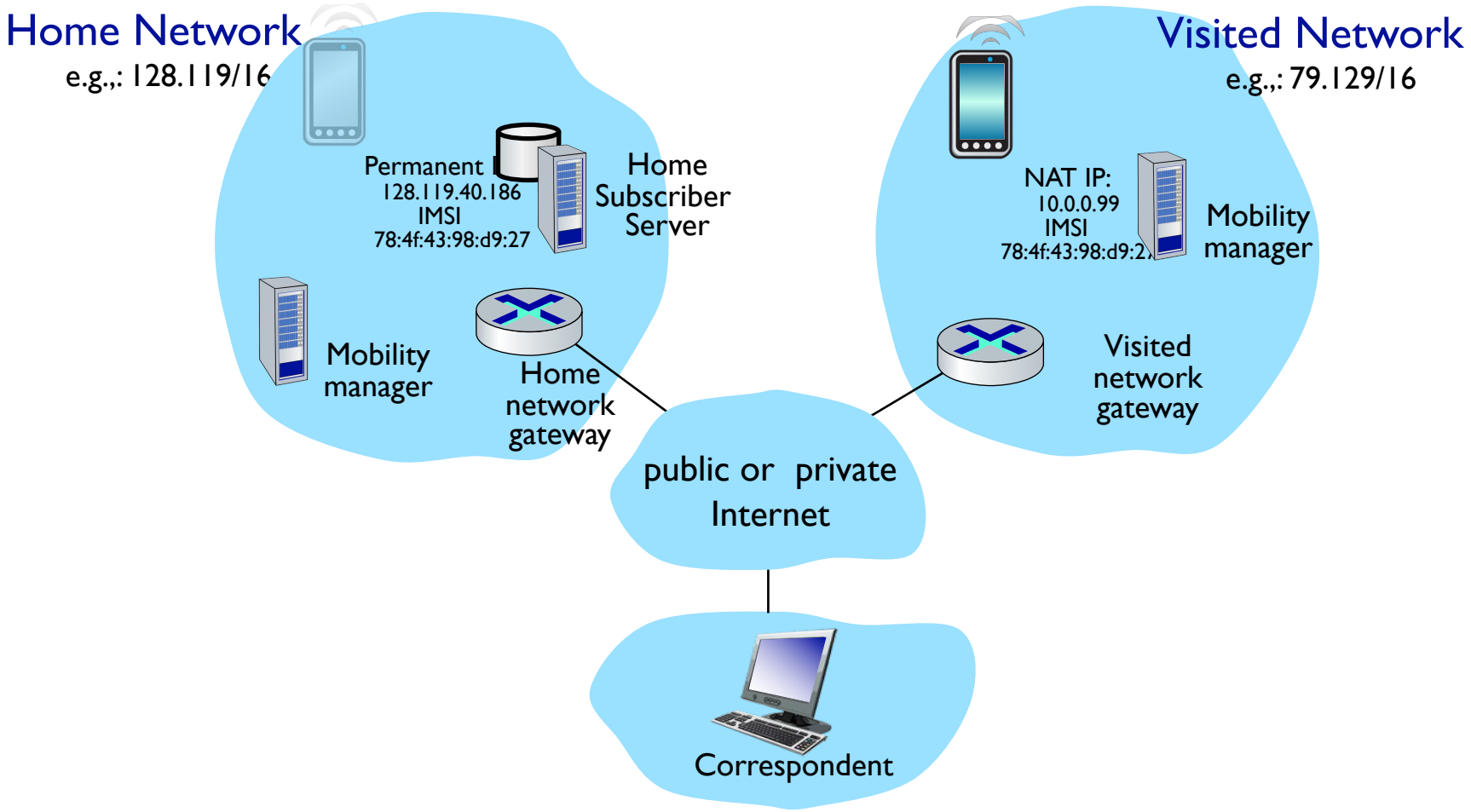
home network:

- (paid) service plan with cellular provider, e.g., Verizon, Orange
- home network HSS stores identify & services info

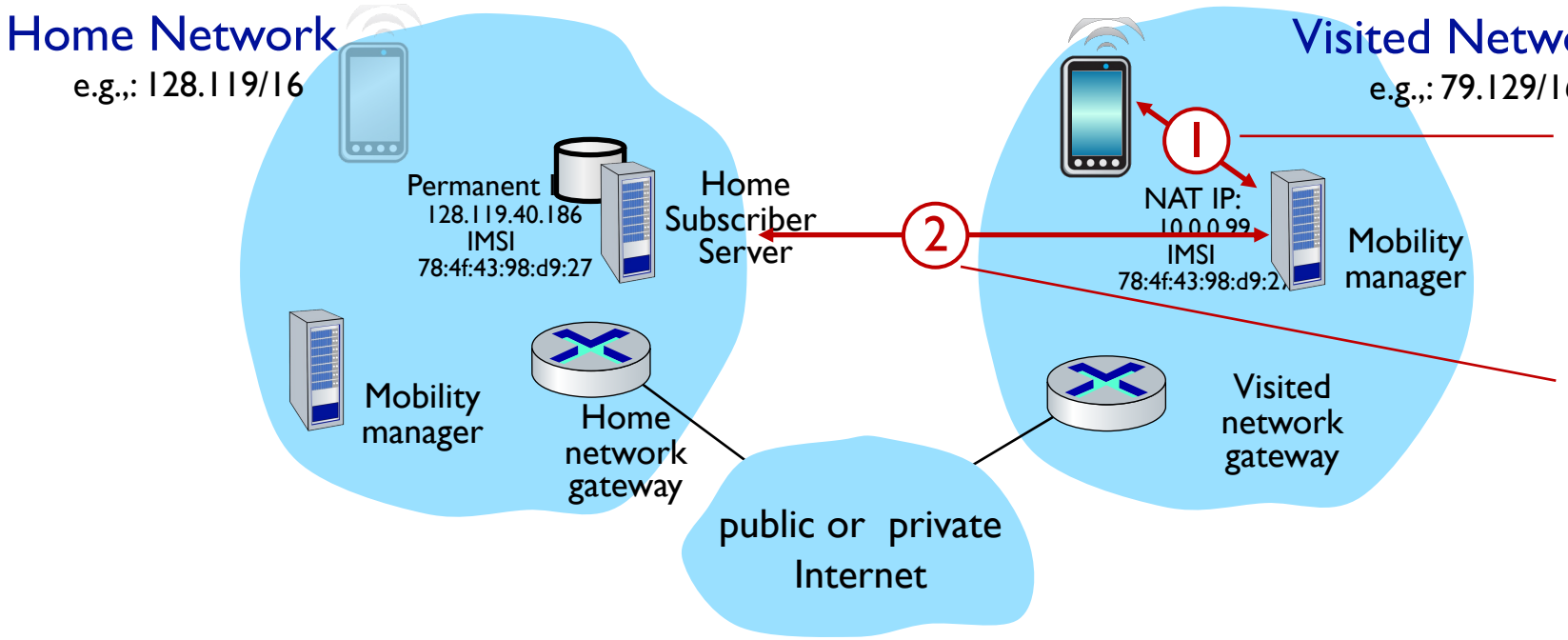
visited network:

- any network other than your home network
- service agreement with other networks: to provide access to visiting mobile

Home network, visited network: generic



Registration: home needs to know where you are!



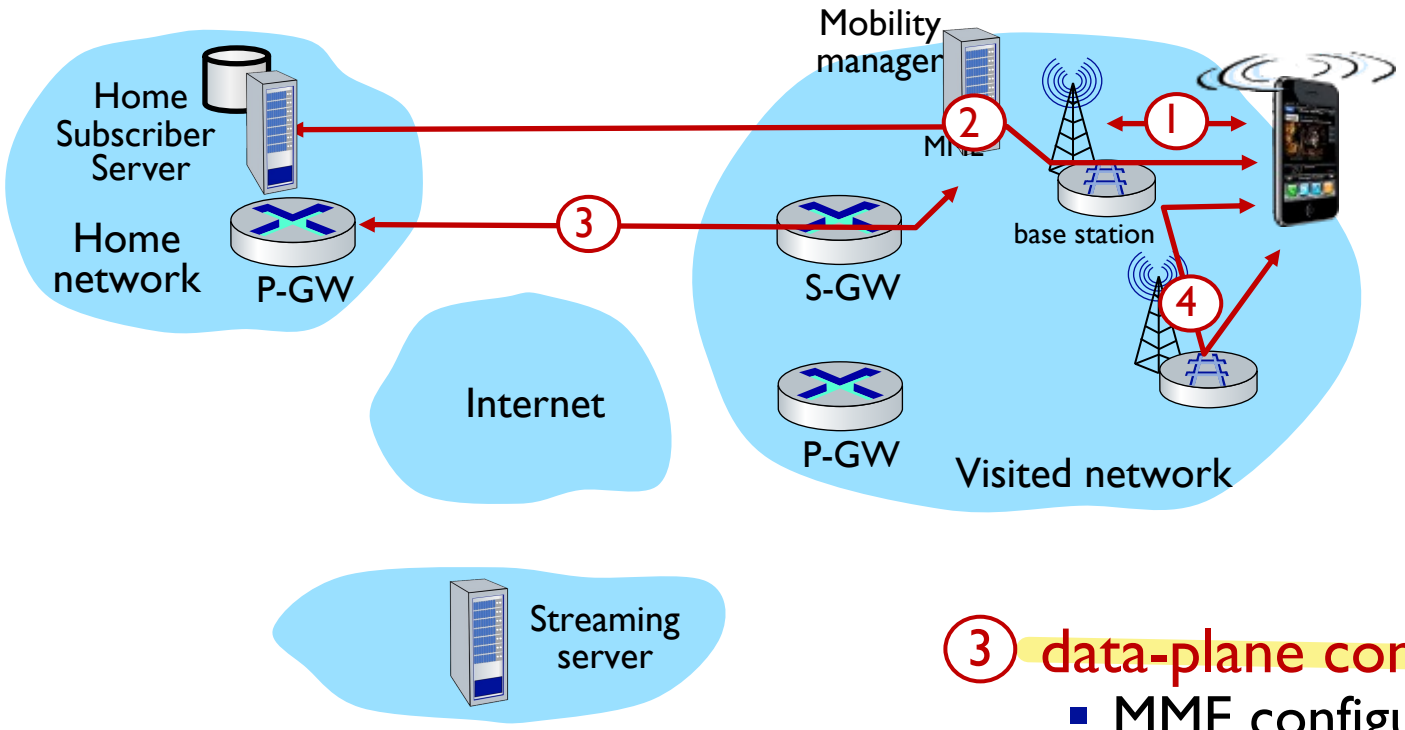
mobile *associates* with visited mobility manager

visited mobility manager *registers* mobile's location with home HSS

end result:

- visited mobility manager knows about mobile
- home HSS knows location of mobile

Mobility in 4G networks: major mobility tasks



① **base station association**:

- covered earlier
- mobile provides IMSI – identifying itself, home network

② **control-plane configuration**:

- MME, home HSS establish control-plane state - mobile is in visited network

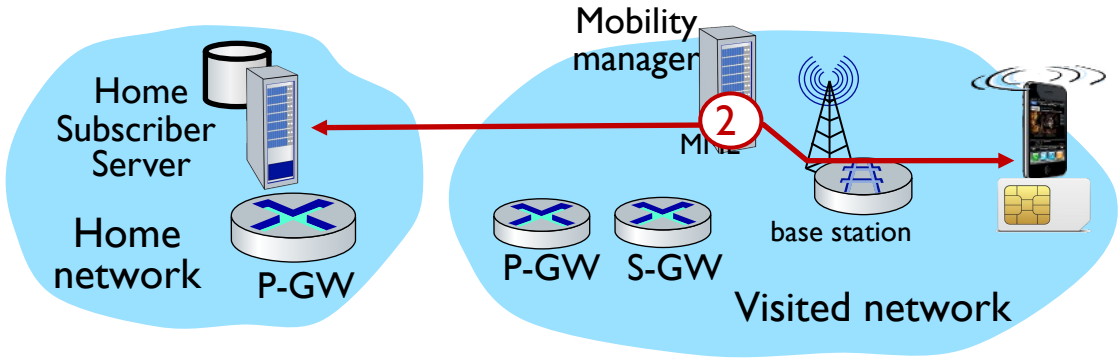
③ **data-plane configuration**:

- MME configures forwarding tunnels for mobile
- visited, home network establish tunnels from home P-GW to mobile

④ **mobile handover**:

- mobile device changes its point of attachment to visited network

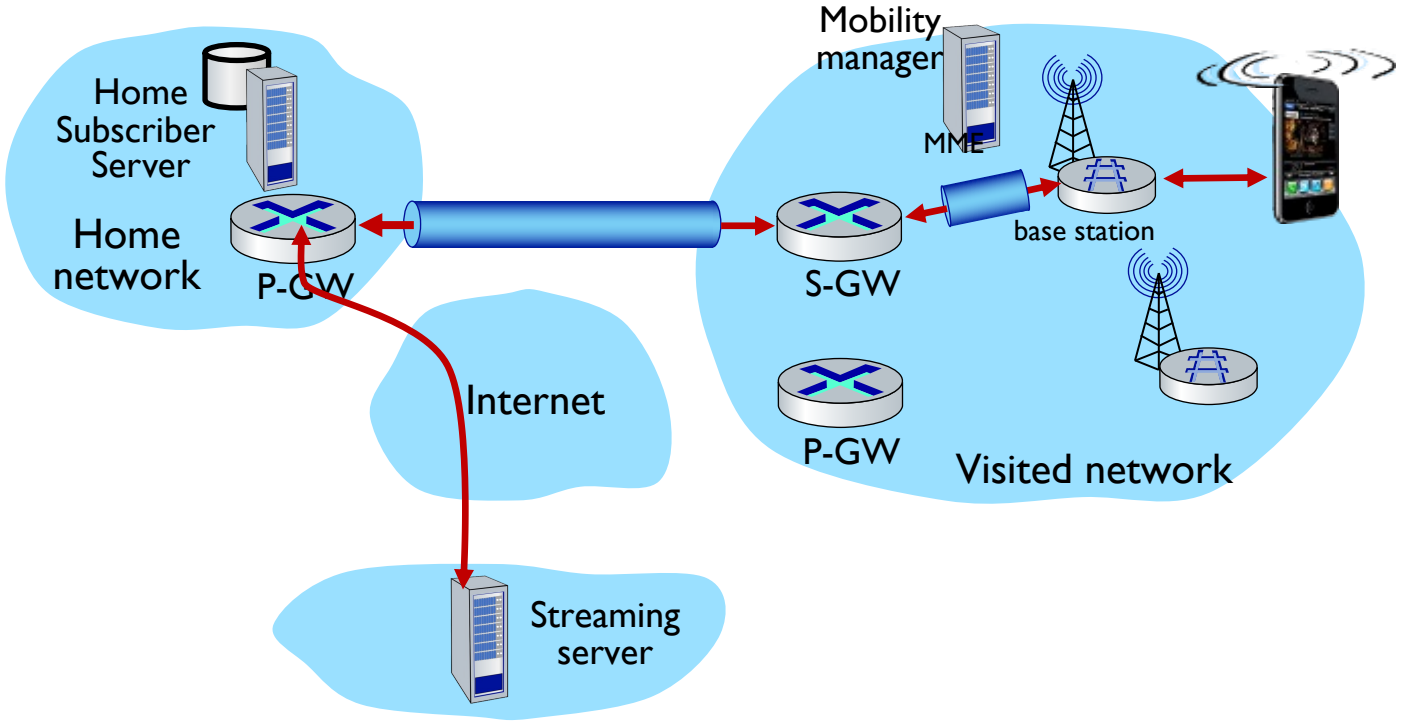
Configuring LTE control-plane elements



- Mobile communicates with local MME via BS control-plane channel
- MME uses mobile's IMSI info to contact mobile's home HSS
  - retrieve authentication, encryption, network service information
  - home HHS knows mobile now resident in visited network
- BS, mobile select parameters for BS-mobile data-plane radio channel

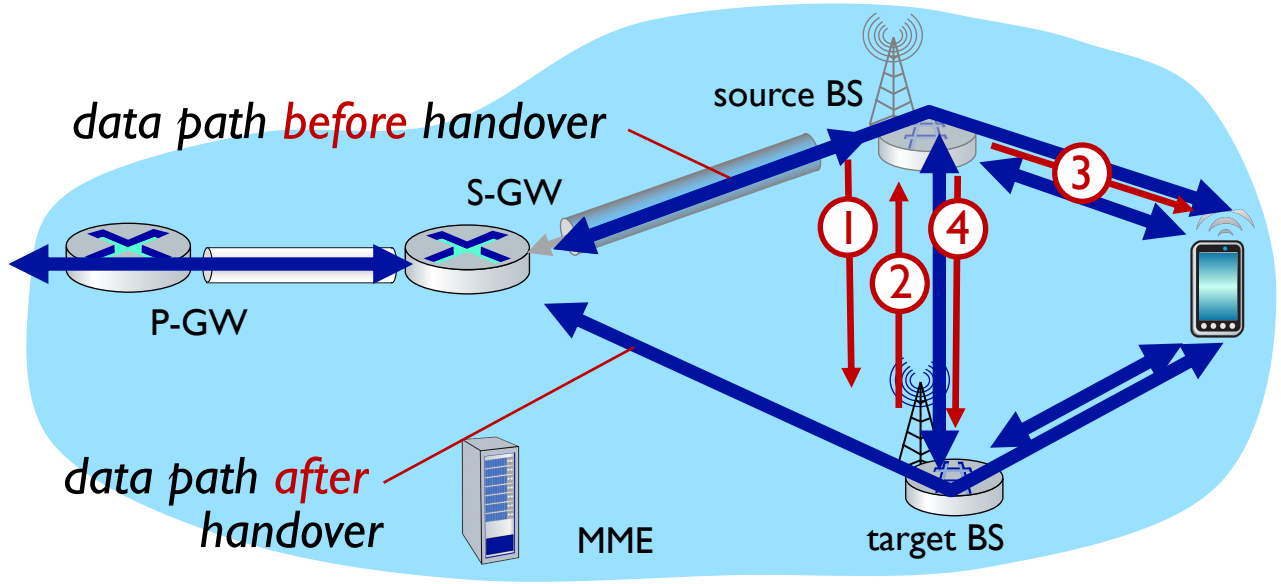
Configuring data-plane tunnels for mobile

- S-GW to BS tunnel: when mobile changes base stations, simply change endpoint IP address of tunnel
- S-GW to home P-GW tunnel: implementation of indirect routing



- tunneling via GTP (GPRS tunneling protocol): mobile's datagram to streaming server encapsulated using GTP inside UDP, inside datagram

Handover between BSs in same cellular network



BS SI RENDE CONTO CHE SEGNALE DEBOLE

1. current (source) BS selects target BS, sends *Handover Request message* to target BS

DI INFORMA CHE L'UTENTE ARRIVA DA LUI

2. target BS pre-allocates radio time slots, responds with HR ACK with info for mobile

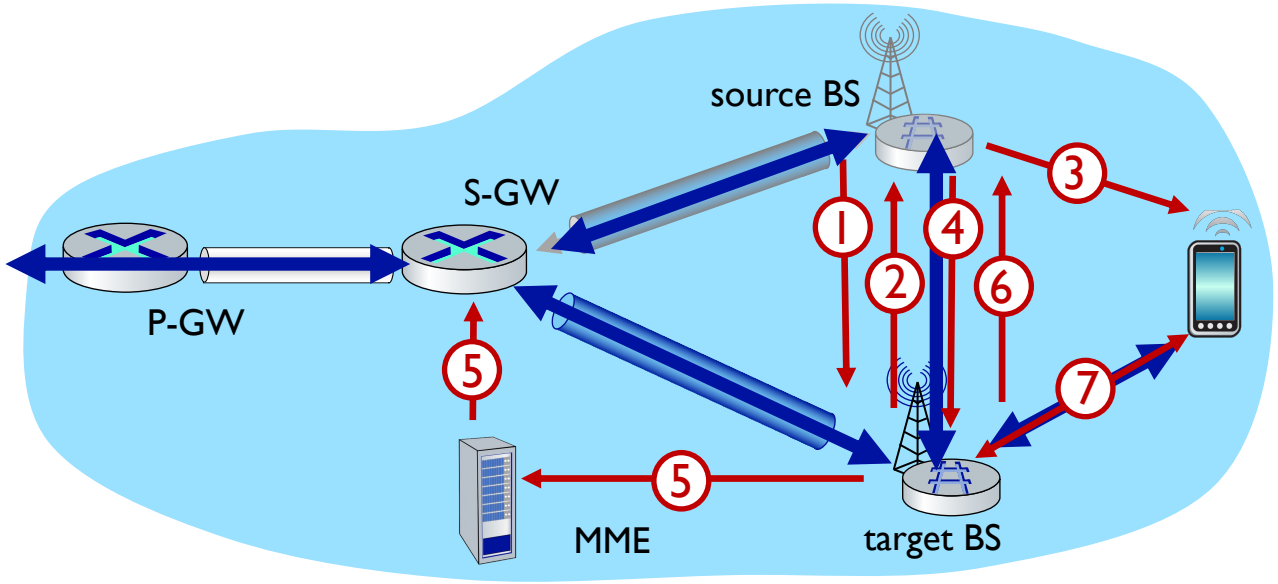
3. source BS informs mobile of new BS
   - mobile can now send via new BS - handover *looks* complete to mobile

4. source BS stops sending datagrams to mobile, instead forwards to new BS (who forwards to mobile over radio channel)

NEWBS DICE: "VECCHIA BS LIBERA PURE LE RISORSE, L'UTENTE ORA E' MIO"

5. FINITE TIME LA NUOVA BS COMUNICA ALLA RETE CHE L'UTENTE SI E' SPOSTATO E QUINDI BISOGNA ELIMINARE IL VECCHIO BEARER E FARNE UNO NUOVO

Handover between BSs in same cellular network



5 target BS informs MME that it is new BS for mobile
- MME instructs S-GW to change tunnel endpoint to be (new) target BS

6 target BS ACKs back to source BS: handover complete, source BS can release resources

7 mobile's datagrams now flow through new tunnel from target BS to S-GW