Global System for Mobile Communications

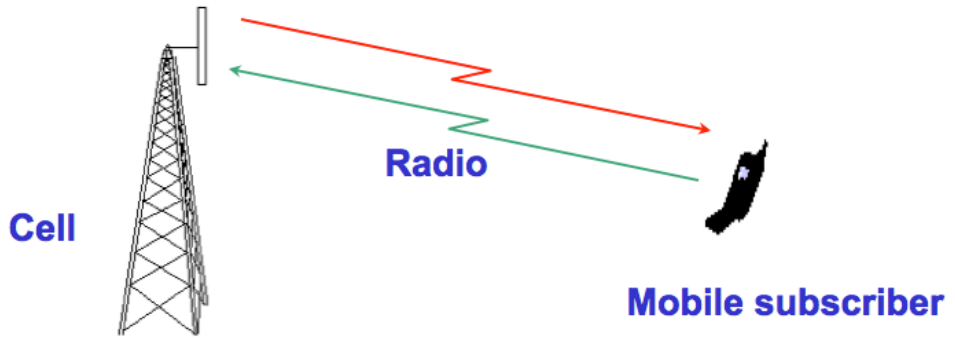
Contents

1. Introduction

- GSM History
  - ✓ 1981
    - Analogue cellular introduced
    - Franco-German study of digital pan-European cellular system
  - ✓ 1987
    - MoU (Memorandum Of Understanding, 合作瞭解備忘錄) signed by over 18 countries
  - ✓ 1989
    - GSM was moved into the ETSI organization
  - ✓ 1990
    - DCS1800 (edited GSM900) specification developed
- Global System for Mobile Communications (GSM)
  - ✓ A set of recommendations and specifications for a digital cellular telephone network (known as a Public Land Mobile Network, or PLMN)

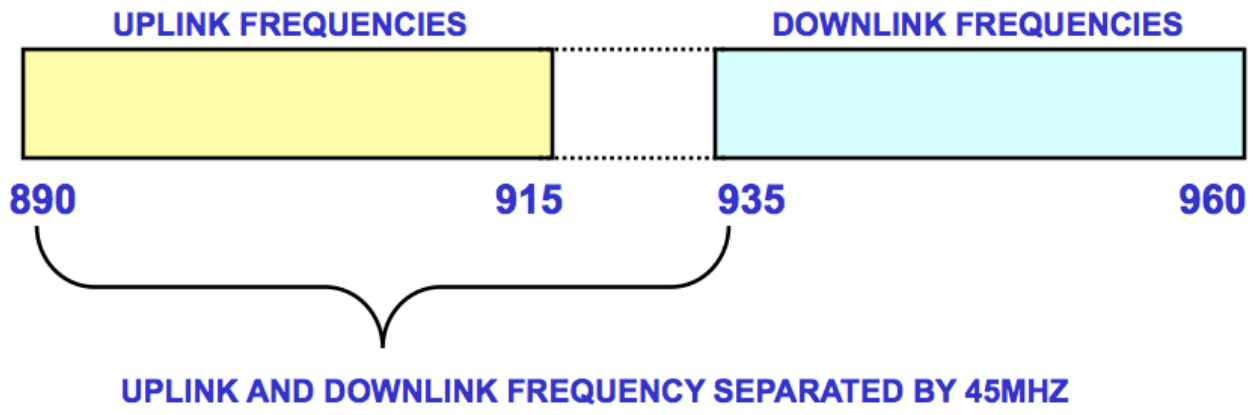
Cellular Telephony

- A cellular telephone system links mobile subscribers into the public telephone system or to another cellular subscriber
- The service area in which mobile communication is to be provided is divided into regions called cells
- Each cell has the equipment to transmit and receive calls from any subscriber located within the borders of its radio coverage area



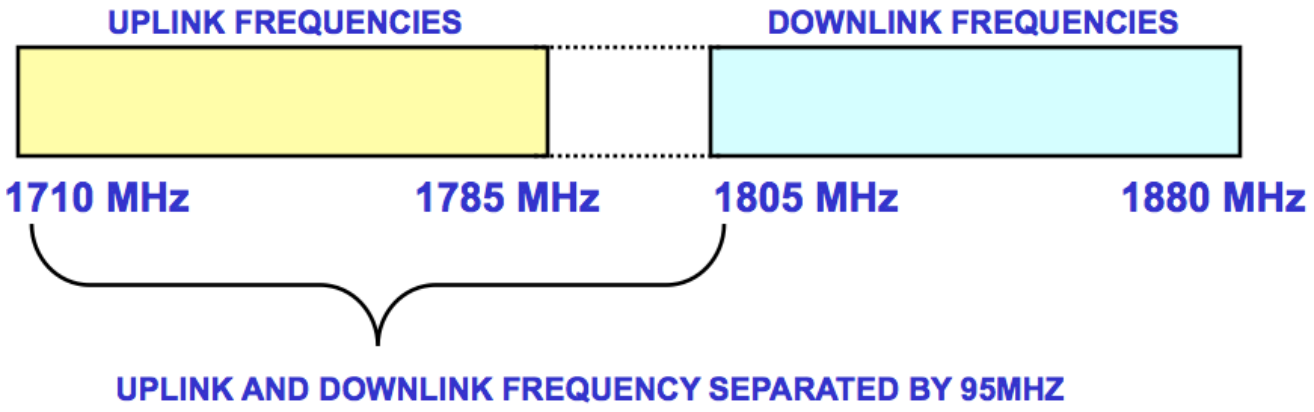
GSM Frequencies

- GSM systems use radio frequencies between 890-915 MHz to receive and between 935-960 MHz to transmit
- RF carriers are spaced every 200 kHz (8 users), allowing a total of 124 carriers to use
- An RF carrier is a pair of radio frequencies, one used in each direction
- Transmit and receive frequencies are always separated by 45 MHz



DCS1800 Frequencies

- DCS1800 systems use radio frequencies between 1710-1785 MHz to receive and between 1805-1880 MHz to transmit
- RF carriers are spaced every 200 kHz (8 users), allowing a total of 373 carriers
- Transmit and receive frequencies are always separated by 95 MHz



- 1. Introduction
- 2. Features of GSM
- 3. Network Components
- 4. Channel Concept
- 5. Coding, Interleaving, Ciphering
- 6. Signaling
- 7. Handover
- 8. Location Update

2. Features of GSM

- Increased capacity
- Audio quality
- Use of standardized open interface
- Improved security and confidentiality
- Cleaner handovers
- Subscriber identification
- Enhanced range of services
- Frequency reuse

Increased Capacity

- The GSM system provides a greater subscriber capacity than analogue systems
- GSM allows eight conversations per 200 kHz channel pair (a pair comprising one transmit channel and one receive channel)
- Digital channel coding and the modulation used makes the signal resistant to interference from cells where the same frequencies are re-used (co-channel interference)

- Note: Co-channel interference (CCI)
  - crosstalk from two different radio transmitters using the same frequency
  - in cellular mobile communication (GSM & LTE Systems, for instance), frequency spectrum is a precious resource which is divided into non-overlapping spectrum bands which are assigned to different cells
    - however, after certain geographical distance, the frequency bands are re-used, i.e. the same spectrum bands are reassigned to other distant cells
    - thus, besides the intended signal from within the cell, signals at the same frequencies (co-channel signals) arrive at the receiver from the undesired transmitters located (far away) in some other cells and lead to deterioration in receiver performance

Audio Quality

- Digital transmission of speech and high performance digital signal processors provide good quality speech transmission
- Since GSM is a digital technology, the signals passed over a digital air interface can be protected against errors by using better error detection and correction techniques
- In regions of interference or noise-limited operation the speech quality is noticeably better than analogue

Use of Standardized Open Interface

- Standard interfaces such as Signaling System C7 (*SS7*) and *X25* are used throughout the system
  - ✓ hence different manufacturers can be selected for different parts of the PLMN
  - ✓ there is a high flexibility in where the network components are situated

- Note: Signalling System No. 7 (SS7)
  - a set of telephony signaling protocols developed in 1975
  - features
    - set up and tear down public switched telephone network (PSTN) telephone calls
    - perform number translation, local number portability, prepaid billing, short message service (SMS), and other mass market services

- Note: X.25
  - an ITU-T standard protocol suite for packet switched wide area network (WAN) communication
  - an X.25 WAN consists of
    - packet-switching exchange (PSE) nodes as the networking hardware
    - leased lines, plain old telephone service connections or ISDN connections as physical links
  - X.25 has, to a large extent, been replaced by less complex protocols, especially the Internet protocol (IP)

Improved Security and Confidentiality

- GSM offers high speech and data confidentiality
  - ✓ subscriber authentication can be performed by the system to check if a subscriber is a valid subscriber or not
  - ✓ calls are encoded and ciphered when sent over air
- The mobile equipment can be identified independently from the mobile subscriber
  - ✓ the mobile has a identity number hard coded into it when it is manufactured
  - ✓ this number is stored in a standard database (EIR) and whenever a call is made the equipment can be checked to see if it has been reported stolen

Cleaner Handovers

- GSM uses *Mobile Assisted HandOver* (*MAHO*) technique
  - ✓ the mobile itself carries out the signal strength and quality measurement of its server and signal strength measurement of its neighbors
  - ✓ this data is passed on the network which then uses sophisticated algorithms to determine the need of handover

Subscriber IDentification

- In a GSM system the mobile station (MS) and the subscriber are identified separately
  - ✓ the subscriber is identified by means of a smart card known as a SIM
  - ✓ this enables the subscriber to use different mobile equipment while retaining the same subscriber number

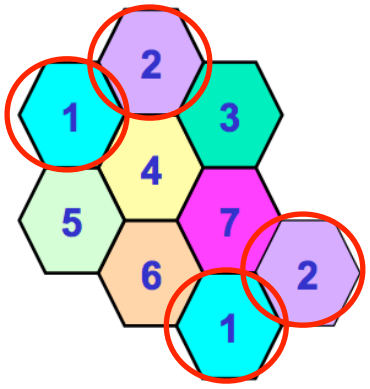
Enhanced Range of Services

- Speech services
  - ✓ normal telephony
- Short Message Service (SMS)
  - ✓ point to point transmission of text message
- Cell broadcast
  - ✓ transmission of text message from the cell to all MS in its coverage area
  - ✓ message like traffic information or advertising can be transmitted

- Fax and data services
  - ✓ data rates available are 2.4 Kb/s, 4.8 Kb/s and 9.6 Kb/s
- Supplementary services
  - ✓ number identification
  - ✓ call barring
  - ✓ call forwarding
  - ✓ charging display etc.

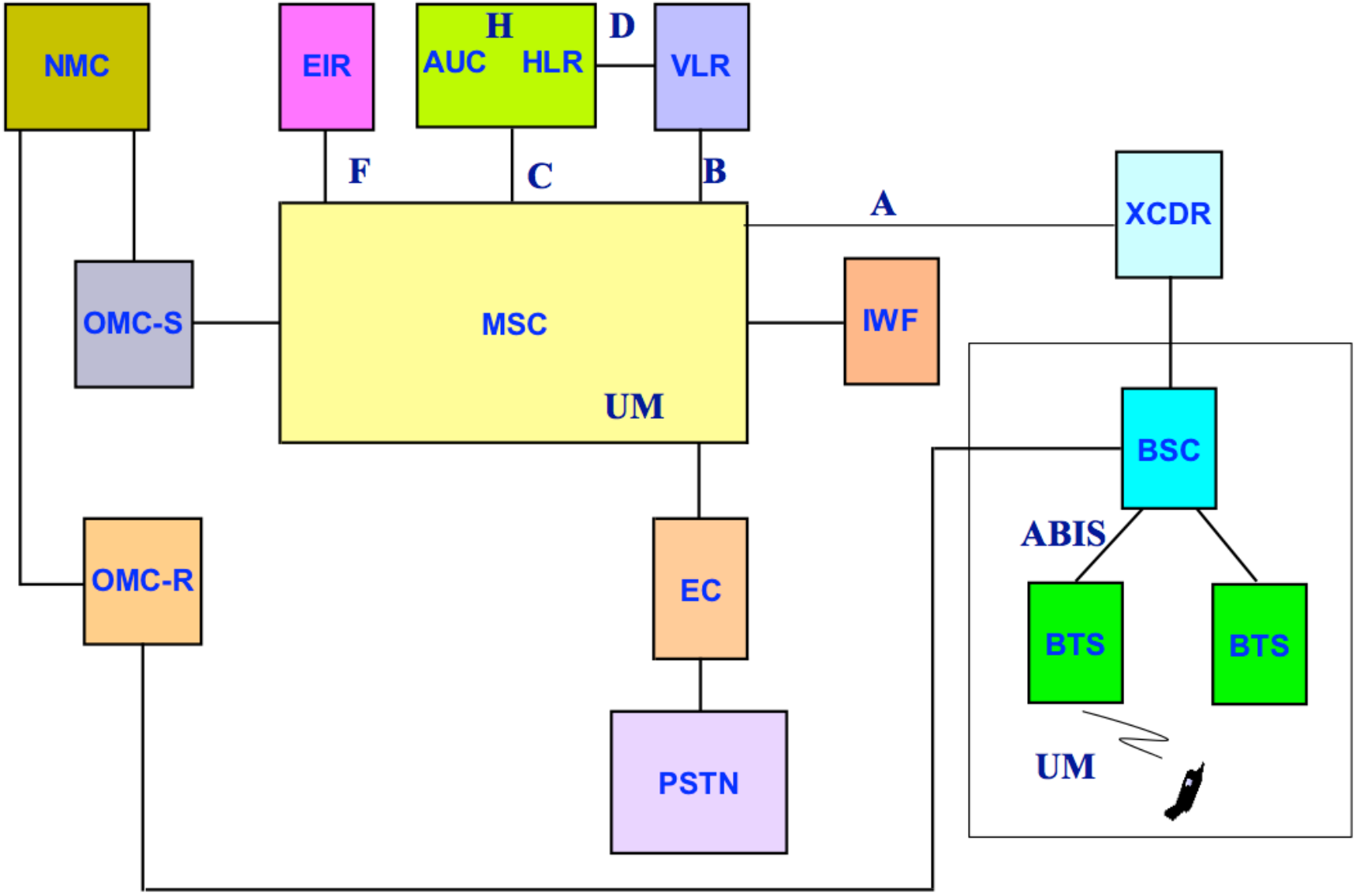
Frequency Reuse

- There are total 124 carriers in GSM
- Each carrier has 8 timeslots (TSs) and if 7 can be used for traffic then a maximum of 868 (124 X 7) calls can be made (note: TS 0 = BCCH)
  - ✓ this is not enough and hence frequencies have to be reused
  - ✓ the same RF carrier can be used for many conversations in several different cells at the same time
- The radio carriers available are allocated according to a regular pattern which repeats over the whole coverage area
  - ✓ the pattern to be used depends on traffic requirement and spectrum availability



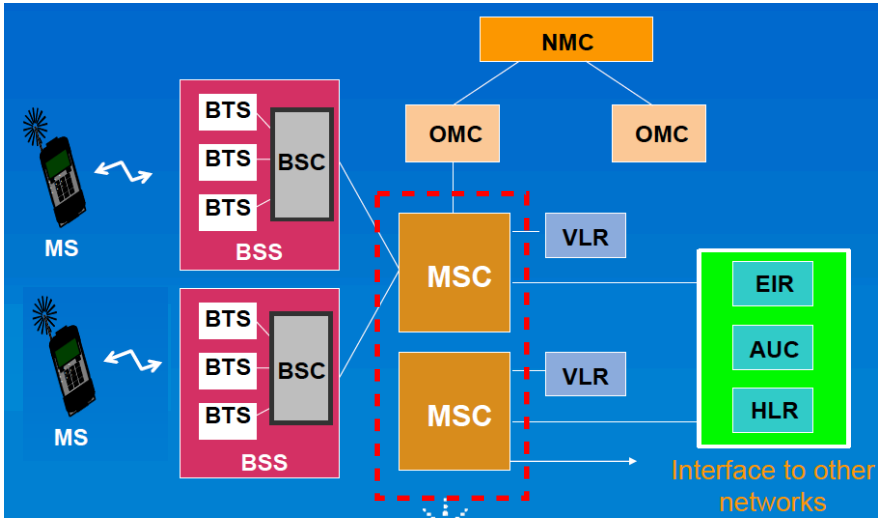
- 1. Introduction
- 2. Features of GSM
- 3. Network Components
- 4. Channel Concept
- 5. Coding, Interleaving, Ciphering
- 6. Signaling
- 7. Handover
- 8. Location Update

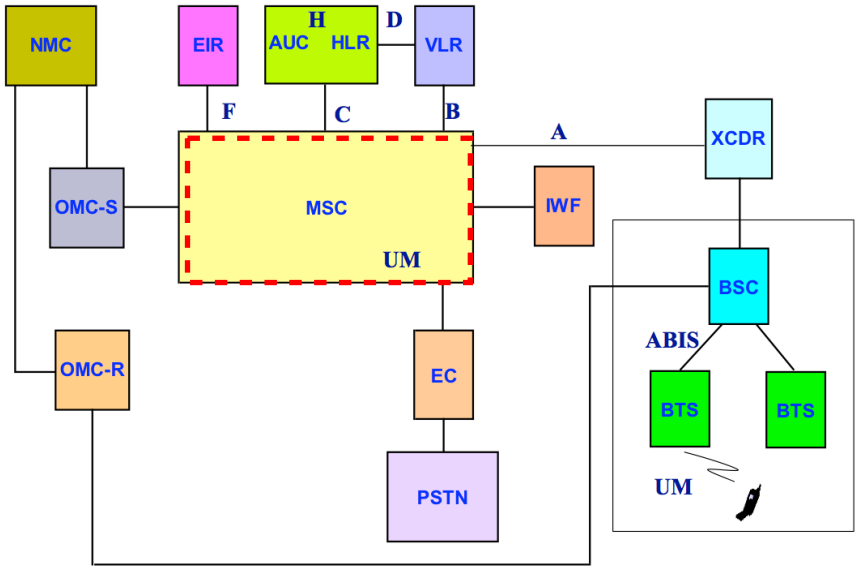
3. Network Components



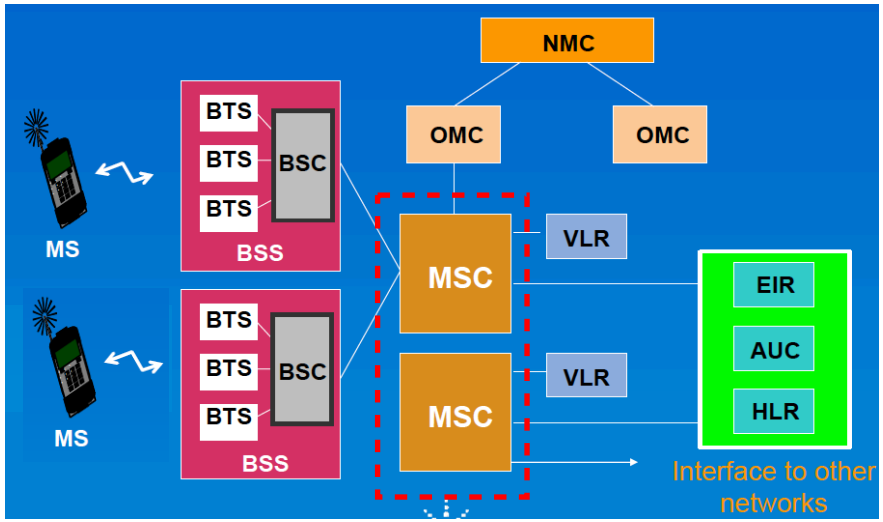
Mobile Switching Center (MSC)

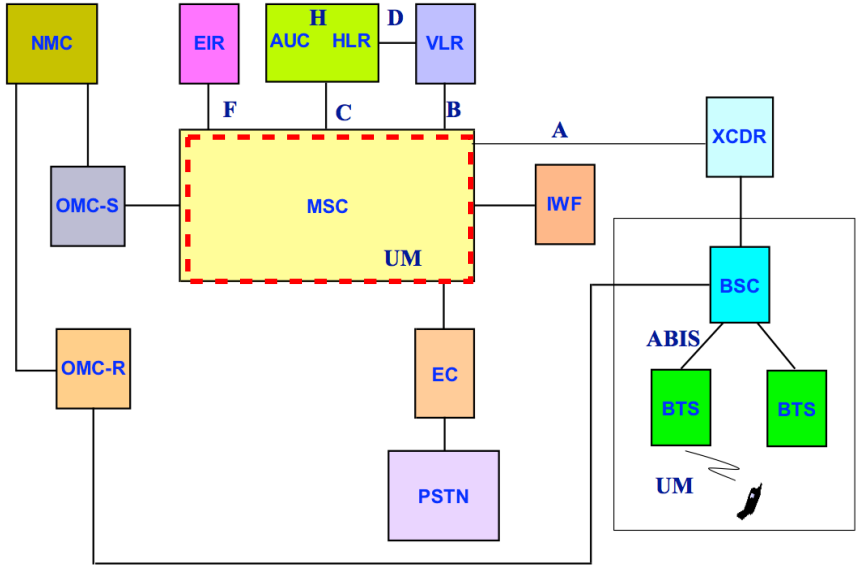
- MSC co-ordinates the setting up of calls to and from GSM users
- MSC is the telephone switching office for MS originated or terminated traffic
- MSC provides the appropriate services
  - ✓ bearer services
  - ✓ teleservices
  - ✓ supplementary services

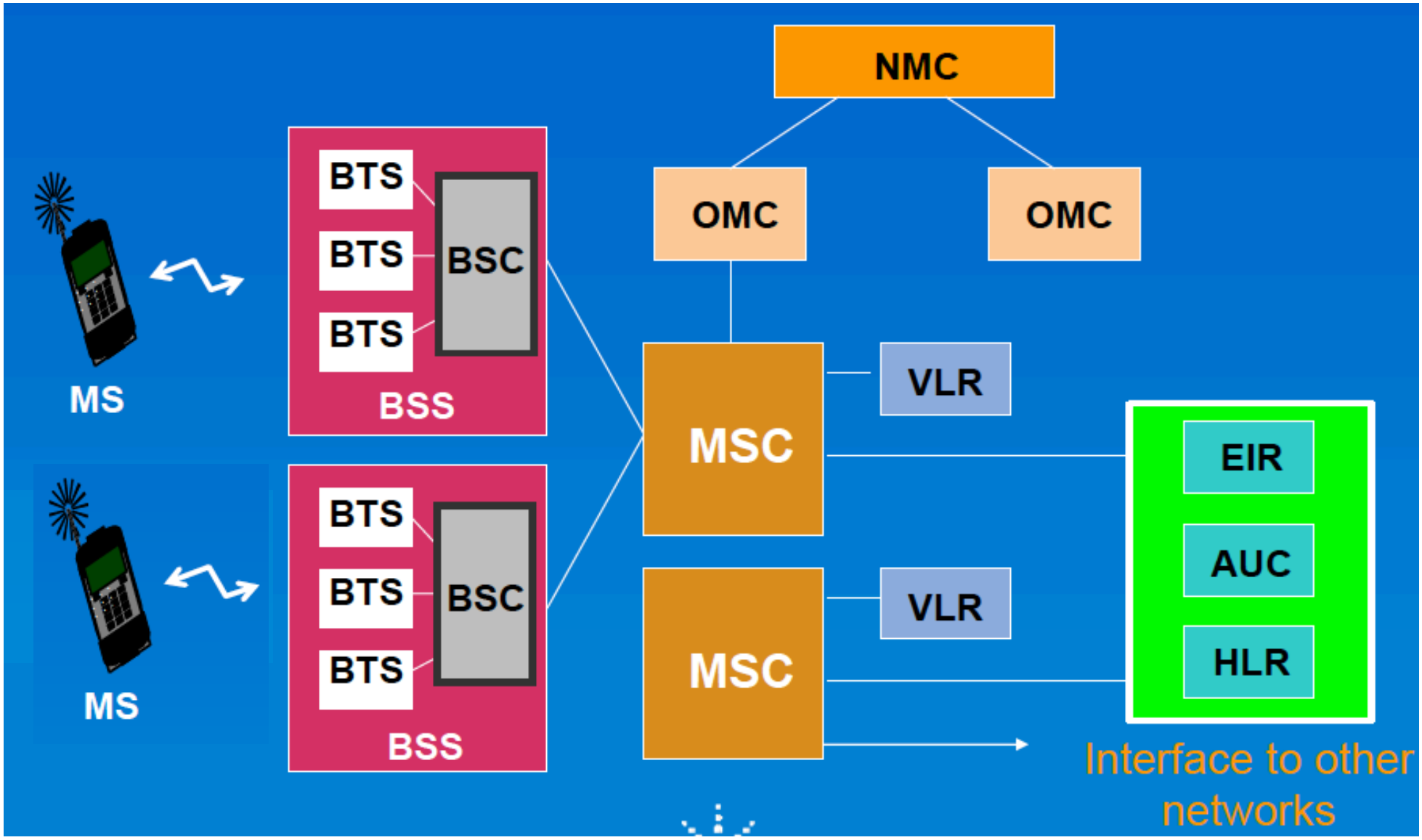




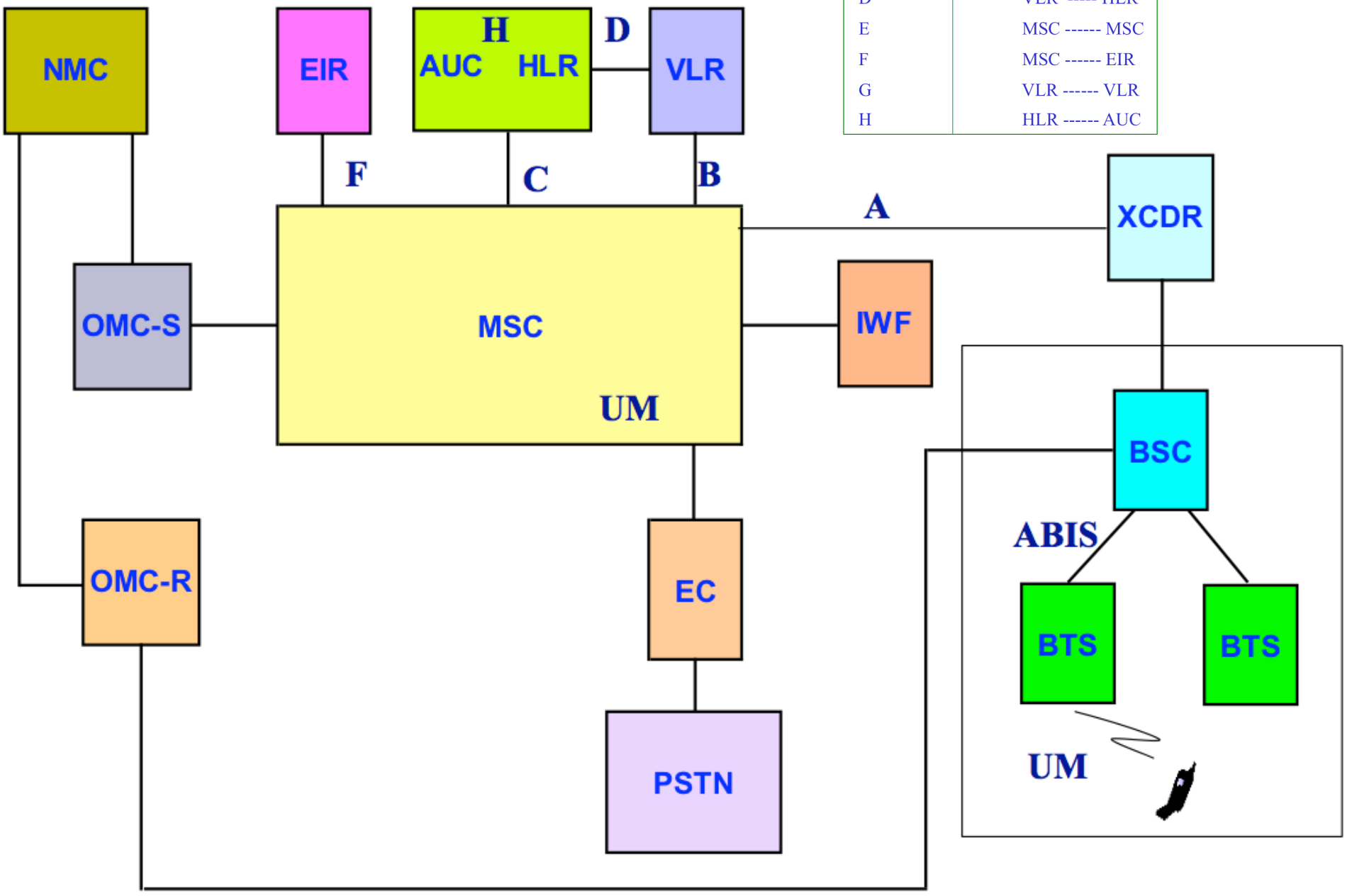
- MSC
  - controls a number of Base Station Sub-systems (BSSs) within a specified geographical coverage area
  - gives the radio subsystem access to the subscriber and equipment databases
- When the MSC provides the interface between PSTN and BSS in the GSM network it is called the *Gateway MSC*






NMC
OMC
OMC
BTS
BTS
BTS
BSC
BSS
MS
MSC
VLR
EIR
AUC
HLR
MS
BTS
BTS
BTS
BSC
BSS
MSC
VLR
Interface to other networks

Name	Interface
Um	MS ----- BTS
Abis	BTS ----- BSC
A	MSC ------ BSC
B	MSC ------ VLR
C	MSC ------ HLR
D	VLR ----- HLR
E	MSC ------ MSC
F	MSC ------ EIR
G	VLR ------ VLR
H	HLR ------ AUC

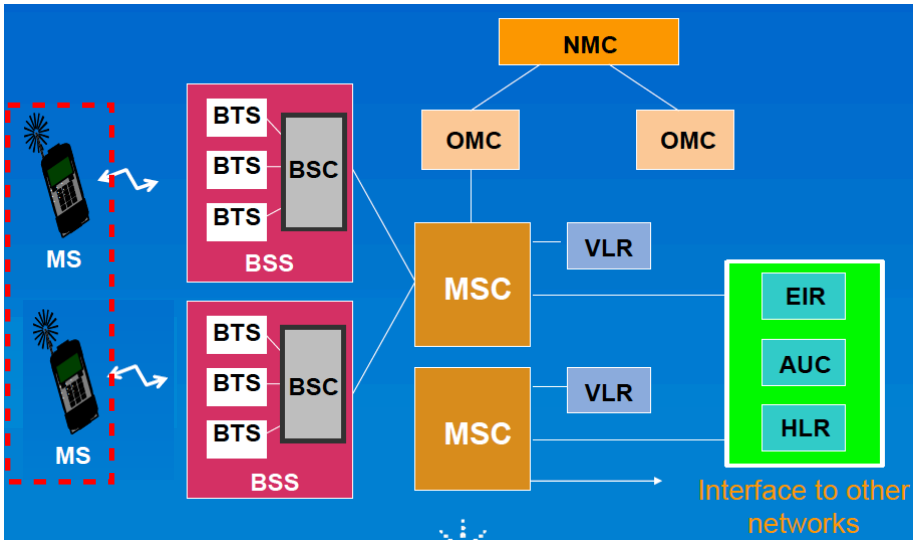


- Some important functions carried out by MSC
  - ✓ call processing
    - control of data/voice call setup
    - inter BSS & inter MSC handovers
    - control of mobility management
  - ✓ operation & maintenance support
    - database management
    - traffic metering
    - managing the interface between GSM & PSTN network

Lucent MSC

Mobile Station (MS)

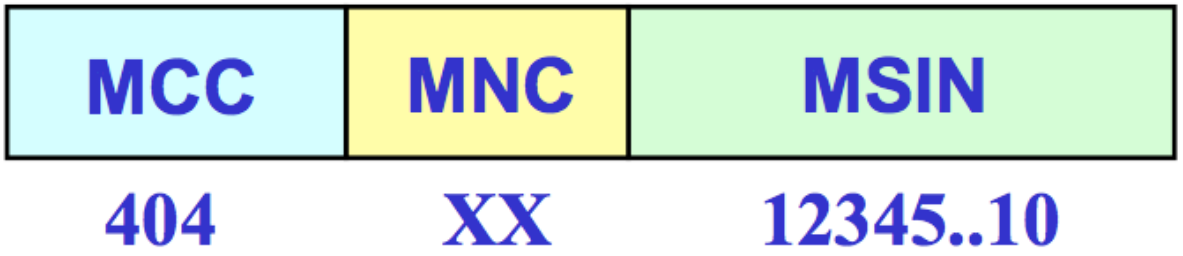
- Mobile Station
  - ✓ Mobile Equipment (ME)
  - ✓ Subscriber Identity Module (SIM)
- Mobile Equipment (ME)
  - ✓ the hardware used by the subscriber to access the network
  - ✓ can be vehicle mounted, with the antenna physically mounted on the outside of the vehicle, or portable mobile unit, which can be handheld



- Subscriber Identity Module (SIM)
  - ✓ identifies the mobile subscriber and provides information about the service that the subscriber should receive
  - ✓ contains several pieces of information
    - International Mobile Subscribers Identity (IMSI)
      - identifies the mobile subscriber
      - only transmitted over the air during initializing
    - Temporary Mobile Subscriber Identity (TMSI)
      - also identifies the subscriber
      - periodically changed by the system to protect the subscriber from being identified by someone attempting to monitor the radio interface

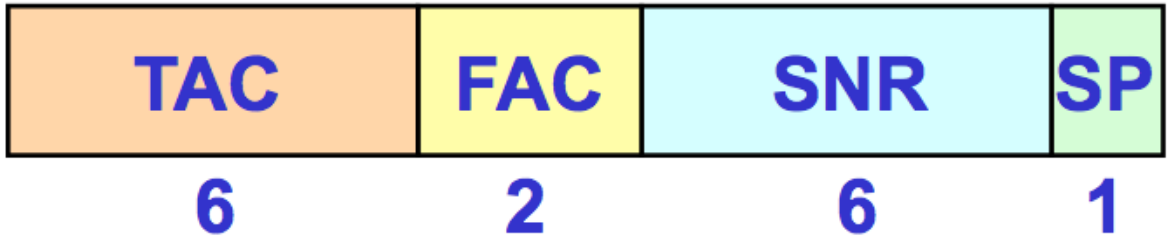
- Location Area Identity (LAI)
  - identifies the current location of the subscriber
- subscribers authentication key (K_i)
  - used to authenticate the SIM card
- Mobile Station International Standard Data Number (MSISDN)
  - the telephone number of the mobile

IMSI



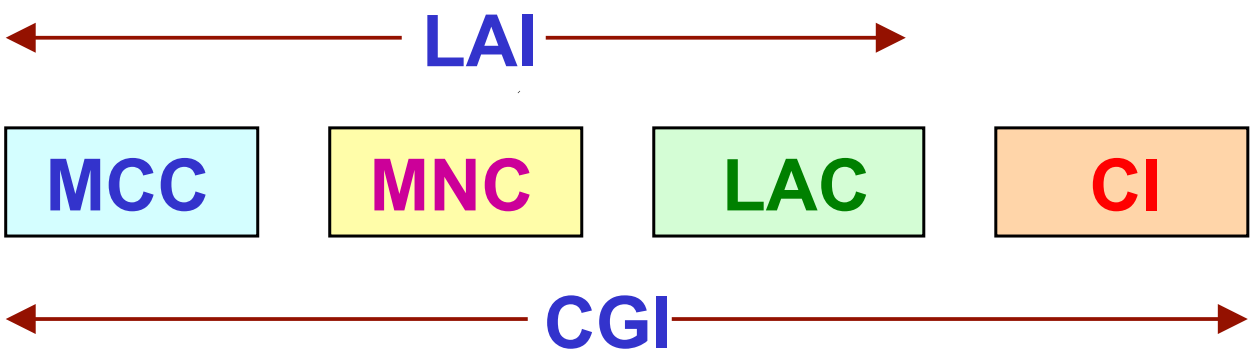
MCC = Mobile Country Code (3 Digits)
MNC = Mobile Network Code (2 Digits)
MSIN = Mobile Subscriber Identity Number

IMEI



TAC = Type Approval Code
FAC = Final Assembly Code
SNR = Serial Number
SP = Spare

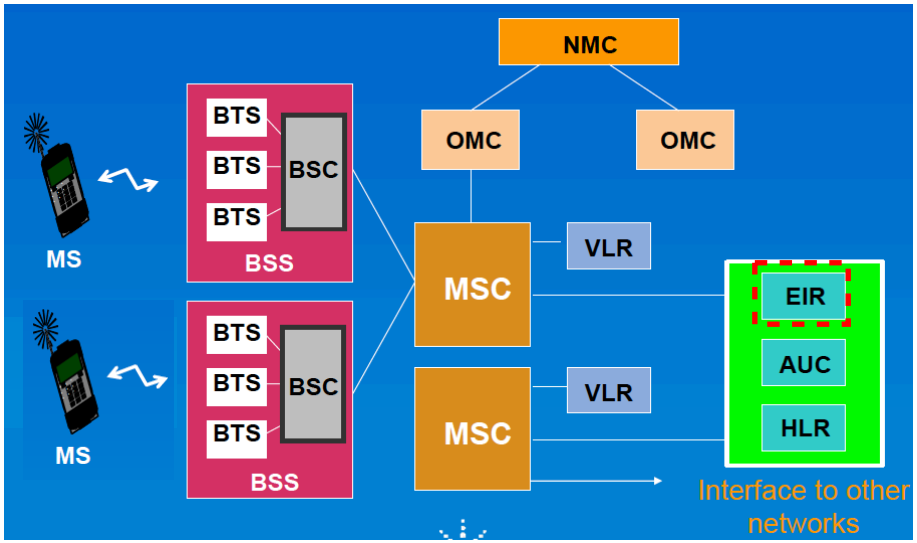
Cell Global Identity (CGI)



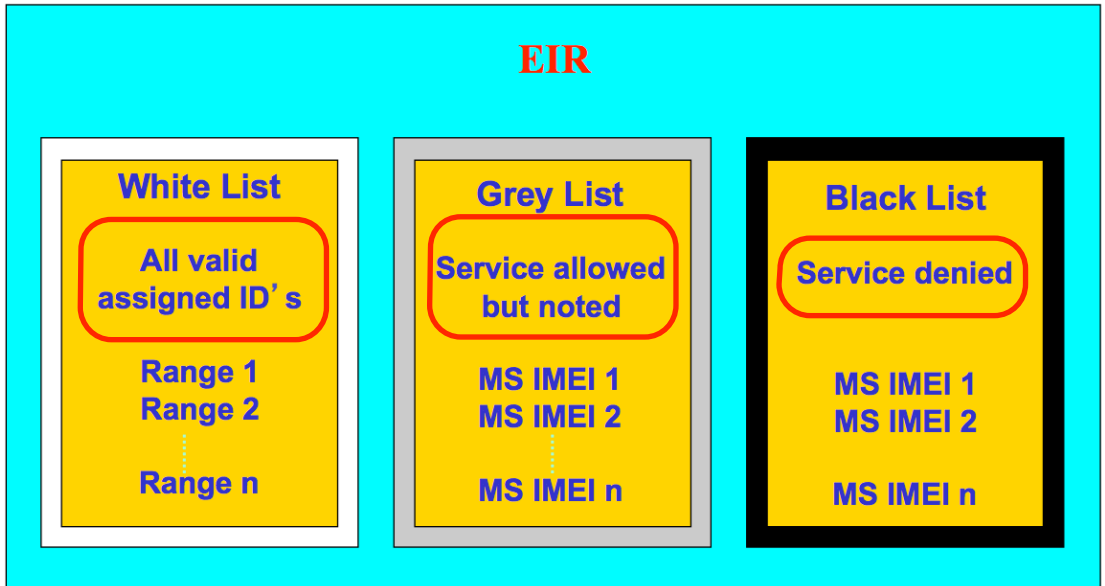
MCC = Mobile Country Code
MNC = Mobile Network Code
LAC = Location Area Identity
CI = Cell Identity

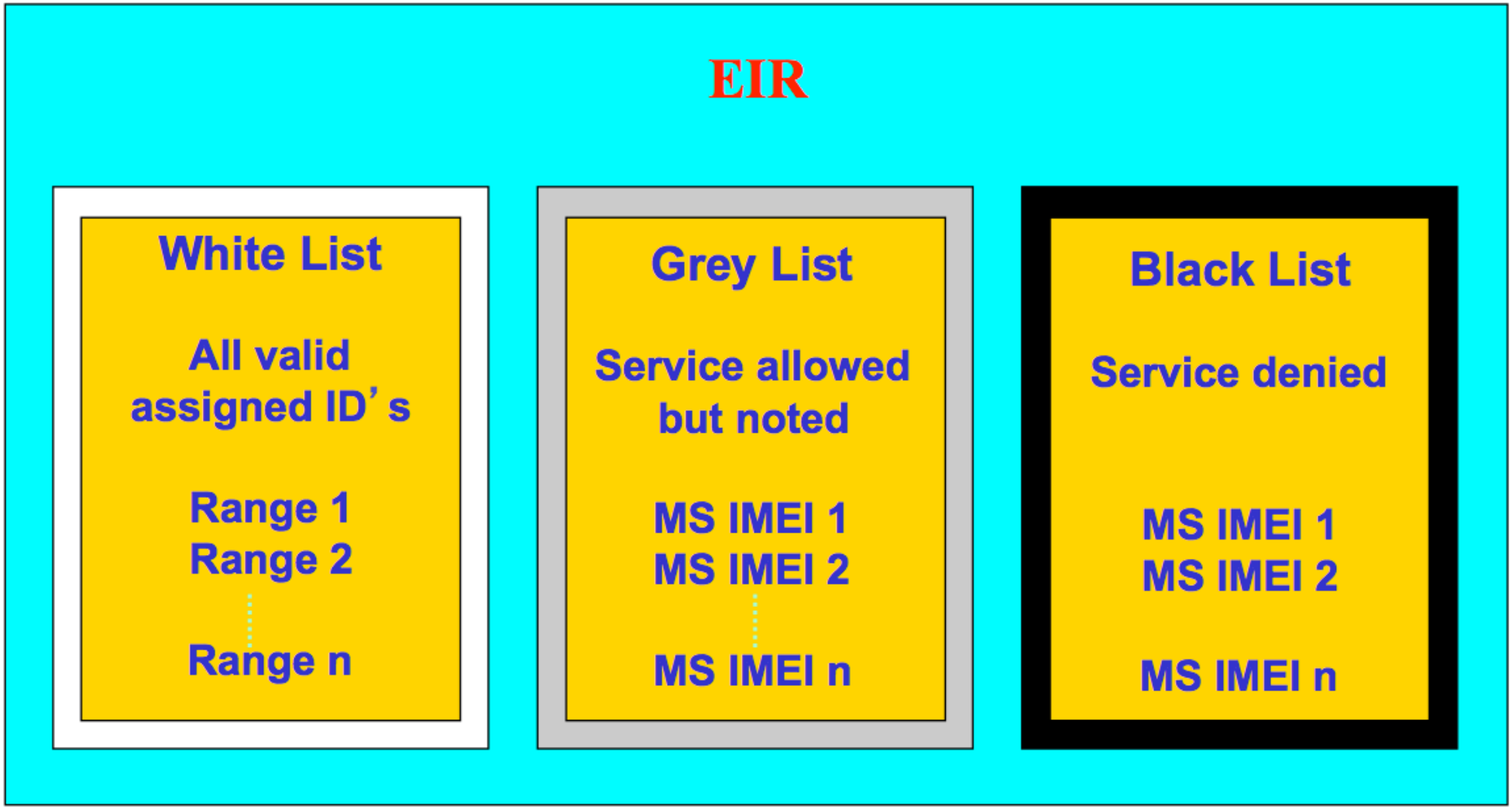
Equipment Identity Register (EIR)

- Contains a centralized database for validating the International Mobile station Equipment Identity (IMEI)
- The EIR database is remotely accessed by the MSC's in the network and can also be accessed by an MSC in a different PLMN



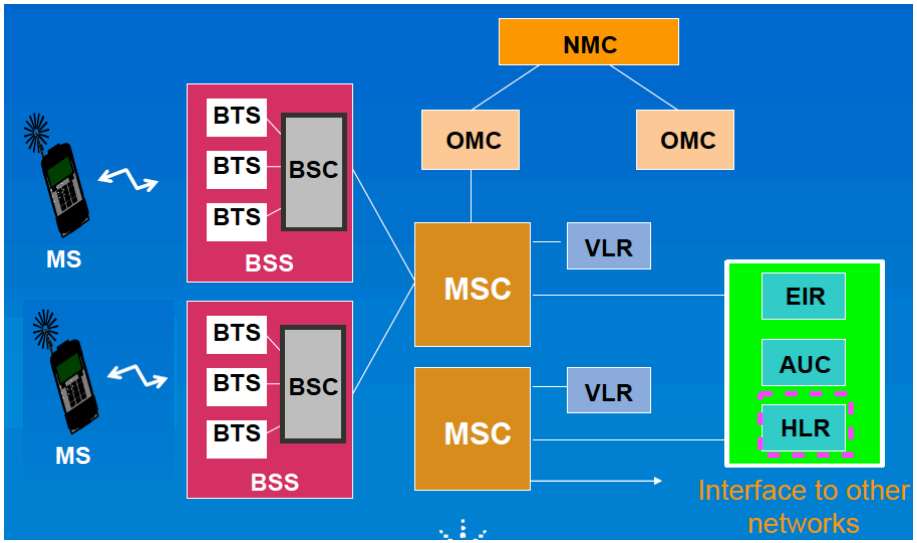
- EIR database contains three lists
  - ✓ White list
    - contains the number series of equipment identities that have been allocated in the different participating countries
    - this list does not contain individual numbers but a range of numbers by identifying the beginning and end of the series
  - ✓ Grey list
    - contains IMEIs of equipment to be monitored and observed for location and correct function
  - ✓ Black list
    - contains IMEIs of MSs which have been reported stolen or are to be denied service




EIR
White List
All valid assigned ID's
Range 1
Range 2
Range n
Grey List
Service allowed but noted
MS IMEI 1
MS IMEI 2
MS IMEI n
Black List
Service denied
MS IMEI 1
MS IMEI 2
MS IMEI n

Home Location Register (HLR)

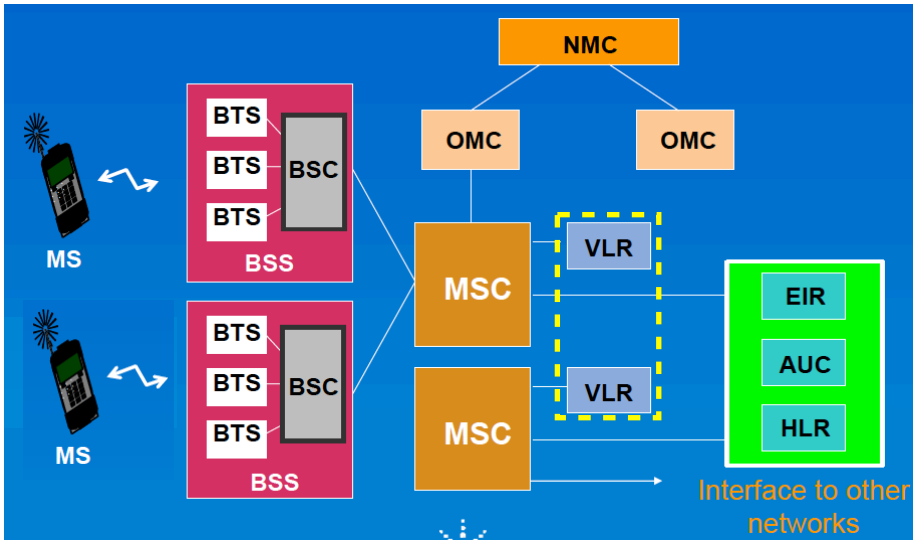
- Contains the master database of all subscribers in the PLMN
- This data is remotely accessed by the MSCs and VLRs in the network
- The data can also be accessed by an MSC or a VLR in a different PLMN to allow inter-system and inter-country roaming
- A PLMN may contain more than one HLR, in which case each HLR contains a portion of the total subscriber database
- The subscribers data may be accessed by IMSI or MSISDN



- The parameters stored in HLR
  - ✓ subscribers ID (IMSI and MSISDN)
  - ✓ current subscriber VLR
  - ✓ supplementary services subscribed to
  - ✓ supplementary services information (eg. current forwarding address)
  - ✓ authentication key and AUC functionality
  - ✓ TMSI and MSRN

Visitor Location Register (VLR)

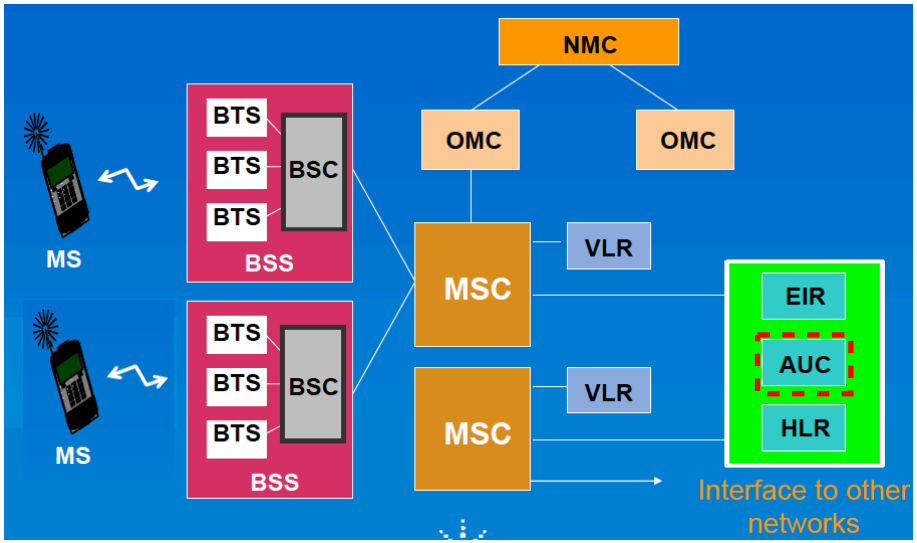
- A local subscriber database, holding details on those subscribers who enter the area of the network that it covers
- The details are held in the VLR until the subscriber moves into the area serviced by another VLR
- The data includes most of the information stored at the HLR, as well as more precise location and status information



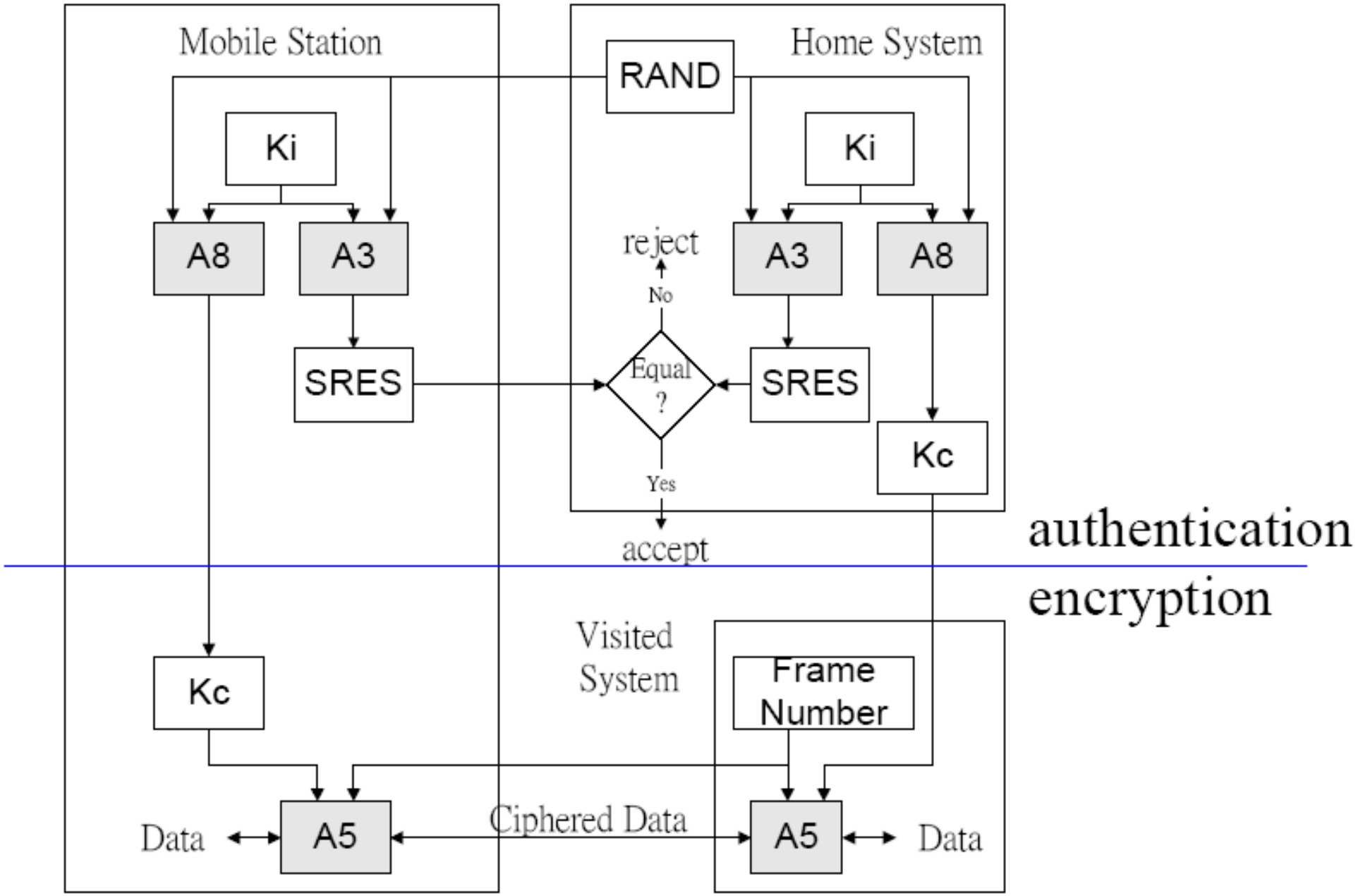
- The additional data stored in VLR
  - ✓ mobile status (Busy / Free / No answer etc.)
  - ✓ Location Area Identity (LAI)
  - ✓ Temporary Mobile Subscribers Identity (TMSI)
  - ✓ Mobile Station Roaming Number (MSRN)

Authentication Centre (AUC)

- A processor system that performs authentication function
- Normally co-located with the HLR
- The authentication process usually takes place each time the subscriber initializes on the system
- Each subscriber is assigned an authentication key (K_i) which is stored in the SIM and at the AUC



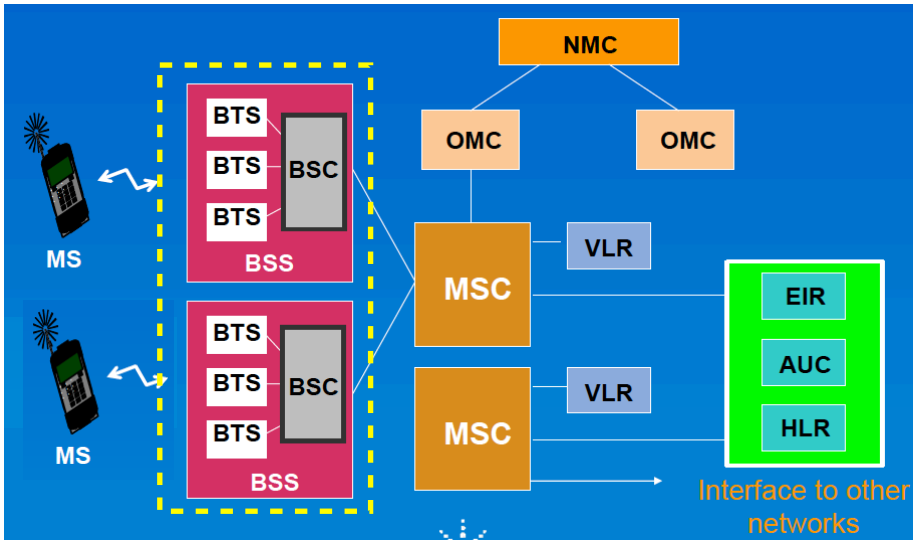
- A random number of 128 bits is generated by the AUC & sent to the MS
  - ✓ MS side
    - the authentication algorithm *A3* uses this random number and authentication key K_i to produce a signed response SRES (Signed Response)
  - ✓ AUC side
    - at the same time the AUC uses the random number and authentication algorithm A3 along with the K_i key to produce a SRES
  - ✓ if the SRES produced by AUC matches the one produced by MS is the same, the subscriber is permitted to use the network



Authentication & Encryption Process

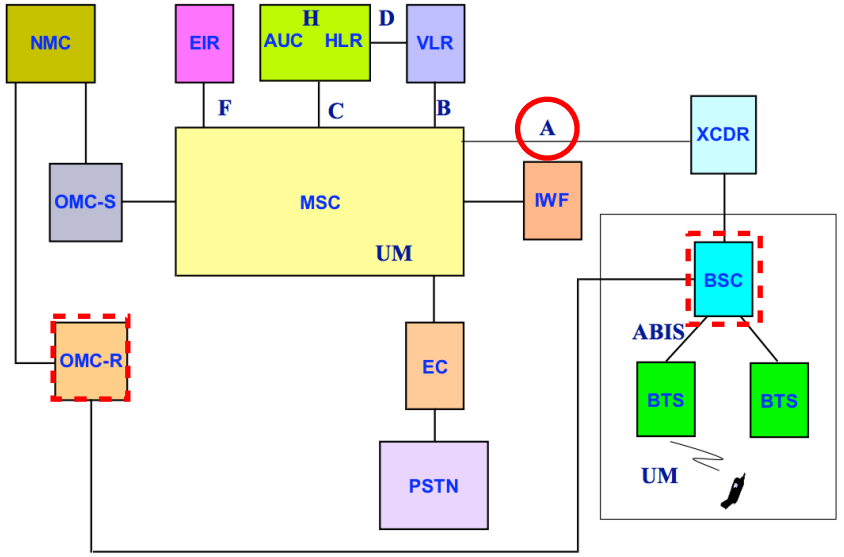
Base Station Sub-System (BSS)

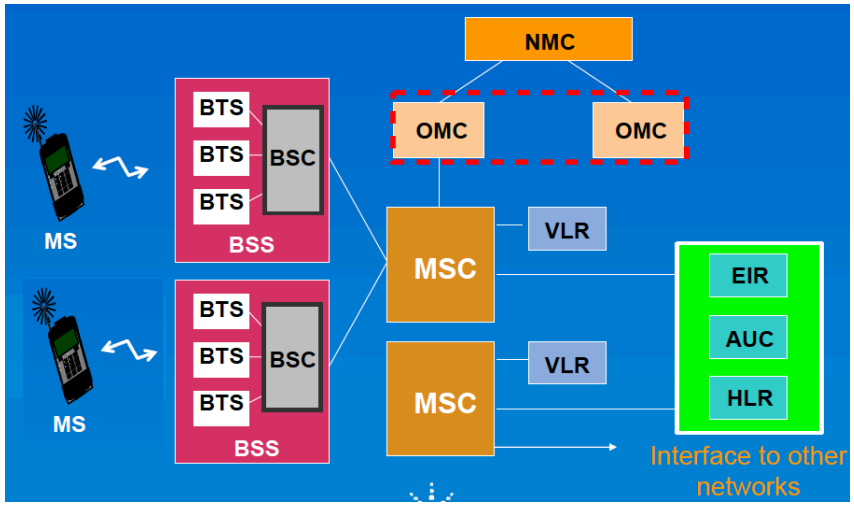
- The fixed end of the radio interface that provides control and radio coverage functions for one or more cells and their associated MSs
- The interface between MS and MSC
- BSS comprises
  - ✓ one or more Base Transceiver Stations (BTSs), each containing the radio components that communicate with MSs in a given area
  - ✓ one Base Site Controller (BSC) which supports call processing functions and the interfaces to the MSC
- Digital radio techniques are used for the radio communications link, known as Air Interface, between the BSS and the MS



Base Station Controller (BSC)

- Provides the control for BSS
- Controls and manages the associated BTSs, and interfaces with Operations and Maintenance Center (OMC)
- The purpose of BSC is to perform a variety of functions
  - ✓ controls the BTS components
  - ✓ performs call processing
  - ✓ performs Operations and Maintenance (O & M)
  - ✓ provides the O & M link (OML) between BSS and OMC
  - ✓ provides A Interface between BSS and MSC
  - ✓ manages the radio channels
  - ✓ transfers signaling information to and from MSs

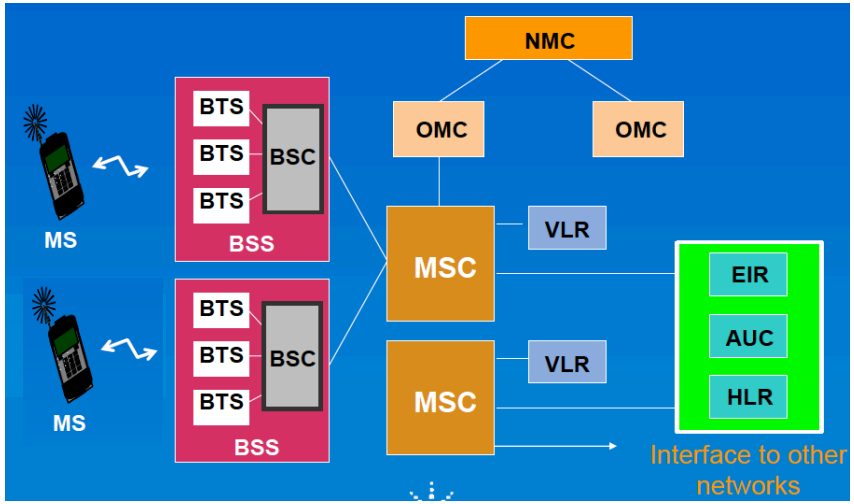




Base Station Controller (BSC) – Siemens BSC

Base Transceiver Station (BTS)

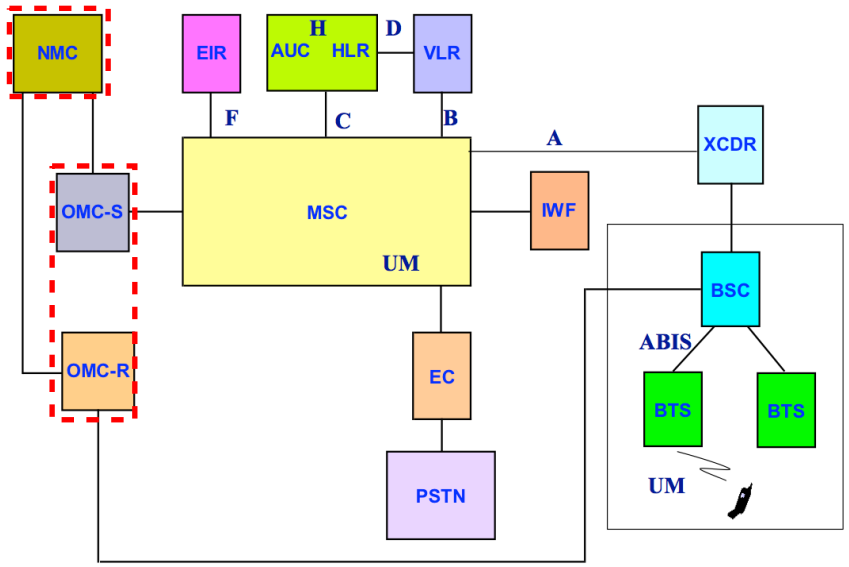
- Consists of the hardware components, such as radios, interface modules and antenna systems that provide the Air Interface between BSS and MSs
- Provides radio channels (RF carriers) between MSs and BSS for a specific RF coverage area
- BTS also has a limited amount of control functionality which reduces the amount of traffic between BTS and BSC

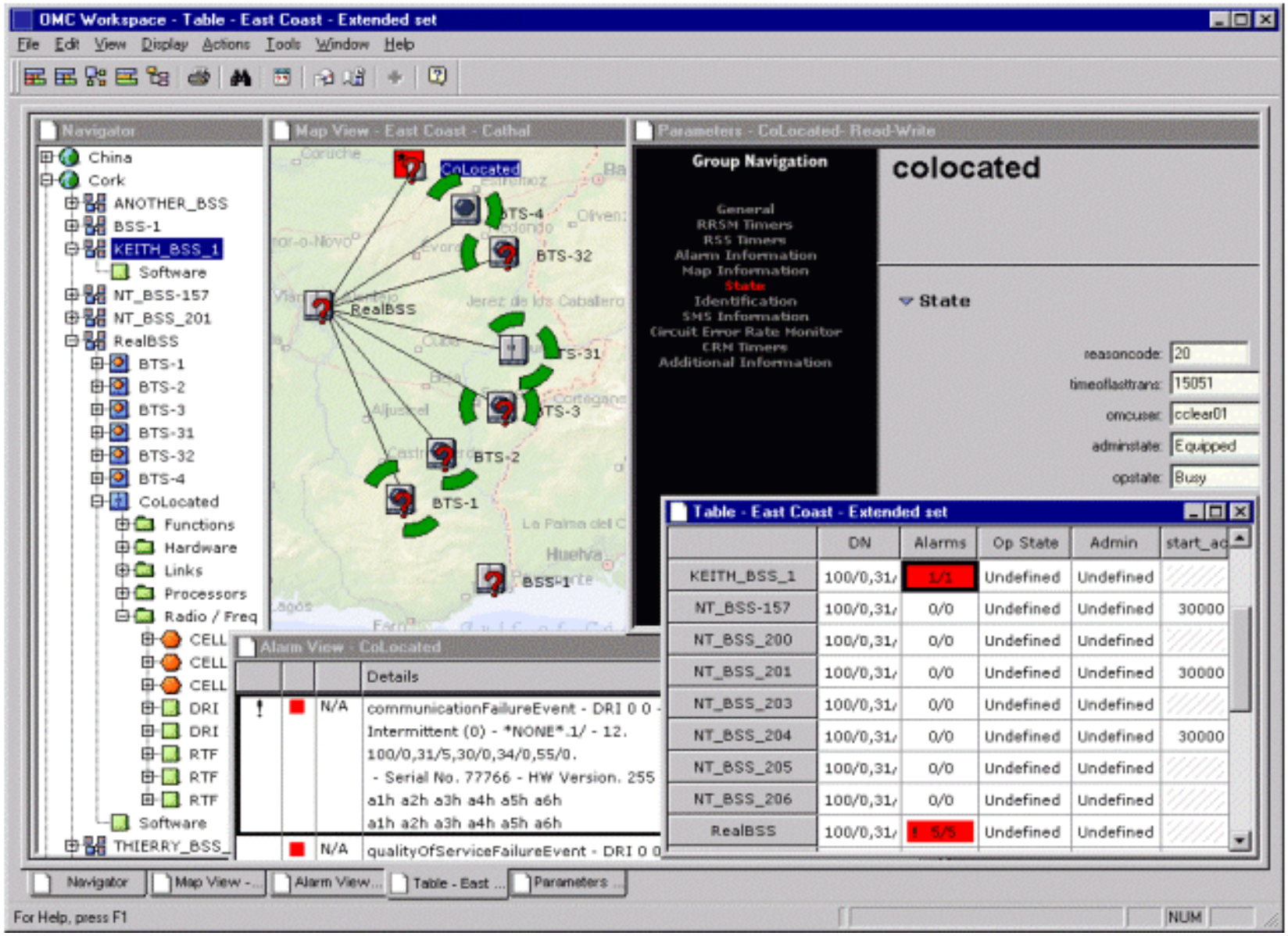


Base Transceiver Station (BTS)

Operation and Maintenance Centre For Radio (OMC-R)

- Controls and monitors the network elements within a region
- Monitors the quality of service being provided by the network
- OMC is used to support NMC (Network Management Center)
- OMC-R main functions
  - ✓ allows network devices to be manually removed for or restored to service. The status of network devices can be checked (tests and diagnostics) from OMC
  - ✓ the alarms generated by the network elements are reported and logged at the OMC
  - ✓ keeps on collecting and accumulating traffic statistics from network elements for analysis
  - ✓ software loads can be downloaded to network elements or uploaded to the OMC



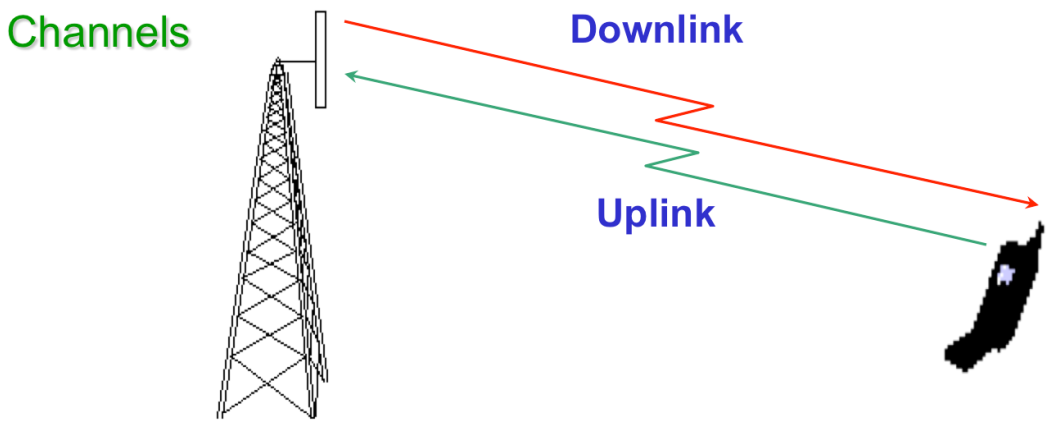


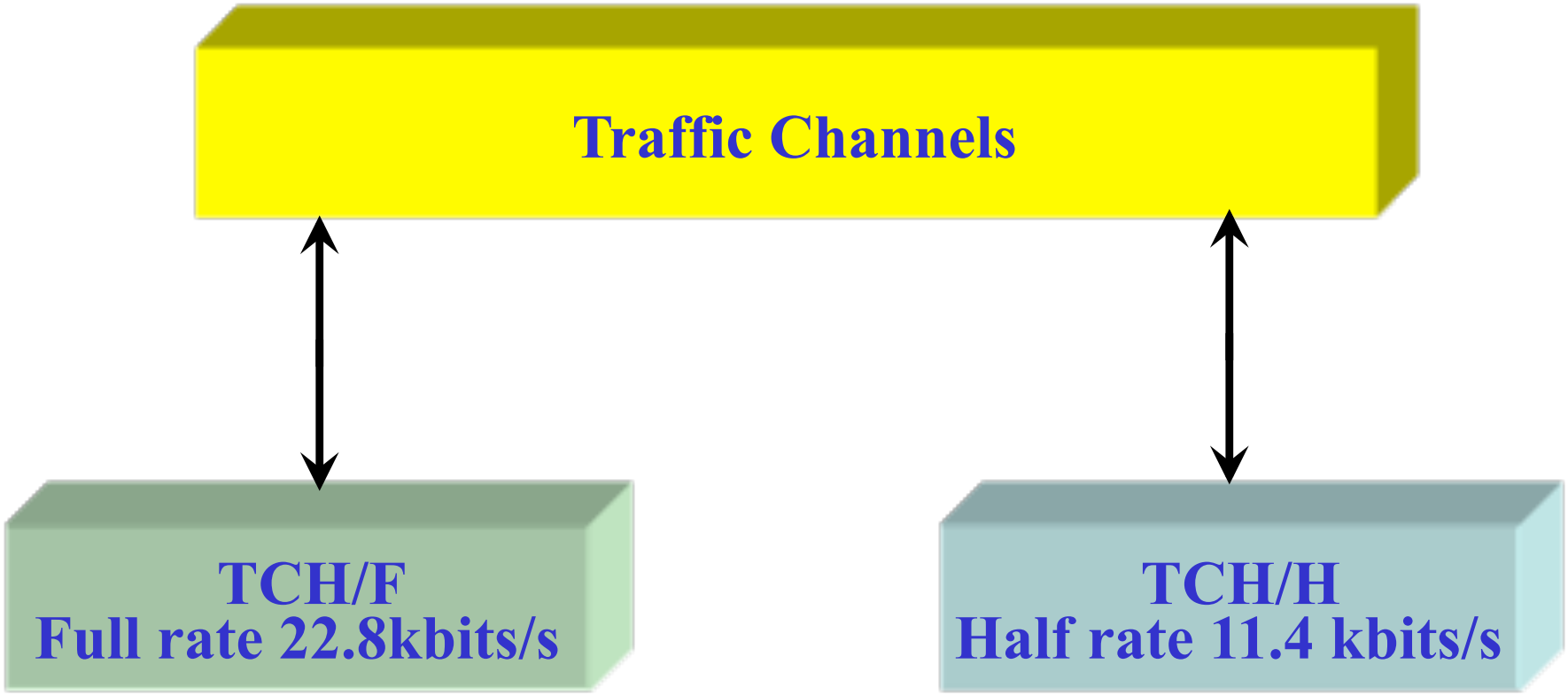
Operation and Maintenance Centre For Radio (OMC-R)

- 1. Introduction
- 2. Features of GSM
- 3. Network Components
- 4. Channel Concept
- 5. Coding, Interleaving, Ciphering
- 6. Signaling
- 7. Handover
- 8. Location Update

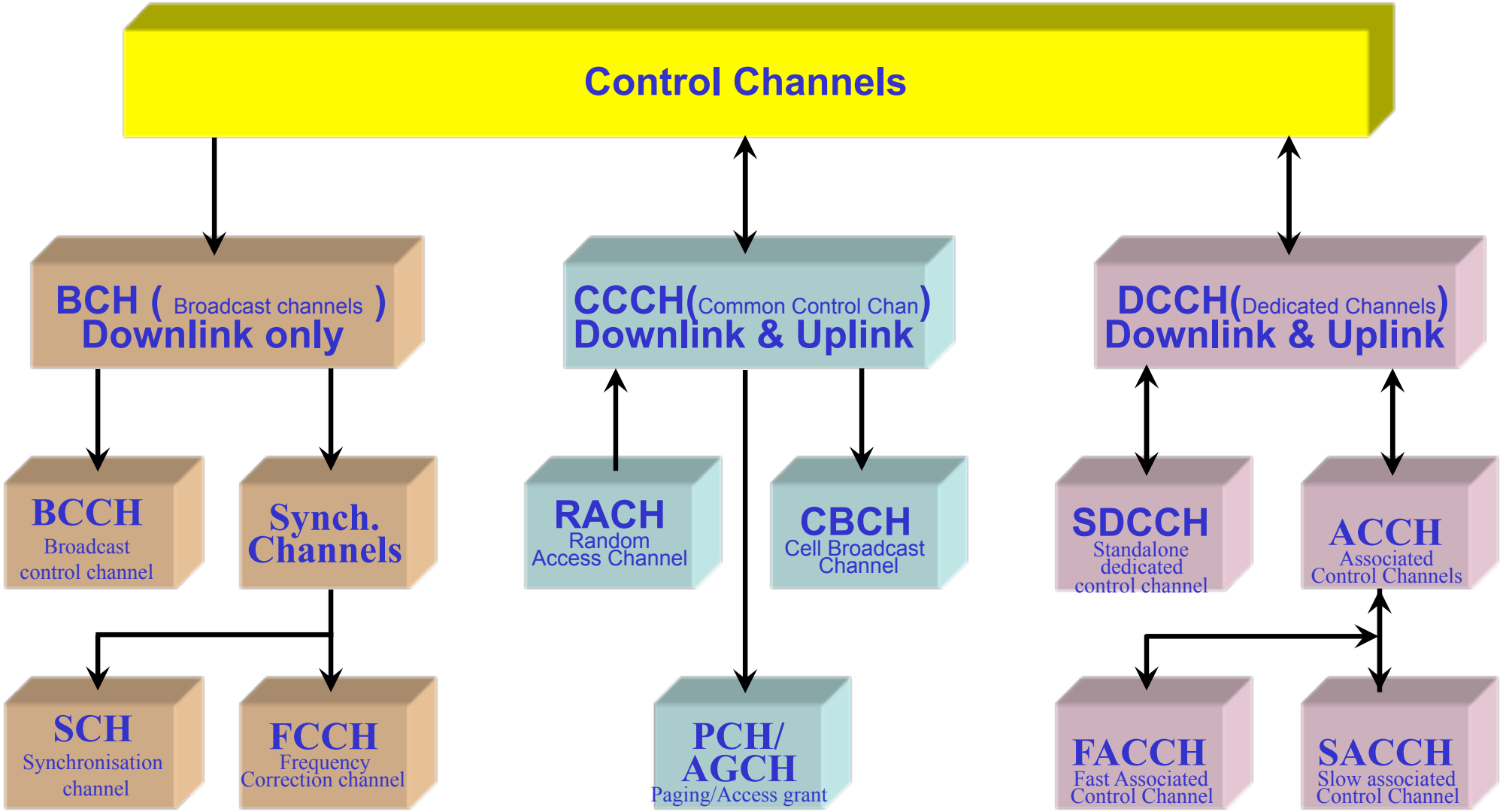
4. Channel Concept

- Physical channel
  - ✓ each timeslot on a carrier is referred to as a physical channel
  - ✓ per carrier there are 8 physical channels
- Logical channel
  - ✓ variety of information is transmitted between MS and BTS
  - ✓ there are different logical channels depending on the information sent
- Logical channels are of two types
  - ✓ traffic channel
  - ✓ control channel





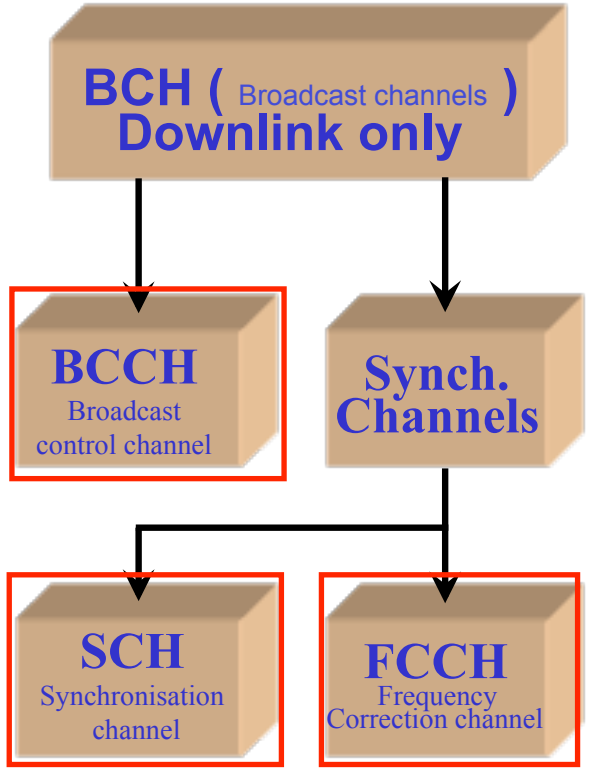
GSM Traffic Channels



GSM Control Channels

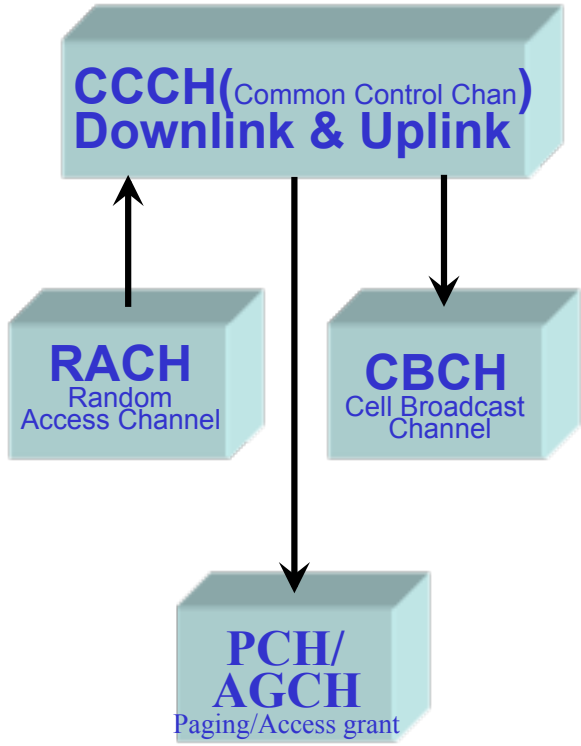
BCH Channels (Broadcast Channels)

- BCCH (Broadcast Control Channel)
  - ✓ downlink only
  - ✓ broadcasts general information of the serving cell called System Information
  - ✓ BCCH is transmitted on timeslot zero (TS 0) of BCCH carrier
  - ✓ read only by idle mobile at least once every 30 secs
- SCH (Synchronization Channel)
  - ✓ downlink only
  - ✓ carries information for frame synchronization
  - ✓ contains TDMA frame number and BSIC (Base Station Identity Code)
- FCCH (Frequency Correction Channel)
  - ✓ downlink only
  - ✓ enables MS to synchronize to the frequency
  - ✓ also helps mobiles of the cells to locate TS 0 of BCCH carrier

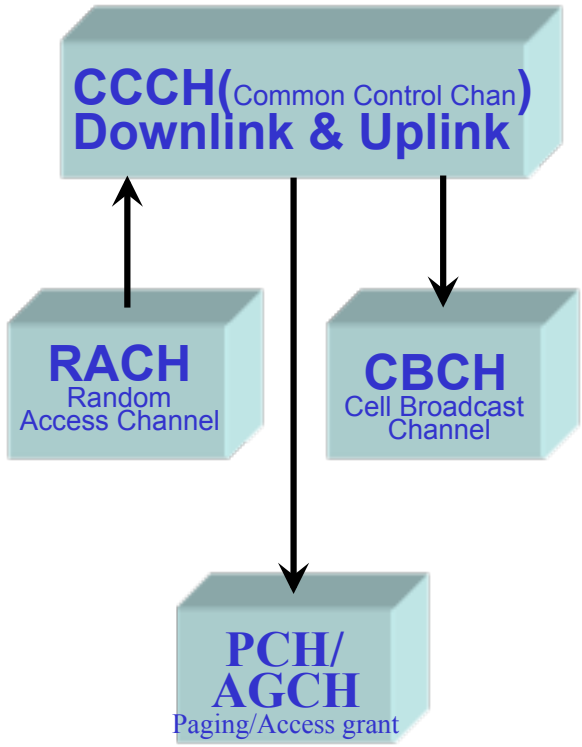


CCCH Channels (Common Control Channels)

- RACH (Random Access Channel)
  - ✓ uplink only
  - ✓ used by MS to access network
- AGCH (Access Grant Channel)
  - ✓ downlink only
  - ✓ used by the network to assign a signaling channel upon successful decoding of access bursts

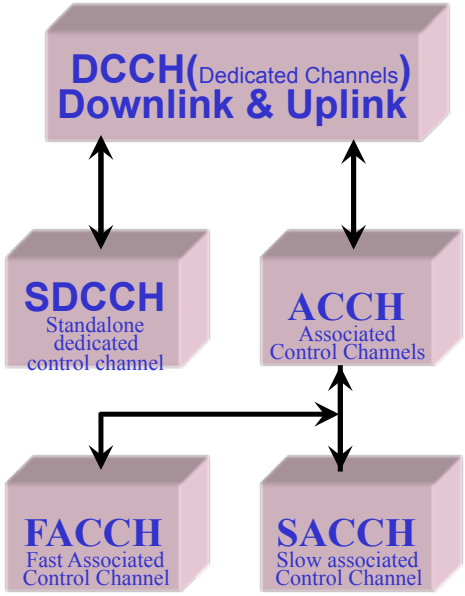


- PCH (Paging Channel)
  - ✓ downlink only
  - ✓ used by network to contact MS
- CBCH (Cell Broadcast Channel)
  - ✓ an optional channel
  - ✓ carries short messages such as traffic and weather announcements



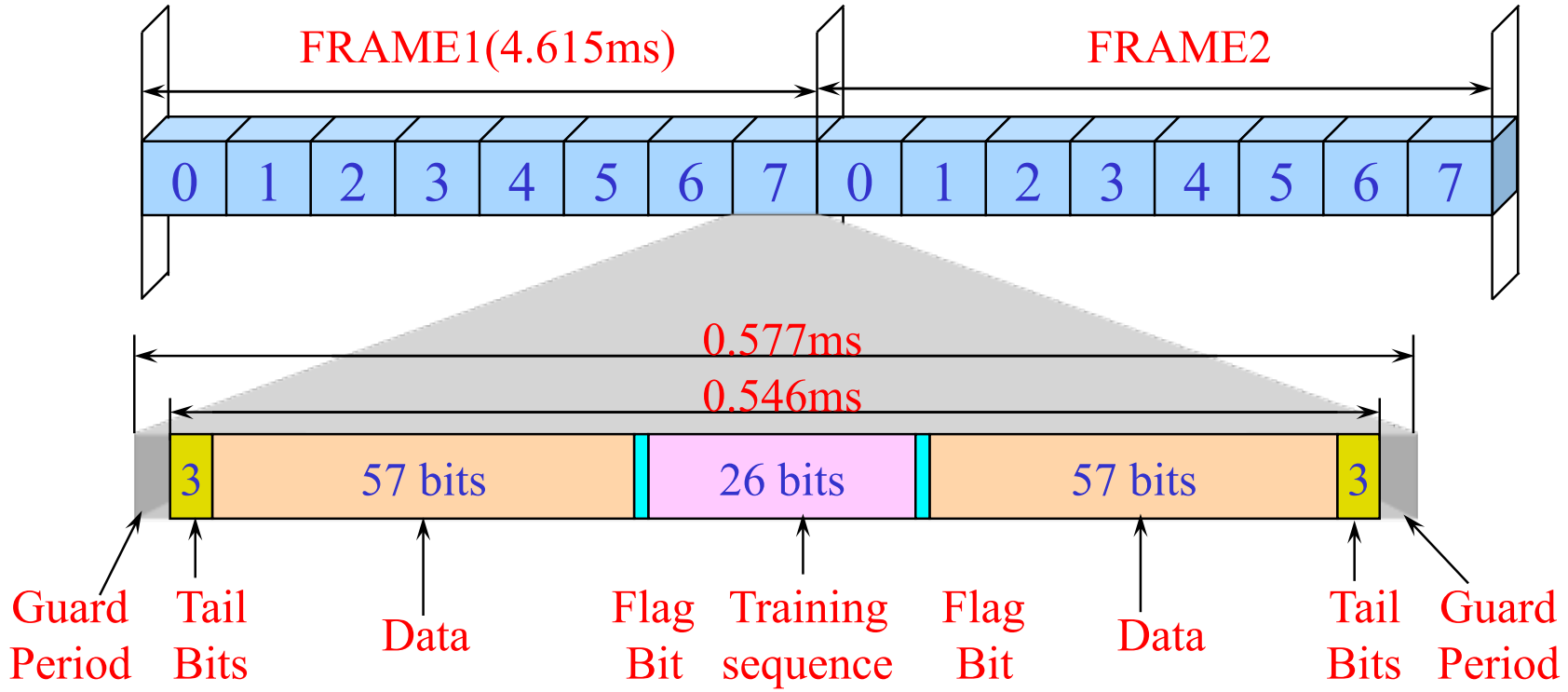
DCCH Channels (Dedicated Channels)

- SDCCH (Standalone Dedicated Control Channel)
  - ✓ uplink and Downlink
  - ✓ used for call setup, location update and SMS
- SACCH (Slow Associated Control Channel)
  - ✓ used on Uplink and Downlink only in dedicated mode
  - ✓ uplink SACCH messages - measurement reports
  - ✓ downlink SACCH messages - control info.
- FACCH (Fast Associated Control Channel)
  - ✓ uplink and Downlink
  - ✓ associated with TCH only
  - ✓ used to send fast messages like handover messages



- A single time slot transmission is called a radio burst
- Four types of radio bursts are defined
  - ✓ normal burst
  - ✓ frequency correction burst
  - ✓ synchronization burst
  - ✓ access burst

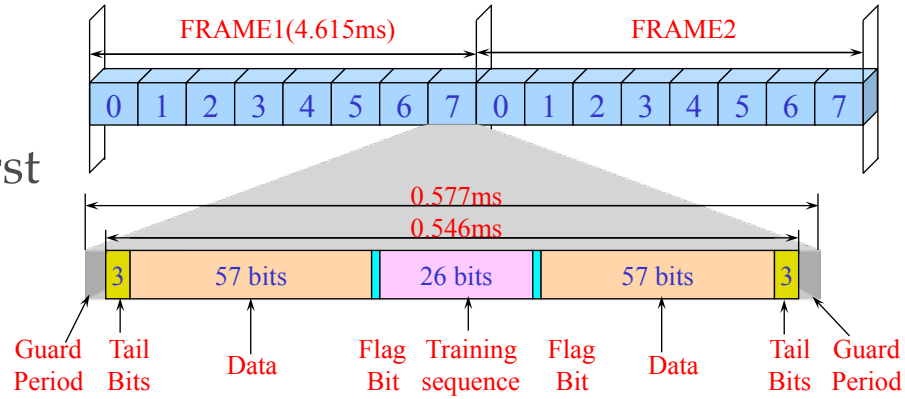
Normal Burst



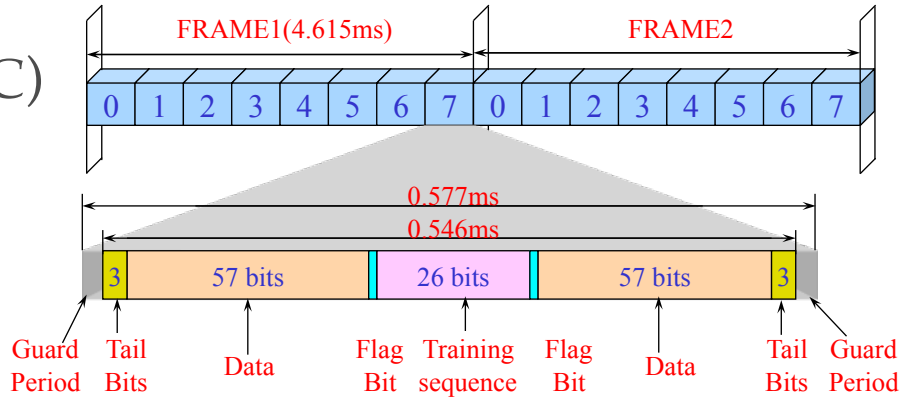
- Carries traffic channel and control channels BCCH, PCH, AGCH, SDCCH, SACCH and FACCH

Normal Burst

- Data
  - ✓ two blocks of 57 bits each
  - ✓ carries speech, data or control info.
- Tail bits
  - ✓ used to indicate the start and end of each burst
  - ✓ three bits always 000
- Guard period
  - ✓ 8.25 bits long
  - ✓ the receiver can only receive and decode if the burst is received within the timeslot designated for it
  - ✓ 8.25 bits corresponding to about 30 *us* is available as guard period for a small margin of error

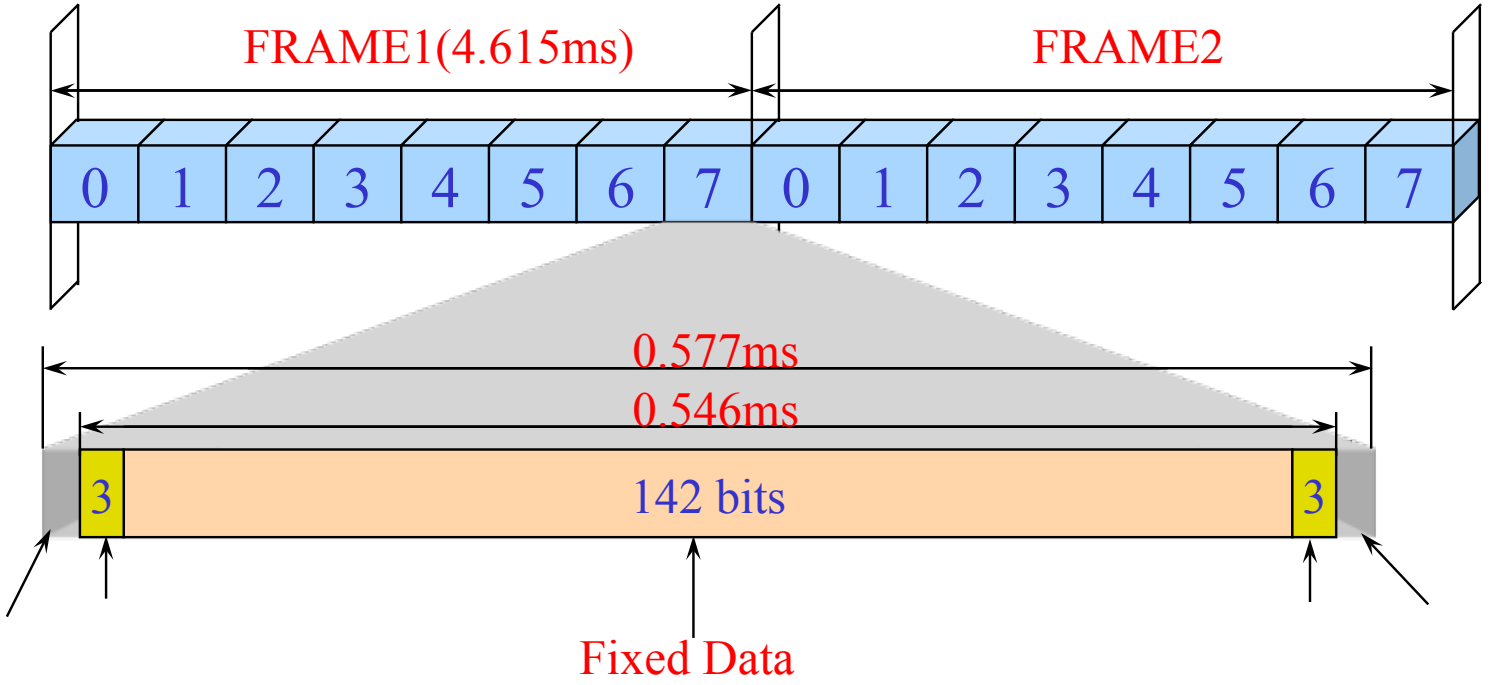


- Flag bits
  - ✓ this bit is used to indicate if the 57 bits data block is used as FACCH (Fast Associated Control Channel)
- Training Sequence
  - ✓ a set sequence of bits known by both the transmitter and the receiver (BCC of BSIC)
  - ✓ when a burst of information is received the equalizer searches for the training sequence code
  - ✓ the receiver measures and then mimics the distortion which the signal has been subjected to [受...影響]
  - ✓ the receiver then compares the received data with the distorted possible transmitted sequence and chooses the most likely one



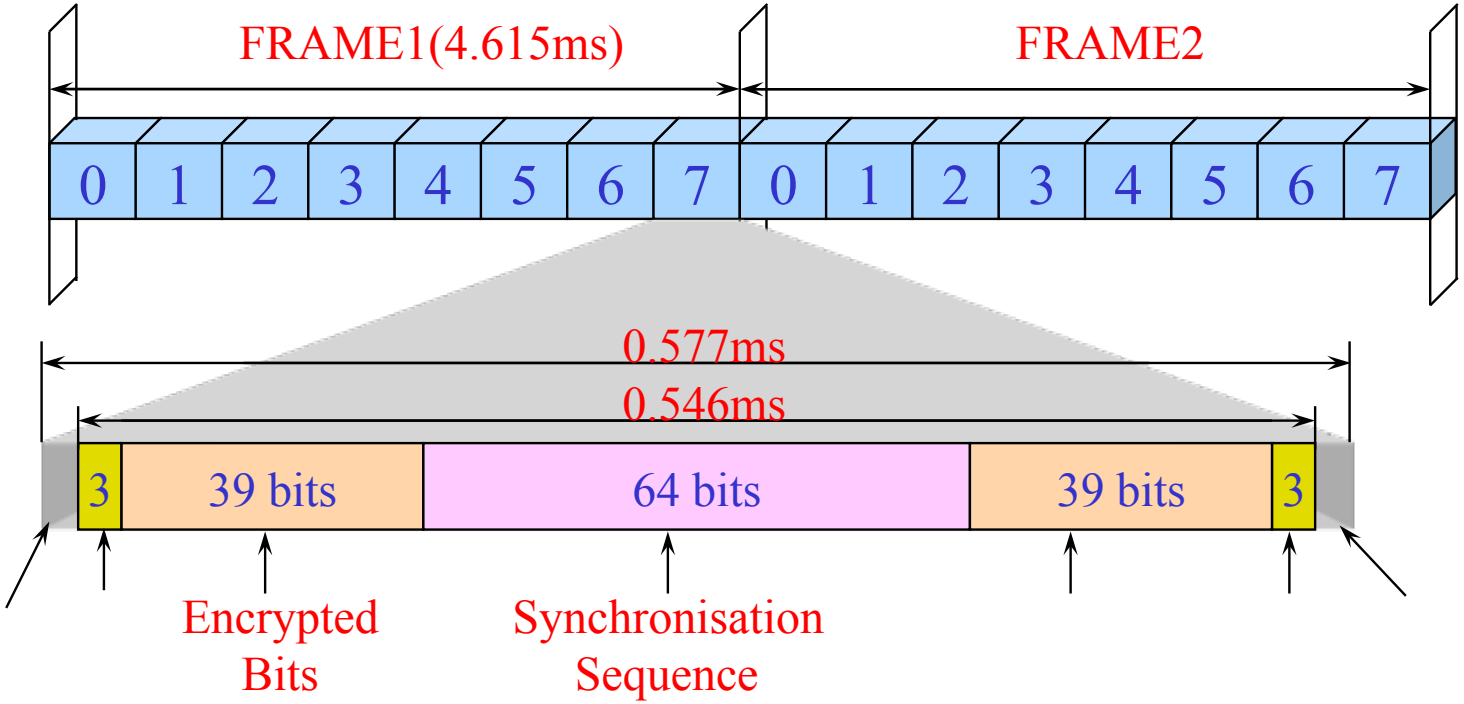
BCC : Base station Color Code
BSIC : Base Station Identity Code

Frequency Correction Burst



- Carries FCCH channel (Frequency Correction Channel)
- Made up of 142 consecutive zeros
- Enables MS to correct its local oscillator locking to that of the BTS

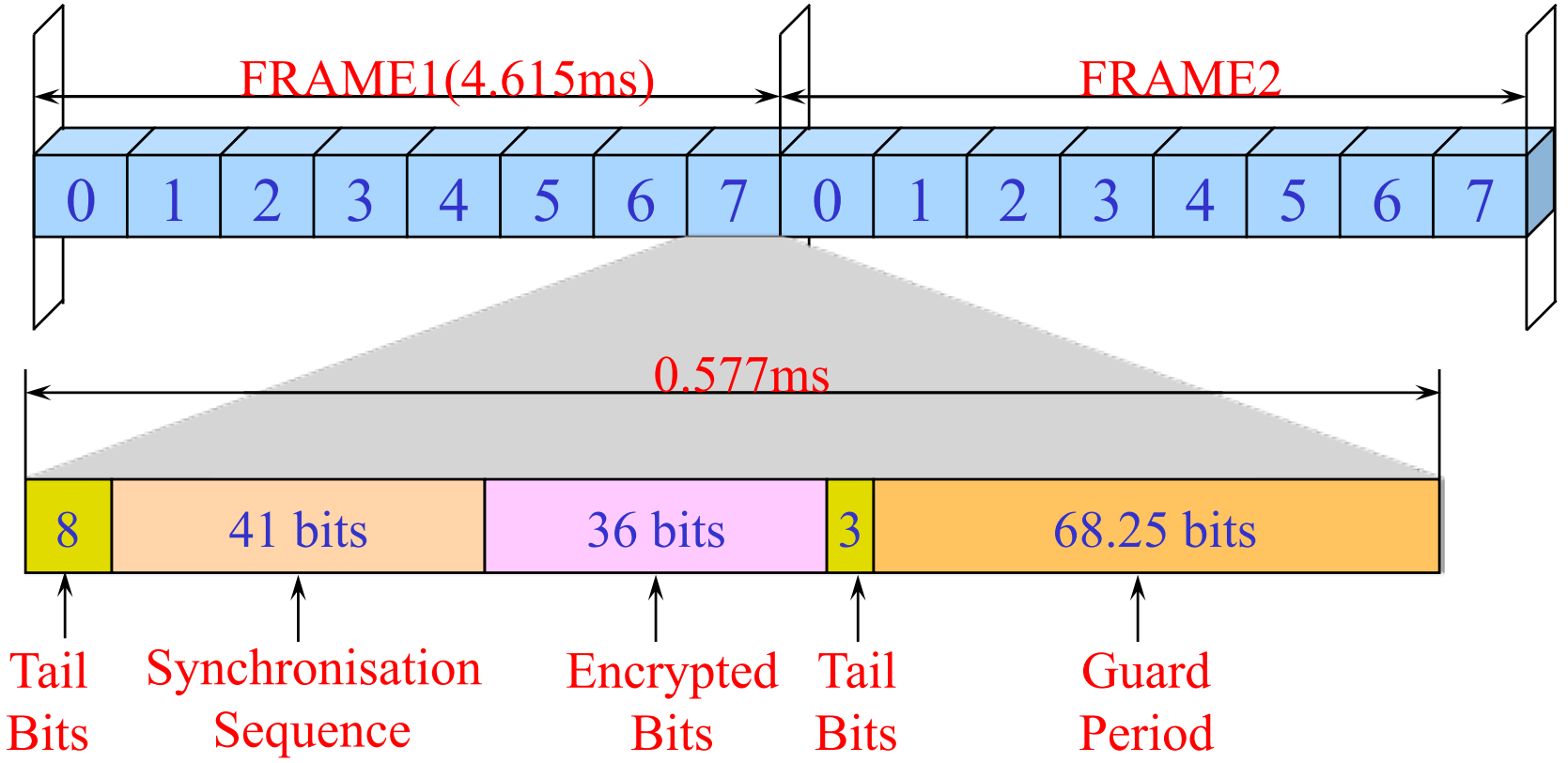
Synchronization Burst



BSIC : Base Station Identity Code

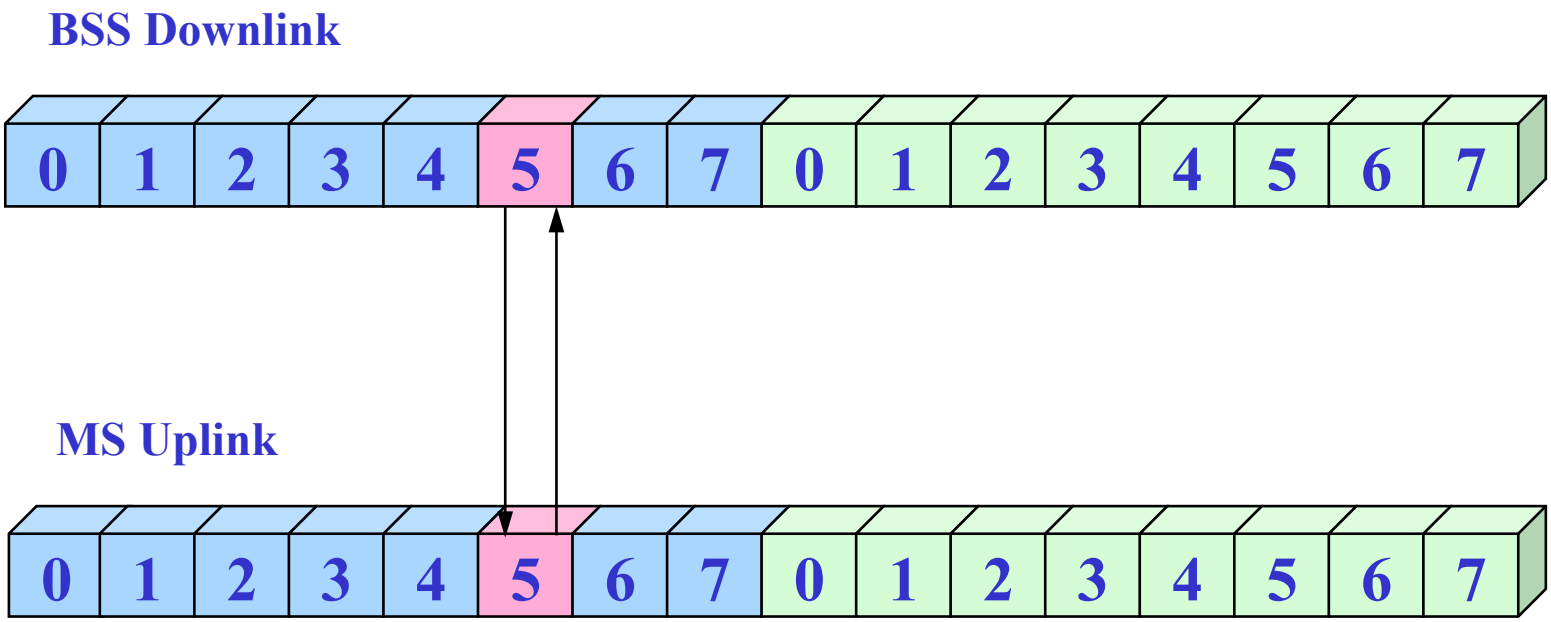
- Carries SCH channel
- Enables MS to synchronize its timings with the BTS
- Contains BSIC and TDMA Frame number

Access Burst

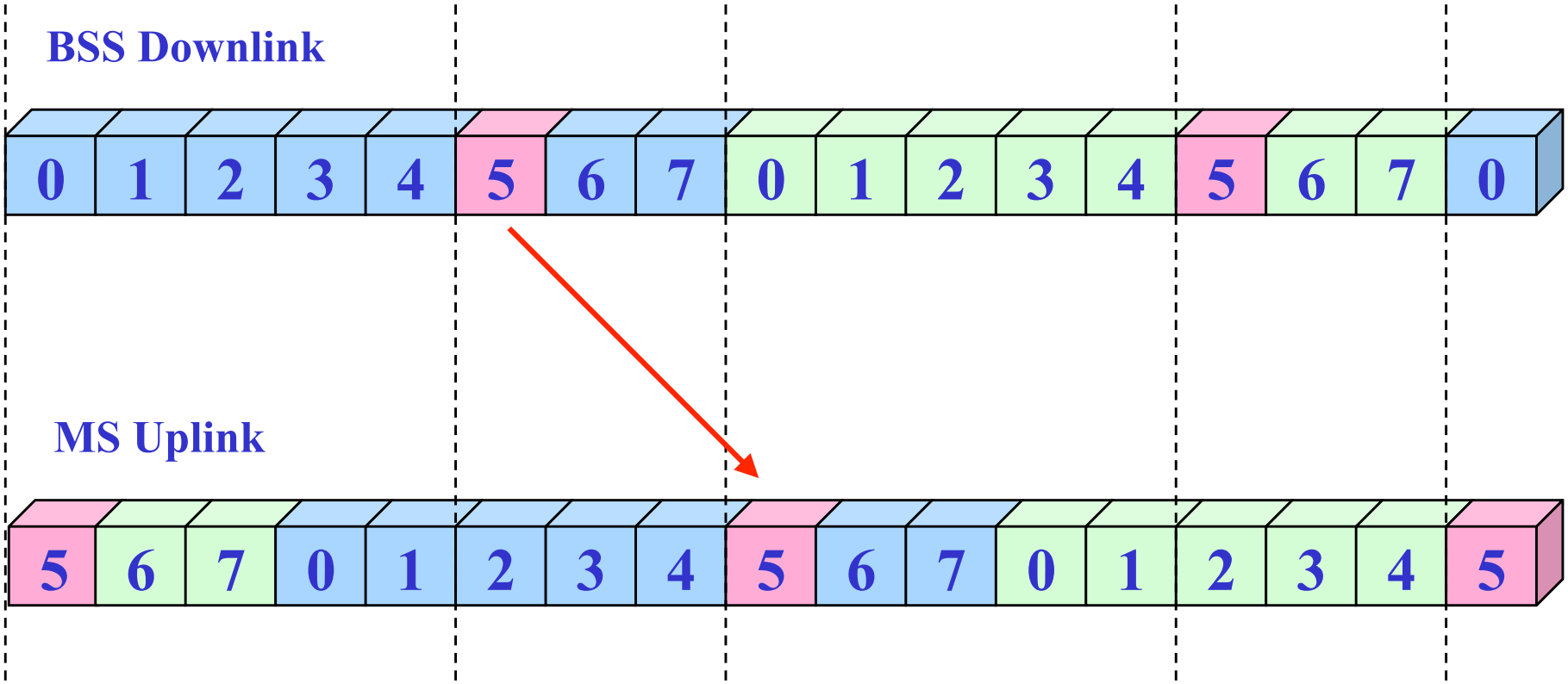


- Carries RACH
- Has a bigger guard period since it is used during initial access and the MS does not know how far it is actually from the BTS

Need for Timeslot Offset

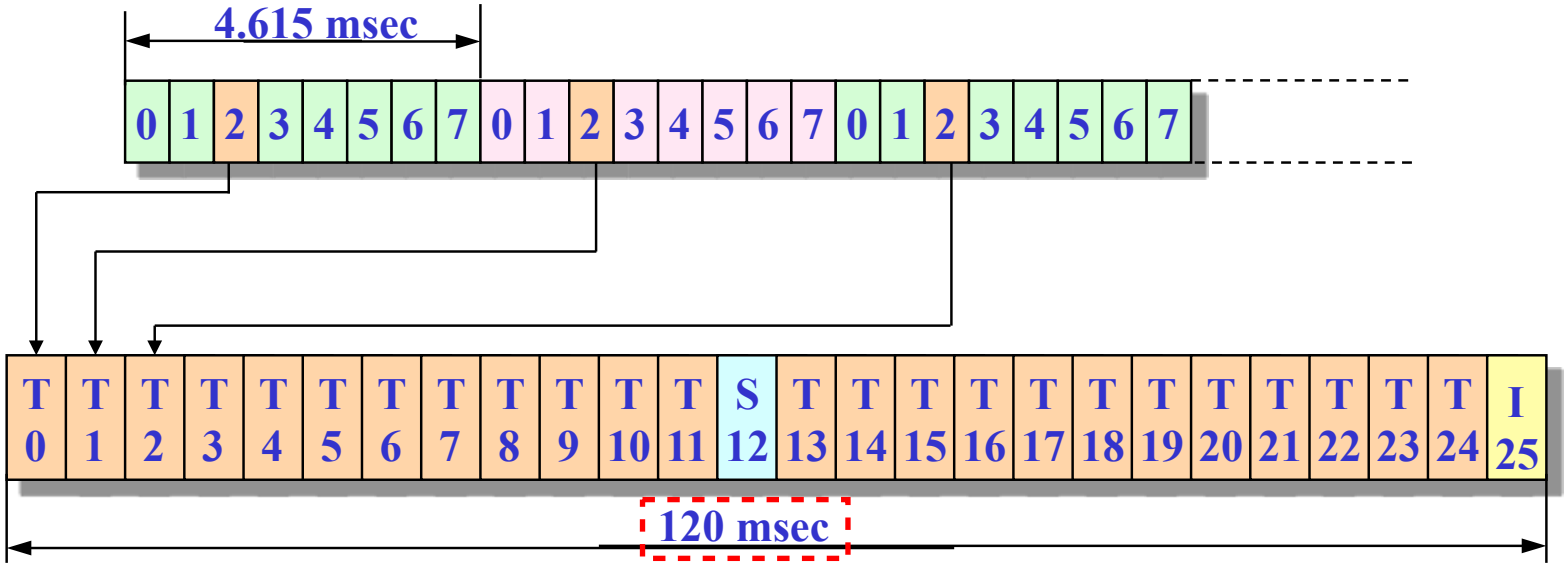


- If Uplink and Downlink are aligned exactly, then MS will have to transmit and receive at the same time
- To overcome this problem a offset of 3 timeslots is provided between downlink and uplink



- As seen the MS does not have to transmit and receive at the same time

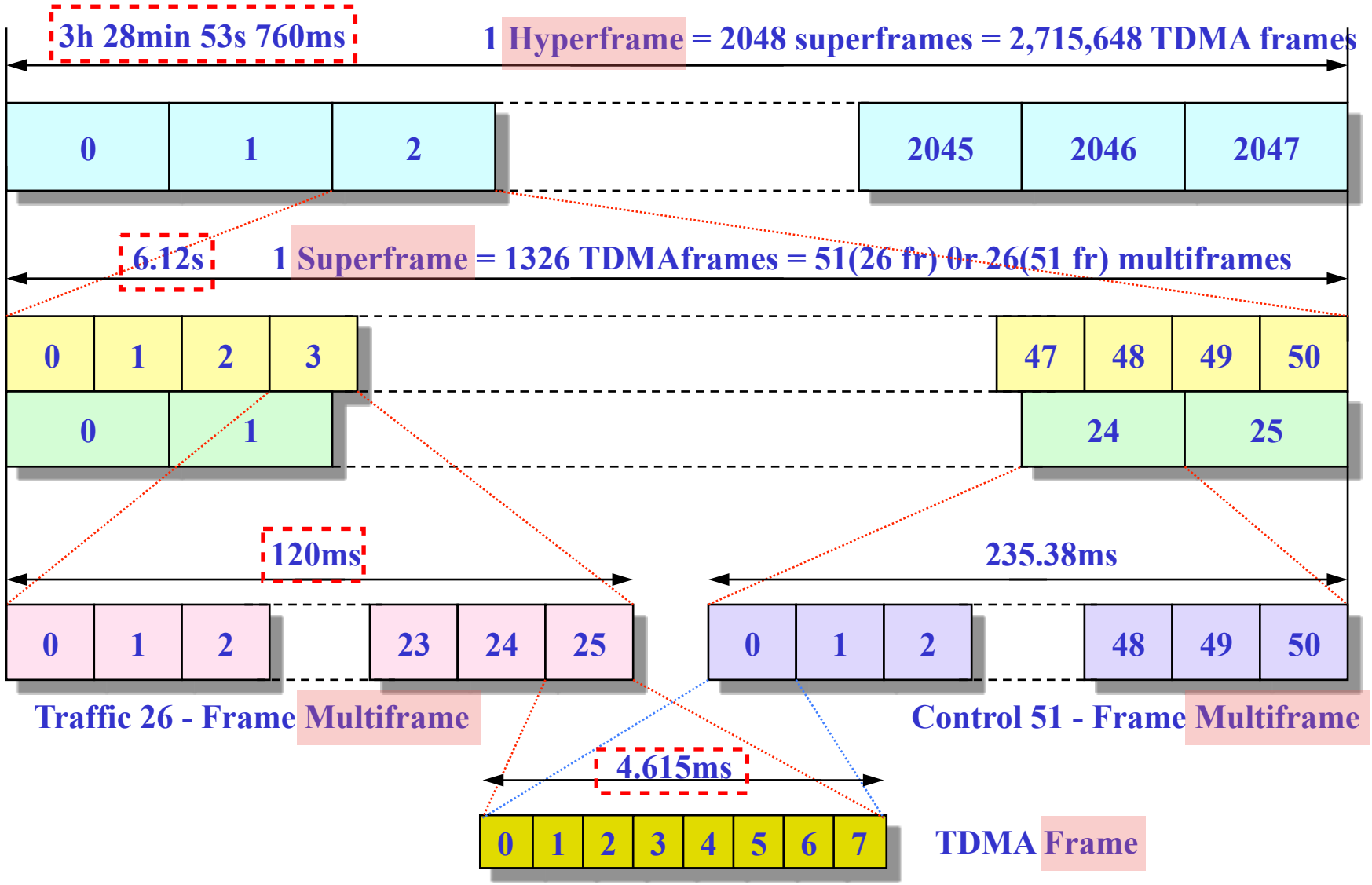
26-Frame Multiframe Structure



SACCH : Slow Associated Control Channel
BSIC : Base Station Identity Code

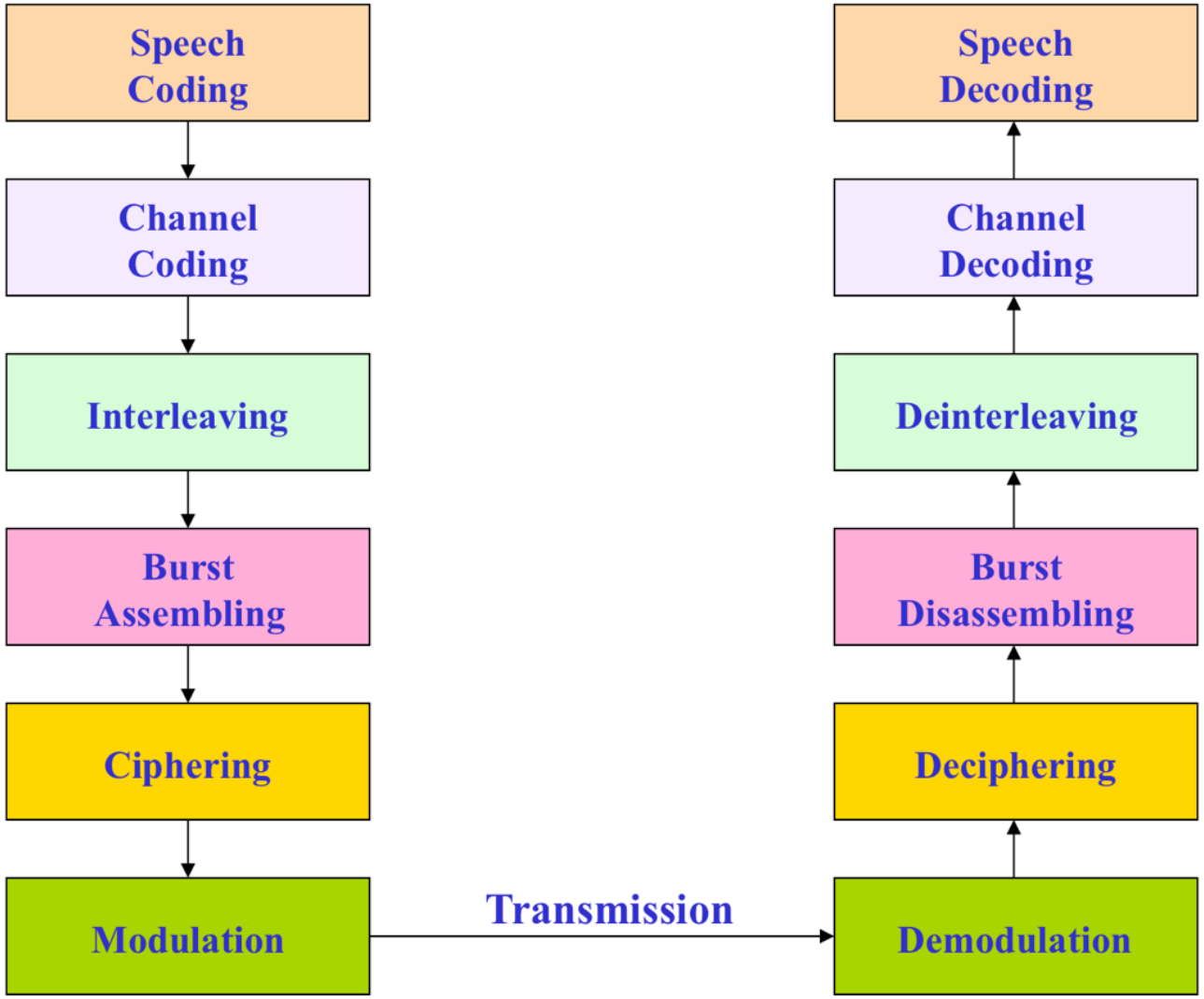
- MS on dedicated mode on a TCH uses a **26-frame multiframe** structure
- Frame 0-11 and 13-24 used to carry traffic
- Frame 12 used as SACCH to carry control information from and to MS to BTS
- Frame 25 is idle and is used by mobile to decode the BSIC of neighbor cells

Hyperframe and Superframe Structure



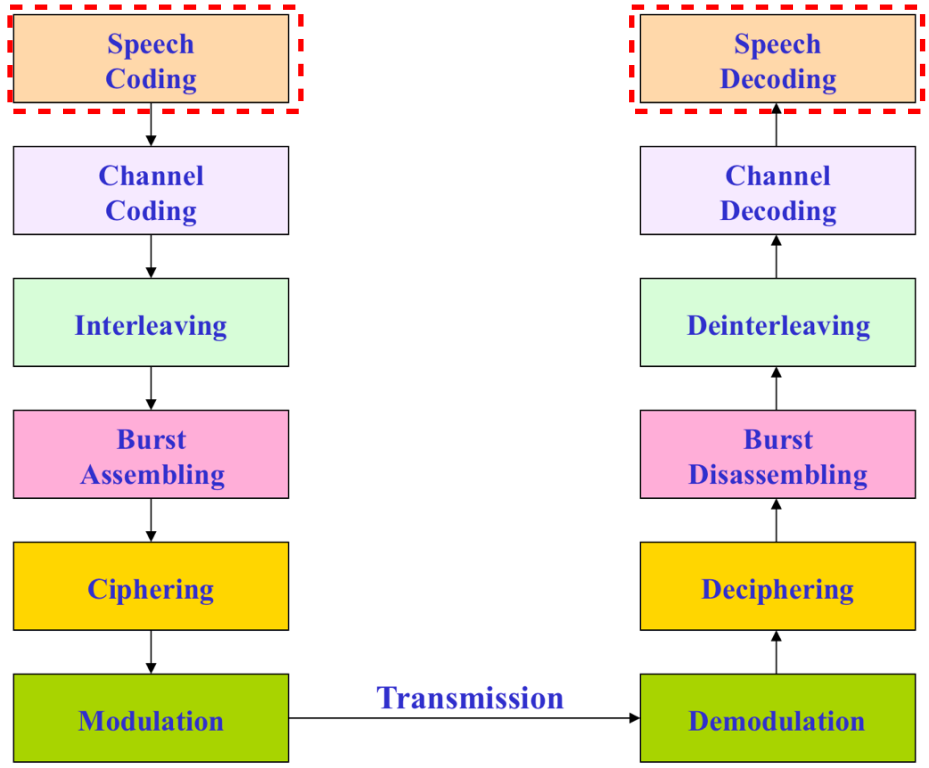
- 1. Introduction
- 2. Features of GSM
- 3. Network Components
- 4. Channel Concept
- 5. Coding, Interleaving, Ciphering
- 6. Signaling
- 7. Handover
- 8. Location Update

5. Coding, Interleaving, Ciphering



Speech Coding

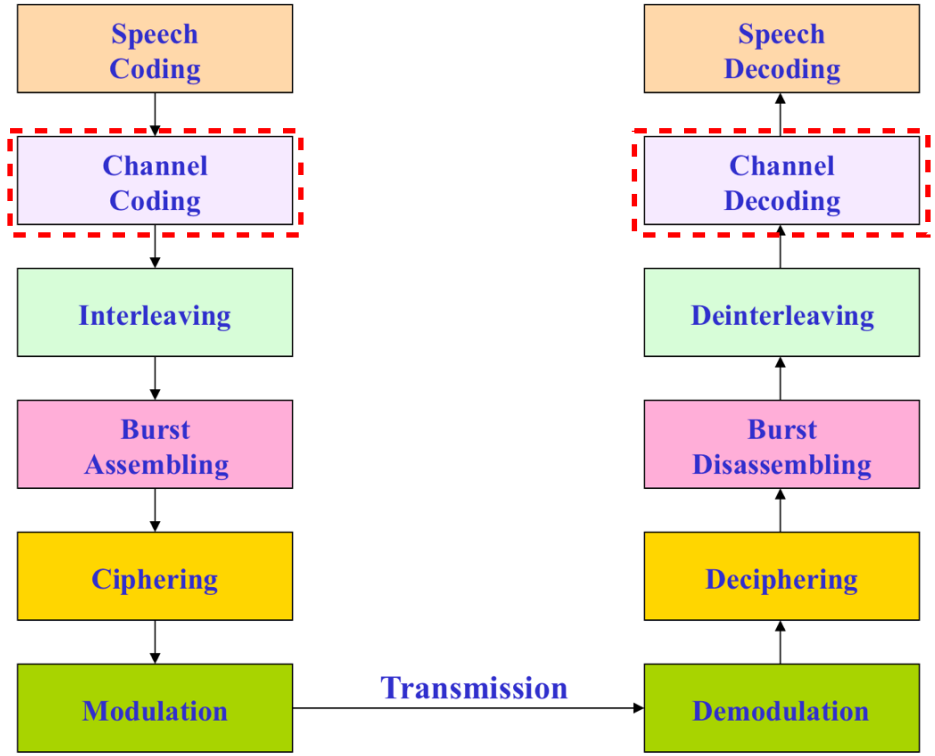
- GSM speech codec transforms the analog signal (voice) into a digital representation, has to meet the following criteria
  - ✓ a good speech quality, at least as good as the one obtained with previous cellular systems
  - ✓ speech codec must not be very complex because complexity is equivalent to high costs



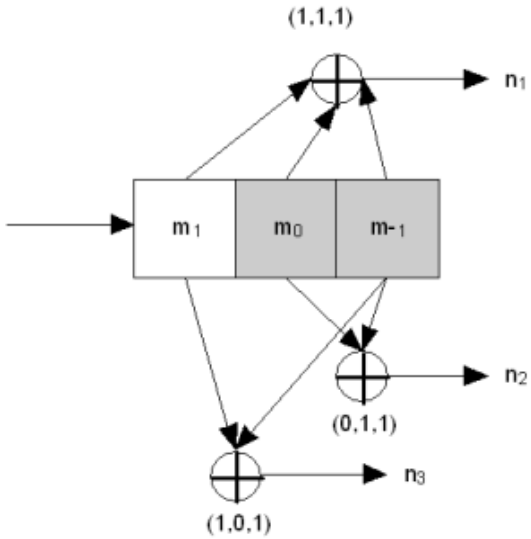
- GSM speech codec: RPE-LTP (Regular Pulse Excitation Long-Term Prediction)
- The speech signal is divided into blocks of 20 ms
  - ✓ these blocks are then passed to the speech codec, which has a rate of 13 kbps, in order to obtain blocks of 260 bits (= 13 kbps x 20 ms)

Channel Coding

- Channel coding adds redundancy bits to the original information in order to detect and correct errors occurred during the transmission
- The channel coding is performed using two codes
  - ✓ block code
  - ✓ convolutional code

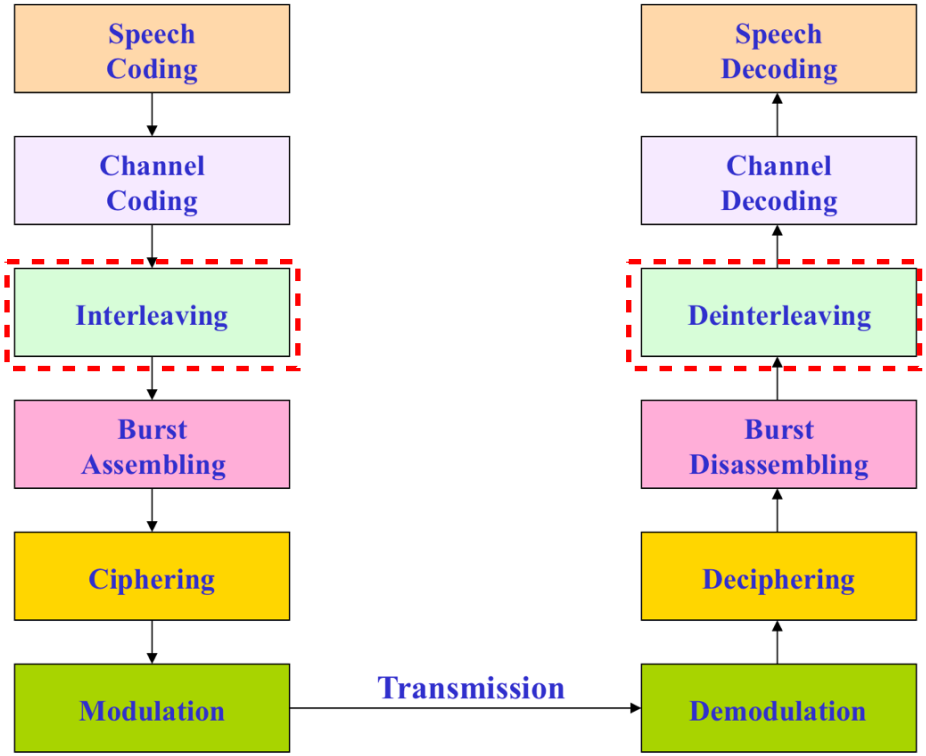


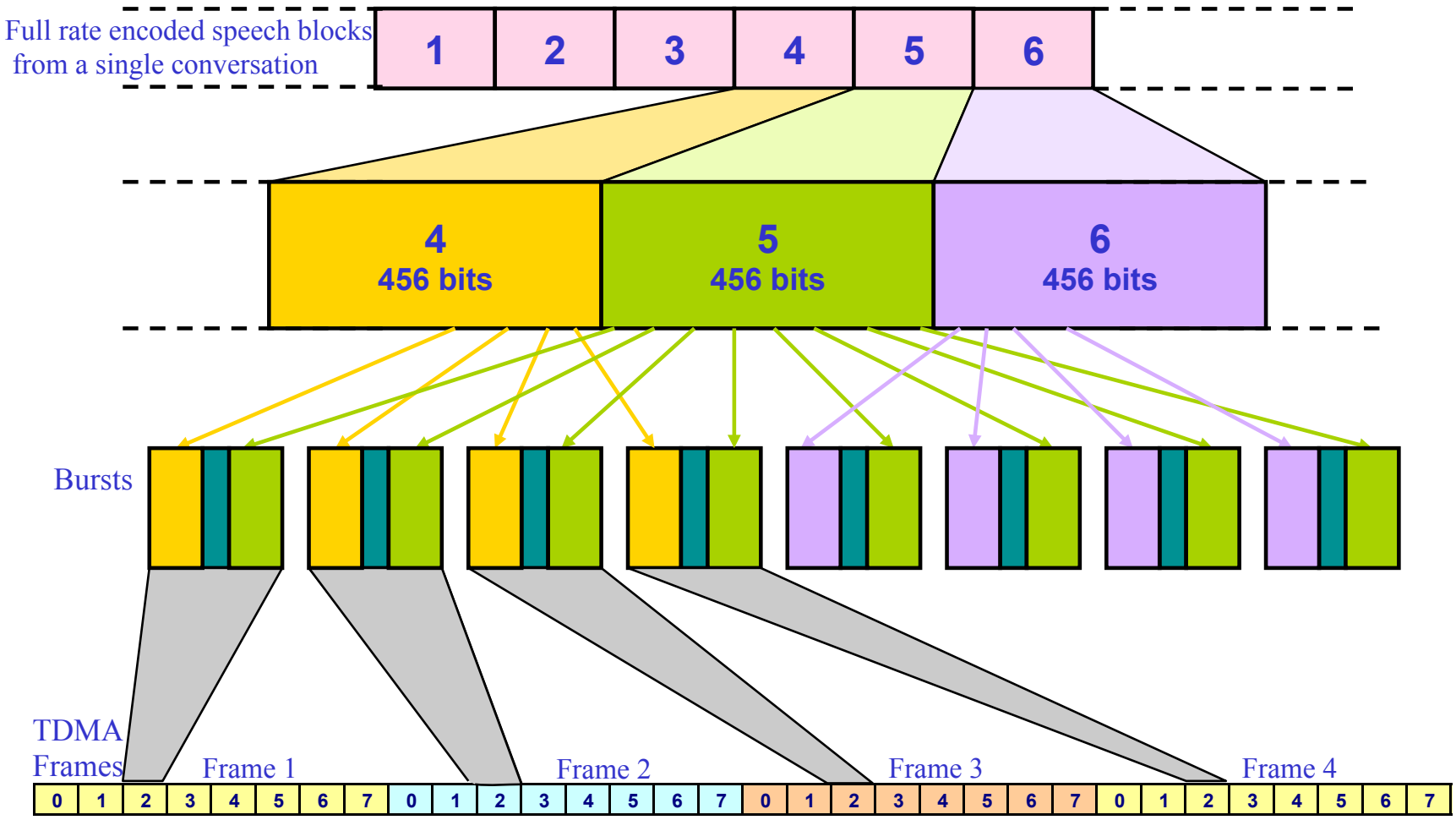
- Block code
  - ✓ receives an input block of 240 bits and adds four zero tail bits at the end of the input block
  - ✓ the output of the block code is consequently a block of 244 bits
  - ✓ every block codes submit *k* bits in their inputs and forwards *n* bits in their output [known as (*n*,*k*) code]
- Convolutional code
  - ✓ adds redundancy bits in order to protect the information
  - ✓ a convolutional encoder contains memory
  - ✓ this property differentiates a convolutional code from a block code
  - ✓ every convolutional code uses *m* units of memor [known as (*n*,*k*,*m*) code]



Interleaving

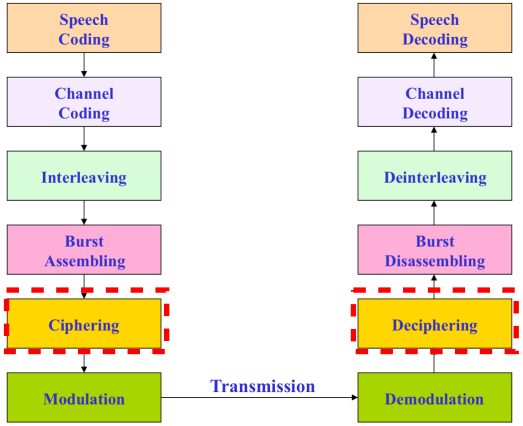
- An interleaving rearranges a group of bits in a particular way
- It is used in combination with FEC codes (Forward Error Correction Codes) in order to improve the performance of error correction mechanisms
- The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing [分散] the errors
- As the errors are less concentrated, it is then easier to correct them

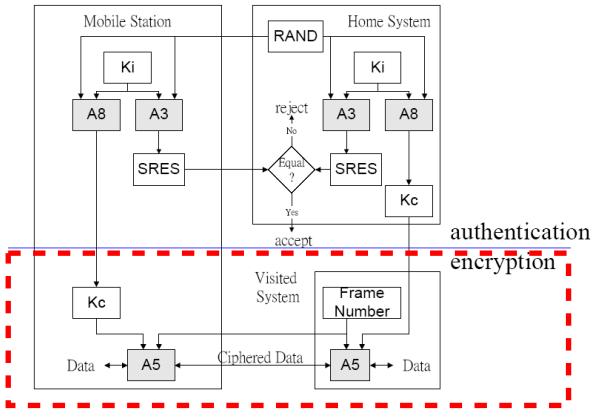


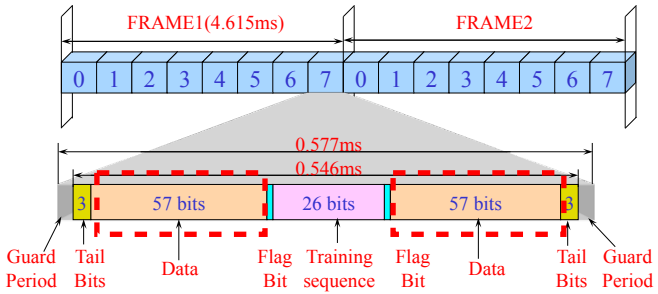

Full rate encoded speech blocks
from a single conversation
1
2
3
4
5
6
4
456 bits
5
456 bits
6
456 bits
Bursts
TDMA
Frames
Frame 1
Frame 2
Frame 3
Frame 4
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7

Ciphering

- Used to protect signaling and user data
- A ciphering key (K_c) is computed using
  - ✓ algorithm A8 stored on SIM card
  - ✓ subscriber key (K_i)
  - ✓ a random number delivered by the network
- A 114 bit cipher sequence is produced using
  - ✓ ciphering key (K_c)
  - ✓ algorithm A5
  - ✓ burst numbers
- This bit sequence is then XORed with the two 57 bit blocks of data included in a normal burst
- Decipher
  - ✓ the receiver use the same Algorithm A5 for the deciphering procedure







Ciphering

Clear Text 0 1 0 0 1 0 1 1 1 0 0 1 . . .

57 bits + 57 bits

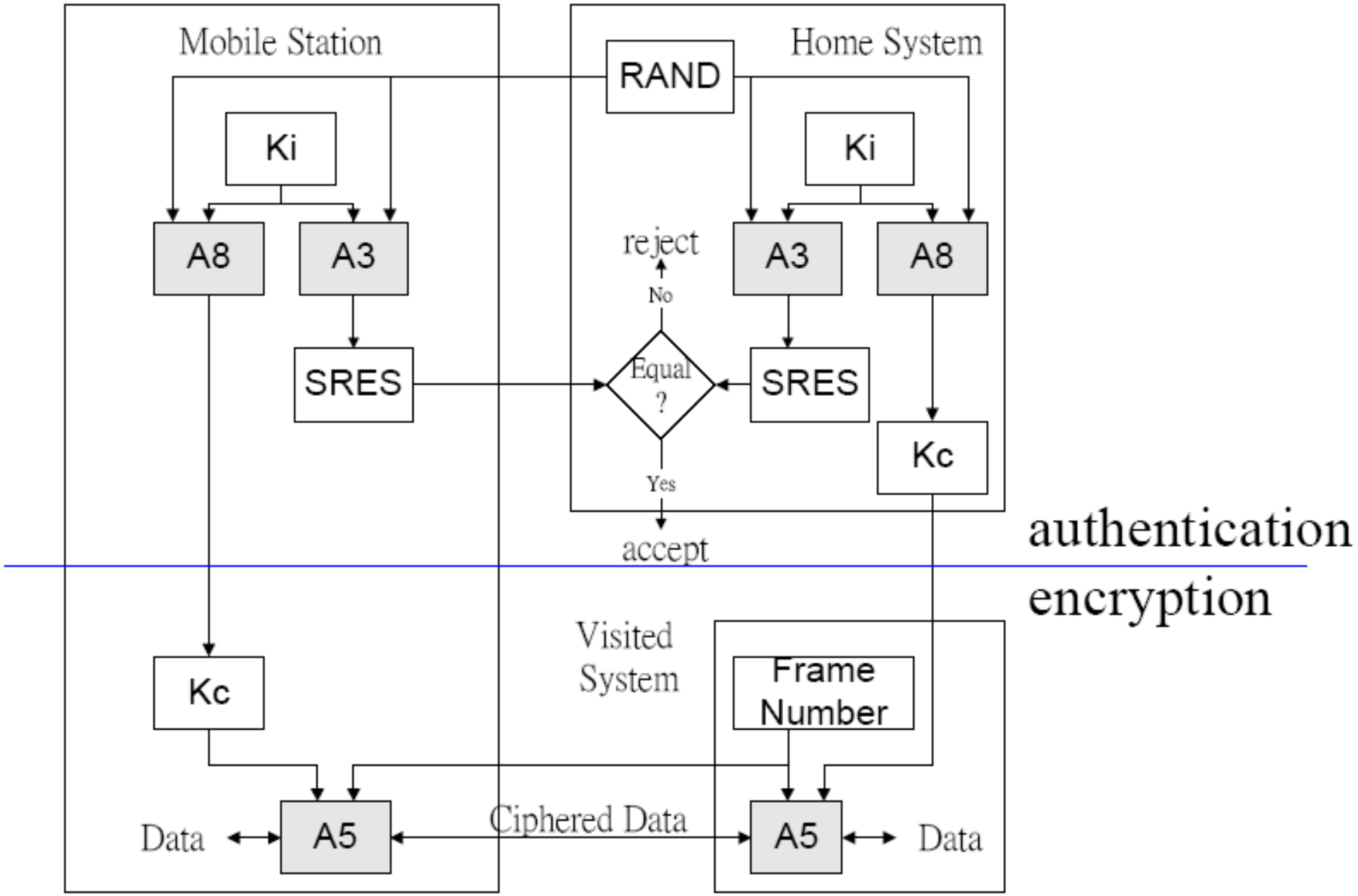
Cipher Sequence 0 0 1 0 1 1 0 0 1 1 1 0 . . .

114 bits

XOR

Ciphered Text 0 1 1 0 0 1 1 1 0 1 1 1 . . .

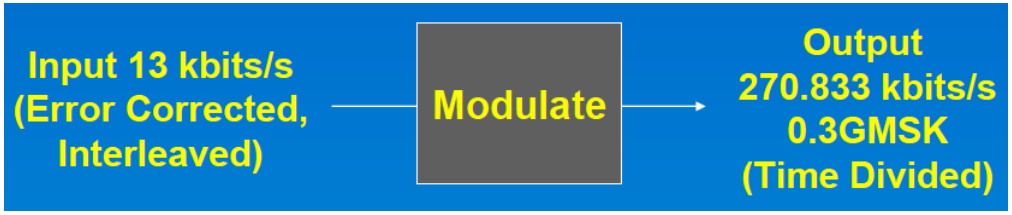
	0	1
0	0	1
1	1	0

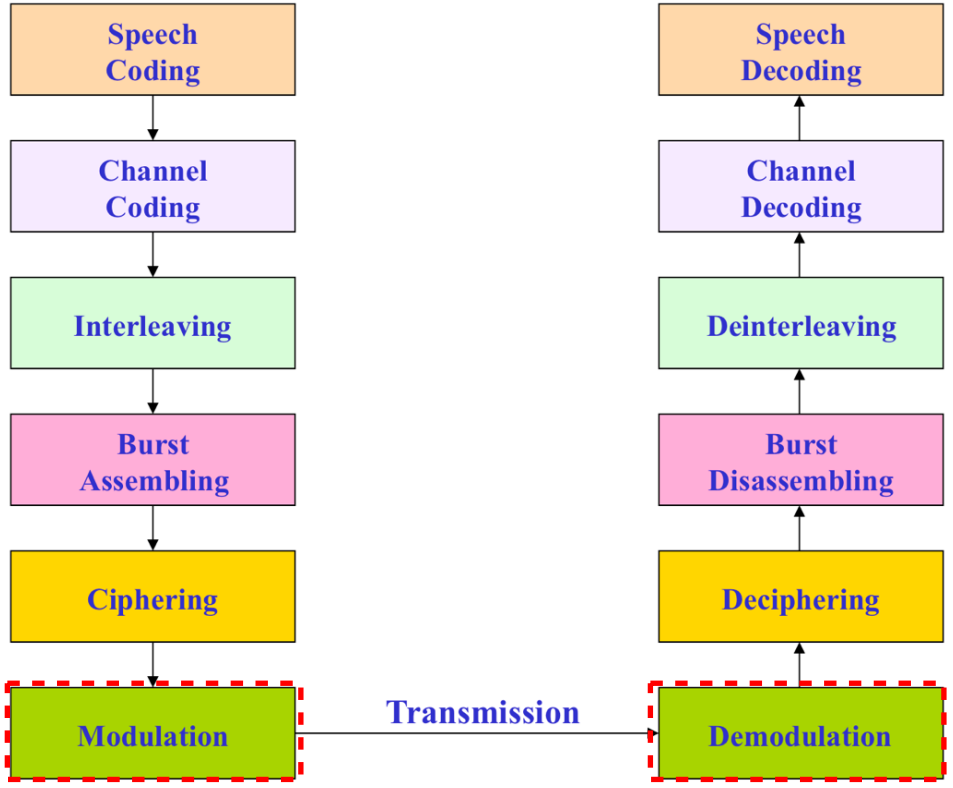


Authentication & Encryption Process

Modulation

- Modulation is done using 0.3 GMSK (0.3 Gaussian Minimum Shift Keying)





- 1. Introduction
- 2. Features of GSM
- 3. Network Components
- 4. Channel Concept
- 5. Coding, Interleaving, Ciphering
- 6. Signaling
- 7. Handover
- 8. Location Update

6. Signaling

- Signaling
  - ✓ in technical systems, it very often refers to the control of different procedures
  - ✓ with reference to telephony, signaling means the transfer of information and the instructions relevant to control and monitor telephony connections
- Today's global telecom networks are included in very complex technical systems, which requires extensive signaling, both
  - ✓ internally in different nodes (for example, exchanges)
  - ✓ externally between different types of network nodes

- Different network nodes must cooperate and communicate with each other to enable transfer of control information

  ✓ **traffic control procedures**

  - set-up, supervision, and release of telecommunication connections and services

  ✓ **database communication**

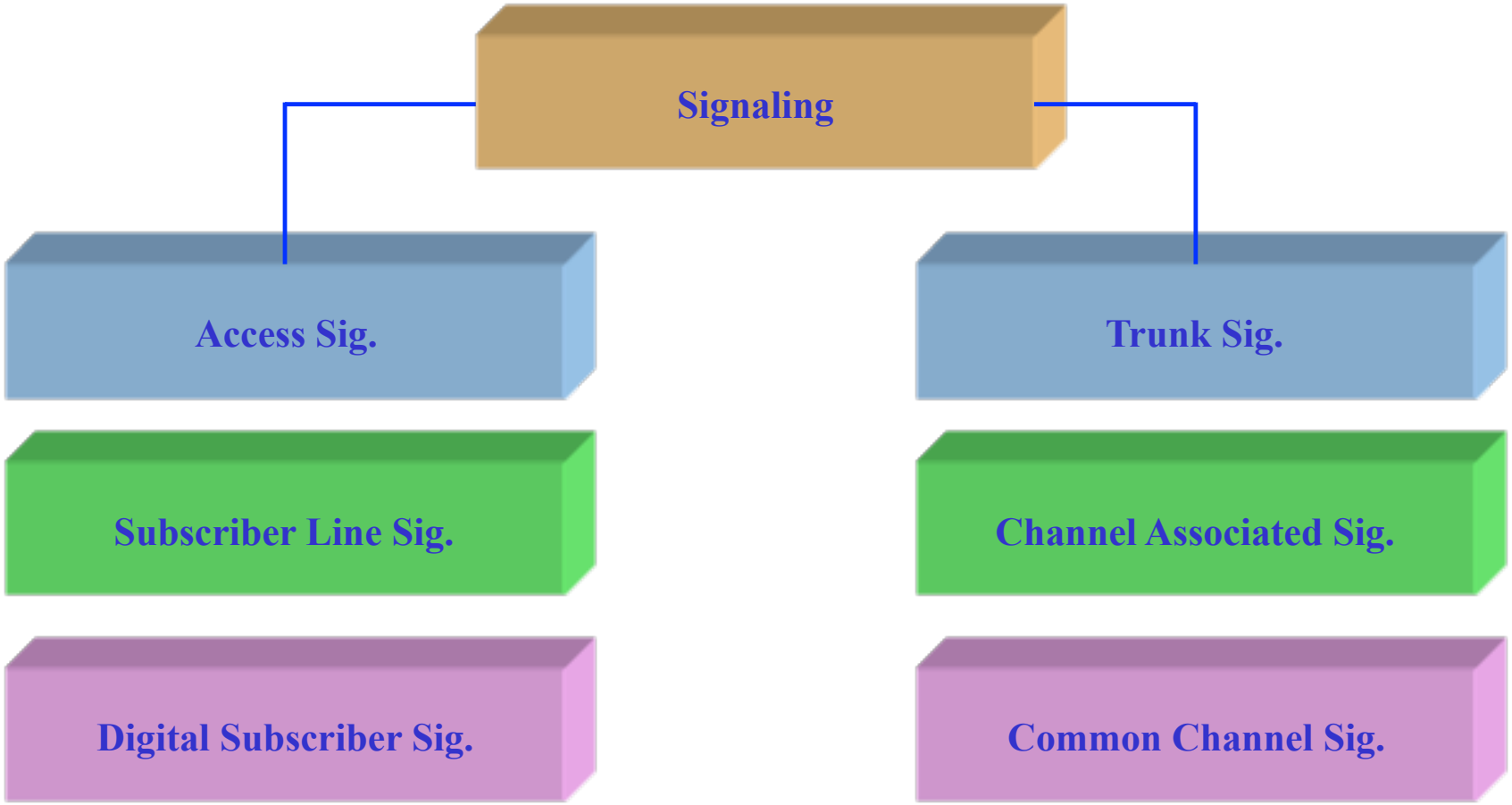
  - database queries concerning specific services, roaming in cellular networks, etc.

  ✓ **network management procedures**

  - blocking or deblocking trunks

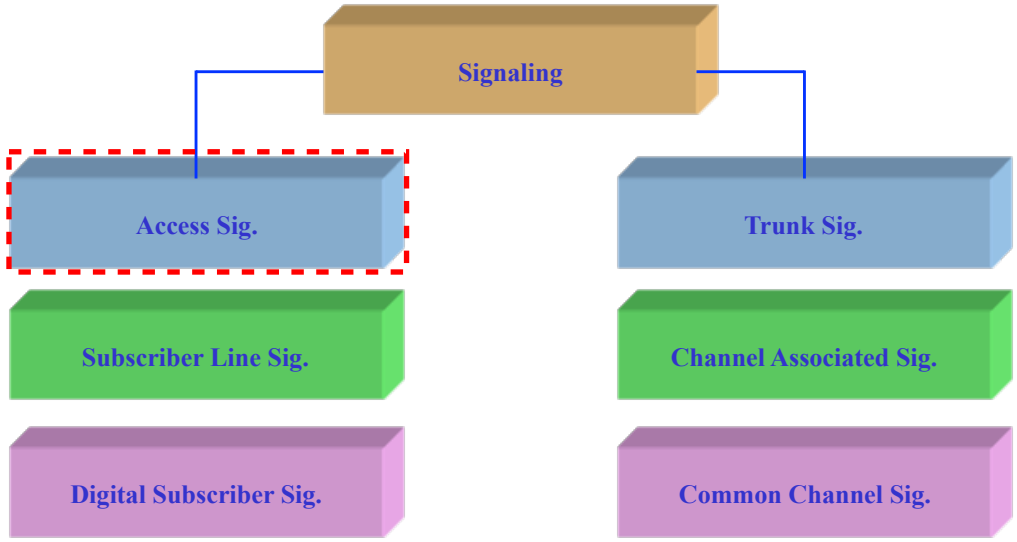
- External signaling has been divided into two basic types
  - ✓ **access signaling**
    - e.g., subscriber loop signaling
    - signaling between a subscriber terminal (telephone) and the local exchange
  - ✓ **trunk signaling**
    - e.g., inter-exchange signaling
    - used for signaling between exchanges

Signaling in Telecommunication Network



Access Signaling

- Access signaling types
  - ✓ PSTN analogue subscriber line signaling
  - ✓ ISDN Digital Subscriber Signaling System (DSS1)
  - ✓ signaling between MS and the network in GSM system



- Signaling on the analogue subscriber line between a telephony subscriber and Local Exchange (LE)

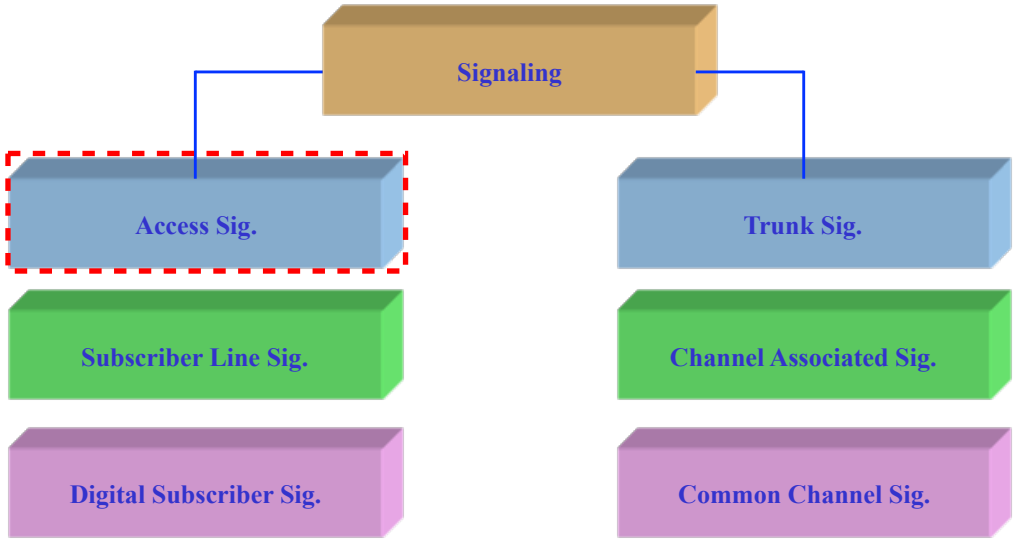
  ✓ on/off hook signals

  ✓ dialed digits

  ✓ information tones (dial tone, busy tone, etc.)

  ✓ recorded announcements

  ✓ ringing signals



* PSTN analogue subscriber line signaling
* ISDN Digital Subscriber Signaling System (DSS1)
* Signaling between MS and the network in GSM system

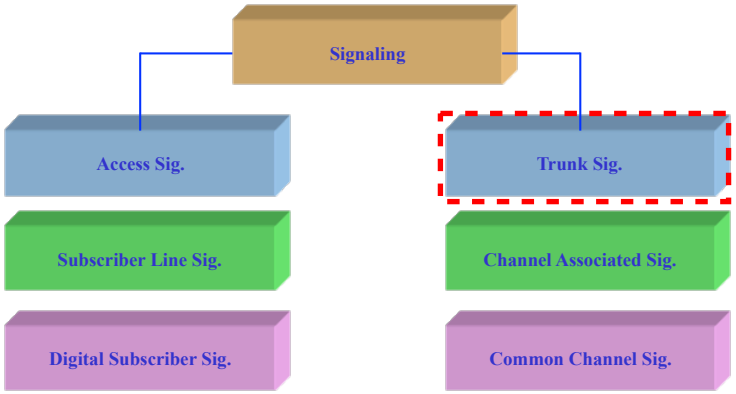
- Dialed digits can be sent in two different ways
  - ✓ decadic [十進位] pulses (used for old-type rotary-dial telephones), or
  - ✓ combination of two tones (used for modern pushbutton telephones) - Dual Tone Multi Frequency (DTMF)
- Information tones (dial tone, ringing tone, busy tone, etc.)
  - ✓ the audio signals used to keep the calling party (the A-subscriber) informed about what is going on in the network during the set-up of a call

- Digital Subscriber Signaling System No. 1 (DSS1)
  - ✓ the standard access signaling system used in ISDN
  - ✓ also called a D-channel signaling system
  - ✓ D-channel signaling is defined for digital access lines only
- Signaling protocols are based on OSI (Open System Interconnection) reference model, layers 1 to 3
  - ✓ consequently, the signaling messages are transferred as data packets between user terminal and local exchange

* PSTN analogue subscriber line signaling
* ISDN Digital Subscriber Signaling System (DSS1)
* Signaling between MS and the network in GSM system

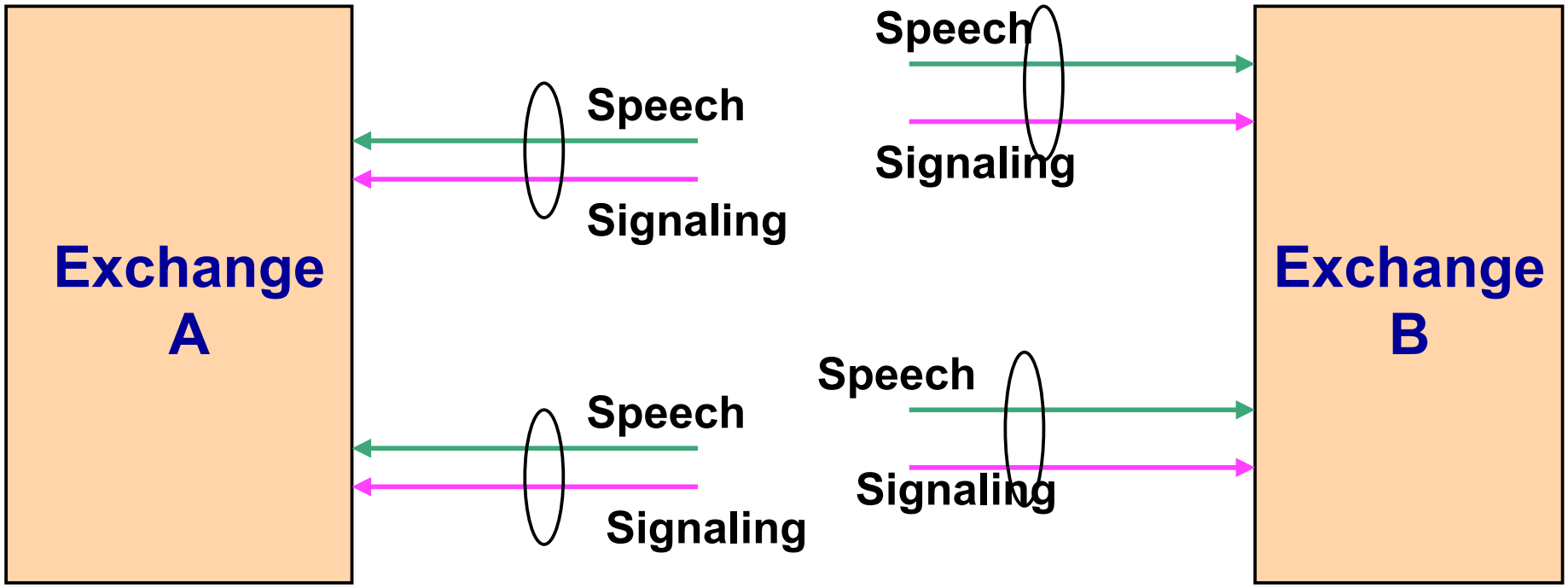
Trunk Signaling

- Trunk signaling is inter-exchange signaling information
- Two commonly used methods for inter exchange signaling
  - ✓ **Channel Associated Signaling (CAS)**
    - the signaling is always sent on the same connection (PCM link) as the traffic
    - signaling is associated with the traffic channel



Pulse-Code Modulation (PCM)

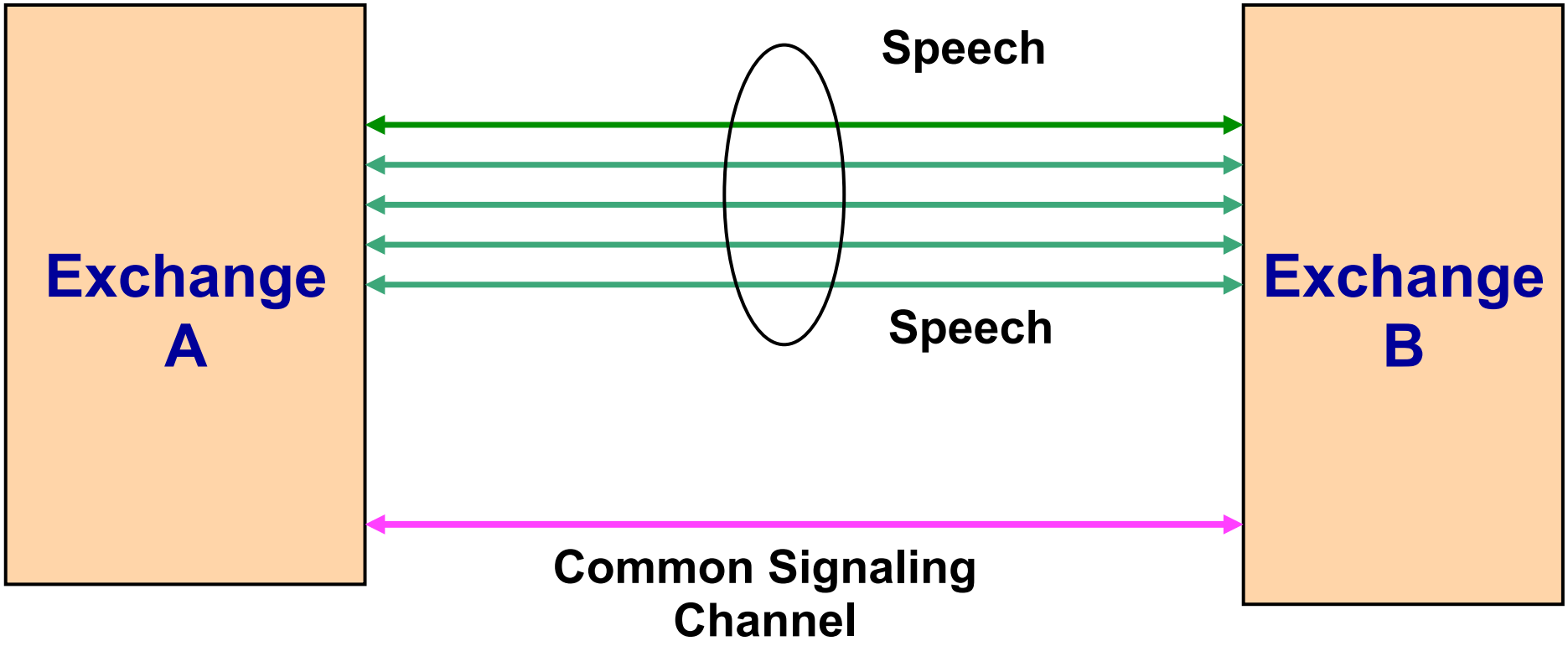
* A method used to digitally represent sampled analog signals. It is the standard form of digital audio in computers, Compact Discs, digital telephony and other digital audio applications.
* In a PCM stream, the magnitude [強度] of the analog signal is sampled regularly at uniform intervals, and each sample is quantized to the nearest value within a range of digital steps.



Channel Associated Signaling (CAS)

✓ Common Channel Signaling (CCS)

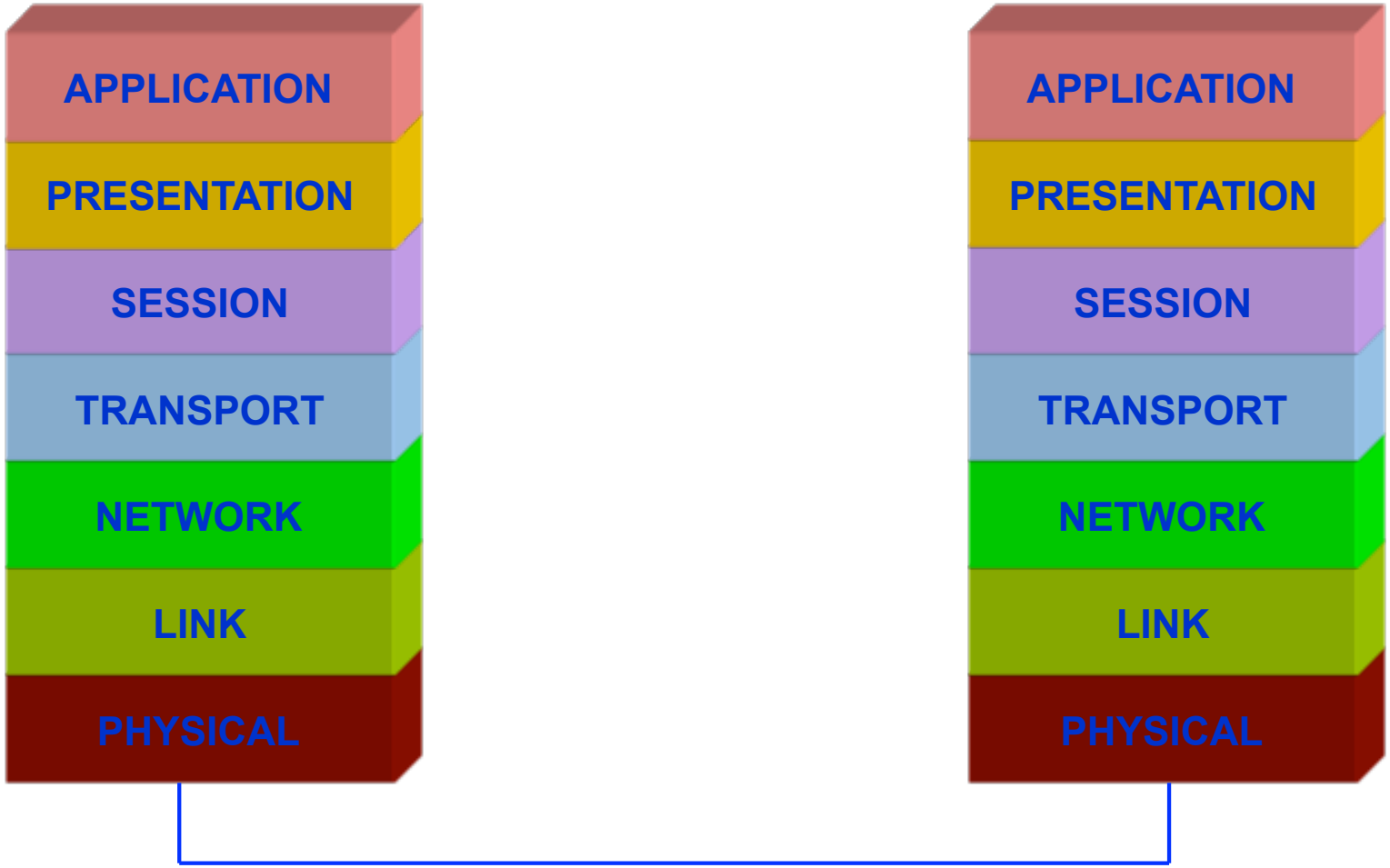
- a dedicated channel, completely separate from the speech channel, is used for signaling
- due to the high capacity, one signaling channel in CCS can serve a large number of speech channels
- GSM uses CCITT Signaling System No. 7 (SS7), which is a CCS system
  - today SS7 is used in many different networks and related services typically between PSTN, ISDN, PLMN & IN services throughout the world



Common Channel Signaling (CCS)

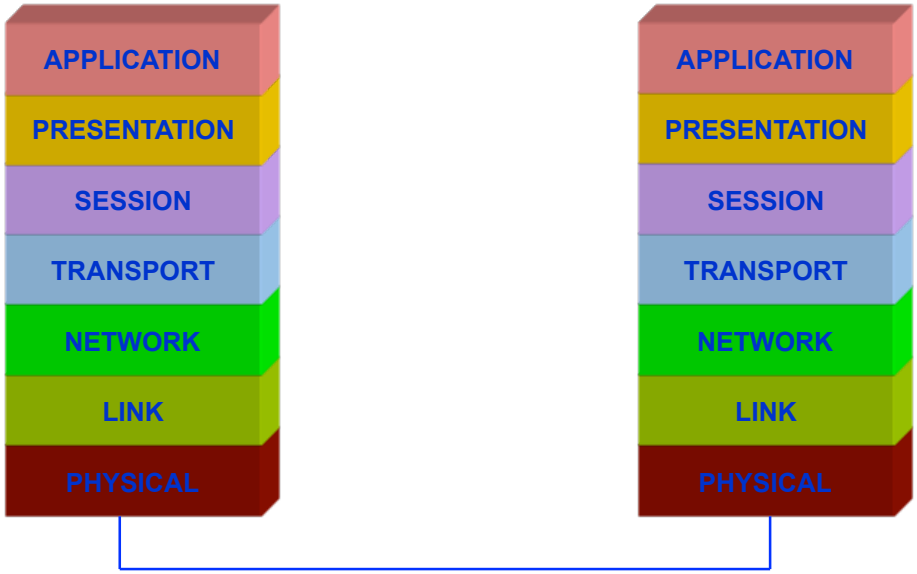
OSI Reference Model

- Signaling System No. 7
  - ✓ a type of packet switched data communication system
  - ✓ structured in a modular and layered way
  - ✓ similar to the Open System Interconnection (OSI) model
- Open systems
  - ✓ the systems that use standardized communication procedures developed from the reference model
  - ✓ all such open systems are able to communicate with each other


APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
LINK
PHYSICAL
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
LINK
PHYSICAL

Communication Process

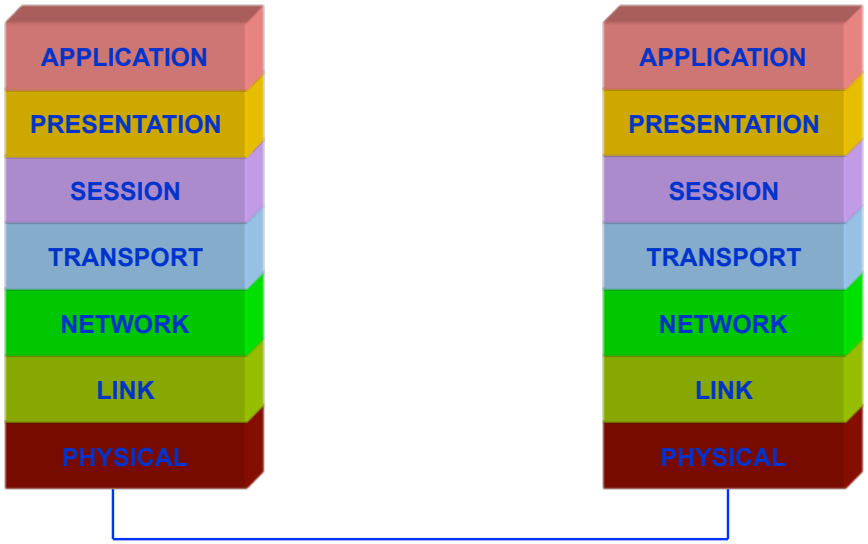
- Each layer has its own specified functions and provides specific services for the layers above
- It is important to define
  - ✓ the interfaces between different layers
  - ✓ the functions within each layer
- The communication between functions always takes place on the same level according to the protocols for that level
  - ✓ only functions on the same level can "talk to each other"



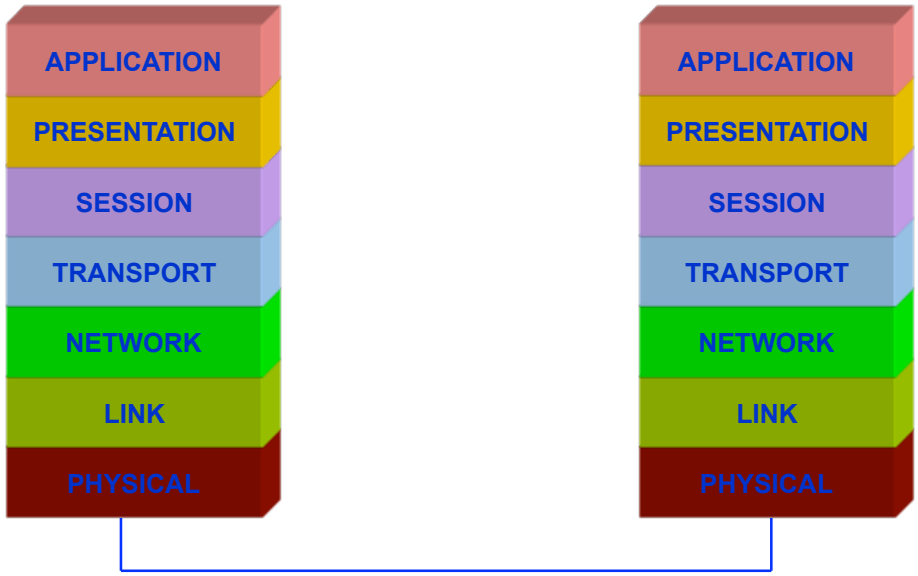
- In the transmitting system
  - ✓ the protocol for each layer adds information to the data received from the layer above
  - ✓ the addition usually consists of a header and/or a trailer
- In the receiving system
  - ✓ the additions are used to identify bits or data fields carrying information for that specific layer only
  - ✓ these fields are decoded by layer functionality and are removed when delivering the message to the applications or layers above
  - ✓ when the data reaches the application layer on the receiving side, it consists of only the data that originated in the application layer of the sending system
- Logically, each layer communicates with the corresponding layer in the other system
  - ✓ this communication is called peer-to-peer communication and is controlled by the layer's protocol

Description of Layers

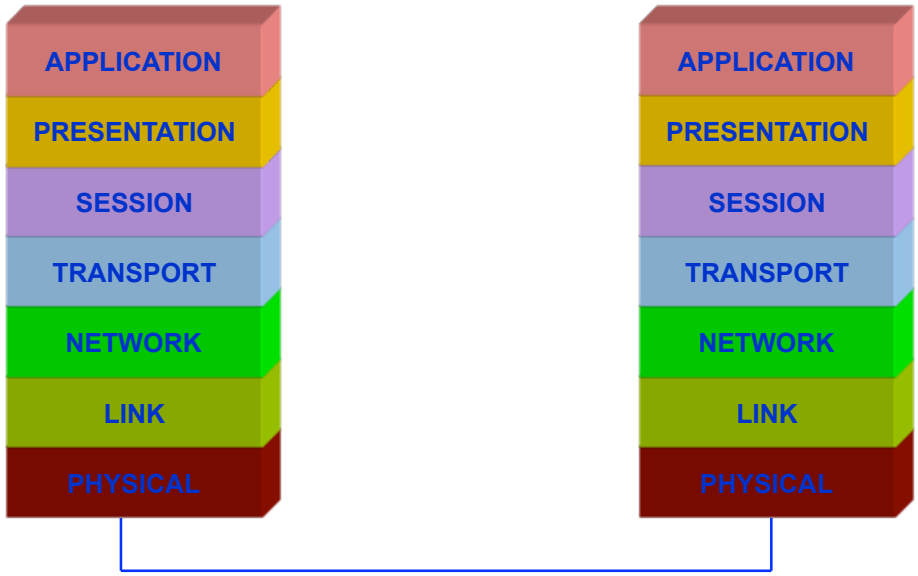
- **Application Layer**
  - ✓ provides services for
    - support of user's application process
    - control of all communication between applications
  - ✓ examples
    - file transfer
    - message handling
    - directory services
    - operation
    - maintenance



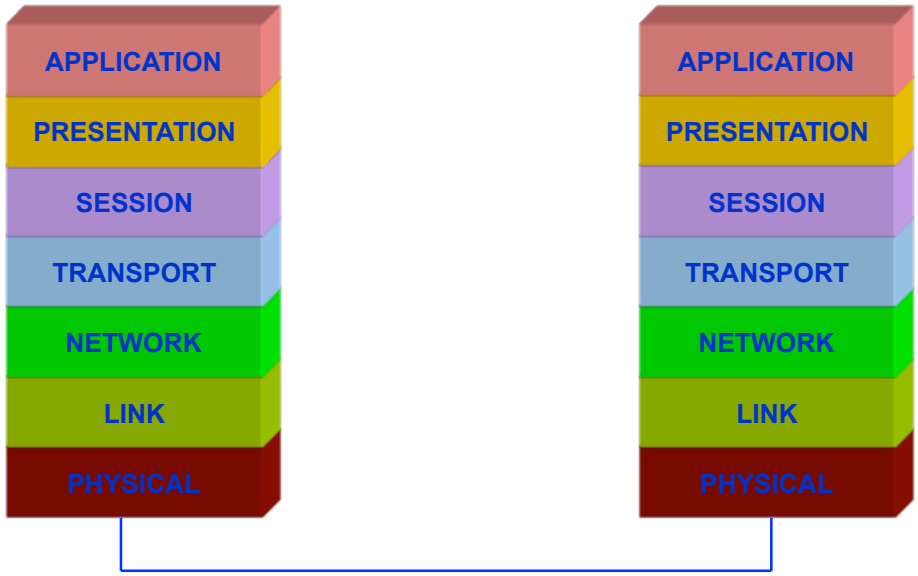
- **Presentation Layer**
  - ✓ defines how data is to be represented, ie., the syntax
  - ✓ transforms the syntax used in the application into the common syntax needed for the communication between applications
  - ✓ contains data compression



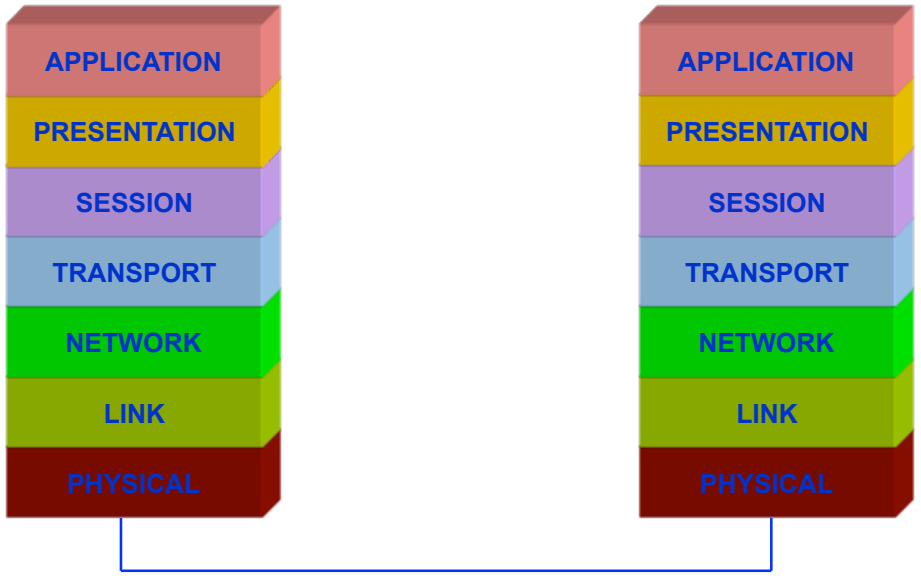
- **Session Layer**
  - ✓ establishes connections between presentation layers in different systems
  - ✓ controls the connection, the synchronization and the disconnection of the dialogue
  - ✓ allows the presentation layer to determine checkpoints, from which the retransmission will start when the data transmission has been interrupted



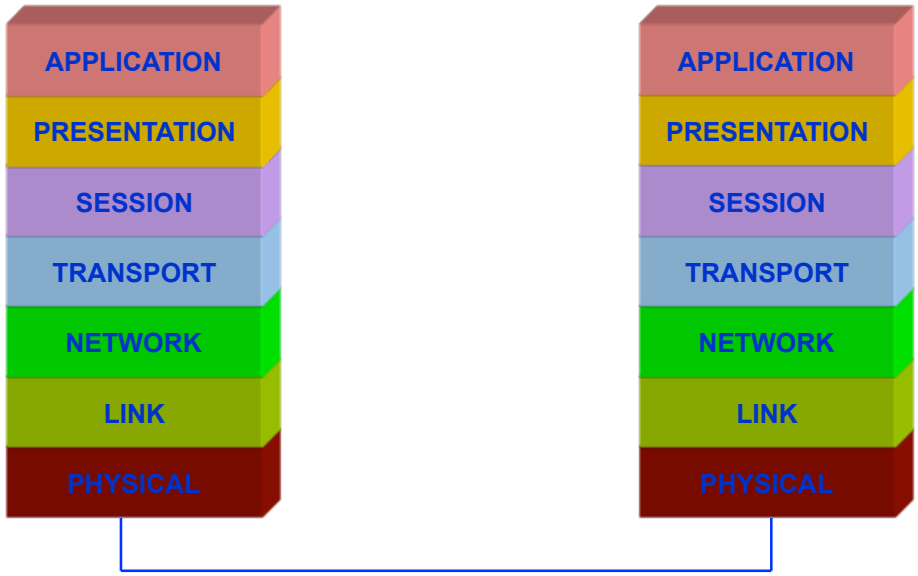
- **Transport Layer**
  - ✓ guarantees that the bearer service has the quality required by the application
    - examples
      - error detection
      - error correction
      - flow control
  - ✓ optimizes data communication
    - example : multiplex or split data streams before they reach the network



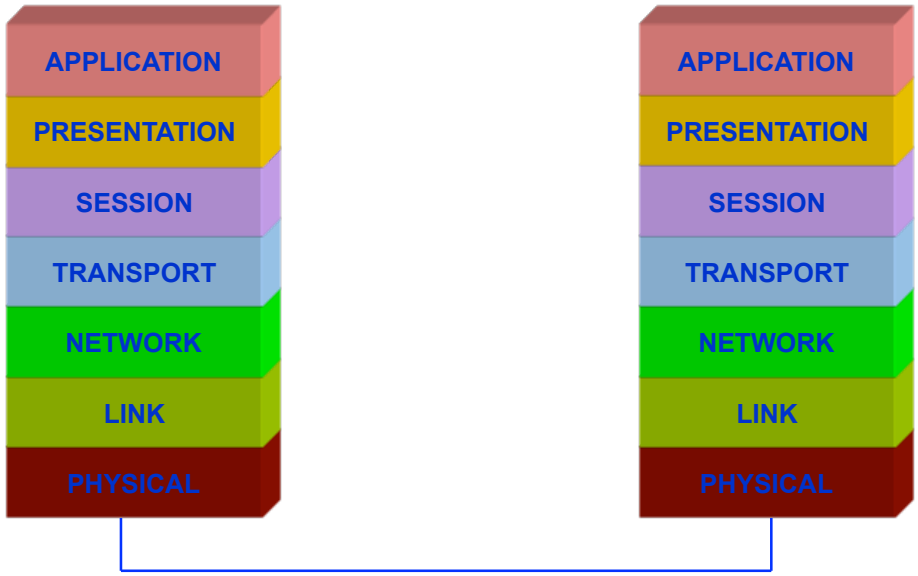
- **Network Layer**
  - ✓ basic service: provide a transparent channel
    - this means that the application requesting a channel ignores network problems and the related signal exchange because that is the task of the lower levels
    - it just requires an open channel, transparent for the transmission of data, between transport layers in different systems
  - ✓ establishes, maintains, and releases connections between the nodes in the network and handles addressing and routing of circuits



- **Data Link Layer**
  - ✓ provides an essentially error-free point-to-point circuit between network layers
  - ✓ contains resources for error detection, error correction, flow control, and retransmission

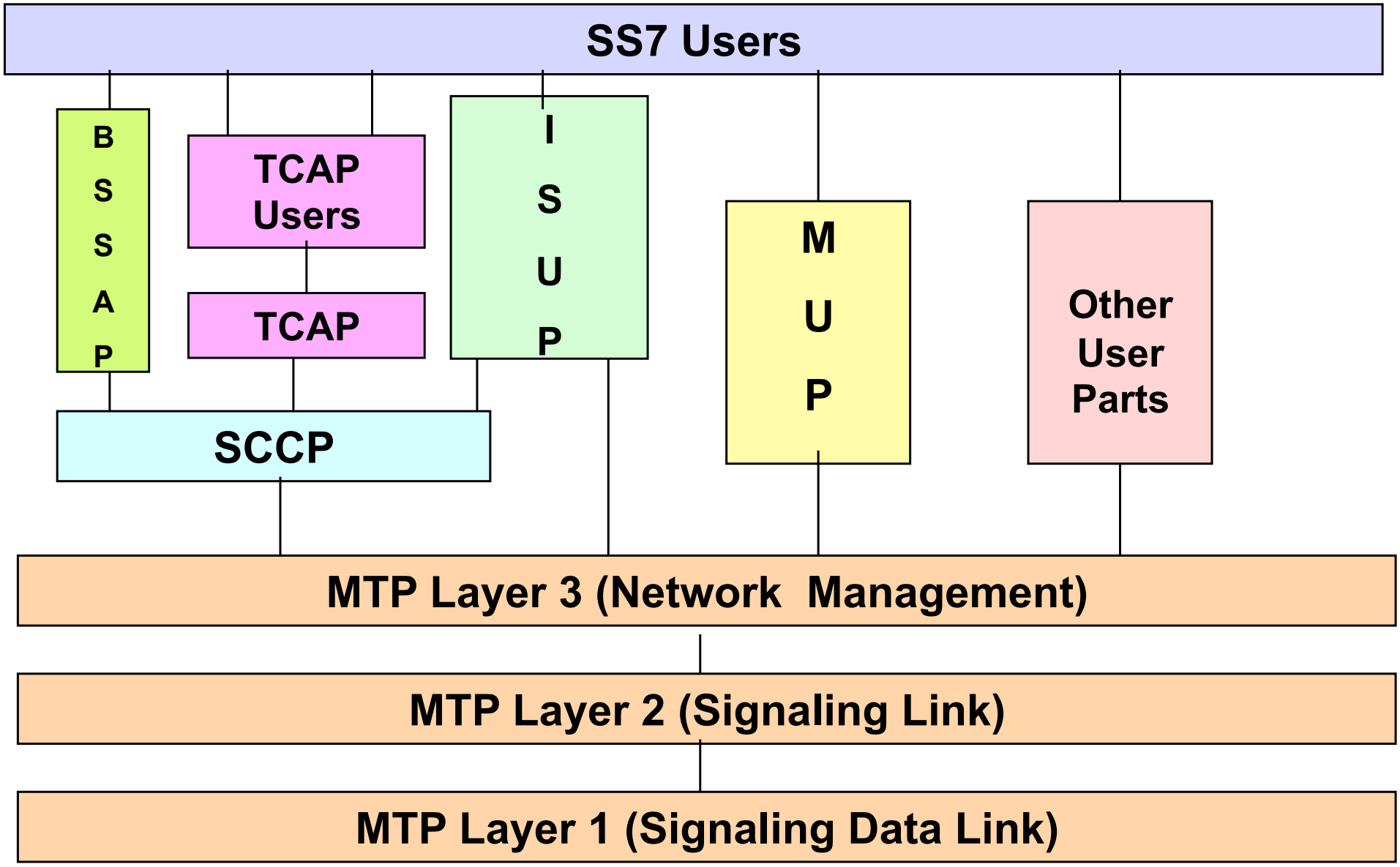


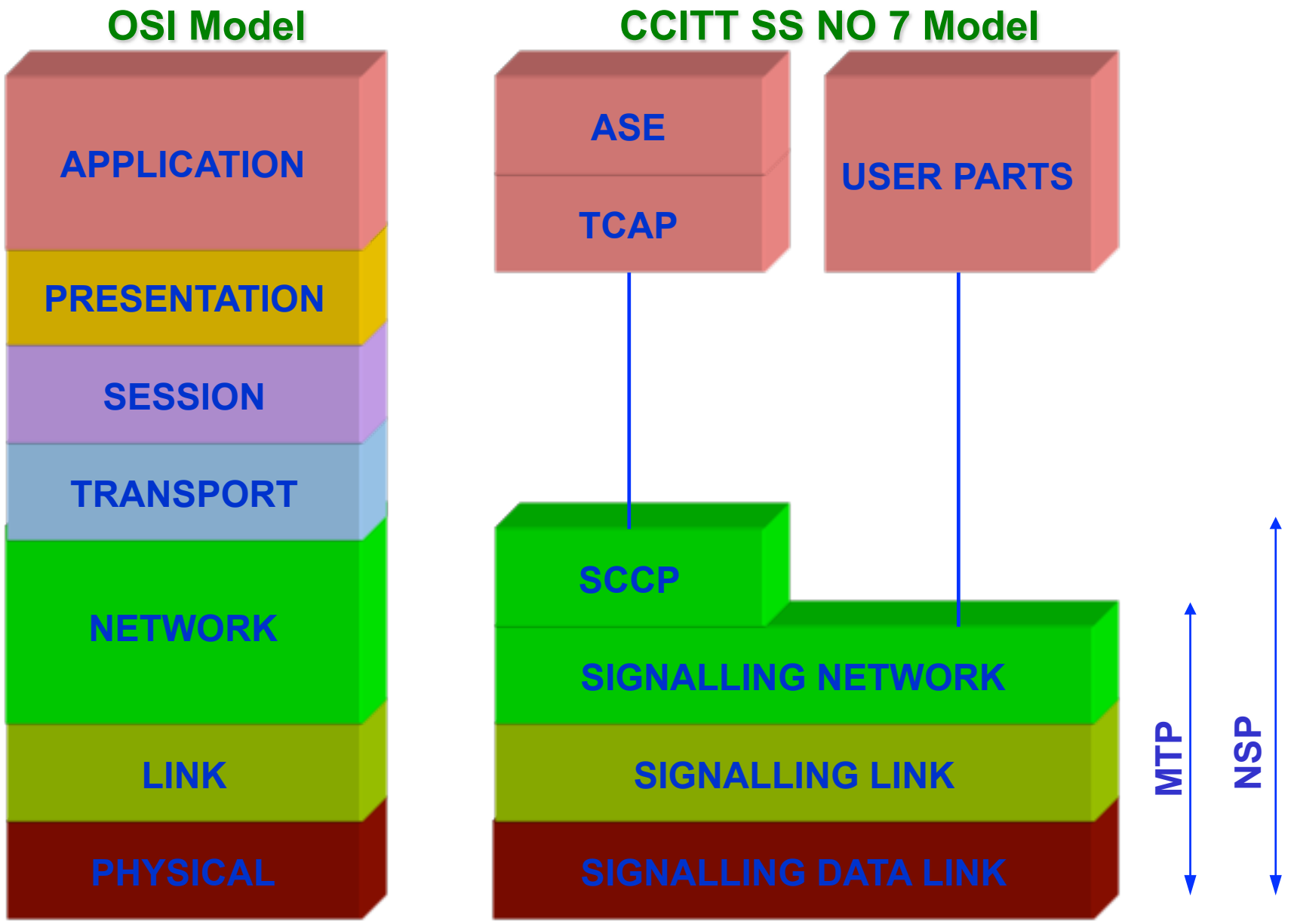
- **Physical Layer**
  - ✓ provides mechanical, electrical, functional, and procedural resources for activating, maintaining, and blocking physical circuits for the transmission of bits between data link layers
  - ✓ contains functions for converting data into signals compatible with the transmission medium
  - ✓ for the communication between only two exchanges
    - Layers 1 and 2 are sufficient
  - ✓ for the communication between all exchanges in the network
    - Layer 3 must be added because it provides addressing and routing



Signaling System No. 7 (SS7)

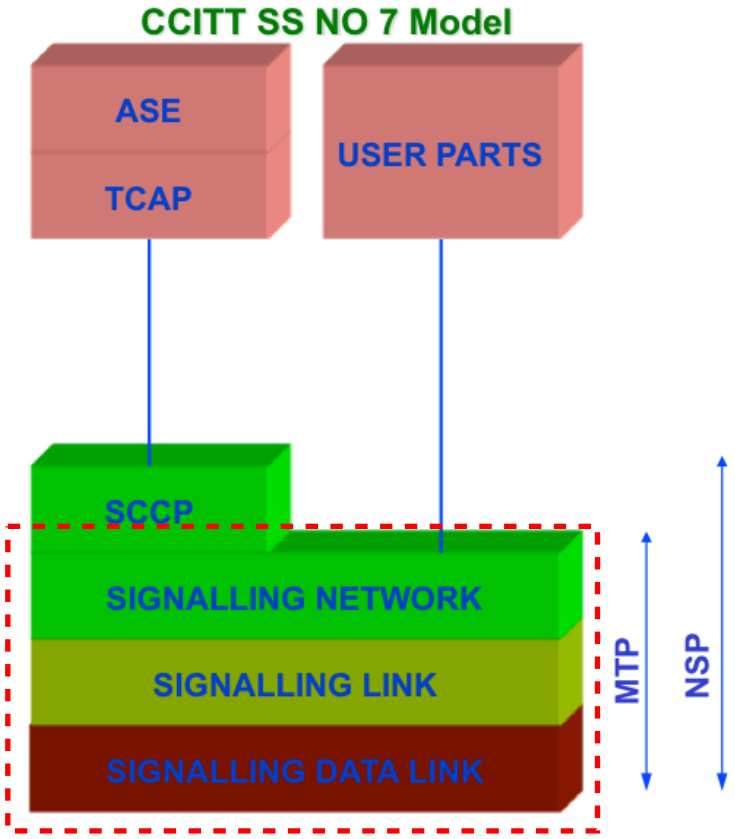
- SS7 is a set of recommendations defining protocols for the internal management of digital networks
- CCITT SS No. 7 is intended primarily for digital networks, both national and international, where the high transmission rates (64 kbps) can be exploited
- The signaling system used in GSM follows the CCITT recommendations


SS7 Users
BSSAP
TCAP Users
TCAP
ISUP
MUP
Other User Parts
SCCP
MTP Layer 3 (Network Management)
MTP Layer 2 (Signaling Link)
MTP Layer 1 (Signaling Data Link)

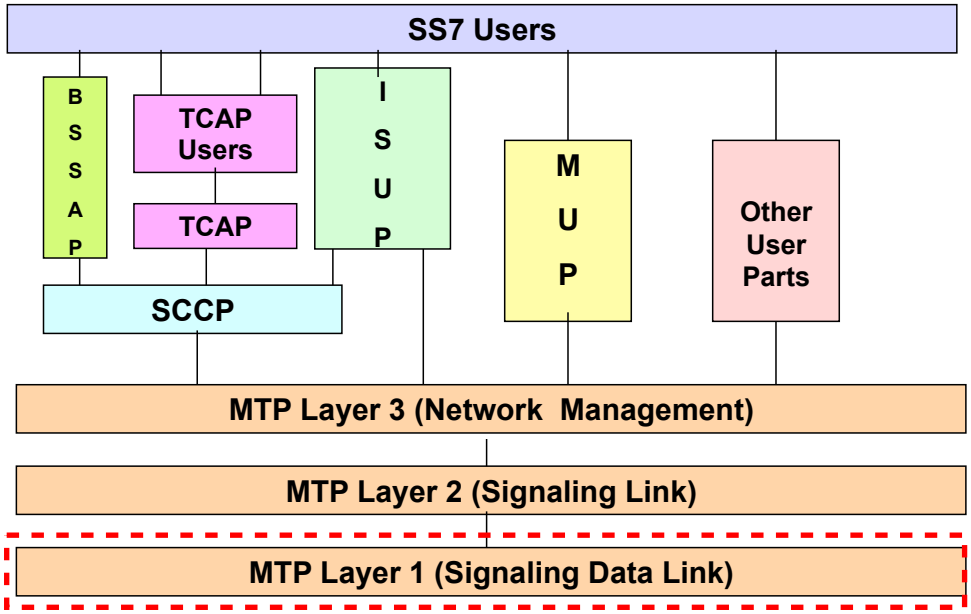

OSI Model
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
LINK
PHYSICAL
CCITT SS NO 7 Model
ASE
TCAP
USER PARTS
SCCP
SIGNALLING NETWORK
SIGNALLING LINK
SIGNALLING DATA LINK
MTP
NSP

Message Transfer Part (MTP)

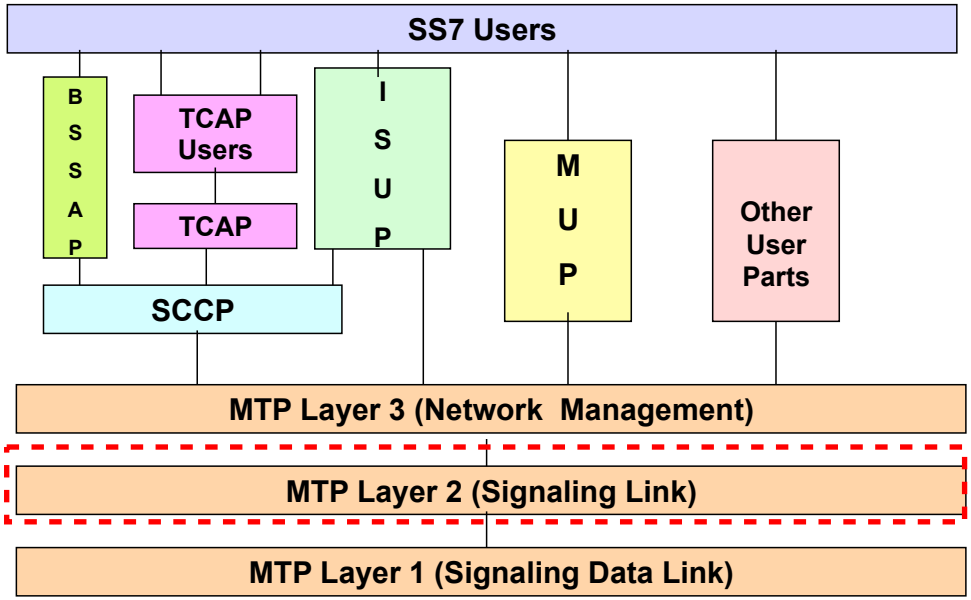
- MTP is used in SS7 by all user parts as a transport system or message exchange
- Messages to be transferred from one user part to another are given to the MTP
- MTP ensures that the messages reach the addressed user part in the correct order without
  - ✓ information loss
  - ✓ duplication
  - ✓ sequence alteration
  - ✓ bit errors



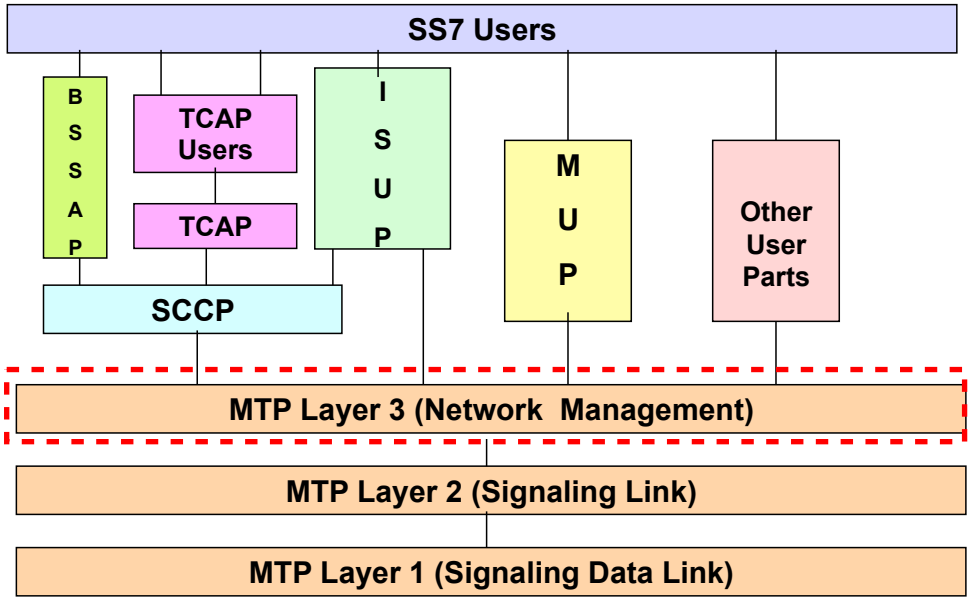
- MTP Level 1 (signaling data link)
  - ✓ defines the physical, electrical and functional characteristics of a signaling data link and the access units
  - ✓ in a digital network, 64 kbps channels are generally used as signaling data links
  - ✓ in addition, analog channels (preferably with 4.8 kbps) can also be used via modems as a signaling data link



- MTP Level 2 (signaling link)
  - ✓ defines the functions and procedures for a correct exchange of user messages via a signaling link
  - ✓ functions
    - delimitation of the signal units by flags
    - elimination of superfluous [多餘的] flags
    - error detection using check bits
    - error correction by retransmitting signal units
    - error rate monitoring on the signaling data link
    - restoration of fault-free operation, e.g., after disruption [破裂] of the signaling data link



- MTP Level 3 (signaling network)
  - ✓ defines the internetworking of the individual signaling links
  - ✓ functions
    - message handling
      - direct messages to the desired signaling link, or to the correct user part
    - signaling network management
      - control of message traffic, e.g., by means of changeover of signaling links if a fault is detected and change back to normal operation after the fault is corrected

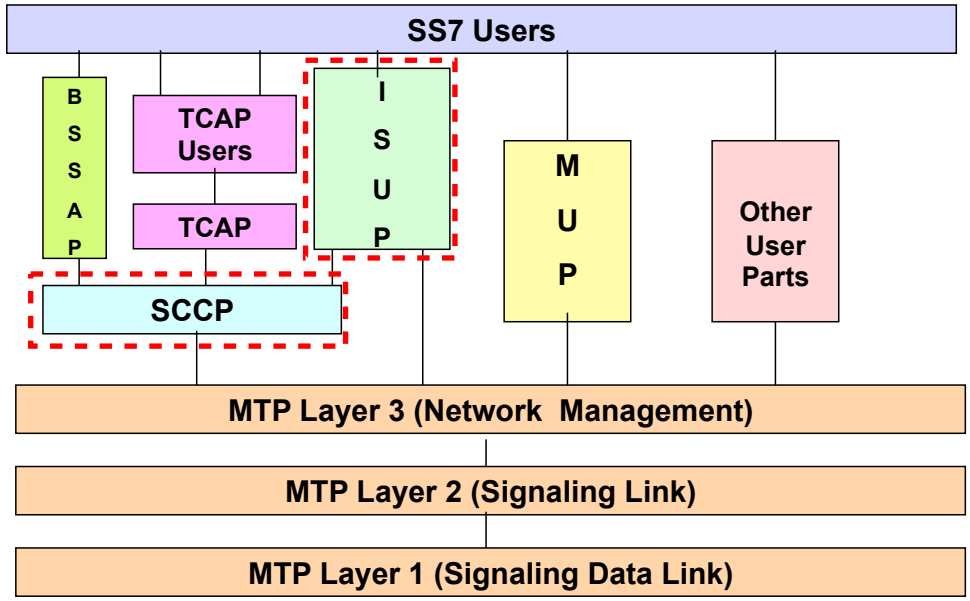


ISDN User Part (ISUP)

- ISUP stands for ISDN User Part
- Integrated Services for Digital Network (ISDN)
  - ✓ a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the PSTN
  - ✓ a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide
  - ✓ it offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kbps

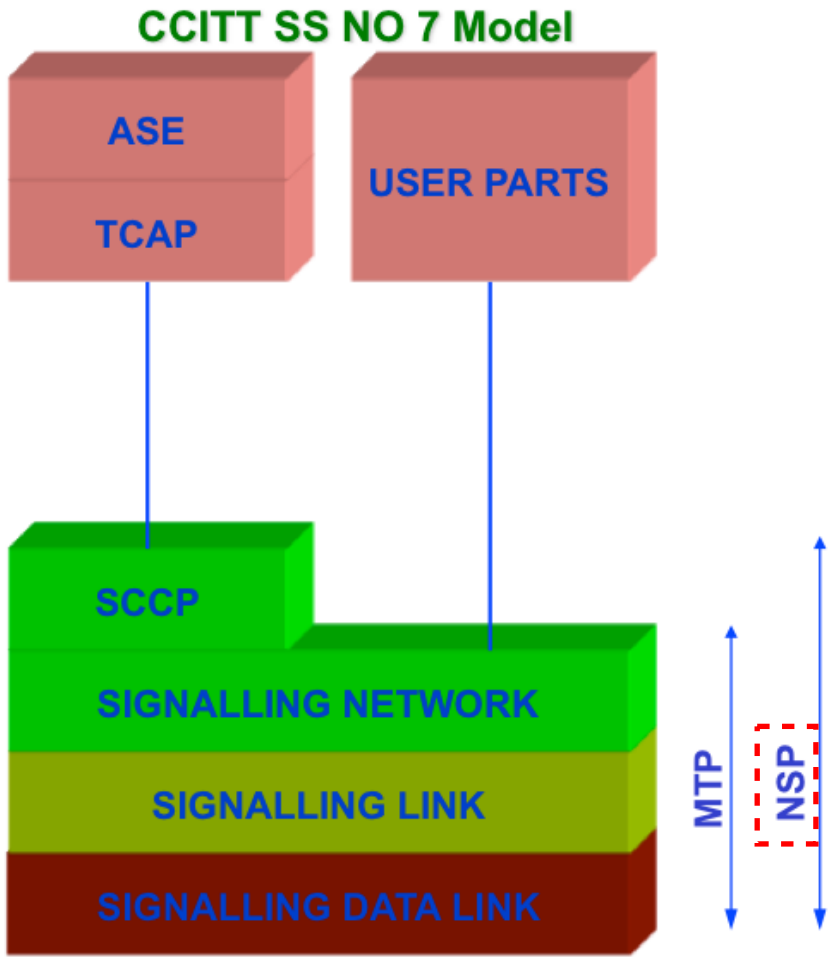
- A major market application for ISDN in some countries is Internet access, where ISDN typically provides a maximum of 128 kbps in both upstream and downstream directions
- Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded
- Basic Rate Interface (BRI, 2B+D, 2B1D)
  - 2 bearer channels (B channels) at 64 kbps each
    - used for voice or user data
  - 1 data channel (D channel) at 16 kbps
    - used for any combination of data, control/signaling, and X.25 packet networking
  - the 2 B channels can be aggregated by channel bonding providing a total data rate of 128 kbps

- ISUP covers the following signaling functions in ISDN
  - ✓ control of calls
  - ✓ processing of services and features
  - ✓ administration of circuits in ISDN
- ISUP has interfaces to MTP and SCCP for the transport of message signal units
- ISUP can use SCCP functions for end-to-end signaling



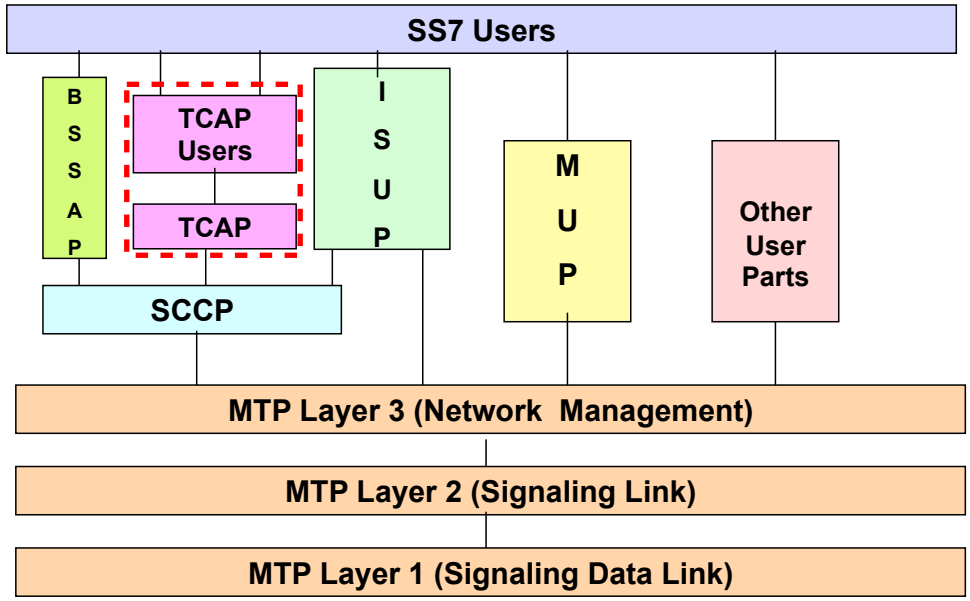
Signaling Connection Control Part (SCCP)

- Used as a supplement to MTP
- Provides additional functions for the transfer of messages between network nodes and between network nodes & other signaling points
- From the point of view of MTP
  - ✓ SCCP is a user with its own service indicator
- Combination of SCCP and MTP is called Network Service Part (NSP)



Transaction Capabilities Application Part (TCAP)

- Defines the messages and protocol used to communicate between applications in nodes
- It is used for
  - ✓ database services such as calling card, 800, and AIN (Advanced Intelligent Network)
  - ✓ switch-to-switch services including repeat dialing and call return
- Because TCAP messages must be delivered to individual applications within the nodes they address, they use the SCCP for transport



- 1. Introduction
- 2. Features of GSM
- 3. Network Components
- 4. Channel Concept
- 5. Coding, Interleaving, Ciphering
- 6. Signaling
- 7. Handover
- 8. Location Update

7. Handover

- GSM handover process uses a mobile assisted technique for accurate and fast handovers to

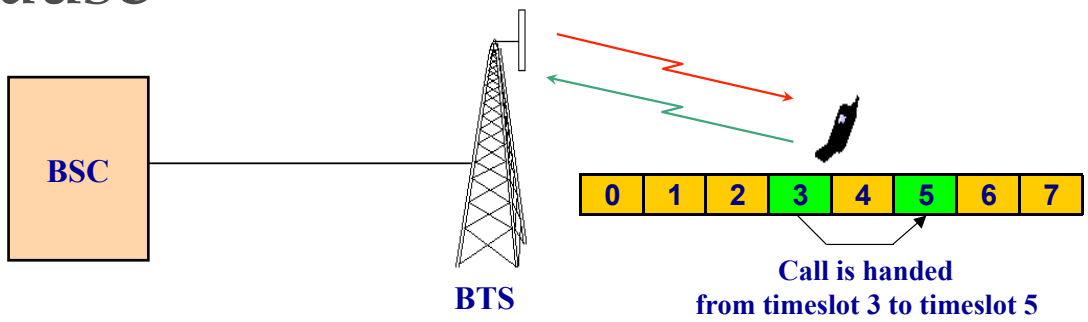
  ✓ maintain user connection link quality

  ✓ manage traffic distribution

- The overall handover process is implemented in MS, BSS & MSC
  - ✓ MS
    - measure radio subsystem downlink performance and signal strengths received from surrounding cells
    - these measurements are sent to BSS for assessment
  - ✓ BSS
    - measures the uplink performance for the MS being served
    - assesses the signal strength of interference on its idle traffic channels
    - perform initial assessment of the measurements in conjunction with defined thresholds and handover strategy
  - ✓ MSC
    - perform assessment requiring measurement results from other BSS or other information resident in MSC

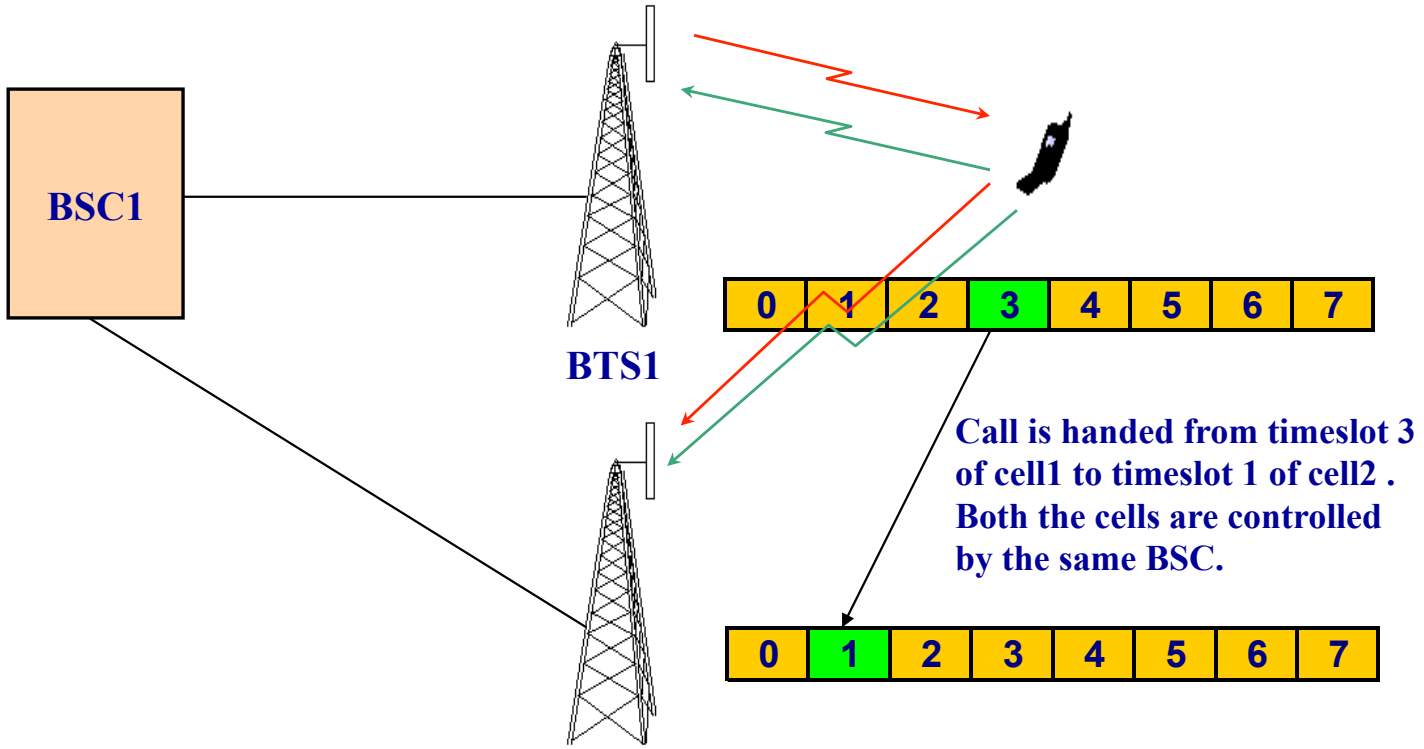
Intra-Cell Handover

- Handover takes place in the same cell from one timeslot to another timeslot of the same carrier or different carriers (but the same cell)
- Intra-cell handover
  - ✓ triggered only if the cause is interference
  - ✓ can be enabled or disabled in a cell



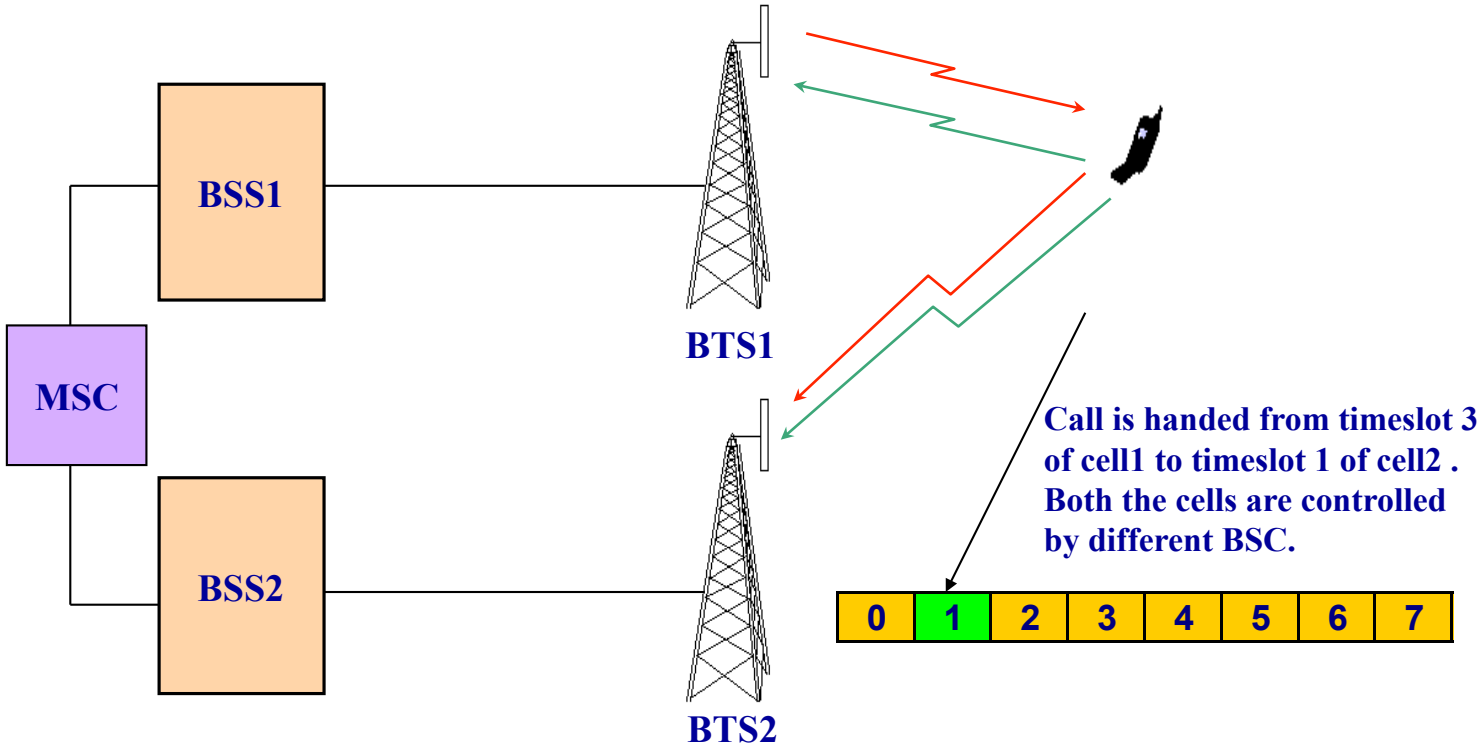
Intra-BSC Handover

- Handover takes place between different cell which are controlled by the same BSC



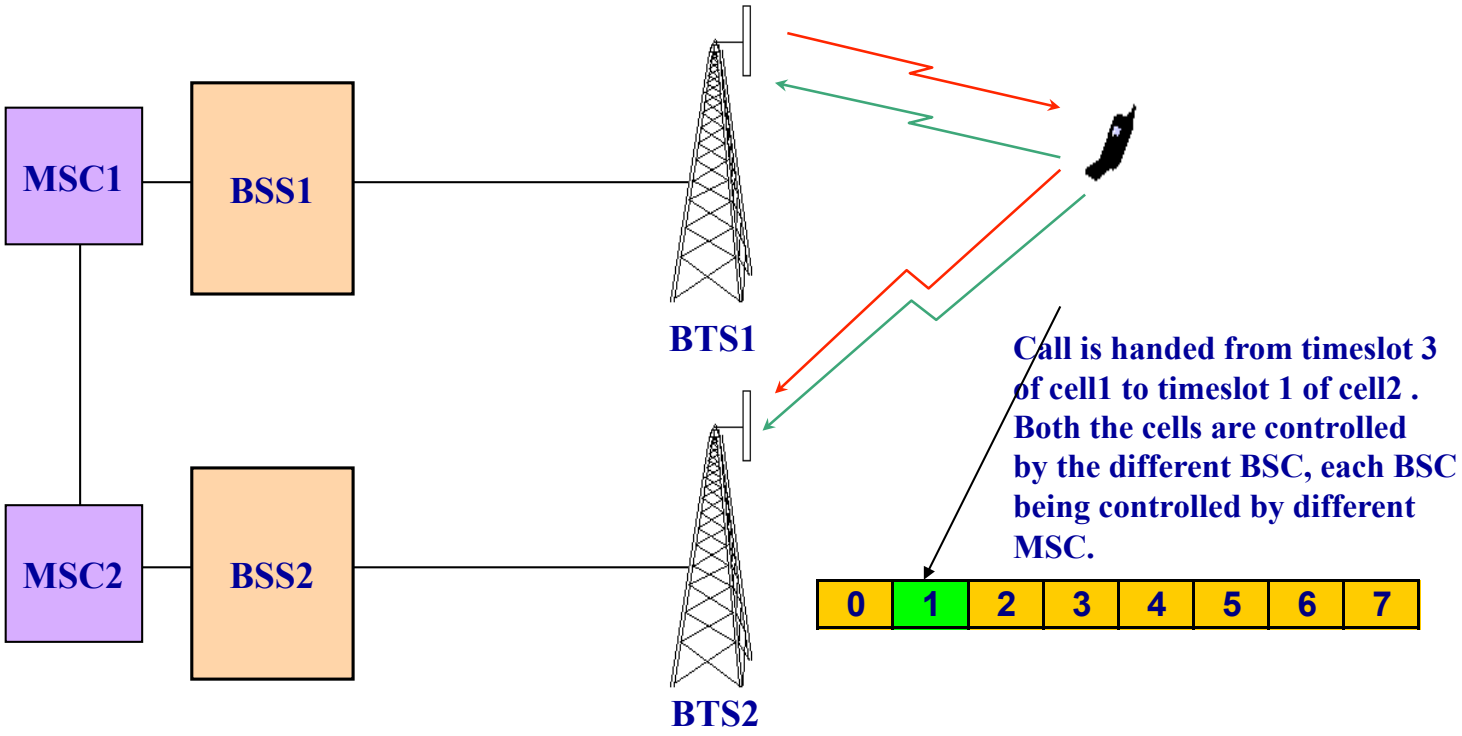
Inter-BSC Handover

- Handover takes place between different cell which are controlled by different BSC



Inter-MSC Handover

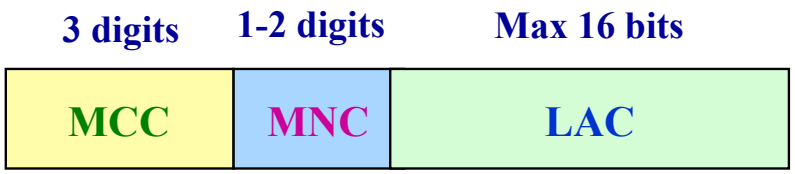
- Handover takes place between different cell which are controlled by different BSC and each BSC is controlled by different MSC



- 1. Introduction
- 2. Features of GSM
- 3. Network Components
- 4. Channel Concept
- 5. Coding, Interleaving, Ciphering
- 6. Signaling
- 7. Handover
- 8. Location Update

8. Location Update

- MSC should always know the location of the MS so that it can contact it by sending pages whenever required
- The mobile keeps on informing the MSC about its current location area or whenever it changes from one LA to another
- This process of informing the MSC is called location update
- The new LA is updated in VLR
- LAI = MCC + MNC + LAC
  - ✓ MCC = Mobile Country Code
  - ✓ MNC = Mobile Network Code
  - ✓ LAC = Location Area Code
    - identifies a location area within a GSM PLMN network
    - max length of LAC is 16 bits (65536 different LAs can be defined in one GSM PLMN)



- Location update types
  - ✓ normal location update
  - ✓ IMSI attach
  - ✓ periodic location update
- Normal location update
  - ✓ mobile powers on and is idle
  - ✓ reads the LAI broadcast on the BCCH
  - ✓ compares with the last stored LAI and if it is different does a location update

- IMSI attach
  - ✓ saves the network from paging a MS which is not active in the system
  - ✓ when MS is turned off or SIM is removed
    - the MS sends a detach signal to the network
    - it is marked as detached
  - ✓ when the MS is powered again it reads the current LAI and if it is same does a location update type IMSI attach
  - ✓ attach/detach flag is broadcast on BCCH sys info.

- Periodic location update
  - ✓ many times the MS enters non-coverage zone
  - ✓ the MSC will keep on paging the MS thus wasting precious resources
  - ✓ to avoid this the MS has to inform the MSC about its current LAI in a set period of time
  - ✓ this time ranges from 0 to 255 decihours [1 decihour = 6 minutes]
  - ✓ periodic location timer value is broadcast on BCCH sys info messages