GSM Network Analysis

GL Communications Inc.

818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878
Phone: (301) 670-4784 Fax: (301) 670-9187 Email: **info@gl.com**
Website: **http://www.gl.com**

What is GSM ?

Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation.

What is GSM ?

Based on ETSI standards

- GSM is a digital system with an over-the-air bit rate of 270 kbps. The frequency range is 1,850 to 1,990 MHz (mobile station to base station)
- GSM utilizes the time or frequency division multiple access (TDMA / FDMA) concept
- GSM uses Gaussian minimum shift keying (GMSK)
- GSM specifications follow the stipulations for the bottom three layers (physical, data link, & network layers) of the OSI model.

Advantages of GSM over Analog System

- Capacity increases
- Reduced RF transmission power and longer battery life
- International roaming capability
- Better security against fraud (through terminal validation and user authentication)
- Encryption capability for information security and privacy
- Compatibility with ISDN, leading to wider range of services

GSM Specifications

GSM 900

- Mobile to BTS (uplink): 890-915 Mhz
- BTS to Mobile(downlink):935-960 Mhz
- Bandwidth : 2* 25 Mhz

GSM 1800

- Mobile to BTS (uplink): 1710-1785 Mhz
- BTS to Mobile(downlink) 1805-1880 Mhz
- Bandwidth : 2* 75 Mhz

PCS 1900 or DCS 1900

- The only frequency used in the United States and Canada for GSM

GSM System Architecture

Network Switching Subsystem (NSS) – Its main components include:

- Mobile Switching Center (MSC)
- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Authentication Center (AUC)
- Equipment Identity Register (EIR)

Base Station Subsystem (BSS) – Its main components include:

- Base Transceiver Station (BTS)
- Base Station Controller (BSC)

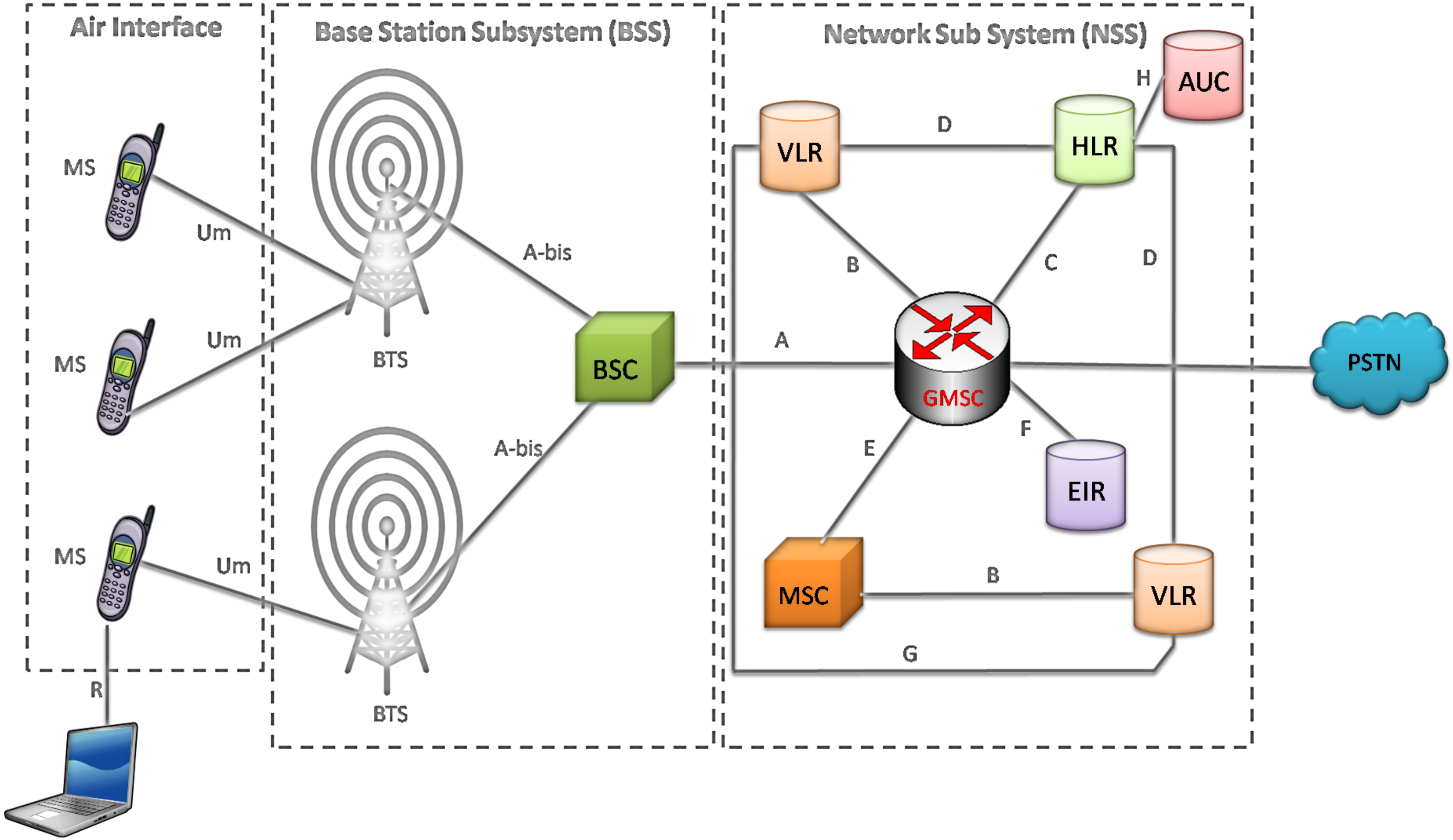
Mobile Station (MS) – Its main components include:

- Mobile Equipment (ME)
- Subscriber Identity Module (SIM)

Operation SubSystem (OSS) – Its main components include:

- Operations and maintenance center (OMC)
- network management center (NMC)
- administration center (ADC)

GSM System Architecture



Base Station Subsystem (BSS)

- Base Transceiver Station (BTS)
  - Encodes, encrypts, multiplexes, modulates and feeds the RF signals to the antenna.
  - Frequency hopping
  - Communicates with Mobile station and BSC
  - Consists of Transceivers (TRX) units
- Base Station Controller (BSC)
  - Manages Radio resources for BTS
  - Assigns Frequency and time slots for all MS’s in its area
  - Handles call set up
  - Transcoding and rate adaptation functionality
  - Handover for each MS
  - Radio Power control
  - It communicates with MSC and BTS

Network Switching Subsystem (NSS)

- Carries out switching functions and manages the communications between mobile phones and the PSTN.
- Allows mobile phones to communicate with each other.
- Includes the following elements –

Mobile Switching Center (MSC) –

- Capable of receiving a short message from a Service Center (SC),
- Interrogating an HLR for routing information and message waiting data, and delivering the short message to the MSC of the receiving MS.

Home Location Registers (HLR) –

- Connection of mobile subscribers and definition of corresponding subscriber data.
- Maintenance of a database of mobile subscribers and corresponding subscriber data.
- Subscription to basic services.
- Registration/deletion of supplementary services.
- Activation/deactivation of supplementary services.

Network Switching Subsystem (NSS)…

- Visitor Location Registers (VLR) –
  - Functions for setting up and controlling calls, including supplementary services.
  - Functions for handling speech path continuity for moving subscribers (handover).
  - Functions for updating mobile subscribers' location (location updating and location canceling) in the different location registers.
  - Functions for updating mobile subscriber data.

- Authentication Center (AUC) -
  - a RANDom number (RAND)
  - a Signed RESponse (SRES)
  - a Ciphering Key (Kc)
    - generates user specific authentication parameters on request of a VLR authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system

- Equipment Identity Register (EIR)
  - Registers GSM mobile stations and user rights stolen or malfunctioning mobile stations can be locked and sometimes even localized

GSM Signaling Interfaces

- Um - Air interface used for exchanges between a MS and a BSS
- Abis - Abis interface allows control of the radio equipment and radio frequency allocation in the BTS.
- A - A interface is between the BSS and the MSC. The A interface manages the allocation of suitable radio resources to the MSs and mobility management.
- B - The B interface between the MSC and the VLR uses the MAP/B protocol. Most MSCs are associated with a VLR, making the B interface "internal".
- C - The C interface is between the HLR and a GMSC or a SMS-G. MAP/C protocol over the C interface is used to obtain the routing information required to complete the call.

Interfaces…

- D - The D interface is between the VLR and HLR, and uses the MAP/D protocol to exchange the data related to the location of the MS and to the management of the subscriber.

- E - The E interface interconnects two MSCs. The E interface exchanges data related to handover between the anchor and relay MSCs using the MAP/E protocol.

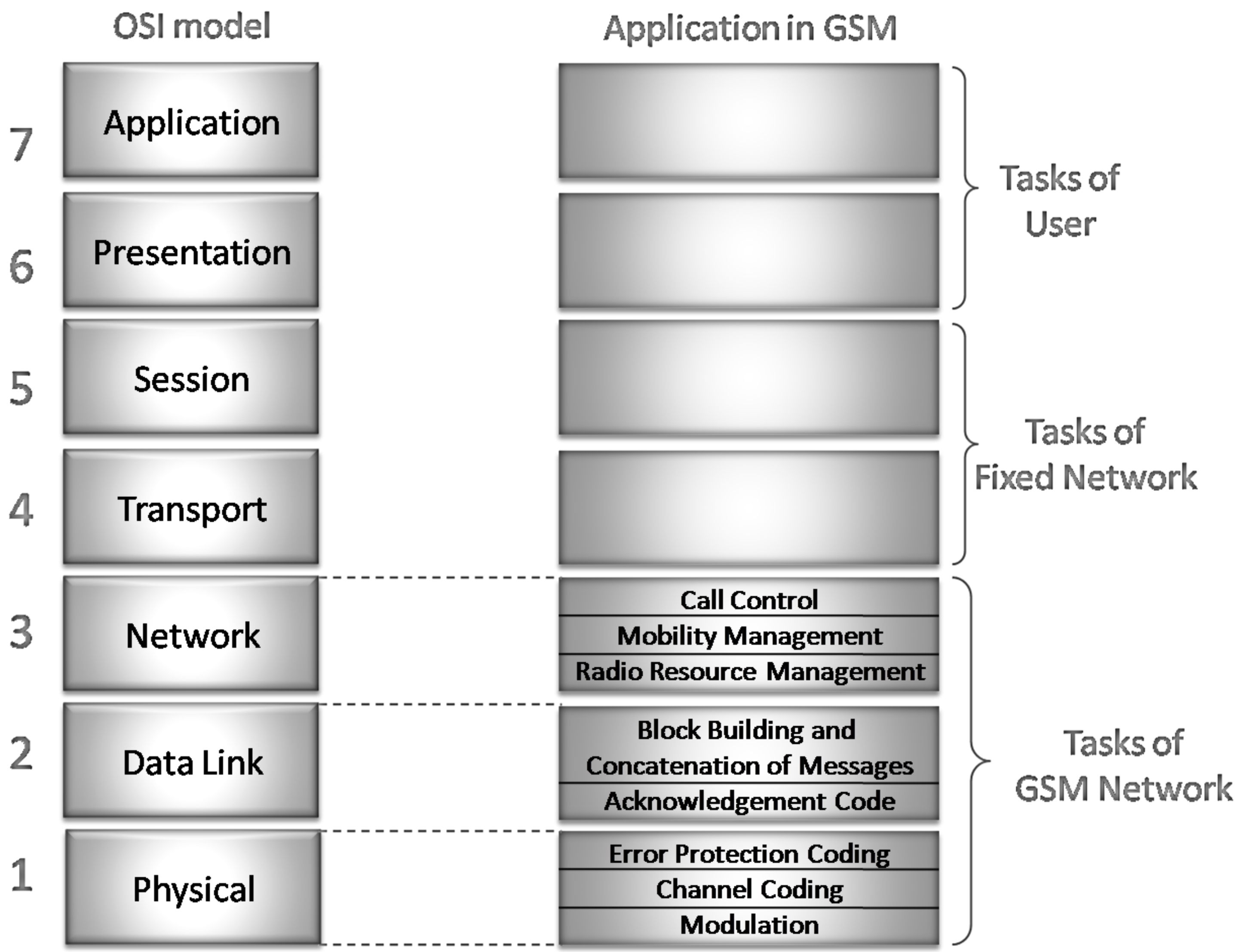
- F - The F interface connects the MSC to the EIR, and uses the MAP/F protocol to verify the status of the IMEI that the MSC has retrieved from the MS.

- G - The G interface interconnects two VLRs of different MSCs and uses the MAP/G protocol to transfer subscriber information, during e.g. a location update procedure.

- H - The H interface is between the MSC and the SMS-G, and uses the MAP/H protocol to support the transfer of short messages.

- I - The I interface (not shown in Figure 1) is the interface between the MSC and the MS. Messages exchanged over the I interface are relayed transparently through the BSS.

Comparing GSM layers with OSI model



OSI model

Application in GSM

7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

1 Physical

Tasks of User

Tasks of Fixed Network

Call Control

Mobility Management

Radio Resource Management

Block Building and Concatenation of Messages

Acknowledgement Code

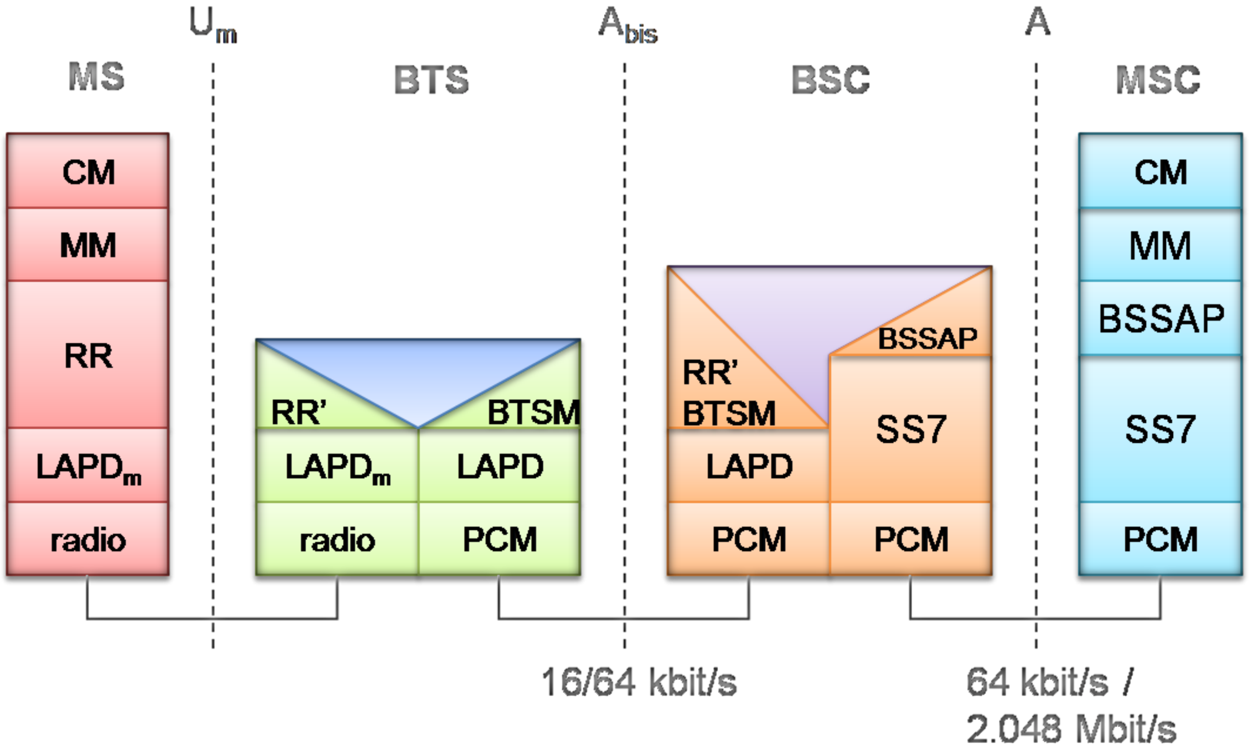
Error Protection Coding

Channel Coding

Modulation

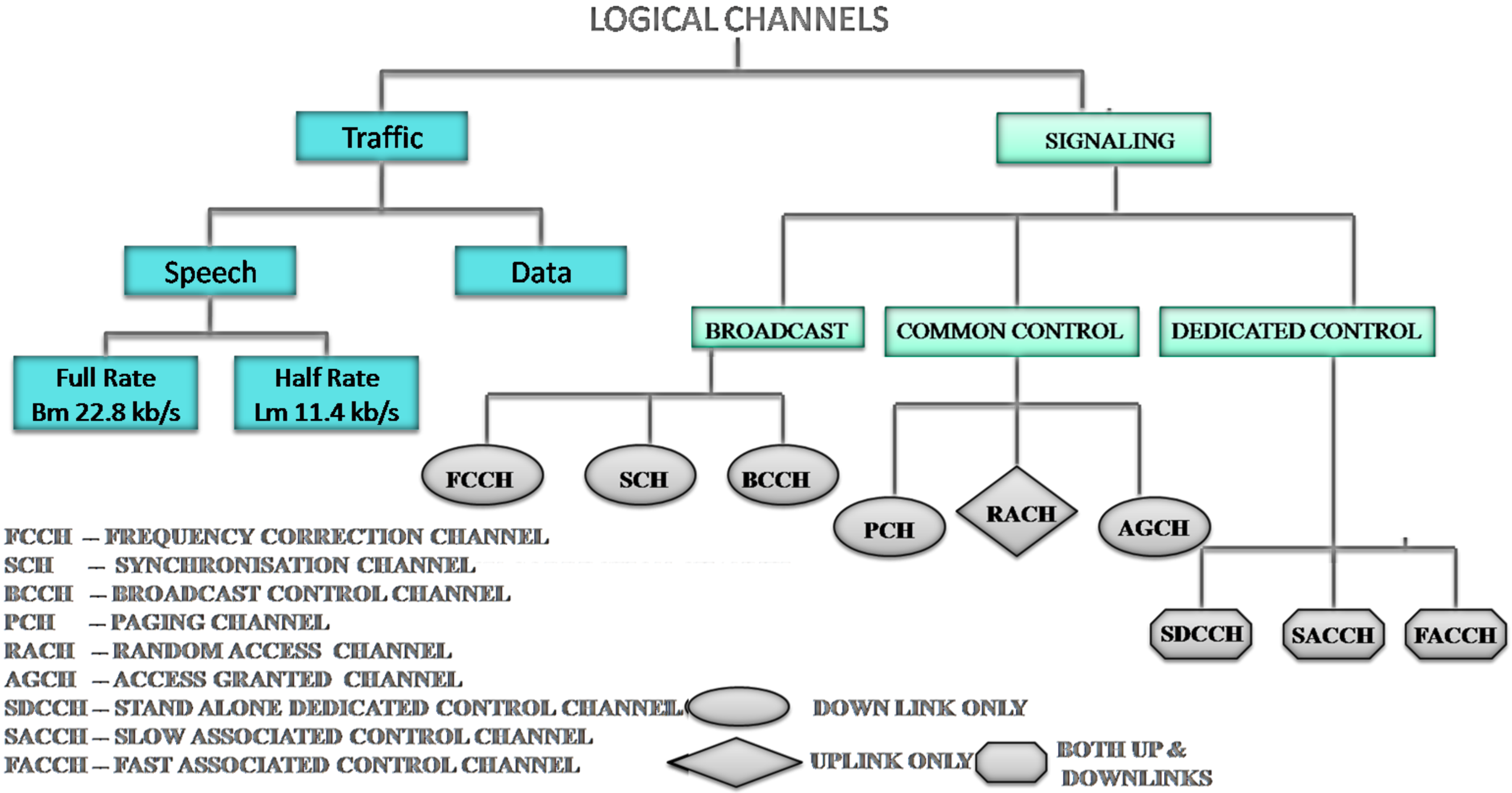
Tasks of GSM Network

GSM Protocol Layers for Signaling



- CM – Connection Management
- MM – Mobility Management
- RR – Radio Resource Management
- LAPDm – Link Access Protocol D-Channel Modified
- BSSMAP Base Station Subsystem Mobile Application Part

Logical Channels

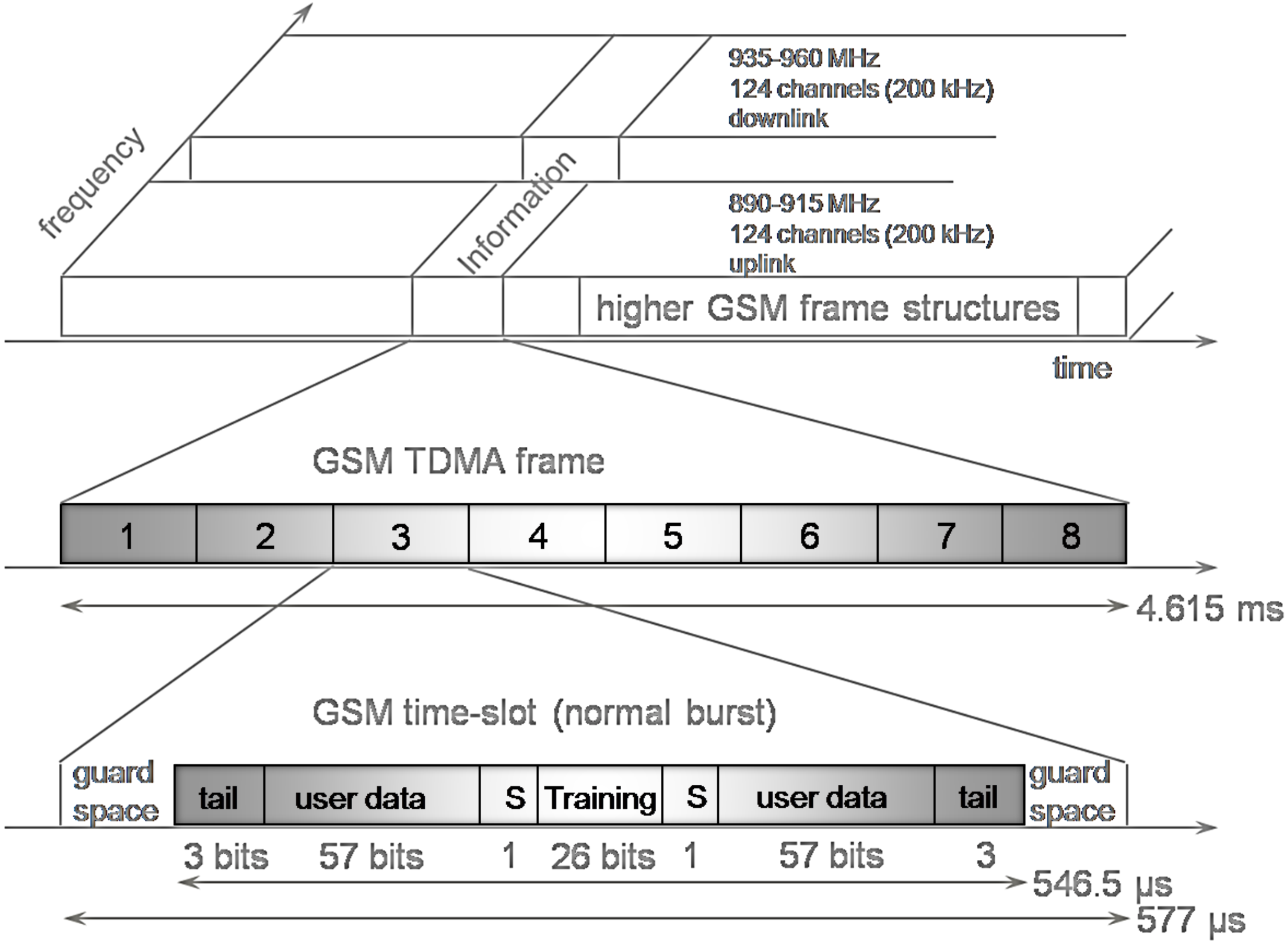


FCCH – FREQUENCY CORRECTION CHANNEL
SCH – SYNCHRONISATION CHANNEL
BCCH – BROADCAST CONTROL CHANNEL
PCH – PAGING CHANNEL
RACH – RANDOM ACCESS CHANNEL
AGCH – ACCESS GRANTED CHANNEL
SDCCH – STAND ALONE DEDICATED CONTROL CHANNEL
SACCH – SLOW ASSOCIATED CONTROL CHANNEL
FACCH – FAST ASSOCIATED CONTROL CHANNEL

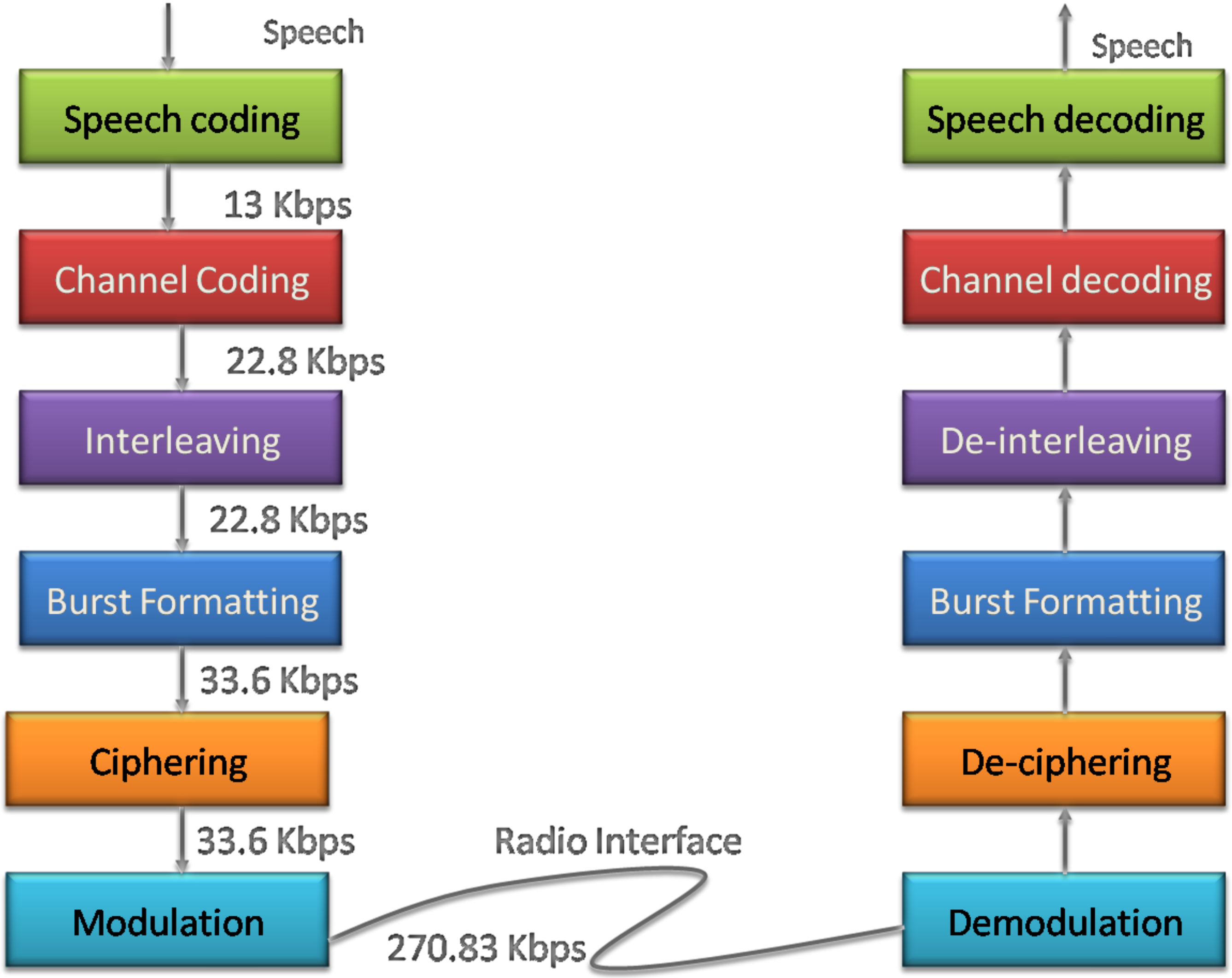
GSM Services

- **Tele-services** Telecommunication services that enable voice communication, fax transmission via mobile phones
  - Offered services - Mobile telephony, Emergency calling
- **Bearer or Data** Services Include various data services for information transfer between GSM and other networks like PSTN, ISDN etc at rates from 300 to 9600 bps
  - Offered services - Short Message Service (SMS), Unified Messaging Services(UMS), Group 3 fax, Voice mailbox, Electronic mail.
- **Supplementary Service**
  - Call related services - Call Waiting, Call Hold, Call Barring, Call Forwarding, Multi Party Call Conferencing, CLIP , CLIR , CUG.

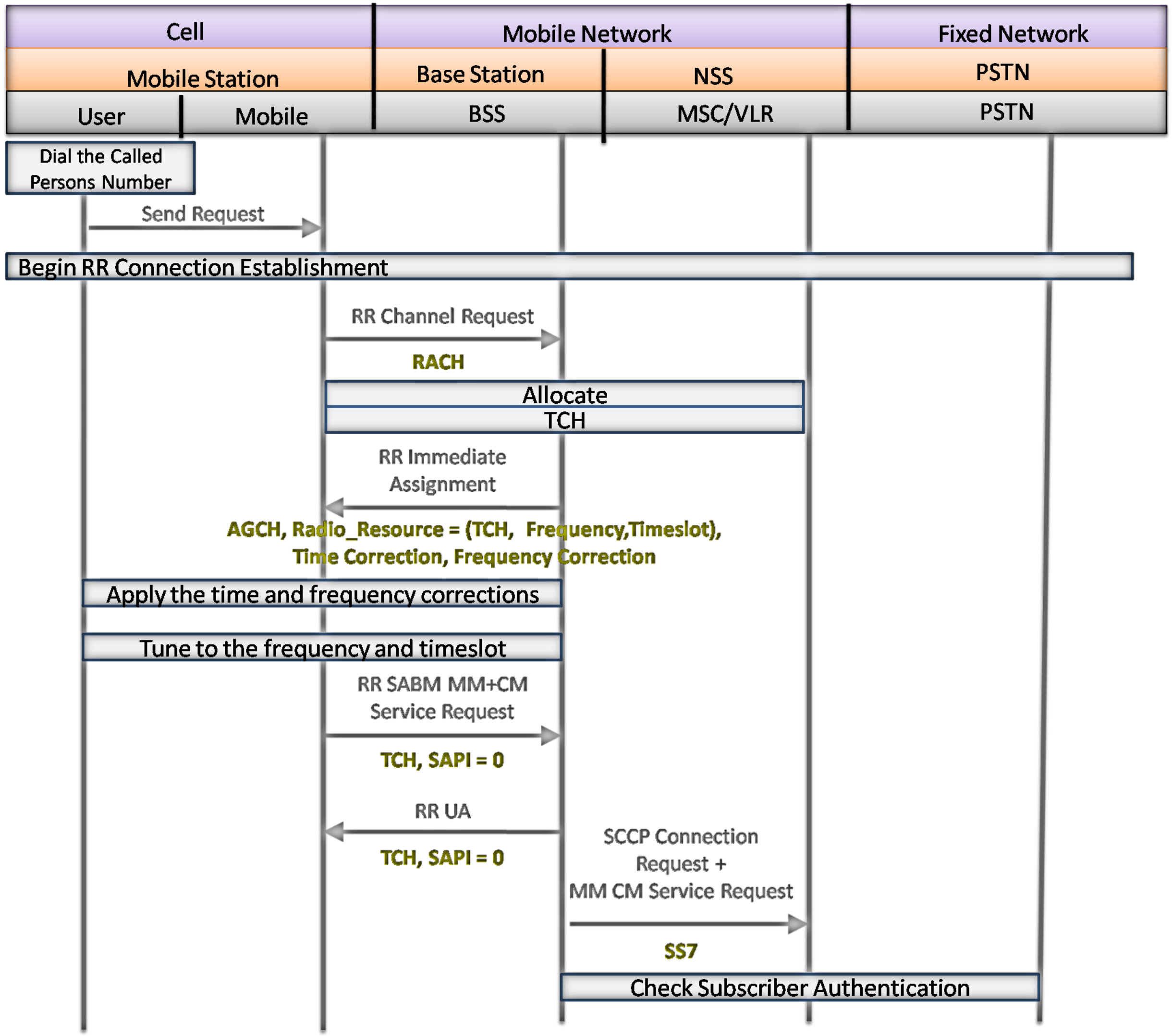
GSM Frame Structure



GSM Operation



GSM Originating Call Flow



Cell | Mobile Network | Fixed Network

Mobile Station | Base Station | NSS | PSTN

User | Mobile | BSS | MSC/VLR | PSTN

Dial the Called Persons Number

Send Request

Begin RR Connection Establishment

RR Channel Request

RACH

Allocate

TCH

RR Immediate Assignment

AGCH, Radio_Resource = (TCH, Frequency,Timeslot), Time Correction, Frequency Correction

Apply the time and frequency corrections

Tune to the frequency and timeslot

RR SABM MM+CM Service Request

TCH, SAPI = 0

RR UA

TCH, SAPI = 0

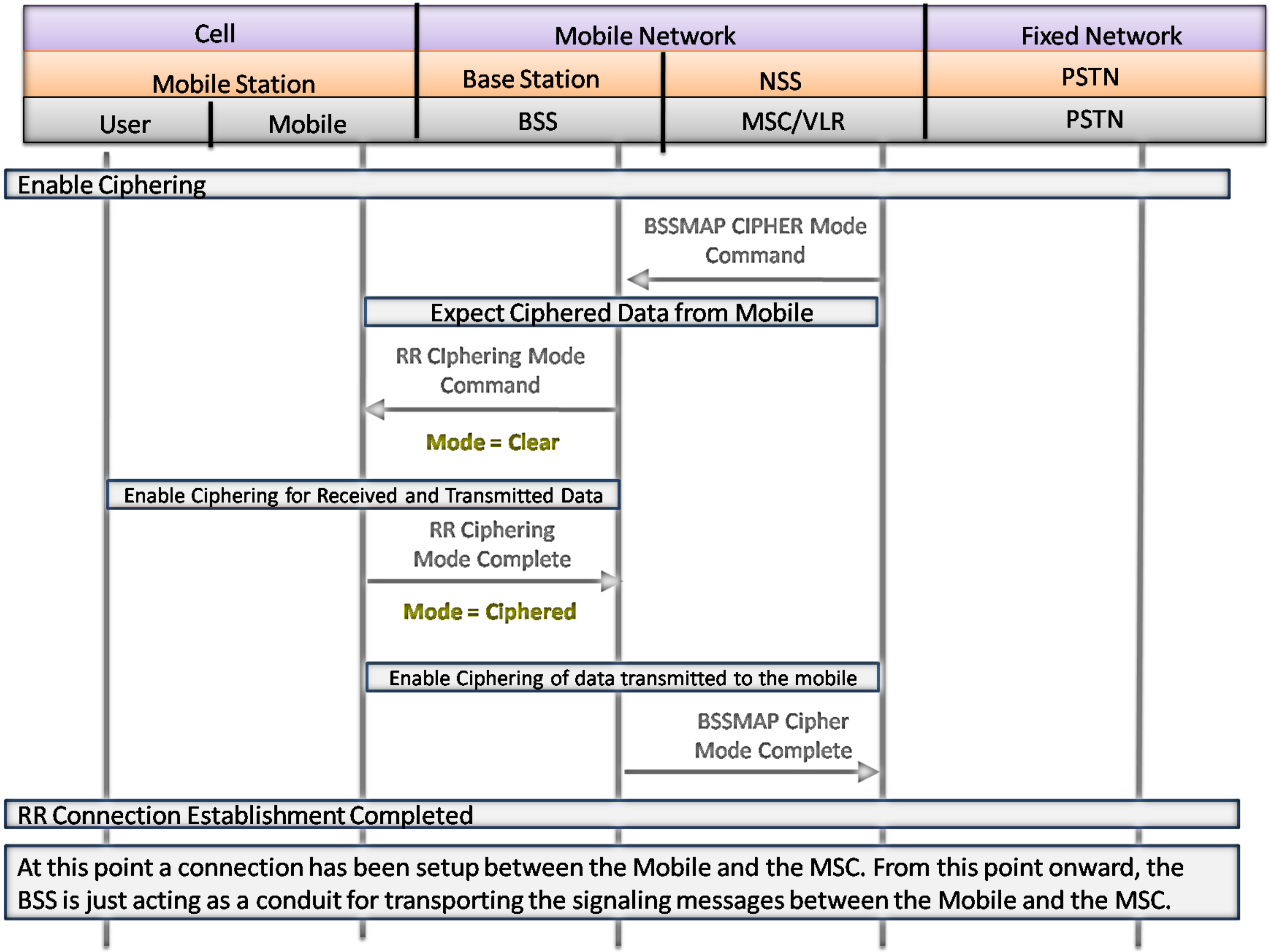
SCCP Connection Request + MM CM Service Request

SS7

Check Subscriber Authentication

GL Communications

GSM Originating Call Flow

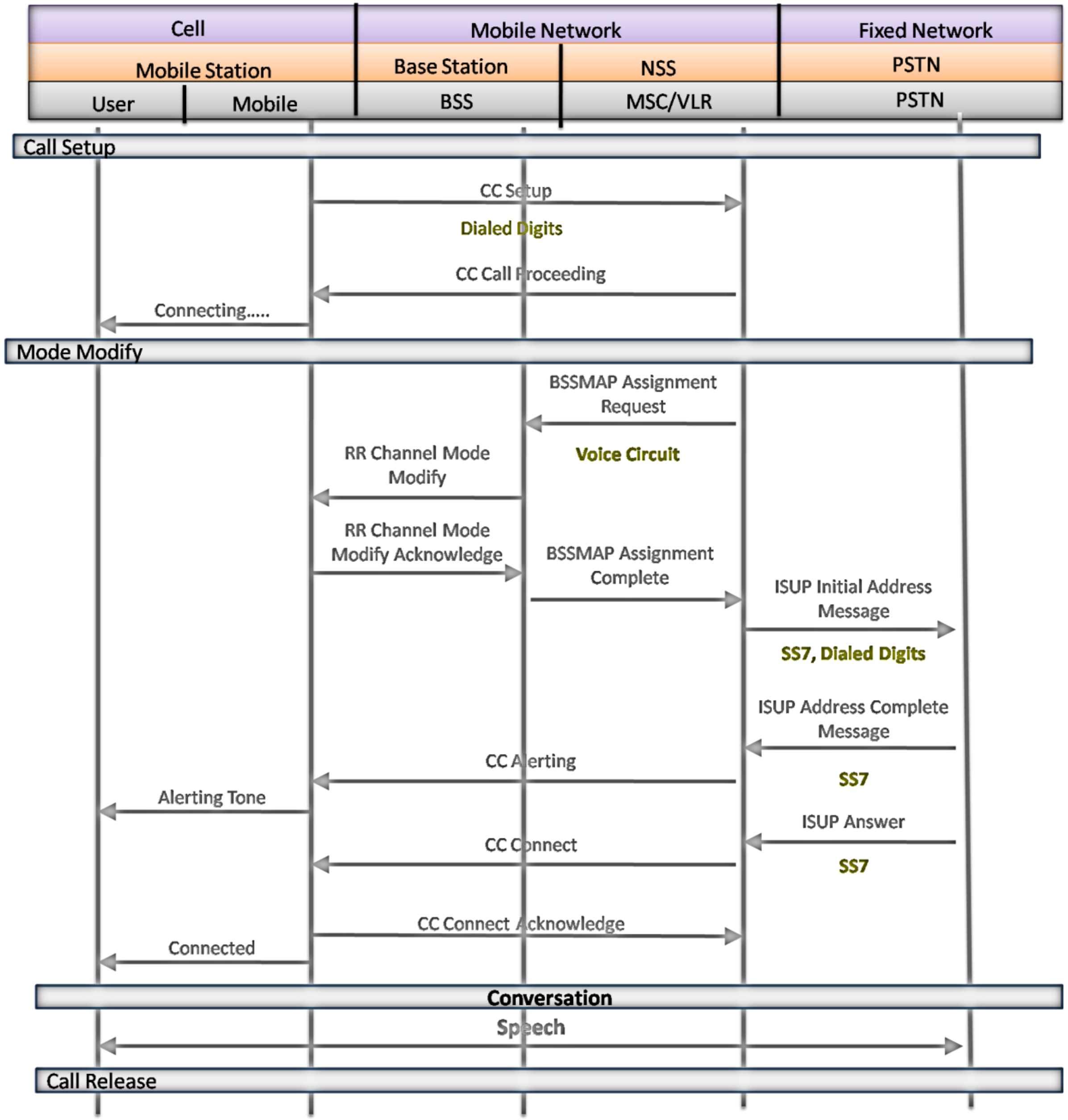


Cell
Mobile Network
Fixed Network
Mobile Station
Base Station
NSS
PSTN
User
Mobile
BSS
MSC/VLR
PSTN
Enable Ciphering
BSSMAP CIPHER Mode Command
Expect Ciphered Data from Mobile
RR CIphering Mode Command
Mode = Clear
Enable Ciphering for Received and Transmitted Data
RR Ciphering Mode Complete
Mode = Ciphered
Enable Ciphering of data transmitted to the mobile
BSSMAP Cipher Mode Complete
RR Connection Establishment Completed

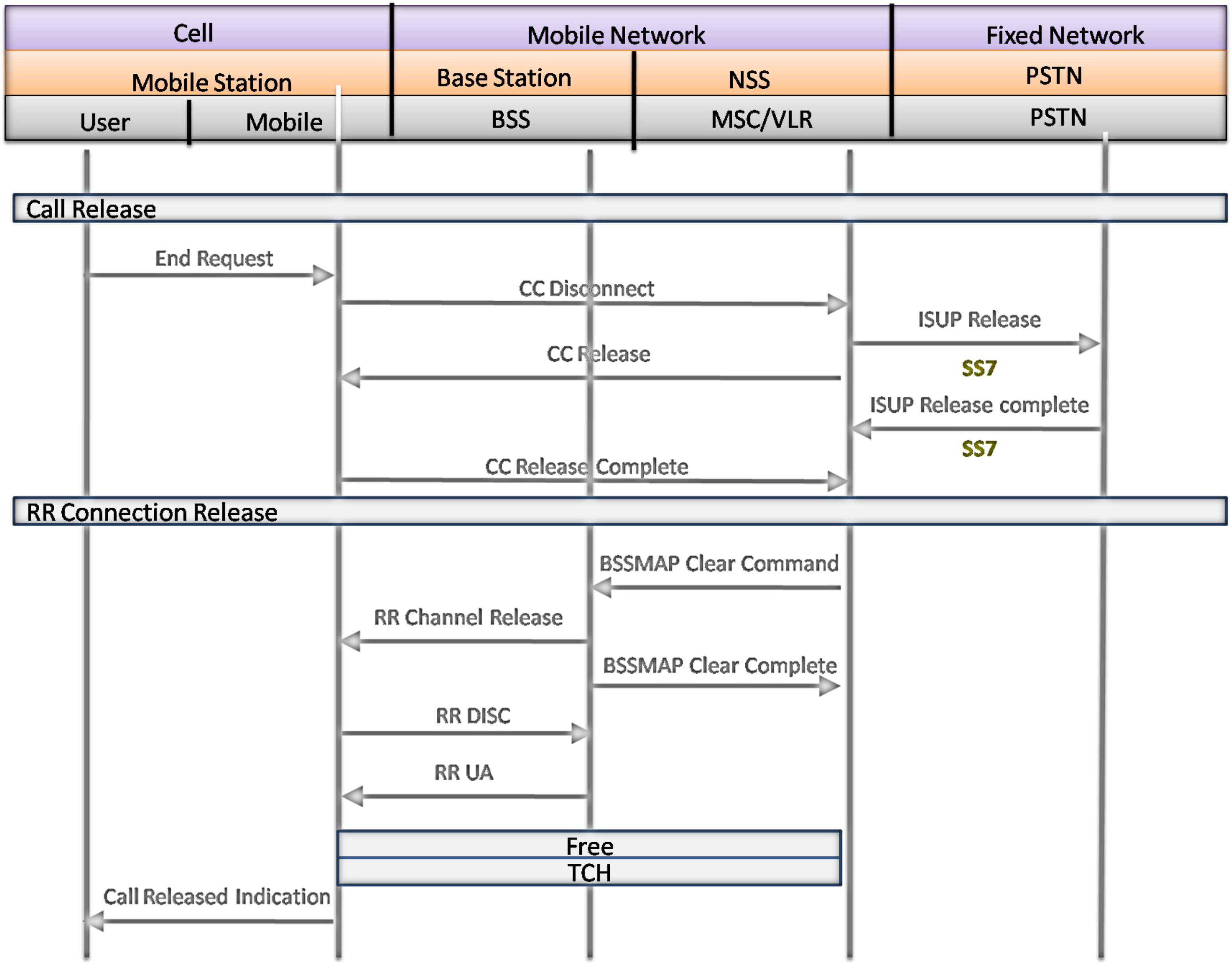
At this point a connection has been setup between the Mobile and the MSC. From this point onward, the BSS is just acting as a conduit for transporting the signaling messages between the Mobile and the MSC.

GL Communications

GSM Originating Call Flow



GSM Originating Call Flow



Message Format

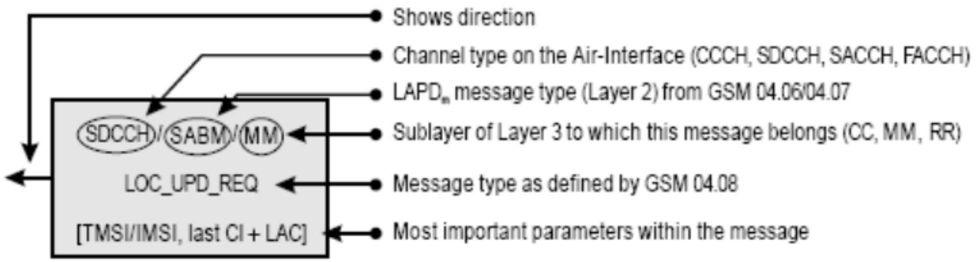

SDCCH / SABM / MM
LOC_UPD_REQ
[TMSI/IMSI, last CI + LAC]
Shows direction
Channel type on the Air-Interface (CCCH, SDCCH, SACCH, FACCH)
LAPD$_m$ message type (Layer 2) from GSM 04.06/04.07
Sublayer of Layer 3 to which this message belongs (CC, MM, RR)
Message type as defined by GSM 04.08
Most important parameters within the message

Figure 1.4(a) Format for messages over the Air-interface (LAPD$_m$, GSM 04.08).

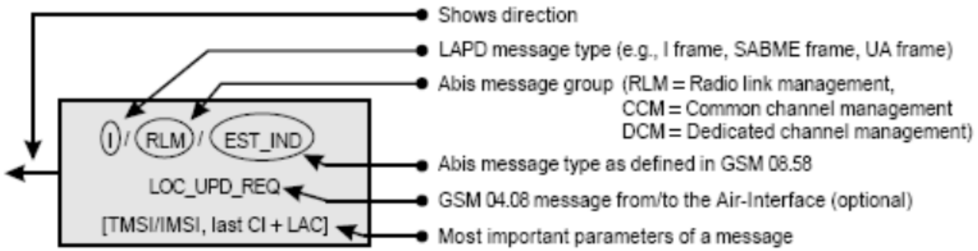

I / RLM / EST_IND
LOC_UPD_REQ
[TMSI/IMSI, last CI + LAC]
Shows direction
LAPD message type (e.g., I frame, SABME frame, UA frame)
Abis message group (RLM = Radio link management,
CCM = Common channel management
DCM = Dedicated channel management)
Abis message type as defined in GSM 08.58
GSM 04.08 message from/to the Air-Interface (optional)
Most important parameters of a message

Figure 1.4(b) Format for messages over the Abis-interface (LAPD, GSM 08.58).

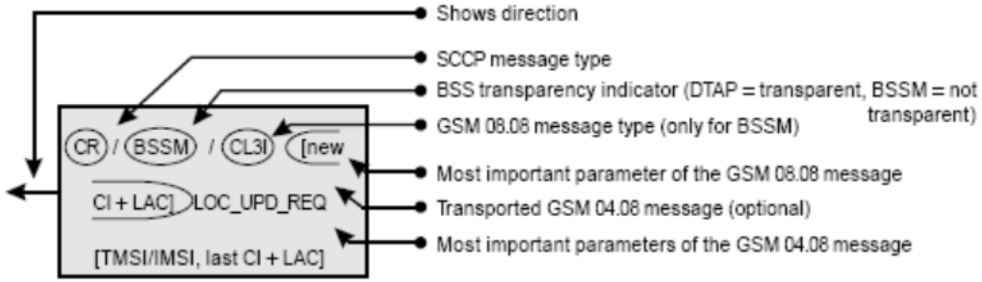

CR / BSSM / CL3I [new CI + LAC] LOC_UPD_REQ
[TMSI/IMSI, last CI + LAC]
Shows direction
SCCP message type
BSS transparency indicator (DTAP = transparent, BSSM = not transparent)
GSM 08.08 message type (only for BSSM)
Most important parameter of the GSM 08.08 message
Transported GSM 04.08 message (optional)
Most important parameters of the GSM 04.08 message

Figure 1.4(c) Format for messages over the A-interface [SS7, signaling connection control part (SCCP), GSM 08.06, GSM 08.08].

Message Format…

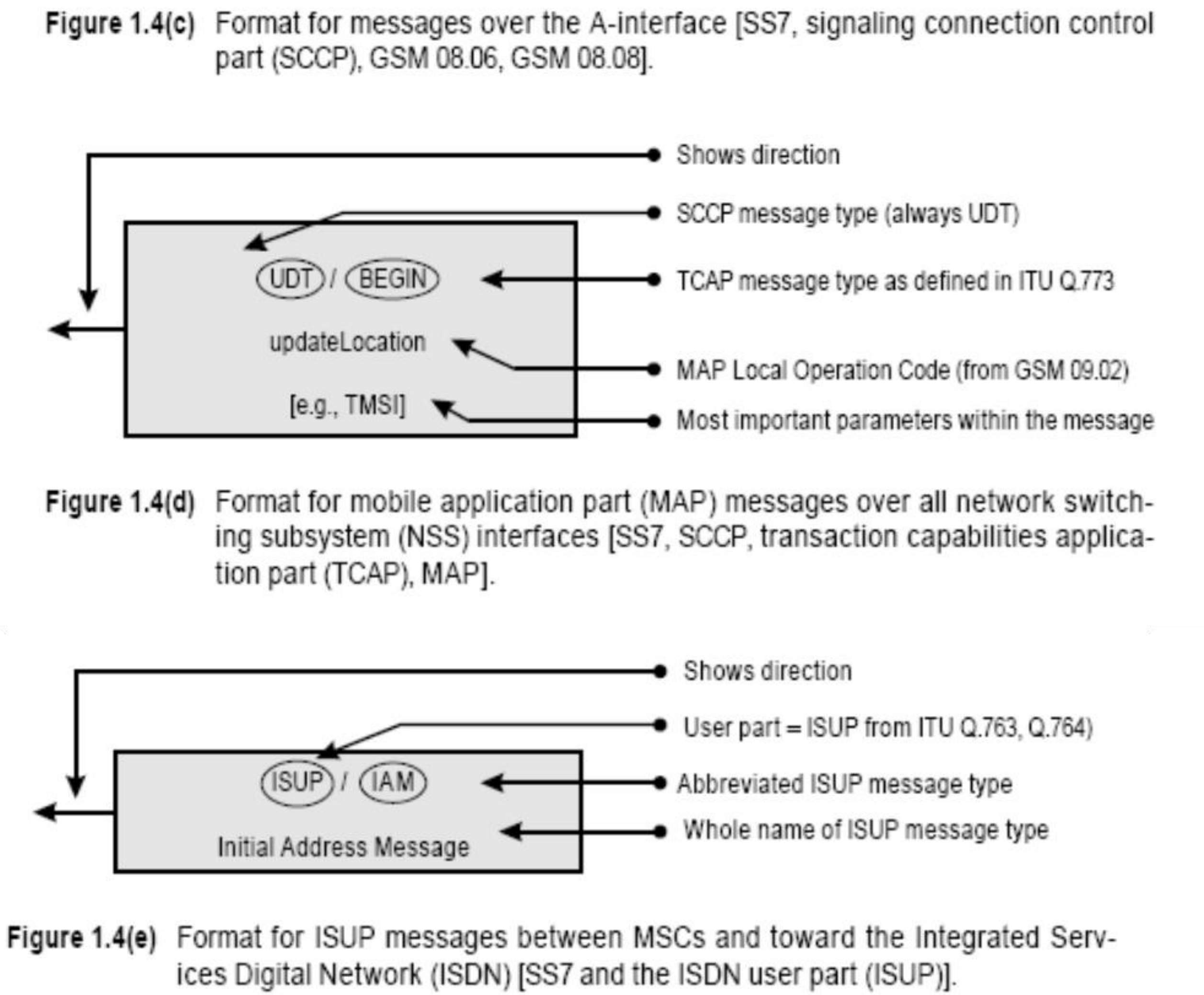


Figure 1.4(c) Format for messages over the A-interface [SS7, signaling connection control part (SCCP), GSM 08.06, GSM 08.08].

Shows direction
SCCP message type (always UDT)
UDT / BEGIN
TCAP message type as defined in ITU Q.773
updateLocation
MAP Local Operation Code (from GSM 09.02)
[e.g., TMSI]
Most important parameters within the message

Figure 1.4(d) Format for mobile application part (MAP) messages over all network switching subsystem (NSS) interfaces [SS7, SCCP, transaction capabilities application part (TCAP), MAP].

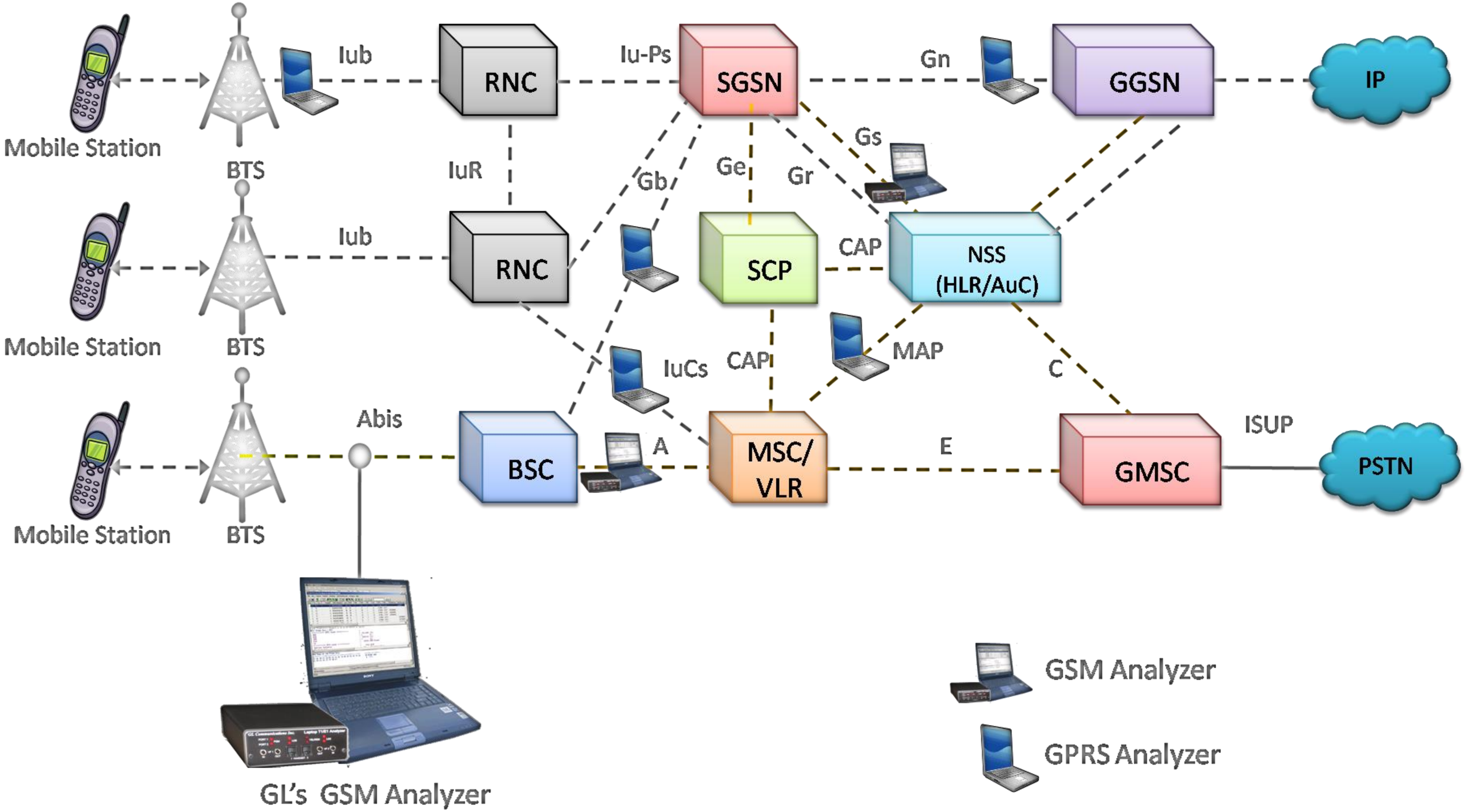
Shows direction
User part = ISUP from ITU Q.763, Q.764)
ISUP / IAM
Abbreviated ISUP message type
Initial Address Message
Whole name of ISUP message type

Figure 1.4(e) Format for ISUP messages between MSCs and toward the Integrated Services Digital Network (ISDN) [SS7 and the ISDN user part (ISUP)].

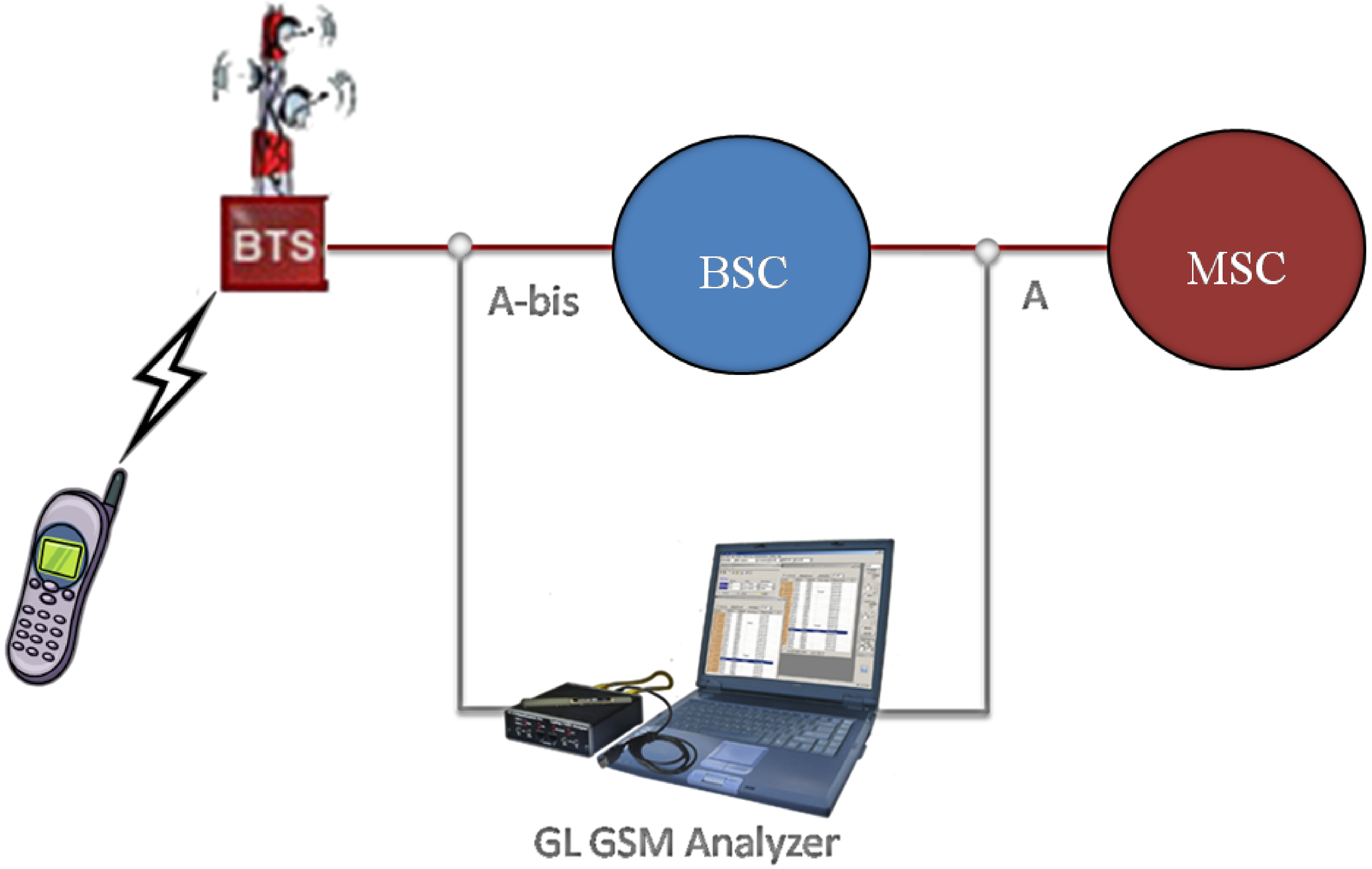
Future of GSM

- 2nd Generation
  - GSM -9.6 Kbps (data rate)
- 2.5 Generation (Future of GSM)
  - HSCSD (High Speed ckt Switched data)
    - Data rate : 76.8 Kbps (9.6 x 8 kbps)
  - GPRS (General Packet Radio service)
    - Data rate: 14.4 - 115.2 Kbps
  - EDGE (Enhanced data rate for GSM Evolution)
    - Data rate: 547.2 Kbps (max)
- 3 Generation
  - WCDMA(Wide band CDMA)
    - Data rate : 0.348 – 2.0 Mbps

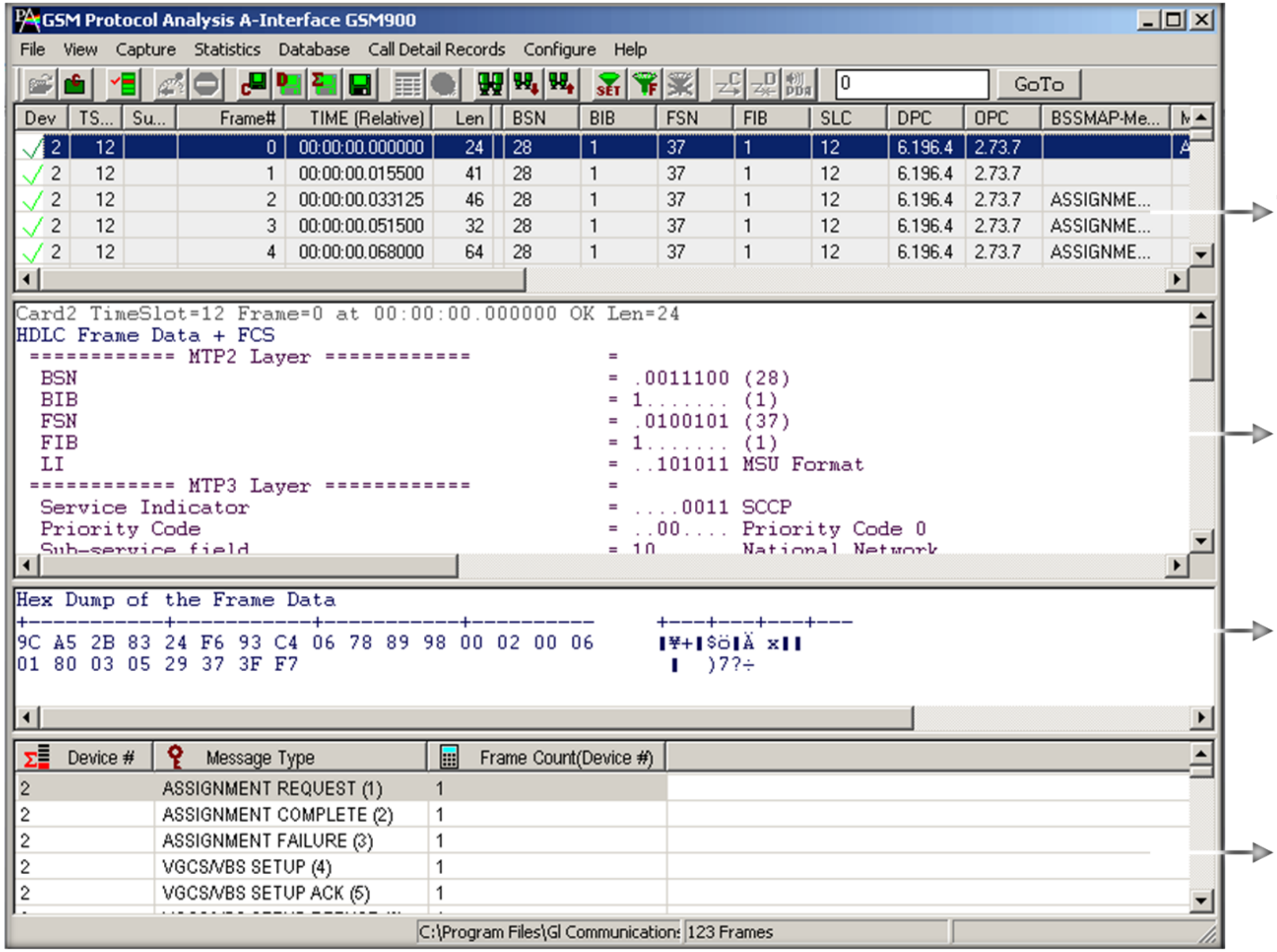
GL's GSM Protocol Analyzer



GL's GSM Analyzer



GL's GSM Analyzer



Dev	TS...	Su...	Frame#	TIME (Relative)	Len	BSN	BIB	FSN	FIB	SLC	DPC	OPC	BSSMAP-Me...	M
✓ 2	12		0	00:00:00.000000	24	28	1	37	1	12	6.196.4	2.73.7		A
✓ 2	12		1	00:00:00.015500	41	28	1	37	1	12	6.196.4	2.73.7		
✓ 2	12		2	00:00:00.033125	46	28	1	37	1	12	6.196.4	2.73.7	ASSIGNME...	
✓ 2	12		3	00:00:00.051500	32	28	1	37	1	12	6.196.4	2.73.7	ASSIGNME...	
✓ 2	12		4	00:00:00.068000	64	28	1	37	1	12	6.196.4	2.73.7	ASSIGNME...	

```
Card2 TimeSlot=12 Frame=0 at 00:00:00.000000 OK Len=24
HDLC Frame Data + FCS
 ============ MTP2 Layer ============           =
  BSN                                          = .0011100 (28)
  BIB                                          = 1....... (1)
  FSN                                          = .0100101 (37)
  FIB                                          = 1....... (1)
  LI                                           = ..101011 MSU Format
 ============ MTP3 Layer ============           =
  Service Indicator                            = ....0011 SCCP
  Priority Code                                = ..00.... Priority Code 0
  Sub-service field                            = 10...... National Network
```

```
Hex Dump of the Frame Data
+-----------+-----------+-----------+----------     +---+---+---+---
9C A5 2B 83 24 F6 93 C4 06 78 89 98 00 02 00 06     ▌¥+▌$ö▌Ä x▌▌
01 80 03 05 29 37 3F F7                              ▌  )7?÷
```

Device #	Message Type	Frame Count(Device #)
2	ASSIGNMENT REQUEST (1)	1
2	ASSIGNMENT COMPLETE (2)	1
2	ASSIGNMENT FAILURE (3)	1
2	VGCS/VBS SETUP (4)	1
2	VGCS/VBS SETUP ACK (5)	1

C:\Program Files\Gl Communication: 123 Frames

Summary View

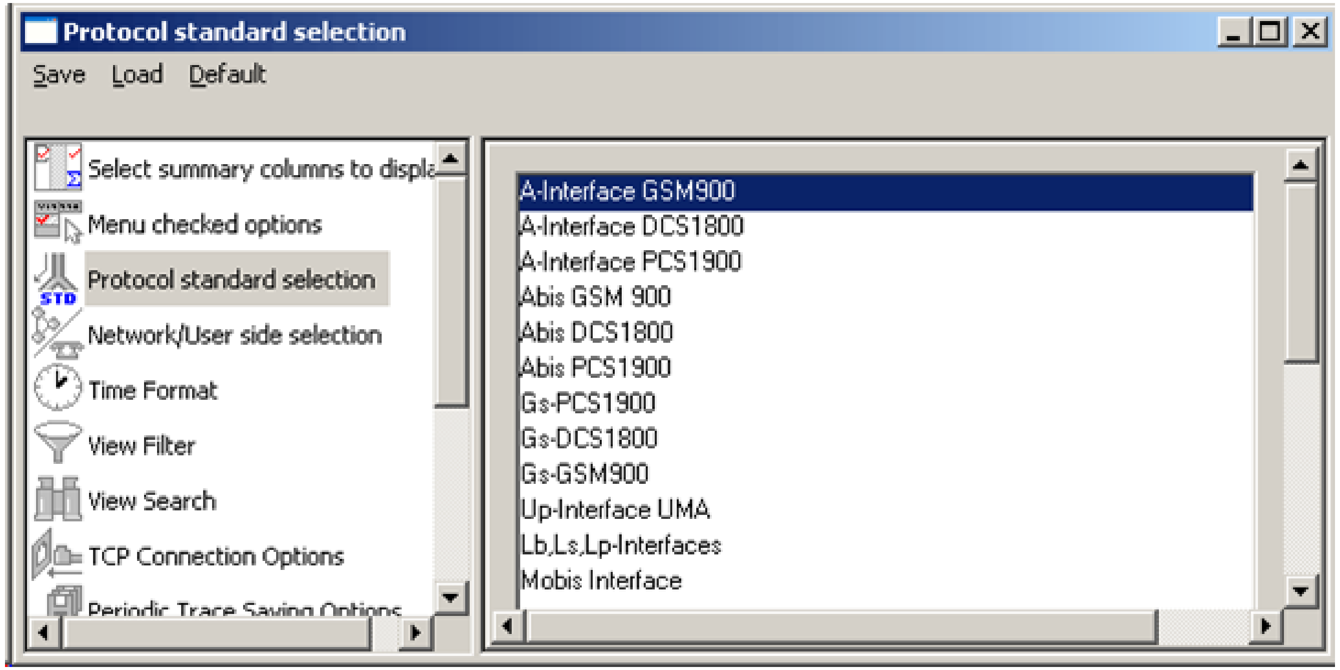
Detail View

Hex Dump View

Statisitcs View

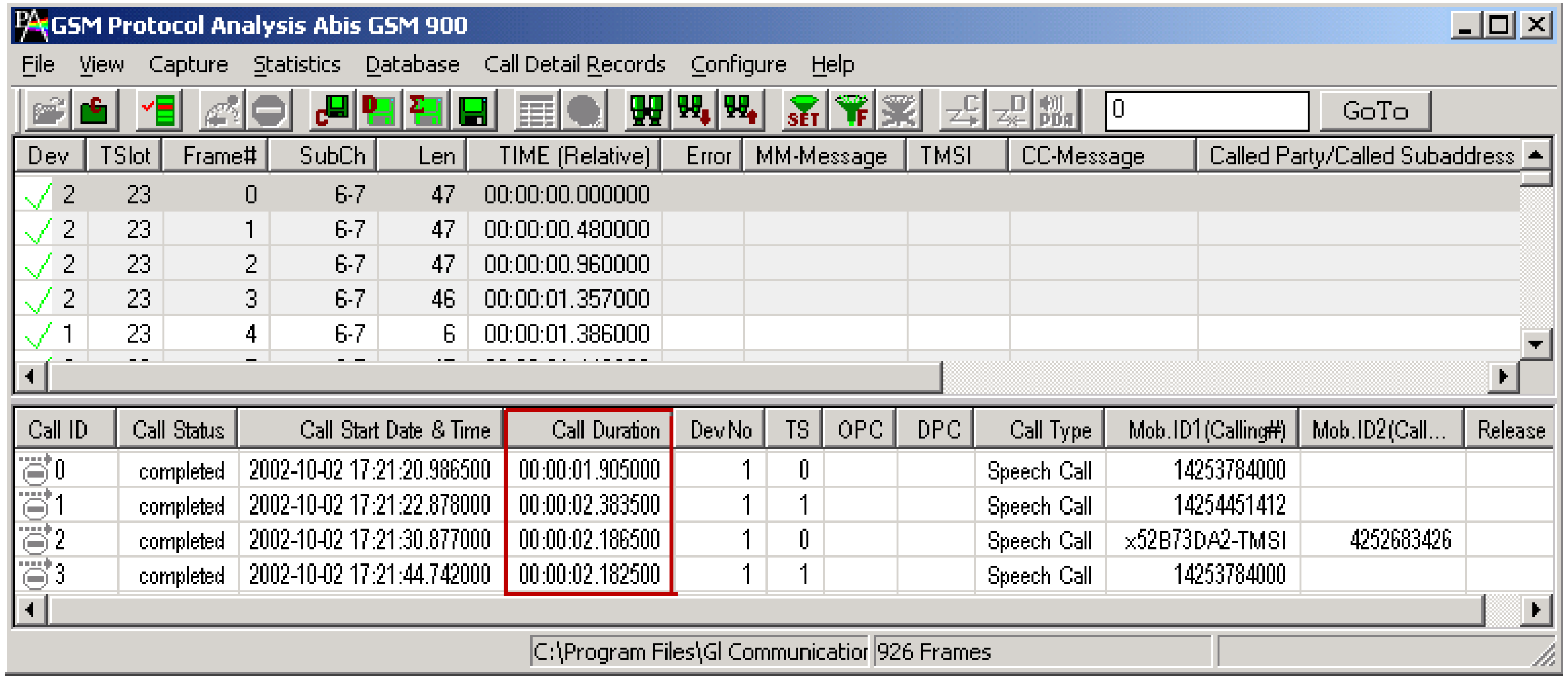
Protocol Standards

- A Interface - MTP2, MTP3, SCCP, BSSMAP, SMS, MM, & CC
- Abis Interface – LAPD, BTSM, RR, SMS, MM & CC
- Gs Interface – MTP2, MTP3, BSSAP+
- Lb, Ls, Lp Interface – RRLP, BSSLAP. SMLCPP, LLP, BSSAP-LE, SCCP, MTP3, & MTP2
- UP Interface - UMA Protocols , TCP, UDP, IP, &MAC
- Motorola Proprietary Mobis Interface


Protocol standard selection
Save
Load
Default
Select summary columns to displa
Menu checked options
Protocol standard selection
Network/User side selection
Time Format
View Filter
View Search
TCP Connection Options
Periodic Trace Saving Options

A-Interface GSM900
A-Interface DCS1800
A-Interface PCS1900
Abis GSM 900
Abis DCS1800
Abis PCS1900
Gs-PCS1900
Gs-DCS1800
Gs-GSM900
Up-Interface UMA
Lb,Ls,Lp-Interfaces
Mobis Interface

Call Detail Records



	Dev	TSlot	Frame#	SubCh	Len	TIME (Relative)	Error	MM-Message	TMSI	CC-Message	Called Party/Called Subaddress
✓	2	23	0	6-7	47	00:00:00.000000					
✓	2	23	1	6-7	47	00:00:00.480000					
✓	2	23	2	6-7	47	00:00:00.960000					
✓	2	23	3	6-7	46	00:00:01.357000					
✓	1	23	4	6-7	6	00:00:01.386000					

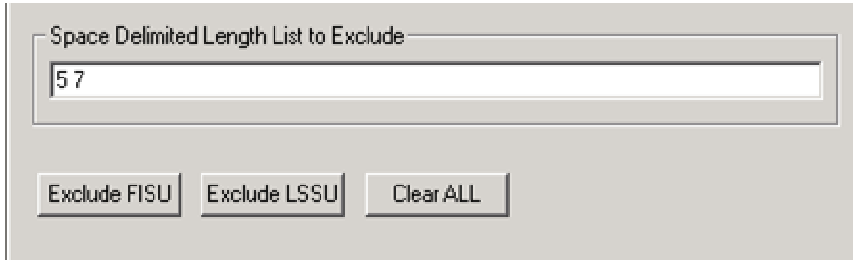
Call ID	Call Status	Call Start Date & Time	Call Duration	Dev No	TS	OPC	DPC	Call Type	Mob.ID1(Calling#)	Mob.ID2(Call...	Release
0	completed	2002-10-02 17:21:20.986500	00:00:01.905000	1	0			Speech Call	14253784000		
1	completed	2002-10-02 17:21:22.878000	00:00:02.383500	1	1			Speech Call	14254451412		
2	completed	2002-10-02 17:21:30.877000	00:00:02.186500	1	0			Speech Call	x52B73DA2-TMSI	4252683426	
3	completed	2002-10-02 17:21:44.742000	00:00:02.182500	1	1			Speech Call	14253784000		

C:\Program Files\Gl Communicatior | 926 Frames

- Call trace defining important call specific parameters such as call ID, status (active or completed), duration, CRV, release complete cause etc are displayed.

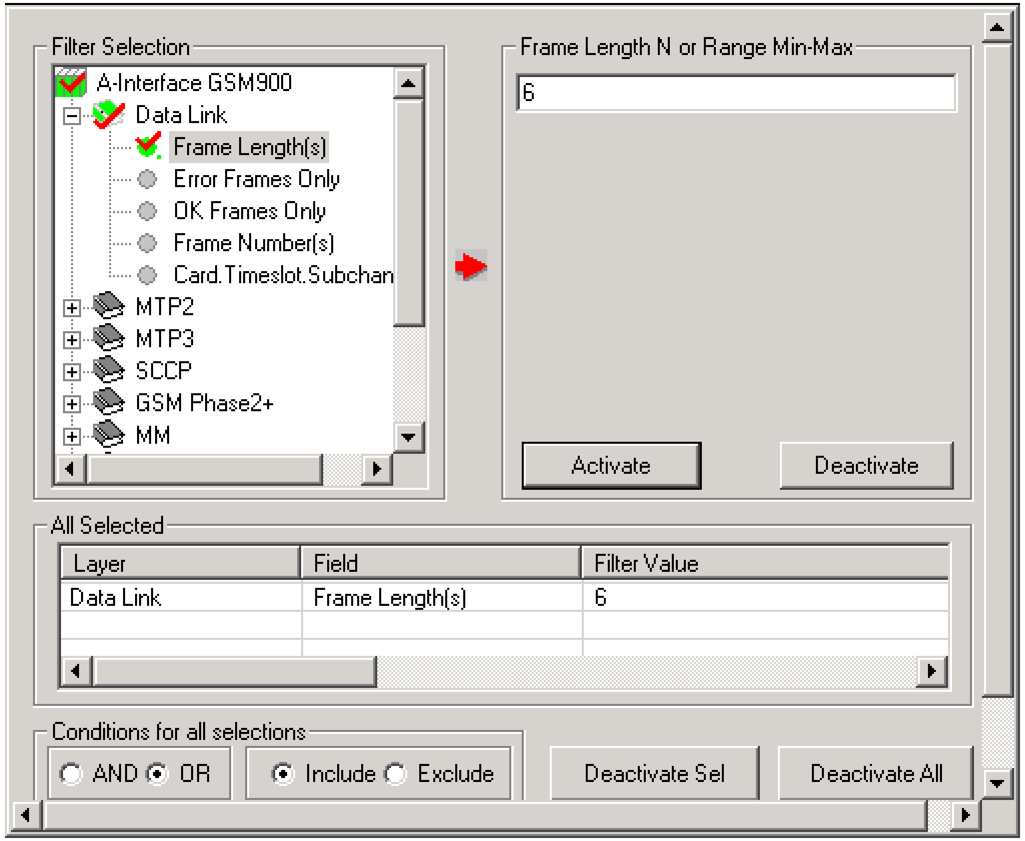
Filter Frames

Real-time Capture Filter



Space Delimited Length List to Exclude: 5 7

Filtering Criteria



Filter Selection

- A-Interface GSM900
  - Data Link
    - ✓ Frame Length(s)
    - Error Frames Only
    - OK Frames Only
    - Frame Number(s)
    - Card.Timeslot.Subchan
  - MTP2
  - MTP3
  - SCCP
  - GSM Phase2+
  - MM

Frame Length N or Range Min-Max: 6

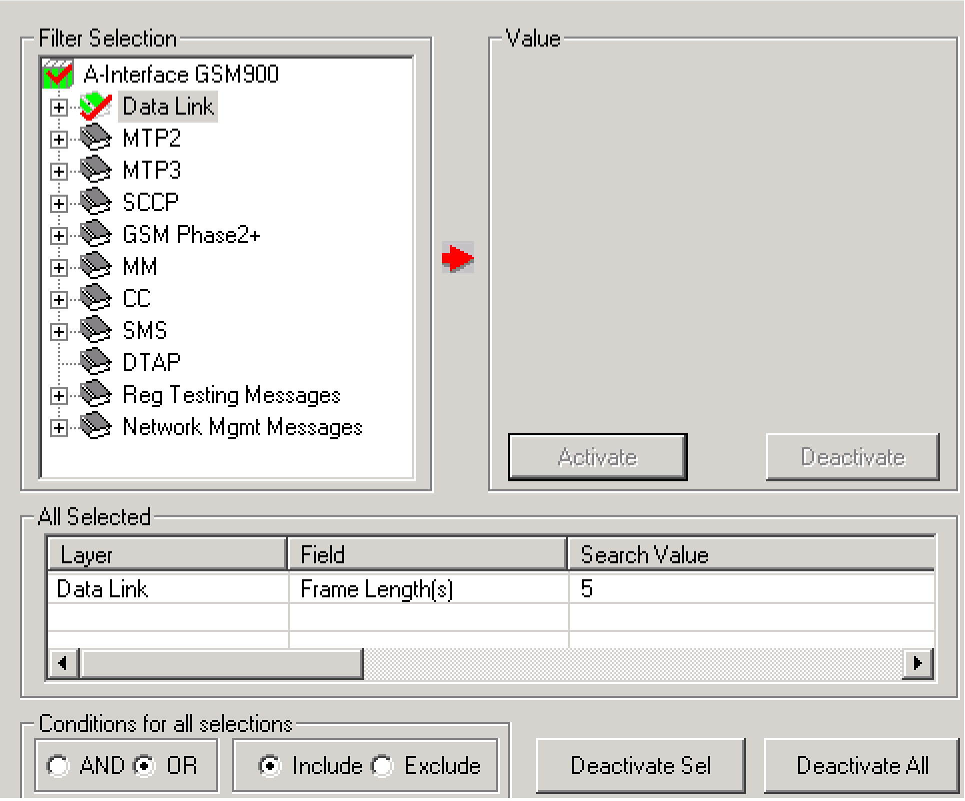
All Selected

Layer	Field	Filter Value
Data Link	Frame Length(s)	6

Conditions for all selections: ○ AND ● OR | ● Include ○ Exclude

- Isolate certain specific frames from all frames in real-time as well as offline
- Real-time Filter applies to the frames being captured and is based on the Frame Length
- The frames can also be filtered after completion of capture according to Frame Number, Time, Length, Error, BSN, BIB, FSN, type of GSM Message and more.

Search Frames



Layer	Field	Search Value
Data Link	Frame Length(s)	5

Conditions for all selections

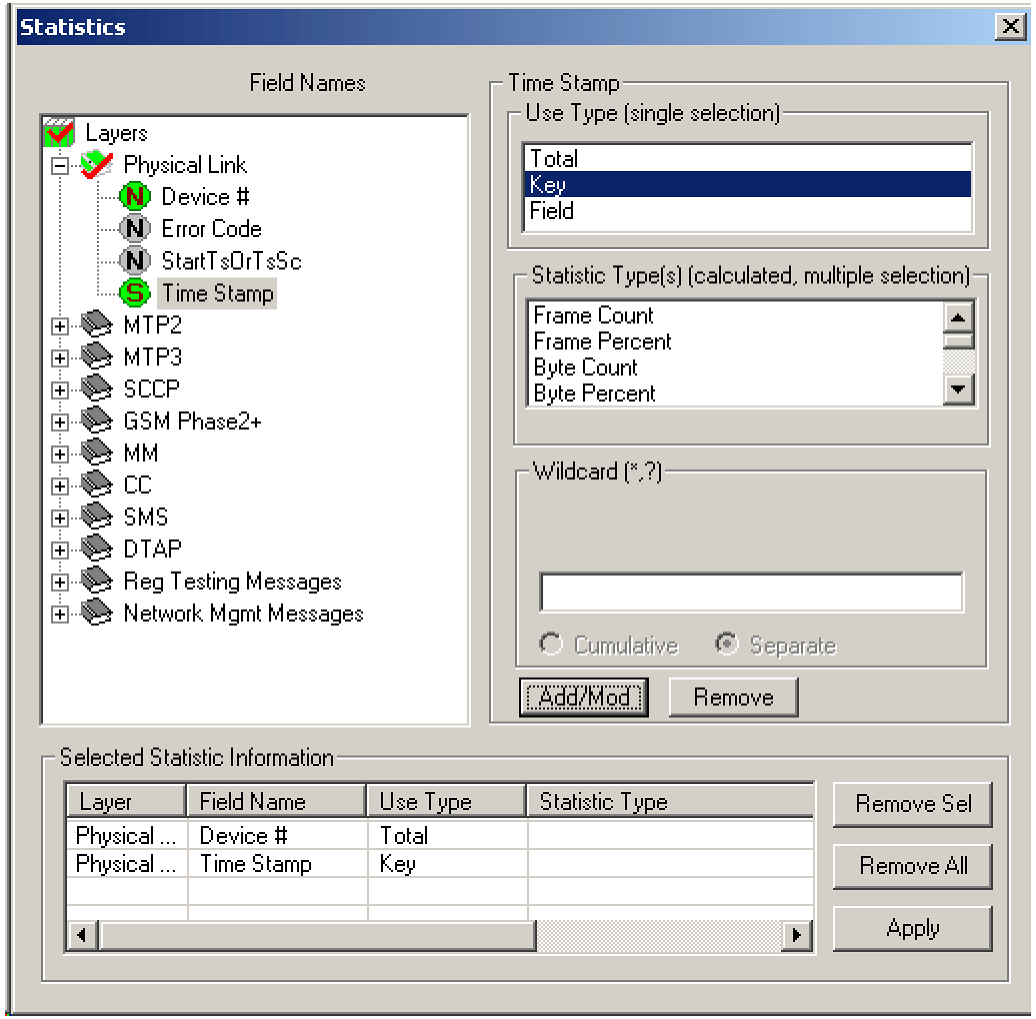
○ AND ● OR

● Include ○ Exclude

- Search features helps users to search for a particular frame based on specific search criteria.

Statistics

- Statistics is an important feature available in protocol analyzer and can be obtained for all frames both in real-time as well as offline mode
- Numerous statistics can be obtained to study the performance of the network based on protocol fields and different parameters.



Use Type (single selection): Key

○ Cumulative ● Separate

Selected Statistic Information

Layer	Field Name	Use Type	Statistic Type
Physical ...	Device #	Total	
Physical ...	Time Stamp	Key	

Applications

- Can be used as independent standalone units as "probes" integrated in a network surveillance systems
- Triggering, collecting, and filtering for unique subscriber information and relaying such information to a back end processor
- Collecting Call Detail Records (CDR) information for billing

THANK YOU!