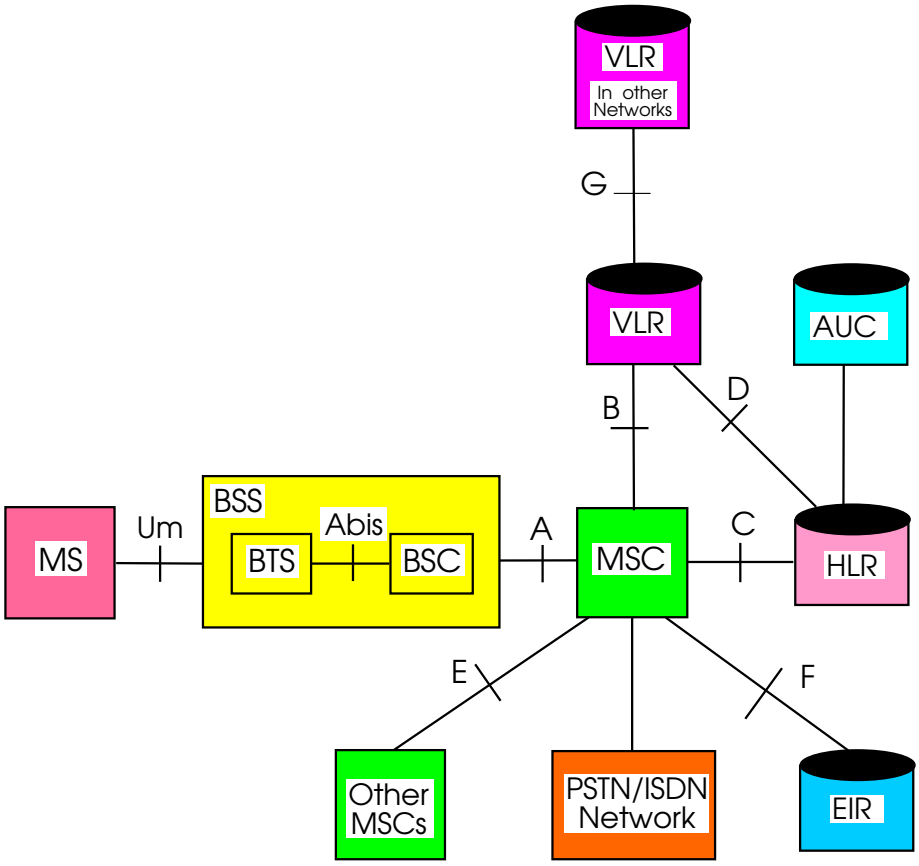
System Architecture Overview

GSM LAND-MOBILE NETWORK REFERENCE MODEL

- Standard open interfaces between entities, often referred to as *network elements* are defined in the GSM Specifications. These interfaces are labeled: A, A-bis, B, C, D, E, F, G, and Um (or air interface).
- Interfaces not labeled with one of the above identifiers are not defined within the GSM specifications.
- Since interfaces between network elements are open and standardized, a given service provider has total flexibility in choosing and mixing different vendor's equipment in their network.
- User information associated with a voice/data call between a mobile station and another entity in the PSTN/ISDN use the Um, Abis, A, and PSTN/ISDN interface. The PSTN/ISDN interface are regulated at the national level and are outside the scope of the GSM recommendations.
- All interfaces other than the ones listed in the previous bullet carry signaling message only (e.g., no voice circuits).

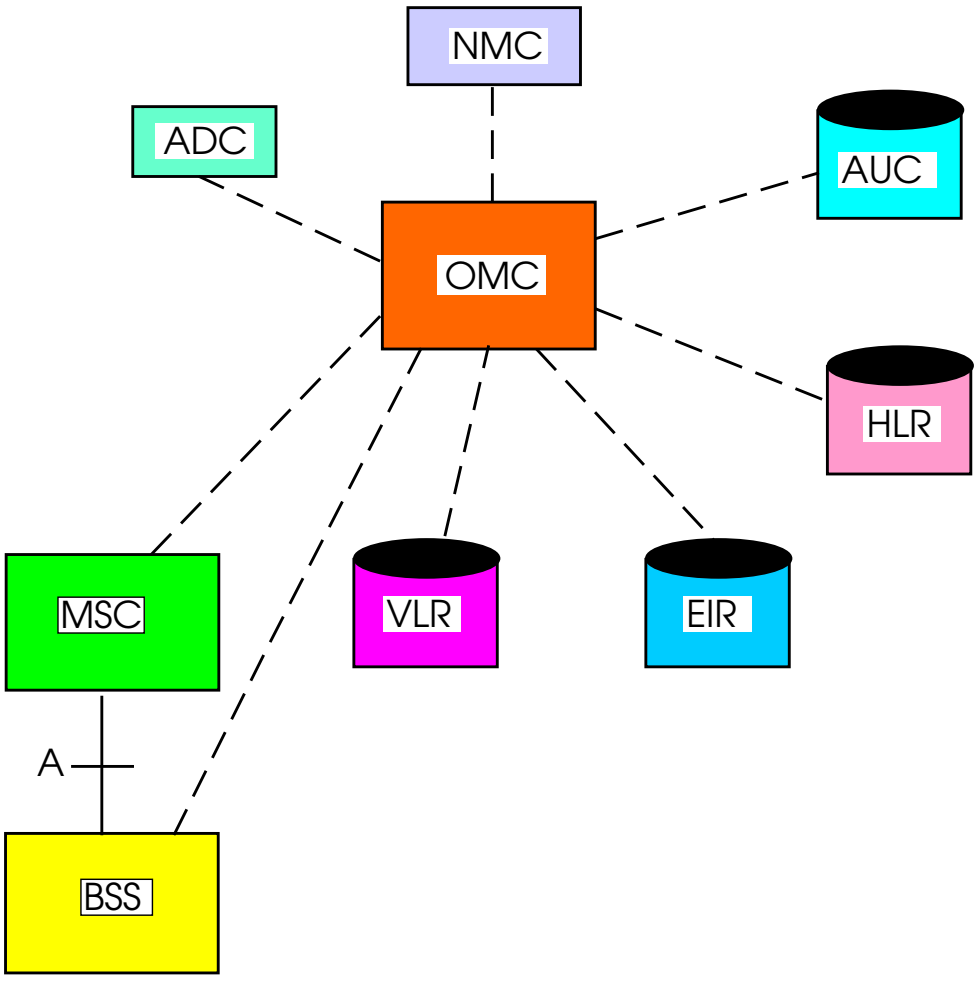
GSM LAND-MOBILE NETWORK REFERENCE MODEL



AUC - Authentication Center
BSC - Base Station Controller
BSS - Base Station System
BTS - Base Transceiver Station
EIR - Equipment Identity Register
HLR - Home Location Register
ISDN - Integrated Services Digital Network
MS - Mobile Station
MSC - Mobile Switching Center
PSTN - Public Switched Telephone Network
VLR - Visitor Location Register

GSM NETWORK MANAGEMENT ARCHITECTURE

GSM NETWORK MANAGEMENT ARCHITECTURE



ADC - Administration Center
AUC - Authentication Center
BSS - Base Station System
EIR - Equipment Identity Register
HLR - Home Location Register
MSC - Mobile Switching Center
NMC - Network Management Center
VLR - Visitor Location Register

THE SS7 ARCHITECTURE

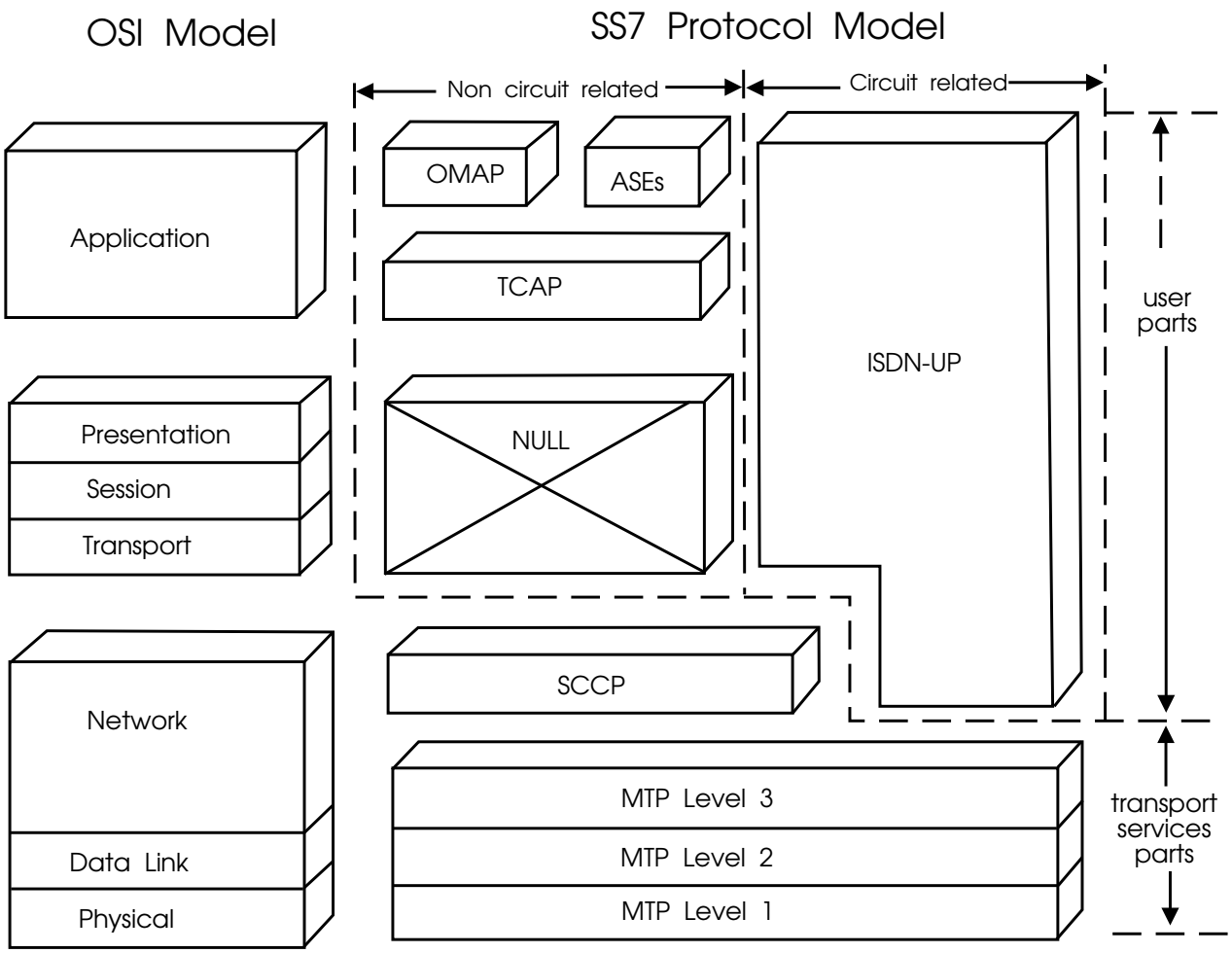
The SS7 protocol levels can be subdivided horizontally into two major parts: the lower part or transport services part and the upper part or user part.

The MTP in the lower part provides a routing service for its users. It consists of three levels: the physical, data link and network levels with corresponding OSI functionality. It uses in its level-3 header level-3 addresses, the Signaling Point Codes (SPC) or Point Codes (PC) to forward "upper part" messages to their destination in the network, that is, to select the next data link to forward the message. Every network entity (STP, 4ESS, 1AESS, 5ESS, NCP), which may generate or receive an SS7 message is labeled with a Signaling Point Code (SPC), called Destination Point Code (DPC) or Origination Point Code (OPC) according to whether it is the destination or the origin of a level-3 MTP message.

Note that a SS7-network user is considered to implement also OSI level 4 to 7 functionality. The fact that the SS7 function is, in the greater scheme of things, a service function does not limit it in terms of OSI functionality.

Other user parts like the Telephone User Part (TUP) and the Data User Part (DUP) are not shown in the diagram. Their functions are provided in the ISDN-UP protocol.

THE SS7 ARCHITECTURE

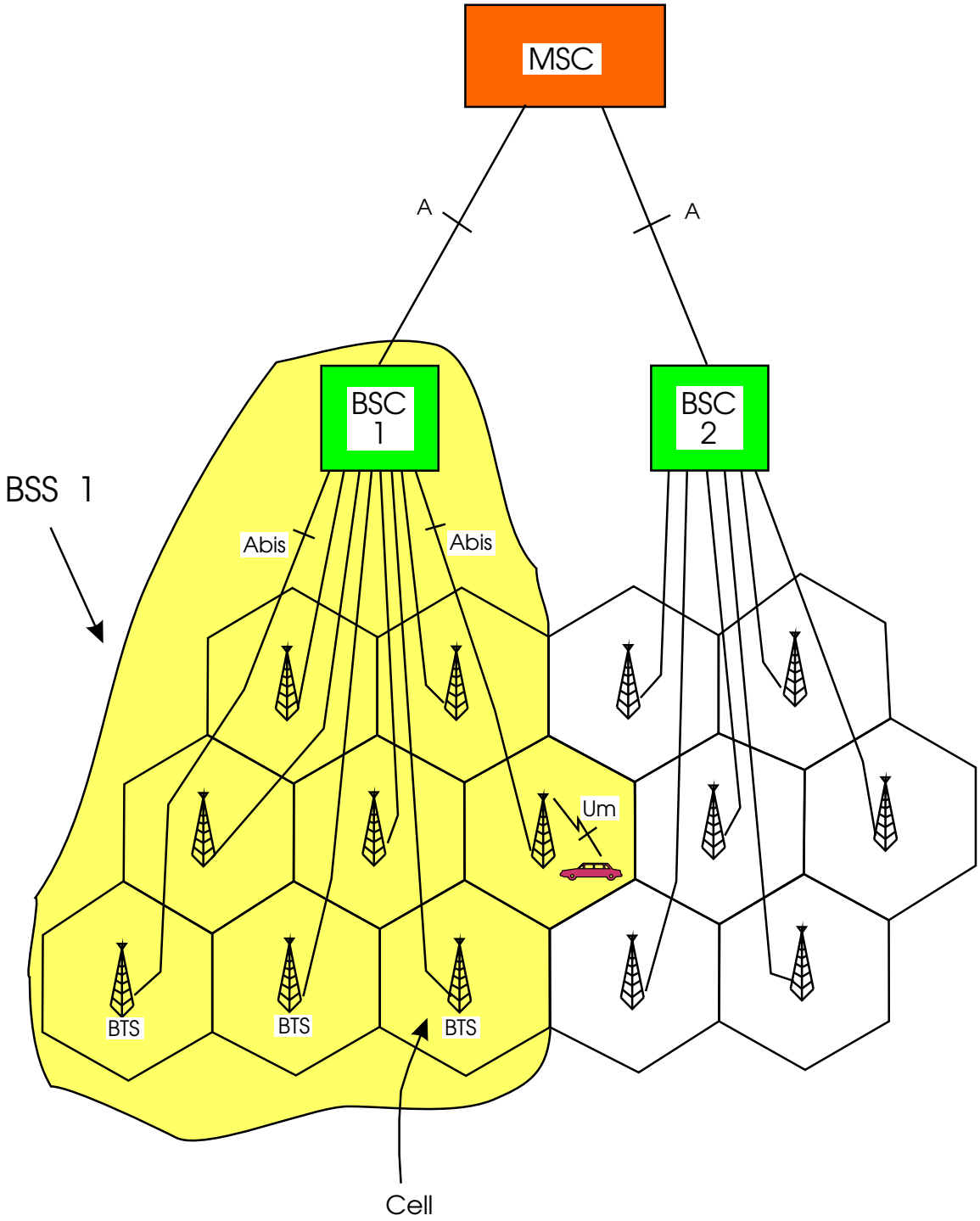


OMAP	Operations Maintenance & Administration Part
ASE	Application Service Element
TCAP	Transaction Capability Application Part
ISDN-UP	ISDN User Part
SCCP	Signaling Connection Control Part
MTP	Message Transfer Part

BASE STATION SYSTEM (BSS) ARCHITECTURE

- A Base Station System (BSS) consists of one Base Station Controller (BSC) and a multiple Base Transceiver Stations (BTSs).
- Each BTS serves a cell area.
- A BTS consists of a controller, radio transmitter/receivers, RF amplifiers, RF combiners, an antenna, and much more.
- BTS equipment will most likely be co-located with the antenna. With the future need for micro-cells it will be necessary, however, to support antennas that can be remote from the rest of the BTS control complex.
- A BSC manages resources and executes procedures that are common to all BTSs. If a BSC is equipped with a time-slot switching fabric, then a BSC can manage handovers between two of its subordinate BTS without involving the MSC.
- BTSs are connected to a BSC over standard 32 channel digital facilities (operating at 2.048 Mbps).
- A BTS can be only be connected to one BSC.
- There does not appear to be a specification within the GSM standards with respect to the maximum number of BTSs that can connect to one BSC (at least the author of this material hasn't stumbled across any requirements yet).
- A BSC is connected to a MSC also over standard 32 channel digital facilities.
- A BSC can only be connected to one MSC.
- A BSC can be physically positioned anywhere (geographically speaking) between a MSC and its BTSs.
- It is advantageous to cluster adjacent BTSs under the the same BSC to minimize the MSC involvement with handovers.

BASE STATION SYSTEM (BSS) ARCHITECTURE



BSS - CONTINUED

BSS Base Station System
BSC Base Station Controller
BTS Base Transceiver Station
BCF Base Control Function
TRX Transceiver

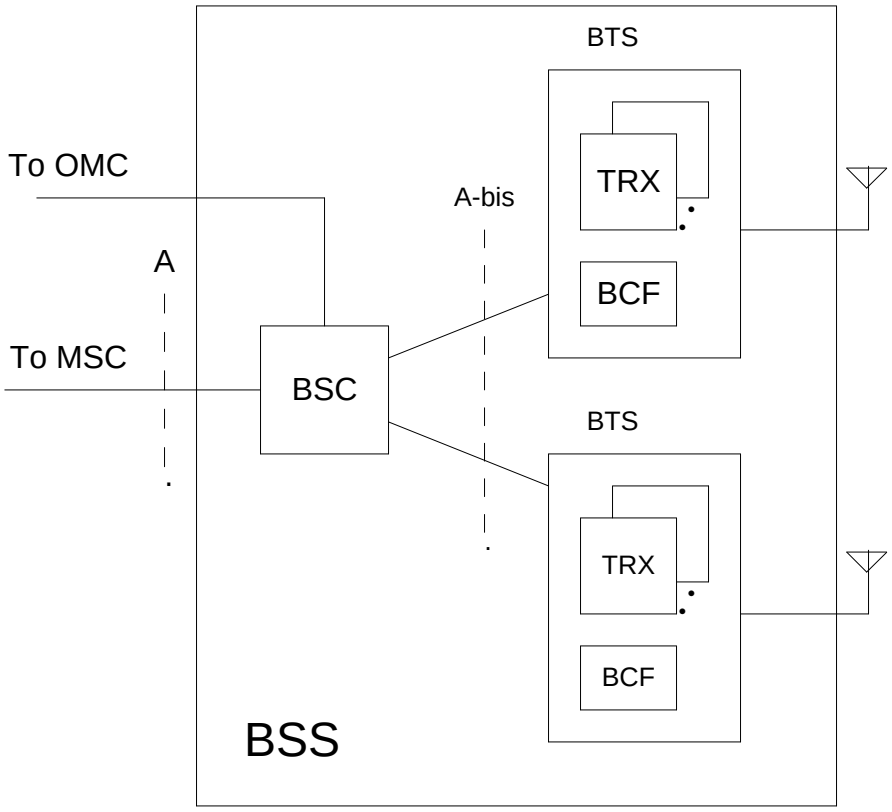
The BSC control one or more BTSs.

The BTS serves one cell in the cellular network and contains one or more TRXs.

The BCF handle common control functions within a BTS.

The TRX serves full duplex communications to the MS.

BSS - CONTINUED



- Responsible for communicating with mobile stations in cell areas
- Radio equipment of a BSS may sustain one or more cells
- One BSC controls one or more BTSs
- One BTS serves one cell

MOBILE-STATION/BASE-STATION INTERFACE

The signaling protocol model for the "air" interface at the mobile station is shown. The physical layer (L1) of this interface is also referred to as the radio subsystem layer. This layer interfaces to the data link layer and the radio resource management sublayer in the Mobile Station (MS) and base station, and to other functional units in the MS and network subsystem (which includes the BSS and the MSC) for supporting traffic channels. At the physical level, most signaling messages carried on the radio path are in 23 octet blocks.

The GSM data link layer (L2) functions include link multiplexing, error detection and correction, flow control, and segmentation to allow for long messages on the upper layers. The protocol is similar to ISDN LAPD and is called *LAPDm*.

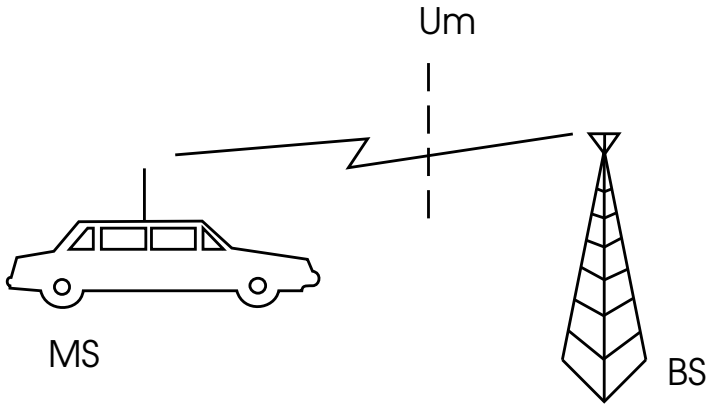
The Radio Resource (RR) layer manages the dialog between the MS and BSS concerning the management of radio connections. It includes such things as connection establishment, control, release, and changes (e.g., during handover).

The Mobility Management (MM) layer deals with supporting such functions as location updating, authentication, and encryption management in a mobile environment.

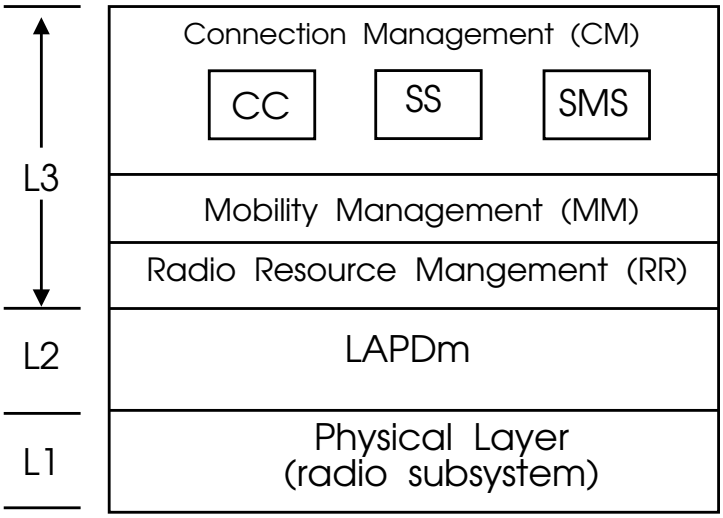
In the Connection Management (CM) layer, the Call Control (CC) entity controls end-to-end call establishment, and the Supplementary Services (SS) entity supports the management of supplementary services. Both protocols are very similar to those used in the fixed network. Finally, the Short Message Service (SMS) protocol of this layer supports the high level functions related to the transfer and management of short message services.

Details on the MS to network interface are described in the GSM 04 series.

MOBILE-STATION/BASE-STATION INTERFACE



Signaling Protocol Reference Model at MS



CC	Call Control entity
SS	Supplementary Services support entity
SMS	Short Message Service support entity
LAPDm	Link Access Procedures on Dm channel

MOBILE SERVICES SWITCHING CENTER (MSC)

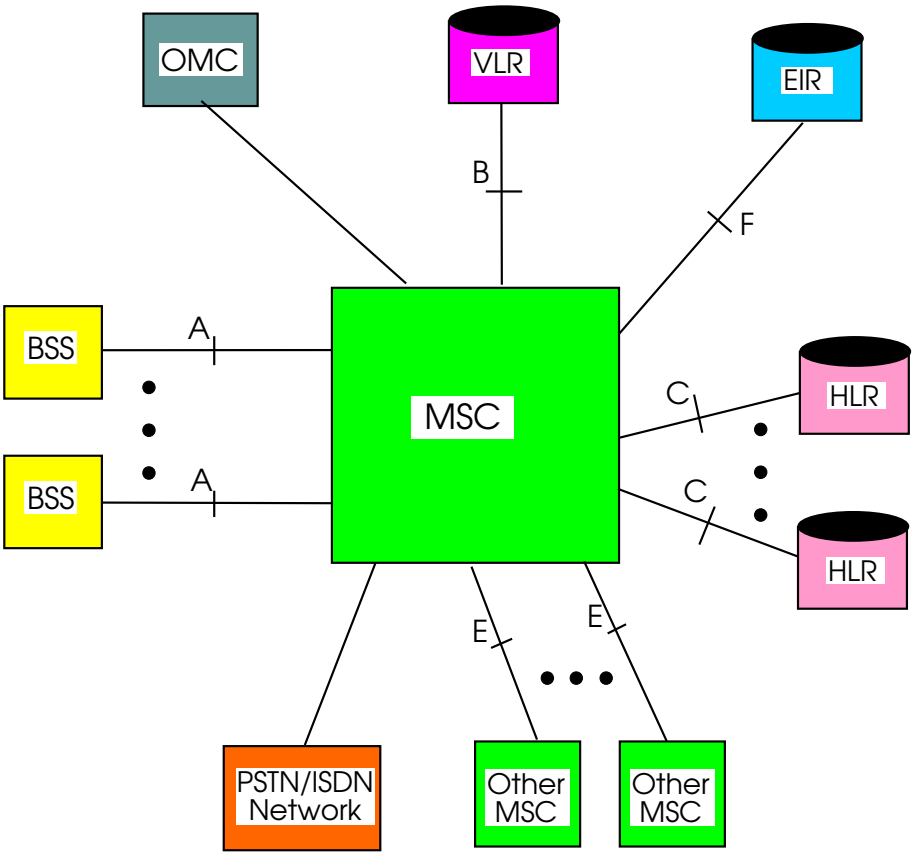
Functions of the MSC include:

- Call handling that copes with mobile nature of subscribers (e.g., paging)
- Management of required logical radio-link channel during calls
- Management of MSC-BSS signaling protocol
- Control of inter-BSS handovers
- Acting as a gateway MSC to interrogate the HLR for routing incoming calls to the called MS
- Exchange of signaling information with other system entities
- Other normal functions of a local exchange switch in the fixed network

MSC interfaces with other network elements.

- An MSC typically controlled by one OMC.
- An MSC can be connected to only one VLR. Therefore, all mobile stations that move around under base stations connected to the MSC are always managed by the same VLR.
- An MSC would communicate typically with one EIR. While it is possible for an MSC to communicate to multiple EIRs, this is highly unlikely since the EIR provides a centralized and geographic independent function.
- The MSC consults an HLR to determine how a call should be routed to a given mobile station. For incoming calls to a mobile station, the MSC would typically consult one HLR. For mobile-to-mobile calls in larger networks, a MSC could consult HLRs of other systems to help minimize the trunk paths to the other mobile station.
- A given MSC can be interconnected to other MSC to support inter-MSC handovers. The E interface is only a signaling interface and should not be confused as a voice path. How voice facilities are connected between MSC are outside the scope of the GSM recommendations. A detailed discussion on inter-MSC voice facilities is provided in the Handover Section in the Call Management Unit.

MOBILE SERVICES SWITCHING CENTER (MSC)



BSS/MSC INTERFACE (A)

The physical layer of the A interface is a 2 Mbps (32 x 64 kbps) standard CCITT digital connection.

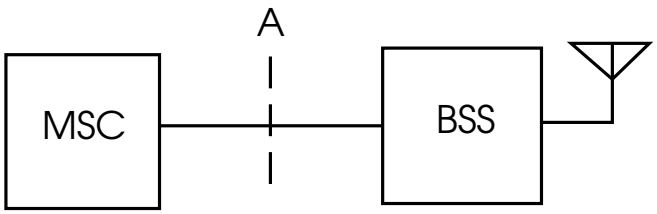
The signaling transport mechanism is handled by the MTP and SCCP parts of SS7. Error free transport is handled by a subset of MTP and the logical connection is handled by a subset of SCCP.

The application parts of divided between BSSAP and BSSOMAP. The BSSAP is further divided into DTAP and BSSMAP. DTAP is in shape of transferring layer 3 messages between the MS and the MSC without BSC involvement in the analysis. BSSMAP is responsible for all aspects of the radio resource handling at the BSS.

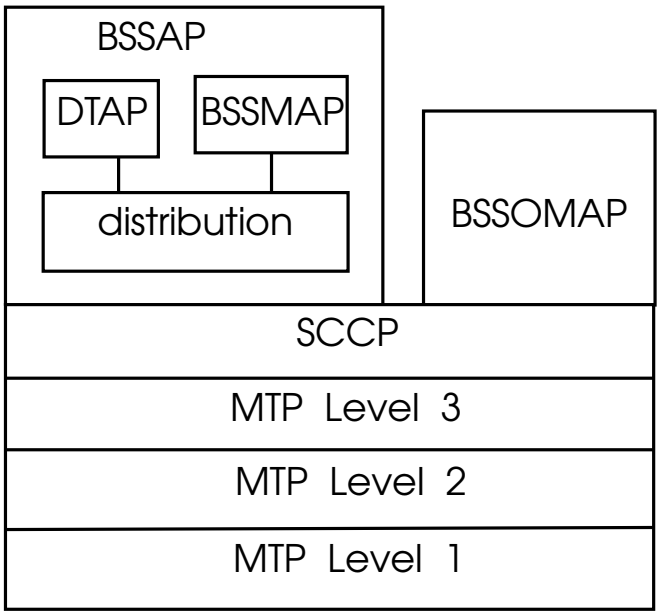
The BSSOMAP supports all the operations and maintenance communications of BSS.

See GSM 08 series for more details.

BSS/MSC INTERFACE (A)



Signaling Protocol Reference Model

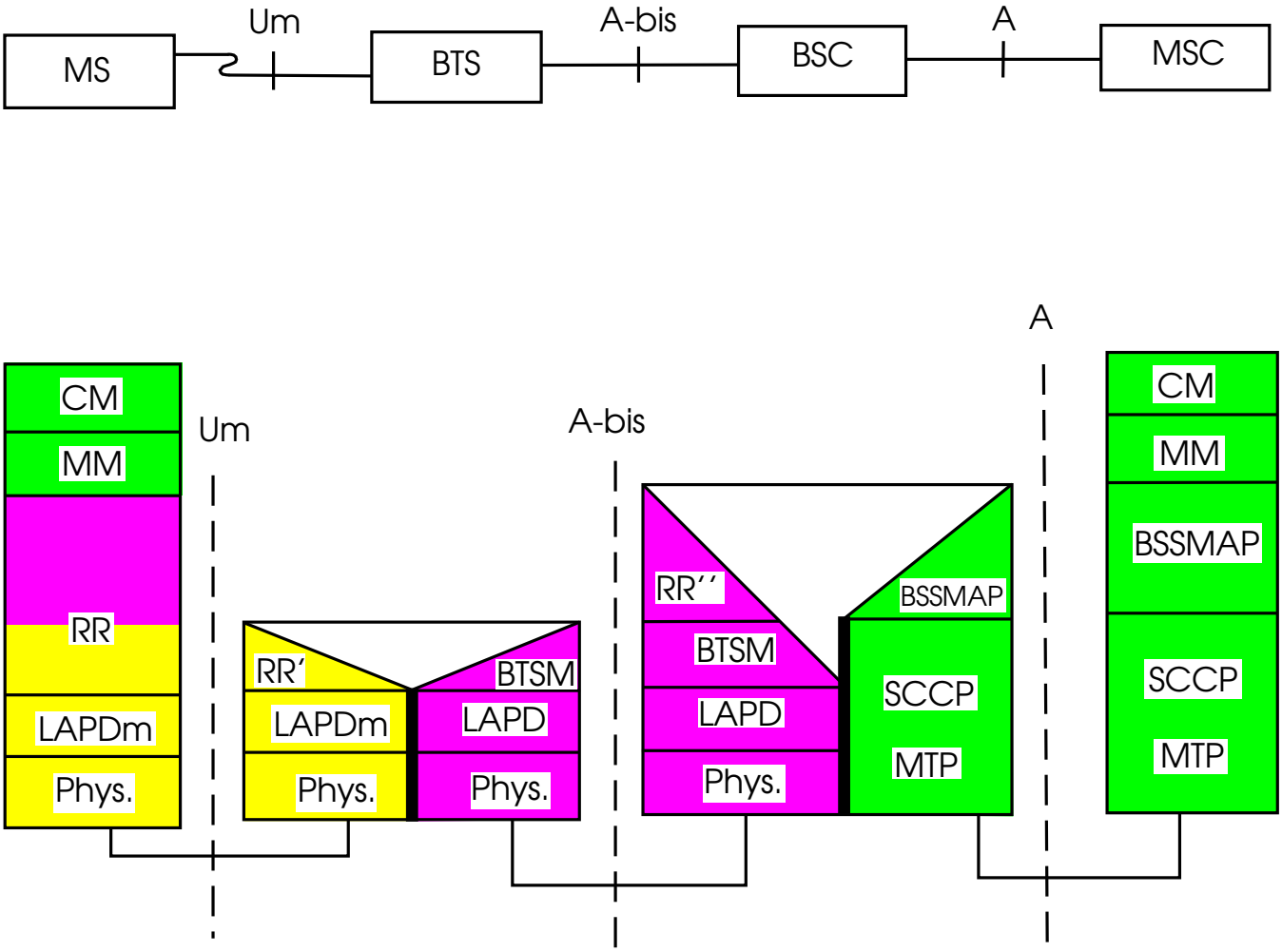


BSSAP	BSS Application Part
DTAP	Direct Transfer Appliation Part
BSSMAP	BSS Management Application Part
BSSOMAP	Operations and Maintenance Application Part
SCCP	Signaling Connection Control Part
MTP	Message Transfer Part

MS-BTS-BSC-MSC SIGNALING PROTOCOL MODEL

CM	Connection Management
MM	Mobility Management
RR	Radio Resource Management
LAPD	Link Access Procedures on D channel
LAPDm	Link Access Procedures on Dm channel
BTSM	BTS Management
BSSAP	BSS Application Part
SCCP	Signaling Connection Control Part
MTP	Message Transfer Part

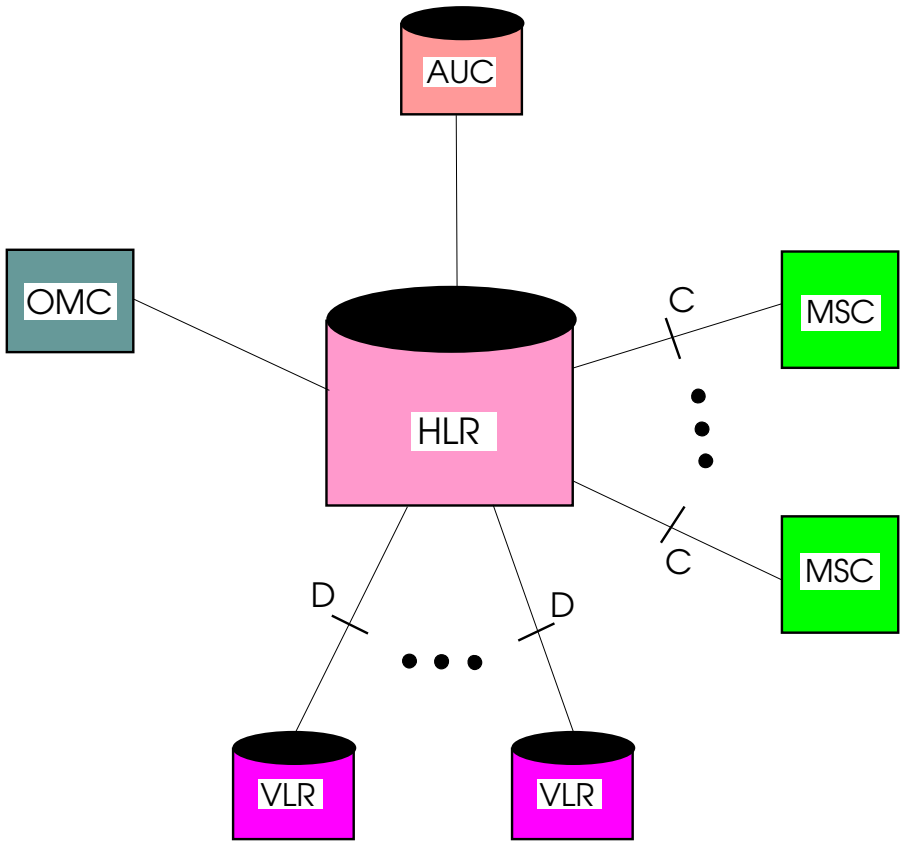
MS-BTS-BSC-MSC SIGNALING PROTOCOL MODEL



HOME LOCATION REGISTER (HLR)

The Home Location Register (HLR) contains the identities of mobile subscribers (called International Mobile Subscriber Identities or IMSIs), their service parameters, and their location information. The location information is stored as a Mobile Station Roaming Number (MSRN) which is a directory number that the network can use to route calls to the Mobile Switching Center (MSC) where the mobile subscriber is located at the time of the call.

HOME LOCATION REGISTER (HLR)



Contains:

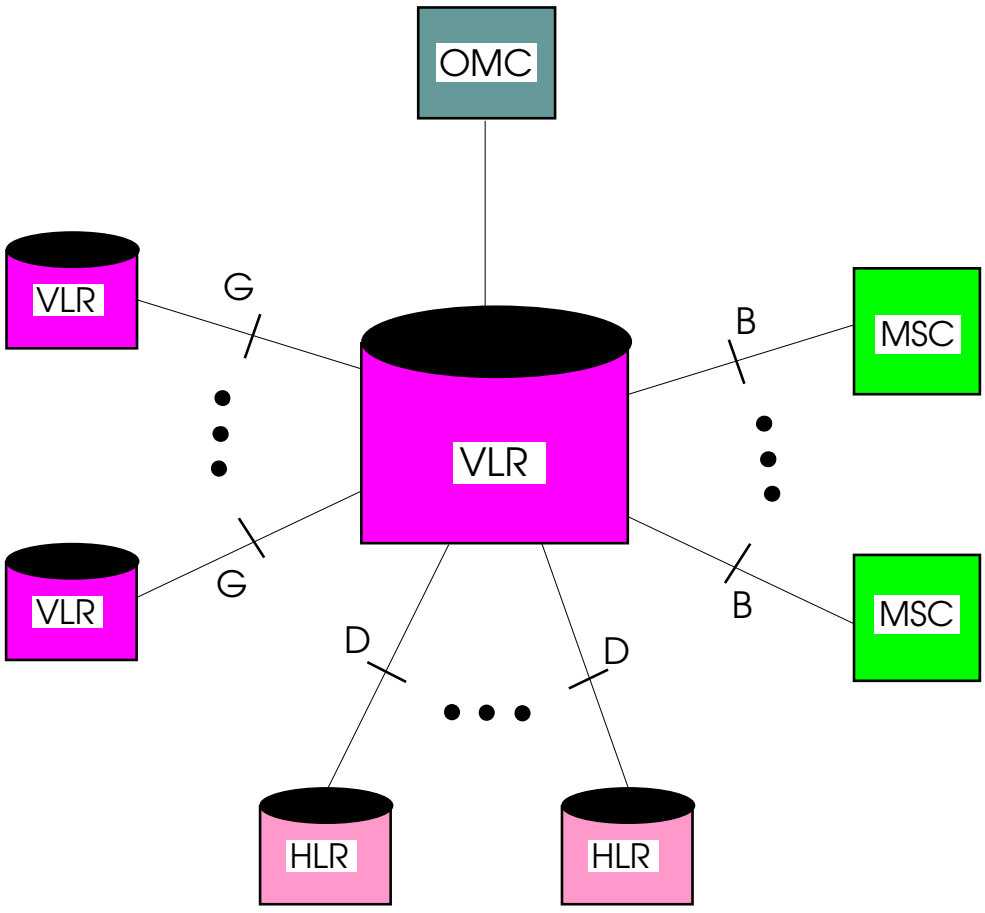
- Identity of mobile subscriber
- Directory number of mobile subscriber
- Subscription information on teleservices and bearer services
- Service restrictions (if any)
- Supplementary services

- Location information for call routing

VISITOR LOCATION REGISTER (VLR)

The Visitor Location Register (VLR) contains the subscriber parameters and location information for all mobile subscribers currently located in the geographic area (i.e., cells) controlled by that VLR. The VLR allocates the MSRN and (when required) a Temporary Mobile Subscriber Identity (TMSI) for secret identification of the mobile subscriber on the radio link.

VISITOR LOCATION REGISTER (VLR)



Contains:

- Identity of mobile subscriber
- Directory number of mobile subscriber
- Copy of subscriber data from HLR

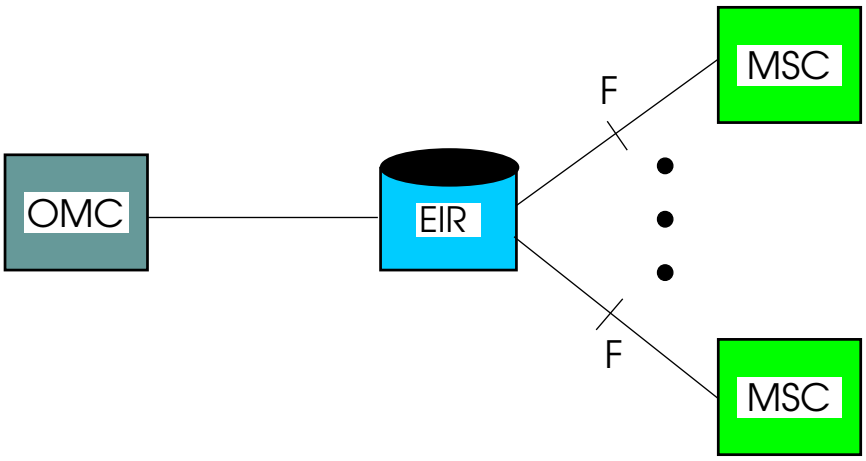
- Location area where mobile is registered
- Temporary mobile subscriber identity

EQUIPMENT IDENTITY REGISTER (EIR)

IMEI International Mobile Equipment Identity

This database is accessed during the equipment validation procedure when a mobile accesses the system. It contains the identities of mobile station equipments (IMEIs) which may be valid, suspect, or known to be fraudulent. In the GSM recommendations, the valid, suspect, and fraudulent list are referred to as the: white, gray and black lists.

EQUIPMENT IDENTITY REGISTER (EIR)



Contains:

- Valid list — list of valid Mobile Equipment identities
- Suspect list — list of Mobile Equipment identities under observation
- Fraudulent list — list of Mobile Equipment identities for which service should be barred

AUTHENTICATION CENTER (AUC)

- Since a GSM cellular system is based on a wireless access method, it is necessary for mobile stations to transmit their identity to the network. The purpose of an Authentication Center (AUC) is to generate authentication parameters that are used by Visitor Location Registers (VLRs) to make sure the identity transmitted by a mobile station is the correct identity and to generate encryption/cipher keys that will be used to encrypt the radio path.
- The Operational Maintenance Center (OMC) interfaces with the AUC for administration purposes, such as adding/changing/deleting Authentication Keys (Ki).
- The only other network element that communicates with an AUC is the corresponding Home Location Register (HLR). No other network elements communicate with the AUC. If a mobile station is visiting other networks, the VLR in the other networks communicate the mobile station's HLR. The HLR, in turn, retrieves information from the AUC and passes this information to the requesting VLR.
- The AUC is a database that contains a unique Authentication Key (Ki) for each mobile subscriber. The AUC also contains algorithms which generate authentication parameters. These algorithms can be CPU intensive.
- GSM does not define the interface between the HLR and AUC. Consequently, this interface is not an open interface. The AUC can be viewed as an adjunct computer to the HLR, which has been delegated the responsibility of managing authentication keys and generating authentication parameters.
- Most vendors will probably integrate the AUC and HLR. The main reason one might want to separate the AUC from an HLR is to not burden an HLR with CPU intensive algorithms.
- The authentication process is discussed in more detail on Pages 3-68 and 3-70. Information regarding encryption (cipher) key generation is provided on Page 3-74.

AUTHENTICATION CENTER (AUC)

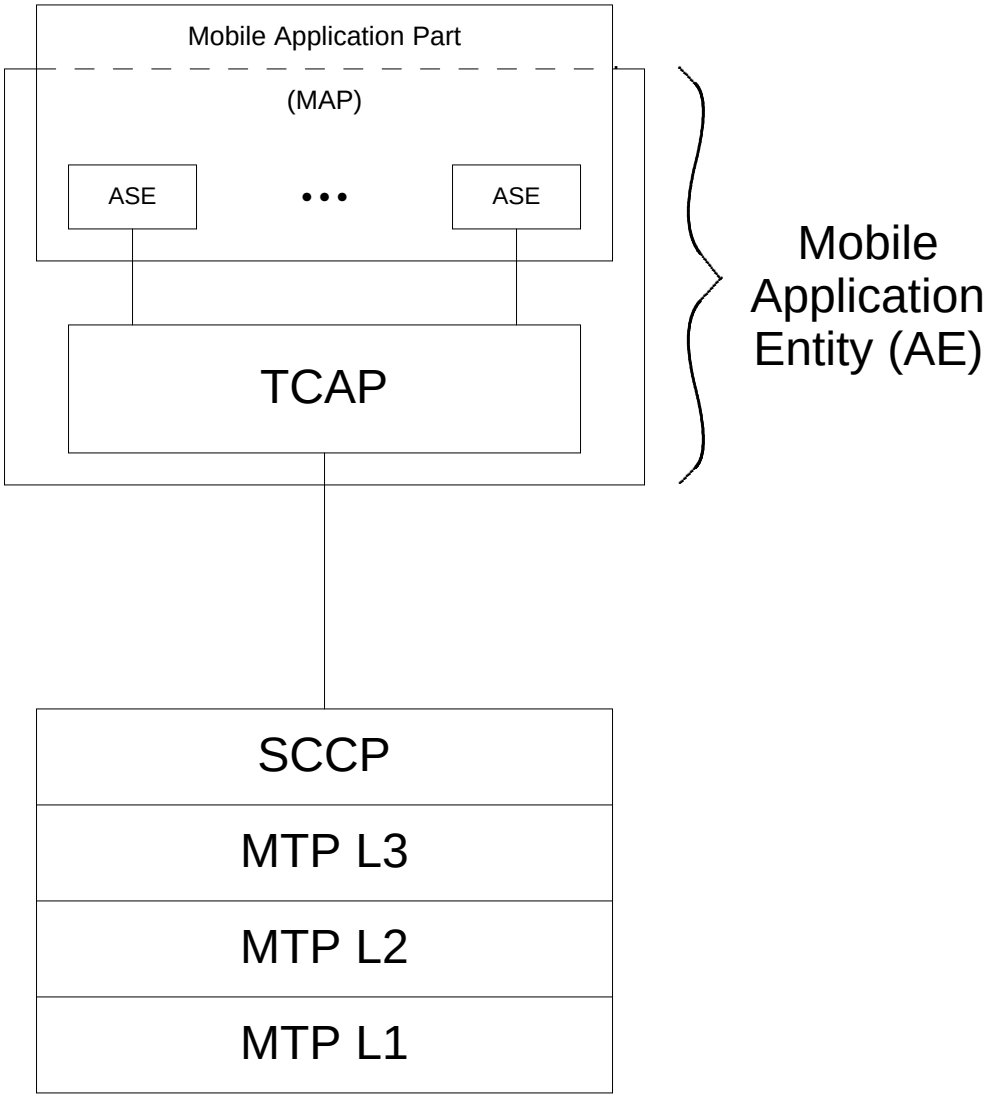
- Contains subscriber authentication data called Authentication Keys (Ki)
- Generates security related parameters needed to authorize service using Ki
- Generates unique data pattern called a Cipher Key (Kc) needed for encrypting user speech and data

MOBILE APPLICATION PART (MAP)

Information transfer between GSM PLMN entities use the Mobile Application Part (MAP) of SS7. MAP consists of a Mobile Application and several Application Service Elements (ASEs). It uses the services of the TCAP part of SS7. The mobile ASEs plus TCAP make up the Mobile Application Entity (AE) of SS7. It uses the SCCP for routing, and only Class 0 (connectionless datagram) service is required.

The MAP layers provide the necessary signaling functions needed to provide services such as setting up mobile facilities for voice and non-voice applications in a mobile network.

MOBILE APPLICATION PART (MAP)



MAJOR PROCEDURES SUPPORTED BY MAP

MAJOR PROCEDURES SUPPORTED BY MAP

- Location registration and cancellation
- Handover procedures
- Handling of supplementary services
- Retrieval of subscriber parameters during call set-up
- Authentication procedures

PUBLIC LAND MOBILE NETWORKS (PLMNs)

The following is the definition of a Public Land Mobile Network (PLMN) from the GSM recommendations[1]

> *A Public Land Mobile Network (PLMN) is established and operated by an administration or Registered Private Operating Agency (RPOA) for the specific purpose of providing land mobile telecommunication service services to the public. A PLMN may be regarded as an extension of a network (e.g., ISDN); it is a collection of MSC areas within a common numbering plan (e.g., same National Destination Code) and a common routing plan. The MSCs are the functional interfaces between the fixed networks and a PLMN for call set-up.*
>
> *Functionally, the PLMNs may be regarded as independent telecommunications entities even though different PLMNs may be interconnected through the ISDN/PSTN Packet/Public Data Networks (PDNs) for forwarding of call or network information. A similar tpe of interconnection may exist for the interaction between the MSCs of one PLMN.*

Presented on the following page is a simple example of two PLMNs. The size of a given PLMN could be small (serve one city), consisting of one of each network element (AUC, HLR, VLR, MSC, and EIR). The largest size PLMN could serve an entire country and can consist of any number and combination of network elements. A PLMN does not cross country boundaries.

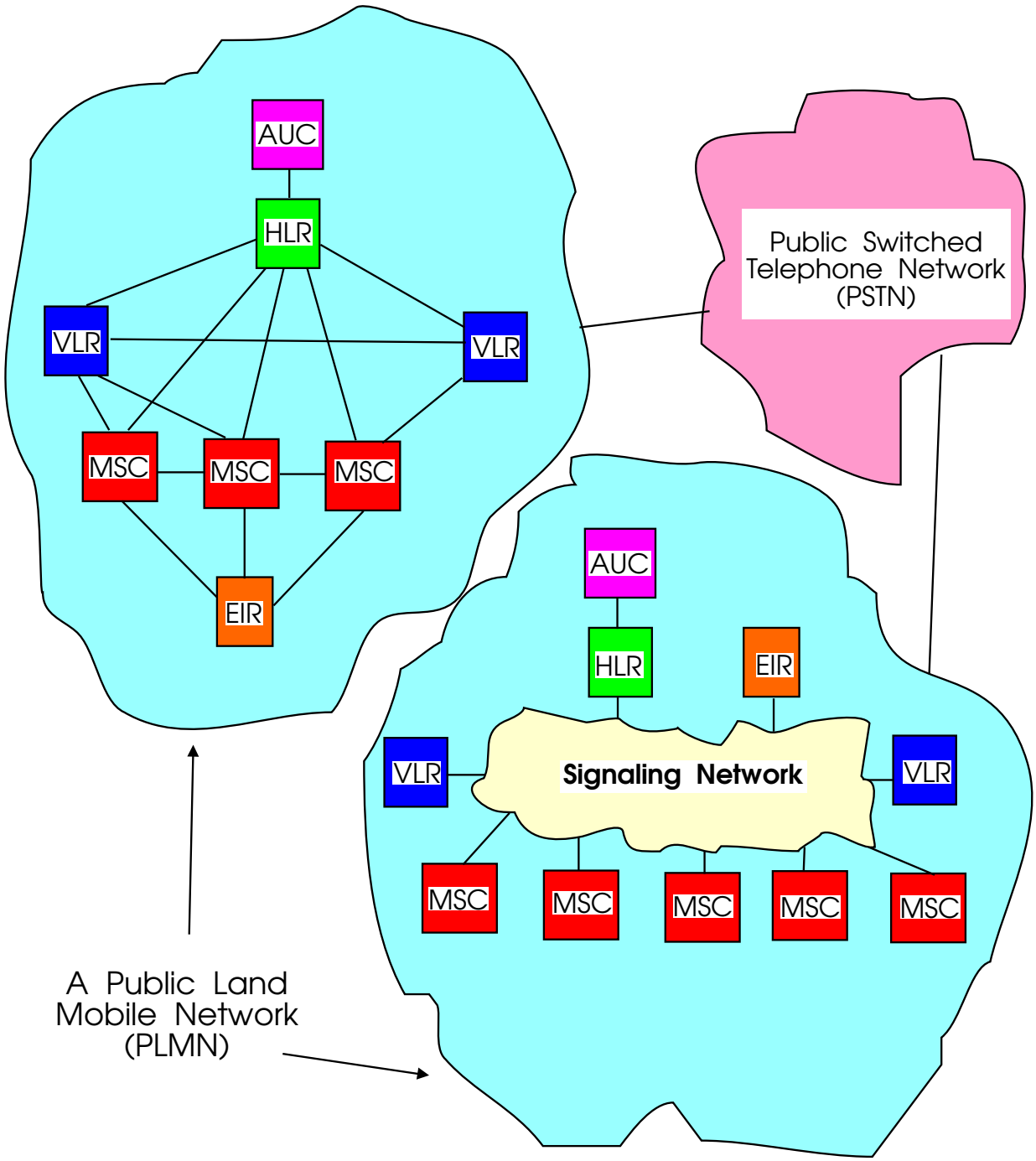
The GSM recommendations do not define the maximum capacity for each network element--this is a vendor specific detail. It is left up to each PLMN operator to purchase network elements from one or more vendors and and properly engineer these network elements. There is not a one-to-one capacity relationship between network elements. For example, a given vendor might provide a product line consisting of a 1000k subscriber HLR, 500k subscriber VLR, and 300k subscriber MSC. The PLMN operator would need to decide how many HLRs, VLRs and MSCs would be required to meet their needs.

With regards to the diagrams on the following page, the solid lines between each network element represent message communication signaling paths. The signaling path topology between network elements is decided by the PLMN operator. One could have dedicated signaling paths between each network element, use a PDN, or a combination of dedicated paths and the use of a PDN.

Not shown in the PLMN examples on the following page are Base Station Systems (BSSs) and Operation Maintenance Centers (OMCs), to keep the vu-graph from being too busy. BSSs and OMCs, of course, are essential components of a PLMN. A PLMN can consist of more than one OMC.

1. GSM Recommendation 03.02, Version 3.1.4, Section 2.5.

PUBLIC LAND MOBILE NETWORKS (PLMNs)



GSM SYSTEM AREA (GSA)

A GSM System Area (GSA) is the entire coverage area where a GSM mobile subscriber can receive wireless access from one or more GSM Public Land Mobile Networks (PLMNs).

Not to be confused with a GSM system area is the definition of a "GSM Service Area". This is the sum of all regions that a GSM subscriber can roam (including their home system area) and get calls from another party without the calling party knowing which region the subscriber happens to be located.

GSM SYSTEM AREA (GSA)

SERVICE QUALITY REQUIREMENTS

SERVICE QUALITY REQUIREMENTS

- Time from switch-on to service ready:

  4 sec in home system
  10 sec in visiting system

- Connect Time to called network:

  4 sec

- Release Time to called network:

  2 sec

- Time to Alert mobile of inbound call:

  4 sec in 1st attempt
  15 sec in final attempt

- Maximum gap due to handover:

  150 ms if intercell
  100 ms if intracell

- Maximum one-way speech delay:

  90 ms

- Intelligibility of speech:

  90%

Contents

Unit 2: System Architecture Overview