## 1.手机的硬件实现方式主要有3种：

只用基带芯片（BP）通常称为feature phone。

基带芯片+协处理器（CP，通常是多媒体加速器）。这是增强了多媒体功能的feature phone。

基带芯片+应用处理器（AP），也就是通常说的智能手机（smart phone）

## 2.功能机、智能机

功能机 <= 只有一颗专门处理数据业务的芯片（modem）

智能机 <= 一颗专门处理数据业务的芯片（modem）外加一颗专门处理应用业务的主芯片（AP）

平板 <= 只有一颗专门处理应用业务的主芯片（AP）

功能机是在不断扩充应用功能的无线通信终端（行业术语叫移动台），而智能手机是增加了无线通信功能的手持式电脑。

## 3.AP、BP

AP：Application Processor，即应用芯片

BP：Baseband Processor，即基带芯片

FCC（美国联邦通信委员会）认证要求将AP和BP分开，因为射频控制相关的功能（信号调制、编码、射频位移等）都是高度的时间相关的，

最好能将这些函数放在一个CPU核上运行，并在这个CPU核上运行一个实时的操作系统，这样AP核上操作系统和驱动的bug就不会导致设备发送灾难性的数据到移动网络中；

并且一旦BP被设计和认证好，不管你采用的操作系统和应用软件怎么变化，它都可以正确的执行通讯功能，手机的设计者也可以更加自由的设计用户界面和应用软件。

AP上面则运行了我们通常的操作系统和应用软件，如Android、Windows phone 7这些。而我们通常所说的双核啊、四核啊这些就是指的其AP核的多少了吧。

因此可以这样理解，AP可以算作是你的电脑，BP则是电脑的modem，没有modem，你没有办法和外界通信。

BP主要的作用是发送和接受各种数据，即和通信息息相关，BP中的DSP实现了协议的算法，对数据进行编解码，BP中的CPU则负责协调控制与基站和AP的通信。

BP中的电源管理模块对手机的待机时间有很大的影响呢，因为大多数时间BP的cpu都应该处于idle状态，每隔一段时间才打开查看paging channel上是否有呼叫进入。

另外，SIM模块也是直接和BP相连接的，对SIM卡的操作也是通过BP进行的。

（IDLE是空闲的意思，在GSM网络中MS有2种状态：空闲和连接。IDLE是MS没有进行通话的状态，此时MS只接收系统消息和属于自己的寻呼组的消息。）

高通以通信芯片起家，又获得了ARM的授权，因此其有能力将AP和BP集成在一个芯片上，AP与BP通过总线通信。而像德州仪器和Nvidia这些不是以通信系统起家的公司，

则AP是AP，BP是BP了。因此高通的芯片用在手机上，那是非常的合适，而如果用在不需要移动网络的平板电脑上，则未必是最合适的吧。

## 4.双模、双待、双通

双模：手机支持两种网络模式。如GSM网络和3G网络中的一种（可以是联通的WCDMA、电信的CDMA2000、移动的TD-SCDMA中的任何一种）。

双待：手机支持两个卡的同时联网待机，而不是双卡中可能会出现的同时只能一个卡处于联网状态的空子，不过如果不想同时待机也可以设置只开SIM卡1或者SIM卡2。

双卡双待双通：两张卡可以同时通话或接受来电（用户根据需要选择切换到哪个卡的通路上）。

单通：即两张卡可以同时待机，但不能同时接通电话。比如其中一张卡在通话时，另一张卡如果来电则会提示“无法接通或忙”。

DSDS:Dual SIM dual standy，即双卡双待；

DSDA:Dual SIM dual active，即双卡双通。

## 5.CS域、PS域

CS：Circuit Switch电路交换；PS：Packet Switch分组交换。

R99规范CN中，传输的本质实际上只有两种形式：电路交换和[分组交换](http://baike.baidu.com/view/65860.htm)。电路交换域（CS域）和[分组交换](http://baike.baidu.com/view/65860.htm)域（PS域）。CS(Circuit Switched Domain)域：指[核心网](http://baike.baidu.com/view/1306584.htm)中为[用户业务](http://baike.baidu.com/view/705147.htm)提供电路交换类型连接的所有网元实体，以及所有支持相关信令的网元实体。电路交换型连接在连接建立时分配专用网络资源，在连接释放时释放专用资源。

CS域是电路承载域，走语音的，PS域是数据域，走得是IP，用于手机上网。

在3G下，接入网同时连接CS和PS，即[核心网](http://baike.baidu.com/view/1306584.htm)分割为CS、PS，打电话信号走CS，数据业务信号走PS。

而在LTE下，取消CS域，CS域业务在PS域实现，如VOIP。

PS域和CS域的区别：

不管是在W、TD还是CDMA中，还是在传统的GSM中，都是存在这两个概念的。CS业务主要是包括一些语音业务，如64K语音等等。但是也包括一些电路型数据业务，最为常见和经典的就是传真；PS业务就是常见的数据业务，也包括流媒体业务、VOIP等等。一些网络，如WLAN、LTE等都是没有CS业务的，他们的语音业务都只能通过VOIP来实现。

（1）CS和PS是针对核心网部分而言的，两者的不同在于交换方式。CS是电路交换，通信之前，资源预留，不同用户独占各自分配的资源，没有统计复用。PS是包交换，不同的用户可以共享同样的资源，统计复用。包交换又分为面向连接和非连接，面向连接预先为数据包指定路由，从而减少路由时间，也在一定程度上保证了数据包的顺利到达；非连接不预先指定路由，各个数据包单独选路。但不管是面向连接和非连接，在对资源的使用上都是采用了存储转发的统计复用方式。所以一般语音走CS域，而手机上网走PS域。但如果是VOIP电话这算是走PS域。

（2）CS域主要负责语音业务，如12.2K语音业务，64K视频电话业务等，PS域用于数据业务，通俗点说也就是上网业务，接入互联网。

（3）CS域叫电路交换域，主要有语音业务（AMR 12.2K），视频电话业务（CS64K）；PS域叫数据交换域，负责数据业务，包括PS384K业务（UE发起384kbps PS域数据业务，是用手机下载一些数据文件等），还有就是高速数据业务包括上传和下载数据业务，也就是HS业务等。

（4）交换方式和业务不一样。CS主要针对实时性要求较高的业务，如语音、视频业务，对延时的要求很高。PS是分组数据业务，体现在数据二字上面，主要提供像PS384HS等上网服务。

（5）CS电弧交换，独占信道主要用于语音，直到通话结束才释放信道，供其他用户使用。PS分组交换（包交换），主要用于数据业务（上网之类），采用分组-转发机制，多用户共用信道资源，使得资源利用率大大提高。

## 6.CSFB：Circuit Switched Fallback，电路域回落。

当LTE终端接受到语音请求时，通过重选回落到2G/3G，完成语音业务后，再重新回到LTE上。

## 7.LTE三种主要语音解决方案

**CS Fallback(CSFB)：**CSFB是LTE终端通过电路域使用语音业务的一种方案，终端平时驻留在LTE网络，使用LTE数据业务，当发起语音呼叫或者接收语音呼叫的时候，终端回落到2G/3G电路域进行语音呼叫，结束后再返回LTE。

**双待机：**具备双待能力的LTE终端可以同时在LTE和2G/3G电路域工作，即同时在LTE网络上使用数据业务，在2G/3G电路域上使用语音业务，实现数据业务和语音业务的并发，无需回落。

SGLTE(simultaneous GSM and LTE)，LTE与GSM同步支持，终端包含了两个芯片。一个是支持LTE的多模芯片，一个是GSM的芯片。可以支持数据语音同时进行。

SVLTE（Simultaneous Voice and LTE），即双待手机方式。手机同时工作在LTE和CS方式，前者提供数据业务，后者提供语音业务。这是纯粹基于手机的方案，对网络无特别要求，不需要部署IMS，缺点是手机成本高、耗电高。目前已经有CDMA 1x和LTE的双待手机，被一些CDMA运营商采用作为IMS部署之前的过渡方案，而GSM/UMTS和LTE的双待手机目前还没有推出。

SVLTE&SGLTE基本是一个概念，是一种单卡双待策略，手机插入一张卡，但可以同时工作在LTE网络和2/3G网络下（如果23G网络是CDMA的，则是SVLTE，如果23G网络是GSM/UTRAN的，则是SGLTE），这样数据业务使用LTE网络，语音业务用23G网络。可以同时工作 。

**VoLTE：**VoLTE是架构在LTE网络上全IP条件下的端到端语音方案。VoLTE的语音作为IP数据传输，无需2G/3G网，全部业务承载于LTE网络上，可实现数据与语音业务在同一网络下的统一。相对于现有的2G/3G网络，通过引入高清编解码等技术，VoLTE可拥有比2G/3G语音，以及时下流行的OTT语音业务更好的用户体验。同时，当终端离开LTE的覆盖区域时，VoLTE能够将LTE上的语音呼叫切换到2G/3G网络上，保证语音呼叫的连续性。

## 8.UICC/CSIM/UIM/RUIM/UTK/SIM/STK/USIM/ISIM/USSD

UICC：通用集成电路卡(Universal Integrated Circuit Card)

CSIM：CDMA2000 1X/EVDO网络中应用的基于UICC架构平台的用户卡称为CDMA用户识别模块CSIM(CDMA Subscriber Identity Module)卡。

UIM：User Identity Module用户识别模块。是应用在cdmaOne手机的一种智能卡，可插入对应的2G手机以使用 移动电话服务。UIM卡的标准化工作由3GPP2（第三代伙伴计划2）负责进行。UMTS的USIM卡上包含了与用户有关的信息，包括IMSI、MSISDN、密钥、服务列表和临时识别符（动态数据）等。

RUIM：CDMA系统定义了Removable User Identity Module(RUIM)，类似GSM系统中SIM卡的观念。可移动用户识别模块RUIM)，也叫做用户识别模块（UIM），和用户识别卡(SIM)是相似的，但是它为网络设计而不是为GSM，例如CDMA。R-UIM卡支持在CDMA和GSM网络之间的漫游。

UTK：UIM card Tool Kit，意思是“UIM卡开发工具包”。要使用手机附加增值业务（如联通电信），都要求将普通的手机UIM卡更换为UTK UIM卡。UTK可以理解为用于开发增值业务的小型编程语言，它允许基于智能卡的用户身份识别模块(UIM卡)运行自己的应用软件。UTK技术为UIM卡的增值业务提供了可开发的环境，即一个简单、易操作的开发平台。

SIM：Subscriber Identity Module，即用户识别卡，是全球通数字移动电话的一张个人资料卡。它采用A 级加密方法制作，存储着用户的数据、鉴权方法及密钥，可供GSM系统对用户身份进行鉴别。同时，用户通过它完成与系统的连接和信息的交换。

STK：SIM Tool Kit，简称“用户识别应用发展工具”，是在[GSM手机](http://baike.baidu.com/subview/3323462/3323462.htm)使用的大容量[SIM卡](http://baike.baidu.com/view/23558.htm)中开发的应用菜单。STK卡是新一代的智能卡，具有很高的存储量（普通的SIM卡的存储量为8K字节，而STK卡容量为32K字节，以后还会继续成倍增加），这就使得它可以存储大量的信息。

USIM：Universal Subscriber Identity Module（全球用户识别卡），也叫做升级 SIM ，是在 UMTS 3G 网络的一个构件。

ISIM：IP Multimedia Service Identity Module即IP多媒体服务身份模块。是一个位于通用集成电路卡（UICC）上的应用，这是一个物理上安全的设备，它可以从UE中插入和取出，在UICC中可以用一个或多个应用。ISIM本身存储了IMS专用的用户数据，主要有IMS运营商所提供。存储的数据可以分为六组：安全密钥，公共用户身份，接入准则参考，私有用户身份，归属网络域名和管理数据。

USSD：Unstructured Supplementary Service Data即非结构化补充数据业务，是一种新型基于GSM网络的交互式数据业务。 当你使用手机键盘输入一些网络已预先制定的数字或者符号比如\*#等，再按send也就是拨号键就可以向网络发送一条指令，网络根据你的指令选择你需要的服务提供给你。

## 9.AT CMD

即Attention，AT指令集是从终端设备(Terminal Equipment，TE)或数据终端设备(Data Terminal Equipment，DTE)向终端适配器(Terminal Adapter，TA)或数据电路终端设备(Data Circuit Terminal Equipment，DCE)发送的。通过TA，TE发送AT指令来控制移动台(Mobile Station，MS)的功能，与GSM 网络业务进行交互。用户可以通过AT指令进行呼叫、短信、电话本、数据业务、传真等方面的控制。

90年代初，AT指令仅被用于Modem操作。没有控制移动电话文本消息的先例，只开发了一种叫SMS BlockMode的协议，通过终端设备(TE)或电脑来完全控制。由Hayes公司发明，已成为事实上的标准并被所有调制解调器制造商采用的一个调制解调器命令语言。每条命令以字母"AT"开头，因而得名。AT后跟字母和数字表明具体的功能。

之后，主要的移动电话生产厂商诺基亚、爱立信、摩托罗拉和HP共同为GSM研制了一整套AT指令，其中就包括对SMS的控制。AT指令在此基础上演化并被加入GSM07．05标准以及的GSM07．07标准，完全标准化和比较健全的标准。如：对SMS的控制共有3种实现途径：最初的BlockMode；基于AT指令的TextMode；基于AT指令的PDUMode。到PDUMode已经取代BlockMode，后者逐渐淡出。GSM模块与计算机之间的通信协议是一些AT指令集，AT指令是以AT作首，字符结束的字符串，AT指令的响应数据包在中。每个指令执行成功与否都有相应的返回。其他的一些非预期的信息(如有人拨号进来、线路无信号等)，模块将有对应的一些信息提示，接收端可做相应的处理。

## 10.小区（Cell，移动通信术语）

移动通信中将无线信号覆盖的区域称之为小区，一般是指一个基站的信号所能覆盖的范围。

早期的移动通信是大区制，也就是在一个区域内建一个基站，且尽可能地提高该基站的信号覆盖范围，这种方法的好处是实现容易，设备简单，但由于受功率和频谱资源限制，系统容量有限，而且扩大容量很困难。因此后来人们提出了小区的方法，即将一个区域划分成很多小的区域，即小区，每个小区用一个基站来进行信号覆盖，相邻的小区使用不同的频率避免干扰，而相隔较远的小区由于基站功率有限，可以使用相同的频率且干扰程度很低，不足以对两个小区用户的通信质量产生致命的影响，这样就实现了频谱复用，大大提高了频谱资源利用率，在相同的频谱和带宽资源下，相比较大区制的方法，由于频谱的复用，系统容量得到很大的提升。这种小区划分区域的方法使得整个区域看起来像由很多蜂巢组成，因此小区又被称之为蜂窝小区。

## 11.HLR、VLR

解释一：

HLR是归属位置寄存器，VLR是拜访位置寄存器。HLR中存放的是在本地开户的信息，VLR中存放的是当前网络中正在使用的用户信息，比如你开户了，HLR中就有你的开户信息，比较全面，但如果你这几天出差漫游到了外地，在本地的VLR中就没有你的信息，而漫游地的MSC就会到我这边的HLR中调用你的信息存放到他的VLR中。

解释二：

HLR是归属位置存储器，用来存储该HLR控制的所有存在的移动用户的相关信息。所有移动用户的重要数据都存储在HLR中，包括用户识别号码、访问能力、用户类别和补充业务等数据，HLR也存储部分漫游移动用户所在MSC区域的有关动态数据。

而VLR是拜访位置存储器，用来服务于其控制区域内移动用户，存储着进入其控制区域内已登记的移动用户的相关信息，为已登记的移动用户提供建立呼叫接续的必要条件。

HLR是个中央数据库，存储用户的所有数据，用户一旦开户，其所有的信息都存在唯一的一个HLR里，而VLR是个动态数据库，存储用户的部分数据，用户漫游后VLR也跟着变化。VLR与用户当前位置相关，只要VLR需要用到其没有的用户数据，就向HLR查询，反过来HLR需要漫游地的信息（如漫游号码等），就向VLR查询。

比喻的说，HLR就像户口本，包括开户和手机等常驻信息；而VLR就是暂住证，只包括漫游号和小区等暂时信息。

## 12.GSM信道

一、业务信道（TCH）：承载话音或用户数据，全速率业务信道（TCH/F）载有总速率为22.8kbit/s的信息。

TCH信道上提供以下信道：1、全速率话音业务信道（TCH/F9.6）；2、9.6kbit/s全速率数据业务信道（TCH/F9.6）；3、4.8kbit/s全速率数据业务信道（TCH/F4.8）；4，小于等于2.4kbit/s全速率数据业务信道（TCH/F2.4）。

二、控制信道：主要携信令或同步数据。

1、广播信道（BCH）用于向MS广播各类信息。可分为

a、FCCH：频率校正信道，用于MS频率校正；

b、SCH：同步信道：用于MS的帧同步和BS的识别；

c、BCCH广播控制信道：用于发送小区信息；

2、公共控制信道（CCCH）：主要携带接入管理功能所需的信令信息，也可用来携带其它信令，CCCH由网络中各MS共同使用，有三种类型：

a、PCH：寻呼信道，用于BTS寻呼MS；

b、RACH：随机接入信道，用于MS随机接入网络上行信道；

c、AGGH准予接入信道，用于给成功接入的接续分配专用控制信道。

3、专用控制信道（DCCH）：是点对点的双向控制信道。根据通信控制过程的需要，将DCCH分配给MS使之BTS进行点对点信令传输，可分为：

a、SDCCH/8：独立专用控制信道；

b、SACCH/C8：与SDCCH/8随路的慢速随路控制信道；

c、SACCH/TF：与TCH/F随路的慢速随路控制信道；

d、FACCH/F：全速率快速随路控制信道；

e、SDCCH/4：与SDCCH/CCCH结合使用的独立专用控制信道；

f、SACCH/C4：与SDCCH/4随路的慢速随路控制信道。

三、信道组合：根据通信的需要，实际使用时总是将不同类型的逻辑作道映射到同一物理信道上，称为信道组合。允许的信道类型有：

a、TCH/F+FACCH/F+SACCH/TF；

b、FCCH+SCH+BCCH+CCCH；

c、FCCH+SCH+BCCH+CCCH+SDCCH/4+SACCH/C4；

d、BCCH+CCCH

## 13.LA&RA

3G中位置区和路由区的概念和GSM及GPRS中的概念完全一致，MSC负责位置区的管理、SGSN负责路由区的管理，二者均要表明的是在当前系统中移动台当前的位置。

位置区和路由区是人为划分的，可能是多个小区的组合，通过一定的标识符加以标识。

位置区LA（Location Area）的标识符是LAI，路由区RA（Routing Area）的标识符是RAI，RA是包含在LA内的。**LAI由MCC、MNC和LAC组成**、而**RAI由MCC、MNC、LAC和RAC组成**，所以RA应小于等于LA。

在网络初期，RA和LA的区域应相等。移动台在作话音呼叫时，跨位置区移动将发生位置区更新；在数据呼叫时，跨路由区移动时将发生路由区的更新过程。系统寻呼时，寻呼过程是在位置区内或路由区内发生寻呼的。

小区（cell）是移动台可以识别的当前在系统中所能驻扎的最小单位，小区可以是扇区（Sector）的概念也可以不是。服务区（Service Area）是移动台所能获得业务提供的最大区域范围。UMTS登记区（URA）的概念只出现在移动性状态管理中，与LA和RA没有关系。在UMTS中移动台进入休眠状态时，会选择一个URA或一个小区内，进入URA-PCH状态进行休眠，取决于移动性管理的当前状态。事实上，系统关心的通信过程还是LA和RA的更新过程。

LAC：Location Area Code。

为了确定移动台的位置，每个GSM PLMN的覆盖区都被划分成许多位置区，位置区码则用于标识不同的位置区。位置区码是为寻呼而设置的一个区域，覆盖一片地理区域，初期一般按行政区域划分(一个县或一个区)，现在很灵活了，按寻呼量划分。当一个LAC下的寻呼量达到一个预警门限，就必须拆分。

格式：位置区码(LAC)包含于LAI中，由两个字节组成，采用16进制编码。可用范围为0001－FFFEH，码组0000H和FFFFH不可以使用(参见GSM规范03.03、04.08和11.11)。一个位置区可以包含一个或多个小区。

传送：LAC在每个小区广播信道上的系统消息中发送。移动台在开机、插入SIM卡或发现当前小区的LAC与其原来储存的内容不同时，通过IMSI附着(IMSI Attach)或位置更新过程向网络通告其当前所在的位置区。网络储存每个移动台的位置区，并作为将来寻呼该移动台的位置信息。

LAC的编码方式每个国家都有相应的规定，中国电信对其拥有的GSM网上LAC的编码方式也有明确的规定(参见邮电部有关GSM的体制规范)。一般在建网初期都已确定了LAC的分配和编码，在运行过程中较少改动。

位置区的大小（即一个位置区码所覆盖的范围大小）在系统中是一个相当关键的因素。如果LAC覆盖范围过小，则移动台发生的位置更新过程将增多，从而增加了系统中的信令流量。反之，若位置区覆盖范围过大，则网络寻呼移动台时，同一寻呼消息会在许多小区中发送，这样会导致PCH信道的负荷过重，同时也增加了Abis接口上的信令流量。

由于移动通信中流动性和突发性都相当强，位置区大小的调整没有统一的标准。运行部门可以根据现在运行的网络，长期统计各个地区的PCH负荷情况和信令链路负荷情况确定是否调整位置区的大小。若前者现象严重可适当将位置区调小，反之可适当调大位置区。一般地，建议在可能的情况下应使位置区尽可能大。位置区码的设置必须严格按照中国电信的有关规定执行，切忌在网络中（全国范围）出现两个或两个以上的位置区采用相同的位置区.

## 14.MOC、MTC

MOC就是Mobile Originated Call,也就是移动拨打固定终端电话的呼叫，即移动主叫；MTC就是Mobile Terminated Call，也就是移动被固定终商拨打的呼叫，即移动被叫。

## 15.空闲模式、专用模式

MS为了能得到或提供各种各样的服务通常需要从网络来获得许多消息。这些在无线接口广播的消息被称做系统消息，可共分为12种类型：type1、2、2bis、2ter、3、4、5、5bis、5ter、6、7、8。系统消息在两种逻辑信道中传送，BCCH或SACCH信道。手机在不同的模式下通过不同的逻辑信道来收听系统消息。

* 在空闲模式下，用BCCH信道（传送系统消息1 至4及7、8）2bis、2ter
* 在专用模式下，用SACCH信道（传送系统消息5和6）5bis、5ter

## 16.TA值

TA就是time advanced，最大时间提前量（TA），是指移动台信号到达基站的实际时间和假设该移动台与基站距离为0时移动台信号到达基站的时间的差值。基站对移动台信号到达的时间始终进行监控，根据到达时间的变化在下行的SACCH发TA命令。

在GSM系统中，在通信过程中，如移动台在呼叫期间向远离基站的方向上移动，则从基站发出的消息将越来越迟的到达移动台。与此同时，移动台的应答信息也会越来越迟的到达基站。而时延过长会导致这样一种情况：基站收到的移动台在本时隙上发送的消息与基站在其下一个时隙收到的另一个呼叫信息重叠起来，而引起干扰，因此引入了时间调整(TA)的措施。我们可以通过TA的值来判断信息的时延情况。

一般在城区由于基站会分布较密，所以TA都是1～2为宜，如超过3就需要引起注意。

但在郊区外较空旷地方，TA可达5，6，除非是一些人迹稀少的地方，一般TA不会超过6，7的。

## 17.UMTS、NAS、CN、RAN、UTRAN、URA、UTRA

UMTS：Universal Mobile Telecommunication System，通用移动通信系统（对应于3GPP标准）

NAS：Non-access stratum[非接入层](http://baike.baidu.com/subview/10118328/10271698.htm)。存在于[UMTS](http://baike.baidu.com/view/76277.htm)的无线通信[协议栈](http://baike.baidu.com/view/174618.htm)中，作为[核心网](http://baike.baidu.com/view/1306584.htm)与用户设备之间的功能层。该层支持在这两者之间的[信令](http://baike.baidu.com/subview/836/836.htm)和数据传输。

CN：Core Network，核心网

RAN：Radio Access Network，无线接入网

UTRAN：UMTS Terrestrial Radio Access Network，UMTS地面无线接入网（4G中为E-UTRAN）。

URA：UTRAN Registration Area，是UTRAN内部区域的划分，适用于UE处于RRC连接状态的情形，而且只能在UTRAN端使用（比如由UTRAN发起的寻呼）。一个URA包含了一个或多个Cell，具体由运营商决定。定义URA是为了更加有效地使用无线资源，这方面有两点原因：

一是从网络侧考虑：

3G以前，UE的移动性管理（MM）仅是由CN端通过登记UE的RAI或者LAI来完成；3G中，通过定义URA，可以使部分移动性管理功能由UTRAN来协作完成，这样通过UTRAN的配合就能更加有效地寻呼到某个UE。

二是从UE侧考虑：

UE的RRC连接有三个状态（CELL，URA，IDLE）。如果UE上有业务，那么此时UE应处于CELL\_DCH状态或者CELL-FACH状态；如果UE上没有业务进行，但UE上将要有业务发生的可能性比较大，那么UE可以长时间处在CELL-PCH或者URA-PCH状态；如果UE上目前没有业务正在进行，而且UE将要发生业务的可能性非常小，那么UE应处在IDLE状态。

之所以要区别CELL和URA两个不同的连接状态，还是为了从节省无线资源的角度考虑的。如果UE处在CELL-PCH状态，但其频繁在小区中切换，那么这样UE要频繁进行小区更新，这样是很消耗UE的资源的；而如果引入了URA-PCH状态，这样小区间的更新将被URA更新取代，UE可以在URA Id发生变化的时候（跨越多个cell）再进行URA更新，而不必频繁地小区更新。

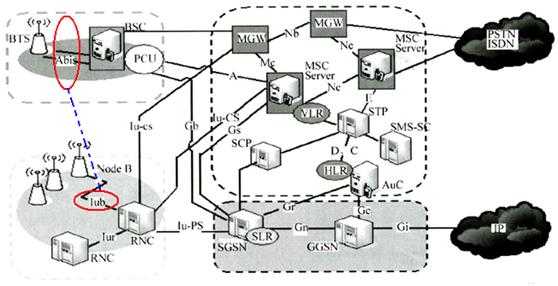
UTRA：Universal Terrestrial Radio Access，原来的“U”是指UMTS，由于UMTS没有在3GPP被接受，所以改为了Universal，指3GPP定义的两种无线接口：UTRA-FDD(WCDMA)和UTRA-TDD(含TD-SCDMA/LCRTDD和HCRTDD)。

UTRA-TDD可以视为CDMA与TDMA相结合的产物。

UTRA-FDD是一个纯粹基于CDMA的系统，通过用户信号的频率和码字来区分彼此。

在UTRA-TDD中上下行链路占用同一频带，但在时间上交替转换传输方向。UTRA-FDD上下行链路占用不同的独立频带。

## 18.Iub接口

Iub接口是RNC和NodeB之间的逻辑接口。Iub接口在UMTS网络中的位置与功能与GSM系统中BTS(Base Tranceiver Station)与BSC(Broadwidth Serve Controller )之间的Abis接口类似。

## 19.RNTI

无线网络临时标识（RNTI Radio Network Temporary Identity）在UE 和UTRAN 之间的信号信息内部作为UE 的标识。

## 20.DSCH、USCH

DSCH - Downlink Shared Channel，下行共享信道

USCH - Uplink Shared Channel，上行共享信道

上行共享信道是TDD模式中的上行传输信道，由几个携带专用控制和业务数据的用户共享。

## 21.WCDMA UE的五种状态

表征了UE连接的级别以及允许使用的传输信道区别：

1、空闲状态，与网络无连接；

2、CELL\_DCH，UE使用专用信道与网络进行通信；

3、CELL\_FACH，占用公共信道FACH/RACH与网络进行通信，传输小流量的数据；

4、CELL\_PCH，UE有RRC连接，但是没有数据传送，只在下行方向监听PICH，UTRAN知道UE在小区级别上的位置；

5、URA\_PCH，有RRC连接，没有数据传送，只监听PICH，与CELL\_PCH不同的是UTRAN只知道UE在URA级别上的位置，通常一个URA会包含多个小区，所以URA\_PCH比CELL\_PCH所需进行小区更新的次数更少。

## 22.PLMN

PLMN （Public Land Mobile Network，公共陆地移动网络），由政府或它所批准的经营者，为公众提供陆地移动通信业务目的而建立和经营的网络。该网路必须与公众交换电话网（PSTN）互连，形成整个地区或国家规模的通信网。

PLMN = MCC + MNC。MCC（mobile country code）移动国家号码，唯一表示移动用户的所属国家，中国的MCC为460。MNC（mobile net code）移动网号，唯一表示该国家中的网络，例如中国移动GSM网为00，中国联通GSM网为01。

46000 中国移动 （GSM）

46001 中国联通 （GSM）

46002 中国移动 （TD-S）

46003 中国电信（CDMA）

46004 空（似乎是专门用来做测试的）

46005 中国电信 （CDMA）

46006 中国联通 （WCDMA）

46007 中国移动 （TD-S）

46008

46009

46010

46011 中国电信 （FDD-LTE）

46020是动车和高铁的调度网

46020是移动的GSM-R铁路专网

46020网络管理器为宽带无线接入网

## 23.直传消息

直传消息是UE和CN之间的，都是NAS的信令，对于RNC来说是透明的，RNC不对内容进行处理，只是进行协议的转换，Uu接口映射为RRC协议的上行直传消息或者下行直传消息，在Iu接口为RANAP协议的直传消息。

## 24.控制面、用户面

用户面就是走的是用户数据，也就是真正的业务内容；

控制面走的是为了承载用户数据而进行的信令交互，主要是承载一些重要的信令消息，控制面的数据其实就是信令的消息内容。

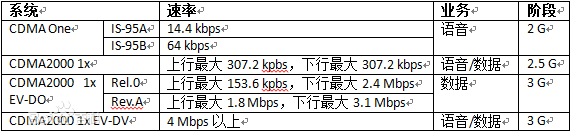
## 25.RANAP

无线接入网络应用协议（RANAP），用于[RNC](http://baike.baidu.com/view/364500.htm)与核心网络的连接，它包括GSM系统BSSMAP。该协议的主要功能有：RAB管理、透明传输NAS消息流程、寻呼、安全模式控制和位置信息报告等。

## 26.1x、EVDO

EVDO 作为 1x 的补充技术，不支持语音。语音仍旧由 1x 承担。

低速数据/语音/短信走的是1x网络。



CDMA2000 1xRTT (RTT－无线电传输技术) 是CDMA2000一个基础层，理论上支持最高达144kbps数据传输速率.尽管获得3G技术的官方资格，但是通常被认为是2.5G或者 2.75G技术，因为它的速率只是其他3G技术几分之一。另外它拥有双倍的语音容量较之之前的CDMA网络。

CDMA2000 1x EV-DO（也称为HRPD）技术，主要对数据业务进行了增强，不支持语音，在1.25MHz的带宽内可提供最高2.4Mbps的下行数据传输速率。DO Rel 0版本已经在韩国、美国和日本等国家商用。目前正在向DO Rel A版本发展，该版本在1.25MHz的带宽内可提供最高3.1Mbps的下行数据传输速率。在DO Rel A的基础上，采用多载波捆绑的方式进一步提高数据速率，形成了DO Rel B标准，也称为空中接口演进（AIE）Phase 1，该标准已经发布。而目前3GPP2正在制定 AIE Phase 2标准，与3GPP的LTE演进类似，同样以OFDM、MIMO等技术为基础。

EVDO（EV-DO)实际上是三个单词的缩写：Evolution（演进）、 Data Only。

其全称为：CDMA2000 1xEV-DO，是CDMA2000 1x演进（3G)的一条路径的一个阶段。这一路径有两个发展阶段，第一阶段叫1xEV-DO，即“Data Only”，它可以使运营商利用一个与IS-95或CDMA2000相同频宽的CDMA载频就可实现高达2.4Mbps的前向数据传输速率，目前已被国际电联ITU接纳为国际3G标准, 并已具备商用化条件。第二阶段叫1xEV-DV。1xEV-DV意为“Data and Voice”，它可以在一个CDMA载频上同时支持话音和数据。2001年10月 3GPP2决定以朗讯、高通等公司为主提出的L3NQS标准为框架，同时吸收摩托罗拉、诺基亚等提出的1xTREME标准的部分特点，来制定1xEV-DV标准。2002年6月，该标准最终确定下来，其可提供6Mbps甚至更高的数据传输速率。

CDMA2000 1xEV-DO技术分析1xEV-DO是一种针对分组数据业务进行优化的、高频谱利用率的CDMA无线通信技术，可在1.25MHz带宽内提供峰值速率达2.4Mbps的高速数据传输服务。这一速率甚至高于WCDMA 5MHz带宽内所能提供的数据速率。为了在不影响现有网络话音通信的前提下支持高速数据业务，1xEV-DO 采用了将语音信道和数据信道分离的方法。这是因为数据和语音具有不同的特性。如延时，数据速率对实时性要求低于语音业务；误码率，数据业务对误比特率的要求高于语音业务；前反向非对称，一般而言，前向数据业务（基站到移动台）的速率需求较反向高出数倍。而语音业务则为严格的对称业务。

1xEV-DO与现有 IS-95 和 CDMA2000 1x网络兼容，从而很好地保护了IS-95 及 CDMA2000 1x运营商的现有投资。其中，1xEV-DO的码片速率、功率需求、信道带宽与 IS-95及 CDMA2000 1X相同；1xEV-DO可沿用现有网络规划及射频部件，基站可与IS-95或 CDMA2000 1x合一，成本低廉。1xEV-DO的功率控制与软切换的方式与 IS-95 及CDMA2000 1x不同，其核心思想是通过动态控制数据速率而非功率，使每个用户以可能得到的最高速率通信。前向链路使用可变时隙的方式时分复用。在 1xEV-DO中，接入点总以最高功率发送，使处于有利位置的用户得到非常高的速率。前向信道上, 1xEV-DO采用虚拟软切换机制，移动台在同一时刻只接收来自同一接入点的数据。根据实时的DRC（动态速率控制）信息，基站可快速地相互切换。同时，基站测量载干比（C/I）并在DRC信道向移动台指示最佳接入点；移动台不断测量导频强度，并不断要求一个与当前信道条件相符合的数据速率。接入点按当时移动台所能支持的最大速率进行编码。当用户需求改变及信道条件改变时，动态地确定优化的数据速率。在反向，1xEV-DO用与 IS-95，CDMA2000 1X相同的软切换技术，移动台发送的信息被多个接入点接收；还有，支持高速分组数据突发。1xEV-DO采用 Turbo 编码技术，反向具有连续的导频。使解调性能得到改善。此外，CDMA2000 1xEV-DO采用增强的无线链路协议（RLP），与TCP协议共同减少误帧率。其强大的空中链路鉴权与加密算法保证了用户的安全。

## 27.EONS、ONS

Operator Name String (EONS)：网络运营商名

Enhanced Operator Name String (EONS)

## 28.DTMF

双音多频信号（Dual-Tone Multi-Frequency, DTMF），电话系统中[电话机](http://wc.yooooo.us/d2lraS8lRTclOTQlQjUlRTglQUYlOUQlRTYlOUMlQkE=)与[交换机](http://wc.yooooo.us/d2lraS8lRTclOTQlQjUlRTQlQkYlQTElRTQlQkElQTQlRTYlOEQlQTI=)之间的一种[用户信令](http://wc.yooooo.us/aHR0cDovL3djLnlvb29vby51cy93L2luZGV4LnBocD90aXRsZT0lRTclOTQlQTglRTYlODglQjclRTQlQkYlQTElRTQlQkIlQTQmYWN0aW9uPWVkaXQmcmVkbGluaz0x)，通常用于发送被叫号码。

在使用双音多频信号之前，电话系统中使用一连串的断续脉冲来传送被叫号码，称为[脉冲拨号](http://wc.yooooo.us/aHR0cDovL3djLnlvb29vby51cy93L2luZGV4LnBocD90aXRsZT0lRTglODQlODklRTUlODYlQjIlRTYlOEIlQTglRTUlOEYlQjcmYWN0aW9uPWVkaXQmcmVkbGluaz0x)。脉冲拨号需要电信局中的操作员手工完成长途接续。

双音多频信号是[贝尔实验室](http://wc.yooooo.us/d2lraS8lRTglQjQlOUQlRTUlQjAlOTQlRTUlQUUlOUUlRTklQUElOEMlRTUlQUUlQTQ=)发明的，其目的是为了自动完成长途呼叫。

双音多频的拨号键盘是4×4的矩阵，每一行代表一个低频，每一列代表一个高频。每按一个键就发送一个高频和低频的正弦信号组合，比如'1'相当于697和1209[赫兹](http://wc.yooooo.us/d2lraS8lRTglQjUlQUIlRTUlODUlQjk=)（Hz）。交换机可以解码这些频率组合并确定所对应的按键。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1209 Hz | 1336 Hz | 1477 Hz | 1633 Hz |
| 697Hz | 1 | 2 | 3 | A |
| 770Hz | 4 | 5 | 6 | B |
| 852Hz | 7 | 8 | 9 | C |
| 941Hz | \* | 0 | # | D |

注意：ABCD四个字母于现代电话已不用。

## 29.PRL

PRL文件是存储在UIM卡上的一个参数文件，全称为：Preferred Roaming List，中文名称为“优选漫游列表”。

PRL系统软件工作原理为：读取特定的二进制文件，此二进制文件包含与本地运营商签订有C网网络漫游协议的其它国家运营商列表及相关网络参数（如SID及频率），并根据此二进制文件生成短信，用一种特殊格式的短信下发至用户手机，手机和UIM卡对特殊短信进行处理，完成PRL信息更新。

当手机开机时，首先会根据PRL列表中的频点列表来进行频点搜索，进而接收系统消息的。

一般的PRL中，会有Primary 频点，也就是基础频点，手机会优先搜素该频点，剩下的就是按照PRL中的顺序，依次搜索，直到搜到合适的频点为止。

## 30.基站扇区和小区

在蜂窝通信网中，基站可设在小区的中心，用全向天线形成圆形的覆盖区，这就是“中心激励”方式。也可将基站设在每个小区六边形的三个顶点上，每个基站采用三副120度扇形辐射的定向天线，分别覆盖三个相邻小区的各三分之一的区域，每个小区由三副120度扇形天线共同覆盖，这就是“顶点激励”方式，而每副天线覆盖的区域就是一个基站扇区。

采用多副定向天线接收的同频干扰功率比采用全向天线明显减小，因此可以减少系统的通道干扰。在不同地点采用多副定向天线可消除小区内障碍物的阴影区。

与小区相比，扇区是一个具有地理意义的概念，而小区是一种逻辑概念，主要是为了方便移动交换中心进行参数配置以及控制用，因此一个扇区可能包含几个小区，通常扇区与基站的天线方向对应，对于有360度天线方向的基站就只有一个扇区，而只具有定向天线的基站就会包含有多个扇区。一般只要无线参数上有不同就会分为一个小区，例如频率不同或者频率相同但扰码不同都分成不同的小区，W网中这两种配置都会出现，此时，按天线的地理覆盖范围，一个扇区就会与一个小区对应，或者包含两个或者两个以上的小区。

## 31.PN、PN offset

PN码（Pseudo-Noise Code），是一具有与白噪声类似的自相关性质的0和1所构成的编码序列，最广为人知的二位元P-N Code是最大长度位移暂存器序列，简称m-序列， 他具有长 2的N次方 - 1个位元， 由一具线性回授的m级暂存器来产生。同时pn码分长码与短码，在CDMA中的担当不同的角色。

常见PN offset就是指PN码偏置指数，在IS-95A CDMA 系统中，PN短码的周期是32768 (就是你看到的2的15次方=32768) chip，将短码每隔64 chip进行划分，于是得到了512 (= 32768 / 64)个不同相位的短码，将这些短码按0至511顺序编号，将该编号称为PN 码偏置指数。

而这512个PN Offset值并不一定能全部被使用，需要根据网络的规模等实际情况确定了步长（Pilot INC）后才能最终确定可以使用的PN Offset值。

在GSM网络，我们知道一个反映时延的参数TA（Timing Advance），通过时间提前量可以判断手机所在的距离区域，1TA＝0.556km（即1km≈2TA）。如果一个呼叫的TA＝4，排除无线传播多径反射产生的时延不计，则可大致判断该呼叫发生在距离基站1.5km-2km之间的区域。通过实际测试，GSM网络的TA与距离的关系符合上述公式。

在CDMA网络，也有通过时延反映距离的参数Access\_pn\_offset。在Motorola CDMA系统中，每一个呼叫建立在Call Detail Log中都会产生一个 Access\_pn\_offset值。Motorola系统对该参数的描述是：手机接入系统时的码片偏移量，可以表示手机与基站之间的距离。

PN offset就是指PN码偏置指数，是CDMA网络基站的测量主要网络识别参数之一。

## 32.CDMA网络的几个重要标识码（ESN/MEID、SID、NID等）

**1、临时本地用户号码（TLDN）**

当呼叫一个移动用户时，为使网络进行路由选择，根据HLR的请求，由VLR分配给被叫用户用于呼叫建立的临时号码。号码中应包含有服务MSCe的位置信息，表示被叫移动用户正在该服务MSC中。该号码在接续完成后即可以释放给其它用户使用。

**2、电子序列号码（ESN）和移动台设备标识（MEID）**

电子序列号（ESN）是唯一识别一个移动台设备的设备序列号，包含32比特，由制造商标识和设备标识两部分组成。其中前14比特为制造商代码，由3GPP2统一分配，后18比特为序列号，由厂商自行分配。

机卡分离终端采用UIM卡。在使用UIM卡的移动台中，UIM\_ID将代替ESN号码参与鉴权。同时终端上还需要另外分配一个ESN。UIM\_ID的长度也为32比特，和ESN共享号码资源，都是由TIA组织在ESN的32位资源池中统一分配。

由于ESN的数量有限，为解决ESN号码资源耗尽的问题，3GPP2定义了新的移动台设备标识MEID来代替ESN的功能。同样，由EUIM\_ID来代替UIM\_ID。

MEID包含56比特，其号码结构为：

C网的几个重要标识码

其中，对于3GPP2专用设备：

(1)RR：A0～FF，全球统一分配；

(2)XXXXXX：生产厂商代码，000000～FFFFFF；

(3)ZZZZZZ：序列号，000000～FFFFFF；

(4)C：校验码(CD)，0~F。

对于兼容3GPP和3GPP2的设备：

(1)RR：99、98、97，全球统一分配；

(2)XXXXXX：生产厂商代码，000000～999999；

(3)ZZZZZZ：序列号，000000～999999；

(4)C：校验码(CD)，0~9。

由于ESN参与构造反向信道，需要将终端的MEID通过SHA-1算法转换为32比特的ESN，反向存在ESN冲突。因此要求原133网号的RAN设备升级支持基站指配的PLCM，新建18x网号的RAN设备支持基站指配的PLCM，从而避免ESN的冲突。

对于机卡合一的终端，为满足国际漫游的需求，要求支持MEID的同时必须支持pESN（伪ESN）；对于机卡分离的终端，EUIM\_ID采用基于ICCID的长格式方案，同时必须支持P-UIMID（伪UIM\_ID）。支持MEID/EUIM\_ID+pESN/P-UIMID的终端接入网络时，优先采用MEID/EUIM\_ID进行鉴权，如网络不支持MEID/EUIM\_ID，则采用pESN/P-UIMID进行鉴权。

何为PLCM?

公共长码掩码PLCM长为42比特，用于前向信道的绕码。基站分配前向业务信道的时候必须通知移动台业务信道的PLCM，在Rev.B及其更低的版本中，基站根据ESN得到PLCM，然后发送给移动台，当不知道ESN的时候基站无法分配前向业务信道。除此之外ESN号面临短缺，以后的应用中可能存在问题。

在Rev.C中允许基站在ECAM消息中发送给移动台和ESN无关联的PLCM。移动台切换时，为了减小网络的复杂性，基站可以通过业务连接消息和通用切换指示消息通知移动台转到基于ESN的PLCM上，而不必发送基站定义的PLCM给切换的目标基站。

**ESN （Electronic Serial Numbers）：电子序列号。**在CDMA 系统中，是鉴别一个物理硬件设备唯一的标识。也就是说每个手机都用这个唯一的ID来鉴别自己, 就跟人的身份证一样。一个ESN有32 bits, 也就是 32/8 = 4 bytes。随着CDMA移动设别的增多，ESN已经不够用了，所以推出了位数更多的MEID。ESN用8位的16进制来表示，如0x801EA066。

**MEID（Mobile Equipment ID）：手机设备识别码。**前面说过了，由于CDMA移动设备增多，导致原来8位的ESN不够用，所以推出了56bits的MEID码，MEID可以表示为14位的16进制码，如0xA1000002B0BEB2。开头的0xA表示CDMA手机，如果是0x9, 就表示多模手机。

**pESN（pseudo ESN）:伪ESN。**pESN的推出是为了解决前向兼容的问题，pESN的格式与ESN是完全一样的，唯一的区别是pESN是采用0x80开头的。MEID转为pESN，就可以在支持ESN的C网内正常使用。MEID转化为pESN具体的方法是，56 bits的MEID通过SHA-1 hash算法，挑出后6位，然后在开头加上0x80。

**3、系统识别码（SID）和网络识别码（NID）**

在cdma2000网中，由一对识别码（SID，NID）共同标识一个移动业务本地网，判决移动台是否发生了漫游。在放用户的时候，用户归属本地网的SID号码应当写入移动台中。网络识别码（NID）由16比特组成，0与65535保留。0表示在某个SID区

中不属于特定NID区的那些基站；65535表示移动用户可在整个SID区中进行漫游。NID的分配由各本地网管理。

**4、位置区识别码（LAI）和登记区域识别码（REG\_ZONE）**

位置区识别码（LAI）唯一标识一个位置区。位置区范围一组相邻小区组成，用于寻呼时通知无线侧寻呼的范围。

REG\_ZONE是用于识别特定的无线覆盖区的号码，用于接入侧判断移动台是否发生位置更新，如果发生更新，需要向网络重新登记。它包含12比特，由各省统一分配。

REG\_ZONE与LAI的规划范围可以一致，也可以不一致。现有网络的REG\_ZONE与LAI一致，为方便管理，要求新分配的REG\_ZONE和LAI也一致。新分配的REG\_ZONE和LAI根据网络规划来设定。

**5、区全球识别码（CGI）和基站识别码（BSID）**

小区全球识别码（CGI）唯一标识一个小区，由LAI＋CI构成，即MCC+MNC+LAC+CI。

其中：

(1)MCC、MNC、LAC的取值同LAI；

(2)CI：2字节BCD编码，MSCe/VLR内有效。

BSID同CI，用于识别扇区，而不是识别基站。当一个基站包含多个扇区的时候，每个扇区使用的BSID都应当不同。

基站识别码为一个16比特的数，由各省统一分配。在A接口中，为了便于管理，规定前12个比特表示基站，后面4个比特表示扇区，和CI相同编号。

## 33.CDMA中的general page message

在实际工作中，寻呼信道会持续发送消息。即使没有数据需要发送，也会发送无业务消息。手机需要持续监控寻呼信道，以确定系统正常。如果一定时间内收不到寻呼信道，手机会进入初始化状态。因此，寻呼信道必须持续发送 general page msg。

基站在所支持的每个CDMA信道上最多发射7个寻呼信道。对于支持的每个CDMA信道，基站发射一个同步信道，至少发射一个寻呼信道。

对于基站发射的每个寻呼信道基站将连续发射有效寻呼信道消息，可以包括无业务消息。

寻呼信道的消息结构包括8bit报文长度的报头，最少2bit最多1146bit的报文正文和一个30bit的CRC代码，所以报文 长度包括报头、正文和CRC，但不包括填充位。寻呼信道发送的消息主要包括：

（1）系统参数信息（system parameter message），提供开销信息，如导频PN序列偏移指数，系统标识符（SID），网络标识符（NID），基站标识符，基站经纬度，基站寻呼信道数page-chan和其他消息；

（2）接入参数信息（access parameter message），定义移动台在接入信道进行发送所需要的消息；

（3）邻区列表消息（neighbor list message ），提供邻近基站参数消息，例如临近基站导频PN序列偏移指数，临近基站寻呼信道的配置与本基站是否相同；

（4）CDMA信道列表（CDMA channel list message），提供CDMA载波列表；

（5）寻呼消息（page message），向移动台提供寻呼，移动台监控寻呼信道消息的每一个时隙；

（6）标准的指令信息（order message），寻呼信道可发送几个指令信息，例如缩位警告，基站查询证实，重播，审查，截获，基站确认，功率的周期性锁定等；

（7）信道分配信息（channel assignment message），该消息通知移动台调谐到一个新的频率上，包括业务信道和寻呼信道。

## 34.CMCC、CU、CT

移动：China Mobile Communication Company

联通：China Unicom

电信：China Telecom

## 35.AT、AN

AT：Access Terminate，用户使用的移动终端。

AN：Access Network，接入网。负责与AT 的无线连接，包括无线资源管理，功率控制等功能。

EVDO中的AT是移动终端，AN相当于BSC（基站控制器）和BTS。

## 36.UATI

UATI就类似于我们的IP地址。每次终端和网络建立通信后，网络都会给终端分配一个唯一的识别码。由于DO的Session需要保存很多信息，因此用一个UATI来标识每个AT的Session，便于AT和网络通信。其作用就是个标识。同DHCP分配的IP地址一样，有生存周期。在生存周期内，即使你断开网线也不会变。——一句话，按照DHCP分配IP地址的原理去理解即可。

中兴文档关于UATI的说明：

属于AT发起的session的呼叫部分,该流程分配UATI(Unicast Access Terminal Identifier)，AN可同时与多个AT之间存在空口会话，为了区分空口会话的AT，AN将为AT分配惟一的终端地址标识

AT在接入信道上发送UATIRequest和RouteUpdate消息，每次AT在接入信道上发送，总会包含RouteUpdate消息 。 AT可能使用ESN，或者随机生成的RATI生成UATI作为自己的标识

AN通过控制信道发送ACAck，以确认接收到接入信道的MAC层包

如果系统配置为AT使用随机RATI，则需要HardwareID请求/响应流程以获得AT的HardwareID；否则，AT使用固定生成的RATI，这种情况RATI和HardwareID是相同的，不需要HardwareID请求/响应流程；AT的HardwareID是一个未登记AT的唯一标识

AN通过控制信道上发送UATIAssignment消息，指示AT进行UATI指配

AT在接入信道上发送UATIComplete消息 ，通知AN指配UATI完成

DO空口协议关于UATI的说明：

A session is a shared state maintained between the access terminal and the access

7 network, including information such as:

8 • A unicast address (UATI) assigned to the access terminal,

9 • the set of protocols used by the access terminal and the access network to

10 communicate over the air-link,

11 • configuration settings for these protocols (e.g., authentication keys, parameters for

12 Connection Layer and MAC Layer protocols, etc.), and

系统收到UATIRequest 消息后，根据一定算法计算出分配给该终端的UATI，并发送UATIAssignment 消息。UATIAssignment 消息中包含UATI104、UATI024 和UATISubnetMask等字段，分别对应于所分配UATI 的高104 位、低24 位以及当前扇区的子网掩码等。

终端收到UATIAssignment 消息后，根据该消息携带的RATI 或UATI 判断其归宿，若属于自身， 则计算UATI= （UATI104|UATI024 ） 及其对应的UATISubnetMask ； 若UATIAssignment 不包含UATI104 和UATISubnetMask 字段，则终端设置UATI=（SectorID[127:24]|UATI024），UATISubnetMask 设为扇区参数消息中的SubnetMask。终端向系统发送UATIComplete 消息作为对UATIAssignment 的应答。

UATI构成：

UATI 是长度为128 位的终端地址标识或会话标识，它的高位默认为子网地址标识，低位作为终端在该子网内的地址标识。UATISubnetMask 表示终端所在的子网掩码，一般情况下，它的高位设为全“1”，低位设为全“0”。如前所述，若UATIAssignment 消息中不包含UATI104和UATISubnetMask，则终端根据扇区参数消息中的SectorID 和SubnetMask 来构造UATI 和UATISubnetMask。UATI 与SectorID 的结构类似，UATI 在会话建立和子网变更时进行更新，而SectorID 在发生切换时进行更新。

考虑到在空中接口传送128 位的UATI 需要占用较多的无线资源，在1x EV-DO 空中接口协议中引入了子网地址映射的概念。将UATI 的高104 位（一般为子网地址）映射成长度为8位的子网色码（ColorCode），构造出在空中传送的长度为32位的UATI短版本结构，亦即UATI=（ColorCode|UATI024）；当子网发生变化时，其ColorCode 也随之改变。AT 与AN 必须存储ColorCode 与子网地址的映射表，AT 在内存中同时保留完整的UATI 长版本结构，亦即UATI=（UATI104| UATI024）。

UATI分配：

在会话建立期间，AN 为参与会话的终端分配惟一性的会话标识或地址标识，系统与终端通过会话标识来判别消息或数据的归宿。在建立新会话时，AT 向AN 发送UATIRequest 消息，请求AN 为其分配UATI。MAC 层将封装UATIRequest 消息的数据分组包头中的终端地址标识类型设为RATI 或UATI。系统收到UATIRequest 消息后，根据一定的算法计算出分配给该AT 的UATI，并发送UATIAssignment消息。此后，通过UATI，AN 与指定AT 进行空中接口不同协议层的各子协议及其属性的协商和配置。

UATI 随着会话的建立而分配，并随会话的结束而释放。会话关闭后，若要新建会话，则需要重新进行UATI 分配和会话协商。

## 37.GSN

为了支持更快速的分组交换数据业务，相对于GSM网络，GPRS网络新增加了GPRS支持节点GSN（GPRS Support Node，GPRS支持节点）。并且根据GSN节点的位置和功能的不同，GSN节点分成了SGSN（Serving GPRS Support Node，服务GPRS支持节点）和GGSN（Gateway GPRS Support Node，网关GPRS支持节点）两类。它们是位于GPRS核心网侧的两个最主要节点。

SGSN主要负责处理MS到GPRS网络之间的通信，负责转发MS的数据到GPRS核心网，并需要根据MS在网络中的具体位置进行移动性管理和会话管理。

GGSN则主要负责在SGSN和外部分组数据网络（Packet Data Network，PDN）之间为MS转发上下行用户数据报文。

在一个PLMN网络中，可能有多个GSN节点。BSC和SGSN之间的接口称为Gb接口，一个PLMN网络内GSN节点之间的接口称为Gn接口。

## 38.PDN

Packet Data Network，包交换数据网络。顾名思义，PDN是指基于分组报文传送的网络，比较常见的是基于IP技术构建的分组数据网络，例如Internet。PDN网络提供了MS期望访问的各种数据应用，通过GGSN和GPRS网络相连，需要执行两个网络协议（例如上行方向：GTP到IP）的转换。电信运营商可以通过将相同类型的业务合并，设置不同的PDN网络为用户提供服务。常见的PDN网络主要有Internet、专门提供WAP类业务的数据网络、企业用户内部网络等。GGSN和外部PDN网络的接口称为Gi接口。

## 39.NSAPI

网络服务接入点标识符（Network Service Access Point Identifier）是 [PDP](http://baike.baidu.com/view/89547.htm)（分组数据协议）上下文的一个索引，其使用由更低层（[SNDCP](http://baike.baidu.com/view/1016510.htm)（子网络相关集中协议））提供的服务。一个 PDP 可能有几种 PDP 上下文属性和网络服务接入点标识符。

在MS中，利用NSAPI来标识分组数据协议的接入点（PDP-SAP）；在SGSN和GGSN中，利用NSAPI来标识与一个PDP地址相对应的PDP上下文，MS在请求一个PDP上下文时，MS会选择一个未使用过的NSAPI。在会话管理信令流程的交互过程中，NSAPI的主要作用就是用于网络层的路由。

该参数在PDP上下文激活流程、PDP上下文修改流程、PDP上下文去激活流程中传递。

## 40.2G-3G-4G

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2G | 2.5G | 2.75G | 3G | 3.5G | 3.75G | 4G |
| GSM | GPRS | EDGE | WCDMA | HSDPA/HSUPA | HSDPA+/HSUPA+ | FDD-LTE |
| 9K | 42K | 172K | 364K | 14.4M | 42M | 300M |

## 41.对称业务、非对称业务

对称业务和非对称业务是指业务而言，与所采用的技术无关。

对称业务是指业务的上下行业务速率（业务量）一致，典型的对称业务是语音业务。

非对称业务是指业务的上下行业务速率不一致，典型的非对称业务是数据业务，上行业务速率可以低，下行业务速率高。

应该说TD技术适应对称业务与非对称业务，其实3G的其他制式对数据的上下行业务速率也是不一样的，主要因为受终端的技术条件限制。

TD中的数据业务可以进行非对称，比如下载时候1个时隙最大128Kpbs，一个载波中，非对称时，可以配置1个上行时隙，5个下行时隙，采用1：5的配置，即一个上传，5个下载，这样下载速率可达：128X5=640Kpbs；同样语音信道采用3：3的对称配置可满足一块载波承载话音用户最大，通俗点就是：每个用户一个下行时隙一个上行时隙，这样6个时隙就可以满足3个用户使用。

## 42.RSSI 、RSCP、RSRP、RSRQ 、dBm

RSSI：（Received Signal Strength Indicator）指特定频带内的功率包括了干扰，是接收信号的强度指示，它的实现是在反向通道基带接收滤波器之后进行的。

RSCP的全称是Receive Signal Channel Power，通常特指导频信道，可以理解为手机接收到的导频信道信号强度。

RSRP(Reference Signal Received Power)主要用来衡量下行参考信号的功率，和WCDMA中CPICH的RSCP作用类似，可以用来衡量下行的覆盖。区别在于协议规定RSRP指的是每RE的能量，这点和RSCP指的是全带宽能量有些差别；

RSRQ (Reference Signal Received Quality)主要衡量下行特定小区参考信号的接收质量。和WCDMA中CPICH Ec/Io作用类似。二者的定义也类似，RSRQ = RSRP \* RB Number/RSSI，差别仅在于协议规定RSRQ相对于每RB进行测量的。

dBm = 10 \* lg(mW）（功率增加一倍，增加3dB）

dBm 就是相对于1mw的功率的比值。如果发射功率是100mw，那么发射功率是20dbm， 也就是1mw的100倍。那么微波发射后通过空气传播衰减强烈，距离发射段3米处也许接收到的功率只有0.001mw了，也就是1mw的千分之一。这时候的RSSI就是-30dbm。所以接受到的功率比1mw大，RSSI为正；比1mw小则为负。一般都是负值，发射功率小，空气衰减大。

语音无线环境，RSSI必须大于-67dbm。数据无线环境可以忍受到-75dbm。RSSI小于-80dbm的时候都可以考虑频谱复用了，所以不要指望用户有啥好体验。-90dbm是给无线扫描器扫来看的。RSSI太大会有干扰，干扰的前提是同频。

## 43.彩信

彩信是不能直接用AT命令发的。

彩信的发送有两种方式WAP和HTTP。一般都用HTTP了，整个WAP协议栈也不容易啊。

粗略说下使用HTTP的方法：

1.将彩信按照彩信的规范编码

2.拨号GPRS。

3.跟彩信中心建立连接（移动的是：server：mmsc.monternet.com, gateway: 10.0.0.172, port：80）

4.将编码过的彩信放入http的body中，发送出去。

收彩信流程：

短信中心会给你发一个短消息，如果你的手机设置是自动接收，就自动接收彩信，如果是设置手动的，你按“接收”。你的手机这时如果开机后就已经ATTACH在GPRS网上了，这时手机PDP激活，拿到IP地址，再到彩信中心（彩信都是发到彩信中心的）去GET你的彩信。如果你的手机没有ATTACH，就先ATTACH，再PDP等。接收彩信完了，手机会回一条消息给彩信中心。

彩信业务的消息流程，分成3个步骤：

第一是发送彩信到彩信中心去，要通过SGSN-GGSN-WAPGW到彩信中心；

第二是才通知短消息给用户，要通过WAPGW-SMC到用户；

第三是取彩信，从手机到SGSN-GGSN-WAPGW到彩信中心，然后返回取的结果。

WCDMA网络中发送短信的过程中能否接通电话、收到短信、收到彩信？

1、WCDMA网络做这个是没问题的，理论上是支持并发业务的；

2、但是有一些手机终端是不支持的，因此，有些用户不能享有这个并发业务的服务了。

彩信是属于ps域的。

PS域是用来传数据业务的，CS用来传语音业务,短信按理说应该是可以通过CS和PS两种方式传的，但是运营商基本上都是通过CS域来传的，例如移动就是将短信通过SDH帧结构中的公务联络字节E1和E2传递的，这两个字节提供的是公务联络语音通路，本身是用于公务联络的，通过这种方式，就能更有效的利用带宽，相当于额外的增加利润。

在GSM中PS数据通过SNDCP，LLC，RLC，MAC传到PHY，CS数据通过LAPDm传到PHY；在3G中无论CS还是PS数据都是通过RLC，MAC传到PHY，此外，PS数据还需要经过PDCP。

目前在中国CS一般是12.2KAMR呼叫和64K语音电话，而PS业务一般是上网，彩信，数据下载业务。

## 44.WCDMA并发

1、WCDMA支持多业务同时进行，可以实现话音与上网同时使用，在WCDMA通信术语中通常叫做Multi-RAB，中文一般叫并发业务。语音和数据同时传时，称为multi call or multi RAB support。这时候，要区分数据是通过什么信道传的 (DCH or HS-DSCH)。

2、在WCDMA中，一个用户语音信道和其他数据信道是分别用不同正交码进行区分，然后再将一个用户的所有的信道进行线性叠加后再加上PN识别然后传输的。

语音和数据同时传时，称为multi call or multi RAB support. 这时候，要区分数据是通过什么信道传的 (DCH or HS-DSCH)。一般来说，ps 数据是不支持软切换的，而语音是支持的。所以基本可以认为切换是基于单个业务的。

主要是用于支持语音和数据并发业务的。

## 45.WEDGE、HEDGE

WEDGE：只支持WCDMA和GSM/GPRS/EDGE；

HEDGE：可以支持HSDPA/WCDMA和GSM/GPRS/EDGE；

## 46.MMI、SS、USSD

MMI是Man-Machine-Interface的缩写。

从功能上来看，有一些从拨号盘拨出去的字符串，它的实际作用不是建立一个通话而是为了完成某种服务，这个就是MMI；从格式上来看，每一个从拨号盘输入的字符串，如果包含有\*或者#，都可以称之为MMI.

 MMI包括Manufacturer defined MMI codes，SIM control codes，SS，USSD等等。

**Manufacturer defined MMI codes**

一些嵌在手机里的服务码，比如你要查询一个手机的IMEI号码，你可以在拨号键盘输入\*#06#，手机的IMEI码会自动弹出来。

**SIM control codes**

比如用来修改SIM卡PIN码的命令，在拨号键盘输入\*\*04\*1234\*6789\*6789#，这将会将SIM卡的PIN码从1234修改成为6789。

**SS**

Supplementary Service，补充服务，比如控制号码显示，呼叫转移等服务的号码串。这些号码串是每部GSM/UMTS/LTE手机中的固定服务号码，运营商是不能对它进行修改的。当手机系统接受到这些服务号码后，先在手机内部进行处理后，再传给网络。比如你随便拿个手机，在拨号盘输入\*21\*123456789#然后点击发送，这个时候你所有的来电都会直接转移到123456789。

**USSD**

与SS相对应的是Unstructured Supplementary Service Data，非结构化补充数据业务。

与SS的区别：一，USSD基本都是运营商根据自己的服务自己定制的，而SS就像上面说的是每个手机固有的；二，SS在发送给网络前，手机首先会自己处理一下，而USSD是完全透明的传送给网络。

**SS和USSD都必须点击发送**后才能生效，而**Manufacturer defined MMI codes和SIM control codes都不需要点击**，输入后直接生效。

MMI格式

Activation：\*SC\*SI#

Deactivation：#SC\*SI#

Interrogation：\*#SC\*SI#

Registration：\*SC\*SI# and \*\*SC\*SI#

Erasure：##SC\*SI#

Action：\*，#，\*#，\*\*，##。

SC：Service Code，由2-3位数字组成

SI：Supplementary Information。

MMI串通常以\*，#，\*#，\*\*，##等开头，以#结束。各个部分间以\*隔开。

## 47.HSDPA、HSUPA、HSPA、HSPA+

WCDMA的发展基本可以分为以下几个不同的版本。

首先是R99/R4版本，这个版本算是WCDMA的早期版本，现在我们通常也把这个版本叫做WCDMA，这个版本可以提供384Kbps的最高上传速度和2Mbps的最高下载速度。

后来WCDMA发展到了R5版本，这时提出了一个技术，就是HSDPA（高速下行分组数据接入技术），这个版本大幅度强化了R99/R4版本的最高下载速度，达到7.2Mbps或者14.4Mbps，我们现在就把这个版本的WCDMA叫做HSDPA。

在接下来技术进一步进化，到了R6版本时，提出了HSUPA（高速上行分组数据接入技术），这个技术在保持R5版本的下行速度不变的情况下大幅度强化了HSDPA的最高上行速度，提升到5.76Mbps，我们现在就把R6版本的WCDMA叫做HSUPA，R5和R6版本统称HSPA。

技术总是进化的，到了R7版本时，HSPA+出现了，这个版本保持R6版本最高上行速度的情况下，强化了R6的最高下行速度，提升到21Mbps/28Mbps/42Mbps，甚至56Mbps/84Mbps！

当然，后续还有R8的HSOPA和FDD-LTE等后续演进技术（这就说明了为什么WCDMA最成熟）。

通俗的理解，HSDPA和HSUPA还有HSPA+都可以算是WCDMA的“儿子”，但是我们通常只把R99/R4的WCDMA版本叫WCDMA，其他版本就直接叫那个版本新加入的技术名字。

## 48.FDD、TDD

多址技术主要是解决多用户共享系统无线资源的问题。频率、时间、正交码是三种易于使用的资源，对应的有三种基本的多址方式，即频分多址（FDMA）、时分多址（TDMA）和码分多址（CDMA）。

双工方式主要是解决系统中用户双向通信的问题。频率、时间是两种较好的方式， 对应的有两种双工方式，即频分双工（FDD）和时分双工（TDD）。

只要是双向通信，就需要一定的双工工作模式。当前2G和3G通信领域使用双工模式主要是频分双工和时分双工，即FDD（Frequency Division Duplex)与TDD（Time Division Duplex），它们是各种无线系统中常用的双工方式。

在现有的3G有三大主流技术标准：WCDMA、CDMA2000和TD-SCDMA，虽然它们都属于CDMA技术，但是从它们的主要应用方面可分为两类：WCDMA、CDMA2000属于FDD标准；而TD-SCDMA属于TDD标准。另外，3.5G的HSDPA系统中兼有FDD和TDD，而4G的前驱Mobile WiMAX兼有TDD、FDD、半双工FDD。

GSM(FDD+TDMA)

FDD（frequency division duplex，频分双工，也叫全双工），传输信号的时候需要两个独立的信道，一个信道传输下行信息，一个信道传输上行信息，两个信道之间有一个保护频段，上下行频率间隔190MHz，两个信道频率对称，以防止临近的接收机和发射机之间产生干扰。

不管900还是1800频段，都被划分成很多频点，这就是FDD；其次，每个频点，又被划分为8个时隙，这就是TDMA。

LTE是基于OFDMA技术、由3GPP组织制定的全球通用标准，包括FDD和TDD两种模式用于成对频谱和非成对频谱。

LTE-TDD，国内亦称TD-LTE，即 Time Division Long Term Evolution（分时长期演进），由3GPP组织涵盖的全球各大企业及运营商共同制定，LTE标准中的FDD和TDD两个模式实质上是相同的，两个模式间只存在较小的差异，相似度达90%。

TD-SCDMA是CDMA（码分多址）技术，TD-LTE是OFDM（正交频分复用）技术。两者从编解码、帧格式、空口、信令，到网络架构，都不一样。

## 49.APN

中国联通的2G业务[WAP浏览器](http://baike.baidu.com/view/267441.htm)中 使用的APN为“UNIWAP”，3G业务WAP浏览器使用的APN为“3GWAP”；中国联通的2G上公网使用的APN为“UNINET”，3G业务上 网卡及上公网使用的APN为“3GNET“。

中国移动上内网的APN为“CMWAP“，上网卡及上公网使用的APN为“CMNET“。

中国电信2G、3G网络中，WAP方式APN是CTWAP，互联网访问使用CTNET。

3GPP 23060附表有APN选择的详细流程。简言之，当UE业务请求时没上报APN，SGSN会根据附表的流程，最终选择一个APN共本次业务激活。通常UE没上报APN情况，SGSN会采用default APN最为用户的本次业务激活APN。

**LTE:**

1.网络首先会下发ESM information request消息，要终端的APN，终端在response消息中反馈所有的APN。

2.激活默认承载时，网络会下发激活Activate default EPS bearer context reqeust消息，说明要激活的是哪个APN的承载。

也就是首先问终端支持哪些，然后告诉终端要用哪个。

ATTACH过程是不需要APN的。只有激活承载时才需要

LTE建立承载是否需要PDN?

1.我们知道在3G中，激活PDP肯定是需要APN的，因为PDP激活请求是由终端发起的，所以必须要携带。

2.在LTE中，默认承载是由网络激活的。所以选择就有多样性，一种是终端必须提供，一种是网络提供，具体需要谁提供就需要看运营商的策略了。以中国移动来说，即使删除了所有的APN，你发现默认承载也是可激活的。

## 50.CDMA中的SID和NID

1、在CDMA网中，移动台根据一对识别码（SID，NID）判决是否发生了漫游。系统识别码（SID）包含15比特。每个移动本地网分配一个SID号码；

网络识别码（NID）由16比特组成，NID的0与65535保留。0用作表示在某个SID区中不属于特定NID区的那些基站。65535用作表示移动用户可在整个SID区中进行漫游。NID的分配由各本地网管理，具体的分配方案待定。

2、在网络中，SID一般标识一个本地网，就是一个地市；NID可以在地市内部进行划分，主要根据核心网的规模划分，一套MSC一般就是一个NID，不同的MSC使用不同的NID；

3、SID必须大于NID（可以等于，对应1个NID的情况）；

4、具体的划分还是取决于运营商的规定，协议上没有具体约束。

## 51.LTE：EPC，EPS

epc = mme + s-gw + p-gw（核心网那一块）

e-utran = enodeb

eps = ue + e-utran + epc

LTE是英文Long Term Evolution的缩写。LTE也被通俗的称为3.9G，具有100Mbps的数据下载能力，被视作从3G向4G演进的主流技术。

2006年9月，3GPP最终确定了LTE（长期演进）：也称之为演进的UTRA和UTRAN（Evolved UTRA and UTRAN）的研究项目。该项研究的目标是确定3GPP接入技术的长期演进计划，使其可以在遥远的将来保持竞争优势，相应的工作项目计划在2007年下半年完成。

3GPP还开展了一项平行研究：即系统架构演进（SAE System Architecture Evolution)(System Architecture Evolution ），来展示核心网络的演进要点。这是一个基于IP的扁平网络体系结构，旨于简化网络操作，确保平稳、有效地部署网络。

分组核心演进(EPC)方案是一套全IP产品系列，旨在帮助运营商通过采用无线长期演进（LTE）技术来提供先进的移动宽带服务。分组核心演进解决方案由四个基础组件构成，包括负责动态移动性和策略的移动性管理模块（MME）和动态业务控制器（DSC）以及业务网关（SGW）和分组数据网络（PDN）网关。

LTE中核心网演进方向为EPC（Evolved Packet Core），包含MME （Mobility Management Entity）和S-GW（Serving Gateway）；无线接入网UTRAN（Universal Terrestrial Radio Access Network）演进方向为EUTRAN（Evolved UTRAN）。

EPC和EUTRAN合称EPS（Evolved Packet System）

## 52.TA及相关的基本概念

TA：Tracking Area，跟踪区。TA是LTE系统为UE的位置管理新设立的概念。

相关概念：

|  |  |  |
| --- | --- | --- |
| LA | Location Area | 位置区 |
| RA | Routing Area | 路由区 |
| LAI | LA Identity | 位置区标识 |
| RAI | RA Identity | 路由区标识 |
| TAI | TA Identity | 跟踪区标识 |
| LAC | LA Code | 位置区编码 |
| RAC | RA Code | 路由区编码 |
| TAC | TA Code | 跟踪区编码 |

LA（位置区：LAI = PLMN + LAC）是2G和3G时代电路域的概念，它使移动交换机（MSC/SEVER）能及时知道终端的位置，当寻呼终端时，移动交换中心就在该终端的位置区中的所有小区进行搜索。在一个位置区内终端不需位置更新；在跨LA移动时，需要发起LA更新过程，以便网络知道终端的位置区；同时终端为了和网络侧保持紧密联系，需要周期性LA更新过程。

RA（路由区：RAI = PLMN+ LAC + RAC）是2G时代和3G时代分组域的概念，它使SGSN能及时知道终端的位置，终端要发起数据传输前，须向SGSN 和 HLR注册，并寻呼路由区内终端。终端可以在一个RA内不需要做RA 更新；在跨路由区移动时将发生RA 更新；同时需要进行周期性RA更新。

**TA的作用**

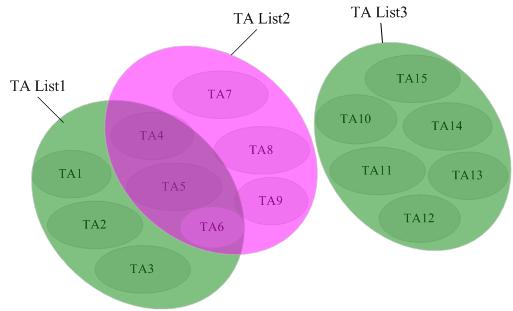
跟踪区（Tracking Area）是LTE系统为UE的位置管理新设立的概念。当UE处于空闲状态时，核心网络能够知道UE所在的跟踪区，同时当处于空闲状态的UE需要被寻呼时，必须在UE所注册的跟踪区的所有小区进行寻呼。

TAI是LTE的跟踪区标识（Tracking Area Identity），是由PLMN和TAC组成。

TAI = PLMN + TAC（Tracking Area Code）

多个TA组成一个TA列表，同时分配给一个UE，UE在该TA列表（TA List）内移动时不需要执行TA更新，以减少与网络的频繁交互；当UE进入不在其所注册的TA列表中的新TA区域时，需要执行TA更新，MME给UE重新分配一组TA，新分配的TA也可包含原有TA列表中的一些TA；每个小区只属于一个TA。

TA是小区级的配置，多个小区可以配置相同的TA，且一个小区只能属于一个TA。



## 53.LTE接受短信

手机在GSM通话过程中，可以通过SDCCH信道接受短信。

手机短信是保存在短信中心中的，当手机接收到短消息后，会返回ACK消息，如果手机在GSM短消息没有接收完全，那么短信中心会将这个短信保留，手机返回LTE网络后会继续发（或者手机返回LTE网络后，短信周期会隔一段发送），短信中心目前保留时间目前一般为一周，这个可以发送的时候进行设定。

短信发送和接收必定要经过SMSC短信中心，但LTE网络没有CS域的概念，所以需要经过SG接口将相应的消息发送到短信中心去。

## 54.LTE IP地址

第一：UE开机后是在哪个过程获得IP的，怎么获得的？

用户在attach过程中就获得了IP地址，由PGW完成，你可以看看S11口的create session request流程就清楚了。

第二：同一个基站下的IP地址属于一个子网么？

IP地址是由PGW来分配的，所以不一定是ENB下是同一个子网。

第三：UE进行基站间的切换后IP地址是如何变化的？

切换过程用户的IP地址是不会改变的，用户只是更换了传输层地址和TEID，一般来说，ATTACH流程伴随的PDN连接，用户一般一个IP地址，直至其Detach掉才释放。

在附着完成时，的确会得到IP，但严格意义上讲，IP分配不是由附着流程来完成的。附着是EMM, IP分配是ESM。

可以认为在附着的同时进行的默认承载激活完成了IP地址的申请和分配(如果不是静态地址的话)，但这不是唯一的获得地址的方式。

终端可以发起PDN连接来获得地址分配，PDN连接可以随附着同时发起，也可以单独发起。

承载激活和PDN连接均为ESM流程。

eNB不参与ESM过程，NAS消息是透传到核心网的，所以用户地址跟ENB无关，切换时也没关系。

这么理解吧，ENB就像一个hub，SGW/MME则像个交换机，而PGW则是个路由器并且还负责了DHCP代理的工作。

## 55.主分集的定义及作用

Radio 0是主集，负责射频信号的发送和接收；Radio1是分集，只接收不发送，基站会把从两个接口收到的信号进行合并处理，从而获得分集增益，因此这里的分集增益是接收增益。

分集接收主要是为了抵消快衰落对接收信号的影响，由于信号在传输过程中因反射等干扰产生多径分量信号，接收端利用多天线同时接收不同路径的信号，然后将这些信号选择、合并成总的信号，以减轻信号衰落的影响，这叫分集接收。分集就是把分散得到的信号集中合并，只要几个信号之间是相互独立的，经恰当的合并后就能得到最大的信号增益。

分集式天线（Diversity Aerials）确保无线信号接收的质量，即便在接收条件差的情况下依然能保证高标准音质。电视台与广播电台的电磁波常会受到高楼或山丘的反射，所以天线会接收到源信号和被反射后延迟到达的信号，接收质量由此受到影响，这就是所谓的多路传输干扰。分集式天线内含若干天线，它会合并不同天线独立接收的信号，以达到过滤干扰信号的目的；

主集一般来说就是能收发两用的天线，分集就是只能接收，当MS的信号通过上行传递给小区天线的时候，主分集同时可以接收到，这样就又两路信号了，然后基站通过判决器，选择一路最好的信号进行解调。注意是选择一路最好的信号哦，而不是对两路信号进行叠加处理哦。这样做的原因是为了空间分集，用两个天线接收同一个信号进行处理，得到一个最好的信号。