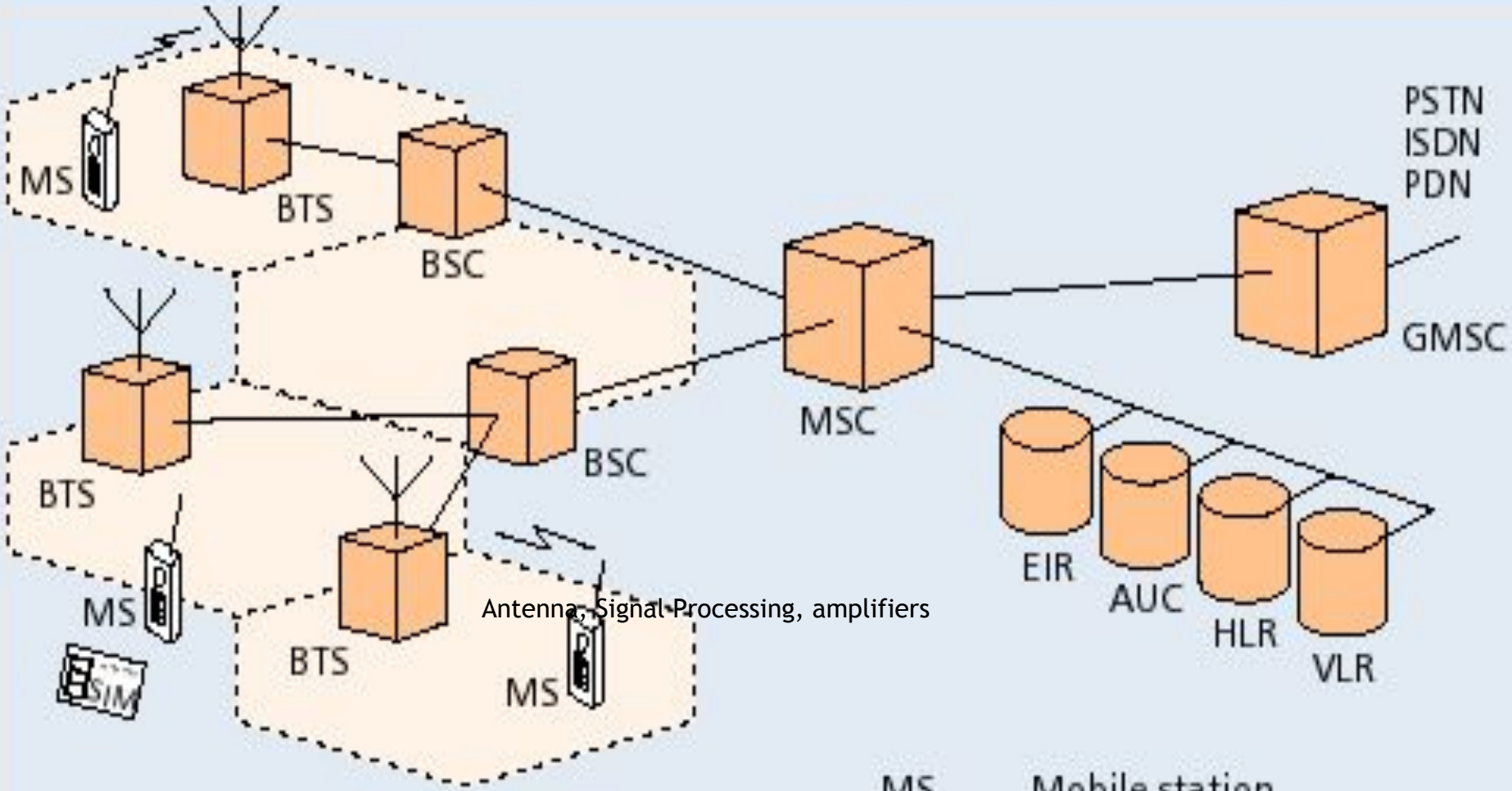
GSM Mobile Services

Module 2

Introduction

- The **Global System for Mobile Communications** (**GSM**) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as mobile phones and tablets
- 2G networks developed as a replacement for first generation (1G) analog cellular networks.
- The GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony.

GSM Architecture

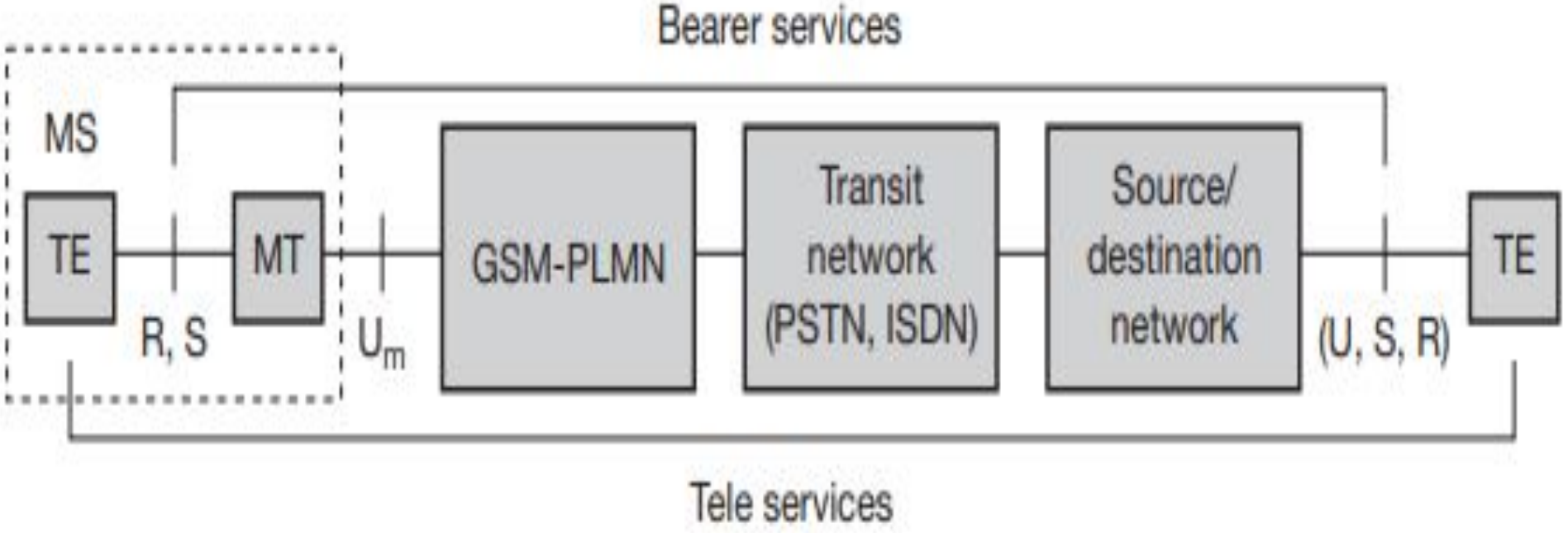


BTS	Base transceiver station	MS	Mobile station
BSC	Base station controller	HLR	Home location register
BSS	Base station subsystem (BTS+BSC)	VLR	Visited location register
MSC	Mobile switching center	EIR	Equiment identity register
GMSC	Gateway MSC	AUC	Authentication center

- GSM has initially been deployed in Europe using 890–915 MHz for uplinks and 935–960 MHz for downlinks – this system is now also called GSM 900
- GSM at 1800 MHz (1710–1785 MHz uplink, 1805–1880 MHz downlink), also called DCS (digital cellular system) 1800,
- The GSM system mainly used in the US at 1900 MHz (1850–1910 MHz uplink, 1930–1990 MHz downlink), also called PCS (personal communications service) 1900
- GSM 400 is a proposal to deploy GSM at 450.4–457.6/478.8–486 MHz for uplinks and 460.4–467.6/488.8–496 MHz for downlinks. This system could replace analog systems in sparsely populated areas
- GSM-Rail (GSM-R, 2002), (ETSI, 2002). This system does not only use separate frequencies but offers many additional services which are unavailable using the public GSM system.
- GSM-R offers 19 exclusive channels for railroad operators for voice and data traffic, emergency calls with acknowledgements, voice group call service (VGCS), voice broadcast service (VBS)

Mobile services

- GSM permits the integration of different voice and data services and the inter working with existing networks. Services make a network interesting for customers.
- GSM has defined three different categories of services: bearer, tele, and supplementary services



a reference model for GSM services.

- A mobile station MS is connected to the GSM public land mobile network (PLMN) via the Um interface. (GSM-PLMN is the infrastructure needed for the GSM network.)
- This network is connected to transit networks, e.g., integrated services digital network (ISDN) or traditional public switched telephone network (PSTN).
- There might be an additional network, the source/destination network, before another terminal TE is connected.
- Bearer services now comprise all services that enable the transparent transmission of data between the interfaces to the network, i.e., S in case of the mobile station, and a similar interface for the other terminal (e.g., S0 for ISDN terminals).
- Interfaces like U, S, and R in case of ISDN have not been defined for all networks, so it depends on the specific network which interface is used as a reference for the transparent transmission of data.

- In the classical GSM model, bearer services are connection-oriented and circuit- or packet-switched. These services only need the lower three layers of the ISO/OSI reference model.
- Within the mobile station MS, the mobile termination (MT) performs all network specific tasks (TDMA, FDMA, coding etc.) and offers an interface for data transmission (S) to the terminal TE which can then be network independent.
- Depending on the capabilities of TE, further interfaces may be needed, such as R, according to the ISDN reference model .
- Tele services are application specific and may thus need all seven layers of the ISO/OSI reference model. These services are specified end-to-end, i.e., from one terminal TE to another

1.Bearer services/Data services

- Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission.
- Transparent bearer services only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur.
- The only mechanism to increase transmission quality is the use of forward error correction (FEC), which codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors,.
- Transparent bearer services do not try to recover lost data in case of, for example, shadowing or interruptions due to handover.

- Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control. These services use the transparent bearer services, adding a radio link protocol (RLP).
- This protocol comprises mechanisms of high-level data link control (HDLC), and special selective-reject mechanisms to trigger retransmission of erroneous data
- Using transparent and non-transparent services, GSM specifies several bearer services for interworking with PSTN, ISDN, and packet switched public data networks (PSPDN) like X.25, which is available worldwide.
- Data transmission can be full-duplex, synchronous with data rates of 1.2, 2.4, 4.8, and 9.6 kbit/s or full-duplex, asynchronous from 300 to 9,600 bit/s

2.Tele services/ telephony services

- GSM mainly focuses on voice-oriented tele services. These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN (e.g., fax)
- telephony, the primary goal of GSM was the provision of high-quality digital voice transmission, offering at least the typical bandwidth of 3.1 kHz of analog phone systems.
- Special codecs (coder/decoder) are used for voice transmission, while other codecs are used for the transmission of analog data for communication with traditional computer modems used in, e.g., fax machines
- emergency number, The same number can be used throughout Europe. This service is mandatory for all providers and free of charge. This connection also has the highest priority, possibly pre-empting other connections, and will automatically be set up with the closest emergency center

- short message service (SMS), which offers transmission of messages of up to 160 characters. SMS messages do not use the standard data channels of GSM but exploit unused capacity in the signaling channels .Sending and receiving of SMS is possible during data or voice transmission
- the enhanced message service (EMS), offers a larger message size (e.g., 760 characters, concatenating several SMs), formatted text, and the transmission of animated pictures, small images and ring tones in a standardized way
- multimedia message service (MMS) offers the transmission of larger pictures (GIF, JPG, WBMP), short video clips etc. and comes with mobile phones that integrate small cameras
- group 3 fax, which is available worldwide. In this service, fax data is transmitted as digital data over the analog telephone network according to the ITU-T standards T.4 and T.30 using modems. Typically, a transparent fax service is used, i.e., fax data and fax signaling is transmitted using a transparent bearer service

3. Supplementary services

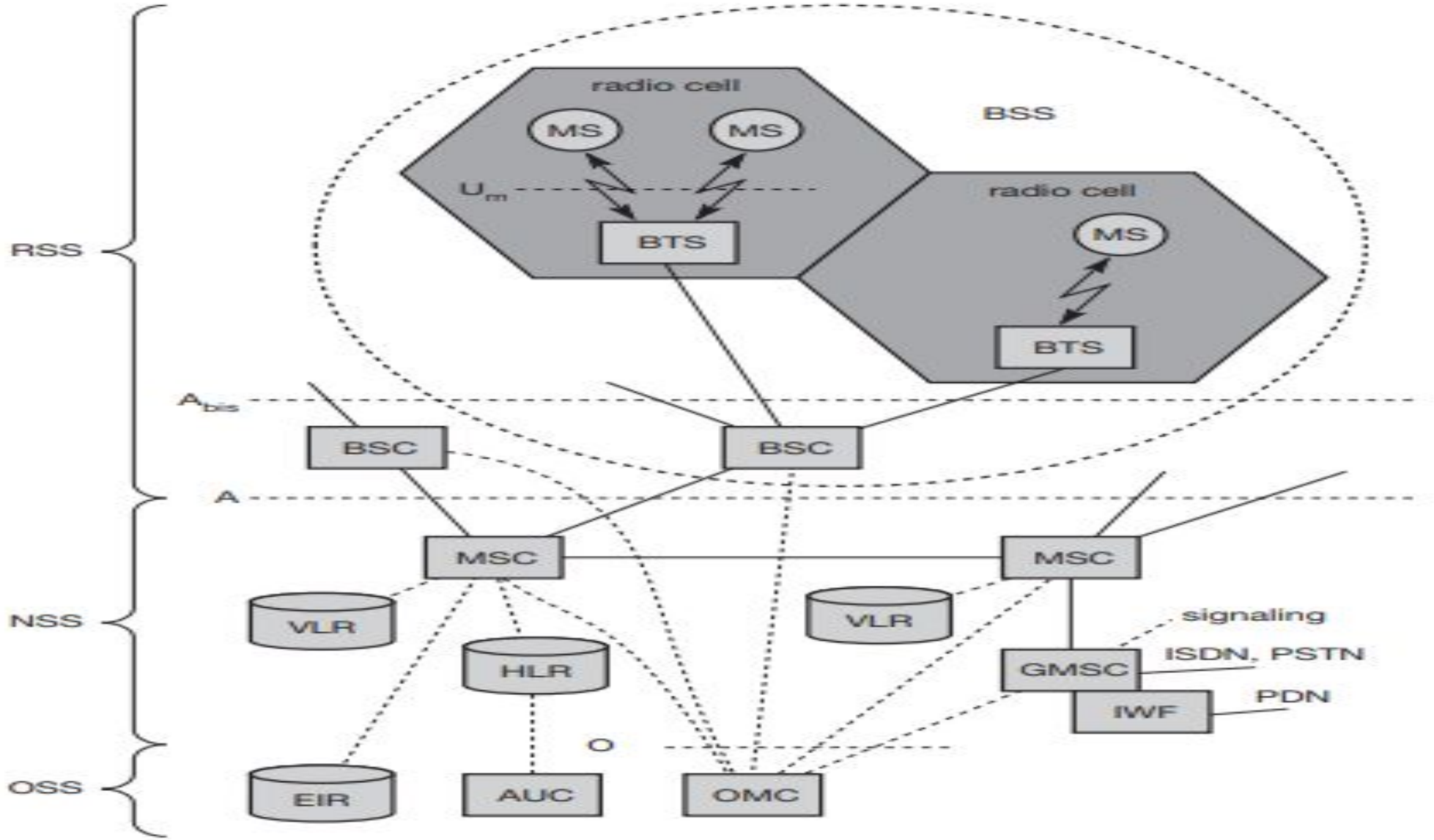
- Similar to ISDN networks, these services offer various enhancements for the standard telephony service, and may vary from provider to provider.
- Typical services are user identification, call redirection, or forwarding of ongoing calls.
- Standard ISDN features such as closed user groups and multiparty communication may be available.
- Closed user groups are of special interest to companies because they allow, for example, a company-specific GSM sub-network, to which only members of the group have access

GSM System Architecture

- As in the telecommunication area, GSM comes with a hierarchical, complex system architecture comprising many entities, interfaces, and acronyms.
- A GSM system consists of three subsystems,

1. the radio sub system (RSS),
2. the network and switching subsystem (NSS),
3. and the operation subsystem (OSS)

Functional Architecture of GSM System



1.Radio subsystem(RSS)

- The radio subsystem (RSS) comprises all radio specific entities, i.e.,

A. the mobile stations (MS) and

B. the base station subsystem (BSS).

- The connection between the RSS and the NSS is via the A interface and the connection to the OSS is via the O interface.
- The A interface is typically based on circuit-switched PCM-30 systems (2.048 Mbit/s), carrying up to 30 64 kbit/s connections,
- whereas the O interface uses the Signaling System No. 7 (SS7) based on X.25 carrying management data to/from the RSS.

A).Mobile station (MS):

- The MS comprises all user equipment and software needed for communication with a GSM network.
- An MS consists of user independent hardware and software and of the subscriber identity module (SIM), which stores all user-specific data that is relevant to GSM like charging and authentication
- MS can be identified via Device-specific mechanisms the international mobile equipment identity (IMEI)
- Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a personal identity number (PIN), a PIN unblocking key (PUK), an authentication key Ki , and the international mobile subscriber identity (IMSI)

- The MS stores dynamic information while logged onto the GSM system, such as, e.g., the cipher key Kc and the location information consisting of a temporary mobile subscriber identity (TMSI) and the location area identification (LAI)
- MS can also offer other types of interfaces to users with display, loudspeaker, microphone, and programmable soft keys.
- Further interfaces comprise computer modems, IrDA, or Bluetooth.
- Typical MSs, e.g., mobile phones, comprise many more vendor-specific functions and components, such as cameras, fingerprint sensors, calendars, address books, games, and Internet browsers.
- Personal digital assistants (PDA) with mobile phone functions are also available.
- The reader should be aware that an MS could also be integrated into a car or be used for location tracking of a container.

B)Base station subsystem (BSS):

- A GSM network comprises many BSSs, each controlled by a base station controller (BSC). Besides a BSC, the BSS contains several BTSs.
- The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part.

a) Base transceiver station (BTS):

- A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission.
- A BTS can form a radio cell or, using sectorized antennas, several cells, and is connected to MS via the U_m interface (ISDN U interface for mobile use), and to the BSC via the A_{bis} interface

- The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.). The Abis interface consists of 16 or 64 kbit/s connections
- A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic.

b)Base station controller (BSC):

- The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS.
- The BSC also multiplexes the radio channels onto the fixed network connections at the A interface

Functions of-

BTS

1. Management of radio channels
2. Management of terrestrial channels
3. Mapping of terrestrial onto radio channels
4. Traffic measurement
5. Authentication
6. Location registry, location update
7. Handover management

BSC

1. Channel coding and decoding
2. Rate adaptation
3. Uplink signal measurement

2.The network switching system (NSS)

- NSS is a GSM element that provides flow management and call processing for mobile devices moving between base stations.
- The switching system consists of the functional units listed below.

A) Mobile Services Switching Center (MSC):

- Mobile Switching Center is integral to the GSM network architecture's central network space.
- The MSC supports call switching across cellular phones and other fixed or mobile network users.
- It also monitors cellular services, including registration, location updates, and call forwarding to a roaming user.

B) Home Location Register (HLR):

- It is a set of data items used for storing and managing subscriptions. It provides data for each consumer as well as their last known position.
- The HLR is regarded as the most significant database because it preserves enduring records about users.
- When a person purchases a membership from one of the operators, they are enlisted in that operator's HLR

C) Visitor Location Register (VLR):

- VLR is a database that provides subscriber information necessary for the MSC to service passengers.
- This includes a short-term version of most of the data stored in the HLR.
- The visitor location register can also be run as a standalone program, but it is usually implemented as a component of the MSC.

3.Operation subsystem (OSS)

- The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operation and maintenance.
- The OSS possesses network entities of its own and accesses other entities via SS7 signaling .
- The following entities have been defined:
- **A)Operation and maintenance center (OMC):**
- The OMC monitors and controls all other network entities via the O interface (SS7 with X.25).
- Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing.
- OMCs use the concept of telecommunication management network (TMN) as standardized by the ITU-T.

B) Equipment Identity Register (EIR):

- It is the component that determines if one can use particular mobile equipment on the system.
- This consists of a list of every functioning mobile device on the system, with each mobile device recognized by its own International Mobile Equipment Identity (IMEI) number

• C) Authentication Center (AuC):

- The AUC is a unit that offers verification and encryption factors to ensure the user's identity and the privacy of every call.
- The verification center is a secure file that contains the user's private key in the SIM card.
- The AUC shields network operators from various types of fraud prevalent in the modern-day cellular world.

Radio interface

- The most interesting interface in a GSM system is Um, the radio interface, as it comprises many mechanisms for multiplexing and media access
- GSM implements

1. SDMA using cells with BTS and assigns an MS to a BTS.
2. FDD is used to separate downlink and uplink
3. Media access combines TDMA and FDMA.

- In GSM 900, 124 channels, each 200 kHz wide, are used for FDMA.
- Due to technical reasons, channels 1 and 124 are not used for transmission in GSM 900.
- Typically, 32 channels are reserved for organizational data; the remaining 90 are used for customers.
- Each BTS then manages a single channel for organizational data and up to 10 channels for user data.

Uplink

- the uplink (radio link from the mobile to the network-that is, mobile transmit, base receive)

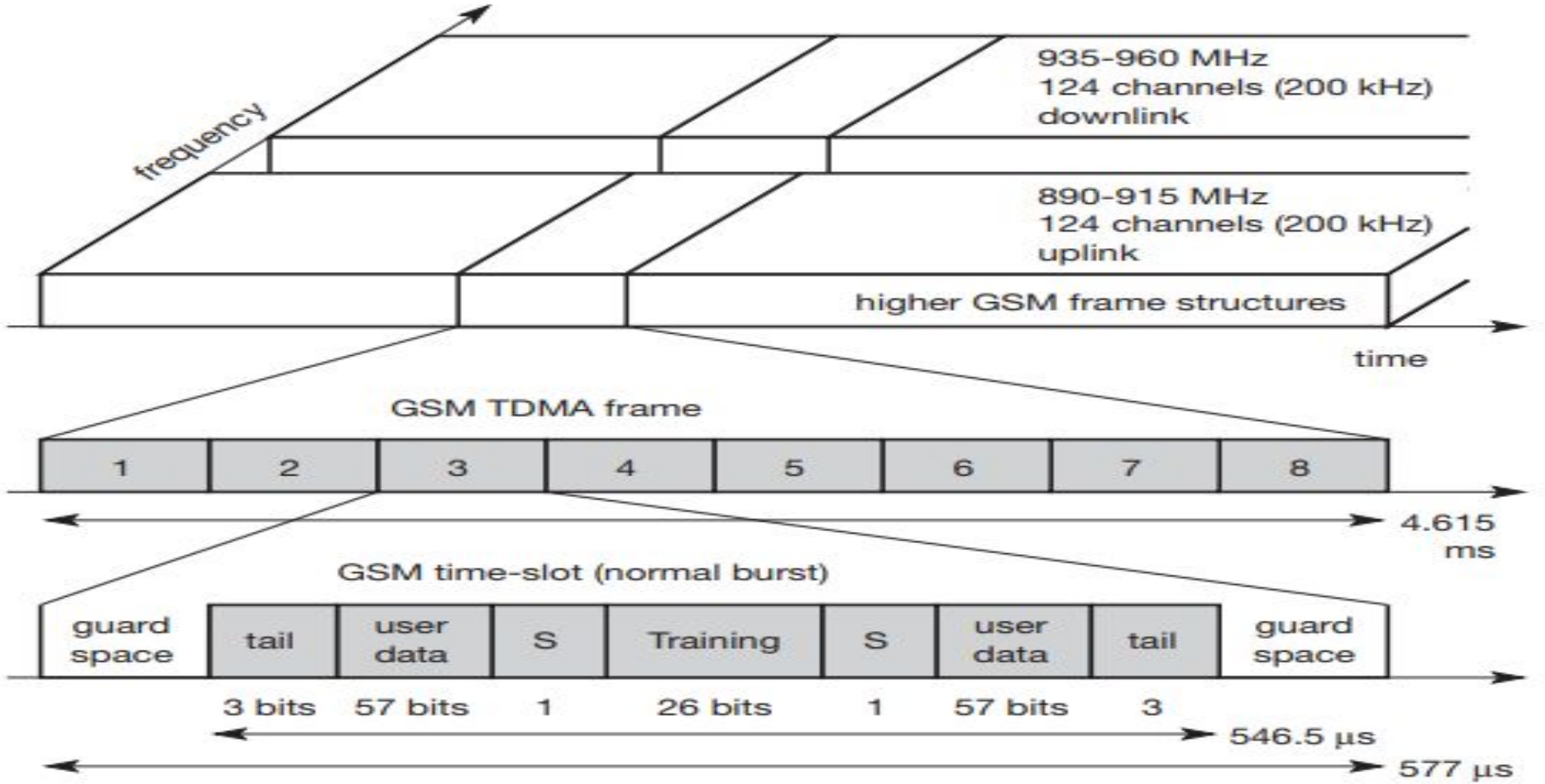
Downlink

- downlink (from the network to the mobile-that is, base transmit, mobile receive) are transmitted on different frequency bands.

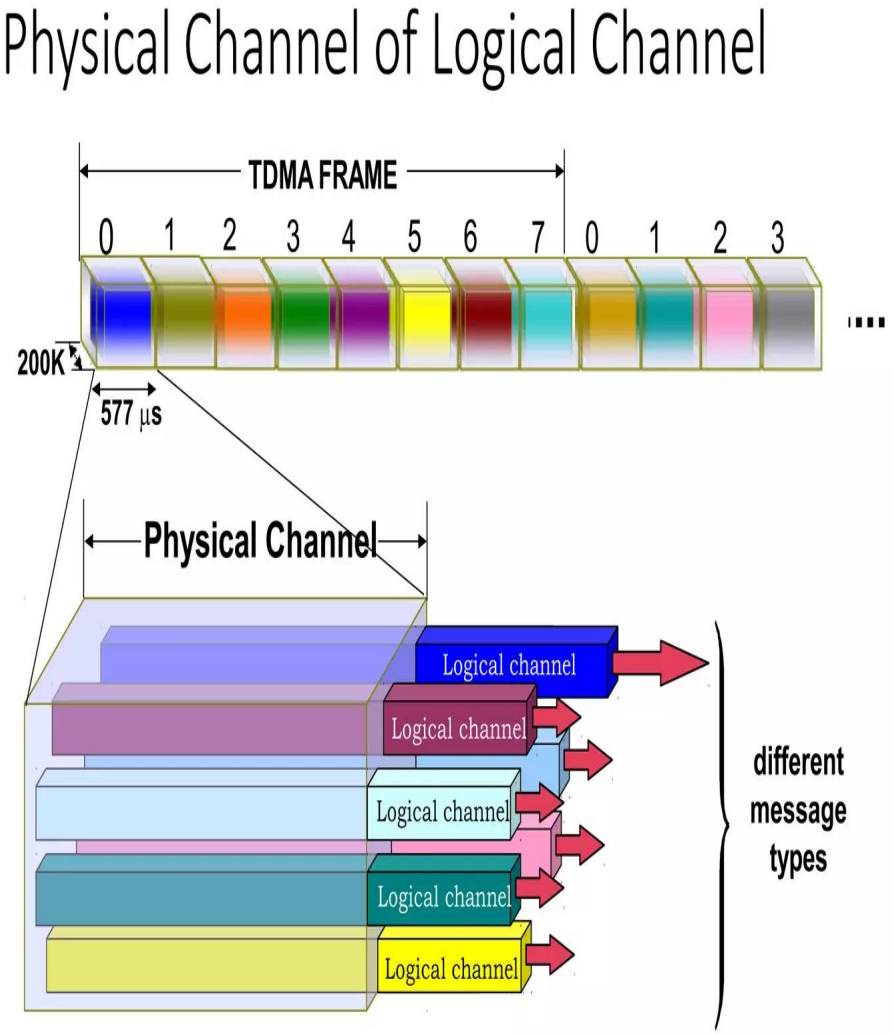
Table 1.1: GSM System Frequency Bands

		Uplink Band	**Downlink Band**
GSM-900		890-915 MHz	935-960 MHz
E-GSM-900		880-915 MHz	925-960 MHz
DCS-1800		1,710-1,785 MHz	1,805-1,880 MHz
PCS-1900		1,850-1,910 MHz	1,930-1,990 MHz
GSM-400	GSM-450	450,4-457,6 MHz	460.4-467.6 MHz
	GSM-480	478.8-486 MHz	488.8-496 MHz
GSM-850		824-849 MHz	869-894 MHz

GSM TDMA frame, slots and bursts



- Each of the 248 channels is additionally separated in time via a GSM TDMA frame, i.e., each 200 kHz carrier is subdivided into frames that are repeated continuously.
- The duration of a frame is 4.615 ms.
- A frame is again subdivided into 8 GSM time slots, where each slot represents a physical TDM channel and lasts for 577 µs.
- Each TDM channel occupies the 200 kHz carrier for 577 µs every 4.615 ms.

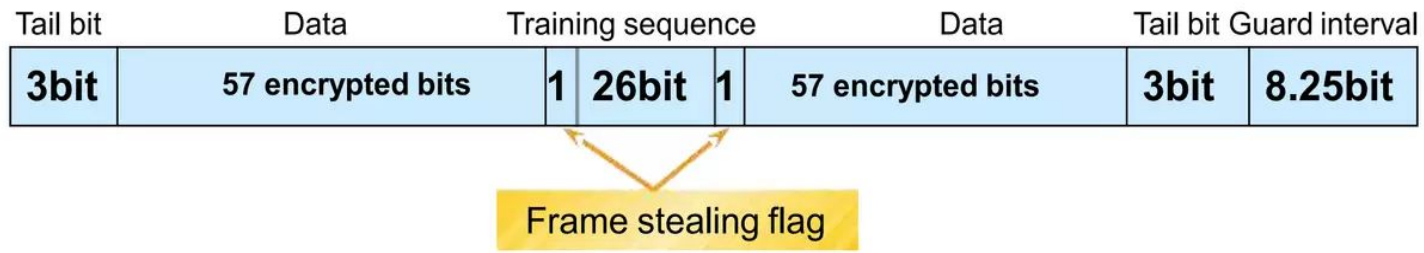


Copyright © 2010 Huawei Technologies Co., Ltd. All rightsreserved.

- Data is transmitted in small portions, called bursts. Figure shows a so called normal burst as used for data transmission inside a time slot (user and signaling data)
- The burst is only 546.5 µs long and contains 148 bits. The remaining 30.5 µs are used as guard space to avoid overlapping with other bursts due to different path delays and to give the transmitter time to turn on and off.
- Filling the whole slot with data allows for the transmission of 156.25 bit within 577 µs.
- Each physical TDM channel has a raw data rate of about 33.8 kbit/s, each radio carrier transmits approximately 270 kbit/s over the Um interface.

Burst

- Normal burst (NB)
  - Used to carry the information of the traffic channel and the control channel except for RACH



- Dummy burst (DB)
  - Used if no data is available for a slot

Copyright © 2010 Huawei Technologies Co., Ltd. All rightsreserved.

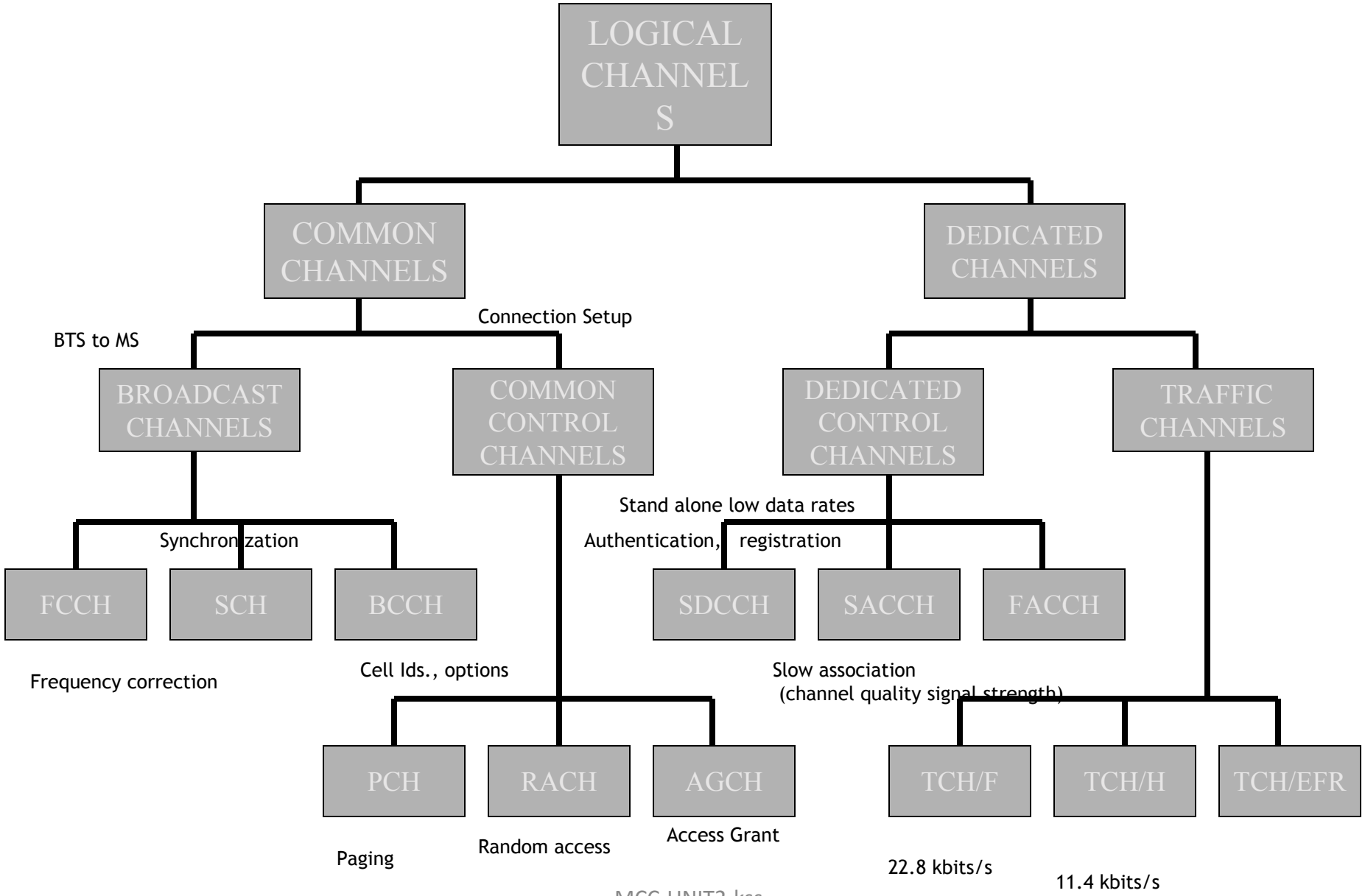
- The first and last three bits of a normal burst (tail) are all set to 0 and can be used to enhance the receiver performance.
- The training sequence(26 bits) in the middle of a slot is used to adapt the parameters of the receiver to the current path propagation characteristics and to select the strongest signal in case of multi-path propagation.
- A flag S (1 bit) indicates whether the data field contains user or network control data.
- Apart from the normal burst, ETSI defines four more bursts for data transmission:

1. a frequency correction burst allows the MS to correct the local oscillator to avoid interference with neighboring channels,
2. a synchronization burst with an extended training sequence synchronizes the MS with the BTS in time,
3. an access burst is used for the initial connection setup between MS and BTS,
4. a dummy burst is used if no data is available for a slot.

Logical channels and frame hierarchy

- **Physical channels :**
- **The combination of an ARFCN and a time slot defines a physical channel**
- In GSM cellular networks, an **absolute radio-frequency channel number** (ARFCN) is a code that specifies a pair of physical radio carriers used for transmission and reception in a land mobile radio system, one for the uplink signal and one for the downlink signal
- **Logical channels : These are channels specified by GSM which are mapped on physical channels.**
- GSM specifies two basic groups of logical channels, i.e., traffic channels and control channels

Logical Channels on Air interface



Traffic channels (TCH)

- GSM uses a TCH to transmit user data (e.g., voice, fax).
- Two basic categories of TCHs have been defined, i.e., full-rate TCH (TCH/F) and half-rate TCH (TCH/H).
- A TCH/F has a data rate of 22.8 kbit/s, whereas TCH/H only has 11.4 kbit/s.
- With the voice codecs available at the beginning of the GSM standardization, 13 kbit/s were required, whereas the remaining capacity of the TCH/F (22.8 kbit/s) was used for error correction (TCH/FS).
- The standard codecs for voice are called full rate (FR, 13 kbit/s) and half rate (HR, 5.6 kbit/s).
- A newer codec, enhanced full rate (EFR), provides better voice quality than FR as long as the transmission error rate is low.
- Data transmission in GSM is possible at many different data rates, e.g., TCH/F4.8 for 4.8 kbit/s, TCH/F9.6 for 9.6 kbit/s, and, as a newer specification, TCH/F14.4 for 14.4 kbit/s

Control channels (CCH):

- Many different CCHs are used in a GSM system to control medium access, allocation of traffic channels or mobility management.
- Three groups of control channels have been defined, each again with subchannels

1.Broadcast control channel (BCCH)

a) frequency correction channel (FCCH)

b) synchronization channel (SCH)

2.Common control channel (CCCH)

a) paging channel (PCH)

b) random access channel (RACH)

c) access grant channel (AGCH)

3.Dedicated control channel (DCCH)

a) stand-alone dedicated control channel (SDCCH)

b) slow associated dedicated control channel (SACCH)

c) fast associated dedicated control channel (FACCH)

1.Broadcast control channel (BCCH):

- A BTS uses this channel to signal information to all MSs within a cell.
- Information transmitted in this channel is, e.g., the cell identifier, options available within this cell (frequency hopping), and frequencies available inside the cell and in neighboring cells.
- The BTS sends information for frequency correction via the frequency correction channel (FCCH) and information about time synchronization via the synchronization channel (SCH), where both channels are subchannels of the BCCH.

2.Common control channel (CCCH):

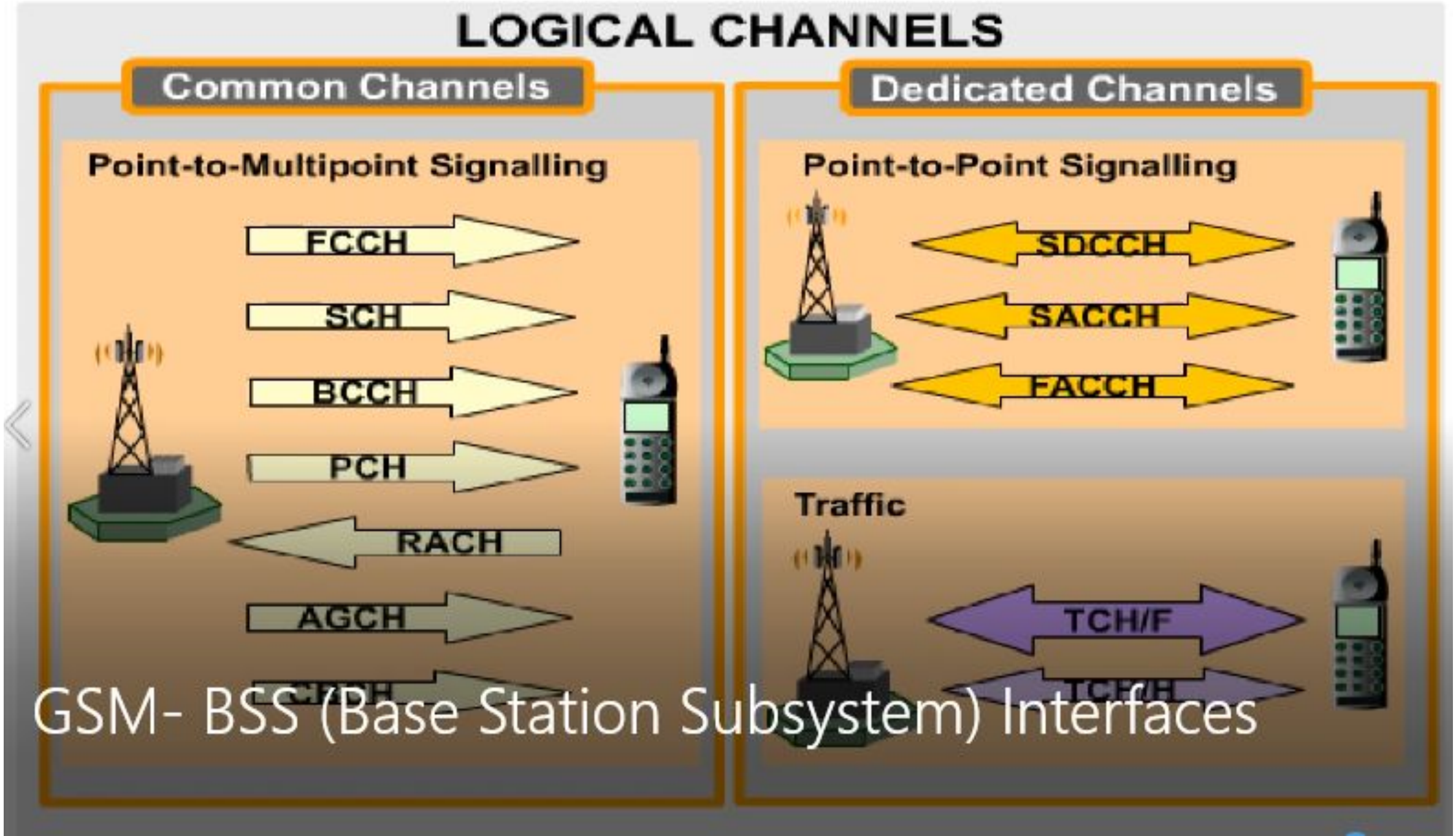
- All information regarding connection setup between MS and BS is exchanged via the CCCH.
- For calls toward an MS, the BTS uses the paging channel (PCH) for paging the appropriate MS.

- If an MS wants to set up a call, it uses the random access channel (RACH) to send data to the BTS.
- The RACH implements multiple access (all MSs within a cell may access this channel) using slotted Aloha. This is where a collision may occur with other MSs in a GSM system.
- The BTS uses the access grant channel (AGCH) to signal an MS that it can use a TCH or SDCCH for further connection setup.

3. Dedicated control channel (DCCH):

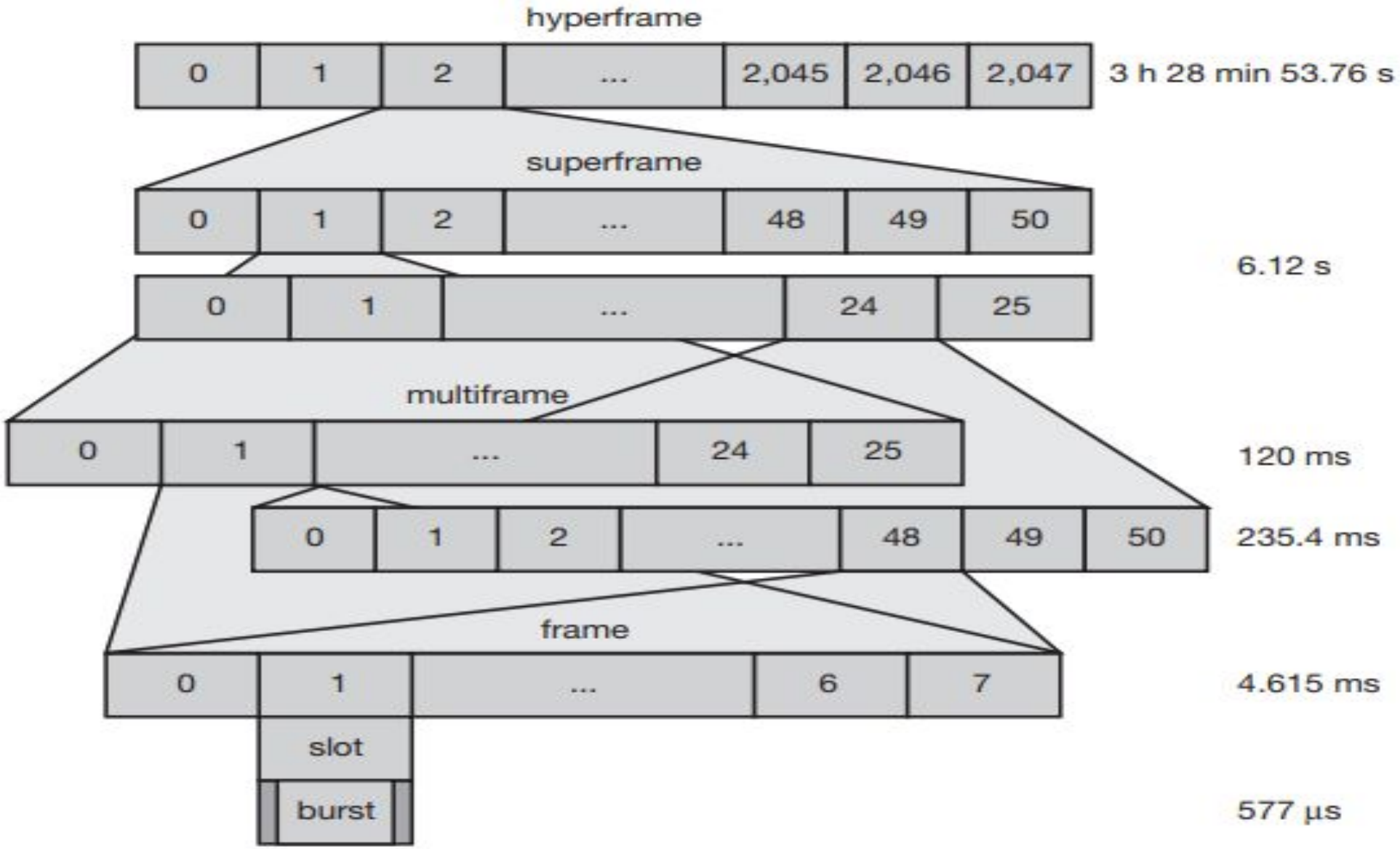
- While the previous channels have all been unidirectional, the following channels are bidirectional.
- As long as an MS has not established a TCH(Traffic Channel) with the BTS, it uses the stand-alone dedicated control channel (SDCCH) with a low data rate (782 bit/s) for signaling

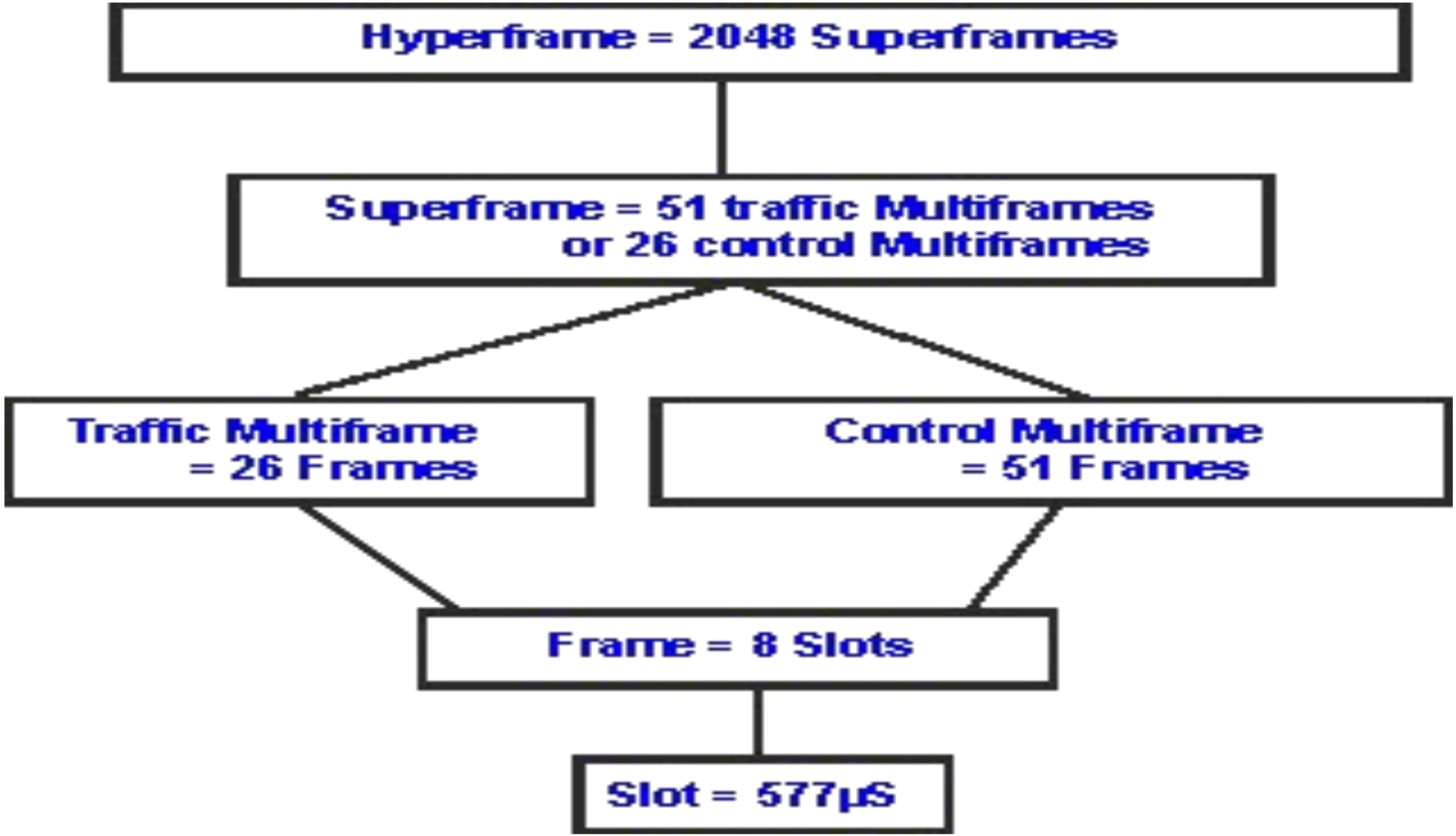
- This can comprise authentication, registration or other data needed for setting up a TCH.
- Each TCH and SDCCH has a slow associated dedicated control channel (SACCH), which is used to exchange system information, such as the channel quality and signal power level.
- Finally, if more signaling information needs to be transmitted and a TCH already exists, GSM uses a fast associated dedicated control channel (FACCH).
- The FACCH uses the time slots which are otherwise used by the TCH.
- This is necessary in the case of handovers where BTS and MS have to exchange larger amounts of data in less time.



GSM- BSS (Base Station Subsystem) Interfaces

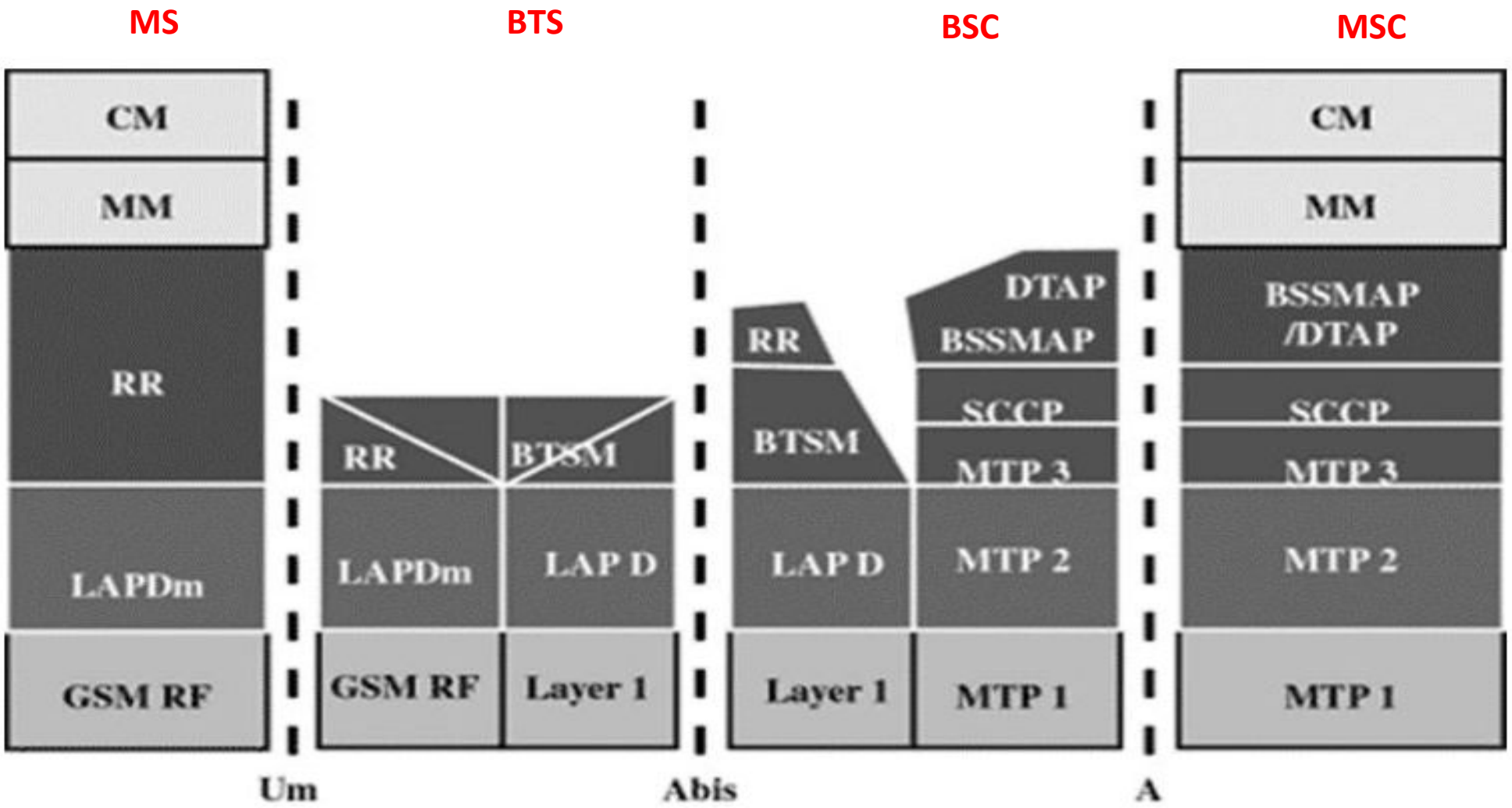
Frame Hierarchy




Hyperframe = 2048 Superframes
Superframe = 51 traffic Multiframes
or 26 control Multiframes
Traffic Multiframe
= 26 Frames
Control Multiframe
= 51 Frames
Frame = 8 Slots
Slot = 577µS

GSM Protocol Architecture

- GSM protocol architecture is a layered model that is designed to allow communications between two different systems
- The lower layers assure the services of the upper-layer protocols.
- Each layer passes suitable notifications to ensure that the transmitted data has been formatted, transmitted, and received accurately.



Protocol Architecture for signaling

1. MS Protocols

- Based on the interface, the GSM signaling protocol is assembled into the following three general layers:

Layer 1: The physical layer.

- It uses the channel structures over the air interface.

Layer 2: The data-link layer.

- Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link access protocol on the Dm channel (LAP-Dm).
- Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7(signaling system 7) is used.

Layer 3: The network layer

GSM signaling protocol's third layer is divided into three sublayers:

i. Radio Resource Management (RR),
ii. Mobility Management (MM), and
iii. Connection Management (CM).

2. MS to BTS Protocols

- **The RR layer** is the lower layer that manages a link, both radio and fixed, between the MS and the MSC. For this formation, the main components involved are the MS, BSS, and MSC.
- The responsibility of the RR layer is to manage the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.
- **The MM layer** is stacked above the RR layer. It handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects.
- Location management is concerned with the procedures that enable the system to know the current location of a powered-on MS so that incoming call routing can be completed.

- **The CM layer** is the topmost layer of the GSM protocol stack. This layer is responsible for Call Control, Supplementary Service Management, and Short Message Service Management.
- Each of these services are treated as individual layer within the CM layer.
- Other functions of **the CC sublayer** include call establishment, selection of the type of service (including alternating between services during a call), and call release.

3.BSC Protocols

- The BSC uses a different set of protocols after receiving the data from the BTS.
- The Abis interface is used between the BTS and BSC. At this level, the radio resources at the lower portion of Layer 3 are changed from the RR to the Base Transceiver Station Management (BTSM).

- The BTS management layer is a relay function at the BTS to the BSC.
- The RR protocols are responsible for the allocation and reallocation of traffic channels between the MS and the BTS. These services include controlling the initial access to the system, paging for MT calls, the handover of calls between cell sites, power control, and call termination.
- The BSC still has some radio resource management in place for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.
- To transit from the BSC to the MSC, the BSS mobile application part or the direct application part is used, and SS7 protocols is applied by the relay, so that the MTP 1-3 can be used as the prime architecture

4. MSC Protocols

- At the MSC, starting from the BSC, the information is mapped across the A interface to the MTP Layers 1 through 3.
- Here, Base Station System Management Application Part (BSS MAP) is said to be the equivalent set of radio resources.
- The relay process is finished by the layers that are stacked on top of Layer 3 protocols, they are BSS MAP/DTAP, MM, and CM. This completes the relay process.
- To find and connect to the users across the network, MSCs interact using the control-signaling network

- Location registers are included in the MSC databases to assist in the role of determining how and whether connections are to be made to roaming users.
- Each GSM MS user is given a HLR that in turn comprises of the user's location and subscribed services. VLR is a separate register that is used to track the location of a user.
- When the users move out of the HLR covered area, the VLR is notified by the MS to find the location of the user.
- The VLR in turn, with the help of the control network, signals the HLR of the MS's new location. With the help of location information contained in the user's HLR, the MT calls can be routed to the user.

Localization and calling

- One fundamental feature of the GSM system is the automatic, worldwide localization of users. The system always knows where a user currently is, and the same phone number is valid worldwide.
- To provide this service, GSM performs periodic location updates even if a user does not use the mobile station (provided that the MS is still logged into the GSM network and is not completely switched off).
- The HLR always contains information about the current location (only the location area, not the precise geographical location), and the VLR currently responsible for the MS, informs the HLR about location changes.
- As soon as an MS moves into the range of a new VLR (a new location area), the HLR sends all user data needed to the new VLR

- Changing VLRs with uninterrupted availability of all services is also called roaming.
- Roaming can take place

i. within the network of one provider,
ii. between two providers in one country (national roaming)
iii. between different providers in different countries (international roaming).

- Localization and calling is divided into three parts.

1. MS registration in the GSM network
2. Mobile terminated call
3. Mobile originated call

- To locate an MS and to address the MS, several numbers are needed:

1. Mobile station international ISDN number (MSISDN):

- The only important number for a user of GSM is the phone number. Remember that the phone number is not associated with a certain device but with the SIM, which is personalized for a user.
- The MSISDN follows the ITU-T standard E.164 for addresses as it is also used in fixed ISDN networks.
- This number consists of -

i. the country code (CC) (e.g., +49 179 1234567 with 49 for Germany),

ii. the national destination code (NDC) (i.e., the address of the network provider, e.g., 179),

iii. the subscriber number (SN).

2.International mobile subscriber identity (IMSI):

- GSM uses the IMSI for internal unique identification of a subscriber.
- IMSI consists of-

i. a mobile country code (MCC) (e.g., 240 for Sweden, 208 for France),

ii. the mobile network code (MNC) (i.e., the code of the network provider),

iii. the mobile subscriber identification number (MSIN).

3.Temporary mobile subscriber identity (TMSI):

- To hide the IMSI, which would give away the exact identity of the user signaling over the air interface, GSM uses the 4 byte TMSI for local subscriber identification.
- TMSI is selected by the current VLR and is only valid temporarily and within the location area of the VLR (for an ongoing communication TMSI and LAI are sufficient to identify a user; the IMSI is not needed). Additionally, a VLR may change the TMSI periodically.

4.Mobile station roaming number (MSRN):

- Another temporary address that hides the identity and location of a subscriber is MSRN.
- The VLR generates this address on request from the MSC, and the address is also stored in the HLR.
- MSRN contains -

i. the current visitor country code (VCC),

ii. the visitor national destination code (VNDC),

iii. the identification of the current MSC together with the subscriber number.

- The MSRN helps the HLR to find a subscriber for an incoming call.

1.MS Registration in GSM Network

- **Step 1**

The MS detects that it has entered a new Location Area and transmits a Channel Request message over the Random Access Channel (RACH).

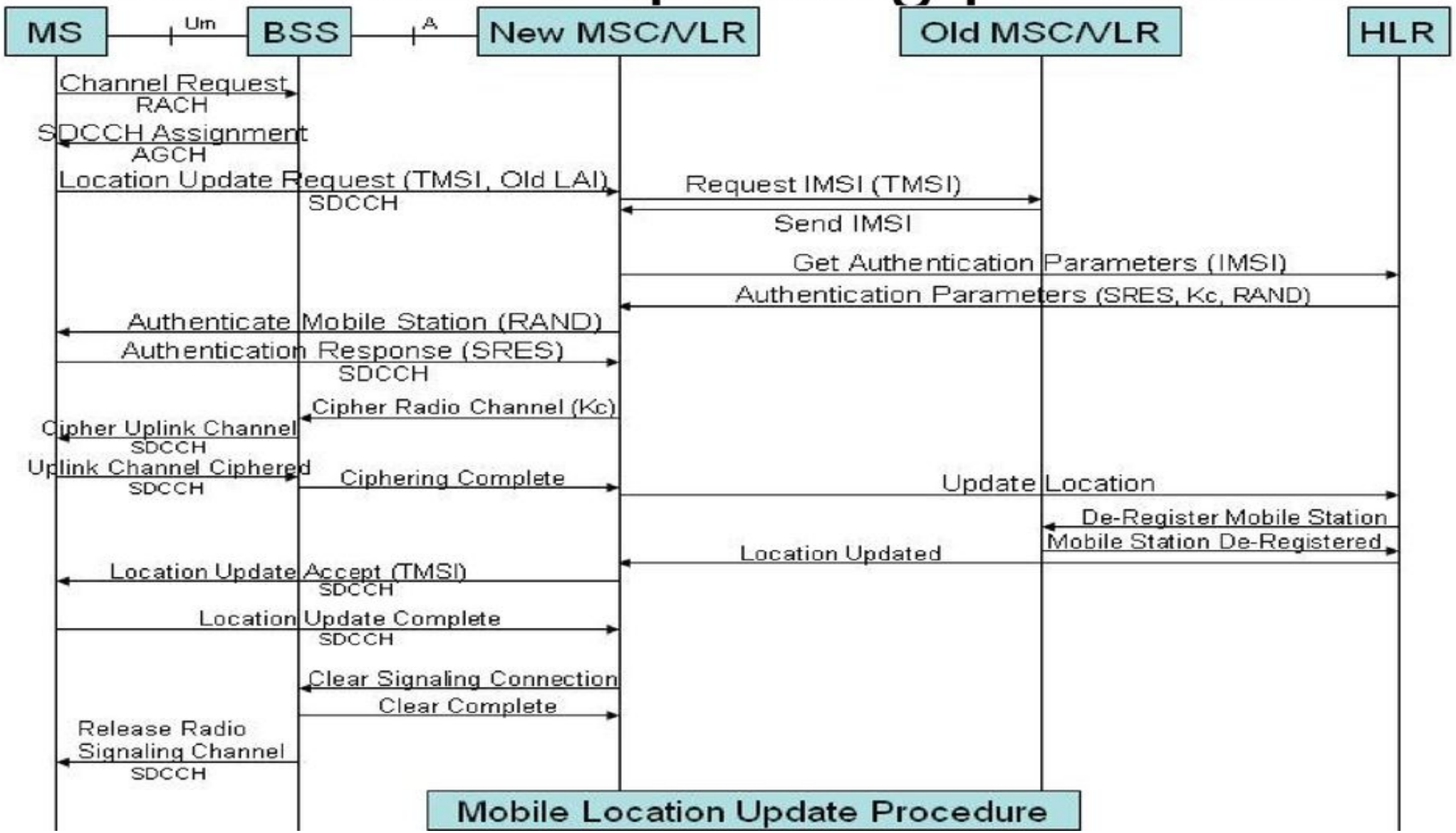
- Step 2

Once the BSS receives the Channel Request message, it allocates a Stand-alone Dedicated Control Channel (SDCCH) and forwards this channel assignment information to the MS over the Access Grant Channel (AGCH). It is over the SDCCH that the MS will communicate with the BSS and MSC.

- Step 3

The MS transmits a location update request message to the BSS over the SDCCH. Included in this message are the MS Temporary Mobile Subscriber Identity (TMSI) and the old Location Area Identification (oldLAI). The MS can identify itself either with its IMSI or TMSI. The BSS forwards the location update request message to the MSC

GSM location updating procedure



- Step 4

The VLR analyzes the LAI supplied in the message and determines that the TMSI received is associated with a different VLR (old VLR). In order to proceed with the registration, the IMSI of the MS must be determined. The new VLR derives the identity of the old VLR by using the received LAI, supplied in the location update request message. It also requests the old VLR to supply the IMSI for a particular TMSI.

- Step 5

The new VLR sends a request to the HLR/AUC (Authentication Center) requesting the “authentication triplets” (RAND, SRES, and Kc) available for the specified IMSI.

- Step 6

The AUC, using the IMSI, extracts the subscriber's authentication key (Ki). The AUC then generates a random number (RAND), applies the Ki and RAND to both the authentication algorithm (A3) and the cipher key generation algorithm (A8) to produce an authentication Signed Response (SRES) and a Cipher Key (Kc). The AUC then returns to the new VLR an authentication triplet: RAND, SRES, and Kc.

- Step 7

The MSC/VLR keeps the two parameters Kc and SRES for later use and then sends a message to the MS. The MS reads its Authentication key (Ki) from the SIM, applies the received random number (RAND) and Ki to both its Authentication Algorithm (A3) and Cipher key generation Algorithm (A8) to produce an authentication Signed Response (SRES) and Cipher Key (Kc). The MS saves Kc for later, and will use Kc when it receives command to cipher the channel.

- Step 8

The MS returns the generated SRES to the MSC/VLR. The VLR compares the SRES returned from the MS with the expected SRES received earlier from the AUC. If equal, the mobile passes authentication. If unequal, all signaling activities will be aborted.

- Step 9

The new MSC/VLR requests the BSS to cipher the radio channel. Included in this message is the Cipher Key (Kc), which was made available earlier during the authentication.

- Step 10

The BSS retrieves the cipher key, Kc, from the message and then transmits a request to the MS requesting it to begin ciphering the uplink channel.

- Step 11

The MS uses the cipher key generated previously when it was authenticated to cipher the uplink channel, and transmits a confirmation over the ciphered channel to the BSS.

- Step 12

The BSS upon ciphering the downlink channel sends a cipher complete message to the MSC. At this point, we are ready to inform the HLR that the MS is under control of a new VLR and that the MS can be de-registered from the old VLR.

- Step 13

The new VLR sends a message to the HLR informing it that the given IMSI has changed locations and can be reached by routing all incoming calls to the VLR address included in the message.

- Step 14

The HLR requests the old VLR to remove the subscriber record associated with the given IMSI. The request is acknowledged.

- Step 15

The HLR updates the new VLR with subscriber data (mobiles subscriber’s customer profile).

- Step 16

The MSC forwards the location update accept message to the MS. This message includes the new TMSI.

- Step 17

The MS retrieves the new TMSI value from the message and updates its SIM with this new value. The mobile sends then an update complete message back to the MSC.

- Step 18

The MSC requests from the BSS that the signaling connection be released between the MSC and the MS.

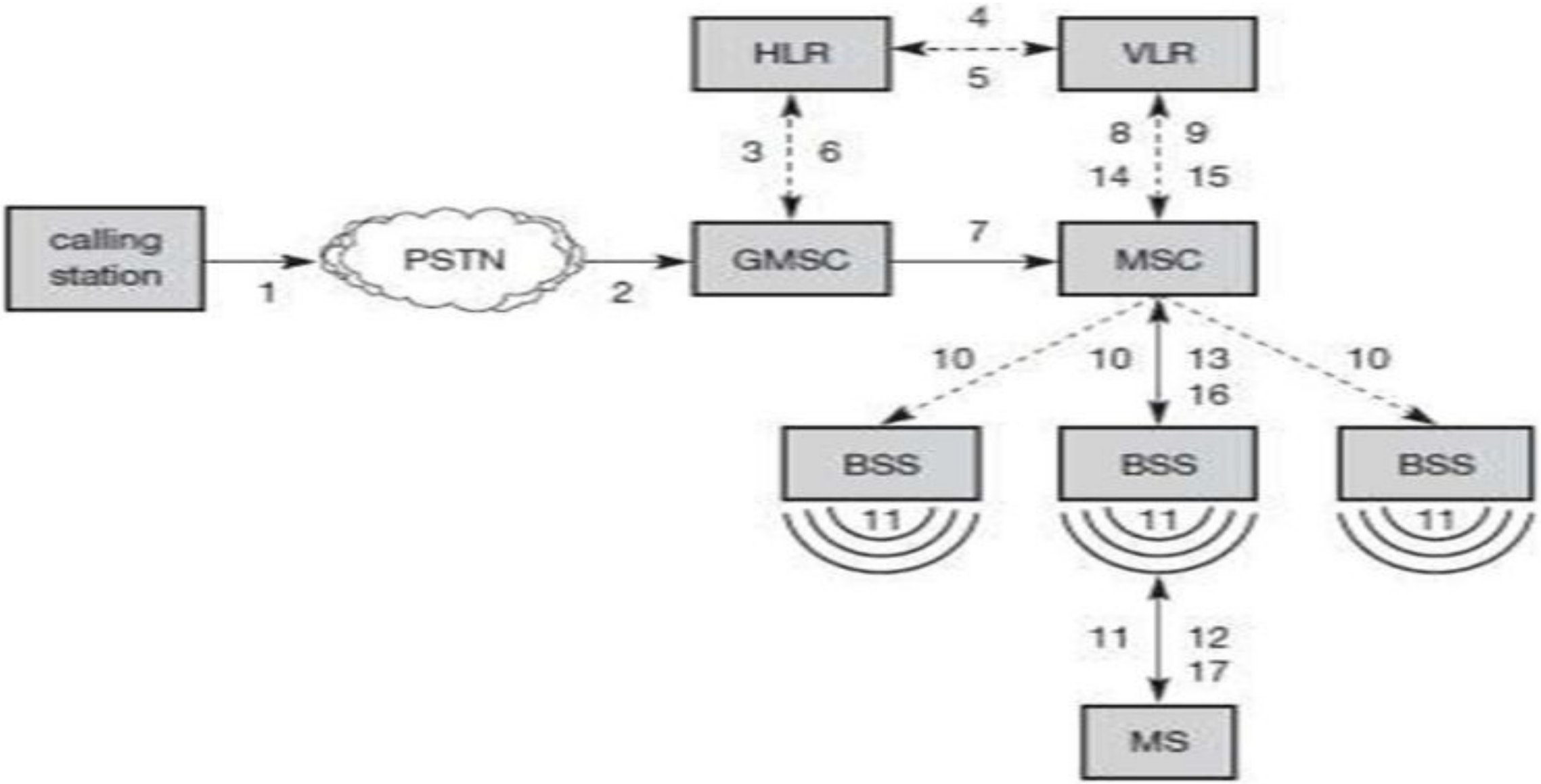
- Step 19

The MSC releases its portion of the signaling connection when it receives the clear complete message from the BSS.

- Step 20

The BSS sends a "radio resource" channel release message to the MS and then frees up the Stand-alone Dedicated Control Channel (SDCCH) that was allocated previously. The BSS then informs the MSC that the signaling connections has been cleared

2.Mobile Terminated Call (MTC)



For a mobile terminated call (MTC), the following figure shows the different steps that take place

Step 1: User dials the phone

Step 2: The fixed network (PSTN) identifies the number belongs to a user in GSM network and forwards the call setup to the Gateway MSC (GMSC).

Step 3: The GMSC identifies the HLR for the subscriber and signals the call setup to HLR

Step 4: The HLR checks for number existence and its subscribed services and requests a Mobile Station Roaming Number (MSRN) from the current VLR.

Step 5: VLR sends the MSRN to HLR

Step 6: Upon receiving MSRN, the HLR determines the MSC responsible for MS and forwards the information to the GMSC

Step 7: The GMSC can now forward the call setup request to the MSC indicated

Step 8: The MSC requests the VLR for the current status of the MS

Step 9: VLR sends the requested information

Step 10: If MS is available, the MSC initiates paging in all cells it is responsible for.

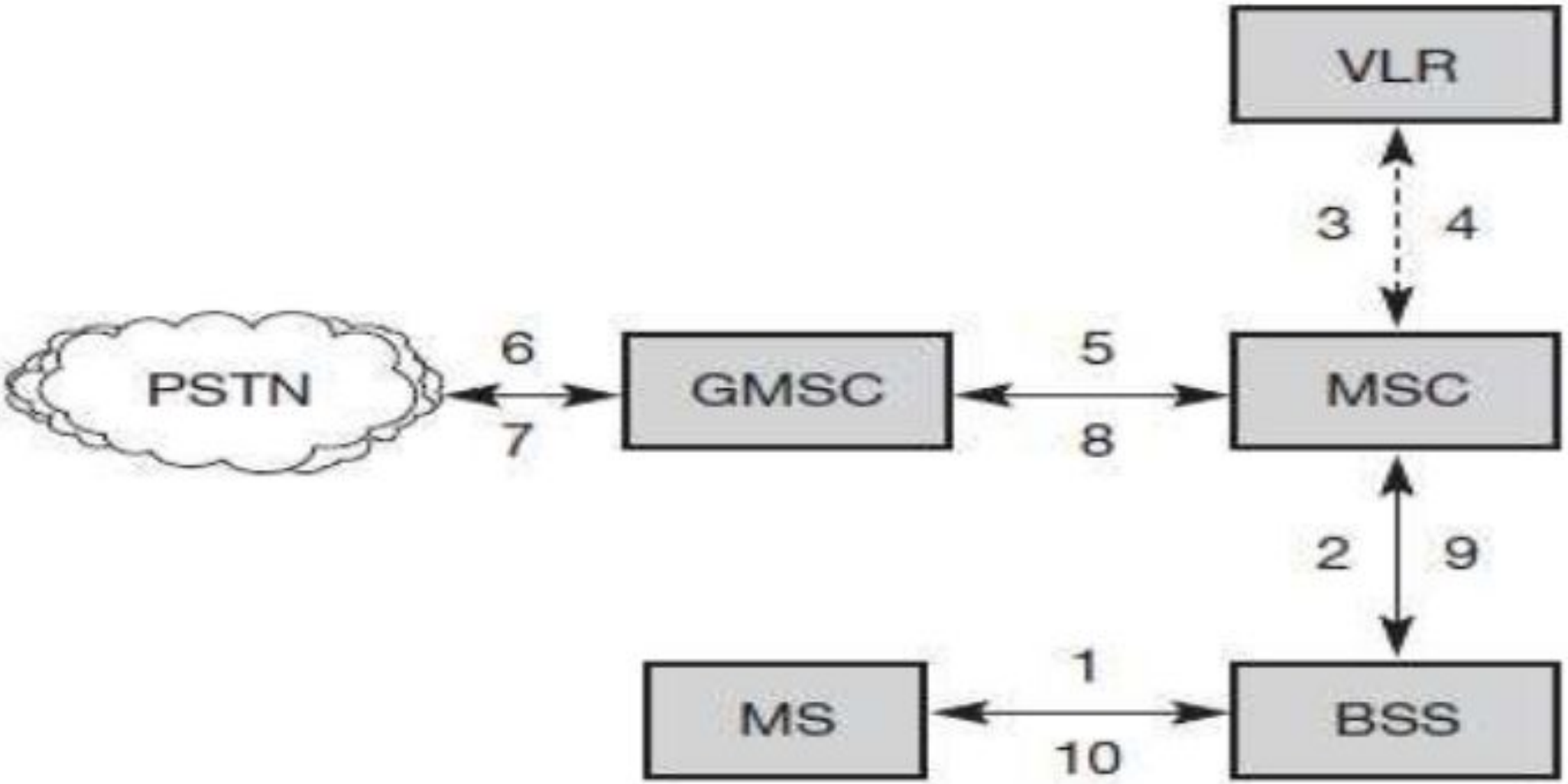
Step 11: The BTSs of all BSSs transmit the paging signal to the MS

Step 12: Step 13: If MS answers.

Step 14: Step 15: VLR performs security checks

Step 16: step 17: Then the VLR signals to the MSC to setup a connection to the MS

Mobile Originated Call (MOC),



- For a mobile originated call (MOC), the following steps take place:

Step 1: The MS transmits a request for a new connection

Step 2: The BSS forwards this request to the MSC

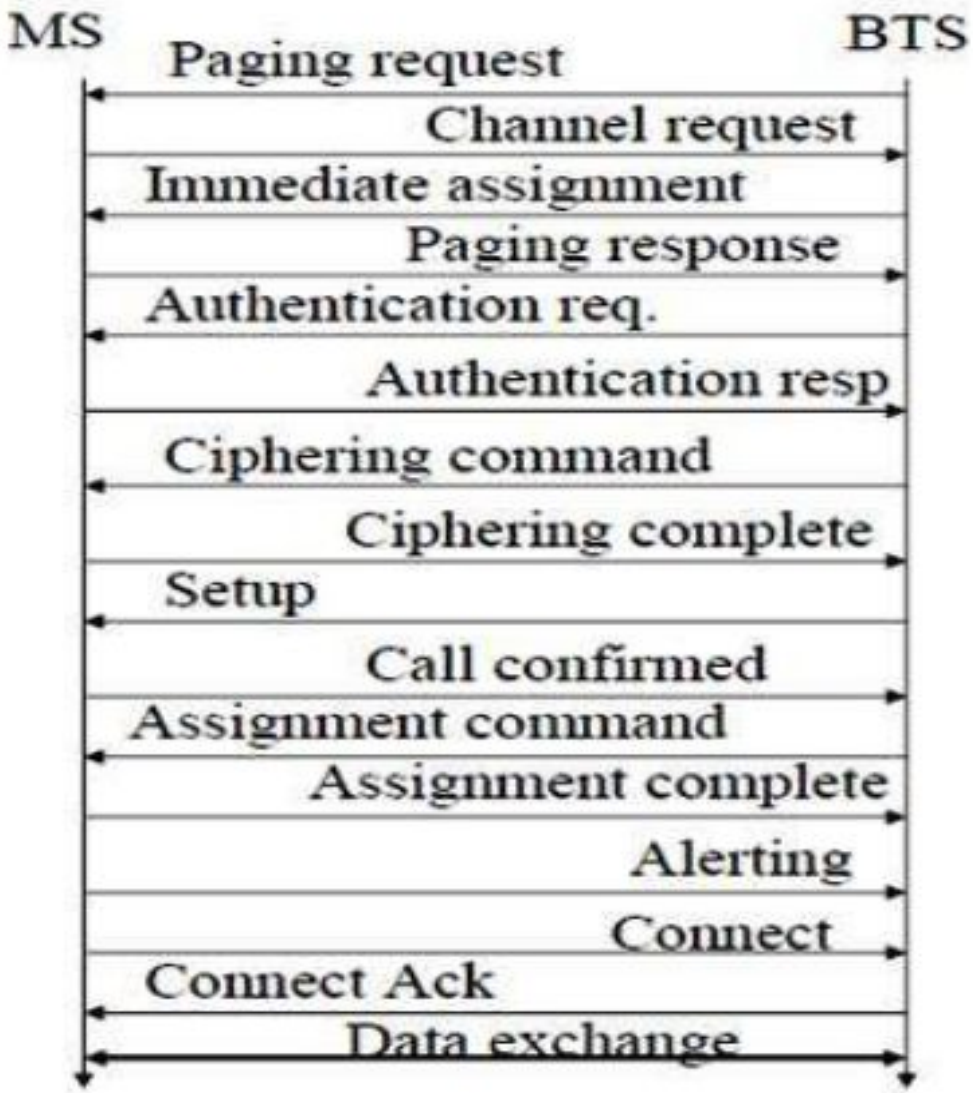
Step 3: Step 4: The MSC then checks if this user is allowed to set up a call with the requested and checks the availability of resources through the GSM network and into the Public Switched Telephone Network(PSTN).

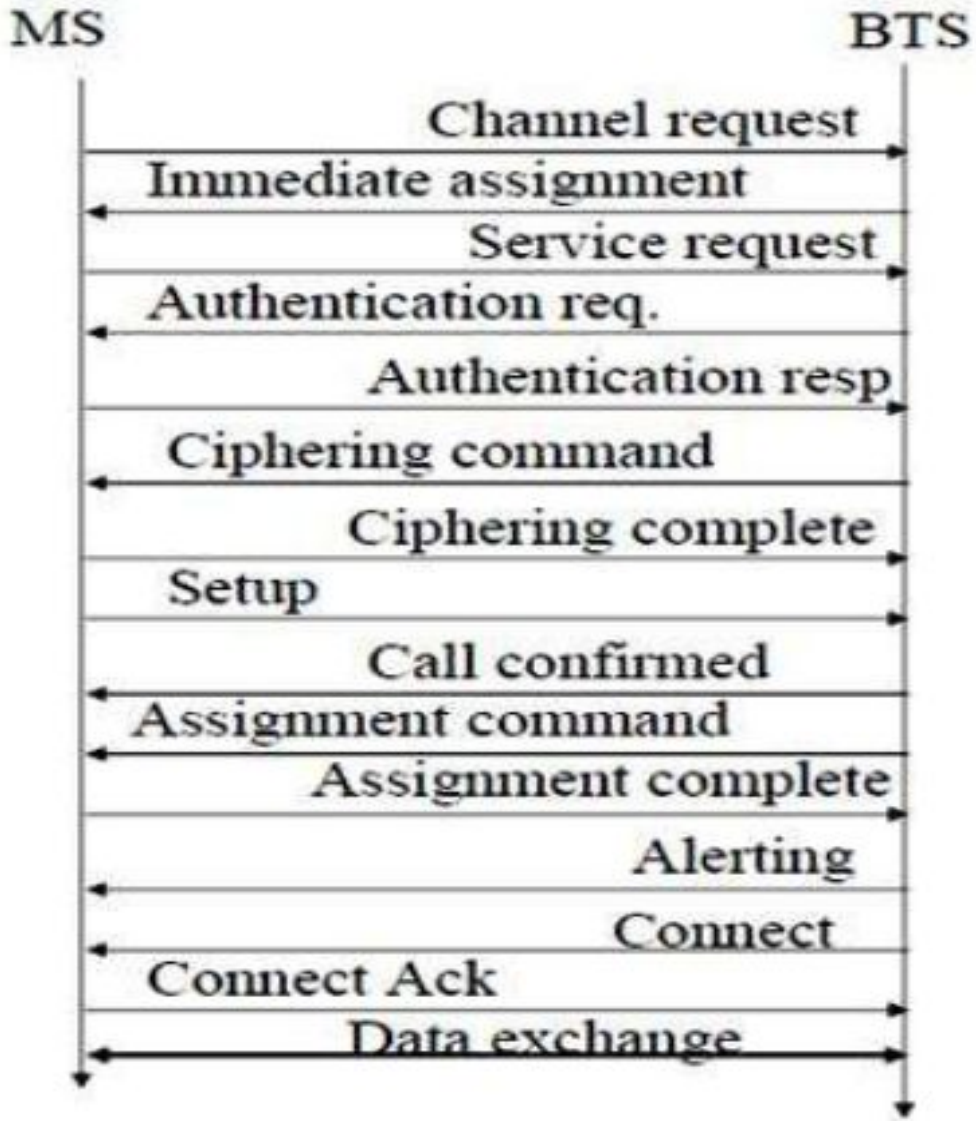
If all resources are available, the MSC sets up a connection between the MS and the fixed network.

Step 5: Step 8:The MSC checks the availability of resources through GSM network and into the PSTN.

Step 9: Step 10: If the resources are available, the MSC set up the connection between MS and the fixed network.

Message flow for MTC and MOC





- In addition to the steps mentioned above, other messages are exchanged between an MS and BTS during connection setup (in either direction). These messages can be quite often heard in radios or badly shielded loudspeakers as crackling noise before the phone rings.
- Paging is only necessary for an MTC, then similar message exchanges follow.
- The first step in this context is the channel access via the random access channel (RACH) with consecutive channel assignment; the channel assigned could be a traffic channel (TCH) or a slower signaling channel SDCCH.
- The next steps, which are needed for communication security, comprise the authentication of the MS and the switching to encrypted communication. The system now assigns TCH (if this has not been done).

- This has the advantage of only having to use an SDCCH during the first setup steps. If the setup fails, no TCH has been blocked. However, using a TCH from the beginning has a speed advantage.
- The following steps depend on the use of MTC or MOC.
- If someone is calling the MS, it answers now with ‘alerting’ that the MS is ringing and with ‘connect’ that the user has pressed the connect button.
- The same actions happen the other way round if the MS has initiated the call.
- After connection acknowledgement, both parties can exchange data.
- Closing the connection comprises a user-initiated disconnect message (both sides can do this), followed by releasing the connection and the radio channel.

Handover in GSM

- Cellular systems require handover procedures, as single cells do not cover the whole service area, but, e.g., only up to 35 km around each antenna on the countryside and some hundred meters in cities
- The smaller the cell size and the faster the movement of a mobile station through the cells (up to 250 km/h for GSM), the more handovers of ongoing calls are required.
- However, a handover should not cause a cut-off, also called call drop. GSM aims at maximum handover duration of 60 ms.

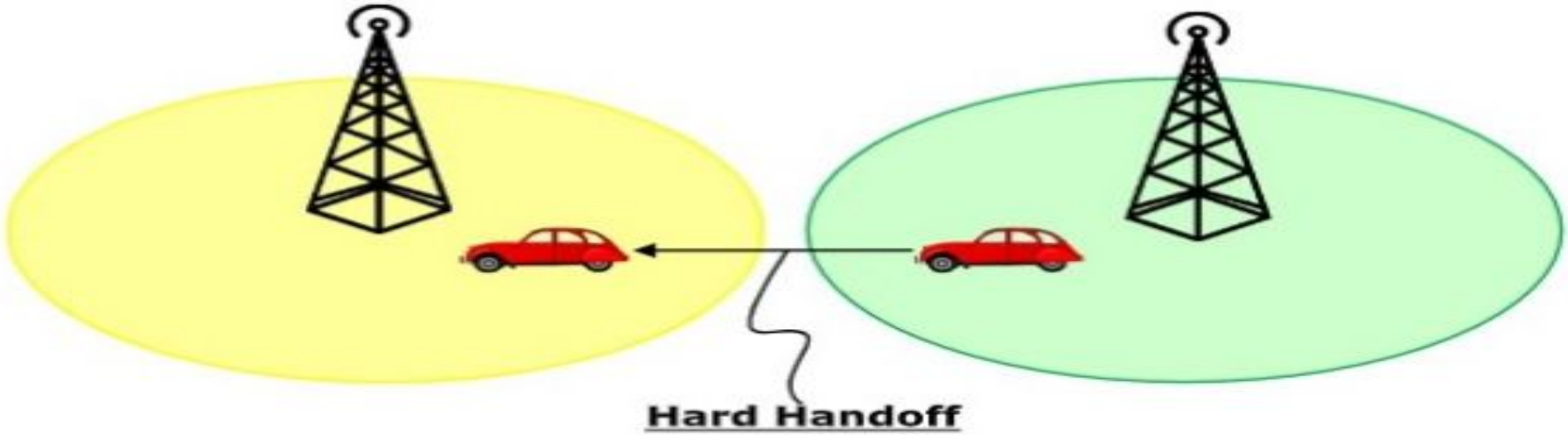
There are two basic reasons for a handover

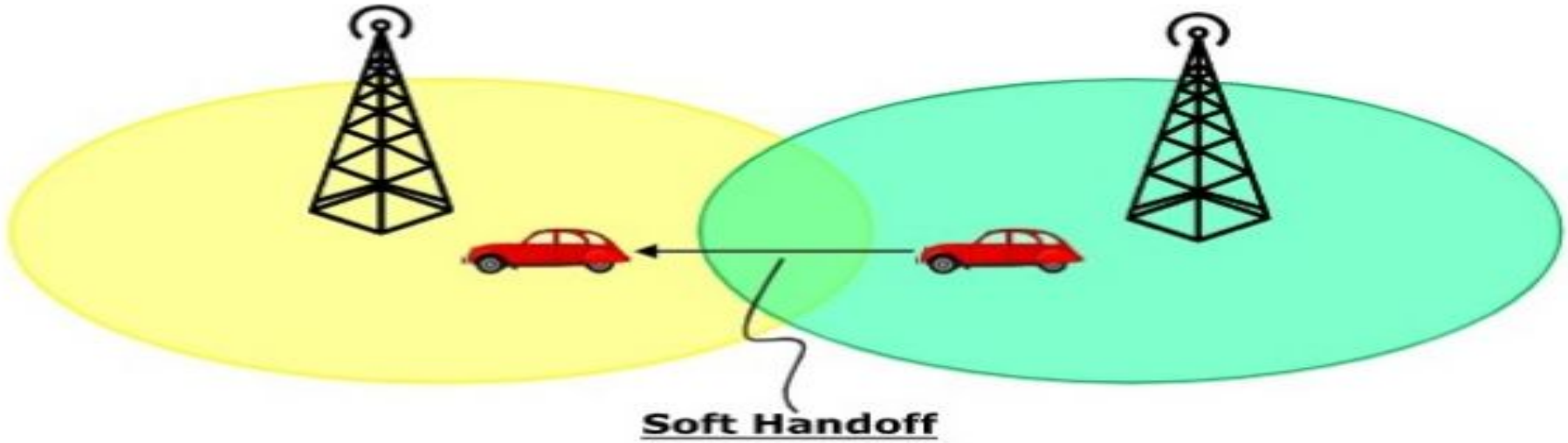
A) The mobile station **moves out of the range** of a BTS or a certain antenna of a BTS respectively. The received signal level decreases continuously until it falls below the minimal requirements for communication.

- The error rate may grow due to interference, the distance to the BTS may be too high (max. 35 km) etc. – all these effects may diminish the quality of the radio link and make radio transmission impossible in the near future.
- B)The wired infrastructure (MSC, BSC) may decide that **the traffic in one cell is too high** and shift some MS to other cells with a lower load (if possible).

  Handover may be due to **load balancing**.

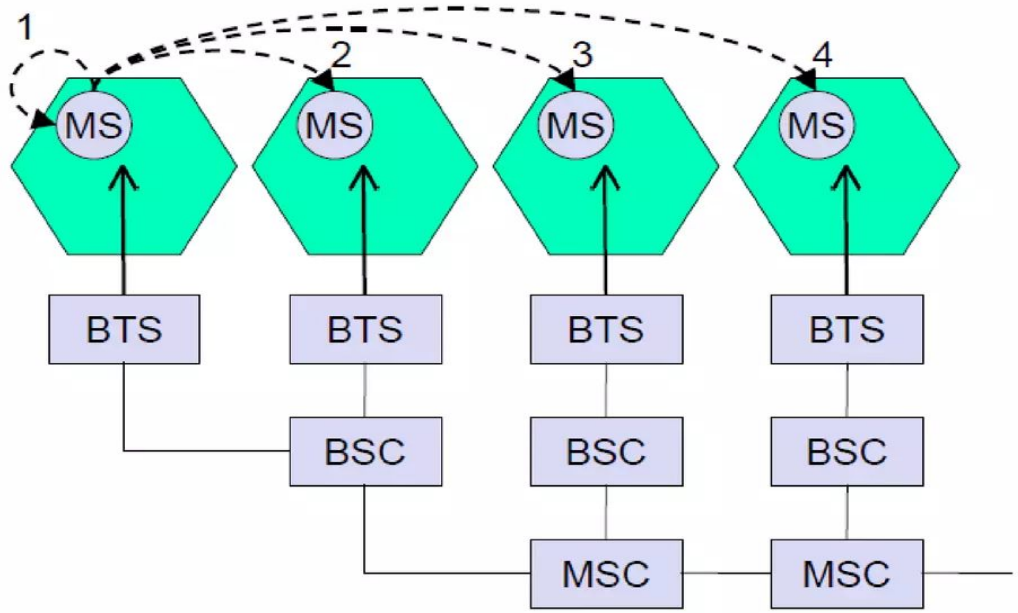
- There are two types of handoffs –
- Hard Handoff – In a hard handoff, an actual break in the connection occurs while switching from one cell to another. The radio links from the mobile station to the existing cell is broken before establishing a link with the next cell. It is generally an inter-frequency handoff. It is a "break before make" policy.
- Soft Handoff – In soft handoff, at least one of the links is kept when radio links are added and removed to the mobile station. This ensures that during the handoff, no break occurs. This is generally adopted in co-located sites. It is a "make before break" policy.


Hard Handoff


Soft Handoff

Types of Handover in GSM

4 types of handover



i) Intra-cell handover:

Within a cell, narrow-band interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario 1).

ii) Inter-cell, intra-BSC handover:

This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2).

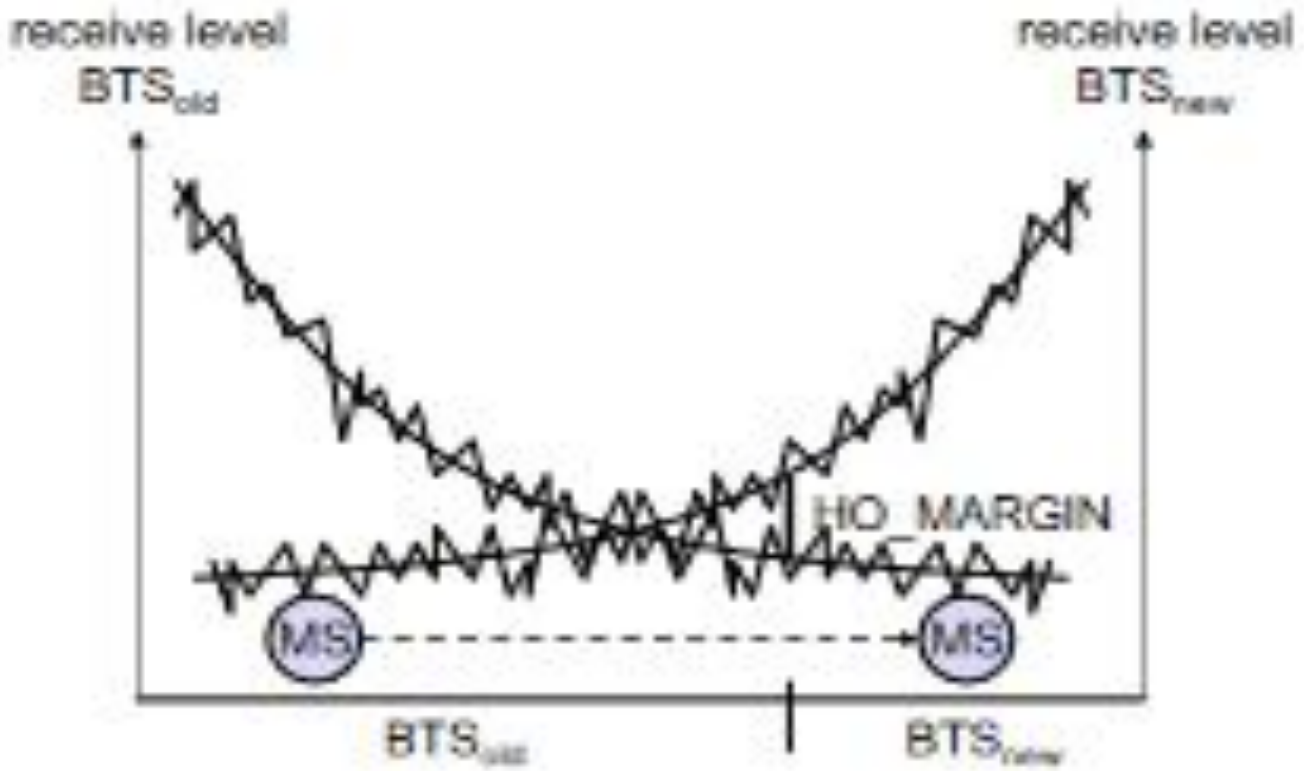
iii)Inter-BSC, intra-MSC handover:

As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3).

iv) Inter MSC handover:

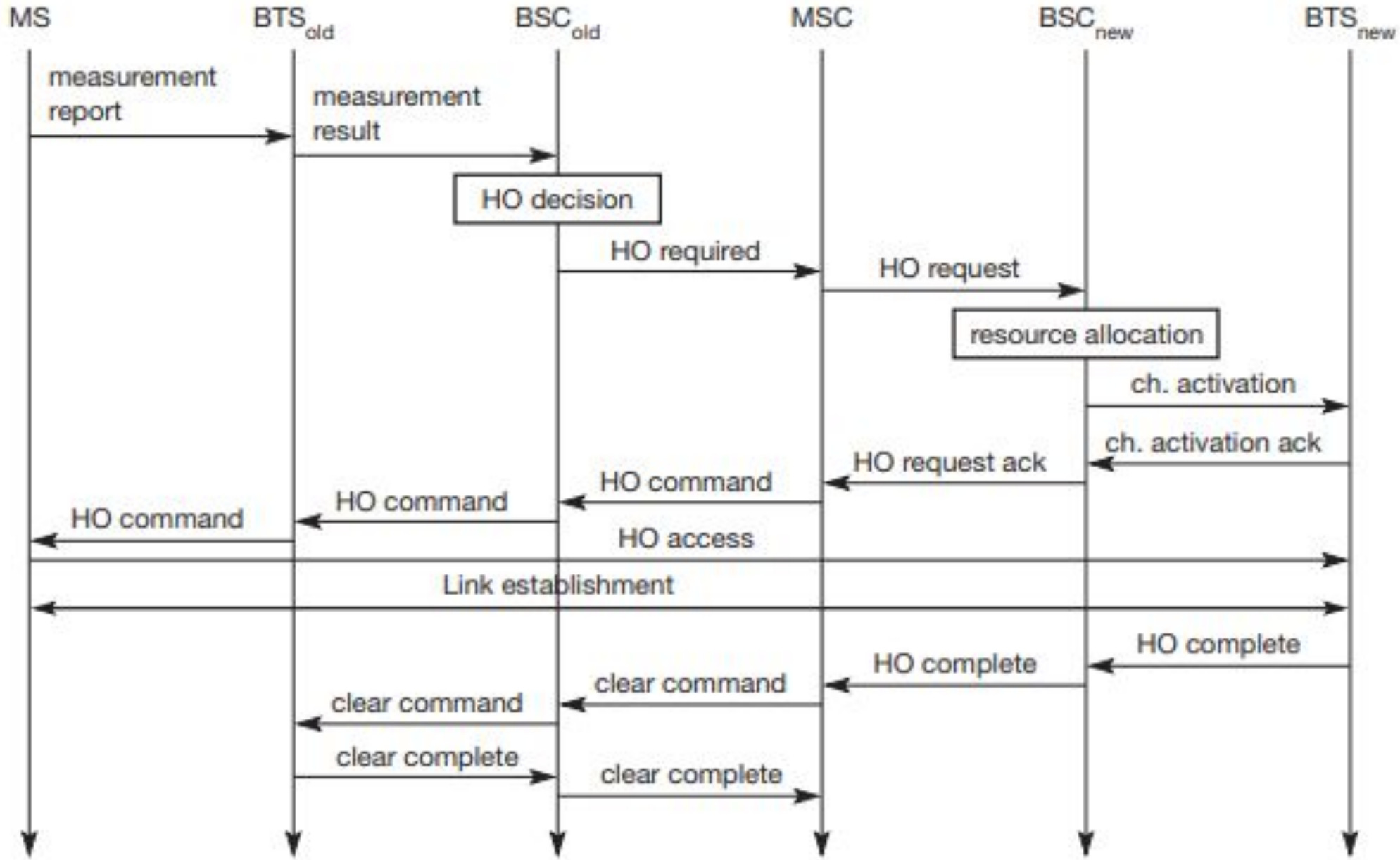
A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4).

Intra-MSC handover



Handover decision depending on receive level

- Figure shows the typical behavior of the received signal level while an MS moves away from one BTS (BTS_{old}) closer to another one (BTS_{new}).
- In this case, the handover decision does not depend on the actual value of the received signal level, but on the average value. Therefore, the BSC collects all values (bit error rate and signal levels from uplink and downlink) from BTS and MS and calculates average values.
- These values are then compared to thresholds, i.e., the handover margin (HO_MARGIN), which includes some hysteresis to avoid a ping-pong effect. (Without hysteresis, even short-term interference, e.g., shadowing due to a building, could cause a handover.)
- Still, even with the HO_MARGIN, the ping-pong effect may occur in GSM – a value which is too high could cause a cut-off, and a value which is too low could cause too many handovers.


MS
BTS old
BSC old
MSC
BSC new
BTS new
measurement report
measurement result
HO decision
HO required
HO request
resource allocation
ch. activation
ch. activation ack
HO request ack
HO command
HO command
HO command
HO access
Link establishment
HO complete
HO complete
clear command
clear command
clear complete
clear complete

- Figure shows the typical signal flow during an inter-BSC, intra-MSC handover.
- The MS sends its periodic measurements reports, the BTS_{old} forwards these reports to the BSC_{old} together with its own measurements.
- Based on these values and, e.g., on current traffic conditions, the BSC_{old} may decide to perform a handover and sends the message HO_required to the MSC.
- The task of the MSC then comprises the request of the resources needed for the handover from the new BSC, BSCnew.
- This BSC checks if enough resources (typically frequencies or time slots) are available and activates a physical channel at the BTSnew to prepare for the arrival of the MS.

- The BTS_{new} acknowledges the successful channel activation, BSC_{new} acknowledges the handover request.
- The MSC then issues a handover command that is forwarded to the MS. The MS now breaks its old radio link and accesses the new BTS.
- The next steps include the establishment of the link (this includes layer two link establishment and handover complete messages from the MS).
- Basically, the MS has then finished the handover, but it is important to release the resources at the old BSC and BTS and to signal the successful handover using the handover and clear complete messages as shown.

SECURITY

- GSM offers several security services using confidential information stored in the AuC and in the individual SIM (which is plugged into an arbitrary MS).
- The SIM stores personal, secret data and is protected with a PIN against unauthorized use.(For example, the secret key Ki used for authentication and encryption procedure is stored in the SIM.)
- The security services offered by GSM are explained below:

A)Access control and authentication:

- The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM.
- The next step is the subscriber authentication . This step is based on a challenge-response scheme

B)Confidentiality:

- All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signaling.
- This confidentiality exists only between MS and BTS, but it does not exist end-to-end or within the whole fixed GSM/telephone network.

C) Anonymity:

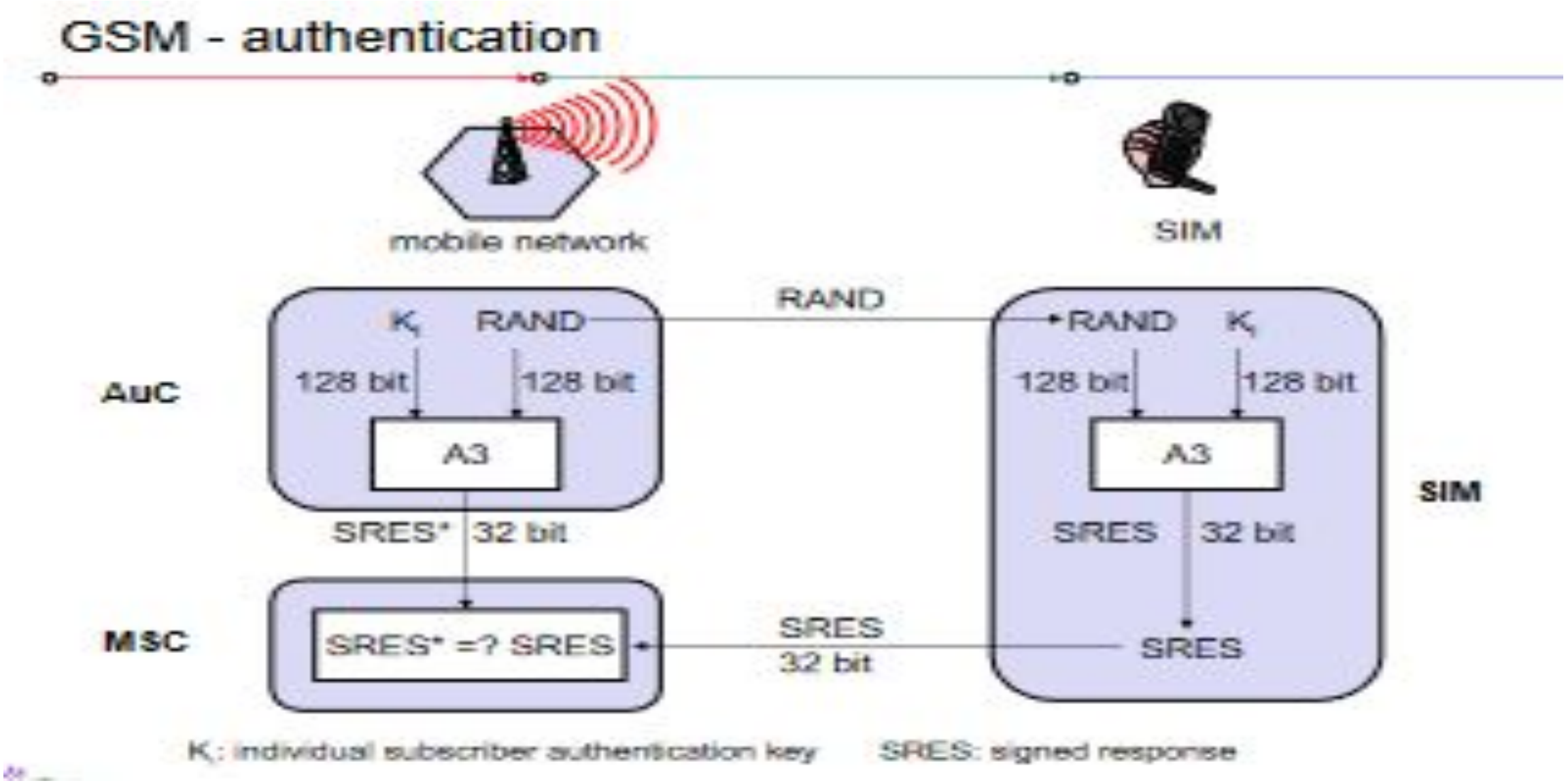
- To provide user anonymity, all data is encrypted before transmission, and user identifiers (which would reveal an identity) are not used over the air.
- Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time.

- Three algorithms have been specified to provide security services in GSM.

1. Authentication using A3 Algorithm
2. Data encryption using A5 and A8 Algorithm

- Algorithm A3 is used for authentication, A5 for encryption, and A8 for the generation of a cipher key.
- In the GSM standard only algorithm A5 was publicly available, whereas A3 and A8 were secret, but standardized with open interfaces.
- Both A3 and A8 are no longer secret, but were published on the internet in 1998. This demonstrates that security by obscurity does not really work.
- As it turned out, the algorithms are not very strong. However, network providers can use stronger algorithms for authentication – or users can apply stronger end-to-end encryption.
- Algorithms A3 and A8 (or their replacements) are located on the SIM and in the AuC and can be proprietary. Only A5 which is implemented in the devices has to be identical for all providers.

A) Authentication

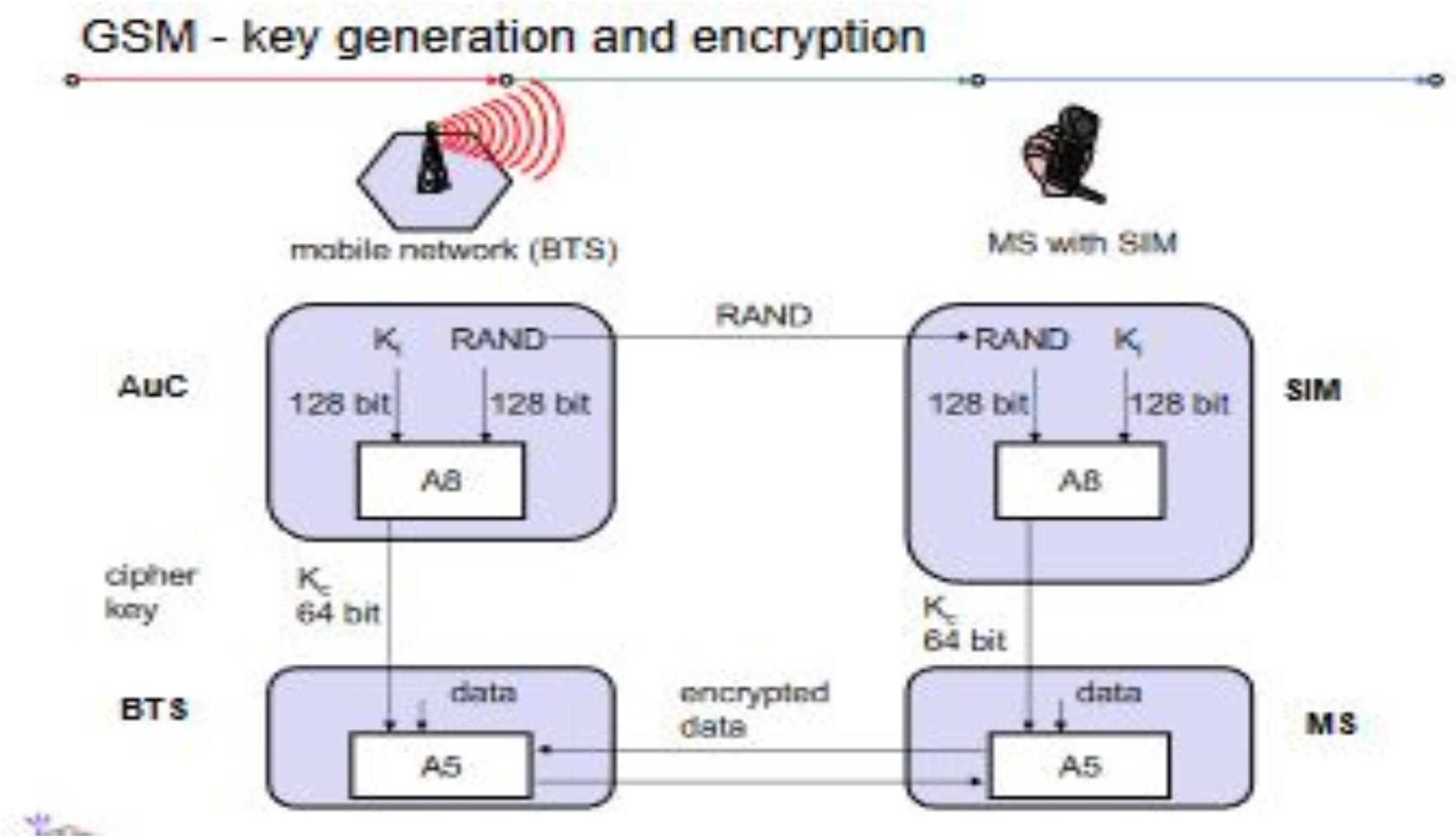


- Before a subscriber can use any service from the GSM network, he or she must be authenticated.
- Authentication is based on the SIM, which stores the individual authentication key Ki, the user identification IMSI, and the algorithm used for authentication A3.

- Authentication uses a challenge-response method:
- The access control AC generates a random number RAND as challenge, and the SIM within the MS answers with SRES (signed response) as response (see Figure .. Subscriber authentication)

- The AuC performs the basic generation of random values RAND, signed responses SRES, and cipher keys Kc for each IMSI, and then forwards this information to the HLR.
- The current VLR requests the appropriate values for RAND, SRES, and Kc from the HLR
- For authentication, the VLR sends the random value RAND to the SIM.
- Both sides, network and subscriber module, perform the same operation with RAND and the key Ki, called A3.
- The MS sends back the SRES generated by the SIM; the VLR can now compare both values. If they are the same, the VLR accepts the subscriber, otherwise the subscriber is rejected.

B) Encryption

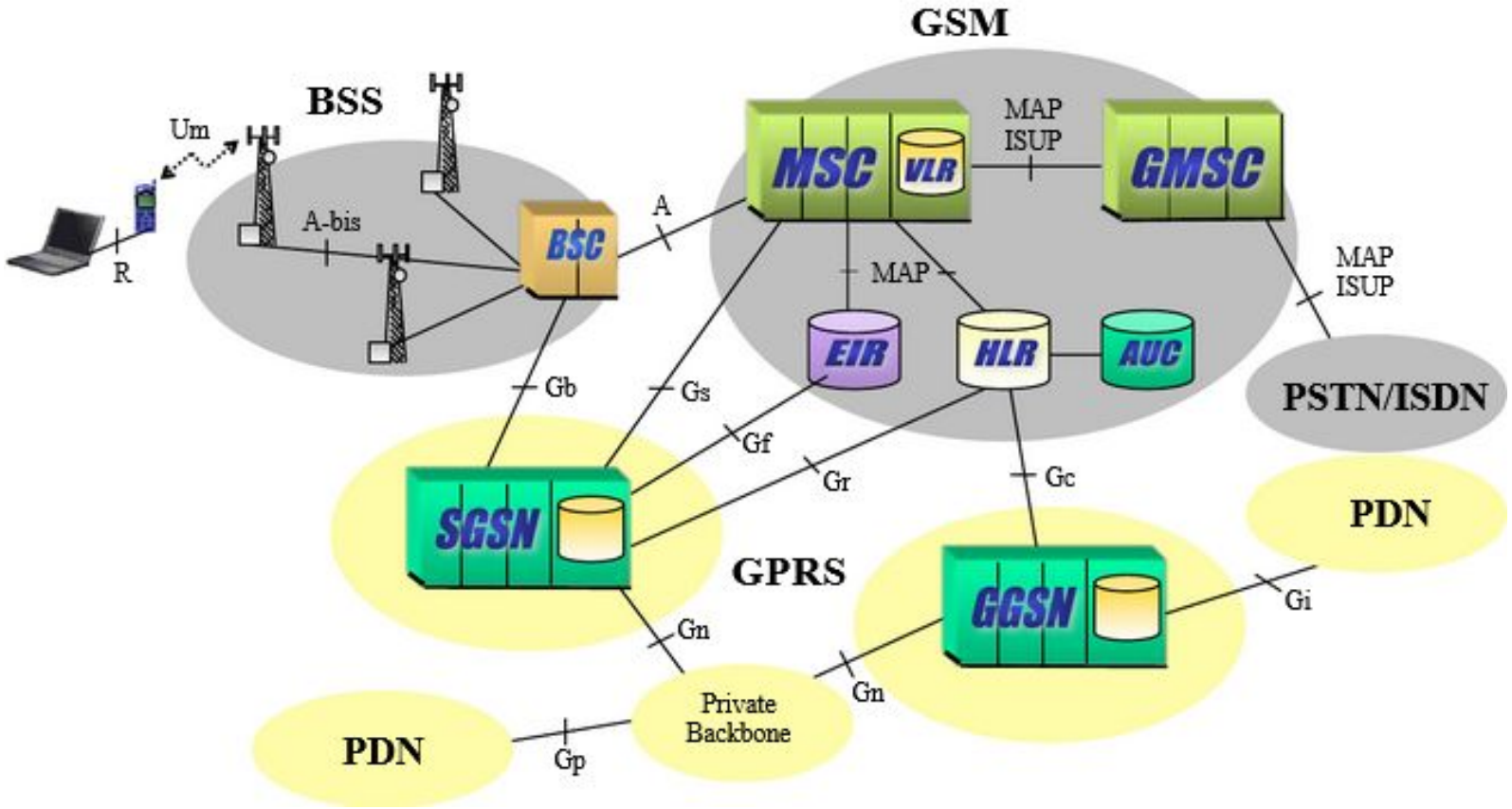


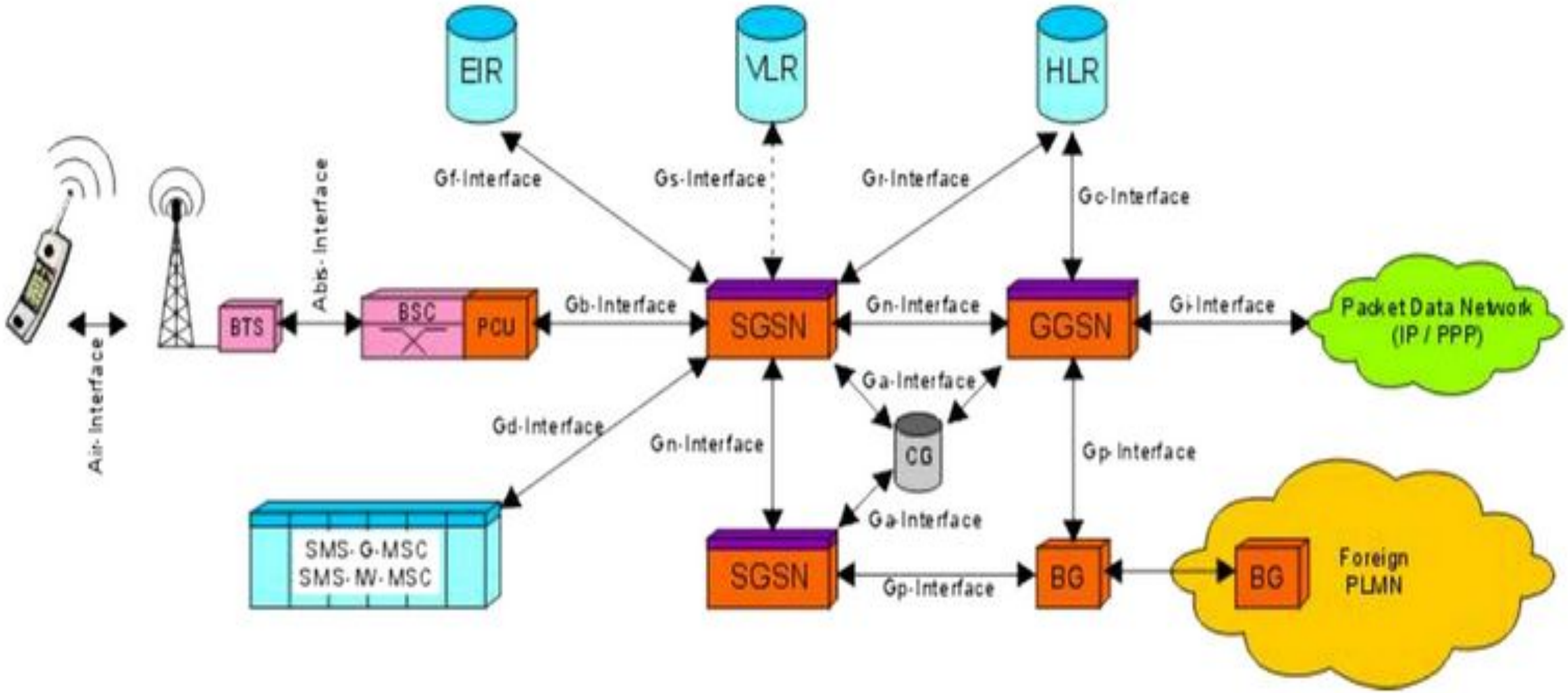
- To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface.
- After authentication, MS and BSS can start using encryption by applying the cipher key Kc (the precise location of security functions for encryption, BTS and/or BSC are vendor dependent).
- Kc is generated using the individual key Ki and a random value by applying the algorithm A8.
- Note that the SIM in the MS and the network both calculate the same Kc based on the random value RAND.

- The key Kc itself is not transmitted over the air interface.
- MS and BTS can now encrypt and decrypt data using the algorithm A5 and
- the cipher key Kc
- As Fig..(Data encryption) shows, Kc should be a 64 bit key – which is not very strong, but is at least a good protection against simple eavesdropping.
- However, the publication of A3 and A8 on the internet showed that in certain implementations 10 of the 64 bits are always set to 0, so that the real length of the key is thus only 54 consequently, the encryption is much weaker.

General packet radio service (GPRS)

- General packet radio service (GPRS) is defined as a mobile communications standard that operates on 2G and 3G cellular networks to enable moderately high-speed data transfers using packet-based technologies.





GPRS Network Architecture

- Entire GPRS network can be divided for understanding into following basic elements.
  A) Packet Control Unit (PCU) :
- This PCU is the core unit to segregate between GSM and GPRS traffic. It separates the circuit switched and packet switched traffic from the user and sends them to the GSM and GPRS networks respectively.
- In GPRS PCU has following two paths.
  1. PCU-MSC-GMSC-PSTN
  2. PCU-SGSN-GGSN-Internet (packet data network)

B)Serving GPRS Support Node(SGSN) :

It is similar to MSC of GSM network. SGSN functions are outlined below.

1. Data compression which helps minimize the size of transmitted data units.
2. Authentication of GPRS subscribers.
3. Routing of data to the corresponding GGSN when a connection to an external network is needed.
4. Mobility management as the subscriber moves from one PLMN area to the another PLMN, and possibly one SGSN to another SGSN.
5. Traffic statistics collections

C)Gateway GPRS Support Node(GGSN) :

- GGSN is the gateway to external networks such as PDN (packet data network) or IP network. It is similar to GMSC of GSM network.
- It does two main functions -
  i)Routes mobile destined packet coming from external IP networks to the relevant SGSN within the GPRS network

ii)Routes packets originated from a user to the respective external IP network

D) Border Gateway (BG) :

It is a kind of router which interfaces different operators GPRS networks. The connection between two border gateways is called GPRS tunnel.

It is more secure to transfer data between two operators using their own PLMN networks through a direct connection rather than via the public Internet which is less secure.

For this both operators need to agree to provide such connectivity and terms and conditions including charging terms.

E) Charging Gateway (CG) :

- GPRS users have to be charged for the use of the network, this is taken care by Charging gateway.
- Charging is done based on Quality of Service or plan user has opted either prepaid or post paid. This charging data generated by all the SGSNs and GGSNs in the network is referred to as Charging Data Records (CDRs).
- The Charging Gateway (CG) collects all of these CDRs, processes the same and passes it on to the Billing System.

F) DNS server :

Connected at ISP location or at IP network. It converts domain name to IP addresses required to establish internet connection and to deliver web pages on user's terminal screen.

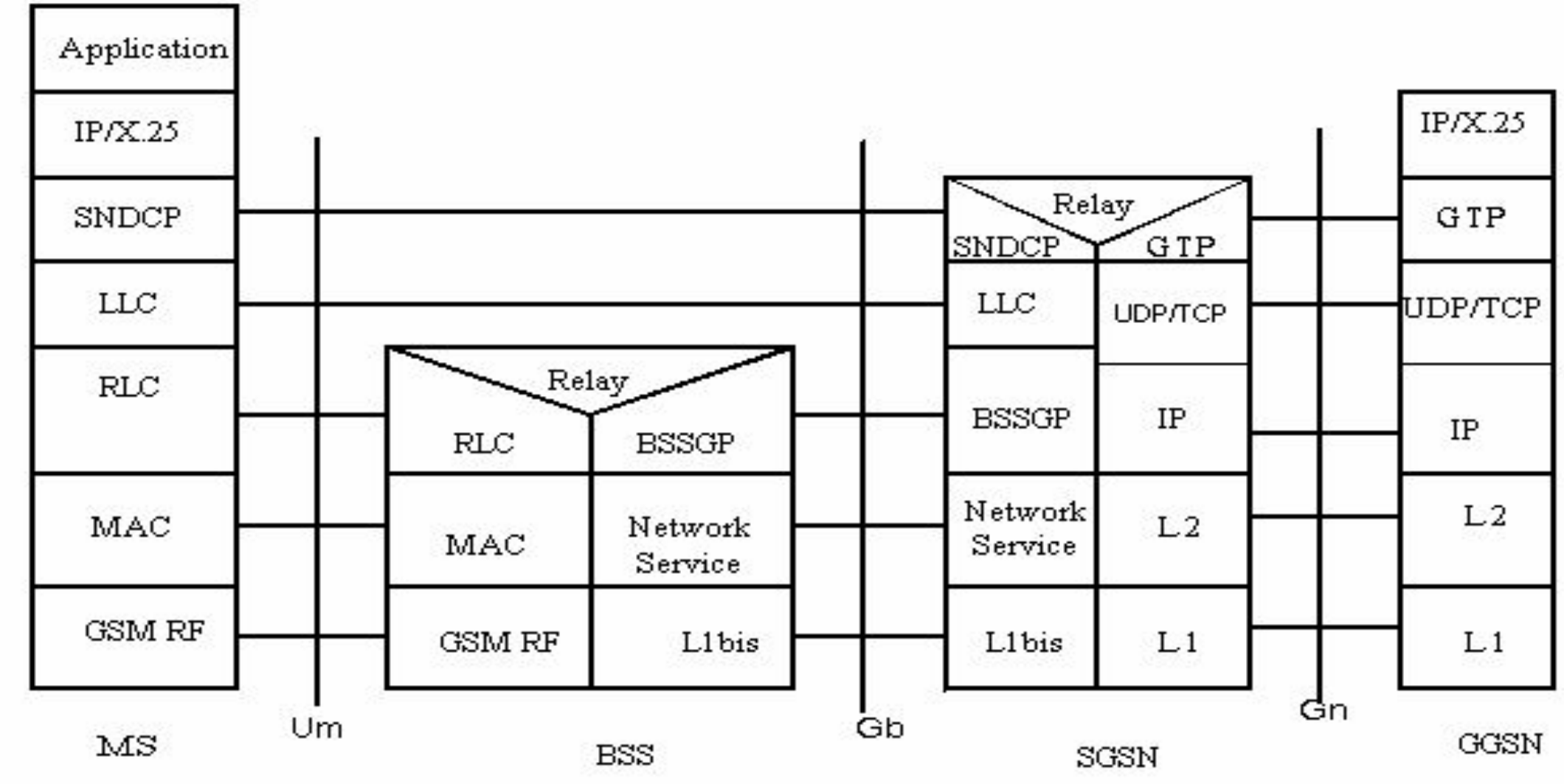
G) Intra PLMN : An IP based network inter-connecting all the above mentioned GPRS network elements in one PLMN area.

H) Inter PLMN : Connection between two different PLMN areas.

GPRS protocol architecture

- All data within the GPRS backbone, i.e., between the GSNs, is transferred using the GPRS tunneling protocol (GTP).
- GTP can use two different transport protocols, either the reliable TCP (needed for reliable transfer of X.25 packets) or the non-reliable UDP (used for IP packets).
- The network protocol for the GPRS backbone is IP (using any lower layers). To adapt to the different characteristics of the underlying networks, the subnetwork dependent convergence protocol (SNDCP) is used between an SGSN and the MS.
- On top of SNDCP and GTP, user packet data is tunneled from the MS to the GGSN and vice versa.
- To achieve a high reliability of packet transfer between SGSN and MS, a special LLC is used, which comprises ARQ and FEC mechanisms for PTP (and later PTM) services.

GPRS transmission plane protocol reference model



- All data within the GPRS backbone, i.e., between the GSNs, is transferred using the GPRS tunneling protocol (GTP).
- GTP can use two different transport protocols, either the reliable TCP (needed for reliable transfer of X.25 packets) or the non-reliable UDP (used for IP packets).
- The network protocol for the GPRS backbone is IP (using any lower layers).
- To adapt to the different characteristics of the underlying networks, the subnetwork dependent convergence protocol (SNDCP) is used between an SGSN and the MS.
- On top of SNDCP and GTP, user packet data is tunneled from the MS to the GGSN and vice versa.
- To achieve a high reliability of packet transfer between SGSN and MS, a special LLC is used, which comprises ARQ and FEC mechanisms for PTP (POINT TO POINT) services.

- A base station subsystem GPRS protocol (BSSGP) is used to convey routing and QoS-related information between the BSS and SGSN.
- BSSGP does not perform error correction and works on top of a frame relay (FR) network.
- Finally, radio link dependent protocols are needed to transfer data over the Um interface. The radio link protocol (RLC) provides a reliable link, while the MAC controls access with signaling procedures for the radio channel and the mapping of LLC frames onto the GSM physical channels.
- The radio interface at Um needed for GPRS does not require fundamental changes compared to standard GSM .
- However, several new logical channels and their mapping onto physical resources have been defined. For example, one MS can allocate up to eight packet data traffic channels (PDTCHs).
- Capacity can be allocated on demand and shared between circuit-switched channels and GPRS. This allocation can be done dynamically with load supervision or alternatively, capacity can be pre-allocated.

Advantages Of GPRS

1. Billing made simple

- When compared to circuit-switched services, GPRS packet transfer offers better consumer billing. When it comes to circuit-switched services, the cost is determined by the length of the connection. One of the significant disadvantages of circuit switching for IoT is cost-efficiency. The connection length determines the subscriber's operating costs in the circuit switch.

2. Increased speed

- A significant advantage of the GPRS system is that it provides a higher data rate than GSM. GSM was designed to transmit data at approximately 14.4 kbit/s at first. Over the 2G network, GPRS, on the other hand, provided data speeds up to 86kbit/s. It made matters like streaming and gaming possible for customers. It allowed for monitoring in enterprises.

3.Always-"on" connectivity

- Another benefit of GPRS is that it is always available. A GPRS connection can provide constant Internet connectivity, quick messaging, and improved SMS transfers. It was also the fastest network ever seen when it was first launched

Disadvantages of GPRS

1.Limited cell capacity

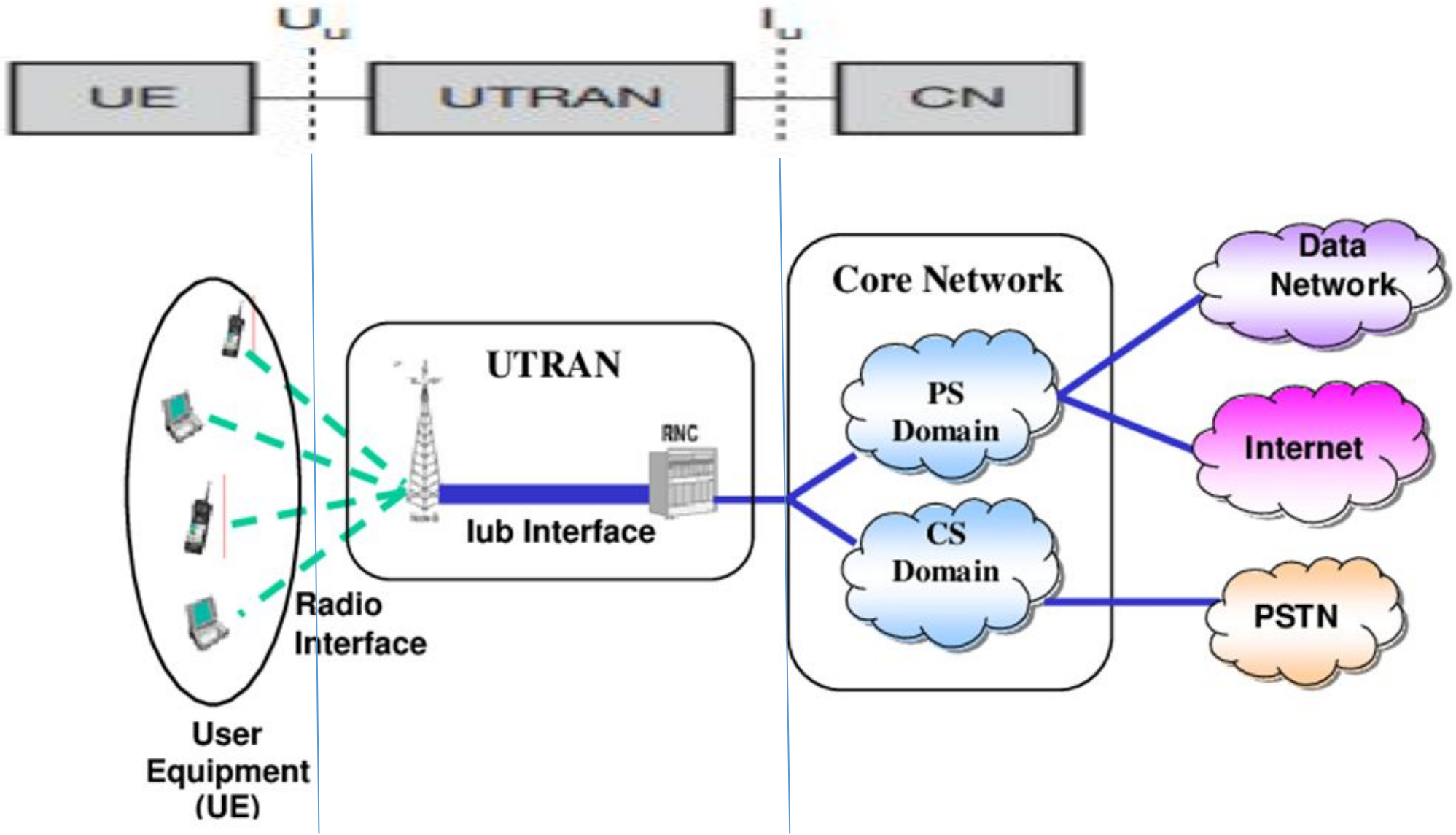
- GPRS is technically adequate for most IoT use cases, but not all. 2G or 3G with GPRS is typically a theoretically acceptable fit if all you need is slow, occasional data transfers. However, for data-intensive applications, the existing cell capacity of a system is impacted by GPRS.

2.Risk of slower speeds

- To achieve the maximum possible GPRS data transmission speed of 172.2 kbps, all eight timeslots should be taken over by an individual user with no error safety. The supported data rates (171.2/384 Kbps) are slower than the current wireless protocols such as HSPA, LTE, LTE-advanced, and so on.

Universal mobile telecommunication system (UMTS)

- UMTS is defined as the third-generation (3G) mobile network built on the global GSM standard, compatible with data transfer up to 2 Megabits per second.
- UMTS is popularly known as a third-generation (3G) cellular network. It was seen as a better cellular technology for data transfer than its predecessor, the GSM technology, which used GPRS and EDGE data services,
- UMTS offers faster data transfer, improved cellular capabilities, greater range/bandwidth, and better radio spectrum efficiency.
- UMTS uses code division multiple access (CDMA) technology, it has a broader bandwidth than other CDMA systems, e.g., CDMA2000. So, it is sometimes referred to as wideband CDMA or WCDMA.



Main components of the UMTS Reference architecture

- A mobile network of the UMTS can be divided into three major parts – user equipment, the access network, and the core network.
- These parts are linked and work together to transfer data through the UMTS mobile network.
- The UTRAN is connected to the user equipment (UE) via the radio interface Uu (which is comparable to the Um interface in GSM).
- Via the Iu interface (which is similar to the A interface in GSM), UTRAN communicates with the core network (CN)

1.The user equipment

- The user equipment is divided into the mobile station, which is the device itself and the SIM card, which describes the U-SIM or universal subscriber identity module. The mobile station cannot transmit signals without the U-SIM. The U-SIM performs three main functions, which include:
- Holding of a subscriber's identity
- Performing authentication algorithms
- Storing authentication and encryption keys

2.The access network

- The access network consists of towers to which the mobile station connects. These towers are known as Node B, intermediates between the mobile station and the rest of the mobile network. There can be one or more Node Bs depending on the size of the network

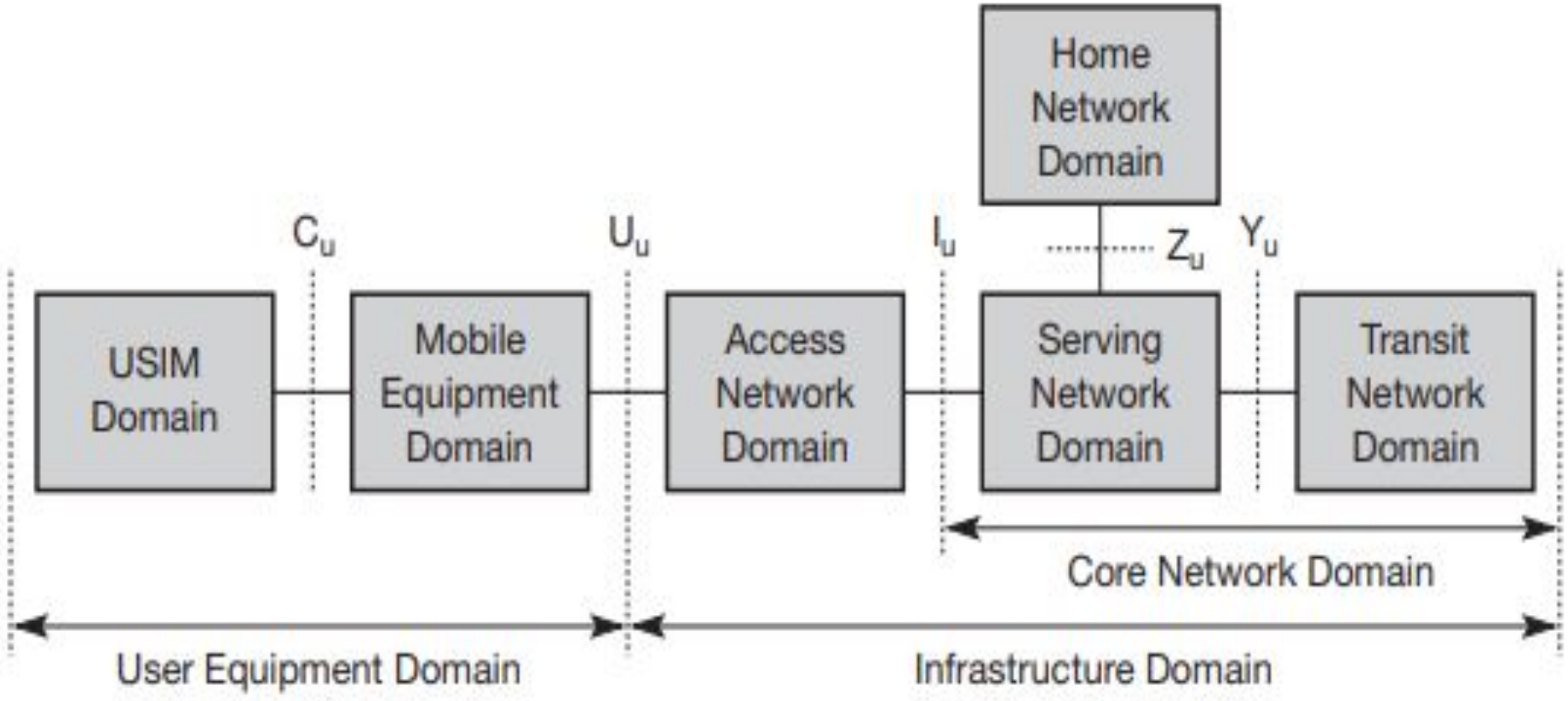
- Another essential component of the access network is the radio network controller (RNC). This is where the intelligence of the access network lies. It processes the data gotten from Node B connected to it. The Node B and RNC composite structure is known as UMTS terrestrial radio access network (UTRAN).
- The interface between the mobile station and the Node B is based on the air Wideband CDMA technology (WCDMA). When Node B receives information from the Radio Network Controller, it spreads it by multiplying it with the CDMA code, modulates it, and then sends the information to the mobile station.
- If the data comes from the mobile station, it must undergo despreading and demodulation at Node B before it gets to the RNC.
- Node B also handles error correction between the station and RNC

- The RNC also acts as an admission controller. For instance, if a mobile station (e.g., a phone) wants to transmit through a voice call, and a particular Node B is congested with other connected devices, the RNC gives it a new CDMA code to connect it to an available Node B.
- Also, since UMTS also sends information in the form of packets of data, like voice calls over Skype, the RNC regulates the bit rate and speed of transmission to ensure hitch-free transmission as this is a real-time activity. If the application is not a real-time activity – such as downloading a file – if a particular Node B is congested, the RNC reduces the bit rate of other devices that do not require real-time feedback.

3.The core network

- This is the backbone network. It consists of a circuit-switched (CS) domain and packet-switched (PS) domain.
- The circuit-switched domain is the part of the network responsible for voice calls, while the packet-switched domain is responsible for carrying the packet data.
- The packet-switched domain takes care of the internet services.
- The CS and PS domains consist of various databases that hold information necessary for running the system.

UMTS domains and interfaces



- UMTS further subdivides the above simplified architecture into so-called domains (see Figure).
- The user equipment domain is assigned to a single user and comprises all the functions that are needed to access UMTS services. Within this domain are the USIM domain and the mobile equipment domain.
- The USIM domain contains the SIM for UMTS which performs functions for encryption and authentication of users, and stores all the necessary user-related data for UMTS.
- Typically, this USIM belongs to a service provider and contains a micro processor for an enhanced program execution environment (USAT, UMTS SIM application toolkit).
- The end device itself is in the mobile equipment domain. All functions for radio transmission as well as user interfaces are located here.

- The infrastructure domain is shared among all users and offers UMTS services to all accepted users. This domain consists of the access network domain, which contains the radio access networks (RAN), and the core network domain, which contains access network independent functions.
- The core network domain can be separated into three domains with specific tasks. The serving network domain comprises all functions currently used by a user for accessing UMTS services. All functions related to the home network of a user, e.g., user data look-up, fall into the home network domain.
- Finally, the transit network domain may be necessary if, for example, the serving network cannot directly contact the home network. All three domains within the core network may be in fact the same physical network. These domains only describe functionalities.

Advantages of UMTS

1. UMTS could be a successor to 2G based GSM advances counting GPRS and EDGE . Gaining a 3rd title 3GSM since it could be a 3G relocation for GSM
2. Support 2Mbit/s information rates.
3. Higher Information rates at lower incremental costs.
4. Benefits of programmed universal wandering also necessarily security and charging capacities, permitting administrators emigrate from 2G to 3G whereas holding numerous of their existing back-office frameworks
5. Gives administrators the adaptability to present unused mixed media administrations to trade clients and buyers
6. This not as it were gives client a valuable phone but moreover deciphers higher incomes for the administrator.

Disadvantages of UMTS

1. It is more expensive than GSM.
2. Universal Mobile Telecommunication System has poor video experience.
3. Universal Mobile Telecommunication System still not broadband.

Applications of UMTS

1. Streaming / Download (Video, Audio)
2. Videoconferences.
3. Fast Internet / Intranet.
4. Mobile E-Commerce (M-Commerce)
5. Remote Login
6. Background Class applications
7. Multimedia-Messaging, E-Mail
8. FTP Access
9. Mobile Entertainment (Games)

Comparison of GSM and UMTS

Features	GSM	UMTS
Network Architecture	Circuit-switched	Circuit-switched and packet-switched
Radio Access Technology	FDMA and TDMA	Wideband CDMA (W-CDMA)
Bandwidth	200 kHz	5 MHz
Data Rate	Up to 384 kbps	Up to 2 Mbps for HSDPA; up to 7.2 Mbps for HSDPA
Applications	Voice and SMS	Multimedia applications
Roaming Support	Limited	Automatic international roaming
Video Quality	Poor	Improved compared to GSM
Cost	Affordable	More expensive than GSM
Broadband	Not broadband	Offers broadband capabilities

'Universal Terrestrial Radio Access' (UTRA)

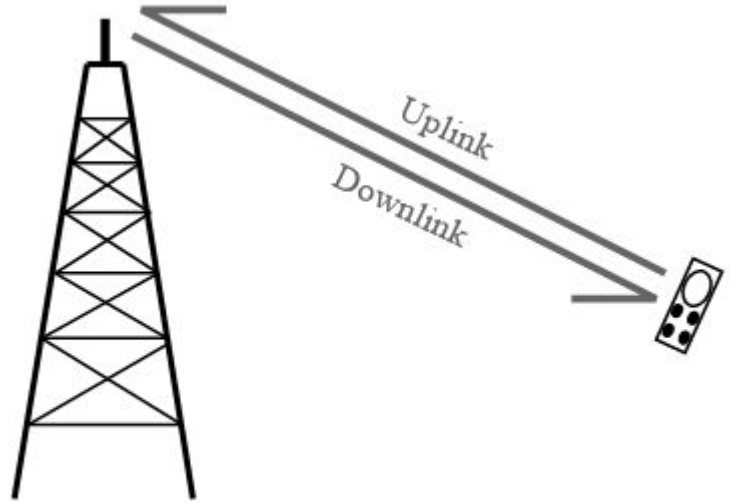
- The radio technology used between mobile terminals and the base stations of 3GPP™ systems is generically known as 'Universal Terrestrial Radio Access' (UTRA) and the access network as 'Universal Terrestrial Radio Access Network' (UTRAN).
- 3GPP™ is a 3rd Generation partnership project bringing together national Standards Development Organizations (SDOs) from around the globe initially to develop technical specifications for the 3rd generation of mobile, cellular telecommunications, UMTS.

UTRA uplink & downlink

- Being a full duplex system, i.e. transmitting simultaneously in both directions, it is necessary to be able to define which direction is which.

- ***Downlink;*** This may also sometimes be known as the forward link, and it is the link from the Node B or base station to the User Equipment (UE).

- ***Uplink;*** This may also sometimes be known as the reverse link, and it is the link from the User Equipment (UE) to the Node B or base station.



Uplink and downlink directions

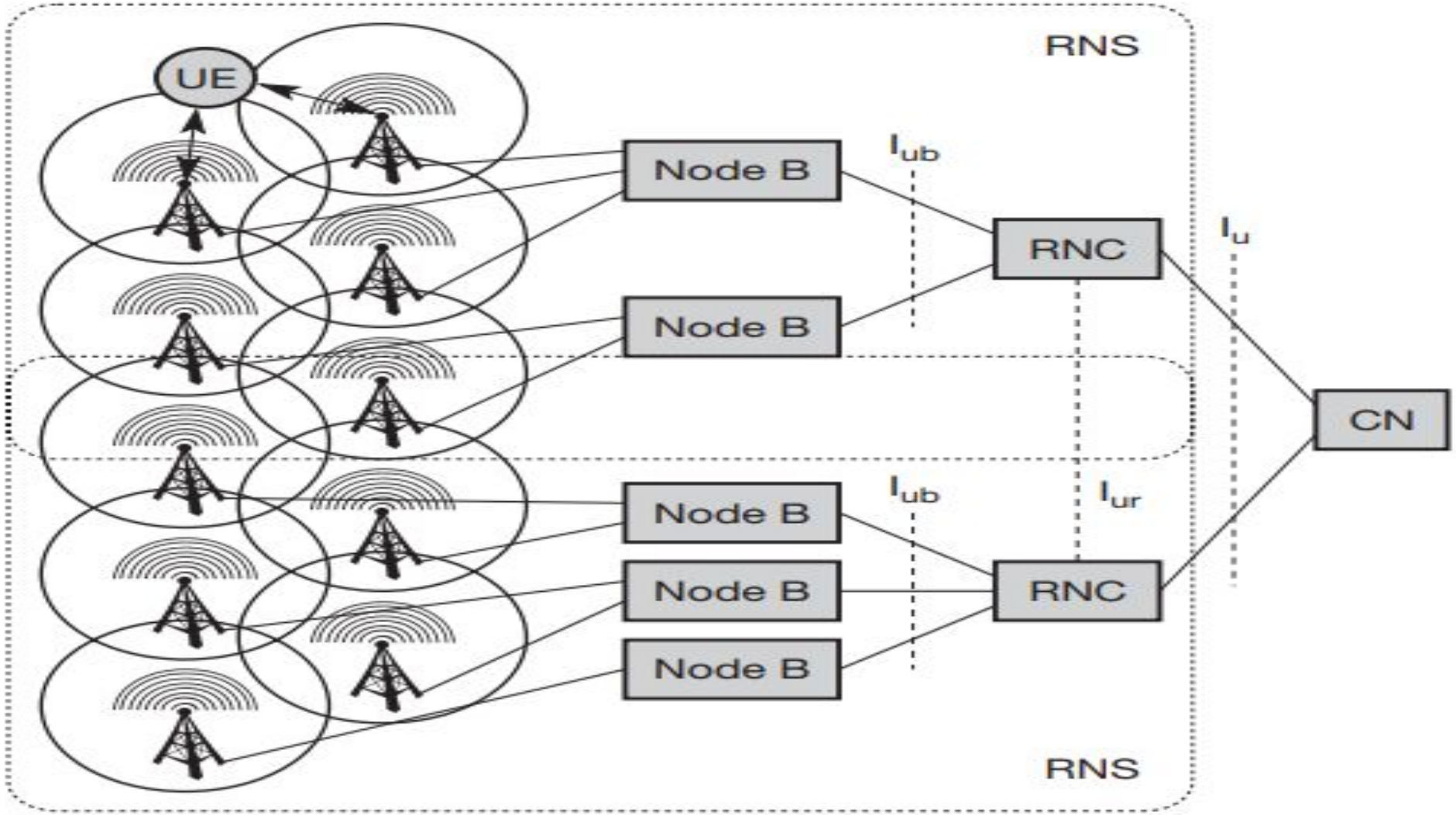
Frequency division and time division duplex

- In view of the fact that transmissions have to be made in both directions, i.e. in both uplink and downlink.
- Two techniques are used to ensure concurrent or near concurrent transmissions in both directions: frequency division duplex and time division duplex.
- ***UTRA-FDD:*** The frequency division duplex version of UTRA uses a scheme whereby transmissions in the uplink and downlink occur on different frequencies. Although this requires double the bandwidth to accommodate the two transmissions, and filters to prevent the transmitted signal from interfering with the receiver..
- ***UTRA-TDD:*** The time division duplex version of the UTRA uses uplink and downlink transmissions that use the same frequency but are timed to occur at different intervals.

KEY SPECIFICATIONS FOR UTRAN OPERATION FOR FDD & TDD

PARAMETER	UTRA FDD	UTRA TDD
Multiple access method	CDMA	TDMA, CDMA
Channel spacing	5 MHz	5 MHz (and 1.6MHz for TD-SCDMA)
Carrier chip rate	3.84 Mcps	3.84 Mcps
Spreading factors	4 .. 512	1 .. 16
Time slot structure	15 slots / frame	15 / 14 slots / frame
Frame length (ms)	10	10
Multirate concept	Multicode, and OVSF[1]	Multicode, multislot and OVSF[1]
Burst types	N/A	(1) traffic bursts (2) random access burst (3) synchronisation burst
Detection	Coherent based on pilot symbols	Coherent based on mid-amble
Dedicated channel power control	Fast closed loop 1500 Hz rate	Uplink: open loop 100 Hz or 200 Hz rate Downlink: closed loop max 800 Hz rate

Universal Terrestrial Radio Access Network, UTRAN



- UTRA network (UTRAN) consists of several radio network subsystems (RNS).
- Each RNS is controlled by a radio network controller (RNC) and comprises several components that are called node B.
- An RNC in UMTS can be compared with the BSC; a node B is similar to a BTS.
- Each node B can control several antennas which make a radio cell.
- The mobile device, UE User equipment, can be connected to one or more antennas
- Having standardised interfaces within various areas of the network including the UTRAN allows network operators to select different network entities from different suppliers. There are several interfaces that are defined for the UTRAN elements

1.Iu : The Iu interface connects the UTRAN to the core network.

2.Iub : The Iub connects the NodeB and the RNC within the UTRAN

3.Iur : The Iur interface allows communication between different RNCs within the UTRAN

1.Radio Network Controller, RNC:

- This element of the UTRAN / radio network subsystem controls the Node Bs that are connected to it, i.e. the radio resources in its domain.
- RNC in UMTS has a broad spectrum of tasks as listed below-

1. Call admission control: It is very important for CDMA systems to keep the interference below a certain level. The RNC calculates the traffic within each cell and decides, if additional transmissions are acceptable or not.
2. Congestion control: During packet-oriented data transmission, several stations share the available radio resources. The RNC allocates bandwidth to each station in a cyclic fashion and must consider the QoS requirements
3. Encryption/decryption: The RNC encrypts all data arriving from the fixed network before transmission over the wireless link (and vice versa).

4. ATM switching and multiplexing, protocol conversion: Typically, the connections between RNCs, node Bs, and the CN are based on ATM. An RNC has to switch the connections to multiplex different data streams.

5. Radio resource control: The RNC controls all radio resources of the cells connected to it via a node B. This task includes interference and load measurements. The priorities of different connections have to be obeyed.

6. Radio bearer setup and release: An RNC has to set-up, maintain, and release a logical data connection to a UE.

7. Code allocation: The CDMA codes used by a UE are selected by the RNC. These codes may vary during a transmission.

8. Power control: The RNC only performs a relatively loose power control (the outer loop). This means that the RNC influences transmission power based on interference values from other cells or even other RNCs.

9. Handover control and RNS relocation: Depending on the signal strengths received by UEs and node Bs, an RNC can decide if another cell would be better suited for a certain connection. If the RNC decides for handover it informs the new cell and the UE. If a UE moves further out of the range of one RNC, a new RNC responsible for the UE has to be chosen. This is called RNS relocation.

10. Management: Finally, the network operator needs a lot of information regarding the current load, current traffic, error states etc. The RNC provides interfaces to manage its network.

2.Node B:

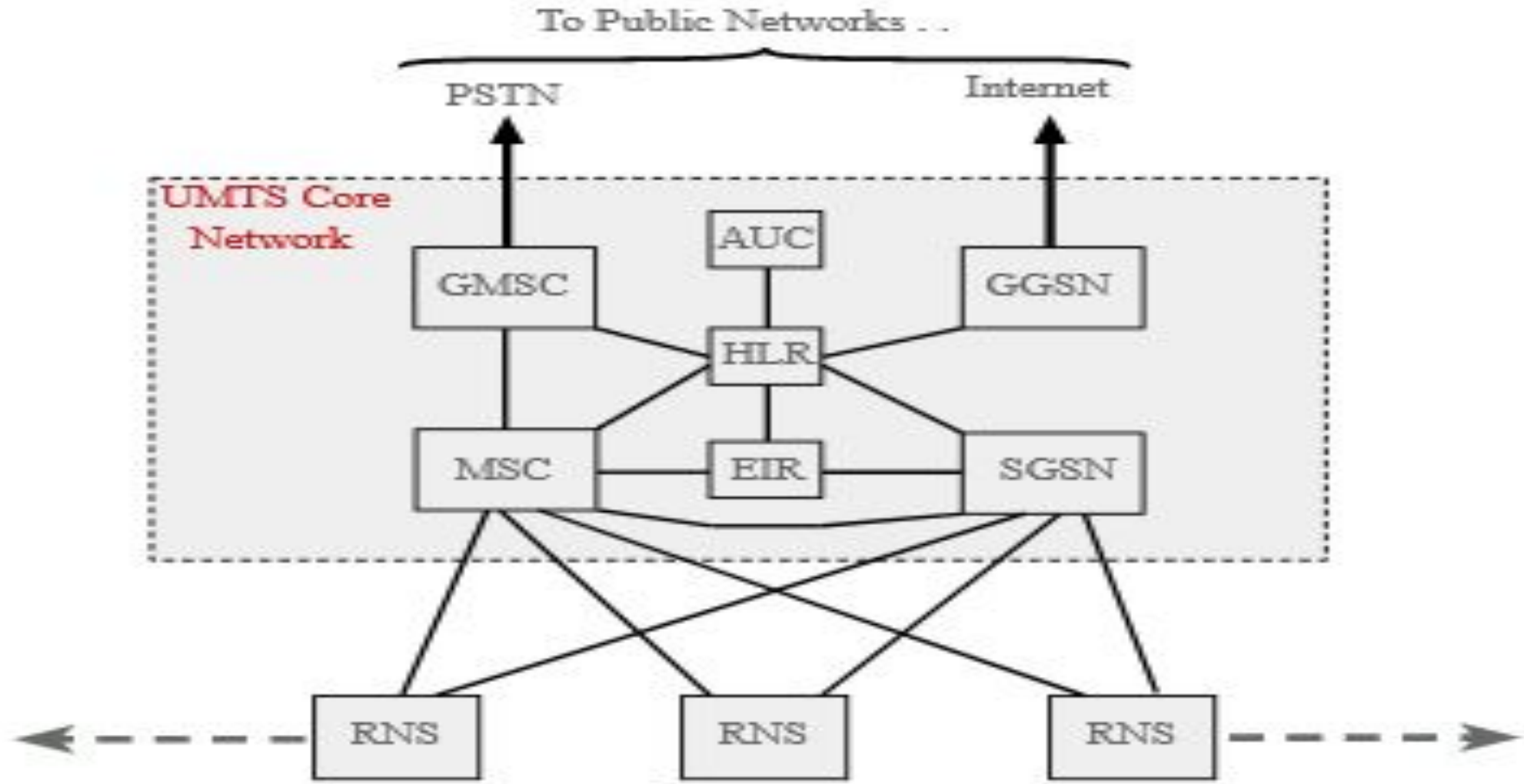
- Node B is the term used within UMTS to denote the base station transceiver. This part of the UTRAN contains the transmitter and receiver to communicate with the UEs within the cell.
- An important task of a node B is the inner loop power control to mitigate near-far effects. This node also measures connection qualities and signal strengths.
- Node B can even support a special case of handover, a so-called softer handover which takes place between different antennas of the same node B
- In order to facilitate effective handover between Node Bs under the control of different RNCs, the RNC not only communicates with the Core Network, but also with neighboring RNCs.

3.User equipment

- As the counterpart of a node B, the UE performs signal quality measurements, inner loop power control, spreading and modulation, and rate matching.
- As a counterpart of the RNC, the UE has to cooperate during handover and cell selection, performs encryption and decryption, and participates in the radio resource allocation process.
- As a counterpart of the CN, the UE has to implement mobility management functions, performs bearer negotiation, or requests certain services from the network.

3G UMTS Core Network

- the UMTS core network was split into two different areas:
- ***Circuit switched elements:*** These elements were primarily based on the GSM network entities and carry data in a circuit switched manner, i.e. a permanent channel for the duration of the call.
- ***Packet switched elements:*** These network entities were designed to carry packet data. This enabled much higher network usage as the capacity could be shared and data was carried as packets which were routed according to their destination.
- Some network elements, particularly those that were associated with registration were shared by both domains and operated in the same way that they did with GSM



UMTS Network Architecture Overview

1.Circuit switched elements

The circuit switched elements of the UMTS core network architecture included the following network entities:

- ***Mobile switching centre (MSC):*** This was essentially the same as that within GSM, and it managed the circuit switched calls under way.
- ***Gateway MSC (GMSC):*** This was effectively the interface to the external networks.

2.Packet switched elements

The packet switched elements of the 3G UMTS core network architecture included the following network entities:

- ***Serving GPRS Support Node (SGSN):*** As the name implies, this entity was first developed when GPRS was introduced, and its use has been carried over into the UMTS network architecture.

- The SGSN provided a number of functions within the UMTS network architecture.
- Mobility management When a UE attached to the Packet Switched domain of the UMTS Core Network, the SGSN generates MM information based on the mobile's current location.
- Session management: The SGSN manage the data sessions providing the required quality of service and it also managed what were termed the PDP (Packet data Protocol) contexts, i.e. the pipes over which the data was sent.
- Interaction with other areas of the network: The SGSN was able to manage its elements within the network only by communicating with other areas of the network, e.g. MSC and other circuit switched areas.
- Billing: The SGSN was also responsible billing. It achieved this by monitoring the flow of user data across the GPRS network. CDRs (Call Detail Records) were generated by the SGSN before being transferred to the charging entities (Charging Gateway Function, CGF).

- ***Gateway GPRS Support Node (GGSN):***
- Like the SGSN, this entity was also first introduced into the GPRS network.
- The Gateway GPRS Support Node (GGSN) was the central element within the UMTS packet switched network.
- It handled inter-working between the UMTS packet switched network and external packet switched networks, and could be considered as a very sophisticated router.
- In operation, when the GGSN received data addressed to a specific user, it checked if the user was active and then forwarded the data to the SGSN serving the particular UE.

3.Shared elements

The shared elements of the 3G UMTS core network architecture included the following network entities:

- ***Home location register (HLR):***

- This database contained all the administrative information about each subscriber along with their last known location. In this way, the UMTS network was able to route calls to the relevant RNC / Node B.
- When a user switched on their UE, it registered with the network and from this it was possible to determine which Node B it communicated with so that incoming calls could be routed appropriately.
- Even when the UE was not active (but switched on) it re-registered periodically to ensure that the network (HLR) was aware of its latest position with their current or last known location on the network.

- ***Equipment identity register (EIR):***
- The EIR was the entity that decided whether a given UE equipment could be allowed onto the network.
- Each UE equipment had a number known as the International Mobile Equipment Identity. This number, as mentioned above, was installed in the equipment and was checked by the network during registration.
- ***Authentication centre (AuC) :***
- The AuC was a protected database that contained the secret key also contained in the user's USIM card.