Mobile and Cellular Networks

Mestrado Integrado em Engenharia de Computadores e Telemática

2019/2020

Home Technologies: WiFi, Bluetooth

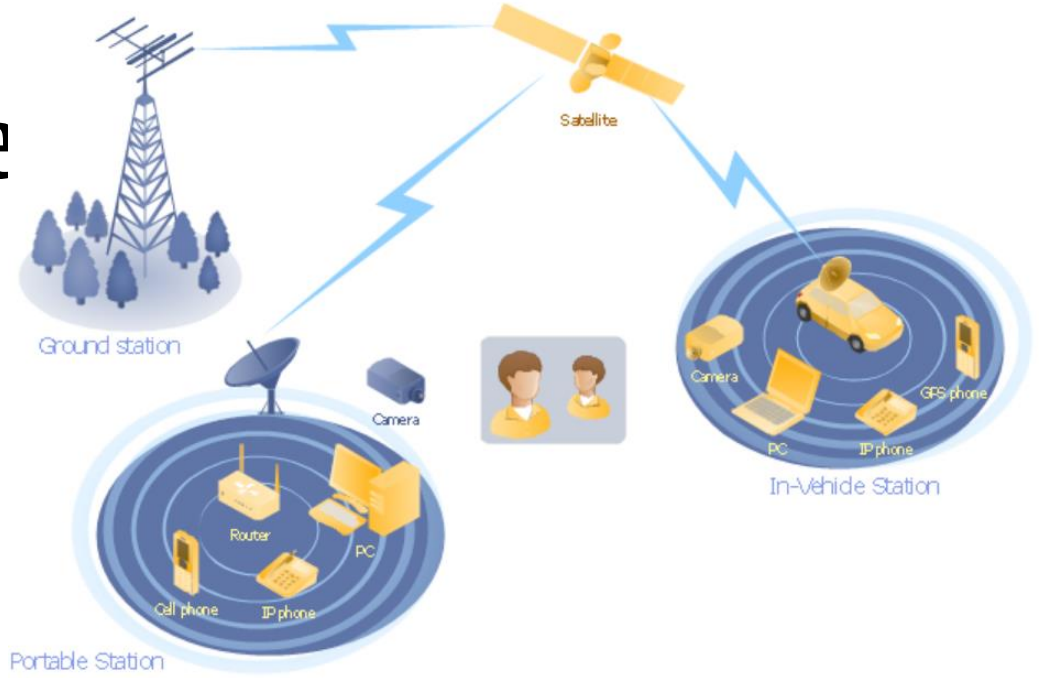
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

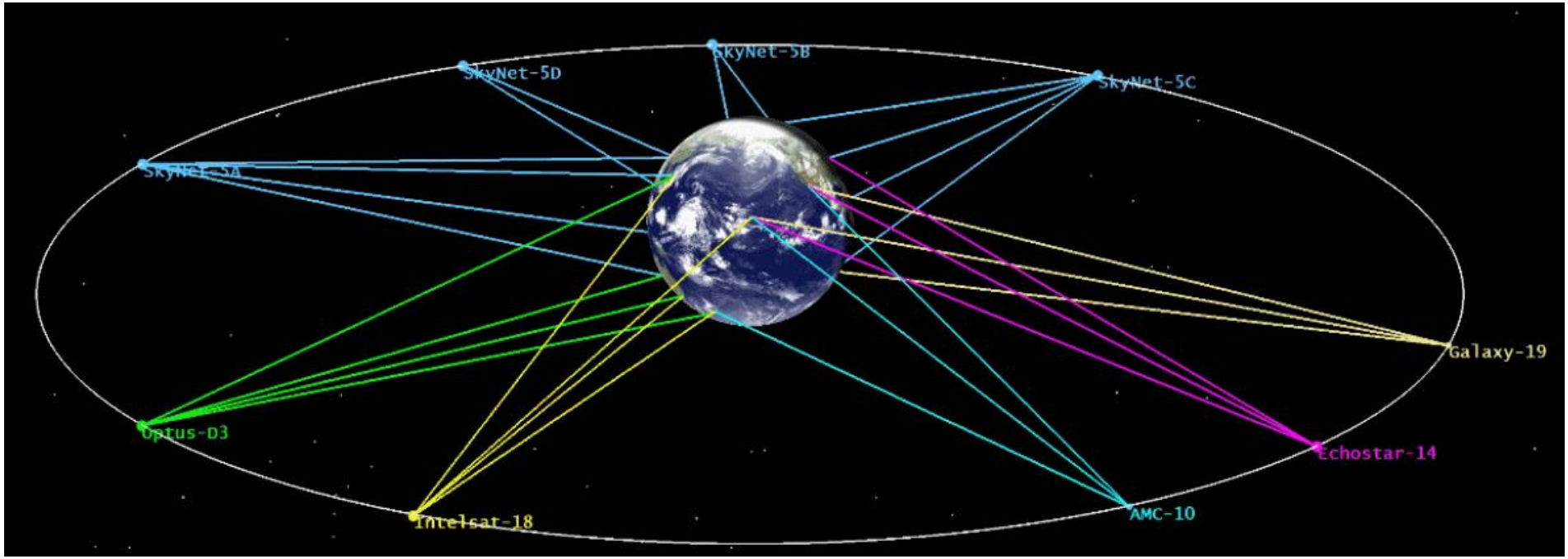
Bluetooth Spec. Evolution

Specifications	1.1	1.2	2.0 + EDR	2.1 + EDR	3.0 +HS	4.0
Adopted	2002	2005	2004	2007	2009	2010
Transmission Rate	723.1 kbps	723.1 kbps	2.1 Mbps	3 Mbps	24 Mbps	25 Mbps
Standard PAN Range	10 m	10 m	10 m	10 m	10 m	50 m
Improved Pairing (without a PIN)				Yes	Yes	Yes
Improved Security		Yes	Yes	Yes	Yes	Yes
NFC Support			Yes	Yes	Yes	Yes

	Speed	Distance	Released Date	Bands	Backward Compatibility	New Hardware Requirement
Version 4.1	24MBs	100 m or 300 feet	4/12/2013	2.4 to 2.485 GHz	Yes	No
Version 4.2	24MBs	100 m or 300 feet	2/12/2014	2.4 to 2.485 GHz	Yes	For some feature
Version 5	48MBs	300 m or 985 feet	16/06/2016	2.4 to 2.485 GHz	No	Yes

Sate

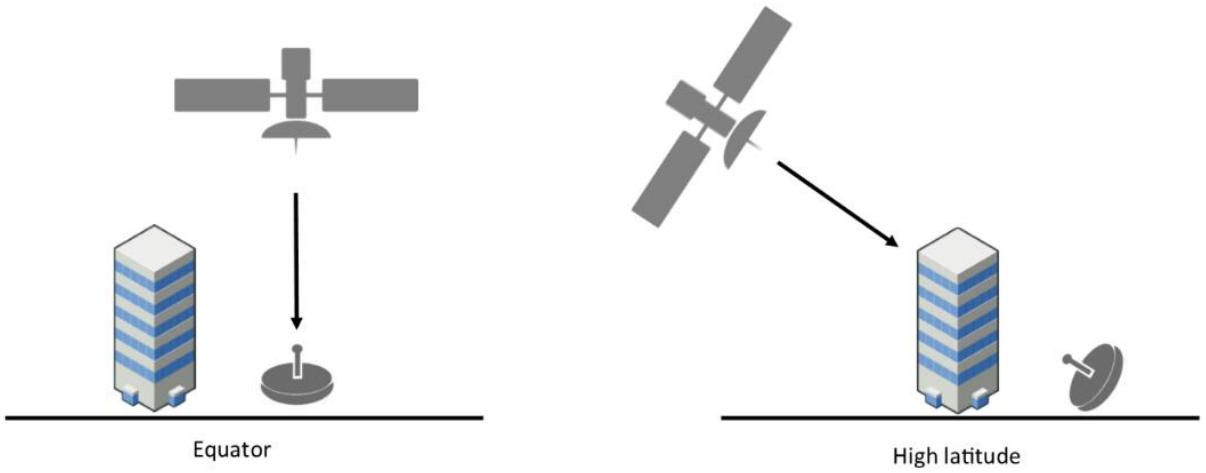

Satellite
Ground station
Camera
Router
PC
Cell phone
IP phone
Portable Station
Camera
GPS phone
PC
IP phone
In-Vehicle Station


SkyNet-5B
SkyNet-5D
SkyNet-5C
Galaxy-19
Optus-D3
Echostar-14
Intelsat-18
AMC-10

Satellite: LEO and MEO

Abbreviation	Orbit Name	Altitude [km]
LEO	Low Earth Orbit	160 to 2000
MEO	Medium Earth Orbit	2000 to <35786
GSO	Geosynchronous Orbit	35786
GEO	Geostationary Equatorial Orbit	35786

- **GEO: 500msec**
- **LEO: 25msec**

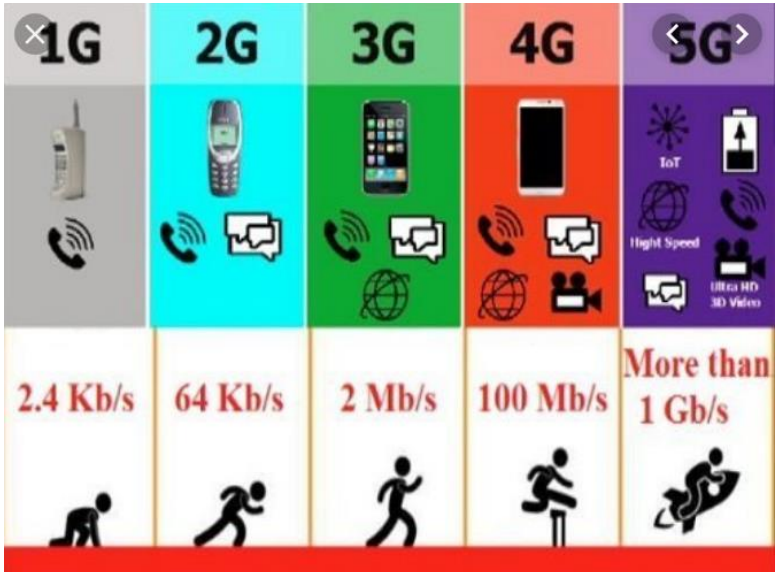


Long Range Technologies for

Network:	Sigfox	LoRa	NB-IoT (Cat NB1)
Type:	PLWAN	PLWAN	DSSS modulation
Low Power:	+++++	++++	++++
Throughput Kbit/s:	0,1	50	100
Bandwidth:	Ultra-narrowband	Narrowband	Narrowband
Latency:	1 – 30s	Based on profile	1.6 – 10s
Standard:	Proprietary	Proprietary	3GPP Rel. 13
Availability world-wide:	++	+++	++
Spectrum:	Unlicensed ISM	Unlicensed ISM	Licensed LTE
Complexity:	Very low	Low	Very low
Coverage / range:	Medium / high	Medium / high	High
Battery life:	Very high	Very high / high	High
Gateway needed:	Yes	Yes	No, but optional
Signal penetration:	High	Medium / high	Medium / high
Security:	+++	+++	+++
Future proof:	+++	+++	+++++

Wide Communication technologies: Cellular

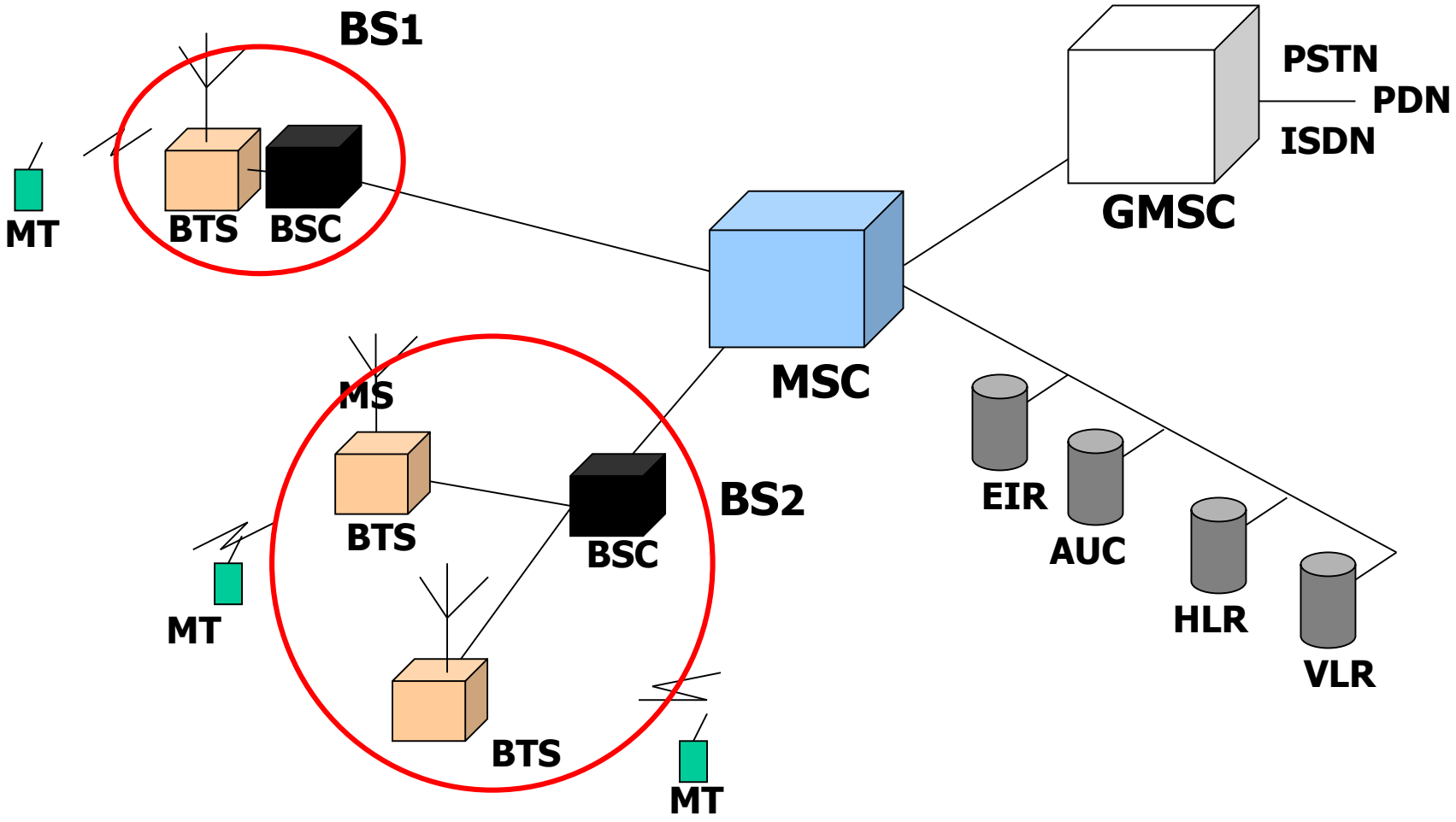
Comparison	2G	3G	4G	5G
Introduced in year	1993	2001	2009	2018
Technology	GSM	WCDMA	LTE, WIMAX	MIMO, mm Waves
Access system	TDMA, CDMA	CDMA	CDMA	OFDM, BDMA
Switching type	Circuit switching for voice and packet switching for data	Packet switching except for air interference	Packet switching	Packet switching
Internet service	Narrowband	Broadband	Ultra broadband	Wireless World Wide Web
Bandwidth	25 MHz	25 MHz	100 MHz	30 GHz to 300 GHz
Advantage	Multimedia features (SMS, MMS), internet access and SIM introduced	High security, international roaming	Speed, high speed handoffs, global mobility	Extremely high speeds, low latency
Applications	Voice calls, short messages	Video conferencing, mobile TV, GPS	High speed applications, mobile TV, wearable devices	High resolution video streaming, remote control of vehicles, robots, and medical procedures



Early cellular systems

- 1G: analog systems (450-900 MHz)
  - Signalling: FSK
  - Share of medium: FDMA
  - NMT (Europe), AMPS (US)
- 2G: digital systems (900, 1800, 1900 MHz)
  - Share of medium : TDMA/CDMA
  - Circuit switching
  - GSM (Europe), IS-136 (US), PDC (Japan)
- 2.5G: extensions for packet switching
  - Digital: GSM → GPRS
- 3G: networks for data applications
  - Higher rates, data, Internet
  - Share of medium : TDMA/CDMA/CDMA
  - IMT-2000 (Europe: UMTS)

GSM architecture



Basic architecture

- Each cell is controlled by a Base Station System (BSS)
- BSS are structured as base station controllers (BSC) + base transceiver station (BTS)
  - BTS comprises the radio transmission and reception devices; manages the signal processing related to the air interface
  - BSC manages the radio interface: allocation, release and handover of radio channels
- BSs are connected to mobile switching center (MSC) through physical lines
- Each MSC is connected to other MSCs
  - ISDN-switch
  - Coordinates and sets up calls to and from Mobile Stations (MS)
- There are MSC connected to the public telephone network (PSTN), the gateway mobile switching center (GMSC).

Mobile Switching Center

- **MSC = Mobile Switching Center**

  Contains:

  - Home Location Register (HLR) - database used to store permanent and semi-permanent subscriber data; it knows in which location area the MS is
  - Visitor Location Register (VLR) - contains all the subscriber data, both permanent and temporary, which are necessary to control a MS in the MSCs coverage area.
  - Autentication Center (Au) - database with subscriber authentication keys and the algorithm required to calculate the authentication parameters to be transferred to the HLR
  - Equipment Identity Registry (EIR) - database contains information on the MS and its capabilities
- **Connects to BSS**

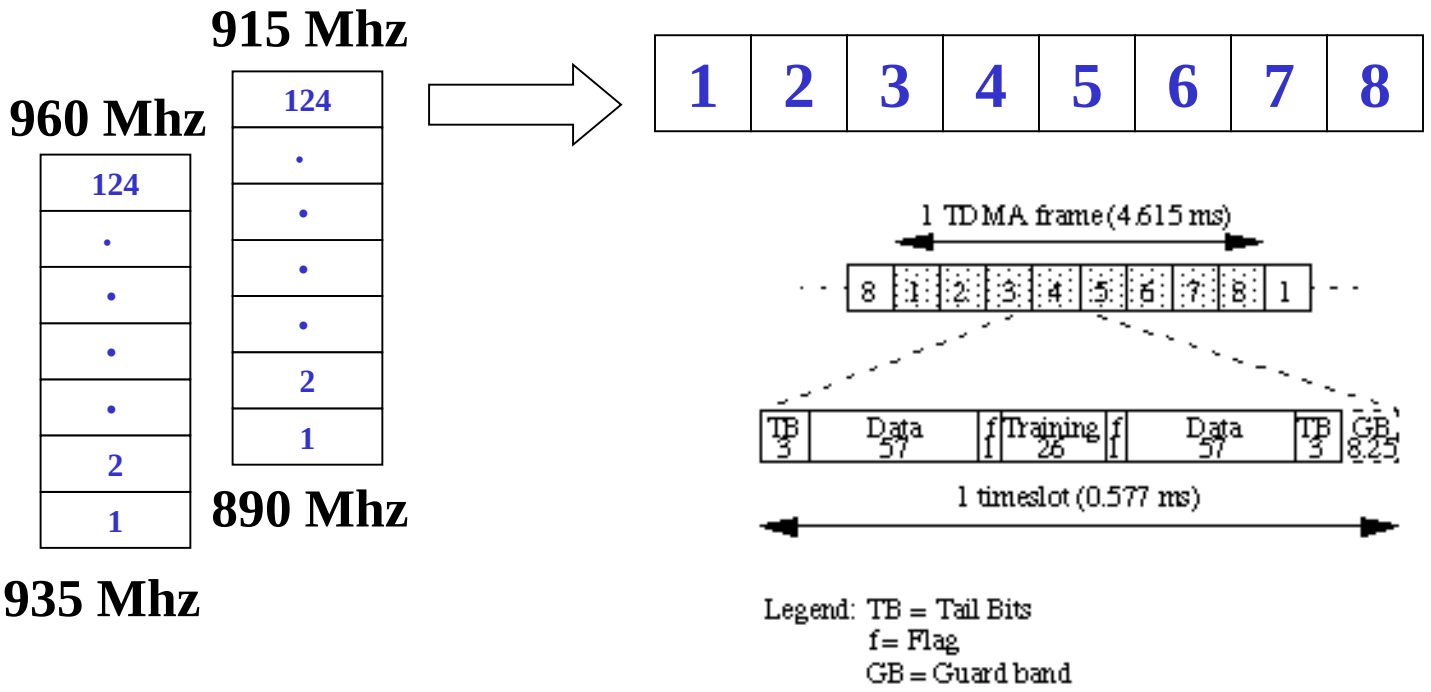
  (Master of the cell, defines channels and access to them...)
- **Contains the registration of its stations**
- **There is a specific signalling channel**
  - **MT-BS (MSC): location, call establishment, answer to a received call**
  - **BS (MSC)-MT: cell identification, location update, establishment of received call**

Handover

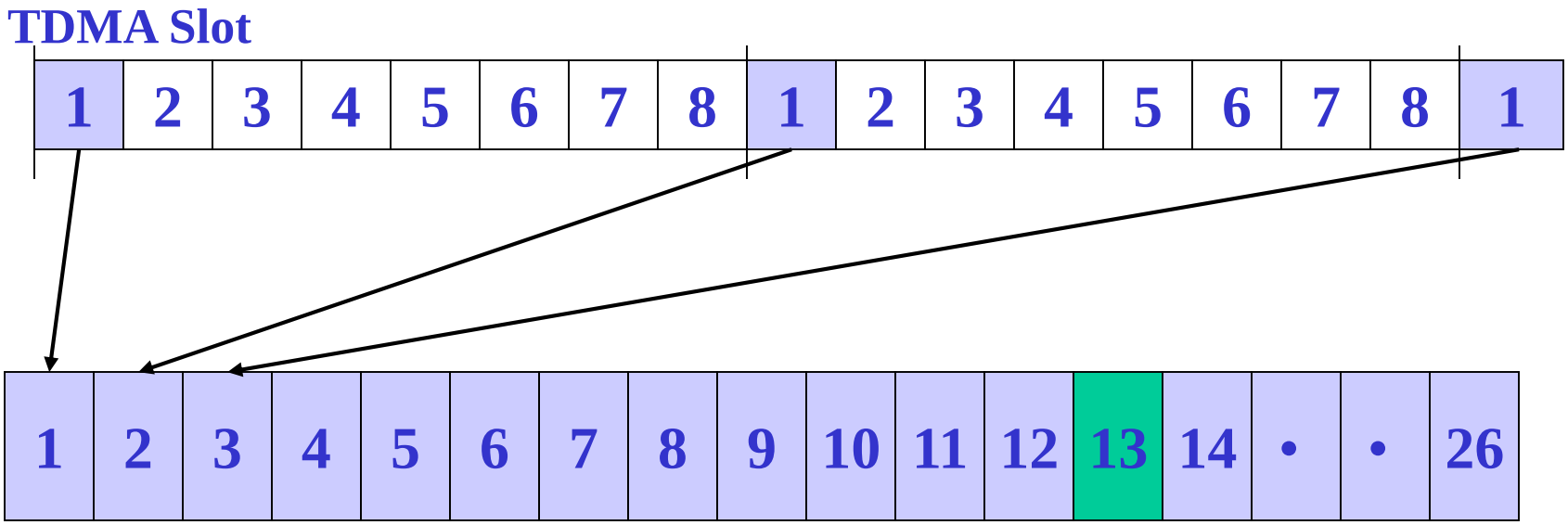
- Executed by BSC (channels) and by MSC (routing)
- Initiated by BS:
  - BS monitors the MN signal
  - When signal is too low, handover
  - Increases the load in BS
- Assisted by MN:
  - BSs transmit beacons
  - MN, listening to the beacon, requests handover
    - Sends to new BS the identity of old BS
  - BS accepts MN, and starts sending its calls
- Inter-system:
  - ~assisted by MN, with extra connections to HLR/VLR

GSM channels

- TDMA structure with 8 timeslots
- Delay of three slots (up and down) → avoids simultaneous rx/tx
- Uplink: 890 - 915 MHz
- Downlink : 935 - 960 MHz
- 124 channels in each band (=> until 8 users per channel)



Frame structure for full-rate channels



TDMA frame in a channel

The normal burst has a throughput after coding of 22.8 kbps, and offers full rate voice at a net bitrate of 13 kbps and data at up to 9.6 kbps.

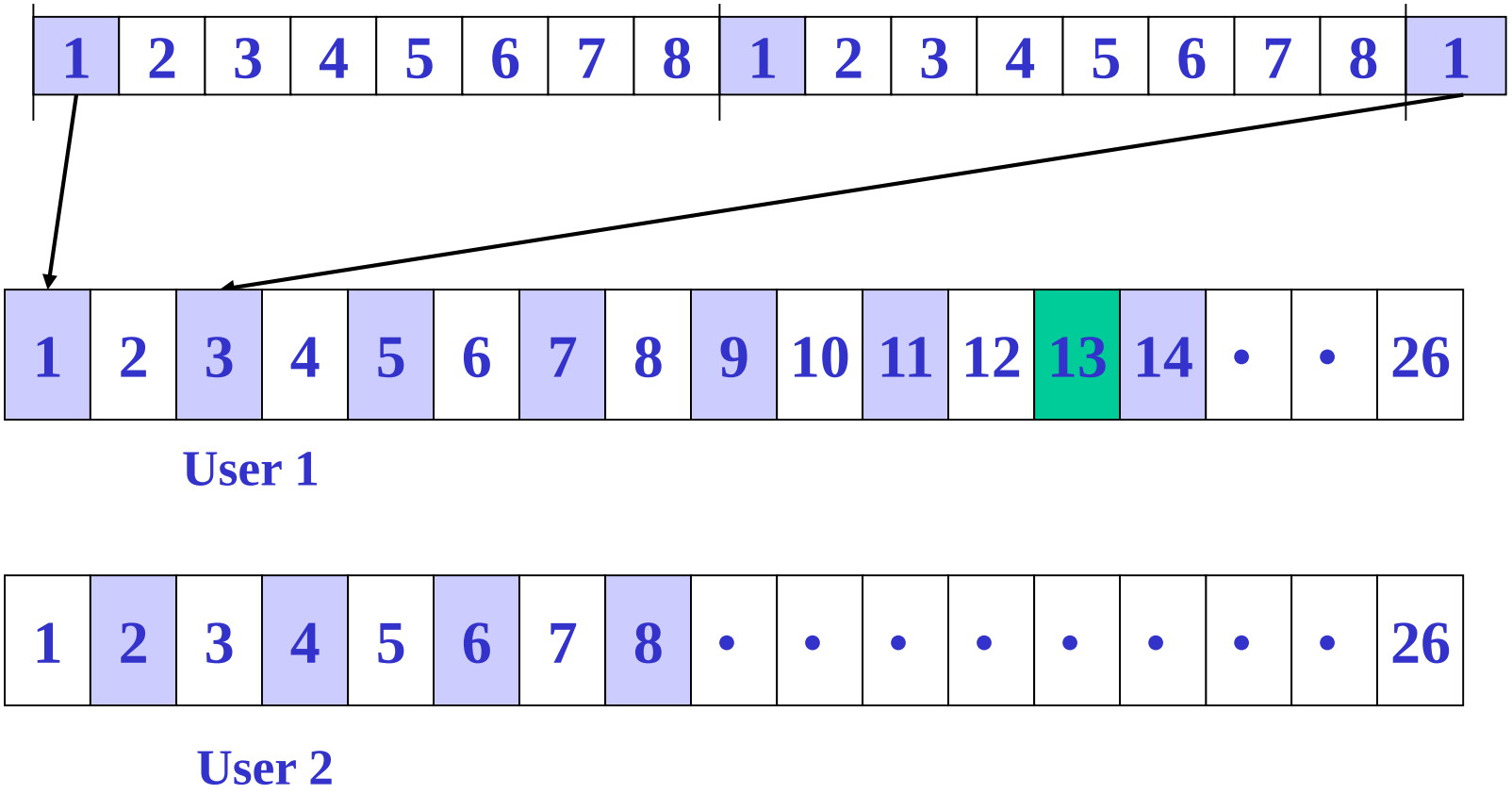
traffic

signalling (S)

Contains information about adjacent cells

Frame structure for half-rate channels

GSM has also specified a half-rate service by time-multiplexing two users onto the TDMA structure (alternate frames in the same timeslot). This service offers a gross bitrate of 11.4 kbps, and data at 4.8 kbps.



Logical channels

- Logical channels are mapped in physical channels. It is a technique to simplify radio resource management.
- A physical channel consists on a specified timeslot in a specified channel
  - GSM distinguishes between *physical channels* (the timeslot) and *logical channels* (the information carried by the physical channels)
- Data channels
  - TCH – Full rate traffic channel
  - TCH/H – Half rate traffic channel
- Signalling channels
  - Synchronizes MN with cell
  - Informs MN about
    - Cell parameters
    - Neighbor cells
    - Channels
  - Performs paging
    - Discovers MN in low-power mode
  - Allows MN to access the network
    - Access in shared mode
    - Fundamental for MN to ask connection
  - BCH – Broadcast channels; CCH – common control channels; DCCH/ACCH – dedicated/associated control channels

Logical channels

BCH : Broadcast channels

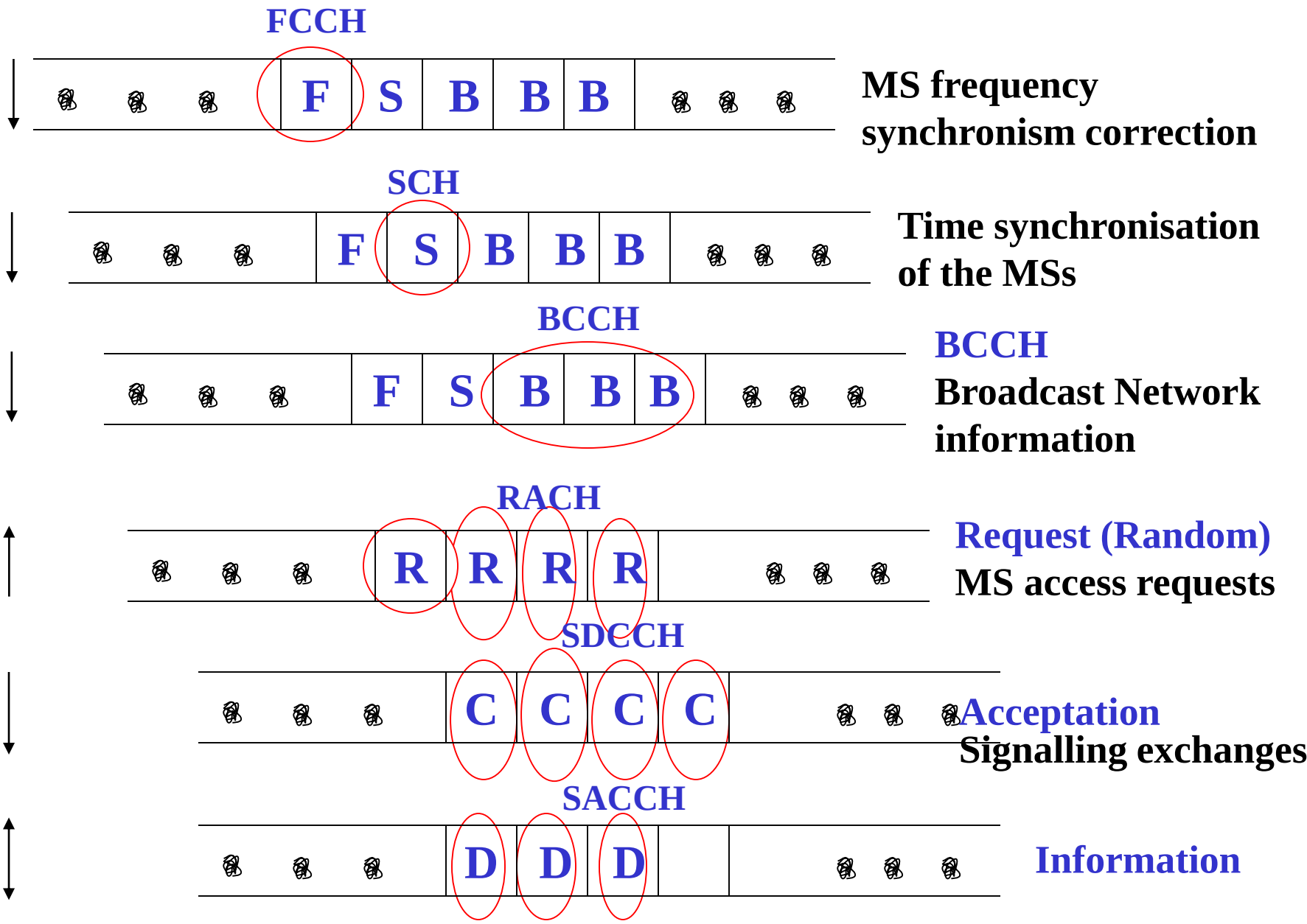
- Broadcast Control Channel (BCCH) - Broadcasts Network information, e.g. for describing the current control channel structure. The BCCH is a point-to-multipoint channel (BSS-to-MS).
- Frequency Correction Channel (FCCH) - MS frequency correction
- Synchronization Channel (SCH) - Synchronisation of the MSs

CCH : common control channels

- Random Access Channel (RACH) - MS access requests, response to call announcement, location update, etc
- Paging Channel (PCH) - MS terminating call announcement

D/ACCH: dedicated/associated control channels

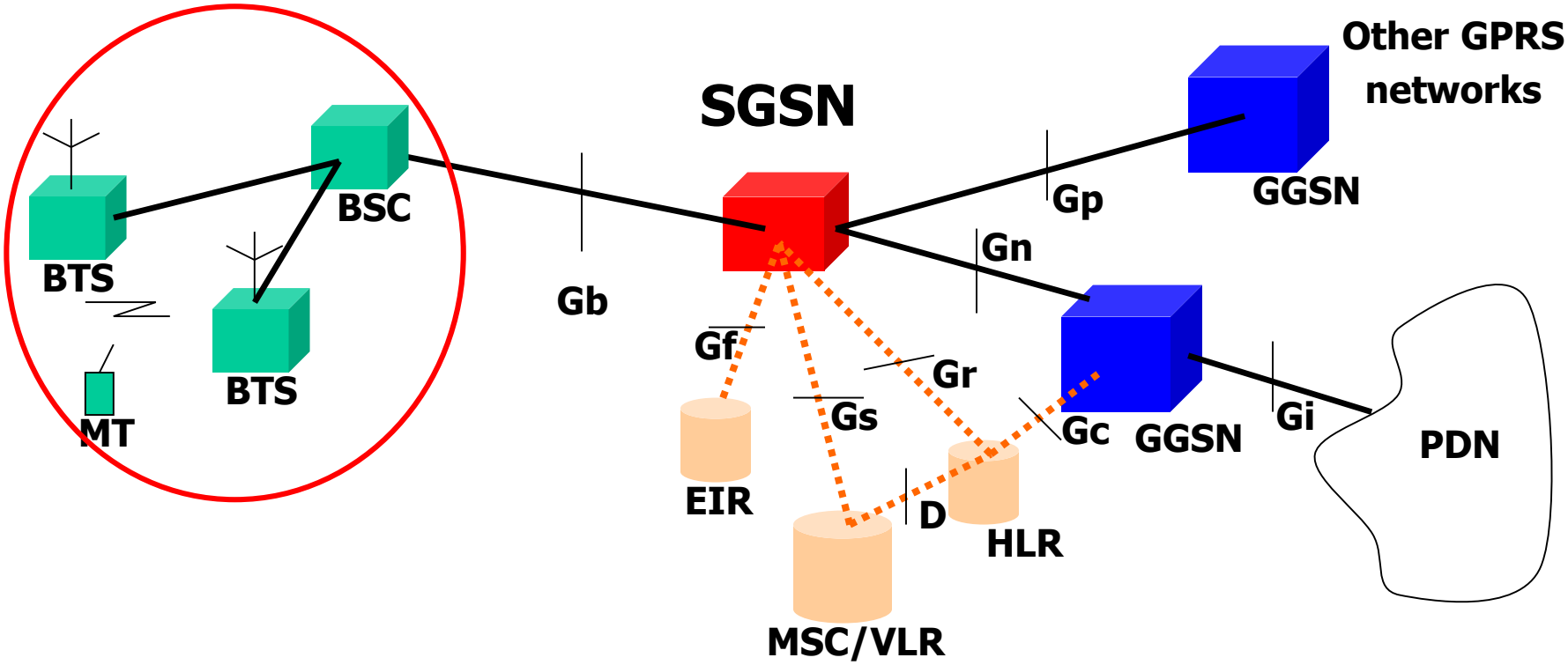
- Stand-alone Dedicated Control Channel (SDCCH) - For signalling exchanges, e.g. during call setup, registration / location updates
- Slow Associated Control Channel (SACCH) - SDCCH in-band signalling, e.g. for link monitoring


FCCH
F S B B B
MS frequency synchronism correction
SCH
F S B B B
Time synchronisation of the MSs
BCCH
F S B B B
BCCH
Broadcast Network information
RACH
R R R R
Request (Random)
MS access requests
SDCCH
C C C C
Acceptation
Signalling exchanges
SACCH
D D D
Information

GPRS

- Transport service dedicated to packet transmission, connection oriented to data network (Internet)
  - Better transmission rates (max 150kbps)
  - Allows burst transmissions
  - New network applications
  - New accounting mechanisms (user oriented: per traffic, e.g.)
- Transmission plane
  - Data packets are transmitted by a tunnel mechanism
- Control plane
  - GTP: a mechanism for tunnel management (create, remove, etc..)
- Radio interface
  - Logic channels changed, its management changed
  - Maintains notion of “master-slave”
- New security features such as ciphering
- New GPRS-specific signalling

GPRS architecture



GPRS on a GSM network - addition of two core modules
Gateway GPRS Service Node (GGSN): Gateway between the GPRS network and public data networks such as IP; Also connects to other GPRS networks to facilitate GPRS roaming
Serving GPRS Service Node (SGSN): Provides packet routing to and from the SGSN service area for all users in that service area

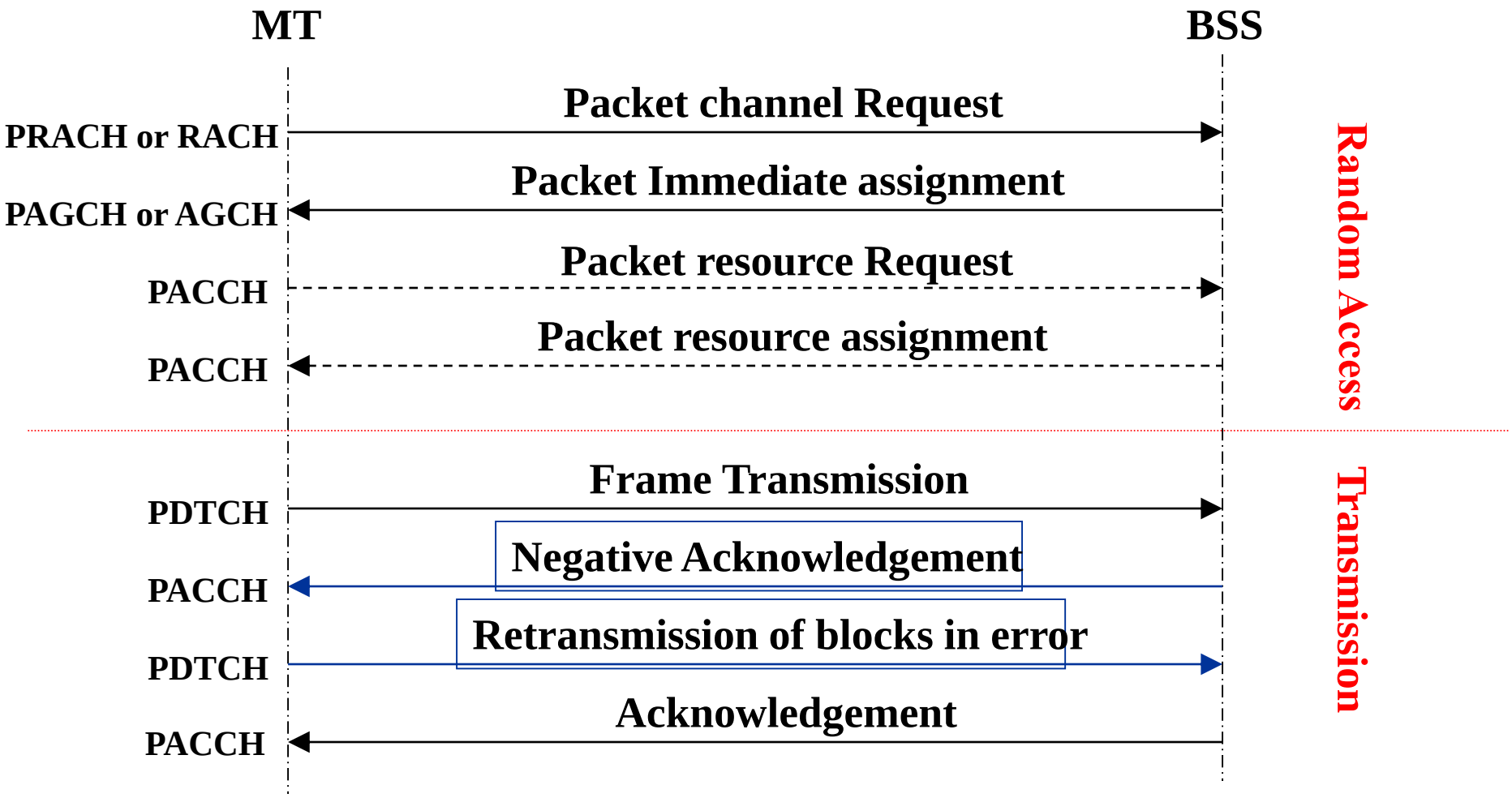
MN registration

There is an explicit registration of MN in the network

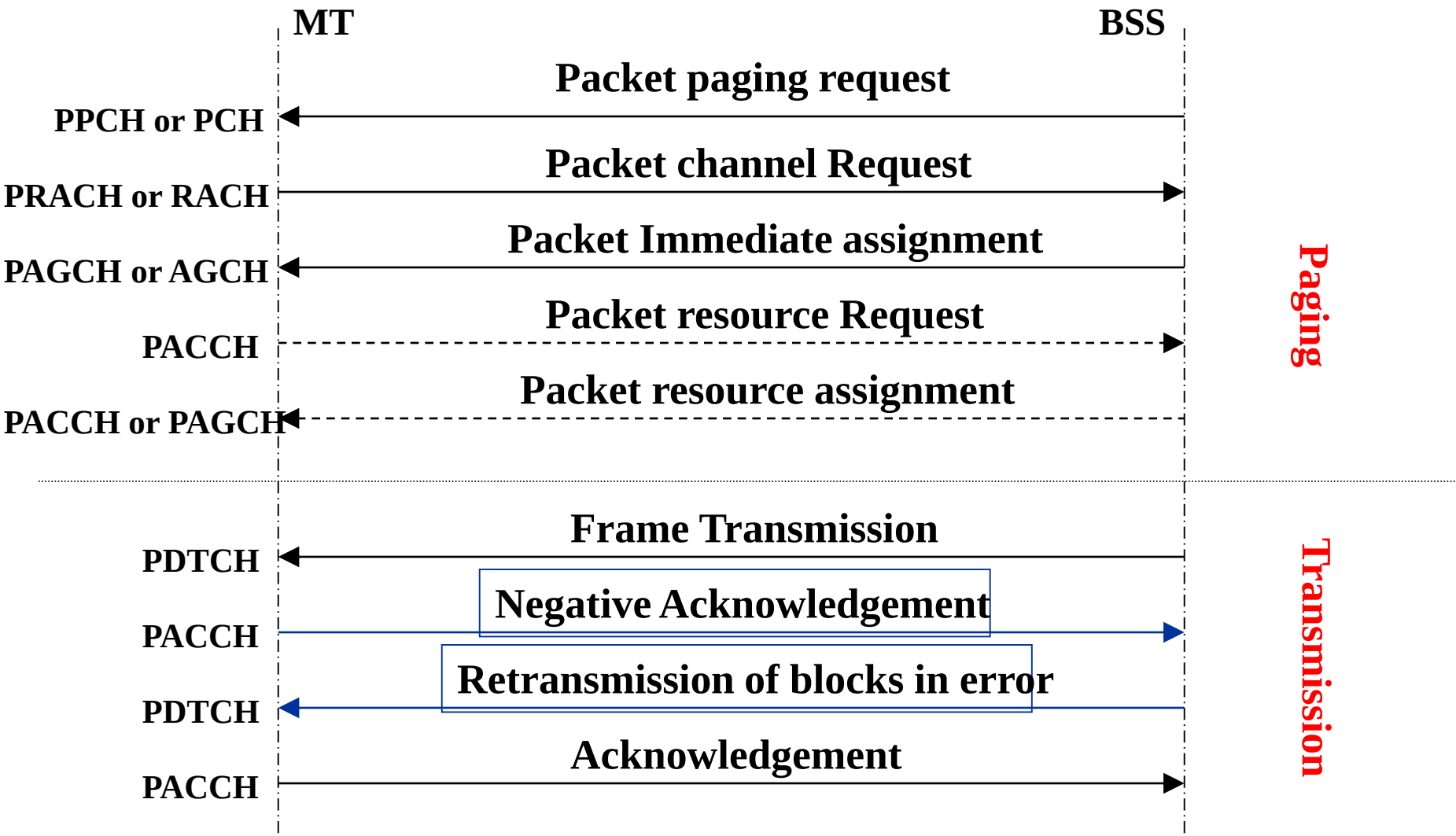
- GPRS attach
- GPRS detach – can be initiated by MN or network
- Location packets are periodically sent

- HLR maintains information about MN status, including
  - GPRS status (ready, standby, idle)
  - QoS profile (priority 3, delay 4, reliability 5, peak and mean throughput 19 and 9)
  - PDP (packet data protocol) context
    - Is a data structure present on both the SGSN and the GGSN which contains the subscriber's session information when the subscriber has an active session.
    - When a mobile wants to use GPRS, it must first attach and then activate a PDP context. This allocates a PDP context data structure in the SGSN that the subscriber is currently visiting and the GGSN serving the subscribers access point.
    - Also stored in SGSN and GGSN

Data transfer (Uplink)

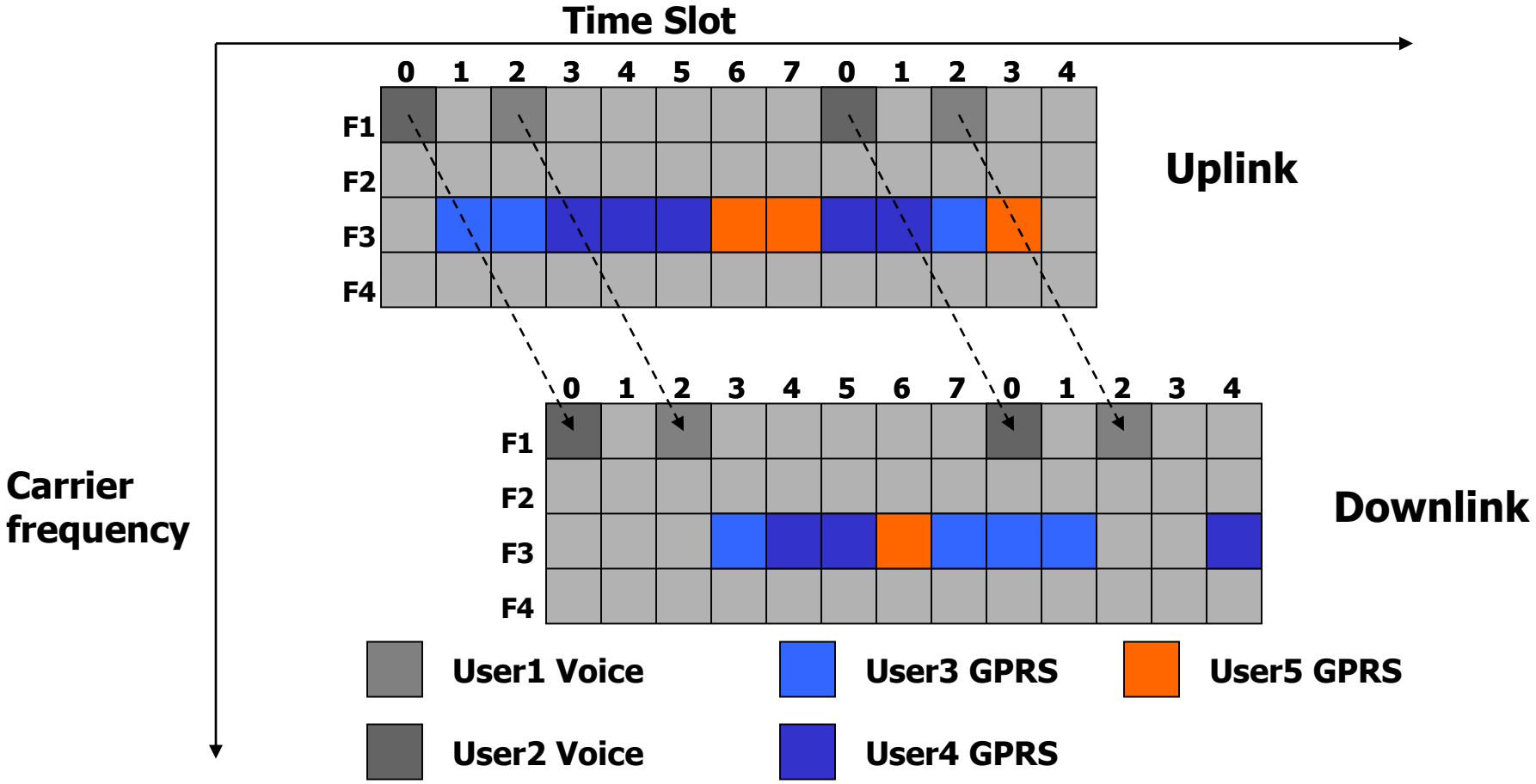


Data transfer (Downlink)



GPRS radio interface

GTP performs tunnelling of user and signalling packets between GPRS nodes
A mobile node can use 8 slots, dinamically allocated
Pointer in the packet indicates where the next packet will come (better for long transmissions)

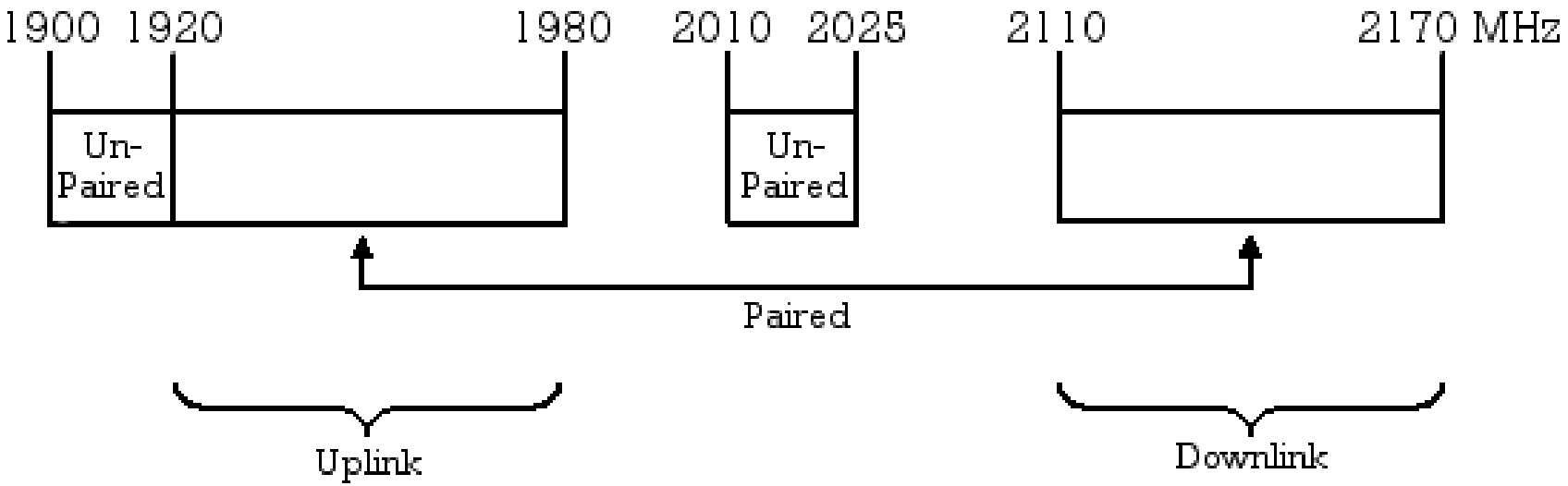


UMTS: first universal celular data system

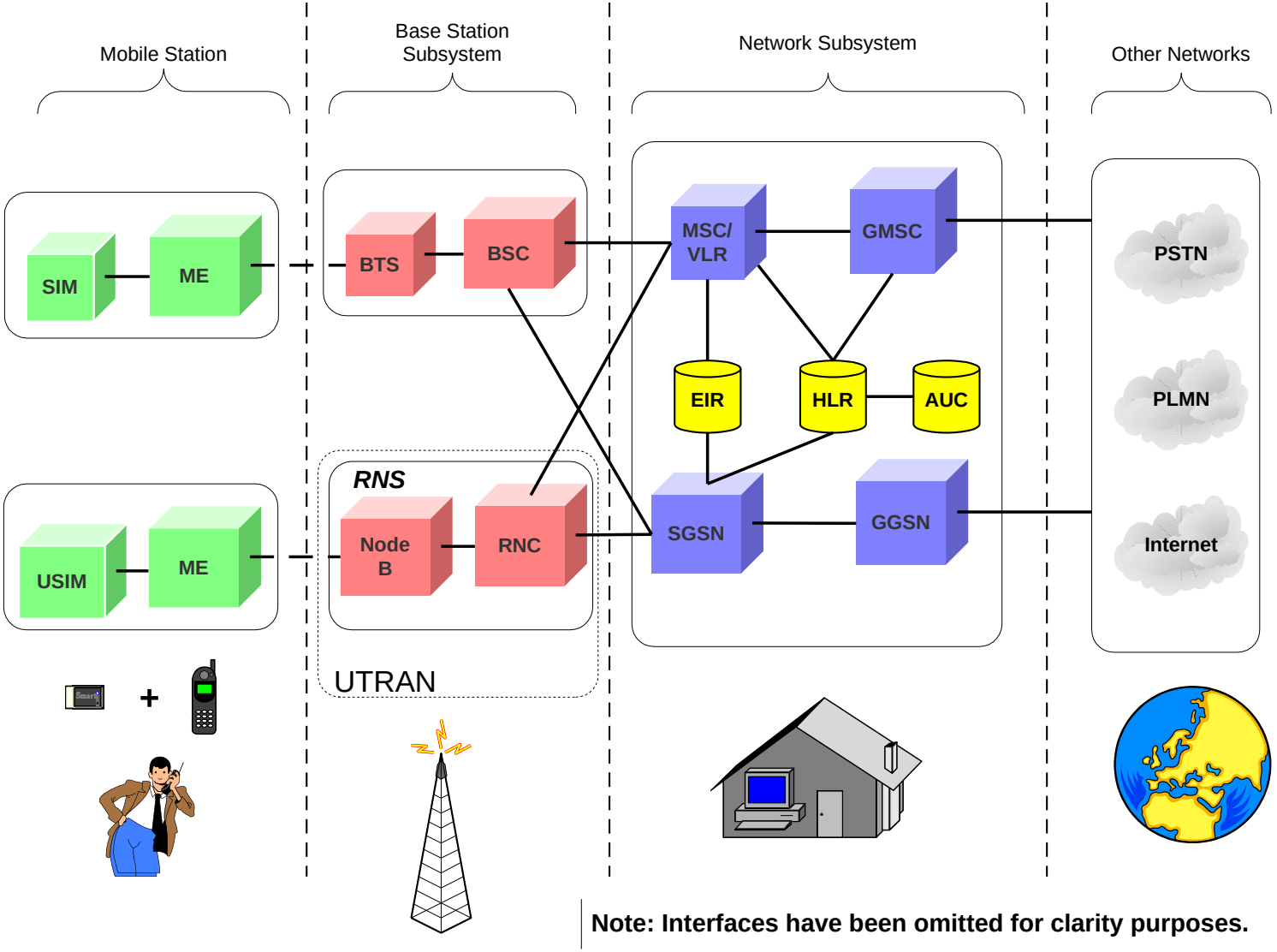
- 3G system
- Oriented to generalized service diffusion and its future users trends
  - Combines cellular, wireless, paging, etc. functions
- “multimedia everywhere”
- Developed as an evolution path of 2.5G systems
  - Progressive evolution (GPRS-EDGE-UMTS)
- Data rates of UMTS are:
  - 144 kbps for rural
  - 384 kbps for urban outdoor
  - 2048 kbps for indoor and low range outdoor

UMTS Frequency Spectrum

- **UMTS Band**
  - **1900-2025 MHz and 2110-2200 MHz for 3G transmission**
  - **In the US, 1710–1755 MHz and 2110–2155 MHz will be used instead, as the 1900 MHz band was already used.**



UMTS Architecture



Note: Interfaces have been omitted for clarity purposes.

UMTS takes advantage of the existing GSM and GPRS networks

The main difference between come with the new radio interface called as Uu.s.

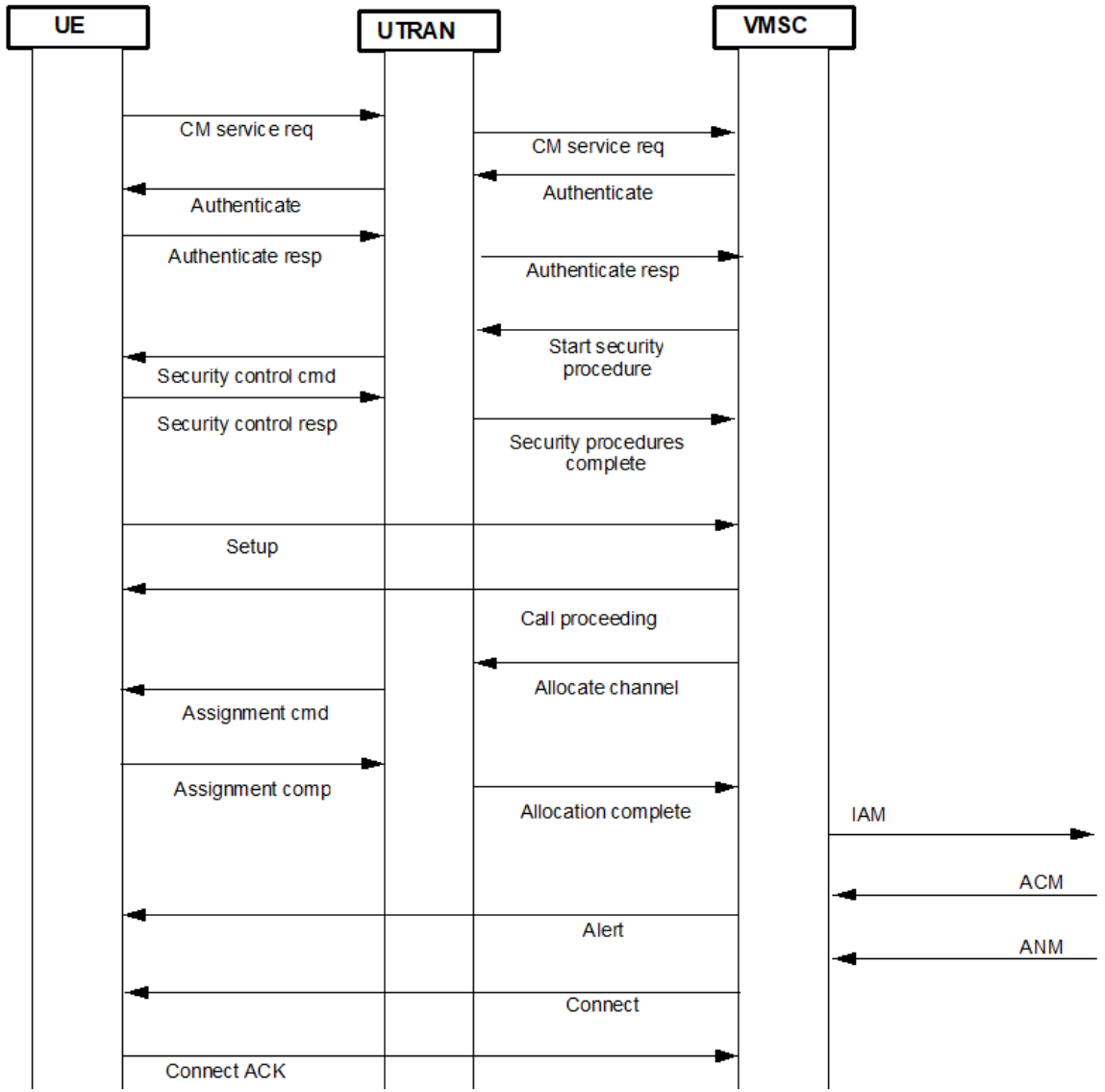
UMTS Network Architecture

- UMTS network architecture consists of three domains
  - Core Network (CN): Provides switching, routing and transit for user traffic
  - UMTS Terrestrial Radio Access Network (UTRAN): Provides the air interface access method for user equipment.
  - User Equipment (UE): Terminals work as air interface counterpart for base stations. The various identities are: IMSI, TMSI, P-TMSI, TLLI, MSISDN, IMEI, IMEISV

UTRAN

- Wide band CDMA technology is selected for UTRAN air interface
  - WCDMA
  - TD-SCDMA
- Base stations are referred to as Node-B and control equipment for Node-B is called as Radio Network Controller (RNC).
  - Functions of Node-B are
    - Air Interface Tx/Rx
    - Modulation/Demodulation
  - Functions of RNC are:
    - Radio Resource Control
    - Channel Allocation
    - Power Control Settings
    - Handover Control
    - Ciphering
    - Segmentation and reassembly

User Call initiation



4G (LTE)

- LTE stands for Long Term Evolution
- Next Generation mobile broadband technology
- Data transfer rates of 100 Mbps
- Based on UMTS 3G technology
- Optimized for All-IP traffic

Advantages of LTE

- High network throughput
- Low latency
- Plug & Play architecture
- Low Operating Costs
- All-IP network
- Simplified upgrade path from 3G networks

for Network Operators

- Faster data downloads/uploads
- Improved response for applications
- Improved end-user experience

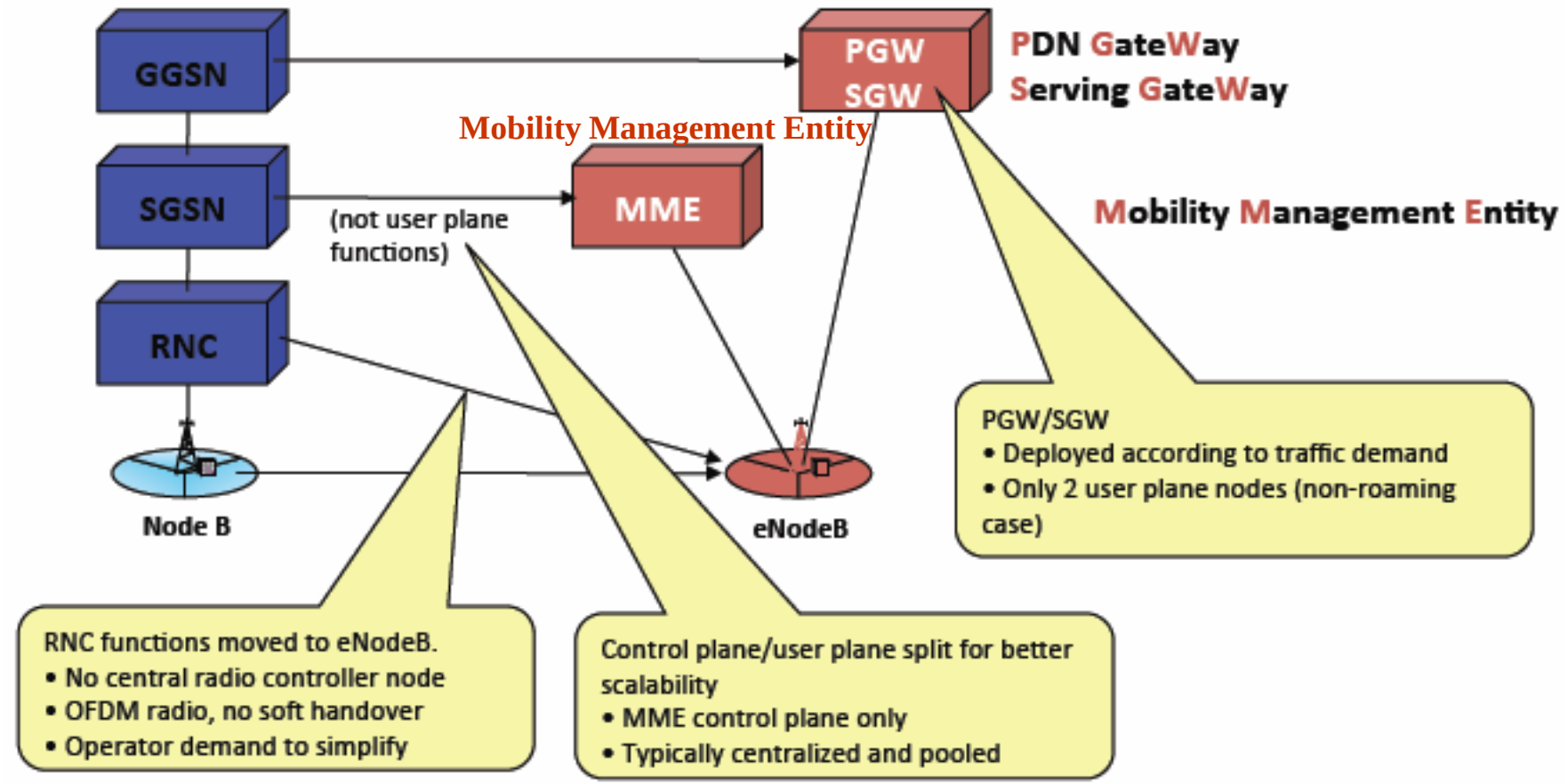
for End Users

Major LTE Radio Technogies

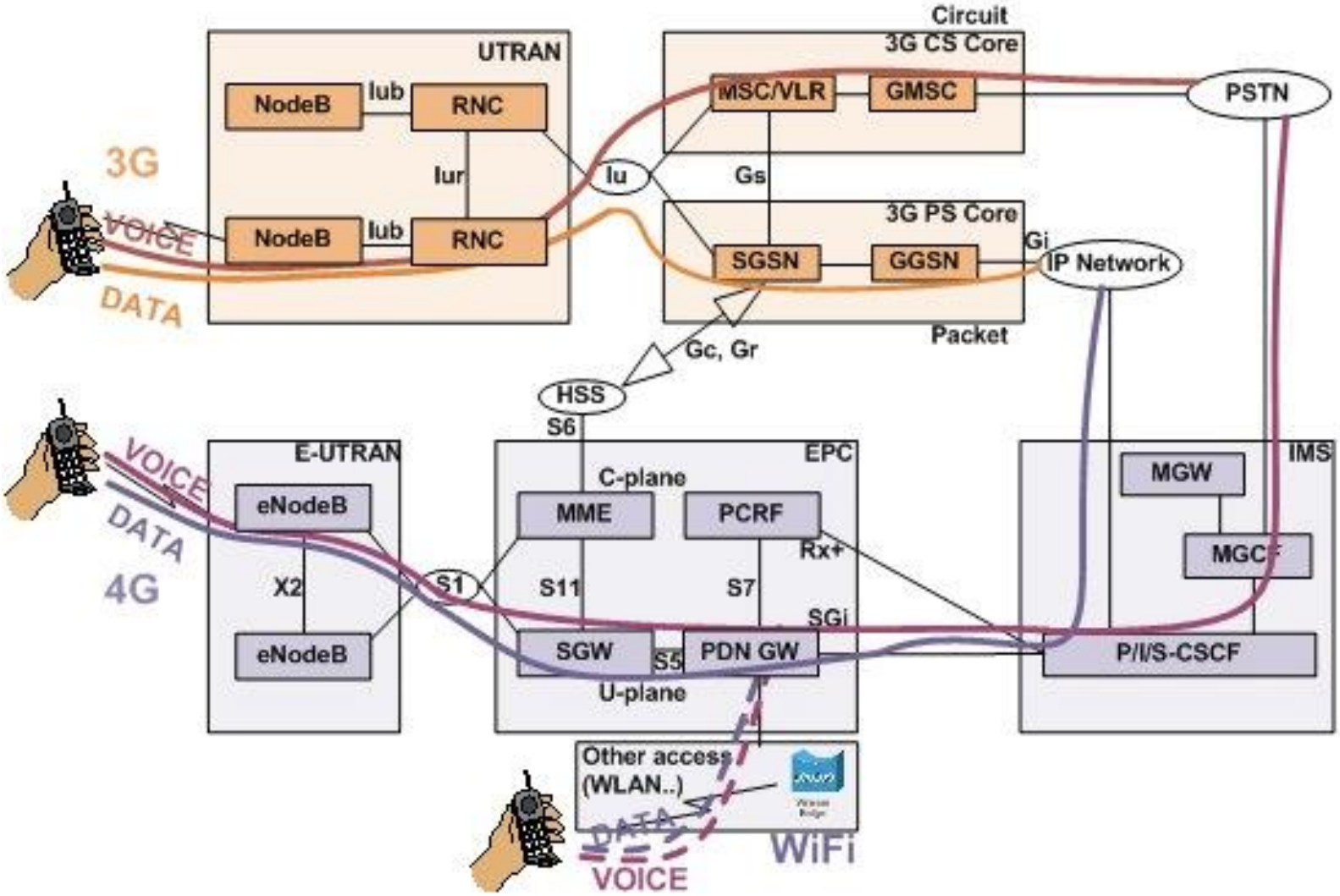
- Uses Orthogonal Frequency Division Multiplexing (OFDM) for downlink
- Uses Single Carrier Frequency Division Multiple Access (SC-FDMA) for uplink
- Uses Multi-input Multi-output(MIMO) for enhanced throughput
- Reduced power consumption
- Higher RF power amplifier efficiency (less battery power used by handsets)

LTE vs UMTS

- Functional changes compared to the current UMTS architecture



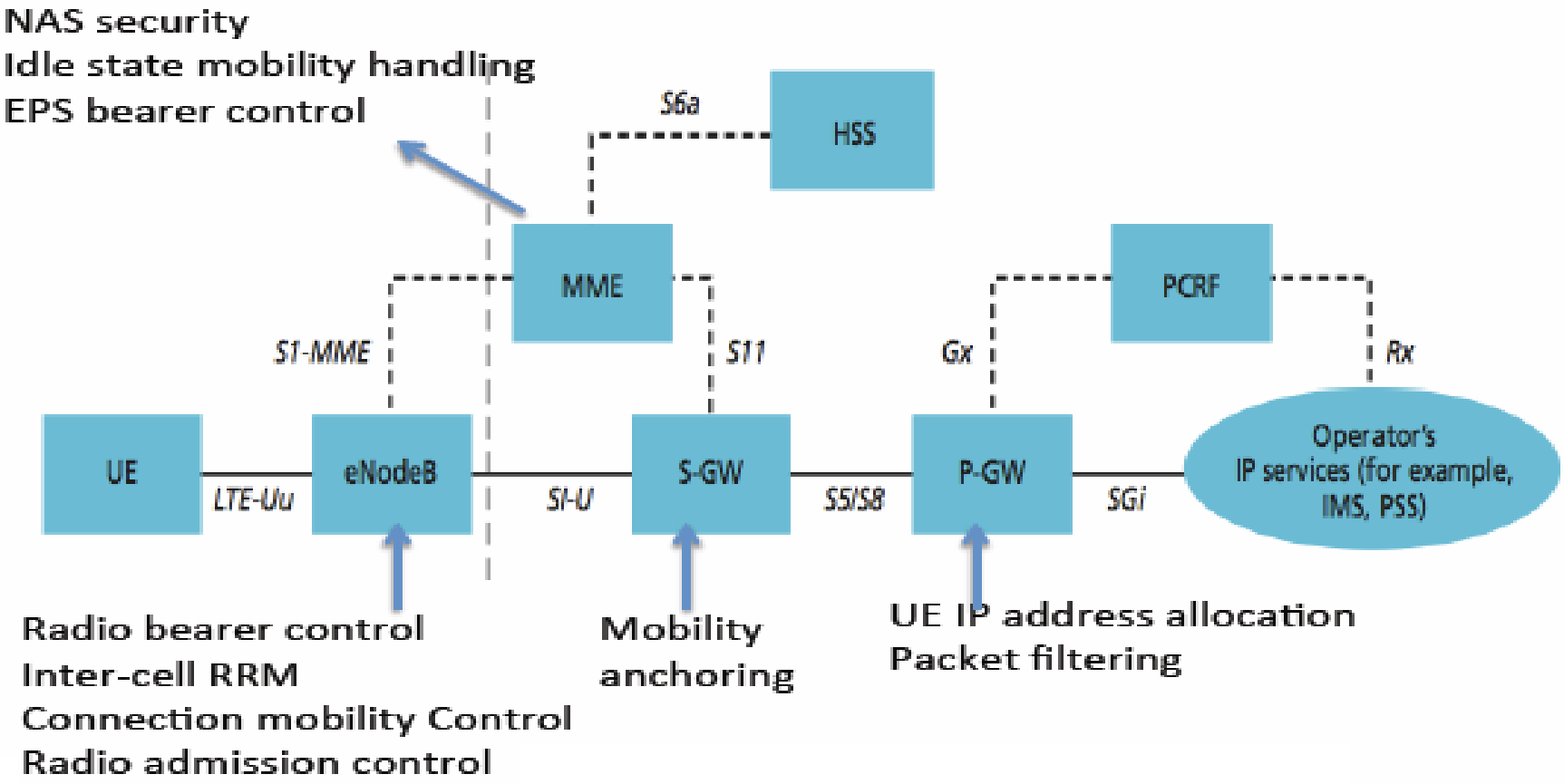
LTE vs UMTS


Circuit
3G CS Core
UTRAN
NodeB
Iub
RNC
MSC/VLR
GMSC
PSTN
3G
Iur
Iu
Gs
VOICE
NodeB
Iub
RNC
3G PS Core
Gi
SGSN
GGSN
IP Network
DATA
Packet
Gc, Gr
HSS
S6
VOICE
E-UTRAN
EPC
IMS
C-plane
MGW
eNodeB
MME
PCRF
DATA
Rx+
MGCF
4G
X2
S1
S11
S7
SGi
eNodeB
SGW
S5
PDN GW
P/I/S-CSCF
U-plane
Other access
(WLAN..)
DATA
WiFi
VOICE

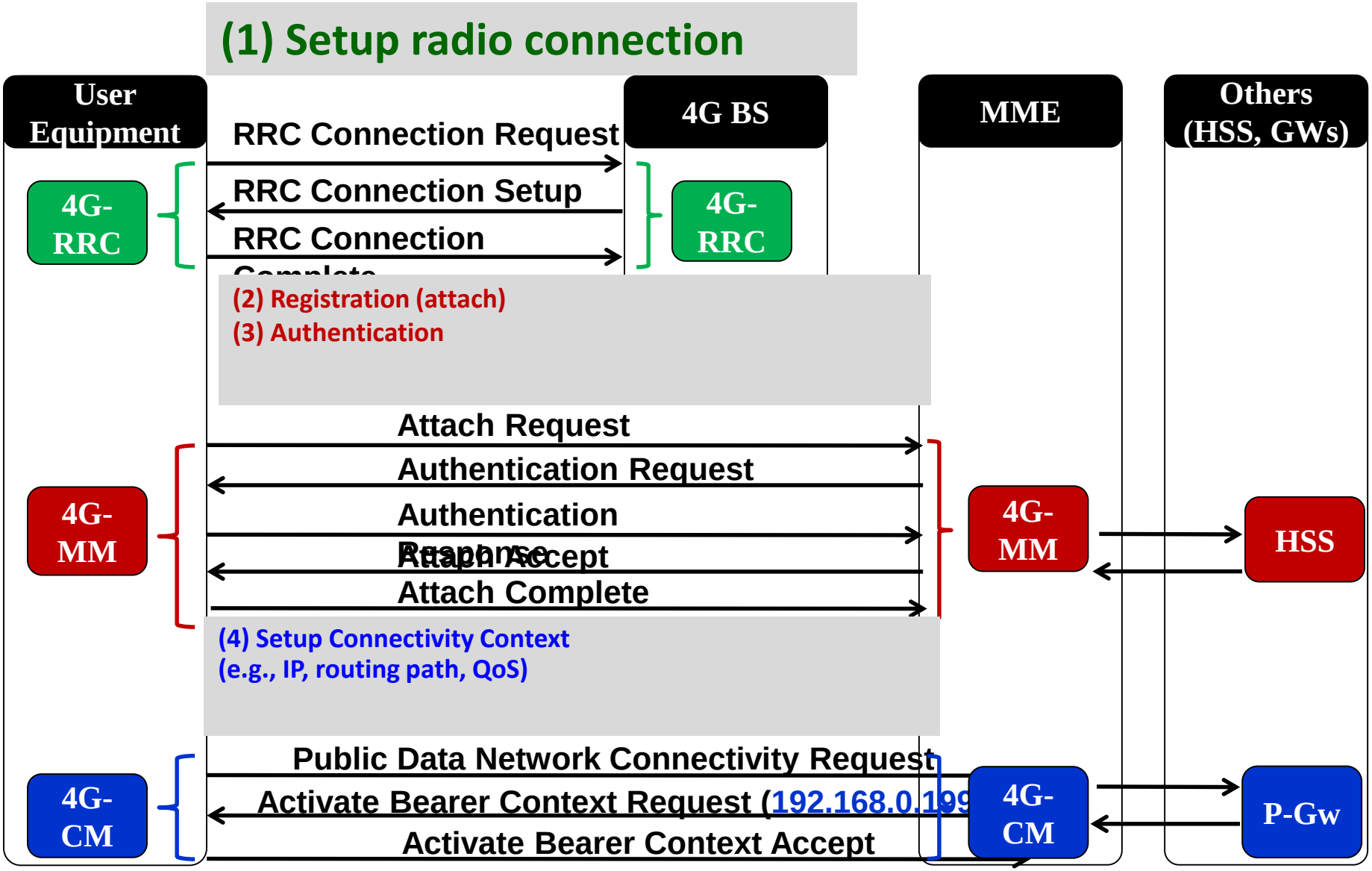
UMTS vs LTE

- LTE with simplified RAN architecture - with only Base stations, called eNodeB; UMTS uses Base stations (NodeB) and Controllers (RNC). In this case, eNB captures the functions of both UMTS NB and UMTS RNC - e.g. scheduling of the radio resources
- LTE uses OFDMA as radio access scheme, while UMTS uses WCDMA
- LTE supports “flexible system BW” - 1.4 to 20MHz, while UMTS uses fixed carrier BW - 5MHz
- LTE is an IP only system, while UMTS supports “old voice” core network and data core network.

LTE Architecture

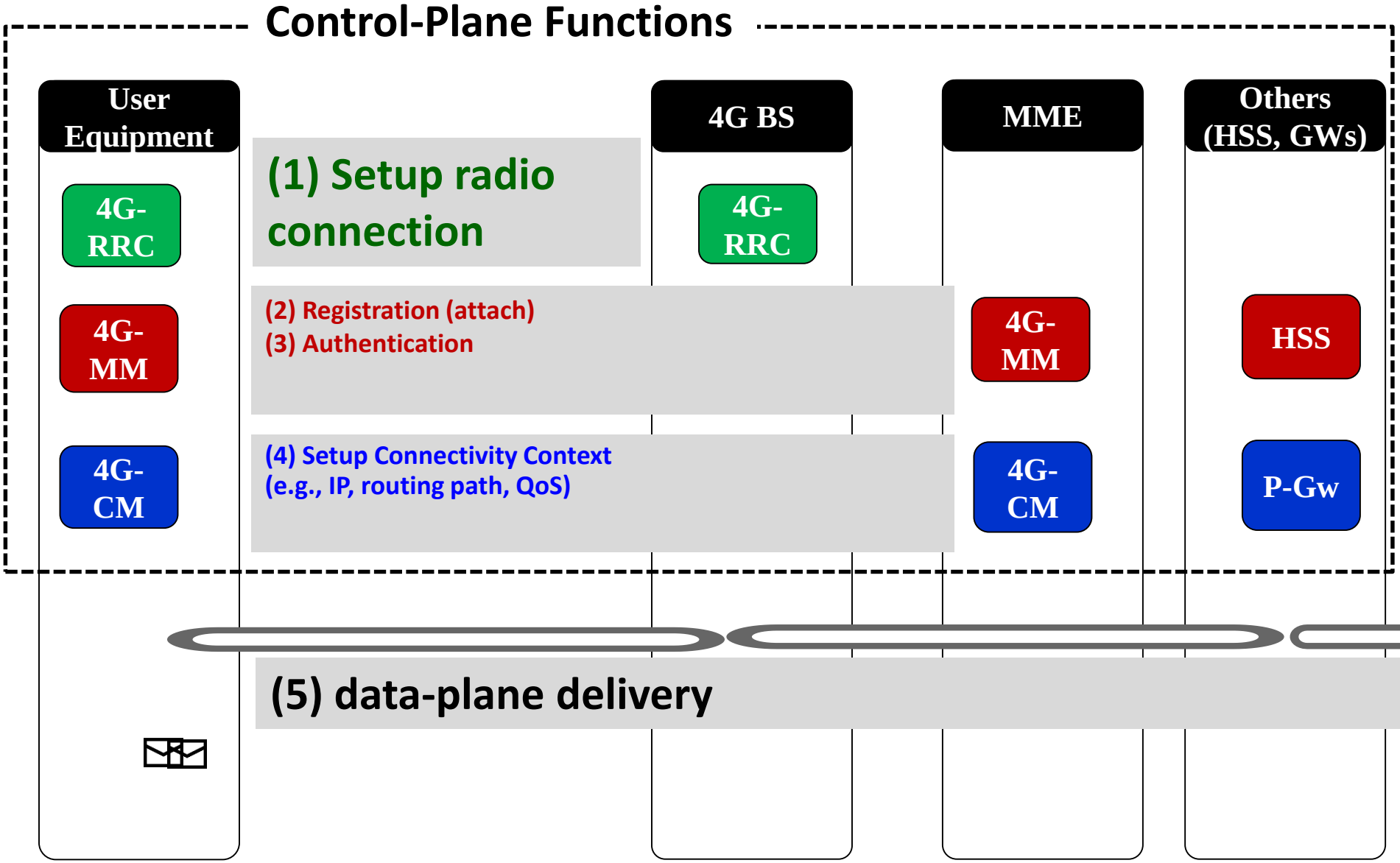


Setting Up Data Service in 4G



PDN: Public Data Network EPS: Evolved Packet System

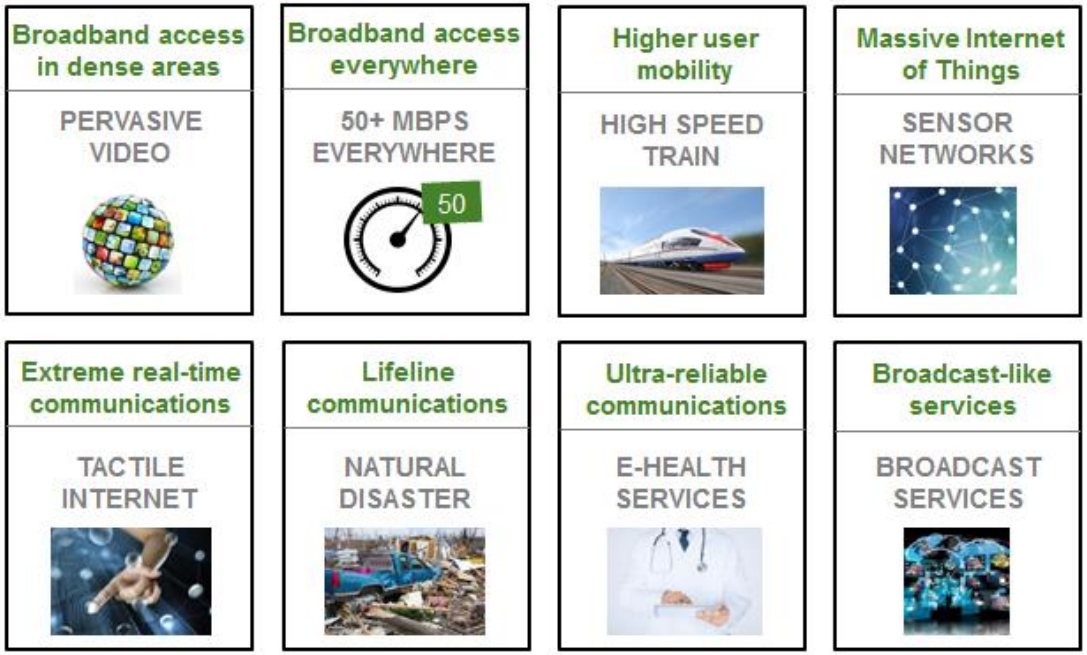
Setting Up Data Service in 4G



5G: what's different?

- **Service, application and business case-led definition**

5G Vision defined around Business Context, and Characterisation based on Use Cases, Business Models and Value Creation

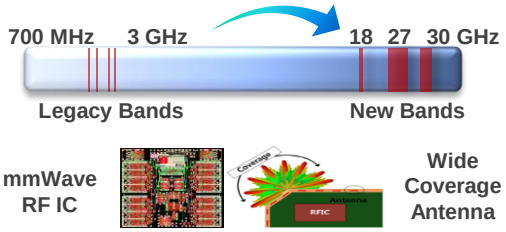


5G: Same network for all

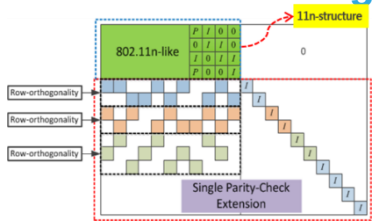
Requirements	Applications	Customer segments	MNO biz model
• 10x bandwidth per connection • Low-ms latency • Five 9's reliability • 100% coverage • >10x connections • 50Mbps per connection everywhere • 1000x bandwidth/area • 10 year battery life • Reduction in total cost of ownership	• Enhanced Mobile BB • Connected vehicles • AR/VR • S-UHD/3D Video • Haptics/Sensing • Massive IoT • Remote machine control • Mission critical services • Fixed-wireless access • …	• Consumer • Auto industry • Health • Industry 4.0 • Agriculture • Smart City/Public sector • Smart building • Utilities • Education • Transport • …	• B2C • B2B • B2B2C

5G 'Parts'

mmWave System/RFIC/Ant.

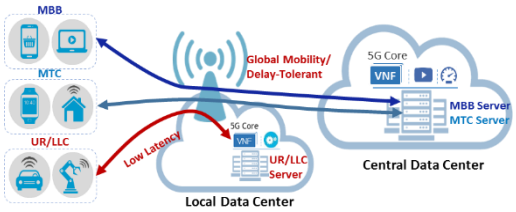


New Channel Coding

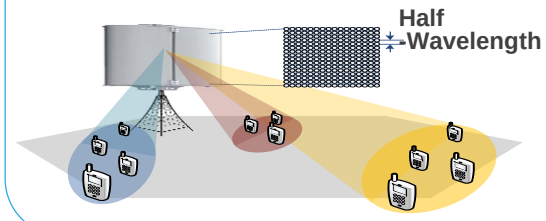


LDPC (Low-Density Parity-Check)

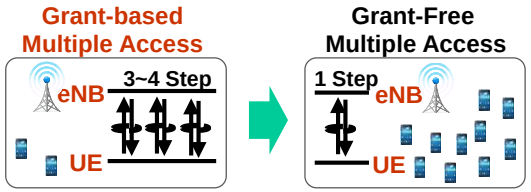
Network Slicing



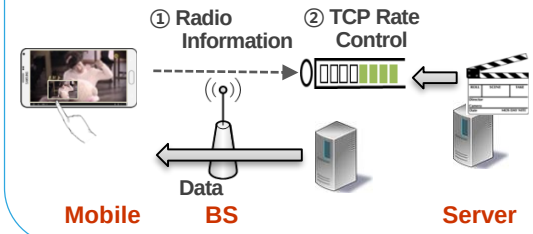
< 6 GHz Massive MIMO



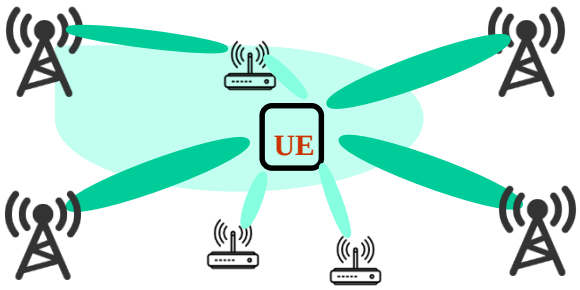
Massive Connectivity (IoT)



Low Latency Network



5G RAN Architecture Extensions



New Air Interface

- **Cyclic Prefix-OFDM – to introduce flexibility in OFDM and mitigate Inter Symbol Interference**
- **Massive MIMO – large numbers of bearers to increase bandwidth in sub-6GHz bands**
- **mmWave – provides access to broad frequency bands for higher bandwidths**
- **Beam Forming – extends range/cell size for mmWave bands**
- **Shortened Transmission Time Interval (TTI) – reduces latency**
- **Flexibility in band sizing – allows previously unavailable bands to be used**

Other RAN innovations

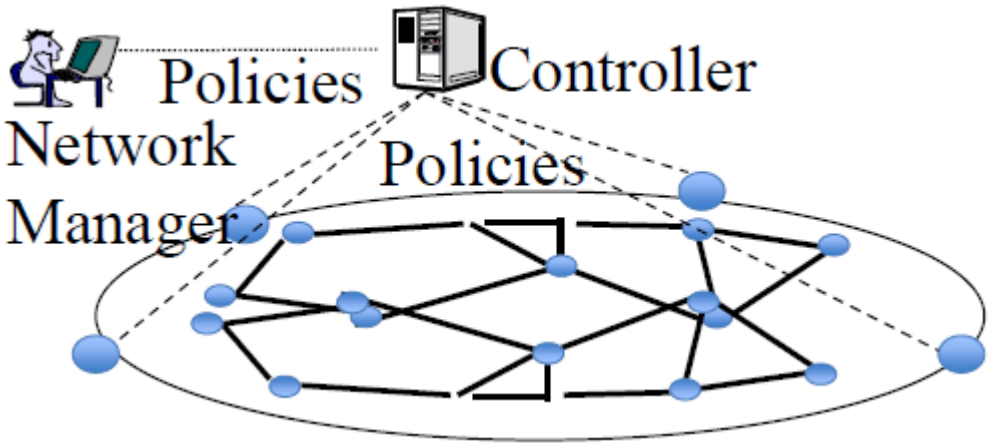
- **CoMP (Coordinated Multipoint) – UE attached to multiple cells to provide greater reliability**
- **Small cell support – greater indoor coverage, increased cell density, self-backhauling**
- **5G-NR in unlicensed bands – extension of mobile ecosystem**
- **Session management split from mobility management – enabler for RAN slicing**
- **D2D, V2X – devices connecting directly, with no network**

Non-Radio 5G

- Software Defined Networking (SDN)
- Network Function Virtualization (NFV)
- Mobile Edge Computing (MEC)
- Cloud Radio Access Network (C-RAN)

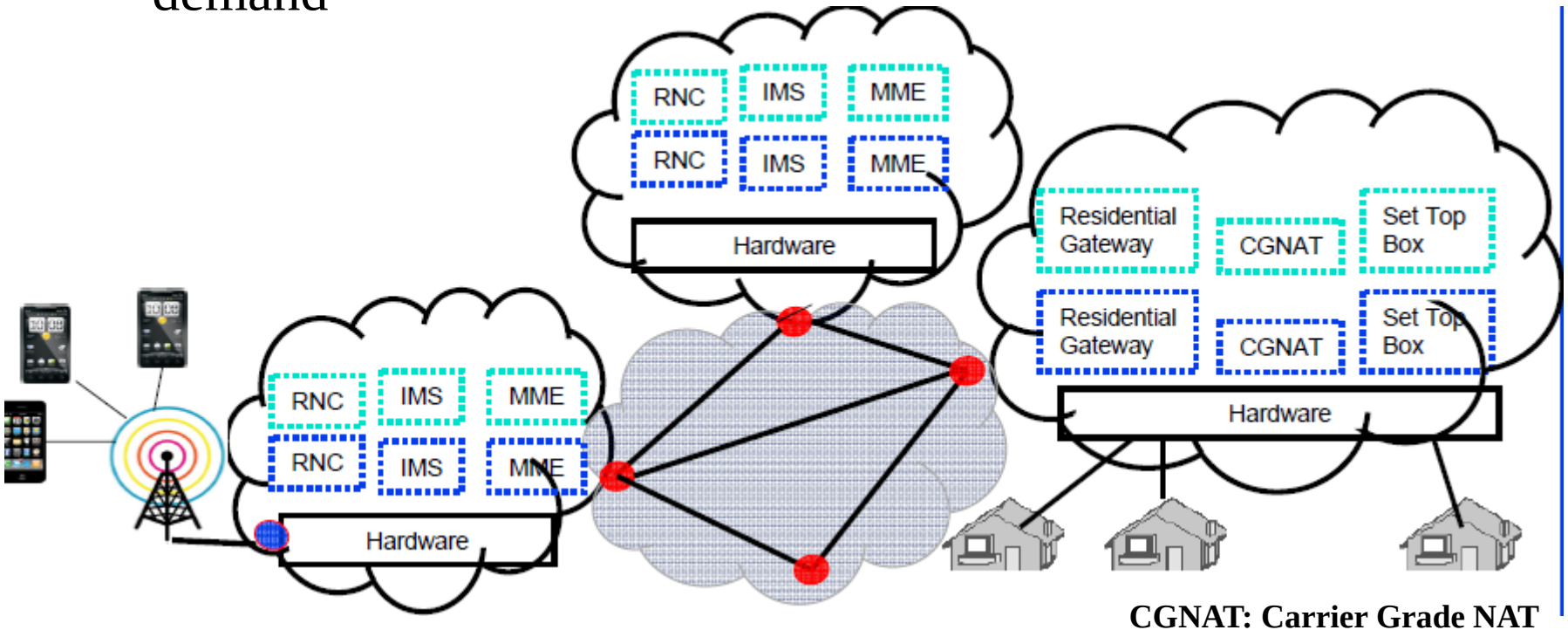
Software Defined Networks (SDN)

- Abstract the Hardware: No dependence on physical infrastructure. Software API.
- Programmable: Shift away from static manual operation to fully configurable and dynamic
- Centralized Control of Policies: Policy delegation and management



Networks Function Virtualization (NFV)

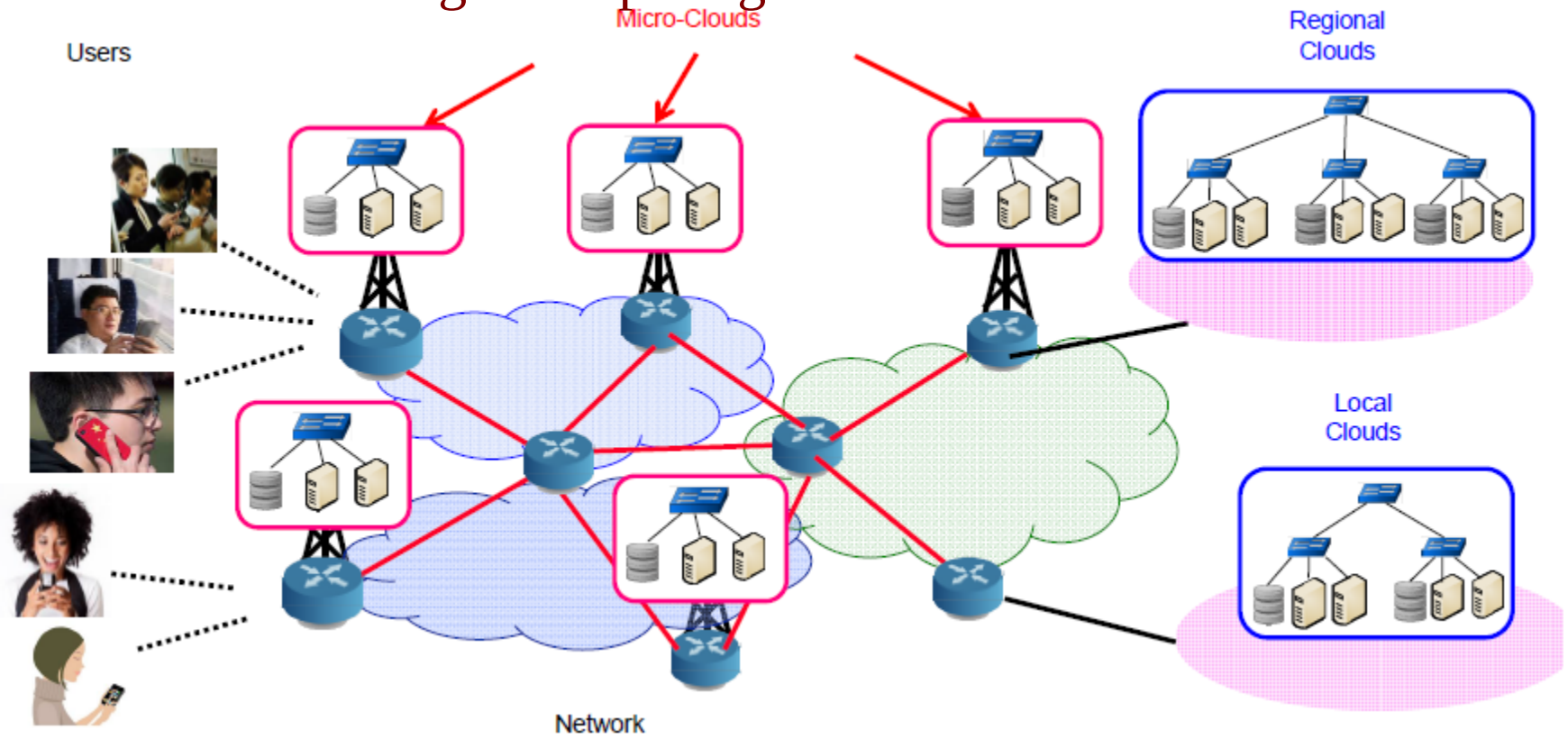
- Standard hardware is fast and cheap → No specialized hardware
- Implement all functions in software
- Virtualize all functions in the Cloud → Create capacity on demand



CGNAT: Carrier Grade NAT

Mobile Edge Computing (MEC)

- To service mobile users/IoT, the computation needs to go to the edge
  - Mobile Edge Computing

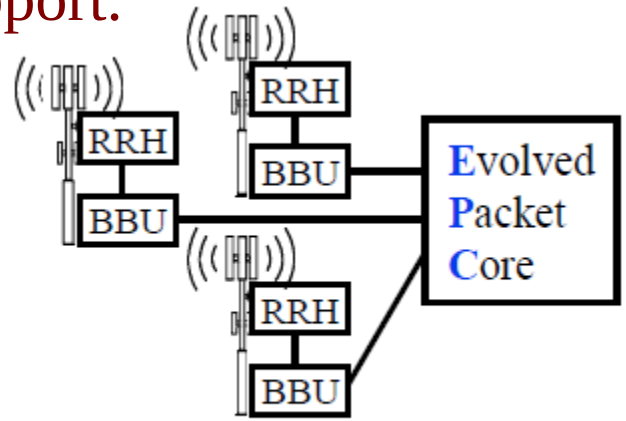


Cloud-Radio Access Network

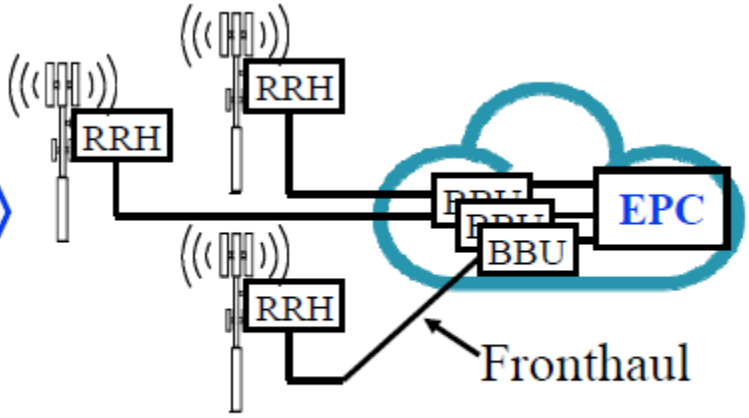
- Centralize baseband processing in a cloud
  - Need to carry high-bit rate signal (after A-to-D conversion) from tower to cloud site ~ 10 Gbps
- Optical fiber, 10 Gbps Ethernet, Microwave can be used depending upon the distance ~ 1-20 km of **fronthaul**
  - Particularly good for dense small cells; multi-provider support.

Remote Radio Head

Base Band Unit

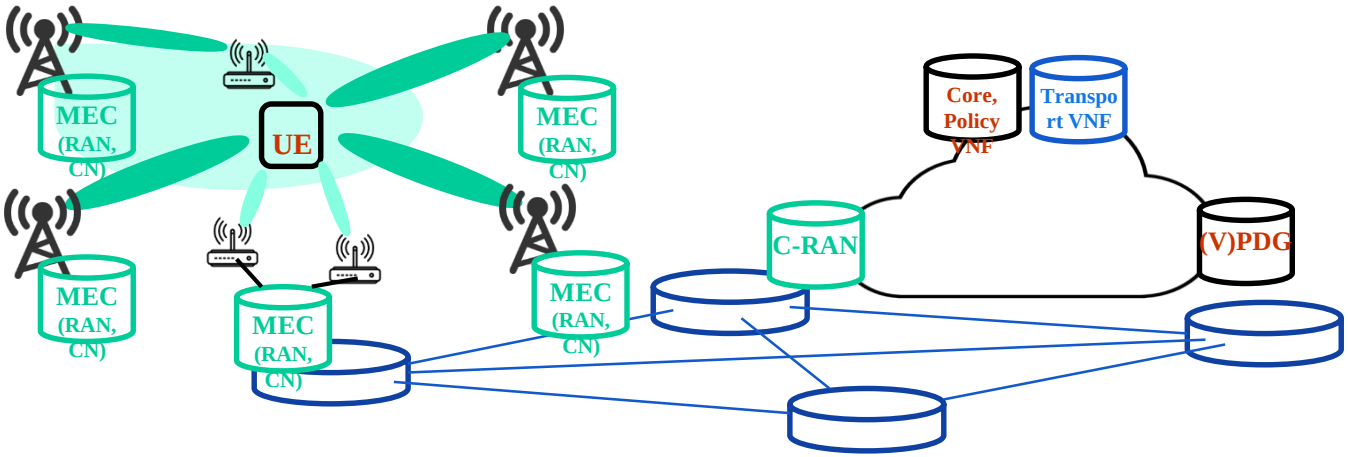


Distributed RAN



Cloud RAN

5G Core Architecture Extensions



‘Softwarisation’ of the network

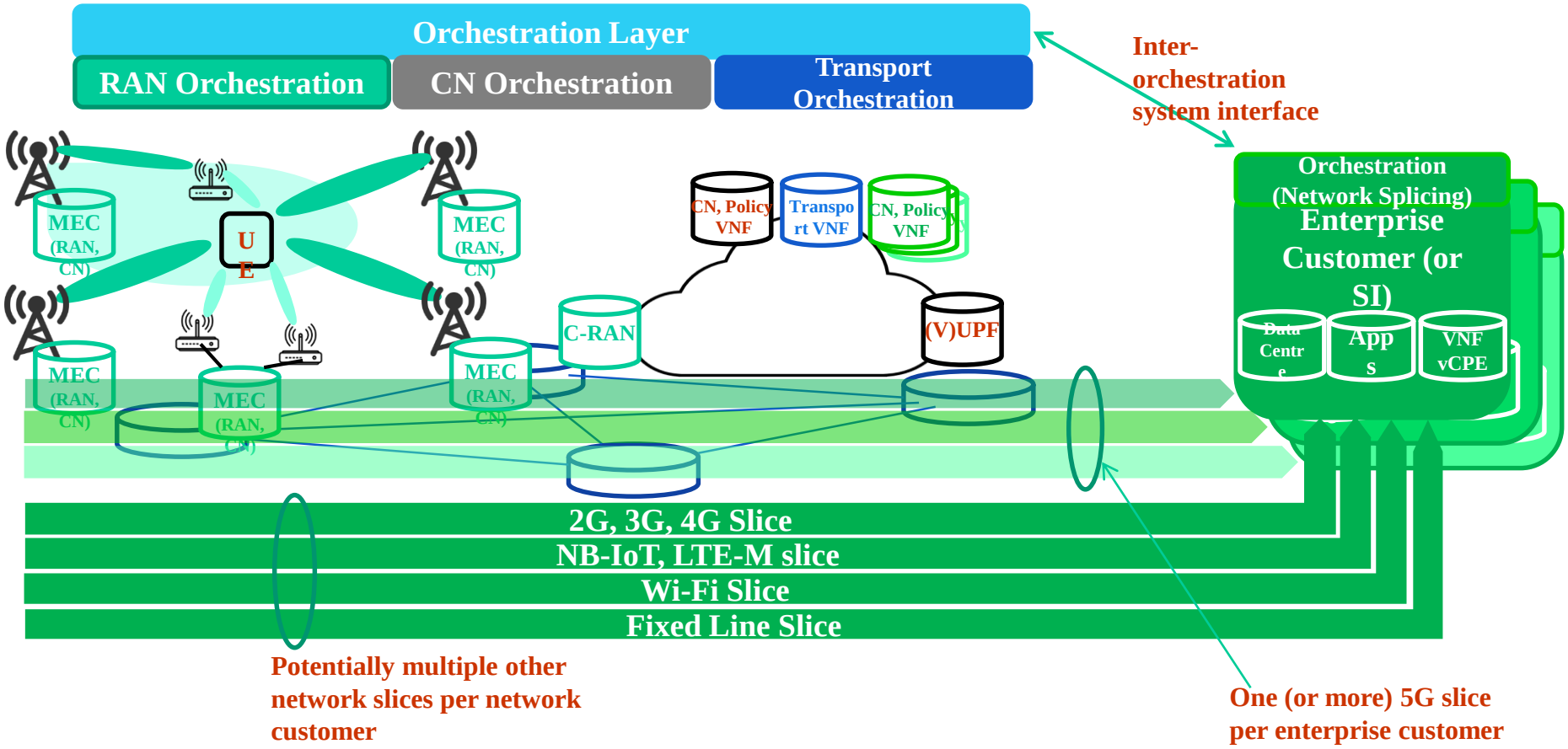
C-RAN – removal of functionality from cell sites to consolidation point in the network

NFV and SDN – enabling flexibility in where functions are deployed and scaled

MEC – pushing Core Network functions and content ingress to cell sites

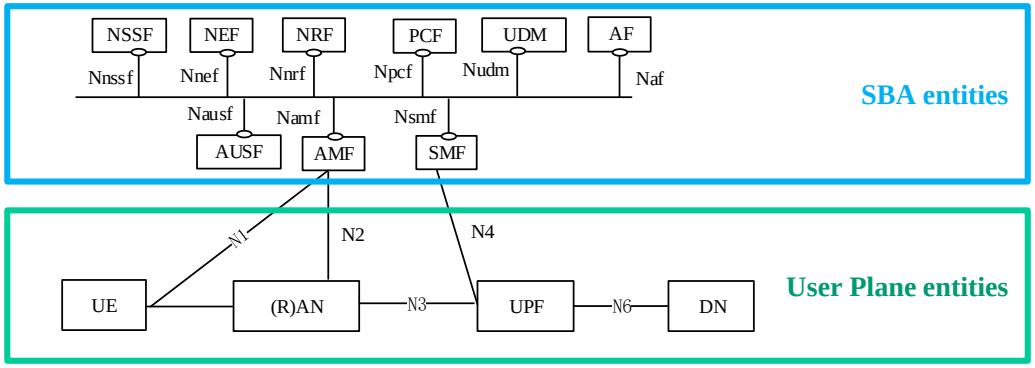
CP/UP split – decoupling of user plane traffic from control plane functions

Multi-slicing



5G Architecture

5G system architecture depicted in the Service Based Architecture (SBA) style (from TS 23.501)

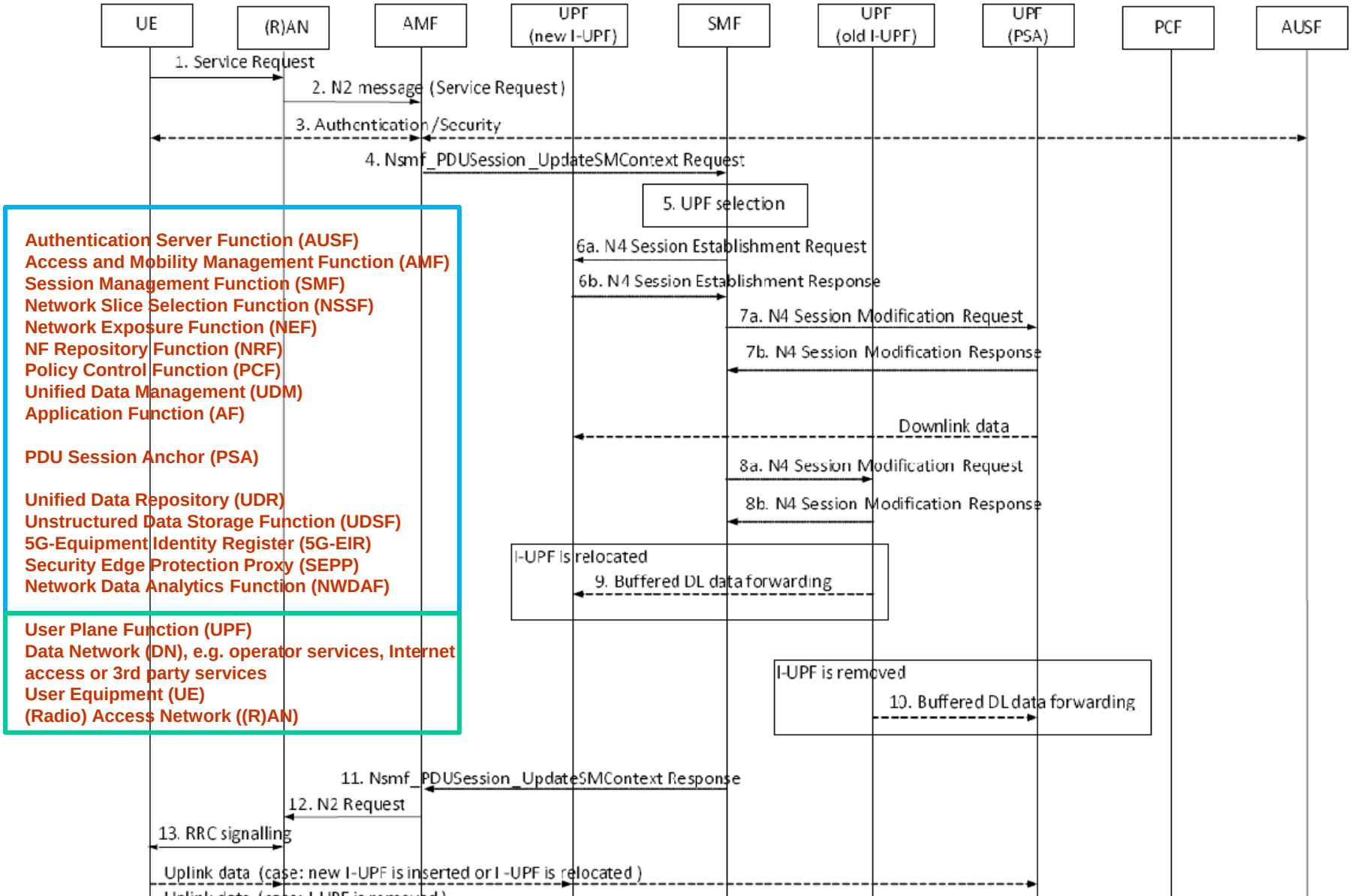


Authentication Server Function (AUSF)
Access and Mobility Management Function (AMF)
Session Management Function (SMF)
Network Slice Selection Function (NSSF)
Network Exposure Function (NEF)
Network Function Repository Function (NRF)
Policy Control Function (PCF)
Unified Data Management (UDM)
Application Function (AF)

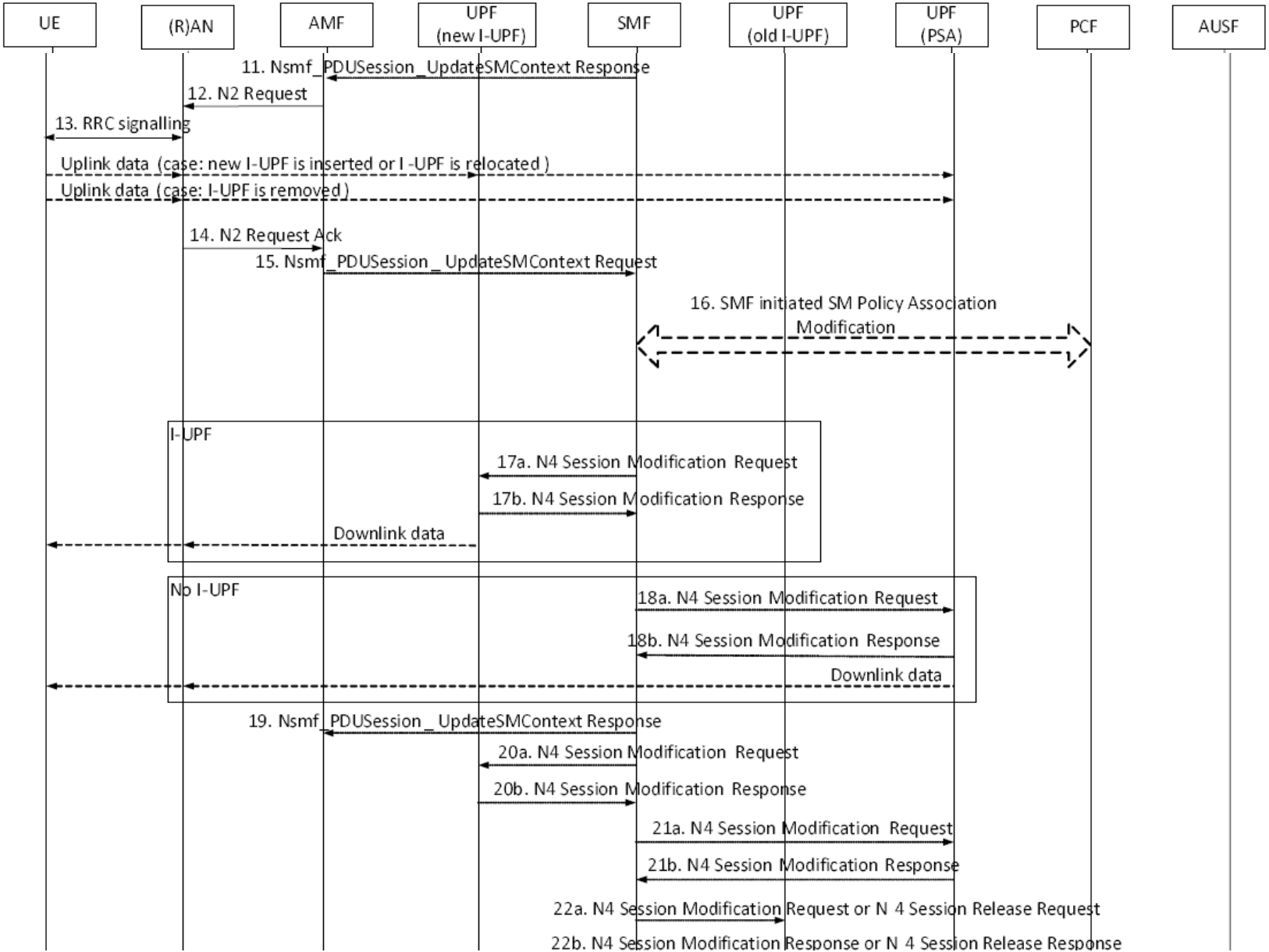
Unified Data Repository (UDR)
Unstructured Data Storage Function (UDSF)
5G-Equipment Identity Register (5G-EIR)
Security Edge Protection Proxy (SEPP)
Network Data Analytics Function (NWDAF)

User Plane Function (UPF)
Data Network (DN), e.g. operator services, Internet access or 3rd party services
User Equipment (UE)
(Radio) Access Network ((R)AN)

5G Service Request



5G Service Request



Heterogeneous Future Networks