NEAR EAST UNIVERSITY

Faculty of Engineering

Department of electrical and Electronic Engineering

MOBILE SWITCHINGCENTER

Graduation Project
EE-400

Student: Mutaz F. Al-Zghoul (950937)

Supervisor: Prof. Dr Fakhreddin Mamedov

Lefkoşa - 2001

CONTENTS

Abbreviations

AC	Alerting channel
AUC	Authentication center
ACCH	A ccr-.r~~+orl rr1.ntr0.l rh.::n~r.ol
ACELP	Algebraic Code Exited linear Prediction
ADP CM	il...daptive Differential Pulse Code Modulation
A r__rru	Access Grant Channel
,1,T T'	Automatic Link Transfer
A17'vIPS	Advanced Mobile Phone System
B-ISD:N	Broadband Integrated Services Digital Network
b/s	Bits per Second
BCCH	Broadcast Control Channel
BCHCODE	Bose-Chaudhuri-Hocquenghem Block Code
BER	Binary Error Rate
BMI	Base station , Mobile Switching Center, and Interworking Function
BSC	Base Site Controller
BSMC	Base Station Manufacturer Code
BSS	Base Station System
BTS	Base Transceiver Station
CAVE	Cellular Authentication and \/oice Encryption
r>r> LL	Call Control
CCH	Control Channel
CCIC	Co-Channel Interference Control
CD1\1A	Code Division Multiple Access
CELP	Code Excited Linear Prediction
CEPT	Conference of European Postal and Telecommunications administration
CFP	Cordless Fixed Part
Ch	Chip
CPP	Cordless Portable Part
CRC	Cyclic Redundancy Check
	Cell Station
	Cellular Subscriber Station
CT2	Cordless Telephone .Secorıd Generation
CT2Plus	CT2, enhanced version
dB	Decibels
,fR,,,.,	Decibels relative to I m\V
	Digital Color Code
DCCH	Digital Control Channel
nr, 1 *Rnn*	Digital Cellular System at 1,Q00 I\.ıfU?
DCS1900	Digital Cellular System at 1,900 Ml-Iz
DECT	Digital European Cordless Telecommunication
DL	Digital Control Channel Locator
DTCH	f'linitc,1 T,-c,ff,,-. ı'h,:,nn,,1
DTMF	Dual-tone Multiple Frequency
UiA	Discontinuous Transmission
DVCC	Digital Verification Color Code
E-BCCH	Extended Broadcast Control Channel
EIP,..	Equipment Identity Register
ES-r-;	Electronic Serial Number

ETSI	European Telecommunications Standards Institute
F-BCCH	Fast Broadcast Control Channel
FACCH	Fast Associated Control Channel
FCC	Federal Communications Commission
FCCH	Frequency Correction Control Channel
FDMA	Frequency Division Multiple Access
FM	Frequency Modulation
FOCC	Forward Control Channel
FSK	Frequency Shift Keying
FT	Fixed Termination
FVC	Forward Voice Channel
GEO	Geostationary Orbit Satellite System
GMSK	Gaussian Minimum Shift Keying
GPS	Global Positioning System
GSM	Global System for Mobile communication
HLR	Home Location Register
IlvIEI	International Mobile Equipment Identity
Th1SI	International Mobile Subscriber Identity
IS	Interim Standard
ISDN	Integrated Services Digital Network
ISPBX	Integrated Services Private Branch Exchange
ITU	International Telecommunication Union
IWU	Interworking Unit
KB/s	Kilobits Per Second
KHZ	Kilohertz
KI	Secret Encryption Key In A GSM System
LAN	Local Area Network
LEO	Low Earth Orbit Satellite System
LPC-RPE	Linear Prediction Coding With Regular Pulse Excitation
MACA	Mobile-Assisted Channel Allocation
MAHO	Mobile Assisted Handoff
MAP	Mobile Applications Part
MB/s	Megabits Per Second
MC-F	Fast Message Channel
MC-S	Slow Message Channel
MEO	Medium Earth Orbit Satellite System
MHZ	Megahertz
l\ıIIN	Mobile Identification Number
MM	Mobility Management
MSC	Mobile Switching Center
MTSO	Mobile Telephone Switching Office
MW	MilliWatt
NA-TDMA	North American Time Division Multiple Access
NAMPS	Narrowband Advanced Mobile Phone Service
NMT	Nordic Mobile Telephone
NT	Network Termination
OA&M	Operations Administration And Maintanance
OACSU	Off Air Call Setup
OQPSK	Off Set Quadrature Phase Shift Keying
OSI	Open Systems Interconnections

PACS	Personal Access Communications Systems
PBX	Private Branch Exchange
PCC	Power Control Channel
PCS	Personal Communications Services
PDC	Pacific Digital Cellular
PHS	Personal Handyphone System
PIM	Personal Information Machine
PRC	Priority Request Channel
PS	Personal Station
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
PT	Portable Termination
QCELP	Qualcomm Code Excited Linear Reduction
RACH	Random Access Channel
RECC	Reverse Control Channel
RP	Radio Port
RPCU	Radio Port Control Unit
RBM	Radio Resources Management
RSSI	Received Signal Strength Indication
RT	Radio Frequency Transmission Management
RVC	Reverse Voice Channel
S-BCCH	Short Message Service broadcast Control Channel
SACCH	Slow Associated Control Channel
SAPI	Service Access Point Identifier
SAT	Supervisory Audio Tone
SBC	System Broadcast Channel
SCCH	Signaling Control Channel
SCF	Shared Channel Feedback
SCH	Synchronization Control Channel
SCM	Station Class Mark
SDC	Synchronous Directive Channel
SDCCH	Stand-Alone Dedicated Control Channel
SFP	Super Frame Phase
SIC	System Information Channel
SID	System Identifier
SIM	Subscriber Identity Module
SOC	System Operator Code
SPACH	Short Message Service, Paging, And Access Response Channel
SS7	Signaling System Number 7
SSD	Shared secret Data
ST	Supervisory Tone
SU	Subscriber Unit
TC	Traffic Channel
TCAP	Transactions Capabilities Applications Part
TCH	Traffic Channel
TCH/F	Full-Rate Traffic Channel
TCH/H	Half-Rate Traffic Channel
TDMA	Time Division Multiple Access
TE	Terrninal Equipment
TETRA	Trans-European Trunked Radio System

TIA	Telecommunications Industry Association
TMSI	Temporary Mobile Subscriber Identity
UIC	User Information Channel
Um	Inteıface Between Terminal And Base Station
USC CH	User-Specific Packet Control Channel
USP CH	User-Specific Packet Channel
VLR	Visitor Location Register
VMAC	Mobile Attenuation Code For Voice Signals
VOX	Voice operated Transmission
VSELP	Vector Sum Excited Linear Prediction
W	Watt
WACS	Wide Area Communications System
WEI	World Error Indicator
µs	Microsecond

ACKNOWLEDGMENTS

First of all I want to thank my family, especially my parents, without their endless support and love for me, I would never achieve my current position, I wish them lives happily always with brothers **Mou'aya, Anas ,Mohamad** and **Do'aa.**

I would like to thank my supervisor **Prof. Dr Fakhreddin Mamedov,** for his benefit support, encouragement enthusiasm that is made this thesis possible and he will always be in my mind and my heart. Then I would like to thank **Mr. Nihat Yilmaz,** under his guidance, I successfully overcome many difficulties and learn a lot about Mobile Communication. In each discussion, he explained my questions patiently.

I also want to thank my advisors **Mr. Kağan Uyar** and **Mr. Merdad Khaledi,** to all my teacher specially **Mr. Tyseer Shanbleh, Dr Şenol Bektaş and Prof. Dr Adnan Khashman** they always helps me a lot either in my study or my life.

Special thanks to my friends **Adnan Amyreh** and **Asim Younis** for helping me in fixing the problems in my computer.

Finally, I want to thank my friends in 1'.1EU **Abo-Iskander, Jamal abo-mutlak ,Mamlok, Jboor, Ziad Hunaiti, Abo-Jack, Abo-Alsafi , Abo-Yaman , Abo-Wadde3 , Abo-Frinend,** Abo-Sharkas, **Omar Hijazi,** Nido, **Houssam & Ahmad Taha, Fabio and Hamdy Elledawy,** Being with them make my time in 1'.1EU full of fun.

ABSTRACT

Mobile telecommunications is one of the fastest growing and most demanding of all telecommunication technologies, it represents an increasingly high percentage of all new telephone subscriptions worldwide.

The GSM network is divided into two systems. Each of these systems is comprised of a number of functional units, which are individual components of the mobile network. The two systems are: Switching System (SS) and Base Station System (BSS).

The Switching System consist of Home Location Register (HLR), Visitor Location Register (VLR), Gate Way Functionality (GMSC), Service Switching Function (SSF), Service Control Function (SCF), Equipment Identity Register (EIR), Authentication Center (AUC). Mobile Switching Center (MSC) is related with all mentioned above elements, it's main objective is to perform the telephony switching functions for the mobile network. It controls calls to and from other telephony and data systems, such as the Public Switching Telephone Network (PSTN), Integrated Services Digital Network (ISDN), Public Data Networks, Private Networks and other Mobile Networks.

Upon completion of this project the student will be able to: list one benefit of having a standard, describe the history of GSM development, list three network components, describe the GSM geographical network structure, list the GSM-900 frequency bands, list three subscriber services provided in the GSM network, list which 2 nodes are contacted for the security procedure in the GSM system and briefly explanation the purpose of authentication, ciphering and equipment check.

Chapter one

Introduction to l\ilobile Telecommunication and GSJ\,1

1.1 Mobile Telephony

Mobile telecommunications is one of the fastest growing and most demanding of all telecommunications technologies. Currently, it represents an increasingly high percentage of all new telephone subscriptions worldwide. In many cases, cellular solutions successfully compete with traditional wire line networks and cordless telephones. In the future, cellular systems employing digital technology will become the universal method of telecommunication.

1.1.1 History of wireless communication

The origins of mobile communications followed quickly behind the invention of radio in the late 1800s. The first applications of mobile radio were related to the navigation and safety of ships at sea. As radio concepts developed, so did its use as a communications tool. The major milestones in the development of wireless communications are summarized in the following table:

Table 1.1 Milestones in development of wireless communications

Date	Activity
1906	Reginald Fesseden successfully transmits human Voice over radio. Up until that time, radio communications consisted of transmissions of Morse Code.
1915	J. A Fleming invents the vacuum tube making it possible to build mobile radios
1921	The Detroit police department used a 2 MJ-1.z frequency in the department's first vehicular mobile radio. The system was only one-way and police had to find a wire line phone to respond to radio messages.
1930s	Amplitude modulation (Alvl) tow-way mobile system Were in place in the US that took advantage of newly Developed mobile transmitters and utilized a "push-to-talk" or half-duplex transmission By the end of the decade channel allocation grew from 11 to 40.

1935	Invention of frequency modulation (FM) improved audio quality. FM eliminated the need for large AM transmitters and resulted in radio equipment, which required less power To operate. This made the use of transmitters in vehicles more practical.
1940s	The Federal Communications Commission (FCC) recognized a communication service it classified as Domestic Public Land Mobile (DPLM) radio service. The first DPLM system was established in St. Louis in 1946 and it utilized the 150 MHz band. The following year, a "highway" system was developed along the New York - Boston corridor using the 35-40 MHz band.
1947	D.H. Ring, working at Bell Laboratories, envisions the cellular connect.
1948	Shockley, Bearden and Britain, at Bell Laboratories, invent the transistor which enables electronic Equipment, including the radio to be miniaturized
1949	Radio Common Carriers (RCCs) were recognized.
1949, 1958	Bell Systems made broadband proposals.
1964	AT&T introduces Improved Mobile Telephone S stem (IMTS).
1968	The FCC began to address issue of new US spectrum requirements.
1969	Nordic countries of Denmark, Finland, Iceland, Norway and Sweden agree to form a group to study and recommend areas of cooperation in telecommunication. This led to the standardization of telecommunications for all members of the Nordic Mobile Telephone (NMT) group, the first comprehensive international standardization group.
1973	The NMT group specifies a feature allowing mobile telephones to be located within and across networks. This feature would become the basis for roaming.
1979	The FCC authorized the installation and testing of the first developmental cellular system in the US (Illinois Bell Tele hone Com an)
1981	Ericsson launches the world's first cellular system in Saudi Arabia based on the analog NMT 450 standard.
1991	The first digital cellular standard (GSM) is launched.
1998	The number of mobile subscribers worldwide has own to over 200 million.

1.1.2 Mobile Standards

Standards play a major role in telecommunications by

- Allowing products from diverse suppliers to be interconnected
- Facilitating innovation by creating large markets for common products

The standards-making process is one of co-operation at many levels, both nationally and internationally and includes cooperation between:

- Industrial concerns within a country.
- These industrial concerns and their governments.
- National governments at an international level.

The primary purpose of a standard for mobile communications is to specify how mobile phone calls are to be handled by a mobile network For example, this includes specification of the following:

- The signals to be transmitted and received by the mobile phone.
- The format of these signals.
- The interaction of network nodes.
- The basic network services which should be available to mobile subscribers.
- The basic network structure (i e. cells, etc.).

Since the development of NMT 450 in 1981, many standards for mobile communication have been developed throughout the world. Each mobile standard has been developed to meet the particular requirements of the country' or interest groups involved in its specification. For this reason, although a standard may be suitable for one country, it may not be suitable for another. The main standards and the main markets in which they are used are summarized in the following table

Table 1.2 the main cellular standards

Year	Standard	Mobile telephone system	Technology	Primary markets
1981	NMT 450	Nordic mobile telephony	Analogue	Europe, Middle East

1983	AMPS	Advanced mobile phone system	Analogue	North and south America
1985	TACS	Tota! access communication System	Analogue	Europe and china
1986	NMT 900	Nordic mobile telephony	Analogue	Europe, Middle East
1991	GSM	Global system for mobile Communication	Digital	World-wide
1991	TDMA (D-AMPS) (IS 136)	Time division multiple access (Digital-AMPS)	Digital	North and South America
11992	GSM 1800	Global system for mobile Communication	Digital	Europe
1993	Cdmaüne (IS95)	Code division multiple access	Digital	N. America, Korea -
1994	PDC	Personal digital cellular	Digital	Japan
1995	PCS 1900	Personal communication Services	Digital	North America

1.2 Global System For Mobile Communication (GSM)

1.2.1 History Of GSM

This history of GSM is outlined in the following table

Table 1.3 GSM milestones

Date	Activity
1982-1985	Comfererıce Europeenne des Postes et telecommunications (CEPT) began specifying a European digital telecommunications standard In the 900 Ml-Iz frequency band. This standard later became known As global system for mobile communication (GSM)

1986	Field tests were held in Paris to select which digital transmission technology to use. The choice was time division multiple access (TDMA) or frequency division multiple access (FDMA).
1987	A combination of TDMA and FDMA was selected as the transmission Technology for GSM. Operator from 12 countries signed a Memorandum of Understanding Committing themselves to introducing GSM by 1991.
1988	CEPT began producing GSM Specifications for a phased implementation. Another five countries signed the MoU.
1989	European Telecommunication standards Institute (ETSI) took over responsibility for GSM specification.
1990	Phase 1 specifications were frozen to allow manufacturers to develop network equipment.
1991	The GSM 1800 standard was released. An addendum was added to the MoU allowing countries outside CEPT To sign..
1922	Phase 1 specifications were completed. First commercial Phase 1 GSM networks were launched. The first international roaming agreement was established between Telecom Finland and Vodafone in UK.
1933	Australia became the first non-European country to sign the MoU. The MoU now had a total of 70 signatories. GSM networks were Launched in Norway, Austria, Ireland, Hong Kong and Australia. The number of GSM subscribers reached one million. The first commercial DCS 1800 system was launched in the U.K.
1994	The MoU now had over 100 signatories covering 60 countries. More GSM networks were launched. The total number of GSM subscribers exceeded 3 million.
1995	The specification for the Personal Communications Services (PCS) was developed in the USA. This version of GSM operates at 1900 MHz. GSM growth trends continued steadily through 1995, with the number of GSM subscribers increasing at the rate of 10,000 per day and rising. In April 1995, of the there were 188 members MoU from 69 countries.

1996	The first GSM 1900 systems became available these comply with the PCS 1900 standard.
1998	At the beginning of 1998 the MoU has a total of 253 members in over 100 countries and there are over 70 million GSM subscribers worldwide. GSM subscribers account for 31% of the worlds mobile market

Figure 1.1 GSM worldwide (indicated by darker areas)

Because GSM provides a common standard, cellular subscribers can use their telephones over the entire GSM service area, which includes all the countries around the world where the GSM system is used.

In addition, GSM provides user services such as high-speed data communication, facsimile and a Short Message Service (SMS). The GSM technical specifications are also designed to work with other standards as it guarantees standard interfaces. Finally, a key aspect of GSM is that-the specifications are open-ended and can be built upon to meet future requirements.

1.2.2 GSM Phases

In the late 1980s, the groups involved in developing the GSM standard realized that within the given time frame they could not complete the specifications for the entire range of GSM services and features as originally planned. Because of this, it was decided that GSM would be released in phases with phase 1 consisting of a limited set of services and features. Each new phase builds on the services offered by existing phases.

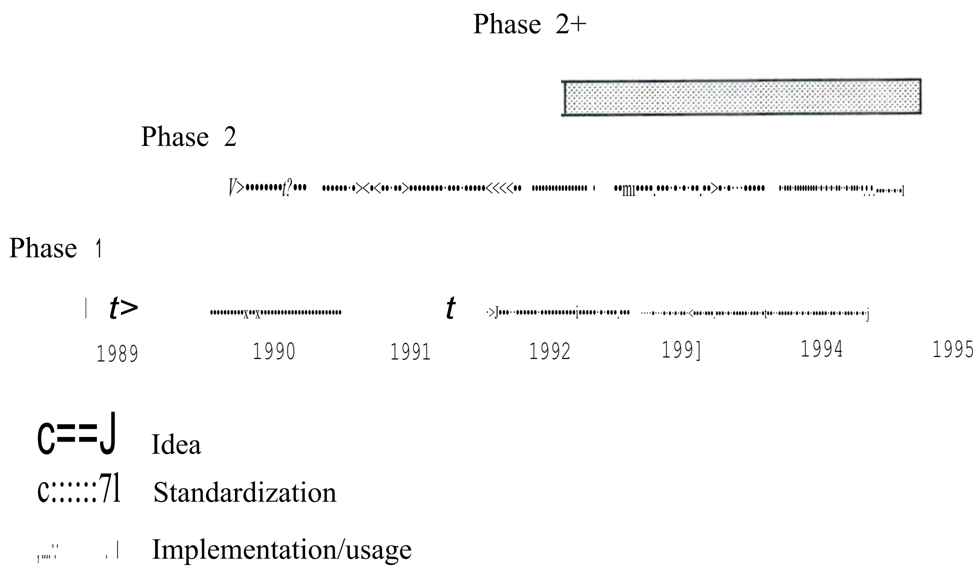


Figure 1.2 GSM phases

Phase 1

Phase 1 contains the most common services including:

- Voice telephony
- International roaming
- Basic fax/data services (up to 9.6 kbits/s)
- Call forwarding
- Call barring
- Short Message Service (SMS)

Phase 1 also incorporated features such as ciphering and Subscriber Identity Module (SIM) cards. Phase 1 specifications were then closed and cannot be modified.

Phase 2

Additional features were introduced in GSM phase 2 including:

- Advice of charge
- Calling line identification
- Call waiting
- Call hold
- Conference calling
- Closed user groups
- Additional data communications capabilities

The tv1S, BSS and 1'--JSS form the operational part cf the system, whereas the OSS provides means for the operator to control them. The horizontal part of the figure corresponds to a chain:

External networks - ---+NSS - -BSS - -MS - -- Users

In Figure 1.2 is given the internal structure of each part of GS~.-1.

1.3.1 1\fobiie Station

P.~ Mobile station consists of two [illegible] elements: the ~Iobile I erminal (MT) and the Subscriber Identity Module (SIM). are [illegible] types [illegible] distinguished principally by their power and application. The 'fixed' terminals are the ones installed in cars. Their maximum alloV'l./ed output power is 20 \1./ The harıdheld terminals have experienced the biggest success thanks to their weight and volume, which are continuously decreasing. These terminals can emit up to 2 \1./. The evolution of technologies allows decreasing the maximum allowed power to 0.8\V.

The SIM card

The SL\.1 is a smart card that identifies the terminal. By inserting the SI}/1 card into the terminal, the user can have access to all the services. Without the Sllvl card, the terminal ıs not operational. J.A. four-digit Personal Identification Number (PIN) protects the SilA: card. In order to identify the subscriber to the system.

[illegible]

[illegible] mobility of the users. In fact, the only element that personalizes a terminal is the SfM card. Therefore, the [illegible] its subscribed servıces ın any terminal uJuıg its Sllvl card.

1.3.2 The Base Station Subsystem

The BSS connects the Mobile Station ~·1S and the t,-1SC. It is in charge of the [illegible] reception. The BSS can be divided into two parts: The Base Transceiver Station (BTS) or Base Station and The Base Station Controller (BSC).

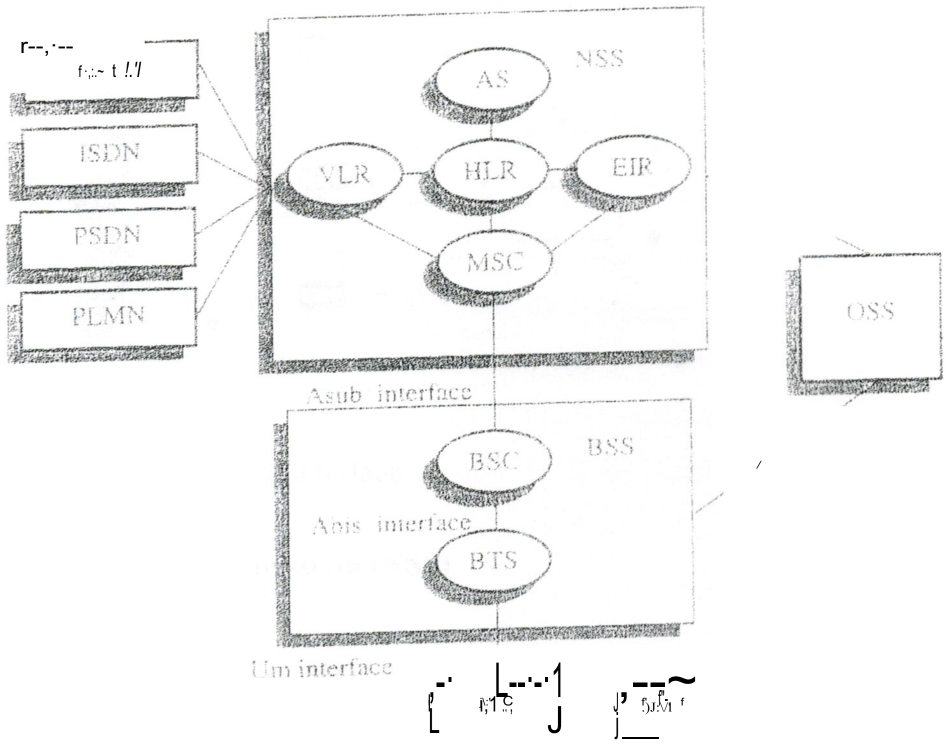


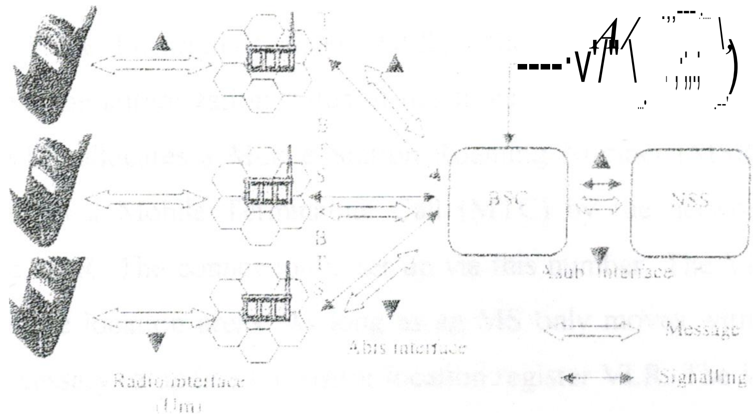
Figure 1.4 internal structure of each part of GSM

The Base Transceiver Station

The BTS corresponds to the transceivers and antennas used in each cell of the network. ABTS is usually placed in the center of a cell Its transmitting power defines the size of a cell.

The Base Station Controller

The BSC controls a group of BTS and manages their radio resources. A BSC is principally in charge of handovers, frequency hopping, exchange functions amid control of the radio frequency power levels of the BTSs. BSC can act as a concentrator for the links between the Abis and Asub interfaces. The BSC involves a separate 'Transco ding And Rate Adaptation Unit (TRAU) for speech coding arid data rate adaptation The BSS components and interfaces are shown in Figure 1A



Figurel.5 BSS components and interface

1.3.3 Network Switching Subsystem (NSS)

Mobile switching center (MSC) is a stored-program controlled digital switching center.

The MSC is the switching center in the PLMN, which

- Acts as a gateway to other networks,
- Is linked to other MSCs in the PLMN,
- Connects the network elements of the NSS with the network elements of the BSS in the coverage area of the PLMN.

The MSC has functions that are familiar from the switching centers of the fixed networks as well as special functions that are not necessary in the switching centers of the fixed networks.

Visitor Location Register (VLR)

The VLR is essentially a database that holds all information on those mobile subscribers currently roaming in the VLR area it controls. The VLR can recognize a mobile subscriber by the following identifiers

- The international mobile subscriber identification (IMSI)
- The local mobile subscriber identification (LMSI).
- Mobile station roaming number (MSRN).
- The temporary mobile station identity (TMSI) together with the local area identity (LAI).

When a mobile subscriber checks into a VLR service area, this information is forward to his home Location Register (HLR). The HLR then sends to the VLR information about the authorization status of this mobile subscriber. For the duration of call setup the VLR allocates a Mobile Station Roaming Number (MSRN); as soon as this is requested in a Mobile Terminating Call (MIC) by the network-access MSC (GMSC) via the HLR. The connection is set up via this number. The VLR service area covers one or more location areas. As long as an MS only moves within one location area, it is not necessary to update the visitor location register VLR. The VLR database is split into a semi permanent and a transient part The semi permanent part is imaged on double disks. The signaling-routing database resides in the semi-permanent part of the VLR database. It contains the IMSI and the LAI digit Translator, which supply the HLR address and the address of the previous VLR. The national roaming database stores the data of the VLR areas in which the mobile subscriber is permitted to set up a connection. The mobile subscriber database resides in the transient part of the VLR database. lt contains the call processing data of the mobile subscribers currently roaming in this area. Its memory is allocated dynamically and separately for each mobile subscriber. The data are distributed in several pools, e.g.:

- In the common data pool with IMSI, ISDN; TMSI, LAI and the registered services;
- In the basic telecommunications data pool with the registered and activated Supplementary services;
- Closed User Group (CUG) data pool (e.g. CUG index)

Another transient database contains the temporary mobile subscriber identities (TMSI). With these an individual mobile subscriber is addressed and identified. The VLR database contains the current ciphering key (KC) and the ciphering key sequence number sent to the MS during authentication.

Home Location Register (HLR)

The HLR contains the main database of the mobile subscribers. The database entries may be generated, deleted and read by the PLMN operator, remotely by an OSS or by a Personalization Center (PCS), for SIM) via the OMS or on the local OMT

By Subscriber Controlled Input (SCI), the mobile subscriber can also remotely input specific subscriber data (for supplementary services).

At call setup, the HLR can identify a mobile subscriber with the aid of the International Mobile Subscriber Identifier (IMSI) and By International Mobile Subscriber Identifier (MSISDN)

The HLR participates in setting up a mobile terminating call (MTC). On setup of an MTC the HLR is requested by the network access MSC (GMSC), to retrieve the mobile subscriber roaming number (MSRN) of the mobile subscriber from the current VLR. The HLR does this and sends the MSRN to the GMSC During a location update the HLR supports the current VLR of the mobile subscriber by supplying the necessary data, and the VLR in turn supplies its VLR address. The HLR database contain us both semi permanent and transient data. The semi permanent data include:

HLR mobile subscriber data and signaling data (network data of the HLR). The transient data include: HLR mobile subscriber data and traffic measurement data.

The semi permanent HLR mobile subscriber data are split into the following data modules and tables:

- Common data module;
- Basic and supplementary services data modules.
- **MSISDN** and bearer capability data module.
- **DUG** data module.
- **GSM** bearer capability information element (BCIE).
- **VLR** roaming table (regional VLR roaming).
- **IMSI** exchange table.

The transient HLR mobile subscriber data are split into the following data modules ,

- Mobility data module (e.g. authentication data, MSRN, relation to VLR address and Local Mobile Subscriber Identifier (LMSI), detach from the IMSI.
- Short message waiting data module.

Authentication Center (AUC)

The AUC is equipped with several security boxes, in which the authentication keys and algorithms required for generation of the authentication parameters of a mobile subscriber are stored ln the AUC for each mobile subscriber a number of authentication parameters RAND (random number), authentication response (SRES, signed response) and Kc (cipher key) are generated, before the mobile subscriber obtains access to the network. The authentication Parameters are used by the VLR for authentication tests, i.e. to determine whether a mobile subscribes authorized for access to the network and call setup.

The Equipment Identity Register (EIR)

The EIR is also used for security purposes. The EIR is a database with information about the equipment types and equipment identities of all mobile radio equipment authorized in its service area. More particularly, it contains a list of all valid terminals. The functions belonging to the ETR perform the equipment identification A terminal is identified by its International Mobile Equipment Identity (IMEI). The EIR allows then to forbid calls from stolen or unauthorized terminals.

The GSM Interlocking Unit (GIWU)

The GIWU corresponds to an interface to various networks for data communications During these communications, the transmission of speech and data can be altered.

1.3.4 The Operation and Support Subsystem

The OSS is connected to the different components of the NSC and to the BSC, in order to control and monitor the GSM system. It is also in charge of controlling the traffic load of the BSS.

However, the increasing number of base stations, due to the development of cellular radio networks, has provoked that some of the maintenance tasks are transcended to the BIS This transfer decreases considerably the costs of the maintenance system

The GSM functions

In GSM are defined five main functions: Transmission, Radio Resource Management (RRM), Mobility Management (MM), Operation, Administration and Maintenance (OAM).

The transmission functions include two sub-functions the transmission of user information and transmission of signaling information. Not all component of the GSM network are strongly related with the transmission functions. The MS, BTS and BSC, are deeply concerned with transmission. But other components, such as the register HLR; VLR or ER are concerned for signaling need.

The role of RRM is to establish, maintain, and release communication links between MS and BSS. RR function is also in charge of maintaining a connection even if user moves from one cell to another. The RR is also responsible for the management of the frequency spectrum and the reaction of the network to changing radio environment conditions. The most important responsibility of RR is handover described below.

Handover

The user movements can produce the need the change a channel or cell, when quality of communication is decreasing. This procedure of changing resource is called handover. Four different types of handovers cab be distinguished:

- Handover of channel in the same cell
- Handover of cells controlled by the same BSC
- Handover of cells belonging to the same MSC but controlled by different types BSCs
- Handover of cells controlled by different MSCs.
- Handover is mainly controlled by the MSC. However to avoid unnecessary signaling information, the first two types of handovers are managed by the BSC

Mobility Management

The MM function is in charge of all the aspects related with the moiety of the user, specially the location management, the authentication and security.

Location Management

When a mobile station is powered on, it performs a location update procedure by indicating its IMSI to the network. The first location update procedure is called the IMSI attach procedure.

The mobile station also performs location updating, in order to indicate its current location, when it moves to a new location area or a different PLMN. This location-updating message is sent to the new MSC/VLR, which gives the location information to the subscribers HLR. If the mobile station is authorized in the new MSC/VLR, the subscriber's HLR cancels the registration of the mobile station with the old MSC/VLR. A location updating is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered. When a mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

Authentication and Security

The SIM card and the Authentication Center are used for the authentication procedure. A secret key, stored in the SIM card and the AC, and a ciphering algorithm is used in order to verify the authenticity of the -user. The mobile station and the AC compute a SRES (Signed Results) using the secret key, the algorithm A3 and a random number generated by the AC. If the two computed SRES are the same, the subscriber is authenticated. The different services to which the subscriber has access are also checked. Another security procedure is to check the equipment identity. If the Uv[El number of the mobile is authorized in the EIR, the mobile station is allowed to commonest the network. In order to assure user confidentiality, the user is registered with a Temporary Mobile Subscriber identity (TMSI) after its first location update procedure.

Phase 2+

Phase 2+ is the phase that is currently being used. The phase 2+ program covered multiple subscriber numbers and a variety of business oriented features, and these days the standardization groups have already begun to define the next phase, 3.

Some of the enhancements offered by Phase 2+ include:

- multiple service profiles
- Private numbering plans
- Access to Centrex services
- Interlocking with GSM 1800, GSM 1900 and the Digital Enhanced Cordless Telecommunications (DECT) standard Priorities and time schedules for new features and functions depend primarily on the interest shown by operating companies and manufacturers and technical developments in related areas.

1.3 Architecture of GSM

GSM as the modern telecommunication system is a complex object. Its implementation and operation are not simple task, neither easy its description.
As shown in Figure 4.10 the GSM architecture consists of four parts:
the Mobile Station (MS), the Base Station Subsystem (BSS), the Network Switching Subsystem (NSS), and Operation and Support Subsystem (OSS).

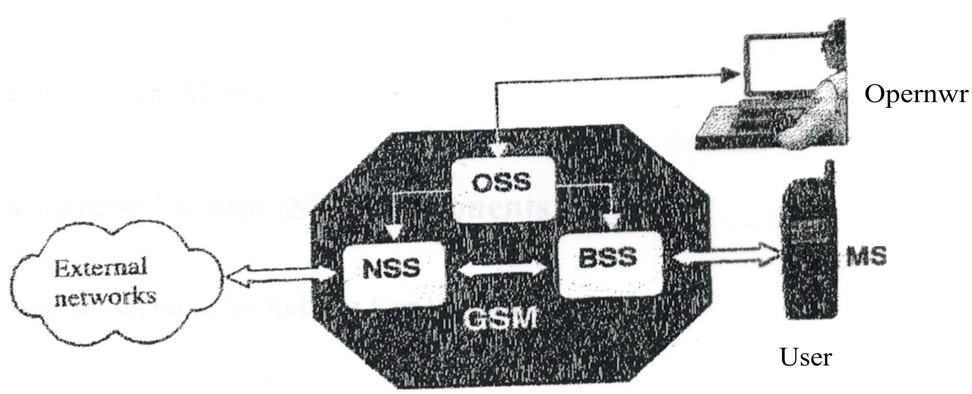


Figure 1.3 GSM Architecture

CHAPTER TWO

GSM COMPONENTS

2.1 GSM Network Components

The GSM network is divided into two systems. Each of these systems is comprised of a number of functional units, which are individual components of the mobile network. The two systems are:

- Switching System (SS)
- Base Station System (BSS)

In addition, as with all telecommunications networks, GSM networks are operated, maintained and managed from computerized centers.

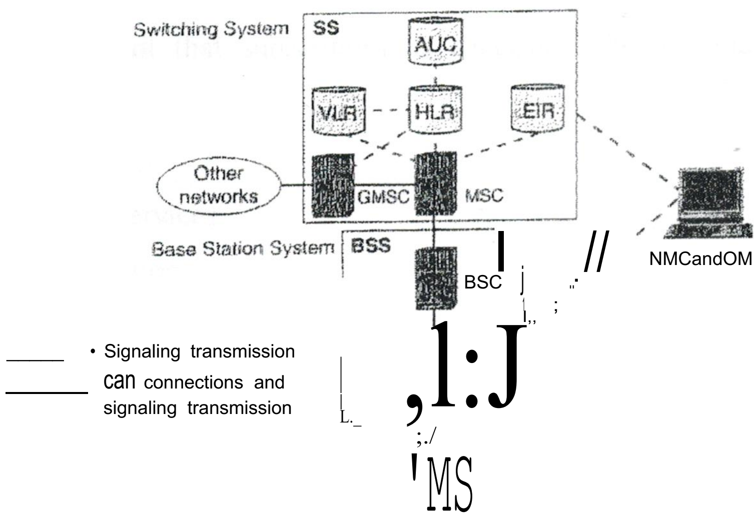


Figure 2.1 System Model

2.2 Switching System (SS) Components

2.2.1 Mobile services Switching Center (MSC)

The MSC performs the telephony switching functions for the mobile network. It controls calls to and from other telephony and data systems, such as the Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), public data networks, private networks and other mobile networks.

Gateway Functionality

Gateway functionality enables an MSC to interrogate a network's HLR in order to route a call to a Mobile Station (MS). Such an MSC is called a Gateway MSC (GMSC) For example, if a person connected to the PSTN wants to make a call to a GSM mobile subscriber, then the PSTN exchange will access the GSM network by first connecting the call to a GMSC. The same is true of a call from an MS to another MS.

Any MSC in the mobile network can function as a gateway by integration of the appropriate software.

2.2.2 Home Location Register (HLR)

The HLR is a centralized network database that stores and manages all mobile subscriptions belonging to a specific operator It acts as a permanent store for a person's subscription information until that subscription is canceled. The information stored includes:

- Subscriber identity
- Subscriber supplementary services
- Subscriber location information
- Subscriber authentication information

The HLR can be implemented in the same network node as the MSC or as a stand-alone database. If the number of subscribers exceeds the capacity of a HLR, additional HLRs may be added.

2.2.3 Visitor Location Register (VLR)

The VLR database contains information about all the mobile subscribers currently located in an MSC service area. Thus, there is one VLR for each MSC in a network The VLR temporarily stores subscription information so that the MSC can service all the subscribers currently visiting that MSC service area. The VLR can be regarded as a distributed HLR as it holds a copy of the HILR information stored about the subscriber When a subscriber roams into a new MSC service area, the VLR connected to that MSC requests information about the subscriber from the subscriber's HLR.

The HLR sends a copy of the information to the VLR and updates its own location information. When the subscriber makes a call, the VLR will already have the information required for call set-up.

2.2.4 Authentication Center (AUC)

The main function of the AUC is to authenticate the subscribers attempting to use a network. In this way, it is used to protect network operators against fraud The AUC is a database connected to the HLR which provides it with the authentication parameters, and ciphering keys used to ensure network security.

2.2.5 Equipment Identity Register (EIR)

The EIR is a database containing mobile equipment identity information, which helps to block calls from stolen, unauthorized, or defective MSs. It should be noted that due to subscriber-equipment separation in GSM, the barring of MS equipment does not result in automatic barring of a subscriber.

2.3 Base Station system (BSS) Components

2.3.1 Base Station Controller (BSC)

The BSC manages all the radio-related functions of a GSM network. It is a high capacity switch that provides functions such as MS handover, radio channel assignment and the collection of cell configuration data. A number of BSCs may be controlled by each MSC

2.3.2 Base Transceiver Station (BTS)

The BTS controls the radio interface to the MS The BTS comprises the radio equipment such as transceivers and antennas, which are needed to serve each cell in the network. A group of BTSs arc controlled by a BSC

2.4 Network Monitoring Centers

2.4.1 Operation and Maintenance Center (OMC)

An OMC is a computerized monitoring center, which is connected to other network components such as MSCs, and BSCs via X.25 data network links. In the OMC, staffs are presented with information about the status of the network and can monitor and control a variety of system parameters. There may be one or several OMCs within a network depending on the network size.

2.4.2 Network Management Center (NMC)

Centralized control of a network is done at a Network Management Center (NMC) Only one NMC is required for a network and this controls the subordinate OMCs. The advantage of this hierarchical approach is that staff at the NMC can concentrate on long term system-wide issues, whereas local personnel at each OMC can concentrate on short term, regional issues.
OMC and NMC functionality can be combined in the same physical network node or implemented at different locations

2.5 lVIobileStation (MS)

A mobile subscriber to communicate with the mobile network uses an MS. Several types of MSs exist, each allowing the subscriber to make and receive calls. Manufacturers of MSs offer a variety of designs and features to meet the needs of different markets

The range or coverage area of an MS depends on the output power of the MS. Different types of MSs have different output power capabilities and consequently different ranges. For example, hand-held MSs have a lower output power and shorter rang than car-installed MSs with a roof mounted antenna.

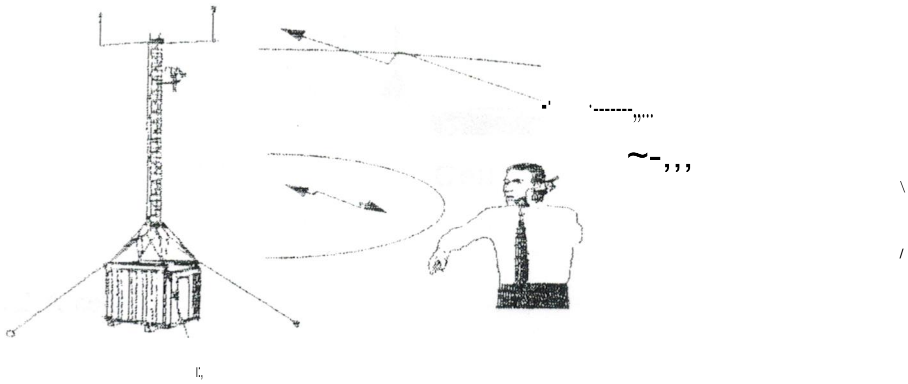


Figure 2.2 Ranges for different types ofMSs

GSM MSs consist of:

- A mobile terminal
- A Subscriber Identity Module (SIM)

Unlike other standards, in GSM the subscriber is separated from the mobile terminal. Each subscriber's information is stored as a "smart card" SIM. The SIM can be plugged into any GSM mobile terminal. This brings the advantages of security and portability for subscribers. For example, subscriber A's mobile terminal may have been stolen. However, subscriber A's own SIM can be used in another person's mobile terminal and the calls will be charged to subscriber A.

2.6 GSM Geographical Network Structure

Every telephone network needs a specific structure to route incoming calls to the correct exchange and then on to the subscriber. In a mobile network, this structure is very important because the subscribers are mobile. As subscribers move through the network, these structures are used to monitor their location.

2.6.1 Cell

A cell is the basic unit of a cellular system and is defined as the area of radio coverage given by one BS antenna system. Each cell is assigned a unique number called Cell Global Identity (CGI). In a complete network covering an entire country, the number of cells can be quite high.

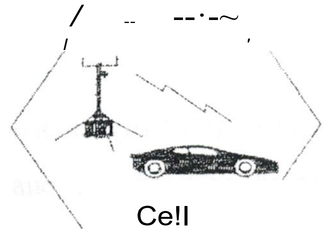


Figure 2.3 A cell

2.6.2 Location Area (LA)

A Location Area (LA) is defined as a group of cells. Within the network, a subscriber's location is known by the LA, which they are in. The identity of the LA in which an MS is currently located is stored in the VLR. When an MS crosses a boundary from a cell belonging to one LA into a cell belonging to another LA, it must report its new location to the network. When an MS crosses a cell boundary within an LA, it does need to report its new location to the network. When there is call for an ~MS, a paging message is broadcast within all cells belonging to an LA

- **MSC Service Area**

An MSC service area is made up of a number of LAs and represents the geographical part of the network controlled by one MSC. In order to be able to route a call to an MS, the subscriber's MSC service area is also recorded and monitored.
The subscriber's MSC service area is stored in the HLR

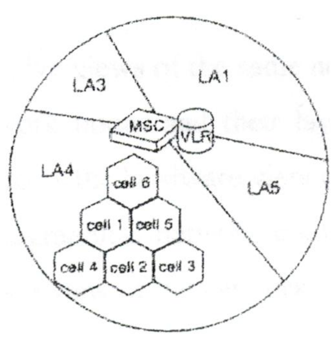


Figure 2.4 MSC service area

- **PLMN SERVICE AREA**

A Public Land Mobile Network (PLMN) service area is the entire set of cells served by one network operator and is defined as the area in which an operator offers radio coverage and access to its network. In any one country there may be several PLMIN service areas, one for each mobile operator's network.

- **GSM SERVICE AREA**

The GSM service area is the entire geographical area in which a subscriber can gain access to a GSM network. The GSM service area increases as more operators sign contracts agreeing to work together. Currently, the GSM service area spans dozens of countries across the world from Ireland to Australia and South Africa.
International roaming is the term applied when an MS moves from one PLMIN to another when abroad.

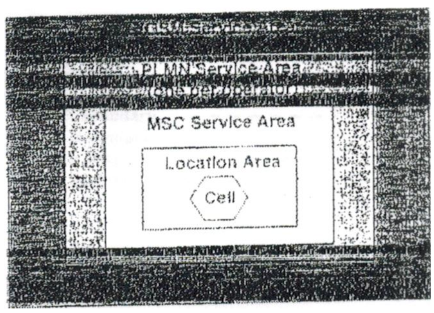
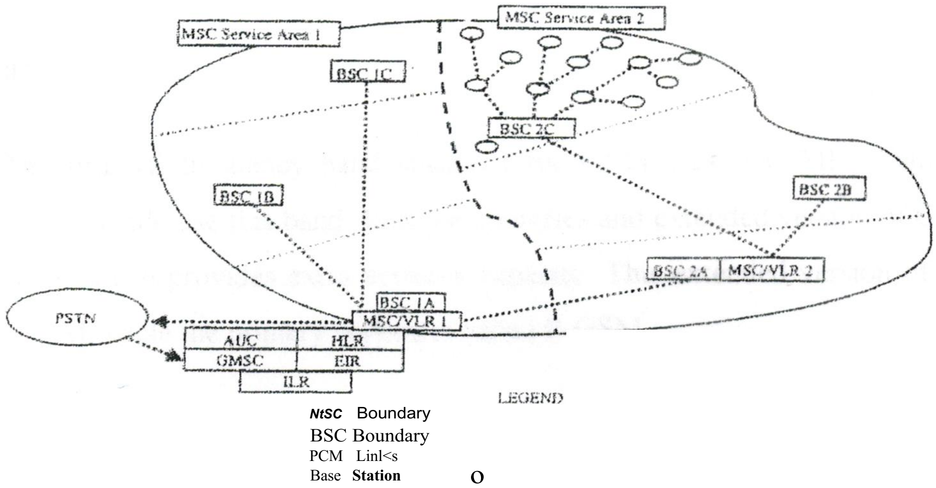


Figure 2.5 Relation Between areas and GSM

The figures below show alternative views of the same network:

- The first figure shows the network nodes and their layout across the network. For simplicity,this may be referred to as the hardware view of the network.
- The second figure shows the geographical network configuration. For simplicity,this may be referred to as the software view of the network.



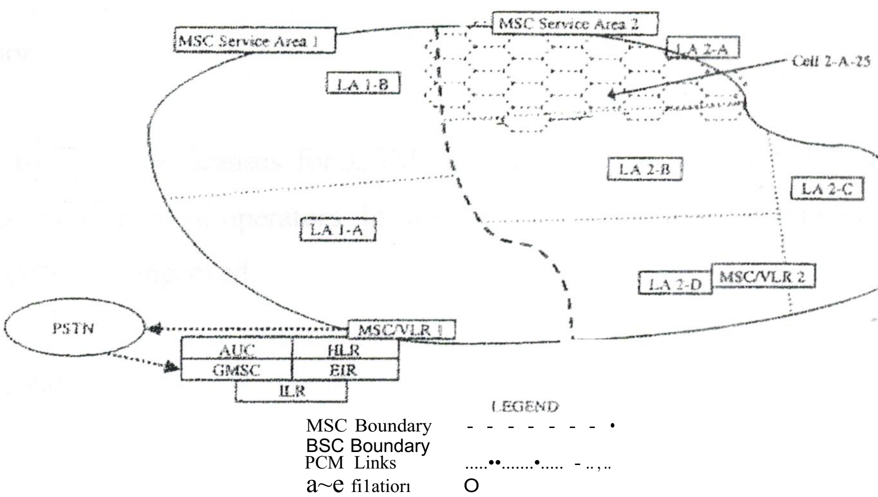


Figure 2.6 "Hardware and Software" view of a sample network

2.7 GSM Frequency Bands

As GSM has grown worldwide, it has expanded to operate at three frequency bands: 900, 1800 and 1900

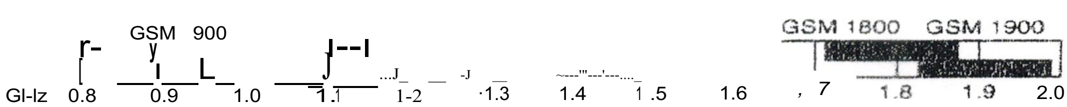


Figure 2.7 GSM Frequency Bands

GSM 900

The original frequency band specified for GSM was 900 MHz. Most GSM networks worldwide use this band. In some countries and extended version of GSM 900 can be used, which provides extra network capacity. This extended version of GSM is called E-GSM, while the primary version is called P-GSM.

In 1990, in order to increase competition between operators, the United Kingdom requested the start of a new version of GSM adapted to the 1800 Ml-lz frequency band. Licenses have been issued in several countries and networks are in full operation.

By granting licenses for GSM 1800 in addition to GSM 900, a country can increase the number of operators In this way, due to increased competition, the service to subscribers is improved.

GSM 1900

In 1995, the Personal Communications Services (PCS) concept was specified in the United States. The basic idea is to enable "person-to-person" communication rather than "station-to station". PCS does not require that such services be implemented using cellular technology, but this has proven to be the most effective method. The frequencies available for PCS are around 1900 MHz..

As GSM 900 could not be used in North America due to prior allocation of the 900 MHz frequencies, GSM 1900 MHz is seen as an opportunity to bridge this gap. The main differences between the American GSM 1900 standard and GSM 900 is that it supports ANSI signaling

GSM 400

Ericsson and Nokia support the work of ETSI on a global standard for GSM on the 450 Ml-Iz frequency band.

Ericsson and Nokia are aiming to make GSM 450 products available for the market during 2001. The believe is that the introduction of GSM in the 450 *NIHz* frequency band will further leverage the success of global GSM.

GSM 400 also provides NMT system operators a logical way to introduce quality digital services and seamless international roaming possibilities.

2.8 Key Terms

During the development of mobile systems, many terms arose which are used to describe the call cases and situations involving MSs. The primary terms used are described below

An MS can have one of the following states:

- **Idle:** the MS is ON but a call is not in progress
- **Active:** the MS is ON and a call is in progress
- **Detached:** the MS is OFF

The following table defines the key terms used to describe GSM mobile traffic cases (there are no traffic cases in detached mode):

Table 2.1 key terms

Mode	Term	Description
Idle	Registration	This is the process in which an MS informs a network that it is attached
	Roaming	When an MS moves around a network in idle mode, it is referred to as roaming
	International Roaming	When an MS moves into a network, which is not its home network, it is referred to a international roaming MSs can only roam into networks with which the home network has a roaming agreement.

Mode	Term	Description
Idle	Location Updating	An MS roaming around the network must inform the network when it enters a new LA. This is called location updating
	Paging	This is the process whereby a network attempts to contact a particular MS. This is achieved by broadcasting a paging message containing the identity of that MS.
Active	Handover	This is the process in which control of a call is passed from one cell to another while the MS moves between cells.

2.9 MS Registration and Roaming

When an MS is powered off it is detached from the network. When the subscriber switches power on, the MS scans the 9"SM frequencies for special channels called control channels. When it finds a control channel, the MS measures the signal strength it receives on that channel and records it When all control channels have been measured, the MS tunes to the strongest one.

When the MS has just been powered on, the MS must register with the network, which will then update the MS' s status to idle. If the location of the MS is noticed to be different from the currently stored location then a location update will also take place.

As the MS moves through the network, it continues to scan the control channels to ensure that it is tuned to the strongest possible channel. If the MS finds one, which is stronger, then the MS retunes to this new control channel" If the new control channel belongs to a new LA, the MS will also inform the network of its new location.

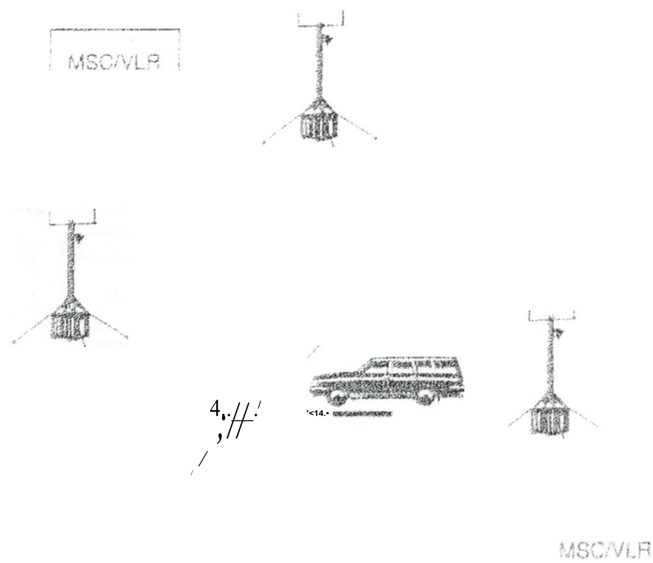


Figure 2.8 Roaming

Chapter Three

Switching System

3.1 Introduction

The Switching System contains the following components

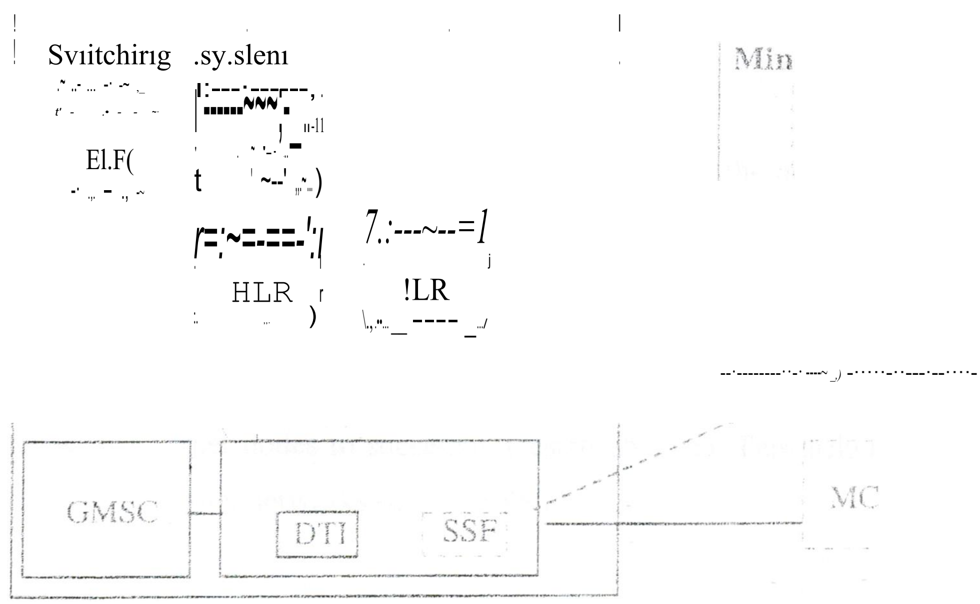


Figure 3.1 Switching Systems

Table 3.1 Switching System components

Type	Abbrev.	Full component name	Platform
Basic	MSC/VLR	Mobile services Switching Center/Visitor Location Register	AXE
	GMSC	Gateway MSC	AXE
	HLR	Home Location Register	AXE
	ILR	Interworking Location Register	A)CE
	A.UC	Authentication Center	Unix /A.)(E
	ELR	Equipment Identity Register	Unix
	DTI	Data Transmission Interface	A.)(E

Additional	MC SSP SCP SDP	Message Center Service Switching Function Service Control Function Service Data Point	MXE AXE AXE Unix

Each network component is described in the remainder of this chapter.

3.2 Mobile Services Switching Center/visitor Location Register (lVISCNLR)

3.2.1 MSC Function

The primary node in a GSM network is the MSC. It is the node, which controls calls both to MS' s and from MS' s. The primary functions of an MSC include the following:

- **Switching and call routing: A MSC** controls call set-up, supervision and release and may interact with other nodes to successfully establish a call. This includes routing of calls from MS's to other networks such as a PSTN.

- **Charging:** an MSC contains functions for charging mobile calls and information about the particular charge rates to apply to a call at any given time or for a given destination. During a call it records this information and stores it after the call, e.g. for output to a billing center.

- **Service provisioning:** supplementary services are provided and managed by a MSC. In addition, the SMS service is handled by MSC' s.

- **Communication with HLR:** the primary occasion on which an MSC and HLR communicate is during the set-up of a call to an MS, when the HLR requests some routing information from the MSC' s..

- **Communication with the VLR:** associated with each MSC is a VLR, with which it communicates for subscription information, especially during call set-up and release.

• **Communication with other MSC's:** it may be necessary for two MSC's to communicate with each other during call set-up or handovers between cells belonging to different MSC's.

• **Control of connected BSC'** s: as the BSS acts as the interface between the MS' s and the SS, the MSC has the function of controlling the primary BSS node the BSC Each MSC may control many BSC's, depending on the volume of traffic in a particular MSC service area. An MSC may communicate with its BSC's during, for example, call set-up and handovers between two BSC's.

• **Direct access to Internet services:** traditionally, an MSC accessed the Internet nodes of an Internet Service Provider (ISP) via existing networks such as the PSTN. However, this function enables an MSC to communicate directly with Internet nodes, thus reducing call set-up time. Direct access can be provided by using an access server called Tigris (from Advanced Computer Communications). This may be integrated in an MSC or stand-alone connected to an MSC

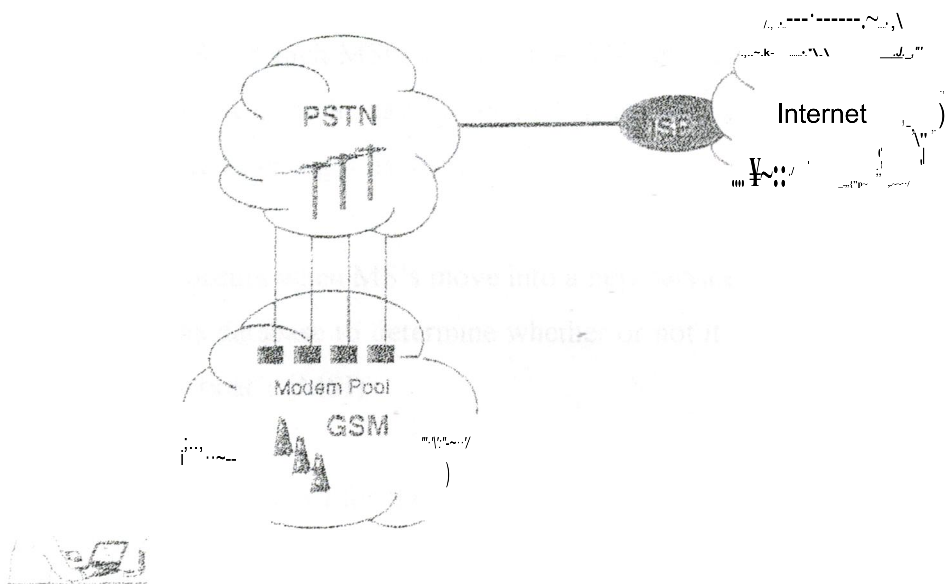


Figure 3.2 Internet access via GSM/PSTN (traditional method)

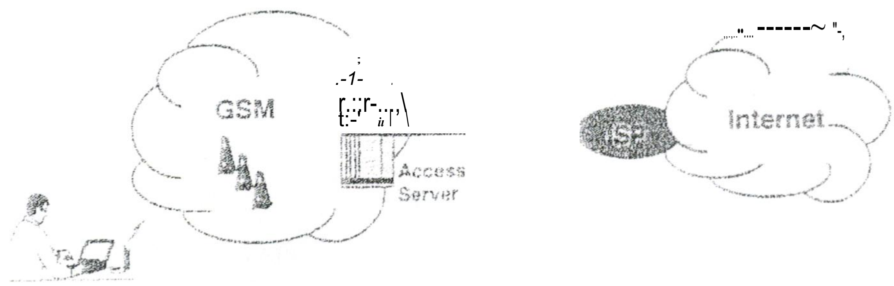


Figure 3.3 Direct access to Internet

- **ISDN Primary Rate Access (PRA):** this function enables an MSC to provide PRA services to subscribers. One network operator can offer PABX connection services, through the PLMN. In this way the operator can compete directly with PSTN operators for ISDN business subscribers.

3.2.2 VLR Function

The role of a VLR in a GSM network is to act as a temporary storage location for subscription information for MSs which are within a particular MSC service area. Thus, there is one VLR for each MSC service area. This means that the MSC does not have to contact the HLR (which may be located in another country) every time the subscriber uses a service or changes its status.

The following occurs when MS' s move into a new service area:

1. The VLR checks its database to determine whether or not it has a record for the MS (based on the subscriber's IMSI)

2. When the VLR finds no record for the MS, it sends a request to the subscriber's HLR for a copy of the MS' s subscription

3. The HLR passes the information to the VLR and updates its location information for the subscriber. The HLR instructs the old VLR to delete the information it has on the MS

4 The VLR stores its subscription information for the MS, including the latest location and status (idle)

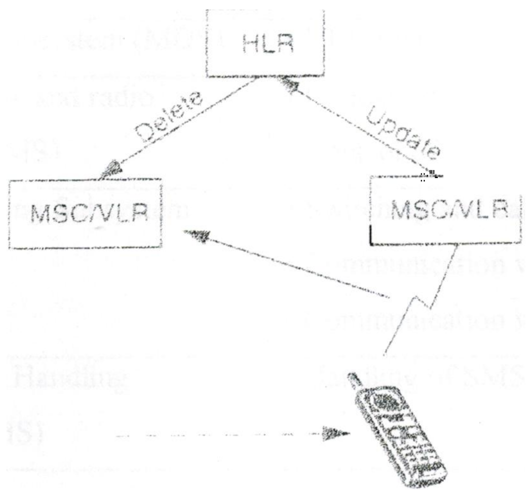


Figure 3.4 VLR-HLR interaction

For the duration when the MS is within one MSC service area, then the VLR contains a complete copy of the necessary subscription details, including the following information:

• Identity numbers for the subscriber

• Supplementary service information (e.g. whether the subscriber has call forwarding on busy activated or not)

• Activity ofMS (e.g. idle)

• Current LA of MS

3.2.3 MSCNLR Implementation

The MSC and VLR are integrated in the same AXE-based node. The reason for this is that there is an extensive amount of information exchange between the two nodes for every call, particularly during call set-up. The MSCVLR interface is completely internal within the AXE, but each is treated as a distinct and separate function. J

An MSC/VLR contains the common APZ and APT subsystems described previously, along with the subsystems in the following table, each of which is implemented in software only.

Table 3.2 MSC/VLR Subsystems

Subsystem	Functions
Mobile Data Subsystem (MDS)	• VLR functions
Mobile Mobility and radio Subsystem (MlvlS)	• Control ofBSCs • Control of handovers involving the MSC
Mobile Switching Subsystem (MSS)	• Switching and call routing • Communication with HLRs • Communication with other MSCs
Short message Handling Subsystem (SHS)	• Handling of SMS messages

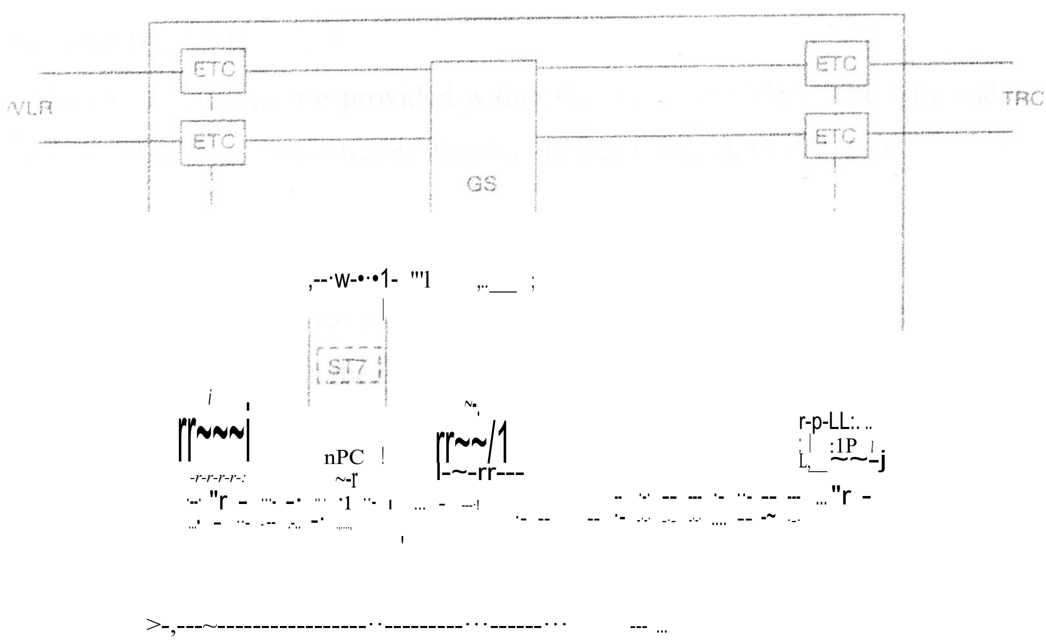


Figure 3.5 MSC/VLR hardware

3.3 Gateway MSC (GMSC)

3.3.1 GMSC Functions

Gateway functionality enables an MSC to interrogate a HLR in order to route a mobile terminating call. It is not used in calls from MS's to any terminal other than another MS.

For example, if a person connected to the PSTN wants to make a call to a GSM mobile subscriber, then the PSTN exchange will access the GSM network by first connecting the call to a GMSC. The GMSC requests call routing information from the HLR that provides information about which MSC/VLR to route the call to. The same is true of a call from an MS to another MS.

3.3.2 GMSC Implementation

Any MSC in the mobile network can function as a gateway by integration of the appropriate software and definition of HLR interrogation information. In effect it then becomes a GMSC/VLR.

Gateway functions are provided within the subsystem MSS. The only additional hardware required is hardware to interface to the signaling link to the HLR.

Gateway Function:

1.Find and interrogate HLR for roaming number.

2.Route the call according to the interrogation.

3.4 Home Location Register (HLR)

3.4.1 HLR Functions

The HLR is a centralized network database that stores and manages all mobile subscriptions belonging to a specific operator. It acts as a permanent store for a person's subscription information until that subscription is cancelled. The information stored includes·

- Subscriber identity (i e. IMSI, MSISDN)
- Subscriber supplementary services

- Subscriber location information (i.e. MSC service area)
- Subscriber authentication information

The primary functions of the HLR include:

- **Subscription database management:** as a database, the HLR must be able to process data quickly in response to data retrieval and update requests from other network nodes. For this reason it acts as a database management system. Each subscriber record contains a substantial amount of parameters.
- **Communication with MSC's:** when setting up calls to an MS, it is necessary for the HLR to contact the MSC serving the MS for routing information. By analyzing the MSISDN, MSC knows which HLR to contact worldwide for that MS's subscription.
- **Communication with GMSC's:** during call set-up to an MS, the GMSC requests MS location information from the HLR, which then provides this in the form of routing information. Also, if the subscriber is detached the HLR will inform the GMSC that there is no need to perform further routing of the call.
- **Communication with AUC's:** before any activity involving change or use of subscription information takes place, the HLR must retrieve new authentication parameters from an AUC.
- **Communication with** VLR's / ILR's: when an MS moves into a new MSC service area the VLR for that area requests information about the MS from the HLR of the subscriber.

The HLR provides a copy of the subscription details, updates its MS location information and instructs the old VLR to delete the information it has about that MS. As the ILR acts as a VLR for AMPS subscribers,' the HLR communicates with it in a similar way.

3.4.2 HLR Implementation

The HLR can be implemented in the same network node as the MSC/VLR (i e. MSC/VLR/HLR) or as a stand-alone database. An MSC/VLR/HLR node is a suitable solution for a small startup GSM network as it saves hardware and signaling load on the links between MSC/VLR and HLR.

A stand-alone HLR is a suitable solution for large networks. It has the following advantages

There are no traffic disturbances creating better reliability

When the HLR is separate from the *.MSC/\TT~R,* there is more capacity available for call handling in the :MSC/VLR

If the number of subscribers exceeds the capacity of a HLR, additional HLR' s may be added

HLR Redundancy

In order to provide additional network reliability, an additional "mated" HLR is used to mirror the data in a HLR and can automatically take over if required.

System Structure

The HLR is an A,XE-based i~~/\1 called HLRA.,."1\1. Along with the standard APZ and APT subsystems the HLR includes the APT subsystem Home location Register Subsystem (HRS) that performs the necessary subscription management.

3.5 Interworking Location Register (ILR)

3.5.1 ILR Functions

ILR offers roaming capabilities between mobile telephony systems complying with different standards. The ILR is specific to the GSMl 900 product portfolio and enables ,.1~l\1PS network subscribers to roam to a GSM 1900 network.

In the near future the ILR will make intersystem roaring possible both directions between all GSM, AMPS/TDMA networks.

For A11PS subscribers who wish to avail of this roaming functionality, their Al\1PS network subscriptions are copied into the HLR side of the ILR. When they roam into the GSM 1900 network, the I-ILR copies this information into the VLR side of the ILR as occurs for normal GSM roaming subscribers.

From the subscriber's point of view however, there is only one subscription.

In the near future, the ILR will make intersystem roaming possible in both directions between all GSM, A11PS/TDJ\1A networks

3.5.2 ILR Implementation

In Ericsson's GSM systems the ILR is AXE-based. It includes the common *APZ* and APT subsystems outlined previously and the following additional subsystems

Table 3.3 ILR subsystems

Subsystem	**Functions**
Home location Register Subsystem (IIRS)	• AlvfPS Subscriber database management
Mobile Intersystem roaming Subsystem (MIS)	• Mapping and translation of services and protocols • Communication with other nodes

ILR hardware is similar to ILR hardware.

3.6 Authentication Center (AUC) and Equipment Identity Register (EIR)

PLMN' s need a higher level of protection than traditional telecommunication networks. Therefore, to protect GSM systems, the following security functions have been defined:

-Subscriber **authentication:** by performing authentication, the network ensures that no unauthorized users can access the network, including those that are attempting to impersonate others.

-Radio **information ciphering:** the information sent between the network and an MS is ciphered. An MS can only decipher information intended for it.

-Mobile **equipment identification:** because the subscriber and equipment are separate in **GSM,** it is necessary to have **a** separate authentication process for the MS equipment. This ensures, e g. that a mobile terminal, which has been stolen, is not able to access the network.

-Subscriber **identity** confidentiality during communication with an MS over a radio link, it is desirable that the real identity (IMSI) of the MS is not always transmitted. Instead a temporary identity (TMSI) can be used. This helps to avoid subscription fraud

The AUC and EIR are involved in the first three of the above features, while the last is handled by MSC/VLRs.

3.6.1 AUC Functions

The primary function of an AUC is to provide information, which is then used by an MSC/VLR to perform subscriber authentication and to, establish ciphering procedures on the radio link between the network and MS' s.

The information provided is called a triplet and consists of:

1. A non predictable RANDom number (RAND)
2. A Signed RESponse (SRES)
3. A ciphering Key (Kc)

Provision of Triplets

At subscription time, each subscriber is assigned a subscriber authentication Key (Ki). Ki is stored in the AUC along with the subscriber's IMSI. Both are used in the process of providing a triplet. The same Ki and IMSI are also stored in the SIM. In an AUC the following steps are carried out to produce one triplet:

1. A non-predictable random number, RAND, is generated
2. RAND and Ki are used to calculate SRES and Kc, using two different algorithms, A3 and A8 respectively
3. RAND, SRES and Kc are delivered together to the HLR as a triplet

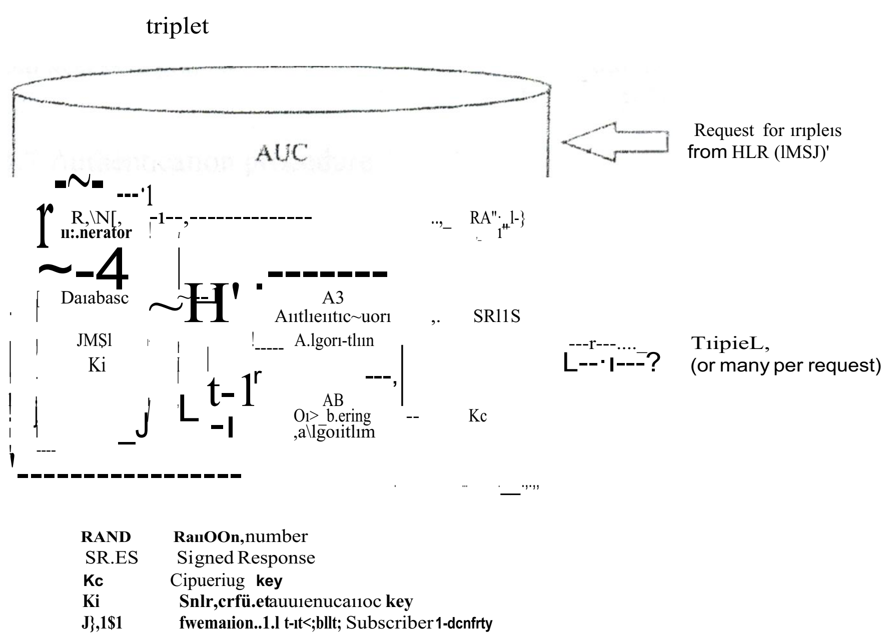


Figure 3.6 Provision of triplet

Authentication Procedure

1. The MSC/VLR transmits the RAND to the MS.

2. The MS computes the signature SRES using RAND and the subscriber authentication key (Ki.) through the A3 algorithm.

3. The MS computes the Kc by using Ku and RAND through A8 algorithm. Kc will thereafter be used for ciphering and deciphering in MS.

4. The signature SRES is sent back to MSC/VLR, which performs authentication, by checking whether, the SRES from the MS and the SRES from the AUC match. If so, the subscriber is permitted to use the network. If not, the subscriber is barred from network access.

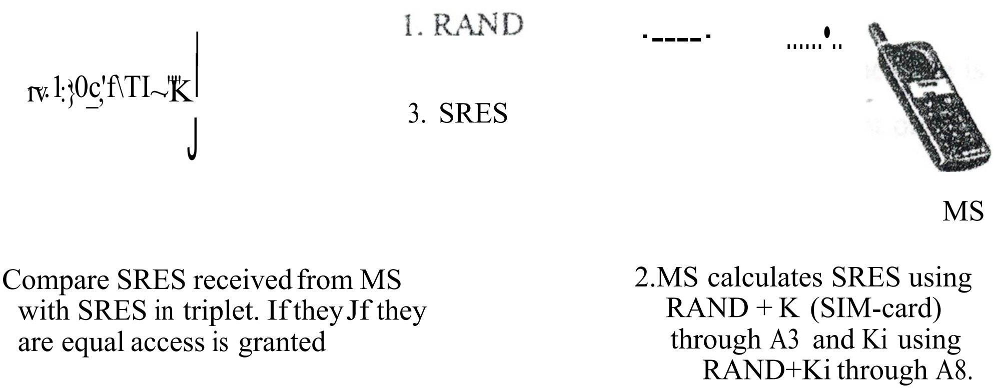


Figure 3.7 Authentication procedure

Authentication can by operator's choice be performed during:

- Each registration
- Each call setup attempt
- Location updating
- Before supplementary service activation and deactivation There can be exceptions for subscribers belonging to other PLMN' s.

Ciphering Procedure

Confidentiality· means that user information and signaling exchanged between BTS's and MS's is not disclosed to unauthorized individuals, entities or processes.

A ciphering sequence is produced using Kc and the TDMA frame number as inputs in the encryption algorithm AS. The purpose of this is to ensure privacy concernıng user information (speech and data) as well as user related signaling elements.

In order to test the ciphering procedure some sample of information must be used. For this purpose the actual ciphering mode command (M) is used.

1. Mand Kc are sent from the MSC/VLR to the BTS.
2. Mis forwarded to the MS.
3. M is encrypted using Kc (calculated earlier with SRES in the authentication procedure) and the TDMA frame number, which are fed through the encryption algorithm, AS.
4. The encrypted message is sent to the BTS.
5. Encrypted M is decrypted in the BTS using Kc, the TDMA frame number and the decryption algorithm, AS.

6.If the decryption of M was successful, the ciphering mode completed message is sent to the MSC. All information over the air interface is ciphered from this point on.

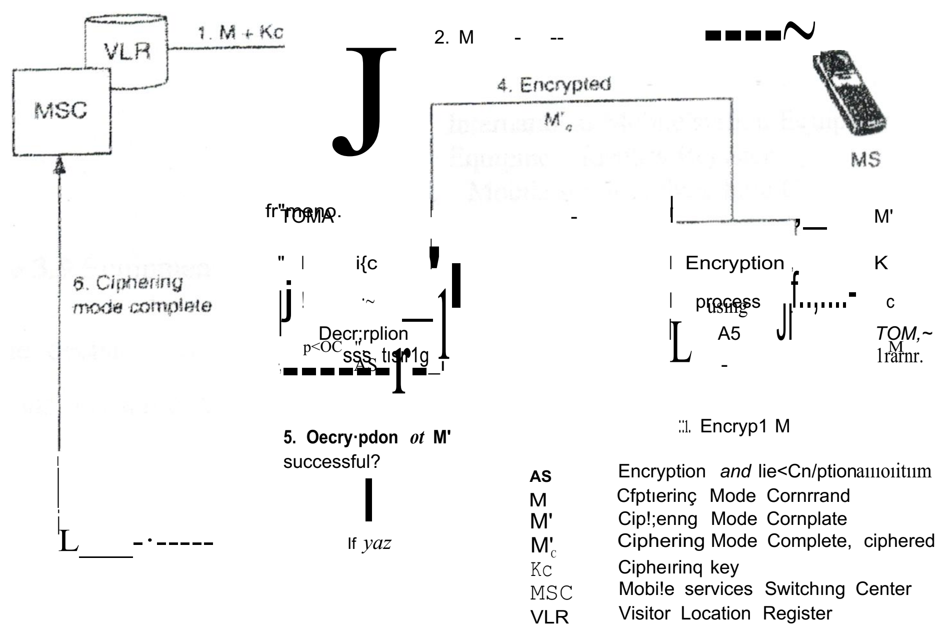


Figure 3.8 cipheringprocedure

3.6.2 EIR Functions

Equipment Identification Procedure

The equipment identification procedure uses the identity of the equipment itself (IMEI) to ensure that the MS terminal equipment is valid.

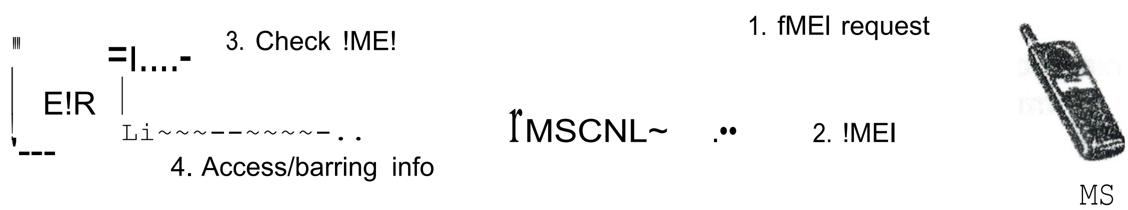
1. The MSCNLR requests the IMEI from the MS.
2. MS sends IMEI to MSC.
3. MSC/VLR sends IMEI to EIR.
4. On reception of IMEI, the EIR examines three lists:

• A **white list** containing all number series of all equipment identities that have been allocated in the different participating GSM countries.

• A **black list** containing all equipment identities that has been barred.

• A **gray list (**on operator level) containing faulty or non -approved mobile equipment.

5. The result is sent to MSC/VLR, which then decides whether or not allow network access for the terminal equipment.



IMEI International Mobile station Equipment Identity
EIR Equipment Identity Register
MSCNLR Mobile services Switching Center

Figure 3.9 Equipment identification

The decision to identify equipment remains with individual operators. GSM specifications recommend identification for each attempted call set-up.

3.6.3 AUC and EIR Implementation

In a GSM network the AUC is connected directly to a HLR. The EIR is connected to an MSC/VLR.

AUC may be implemented on either AXE or Unix (from Sema Group). The EIR is implemented on a Unix platform from Sema Group.

If implemenıed on AXE, the most common configuration for an AUC is integrated with a HLR as an AUC/HLR node. This reduces the signal processing requirements of both. The AUG is implemented using the AUG Application Module (AUCAM).

The most common implementation is a Unix-based AUC/EIR node, which provides the following benefits to the operator:

- AUC and EIR processing is physically separated from the switching function in the MSC. This provides better network planning flexibility when the network needs to be expanded.
- The common platform is based on standard industry computer hardware (HW) and software (SW).

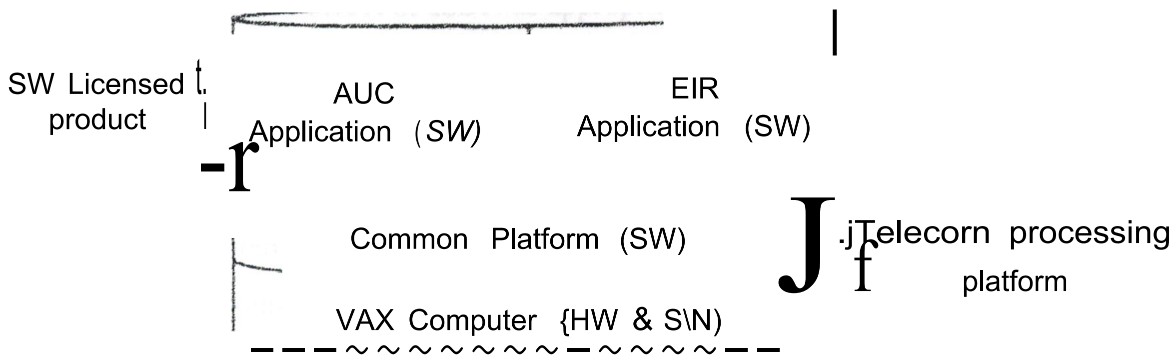


Figure 3.10 AUC / EIR product structure

3.7 Data Transmission lnterface-{DTI)

This section gives a brief introduction to the data handling capabilities of GSM systems. For a more detailed survey of such functions, please refer to the appendix titled "Data Services".

3.7.1 DTI Functions

The DTI implements the GSM Inter-Working Function (IWF). It performs data handling functions such as data rate conversion and provides the functions necessary for data interworking between GSM networks and other networks, including:

• **Data Traffic to/from PSTN:** this involves modem and fax calls. For connections to the PSTN a modem is selected by the DTI to perform the necessary rate and format conversions.

• **Data Traffic to/from ISDN:** the whole set of data communications towards ISDN is available, since the MSC/DTI is capable of signaling and mapping basic service information between the ISDN and the GSM network.

• **Data Traffic to/from PDNs:** the DTI handles data traffic to and from Public Data Networks (PDNs) such as the Packet Switched PDN (PSPDN) and Circuit Switched PDN (CSPDN).

• **Data Traffic between** mobiles: the data traffic inside the PLMN must pass through the DTI to handle the protocol used for rate adaptation in the radio path.

• **HSCSD:** this version of High Speed Circuit Switched Data (HSCSD) allows the connection of 2, 3, or 4 time slots on one radio channel each carrying 9.6 k bits/s. The DTI handles rate conversion to PSTN or ISDN as appropriate.

3.7.2 DTI Implementation

The DTI is integrated within an MSCNLR, The :OTI is managed by the Data Transmission Subsystem (DTS).

The DTI sub-rack contains eight plug-in units, each one supporting four data channels. Therefore, each DTI sub-rack can support a total of 32 simultaneous data calls.

3.8 Message Center (MC)

3.8.1 MC Function

An MC may be added to a GSM network to provide one or more of the following messaging services:

• Voice mail
• Fax mail
• Short Message Service (SMS) text messages
• SMS Cell Broadcast (SMSCB) text messages

These services can generate considerable revenue for a network operator, as they are becoming increasingly popular.

Voice Mail

Voice mail ensures that all calls to a person can be completed, even when a person does not answer calls. A calling party can record a voice message for the subscriber they are calling.

A subscriber can use their MS to select diversion to voice mail based on a particular event or status (e.g. busy, unreachable).

The subscriber is informed that they have voice messages in their mailbox by means of either a short text message or phone call from the network at regular intervals. If their MS is detached, this indication is sent when the subscriber next attaches to the network. The subscriber can then retrieve their voice mail messages at a later stage. Functions for storing voice messages over a long period also exist.

Fax Mail

Fax mail operates similarly to voice mail. For MS's that support fax, a subscriber can set diversion for all or some fax calls to a fax mailbox. When the MS is next attached to the network, the network will deliver the fax message to a fax machine identified by the MS.

SMS

A short text message consists of up 160 alphanumeric characters, entered at a Short Message Entity (SME) such as an MS (using the keypad) or computer terminal.

A short message always originates or terminates in a GSM network, meaning that a short message can not be sent between two SMEs residing outside a GSM network.

The short message originator knows if the message delivery is successful or unsuccessful via notification. When a message is submitted, the deferred delivery option can be requested. This option makes it possible to specify the time the message is to be delivered. An MC, which handles SMS messages is often referred to as an SMS Center (SMS-C). When a message is to be forwarded to an MS, the system must first determine where the MS is situated. As in ordinary voice traffic, a gateway requests the routing information. The gateway is called the SMS GMSC.

Each short message is time stamped by the SMS-Center when it is submitted. A message is deleted once the delivery is successful or once the time specified in deferred delivery expires.

When a message is buffered, the SMS-C regularly attempts to deliver the message, at intervals defined by the operator.

SMSCB

The SMSCB service enables a message of up to 93 alphanumeric characters to be delivered to all attached MS' s in one cell. This may be useful for identifying key phone numbers in the cell's area such as that of a hospital or police station. Alternatively, it may be used for advertising services within the cell (e.g. "Superfood Restaurant in this area at the junction ofM8 and 133").

3.8.2 MC Implementation

One MC node may handle one or more messaging service. For example, depending on the amount of SMS traffic, it may be more efficient to have one MC acting as an SMS-C only, with other messaging services handled by another separate MC. It is also possible to integrate SMS-C functions on an MSC, leading to the term SMS Interworking MSC (SMS-IWMSC). Additionally, the SMS GMSC functions may reside in the same node as the GMSC functions used for voice calls.

The most important component of l\1XE is the message kernel. The message kernel is .the central.message store and forward nucleus responsible for safe storage of messages, routing and retry attempts.

SMS~CApplication

MXE Platform

Figure 3.11 SMS-C on l\1XE

3.9 Service Switching Function (SSF), Service Control Function (SCF) and Service Data Point (SOP)

This section gives a brief introduction to the Mobile Intelligent Network (MIN) handling capabilities of Ericsson's GSM systems. For a more detailed survey of such functions, please refer to the appendix titled "Mobile Intelligent Network Services".

Mobile Intelligent Network (MIN) nodes can be added to a basic GSM network to provide value-added services such as Free phone and Personal Number to subscribers. MIN nodes include:

- **Service Switching Function (SSF):** an SSF acts as an interface between the call control functions of the mobile network and the service control functions of a Service Control Point (SCP). SSF is an AXE-based AM (SSFAM) and may be integrated within an MSC/VLR (recommended) or stand-alone.

- **Service Control Function (SCF):** a SCP contains the intelligence of a MIN service or services. This intelligence is realized in software programs and data. SCP is also an AXE-based AM (SCF AM) and the recommended configuration is as a stand-alone node, accessible by all MSC/SSPs.

- **Service Data Point (SDP):** an SDP manages the data, which is used by a MIN service.

Chapter four

MSCNLR OPERATION

4.1 Introduction

The S7 consists of various functional elements where the Message Transfer Part (MTP) is the common platform. MTP serves different user parts, such as Telephony User Part (TUP), Integrated Services Digital Network User Part (ISUP), and other functional elements like Signaling Connection Control Part(SCCP).

SCCP provides additional functionality to fulfill the need for extended services in certain applications.

An example of an extended service is communication with the databases, Home Location Register (HLR) and Visitor Location Register (VLR), without any speech connection, e.g. communication during Location Updating.

The combination of the MTP and the SCCP is called the Network Service Part (NSP).

SCCP supports two network services:

- Connection Oriented (CO)
- Connection Less (CL)

See Figure 4.1.

The CO transfers many or long signaling messages between two nodes. In this case, it makes sense to "establish a logical connection" between the sender and receiver.

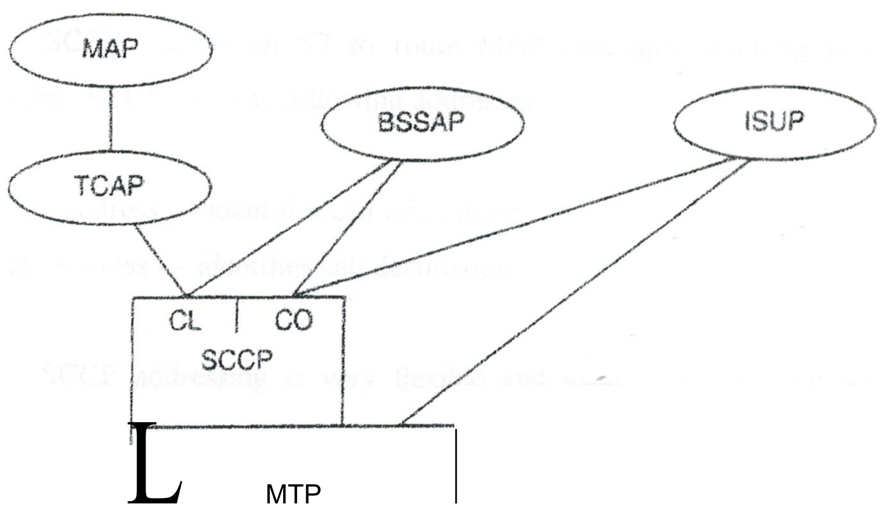
The CL transfers short messages, including routing information, to their destination.

When the MS is powered on in an MSC/VLR service area, the MS must carry out a Location Update. If the IMSI is not recognized in the VLR, the VLR then requests subscriber information from the HLR where the MS' s subscription is held. Remember when a new subscription is taken out, the subscription belongs to one HLR and the MS becomes a visitor whenever it is powered on in a MSC/VLR service area.

The VLR uses MAP signaling to communicate with the HLR to carry out a location update. All MAP signaling uses SCCP and the SCCP nodes are addressed using a Global Title (GT). A GT is similar to a dialed number and is based on the E.164 sen es.

The MS has only sent the IMSI up to the MSC/VLR, which is based on the E.212 series, this is not a dialed number in the telephony network. For the VLR to communicate with the HLR, the IMSI must be modified to a format allowing it to be used in the SCCP network. This new number series is referred to as a Mobile Global Title (MGT) and is based on the E.214 series, made up of the CC + NDC + MSIN. The CC identifies the country code and NDC the network. The MGT is only ever used for Location Updating.

This MGT would then be used to route the MAP signal through the SCCP network from a VLR to the subscribers HLR.



CO = Connection-Oriented

CL= Connection-Less

Figure 4.1 SCCP and other protocols

The protocol between the Mobile services Switching Center/Visitor Location Register (MSC/VLR) and the Base Station Controller (BSC) is called Base Station System Application Part (BSSAP).

BSSAP requires both the Connection Oriented (CO) and the Connection Less (CL) service. The MSC/VLR, HLR, and GMSC communicate via the Mobile Application Part (MAP), using only the Connection Less (CL) mode. The Transaction Capabilities Application Part (TCAP) supports MAP. However, there is no need to describe TCAP functionality to understand how GSM works.

Note: BSSAP and TCAP are not explained here.

While SCCP performs tasks similar to MTP; e.g. routing, SCCP allows only routing ofMAP/BSSAP messages MTP and SCCP should be considered as two different networks that are linked together.

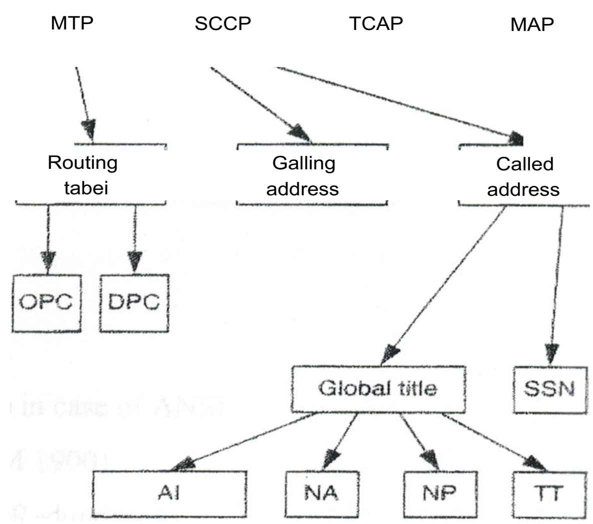
4.2 SCCP Addressing

SCCP enables an S7 to route MAP messages. Routing is always based on addresses. SCCP uses the following addresses:

- Calling address - identifies call origination
- Called address - identifies call destination

SCCP addressing is very flexible and makes use of three separate elements:

- Destination Point Code (DPC)
- Global Title (GT)
- Sub System Numbers (SSN)



NA= Nature of Address

SSN = SCCP Subsystem Number

Al = Address Information

TT = Translation Table

NP = Numbering Plan

Figure 4.4 SCCP addressing

One, two, or three elements may be .present in the address information for the called and the calling party. The form of the address depends on the service, application, and underlying network. The Address Indicator shows which information elements are present.

4.2.1 Global Title (GT)

The GT is of variable length, and can contain specified combinations of:

- Address Information (Al)
- Nature of Address *(NA)*
- Numbering Plan (NP)
- Translation Type (PT)

It does not contain information that allows routing in the signaling network. The translation function is required.

The following sections contain details and typical values for some of the elements previously listed:

Sub System Number (SSN)

The terminating node examines the SSN to identify the concerned user (node).

6 HLR

7 VLR

8 GMSC,MSC

9 EIR

10 AUC

12 SC

222 BSC (BSSAP) in case of ANSJ signaling (GSM 1900)

224 HLR-R (HLR Redundancy)

254 BSÇ (BSSAP) in case of CCITT signaling (GSM *900)*

3 ISUP (ifISUP uses SCCP)

Address Information (Al)

This is an address according to the numbering plan indicated. (See the example in Numbering Plan).

Nature of Address (NA)

NA indicates if the address is

3 National

4 International

format according to the numbering plan used. -

Numbering Plan (NP)

NP indicates the numbering scheme from which the address originates:

1 ISDN/Telephony Numbering Plan (E.163/E.164)
e.g. MSISDN, GT address

7 ISDN/Mobile Numbering Plan (E.2 14)
e.g. IMSI, MGT (Location Updating)

Translation Type (TT)

A GT requires a translation function. The TT directs the message to the appropriate Global.Title (GT) translation.

It is possible for the Address Information (AI) to be translated into different values for different combinations ofDPCs, SSNs and GTs.

0	CCITT signaling
9	ANSI signaling
1-8,	Used for the Service Center (SC) interface
10-254	MTS exchange property SMSFMOSMTRTYPE

Example:

NA=4, NP=l, AI=49 172, TT=O

NP indicates a normal ISDN telephony number. NA indicates international format for AL. Therefore, 49 is the Country Code (CC) for Germany and 172 is the NDC for D2 operator, and the Translation Type (TT) is CCITT signaling.

4.3 iMSi Number Series Analysis

Whenever a new roaming agreement is taken out, then information on how to convert the IMSI to a MGT must be specified in each MSC/VLR; this needs to be specifiedeven for the PLMN' s own subscribers.

The Il\1SI Number Series Analysis also gives information about what the MS is allowed to do within the current PLMN. This can differ from one roaming agreement to another.

```
                    *****   IMSI ~11.JMBER ANALYSIS   *****

HGIS!:  L."!s!SIS=  415  Ol ,
                         M"'  5-961   3 2 ,.  MODIFICATION+MSIN  => NS  (C7GSI)
                         NA=4,                INTER."lATIONAL   NUMBER PLAN
                         A."ffiES=
                         OBA-30&              BO F'OR ORIGINATING  CALLS
                         CBA-63&              CALL  BARRING  FOR  LEBANON  SfJBS.
                         E0=22&
                         PLI1N-O&             ANNOUNCEMENT  LANG.  INDICATION
                         ERI.S-15&          ! ERICSSON  SPECIFIED  SERVICES
                                              B0=1  =>  SPN,  Bl=l  •> IC!,
                                              B2ozl  ::c> OIN,  B3=1  ,,.> DMSISDN
                         MAPVER-1&            MAP  VERSION
                         NPJ~G-0&:            ROAM.  RESTR.  GR<)iJP
                         OI,n.'Ms&          ! OWN  PLMN
                         W\TMS;               NATIONAL  PLMN
```

Figure 4.3 IMSI Number Series AnalysisData Transcript

Figure 4.3 shows the command and some of the parameters to specify a new agreement. The M parameter is the modification from the IMSI to the MGT.

The ANRES parameter specifies what an MS with an IMSI starting with 415 01 is allowed to do in the network.

With regard to Location Updating, two of the A..NRES parameters are of interest, they are:

- ERIS
- MAP V'ER

Both relate to the *MAJ>* signaling requirements between the VLR and the HLR. The value ranges and the meaning of these values are given in the AI for the owning block of the parameter, e.g. 1\1.APVER is owned by MAPVC.

In figure 4.3 the IMSIS of 415 01 is being converted to a :MGT of961 3 2 by the parameter M, M=5-961 3 2. The MGT is in the international format.

To support communication between the VLR and the HLR the ANRES parameters of ERIS and M..APVER are important.

- ERIS is used to identify that the HLR will support Single Personal Number, Immediate Call Itemization, Originating Intelligent Network and Dual MSISDN.
- MAPVER indicates the :MAP that is to be used to the HLR. MAPVER- 1 means that :MAP version 2 is to be used.

Some of the other parameters are mandatory parameters but are not relevant for Location Updating.

The IMSI Number Series Analysis Table is made up of an operating and non-operating side; changes are made to the non-operating side and then switched.

4.4 B-number Analysis

The data described to this point is used to define the Bvnumber analysis tables. An example of an extract of a B-number Analysis table is shown in Figure 4.4

B-NUMBER ANALYSIS DATA

OPERA TING AREA

B-NUMBER	MISCELL	FIN	ROUTE	CHARGE	LA
8-0					
8-1					
8 -2					
S-3					
8-30					
8-31					
8-32					
8-33					
8-34					
8-35					
8-350					
8-351					
Se352					
8-3§3389200			RC=30		11-15
41-0					
41-1					
41-2					
41-3					
41-30					
41-31					
41~32					
41-33					
41-34					
41-35					
41~350					
41-351					
41-352					
41-35387200050			RC=20		11-1$

Figure *4.4* Bsrıumber Analysis Data

4.5 GMSC Call Handling

Back to the example: the incoming call set-up message from the ISDN is received in the GMSC: See Figure4.5

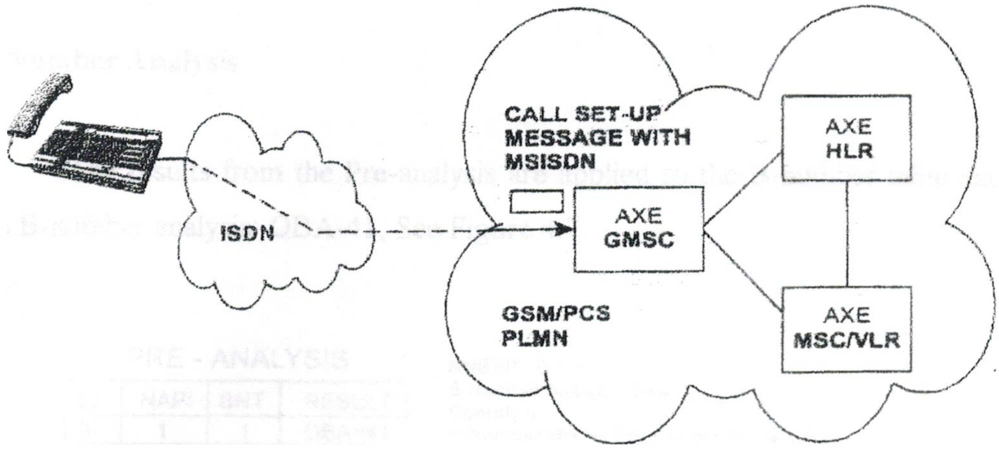


Figure 4.5 Call Set-up Message Received in GMSC

Pre-Analysis of B-Number

In this example, the call set-up message contains the following components:

• B-number (35387200050)

- NAPI=1

- BNT=1

These are transferred to the Register function block RE along with the incoming route data, such as BO=O. The Register Function (RE) initiates the Pre-number analysis.

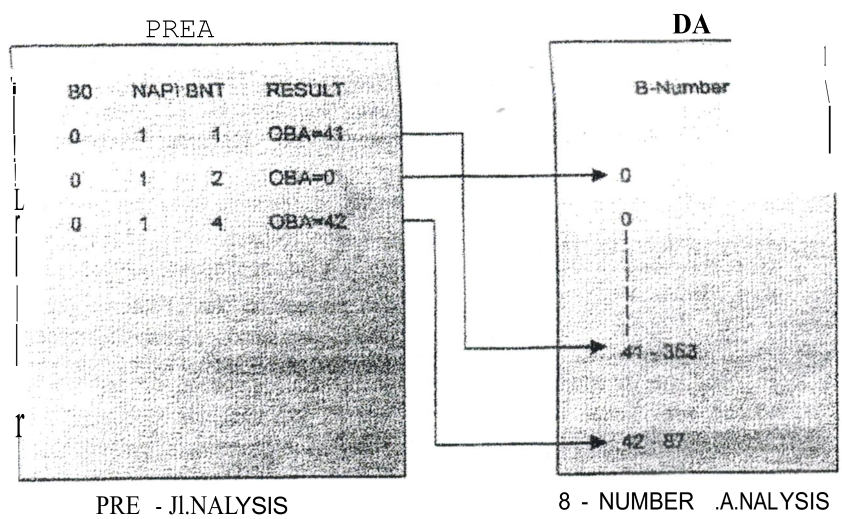


Figure 4.6 Pre-number Analysis

BeNumber **Analysis**

The results from the Pre-analysis are applied to the B-number table and used in the B-number analysis: OBA-41. See Figure 4.7.

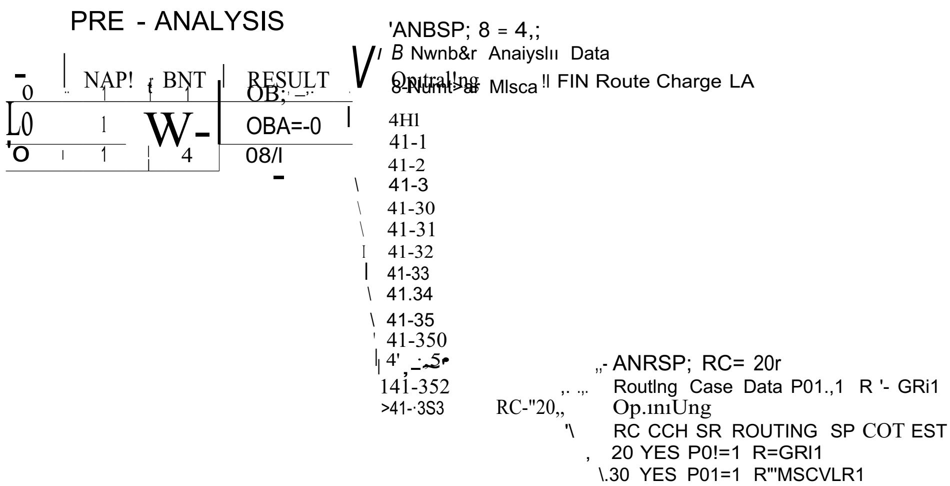


Figure ***4.***7 Analysis Results

CONCLOUSION

A general objective of the GSM system is to provide a wide range of services and facilities, both voice and data. Another objective is to give compatibility considered mobile subscriber the access to any mobile subscriber in any country, which operates the system, and provides facilities for automatic roaming, locating and updating the mobile subscribers status.

As we mentioned in the second chapter the GSM network architecture consist of four parts: the mobile station (MS), the base station subsystem (BSS), the network switching subsystem (NSS) and operation and support subsystem (OSS).

Switching system components are home location register (HLR), visitor location register (VLR), gate way functionality (GMSC), service switching function (SSF), service control function (SCF), equipment identity register (EIR) and authentication center (AUC), Network switching subsystem (NSS) which is the mobile switching center (MSC).

The primary node in a GSM network is the MSC. It is the node, which controls calls both to MS's and from MS's. the primary functions of a MSC are: switching and call routing, charging mobiles, service provisioning, communication with HLR, VLR and MSC's, control of connected BSC's, direct access to internet services and ISDN primary rate access (PRA).

The future generation of GSM will be the use of Phase 3 (3G): different types of services at the same time. UMTS (Universal Mobile Telecommunication System), up to two Mbits/s speed, ability to use multimedia functions, ability to download large files or sites, high quality audio, video conferencing and finallye-commerce.

REFERENCES

[1] Mamedov F.S., Telecommunication, Near East University, Nicosia, 2000.

[2] GSM System Survey, Ericsson Radio Systems AB, Stockholm, 2000.

[3] GSM MSC/Operation, Ericsson Radio System AB, Stockholm, 1999.

[4] AXE / GSM Overview, Ericsson Radio System AB, Stockholm, 1999.