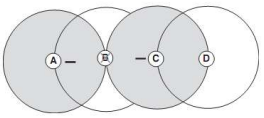
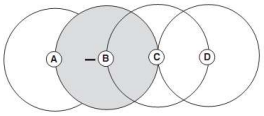
移动通信和无线网络安全

第二讲 面向语音的无线网络

隐藏终端问题和暴露终端问题





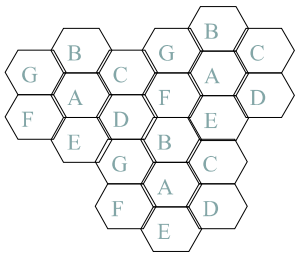
二、蜂窝架构

蜂窝概念

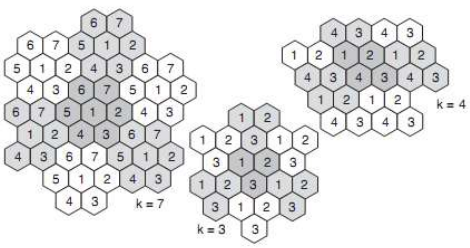
- 蜂窝通信是一种使用频率复用的智能方法，以使有限的带宽可以容纳巨大数量的用户。
  - 其基本原理是把覆盖区域分为大量相连的小区域，每个小区域都使用自己的、低功率的无线基站。由于同样的频谱在分散的区域内可以被多次复用，这样，每次建立一个新的基站（一个小区域）时，容量就会增加。
    - 小区域被称为小区或单元（cell），一组小区组成区群（cluster）。
    - 一个区群中小区的数量称为区群大小或频率复用因子。
  - 需要对这些小区域以智能的方式分配信道，以避免两种干扰：
    - 同频道干扰（cochannel interference）
    - 邻道干扰（adjacent channel interference）

蜂窝拓扑结构

- 蜂窝拓扑结构图

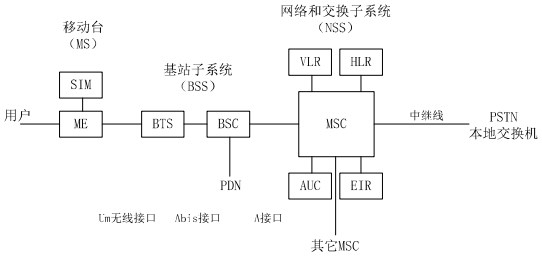


  - 使用蜂窝拓扑可以有效实现频率复用。



蜂窝拓扑结构

- 典型蜂窝网络GSM的组成



- 越区切换（handoff）过程
  - 当某移动终端离开一个小区时，就会询问所有邻近的基站收到该电话的信号的强弱。该基站随后将控制权转交给获得最强信号的小区。该电话随即被告之它有新的管理者，并且如果正在进行通话，它会被要求切换到新的信道。

三、第一代蜂窝架构

第一代蜂窝网架构

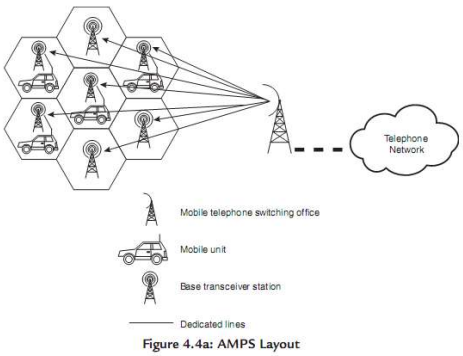
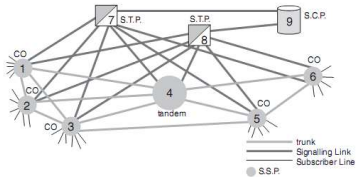


Figure 4.4a: AMPS Layout

- The Architecture of PSTN
  - the signaling network: Signaling System #7 (SS7)
  - the media network:

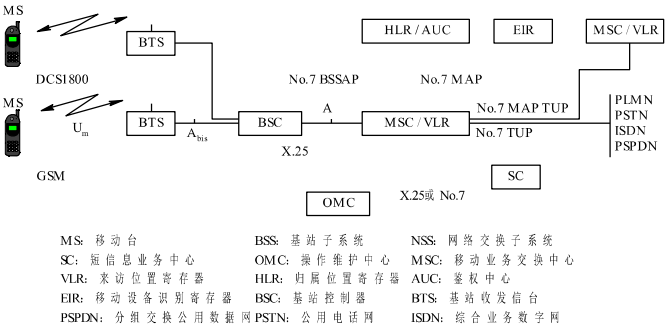


- Media Network:
  - Central Office (CO)：中心局（电话总机）
  - tandem office：汇接局
  - Trunks：干线
    - 每个端局有大量的外线引到附近的一个或多个交换中心，即长途局(toll office)，也称汇接局(tandem office)；连接端局和长途局的线路叫做长途接续干线(toll connecting trunks)。

- **Signal Network**
  - 包括监控的功能及定址的处理，并且提供通話信息
  - 带外信令 (Out-of-band Signaling)
  - 第七号信令系統 (Signaling System No.7, SS7)
- **Signaling Points (SP): Echanging control messages to perform call management.**
  - 服务交换点 (Service Switching Point, SSP)
    - SS7 的电话交换机，以trunk互连
  - 信令传送点 (Signal Transfer Point, STP)
    - 传送信息的路由器 (router)
    - 为符合可靠性要求，STP采用成对的方式存在
  - 业务控制点（SCP）(Service Control Point, SCP)
    - 每个SCP都有一个应用，用于根据子系统号码查找需要的数据库。

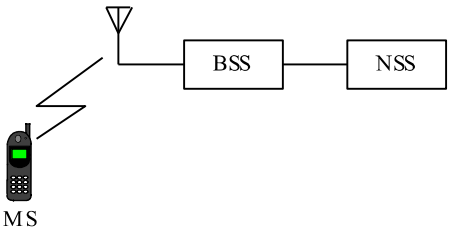
四、第二代蜂窝网

GSM系统组成



MS：移动台　BSS：基站子系统　NSS：网络交换子系统
SC：短信息业务中心　OMC：操作维护中心　MSC：移动业务交换中心
VLR：来访位置寄存器　HLR：归属位置寄存器　AUC：鉴权中心
EIR：移动设备识别寄存器　BSC：基站控制器　BTS：基站收发信台
PSPDN：分组交换公用数据网 PSTN：公用电话网　ISDN：综合业务数字网

GSM系统整体结构框图



GSM蜂窝移动通信系统的简单组成

GSM系统主体部分

1. 网络交换子系统(NSS, Network Switch Subsystem)

1) 移动业务交换中心(MSC, Mobile Services Switching Center)

MSC是GSM系统的核心，是对位于它所覆盖区域中的移动台进行控制和完成话路交换的功能实体，也是移动通信系统与其他公用通信网之间的接口。 它使用户使用各种业务成为可能。

MSC的具体功能如下:

· MSC可从三种数据库(HLR、VLR和AUC)中获取处理用户位置登记和呼叫请求所需的全部数据。反之，MSC也可根据其最新得到的用户请求信息(如位置更新，越区切换等)更新数据库的部分数据。

· MSC作为网络的核心，应能完成位置登记、 越区切换和自动漫游等移动管理工作。同时具有电话号码存储编译、呼叫处理、路由选择、回波抵消、超负荷控制等功能。

· MSC还支持信道管理、数据传输以及包括鉴权、信息加密、 移动台设备识别等安全保密功能。

MSC可为移动用户提供以下服务:

· 电信业务。 例如通话、 紧急呼叫、 传真和短信息服务等:

· 承载业务。 例如3.1 kHz电话, 同步数据0.3~2.4 kb/s及分组组合和分解(PAD)等。

· 补充业务。例如呼叫转移、呼叫限制、呼叫等待、电话会议和计费通知等。

对于容量比较大的GSM系统, 一个网络子系统NSS可包括若干个MSC、VLR和HLR, 当固定网用户呼叫GSM移动用户时, 无需知道移动用户所处的位置, 此呼叫首先被接入到入口移动业务交换中心(亦称移动关口局, 简称GMSC)中, 入口交换机负责从HLR中获取移动用户位置信息, 且把呼叫转接到移动用户所在的MSC那里。

2) 来访位置寄存器(VLR, Visitor Location Register)

VLR是一个数据库, 负责存储MSC为了处理所管辖区域中MS(统称来访用户)的来话接听和去话呼叫所需检索的信息, 例如用户的号码, 所处位置区域的识别, 向用户提供的服务等参数。

具体来讲, VLR是为其控制区域内的移动用户服务的, 它存储着进入其控制区域内的已登记的移动用户的相关信息, 从而为该用户以后的呼叫连接创造了前提条件。VLR从该移动用户所在的归属位置寄存器(HLR)处获得并存储该用户的数据。 一旦用户离开该VLR的控制区域, 则重新在他所进入的另一个VLR登记, 原VLR将取消临时记录的该移动用户的数据。 因此, VLR可看作是一个动态的用户数据库。

3) 归属位置寄存器(HLR, Home Location Register)

HLR是GSM系统的中央数据库, 主要存储着管理部门用于移动用户管理的相关数据, 具体包括两类信息: 一是有关用户的参数, 即该用户的相关静态数据, 包括移动用户识别号码、 访问能力、用户类别和补充业务等; 二是有关用户目前所处状态的信息, 即用户的有关动态数据, 如用户位置更新信息或漫游用户所在的MSC/VLR地址及分配给用户的补充业务等。 每个移动用户都应在其HLR处注册登记。

HLR可以与MSC/VLR一一对应, 也可以一个HLR控制若干个MSC/VLR或整个区域的移动网。

4) 鉴权中心(AUC, Authentication Center)

AVC也是一个数据库, 保存着关于用户的三个参数(随机号码RAND、 响应数SRES和密钥Kc)。 其作用是: 通过鉴权能够确定移动用户的身份是否合法, 还能够进一步满足用户的保密性通信等要求。

鉴权是GSM系统采取的一种安全措施, 用来防止无权用户接入系统和保证通过无线接口的移动用户通信的安全。 任何手机在通话前都要先经过鉴权, 待得到系统确认, 承认其为合法用户后, 方可进入通话接续。 在此过程中, AUC起到了关键的作用。

5) 设备识别寄存器(EIR, Equipment Identity Register)

对移动台身份的核准包括三个组成部分: 入网许可证的核准号码、装配工厂号和手机专用号。 针对不同的核准结果, 移动台的IMEI会分列于白色清单、黑色清单或灰色清单这三种表格之一。 白色清单中收录了所有的核准号码, 拥有该清单中的号码的移动台可以正常使用网络; 黑色清单中收录了所有的挂失移动台和禁止入网移动台的号码, 拥有这些号码的移动台会被暂时禁用(闭锁); 灰色清单收录了所有的出现异常或功能不全, 但不足以禁用的移动台的号码, 拥有这些号码的移动台会受到网络的监视, 随时可能被鉴别出其非法身份。这样便可以确保入网移动设备不是被盗用的或是故障设备, 确保注册用户的安全性。一旦手机丢失, 只要向系统报告该手机的IMEI号码, EIR就会将其列入黑色清单, 使得盗用者空欢喜一场。

2. 基站子系统(BSS, Base Station Subsystem)

基站子系统又称无线子系统, 因为它是GSM系统中与无线蜂窝网络关系最直接的基本组成部分, 主要负责系统的无线方面。 它是一种在特定的蜂窝区域内建立无线电覆盖的设备, 负责完成无线发送、 接收和管理无线资源。

从整个GSM网络来看, 基站子系统(简称基站)介于网络交换子系统和移动台之间, 起中继作用。一方面, 基站通过无线接口直接与移动台相接, 负责空中无线信号的发送、接收和集中管理; 另一方面, 它与网络交换子系统中的移动业务交换中心(MSC)采用有线信道连接, 以实现移动用户之间或移动用户与固定用户之间的通信, 传送系统信号和用户信息等。以移动台用户与固定网络用户之间的通信为例: 基站接收到移动台的无线信号, 经过简单处理之后即传送给移动交换中心, 经过交换中心的交换机等设备的处理, 再通过固定网络(PLMN或ISDN等)传送给固定用户, 即可实现正常的网络通信了。

从组成上看，基站子系统主要包括两类设备：基站收发信台(BTS)和基站控制器(BSC)。通常来说，一个基站只包括一个BSC，而一个BSC根据话务量的需要可以控制一个或多个BTS。BTS可以与BSC直接相连，从而构成一个整体基站系统，其覆盖区为包含若干相邻小区的单一区域；BTS与BSC也可以通过基站接口设备(BIE)采用远端控制(当BSC与BTS间距离超过15 m时)的连接方式相连，此时基站系统服务区为若干个无线覆盖区，如图2-3所示。

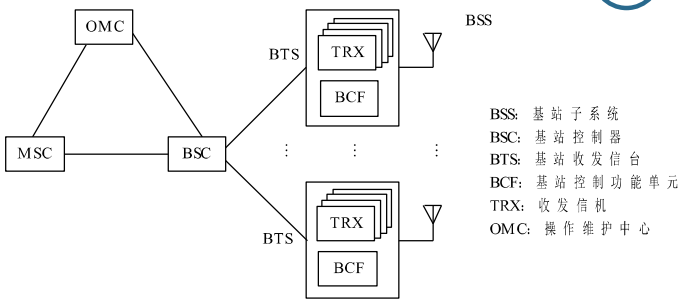
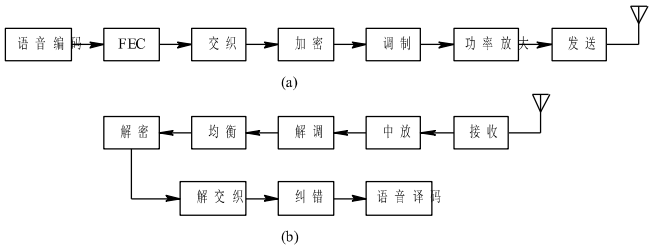


图 2-3 基站原理框图

1) 基站收发信台(BTS, Base Transfer and Receive Station)

BTS属于基站子系统的无线接口设备，完全由BSC控制，主要负责无线传输，完成无线与有线的转换、 无线分集、 无线信道加密、 无线调制、 编码等功能。 具体来说，它可以接收来自移动台的信号，也可以把BSC提供的信号发送给移动台，从而完成BSC与无线信道之间的信号转换。



基站收/发信机组成结构图
(a) 基站发信机; (b) 基站收信机

2) 基站控制器(BSC, Base Station Control)

BSC在BSS子系统内充当控制器和话务集中器，它主要负责管理BTS，而且当BSC与MSC之间的信道阻塞时，由它进行指示。BSC同时具有对各种信道的资源管理、小区配置的数据管理、操作维护、 观察测量和统计、功率控制、切换及定位等功能，是一个很强的功能实体。

基站控制器的核心是交换网络(SW)和公共处理器(CPR)。交换网络完成A_{bis}接口与A接口上64 kb/s的话音/数据业务信道的内部交换。 其容量配置应根据系统容量的需要，可以是16个2 Mb/s端口，也可以是64个2 Mb/s端口。 BSC是多处理器系统，每个功能模块都有各自的处理器。CPR作为公共处理器对BSC内部各模块进行控制管理，包括对内部数据库的管理,以及后备程序寄存器和各种软件的管理。此外，CPR通过X.25接口与系统的操作维护中心(OMC)相连接。CPR还提供RS-232接口，可用于BSC内部的人机通信。

BSC通过A接口与MSC相连，BSC端的接口设备是数字中继控制器(DTC)。 BSC通过A_{bis}接口与BTS相连，BSC端的接口设备是终端控制单元(TCU)，由此构成一个简单的通信网络。

此外，基站子系统还应包括码变换器(TC)和相应的子复用设备(SM)。 码变换器通常放在BSC和MSC之间，可以增加组织网络时的灵活性并可减少传输设备的配置数量。

3. 移动台(MS, Mobile Station)

移动台有三种类型：车载型、 便携型和手持型。车载型移动台(简称车载台)的主体设备安装在车辆的内部，天线与主体设备分离，安装在车外。 车载台可以在较大功率下使用。便携型移动台(简称便携台)为用户手提携带的设备，其天线与设备安装在一起。便携台可以支持系统所要求的所有功率。便携台也可以安装在车辆上，并且通常都具备车辆安装时所用的接头。手持型移动台(简称手持台或手持机)即现在人们通用的手机。与车载台和便携台相比，手机的体积更小、重量更轻、携带更方便，因而是移动台的主流发展方向。手机同样可以安装在车辆上，并且通常具备安装插头。 当安装在车辆上时，可使用外部天线。

1) 移动终端(MT, Mobile Terminal)

移动终端就是“机”，它是移动台的主体，是完成语音编码、信道编码、信息加密、 信息的调制和解调、 信号的发射和接收的主要设备。它可以通过天线接收来自外界无线信道的信号，然后经过一系列的变换和处理，还原成话音信号，供用户接听；相反的，它也可以将用户的话音信号，经过一系列相反的变换和处理，转变成适合无线信道传输的信号形式，通过天线发送出去。 移动终端的组成原理框图如图所示。

1. 基站(BS)与移动台(MS)之间的无线接口—U_m接口

在GSM系统中，移动台通过无线通道与网络的固定部分相连，使用户可以接入网中，从而得到通信服务。移动台(MS)和基站(BS)设备的研制开发是允许分别进行的。为了实现它们的互连，对无线通道上信号的传输必须做出一系列规定，建立一套标准。这套关于无线通道信号传输的规范就是所谓的无线接口，即U_m接口，如图2-7所示。

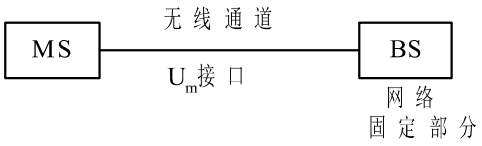


图 PLMN无线接口

作为第二代数字蜂窝移动通信网，GSM的无线接口采用开放系统互连(OSI)参考模型的概念来规定其协议模型。

OSI参考模型的基本结构是分层。根据分层的概念，通信处理过程可以看作是由低层到高层的若干有序的逻辑层次构成。每层都存在实体单元。 在不同系统中的为实现共同目的而必须交换信息的同一层实体称为对等实体(Peer Entities)。相邻层次中的实体通过共同层面相互作用。低层向高层提供服务。也就是，第N+1层所提供的服务是第N层及以下所有各层所提供的服务和功能的组合。

各相邻层之间的服务是通过业务原语来实现的。业务原语表示的是相邻层之间的信息与控制的逻辑交换，并不规定或约束这种交换是如何实现的。业务原语还用于各层次与移动管理实体之间的信息交换。一般地说，第*N*+1层与第*N*层间交换的原语有如下4种类型:

(1) 请求原语类型。 高层向其相邻低层请求一种业务时使用的原语。

(2) 指示原语类型。 提供某种业务的层次通知其相邻高层注意与请求类原语有关的活动时使用的原语。

(3) 响应原语类型。 某层确认收到某个低层的指示原语时使用的原语。

(4) 证实原语类型。 提供请求业务的层为证实操作活动已经完成时使用的原语。

第一层是物理层，为最低层。它包括各类信道，为高层信息的传输提供基本的无线信道。其连接内容包括: ① 工作频段: 890~915 MHz(移动台发), 935~960 MHz(基地台发); ② 射频载波: 124个; ③ 载波间隔: 200 kHz; ④ 多址方式: TDMA; ⑤ 基本帧: 8时隙/每载波; ⑥ 信道速率: 270.83 kb/s, 码元宽度3.7 μs; ⑦ 每时隙信道比特率: 22.8 kb/s; ⑧ 调制方式: GMSK, 调制指数: 0.30; ⑨ 分集方式: 每秒跳频217次，交错信道编码，自适应均衡(可均衡量达16 μs的时延传播)等。

第二层是数据链路层，为中间层，记为LAPDm。 它包括各种数据传输结构，对数据传输进行控制。 数据链路层接受物理层的服务，并向第三层提供服务。

第三层为最高层，记为L3。它提供GSM和与其相连接的其他公众移动网建立、 维护和终止电路交换连接的功能。 它还提供必要的支持补充业务和短信息业务的控制功能以及移动管理和无线资源管理的功能。第三层又可分为无线资源管理(RM)、 移动特性管理(MM)和呼叫管理三个子层。

2. 基站(BS)与移动业务交换中心(MSC)之间的A接口

A接口实质上是基站控制器(BSC)与MSC之间的接口，属于固定网络接口。该接口的信令协议基于CCITT的7号信令系统(No.7)。 A接口支持网络向移动用户提供的所有业务，同时支持在PLMN内分配无线资源以及对这些资源的管理。

A接口可用下述特性来规定:

(1) 物理和电气参数;

(2) 信道结构;

(3) 网络操作过程;

(4) 操作与维护信息支持。

3. 基站收/发信机(BTS)与基站控制器(BSC)之间的接口—A_{bis} A_{bis}接口是BTS与BSC之间的固定网络接口，主要为BTS和BSC完成各种功能时提供信息交换。当BTS和BSC不在同一地点时，必须有此接口。反之不然。 A_{bis}接口支持网络对移动用户提供的所有业务，同时还支持BTS内的无线设备控制和无线频率分配。

A_{bis}接口由下述特性所规定:

(1) 物理和电气参数;

(2) 信道结构;

(3) 信令传输程序;

(4) 配置和控制程序;

(5) 操作与维护信息支持。

4. 移动业务交换中心(MSC)与公众网之间的ISUP和TUP接口

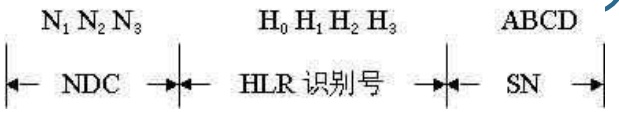
ISUP(ISDN User Part)是No.7信令系统的ISDN用户部分，它定义了综合业务数字网(ISDN, Integrated Server Data Network)中电路交换业务控制，包括话音业务(如电话)和非话业务(如电路交换数据通信)控制所必需的信令消息、 功能和过程; TUP(Telephone User Part)是No.7信令系统的电话用户部分，它规定了电话业务中呼叫控制所需的信令程序以及实现这些信令程序所需的消息和消息格式。 通过这两个功能级，MSC可分别与ISDN和公众电话交换网(PSTN)配接，因此，GSM系统具有广泛的联网能力。

GSM系统的编号

- MSISDN
- IMSI
- TMSI
- IMEI
- MSRN
- LMSI
- LAI
- CI
- BSIC

MSISDN

- Mobile Subscriber Integrated Services Digital Network (MSISDN) number
  - **移动用户的MSISDN号码相当于固定网的用户电话号码，是供用户拨打的公开号码。**
  - **MSISDN的编码方法按照CCITT的建议，号码结构如下：**

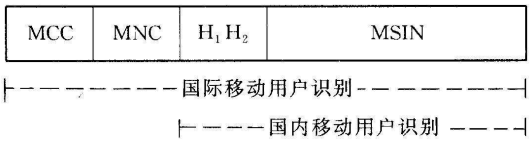


- **数字蜂窝移动业务接入号NDC：13S(S＝9、8、7、6、5这些为中国移动通信公司的接入网号；中国联通公司目前的接入网号为130，131);**
- **HLR识别号：H0 H1 H2 H3 ，我国的H0 H1 H2 H3分配分为H0=0和H0≠0两种情况。**
- **移动用户号：ABCD，由各HLR自行分配。**

IMSI

- **国际移动用户识别(IMSI, International Mobile Subscriber Identity)**
  - 每个GSM移动用户都有一个IMSI, 而且具有全球惟一性和永久不变性(更换身份证或丢失SIM卡的情况除外)。IMSI用于GSM通信网的所有信令中, 在用户的SIM卡、 系统的HLR和VLR中都有存储。

IMSI号码的结构为:

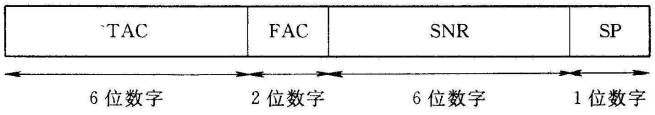


- MCC：Mobile Country Code，移动国家码，共3位，中国为460;
- MNC:Mobile Network Code，移动网络码，共2位，中国电信CDMA系统使用03，一个典型的IMSI号码为460030912121001;
- MSIN:Mobile Subscriber Identification Number共有10位，其结构如下：

  H1H2 + M0M1M2M3 + ABCD
  - H1H2:用户在其PLMN中的HLR地址
  - M0M1M2M3和MDN号码中的H0H1H2H3可存在对应关系
  - ABCD四位为自由分配。

IMEI

- **国际移动台设备识别码(IMEI, International Mobile Equipment Identity)**
  - 惟一地标识一个移动台设备的编码
  - IMEI编码最多由15位十进制数字组成。



- TAC(Type Approval Code)是型号批准码, 6位数, 由欧洲型号认证中心统一分配, 在设备通过验收时提供给生产厂家。
- FAC(Factory Assembly Code)是生产厂家装配码, 2位数, 用以识别生产厂家及设备装配地。
- SNR(Serial Number)是序号码, 6位数, 由生产厂家分配, 用以识别特定的设备。
- SP(Spare)是备用号码, 1位数, 以备将来之用。
- 在GSM的Phase2+阶段, IMEI被扩展到了16位。其中, 最后2位用来标明终端软件的版本号SVN(Software Version Number), 因此简写为IMEISV。

TMSI

- **临时移动台标识(TMSI, Temporary Mobile Station Identity)**
  - **为加强系统的保密性而在VLR内分配的临时用户识别号。它在某一VLR区域内与IMSI唯一对应。**
  - **分配原则**
    - **包含四个字节**
    - **不能全为1，全为1表示无效TMSI**

MSRN

- **移动台漫游号(MSRN, Mobile Station Roaming Number)**
  - 移动台漫游号码是当移动台由所属的MSC / VLR业务区漫游至另一个MSC / VLR业务区中时, 为了将对它的呼叫顺利发送给它而由其所属MSC / VLR分配的一个临时号码。
  - MSRN与MSISDN结构相同

本地移动用户识别码(LMSI)

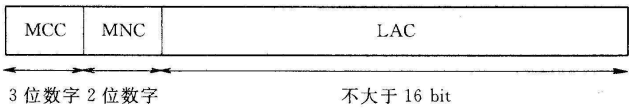
- 为了加速VLR对用户数据的查询，还可使用辅助性的本地移动用户识别码LMSI，它是在位置更新时，VLR暂分配给来访用户的一个唯一识别码。LMSI虽属可选，但如果在每次呼叫基础上分配移动用户漫游号MSRN时，则需使用LMSI。
- 长度：4个字节，没有具体定义。

LA(Location Area)

- **当我们在一个MSC/VLR的业务区域内搜寻被叫用户时，我们发现在这样大的区域内搜寻一个用户，会花费MSC/VLR大量的工作量。因此，有必要将MSC/VLR的业务区域划分成若干较小的区域，这些小的区域称为位置区LA**

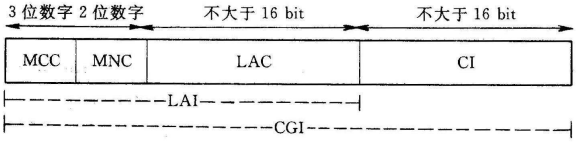
LAI

- 位置区识别(LAI, Location Area Identity)



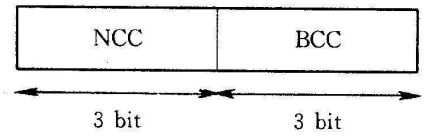
CI

- 全球小区识别码(CGI, Cell of Global Identity)
  - 在LAI后加上CI(Cell Identify，小区识别码）
  - CI长度：两字节

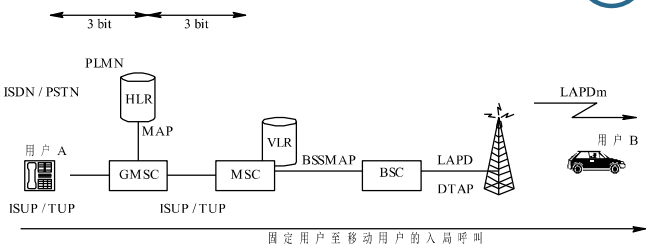


BSIC

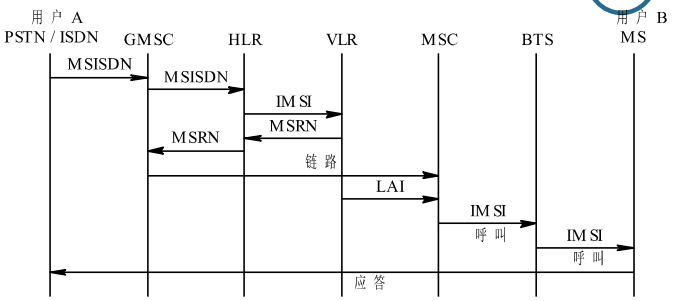
- 基站识别色(BSIC, Base Station Identity Color)码
  - 基站识别色码用于移动台识别使用相同载波的不同基站



- 第一步：固定网络用户A拨打GSM网用户B的MSISDN号码, A所处的本地交换机根据此号码与GSM网的相应入口交换局(GMSC)建立链路, 并将此号码传送给GMSC。
- 第二步：GMSC据此号码分析出B的HLR, 即向该HLR发送此MSISDN号码, 并向其索要B的漫游号码(MSRN)
- 第三步： HLR将此MSISDN号码转换为移动用户识别码(IMSI), 查询内部数据, 获知用户B目前所处的MSC业务区, 并向该区的VLR发送此IMSI号码, 请求分配一个MSRN。
- 第四步：VLR分配并发送一个MSRN给HLR
- 第五步：再由HLR传送给GMSC。
- 第六步：GMSC有了MSRN, 就可以把入局呼叫接到B用户所在的MSC处。
- 第七步：MSC根据从VLR处查到的该用户的位置区识别码(LAI), 将向该位置区内的所有BTS发送寻呼信息(称为一起呼叫), 而这些BTS再通过无线寻呼信道(PCH)向该位置区内的所有MS发送寻呼信息(也是一起呼叫)。
- 第八步：B用户的MS收到此信息并识别出其IMSI码后(认为是在呼叫自己), 即发送应答响应。

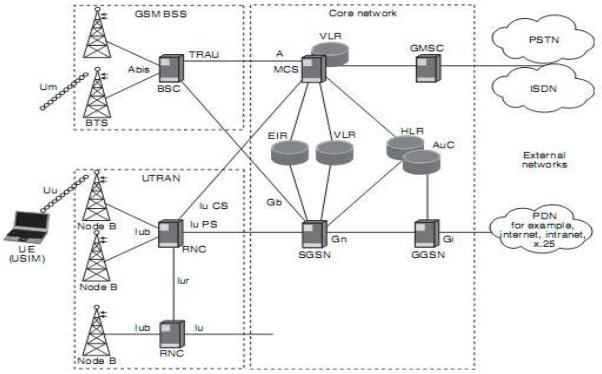


固定用户至移动用户的入局呼叫框图



固定用户至移动用户的入局呼叫流程图

五、第三代蜂窝网



- 与2G网络的区别
  - 使用码分多址(CDMA)
  - 强调从网络核心到网络边缘的智能移动
  - 语音网络和IP网络的整合