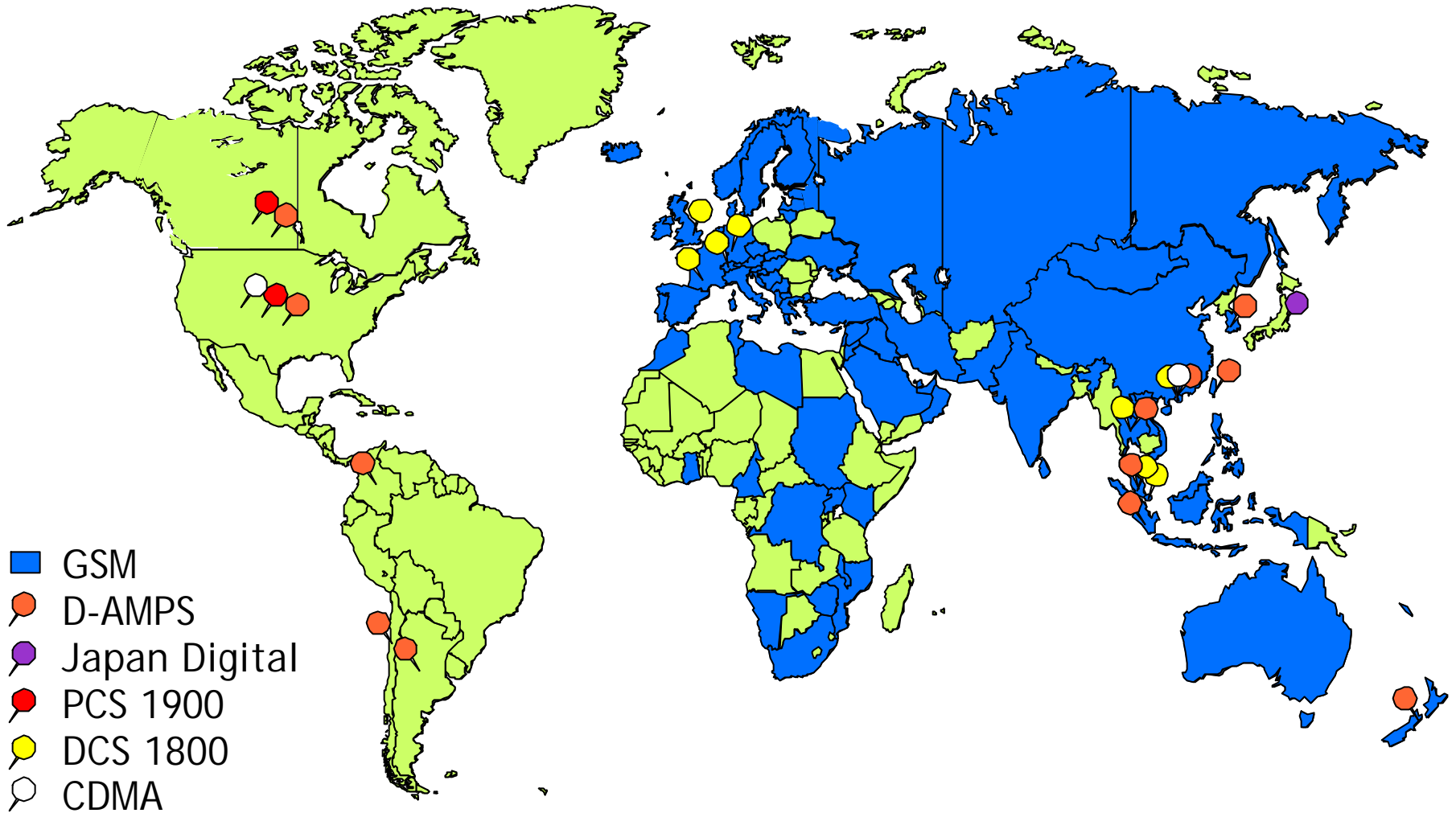

The Global System for Mobile communications (GSM)

Overview

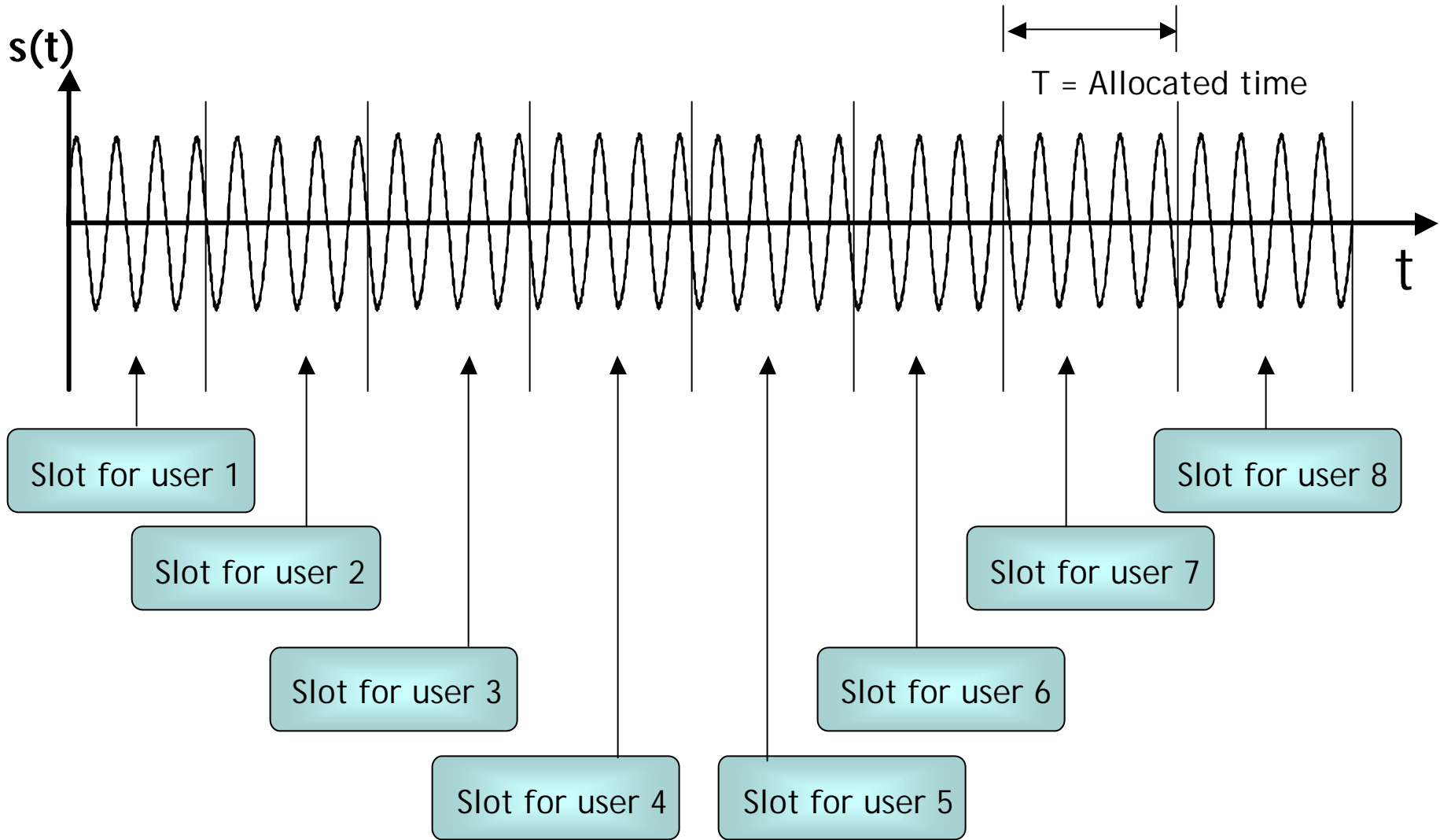
Digital Cellular Systems World-wide



Multiple Access Techniques

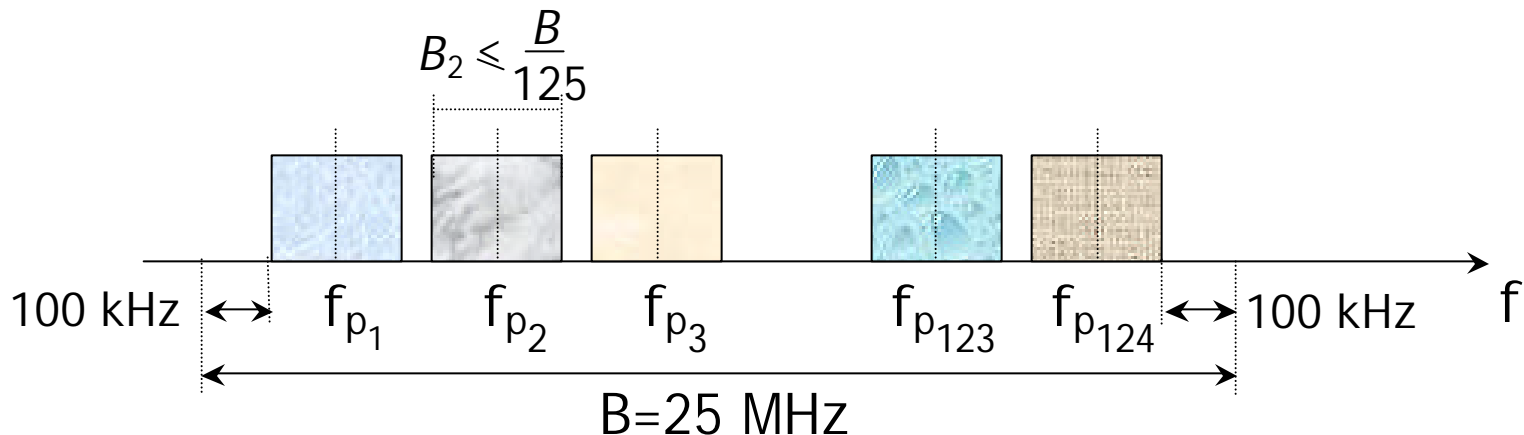
- In the GSM/DCS mobile system each free physical channel can be used by every subscriber and there are not channels permanently dedicated to single user
 - This policy requires the introduction of 2 different techniques for the multiple access
 - ▶ Time Division Multiple Access (TDMA)
 - ▶ Frequency Division Multiple Access (FDMA)
-

TDMA principle



FDMA

- Besides the TDMA in the GSM/DCS we have also the FDMA technique
 - ▶ GSM/DCS is characterised by a hybrid access to the channel
- Each frame of 8 physical channels are multiplexed in the frequency domain
 - ▶ each frame is transmitted in a sub-band of 200 kHz
 - ▶ 124 carriers are available (the last one is not used for limiting the aliasing with other transmission systems)



Carrier Frequency Range

GSM

Uplink: 890 - 915 MHz

Downlink: 935 - 960 MHz

Carrier Pairs (in MHz)

890.0 935.0

890.1 935.1

890.3 935.3

....

914.9 959.9

915.0 960.0

Duplex Frequency = 45 MHz

124 Carriers

DCS

Uplink: 1710 - 1785 MHz

Downlink: 1805 - 1880 MHz

Carrier Pairs (in MHz)

1710.0 1805.0

1710.1 1805.1

1710.3 1805.3

....

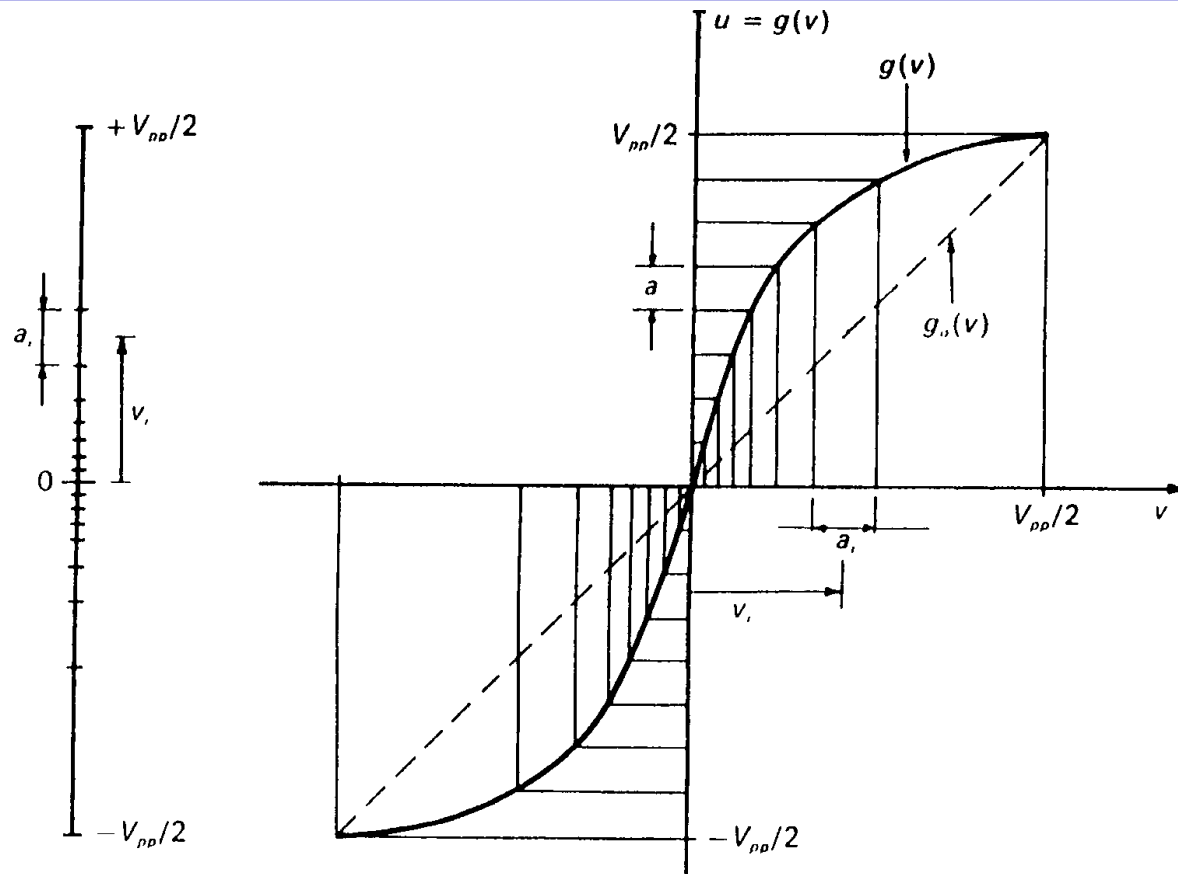
1784.9 1879.9

1785.0 1880.0

Duplex Frequency = 95 MHz

374 Carriers

GSM Quantisation




- It is a logarithmic quantiser
- It uses 13 bits : 2^{13} quantisation levels


Speech Encoder

- In the traditional telephone network the voice signal has a bandwidth ranging between 300 Hz and 3,4 kHz and it is quantised with a bit sequence at 64 kb/s (8 bits/Sampler • 8 kSampler/s)
 - GSM/DCS adopts a speech encoder able to transmit voice with a data rate of 13 kb/s, ensuring at the same time
 - ▶ a voice quality similar to the ETACS standard
 - ▶ high robustness against transmission errors
 - ▶ limited transmission delay
 - ▶ low power consumption
 - ▶ low cost implementation
-

RPE-LTP (1)

- Regular Pulse Excitation/Long Term Prediction is the algorithm used by the GSM/DCS speech encoder
 - It performs an analysis of the voice for 20 ms consecutively
 - the RPE technique tries to reproduce the signal with an equispaced impulse sequence filtered by a specific digital filter whose transfer function in the frequency domain estimates the voice spectrum envelop
 - The speech is digitalised sampling at 8 kHz and quantising with 13 bits
 bit rate of 104 kb/s
-

RPE-LTP (2)

- This signal is then split up in sequences of 160 samples each 20 ms
 - Samples are analysed to evaluate the coefficients of the Linear Predictive Coding (LPC) filter whose transfer function estimates the voice spectrum envelop
 - With the Long Term Prediction algorithm the coding of the samples is accomplished
 - As result we get a burst of 260 bits each 20 ms
 bit rate of 13 kb/s
 - It is foreseen the introduction in a next future of an encoder able to operate at 6,5 kb/s
-

Channel Coding

- Noise, distortion and attenuation through the transmission channel determines a degradation of the signal
 - Using a coding of the transmitted information with the insertion of some redundancy symbols we manage to ensure a higher protection against errors
 - Of course this advantage is paid in terms of a higher number of transmitted bits and a reduction of the bit rate
-

Channel encoders in GSM/DCS

- A cascade of 3 different types of coding are adopted in the GSM/DCS system
 - ▶ parity code
 - ▶ cyclic code (Linear Block Code)
 - ▶ convolutional code
 - Each information sequence of 260 bits is represented with a coded word of 456 bits (260 information bits + 196 coded bits)
 - The required bit rate after the channel encoder is 22.8 kb/s
-

Diagonal Interleaver

- It is a technique usually used in the radio transmission systems in order to reduce the burst errors in single coded word
 - It is performed permuting in a deterministic way the transmission order of bits
 - It allows scattering an eventual burst error determined by the channel over more coded words
 - ▶ this ensures the possibility of a proper correction even of long error sequences
-

GMSK

- This is the modulation adopted in the GSM/DCS system
 - Its main features as all the CPM consists in ensuring a continual phase at each bit period T in the transition from a symbol to the next one
 - It is performed with a FSK modulator with a gaussian filter useful to increase the frequency efficiency
 - ▶ the Power Spectral Density (PSD) of the modulated signal with this filter is characterised by a narrower bandwidth
 - ▶ the aliasing with the adjacent channel is limited
 - The modulated signal has a constant envelope
 - ▶ no problems with the non linear distortion introduced by the HPA
-

Burst and Frame Features

- The length of each burst (time slot) is of $577 \mu\text{s}$
- It includes 156.25 bits
- Each bit has a length of $3,69 \mu\text{s}$
- The length of a frame is

$$577 \mu\text{s} \cdot 8 = 4.615 \text{ ms}$$

- The bit rate required to transmit a frame through the Air Interface is

$$156.25 / 0.577 \mu\text{s} = 270.8 \text{ kb/s}$$

- In each PCM time slot ($125/32 \mu\text{s}$) 8 bits are transmitted
-

Classification of the Bursts (1)

- ❑ Frequency Correction Burst
 - ▶ used just to transmit Frequency Correction Channel (FCCH)
 - ▶ 142 bits are set to "1"

 - ❑ Synchronisation Burst
 - ▶ used to transmit synchronisation information
 - ▶ the training sequence includes a well known sequence of bits

 - ❑ Dummy Burst
 - ▶ it contains no information but only filling bits
-

Classification of the Bursts (2)

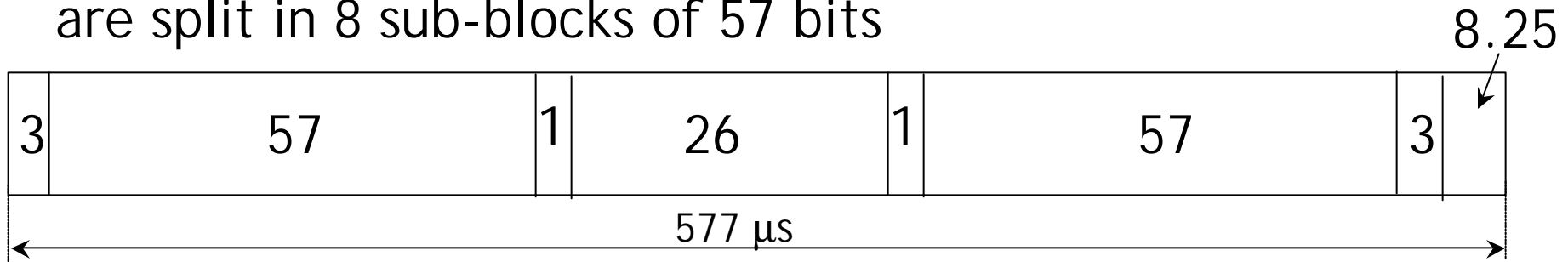
□ Access Burst

- ▶ used to send the Random Access CHannel (RACH) information
- ▶ RACH contains the first message from MS to BTS
- ▶ it has a long guard period to allow BTS to calculate the MS distance from the BTS and to provide timing advance information to MS

□ Normal Burst

Normal Burst

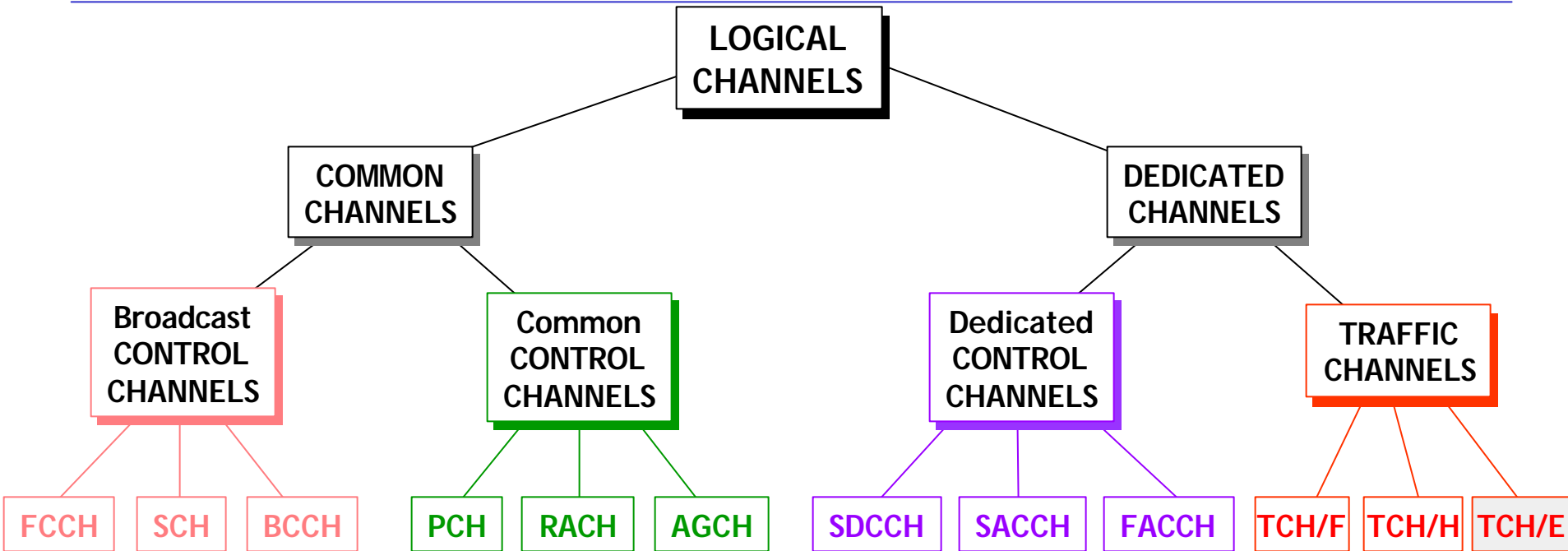
- It is used to transmit both information and control bits
- It involves 156.25 bits
 - ▶ 2 x 3 tailing bits
 - fixed to 0 and used to initialise the Viterbi's equaliser memory
 - ▶ 2 x 57 sequences of information coded bits (payload)
 - ▶ 2 x 1 service bit
 - ▶ 26 bits as training sequence
 - used at the receiver for the equalisation
 - ▶ 8.25 bits as guard period for protection between 2 adjacent TSs
- The 456 information coded bits to be transmitted each 20 ms are split in 8 sub-blocks of 57 bits



Logical Channels

- The physical channels (one timeslot per radio channel) shown in the previous slides represent the entity transmitted through the Air interface
 - Each physical channel is used to transmit a logical channel with different functions
 - Logical channels can be divided in 2 main groups
 - ▶ Traffic Channel (TCH)
 - used to transmit both data and voice payload
 - ▶ Control Channel (CCH)
 - used for signalling and control
-

Logical Channels



FCCH=Frequency Correction CHannel

SCH=Synchronisation Channel

BCCH=Broadcast Control CHannel

PCH=Paging CHannel

RACH=Random Access CHannel

AGCH=Access Grant CHannel

SDCCH=Stand-alone Dedicated Control Channel

SACCH=Slow Associated Control Channel

FACCH=Fast Associated Control Channel

TCH/F=Traffic Channel Full rate

TCH/H=Traffic Channel Half rate

TCH/E=Traffic Channel Enhanced Full rate

Control Channels

- Broadcast Control Channels
 - ▶ broadcasted (wireless point-to-multipoint) by the BTSs
 - ▶ they contains general information about the network
 - ▶ three different types of broadcasted channels are identified
 - Common Control Channels
 - ▶ used to transmit control information for the set up of a point-to-point connection
 - ▶ three different types of common channels are identified
 - Dedicated Control Channels
 - ▶ assigned to a specific connection for signalling exchange (set up, send measurements reports and handover)
 - ▶ three different types of dedicated channels are identified
-

Broadcast Control Channels (1)

🕒 Frequency Correction CHannel (FCCH)

- pure sine wave not modulated, used for the frequency correction
- the MS searches for this channels when it is switched on

🕒 Synchronisation CHannel (SCH)

- after the locking to the frequency the MS synchronises with the SCH and identifies the 6 adjacent BTSs
 - SCH contains
 - the Base Station Identity Code (BSIC) of the BTSs
 - » it is used to measure the strength of the signal broadcasted by the BTSs
 - TDMA frame number (used for ciphering)
-

Broadcast Control Channels (2)

🕒 Broadcast Control Channel (BCCH)

- used to broadcast common information about the BTS to all subscribers located within the coverage area of that specific BTS
 - it is composed by 184 bits
 - it carries the BTS available frequencies
 - list of all frequency carriers used inside a cell
 - it takes the frequency hopping sequence
 - inside a cell the MS can broadcast over different frequencies
 - the order of these changes is called frequency hopping sequence
 - it carries the surrounding cell information
 - information about frequency carriers used in adjacent cells
 - it reports the channel combination
 - it defines how the eleven (twelve) logical channels are mapped into the physical channels (this mapping varies cell by cell)
-

Common Control Channels

- 🕒 Paging Channel (PCH)
 - ▶ BTS uses to page a MS
 - ▶ a downlink channel only

 - 🕒 Random Access Channel (RACH)
 - ▶ MS uses RACH
 - to respond to the PCH
 - to request a dedicated control channel
 - ▶ it can be used for e.g. mobile originated calls
 - ▶ an uplink channel only

 - 🕒 Access Grant Channel (AGCH)
 - ▶ used to answer to a RACH access request and to assign a Stand alone Dedicated Control CHannel (SDCCH)
 - ▶ a downlink channel only
-

Dedicated Control Channels (1)

- 🕒 Stand alone Dedicated Control Channel (SDCCH)
 - ▶ bi-directional channel
 - ▶ used for signalling procedures during
 - transmission of short messages
 - authentication
 - location updates
 - call set up
 - assignment of TCH

 - 🕒 Slow Associated Control Channel (SACCH)
 - ▶ associated at each SDCCH and TCH
 - ▶ used to
 - transmit sometimes short messages
 - transmit measurement reports
 - control MS power
 - time alignment
-

Dedicated Control Channels (2)

- 🕒 Fast Associated Control Channel (FACCH)
 - ▶ used during handover
 - ▶ it is mapped into a TCH
 - ▶ physically replaces one TCH burst each 20 ms of speech (steal mode)
-

Traffic Channels (1)

🕒 Traffic Channel, Full Rate

- ▶ bi-directional channel
- ▶ used for user data transmission
- ▶ user bit rate
 - voice 13 kb/s
 - data 9.6 kb/s, 4.8 kb/s, 0.3 ÷ 2.4 kb/s

🕒 Traffic Channel, Half Rate

- ▶ bi-directional channel
 - ▶ used for data transmission
 - ▶ user data bit rate
 - voice 6.5 kb/s
 - data 4.8 kb/s , 0.3 ÷ 2.4 kb/s
-

Traffic Channels (2)

🕒 Traffic Channel, Enhanced Full Rate

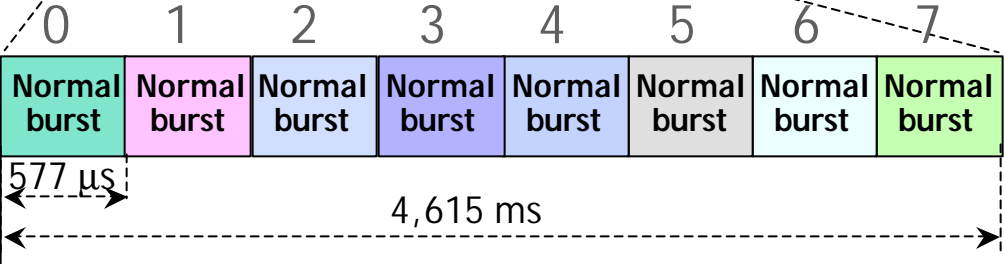
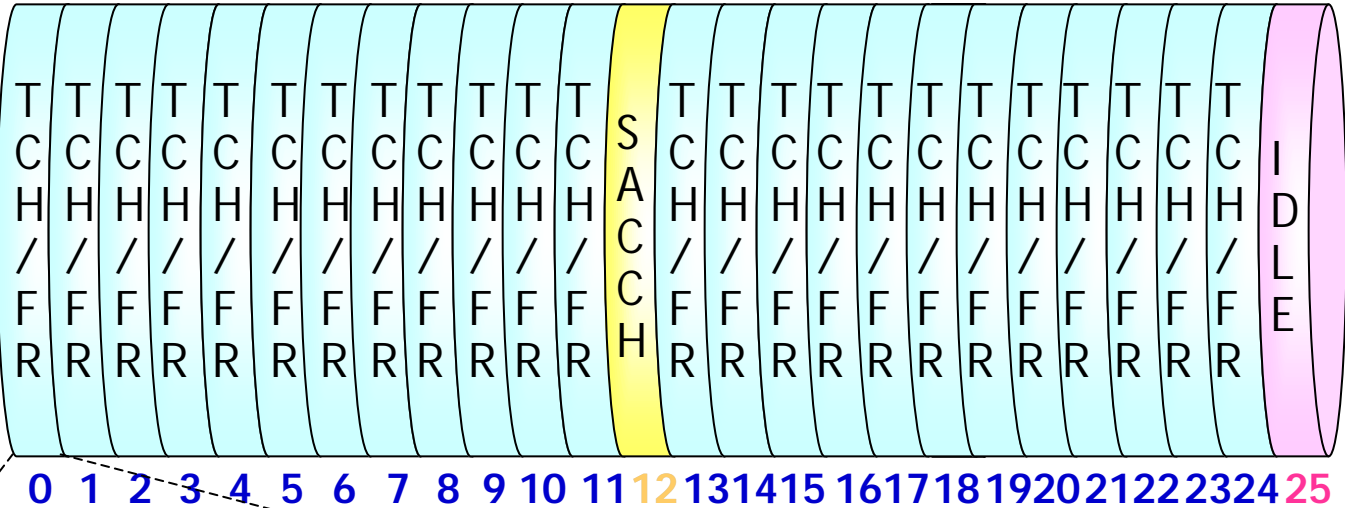
- ▶ bi-directional channel
 - ▶ used for user information transmission
 - ▶ user bit rate
 - voice 13 kb/s
 - it guarantees a better quality compared with the quality ensured by the TC Full Rate
 - data 9.6 kb/s, 4.8 kb/s, 0.3 ÷ 2.4 kb/s
-

Hierarchy of the TDMA frame

- Each TDMA frame can be mapped in 2 different structures
 - ▶ a multiframe of 26 frames
 - used for the voice channels
 - its length is of $4.615 \text{ ms} \cdot 26 = 120 \text{ ms}$
 - ▶ a multiframe of 51 frames
 - used for the signalling and control channels
 - its length is of $4.615 \text{ ms} \cdot 51 = 235.37 \text{ ms}$
 - These multiframe are organised in superframe of $26 \cdot 51$ multiframe for a total length of 6,12 s
 - 2048 superframes are merged in an iperframe
-

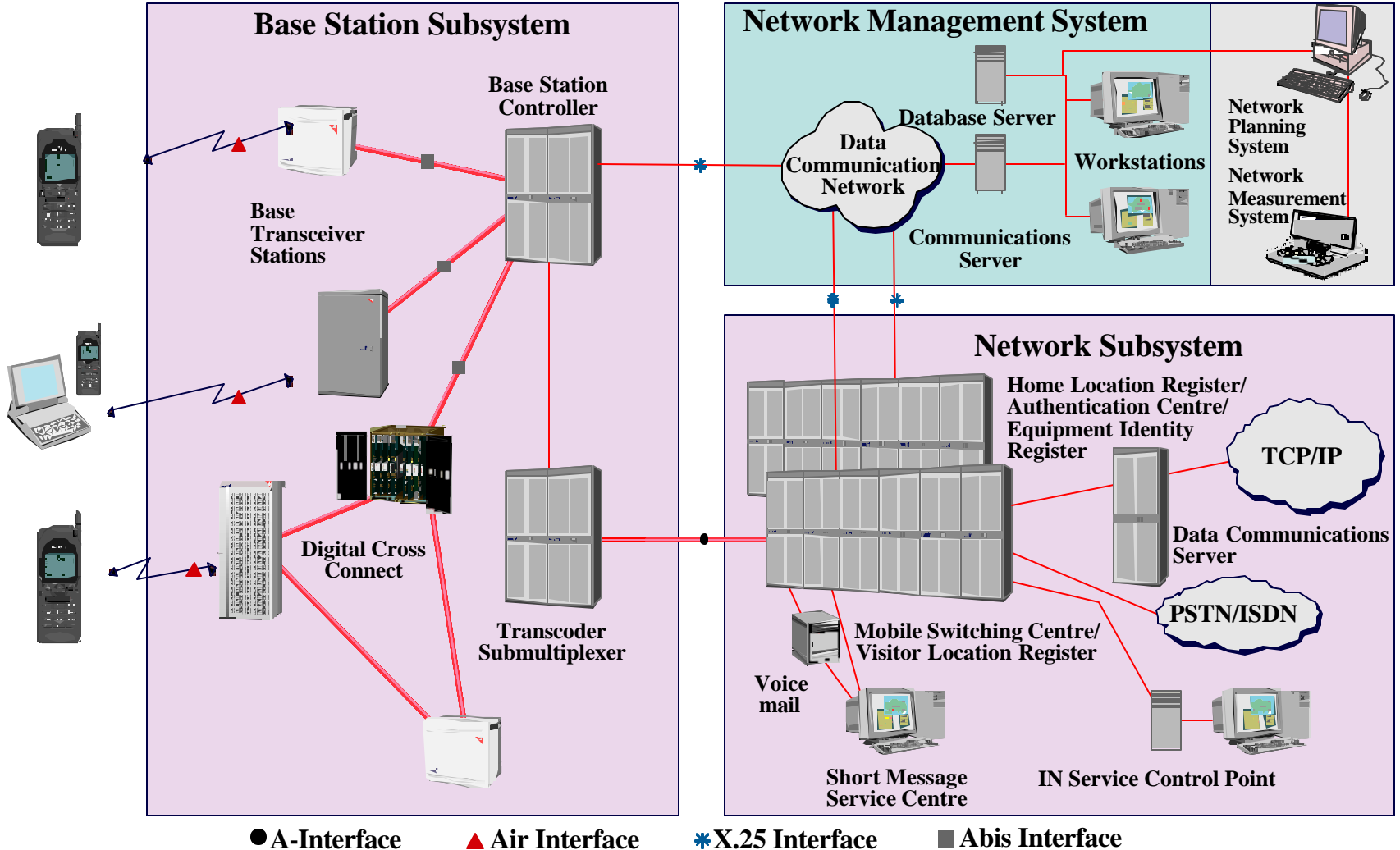
Full Rate Traffic Channel Multiframe

Downlink, Uplink



GSM/DCS Network Architecture

Mobile Stations



MS (1)

- The MS is the equipment required to use the services provided by the GSM network
 - From a portability viewpoint the MS is classified in
 - A.** vehicle mounted station
 - B.** portable station
 - C.** *hand-held station*
 - From a *peak power* viewpoint the MSs are classified in

Class 1	20 W	A. e B.
Class 2	8 W	A. e B.
Class 3	5 W	C.
Class 4	2 W	C.
Class 5	0,8 W	C.
-

MS (2)

- All MSs must be able to vary their emission power with a command driven by the BTS
 - From a functional viewpoint each MS can be identified as a whole of the
 - ▶ Mobile Equipment (ME) or Mobile Termination (MT)
 - ▶ Terminal Equipment (TE)
 - ▶ Terminal Adapter (TA)
 - ▶ Subscriber Identity Module (SIM)
-

Mobile Equipment (or MT)

- It carries out all functions related to
 - ▶ voice coding/decoding
 - ▶ channel coding
 - ▶ transmission over the radio interface
 - ▶ ciphering
 - ▶ management of
 - the radio channel
 - the signalling
 - the mobility
 - Each ME is identified univocally by an International Mobile Equipment Identity (IMEI) code
-

Terminal Equipment

- It is an user terminal represented by one or more devices connected to a ME
 - ▶ data terminal
 - ▶ telex
 - ▶ fax machine
 - TE can be classified basing on the type of its interface
 - ▶ TE1 whether the interface is ISDN compliant
 - ▶ TE2 if the interface is not ISDN compliant (V.24/V.28, X.21, X.25, ...)
-

Terminal Adapter

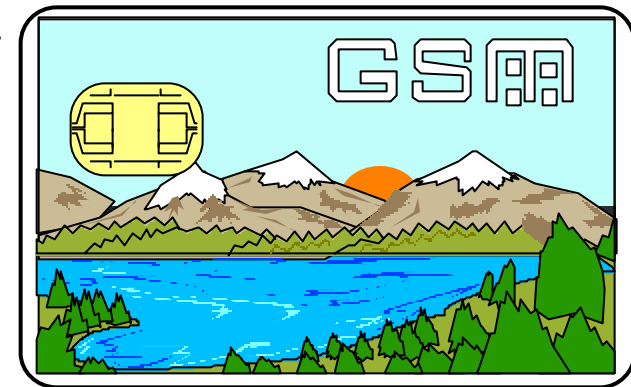
- It is used as a gateway between the TE and the ME
 - It is required when the external interface of the ME follows the ISDN standard and the TE presents a terminal-to-modem interface
-

SIM

- It is basically
 - ▶ a removable smart card in compliance with the ISO 7816 standard
 - ▶ a plug-in module (25 x 15 mm)
 - It includes a Motorola microprocessor 6805 with all the subscriber-related information
 - The interface between the SIM and the other components of the ME (SIM-ME interface) is fully defined in the Technical Specifications
 - SIM (and consequently MS) is protected by a Personal Identification Number (PIN)
 - It has a PIN Unblocking Key (PUK) used to unblock it
-

Information stored in a SIM card (1)

- Serial number
- International Mobile Subscriber Identity (IMSI)
- Security authentication and cyphering information
 - ▶ A3 and A8 algorithm
 - ▶ K_i , K_c
- Temporary Network information (LAI, TMSI)
- List of services subscribed by the user
- Personal Identity Number (PIN)
- Personal Unblocking Number (PUK)



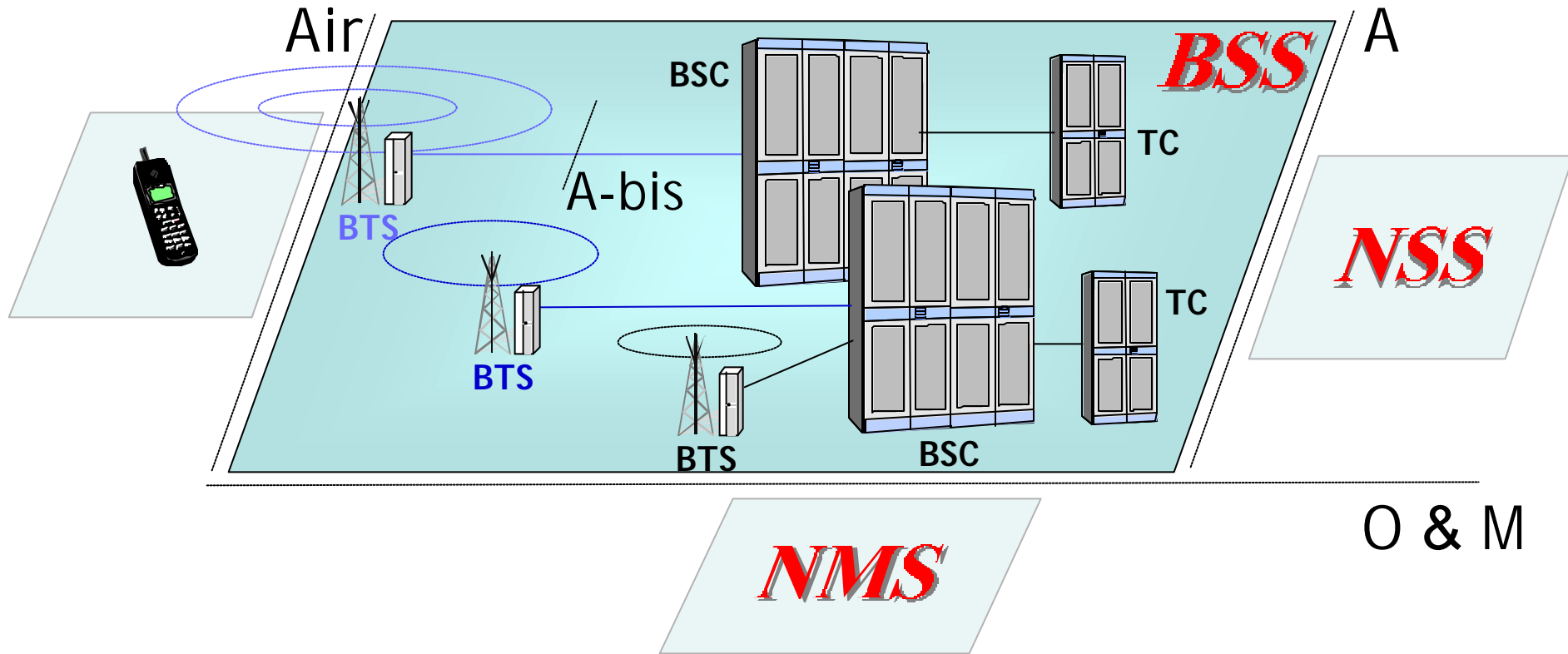
Information stored in a SIM card (2)

- Access rights
 - Prohibited networks
 - Call messages
 - Phone numbers
-

BSS

- BSS includes the network elements taking care of the radio cellular resources within the GSM network
 - On one side, it is directly linked to the MSs through the radio interface (Air interface)
 - On the other side it is interconnected with the switches of the NSS
 - ▶ its role consists in connecting MS and NSS and hence in connecting the caller to the other users
 - It is controlled by the NMS (or OSS)
-

BSS Elements



Base Transceiver Station (BTS)

Base Station Controller (BSC)

Transcoder (TC)

BSS Functions

- Radio path control
 - Air and A interface signalling
 - BTS and TC control through the BSC
 - Hierarchical synchronisation
 - ▶ MSC synchronises BSCs and each BSC further synchronises the controlled BTSs
 - Mobility management
 - ▶ different cases of handovers
 - Speech transcoding
 - Acquisition of statistical data
-

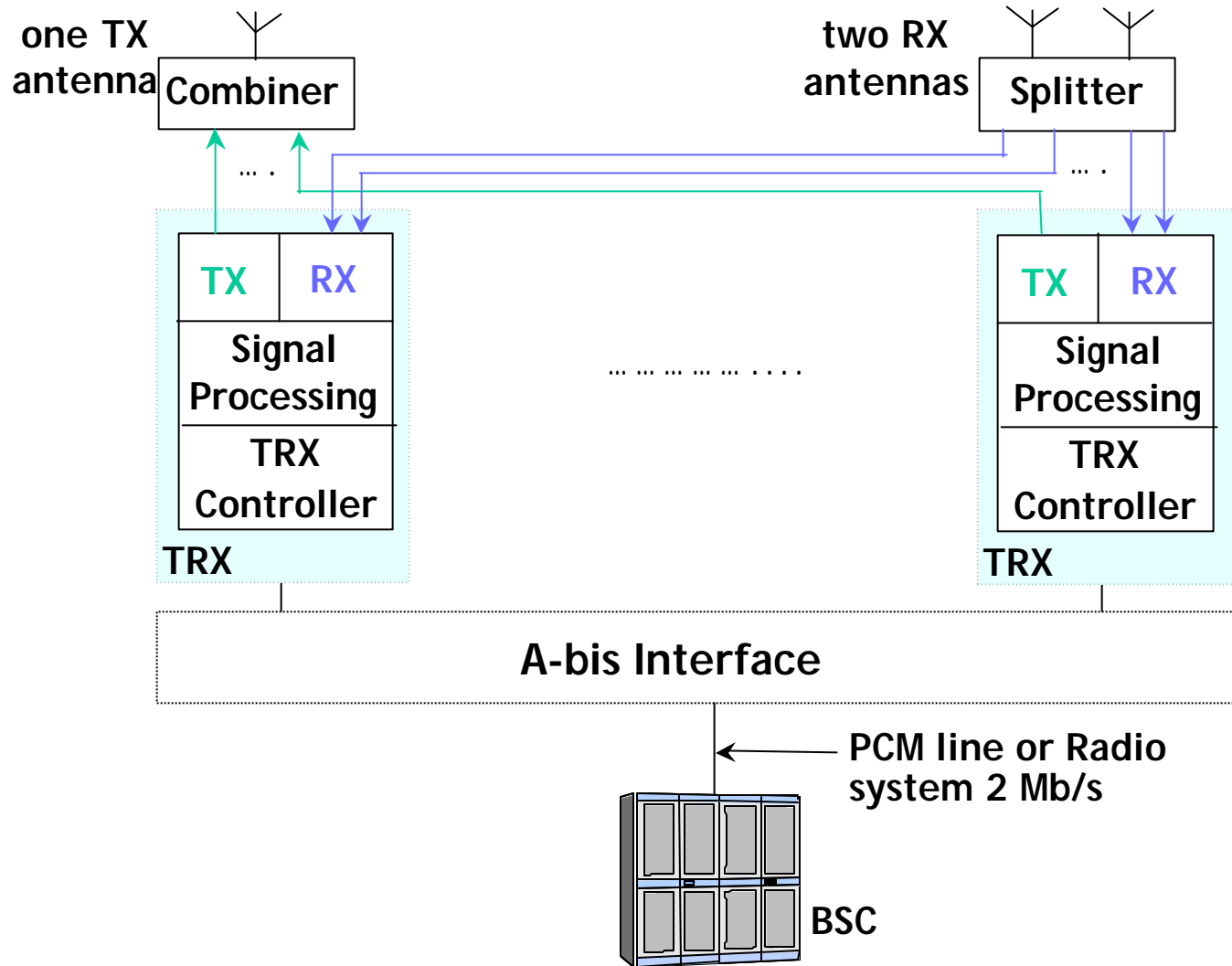
BTS

- BTS is a network element with transmission and reception devices (transceivers) to and from the MS, including
 - ▶ antennas
 - ▶ signal processing specific devices for the Air interface management
 - It can be considered as a complex radio modem controlled by the BSC
 - It is involved also in the transmission and reception with the BSC through the A-bis interface
 - It has just executive functions (no management)
-

BTS Functions

- Broadcast/receive to/from the MS either signalling and traffic signals
 - Perform source and channel coding
 - Modulate/Demodulate signals to be broadcasted/received through the Air interface radio channel
 - Multiplex the information to be transmitted over each carrier
 - Measure the quality of the signalling and traffic signals in the downlink and uplink channels
 - Transmit/receive signalling and traffic signals to/from the BSC through the A-bis interface
-

BTS Scheme



BSC

- It is the second canonical element of the BSS with management tasks
 - On one side it is connected to several BTSs and on the other to the NSS (MSC) through the A interface
 - It controls the radio network
 - It can be considered as a small switching exchange
-

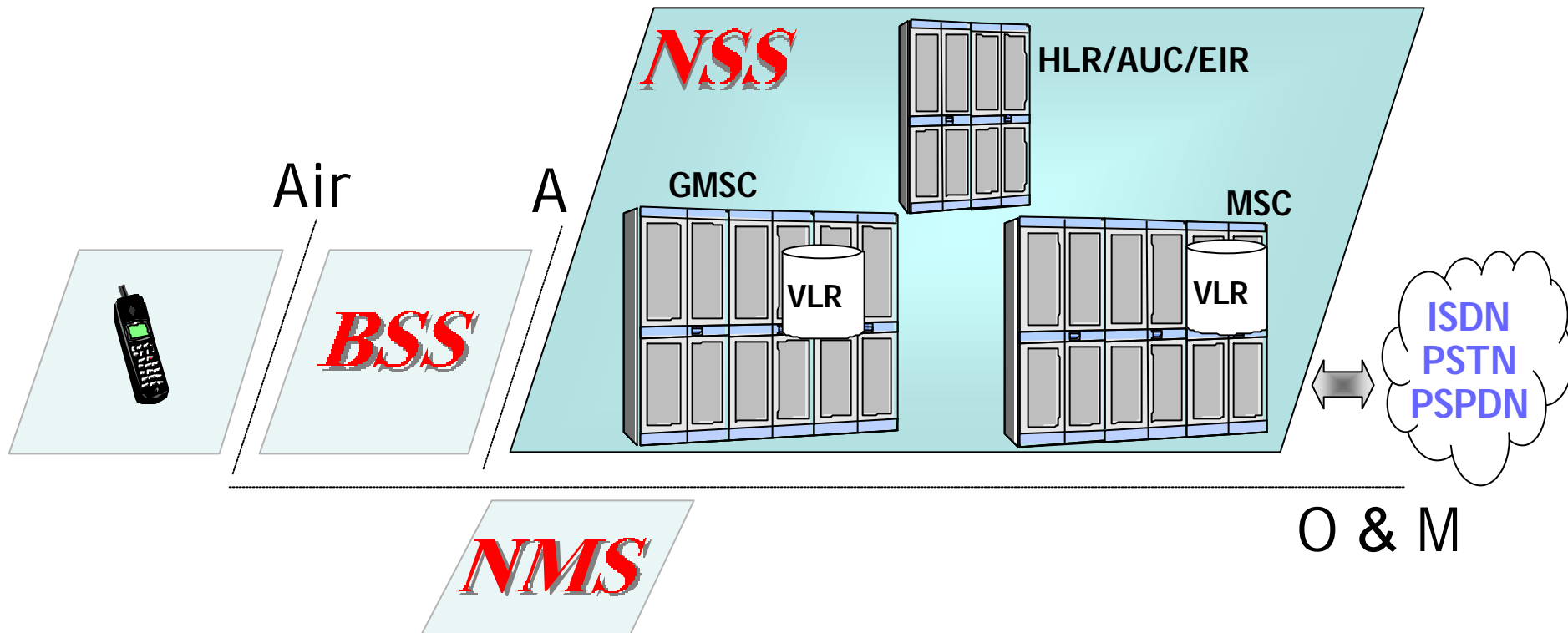
BSC Functions

- Control and supervise the BTSs
 - Configure each cell with the allocation and the release of traffic and signalling channels
 - Manage the paging operation
 - Collect the signals quality measures acquired by the BTSs over the downlink and uplink channels
 - Manage all the radio interfaces
 - Manage the handover procedures
 - Transcode and Sub-multiplex the bit stream
 - Operate and sustain the whole BSS
-

NSS

- The Network and Switching Sub-system includes the main switching functions of the GSM network
 - It directly interoperates with external networks (PSTN, ISDN, PSPDN)
 - In the NSS, databases for the subscriber data and mobility management are installed
 - A further function consists in managing the communication between the GSM subscriber and other telecommunication network users
-

NSS Elements



- Mobile services Switching Centre (MSC) or Gateway MSC
- Visitors Location Register (VLR)
- Home Location Register (HLR)
- Authentication Centre (AUC)
- Equipment Identity Register (EIR)

NSS Functions (1)

- Call control
 - ▶ identification of the subscriber
 - ▶ establishing a call and release of the connection after the call is over
 - Mobility management
 - ▶ taking care of the location of the subscribers before, during and after a call
 - Collecting the charging information about a call
 - ▶ number of the caller and of the called subscriber
 - ▶ length and type of the provided services
 - ▶
-

NSS Functions (2)

- Transfer the acquired charging information to the Billing centre
 - Signalling with other networks and BSS through the different interfaces
 - Subscriber data handling
 - ▶ Data storage permanently or temporarily in some databases
-

MSC

- The MSC main scope consists in performing switching functions
 - It co-ordinates the setting-up of the call to and from the GSM users located in the area of its competence
 - It controls more BSCs
 - MSC has interfaces with BSS on one side and with the external networks on the other side
 - ▶ the interface with external networks requires a gateway (GMSC) for adaptation
-

GMSC

The Gateway MSC is able to route calls coming from

- ▶ MSCs of other PLMN
 - ▶ PSTN and ISDN switching exchanges
-

VLR

- VLR is charge of temporarily storing subscription data for those MSs currently present within its coverage area
 - ▶ International Mobile Subscriber Identity (IMSI)
 - ▶ Mobile Subscriber ISDN (MSISDN)
 - ▶ supplementary services subscribed
 - ▶ authentication and ciphering parameters
 - ▶ Location Area Identity (LAI)
 - VLR keeps location registrations and updates as long as subscriber is within its coverage area
 - It is always associated with one or more MSCs
-

HLR

- It stores the static subscriber information relevant to the provision of the telecommunication services
 - ▶ independently of the current location of the MS
 - These data are permanently stored
 - The only temporary data regards the dynamic data, variable in real time
 - ▶ LAC identifying the LA where is currently the MS
 - ▶ parameters of the new subscribed supplementary services
 - It is able to handle roughly a hundred thousand subscribers' data
-

HLR Functions

- HLR must recognise the VLR identification number for the MS location
 - Update this field in its database
 - Send the routing information (Mobile Station Roaming Number - MSRN) to the requesting GMSC
 - Enable and disable the supplementary services
 - Store and provide the authentication and ciphering triplets to the requesting VLR
 - Manage the subscriber's data
 - Manage the user password for the "Call Barring" supplementary service
-

Mobile Station Roaming Number

- The MSRN format is the same as MSISDN, but it is temporary
 - $MSRN = CC + NDC + SN$
 - ▶ CC = Country Code
 - ▶ NDC = National Destination Code
 - ▶ SN = Subscriber Number
 - SN points to a database
 - ▶ in case of MSISDN located in the HLR
 - ▶ in case of MSRN stored temporarily in the VLR
 - MSRN includes sufficient information to enable the GMSC to route the call to the target MSC
-

AUC

- It is the GSM functional unit managing the authentication and ciphering procedures of the information broadcasted through the radio channel
 - It creates for each subscriber the required triplet for the ciphering
 - ▶ RANDom number (RAND)
 - ▶ Signed RESponse (SRES)
 - ▶ ciphering key K_c
 - AUC stores the authentication key K_i (32 hexadecimal digits) protecting with an encryption algorithm
-

EIR

- The Equipment Identification Register main goal consists in storing the International Mobile Equipment Identity (IMEI)
 - EIR is a database installed in the NSS allowing at the GSM network to verify the authorisation of the active MEs
 - ▶ White list
 - include the IMEIs allocated to all approved MEs
 - ▶ Grey list
 - include IMEIs of faulty MEs, whose fault is not important enough to justify plain barring
 - include IMEIs of non homologated MEs (optional)
 - ▶ Black list
 - include the range of IMEIs related to stolen MEs and not authorised to access to the network
-