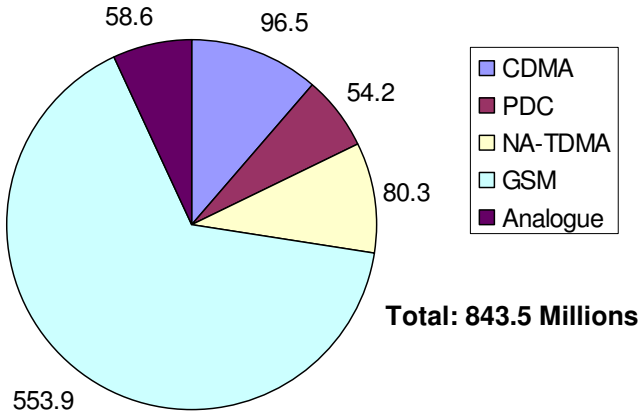
Cellular Subscribers Worldwide (June 2001)

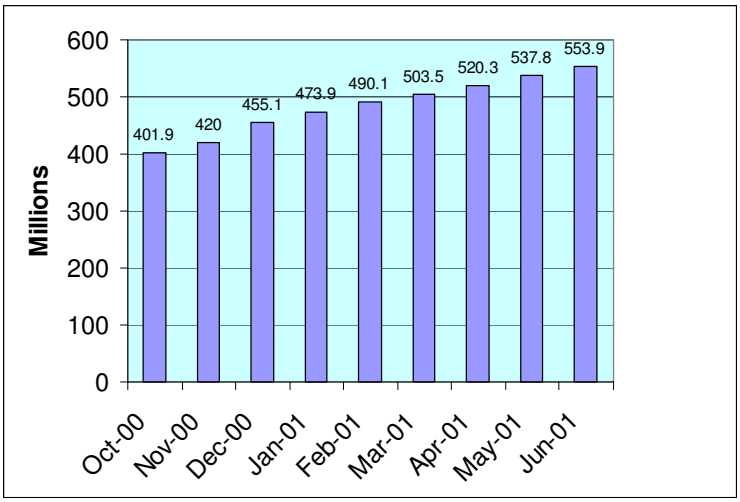


Total: 843.5 Millions

Number of GSM subscribers has reached 1 billion in Jan 2004, in over 200 countries

Source: www.gsmworld.com

GSM World Subscribers Growth



3

Source: www.gsmworld.com

GSM History

- In early 1980s, there were many incompatible cellular systems in Europe
- Standardization activities started in 1982
  - Started as *Groupe Special Mobile* in the 1982 CEPT (Conference of European Posts and Telegraphs)
  - Changed to ***G**lobal **S**ystem for **M**obile Communications*
  - Administered by ETSI (European Telecommunications Standardization Institute) since 1989
- Commercially launched in 1992 in Europe (900 MHz)
  - Later systems: 1800 MHz (GSM 1800)
- Launched in the US in 1996 (PCS band, 1900 MHz)
- Pan-European standard but deployed globally

4

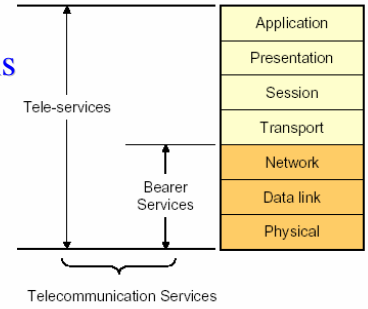
Objectives

- Total mobility
  - Automatic roaming and handoff across many networks and countries
- Security
- Compatible with PSTN networks
  - ISDN
- Efficient use of frequency spectrum
- High speech quality
- Low terminal and service costs
  - Open interfaces (specifications documents more than 5000 pages)
- Broad speech and data services offerings

5

Services Offered by GSM

- Follows ITU-T definitions
- Tele Services
  - Telephony, Emergency
  - SMS
  - Data Services
  - …
- Bearer Services
  - Digital data transport: 2.4, 4.8 and 9.6 kbps
- Supplementary Services
  - Call forwarding etc…



6

GSM Identifiers

- Mobile Subscriber ISDN Number (MSISDN)
  - Actual phone number (ITU's E.164)
  - Strict separation between subscriber identification (IMSI) and phone number (MSISDN)
  - Several MSISDNs can be assigned to a single IMSI (for service selection)
  - The mapping between MSISDN and IMSI is not public
- International Mobile Subscriber Identifier (IMSI)
  - Unique subscriber identification, stored in the SIM-card
- International Mobile Equipment Identifier (IMEI)
  - Unique identification number of the MS

7

GSM Identifiers - cont

- Temporary Mobile Subscriber Identity (TMSI)
  - Temporary assigned to the MS by the VLR - unique within the VLR
  - LAI combined with TMSI uniquely identifies MS within the network
  - Eliminates the need to transmit subscriber identity
- Mobile Station Roaming Number (MSRN)
  - Unique local ISDN number used for mobile terminating calls
- Location Area Identity (LAI)
  - To identify a location area
  - For mobility management

8

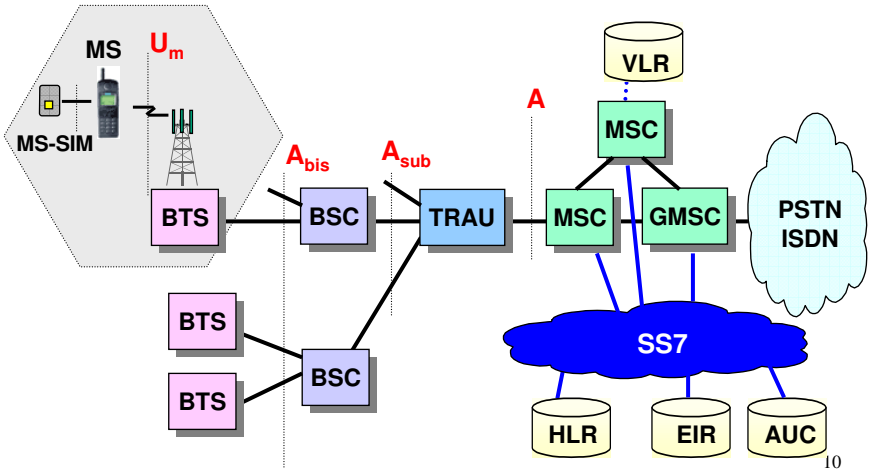
GSM Network Elements

PLMN
(Public Land Mobile Network)

PLMN contains the following elements:

- SIM Subscriber Identity Module
- MS Mobile station
- BTS Base transceiver station
- BSC Base station controller
- TRAU Transcoding rate adaptation unit
- MSC Mobile Switching Center
- VLR Visitor location registry
- HLR Mobile location registry
- EIR Equipment Identification registry

Network Architecture



10

The Base Station Subsystem BSS

- *Base Transceiver Station* (BTS)
  - Radio frequency domain processing
  - Radio Resource Management
- *Base Station Controller* (BSC)
  - Control several BTSs
  - Interface with the MSC
  - Call processing & intra-BSC handover
- *Transcoding and Rate Adaptation Unit* (TRAU)
  - Conversion between PCM and GSM-codec output
  - Bit rate adaption of data channels

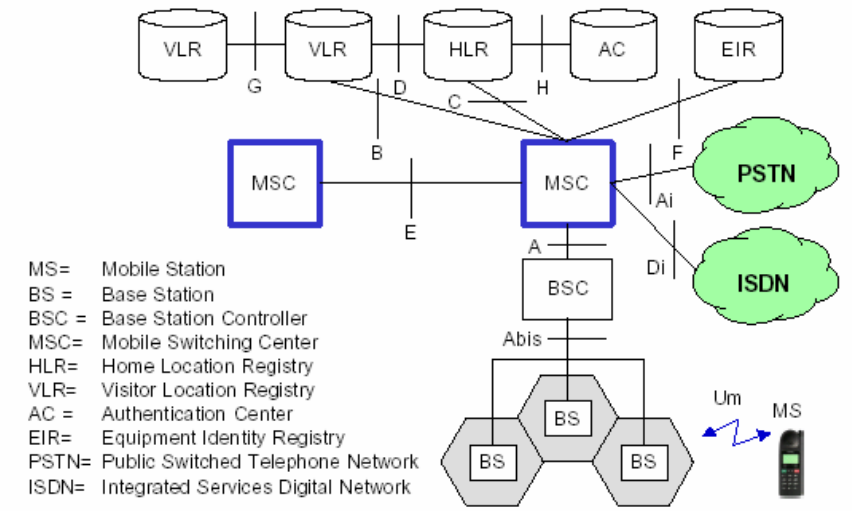
11

The Network Subsystem NSS

- The Mobile Switching Centre (MSC)
- Gateway Mobile Switching Centre (GMSC)
- The Home Location Register (HLR)
  - Subscriber identity and service profiles
- The Visitor Location Register (VLR)
  - Location information, security information
- The Equipment Identity Register (EIR)
- The Authentication Center (AuC)

12

Open Interfaces

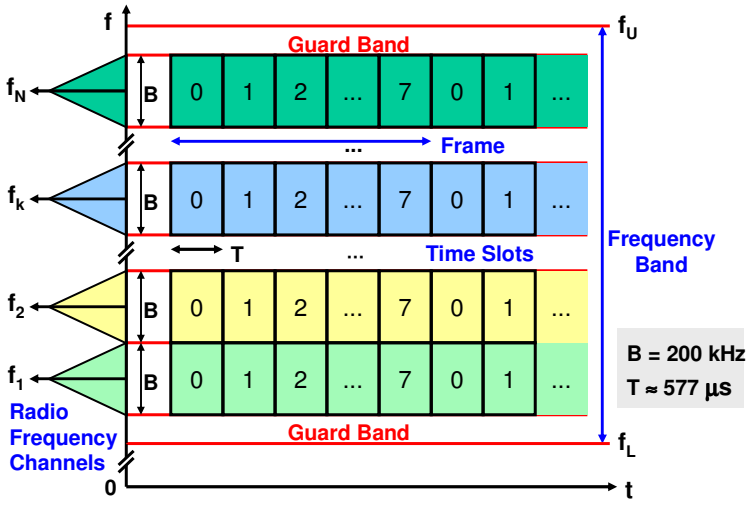


RF Channels Characteristics

- Total allocation: 50 MHz
  - 25 MHz each direction
  - 200 kHz each carrier
  - 124 pairs of FDMA super channels
- Each FDMA super-channel has a data rate of 270 kbps
  - Provides 8 TDMA traffic channels
  - Voice communications use a Residually Excited Linear Predictive (RELP) vocoder - 13 kbps
- Total of 8 x 124 = 992 full duplex RF channels

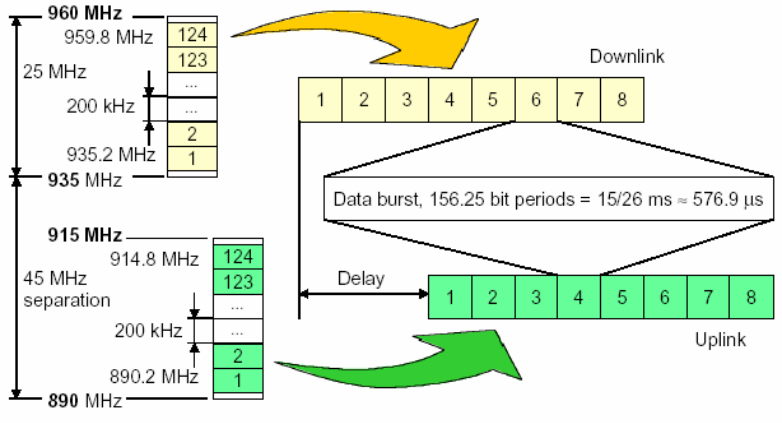
14

Radio Transmission
FDMA & TDMA



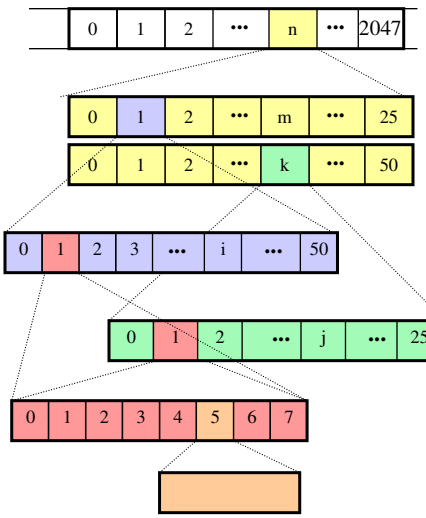
15

Time Slots Structure



16

Frame Hierarchy



Hyperframe = 2048 Superframes
= 2,715,648 TDMA Frames
(3 h 28 min 53.76 s)

Superframe = 26 * 51 Multiframes
= 1325 TDMA Frames
(6.12 s)

BCH Multiframe (235.38 ms)

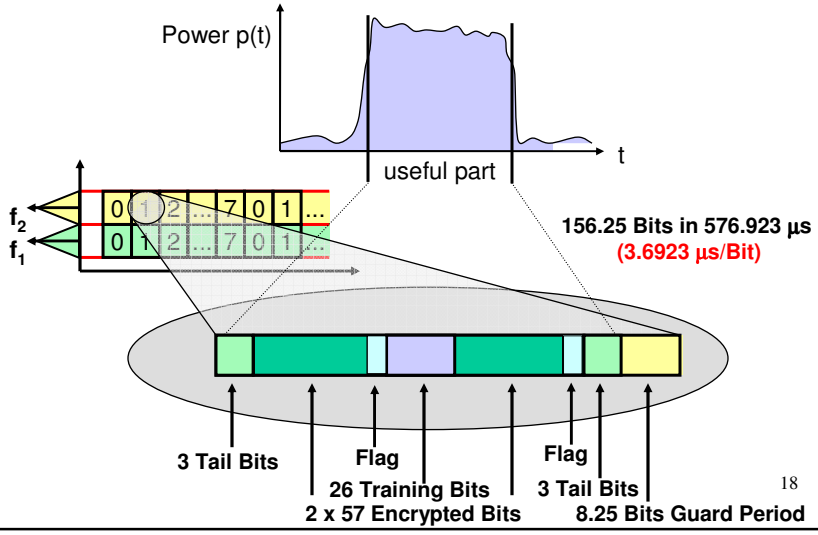
TCH Multiframe (120 ms)

TDMA Frame (≈4.615 ms)

Burst (≈577 µs)

17

Burst



18

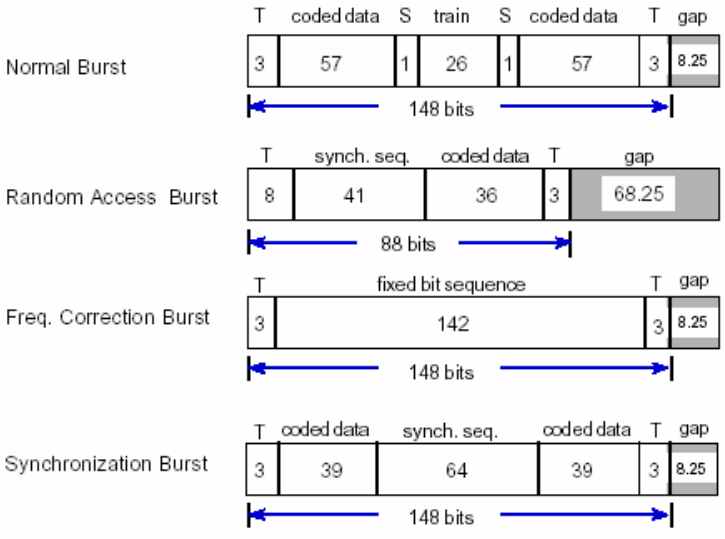
Type of Bursts

Five different types of bursts

- Normal burst
  - Traffic and control payload
- Frequency correction burst
  - All zeroes sequence
- Synchronization burst
  - A special fixed sequence
- Random access burst
  - Extended guard period of 68.25 bits (252 µs)
- Dummy burst

19

Burst Structures



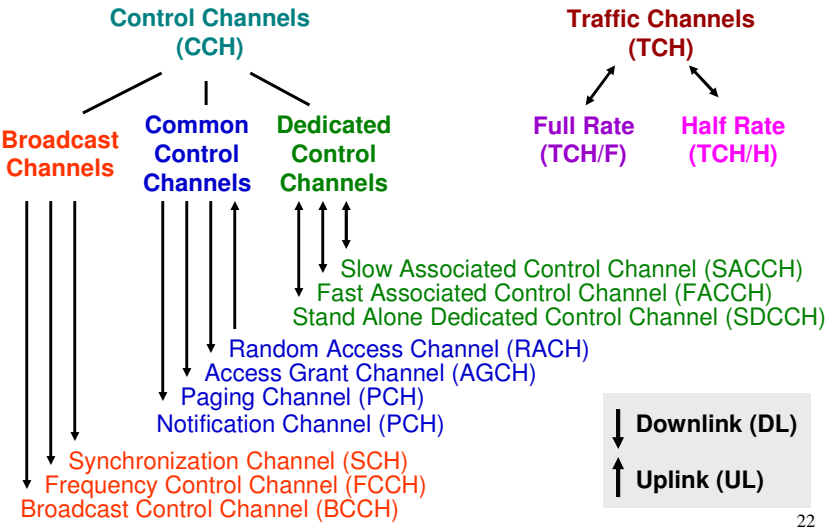
20

Slow Frequency Hoping

- In GSM, TDMA bursts can be optionally transmitted in a pre-calculated sequence of different frequencies
  - Algorithm pre-programmed in the mobile station
- If a TDMA burst happens to be in a deep fade, then next burst most probably will not be
  - Different carrier frequency have different fading characteristics
- Effective to avoid RF quality problems caused by fading

21

Logical Channels



22

Control Channels

- Control channels fall into three categories:
  1. Broadcast: BCCH, FCCH, SCH
     - One way, from base to mobile
  2. Common Control: RACH, AGCH, PCH
     - One way, some from base to mobile and some from mobile to the base
  3. Dedicated: SDCCH, SACCG, FACCH
     - Two-way, stand-alone or embedded in the traffic channels
- All signaling channels share one carrier in a cell
  - the dedicated control channels may be transmitted on traffic carriers

23

Broadcast Channels

- Frequency Correction Channel (FCCH)
  - Carries information for frequency correction
- Synchronization Channel (SCH)
  - Carries information for frame synchronization and for identification of the BTS
- Broadcast Control Channel (BCCH)
  - Broadcasts general information on the BTS
  - Broadcasts cell-specific information, e.g. control channel organization, frequency hopping sequences, cell identification, etc.

24

Common Control Channels

- Paging Channel (PCH) - downlink only
  - for paging purposes
- Random Access Channel (RACH) - uplink only
  - used by any MS to request allocation of a signalling channel (SDCCH)
  - a slotted Aloha protocol is used, so collisions among MSs may happen
- Access Grant Channel (AGCH) - downlink only
  - used to allocate a SDCCH or a TCH
- Notification Channel (NCH) - downlink only
  - notify MS of voice group and voice broadcast calls (ASCI feature)

25

Dedicated Control Channels

- Stand Alone Dedicated Control Channel (SDCCH)
  - used for call setup (authentication, signaling, traffoc channel assignment), location updates and SMS
- Slow Associated Control Channel (SACCH)
  - always coupled with a SDCCH or TCH
  - for communicating measurement data and control parameters
- Fast Associated Control Channel (FACCH)
  - to response to increased signaling demand, e.g. during handover
  - bandwidth (bit slots) are stolen from the associated TCH (traffic data are preempted)

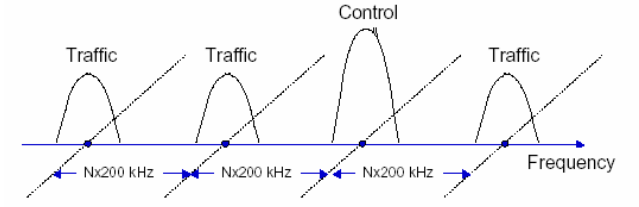
26

Traffic Channels

- GSM support two types of traffic channels
  - full rate (TCH/F): 22.8 kbps
  - half rate (TCH/H): 11.4 kbps
- Mapping to physical channel
  - full rate traffic channel - 1 timeslot
  - half rate traffic channel - 1 timeslot in alternating frames
- Full rate channel may carry
  - 13 kbps speech or data at 2.4, 4.8 or 9.6 kbps
- Half rate channel may carry
  - 6.5 kbps speech or data at 2.4 or 9.6 kbps

27

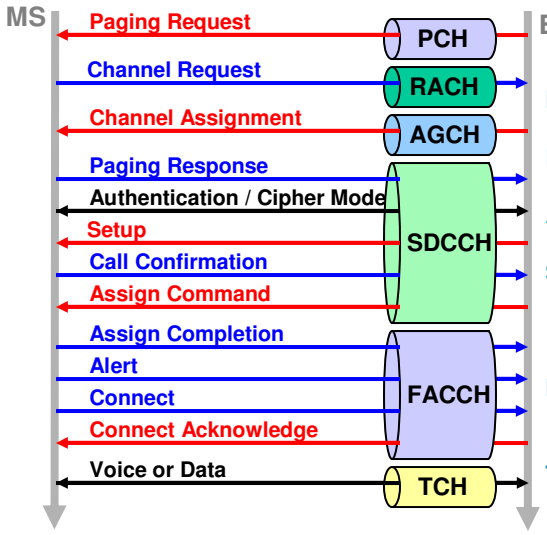
Control and Traffic Channels



- The carriers in a given cell are separated by Nx200 kHz
  - N is the frequency reuse cluster size (4 in GSM)
- The traffic carriers have 26-multi-frame structure
- The control carrier has 51-multi-frame structure
- The control carrier has higher energy than traffic carriers

28

Channel Usage
MS Terminating Calls



PCH Paging Channel

RACH Random Access Ch.

AGCH Access Grant Ch.

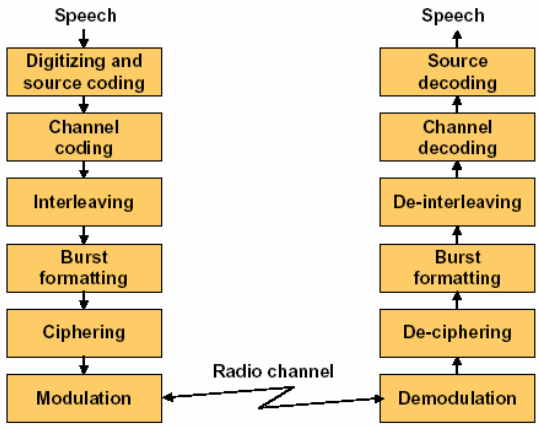
SDCCH Stand-alone Dedicated Control Channel

FACCH Fast Associated Control Channel

TCH Traffic Channel

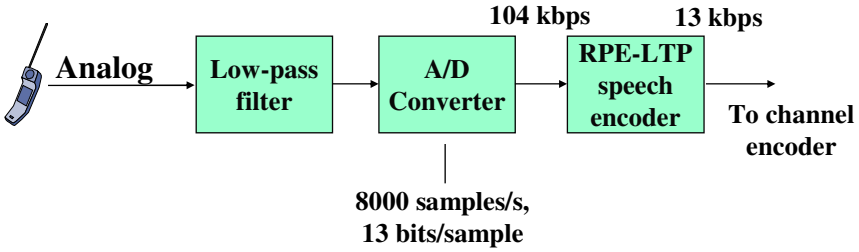
29

Speech Processing



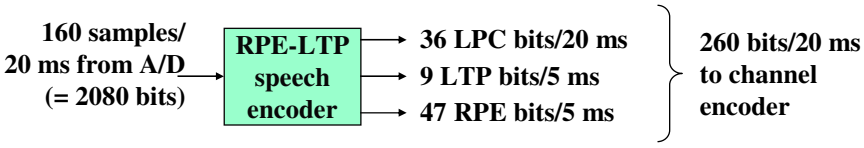
30

Speech Coding



31

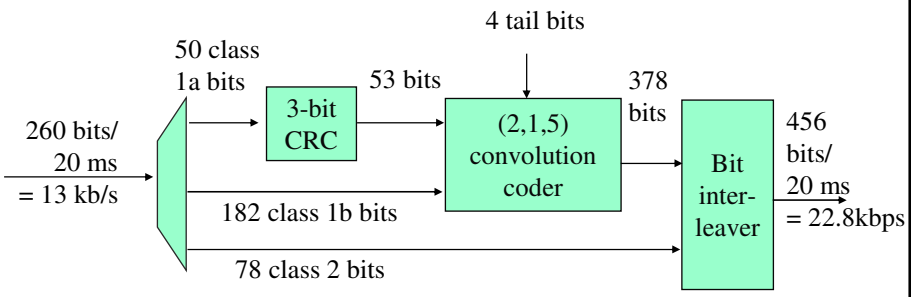
Speech Encoder



LPC: linear prediction coding filter
LTP: long term prediction filter
RPE: regular pulse excitation signal

32

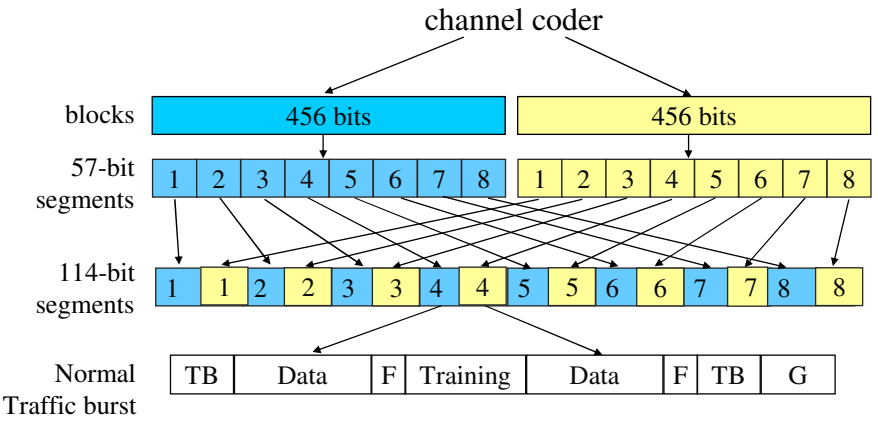
Channel Encoding



Class 1a: CRC (3-bit error detection) and convolutional coding (error correction)
Class 1b: convolutional coding
Class 2: no error protection

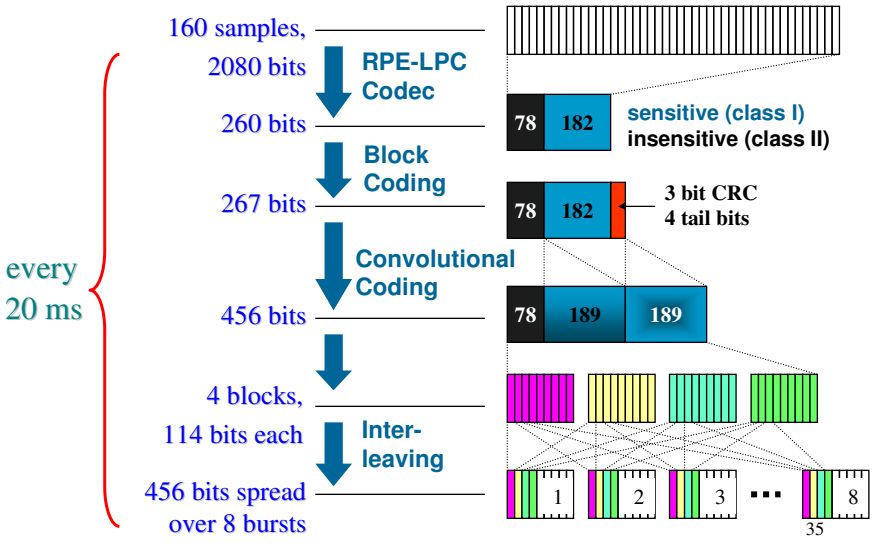
33

Interleaving



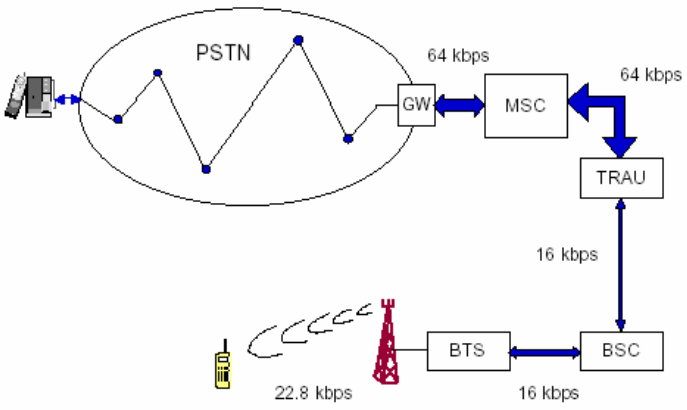
34

Speech Data Processing



35

Voice Transmission Path



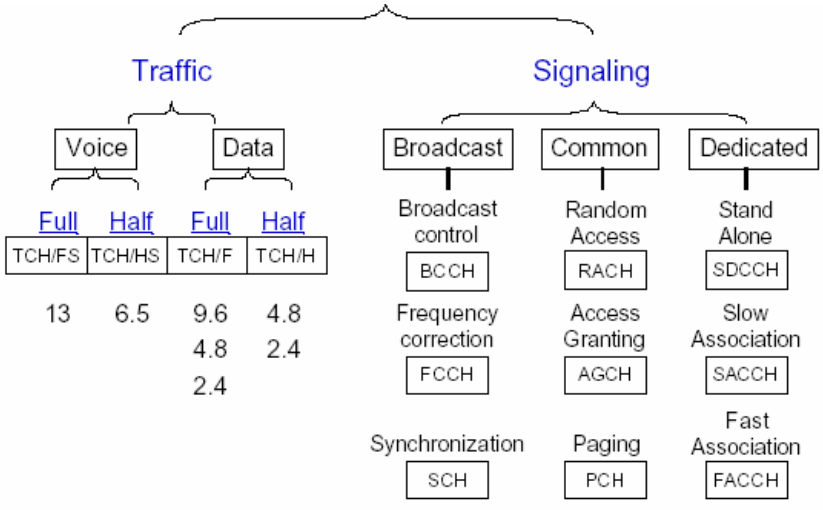
36

Logical Channels Summary

- ***Traffic*** and ***Control*** (or ***Signaling***)
- Two types of ***traffic channels***: full rate and half-rate
- ***Control channels*** are divided into three groups
  - **Broadcast (BCH)**
    - point to multi-point
    - downlink only
  - **Common (CCH)**
    - bi-directional
    - shared by more than one MSs
  - **Dedicated (DCH)**
    - point-to-point
    - bi-directional
    - assigned to a particular MS

37

GSM Logical Channels Another View

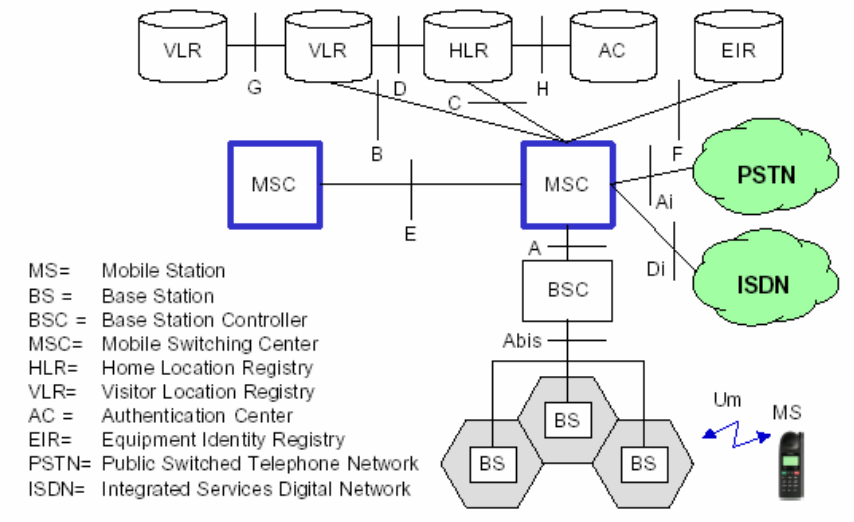


GSM Networking Features

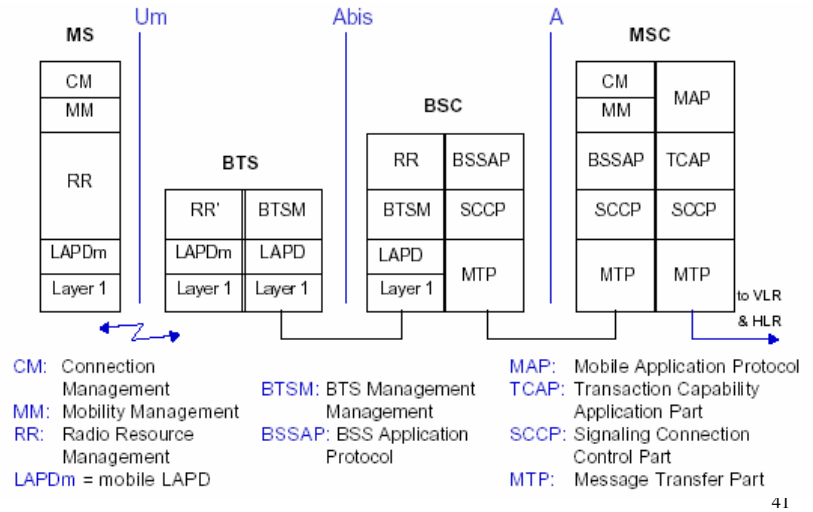
- Global roaming
  - Most operators support international roaming
  - Including roaming between different frequency bands
- Mobile Application Part (MAP) is the primary networking protocol
- Utilize Intelligent Network technologies
  - SS #7
  - SCP
  - CAMEL (Customized Applications for Mobile Enhanced Logic) in Phase 2+
- Open interfaces between network elements

39

Open Interfaces



GSM Protocol Stacks



41

GSM Signaling

- Network elements (e.g. MSC and HLR) exchange signaling information via messages
- On the NSS side, signaling messages are exchanged using ***MAP (Mobility Application Part)*** protocol
  - Between MSC, HLR, VLR, EIR and AuC
- **MAP** is built on top of SS #7 protocol suite
  - TCAP (Transaction Capability Application Part)
  - SCCP (Signaling Connection Control Part)
  - MTP (Message Transfer Part)
- GSM signaling is very *messaging-intensive*

42

GSM Network Layer

GSM network layer is divided into three sublayers

- **Radio Resource Management** (RR)
  - Manage RF channels
  - Establishment, maintenance and termination of RF connections
- **Mobility Management** (MM)
  - Location registration, location tracking and security processing
- **Connection Management** (CM)
  - Establishment, maintenance and termination of circuit-switched calls

43

Mobility Management

- Location registration and update
  - IMSI attach and detach
  - Location updates to keep MS's data in VLR and HLR current
- Location tracking
  - HLR and VLR
- Network security
  - via authentication triplets
- Handover

44

VLR - Visitor Location Register

- Each MS currently in the location area served by the VLR has an entry in the VLR database
- Major fields in the VLR database include
  - IMSI
  - TMSI
  - Current location area
  - Supplementary service information
  - Authentication triplets from HLR
  - HLR number

45

Location Registration

- Required when the MS is about to receive network services (deregistration when about to leave)
- **IMSI Attach** - power up
  - MS registers with the network using IMSI
  - A TMSI is assigned and is stored in the SIM-card
  - All subsequent network transactions use TMSI
- **IMSI Detach**
  - When the MS deems not to be in the Location Area, it is detached from the VLR
  - e.g. power down
- The HLR knows the current location of the MS
  - The VLR reports the location of the MS to the HLR

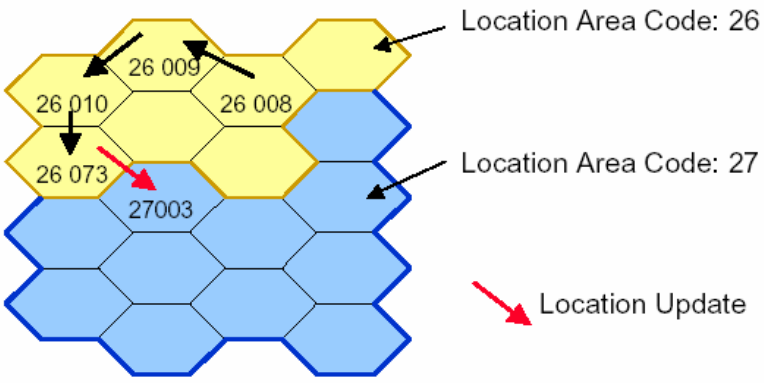
46

Location Update

- Required when MS enters a new Location Area
- Or initiated by the MS periodically – timer based
- Update of entries in HLR and VLR
- Might lead to a change of the current VLR
- Two types of Location Update
  - Intra-VLR
  - Inter-VLR (MS‘s data in the old VLR is deleted)

47

Location Area and Location Update



Mobility Management Network Security

- Location registration and location update always requires authentication
- Each authentication transaction consumes one authentication triplet
- An MS‘s entry in the VLR contains a set of triplets for that particular MS
- When remaining triplets is below a certain threshold, the VLR requests a new set from the HLR

49

Network Security

- **Access control and authentication**
  - secret PIN (personal identification number)
  - challenge and response process
- **Confidentiality of traffic**
  - voice and signaling encrypted on the wireless link after successful authentication
- **Anonymity**
  - TMSI - Temporary Mobile Subscriber Identity
  - encrypted signaling data

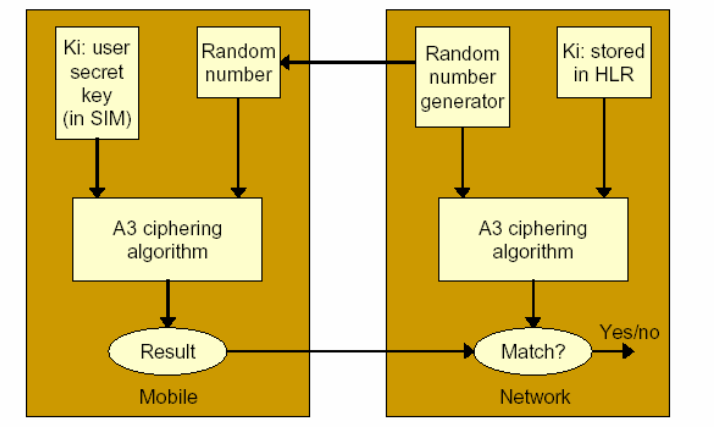
50

Ciphering Algorithms

- Three ciphering algorithms are specified in GSM
  - A3 for authentication
  - A5 for encryption
  - A8 for key generation

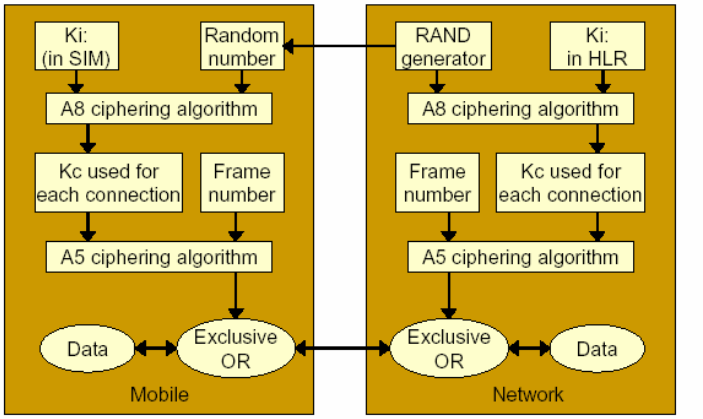
51

Authentication



52

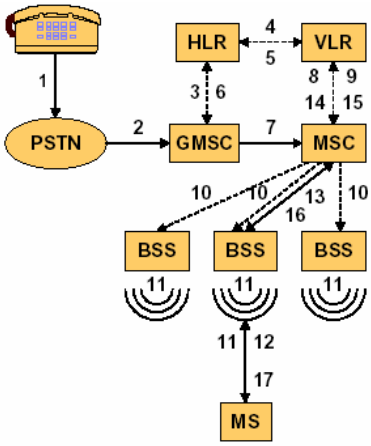
Encryption (Ciphering)



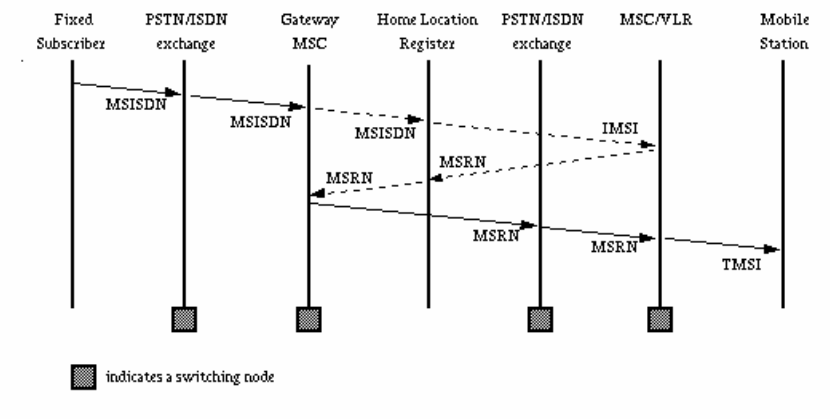
53

Call Processing
Mobile Terminating Calls

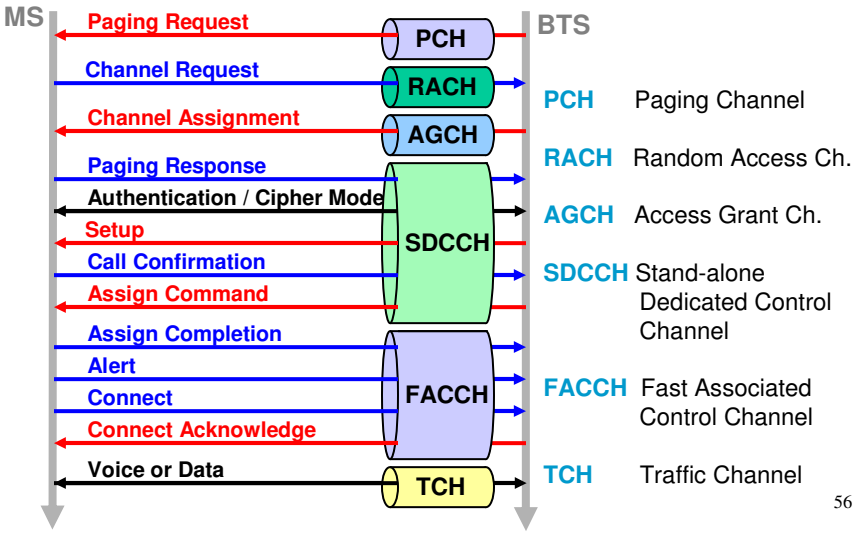
1: calling a GSM subscriber
2: forwarding call to GMSC
3: signal call setup to HLR
4, 5: request MSRN from VLR
6: forward responsible MSC to GMSC
7: forward call to current MSC
8, 9: get current status of MS
10,11: paging of MS
12,13: MS answers
14,15: security checks
16,17: set up connection



Addressing during MS Terminating Calls



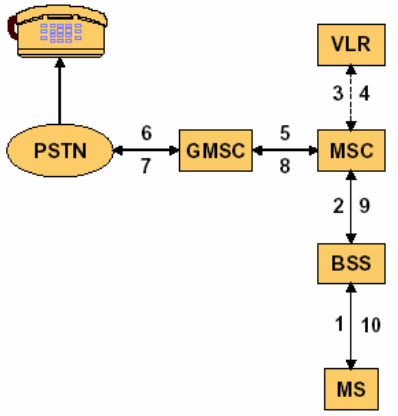
Messages on RF channels MS Terminating Call



56

Call Processing
Mobile Originating

1,2: connection request
3,4: security check
5-8: check resources (free circuit)
9,10: set up call



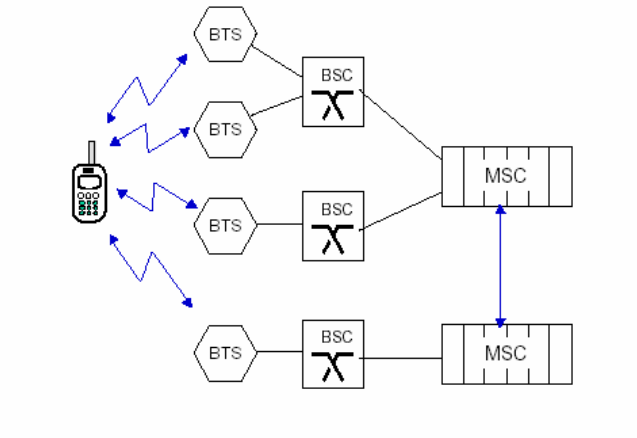
GSM Handover

Three types:

1. **Intra-BSC**
   - Old and new BTSs are controlled by the same BSC
   - The MSC is not involved
2. **Intra-MSC**
   - Old and new BTSs are attached to different BSCs
   - The BSCs are attached to the same MSC
3. **Inter-MSC**
   - Handover to a new MSC
   - Serving MSC becomes anchor MSC
   - IMT (Inter Machine Trunk) is required

58

Handover Types



59

GSM Handover Characteristics

- For an inter-MSC handover, the anchor MSC remains responsible of most call related functions
- Mobile Assisted Hand Over (MAHO)
  - During idle time slots, the MS scans the BCCH of up to 16 neighboring cells and forms a list of 6 candidates
  - This information is sent to the BSC and MSC at least once per second
- The MSC can initiate a handover for traffic balancing purposes

60

Short Message Services

- Ability to send and receive alphanumeric messages
  - up to 160 characters
  - store and forward
  - guaranteed delivery regardless state of the MS
  - can be stored in the SIM for later retrieval
- SM-SC (Short Message Service Center)
  - responsible for storing and relaying messages
  - transportation of messages to and from MSs using SM-TP (Short Message Transport Protocol)
  - outside of the scope of GSM specifications

61

GSM Phases

- Since the beginning, GSM was designed to be deployed in phases
- **Phase 1** - until 1996
  - Standard tele-, bearer- and supplementary services
- **Phase 2** - replaced Phase 1 in 1997
  - Additional services, e.g. SMS
  - GSM 900 and DCS 1800 merger
  - Half Rate and Enhanced Full Rate vocoders

62

GSM Phases - cont

- **Phase 2+** - yearly releases 1996 to 1999
  - More supplementary services
  - High Speed Circuit Switched Data (HSCSD) (14.4 Kbps and higher)
  - General Packet Radio Service (GPRS)
  - Advanced Speech Call Items (ASCI)
  - Expanded Service Platforms (CAMEL)
- **Phase 3** - Enhanced Data for GSM Evolution (EDGE)
  - Same TDMA frame structure but with 8-PSK modulation (3 bits/symbol)
  - High-speed wireless data services

63

ASCI

- **Advanced Speech Call Items**
- For Professional Mobile Radio (PMR) sectors, e.g.
  - police and fire departments
  - transportation companies
  - airports and railways (GSM-R)
- PMR requires special functions for
  - group communications
  - priority schemes (emergencies)

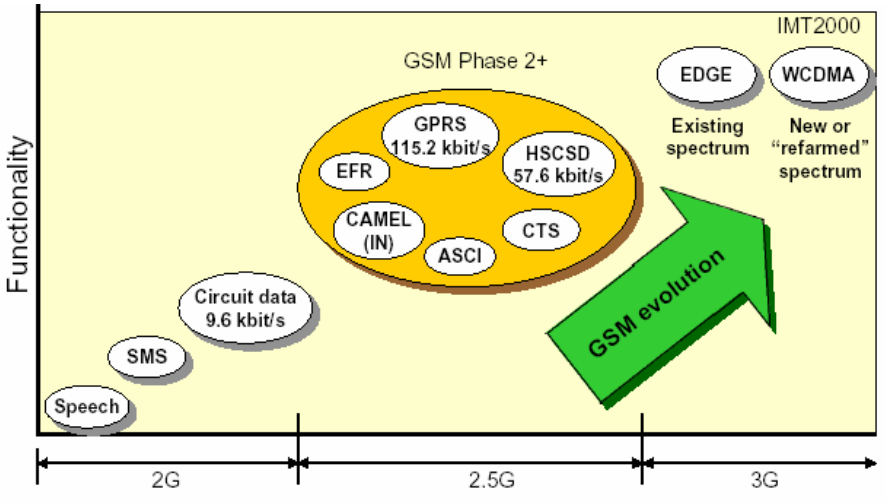
64

ASCI - cont

- The Advanced Speech Call Items:
  - **Voice Broadcast Service** (VBS)
    - Call to all users of a closed group within a ***Group Call Area***
  - **Voice Group Call Service** (VGCS)
    - Call to all group members, originating from any user (semi-duplex)
  - **Enhanced Multi-Level Precedence and Pre-emption Service (eMLPP)**
    - Definition of priority levels for critical missions and emergencies

65

GSM Evolution



GSM Status

- A run-away success!!
  - More than ½ billion of subscribers globally (Jun 2001)
- Many innovations for wireless communications systems
  - Networking technology is used as a base for 3G wireless systems **(MAP)**
  - SIM cards to provide personal mobility
- SMS service are becoming very popular
  - Billions of messages sent and received every month!!
- Evolving towards 3G
  - GPRS as the stepping stone (2.5G)

67

GSM Specifications

- *00 Series:* Preamble
- *01 Series*: GSM overview
- *02 Series:* Service aspects
- *03 Series:* Network architecture, call routing, performance objectives
- *04 Series:* Interface and protocols between mobiles and BSS
- *05 Series:* Physical layer on radio path: multiple access, channel coding, modulation, transmission

68

GSM Specifications

- *06 Series:* Speech coding aspects
- *07 Series:* Terminal adaptors for mobile stations
- *08 Series:* Base station and MSC interface
- *09 Series:* Interworking with PSTN and packet data networks
- *10 Series:* Service interworking, short message service
- *11 Series:* Equipment specification
- *12 Series*: Operation and maintenance, tariffs, traffic administration

www.etsi.org

http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html

www.iec.org/online/tutorial/

69