第一章移动通信的发展历程

1.1 移动通信的发展历程

当今的社会已经进入了一个信息化的社会，没有信息的传递和交流，人们就无法适应现代化的快节奏的生活和工作。人们期望随时随地、及时可靠、不受时空限制地进行信息交流，提高工作的效率和经济效益。移动通信可以说从无线电发明之日就产生了。1897 年，马可尼所完成的无线通信实验就是在固定站与一艘拖船之间进行的。而蜂窝移动通信的发展是在二十世纪七十年代中期以后的事。移动通信综合利用了有线、无线的传输方式，为人们提供了一种快速便捷的通讯手段。由于电子技术，尤其是半导体、集成电路及计算机技术的发展，以及市场的推动，使物美价廉、轻便可靠、性能优越的移动通信设备成为可能。现代的移动通信发展至今，主要走过了两代，而第三代现在正处于紧张的研制阶段，部分厂家已经推出实验产品。

第一阶段是模拟蜂窝移动通信网。时间是本世纪七十年代中期至八十年代中期。1978 年，美国贝尔实验室研制成功先进移动电话系统（AMPS），建成了蜂窝状移动通信系统。而其它工业化国家也相继开发出蜂窝式移动通信网。

这一阶段相对于以前的移动通信系统，最重要的突破是贝尔实验室在七十年代提出的蜂窝网的概念。蜂窝网，即小区制，由于实现了频率复用，大大提高了系统容量。

第一代移动通信系统的典型代表是美国的AMPS系统和后来的改进型系统TACS，以及 NMT 和 NTT 等。AMPS（先进的移动电话系统）使用模拟蜂窝传输的800MHz频带，在北美、南美和部分环太平洋国家广泛使用；TACS（总接入通信系统）使用 900MHz 频带，分 ETACS（欧洲）和 NTACS（日本）两种版本，英国、日本和部分亚洲国家广泛使用此标准。

第一代移动通信系统的主要特点是采用频分复用，语音信号为模拟调制，每隔 30KHz/25KHz 一个模拟用户信道。第一代系统在商业上取得了巨大的成功，但是其弊端也日渐显露出来：

(1)频谱利用率低

(2)业务种类有限

(3) 无高速数据业务

(4) 保密性差，易被窃听和盗号

(5) 设备成本高

(6) 体积大，重量大

为了解决模拟系统中存在的这些根本性技术缺陷，数字移动通信技术应运而生，并且发展起来，这就是以 GSM 和 IS-95 为代表的第二代移动通信系统，时间是从八十年代中期开始。欧洲首先推出了泛欧数字移动通信网（GSM）的体系。随后，美国和日本也制订了各自的数字移动通信体制。数字移动通信网相对于模拟移动通信，提高了频谱利用率，支持多种业务服务，并与 ISDN等兼容。第二代移动通信系统以传输话音和低速数据业务为目的，因此又称为窄带数字通信系统。

第二代数字蜂窝移动通信系统的典型代表是美国的 DAMPS 系统、IS-95 和欧洲的 GSM

系统。

(1) GSM（全球移动通信系统）发源于欧洲，它是作为全球数字蜂窝通信的TDMA 标准而设计的，支持 64Kbps 的数据速率，可与 ISDN 互连。GSM使用 900MHz 频带，使用 1800MHz 频带的称为 DCS1800。GSM 采用FDD 双工方式和TDMA多址方式，每载频支持8个信道，信号带宽200KHz。GSM 标准体制较为完善，技术相对成熟，不足之处是相对于模拟系统容量增加不多，仅仅为模拟系统的两倍左右，无法和模拟系统兼容。

(2)DAMPS（先进的数字移动电话系统）也称 IS-54（北美数字蜂窝），使用 800MHz 频带，是两种北美数字蜂窝标准中推出较早的一种，指定使用 TDMA 多址方式。

(3) IS-95 是北美的另一种数字蜂窝标准，使用 800MHz 或 1900MHz 频带，指定使用 CDMA 多址方式，已成为美国 PCS（个人通信系统）网的首先技术。

GSM 发展历程如下：

- ✓ 1982 年，欧洲邮电行政大会 CEPT 设立了“移动通信特别小组”即 GSM，以开发第二代移动通信系统为目标。
- ✓ 1986 年，在巴黎，对欧洲各国经大量研究和实验后所提出的八个建议系统进行现场试验。
- ✓ 1987 年，GSM 成员国经现场测试和论证比较，就数字系统采用频分双工－窄带时分多址（FDD－TDMA）、规则脉冲激励－长期预测话音编码（RPE-LTP）和高斯滤波最小频移键控（GMSK）调制方式达成一致意见。
- ✓ 1988 年，十八个欧洲国家达成 GSM 谅解备忘录(MOU)。
- ✓ 1989 年，GSM 标准生效。

该阶段标准称为 PH ASE I，主要定义了 900M 频段的技术标准。随着系统应用日益广泛，需求不断增加，GSM 推出了：PHASE II 标准，它除了对 PHASE I 标准进行必要的修正和业务补充外，主要增加了 1800M 频段的技术标准；PHASE II ＋标准，主要增加了 GPRS 部分的内容。

- ✓ 1991 年，GSM 系统正式在欧洲问世，网路开通运行。移动通信跨入第二代。

由于第二代移动通信以传输话音和低速数据业务为目的，从 1996 年开始，为了解决中速数据传输问题，又出现了2.5代的移动通信系统，如GPRS 和IS-95B。

移动通信现在主要提供的服务仍然是语音服务以及低速率数据服务。由于网络的发展，数据和多媒体通信的发展势头很快，所以，第三代移动通信的目标就是移动宽带多媒体通信。

从发展前景看，由于自有的技术优势，CDMA技术已经成为第三代移动通信的核心技术。

为实现上述目标，对3G无线传输技术（ RTT ： Radio Transmission Technology）提出了以下要求：

(1) 高速传输以支持多媒体业务。

- ✓ 室内环境至少 2Mbps；
- ✓ 室内外步行环境至少 384kbps；
- ✓ 室外车辆运动中至少 144kbps；
- ✓ 卫星移动环境至少 9.6kbps。

(2) 传输速率能够按需分配。

(3) 上下行链路能适应不对称需求。

第三代移动通信系统最早由国际电信联盟（ITU） 于 1985 年提出，当时称为未 来 公众陆地移动通信系统（ FPLMTS ，Future Public Land Mobile Telecommunication System），1996年更名为IMT-2000 （International Mobile Telecommunication-2000），意即该系统工作在 2000MHz 频段，最高业务速率可达 2000kbps，预期在 2000 年左右得到商用。主要体制有WCDMA、cdma2000 和 TD－SCDMA。1999年11月 5 日，国际电联 ITU-R TG8/1 第 18 次会议通过了“IMT-2000 无线接口技术规范”建议，其中我国提出的 TD-SCDMA 技术写在了第三代无线接口规范建议的 IMT-2000 CDMATDD 部分中。

1.2移动通信的关键技术

1.2.1 多址方式

1.2.1.1 多址技术

多址技术使众多的用户共用公共的通信线路。为使信号多路化而实现多址的方法基本上有三种，它们分别采用频率、时间或代码分隔的多址连接方式，即人们通常所称的频分多址（FDMA）、时分多址（TDMA）和码分多址（CDMA）三种接入方式。图2-1用模型表示了这三种方法简单的一个概念。

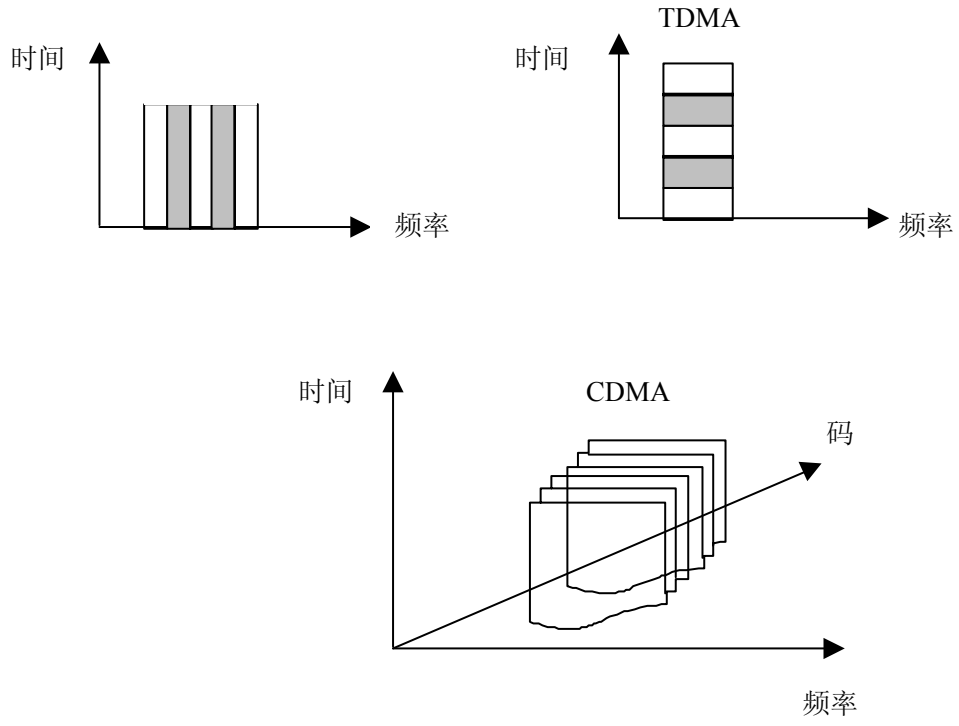


图 1-1 三种多址方式概念示意图

FDMA 是以不同的频率信道实现通信的，TDMA 是以不同的时隙实现通信的，CDMA 是以不同的代码序列实现通信的。

移动通信

1. 频分多址（FDMA）

频分，有时也称之为信道化，就是把整个可分配的频谱划分成许多单个无线电信道（发射和接收载频对），每个信道可以传输一路话音或控制信息。在系统的控制下，任何一个用户都可以接入这些信道中的任何一个。

模拟蜂窝系统是 FDMA 结构的一个典型例子，数字蜂窝系统中也同样可以采用 FDMA，只是不会采用纯频分的方式，比如 GSM 系统就采用了 FDMA。

2. 时分多址（TDMA）

时分多址是在一个宽带的无线载波上，按时间（或称为时隙）划分为若干时分信道，每一用户占用一个时隙，只在这一指定的时隙内收（或发）信号，故称为时分多址。此多址方式在数字蜂窝系统中采用，GSM 系统也采用了此种方式。

TDMA是一种较复杂的结构，最简单的情况是单路载频被划分成许多不同的时隙，每个时隙传输一路猝发式信息。TDMA中关键部分为用户部分，每一个用户分配给一个时隙（在呼叫开始时分配），用户与基站之间进行同步通信，并对时隙进行计数。当自己的时隙到来时，手机就启动接收和解调电路，对基站发来的猝发式信息进行解码。同样，当用户要发送信息时，首先将信息进行缓存，等到自己时隙的到来。在时隙开始后，再将信息以加倍的速率发射出去，然后又开始积累下一次猝发式传输。

3. 码分多址（CDMA）

码分多址是一种利用扩频技术所形成的不同的码序列实现的多址方式。它不像 FDMA、TDMA 那样把用户的信息从频率和时间上进行分离，它可在一个信道上同时传输多个用户的信息，也就是说，允许用户之间的相互干扰。其关键是信息在传输以前要进行特殊的编码，编码后的信息混合后不会丢失原来的信息。有多少个互为正交的码序列，就可以有多少个用户同时在一个载波上通信。每个发射机都有自己唯一的代码（伪随机码），同时接收机也知道要接收的代码，用这个代码作为信号的滤波器，接收机就能从所有其他信号的背景中恢复成原来的信息码（这个过程称为解扩）。

1.2.2 功率控制

所有的 GSM 手机都可以以 2dB 为一等级来调整它们的发送功率,GSM900移动台的最大输出功率是8W（规范中最大允许功率是20W，但现在还没有20W 的移动台存在）。DCS1800 移动台的最大输出功率是 1W。相应地，它的小区也要小一些。

当手机在小区内移动时，它的发射功率需要进行变化。当它离基站较近时，需要降低发射功率，减少对其它用户的干扰，当它离基站较远时，就应该增加功率，克服增加了的路径衰耗。

1.2.3 蜂窝技术

1.2.3.1 频率复用（蜂窝技术）

移动通信的飞速发展一大原因是发明了蜂窝技术。移动通信的一大限制是使用频带比较有限，这就限制了系统的容量，为了满足越来越多的用户需求，必须要在有限的频率范围尽可能大地扩大它的利用率，除了采用前面介绍过的多址技术等以外，还发明了蜂窝技术。

那么什么是蜂窝技术呢？

移动通信系统是采用一个叫基站的设备来提供无线服务范围的。基站的覆盖范围有大有小，我们把基站的覆盖范围称之为蜂窝。采用大功率的基站主要是为了提供比较大的服务范围，但它的频率利用率较低，也就是说基站提供给用户的通信通道比较少，系统的容量也就大不起来，对于话务量不大的地方可以采用这种方式，我们也称之为大区制。采用小功率的基站主要是为了提供大容量的服务范围，同时它采用频率复用技术来提高频率利用率，在相

同的服务区域内增加了基站的数目，有限的频率得到多次使用，所以系统的容量比较大，这种方式称之为小区制或微小区制。下面我们简单介绍频率复用技术的原理。

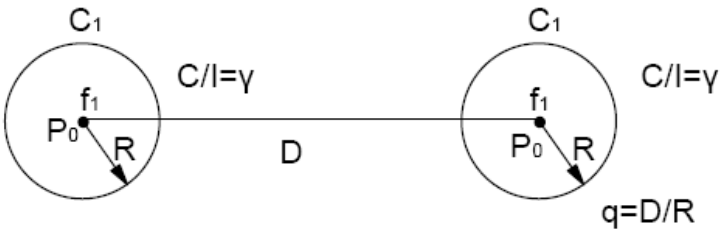


图 1-2 D/R 比

1. 频率复用的概念

在全双工工作方式中，一个无线电信道包含一对信道频率，每个方向都用一个频率作发射。在覆盖半径为 R 的地理区域 C1内呼叫一个小区使用无线电信道 F1，也可以在另一个相距 D、覆盖半径也为 R 的小区内再次使用 F1。频率复用是蜂窝移动无线电系统的核心概念。在频率复用系统中，处在不同地理位置（不同的小区）上的用户可以同时使用相同频率的信道（见图 2-2），频率复用系统可以极大地提高频谱效率。但是，如果系统设计得不好，将产生严重的干扰，这种干扰称为同信道干扰。这种干扰是由于相同信道公共使用造成的，是在频率复用概念中必须考虑的重要问题。

2. 频率复用方案

可以在时域与空间域内使用频率复用的概念。在时域内的频率复用是指在不同的时隙里占用相同的工作频率，叫做时分多路（TDM）。在空间域上的频率复用可分为两大类：

1)两个不同的地理区域里配置相同的频率。例如在不同的城市中使用相同频率的 AM 或 FM 广播电台。

2)在一个系统的作用区域内重复使用相同的频率——这种方案用于蜂窝系统中。蜂窝式移动电话网通常是先由若干邻接的无线小区组成一个无线区群，再由若干个无线区群构成整个服务区。为了防止同频干扰，要求每个区群（即单位无线区群）中的小区，不得使用相同

频率，只有在不同的无线区群中，才可使用相同的频率。单位无线区群的构成应满足两个基本条件：

若干个单位无线区群彼此邻接组成蜂窝式服务区域

邻接单位无线区群中的同频无线小区的中心间距相等。

一个系统中有许多同信道的小区，整个频谱分配被划分为 K 个频率复用的模式，即单位无线区群中小区的个数，如图3所示，其中 K=3、4、7，当然还有其它复用方式，如 K=9、12 等。

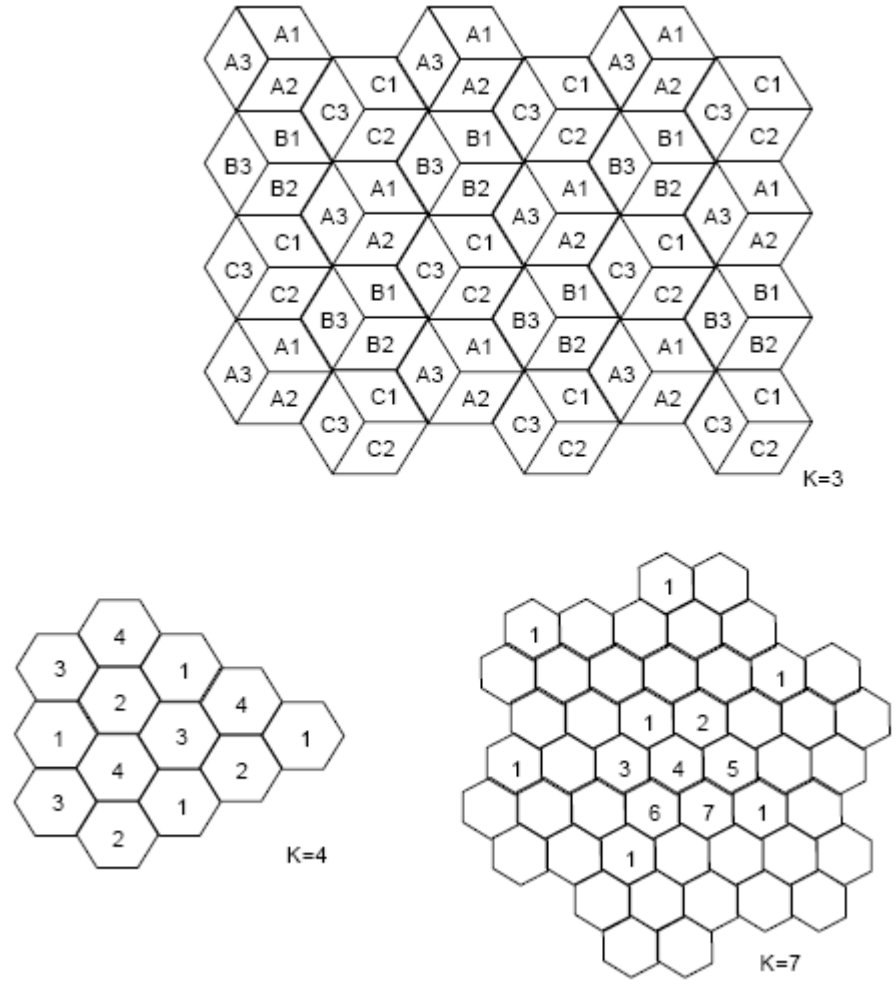


图 1-3 N 小区复用模式

允许同频率重复使用的最小距离取决于许多因素，如中心小区附近的同信道小区数，地理地形类别，每个小区基站的天线高度及发射功率。

频率复用距离 D 由下式确定：

$$D = \sqrt{3KR}$$

其中，K 是图 2中所示的频率复用模式。则

D=3.46R K=4

D=4.6R K=7

如果所有小区基站发射相同的功率，则 K 增加，频率复用距离 D 也增加。增加了的频

率复用距离将减小同信道干扰发生的可能。

从理论上来说，K 应该大些，然而，分配的信道总数是固定的。如果 K 太大，则 K 个小区中分配给每个小区的信道数将减少，如果随着 K 的增加而划分 K个小区中的信道总数，则中继效率就会降低。同样道理，如果在同一地区将一组信道分配给两个不同的工作网络，系统频率效率也将降低。

因此，现在面临的问题是，在满足系统性能的条件下如何得到一个最小的K值。解决它必须估算同信道干扰，并选择最小的频率复用距离 D 以减小同信道干扰。在满足条件的情况下，构成单位无线区群的小区个数 $K= i^2 + ij + j^2$（i、j） 均为正整数，其中一个可为零，但不能两个同时为零），取 i = j = 1，可得到最小的 K 值为 K=3（见图1-3）

1.2.4 分集技术

分集技术是指系统同时接收衰落互不相关的两个或更多个输入信号后，系统分别解调这些信号然后将他们相加，这样系统可以接收到更多有用信号，克服衰落。

移动通信信道是一种多径衰落信道，发射的信号要经过直射、反射、散射等多条传播途径才能达到接收端，而且随着移动台的移动，各条传播路径上的信号幅度、时延及相位随时随地发生变化，所以接收到的信号的电平是起伏、不稳定的，这些多径信号相互叠加就会形成衰落。叠加后的信号幅度变化符合瑞利分布，又称瑞利衰落。瑞利衰落随时间急剧变化时，称为“快衰落”。快衰落严重衰落深度达到20~30dB。瑞利衰落的中值场强只产生比较平缓的变化，称为“慢衰落”，且服从对数正态分布。

分集技术是克服叠加衰落的一个有效分发。由于具有频率、时间、空间的选择性，因此分集技术包括频率分集、时间分集、空间分集。

减弱慢衰落采用空间分集，即用几个独立天线或在不同场地分别发射和接收信号，以保证各信号之间的衰落独立。

根据衰落的频率选择性，当两个频率间隔大于信道带宽相关带宽时，接收到的此两种频率的衰落信号不相关，市区的相关带宽一般为 50kHz 左右，郊区的相关带宽一般为 250kHz 左右。而 CDMA 的一个信道带宽为 1.23MKz，无论在市区还是郊区都远远大于相关带宽的要求，所以 CDMA 的宽带传输本身就是频率分集。

时间分集是利用基站和移动台的 RAKE 接收机来完成的。对于一个信道带宽为 1.23MHz 的 CDMA 系统，当来自两个不同路径信号的时延为 1us 时，也即这两条路径相差大约 300m 时，RAKE接收机就可以将它们分别提取出来而不混淆。

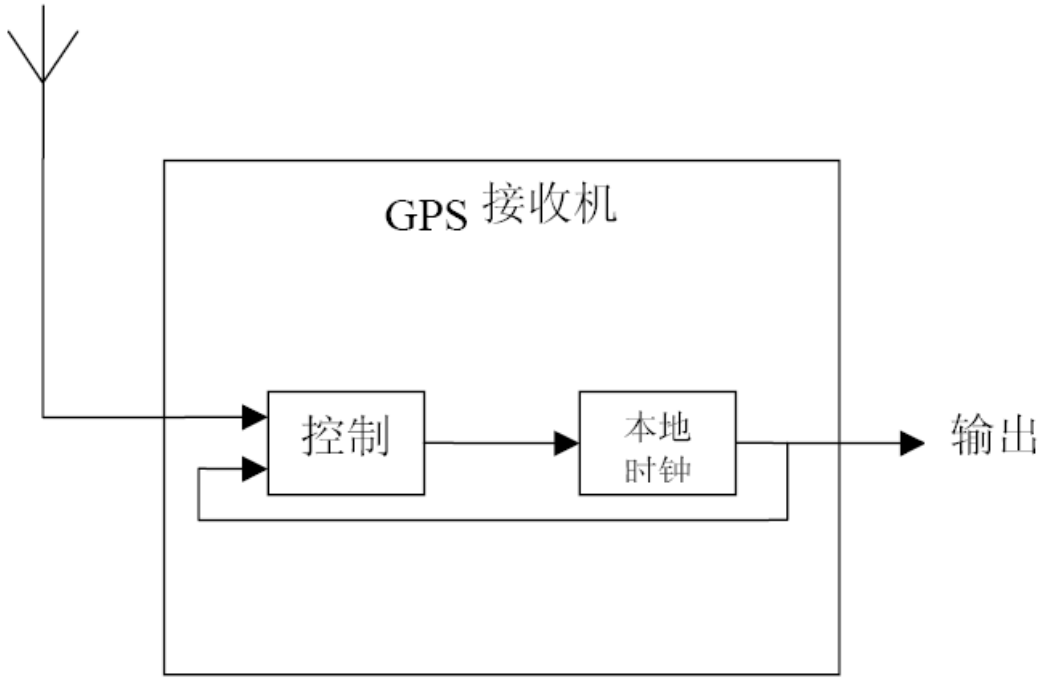
1.2.5 GPS 同步问题简介

GPS 的作用

在大多数 BTS 系统中，GPS 接收机都是其他公司提供的。这些 GPS 接收机一般向 BTS 提供三个信号。

其中 19.6608MHz 是 CDMA 进行解调的基本频率。UTC 用于计算长码的相位。偶秒用于同步短码和超帧。某些公司的接收机还向 BTS 提供某些内部使用的特殊基准频率。

1.2.5.1失去 GPS 后的问题



如图所示，GPS接收机中的信号不是直接从 GPS中输出的，而是通过控制本地时钟，由本地时钟输出的。因此，突发性干扰（例如：自然界中的闪电造成 GPS 信号瞬时中断）将在控制系统的作用下被消除，不会对输出信号造成任何影响。对于长时间的信号中断，本地时钟仍然可以输出信号，但会逐步发生漂移。具体能够稳定工作的时间决定于本地时钟的质量。大部分系统可以稳定工作 2 天左右。

1.2.5.2 备用手段

1. 高精度本地时钟

如上文所述，GPS 消失以后，接收机自带的时钟仍然可以长时间工作，通过采用高精度的时钟，可以延长工作时间。这种的方案对现有设备改动最小，因为接收机中都自带时钟，且是可选的。但它不能长时间工作。

2. 局部同步网

与目前固定网使用的同步网相比，CDMA 系统额外需要一个时间信号，可以在同步网的基础上增加偶秒脉冲，实现 CDMA 系统的同步。但这需要增加相应的同步信号传输设备，当网络中基站数量很多时，特别时发展到微蜂窝阶段时上述传输设备很难实现。但这种方案可靠性最高。

3. 使用 GLONASS

GLONASS 是俄国发射的类似 GPS 的系统。由于它不区分军用和民用，所以实际可以提供比GPS 民用标准更高的精度。某些公司已经可以提供GPS、GLONASS 系统双备份的接收机。但成本将增加。

考虑靠到成本问题，本体制仍然要求使用 GPS 系统。

1.3 无线信道

1.3.1 从原始信号到无线电波的转换

1.3.1.1 无线接口

话音信号在无线接口路径的处理过程如图1-4。

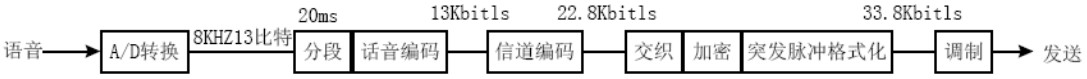


图 1-4 语音在 MS 中的处理过程

1. 信号采样

首先，语音通过一个模/数转换器，实际上是经过 8KHz 抽样、量化后变为每125us 含有 13bit 的码流；每 20ms 为一段，再经语音编码后降低传码率为——13Kbit/s；经信道编码变为22.8Kbit/s；再经码字交织、加密和突发脉冲格式化后变为 33.8Kbit/s 的码流，经调制后发送出去。接收端的处理过程相反。

2. 语音编码

此编码方式称为规则脉冲激励——长期预测编码(RPE-LTP)，其处理过程是先进行 8KHz 抽样，调整每 20ms 为一帧，每帧长为 4 个子帧，每个子帧长 5ms，纯比特率为 13Kbit/s。

现代数字通信系统往往采用话音压缩编码技术，GSM 也不例外。它利用语声编码器为人体喉咙所发出的音调和噪声，以及人的口和舌的声学滤波效应建立模型，这些模型参数将通过 TCH 信道进行传送。

语音编码器是建立在残余激励线性预测编码器（REIP）的基础上的，并通过长期预测器（LTP）增强压缩效果。LTP 通过去除话音的元音部分，使得残余数据的编码更为有利。语音编码器以20ms为单位，经压缩编码后输出260bits，因此码速率为 13Kbps。根据重要性不同，输出的比特分成182bits和 78bits 两类。较重要的 182bits 又可以进一步细分出 50 个最重要的比特。

与传统的 PCM 线路上语声的直接编码传输相比，GSM 的 13Kbps 的话音速率要低得多。未来的更加先进的话音编码器可以将速率进一步降低到 6.5Kbps（半速率编码）。

3. 信道编码

为了检测和纠正传输期间引入的差错，在数据流中引入冗余通过加入从信源数据计算得到的信息来提高其速率，信道编码的结果一个码字流；对话音来说，这些码字长 456 比特。

由语音编码器中输出的码流为 13Kbit/s，被分为 20ms 的连续段，每段中含有260 比特，其中特细分为：

50 个非常重要的比特

132 个重要比特

78 个一般比特

对它们分别进行不同的冗余处理，如图1-5所示。

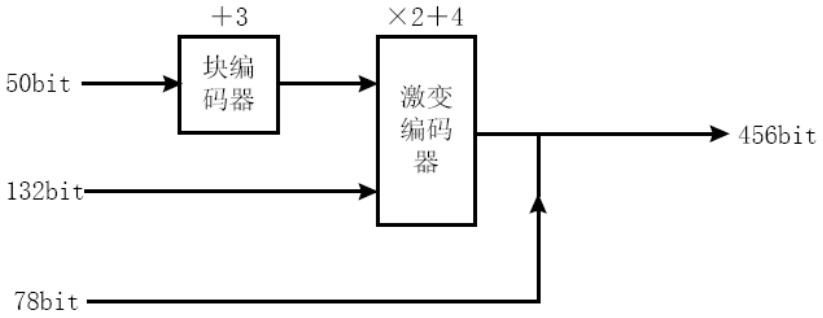


图 1-5 信道编码过程

其中，块编码器引入 3 位冗余码，激变编码器引入 2 倍冗余后再加 4 位尾比特。

用于 GSM 系统的信道编码方法有三种：卷积码、分组码和奇偶码。具体原理见有关资料，在这里就不再赘述了。

4. 交织

在编码后，语音组成的是一系列有序的帧。而在传输时的比特错误通常是突发性的，这将影响连续帧的正确性。为了纠正随机错误以及突发错误，最有效的组码就是用交织技术来分散这些误差。

交织的要点是把码字的b个比特分散到n个突发脉冲序列中，以改变比特间的邻近关系。n值越大，传输特性越好，但传输时延也越大，因此必须作折衷考虑，这样，交织就与信道的用途有关，所以在 GSM 系统中规定了几种交织方法。

在 GSM 系统中，采用二次交织方法。

由信道编码后提取出的 456 比特被分为 8 组，进行第一次交织，如图1-6。

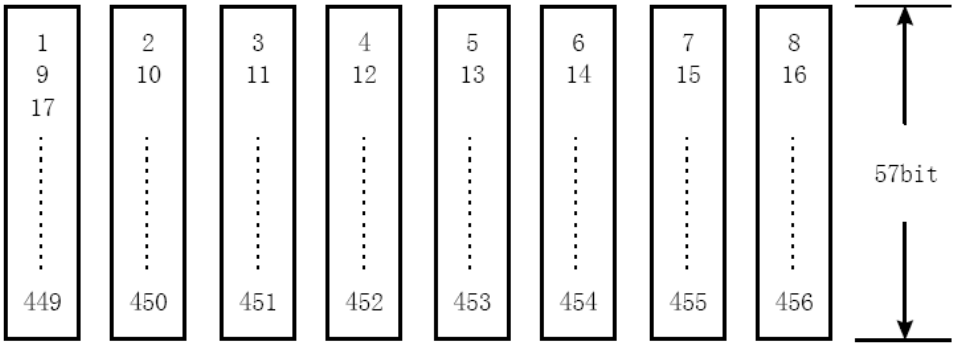


图 1-6 456 比特交织

由它们组成语音帧的一帧，现假设有三帧语音帧如图1-7

图 1-7 三个语音帧

而在一个突发脉冲中包括一个语音帧中的两组，如图1-8所示。

图 1-8 突发脉冲的结构

其中，前后 3 个尾比特用途消息定界，26 个训练比特，训练比特的左右各 1个比特作为“挪用标志”。而一个突发脉冲携带有两段 57 比特的声音信息。（突发脉冲将在后一章介绍）如表 1，在发送时，进行第二次交织。

表 1-1 语音码的二次交织

A	
A	
A	
A	
B	A
B	A
B	A
B	A
C	B
C	B
C	B
C	B
	C
	C
	C
	C

5. 调制技术

GSM 的调制方式是 0.3GMSK。0.3 表示了高斯滤波器的带宽和比特率之间的关系。

GSMK 是一种特殊的数字调频方式，它通过在载波频率上增加或者减少67.708KHz，来表示 0 或 1，利用两个不同的频率来表示 0 和 1 的调制方法称为 FSK。在 GSM 中，数据的比特率被选择为正好是频偏的 4 倍，这可以减小频谱的扩散，增加信道的有效性，比特率为频偏 4 倍的 FSK，称为 MSK——最小频移键控。通过高斯预调制滤波器，可以进一步压缩调制频谱。高斯滤波器降低了频率变化的速度，防止信号能量扩散到邻近信道频谱。

0.3 GSMK 并不是一个相位调制，信息并不是象 QPSK 那样，由绝对的相位来表示。它是通过频率的偏移或者相位的变化来传送信息的。有时把 GMSK画在 I/Q平面图上是非常有用的。如果没有高斯滤波器，MSK 将用一个比载波高 67.708KHz 的信号来表示一个待定的脉冲串 1。如果载波的频率被作为一个静止的参考相位，我们就会看到一个 67.708KHz 的

信号在 I/Q 平面上稳定地增长相位，它每秒种将旋转 67,708 次。在每一个比特周期，相位将变化90° 一个 1 将由 90° 相位增长表示，两个 1将引起 180° 相位增长，三个 1将引起 270° 相位增长，如此等等。同样地，连续的 0也将引起相应的相位变化，只是方向相反而已。高斯滤波器的加入并没有影响 0和 1的90° 位增减 变化，因为它没有改变比特率和频偏之间的四倍关系，所以不会影响平均相位的相对关系，只是降低了相位变化时的速率。在使用高斯滤波器时，相位的方向变换将会变缓，但可以通过更高的峰值速度来进行相位补偿。如果没有高斯滤波器，将会有相位的突变，但相位的移动速度是一致的。

精确的相位轨迹需要严格的控制。GSM 系统使用数字滤波器和数字 I/Q 调制器去产生正确的相位轨迹。在GSM 规范中，相位的峰值误差不得超过20°,均方误差不得超过5°

6. 跳频

在语音信号经处理，调制后发射时，还会采用跳频技术——即在不同时隙发射载频在不断地改变（当然，同时要符合频率规划原则）。

引入跳频技术，主要是出于以下两点考虑。

(1)由于过程中的衰落具有一定的频带性，引入跳频可减少瑞利衰落的相关性。

(2)由于干扰源分集特性：在业务密集区，蜂窝的容量受频率复用产生的干扰限制，因为系统的目标是满足尽可能多买主的需要，系统的最大容量是在一给定部分呼叫由于干扰使质量受到明显降低的基础上计算的，当在给定的 C/I 值附近统计分散尽可能小时，系统容量较好。我们考虑一个系统，其中一个呼叫感觉到的干扰是由许多其它呼叫引起的干扰电平的平均值。那么，对于一给定总和，干扰源的数量越多，系统性能越好。

GSM系统的无线接口采用了慢速跳频（SFH）技术。慢速跳频与快速跳频（FFH）之间的区别在于后者的频率变化快于调制频率。GSM 系统在整个突发序列传输期，传送频率保持不变，因此是属于慢跳频情况，如图1-9所示。

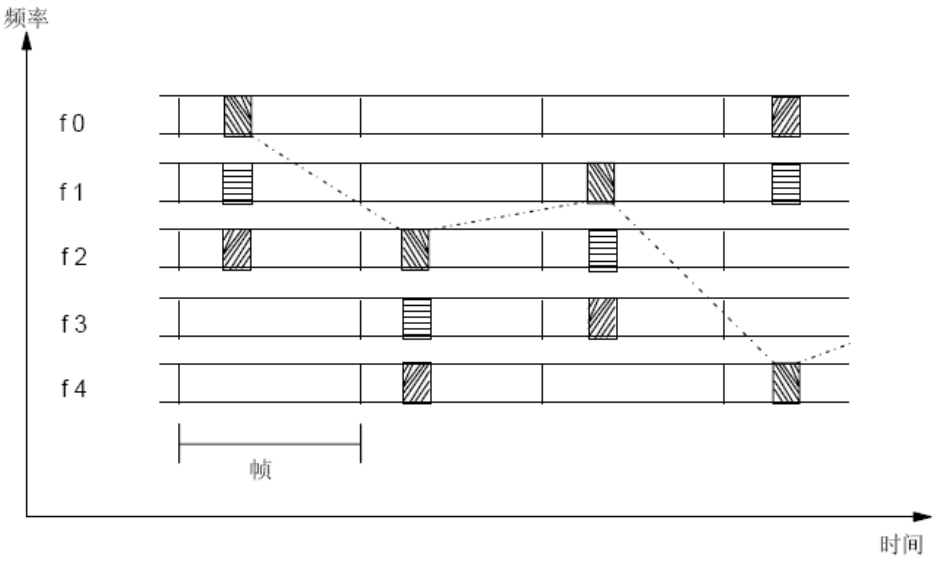


图 1-9 GSM 系统调频示意图

在上、下行线两个方向上，突发序列号在时间上相差 3BP，跳频序列在频率上相差45MHz。

GSM 系统允许有 64 种不同的跳频序列，对它的描述主要有两个参数：移动分配指数偏置 MAIO 和跳频序列号 HSN。MAIO 的取值可以与一组频率的频率数一样多。HSN 可以取 64 个不同值。跳频序列选用伪随机序列。

通常，在一个小区的信道载有同样的 HSN 和不同的 MAIO，这是避免小区内信道之间的干扰所希望的。邻近小区不会有干扰，因它们使用不同的频率组。

为了获得干扰参差的效果，使用同样频率组的远小区应使用不同的 HSN。对跳频算法感兴趣的读者，可参阅 GSM Rec.05.02，这里不再细述。

7. 时序调整

由于 GSM 采用 TDMA，且它的小区半径可以达到 35km，因此需要进行时序调整。由于从手机出来的信号需要经过一定时间才能到达基地站，因此我们必须采取一定的措施，来保证信号在恰当的时候到达基地站。

如果没有时序调整，那么从小区边缘发射过来的信号，就将因为传输的时延和从基站附近发射的信号相冲突（除非二者之间存在一个大于信号传输时延的保护时间）。通过时序调整，手机发出的信号就可以在正确的时间到达基站。当 MS 接近小区中心时，BTS 就会通知它减少发射前置的时间，而当它远离小区中心时，就会要求它加大发射前置时间。

当手机处于空闲模式时，它可以接收和解调基地站来的 BCH信号。在BCH信号中有一个 SCH 的同步信号，可以用来调整手机内部的时序，当手机接收到一个 SCH 信号后，它并不知道它离基站有多远。如果手机和基站相距 30km的话，那么手机的时序将比基站慢 100us。当手机发出它的第一个 RACH 信号时，就已经晚了100us，再经过100us 的传播时延，到达基站时就有了200us的总时延，很可能和基站附近的相邻时隙的脉冲发生冲突。因此，RACH 和其它的一些信道接入脉冲将比其它脉冲短。只有在收到基站的时序调整信号后，手机才能发送正常长度的脉冲。在我们的这个例子中，手机就需要提前 200us发送信号。

1.3.1.2帧和信道

1. 基本术语简介

SM 系统在无线路径上传输要涉及的基本概念最主要的是突发脉冲序列（Burst），简称突发序列，它是一串含有百来个调制比特的传输单元。突发脉冲序列有一个限定的持续时间和占有限定的无线频谱。它们在时间和频率窗上输出，而这个窗被人们称为隙缝（Slot）。确切地说，在系统频段内，每200KHz 设置隙缝的中心频率（以 FDMA 角度观察），而隙缝在时间上循环地发生，每次占 15/26ms 即近似为 0.577ms（以 TDMA 角度观察）。在给定的小区内，所有隙缝的时间范围是同时存在的。这些隙缝的时间间隔称为时隙（Time Slot），而它的持续时间被用于作为时间单元，标为 BP，意为突发脉冲序列周期（Burst Period）。

我们可用时间/频率图把隙缝画为一个小矩形，其长为 15/26ms、宽为 200KHz，

如图1-4所示。类似地，我们可把GSM所规定的200KHz带宽称为频隙（Frequency Slot），相当于 GSM 规范书中的无线频道（Radio Frequency Channel），也称射频信道。

时隙和突发脉冲序列两术语，在使用中带有某些不同的意思。例如突发脉冲序列，有时与时—频“矩形”单元有关，有时与它的内容有关。类同地，时隙含有其时间值的意思，或

意味着在时间上循环地使用每八个隙缝中的一个隙缝。

使用一个给定的信道就意味着在特定的时刻和特定的频率，也就是说在特定的隙缝中传送突发脉冲序列。通常，一个信道的隙缝在时间上不是邻接的。

信道 对于每个时隙具有给定的时间限界和时隙号码TN（Time Slot Number），这些都是信道的要素。一个信道的时间限界是循环重复的。

与时间限界类似，信道的频率限界给出了属于信道的各隙缝的频率。它把频率配置给各时隙，而信道带有一个隙缝。对于固定的频道，频率对每个隙缝是相同的。对于跳频信道的隙缝，可使用不同的频率。

帧（Frame）通常被表示为接连发生的 i 个时隙。在 GSM 系统中，目前采用全速率业务信道，i取为 8。TDMA 帧强调的是以时隙来分组而不是 8BP。这个想法在处理基站执行过程中是很自然的，它与基站执行许多信道的实际情况相吻合。但是从移动台的角度看，8BP 周期的提法更自然，因为移动台在同样的一帧时间中仅处理一个信道，占用一个时隙，更有“突发”的函意。

一个 TDMA 帧包含 8 个基本的物理信道。

物理信道（Physical Channel）采用频分和时分复用的组合，它由用于基站（BS）和移动台（MS）之间连接的时隙流构成。这些时隙在 TDMA 帧中的位置，从帧到帧是不变的，参见图1-10。

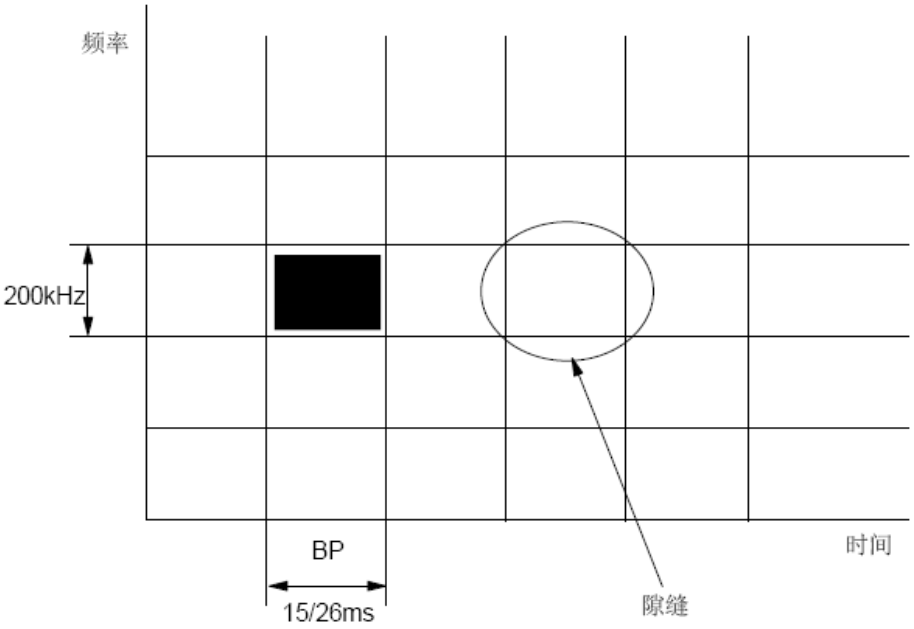


图 1-10 时间和频率中的隙缝

逻辑信道（Logical Channel）是在一个物理信道中作时间复用的。不同逻辑信道用于 BS 和 MS 间传送不同类型的信息，例如信令或数据业务。在 GSM建议中，对不同的逻辑信道规定了五种不同类型的突发脉冲序列5.2.2 帧结构。

图1- 11示出了 TDMA 帧的完整结构，还包括了时隙和突发脉冲序列。必须记住，TDMA 帧是在无线链路上重复的“物理”帧。

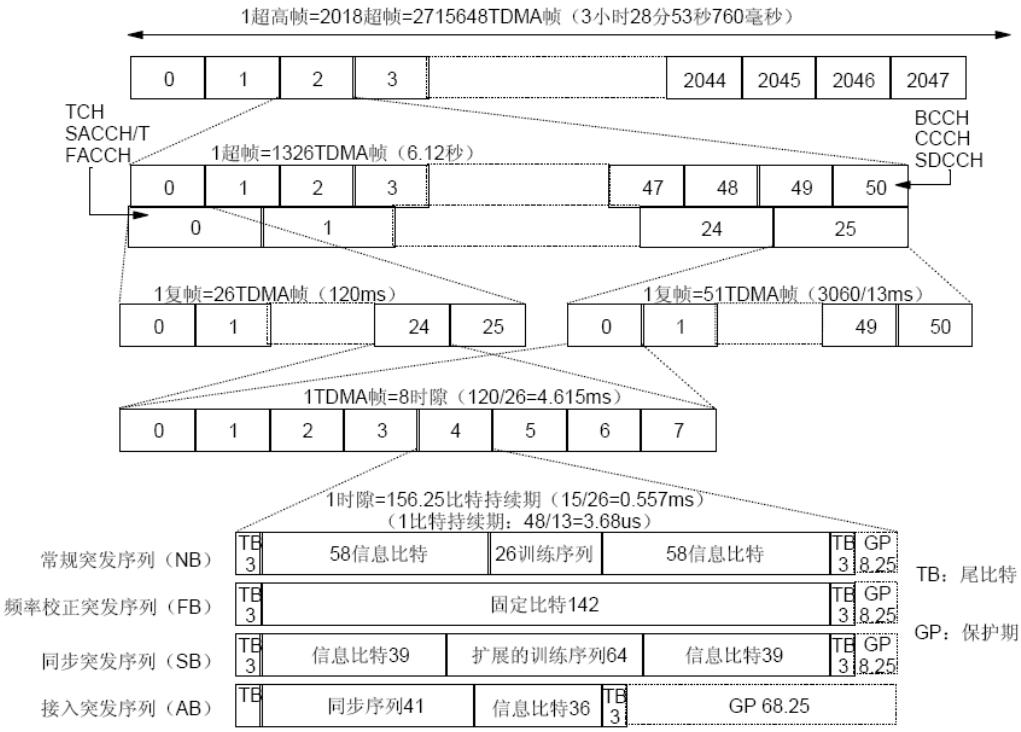


图 1-11 帧、时隙和突发脉冲序列

每一个 TDMA 帧含 8 个时隙，共占 60/13≈4.615ms。每个时隙含 156.25 个码元，占 15/26≈0.557ms。

多个 TDMA 帧构成复帧（Multiframe），其结构有两种，分别含连贯的 26 个或 51 个 TDMA 帧。当不同的逻辑信道复用到一个物理信道时，需要使用这些复帧。

含 26 帧的复合帧其周期为120ms，用于业务信道及其随路控制信道。其中24 个突发序列用于业务，2 个突发序列用于信令。

含 51 帧的复合帧其周期为 3060/13≈235.385ms，专用于控制信道。

多个复帧又构成超帧（Super frame）它是一个连贯的 51×26TDMA 帧，即一个超帧可以是包括 51 个 26TDMA 复帧，也可以是包括 26 个 51TDMA 复帧。超帧的周期均为 1326 个 TDMA 帧，即 6.12 秒。

多个超帧构成超高帧（Hyper frame）。它包括 2048 个超帧，周期为 12533.76秒，即 3 小时 28 分 53 秒 760 毫秒。用于加密的话音和数据，超高帧每一周期包含 2715648 个 TDMA 帧，这些 TDMA 帧按序编号，依次从 0 至 2715647，帧号在同步信道中传送。帧号在跳频算法中也是必需的。

2. 信道类型和组合

无线子系统的物理信道支撑着逻辑信道。逻辑信道可分为业务信道(Traffic Channel)和控制信道(Control Channel)两大类，其中后者也称信令信道(Signalling Channel)。

一、业务信道

业务信道（TCH）载有编码的话音或用户数据，它有全速率业务信道（TCH/F）和半速率业务信道（TCH/H）之分，两者分别载有总速率为 22.8 和 11.4kbit/s的信息。使用全速率信道所用时隙的一半，就可得到半速率信道。因此一个载频可提供 8 个全速率或 16 个半

速率业务信道（或两者的组合）并包括各自所带有的随路控制信道。

1、话音业务信道

载有编码话音的业务信道分为全速率话音业务信道（TCH/FS）和半速率话音业务信道（TCH/HS），两者的总速率分别为 22.8 和 11.4kbit/s。

对于全速率话音编码，话音帧长 20ms，每帧含 260 比特，提供的净速率为 13kbit/s。

2、数据业务信道

在全速率或半速率信道上，通过不同的速率适配、信道编码和交织，支撑着直至 9.6kbit/s 的透明和非透明数据业务。用于不同用户数据速率的业务信道，具体有：

- ✓ 9.6kbit/s，全速率数据业务信道（TCH/F9.6）
- ✓ 4.8kbit/s，全速率数据业务信道（TCH/F4.8）
- ✓ 4.8kbit/s，半速率数据业务信道（TCH/H4.8）
- ✓ ≤2.4kbit/s，全速率数据数据业务信道（TCH/F2.4）
- ✓ ≤2.4kbit/s，半速率数据数据业务信道（TCH/H2.4）

数据业务信道还支撑具有净速率为 12kbit/s 的非限制的数字承载业务。

在 GSM 系统中，为了提高系统效率，还引入额外一类信道，即 TCH/8，它的速率很低，仅用于信令和短消息传输。如果 TCH/H 可看作为 TCH/F 的一半，则 TCH/8 便可看作为 TCH/F 的八分之一。TCH/8 应归于慢速随路控制信道（SACCH）的范围。

二、控制信道

控制信道（CCH）用于传送信令或同步数据。它主要有三种：广播信道（BCCH）、公共控制信道（CCCH）和专用控制信道（DCCH）。

1、广播信道

广播信道仅作为下行信道使用，即 BS 至 MS 单向传输。它分为如下三种信道：

① 频率校正信道（FCCH）

载有供移动台频率校正用的信息。

② 同步信道（SCH）

载有供移动台帧同步和基站收发信台识别的信息。实际上，该信道包含两个编码参数。

基站识别码（BSIC），它占有 6 个比特（信道编码之前），其中 3 个比特为0～7 范围的 PLMN 色码，另 3 个比特为 0～7 范围的基站色码（BCC）。

简化的 TDMA 帧号（RFN），它占有 19 个比特。

③ 广播控制信道（BCCH）

通常，在每个基站收发信台中总有一个收发信机含有这个信道，以向移动台广播系统信息。BCCH 所载的参数主要有：

CCCH（公共控制信道）号码以及 CCCH 是否与 SDCCH（独立专用控制信道）相组合。

为接入准许信息所预约的各 CCCH 上的区块（block）号码。

向同样寻呼组的移动台传送寻呼信息之间的 51TDMA 复合帧号码。

2、公共控制信道

公共控制信道为系统内移动台所共用，它分为下述三种信道：

① 寻呼信道（PCH）

这是一个下行信道，用于寻呼被叫的移动台。

② 随机接入信道（RACH）

这是一个上行信道，用于移动台随机提出入网申请，即请求分配一个 SDCCH。

③ 准予接入信道（AGCH）

这是一个下行信道，用于基站对移动台的入网请求作出应答，即分配一个SDCCH 或直接分配一个 TCH。

3、专用控制信道

使用时由基站将其分给移动台，进行移动台与基站之间的信号传输。它主要有如下几种：

① 独立专用控制信道（SDCCH）

用于传送信道分配等信号。它可分为独立专用控制信道（SDCCH/8）与 CCCH相组合的独立专用控制信道（SDCCH/4）。

② 慢速随路控制信道（SACCH）它与一条业务信道或一条 SDCCH 联用，在传送用户信息期间带传某些特定信息，例如无线传输的测量报告。该信道包含下述几种：

- ✓ TCH/F 随路控制信道（SACCH/TF）。
- ✓ TCH/H 随路控制信道（SACCH/TH）。
- ✓ SDCCH/4 随路控制信道（SACCH/C4）。
- ✓ SDCCH/8 随路控制信道（SACCH/C8）。

③ 快速随路控制信道（FACCH） 与一条业务信道联用，携带与 SDCCH 同样的信号，但只在未分配 SDCCH 时才分配 FACCH，通过从业务信道借取的帧来实现接续，传送诸如“越区切换”等指令信息。FACCH 可分为如下几种：

TCH/F 随路控制信道（FACCH/F）。

TCH/H 随路控制信道（FACCH/H）。

除了上述三类控制信道外，还有一种小区广播控制信道（CBCH），它用于下行线，载有短消息业务小区广播（SMSCB）信息，使用像 SDCCH 相同的物理信道。

图1-12归纳了上述逻辑信道的分类。

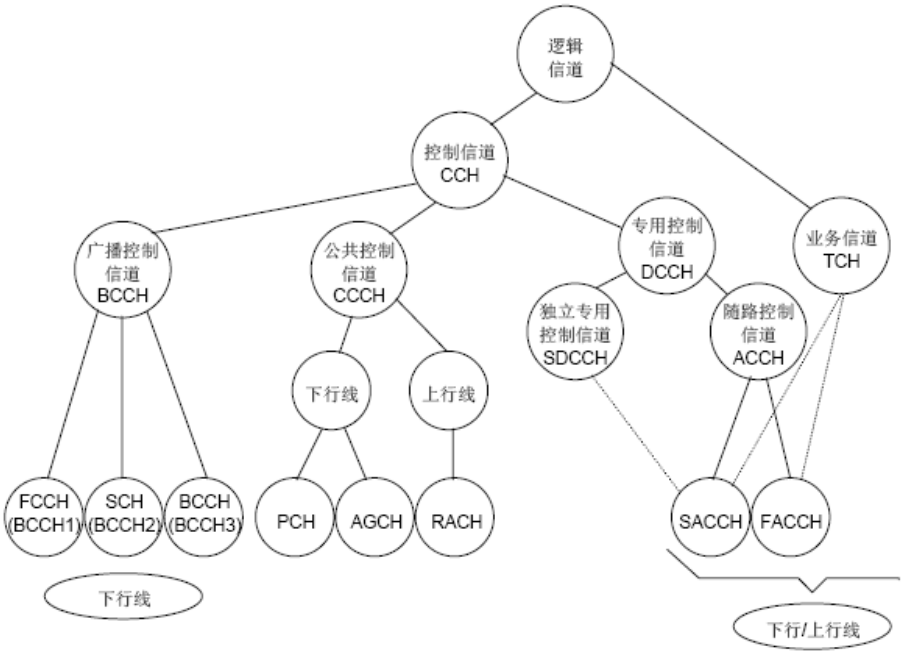


图 1-12 逻辑信道类型

三、信道组合

可能的信道组合有多种，例如：

- ✓ TCH/F+FACCH/F+SACCH/TF
- ✓ TCH/H+FACCH/H+SACH/TH 26—复帧
- ✓ FCCH+SCH+BCCH+CCCH
- ✓ FCCH+SCH+BCCH+CCCH+SDCCH/4+SACCH/C4
- ✓ BCCH+CCCH
- ✓ SDCCH/8+SACCH/C8 51—复帧

其中 CCCH=PCH+RACH+AGCH；上述组合的第 3 和第 4 种，严格地分配到小区配置的 BCCH 载频的时隙 0 位置上。

图1-13和图 14示出了全速率情况下，支撑广播、公共控制和业务信道的复帧格式。

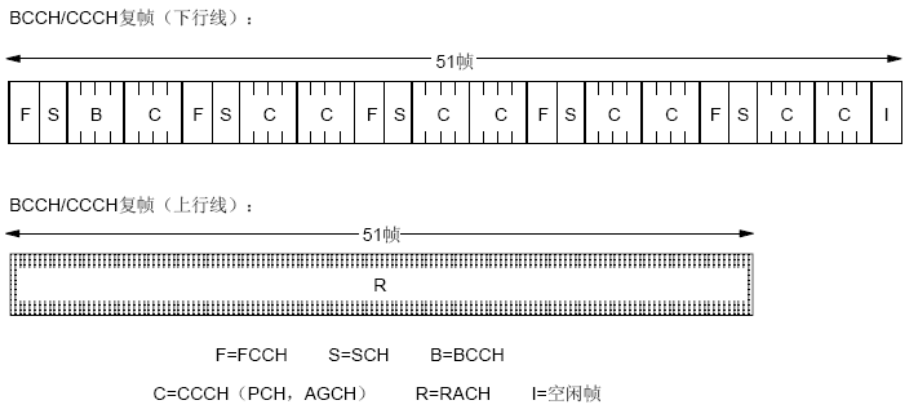


图 1-13 广播和公共控制信道的复帧

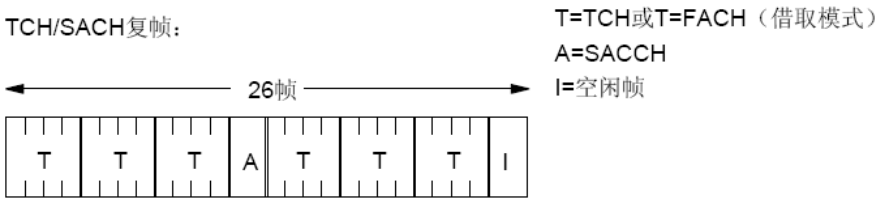


图 1-14 业务信道的复帧

四、信道的作用

下面我们通过一个最常用的例子：手机的上网过程，来看看系统是如何使用这些逻辑信道的。

手机开机、扫频

手机开机以后，立刻开始扫描网络，寻找可用的频点；

手机锁频（FCCH）

手机找到可用频点后，通过 FCCH 信道上的“频率校正信号”，锁定该频点频率；

手机同步（SCH）

手机锁定该频点后，通过 SCH 信道上的“同步信号”与该频点的 0 时隙同步；

手机接收系统消息（BCCH）

手机与该频点的0时隙同步后，就可以从该时隙获取该频点所在小区的系统消息。系统消息的内容很多，在这一步，手机主要通过系统消息确定该频点是否为该手机所在网络（移动、联通）的频点，如果是，手机将开始接入过程；如果不是，手机会放弃该频点，继续扫频，寻找其他频点。

手机（MS）向基站（BTS）发送“接入请求”消息（RACH）

手机向基站发出“接入请求”，要求基站给它分配一个 SDCCH 信道；

基站（BTS）向手机（MS）发送“接入允许”消息（AGCH）

如果基站有信令信道资源，就会向手机发送“接入允许”消息，并在该消息中告知手机所需的 SDCCH 信道号；

手机（MS）向基站（BTS）发送“位置更新请求”消息（SDCCH）

在“位置更新请求”消息中，手机会将其 IMSI 号码上报给 BTS，由 BTS 上报给 BSC－>MSC－>HLR，以检验手机用户的合法性；

基站（BTS）向手机（MS）发送“位置更新接受”消息（SDCCH）

如果通过检测，发现用户的 IMSI 是合法的，基站就会向手机发送“位置更新接受”消息； 如果发现用户的IMSI是非法的，基站就会向手机发送“位置更新拒绝”消息，并说明拒绝的原因；

手机显示网标，上网成功。（某些型号的手机，在“位置更新接受”消息下发之前，就把网标显示出来了，这时手机实际并未上网，即所谓的“假上网”）

其他信道的作用如下：

PCH（寻呼信道）用于手机做被叫，寻呼该手机的消息，通过该信道发送；

ACCH（随路控制信道，包括 SACCH 和 FACCH）用于手机在通话期间传送必要的信令消息，如切换。所谓的随路，就是在“话路”中传送信令消息，区别于只用于传送信令的 SDCCH 信道。

1.3.2 各逻辑信道的作用

1.3.2.1系统消息

1. 系统消息的作用

在 GSM 移动通信系统中，系统消息的发送方式有两种，一种是广播消息，另一种是随路消息

移动台在空闲模式下，与网络设备间的联系是通过广播的系统消息实现的。网络设备向移动台广播系统消息，使得移动台知道自己所处的位置，以及能够获得的服务类型，在广播的系统消息中的某些参数还控制了移动台的小区重选。

移动台在进行呼叫时，与网络设备间的联系是通过随路的系统消息实现的。网络设备向移动台发送的随路系统消息中的某些内容，控制了移动台的传输、功率控制与切换等行为。

广播的系统消息与随路的系统消息是紧密联系的。在广播的系统消息中的内容可以与随路的系统消息中的内容重复。随路的系统消息中的内容可以与广播的系统消息中的内容不一致，这主要是由于随路的系统消息只影响一个移动台的行为，而广播的系统消息影响的是所有处于空闲模式下的移动台。

2. 系统消息包含种类及内容

(1)系统消息 1

系统消息 1 为广播消息。

内容：

小区信道描述：为移动台跳频提供频点参考。

随机接入信道控制参数：控制移动台在初始接入时的行为。

系统消息 1 的剩余字节：通知信道位置信息。

(2)系统消息 2

系统消息 2 为广播消息。

内容：

邻近小区描述：移动台监视邻近小区载频的频点参考。

网络色码允许：控制移动台测量报告的上报。

随机接入信道控制参数：控制移动台在初始接入时的行为。

(3)系统消息 2bis

系统消息 2bis 为广播消息。

内容：

邻近小区描述；移动台监视邻近小区载频的频点参考。

随机接入信道控制参数：控制移动台在初始接入时的行为。

系统消息 2bis 剩余字节：填充位，无有用信息。

(4)系统消息 2ter

系统消息 2ter 为广播消息。

内容：

附加多频信息：要求的多频测量报告数量。

邻近小区描述：移动台监视邻近小区载频的频点参考。

系统消息 2ter 剩余字节：填充位，无有用信息。

(5)系统消息 3

系统消息 3 为广播消息。

内容：

小区标识：当前小区的标识。

位置区标识：当前小区的位置区标识。

控制信道描述：小区的控制信道的描述信息。

小区选项：小区选项信息。

小区选择参数：小区选择参数信息。

随机接入信道控制信息：控制移动台在初始接入时的行为。

系统消息 3 剩余字节：小区重选参数信息与 3 类移动台控制信息。

(6)系统消息 4

系统消息 4 为广播消息。

内容：

位置区标识：当前小区的位置区标识。

小区选择参数：小区选择参数信息。

随机接入信道控制信息。控制移动台在初始接入时的行为。

小区广播信道描述：小区的广播短消息信道描述信息。

小区广播信道移动分配信息：小区广播短信道跳频频点信息。

系统消息 4 剩余字节；小区重选参数信息。

(7)系统消息 5

系统消息 5 为随路消息。

内容：

邻近小区描述：移动台监视邻近小区载频的频点参考。

(8)系统消息 5bis

系统消息 5bis 为随路消息。

内容：

邻近小区描述；移动台监视邻近小区载频的频点参考。

(9)系统消息 5ter

系统消息 5ter 为随路消息。

内容：

附加多频信息：要求的多频测量报告数量。

邻近小区描述；移动台监视邻近小区载频的频点参考。

(10)系统消息 6

系统消息 6 为随路消息。

内容：

小区标识；当前小区的标识。

位置区标识：当前小区的位置区标识。

小区选项：小区选项信息。

网络色码允许：控制移动台测量报告的上报。

(11)系统消息 7

系统消息 7 为广播消息。

内容：

系统消息 7 剩余字节：小区重选参数信息。

(12)系统消息 8

系统消息 8 为广播消息。

内容：

系统消息 8 剩余字节：小区重选参数信息。

(13)系统消息 9

系统消息 9 为广播消息。

内容：

随机接入信道控制信息：控制移动台在初始接入时的行为。

系统消息 9 剩余字节：广播信道参数信息。

1.4 CDMA 协议导读

1.4.1 TIA41D 协议导读

1.4.1.1 协议介绍

本标准规定了 CDMA 数字蜂窝移动通信网的交换中心、位置寄存器、鉴权中心及短消息中心之间的移动应用部分的信令。其中包括了消息流程、消息和参数的定义及具体的编码。主要涉及 MSC、VLR、HLR、AC、SME 和 MC之间的接口，其中包括 B、C、D、E、H、M、N 和 Q 接口。

1.4.1.2 协议导读

协议内容可以分为下面几个大部分：

- ✓ 切换流程：主要介绍各种局间切换的成功和失败流程，以及切换过程中的重要消息说明。
  参 见 ： CHAPTER 2 “INTERSYSTEM HANDOFF INFORMATION FLOWS”
- ✓ 自动漫游流程：
  参见：CHAPTER 3 “AUTOMATIC ROAMING INFORMATION FLOWS ”分别介绍如下内容：
  (1)普通业务流程
  参见： CHAPTER 3 SECTION 5 “BASIC AUTOMATIC ROAMING SENARIOS”
  (2)补充业务流程
  参见：CHAPTER 3 SECTION 6 “VOICE FEATURE SENARIOS”
  (3)短消息流程
  参 见 ： CHAPTER 3 SECTION 7 “SHORT MESSAGE SERVICE SENARIOS”
- ✓ 操作、维护和管理：主要介绍 MAP 电路的操作、维护部分。
  参见：CHAPTER 4 “AUTOMATIC ROAMING INFORMATION FLOWS ”
- ✓ 消息、参数：消息功能及消息中携带内容说明；参数结构和功能说明。
  参见：CHAPTER 5 “SIGNALING PROTOCOLS”
  分别介绍如下内容：
  (1)消息
  参见：CHAPTER 5 SECTION 6.4 “MAP OPERATIONS”
  (2)参数
  参见：CHAPTER 5 SECTION 6.5 “MAP PARAMETERS”
- ✓ 流程伪码说明：
  参见：CHAPTER 6 “SIGNALING PROCEDURES”

1.4.2 IOS40 协议导读

1.4.2.1 协议介绍

本标准规定了 CDMA 数字蜂窝移动通信网的交换中心 MSC、BSC、PCF、PDSN 之间接口的流程、消息和参数。如图1-15所示：

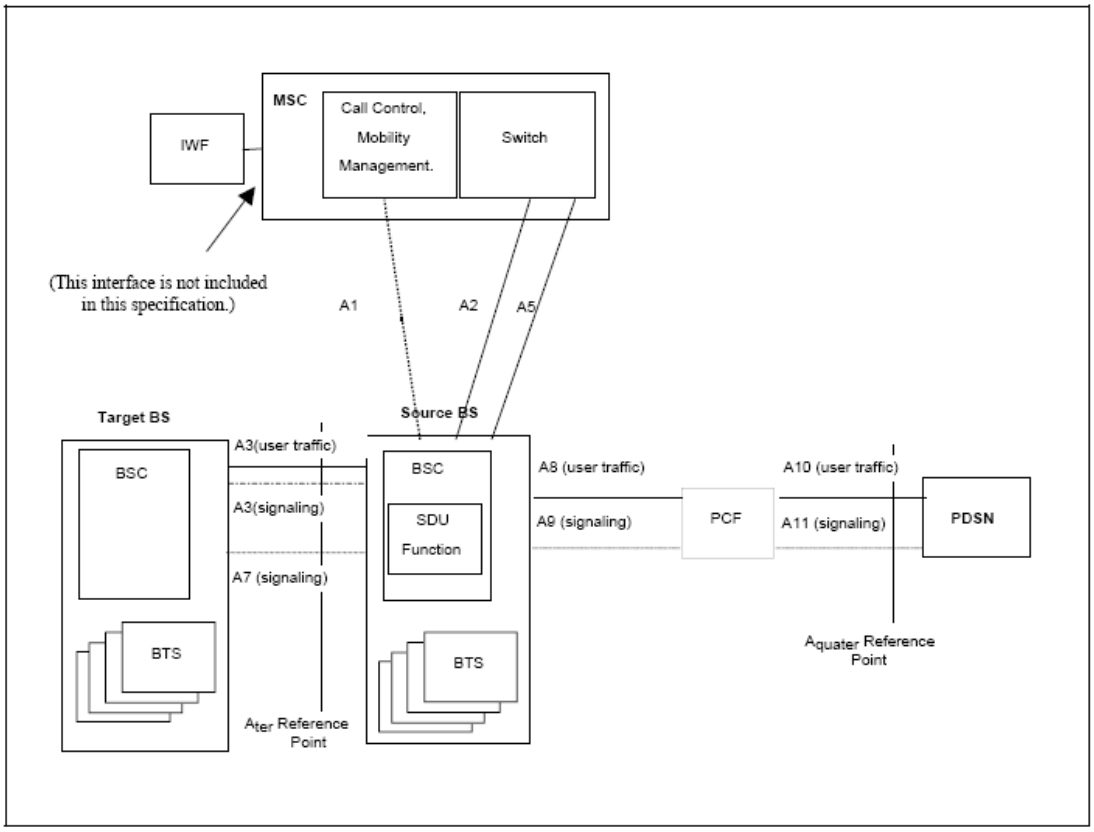


图 1-15 网络参考模型

1.4.2.2 协议导读

协议内容可以分为下面几个大部分：

- ✓ 普通呼叫、补充业务、数据业务：主要介绍各个流程中的消息交互过程。
- ✓ 参见：IOS400_Sect-2.0-2.6_991105
- ✓ 短消息、OTASP、PACA：主要介绍各个流程中的消息交互过程。
- ✓ 参见：IOS400_Sect-2.7-2.15_991105
- ✓ 切换、鉴权、位置管理、电路管理、传输层消息交互介绍：主要介绍切换、鉴权和位置管理流程以及电路管理部分。
- ✓ 参见：IOS400_Sect-3-5_991105
- ✓ 消息：消息功能及消息中携带内容说明。
- ✓ 参见：IOS400_Sect-6.1_991105
- ✓ 参数、定时器：介绍参数结构和功能，定时器时长和功能。
- ✓ 参见：IOS400_Sect-6.2_991105

1.4.3 智能业务相关协议

1.4.3.1 3GPP2 介绍

3GPP2 是开发 CDMA 的第三代移动通讯 3G 规范的组织，包括如何从 ANSI/TIA/EIA-41 网络到 3G 网络的演进。3GPP2 是 ITU 的 IMT-2000 的成员，为了加强 3GPP 和 3GPP2 的联系，ETSI 作为 3GPP2 的观察员，同样，TIA 作为 3GPP 的观察员。

3GPP2 分为五个技术工作组 TSG：

- ✓ TSG-A (A-Interface System)
- ✓ TSG-C (cdma2000)
- ✓ TSG-N (ANSI-41/WIN)
- ✓ TSG-P (Wireless Packet Data Interworking)
- ✓ TSG-S (Services and Systems Aspects) ，包括 ALL IP

1.4.3.2 智能协议介绍

CDMA 标准发展到一定阶段引入了无线智能网 WIN Wireless Intelligent Network) 的概念，WIN 采用智能网的原理在原来的网络功能模型中增加了智能网的功能模块:包括具有 SSF 功能的 MSC SCP IP SN 等功能实体；同时

规定了这几个功能实体之间的消息流程作为 ANSI-41 的一部分与移动应用部分 (MAP) 共同提供 WIN 业务 。 智能业务相关协议被包含 在TSG-N(ANSI-41/WIN)系列协议中，智能系列标准是作为 IS41D 规范的一个补充，所以从编写格式、目录组织和内容上均与其保持一致。

1. 协议介绍

3gpp2 发布规范\3gpp2\TSG-N\ N.S0013-0_v1.0.pdf(WIN Phase 1，即我们常说的 IS771)，本规范规定了 800MHz 数字蜂窝移动通信系统实现无线智能网(WIN)第一阶段时定义的智能业务种类和业务交互时不同系统间互操作的技术规范其中包括了消息流程消息和参数的定义及具体的编码。

3gpp2发布规范\3gpp2\TSG-N\ NS0018（TIA/EIA-41-D Pre-Paid Charging），本规范是基于 TIA PN-4287 的一个扩充规范，详细介绍了预付费业务流程。

3gpp2发布规范\3gpp2\TSG-N\3GPP2 N.S0004-0 v 1.0（即我们常说的IS848），WIN Phase 2，介绍了以下新增智能业务：

-- Freephone （被叫集中付费业务）

2. 协议导读

3gpp2 发布规范\3gpp2\TSG-N\ N.S0013-0_v1.0.pdf(WIN Phase 1，即我们常说的 IS771)

第一章：范围，主要对该文档的内容，适用范围和组织结构等方面进行概述。

第二章：无线智能网第一阶段的智能业务定义，主要内容为智能业务介绍；

第一阶段定义的智能业务有来话呼叫筛选业务和语音控制业务。

第二章：新增智能业务概述，介绍业务的操作维护以及新增业务与其他补充

业务的交互。

第三章：业务功能总体概述，各功能实体间消息交互图。

第四章：业务流程。规定了为支持新增智能业务，在 WIN 阶段1阶段，MSC/VLR，HLR，SCP 和 IP 之间需要增加的消息流程。

第五章：在 TIA-41D 的基础上更改的 MAP 消息和参数定义。

第六章：业务流程的处理伪码和操作定时器的值定义。

第七章：WIN 的网络参考模型。

3GPP2 N.S0018（TIA/EIA-41-D Pre-Paid Charging Revision: 1）本规范是基于 TIA PN-4287 的一个扩充规范，详细介绍了预付费业务。

第一章：范围，主要描述预付费业务的背景，概述该文档的内容，适用范围和组织结构。

第二章：预付费业务概述，介绍预付费业务的操作维护以及该业务与其他补充业务的交互。

第三章：业务功能总体概述，各功能实体间消息交互图，

第四章：预付费业务流程。规定了为支持预付费业务，在 WIN 阶段 1 的基础上，MSC/VLR，HLR，SCP 和 IP 之间需要增加的消息流程。

第五章：在 TIA-41D 的基础上更改的 MAP 消息和参数定义。

第六章：预付费业务流程的处理伪码和操作定时器的值定义。

第七章：网络参考模型。

3gpp2 发布规范\3gpp2\TSG-N\3GPP2 N.S0004-0 v 1.0：

第一章：范围，主要对于该文档的内容，适用范围和组织结构等方面进行概述。

第二章:新增智能业务概述,介绍业务的操作维护以及新增业务与其他补充业务的交互。

第三章：业务功能总体概述，各功能实体间消息交互图。

第四章：业务流程。规定了为支持新增智能业务，在 WIN 阶段 1 的基础上，MSC/VLR，HLR，SCP 和 IP 之间需要增加的消息流程。

第五章：在 TIA-41D 的基础上更改的 MAP 消息和参数定义。

第六章：新增业务流程的处理伪码和操作定时器的值定义。

第七章：网络参考模型。

第二章 网络体系结构和演进

2.1 WCDMA系统结构

UMTS(Universal Mobile Telecommunications System、通用移动通信系统)是采用WCDMA空中接口技术的第三代移动通信系统，通常也把UMTS系统称为WCDMA通信系统。UMTS系统采用了与第二代移动通信系统类似的结构，包括无线接入网 络 （ Radio Access Network ，RAN ） 和核心网络（ CoreNetwork， CN）。其中无线接入网络用于处理所有与无线有关的功能，而CN处理UMTS系统内所有的话音呼叫和数据连接，并实现与外部网络的交换和路由功能。CN从逻辑上分为电路交换域(Circuit Switched Domain, CS)和分组 交 换 域（ Packet Switched Domain, PS ） 。 UTRAN、CN与用户设备 （UserEquipment，UE）一起构成了整个UMTS 系统。其系统结构如图2-1所示。

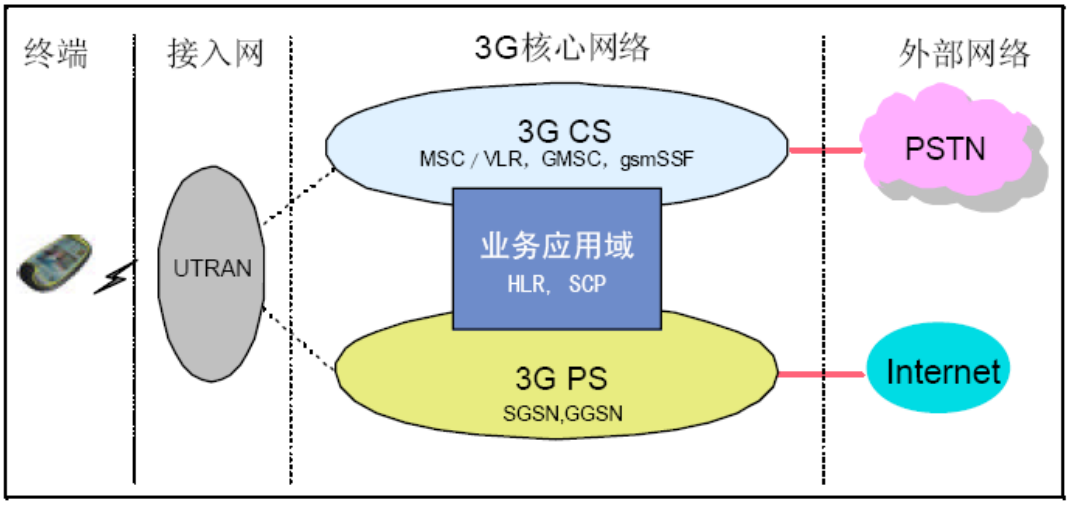


图 2-1 UMTS 的系统结构

从3GPP R99标准的角度来看，UE和UTRAN（UMTS的陆地无线接入网络）由全新的协议构成 ， 其设计基于WCDMA无线技术 。而CN 则采用了GSM/GPRS的定义，这样可以实现网络的平滑过度，此外在第三代网络建设的初期可以实现全球漫游。

2.1.1 UMTS系统网络构成

UMTS网络单元构成如图2-2所示。

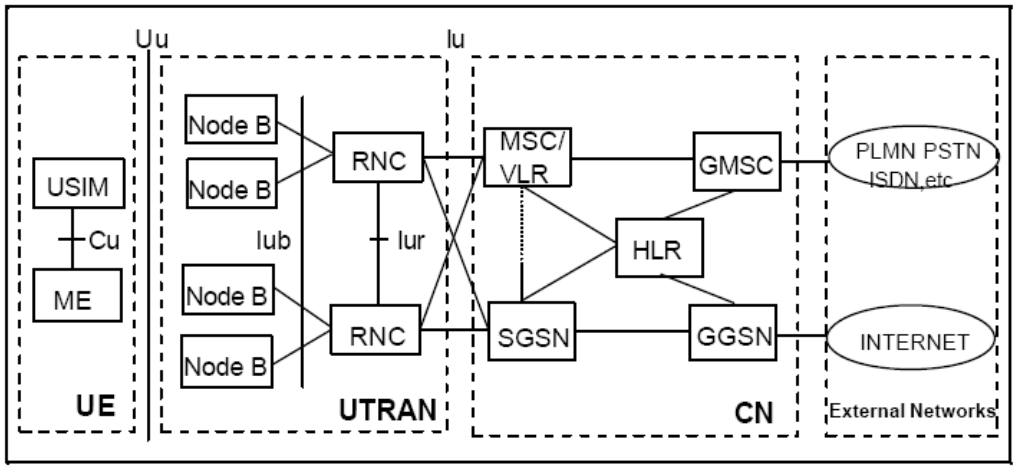


图2-2的UMTS系统网络构成示意图

从图3-2的UMTS系统网络构成示意图中可以看出，UMTS系统的网络单元包括如下部分：

1. UE （User Equipment）

UE是用户终端设备，它主要包括射频处理单元、基带处理单元、协议栈模块以及应用层软件模块等；UE通过Uu接口与网络设备进行数据交互，为用户提供电路域和分组域内的各种业务功能，包括普通话音、数据通信、移动多媒体、Internet应用（如E-mail、WWW浏览、FTP等）。

UE包括两部分：

ME（The Mobile Equipment），提供应用和服务

USIM（The UMTS Subsriber Module），提供用户身份识别

2. UTRAN（UMTS Terrestrial Radio Access Network，UMTS）

UTRAN ，即陆地无线接入网 ，分为基站 （ Node B）和无线网络控制器（RNC）两部分。

Node B

Node B是WCDMA系统的基站（即无线收发信机），包括无线收发信机和基带处理部件。通过标准的Iub接口和RNC互连，主要完成Uu接口物理层协议的处理。它的主要功能是扩频、调制、信道编码及解扩、解调、信道解码，还包括基带信号和射频信号的相互转换等功能。

Node B由下列几个逻辑功能模块构成：RF收发放大，射频收发系统（TRX），基带部分（BB），传输接口单元，基站控制部分。

RNC（Radio Network Controller）

RNC是无线网络控制器，主要完成连接建立和断开、切换、宏分集合并、无线资源管理控制等功能。具体如下：

(1) 执行系统信息广播与系统接入控制功能；

(2) 切换和RNC迁移等移动性管理功能；

(3) 宏分集合并、功率控制、无线承载分配等无线资源管理和控制功能。

3. CN（Core Network）

CN，即核心网络，负责与其他网络的连接和对UE的通信和管理。主要功能实体如下：

(1) MSC/VLR

MSC/VLR是WCDMA核心网CS域功能节点，它通过Iu_CS接口与UTRAN相连，通过PSTN/ISDN接口与外部网络（PSTN、ISDN等）相连，通过C/D接口与HLR/AUC 相连，通过E接口与其它MSC/VLR、GMSC或SMC相连，通过CAP接口与SCP相连，通过Gs接口与SGSN相连。MSC/VLR的主要功能是提供CS域的呼叫控制、移动性管理、鉴权和加密等功能。

(2) GMSC

GMSC是WCDMA移动网CS域与外部网络之间的网关节点，是可选功能节点，它通过PSTN/ISDN接口与外部网络（PSTN、ISDN、其它PLMN）相连，通过C接口与HLR相连，通过CAP接口与SCP相连。它的主要功能是完成VMSC功能中的呼入呼叫的路由功能及与固定网等外部网络的网间结算功能。

(3) SGSN

SGSN（服务GPRS支持节点）是WCDMA核心网PS域功能节点，它通过Iu_PS接口与UTRAN相连，通过Gn/Gp接口与GGSN相连，通过Gr接口与HLR/AUC相连，通过Gs接口与MSC/VLR，通过CAP接口与SCP相连，通过Gd接口与SMC相连，通过Ga接口与CG相连，通过Gn/Gp接口与SGSN相连。

SGSN的主要功能是提供PS域的路由转发、移动性管理、会话管理、鉴权和加密等功能。

(4) GGSN

GGSN（网关GPRS支持节点）是WCDMA核心网PS域功能节点，通过Gn /Gp接口与SGSN相连，通过Gi接口与外部数据网络（Internet /Intranet）相连。

GGSN提供数据包在WCDMA移动网和外部数据网之间的路由和封装。

GGSN主要功能是同外部IP分组网络的接口功能，GGSN需要提供UE接入外部分组网络的关口功能，从外部网的观点来看，GGSN就好象是可寻址WCDMA移动网络中所有用户IP的路由器，需要同外部网络交换路由信息。

(5) HLR

HLR（归属位置寄存器）是WCDMA核心网CS域和PS域共有的功能节点，它通过C接口与MSC/VLR或GMSC相连，通过Gr接口与SGSN相连，通过Gc接口与GGSN相连。HLR的主要功能是提供用户的签约信息存放、新业务支持、增强的鉴权等功能。

4. OMC

OMC功能实体包括设备管理系统和网络管理系统。

设备管理系统完成对各独立网元的维护和管理，包括性能管理、配置管理、故障管理、计费管理和安全管理等功能。

网络管理系统能够实现对全网所有相关网元的统一维护和管理，实现综合集中的网络业务功能，同样包括网络业务的性能管理、配置管理、故障管理、计费管理和安全管理。

5. External networks

External networks，即外部网络，可以分为两类：

电路交换网络（CS networks ）：提供电路交换的连接，象通话服务。

ISDN和PSTN均属于电路交换网络。

分组交换网络（ PS networks）：提供数据包的连接服务，Internet属于分组数据交换网络。

2.1.2 系统接口

从图3-2的UMTS网络单元构成示意图中可以看出，WCDMA系统主要有如下接口：

1. Cu 接口

Cu接口是USIM卡和ME之间的电气接口，Cu接口采用标准接口。

2. Uu接口

Uu接口是WCDMA的无线接口。UE通过Uu接口接入到UMTS系统的固定网络部分，可以说Uu接口是UMTS系统中最重要的开放接口。

3. Iu接口

Iu接口是连接UTRAN和CN的接口。类似于GSM系统的A接口和Gb接口。Iu接口是一个开放的标准接口。这也使通过Iu接口相连接的UTRAN与CN可以分别由不同的设备制造商提供。

4. Iur接口

Iur接口是连接 RNC之间的接口，Iur接口是UMTS系统特有的接口，用于对RAN中移动台的移动管理。比如在不同的RNC之间进行软切换时，移动台所有数据都是通过Iur接口从正在工作的RNC传到候选RNC。Iur是开放的标准接口。

5. Iub接口

Iub接口是连接Node B与RNC的接口，Iub接口也是一个开放的标准接口。 这也使通过Iub接口相连接的RNC与Node B可以分别由不同的设备制造商提供。

2.2 UTRAN的基本结构吧

UTRAN的结构如图2-3所示：

UTRAN包含一个或几个无线网络子系统（RNS）。一个RNS由一个无线网络控制器（RNC）和一个或多个基站（Node B）组成。RNC与CN之间的接口是Iu接口，Node B和RNC通过Iub接口连接。在 UTRAN内部，无线网络控制器（RNC）之间通过Iur互联，Iur可以通过RNC之间的直接物理连接或通过传输网连接。RNC用来分配和控制与之相连或相关的Node B的无线资源。Node B则完成Iub接口和 Uu接口之间的数据流的转换，同时也参与一部分无线资源管理。

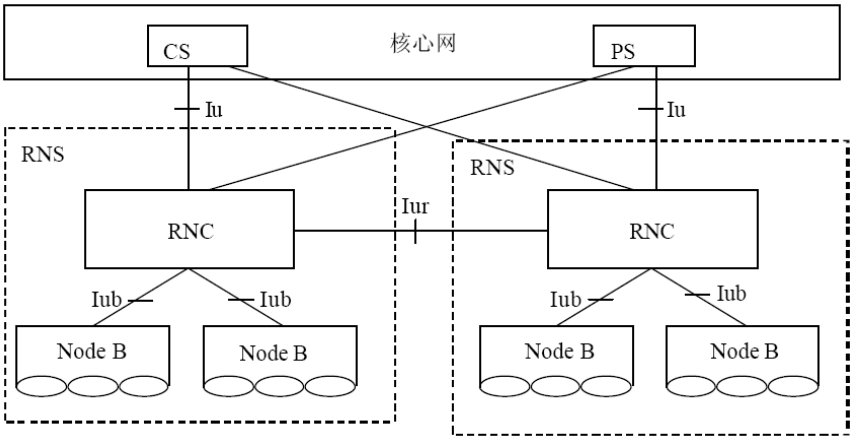


图 2-3 UTRAN 的结构

2.2.1 RNC（Radio Network Controller）

RNC，即无线网络控制器，用于控制UTRAN的无线资源。 它通常通过Ｉｕ接口与电路域（MSC）和分组域（SGSN）以及广播域（BC）相连（图上未标），在移动台和UTRAN之间的无线资源控制（RRC）协议在此终止。它在逻辑上对应GSM网络中的基站控制器（BSC）。

控制Node B的RNC称为该Node B的控制RNC（CRNC），CRNC负责对其控制的小区的无线资源进行管理。

如果在一个移动台与UTRAN的连接中用到了超过一个 RNS的无线资源，那么这些涉及的RNS可以分为：

服务RNS（SRNS）：管理UE和UTRAN之间的无线连接。它是对应于该UE的Iu接口（Ｕｕ接口）的终止点。无线接入承载的参数映射到传输信道的参数，是否进行越区切换，开环功率控制等基本的无线资源管理都是由SRNS中的SRNC（服务RNC）来完成的。一个与UTRAN相连的UE有且只能有一个SRNC。

漂移RNS（DRNS）：除了SRNS以外，UE所用到的 RNS称为DRNS。其对 应 的RNC则 是DRNC 。一 个 用 户 可 以 没 有 ， 也 可 以 有 一 个 或 多个DRNS。

通常在实际的RNC中包含了所有CRNC、SRNC和DRNC的功能。

2.2.2 Node B

Node B是WCDMA系统的基站（即无线收发信机），通过标准的Iub 接口和RNC互连，主要完成Uu接口物理层协议的处理。它的主要功能是扩频、调制、信道编码及解扩、解调、信道解码，还包括基带信号和射频信号的相互转换等功能。 同时它还完成一些如内环功率控制等的无线资源管理功能。它在逻辑上对应于GSM网络中基站（BTS）。

Node B由下列几个逻辑功能模块构成：RF收发放大，射频收发系统（TRX），基带部分（Base Band），传输接口单元，基站控制部分。如下图2-4所示：

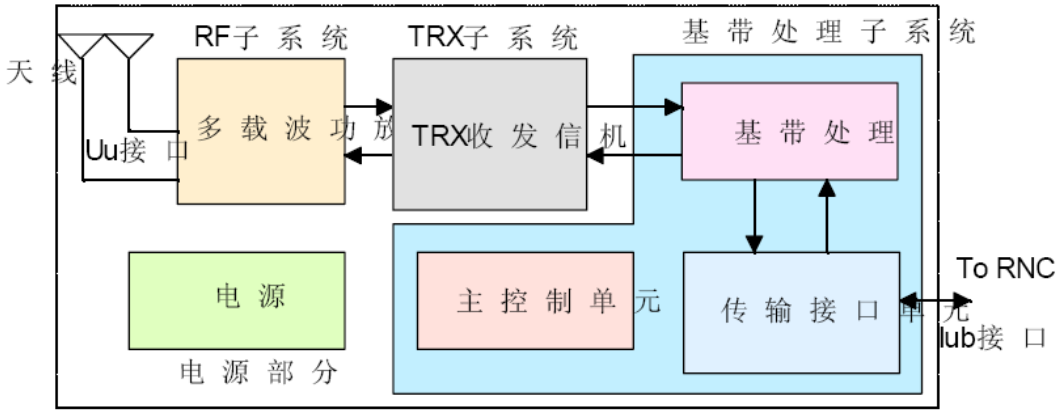


图 2-4 Node B 的逻辑组成框图

2.2.3 UTRAN各接口的基本协议结构

UTRAN各个接口的协议结构是按照一个通用的协议模型设计的。设计的原则是层和面在逻辑上是相互独立的。如果需要，可以修改协议结构的一部分而无需改变其他部分，如图3-5所示。

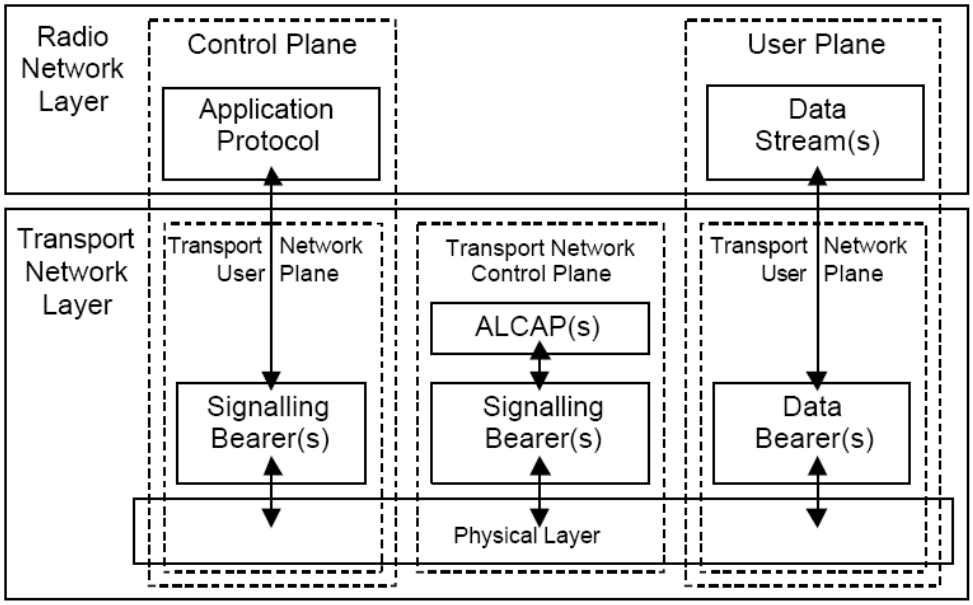


图 2-5 UTRAN 接口的通用协议模型

从水平层来看，协议结构主要包含两层：无线网络层和传输网络层。所有与陆 地 无 线接入网有关的协议都包含在无线网络层 ， 传输网络层是指被UTRAN所选用的标准的传输技术，与UTRAN的特定的功能无关。

从垂直平面来看，包括控制面和用户面。

控制面包括应用协议（Iu接口中的RANAP，Iur接口中的RNSAP，Iub接口中的NBAP）及用于传输这些应用协议的信令承载。应用协议用于建立到UE的承载（例如在Iu中的无线接入承载及在Iur、Iub中无线链路），而这些应用协议的信令承载与接入链路控制协议（ALCAP）

的信令承载可以一样也可以不一样，它通过O&M操作建立。

用户面包括数据流和用于承载这些数据流的数据承载。用户发送和接收的所有信息（例如话音和数据）是通过用户面来进行传输的。传输网络控制面在控制面和用户面之间，只在传输层，不包括任何无线网络控制平面的信息。它 包 括 ALCAP 协 议 （接入链路控 制 协 议 ）和 ALCAP所需的信令承载 。

ALCAP建立用于用户面的传输承载。引入传输网络控制面，使得在无线网络层控制面的应用协议的完成与用户面的数据承载所选用的技术无关。

在传输网络中，用户面中数据面的传输承载是这样建立的：在控制面里的应用协议先进行信令处理，这一信令处理通过 ALCAP协议触发数据面的数据承载的建立。并非所有类型的数据承载的建立都需通过ALCAP协议。如果没有ALCAP协议的信令处理，就无需传输网络控制面，而应用预先设置好的数据承载。ALCAP的信令承载与应用协议的信令承载可以一样也可以不一样。

ALCAP的信令承载通常是通过O&M操作建立的。

在用户面里的数据承载和应用协议里的信令承载属于传输网络用户面。在实时操作中，传输网络用户面的数据承载是由传输网络控制面直接控制的，而建立应用协议的信令承载所需的控制操作属于O&M操作。

综上所述，UTRAN遵循以下原则：

1） 信令面与数据面的分离；

2）UTRAN/CN功能与传输层的分离， 即无线网络层不依赖于特定的传输技术；

3） 宏分集（FDD Only）完全由UTRAN处理；

4）RRC连接的移动性管理完全由UTRAN处理。

2.2.4 UTRAN完成的功能

(1) 和总体系统接入控制有关的功能

准入控制

拥塞控制

系统信息广播

(2) 和安全与私有性有关的功能

无线信道加密/解密

消息完整性保护

(3) 和移动性有关的功能

切换

SRNS迁移

(4) 和无线资源管理和控制有关的功能

无线资源配置和操作

无线环境勘测

宏分集控制（FDD）

无线承载连接建立和释放（RB控制）

无线承载的分配和回收

动态信道分配DCA（TDD）

无线协议功能

RF功率控制

RF功率设置

(5) 时间提前量设置（TDD）

(6) 无线信道编码

(7) 无线信道解码

(8) 信道编码控制

(9) 初始（随机）接入检测和处理

(10) NAS消息的CN分发功能

2.2 GSM 数字蜂窝移动通信技术

GSM 的主要技术可用手机中话音的编码方法和收、发信过程来说明。

2.2.1GSM 话音处理和收、发信过程

一个 GSM 手机话音通道的功能框图如图 2-6 所示。

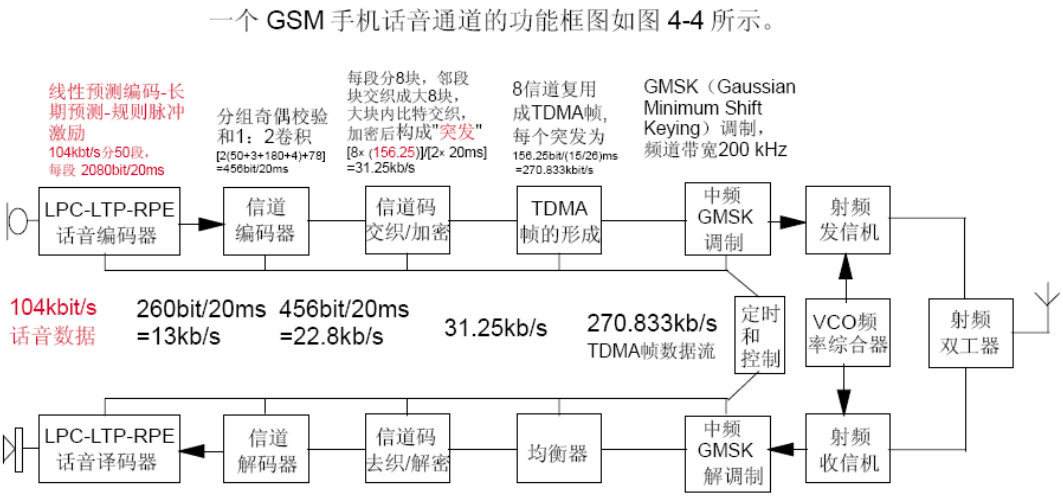


图 2-6 GSM 手机话音通道的功能框图

GSM 业务信道的带宽仅 200kHz，因此，其话音编码器的输出速率不能太高，被限制在 13kb/s 之内，甚至还可压缩一半或更多，以增加系统容量。

众所周知，无线信道的环境远比有线差，GSM 技术要在比 64kb/s 低数倍的编码速率和无线信道环境下，达到与有线电话相近的通话质量和安全、保密性，就必须采用诸如线性预测编码-长期预测- 规则脉冲激励（LPC-LTP-RPE）话音编/译码器、分组奇偶校验和 1：2 卷

积信道编/解码器、信道码交织和加密、TDMA 帧形成、高斯最小相移键控（GMSK）调制、VCO 频率综合、以及鉴权等许多先进技术。

话音编/译码器可在保证话音质量的前提下，利用相邻 20ms 话音码段内容变化甚微和有一定相关性的特点，大幅度压缩话音编码的速率。

分组奇偶校验和 1：2 卷积信道编/解码器对 20ms 码段中的话音码按重要程度分组，分别加入不同数目的奇偶校验码，并按卷积算法和 1：2 的比例增加冗余码， 以提高话音码的抗干扰能力，适应无线信道的多干扰环境。

无线电波会随机地在某些时段内严重起伏波动的现象称为衰落。衰落可能导致接收的信道码在一段时间内严重劣化或丢失。显然，如果劣化或丢失码段的风险落到一个用户的头上，将是难予承受的。因此，有必要分散风险，即让较多的用户来共同承担这一衰落风险。此外，无线信道易被窃听，加密是必须的。交织和加密是一种分散衰落风险和防窃听的手段。交织是把众多用户的话音码按给定的方式或算法进行混合，使一个时段内的信道码中包含众多用户的话音码，而不是一个用户的话音码，以共担衰落风险。加密是用收、发双方约定的一段伪随机码做加密码， 对信道码扰码（例如做模二加）。

形成 TDMA 帧是实现频分信道时分复用的重要步骤。

高斯最小相移键控（GMSK）调制是一种节省带宽的高效调制技术，以保证每信道仅占 200kHz 带宽。

VCO 频率综合技术可保证按频率规划及时和准确地调节压控本地振荡器的频率，使移动台能在任何蜂窝小区内工作。

鉴权则是保证合法用户接入和防止非法接入的重要手段。

GSM 手机的话音处理和收、发信过程可简单描述如下：

进入手机的模拟话音经 8kHz 抽样和模/数（A/D）变换，形成 13bit 均匀量化的 104kb/s 话音数据，并分成 20 ms 的小段，每段 2080bit。

线性预测编码-长期预测-规则脉冲激励(LPC-LTP-RPE)话音编码器将 104kb/s话音数据压缩 8 倍，生成 13kb/s 话音码，每 20ms 一小段，每段 260 bit。

信道编码器按各话音比特的重要性，把 20ms 话音码段分成重要(50bit)、比较重要(132bit)和不太重要(78 bit)三个分组。在前两个分组的尾部，分别加入 3、4 bit 奇偶校验码。然后，对这两分组共 189 bit 做 1：2 卷积，再加上未卷积的 78 bit 不重要比特分组，形成每 20ms 一小段，每段 456 bit，速率为 22.8 kb/s的 GSM 数字话音信道编码。

两次交织和加密的第一次把 456 bit /20ms 话音信道码小段分成 8 块，每块 57 bit，前后两个 20 ms 小段的块交织，组合成 8 个 114bit 的块，即{[8×(2×57)]/[2×20] = 22.8kb/s} 。

第二次把每个 114bit 块内来自两个 20 ms 话音码小段的 57bit 块相互进行逐比特交织，形成第二次交织后的新 114bit 块；再把这些 114bit 块和一个 114bit的加密码块作模 2 加，以实现加密。

加密后的 114bit 块再加进训练序列和头、尾比特及保护比特，形成 156.25bit的“突

发”(Burst)块，速率为{[8×(156.25)]/[2×20ms] =31.25kb/s } 。至此，每路话音将以“突发”的形式出现。不过这里的“突发”处于 TDMA 前，不是我们通常讲的空中接口 Um 上的“突发”。

8 个信道的“突发”经时分复用，构成一个 TDMA 帧。该帧中的每个“突发”就是 Um 接口上每路信号的一个传输单位，如图 2-7 所示。

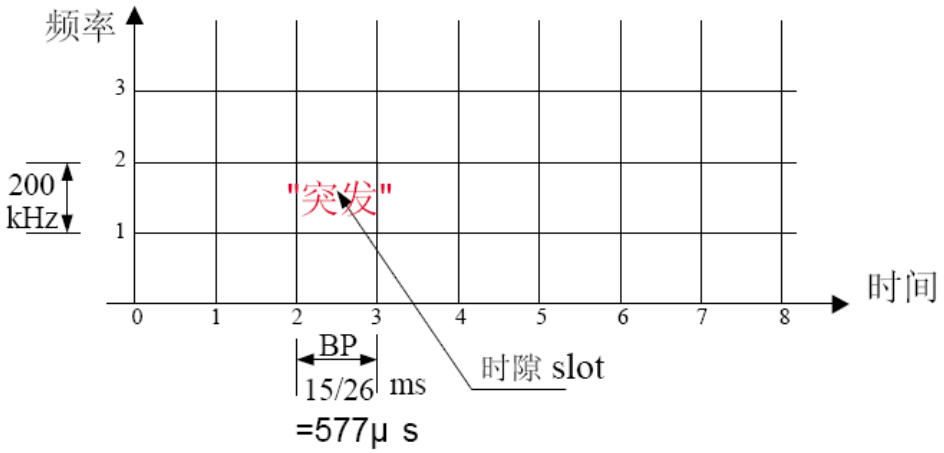


图 2-7 空中接口 Um 频道中的“突发”

空中接口中，每个“突发”包括信息比特、训练比特、尾比特和保护比特，共计 156.25 比特，占用一个持续时间 577μs (15/26ms)的时隙(slot)，信号速率为 156.25bit/577μs = 270.833kbit/s。

有 5 类“突发”，它们是正常“突发” (NB)、频率校正“突发”(FB)、 同步“突发”(SB)、随机接入“突发”(AB) 和虚拟“突发” (DB) 。正常“突发”(NB) 承载话音业务，虚拟“突发” (DB)的结构与正常“突发” 相同，但不承载有效信息，而是承载已规定的比特序列，用于在基站无信息下发时，做填充“突发”，其它“突发”提供控制信道。

8 个长度为 577μs 的“突发”组成一个帧长为 4.62 ms 的 TDMA 帧，支持业务信道和各种控制信道。由于业务信道和各种控制信道被错开配置在不同TDMA 帧的指定时隙内，因此，要若干个 TDMA 帧才能组成一个业务信道帧或控制信道帧，这若干个 TDMA 帧合称为复帧。

业务信道的复帧长度和控制信道的复帧长度不同，因此，有 26 复帧、51 复帧、超帧和超高帧等多种类型的复帧。26 个 TDMA 帧组成的长 120 ms 的复帧称为 26 复帧，用于业务信道及随路控制信道；51 个 TDMA 帧组成的复帧称为51 复帧，用于其它控制信道；同时把 26 复帧和 51 复帧的公倍数，即 26×51 = 1326 个 TDMA 帧的组合称为一个超帧；为实现加密，以 2048 个超帧构成一超高帧，帧长 3 小时 28 分 53 秒 760 毫秒，包含 2715648 个 TDMA 帧，并依顺序从 0 到 2715647 为超高帧中的 TDMA 帧编号，称为帧号。帧号在同步信道（SCH）中传送，供加密、跳频等算法使用。

270.833kbit/s 数据流对中频做 GMSK（Gaussian Minimum Shift Keying）调制，频道占用带宽 200 kHz。中频已调信号变成射频发送。

VCO 频率综合器支持方便地改变发射频率。

双工器使发信机和收信机共用天线，收信过程则与发信相反。

2.2.2 GSM 系统中的逻辑信道

GSM 系统的物理信道指每个频点 8 个时分信道。这些物理信道既要传输业务信号又要传输控制信号。由于业务信号和控制信号的多样性，每种信号要求有相应的逻辑信道支持，因此，如图 2-8 所示，在 Um接口上定义了一系列逻辑信道，以不同类型的“突发”传送业务信息和各种控制消息。逻辑信道是对物理信道通过不同的复帧结构和时隙配置作时间复用的结果，有业务信道和控制信道两大类和许多种。

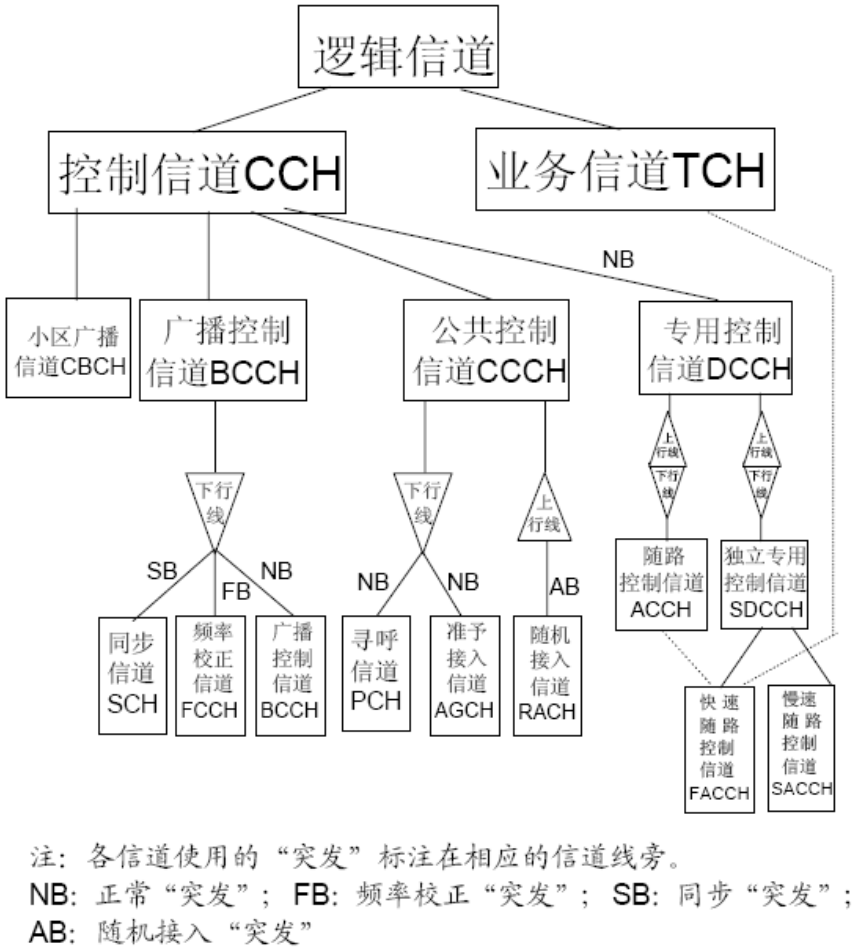


图 2-8 GSM 移动通信系统逻辑信道的种类

1. 承载话音或用户数据的业务信道(TCH)

- ✓ 全速率(22.8kbit/s)话音信道(TCH/FS)；
- ✓ 半速率话音信道(TCH/HS)；
- ✓ 9.6kbit/s 全速率数据信道(TCH/F9.6)；
- ✓ 4.8kbit/s 全速率数据信道(TCH/F4.8)；
- ✓ ≤2.4kbit/s 全速率数据信道(TCH/F2.4)

2. 控制信道(CCH)

包括广播信道(BCH)， 公共控制信道(CCCH)，专用控制信道(DCCH)和小区广播信道(CBCH)。

(1)广播信道（BCH）是从基站到移动台一点对多点的单向下行控制信道，用于向移动台广播各类信息，并可细分为：

- ✓ 频率校正信道 FCCH：使用 FB 型“突发”用于移动台的频率校正；
- ✓ 同步信道 SCH：发送移动台的帧同步(TDMA 帧号)和基站识别码；
- ✓ 广播控制信道 BCCH：用于发送 CCCH 号等小区信息，并使移动台预同步；

(2)公共控制信道（CCCH）是小区内各移动台共用，传送接入管理信令或其他信息的信道。这些信息以 NB 型“突发”映射到小区第一个频点的TS0 时隙。CCCH 包括：

- ✓ 寻呼信道 PCH： 一点对多点下行控制信道，用于基站寻呼（搜索）移动台；
- ✓ 随机接入信道 RACH：唯一映射到上行第一个频点 TS0 时隙的点对点信道，用于 MS 申请 SDCCH，响应寻呼和主叫/登记时的接入；
- ✓ 准予接入信道 AGCH：分配给成功接入的移动台的点对点下行 SDCCH信道

(3)专用控制信道（DCCH）是按需分配给移动台，与基站进行点对点双向

信令传输的信道，使用第一个频点的 TS1，每 102 个 TDMA 帧复用一次，其间，空闲 3 帧，且上、下行的 TS1 间有一定的时间偏移。DCCH 包括：

- ✓ 独立专用控制信道 SDCCH/8：用在分配 TCH 前的呼叫建立过程中传送登记、鉴权、越区切换等信令；
- ✓ 与 BCCH/CCCH 结合使用的独立专用控制信道 SDCCH/4；
- ✓ 与 SDCCH/8 随路的慢速随路控制信道 SACCH/C8：传送无线传输测量报告，实现功率控制；
- ✓ 与 SDCCH/4 随路的慢速随路控制信道 SACCH/C4；
- ✓ 与 TCH/F 随路的慢速随路控制信道 SACCH/TF；
- ✓ 全速率快速随路控制信道 FACCH/F：在未分配 SDCCH 时，用来传SDCCH 的信号，向移动台送挂机消息。

应当注意的是，未通话时，随路控制信道由 SDCCH 提供，而通话中，则包含（随）在业务信道内。

(4) 小区广播信道(CBCH)是用于下行方向广播小区短消息的信道，它使用和 SDCCH 相同的逻辑信道。

小区仅一个频点时，所有控制信道全映射到 TS0 时隙；有 2～3 个频点时，BCH/CCCH 用第一个频点的 TS0 时隙，DCCS 用第一个频点的 TS1 时隙；更多频点时，BCH/CCCH 除用第一个频点的 TS0 时隙外，还可用 TS2、TS4、TS6 时隙，DCCS 用第一个频点的 TS1 时隙。

SACCH/T 和 FACCH 与 TCH 组合进 26 复帧；各种 CCH 错开配置在不同帧的 TS0 时隙传送，并组合成 51 复帧。

2.2.3 GSM 移动通信系统的结构

GSM 通信系统由移动台(MS)、基站子系统（BSS）、网络子系统（NSS）、运行和管理系统（OMC）等功能单元组成。图 2-9 是符合 GSM 技术规范的华为公司 M900/1800 GSM 系统的结构示意图。让我们利用此图来说明 GSM移动通信系统的一般结构。

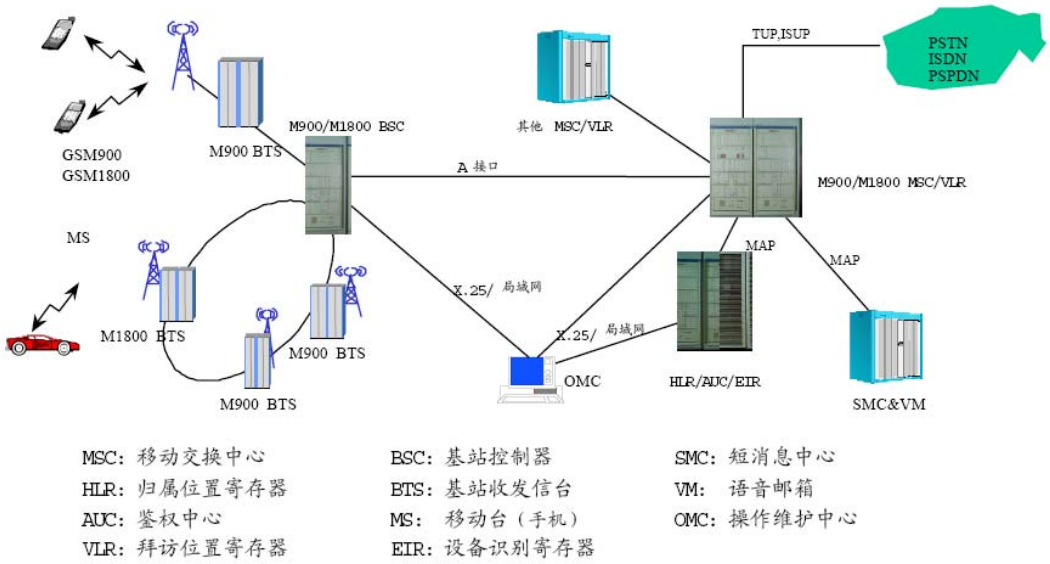


图 2-9 华为公司 M900/1800 GSM 系统的结构示意图

移动台（如车载台，手机等）包括发信机和具有分集接收功能的收信机及天馈线等单元。移动台与基站间的接口是开放的空中无线接口 Um，工作频率由与其连通的基站信道确定。

基站又称为基站收发信台（BTS）可以有多套工作于不同频率的收、发信机和共用的天线馈线等设备。每个基站的通信服务范围，称为无线小区（覆盖区）或蜂窝小区。无线小区的大小主要由频率配置、发射功率和基站天线高度等因素决定。基站是移动台和移动业务交换中心互连的桥头堡。

由于基站众多，为管理方便，在基站与移动业务交换中心之间引入基站控制器（MSC）。一个基站控制器管理和控制若干基站，它们之间的通道接口称为 Abis 接口。

基站控制器和所属的基站构成基站子系统（BSS）。基站控制器内通常包含码变换器/速率适配单元(TRAU)。该单元在话音业务中，完成 A 接口 64kb/sA 律 PCM 话音编码与 GSM 的 13kb/s RPE-LPT 声码间的转换，以实现 GSM用户和固定电话用户间的通信和 No.7 信令在 A 接口透明传输；在数据业务中，实现对数据信号的速率适配。

移动交换中心（MSC）与所辖各基站控制器的连接接口称为 A 接口。MSC 完成业务信道的交换和移动通信系统的集中控制与管理。移动业务交换中心通过 中 继 线 和 相 应 的接口和网关及PSTN/ISDN 和分组交换公用数据网（PSPDN）互通。

大家知道，固定电话端局可以根据与电话机有固定连接的用户线来识别用户，而移动交换中心不可能与移动台有这样的固定连接。为识别移动台，必须建立称之为归属位置寄存器（HLR）的数据库， 以存储其所辖用户手机或移动台的身份及业务数据并管理这些用户数据；此外，还要设置产生鉴权参数以认证移动用户身份的鉴权中心（AUC）和识别移动台

（手机）国际移动设备身份号(IMEI)的设备识别寄存器（EIR）。

为实现移动台（手机）的漫游，每个移动交换中心（MSC）要设置拜访位置寄存器（VLR）作为登录访问其辖区的漫游移动用户身份的动态数据库。MSC和 VLR 相互配合，为漫游用户做位置更新登记，向用户原地的 HLR 询问和存储其身份数据，并给该用户分配一个暂时移动台标识码（TMSI）。MSC、VLR常 放 在一 起， 记 为 MSC/VLR 。HLR 、 AUC、 EIR 也 可放在 一 起，记为HLR/AUC/EIR,并可以由若干 MSC 共用。在某些情况下,可不设 EIR。

网络子系统（NSS）主要包括移动交换中心（MSC）和访问位置寄存器（VLR）、归属位置寄存器（HLR）、鉴权（认证）中心（AUC）、和设备识别寄存器（EIR）。

若在网络子系统内设置短消息中心和语音信箱（SNC & VM）， 则可在话音和数据业务外，提供短消息和语音信箱业务。

运行和管理系统（OMS）包括操作维护中心（OMC）和操作维护终端（OMT），通过 X.25 分组交换网或局域网，管理各功能单元。

MSC 和 BSC 以及 BSC 和 BTSs 之间应采用光纤传输，建立光纤连接尚有困难时，可采用无线连接作为过渡。

2.2.4主要接口和功能

GSM 通信系统的主要接口如下：

1. 空中接口 Um

定义为移动台（手机）与基站收发信台（BTS）之间的无线通信接口，传递无

线资源管理，移动性管理、接续管理和业务等信息。为能横向兼容不同厂家的移动台（手机）产品，Um是一个开放型接口，即有公开的接口标准和规范。

2. A 接口

定义为移动交换中心与基站控制器之间的2.048Mb/s PCM 数字传输链路

（E1）接口，传递移动台管理、基站管理、移动性管理、接续管理和业务等信息。为能使不同厂家的移动交换中心和基站控制器横向兼容，A 是一个开放型接口，即有公开的接口标准和规范。

3. Abis 接口

定义为基站控制器（BSC）和基站收发信台（BTS）之间的通信接口。它不是开放型接口，而是BSS 内部接口，可由各厂家自定规范。Abis 接口支持

GSM 向用户提供的所有服务和无线资源分配及对 BTS 无线设备的控制。

4. No.7 信令接口

包括移动交换中心与各类寄存器间的 MAP（移动应用部分）接口和移动交换中心与 PSTN/ISDN 间的 TUP/ISUP（电话用户部分/ISDN 用户部分）接口等。

2.2.5 GSM 系统的编号计划

固定电话网的有线封闭环境使每部电话只需要一个号码即可，编号计划比较简单。

GSM 系统的空中接口使移动台（手机）的接入操作完全暴露在空间，为保证接入的保密性和合法性，并支持寻呼和漫游，移动台（手机）用户在国内实行等位长统一编码，且被称为移动用户国际 ISDN 号（MSISDN）的移动用户电话号码和网络识别用户以进行接续操作的号码，即国际移动用户识别码（IMSI）是不同的。

为了避免IMSI在空中被窃取，甚至可在用户进行位置更新登记时，由MSC/VLR 给该用户分配一个有时效的临时移动用户标识码（TMSI）来替代IMSI。

当漫游用户被呼叫时,该用户所在当前 MSC/VLR,还要为其分配一个引导入呼的号码(称为移动用户漫游号码 MSRN）。此外，移动台（手机）出厂时有一个唯一的国际移动设备识别码（IMEI）。

GSM 网络本身也有一套号码，例如，国家代码（CC），我国为 86； 国内目的地编码(NDC=N1N2N3)，邮电（中国移动）为 135～139，联通为 130、131；HLR 识别号 H1H2H3，其中，H1H2 由国家电信管理当局分给各省和直辖市，H3 则由省电信管理局规定；移动台国家代码（MCC），我国为 460；移动通信网代码（MNC），邮电（中国移动）为 00；联通为 01；标识某 PLMN 中HLR 的网络代码（NC），NC =N1N2N3H1H2H3；由 2 字节 BCD 码（16 进制格式 X1X2X3X4）构成的位置区码（LAC）；由 2 字节 BCD 码（16 进制格式 Y1Y2Y3Y4）构成的小区识别码（CI）；位长 3bit 的国家色码（NCC）和位长 3bit 的基站色码（BCC）等。以这些基本代码作为小单元，可组织和定义出一系列 GSM 网络子系统中有关设施或服务区的识别码。

这里，简要介绍几种主要的号码：

1. 按 IDSN 时代的编号计划(E.164)定义的移动用户国际 ISDN 号码(MSISDN)：

MSISDN(最长 15 位) ＝ CC ＋ NDC ＋ （0～9） ＋ SN

其中，CC：国家代码，我国为 86；

NDC=N1N2N3： 国内目的地编码(中国移动:135～139；联通:130,131)；

SN：用户号码，即某移动局 HLR 所辖用户号，SN=H1H2H3 ABCD；

H1H2H3 是 HLR 识别号，H1H2 由电信管理当局分配给各省和直辖市；

H3 由各省电信管理局规定；

国内有效号码（即常用的 11 位用户手机号）= NDC ＋ （0～9）＋ SN

= 139(～130) ＋（0～9）＋ H1H2H3 ABCD

例如：中国移动 D 市 H1H2H3 为 408 的 HLR 的可用 MSISDN 号范围为:

139(～135) 0 408 0000～ 139(～135) 9 408 9999，共计五十万号。

2. 按陆地移动台标识计划(E.212)定义的国际移动用户识别码(IMSI)：

IMSI(15 位) ＝ MCC ＋ MNC ＋ MSIN

其中，MCC：移动台国家代码，我国为 460；

MNC：移动通信网代码(中国移动：00；联通：01)

MSIN：移动台标识号码，MSIN＝H1H2H3 9 XXXXXX，

IMSI 存储于 HLR、VLR 和 SIM 卡中，在 Um 和 MAP 接口上传送，

例如：中国移动 D 市 H1H2H3 为 408 的 HLR 的可用 IMSI 号范围为:

460 00 408 9 000000～460 00 408 9 999999，共计一百万号

3. 临时移动用户识别码（TMSI）：

TMSI 是为避免 IMSI 暴露于空中被窃取而采用的一种保密措施。在用户位置更新成功后，由用户当前所在 MSC/VLR 分配给该用户替代 IMSI 的临时识别码，最大长度为 32bit，具体结构由运营商决定，并通常和位置区识别码（LAI）一起使用， 且至少在每次位置更新后改变。

4. 移动用户漫游号（MSRN）：

MSRN ＝ CC ＋ N1N2N3 ＋ 0 ＋ M1M2M3 ＋ ABC

其中，M1M2M3 是 MSC/VLR 的标识号或局号，也称为 LSP；

M1M2 与 H1H2 同；

例如：D 市某 MSC 的 MSC/VLR 号码 = 86 139 0 408

ABC：VLR 临时分配给被叫用户的漫游号；

例如：中国移动 D 市 861390408 局的 MSC/VLR 所能供分配的 MSRN 号码范围是：

86 139 0 408 000～ 86 139 0 408 999，共计一千号；

5. 国际移动设备识别码（IMEI）

IMEI ＝ TAC ＋ FAC ＋ SNR ＋ SP；

其中，TAC：由欧洲型号认证中心分配的允许类型码，长度 5 位；

FAC：由厂家编制的表示生产厂家和装配地的最后组装号，长度 2 位；

SNR：厂家制定的产品串号，长度 5 位；

SP： 备用的 1 位空号；

使用 IMEI 可防止非法移动台（手机）入网。也可暂时不使用 IMEI 以节省投资。

6. 按 SCCP 的陆地移动全球标题结构(E.214)定义的全局码(GT)：

GT(最长 15 位) ＝ CC ＋ NC ＋ MSIN * ≈ MSISDN

其中，NC：网络代码，NC =N1N2N3H1H2H3，用于标识某 PLMN 中的 HLR。MSIN* 表示略去 MSIN 后几位后的编码。

GT 由 IMSI 导出，为不使 GT 超长，可略去 MSIN 的后几位。

7. MSC/VLR 号码＝ CC＋ N1N2N3 ＋ 0 ＋ M1M2M3

例如：中国移动 D 市某局 MSC/VLR 的号码为 86 138 0 408

8. HLR 号码 ＝ CC＋N1N2N3＋H1H2H3＋0000

例如：中国移动 D 市某 HLR 的号码为 86 139 408 0000

9. 位置区识别码（LAI）

LAI＝ MCC ＋ MNC ＋ LAC

其中，LAC 是由 2 字节 BCD 码（16 进制格式 X1X2X3X4）构成的位置区码，总共有 65536 个位置区，X1X2 由电信管理当局统一分配，X3X4 由运营商自定。

LAI 主要用于识别一个漫游用户当前所在的 VLR 辖区，亦即 GSM 系统的一个寻呼区；

10. 全球小区识别码（CGI）

CGI＝ LAI ＋ CI

其中，CI 是由 2 字节 BCD 码（16 进制格式 Y1Y2Y3Y4）构成的小区识别码，由各 MSC 自定。

CGI 主要用于区分 LAI 中的小区；

11. 基站识别码（BSIC）

LAI＝ NCC ＋ BCC

其中，NCC 是位长 3bit（XY1Y2）的国家色码，X 表示运营商（中国移动 X=1；

中国联通 X=0），Y1Y2 由电信管理当局统一分配。

BCC 是位长 3bit 的基站色码， 由运营商自定。

BSIC 主要用于区别相邻国家（或省）间的相邻基站。

3.2.6 鉴权和加密功能

为保证移动台（手机）接入网络的合法性和安全性，每次呼叫和位置更新时

都要对用户进行鉴权，并对空中接口上的话音信号进行加密。在用户 SIM 卡中，存有用户的 MSISDN、IMSI、TMSI、LAI 等号码、鉴权钥Ki 和鉴权算法 A3、产生加密钥 Kc 的加密算法 A8、以及用户密码（PIN）等。

权鉴中心（AUC）是为用户生成用户鉴权三元参数组 RAND/SRES/Kc 的设备。AUC 中存有每个用户的 IMSI、鉴权钥 Ki 和鉴权算法 A3 以及产生加密钥 Kc的算法 A8。

AUC 中的随机数据发生器不断产生随机数 RAND。当需鉴权用户所属 HLR 代表该用户向 AUC 申请鉴权三元参数组时，AUC 用不断产生的随机数 RAND和该用户的鉴权钥 Ki 按 A3，A8 算法：

SRES(符号响应)=A3(RAND+Ki)； Kc =A8(RAND+Ki)

每次生成 5 套三元参数组 RAND/SRES/Kc 提供给相应的 HRL。

鉴权的流程如下：

当移动用户位置更新后开机或呼叫时，该用户当前所在 VLR 就向该用户归属的 HLR 索取 5 套三元参数组，并任选其中一套用于鉴权。VLR 把所选用那套三元参数组中的 RAND 发给该用户的 MS。

该 MS 以收到的 RAND 和自己的 Ki，通过 A3 和 A8 算法：

SRES(符号响应)=A3(RAND+Ki)； Kc =A8(RAND+Ki) ，

计算出 SRES 和 Kc，并把算得的 SRES 回送给用户当前所在的 MSC/VLR。

该 VLR 把 MS 回送的 SRES 与所选用三元参数组的 SRES 作比较，若两者相同，则鉴权通过；否则，就认为该 MS 为非法用户，并拒绝服务。

为对空中接口中的话音进行加密，用户当前所在 MSC/VLR 通过加密指令，令BTS 和 MS 各自用该用户的 Kc、TDMA 帧号和 A5 算法：

扰码或解扰码=A5(Kc+TDMA 帧号+加密令+音码)

对话音数据扰码和解扰码，以实现空中接口的话音加密。

2.2.7 GSM 呼叫流程描述

让我们以 D 市一手机用户在 G 市办事后漫游到 S 市做位置更新登记、主呼和被呼以及移动中通话等四种典型情况下 GSM 网络的运作流程来说明 GSM 移动电话的呼叫和通话过程。由于上节已介绍了鉴权的过程，本节的描述将略去呼叫中必有的鉴权环节。

1. 位置更新登记

设某用户 W 在 D 市购手机和开户，运营商（中国移动 D 市 408 局）分配给他手机的国内有效号码（MSISDN）为 13904087689，对应的国际移动用户识别码(IMSI)460004089123456 已烧录于 SIM 卡中，该用户自设开机密码（PIN）8888。

W 在 G 市办事时使用了手机，他离开 G 市时 SIM 卡中存储有 G 市的位置区识别码 LAI-G 和曾访问过的 G 市某 VLR（记为 PVLR）分配的临时移动用户识别码 TMSI-G。

当 W 漫游到 S 市首次开机时，如图 2-10 所示，其手机自动进行位置更新（移动台漫游登记）的流程如下：

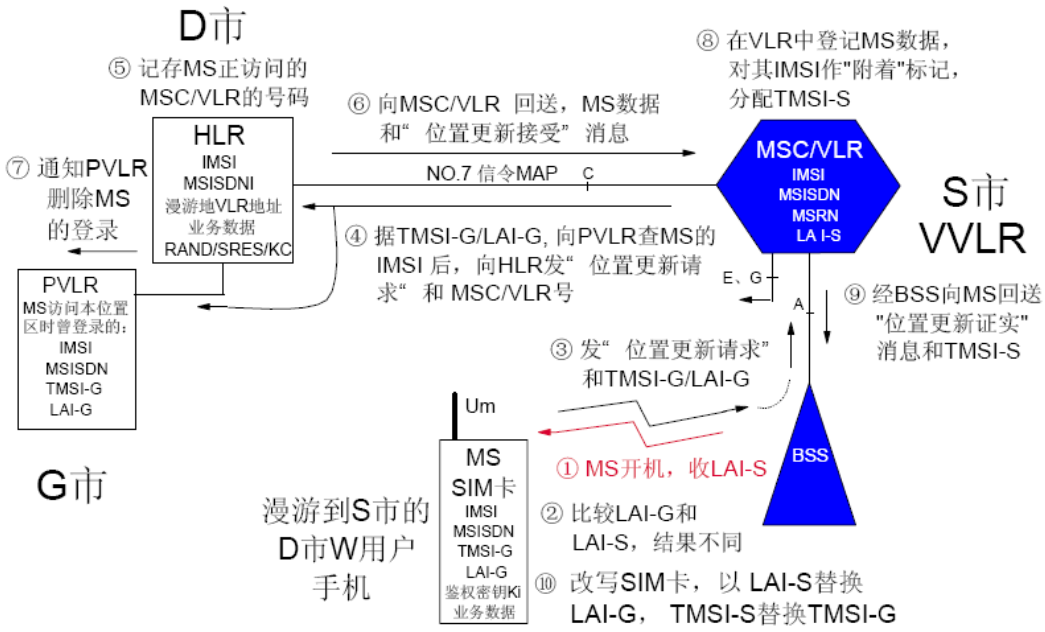


图 2-10 位置更新(移动台漫游登记)的流程

W 用户手机把收到S 市某基站广播的位置区识别码 LAI-S 与 SIM 卡存储的LAI-G 相比较，判知其已到达一个新位置区，就向该基站发“位置更新请求”和从前在 G 市做位置登记的记录 TMSI-G/LAI-G。

管辖该基站的 S 市某 MSC/VLR 是 W 手机当前正访问的 VLR（记为 VVLR）。它根据 TMSI-G/LAI-G 向 G 市 PVLR 查询 W 手机的 IMSI，从而获知 W 手机的 D 市 HLR 地址，于是在鉴权后向该 HLR 发查询 W 用户有关资料的“位置更新请求”和自己的 MSC/VLR（即 VVLR）号码。

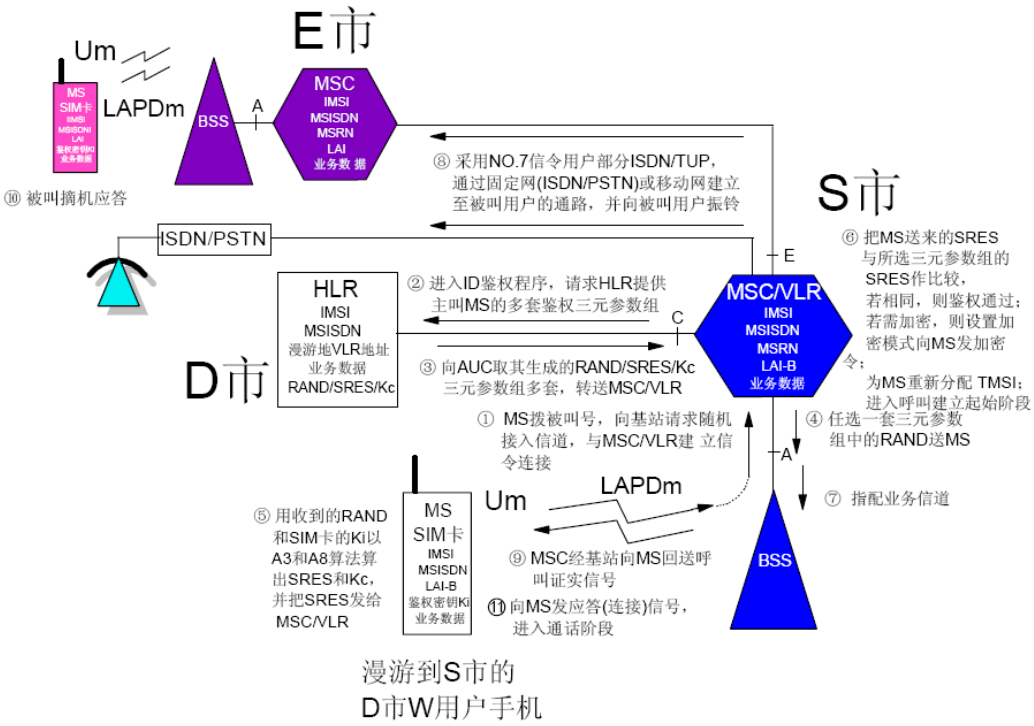


图 2-11　漫游移动台呼叫的流程

3. 漫游手机被叫

如图3-12 所示，某用户通过 F 市的移动网关局（GMSC）呼叫漫游到 S 市的D 市 W 用户，其呼叫流程如下：

F 市 GMSC 接收和分析由主叫所在网络转发的被叫手机号码后知被叫是 D 市W 用户，就向 D 市 HLR 查询 W 用户当前的位置。

D 市 HLR 已知 W 用户当前登记于 S 市 VVLR,遂向该 VLR 发“移动用户漫游号(MSRN)请求”。

S 市 MSC/VLR（即 VVLR）响应此请求，为 W 用户手机分配一个 MSRN（例如 861390220135），并回送给 D 市 HLR。

D 市 HLR 响应 F 市 GMCS 的查询，回告 MSRN。

F 市 GMSC 在 MSRN 的引导下，选择和建立至 S 市 MSC/VLR 通路。

S 市 MSC/VLR 通过基站寻呼 W 用户并建立连接，同时释放分配给 W 用户的MSRN。

W 用户手机振铃，用户摘机通话。

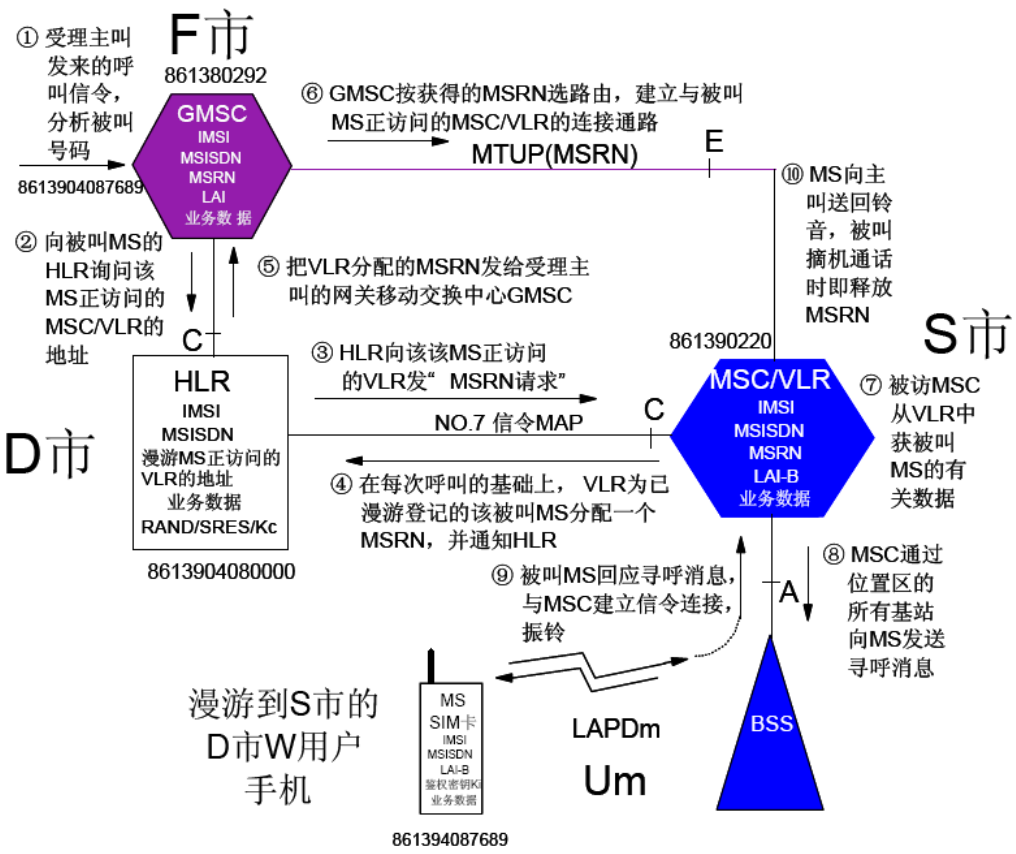


图 2-12　呼叫漫游中的移动用户的流程

4. 通话中移动用户信道的切换

为保证通信质量，网络酌情把正进行呼叫或通话中的 MS 从一个业务信道转换到另一个业务信道的过程称为切换。切换可在基站小区内同一或不同载频的时隙间、 同一 BSC 所属不同小区(基站)的信道间、同一 MSC 所属不同 BSC的信道间或不同 MSC 的信道间进行，即切换可在时隙、载频、小区、BSC或 MSC 之间发生。

MS 跨位置区在不同 MSC 的信道间切换的流程如图 2-13 所示：

移动中的 MS 对邻近小区 BTS 的功率、距离和话音质量进行测量，将结果报告给基站；经基站预处理后转送 BSC 进行计算并与切换门限比较，确定是否向 MSC-A 发“切换请求”；当需要切换时，MSC-A 请求 MSC-B 在其位置区LAI-B 备好无线信道，并在 MSC-A 和 MSC-B 间建立连接；然后，MSC-A 命令 MS 切换到 MSC-B 已备好的信道上，并在获 MS 的切换确认信息后，释放原占用的资源。

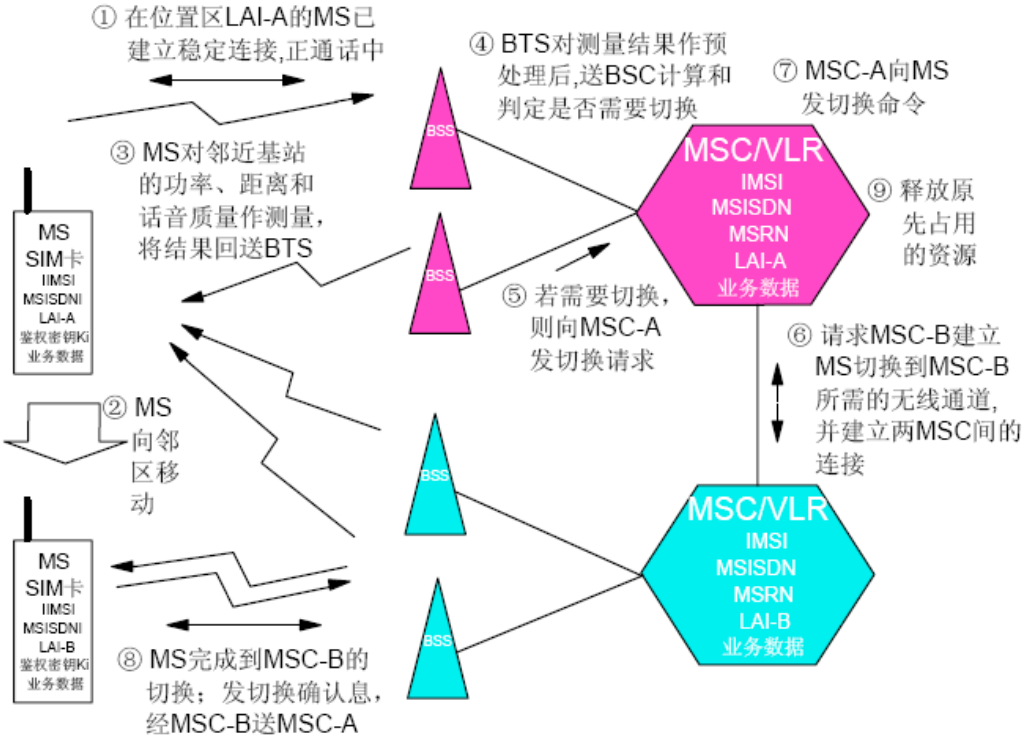


图 2-13 切换的基本流程

2.2.8 GSM 的业务种类

GSM 是以电路交换为基础的全数字化移动通信系统，能提供下列三类业务，但其带宽有限，数据业务的速率在 9.6kb/s 以下。

- ✓ 电信业务：电话、短消息、可视图文、消息处理系统、传真
- ✓ 承载业务：异步/同步双工数据、电路交换/分组交换
- ✓ 补充业务：号码显示/限制、呼叫前转、反向计费、多方会话、呼叫等待/保持/转换、计费通知、呼叫闭锁等

2.2.9 GSM 的特点

GSM 是在全球应用最广泛的第 2 代移动通信系统，有下列主要特点：

- ✓ 频谱效率高：采用声码器、信道编码、交织、均衡、蜂窝等技术，压缩
- ✓ 信道带宽和重复利用频率；
- ✓ 容量：比 TACS 系统高 3～5 倍，但仍不能满足需求；
- ✓ 带宽有限；
- ✓ 话音质量：与有线固定电话相当；
- ✓ 安全性：采用 A3(RAND+Ki)=SERS 鉴权和 A8(RAND+Ki)=Kc 加密，安全有保障；
- ✓ 移动性：用 SIM 卡可不带机漫游，全球漫游计费由 MoU 协调；
- ✓ 接口开放性：Um、A、是标准开放接口、Abis 是准开放接口；
- ✓ 互通性：与 PSTN、ISDN 以 No.7 信令互通。

- ✓ 随着电子商务的迅速发展和 Internet 广泛应用并日益深入人们的生活，以GSM为代表的 2G 系统在带宽、容量和数据传输方式等方面已不能满足移动（无线）上网的发展前景和需求，适应这个需求的第三代数字移动通信系统（3G）即将投入商用。

2.3 第三代数字移动通信系统（3G）

第三代移动通信系统（3G）被国际电信联盟 ITU 定名为 IMT-2000(国际移动通信2000年)，其目的在于以全球统一的频率和标准、实现全球漫游和提供各种宽带业务。IMT-2000无线传输使用2000MHz频段，两个工作频段为1885～ 2025MHz 和 2110～ 2200MHz，两段带宽总共 230MHz，其中，1980～ 2010MHz 和 2170～ 2200MHz 用于卫星通信。IMT-2000 数据传输速率要求在室内环境达到 2Mb/s，室外步行环境达到 384kb/s，室外车辆中达到 144kb/s，卫星移动环境中达到 96kb/s，能提供目前 PSTN/ISDN 和其他公网的大多数业务和有移动通信附加业务以及通用个人电信(UPT)业务。

IMT-2000 的功能模型及接口如图2-14 所示。

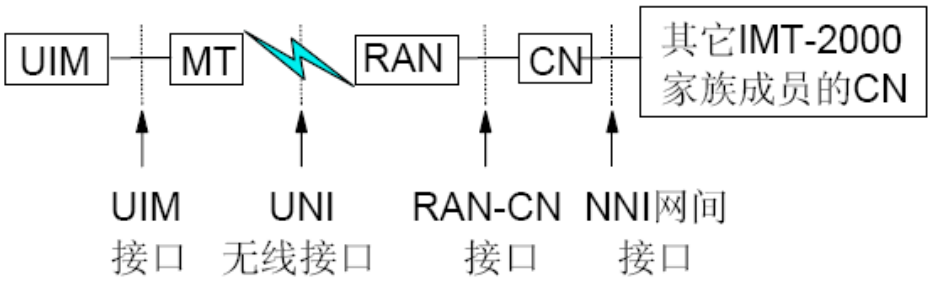


图 2-14 IMT-2000 的功能模型及接口

图中， UIM(User Identify Module)是用户识别模块，MT(Mobile Terminal)是移动终端，RAN(Radio Access Network)为无线接入网，CN(Core Network)表示核心网，各模块间的接口如图所示。

CDMA技术使用单一的频率，并可在整个系统区域内重复使用，小区复用系数为 1，各个用户采用一组正交码来区分，频率规划简单，频谱利用率高，容量大；在相同的频段内提供的系统容量比模拟 TDMA 系统大 10～ 20 倍，比TDMA 数字系统大 4～ 6 倍；使用功率控制技术、智能天线、干扰消除等技术后可进一步提高系统容量。因此，IMT-2000 技术方案基本上统一以宽带码分多址（CAMA）技术为核心。

IMT-2000 有如下特点：

全球性标准和系统(两大阵营：欧洲 GSM MAP 的 3GPP、美国 ANSI-41 的3GPP2)；

业务多样性(话音、数据、图象、多媒体、Internet 接入等）和可变性(按需分配带宽)；

高比特率分组数据，速率：144kb/s～2Mb/s；

兼容性：能与各种移动通信系统融合，互连互通，便于 2G 平滑演进，过渡到3G；

保密、安全、易操作。

2.3.1 IMT-2000 无线接口和无线传输技术方案

围绕 IMT-2000 的竞争十分急烈。截至 1998 年的 6 月底，提交 1TU 的第三代地面候选无线接口技术多达 10 种。最后，IMT-2000 无线接口规范(IMT.RSPC)接纳了 5 个无线接口，即 W-CDMA、cdma2000、TD-SCDMA、UWC136 和EP-DECT。W-CDMA 是欧洲和日本支持的方案，cdma2000 是由美国提出的方案，UWC-136 是基于 IS-136（D-AMPS）的 TDMA 方案，EP-DECT 是在欧洲 DECT 基础上稍加改进而来的，我国提出的 TD-SCDMA 采用 TDMA 和CDMA 混合接入方案。

IMT-2000 的标准和系统分为欧洲 GSM MAP 的 3GPP 和美国 ANSI-41 的3GPP2 两大阵营，已接纳的 5 个无线接口标准和无线传输技术（RTT，RadioTransmission Technology）方案尚待各国电信当局和运营商选用。

IMT-2000 无线接口规范(IMT.RSPC)5 个无线接口标准的名称是：

- ✓ IMT-2000 CDMA-DS(简称 IMT-DS)：UTRA FDD/WCDMA，
- ✓ IMT-2000 CDMA-TTD(简 称 IMT-TD)： TDCDMA/TD-SCDMA/UTRATDD
- ✓ IMT-2000 CDMA-MC(简称 IMT-MC)：CDMA2000 MC/WCDMAone
- ✓ IMT-2000TDMA SC(简 称IMT-SC)： UWC(Universal WirelessCommunication)-136
- ✓ IMT-2000 FDMA/TDMA(简称 IMT-FT)：DECT

其中，DS（Direct Spread）是直接扩频；MC（Multi-Carrier）是多载波； SC（Single Carrier）是单载波。

与这些接口相应的无线传输技术方案如表 2-2 所示。

方案	双工方式	空中接口	网络平台	技术基础	提交者
WCDMA (Wideband CDMA)	FDD/TDD	WCDMA	ATM/BISDN	全新，越过2G	日本：ARIB
UTRA	FDD/TDD				欧洲：ETSI
TDCDMA (Time Division CDMA)	TDD	GSM过渡	GSM过渡	2G/3G平滑过渡	西门子
TD-SCDMA (TD Syn. CDMA)	TDD	GSM过渡	GSM过渡	2G/3G平滑过渡	中国：CATT
WCDMAone	FDD	IS-95过渡	IS-95过渡		

UMTS：Universal Mobile Telecommunication System(通用移动通信系统)；
UTRA ：UMTS Terrestrial Radio Access（通用移动通信系统陆地无线接入）；

UTRA 是 ETSI 针对 3G(IMT-2000)提出的解决方案和欧洲的 3G 无线多媒体标准，与 TDCDMA 和 WCDMA 比较接近。因此，三者被融合为 W-CDMA（也写成 WCDMA）。于是，5 种无线接口标准的竞争实际上变成 3GPP 的 WCDMA和 TD-CDMA 和 3GPP2 的 cdma2000 两大阵营，三大标准的竞争。特别是WCDMA 和 cdma2000 的竞争。

2.3.2 CDMA 技术和三大标准的评述

大家知道，信源码的功率主要集中在相对较窄的频谱宽度内。CDMA 采用扩频技术，以频谱很宽的扩频码对信源码进行扩频处理，使信源码的频谱扩展数十到数百倍，扩频后的信号功率被分散在很宽的频内，各频率分量的功率也按相应倍数下降。

不同扩频码的频谱分布不同，因此，不同用户的信源码经各自对应的扩频码扩频后，可以叠加在一起，而各频率分量的功率并无明显增加。多用户扩频信号的集合信号类似于“白噪声”，具有比较均匀分布的功率密度谱，并可采用适当的调制方式共用一个频分或时分信

道由空中接口发送出去。

扩频码系列是具有一定长度和码片速率的正交特征码系列。所谓正交，好比“一把钥匙开一把锁”。“扩频”已把一个个用户的信源码用特地为各用户定制的“扩频码锁”锁进了称之为信道的“公用货柜”的一个个小抽屉中。

想要接收某用户的信息，只能使用为该用户特配的扩频码做“钥匙”，才能打开装有那个用户信源码的小抽屉。

因此，CDMA 是采用扩频技术使多用户同时共享包括频谱、时间、功率、空间和特征码等要素的无线资源，实现多址联接的通信方式。

CDMA 与 FDMA、TDMA 的最大不同点在于它能统计复用无线资源，即所有CDMA 用户动态共享频率、时间和功率资源，而仅依靠特征码来区分各用户。

当前，CDMA 有第二代窄带 CDMA 和第三代宽带 CDMA 两类标准和系统。

第二代窄带 CDMA 系统以美国 Qualcomm 公司推出的码分多址(CDMA)直接扩频技术为代表，有关标准是 TIA/EIA IS-95，IS-95A，IS-96，IS-97，IS-98，IS-99。

IS-95(CDMA)系统的工作频段，基站为 869～894MHz，移动台为824～849MHz；双工间隔 45MHz；而射频载频间隔为 1250kHz，比 D-AMPS 的30kHz 和 GSM 的 200 kHz 宽得多。

在 IS-95(CDMA)系统中,不同的用户具有不同的特征码,频率规划比较简单,但 CDMA 系统覆盖和容量覆盖需要很好的协调，如果某个小区业务负载过重则会导致覆盖范围减小，甚至会出现覆盖盲区。在 IS-95 中，采用了软切换、快速功率控制等技术，无线资源管理和接入控制比较复杂。

IS-95（CDMA）具有抗干扰能力强、系统容量大和无线资源利用率比较高等优点，并能与 AMPS 系统兼容。中国联通正在建设这种 CDMA 网络。

第三代 CDMA 系统采用了更宽的带宽、更高的码片速率。在提交给 1TU 有关IMT-2000 的方案中，几乎所有的方案使用的带宽在名义上都是 5MHz，可提供 2Mb/s的数据速率。宽带 CDMA 系统本身具有频率分集作用，比窄带 CDMA系统能更好地克服多径衰落。改善通信质量和载波特性。

第三代 CDMA 系统中一般采用时分复用或码分复用方案来提供多业务（多速率）服务。即把不同速率和业务质量（QoS）要求的业务完全分割开来，独自编码和交织，以时分或码分复用方式映射到不同物理数据信道中，并对各个业务信道进行单独控制，灵活应用。

第三代 CDMA 一般采用对称 WQPSK（balanced QPSK）和双信道 QPSK（dual-channel QPSK）扩频调制。

收信方面，第三代 CDMA 上行链路采用相干检测技术，收信性能改善 3dB 左右。下行链路采用比第二代 CDMA 更快的功率控制技术，能更好地克服多径衰落的影响，并通过分集接收来改善下行链路的性能。上行和下行链路都采用了多用户检测（MUD）技术，以充分挖掘无线信道潜力，增加系统容量。

此外. 第三代 CDMA 还采用了智能天线技术。智能天线是一种多波束、用户跟踪、自适应定向的天线阵。当用户一定时，可以减少其它用户信号的干扰。

下行链路中使用附加导频来使接收机能对信道进行评估。

对业务密集的热点地区，第三代 CDMA 采用分层小区的方案：在微蜂窝或微微蜂窝上面叠加一个宏蜂窝，不同的蜂窝使用不同的频率。

到目前为止,基于 CDMA 的第三代移动通信系统主要有两种方案:同步方案和异步方案。其主要区别就是基站间是否需要同步。在提交给 ITU 的方案中，ETSI、ARIBTTA II 的

WCDMA 属于异步网络方案；美国 TR45.5 的cdma2000 是同步方案。

cdma2000 的核心是由 Lucent、Motorola、Nortel 和 Qualcomm 联合提出的Wideband cdmaOne 技术。cdma-2000 采用 MC-CDMA（多载波 CDMA）多址方式，可支持话音、分组、数据等业务，并且可实现 QoS 的协商。对于射频带宽为 N X 1.25MHz 的 cdma2000 系统，采用多个载波来利用整个频带。

cdma2000 的功率控制有开环、闭环和外环三种方式，还可采用辅助导频、正交分集、多载波分集等技术来提高系统的性能。

WCDMA（UTRA FDD）的核心网基于 GSM-MAP，可有效支持电路交换业务（如 PSTN、ISDN 网）、分组交换业务（如 IP 网）和其它宽带业务。它的灵活的无线协议可在一个载波内对同一用户同时支持话音、数据和多媒体业务。

通过透明或非透明传输块来支持实时、非实时业务。业务质量可通过对诸如延迟、误比特率、误帧率等参数的调整来改善。

WCDMA采用DS-CDMA多址方式，码片速率是3.84Mcps，载波带宽为5MHz。系统不采用 GPS 精确定时，不同基站可选择同步和不同步两种方式，可以不受 GPS 系统的限制。在反向信道上，采用导频符号相干 RAKE 接收的方式，解决了 CDMA 中反向信道容量受限的问题。

WCDMA 采用精确的包括基于 SIR 的快速闭环、开环和外环等多种功率控制方式，可有效满足抵抗衰落的要求。

WCDMA 还可采用一些先进的技术，如自适应天线（Adaptive antennas）、多用户检测（Multi-user detection）、分集接收（正交分集、时间分集）、分层式小区结构等，来提高整个系统的性能。

Cdma2000 和 WCDMA 都是采用 FDD 方式的系统。

我国提出的第三代移动通信国际标准——TD－SCDMA（时分双工同步码分多址）标准是采用 TDD 方式的系统。它已成为国际电信联盟标准，与 WCDMA和CDMA2000并列为第三代移动通信世界三大主流标准之一。TD-SCDMA标准也属于 3GPP 的 UMTS。

采用 TDD 方式的系统，特别是 TD-SCDMA，在同样满足 IMT-2000 要求的前提下，具有如下特点：

能使用各种频率资源，不需要成对的频率，适用于不对称的上下行数据传输速率，特别适用于 IP 型的数据业务；

上下行工作于同一频率，对称的电波传播特性使之便于使用诸如智能天线等新技术，达到提高性能、降低成本的目的；

系统设备成本较低，将可能比 FDD 系统低 20%-50%。

不过 TDD 系统比 FDD 系统也有一些不足之处，主要表现在如下两个方面：

- ✓ 终端的移动速度只能在 120km/h 以内，而 FDD 系统可达到 500km/h。
- ✓ 由于要考虑上下行时隙的保护时间，小区半径有所限制，TD-SCDMA系统的最大小区半径为 10km 左右，而 FDD 系统的小区半径完全由发射功率和传播条件确定，没有限制。

cdma2000 要依赖全球定位系统（GPS）实现同步，而 GPS 是由美国控制的军用技术，且此方案与目前在全球获得广泛应用的 GSM 系统不兼容，可能难被其他国家接受。

欧洲国家深受 GSM 巨大成功的鼓舞，极力推崇 W-CDMA 标准。

我国可能采用 W-CDMA 和 TD-SCDMA。

目前，多数人预测第三代移动通信网络的前景将是几种标准共存互补的网络。例如以 FDD 技术的无线基站用来完成全球无缝覆盖， TDD 技术的基站用来在城市人口集中地区提供高密度和容量的话音、数据及多媒体业务。

这可以从未来 10 年内我国对第三代移动通信需来的技术和经济评估中看出一些端倪。

若未来 10 年内，我国第三代移动通信用户按 2 亿户来考虑，将各种数据和话音业务合并折算的每用户平均话务量为 0.05Erl。设每个基站占用 5MHz 带宽，且 FDD 基站和 TD-SCDMA 基站的容量基本相同，每基站大约支持 120Erl，即可提供 5,000 用户(留 20%供越区切换使用)。考虑到我国用户的 80-90%在大中城市，即 90%的业务集中在大中城市，为实现全国的无缝覆盖,3G 网络要设 8,000 至 10,000 个业务量较低的 FDD 基站(每个基站的覆盖半径为 5 至30 公里),并另外增加大约 40,000 至 50,000 个 TDD 基站来解决城市及郊区高用户密度的业务需求。

3G 核心网的价格和无线接入网所使用的技术无关。而基站的价格，目前，我们有把握地说在相同容量下，TD-SCDMA9（TDD）基站价格将比 GSM 基站低 20%， 而 WCDMA 的 FDD 基站价格估计不可能比 GSM 低。因此，可认为相同容量的 TD-SCDMA 基站比 FDD 基站便宜 30%至 50%。

在上述考虑下,用 FDD 作全国覆盖而用 TDD 来提供城市的话务量(10,000 个FDD 基站和 40,000 个 TD-SCDMA 基站)比全部用 FDD 基站则至少将节省 50至 100 亿美元的设备投资。而且，使用 TDD 系统，所占用的频率资源比使用FDD设备少一半，可为运营商和用户节省一半的频率占用费。此外，对不对称的数据业务，TDD 系统的效率更高，必将为运营商和用户带来更大的利益。

因此，我国的 TD-SCDMA 标准有很好的应用前景。

2.3.3 3G 的关键技术

3G 方案中采用的主要关键技术有：

- ✓ 多载波调制：将一个信道带宽分成 N 个载波作自适应多进制调制，载波数随信道速率增减，进制数随信道衰落和忙闲调节；
- ✓ 多址技术：灵活的多载波信道和按需分配带宽的 CDMA 技术；
- ✓ 软件无线电：综合采用数字信号处理，微电子和软件等技术的硬件平台，可通过加载软件来实现硬件升级，使系统获得新功能；

- ✓ 智能天线：赋形天线的波束能跟踪用户，以降低发射功率，减小干扰；
- ✓ ATM：实现宽带分组交换核心网；
- ✓ 智能网技术：支持开发新业务。

2.3.4 IMT-2000 系统的基本结构

IMT-2000 系统由移动台 MS、一系列基站收发信台（BTS-A、BTS-B 等）和基站控制与移动交换综合仿真设备 MCC-SIM 构成，如图2-15 所示。

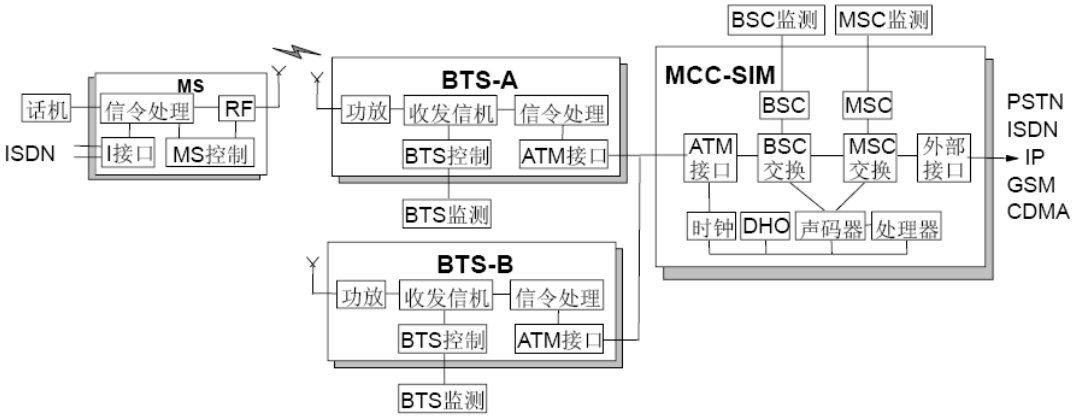


图 2-15 IMT-2000 系统的基本结构

移动终端 MS 提供话音业务和外部高速数据接口;基站收发信台(BTS)实现IMT-2000 的无线接口功能;综合 BSC 和 MSC 功能的仿真设备 MCC-SIM 提供无线链路控制、交换控制、呼叫控制和外部接口等功能，以及 HLR、VLR、AUC 的功能。

2.4 2G 向 3G 过渡的策略和方案

在 2G 已广泛应用并不断扩展和 3G 尚待试点推广的背景下,为适应和满足用户当前在较高速率数据业务和移动办公等方面的需求和充分发挥2G 网络覆盖广，普及面大的优势，各种 2G 向 3G 过渡的策略和方案应运而生，并通常把它们简称为二代半（2.5G）技术或方案。

GSM 的电路型数据基本速率为 9.6kbps，如果采用高速电路交换（HSCSD）技术，数据速可提高到 57.6kbps，且易实现，但其呼叫建立时间长和多时隙捆绑的工作方式会造成频谱资源的紧张与浪费，因而生命周期较短，难以满足国内 GSM 市场的发展需求。

EDGE（Enhancde Data Rates for GSM Evolution，GSM 演进的增强型数据率）是欧洲电信标准协会（ETSI）提出的使 GSM 数据传输速率扩展到 384 kb/s的技术，故亦称为 GSM-384。这一速率达到了第三代移动通信系统数据传输速率的下挡范围，能为用户提供许多 3G 业务，但需要的软硬件投资很大，限制了它的大规模发展。

GPRS（通用分组无线业务）是一种经济有效的分组数据无线传输技术，具有支持移动上网浏览的功能；能实现按比特收取用户通信费用；对 GSM 网络的改动较少；速率能达到 115kbps，可满足初期大部分用户对 3G 业务的需求并很快为运营商带来效益，提高竞争能

力等优点。GPRS 作为二代半的产品迅速进入市场，可以有效的保护电信运营商的投资，更容易与现有的网络在业务上兼容。

2.4.1 GPRS(通用分组无线业务)技术和网络

当前我国电信市场迫切需要的是通过 GSM网接入 Internet 的解决方案。GPRS就是这样一种二代半技术方案。如图 2-16 所示，它的基本思路是在支持话音和电路型数据业务的

GSM网络上叠加一个支持分组数据业务和能与外部分组网或 Internet 互联的有通用分组无线业务功能的 GPRS Infrastructure（通用分组无线业务基础设施）。

话音和电路型数据业务仍由GSM系统和 MSC/VLR支持，在BSC中增加RAN-RAN 接口，以支持 3G 的越区软切换，这时，BSC 变成 RNC，HLR/AUC由 2G/2.5G 共用，分组数据业务则由 GPRS 基础设施提供。

作为基于分组的体系结构，GPRS是为在无线系统和公共分组网络之间交换数据而引入的全新网络体系结构。GPRS基础设施的两大主要功能是保持对所连接主机位置的跟踪和提供对Internet/ISP/内部网基础设施的接入。

GPRS 基础设施包括 SGSN（服务型 GPRS 支持节点和 GGSN（网关型 GPRS支持节点）两种类型的节点。

SGSN 是为 MS 提供移动性管理、路由选择等服务的节点，处理用户注册、加密、移动、会话管理和基于位置的具体事务，以实现 GSPS 网与原 GSM 网互通，把 GPRS 连接到无线环境。

GGSN 是接入外部数据网络和业务的节点，用于实现 GPRS 网与外部网络（如内部网、ISP、AS 等）的互连。

BSS 和 SGSN 间的 Gb 接口是 2Mb/s 帧中继链路。在帧中继上运行的特定协议 BSSGP（BSSGPRS 协议）能在 BSS 与 SGSN 之间传输路由和 QoS 相关信息。

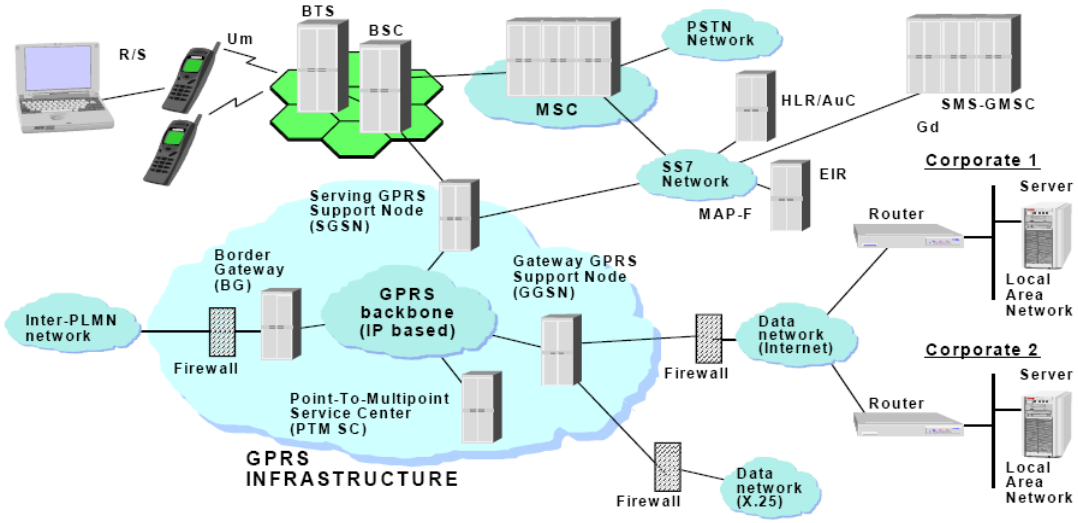


图 2-16 叠加在 GSM 网上的 GPRS 基础设施

移动台(终端)和 SGSN 之间的 IP 流量封装在 SNDCP(子网相关型收敛协议)中，SNDCP提供 IP 包的虚拟连接，并执行 IP 流量计算、分段和压缩等任务。

SGSN 与 GGSN 之间的 Gn 接口令到达 SGSN 的 IP 包通过朝向 GGSN 的特殊隧道中继和传输。此隧道基于称为 GTP（GPRS 通道协议）的 ETSI 协议。

GTP 信令有保持隧道（利用回声）、管理隧道（建立、更新、删除）、更新隧道位置以及管理终端移动（接管）等四个主要功能。

GGSN 到外部网的 Gi 接口提供对外部网（包括 ISP、公司内部网、自动系统）的接入。

GPRS 采用分组交换形式承载的数据业务，不需利用电路交换资源。它能提供的数据速率取决于所采用的编码方案，在标准中有四种编码数据速率，分别为每信道 9.05、13.4、15.6 和 21.4kb/s。由于用户能动态共享一个频点的全部 8 个业务信道，最大的数据吞吐量可高达每用户 171kb/s。不过，由于信道编码和多时隙分配需要一些开销，更现实的最高吞吐量为 115kb/s。在服务

质量尚可的条件下，多数应用的传输速率可能比 115kb/s 低得多。GPRS 能更高效利用无线资源和以更合理的收费方式提供丰富的业务类型，例如，点对点业务(PTP)；点对多点业务(PTM)；匿名接入 PIM；补充业务和 SMS 等。

考虑到 2G 的多样性和保护 2G 的庞大投资，ITU 放弃了对 3G 空中接口和网络技术的一致性要求，而致力于建立3G 网络接口及其互通的标准。于是IMT-2000 变成有共同目标要求，包容了多种技术的 3G 演进方案集。

GPRS 是我国移动通信网络从 GSM 到 WCDMA 和（或）TD-SCDMA 平滑过渡的重要步骤。

2.4.2 2G 向 3G 演进的策略

2G 和 3G 网络都可分成无线接入网和核心网两部分，有两种演进策略：

一开始就建 3G 核心网，2G 与 3G 间采用功能单元互通，使 2G 的无线接入网直联到3G核心网上，从而淘汰2G 核心网(如3GPP2组织的IMT-MC)初期不建 3G 核心网，而是增强 2G 核心网功能，使 3G 的无线接入网通过适配功能单元接入到增强 2G 核心网中，既提供 3G 业务，又保护 2G投资。待技术和经济条件有利时，再逐步建 3G 核心网并淘汰 2G 核心网(如欧洲 ETSI、中国 CWTS、美国 T1、韩国 TTA、日本 ARIB/TTC组成的 3GPP 组织的 IMT-TD)

第三代移动通信网络的建设是一个长期的过程，特别是为解决 3G 的覆盖问题，同时建设核心网和接入网的高投入是初期难予承受的。因此世界各国普遍采用以第二代移动通信网络为基础向 3G 演进的发展策略，即与 2G 系统尽量兼容，实现 2G 到 3G 间的平滑过渡，以较少的投入解决 3G 初期的漫游问题。不同的运营者可能会在某一阶段只建设 3G 核心网、控制网和无线接入网的部分网络和实现 IMT－2000 的部分功能。网络模块可以保证各层具有一定的独立性。

2.4.3 我国 GSM 向 TD-SCDMA 过渡的方案

2000 年底，我国以 GSM 为主的第二代移动网用户已达 7000 万户，移动通信频率分配也是根据ITU-T的要求进行的。因此，第三代移动通信网络的建设必须充分与 GSM 系统兼容。我国的第三代的核心网络必然应以 GSM－MAP协议为主，从 GSM 核心网络演进而来，并采用

3GPP 的标准化技术，其中GPRS 构成的核心网络将起主要的过渡作用。

我国 2G 向第三代移动网演进的步骤应该是：

(1) 大力发展和建立广泛的 GPRS 网络，用双频 TDMA/CDMA 双模终端，在局部地区提供 3G 业务；

(2) 通过升级 GSM/GPRS 网络中的核心网络节点，如 MSC/GSN，使之提供WCDMA 网络所需的 Iu 接口，并增加 WCDMA 系统协议处理能力，即可以使GSM/GPRS 核心网节点具有 WCDMA 核心网的功能，在保证与原有的GSM/GPRS 兼容前提下，实现 UTRAN 接入。

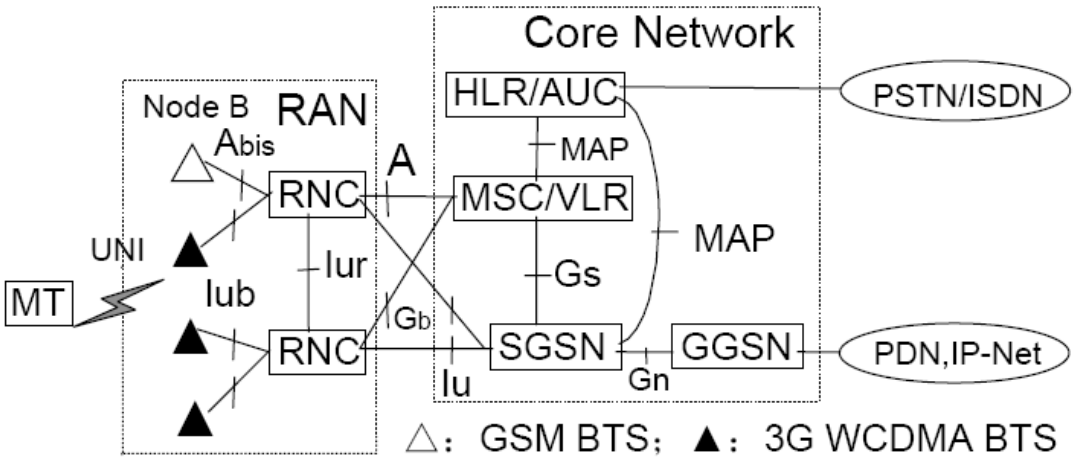


图 2-17 通过 GPRS 由 2G 向 3G 过渡的示意图

如图 2-17 所示，为在 GSM 网络中提供第三代移动通信业务，GSM 网络扩容时，使用过渡的 BSS(基站分系统)，而保持 GSM 的核心网络，通过 A 接口和Gb 接口分别提供话音(包括电路交换型数据)和分组数据业务，继续使用 GSM的 SIM 卡、鉴权中心、短消息中心和网络管理。这样，在任何有 GSM MSC的地方都可能使用此方式来扩大容量并提供第三代移动通信业务。

在此基础上，建立和使用过渡性 3G 核心网，这是一种在 GSM MSC 的基础上增加 ATM 交换功能和新的 Iu 接口，并仍然使用 GSM 鉴权中心等单元的网络。

上述演进方案全部使用具有国际标准的接口和尽可能利用 GSM 核心网的功能，并使用双频双模用户终端和更换部分 GSM 网的硬件和软件。

过渡的初期(2002－2004 年)，先在移动用户密集地区或数据和多媒体业务需求大的地区，依托GSM 网开通主要是以 TDD 系统为主，使用TDMA/CDMA 双模终端的第三代移动通信业务。

从 2004 开始，逐步停止 GSM 系统扩容， 较大规模地建设第三代移动通信FDD 和 TDD 网络，逐步完成演进过程。在 TDD 系统的选取上，以我国提出的 TD-SCDMA 为主，并综合采用 WCDMA 等标准，以获得最好的性能价格比。

2.4.4 无线应用协议 WAP

电子商务作为一种新兴的现代商务模式，自 20 世纪 90 年代以来得到了迅速发展，显

现了巨大的经济贸易潜力。随时随地通过移动终端接入国际互联网和公司内部网的移动电子商务解决方案将从根本上改变人们消费购物行为，成为人们竞相追逐的热点。1997 年夏，爱立信、诺基亚、摩托罗拉和 Unwired Planet 共同倡导开发的无线应用协议（WAP），作为移动通信和互联网间的“桥梁”，它使人们能最大限度地摆脱电脑和连线的束缚,通过 WAP 手机就可以便捷地接入互联网。

WAP(无线应用协议)已发展成无线网络通信应用的全球性工业标准，即 WAP标准， 并成立了有手机和系统制造商、运营者、业务提供商、软件开发商、内容提供商等各方面一百多成员参加的 WAP(无线应用协议)论坛。

WAP 标准包括应用、会话、交易、安全和传输层方面的一系列规程，是一个能避免网络割接，实现 GSM 手机与 Internet 互连，保护 GSM 网投资，为运营商快速开拓移动上网和无线增值业务市场的全球性开放协议，已得到全球75%的手机厂家和有一亿多用户的运营商们的支持。

WAP 标准以 Internet 模式为基础,继承和充分利用 XML(可扩展标识语言)、UDP、IP 等现有 Internet 规范，结合无线环境(信道低带宽、高时延、不稳定，手机屏幕小、存储器容量有限)，进行优化和创新，并通过论坛成员间的互操作试验而不断发展，已成为无线网上的“TCP/IP”。

WAP 是端到端协议，只要求 WAP 手机和 WAP 代理服务器支持。WAP 对现有移动网络透明，不需对现有网络协议做任何改动，适用于各种空中接口和各种移动或无线终端，可在 GSM、CDMA 等网上实现。

WAP 还定义了 WAE(无线应用环境)作为开发各种新无线业务和应用的工具。

中国移动帅先于 2000 年 3 月 28 日在上海、北京、天津、广州、杭州、深圳等六大城市同时开出全球通 WAP 商用试验网，WAP 用户可以在这六大城市中使用漫游业务，多了一个浏览因特网信息的新手段。这标志着我国无线通信技术进入了一个新的发展阶段。

WAP 协议为把因特网信息内容及增值业务传送到移动终端（数字移动电话、寻呼机、个人数字助理、电子阅读器等）提供了一个开放的通用标准。此项WAP 业务为具有数据业务功能的手机用户提供直接上网的功能,用户可通过手机首先访问中国移动通信集团公司的 WAP 门户站点，接入码为 172，门户站点：wap.chnmobile.com。

用户使用 WAP 业务需在 WAP 手机上进行参数设置,这样即可直接从手机上获取专门为 WAP 用户定制的信息，包括新闻、天气预报、股票信息、娱乐游戏、体育消息、健康常识、电子商务等信息，并以此站点为起点，通过友情链接可进入上海、北京、广州、深圳、杭州、天津站点浏览当地的各类信息。

还可浏览因特网上其他的 WAP 信息站点。

第三章　核心网

3.1 核心网络基本结构

核心网（CN）从逻辑上又可划分为 电路域（CS域）、分组域 （PS域）和广播域 （BC域）。CS域设备是指为用户提供“电路型业务”，或提供相关信令连接的实体。 CS域特有的实体包括： MSC、GMSC、VLR、IWF。PS域为用户提供“分组型数据业务”，PS域特有的实体包括：SGSN和GGSN。其他设备如HLR（或HSS）、AuC、EIR等为CS域与PS域共用。

WCDMA的网络总体结构定义在3GPP TS 23.002中。目前具有三个版本，分别为：

R99 —3GPP TS 23.002 V3.4.0, 2000-12

R4 —3GPP TS 23.002 V4.1.0, 2000-12

R5 —3GPP TS 23.002 V5.1.0, 2000-12

3GPP在98年底99年初开始制定 3G的规范。R99版本计划在1999底完成，最后是在2000.3完成。后来意识到按年度命名版本会给实现带来困难，因为年度版本不能保持一个相对稳定的规范集，因此决定从R99后不再按年来命名版本，同时把R2000的功能分成两个阶段实施：Rel4和Rel5；以后升级将按R6，R7... 的方式命名版本。原则上R99的规范是Rel4规范集的一个子集，若在R99中增加新的特征，就把它升级到Rel4。同样Rel4规范集是Rel5规范集的子集，若在 Rel4中增加了新的特征就把它升级到 Rel5。 按 计 划Release4要在2001.3完成，Release5要在2001.12完成。

对于以上三个版本，PS域特有设备主体没有变化，只进行协议的升级和优化；CS域设备变化也不是非常大。在R4网络中，根据需要(G)MSC可被(G)MSC Server和MGW替代，新增了一个R-SGW，HLR也可被替换为HSS（规范中没有给出明确说明）。在R5网络中，如果有 IMS（IP多媒体子系统），则网络使用HSS以替代HLR。

3.1.1 R99网络结构及接口

为了确保运营商的投资利益，在R99网络结构设计中充分考虑了2G/3G 兼容性问题，以支持 GSM/GPRS/3G的平滑过渡。因此，在网络中CS域和PS域是并 列 的 ，R99 核 心 网 设 备 包 括 ： MSC/VLR 、IWF 、SGSN 、GGSN 、HLR/AuC、EIR等。为支持3G业务，有些设备增添了相应的接口协议，另外对原有的接口协议进行了改进。

图4-1是PLMN的基本网络结构（包括CS域和PS域），图中所有功能实体都可作为独立的物理设备。

CS域的接口：

A 接口和 Abis 接口定义在 GSM08-series 技术规范中； Iu-CS接口定义在 UMTS25.4xx-series 技术规范中；B, C, D, E, F 和 G接口则是以No.7信令方式实现相应的移动应用部分（MAP），用于完成数据交换。H接口未提供标准协议。

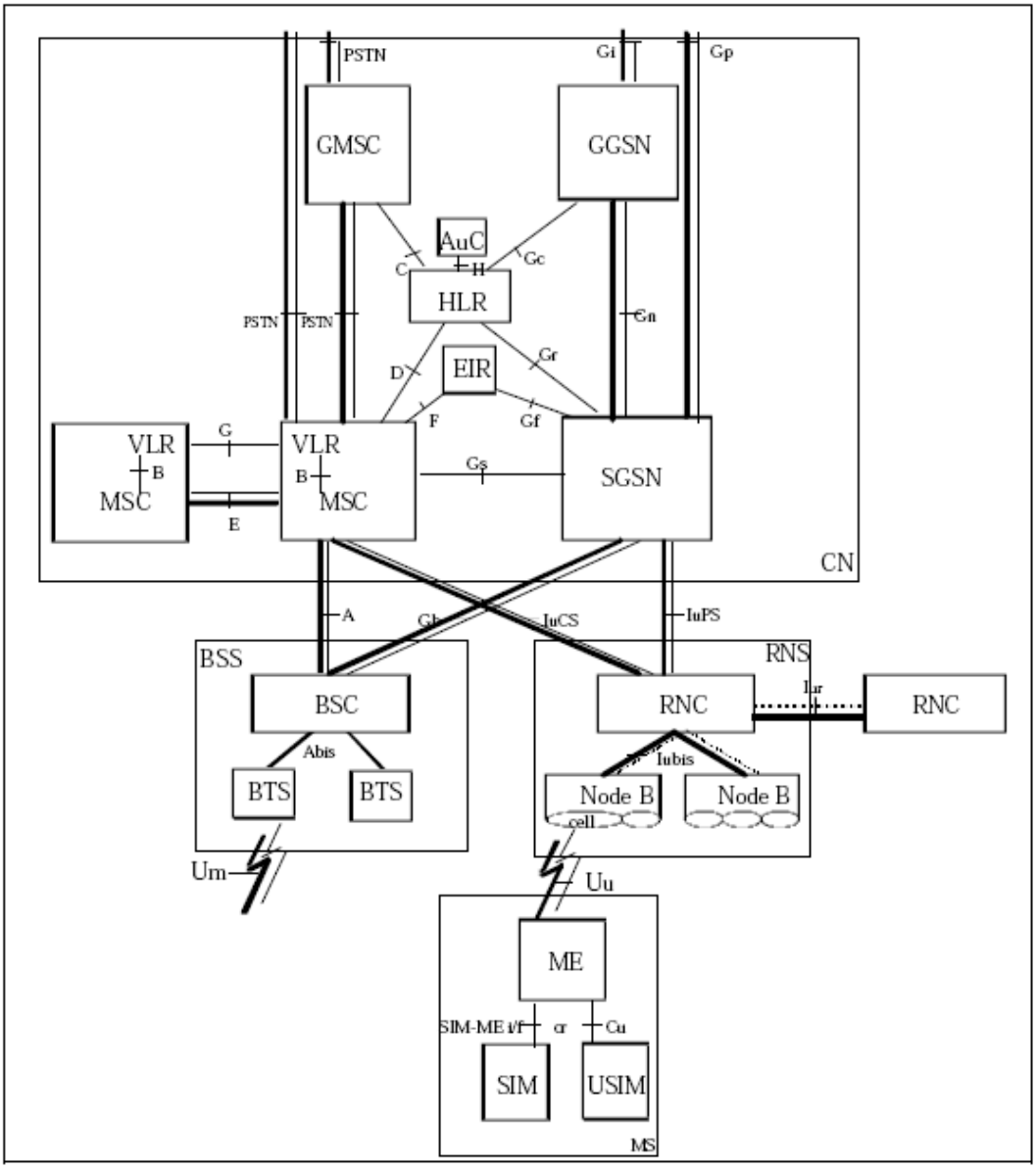
PS域的接口：

Gb 接 口定义 在 GSM08.14、 08.16和 08.18 技术规范中， Iu-PS接 口 定义 在

UMTS25.4xx-series 技术规范中；Gc/Gr/Gf/Gd接口则是基于No.7信令的MAP 协议， Gs实现SGSN与MSC之间的联合操作，基于SCCP/BSSAP+协议，Ge基于CAP协议，Gn/Gp协议由GTP V0升级到V1版本，Ga/Gi协议没有太大改动。

说明：

在 实 际应 用中一些功能可能会结合到同一个物理实体中，如 MSC/VLR，HLR/AuC，SGSN/MSC/VLR，使某些接口成为内部接口。



粗线： 表示支持用户业务的接口

点划线： 表示支持信令的接口

图3-1 R99网络结构图

R99中CS域的功能实体包括有：MSC、VLR、HLR、AuC、EIR等。其中，运营 商 可 以 根 据 连 接 方 式 的 不 同 将 MSC 设 置 为 GMSC 、 SM-GMSC 、SM-IWMSC等。为实现网络互通，在系统中配置IWF（一般结合于MSC）。

除上述功能实体之外,PS域特有的功能实体包括SGSN和GGSN,为用户提供分组数据业务。

R99的主要功能实体包括：

移动交换中心（MSC）

MSC为电路域特有的设备，用于连接无线系统（包括BSS、RNS）和固定网。MSC完成电路型呼叫所有功能，如控制呼叫接续，管理MS在本网络内或与其他网络（如PSTN/ISDN/PSPDN、其他移动网等）的通信业务，并提供计费信息。

拜访位置寄存器（VLR）

VLR 为电路域特有的设备，存储着进入该控制区域内已登记用户的相关信息，为移动用户提供呼叫接续的必要数据。当MS漫游到一个新的VLR区域后，该VLR向HLR发起位置登记，并获取必要的用户数据；当MS漫游出控制范围后，需要删除该用户数据，因此VLR可看作为一个动态数据库。

一个VLR可管理多个MSC，但在实现通常都将MSC和VLR合为一体。

归属位置寄存器（HLR）

HLR为CS域 和PS域共用设备，是一个负责管理移动用户的数据库系统。PLMN可以包含一个或多个HLR，具体配置方式由用户数、系统容量、以及网络结构所决定。 HLR存储着本归属区的所有移动用户数据，如识别标志、位置信息、签约业务等。

当用户漫游时， HLR接收新位置信息，并要求前VLR删除用户所有数据。当用户被叫时，HLR提供路由信息。

鉴权中心（AuC）

AuC为CS域 和PS域 共用设备， 是存 储用 户鉴权算法和加密密钥的实体。AuC将鉴权和加密数据通过HLR发往VLR、MSC以及SGSN,以保证通信的合法和安全。每个AuC和对应的 HLR关联，只通过该HLR和外界通信。通常AuC和HLR结合在同一物理实体中。

设备识别寄存器（EIR）

EIR为CS域和PS域共用设备，存储着系统中使用的移动设备的国际移动设备识别码（IMEI）。其中，移动设备被划分 “白”、“灰”、“黑”三个等级，并分别存储在相应的表格中。

一个 最小化的EIR可以只包括最小“ 白表”（设备属于“白”等级）。

网关MSC（GMSC）

GMSC是电路域特有的设备。 GMSC作为系统与其它公用通信网之间的接口，同时还具有查询位置信息的功能。如MS被呼时，网络如不能查询该用户所属的HLR，则需要通过GMSC查询，然后将呼叫转接到MS目前登记的MSC中。

具体由运营商决定那些 MSC可作为 GMSC，如部分MSC或所有的MSC。

SGSN

SGSN为PS域特有的设备，SGSN提供核心网与无线接入系统BSS、RNS的连接，在核心网内，SGSN与GGSN/GMSC/HLR/EIR/SCP等均有接口。SGSN完成分组型数据业务的移动性管理、会话管理等功能，管理MS在移动网络内的移动和通信业务，并提供计费信息。

GGSN

GGSN也是分组域特有的设备。 GGSN作为移动通信系统与其它公用数据网之间的接口，同时还具有查询位置信息的功能。如 MS被呼时，数据先到GGSN，再由 GGSN向HLR查询用户的当前位置信息，然后将呼叫转接到目前登记的SGSN中。GGSN也提供计费接口。

R99中核心网的接口协议如表 3-1所示：

表3-1 R99 核心网的接口名称与含义

接口名	连接实体	信令与协议
A	MSC——BSC	BSSAP
Iu-CS	MSC——RNS	RANAP
B	MSC——VLR	
C	MSC——HLR	MAP
D	VLR——HLR	MAP
E	MSC——MSC	MAP
F	MSC——EIR	MAP
G	VLR——VLR	MAP
Gs	MSC——SGSN	BSSAP+
H	HLR——AuC	
	MSC——PSTN/ISDN/PSPDN	TUP/ISUP
Ga	GSN——CG	GTP'
Gb	SGSN——BSC	BSSGP
Gc	GGSN——HLR	MAP
Gd	SGSN——SMS-GMSC/IWMSC	MAP
Ge	SGSN——SCP	CAP
Gf	SGSN——EIR	MAP
Gi	GGSN——PDN	TCP/IP
Gn	GSN——GSN（Inter PLMN）	GTP
Gr	GSN——GSN（Intra PLMN）	GTP
Iu-PS	SGSN——HLR	MAP
Gp	SGSN——RNC	RANAP

R99中核心网的各接口功能如下：

A接口

A接口指MSC与BSC之间的接口。BSS-MSC接口用于传送如下信息：

- BSS 管理
- 呼叫处理
- 移动性管理

Iu-CS接口

Iu-CS 接口是MSC与RNS之间的接口，具体定义在UMTS 25.41x-series技术规范中。RNS-MSC接口用于传送如下信息：

- RNS管理
- 呼叫处理
- 移动性管理.

B接口

B接口是MSC和VLR间的接口，其所依赖的信令方式没有具体规定。B接口实现的功能有：

- MSC从VLR中获得用户信息。
- 当MS进行位置更新操作时，MSC通知VLR记录位置信息。
- 当MS激活一个特定补充业务或修改业务相关数据时，MSC通过VLR通知HLR更新数据。

C接口

C接口是MSC与HLR之间的接口。在此接口上，MSC采用基于No.7信令方式的MAP协议来实现以下功能：

- 在MS被呼时，HLR将路由信息传递到GMSC；

短消息业务

对于 CAMEL应用，本接口主要用于获取移动用户终呼时的路由信息，用户状态，签约信息等。

D接口

D接口是VLR与HLR之间的接口。本接口用于交换有关MS位置信息及用户管理信息，通过基于No.7信令系统中的MAP协议实现如下功能：

- 鉴权
- 位置更新
- 在呼叫建立时检索用户数据
- 补充业务
- VLR恢复

为支持移动用户能够在整个服务区内发起或接收呼叫，HLR和VLR间进行数据交换。当MS发生位置更新时，VLR通知HLR当前MS的位置，以及漫游号码。HLR则向VLR发送支持业务处理所需要的用户数据。同时，HLR指示MS以前所在的VLR删除该用户信息。HLR与VLR间的数据交换还发生在用户更新签约业务，或者管理者修改相关签约业务参数时。

对于 CAMEL应用，本接口用以向拜访PLMN传送CAMEL用户数据以及提供MSRN。

E接口

E接口指 MSC与MSC之间的接口。通过基于No.7信令的MAP协议，本接口主要完成以下功能：

- 切换
- 短消息业务
- MSC间切换后的呼叫控制

MAP 控制 MSC间 的切换 。如 MS通 话 时 ， 从 一 个MSC区 域 移 动 到 另一 个 MSC区域，这时为保证正常通话需要进行切换。MSC间通过MAP协议保证切换操作顺利进行。在切换操作完成后，MSC间传送一些A接口消息。

F接口

F 接 口 是 MSC与 EIR之间的接口 。 当MSC需要检查国际移动设备识别码（IMEI）的合法性时，需要通过F接口与EIR交换与IMEI有关的信息。本接口通过基于No.7信令的MAP协

议实现以上功能。

G接口

G接口是VLR与VLR之间的接口。通过基于No.7信令的MAP协议完成如下功能：

- 位置更新：当MS漫游到一个新的VLR后，向前VLR索取IMSI
- 鉴权：将鉴权参数由先前VLR传送给当前的VLR

Gs接口

Gs接口是MSC与SGSN间的接口。Gs接口采用基于No.7信令（使用无连接的SCCP ，没有TCAP）的BSSAP+协议来完成信令互通。SGSN可通过Gs接口向MSC/VLR发送MS位置信息。SGSN也可通过Gs接口接收到来自 MSC/VLR的寻呼信息。通过Gs接口，MSC/VLR可向SGSN声明，MS正执行由MSC处理的业务。

H接口

H接口是HLR与AuC之间的接口，接口形式没有具体标准。主要完成的功能是：当HLR接收到一个请求用户鉴权和加密数据的消息时，如 HLR没有这些信息，则向AuC请求这些数据。

MSC与外部网络的接口

这里是指 MSC与 PSTN/ISDN等外 部网络的接口。由于 MSC是基于普通的ISDN交换，在呼叫控制方面具有和固定网交换一样的接口。对于电路呼叫，GSM技术规范中给出的信令接口是SS7的TUP和ISUP。

Ga接口

Ga接口是指GSN(包括SGSN/GGSN)与CG之间的接口,接口协议GTP’基于UDP/IP或者TCP/IP协议栈，主要完成计费信息的输出功能。

Gb接口

Gb接口是2.5G GPRS系统使用的接口，为兼容GPRS而保留的。

Gc 接口

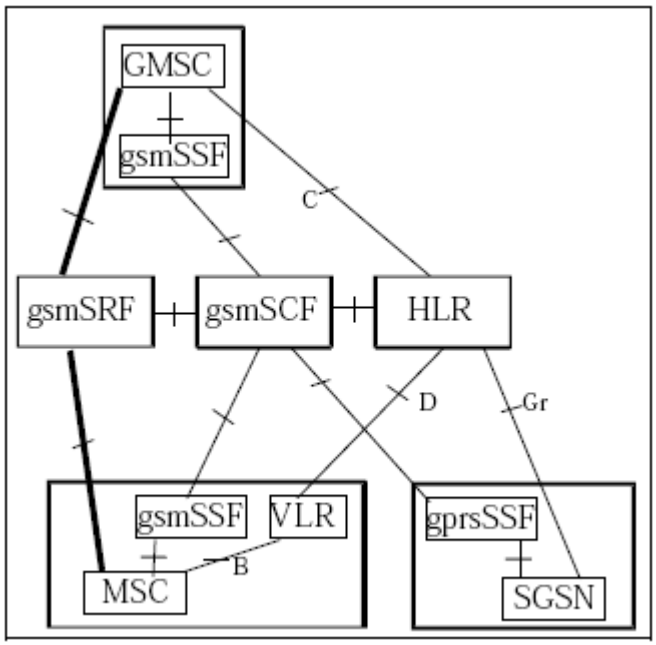
Gc接口是GGSN与HLR之间的接口,实现GGSN与HLR之间的信息交互功能。有两种实现方法：一是基于MAP协议，在GGSN上直接出七号接口；另一种方法是GGSN借助SGSN提供与HLR之间的MAP接口。这部分与GPRS相同。

Gd接口

Gd接口在SGSN与SMS-GMSC/IWMSC之间的接口，基于MAP协议，实现短消息的收发功能。

Ge接口

Ge接口是SGSN与SCP之间的接口,基于CAP协议实现分组域的智能业务。在R99中MSC与SCF之间的接口没有特定名称，它们之间通信采用CAP方式。



粗线： 表示支持用户业务的接口

点划线： 表示支持信令的接口

图 3-6 CAMEL 相关结构图

Gf接口

Gf接口是SGSN与EIR之间的接口，当SGSN 需要检查国际移动设备识别码（IMEI）的合法性时，需要通过Gf接口与EIR交换与IMEI有关的信息。本接口通过基于No.7信令的MAP协议实现以上功能。

Gi接口

Gi接口是GGSN与外部数据网之间的接口，基于TCP/IP协议实现外部分组网络的互联功能。

Gn/Gp接口

Gn/Gp接口是GSN与GSN之间的接口，基于GTP协议实现隧道传输功能，包括信令面GTP-C和用户面GTP-U。GTP-C完成隧道的管理和其它信令消息的传输功能，GTP-U传输用户面的数据包。

Gr接口

Gr接口是SGSN与HLR之间的接口,本接口用于交换有关MS位置信息及用户管理信息,通过基于No.7信令系统中的MAP协议实现如下功能：

- 鉴权
- 路由区更新
- 在会话建立时检索用户数据
- SGSN恢复

为支持移动用户能够在整个服务区内发起或接收呼叫，HLR和SGSN间进行数据交换。当MS发生路由区更新时，SGSN通知HLR当前MS的位置，以及漫游号码。HLR则向SGSN发送支持业务处理所需要的用户数据。同时，HLR指示MS以前所在的SGSN删除该用户信息。HLR与SGSN

间的数据交换还发生在用户更新签约业务，或者管理者修改相关签约业务参数时。

Iu-PS接口

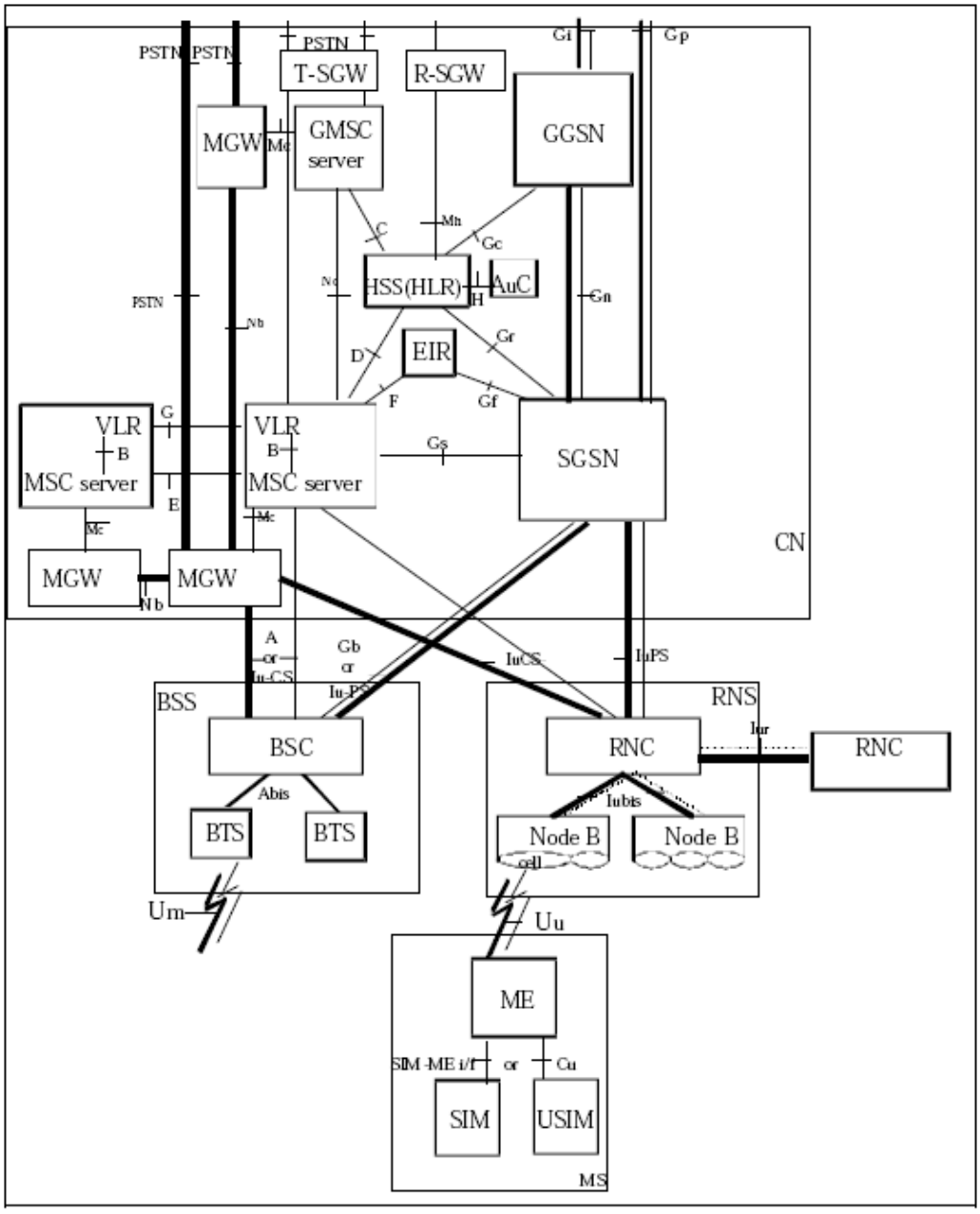
Iu-PS接口是SGSN与RNC间的接口，具体定义在UMTS 25.41x-series技术规范中。RNC-SGSN接口用于传送如下信息：

- RNC管理
- 会话管理
- 移动性管理

3.1.2 R4网络结构及接口

图3-2是R4版本的 PLMN基本网络结构，图中所有功能实体都可作为独立的物理设备。关于Nb，Mc和Nc等接口的标准还没有开始制订。

在 实 际应 用中一些功能可能会结合到同一个物理实体中，如 MSC/VLR，HLR/AuC等，使得某些接口成为内部接口。



粗线： 支持用户业务的接口

点划线： 支持信令的接口

注：(G)MSC Server 和 MGW 可集成为单个物理实体(G)MSC

图 3-2 R4 的网络结构图

R4版本中PS域的功能实体SGSN和GGSN没有改变，与外界的接口也没有改变。CS域的功能实体仍然包括有：MSC、VLR、HLR、AuC、EIR等设备，相互间关系也没有改变。但为了支持全IP网发展需要，R4版本中CS域实体有所变化，如：

（1）MSC根据需要可分成两个不同的实体：MSC服务器（MSC Server，仅用以处理信令），和媒体网关（MGW，用于处理用户数据），MSC Server 和MGW共同完成MSC功能。对应的GMSC也分成GMSC Server 和MGW。

MSC服务器（MSC Server）

MSC Server主要由MSC的呼叫控制和移动控制组成，负责完成CS域的呼叫处理等功能。

MSC Server终接用户-网络信令，并将其转换成网络-网络信令。

MSC Server也可包含VLR以处理移动用户的业务数据和CAMEL相关数据。

MSC Server可通过接口控制MGW中媒体通道的属于连接控制的部分呼叫状态。

媒体网关（MGW）

MGW是PSTN/PLMN的传输终接点，并且通过Iu接口连接核心网和UTRAN。MGW可以是从电路交换网络来的承载通道的终接点，也可是分组网来的媒体流（例如，IP网中的RTP流）的终接点。在Iu上， MGW 可支持媒体转换、承载控制和有效载荷处理（例如，多媒体数字信号编解码器，回音消除器，会 议 桥 等 ），可 支 持 CS业 务 的 不 同Iu 选 项（ 基 于 AAL2/ATM， 或 基 于RTP/UDP/IP)。

MGW：

- 与 MGCF，MSC服务器和 GMSC服务器相连，进行资源控制
- 拥有并使用如回音消除器等资源
- 可能需要具有多媒体数字信号编解码器

MGW可具有必要的资源以支持 UMTS/GSM传输媒体。进一步， 可要求H.248裁剪器支持附加的多媒体数字信号编解码器和成帧协议等。

MGW的承载控制和有效载荷处理能力也用于支持移动性功能,如SRNS 重分配/切换 和定位。目前期待H.248标准机制可运用于支持这些功能。

GMSC Server

GMSC server主要由GMSC的呼叫控制和移动控制组成。

（2）HLR可更新为归属位置服务器（HSS）

（3）R4新增一个实体：漫游信令网关（R-SGW）

在基于No.7信令的 R4之前的网络，和可能基于 IP传输信令的R99之后网络之间，R-SGW完成传输层信令的双向转换 （Sigtran SCTP/IP 对 No.7 MTP）。R-SGW 不对 MAP / CAP 消息进行翻译，但对SCCP层之下消息进行翻译，以保证信令能够正确传送。

为支持R4版本之前的CS终端，R-SGW实现不同版本网络中ＭＡＰ-E和MAP-G消息 的 正确 互 通。 也 就 是 ， 保 证Ｒ４网 络实体中基 于 IP 传输的 ＭＡＰ消 息，与ＭＳＣ／ＶＬＲ（Ｒ４版本前）中基于Ｎｏ． ７传输的ＭＡＰ消息能够互通。

在R4网络中也新增一些接口协议，如表4-2所示。

表3-2 R4 核心网外部接口名称与含义

接口名	连接实体	信令与协议
A	MSC——BSC	BSSAP
Iu-CS	MSC ——RNS，MSC——BSC	RANAP
B	MSC——VLR	
C	MSC——HLR	MAP
D	VLR——HLR	MAP
E	MSC——MSC	MAP
F	MSC——EIR	MAP
G	VLR——VLR	MAP

Gs	MSC——SGSN	BSSAP+
H	HLR——AuC	
	MSC——PSTN/ISDN/PSPDN	TUP/ISUP
Ga	SGSN——CG	GTP'
Gb	SGSN——BSC	BSSGP
Gc	GGSN——HLR	MAP
Gd	SGSN——SM-GMSC/IWMSC	MAP
Ge	SGSN——SCP	CAP
Gf	SGSN——EIR	MAP
Gi	GGSN——PDN	TCP/IP
Gp	GSN——GSN（Inter PLMN）	GTP
Gn	GSN——GSN（Intra PLMN）	GTP
Gr	SGSN——HLR	MAP
Iu-PS	SGSN——RNC	RANAP
Mc	(G)MSC Server——MGW	
Nc	MSC Server——GMSC Server	
Nb	MGW ——MGW	
Mh	HSS——R-SGW	

R4中核心网的各接口功能如下：

A接口

A接口指MSC与BSC之间的接口。 实现方式和功能与R99相似。

Iu-CS接口

Iu-CS接口可以是 MSC与其RNS之间的接口，也可以是MSC与BSS之间的接口，这与R99有较大区别。当作为RNS-MSC接口时，用于传送如下信息：

- RNS管理
- 呼叫处理
- 移动性管理

当作为BSS-MSC接口时，用于传送如下信息：

- BSS管理
- 呼叫处理
- 移动性管理

需要注意的是，在R4版本中BSS-MSC接口可以采用A接口方式，或Iu-CS接口方式。具体采用哪种接口形式，与MS工作模式有关：

- A/Gb模式，如R4版本前终端，或工作在没有Iu接口的BSS中的R4终端
- Iu模式（也就是 Iu-CS和 Iu-PS），如工作在有Iu接口的BSS中的R4终端

终端没有其他允许的工作模式 （如 A/Iu-PS模式或 Iu-CS/Gb 模式）。

B接口

B接口是MSC Server和VLR间的内 部接 口。实现方式和功能与R99类似，只是由MSC中的MSC Server来完成相应的功能。

C接口

C接口是 MSC Server与HLR之间的接口。 实现方式和功能与R99类似，只是由MSC中的MSC Server来完成。

D接口

D接口是VLR与HLR之间的接口。本接口实现方式和功能与R99相似。

E接口

E接口是MSC Server 与 MSC Server之间的接口。本接口实现方式和功能与R99相似。

F接口

F接口是MSC Server与EIR之间的接口。 本接口实现方式和功能与R99相似。

G接口

G接口是VLR与VLR之间的接口。 本接口实现方式和功能与R99相似。

Gs接口

Gs接口是MSC/VLR与SGSN间的接口。本接口实现方式和功能与Ｒ９９相似。

H接口

H接口是HLR与AuC之间的接口，本接口实现方式和功能与R99相似。

MSC与外部网络的接口

本接口实现方式和功能与R99相似。

以下是 R4版本中新增的接口：（在协议中称它们为参考点，但尚没有接口和参考点有何区别的明确定义，因此可认为它们具有相同的含义。目前还没有制订出相应的标准协议）

Mc参考点

本参考点是 (G)MSC Server与MGW间的接口（ Mc也是MGCF和MGW间的接口）。它具有如下特点：

- ✓ - 遵从 H.248标准
- ✓ - 能不受H.323限制，支持不同呼叫模式和媒体处理方式的柔性连接
- ✓ - 支持开放结构
- ✓ - 动态共享MGW物理节点资源
- ✓ - 动态共享不同域间的传输资源

Nc参考点

本参考点是MSC Server与GMSC Server间的接口。通过该接口，使不同网络间的通话能顺利进行。如， Nc可为ISUP或ISUP的改进：承载独立呼叫控制（bearer independent call control ，BICC）。Nc的信令传输方式可以有很多种形式，包括IP。

Nb参考点

本参考点是MGW-MGW间的接口。通过该接口，执行承载控制和传输。用户数据的传输方式可以是RTP/UDP/IP或AAL2。在R4网络结构中， Nb上的用户数据传输和承载控制可以有不同的方式，如AAL2/Q.AAL2, STM/none, RTP/H.245等。

Mh参考点

本参考点是HSS和R-SGW间的接口。本接口在HSS和R99及R99以前的网络之间交换移动管

理和签约数据等信息。Mh用于支持R4或更高版本的用户漫游到低版本网络。

当PLMN网络支持CAMEL时，网络结构以及接口如同R99，没有发生改变。

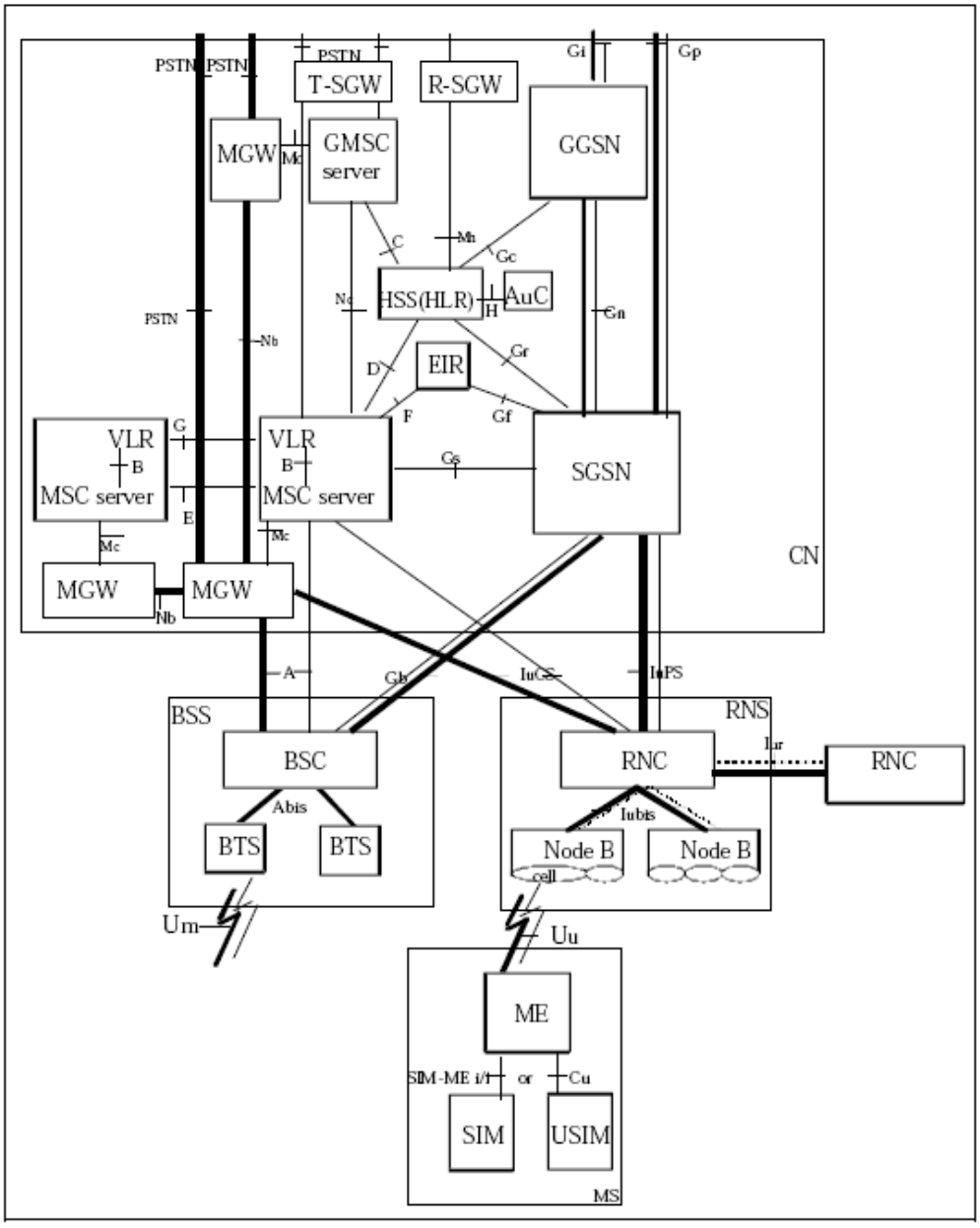
Gc/Gr

与R99的接口类似，只是HLR改为HSS。

其它分组域的接口与R99中相同，在此不再描述。

3.1.3 R5网络结构及接口

图3-3(a)是R5版本的 PLMN基本网络结构（没有包括 IM子系统部分），主要表示的是CS域的功能实体和接口。图中所有功能实体都可作为独立的物理设备。



粗线：支持用户业务的接口

点划线：支持信令的接口

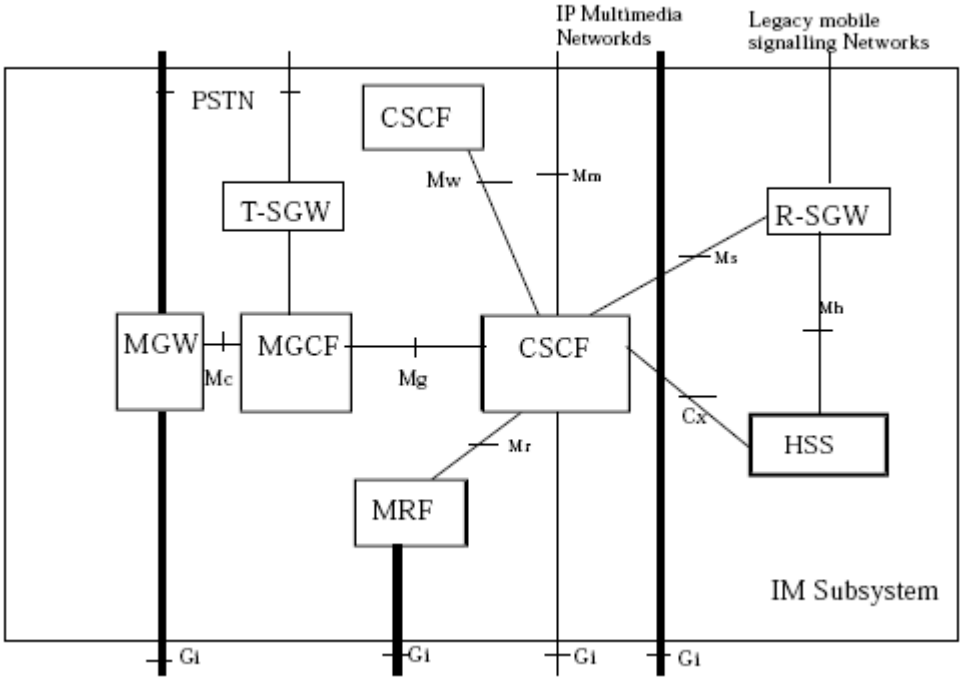
注：(G)MSC Server和MGW可集成为单个物理实体(G)MSC

图 3-3(a) R5 的网络结构图

R5版本的网络结构和接口形式和R4版本基本一致。差别主要是：当PLMN包括IM子系统时，HLR被HSS所替代。另外，接口差别是BSS和MSC之间只有A接口，不象R4中有Iu-CS接口。

为简洁起见，不再赘述R5的接口协议。CS域和CAMEL实体的连接关系也没有发生改变。

图3-3(b)是R5版本的 IMS基本网络结构，主要表示的是IMS域的功能实体和接口。图中所有功能实体都可作为独立的物理设备。



粗线： 支持用户业务的接口

点划线： 支持信令的接口

注： CSCF与UE之间的Gm接口，由于布局的原因没有在图中表示出来，但也是IM子系统的接口。

图3-3(b) R5的IMS网络结构图

R5新增的物理实体有：

（1）归属位置服务器（HSS）

当网络具有IM子系统时，需要利用HSS替代HLR。

HSS是网络中移动用户的主数据库，存储有支持网络实体完成呼叫/会话处理相关的业务信息。例如，HSS通过进行鉴权、授权、名称/地址解析、位置依赖等，以支持呼叫控制服务器能顺利完成漫游/路由等流程。

和HLR一样，HSS负责维护管理有关用户识别码、地址信息、安全信息、位置信息、签约服务等用户信息。基于这些信息，HSS可支持不同控制系统

（CS域控制，PS域控制，IM控制等）的CC/SM实体。

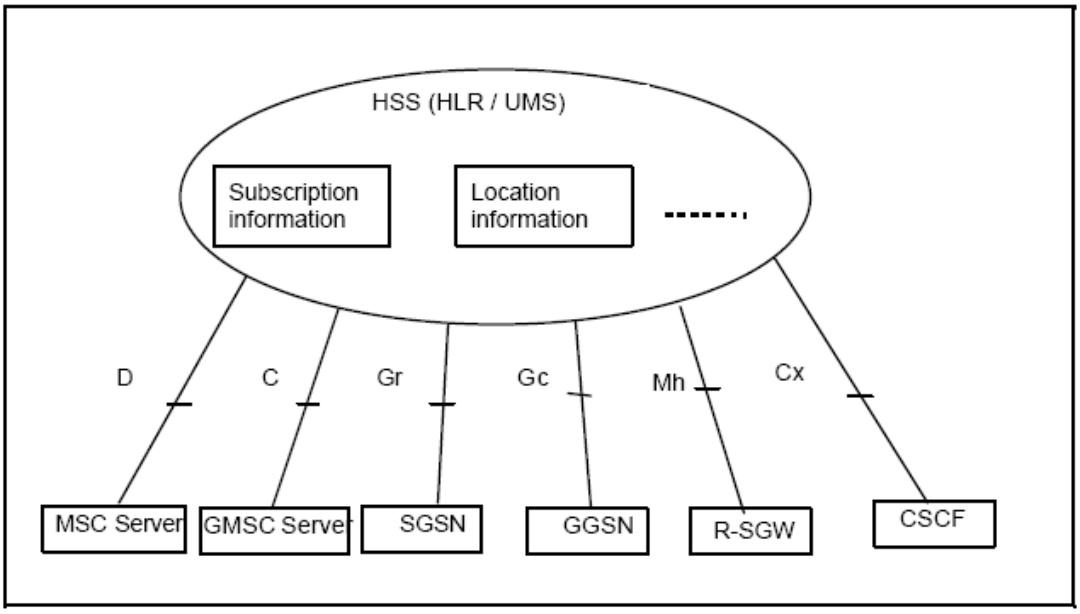


图3-4 HSS的基本结构与接口

HSS可集成不同类型的信息，在增强核心网对应用和服务域的业务支持同时，对上层屏蔽掩盖不同类型的网络结构。 HSS支持的功能包括：IM子系统请求的用户控制功能；PS域请求的有关HLR功能子集；CS域部分的 HLR功能（如果容许用户接入CS域，或漫游到传统网络）。HSS结构如下所示：

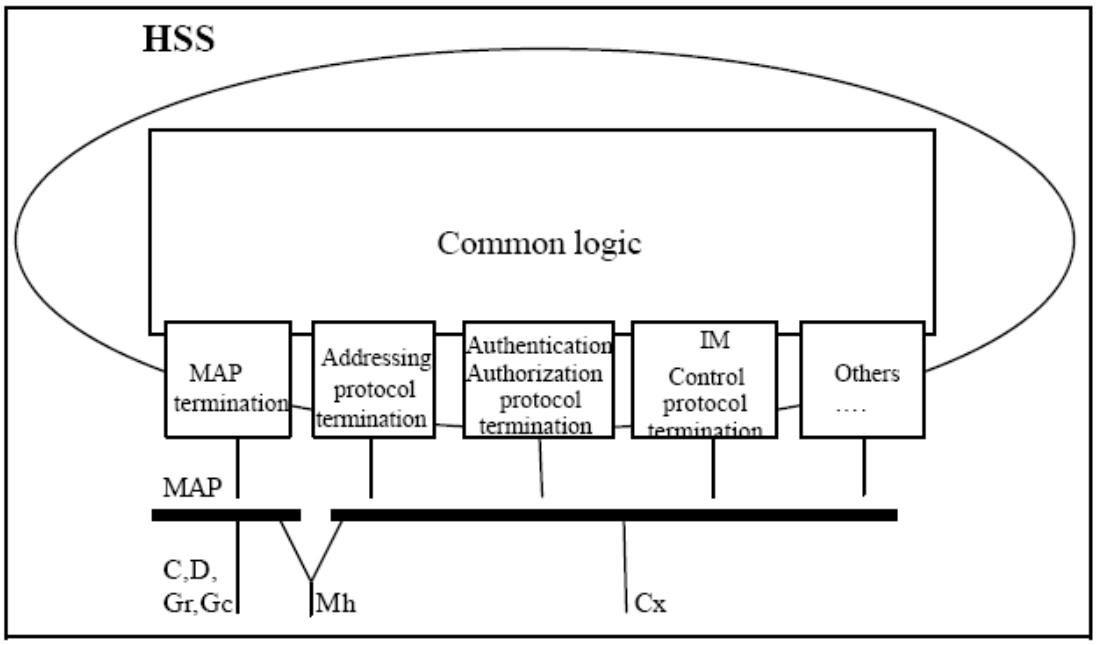


图3-5 HSS的结构示意

（2）呼叫状态控制功能（CSCF）

CSCF 的 功 能 形 式 有 ：Proxy CSCF （P-CSCF)， Serving CSCF (S-CSCF) 或 Interrogating CSCF (I-CSCF)。

P-CSCF：是UE在IM子系统中的第一个接入点

S-CSCF：处理网络中的呼叫的会话状态

I-CSCF ：主要是运营商网内的到运营商的用户的所有连接的接入点。

CSCF 完成以下功能：

- ✓ ICGW（入呼网关，在I－CSCF中实现）

作为第一个接入点，完成入呼的路由功能

入call业务的触发(如呼叫的显示/呼叫的无条件转发)

地址的查询处理

与HSS的通信

- ✓ CCF（呼叫控制功能，在S－CSCF中实现）

呼叫的建立/终结与状态/事件的管理

与MRF交互支持多方的会话与其他业务

用于计费，审核，监听等用途所需的事件上报

接收与处理应用层的登记

地址的查询处理

向应用与业务网络(VHE/OSA)提供业务触发机制(service capabilitiesfeatures)

根据服务的网络调用基于位置的业务

检查呼出的权限

- ✓ SPD（业务描述数据库）

与归属网络的HSS交互获取IM域的用户描述数据信息,根据与归属网络签定的SLA进行存储。

通知归属网络呼叫发起方的接入(包括 CSCF的信令传输地址，用户的ID等，ffs)

cache接入相关的信息(终端的 访问用户的IP地址 etc.)

- ✓ AH （寻址处理）

分析，转换，修改，映射地址

网络之间互联路由的地址处理

（3）媒体网关控制功能 (MGCF)

MGCF完成的功能：

- ✓ 控制MGW中媒体信道的连接控制的呼叫状态控制。
- ✓ 与CSCF通信。
- ✓ 根据入呼的路由号码选择 CSCF。
- ✓ 进行ISUP 与 IM 子系统的呼叫控制协议的转换。
- ✓ 带外信息的接收与转发到 CSCF/MGW

（4）传输信令网关功能 (T-SGW)

T-SGW完成以下功能：

映射呼叫相关的信令到/从PSTN/PLMN为IP承载，并将它发送到/从MGCF。.

必须提供PSTN/PLMN <-> IP 的传输层的地址映射。

（5）多媒体资源功能(MRF)

MRF完成的功能：

完成多方呼叫与多媒体会议功能，与 H.323的 MCU 功能相同。

在多方呼叫与多媒体会议中负责承载的控制 （与 GGSN 和 MGW 一起完成)。

与CSCF通信，完成多方呼叫与多媒体会话中的业务确认功能。

R5中核心网的各参考点功能定义如下：

Cx参考点

本参考点接口完成CSCF 与HSS之间的信息传递，包括：

S－CSCF的分配信息

从HSS到CSCF的路由信息

UE与HSS的信息通过CSCF的隧传

Gm参考点

本参考点接口完成UE与CSCF的通信，功能：

向CSCF注册

呼叫的发起与终结

增补业务的控制

Gm也支持UE与S－CSCF之间的信息传递：

向S－CSCF的注册

向S－CSCF的用户业务请求

业务与业务的鉴权

CSCF请求拜访网络中的核心网络资源

Mc参考点

本参考点接口完成 MGCF与MGW，MSC Server与MGW ，GMSC Server与MGW之间的信息传递，包括：

兼容ITU-T SG16与IETF MEGACO WG的 H.248标准

完成灵活的连接处理，支持不同的呼叫模型，不同的媒体处理

支持开放的结构，支持控制的分组的接口定义.

支持对MGW的物理节点资源的动态共享，一个物理上的 MGW可以逻辑上分为多个虚拟的 MGWs/domains，每个虚拟的MGW支持静态配置的终端。

动态共享传输资源

Mc接口的功能还需要支持移动相关的特性，如：SRNS重新分配/切换。

Mg参考点

本参考点接口完成MGCF与CSCF之间的信息传递，包括：Mg接口可能采用SIP标准。

Mm参考点

本参考点是CSCF与外部IP网络之间的接口，用于从另一个 VoIP呼叫控制服务器或终端的呼叫请求。

Mr参考点

本参考点是CSCF与MRF之间的接口，允许 CSCF 控制MRF中的资源。

Ms参考点

本参考点是CSCF与R-SGW之间的接口。

Mw参考点

本参考点是CSCF与CSCF之间的接口，用于I－CSCF转发移动终端的呼叫到S－CSCF。

到SCP的参考点

本参考点是包括从SGSN到SCP，从S－CSCF（或I－CSCF）到SCP，从MSC Server到SCP，从GMSC Server到SCP之间的接口。从 CSCF 到SCP的接口需要支持现有的基于CAMEL的业务。

3.2 主要接口协议

典型的WCDMA网络模型如下：

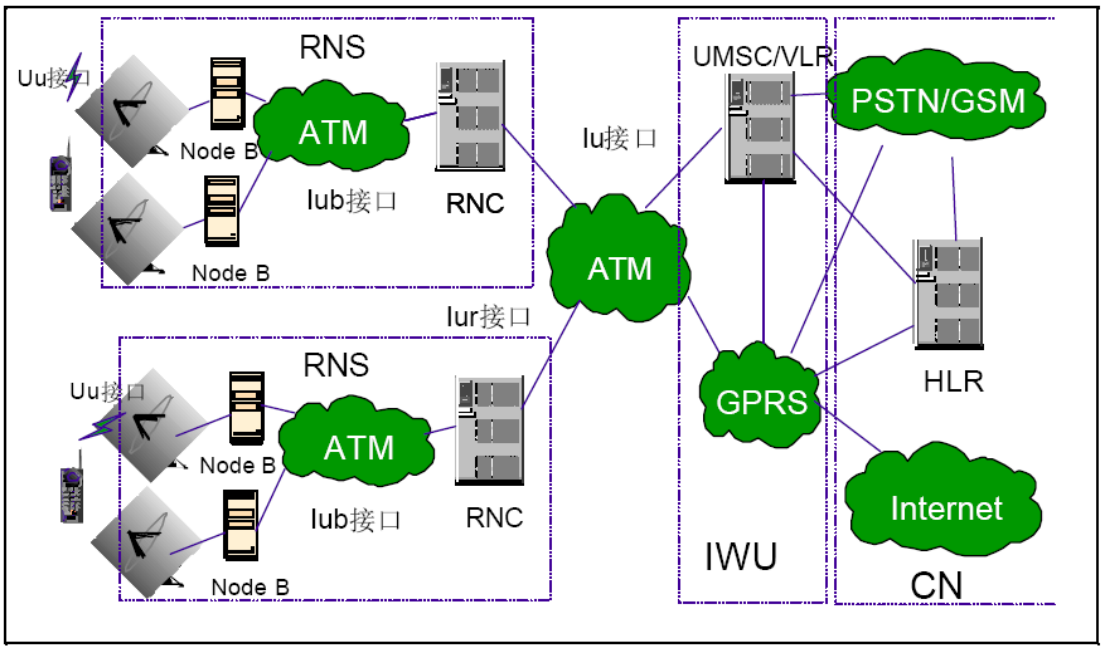


图 3-6 WCDMA 网络模型

WCDMA网络的标准接口主要包括Uu 、Iub、Iur、Iu等。WCDMA的网络接口具有以下三个特点：

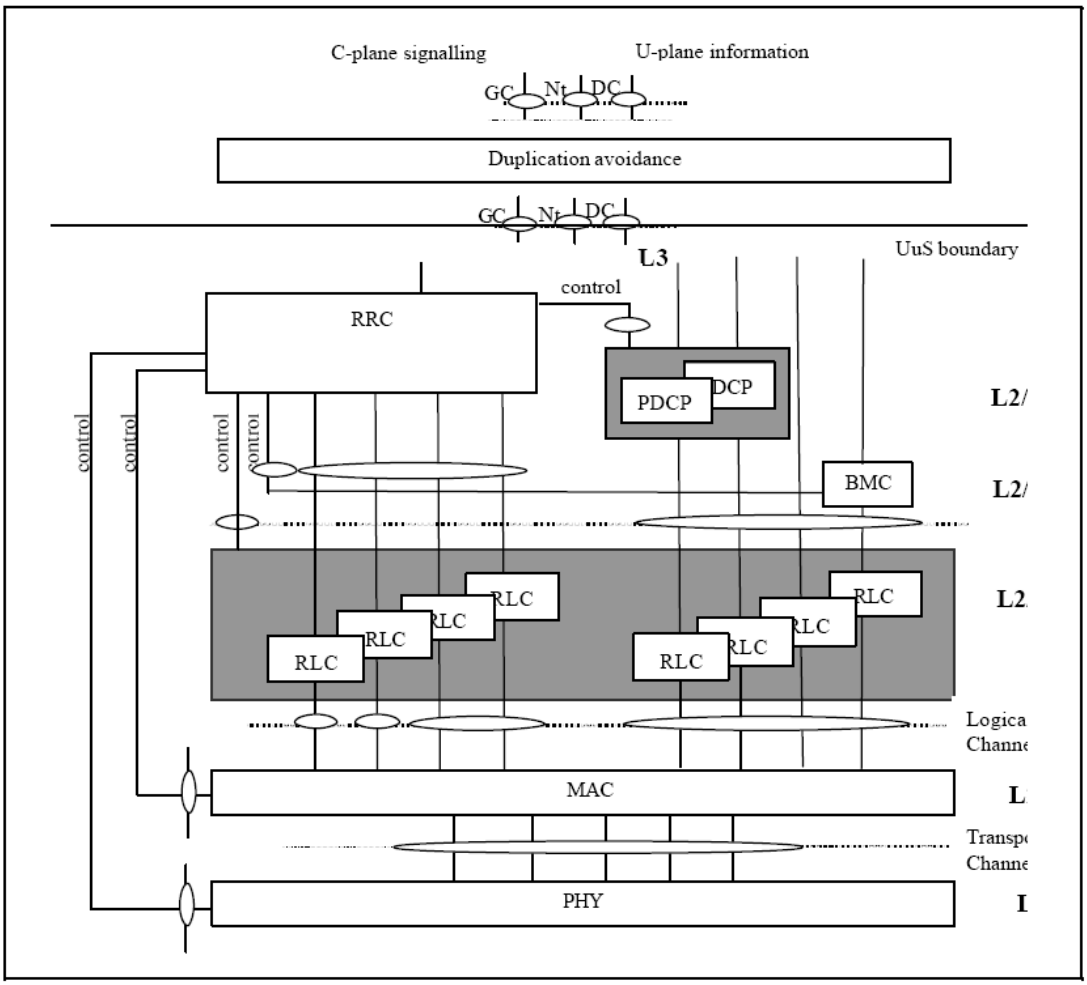
所有接口具有开放性；

将无线网络层与传输层分离；

控制面和用户面分离。

3.2.1 Uu接口

1. Uu接口协议



GC：通用控制　　BMC：广播/多点传送控制协议

Nt：通知　　RLC：无线链路控制

DC：专用控制　　MAC：媒体接入控制

RRC：无线资源控制　　PHY：物理层

PDCP：分组数据会聚协议

图3-7　无线接口协议结构

无线接口一般指用户设备（ UE）和网络之间的Uu接口。无线接口的协议结构如图1-12所示，无线接口分为三个协议层：

物理层（L1）；

数据链路层（L2）；

网络层（L3）。

L2被进一步分成媒体接入层（ MAC）、无线链路控制层（RLC）、分组数据会聚协议层（PDCP）和广播/多点传送控制层（BMC）。

L3和RLC被分成控制面和用户面。PDCP和BMC仅在用户面存在。

在控制面， L3被分成几个子层。处于最 底的子层被称为无线资源控制层（RRC），它属于接入层，终止于UTRAN。RRC之上的子层提供“复制避免（Duplication avoidance)”

功能，它终止于CN，向高层提供非接入层业务。高层信令如移动管理（MM）和呼叫控制（CC）属于非接入层。

RLC子 层提供与无线传输技术紧密相关的自动重复请求（ARQ）功能。

RLC在控制平面和用户平面上没有差别。

图中的方框代表对应协议的一个实体。同层通信的业务接入点 (SAPs)用圆圈在层与层之间的接口处标识。位于MAC和物理层之间的业务接入点提供传输信道。位于RLC和MAC之间的业务接入点提供逻辑信道。在控制面里，复制避免”和高层（移动管理，呼叫管理）之间的接口被定义为通用控制、通知和专用控制业务接入点。

从图中可以看到：在RRC和RLC，RRC和MAC，RRC和L1，RRC和PDCP以及RRC和 BMC之间存在连接。RRC通过这些接口控制低层的配置。因此，在RRC和每个低层（ PDCP、RLC、MAC和L1）之间分别定义了一个独立的控制业务接入点。

2. Uu接口一般原则

Uu接口是一个开放的接口，实现不同厂商的NodeB和UE进行互连；

物理层功能基本上在NodeB实现；

MAC层以上协议基本上在RNC终结，无线资源由RNC集中管理；

采用逻辑信道/传输信道/物理信道3层映射关系；

测量根据RRM算法需要可配置，NodeB对测量报告不做处理。

3. Uu接口功能

广播、寻呼和RRC连接功能；

切换和功率控制的判决和执行；

无线资源的管理和控制；

WCDMA基带和射频处理。

3.2.2 Iub接口

Iub接口是RNC与NodeB之间的接口。

1. Iub接口协议

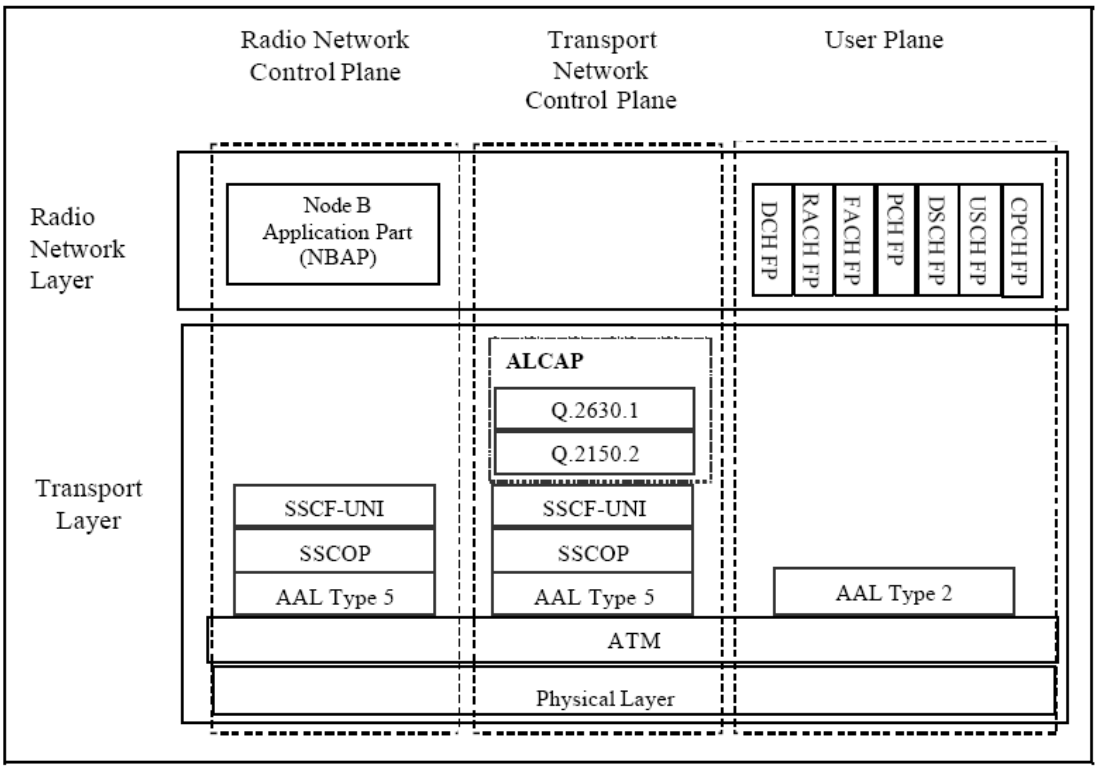


图 3-8 Iub 接口协议图

Iub 接口协议结构由两个功能层组成：

无线网络层，规定与 Node B 操作相关的程序。由无线网络控制平面和无线网络用户平面组成。

传输层，规定了在 Node B 和 RNC 之间建立网络连接的程序。每个 RACH、每个 FACH 和每个 CPCH 传输信道都应有一个专用的 AAL2 连接。

无线网络层和传送层有着明显的区分。因此，无线网络信令和 Iub 数据流与数据传送资源和业务的处理是区分开来的，如图 3-9 所示。资源和业务的处理由传送信令来控制。传送信令由 Iub 接口上的信令承载来传递。

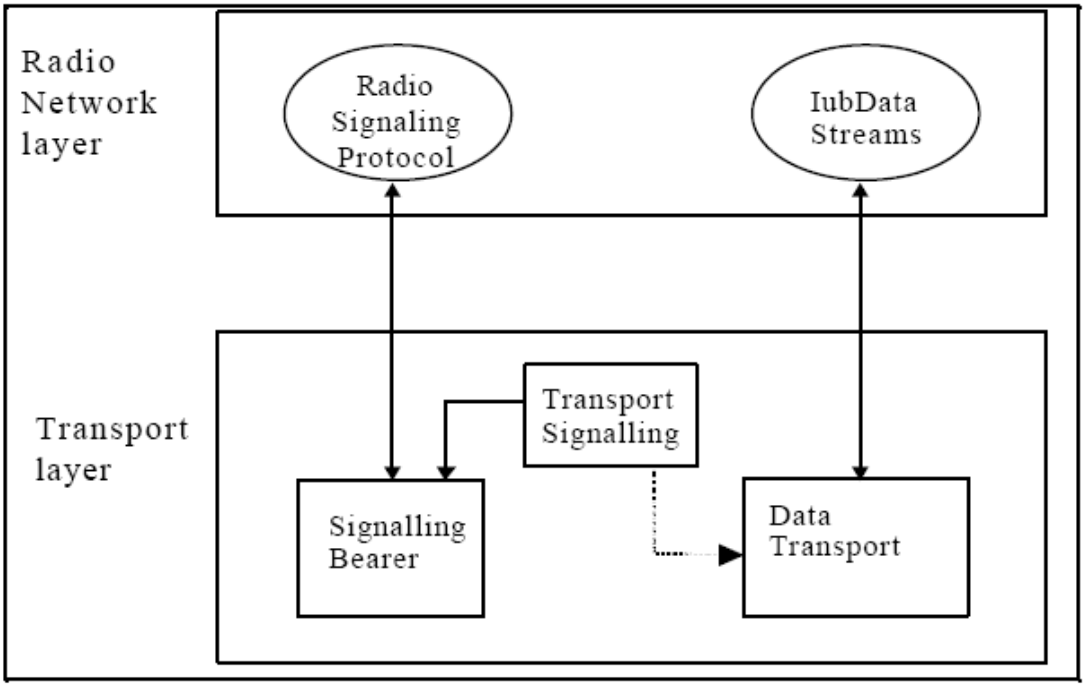


图3-9 无线网络协议的区分和在Iub上的传送

2. Iub接口的一般原则

Iub接口开放，实现不同厂家的RNC和NodeB 的互连；开放Iub接口后，可以用不同厂商的NodeB设备建设WCDMA网络，组网方式灵活。

Iub接口支持NodeB的逻辑O&M；

Iub接口无线网络功能和传输网络功能的分离，以便未来引进新技术。

3. Iub接口能力

在Iub接口上传送的信息包括：

与无线应用相关的信令

Iub接口允许RNC和Node B之间协商无线资源，如增加和删除Node B控制的小区。控制广播信道和寻呼信道的信息和要在广播信道和寻呼信道上传输的信息也要通过Iub接口传输。此外，还包括Node B和RNC之间的O&M信息。

DCH数据流

Iub接口提供上、下行DCH Iub帧在RNC与Node B之间的传输方法，DCH数据流对应于在DCH传送信道上传递的数据。

RACH数据流

Iub接口提供上行RACH传输帧在RNC与BTS之间的传输方法，RACH数据流对应于在RACH传送信道上传递的数据。

FDD CPCH数据流

Iub提供接口提供上行CPCH帧在RNC与BTS之间的传输方法。

FACH数据流

Iub接口提供下行FACH传输帧在RNC与BTS之间的传输方法，FACH数据流对应于在FACH传送信道上传递的数据。

DSCH数据流

Iub 接口提供下行共享信道，DSCH数 据帧 在RNC与BTS之间的传输方法，DSCH数据流对应于用于一个UE的DSCH传送信道上传递的数据。一个UE可以有多个DSCH数据流。

TDD USCH数据流

Iub接口提供上行共享信道，USCH数据帧在RNC与BTS之间的传输方法。

PCH数据流

Iub接口提供PCH传输帧在RNC与BTS之间的传输方法。PCH数据流对应于在PCH传送信道上传递的数据。

4. Iub的功能

Iub接口的功能有：

(1) 传送资源的管理

是指对由传送信令控制的传送资源进行管理，即对信令承载进行管理。

(2) NodeB的操作与维护，包括

Iub链路管理

小区配置管理

无线网络性能管理

资源管理

公共传输信道管理

无线资源管理

系统信息升级

(3) 实现专用的O&M传送

(4) 公共信道的流量管理

管理控制

功率控制

数据传送

(5) 专用信道的流量管理

无线链路建立

信道分配/取消分配

功率管理

测量报告

专用传输信道管理

数据传送

(6) 下行共享信道的流量管理

信道分配/取消分配

功率管理

传输信道管理

数据传送

(7) 上行共享信道的流量管理

信道分配/取消分配

功率管理

传输信道管理

数据传送

(8) 定时和同步管理

传输信道同步（帧同步）

基站-RNC同步

基站间同步

3.2.3 Iur接口

UTRAN内任何两个RNC之间的逻辑连接被称作Iur接口。

1. Iur接口协议结构

Iur接口协议结构包括下面两个功能层：

无线网络层，定义了在PLMN内与两个RNCs 的相互作用相关的程序。无线网络层包括一个无线网络控制平面和一个无线网络用户平面。

传送层，定义了用于在PLMN内两个RNCs之间建立物理连接的程序。

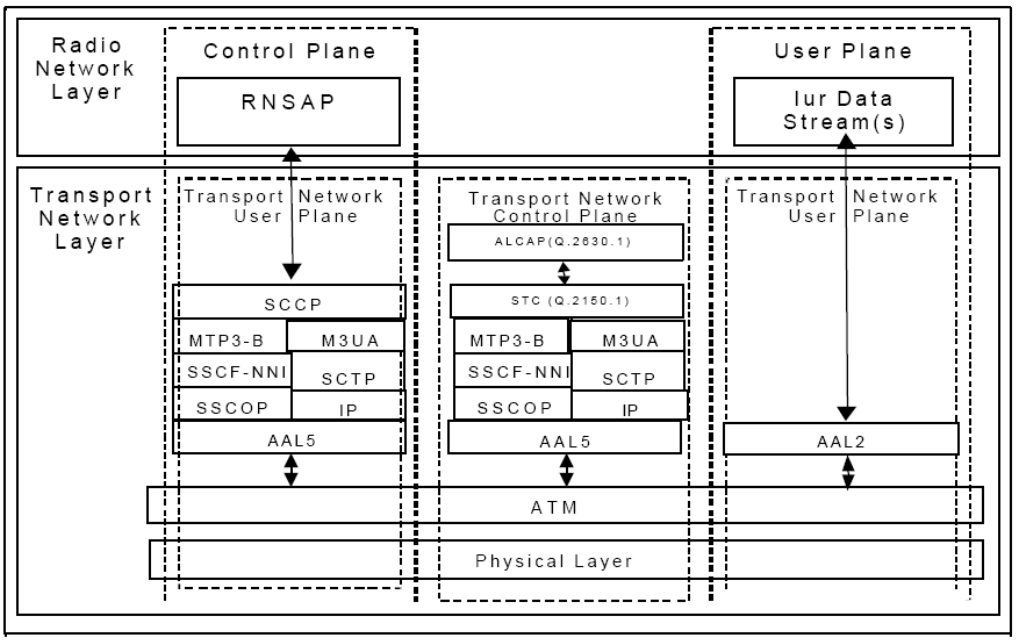


图3-10 Iur接口协议结构

在无线网络层和传送层之间存在着明显的区别。因此，无线网络信令和 Iur 数据流与数据传送资源和业务处理是分开的，如图 3-11 所示。数据传送资源和业务处理由传送信令控

制。传送信令由 Iur 接口的一个信令承载来传递。

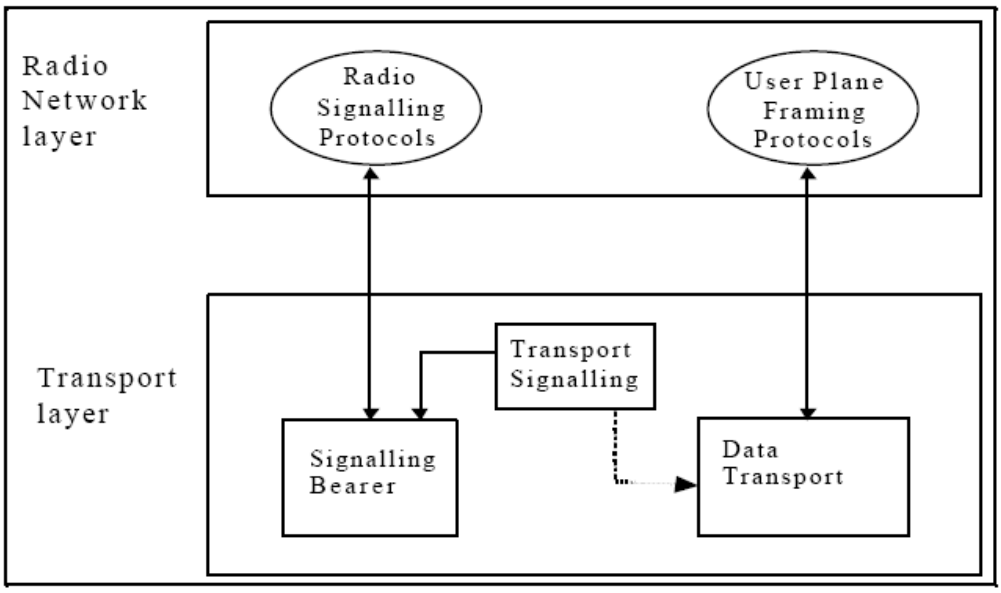


图3-11 无线网络协议和Iur上传送的区分

2. Iur接口上DRNS逻辑模型

图3-12的模型显示了从SRNC看到的漂移无线网络子系统。它做成一个“黑箱”模块，在黑箱的Uu侧为无线链路集合，在Iur一侧为用户平面接入端口集合。

无线链路与Iur用户端口通过 DRNS的内部传送机制连接在一起。在端口间的连接的控制操作是从SRNC通过Iur控制平面端口发送到DRNC的。

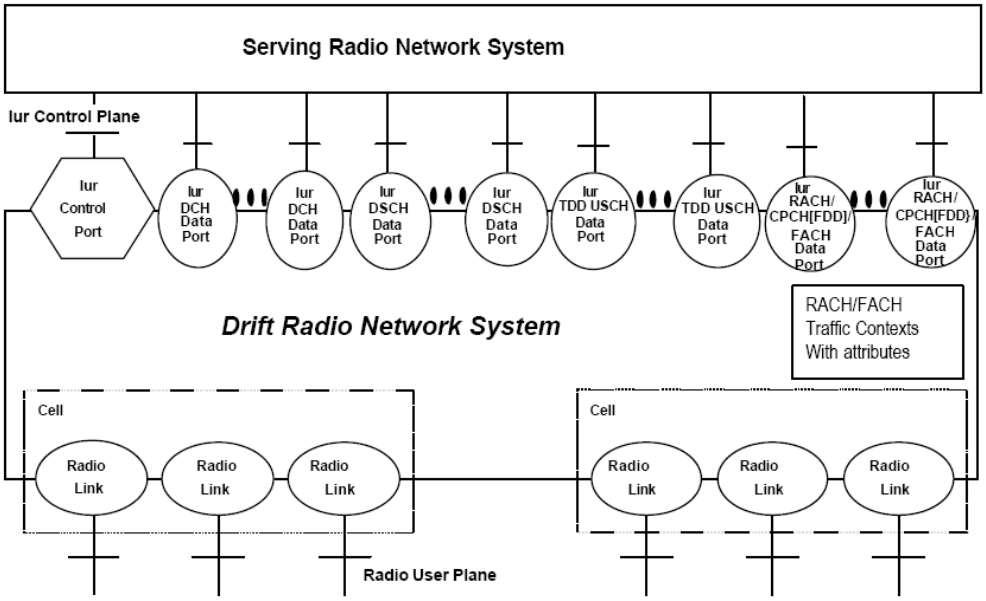


图 3-12 漂移 RNS 逻辑模型

3. Iur接口一般原则

Iur接口是一个开放的接口，实现不同厂商的RNC之间互连。

实现接口上无线网络层与传输网络层的分离，使得各自可以引入更新的技术。

Iur接口将支持两个RNCs之间的信令信息的交换，另外该接口应能支持一个或多个Iur数据流。

从逻辑的观点来看，Iur是两个RNCs之间的一个点到点的接口。即使在两个RNCs之间缺少物理上的直接连接时，点到点的逻辑接口也应能实现。

如果RRC连接是基于专用信道，Iur标准允许增加/删除属于任何RNS（同一PLMN内）的小区的无线链路。

Iur接口规范允许一个RNC可以访问任何其它RNC（同一PLMN内）以建立Iur信令承载。

Iur接口规范允许一个RNC可以访问任何其它RNC（用一PLMN内）以建

立Iur数据承载。

RNSAP允许使用多种的访问机制作为信令承载。

4.Iur接口能力

（1）在Iur接口上传输的信息可以分成如下几类：

与无线应用相关的信令

Iur接口应提供支持RNSs间无线接口的移动性的能力，它包括对切换、无线资源的处理和RNSs间同步的支持。

Iub/Iur DCH数据流

Iur接口提供上行和下行Iub/Iur DCH帧传输的方法，通过DRNC来传递SRNC和Node B(DRNS)之间的用户数据和控制信息。

Iur RACH/CPCH［FDD］数据流

Iur DSCH数据流

Iur DSCH数据流对应于用于一个UE的在一个DSCH传输信道上传递的数据。UE可以有多个Iur DSCH数据流。

Iur接口提供上行和下行MAC-c/sh SDUs传输的方法。另外，它也能为SRNC提供报告排队情况的方法，为DRNC提供到SRNC的容量分配的方法。

［TDD Iur USCH数据流］

Iur USCH数据流对应于用于一个 UE的在一个USCH传输信道上传递的数据。

UE可以有多个Iur USCH数据流。

Iur RACH/CPCH［FDD］数据流

Iur FACH 数据流

（2）Iur接口特性

Iur接口使用SCCP来支持RNC之间的信令消息，同时定义了RNSAP为SCCP的一个用户功能。对于每一对DRNC与UE，RNSAP使用一条信令连接。

SCCP 具有面向连接与面向无连接的过程。

目前，SCCP连接总是由 SRNC发起（典型情况是伴随着 RADIO LINK SETUP REQUEST

消息），SCCP 释放是由SRNC发起。

RNSAP可以使用SSN、SPC和/或GT及它们的组合作为SCCP 访问机制。

5. Iur接口协议的功能

(1) 传送网络管理

(2) 公共传送信道的业务管理

公共传送信道资源的准备

寻呼

(3) 专用传送信道的业务管理

无线链路的建立/增加/删除

测量的上报

(4) 下行共享传送信道和［TDD 上行共享传送信道］的业务管理

无线链路的建立/增加/删除

容量的分配

(5) 公共和专用测量目标的测量报告

3.2.4 Iu接口

1. 概述

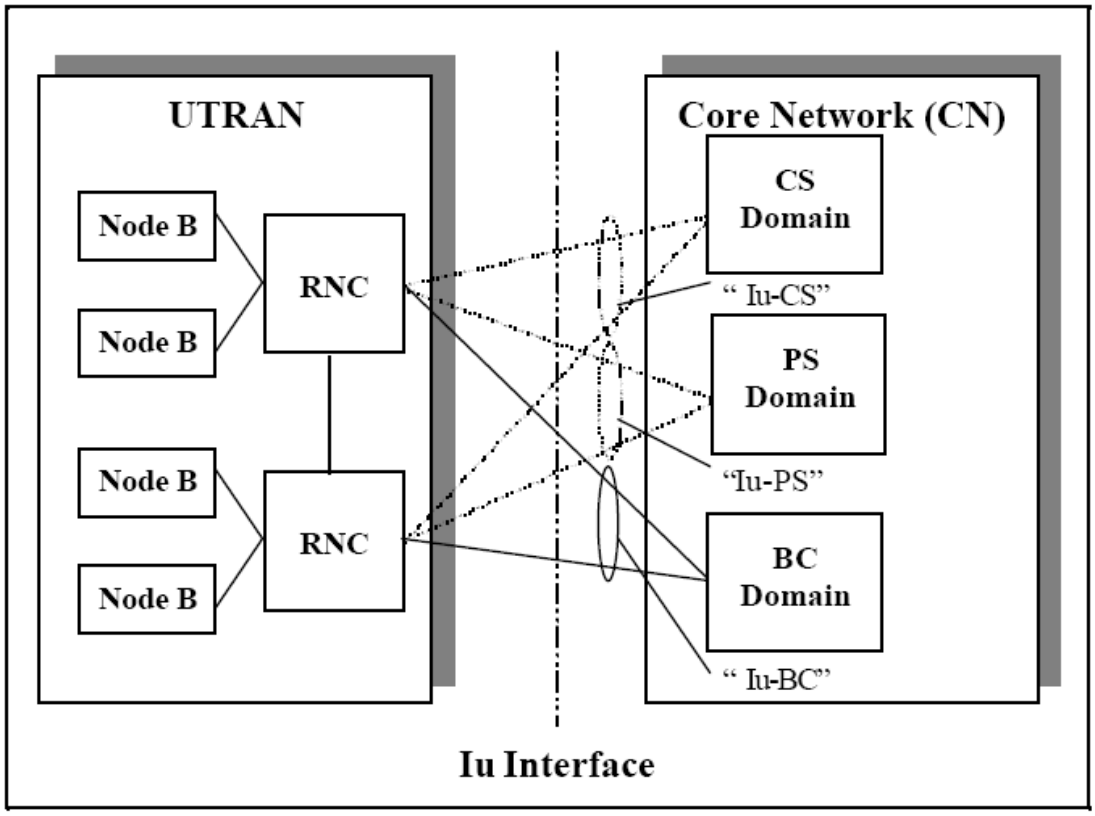


图3-13 核心网和UTRAN之间的接口图

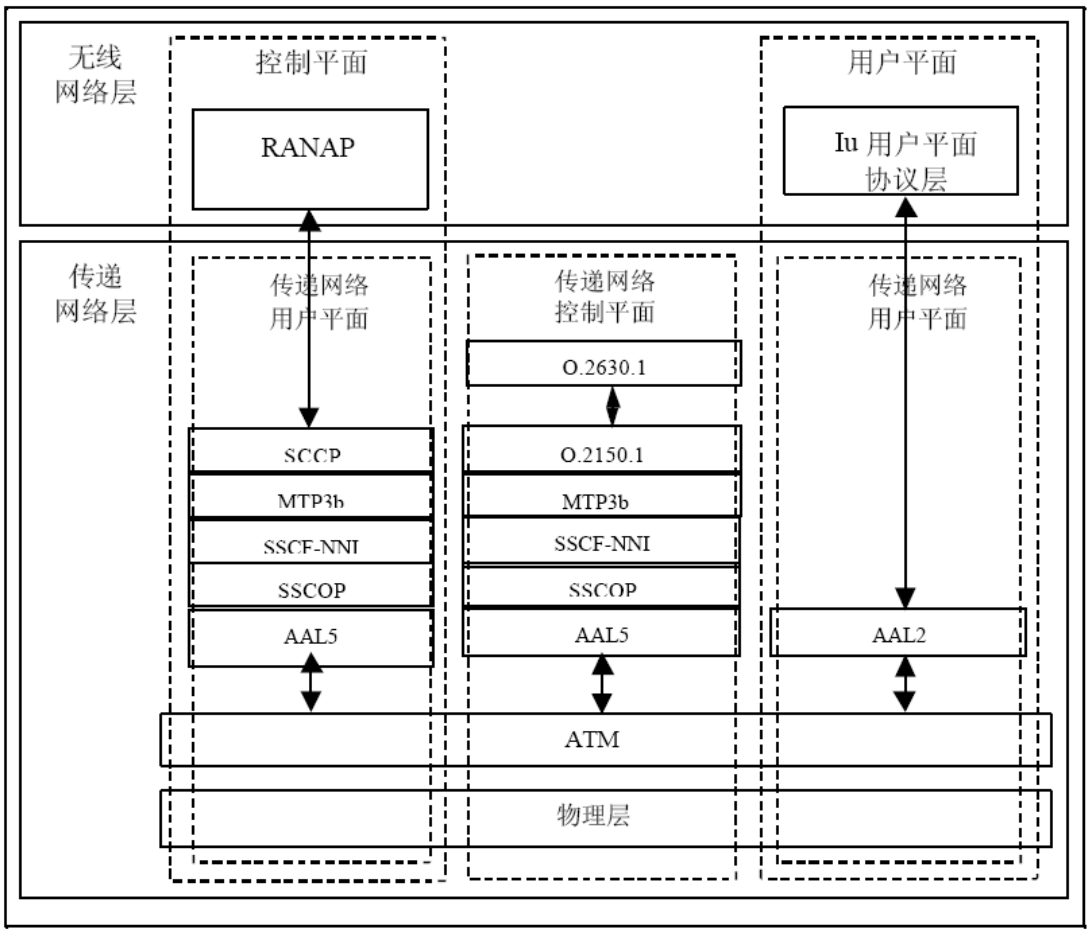
Iu接口规定了核心网和UTRAN之间的接口，如图3-13所示，对于一个RNC最多存在3个不

同的Iu接口：与CS域（核心网电路交换部分）连接的Iu-CS（面向电路交换域）；与PS域（核心网分组交换部分）连接的Iu-PS（面向分组交换域）；与BC域连接的Iu-BC（面向广播域）。对于PS与CS分开的核心网结构，CS和PS两个域中存在各自的信令连接和用户数据连接，对传输层和无线网络层均是如此。对于PS与CS组合在一起的核心网结构，CS和PS两个域中存在各自的用户数据和SCCP连接，对无线网络层和传输层均是如此。对于CS域，一个RNC至多能连接到一个CN接入点上。对于PS域，一个RNC连接到一个CN接入点上。对于BC域，一个RNC可连接到多个CN接入点上。

2. Iu接口协议结构

同其他接口的协议栈类似，Iu接口的协议栈在纵向分为两个平面：控制平面和用户平面；在横向分为两个层次：无线网络层和传输网络层。“RANAP”和“Iu UP协议层”分别为无线网络层上Iu接口上的控制面协议和用户面协议。Iu接口的无线网络信令由无线接入网络应用部分RANAP和业务域广播协议SABP构成， RANAP和SABP 协议构成处理CN和UTRAN之间所有程序的机制。RANAP可以透明地在CN和UE之间传送消息而不需要UTRAN解释和处理。

根据CN节点所处的域不同，Iu接口协议栈又分为面向电路交换域和面向分组交换域两种结构，如图3-14和图3-15所示。面向电路交换域在传输网络层是采用直接通过AAL2或AAL5映射到 ATM的形式，而面向分组交换域在传输网络层则是采取IP over ATM的形式。



注意：AAL5只用于作信令适配，AAL2可用于信令或用户数据的适配。

图3-14 Iu-CS的协议结构

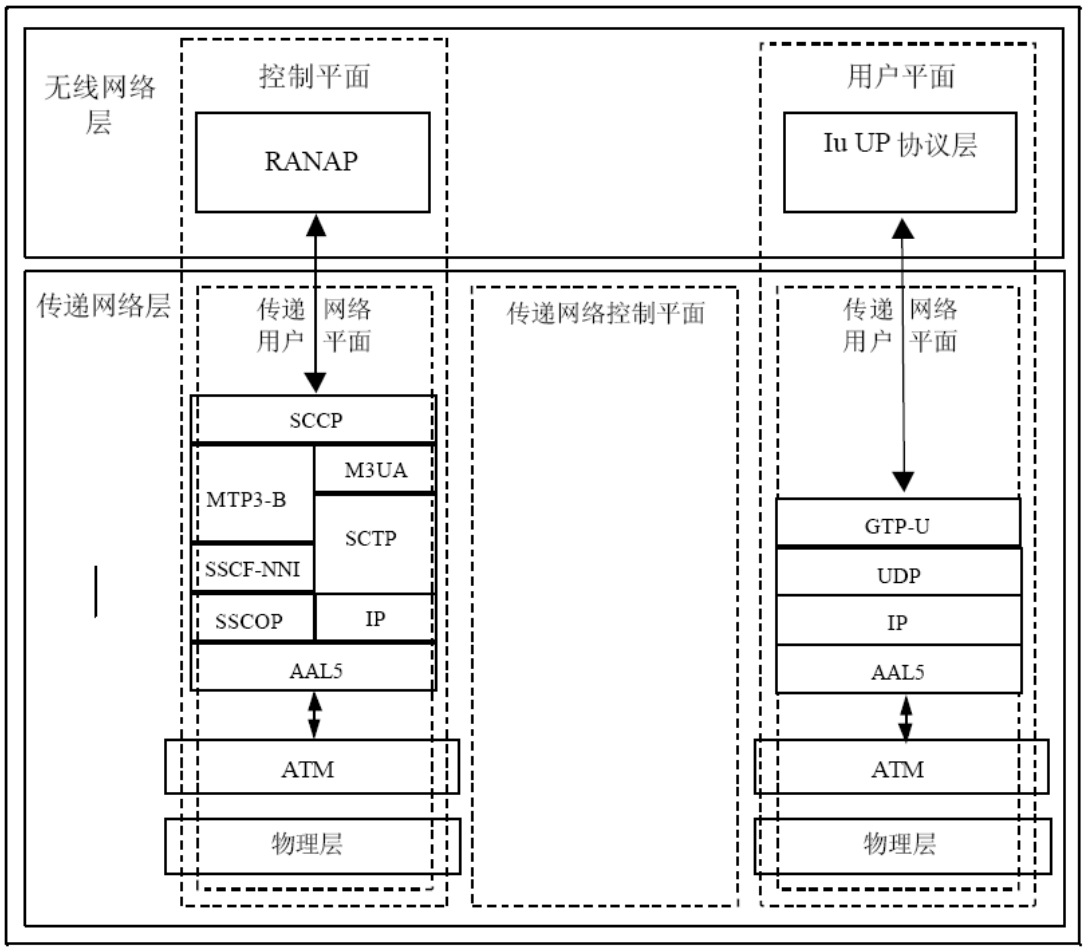


图 3-15 Iu-PS的协议结构

(1) Iu 接口的协议分成两个平面：

用户平面协议：实现无线接入业务，即通过接入层传送用户数据。

控制平面协议：用于控制UE和网络之间的无线接入载体和连接（包括请求的业务，控制不同的传输资源，切换和流量等）。还包括NAS消息的透明传输。

(2) Iu连接原则

Iu接口具有分层结构，某个高层实体控制若干低层实体。

每个CN接入点可以连接到多个RNC接入点

对每个CN域，每个RNC接入点只能连接到一个CN接入点

3. Iu接口一般原则

Iu接口是一个开放的、多厂商设备兼容的标准接口；

Iu支持在协议层的UE的分离；

Iu支持UE与CN之间的透明非接入层信令的传输；

对于控制面和用户面，Iu规则必须支持无线网络层和传输网络层分离，

允许他们各自独立改变。

4. Iu接口能力

Iu接口支持：

建立、维护和释放无线接入承载的程序；

完成系统内切换、系统间切换和SRNS重定位的程序；

支持小区广播业务的程序；

与特定UE无关的一系列程序；

在协议等级上为用户特定信令管理分离每个用户；

UE和CN之间NAS信令消息的传送；

从CN向UTRAN传送请求的位置业务，和从UTRAN到CN的位置信息。位置信息可以包括地理区识别符或与未定参数的坐标；

为单个UE立即接入多个CN域；

为分组数据流资源预留的机制。

5. Iu接口特性

(1) 信令承载

传送CN和RNC之间的信令消息使用SCCP。为此规定一个SCCP的用户功能模块，称为无线接入网应用部分（ RANAP）。RANAP使用SCCP的无连接和面向连接业务。RANAP 可以用 SSN、 SPC和 GT 以及它们的任何组合进行SCCP 的寻址。

(2) 用户数据承载

使用AAL2做为到CS的用户数据承载；

AAL2协议用于动态建立Iu接口到CS的AAL-2连接；

使用GTP-U做为到PS的用户数据承载；

RANAP信令用于建立、修改和释放到PS的GTP-U通道。

6. Iu接口协议的功能划分

Iu接口功能

处理CN和UTRAN间的各种过程；

在CN和UE间透明地传输信息。

本节定义了核心网和UMTS无线接入网络之间的功能，表2-3列出了核心网和无线接入网之间的功能。

表3-3 Iu接口的功能划分

功能	UTRAN	CN
RAB 管理功能:		
RAB 建立、修改和释放	X	X
RAB 特性映射 Iu 传输承载	X	
RAB 特性映射 Uu 承载	X	
RAB 询问、占先和优先级	X	X

无线资源管理功能：		
无线资源接纳控制	X	
广播信息	X	X
Iu 链路管理功能：		
Iu 信令链路管理	X	X
ATM VC 管理	X	X
AAL2 建立和释放	X	X
AAL5 管理	X	X
GTP-U 隧道管理	X	X
TCP 管理	X	X
缓冲区管理	X	
Iu 用户平面 (RNL) 管理:		
Iu 用户平面帧协议管理		X
Iu 用户平面帧协议初始化	X	
移动性管理功能 ：		
位置信息报告	X	X
切换和重定位	X	X
RNC 之间硬切换, Iur 未使用或不可用	X	X
服务 RNS 重定位(MSC 内/MSC 间)	X	X
系统间硬切换(UMTS-GSM)	X	X
寻呼触发		X
安全功能：		
数据保密		
无线接口加密	X	
密钥管理		X
用户识别保密	X	X
数据完整性		
完整性检查	X	
完整性钥管理		X

第四章　基本信令流程

4.1 UE的状态与寻呼流程

4.1.1 UE状态

UE有两种基本的运行模式：空闲模式和连接模式。上电开始，UE就停留在空闲 模式下 ，通 过非 接 入 层标识如IMSI、 TMSI 或 P-TMSI等 标志来区分。

UTRAN不保存空闲模式UE的信息，仅能够寻呼一个小区中的所有UE或同一个寻呼时刻的所有UE。

当 UE 完 成 RRC 连接建立时， UE才从空闲模式转移到连接模式 ：

CELL_FACH或CELL_DCH状态。 UE的连接模式，也叫UE的RRC状态，反映了UE 连接的级别以及 UE可以使用哪一种传输信道。当RRC连接释放时，UE从连接模式转移到空闲模式。

UE在连接模式下，一共有如下4种状态：

1. CELL_DCH状态

CELL_DCH状态有如下特征：

在上行和下行给UE分配了一个专用物理信道

根据UE当前的活动集可以知道UE所在的小区

UE可以使用专用传输信道、下行/上行共享传输信道或这些传输信道的组合

UE进入CELL_DCH状态有如下2种方法：

1） UE在空闲模式下，RRC连接建立在专用行道上，因此UE从空闲模式进入CELL_DCH状态；

2） UE处于CELL_FACH状态下使用公共传输信道，通过信道切换后使用专用传输信道，UE从CELL_FACH状态进入到CELL_DCH状态。

2. CELL_FACH状态

CELL_FACH状态具有如下特征：

没有给UE分配专用传输信道

UE连续监听一个下行FACH信道

为UE 分配了一个默认的上行公共信道或上行共享传输信道（例如，RACH），使之能够在接入过程中的任何时间内使用

UE的位置在小区级为UTRAN所知，具体为UE最近一次发起小区更新时报告的小区

在CELL_FACH子状态，UE执行下面的动作：

监听一个FACH

监听当前服务小区的BCH传输信道，解码系统信息消息

在小区变为另一个UTRA小区时，发起一个小区更新过程

除非选择了一个新小区，否则使用在当前小区中分配的C-RNTI作为公共传输信道上的UE标识

在RACH上传送上行控制信令和小数据包

在CELL_FACH状态下，如果数据业务在一段时间里 未被激活，UE 将进入CELL_PCH状态，以减少功率的损耗。并且，当UE暂时脱离CELL_PCH状态执行小区更新，更新完成后，如果UE和网络侧均无数据传输需求，它将返回CELL_PCH。

3. CELL_PCH 状态

CELL_PCH状态具有如下特征：

没有为UE分配专用信道

UE使用非连续接收（DRX）技术，在某个特定的寻呼时刻监听PCH传输信道上的信息不能有任何上行的活动

UE的位置在小区级为UTRAN所知，具体为UE在CELL_FACH状态时最近一次发起小区更新时所报告的小区

在CELL_PCH状态，UE进行以下活动：

根据DRX 周期监听寻呼时刻，并接收PCH上的寻呼消息

监听当前服务小区的BCH传输信道，以解码系统信息

当小区改变时发起小区更新过程

在该状态下不能使用 DCCH逻辑信道。如果网络试图发起任何活动，它需要在UE所在小区的PCCH逻辑信道上发送一个寻呼请求。

UE转换到CELL_FACH状态的方式有两个，一是通过 UTRAN寻呼，二是通过任何上行接入。

4. URA_PCH状态

URA_PCH状态具有如下特征：

没有为UE分配专用信道

UE使用DRX技术，在某个特定的寻呼时刻监听PCH传输信道上的信息

不能有任何上行的活动

UE的位置在URA级为UTRAN所知，具体为 UE在CELL_FACH状态时最近一次发起URA更新时所报告的URA

在URA_PCH状态，UE进行以下活动：

根据DRX周期监听寻呼时刻，并接收PCH上的寻呼消息

监听当前服务小区的BCH传输信道，以解码系统信息

当URA改变时发起URA更新过程

在该状态下不能使用 DCCH逻辑信道。如果网络试图发起任何活动，它需要在UE所在URA的PCCH逻辑信道上发送寻呼请求。

在URA_PCH状态， 没有资源分配给数据传输用。因此，如果UE有数据要传送，需要首先转换到CELL_FACH状态。

4.1.2 寻呼流程

与固定通信不同，移动通信中的通信终端的位置不是固定的，为了建立一次呼叫，核心网（ CN）通过Iu接口向UTRAN发送寻呼消息， UTRAN则将CN寻呼消息通过Uu接口上的寻呼过程发送给 UE，使得被寻呼的UE发起与CN的信令连接建立过程。

当UTRAN收到某个CN域（CS域或PS域）的寻呼消息时，首先需要判断UE是否已经与 另一个 CN域建立了信令连接 。如果没有建立信令连接 ，那么UTRAN只能知道UE当前所在的服务区，并通过寻呼控制信道将寻呼消息发送给UE ，这 就是PAGING TYPE 1 消 息 ； 如 果 已经建立信令连接 ，在CELL_DCH或CELL_FACH状态下， UTRAN就可以知道UE当前活动于哪种信道上，并通过专用控制信道将寻呼消息发送给UE，这就是PAGING TYPE 2消息。因此针对UE所处的模式和状态，寻呼可以分为以下两种类型。

1. 寻呼类型

(1) 寻呼空闲模式或PCH状态下的UE

这一类型的寻呼过程使用PCCH（寻呼控制信道）寻呼处于空闲模式、CELL_PCH或URA_PCH状态的UE，用于向被选择的UE发送寻呼信息，其作用有如下三点：

为了建立一次呼叫或一条信令连接，网络侧的高层发起寻呼过程；

为了将UE的状态从CELL_PCH或URA_PCH状态迁移到CELL_FACH状态，UTRAN发起寻呼以触发UE状态的迁移；

当系统消息发生改变时，UTRAN发起空闲模式、CELL_PCH和URA_PCH状态下的寻呼，以触发UE读取更新后的系统信息。

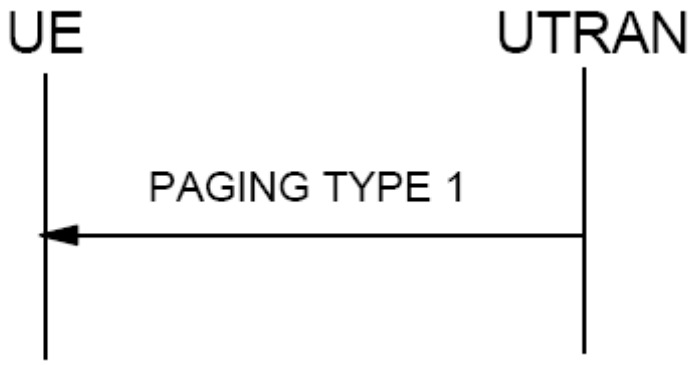


图 4-1 寻呼空闲模式和 PCH 状态下的 UE

UTRAN通过在PCCH上一个适当的寻呼时刻发送一条PAGING TYPE 1消息来启动寻呼过程，该寻呼时刻和 UE的IMSI有关。UTRAN可以选择在几个寻呼时机重复寻呼一个UE，以增加UE正确接收寻呼消息的可能。

(2) 寻呼CELL_DCH或CELL_FACH状态下的UE

这一类型的寻呼过程用于向处于连接模式CELL_DCH或CELL_FACH状态的某个UE发送专用寻呼信息。

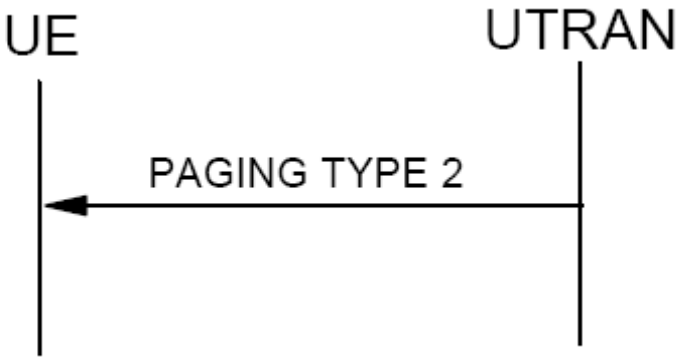


图 4-2 寻呼 CELL_DCH 或 CELL_FACH 状态下的 UE

对于处于连接模式CELL_DCH或CELL_FACH状态的UE，UTRAN通过在图6-2寻呼CELL_DCH或CELL_FACH状态下的UE

对于处于连接模式CELL_DCH或CELL_FACH状态的UE，UTRAN 通 过 在DCCH（专用控制信道）上发送一条PAGING TYPE 2消息来发起专用寻呼过程。这种寻呼也叫做专用寻呼过程。

2. 寻呼过程举例

1）CN发起寻呼，UE处于空闲模式

在这种情况下，UTRAN通过发送PAGING TYPE 1消息来寻呼UE。

2）CN发起寻呼，UE处于连接模式的CELL_DCH或CELL_FACH状态

在这种情况下，UTRAN通过发送PAGING TYPE 2消息来寻呼UE。

3）CN发起寻呼，UE处于连接模式的CELL_PCH或URA_PCH状态

在这种情况下， UTRAN首先通过发送 PAGING TYPE 1消息将UE 的状态从CELL_PCH或URA_PCH状态迁移到 CELL_FACH状态，然后再发送PAGINGTYPE 2消息来寻呼UE。

4）UTRAN发起寻呼，UE处于连接模式的CELL_PCH或URA_PCH状态

在这种情况下，UTRAN通过发送PAGING TYPE 1消息来寻呼UE，使得UE迁移到CELL_FACH状态。

4.2 空闲模式下的UE

4.2.1 概述

当UE开机后或在漫游中，它的首要任务就是找到网络并和网络取得联系。只有这样，才能获得网络的服务。因此，空闲模式下UE的行为对于UE是至关重要的。那么，UE是如何完成这个功能的呢？本节就来讲解这个过程。

UE在空闲模式下的行为可以细分为PLMN选择和重选，小区的选择和重选和位置登记。这三个过程之间的关系如图4-3所示。

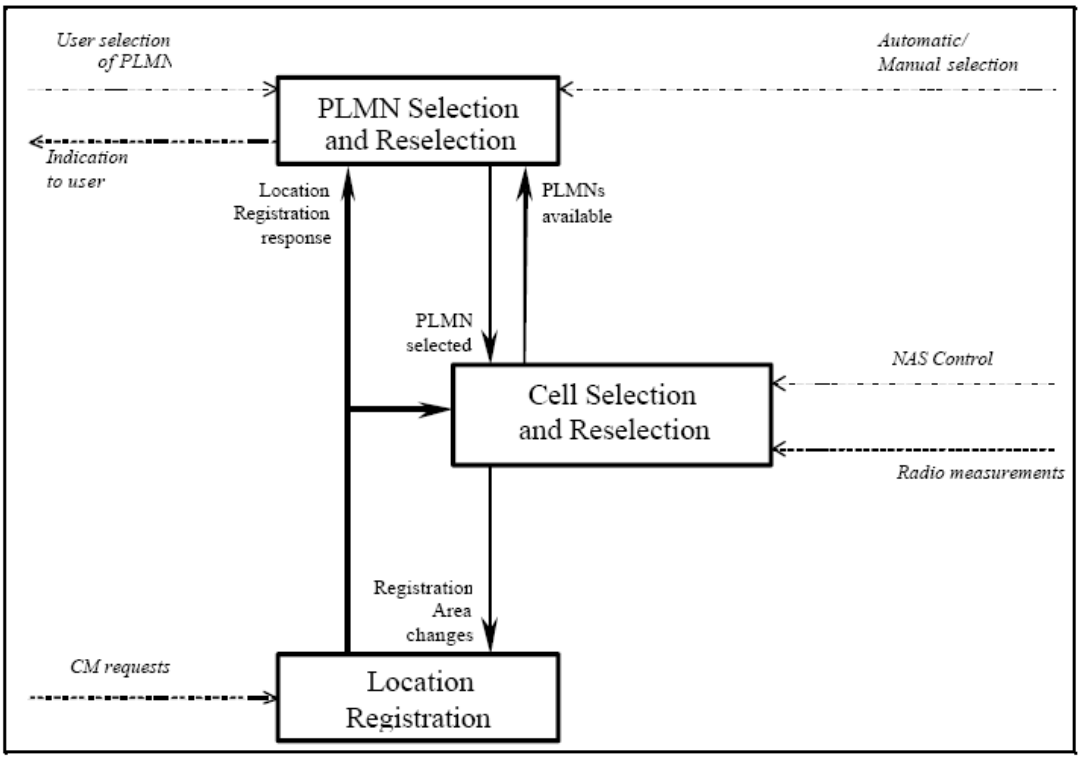


图 4-3 Overall Idle Mode process

当UE开机后，首先应该选择一个PLMN。当选中了一个 PLMN后，就开始选择属于这个PLMN的小区。当找到这样的一个小区后，从系统信息（广播）中就可以知道临近小区（neighboring cell）的信息，这样，UE就可以在所有这些小区中选择一个信号最好的小区，驻留下来。紧接着，UE就会发起位置登记过程（attach or location update）。成功后，UE就成功的驻留在这个小区中了。驻留的作用有4个：

使UE可以接受PLMN广播的系统信息。

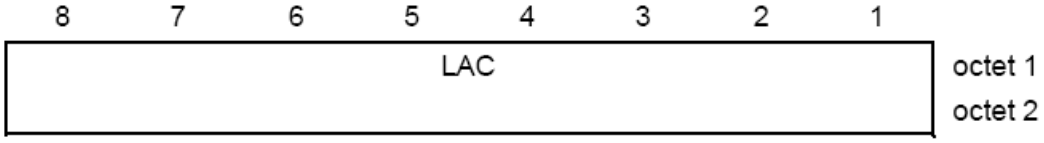
可以在小区内发起随机接入过程。

可以接收网络的寻呼。

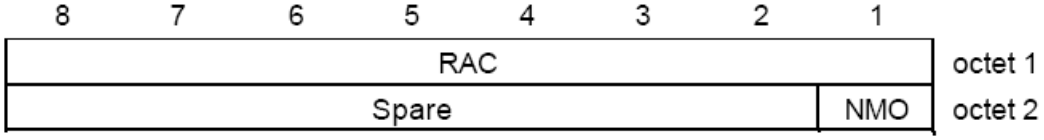
可以接收小区广播业务。

当UE驻留在小区中，并登记成功后，随着UE的移动，当前小区和临近小区的信号强度都在不断变化。 UE就要选择一个最合适的小区，这就是小区重选过程。这个最合适的小区不一定是当前信号最好的小区，为什么呢？因为，比如UE处在一个小区的边缘，又在这两个小区之间来回走，恰好这两个小区又是属于不同的LA或者RA。这样，UE就要不停的发起位置更新，即浪费了网络资源，又浪费的UE的能量。因此，在所有小区中重选哪个小区是有一定规则的，这个规则会在后面详细描述。

当UE重选小区，选择了另外一个小区后，发现这个小区属于另外一个 LA 或者RA，UE就要发起位置更新过程，使网络获得最新的UE的位置信息。UE是如何知道 LA或者RA变化了呢？在系统广播信息中的SIB1中有：CN commonGSM-MAP NAS system information 和 PS domain system information 。CN common GSM-MAP NAS system information中的内容是：



PS domain system information中的内容是：



因此，UE是知道LAC/RAC是否改变的。

如果位置登记或者更新不成功，比如当网络拒绝UE时。或者当前的PLMN出了覆盖区，UE可以进行PLMN重选，以选择另外一个可用的PLMN。

4.2.2 PLMN选择和重选

PLMN选择和重选的目的是选择一个可用的（就是能提供正常业务的），最好的PLMN。UE通过什么来达到这一目的呢？UE会维持一个PLMN列表，这些列表将 PLMN按照优先级排列，然后从高优先级向下搜索，找到的自然是最高优先级的PLMN。另外，PLMN选择和重选的模式有两种，自动和手动。

简而言之，自动选网就是UE按照PLMN的优先级顺序自动的选择一个PLMN，手动选网呢，将当前的所有可用网络呈现给用户，将权利给用户，由用户选择一个PLMN。

在这个列表中，RPLMN （registered PLMN）优先级最高。RPLMN就是上次

注册成功的PLMN。当UE关机后，怎么才能知道上次登记的是哪个PLMN?

Bytes	Description	M/O	Length
1 to 4	TMSI	M	4 bytes
5 to 9	LAI	M	5 bytes
10	RFU	M	1 byte
11	Location update status	M	1 byte

EFPSLOCI 的内容是：

Bytes	Description	M/O	Length
1 to 4	P-TMSI	M	4 bytes
5 to 7	P-TMSI signature value	M	3 bytes
8 to13	RAI	M	6 bytes
14	Routing Area update status	M	1 byte

在这两个文件中， LAI（=MCC+MNC+LAC）和/或RAI （=LAI+RAC）就记录了MCC和MNC，就是RPLMN。

无论自动选网还是手动选网， UE开机后，首先就会尝试RPLMN，成功后，就不会有后续

过程。如果不成功，UE就会生成一个PLMN列表（按照优先级）：

i) HPLMN

ii) 在USIM文件“ User Controlled PLMN Selector with Access Technology”中的PLMN（这些PLMN在USIM中是按照优先级排列的）；

iii)在USIM文件“Operator Controlled PLMN Selector with Access Technology”中的PLMN（这些PLMN在USIM中是按照优先级排列的）；

iv)信号质量较好的PLMN， 这些PLMN的排列是随机的；

v)其他的PLMN，以信号质量从高到低的顺序排列。

在USIM卡中,文件EFIMSI 记录了IMSI(MCC+MNC+MSIN),UE从这个文件就可以获取HPLMN。

ii) 和 iii)分别是USIM中的文件EFPLMNwAcT和EFOPLMNwACT。iv)和v)是由UE一个频率，一个频率搜索得到的。

UE就按照上述有优先级的PLMN列表一个一个的搜索并尝试位置登记。

由于UMTS是从GSM演进过来的，但两者的接入技术截然不同（ GERAN vs.UTRAN），因此对于每一个PLMN需要指明优先选用的接入技术。接入技术的优先级就在“…with Access Technology”文件中指出。如果没有指出，那么一般而言，优先选用的是GERAN。

当UE尝试与网络进行接触时，网络由于种种原因有时会拒绝UE的请求。根据拒绝原因的不同，UE的行为也会截然不同。罗列如下：

#3 Illegal MS

#6 Illegal ME

#8 GPRS services and non-GPRS services not allowed

此时， ME将SIM视为非法，直到SIM拔出或者关机。这种状态和没有SIM的状态基本上是一样的。此时UE仅能提供限制服务。在这种状态下，UE仍然需要进行小区重选，并且当失去覆盖时，进行PLMN 重选。

#2 unknown in HLR

IMSI

此时，ME的电路域部分将SIM视为非法，分组域仍然有可能提供正常的业务。根据分组域的状态，UE可能进行或不进行PLMN重选。

#7

GPRS services not allowed

此时，ME的分组域部分将SIM视为非法，电路域仍然有可能提供正常的业务。根据电路域的状态，UE可能进行或不进行PLMN 重选。

#11 PLMN not allowed

比如中国移动的用户如果尝试注册到中国联通的网络中时，就会收到这个原因。当UE收到这个原因的拒绝时，会将此PLMN加到“forbidden PLMN” 列表中。这个列表同时存在于ME的RAM和SIM卡的EFFPLMN中，在自动模式下，如果不得不选中这个 PLMN （比如当前只有这个PLMN的情况），UE发现这个PLMN在“forbidden PLMN”列表中，就不会再尝试登记，节省了网络资源，但限制业务（limited service）还是可以获得的。为什么要将此列表保

存在SIM中呢？这样当手机下一次开机时，仍然可以获得这个列表，并不会再尝试登记（自动模式下）。如果一旦中国移动和中国联通实现了漫游，如何将这个PLMN从“forbidden PLMN list”中去掉呢？这就需要使用手动模式。在手动模式下，UE会将当前有覆盖的所有的PLMN都呈现给用户，无论它是否是被禁止的，这样用户就可以选一个被禁止的 PLMN。而一个被禁止的PLMN一旦登记成功，将会从“forbidden PLMN”列表中删除，包括SIM中的。

当收到这个原因时，UE就可能发起PLMN 重选以选一个可用的PLMN。

#12

#13

Location area not allowed

Roaming not allowed in this location area

收到这个原因时，UE会将这个LA分别加到“forbidden location areas forregional provision of service”和“forbidden location areas for roaming”列表中。

这两个列表和“forbidden PLMN ”列表处理有些不同，就是这两个列表在USIM中是不存在的。当UE关机后，这两个列表就会失去。还有一点需要注意的是，这两个原因都是针对整个LA的，包含所有的RA。

当UE收到这个原因的拒绝时，一般可以不进行PLMN 重选，而是等待用户移动，进入一个可以提供服务的LA。

还有其他情况需要进行PLMN 重选吗？有的，下面就是两种典型的情况。

1. 用户重选

无论是在自动模式还是在手动模式，用户都可以请求网络重选。网络重选时， UE也要生成一个PLMN列表，这个列表和上述列表有一些不同。具体内容如下：

在自动模式下，列表是：

i) HPLMN ；

ii)在USIM文件“ User Controlled PLMN Selector with Access Technology”中的PLMN（这些PLMN在USIM中是按照优先级排列的）；

iii)在USIM文件“Operator Controlled PLMN Selector with Access Technology”中的PLMN（这些PLMN在USIM中是按照优先级排列的）；

iv) 信号质量较好的PLMN，这些PLMN的排列是随机的；

v) 其他的PLMN，以信号质量从高到低的顺序排列；

vi) 先前选择的PLMN。

而在手动模式下，PLMN列表和前面的列表是相同的。

2. 用户登记到归属国家的VPLMN

这种情况就是，比如，中国联通的用户登记到中国移动的网络上（如果可以的话）。 由于这些网络的MCC是相同的，只是MNC不同，UE是可以判断出这种情况的。在这种情况下，用户的通信一般而言要付出更多的代价。因此， UE会尽量回到归属网络中。采取的措施是UE

周期性的查找归属网络。 这个周期是有SIM规定的，在文件EFHPLMN中定义。当然，如果运营商愿意， 也可以禁止这个功能，此时文件EF HPLMN中的值就是0。

这两个过程其实是比较复杂的，因为，在进行用户重选或者HPLMN搜索时，原有的服务还要正常进行，还要可以发起呼叫或接收寻呼。这就要求UE在不是Paging Occasion的无线帧上进行搜索PLMN的过程，当用户发起呼叫或者需要接收寻呼时，要立刻切换回原来的频率提供服务。

图4-4、4-5、4-6概要的说明了 PLMN 选择与重选和位置登记过程。为了理解

下面的图，一些解释如下：

Allowable PLMN 一个不在forbidden PLMN列表中的PLMN。

Available PLMN 一个满足小区选择准则的 PLMN。这个准则将在

后面小节中描述。

Trying RPLMN UE正在尝试在RPLMN上进行位置登记。

On PLMN UE已经成功的在一个PLMN上注册。

Trying PLMN UE正在尝试在一个PLMN上进行位置登记。

Wait for PLMNs to appear 目前没有可用 PLMN， UE正在等待一个新 的PLMN出现。

HPLMN search in progress UE正在尝试发现HPLMN是否存在。

No SIM SIM不存在，或者ME认为SIM不存在（收到特定的位置登记拒绝原因后）。

Not on PLMN UE在选中的PLMN上注册失败。

Updated 位置登记成功。

Idle, No IMSI UE在收到上述的拒绝原因#3， #6和#8时两个域

（CS 和PS）都进入，在收到#2和#7时只有相应的域进入此状态，此时，其他域的状态可能是

updated，not updated or roaming not allowed。

Roaming not allowed 收到拒绝原因#11，#12和#13后进入。

Not updated 不是由于上述两种情况的位置登记失败。比如，其他拒绝原因或者UE无法判断网络是否收到位置登记请求等。

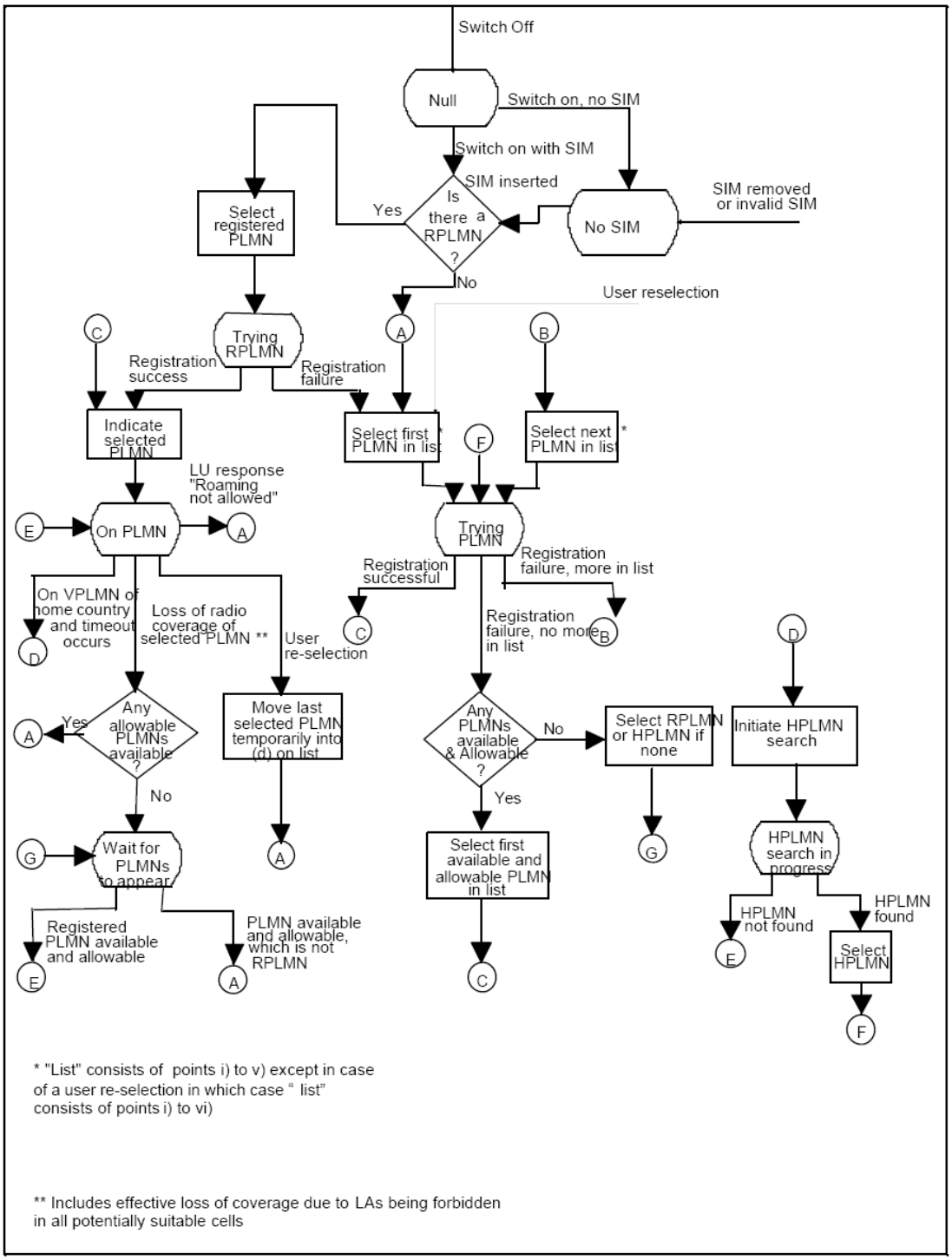


图4-4 PLMN 选择状态图（自动模式）

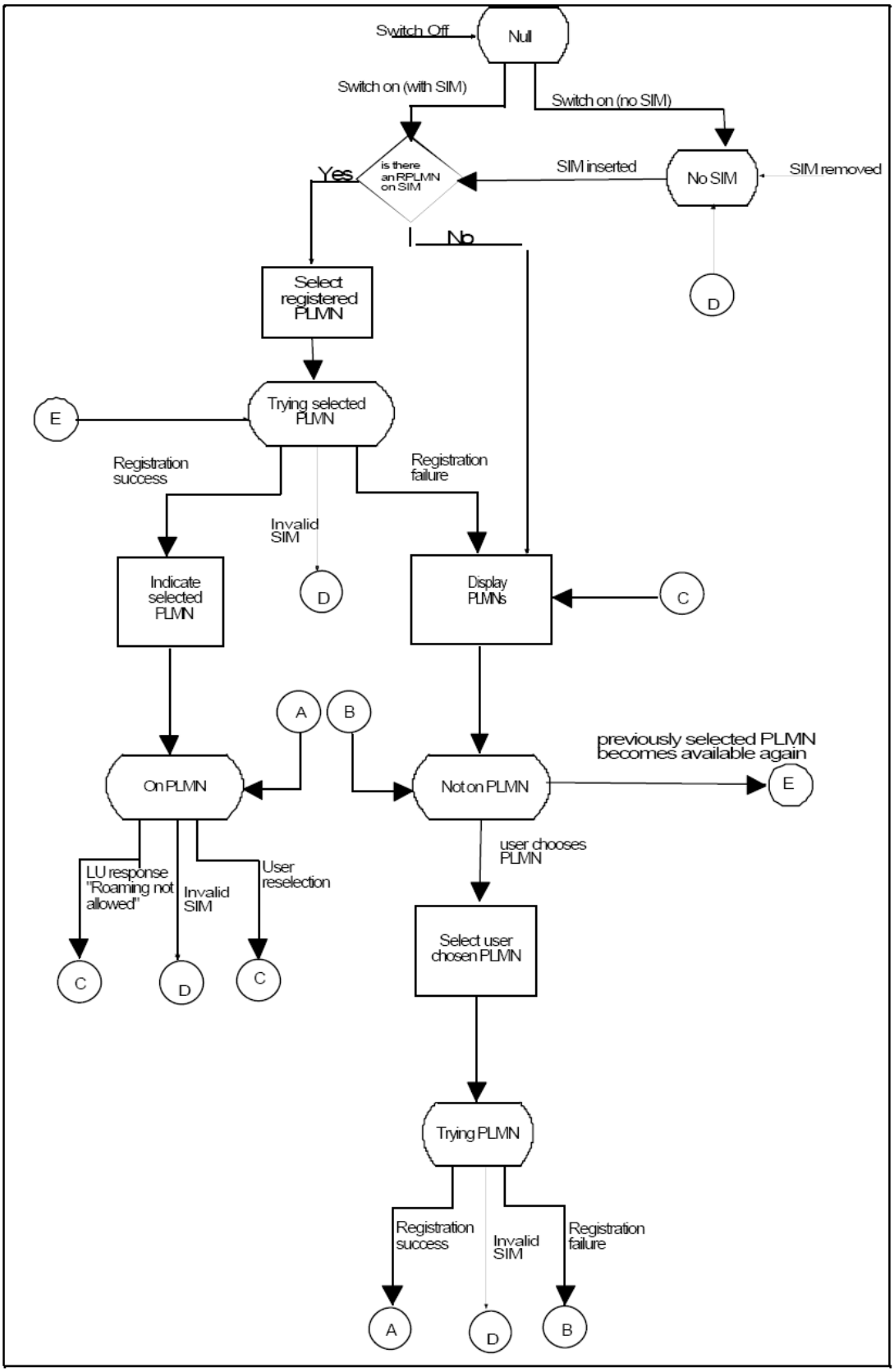


图4-5 PLMN选择状态图（人工模式）

4.2.3 小区选择和重选

当PLMN选定之后,就要进行小区选择,目的是选择一个属于这个PLMN的信号最好的小区。

首先，如果UE存有这个PLMN的一些相关信息，比如频率，扰码等。UE就会首先使用这些信息进行小区搜索（Stored information cell selection）。这样就可以较快的找到网络。因为，大多数情况，UE都是在同一个地点关机和开机，比如晚上关机，早晨开机等等。这些信息保存在 SIM卡中或者在手机的non-volatile memory中。

1. 小区选择

小区选择的过程大致如下:

1） 小区搜索。

小区搜索的目的是找到一个小区，尽管它可能不属于选择的 PLMN的。小区搜索的步骤如下（当然，首先要锁定一个频率）：

1. 时隙同步。由于在UTRAN中所有的primary SCH的同步码都是相同的，并且在每个slot的前256chips中发送，每个slot中都是相同的。UE使用一个matched filter或者类似的技术就可以很容易获得时隙同步。

2. 时隙同步后，就要进行帧同步。帧同步是使用 secondary SCH的同步码实现的。Secondary SCH的同步码一共有 16个，在每个时隙中是不同的，按照在每个时隙中码字的不同形成64组码序列。这64组码序列有一个特性：他们的循环移位后的结果是唯一的。因此UE就使用这64组码序列一个一个的和接收到的信号相关,相关值最大的那个就是这个小区所用的secondary 同步序列，同时也确定了这个小区的扰码组和帧同步。

3.获得这个小区的primary scrambling code（主扰码）。获取这个码字后，由于 CPICH和 PCCPCH都使用这个扰码而且他们的信道码是固定的，UE就可以读广播信道了。在上一步骤中，UE获得了本小区的扰码组。这个扰码组中有 8个主扰码，UE如何知道系统到底使用了那个？通常，UE就一个一个在CPICH上试，直到找到相关结果最大的一个。这就确定了主扰码。

显然，如果UE已经知道这个小区的一些信息，比如使用那个频率，甚至主扰码，上述b，c步骤就可以大大加速。

2） 读广播信道。

UE从上述1)的步骤c.中获得了PCCPCH的扰码,而PCCPCH的信道码是已知的,在整个UTRAN中是唯一的。UE就可以读广播信道的信息了。

1. MIB的调度信息（scheduling information）是已知的，即为SIB_POS=0，

SIB_REP =8 。UE在SFN=0,8,16,... 的无线帧(radio frame) 中就可以读到MIB。UE 是如何知道SFN的 呢？在SYSTEM INFORMATION消息中，如果此消息是发送在 BCH（PCCPCH）上的，消息的第一个域就是SFNprime，它的值就是这个 传输块（transport block）对应的起始SFN。取值是（ 0, 2, 4, 6, …, 4094）。 PER编码后它的值是（0..2047）。这样可以节省一个bit。为什么SFN的值是0, 2, 4, …？因为BCH

的TTI是20ms ，包含两个无线帧（radio frame），因此SFNprime只能以2为步长。

2. 读到MIB后，UE就可以判断当前找到的PLMN是否就是要找的PLMN，因为在MIB中有PLMN identity域，如果是，UE就根据 MIB中包含的其他SIB的调度信息（scheduling information），找到其他的SIB并获得其内容。如果不是，UE只好再找下一个频率，又要从头开始这个过程（从小区搜索开始）。

3. 如果当前PLMN是UE要找的PLMN，UE读 SIB3，取得“ Cell selection andre-selection info ”，在这个IE （ Cell selection and re-selection info for SIB3/4）中，读Qqualmin，Qrxlevmin和Maximum allowed UL TX power（UE_TXPWR_MAX_RACH），然后按照下列公式计算：

Squal = Qqualmeas - Qqualmin

Srxlev = Qrxlevmeas - Qrxlevmin - Pcompensation

其中:

Squal	Cell Selection quality value, (dB) Not applicable for TDD cells or GSM cells.
Srxlev	Cell Selection RX level value (dB)
$Q_{qualmeas}$	Measured cell quality value. The quality of the received signal expressed in CPICH E_C/N_0 (dB) for FDD cells. Not applicable for TDD cells or GSM cells.
$Q_{rxlevmeas}$	Measured cell RX level value. This is received signal, CPICH RSCP for FDD cells (dBm), P-CCPCH RSCP for TDD cells (dBm) and RXLEV for GSM cells (dBm).
Qqualmin	Minimum required quality level in the cell (dB). Not applicable for TDD cells or GSM cells.
Qrxlevmin	Minimum required RX level in the cell. (dBm)
Pcompensation	Max(UE_TXPWR_MAX_RACH – P_MAX, 0) (dB)
UE_TXPWR_MAX_RACH	Maximum TX power level an UE may use when accessing the cell on RACH (read in system information), (dBm)
P_MAX	Maximum RF output power of the UE, (dBm)

如果：

Squal > 0

Srxlev > 0

则UE认为此小区即为一个 suitable cell。驻留下来，并读其他所需要的系统信息，随后UE将发起位置登记过程。

如果不满足上述条件，UE读SIB11，Measurement control system information，Intra-frequency measurement system information，Intra-frequency cell info list，cell info， Primary CPICH info，Reference time difference to cell和Cell Selection and Re-selection info for SIB11/12。 在 CPICH info中 ， UE可 以 得 到 primaryscrambling code。UE根据临区的primary scrambling code，由于CPICH的信道码在整个UTRAN是唯一的，又根据 Reference time difference to cell ，可以很容易测得临区的Qqualmeas和Qrxlevmeas，在IE Cell Selection and Re-selection info for SIB11/12中，UE可以知道临区的Maximum allowed UL TX power，Qqualmin和Qrxlevmin，这样UE就可以算出临区的Squal和Srxlev并判断临区是否满足上述selection criteria。

UE又可以读Inter-frequency measurement system information， Inter-frequency cell info list， frequency info and cell info，Cell info，Cell info和上面是一样的。

Frequency info中包含了UARFCN uplink（Nu）和UARFCN downlink（Nd），由这些信息， UE就可以算出临区的Squal和Srxlev并判断临区是否满足上述selection criteria。

如果UE发现了任何一个临区满足selection criteria，UE就驻留在此小区中，并读其他所需要的系统信息，随后UE将发起位置登记过程。

如果UE发现没有一个小区满足selection criteria。UE就认为没有覆盖，就会继续PLMN选择和重选过程。

2. 小区重选

UE在空闲模式下，要随时监测当前小区和临区的信号质量，以选择一个最好的小区提供服务。这就是小区重选过程(cell reselection)。小区重选过程分为 有HCS （ hierachical cell structure）和没有 HCS两种情况。有没有 HCS在SIB11，Measurement control system information，Use of HCS指出。有HCS的情况比较复杂，这里就不作介绍了。

3. 离开连接模式的小区选择

当UE 从连接模式回到空闲模式时，要做小区选择，以找一个合适的小区（suitable cell）。这个选择过程和普通的小区选择过程是一样的。不过此时候选小区就是连接模式时用到的小区。如果在这些小区中找不到合适的小区，应该使用stored information cell selection。

4. 任意小区选择

任意小区选择的意思就是随便选择一个小区，只要它满足criteria S即可。在这种情况下，UE进入limited service状态。

图4-7表明了小区选择和重选的大致过程。

为了理解这些过程，一些名词解释如下：

Suitable Cell：是一个UE可以在其中获得正常服务（normal service）的小区。

Acceptable Cell: 满 足 cell selection的 criteria S， 但只能获得受限服务（limited service）的小区。

Camped normally UE驻留在小区中，可以获得normal service。这个小区一定是suitable cell。

Camped on any cell UE驻留在小区中，可以获得limited service。这个小区一定是acceptable cell。

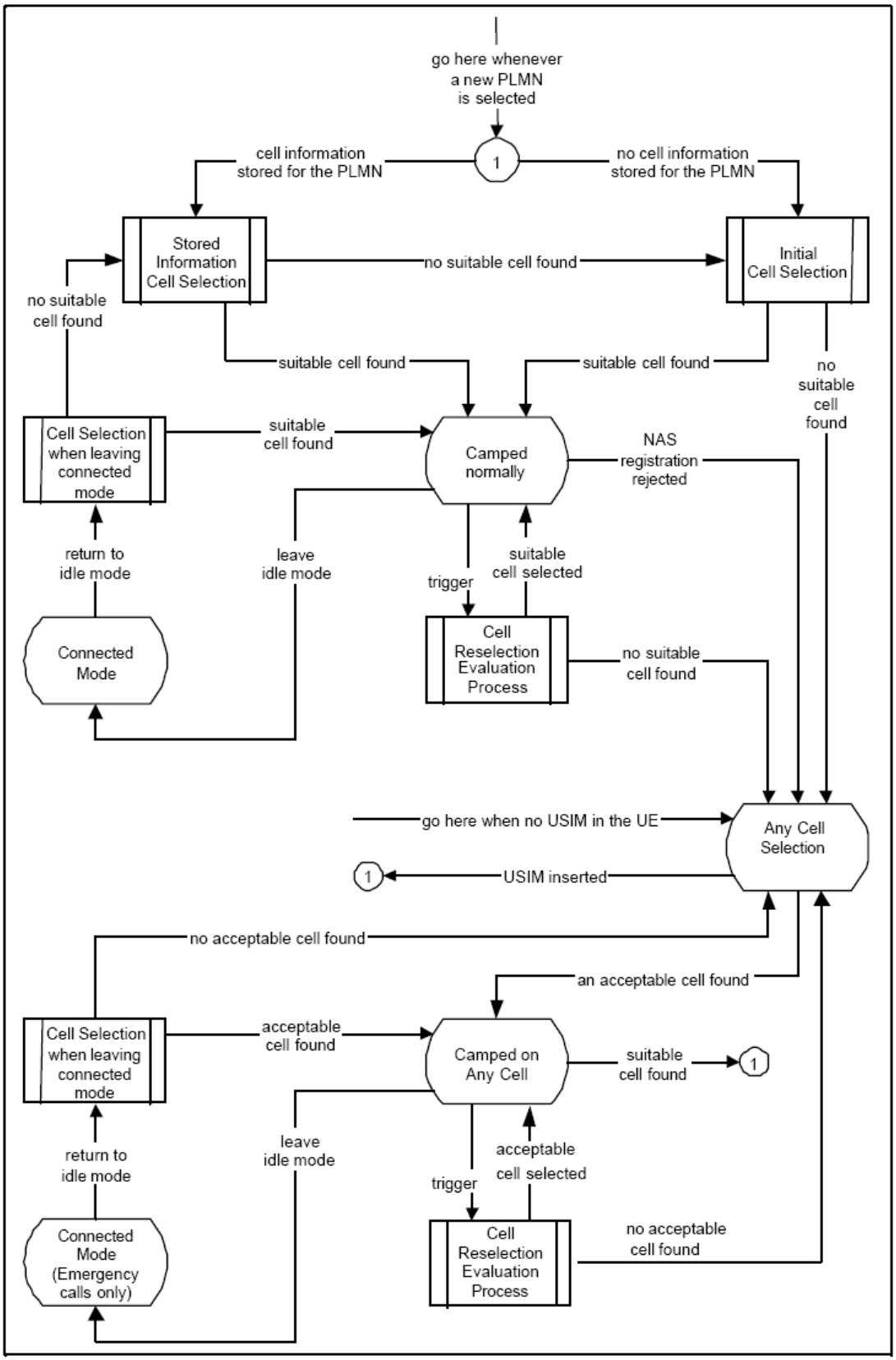


图 4-7 空闲模式下的小区选择与重选

4.2.4 位置登记

这些过程请参见MM，GMM的过程。

4.3 电路域移动性管理

4.3.1 位置更新

位置更新过程是由 HLR、MSC/VLR等实体之间逻辑配合完成。HLR记录移动用户当前位置信息和所有用户数据；VLR记录漫游到由该VLR控制位置区的移动用户的相关用户数据； MSC处理移动用户的位置登记进程，与移动用户对话并与HLR、VLR交互信息。

位置更新包括位置登记、周期性位置登记、用户数据删除等。

——位置登记

引起移动用户发生正常位置登记的条件是：移动设备开机时以及移动用户发生漫游引起位置改变。

——周期性位置登记

通过周期性位置登记（位置更新），PLMN可以保持追踪移动用户当前的状态，特别是保持长时间没有操作的用户与网络的联系。位置更新时间周期和保护时间可以由PLMN运营商根据具体话务和用户习惯来设定调整。

——用户数据删除

指将用户记录从VLR中删除，包括用户漫游产生的用户数据删除、用户长时间无操作引起的用户数据删除、以及系统管理员对无效用户记录所进行的删除。

图4-8是一个典型的位置更新流程图，基本包含了上述三个过程。

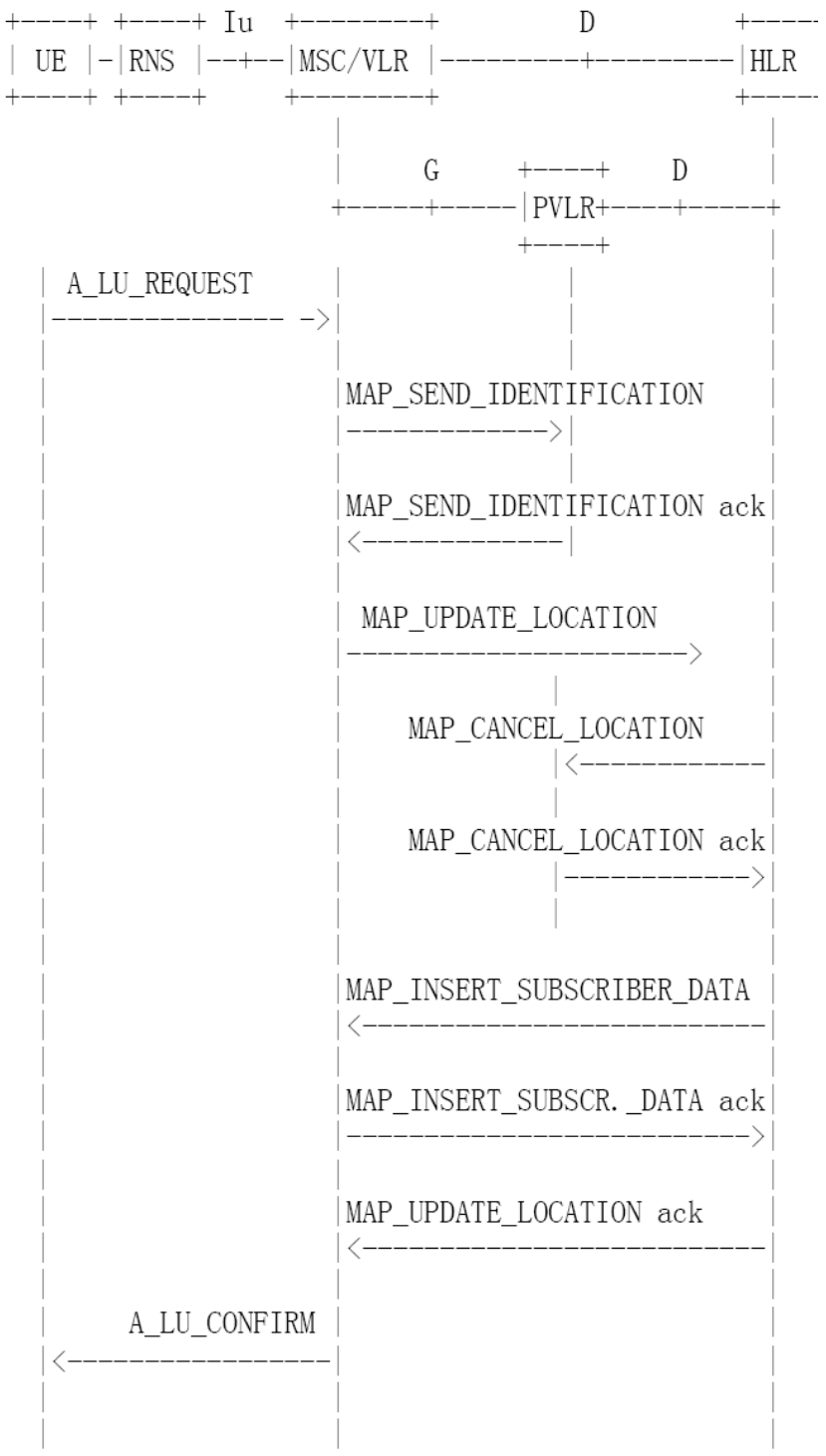


图4-8 位置更新流程图

1. MSC/VLR接收到用户用TMSI发起的位置更新请求后，如果TMSI不认识：若携带的前位置信息为临近VLR的位置区，则发起向PVLR取识别的流程；若前位置区为非临近VLR的位置区或者到PVLR取识别失败，则发起要求手机提供IMSI的流程。要求手机提供IMSI的流程在图中没有画出。

2. 如果用户在本VLR首次位置登记，则发起到HLR的位置更新请求。

3. HLR 接 收 到 MSC/VLR 的位置更新请求后，发 现如果用户漫游的MSC/VLR号码发生改变，向PVLR发起位置删除流程，删除PVLR中的用户信息。

4. 如果漫游拒绝，HLR直接向MSC/VLR发出携带拒绝信息的位置更新响应；否则首先向MSC/VLR插入用户数据，然后根据插入用户数据的结果，判断是下发位置更新接受还是位置更新拒绝。

4.3.2 去活

去活过程即移动用户关机，MS发起DETACH的流程，MSC/VLR置用户状态为IMSI分离，该流程一般不通知HLR。若该MS被拨打，MSC会将用户关机情况直接通知主叫方。其流程图相当简单，如图6-9：

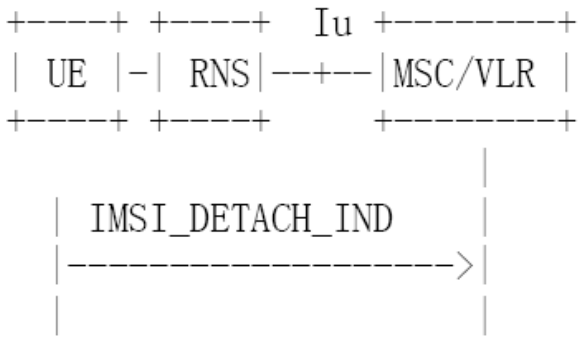


图4-9 关机流程图

当MS关机时，向网络发出关机信号，MSC/VLR记录用户已经关机。另，有些型号的移动终端，在通话期间直接关电源时，也可以发起DETACH流程。

4.3.3 鉴权流程

一个成功的鉴权过程可以用流程图来表示，如图 6-10 所示。

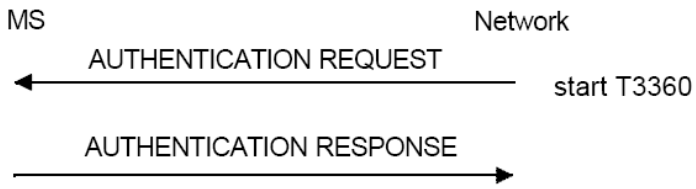


图4-10 鉴权成功

鉴权流程由网络侧发起，其目的是：由网络来检查是否允许终端接入网络；提供鉴权参数五元组中的随机数数组，供终端计算出加密密钥（CK）；同时，供终端计算出与网络侧进行一致性检查的密钥（ IK）；最后一个目的是可以提供终端对网络的鉴权。

与GSM的鉴权流程相比，3G的鉴权流程增加了一致性检查的功能及终端对网络的鉴权功能。这些功能使3G的安全特性有了进一步的增强。

网络侧在发起鉴权前，如果 VLR内还没有鉴权参数五元组，此时将首先发起到HLR取鉴

权集的过程，并等待鉴权参数五元组的返回。鉴权参数五元组的信息包含RAND、XRES、AUTN、CK和IK。

在检测到鉴权参数五元组的存在后，网络侧下发鉴权请求消息。此消息中将包 含 某 个五元组的RAND和AUTN。用户终端在接收到此消息后，由其USIM验证AUTN，即终端对网络进行鉴权，如果接受，USIM卡将利用RAND来计算出CK与IK和签名XRES。如果USIM认为鉴权成功，在鉴权响应消息中将返回XRES。

网络侧在收到鉴权响应消息之后，比较此鉴权响应消息中的XRES与存储在VLR数据库中的鉴权参数五元组的XRES，确定鉴权是否成功：成功，则继续后面的正常流程；不成功，则会发起异常处理流程，释放网络侧与此终端间的连接，并释放被占用的网络资源、无线资源。

在成功的鉴权之后，终端将会把 CK（加密密钥）与IK（一致性检查密钥）存放到USIM卡中。

有些情况下，终端会在收到鉴权请求消息后，上报鉴权失败！典型的鉴权失败的原因有下面两种：

手机终端在对网络鉴权时，检查由网络侧下发的鉴权请求消息中的 AUTN参数，如果其中的“MAC”信息错误，终端会上报鉴 权失败消息，原因值为MAC Failure。

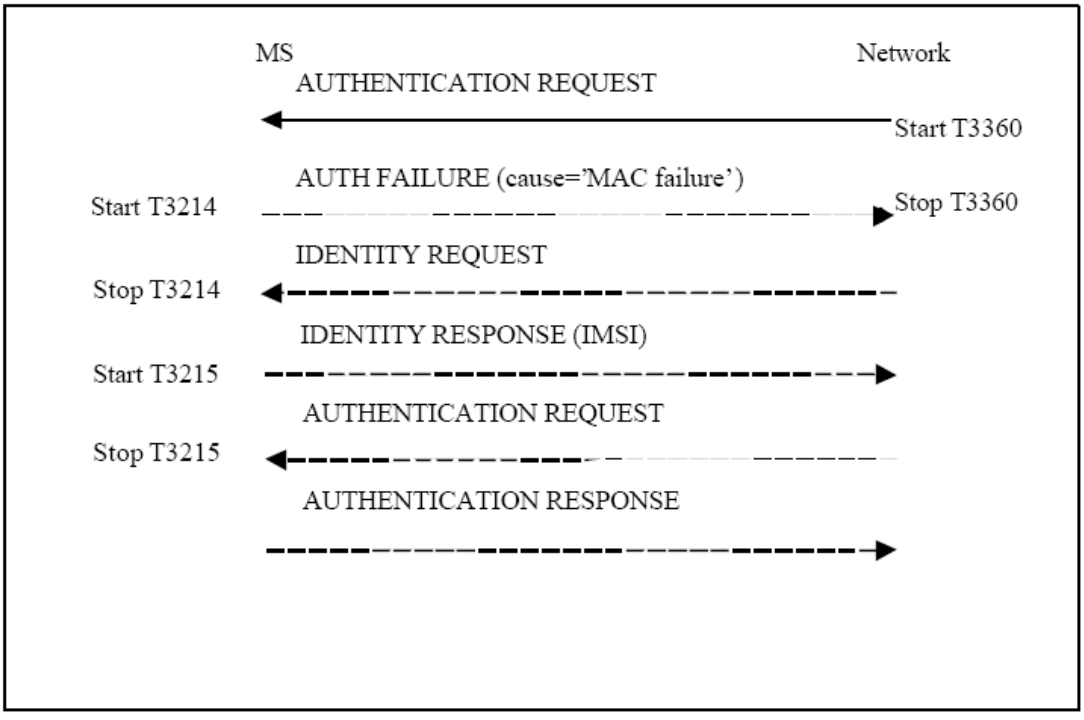


图4-11 鉴权失败（失败原因为MAC Failure）

此时，网络侧将根据手机终端上报的用户标识来决定是否发起识别过程。如果当前的标识为 TMSI（或P-TMSI），则发起识别流程，要求手机终端上报IMSI信息。然后再次发起鉴权流程。

另外一种鉴权失败的情况是手机终端检测到AUTN消息中的SQN的序列号错误，引起鉴权失败，原因值为：Synch failure!（同步失败）

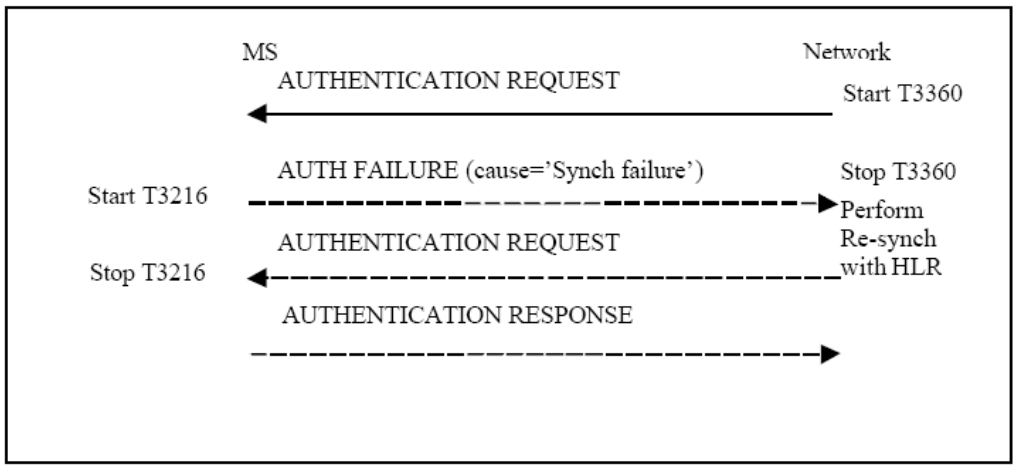


图4-12 鉴权失败（原因值为Synch failure）

此时，网络侧的VLR将删除所有鉴权参数5元组，并发起到HLR的同步过程，要求HLR 重新插入鉴权参数五元组，然后再开始鉴权过程。

4.4 分组域移动性管理流程

4.4.1 MM功能概述

移动性管理（MOBILITY MANAGEMENT）和会话管理（SESSIONMAMAGEMENT）以及短消息（SHORT MESSAGE SERVICES）共同组成3GPP协议中的连接层，在UMTS系统中，MM处于RANAP层之上，为SM和SMS提供信令传送，实现了用户在网络中的移动性管理。 移动性管理主要完成用户的附着、分离、安全流程、路由区更新、位置更新等功能。

1. 术语介绍

GMM/PMM

GSM和UMTS系统分组业务的移动性管理，本文主要介绍UMTS系统中的分组域的移动性管理特性。

MM CONTEXT

GMM的用户上下文，包括了用户签约数据、鉴权集

GMM在协议栈中的位置如图4-13所示，与SM、SMS的关系如图4-13所示。

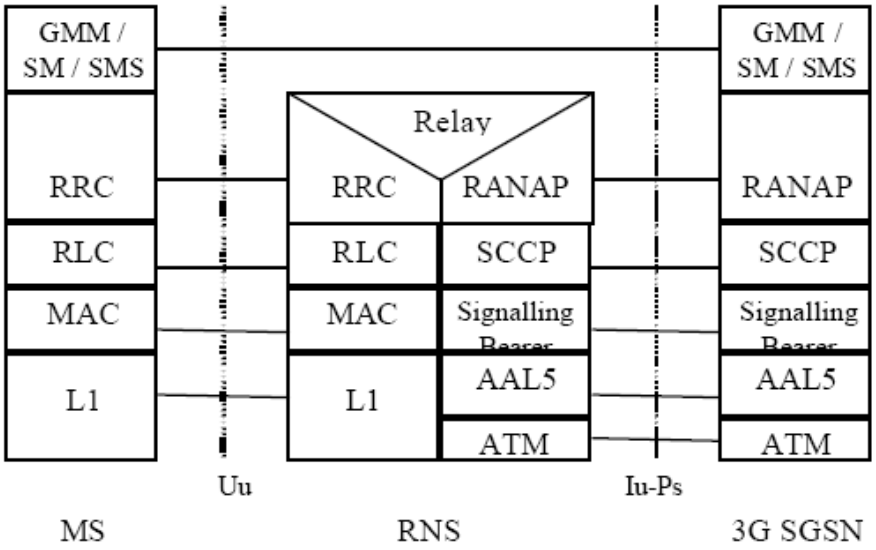


图4-13 UMTS系统下的分组域中手机和网络侧的控制面协议

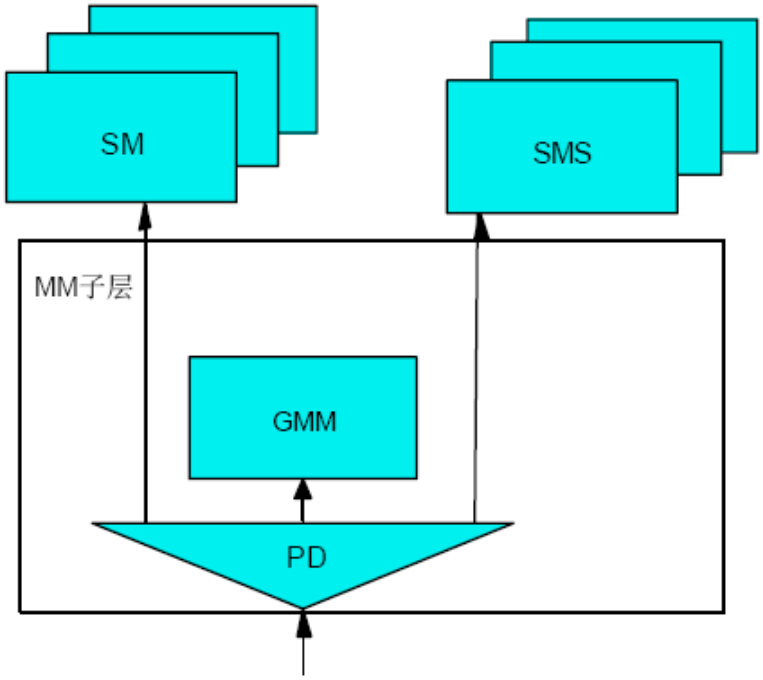


图4-14 UMTS系统下的分组域移动性管理与相关单元的关系图

GMM与SM之间的原语

GMMSM-RELEASE-IND

GMMSM-UNITDATA-REQ

GMMSM-UNITDATA-IND

GMM和SMS之间的原语

PMMSMS_REL_REQ

PMMSMS_ERROR_IND

PMMSMS_UNITDATA_REQ

PMMSMS_UNITDATA_IND

4.4.2 移动性管理状态

UMTS系统中的分组移动性管理的状态可以分为 ： PMM-DETACHED 、PMM-IDLE、PMM-CONNECTED；在手机侧和网络侧状态信息通过MM移动性管理上下文进行管理。

如图6-45，图中明确的表示移动性管理的状态与会话管理的状态是无关的，也就是移动性管理处在连接态，会话管理可以处在激活态或者非激活态；移动性管理处在空闲态，会话管理可以处在激活态或者非激活态。状态迁移关系描述如下：

1）PMM-DETACHED到PMM-CONNECTED

通过分组域的附着，移动性管理的状态由分离态迁移到连接态；

2）PMM-CONNECTED到PMM-IDLE

通过分组域的信令连接释放，移动性管理的状态由连接态迁移到空闲态；

3）PMM-IDLE到PMM-CONNECTED

通过分组域信令连接的建立，移动性管理的状态由空闲态迁移到连接态；

4）PMM-CONNECTED到PMM-DETACHED

通过分组域的分离或者附着拒绝、路由区更新拒绝，移动性管理的状态由连

接态迁移到分离态；

5）PMM-IDLE到PMM-DETACHED

通过隐式的分组域的分离，移动性管理的状态由空闲态迁移到分离态；

6）PMM-CONNECTED到PMM-CONNECTED

在重定位过程中，移动性管理的状态保持在连接态。

注： 在某种错误影响下：可能出现MS和网络侧的状态不同步，通过路由更新过程就可以实现同步。

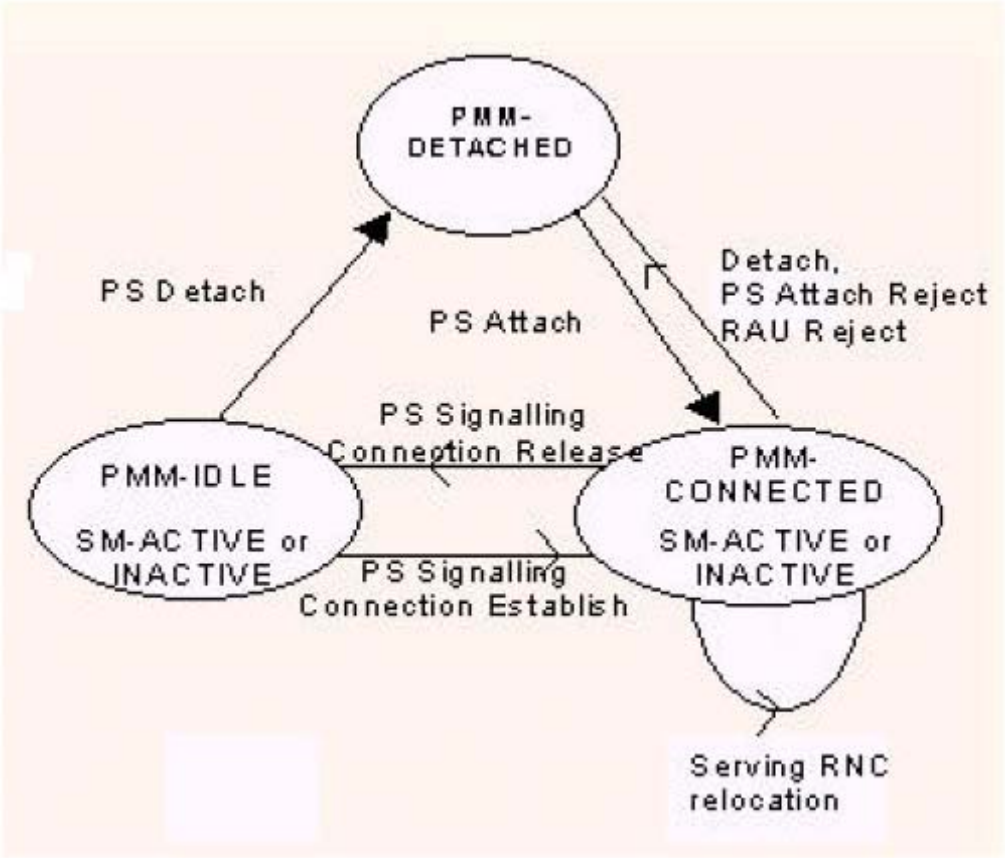


图4-15 UMTS系统的分组域移动性管理的状态迁移图

4.4.3 GMM的定时器功能

(1) Ready Timer

Ready Timer定时器的概念在UMTS系统中不再存在，如果用户消息中带有协商的Ready Timer定时器，网络侧将其保存，等到发生系统间改变的时候，启用。

(2) Mobile Reachable Timer

网络侧监视手机周期更新的定时器，比手机保存的周期更新定时器略长一些，如果移动性管理的状态进入连接态（PMM-CONEECTED），则该定时器立刻停止；直至移动性管理的状态进入空闲态（PMM-IDLE），重新启动移动台可及定时器。如果Mobile Reachable Timer定时器超时，用户的寻呼允许标志（PPF）被清除。

4.5.4 SGSN和MSC/VLR之间的联系

(1) SGSN和MSC/VLR之间的联系会通过以下的过程建立：

联合GPRS/IMSI附着/分离

已经IMSI附着的用户的GPRS附着

已经GPRS附着的用户的IMSI附着（发生的是联合路由区更新）

(2) 电路域寻呼（CS Paging）：

对于一个联合附着的用户，MSC/VLR可以通过SGSN发送电路域寻呼

(3) 非GPRS业务提醒（Non-GPRS Alert）：

MSC/VLR要求SGSN通知MSC/VLR手机的活动情况，会将非GPRS业务提醒标志（ NGAF）置位，SGSN移动性管理一旦发现该用户活动，立刻通知MSC/VLR，然后清除NGAF。

(4) MS信息过程（MS Information Procedure）：

MSC/VLR需要用户的身份信息和位置信息时，可以通过Gs接口从SGSN本地获得或通过SGSN下发信息请求，取得MSC/VLR所需信息。

(5) MM信息过程（MM Information Procedure）：

MSC/VLR可以通过SGSN将网络信息发送给用户，SGSN会将信息下传。

4.4.5 MM过程

在UMTS系统中，MM过程是指利用各个接口实现消息的传递，具体的有：通过Iu接口、Gr接口、Gs接口实现消息的传递等。

4.4.6 GPRS附着功能

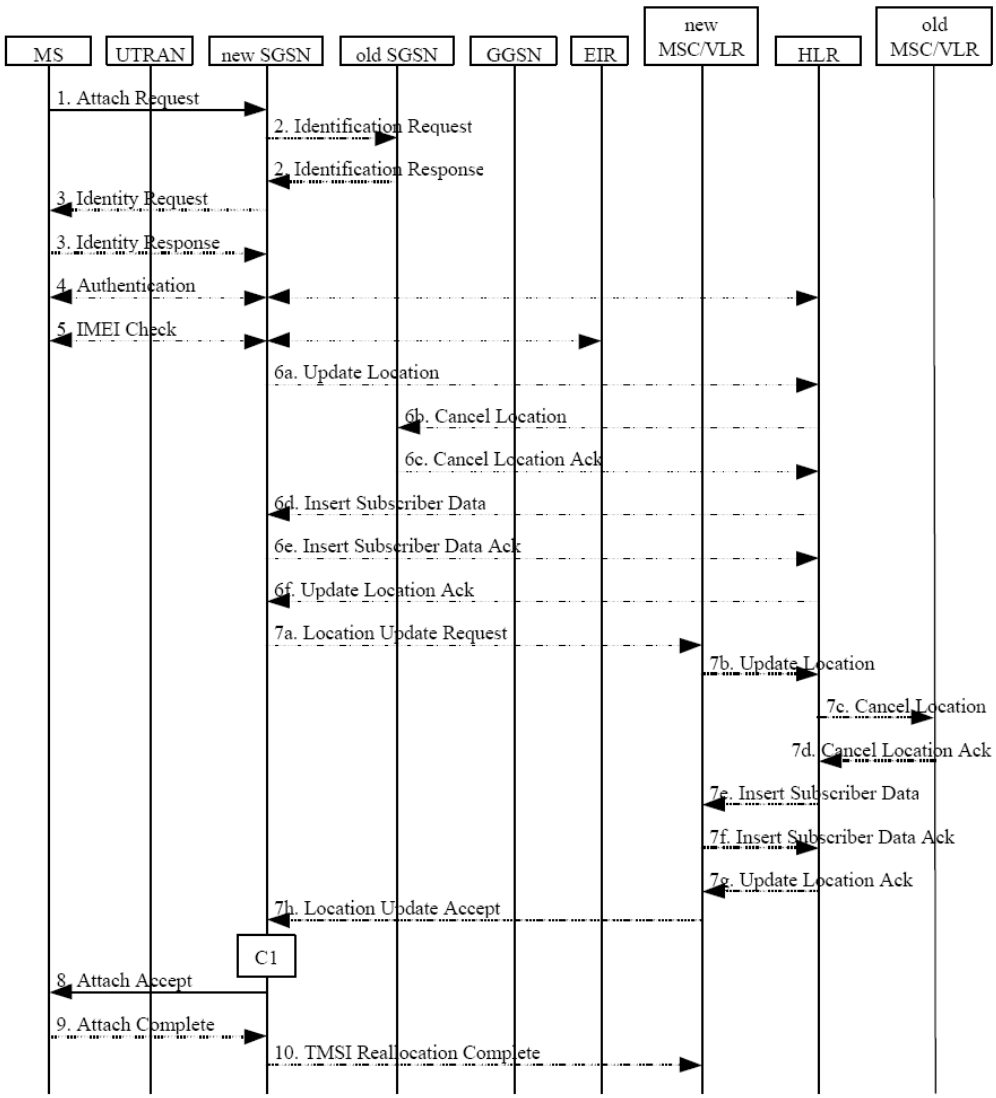


图4-16 附着流程

1）用户通过发送附着请求发起附着流程。用户在附着请求消息中携带有IMSI or P-TMSI and old RAI，Core Network Classmark，KSI，Attach Type，old P-TMSI Signature，Follow On Request，DRX Parameters，如果用户没有合法的P-TMSI，用户会带上 IMSI；如果用户有合法的P-TMSI，用户应该使用 P-TMSI和配对的路由区标识，同时如果具有P-TMSI签名的话，也应该带上。附着类型指示用户请求执行何种附着过程，即GPRS附着、联合附着以及已经IMSI附着的 GPRS附着。DRX参数指示用户是否使用非连续接收和DRX循环周期长度。SGSN可以根据Follow On Request指示，决定在附着结束后，是否释放同用户的分组业务信令连接。

2）如果用户使用P-TMSI附着，并且自上次附着改变了SGSN，新SGSN应该发送身份识别请求给老的SGSN,带上用户的P-TMSI和相应的路由区标识以及老的P-TMSI签名,如果有的话。老SGSN回应身份识别响应消息，包含用户的IMSI和鉴权集。如果用户在老SGSN未知，老SGSN回应消息带上相应的原因值；如果用户的P-TMSI和签名不匹配，老SGSN回应消息带上相应的原因值。

3）如果用户在老 SGSN为未知，新SGSN应该发起身份识别请求给用户，身份类型指示IMSI。用户应该报告自己的IMSI给SGSN。

4）如果用户的移动性管理上下文在网络侧不存在，鉴权过程是必须的。如果将要重分配P-TMSI，并且网络支持加密，加密模式应该被设置。

5）移动台设备检查功能定义在身份检查流程中，此功能现均不实现。

6）如果 SGSN号码自从上次分离后发生改变，或者是用户的第一次附着，

SGSN应该通知HLR。

A. SGSN发送一条UpdateLocation消息（带有SGSN号码、SGSN地址、IMSI）给HLR；

B. HLR发送Cancel Location（带有IMSI、取消类型）消息给老的SGSN同时置取消类型为Update Procedure；

C. 老SGSN以Cancel Location Ack（带有IMSI）消息确认收到HLR的Cancel Location。如果该用户有任何正在进行中的流程，老SGSN应该等待这些流程结束，然后才能删除用户的MM上下文和PDP上下文；

D. HLR发送插入用 户签约数据消息（带有 IMSI、 GPRS 签约数据）给新SGSN；

E. 新SGSN证实用户存在于新的路由区中，如果用户签约数据限制用户在此路由区附着，SGSN应该拒绝用户的附着请求，带以恰当的原因值，同时可以回应插入签约数据确认消息给HLR。如果签约数据检查由于其他原因失败，SGSN应该拒绝用户附着请求，带上合适的原因值，同时回应HLR插入签约数据确认消息（带有IMSI、原因值）。如果所有签约数据检查通过，SGSN为用户构造MM上下文，同时回应HLR插入签约数据确认消息（带有IMSI）。

F. HLR在删除旧的MM上下文和插入新的MM上下文完成后，发送Update Location Ack消息给SGSN确认SGSN的Update Location消息。如果Update Location被HLR拒绝，SGSN带上合适的原因值拒绝用户的附着请求。

7）如果在步骤1中的附着类型指示已经IMSI附着的用户进行 GPRS附着，或者联合附着，那么 VLR应该被更新，如果配置了Gs接口的话。VLR号码可以从路由区信息导出。SGSN在上

面的步骤6d），即收到HLR的第一次插入用户签约数据消息时，就可以开始Location Update流程，这将导致用户在VLR中被标记上GPRS附着。

A. SGSN 发送 Location Update 消息（带有新的位置区标识 LAI 、IMSI 、SGSN号码、Location Update Type），Location Update Type指示IMSI附着，如果用户附着类型是联合附着的话；否则，Location Update Type 应该指示正常Location Update。VLR通过储存SGSN的号码创建和SGSN的关联；

B. 如果位置区更新发生在MSC之间，新的VLR发送 Update Location消息（IMSI、新的VLR号码）给HLR；

C. 如果位置区更新发生于MSC之间，HLR发送Cancel Location（带有IMSI）消息给老VLR；

D. 老VLR以Cancel Location Ack消息确认（带有IMSI）；

E. 如果位置区更新发生在 MSC之间，HLR发送插入用户签约数据消息给新的VLR；

F. VLR以插入签约数据确认消息（带有IMSI）确认。

G. 在完成MSC间的Location Update 流程后，HLR以Update Location Ack消息（带有IMSI）给新的VLR；

H. VLR回应Location Update Accept（带有VLR 号码、TMSI）消息给SGSN；

8）SGSN选择Radio Priority SMS，发送附着接受消息（带有P-TMSI、VLR号码、TMSI 、P-TMSI 签名、 Radio Priority SMS）给用户。如果重新分配了P-TMSI，应该在消息中带上。

9）如果 P-TMSI或者TMSI改变，用户以附着完成消息给SGSN确认新分配的

TMSI。

10）如果TMSI发生改变，SGSN发生TMSI重分配完成消息给VLR以确认重分配的TMSI。

如果附着请求不能被接受，SGSN回送附着拒绝消息（带有 IMSI、Cause）给用户。

4.4.7 分离功能

1. MS发起的分离

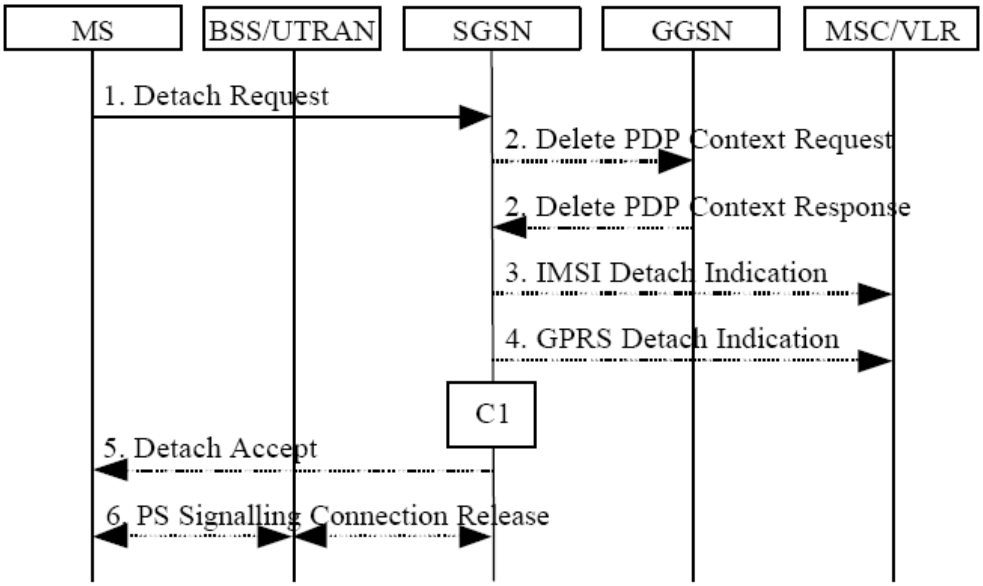


图4-17 M S发起的分离

1）用户发送分离请求消息（带有Detach Type，P-TMSI，P-TMSI Signature，Switch Off）给SGSN，从而发起分离流程。Detach Type指示将要进行何种类型的分离流程，即GPRS分离、IMSI分离、联合分离。 Switch Off指示用户的分离是否是因为关机。分离请求消息带有用户的 P-TMSI和P-TMSI签名，签名是用来检查用户分离消息的合法性的。如果用户的签名不合法或者没有带，SGSN应该发起鉴权。

2)如果是 GPRS分离,存在于 GGSN中属于该用户的激活的PDP上下文的去活,是通过SGSN向GGSN发送删除PDP上下文请求消息（带有TEID）来实现的。GGSN以删除PDP上下文响应消息予以确认。

3）如果是IMSI分离，SGSN应该发送IMSI分离指示消息给VLR。

4）如果用户需要在 GPRS分离同时保留 IMSI附着，SGSN应该发送GPRS分离指示消息给VLR。VLR删除和SGSN的关联，并且不再通过SGSN发起寻呼和Location Update。

5）如用户不是因为关机发起分离，SGSN应该回应分离接受消息给用户。

6）如果用户发起GPRS分离，SGSN释放PS域信令连接。

2. 网络侧发起的分离

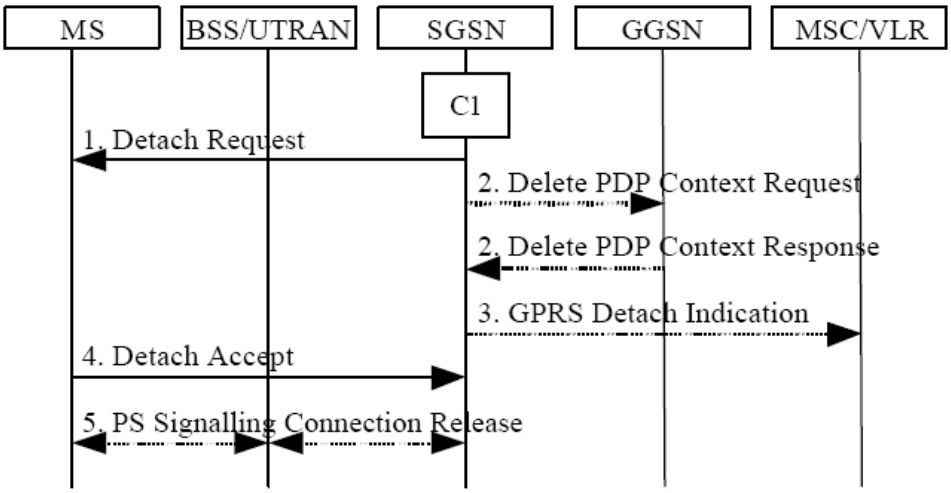


图4-18 网络侧发起的分离过程

1）SGSN以分离请求消息（带有分离类型）通知用户已经被分离。分离类型指示用户是否被要求重新附着和重新激活原先分离前激活的PDP上下文。如果是，在分离完成后，附着流程将会发起。

2 ）SGSN通知GGSN删除PDP上下文请求消息（带有TEID），以通知GGSN去活该用户激活的PDP上下文。GGSN以删除PDP上下文响应消息确认SGSN的删除请求。

3）如果用户是联合附着，SGSN应该发送GPRS分离指示消息（带有用户IMSI）通知VLR。VLR去除和SGSN的关联，不再通过SGSN进行寻呼和位置区更新。

4）用户可能在收到SGSN的分离请求后的任何时候发送分离接受消息给SGSN。

5）在收到用户的分离接受消息后，如果分离类型不要求用户重新附着，那么SGSN将释放分组域的信令连接。

3. HLR发起的分离过程

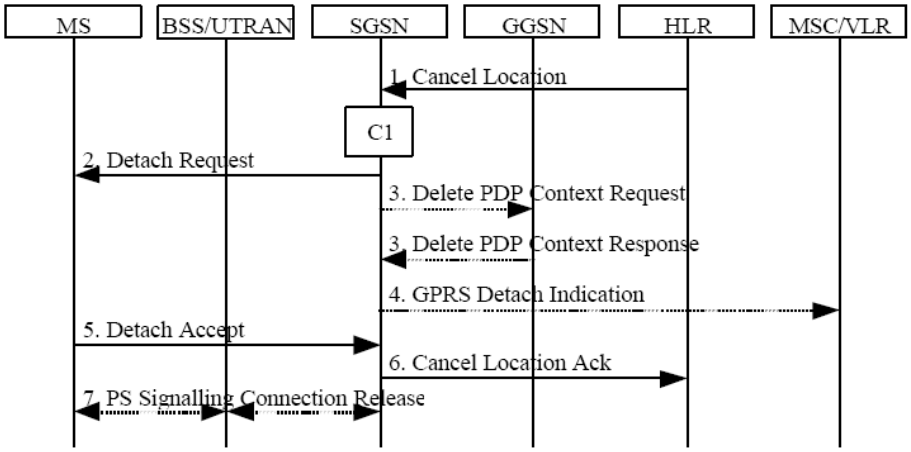


图4-19 HLR发起的分离过程

1）如果 HLR要立即从SGSN删除签约用户的MM上下文和PDP上下文，HLR应该发送Cancel Location（带有IMSI、Cancellation Type）消息给SGSN，同时置Cancellation Type 为

Subscription Withdrawn。

2）SGSN以分离请求消息（带有分离类型）通知用户已经被分离。分离类型指示用户是否被要求重新附着和重新激活分离前原激活的PDP上下文。

3 ）SGSN通知GGSN删除PDP上下文请求消息（带有TEID），以通知GGSN去活该用户激活的PDP上下文。GGSN以删除PDP上下文响应消息确认SGSN的删除请求。

4）如果用户是联合附着，SGSN应该发送GPRS分离指示消息（带有用户IMSI）通知VLR。VLR去除和SGSN的关联，不再通过SGSN进行寻呼和位置区更新。

5）用户可能在收到SGSN的分离请求后的任何时候发送分离接受消息给SGSN。

6）SGSN应该以Cancel Location Ack消息（带有IMSI）确认MM上下文和PDP上下文的删除。

7）在收到用户的分离接受消息后，如果分离类型不要求用户重新附着，那么SGSN将释放分组域的信令连接。

4.5 呼叫控制

4.5.1 移动起始呼叫建立

当MS想发起一个呼叫时，MS要使用无线接口信令与网络建立通信，并发送一个包含有被叫用户号码的消息。CN将建立一个到该MS的通信信道，并使用被叫方地址创建一个IAM消息发送到被叫方。

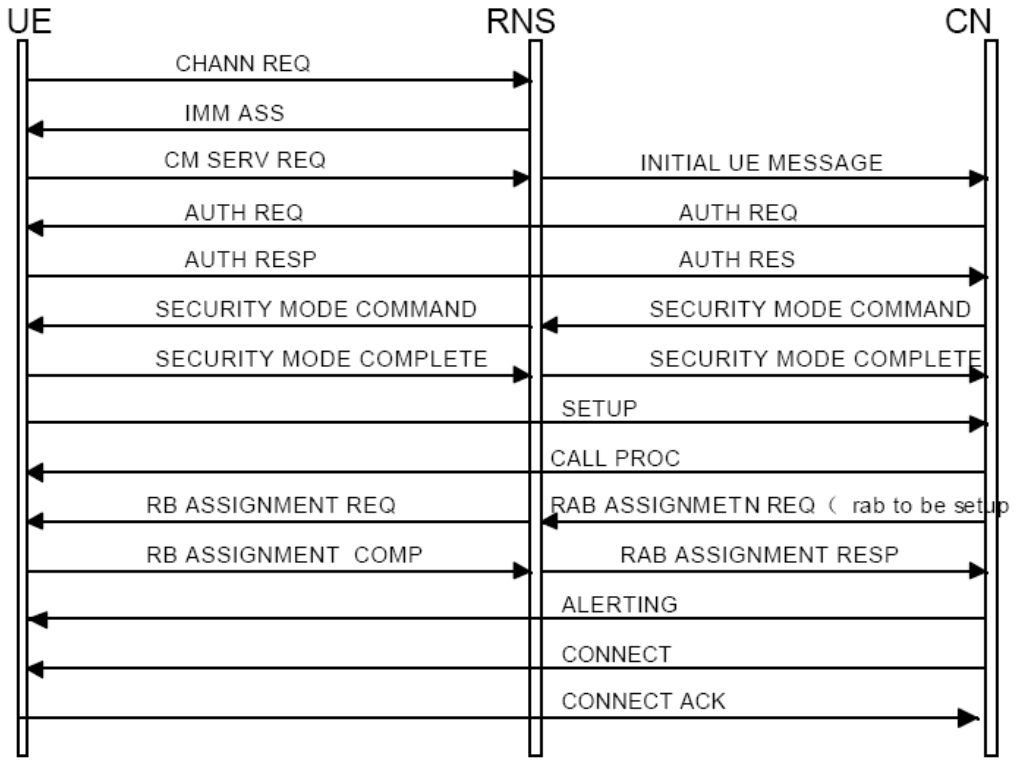


图4-20 移动起始呼叫建立过程

1）MS在随机访问信道上发送CHANNEL REQUEST消息给网络。

2）网络回应IMMEDIATE ASSIGNMENT消息，使得MS可占用指定的专用信道。

3）MS向CN发初始服务请求消息CM SERVICE REQUEST。

4）网络将发起鉴权和加密过程。

5）在发送SECURITY MODE COMPLETE消息之后，MS通过发送SETUP消息给移动台而发起呼叫的建立过程。

6）网络将回CALL PROCEEDING消息。

7）对于早指配，在网络发起固定网络的呼叫建立之前要为 MS分配一个通信信道。

8）当被叫振铃时，网络则要向主叫MS发一个ALERTING消息。

9）当被叫方应答后，将发送一个CONNECT消息给网络，网络再将其传给主叫侧。

10）当从主叫MS回CONNECT ACKNOWLEDGE消息之后即完成了呼叫建立的过程。

4.5.2 移动终止呼叫的建立

若CN收到IAM消息后，若允许该到来的呼叫建立，则CN要使用无线接口信令寻呼MS。当MS以PAGE ACK消息回应，CN收到后即建立一个到MS的通信信道。

移动终止呼叫用于移动用户做被叫时的情况，此时由网络发起呼叫的建立过程。

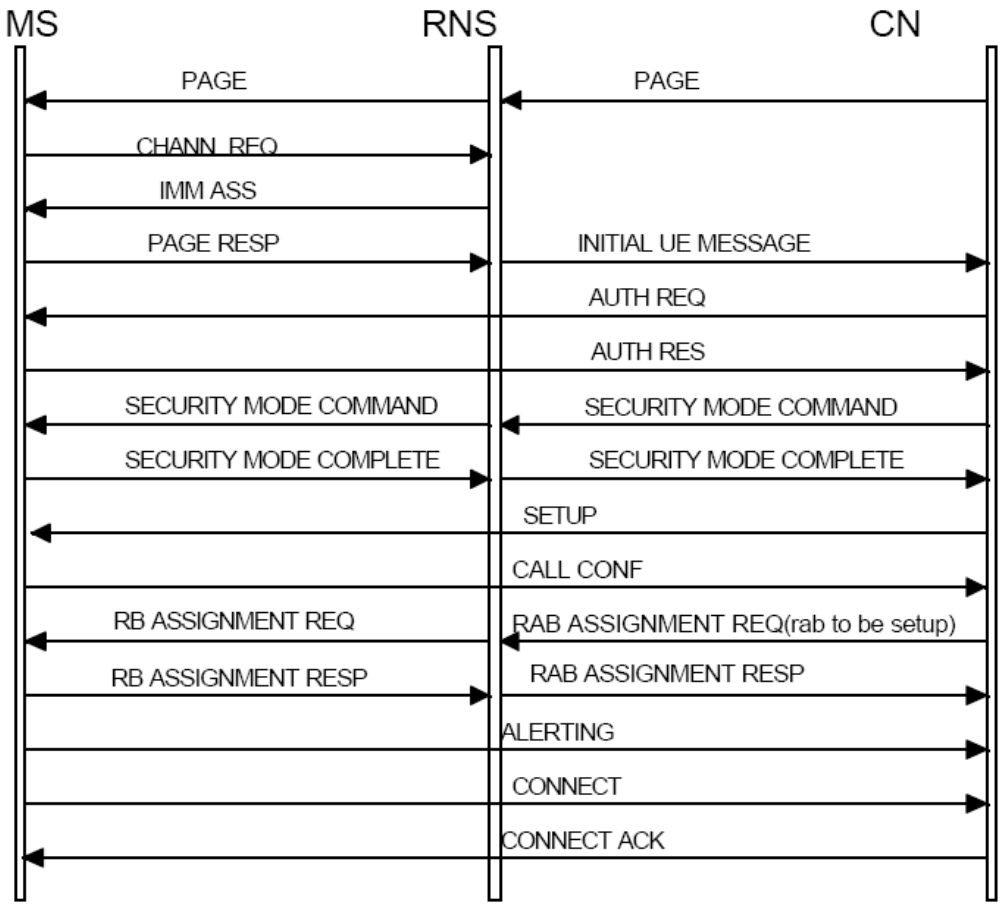


图4-21 移动终止建立过程

1）CN向RNS发送一个PAGE消息，RNS在寻呼信道上广播该寻呼消息。

2）被叫 MS监测到该寻呼，将向RNS发送一个信道请求，RNS回应立即指配命令，指示MS使用指定的信令信道。

3）然后 MS将在该信令信道上发送一个寻呼响应消息，CN收到MS的寻呼响应消息后，将发起鉴权和加密过程。

4）CN将发送SETUP消息给RNS，该消息中包含有该呼叫的承载能力。

5）当MS从RNS接收到SETUP消息，它将回应一个CALL CONFIRMED消息。如果协商的承载能力参数有变化，则该消息中要包含有承载能力信息。

6）当 CN从 RNS接 收 到CALL CONFIRMED消 息时， CN将 向RNS 发 送RAB ASSIGNMENT REQ消息要求进行无线信道的指配， RNS将通过向MS发指配消息命令MS调节到一个指定的通信信道上，MS调到指定的信道上之后，将向RNS发送指配完成消息。

7）RNS向CN发RAB ASSIGNMENT RESP消息。

8）MS发送ALERTING消息指示被叫用户振铃。

9）当被叫用户应答时，被叫MS将发送一个CONNECT消息经过RNS到CN，

10）CN将给MS回应CONNECT ACK消息，呼叫建立过程结术。

4.5.3 RAB流程

1. RAB管理功能

RAB（Radio Access Bearer）定义在 UE和CN之间建立。根据签约用户数据、CN业务能力和UE业务请求的QoS的不同而使用不同的RAB。

RAB ID与NAS绑定信息有关。例如，在电路域，RANAP 层的RAB ID与CC子层的SI在数值上相同。SI由UE来分配，CN在分配RAB ID时把SI和RAB ID一一对应起来。对一个UE来说，RAB ID在RB（Radio Bearer）和Iu承载上是全局的，而且一个RAB ID对应一个唯一的用户面连接的实例（一个Iu UP实例）。

CN控制RAB的建立、修改和释放。RAB建立、修改和释放是CN发起的功能。

RAB建立、修改和释放是UTRAN执行的功能。RAB释放请求是UTRAN发起的功能（当UTRAN不能与UE保持RAB时触发该功能）。

在RAB建立时CN把RAB映射到Uu接口承载上。UTRAN把RAB映射到Uu接口传输承载和Iu接口传输承载上。

在CS域如果使用AAL2承载，UTRAN负责发起AAL2连接建立和释放。

RAB的优先级由CN根据签约信息、QoS信息等内容决定。CN在请求RAB建立、修改消息中指定优先级、预占能力和排队特性。 UTRAN执行RAB排队和资源预占。

2. AB接入控制

当CN接收到请求建立或修改RAB时（在R99电路域规范中RAB QoS用BC IE来映射）， CN验证是否该用户允许使用请求参数的RAB，根据验证CN将接受或拒绝该请求。

当UTRAN从CN接收到建立或修改RAB的请求时，准入控制实体根据当时的无线资源条件的

分析判断是否接受或拒绝。

3. AB建立，释放，修改控制流程

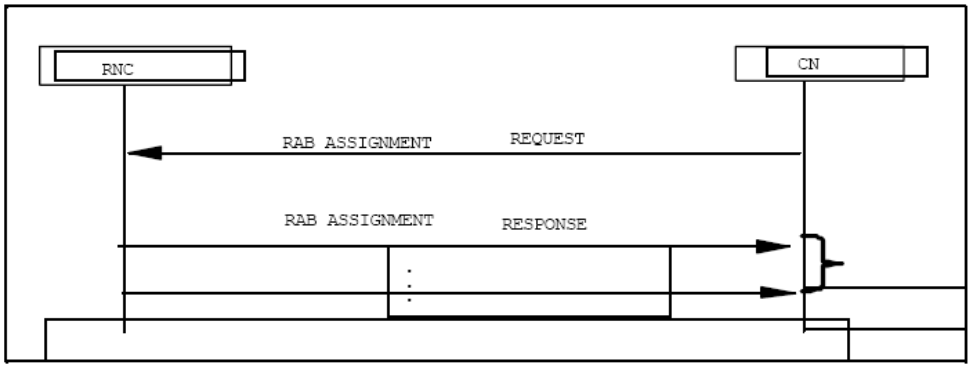


图4-22 Iu接口RAB Assignment 过程

RAB Assignment过程的目的是修改和/或释放已经建立的RAB，和/或建立新的RAB。 本过程是面向连接的。

CN 首先发送 RAB Assignment Request 消息给 RNC，然后CN启动定时器TRABAssgt。在一条RAB Assignment Request消息中， CN可以要求 UTRAN建立/修改/释放一个或几个RABs，本消息包含以下信息，主要是：

带有承载特性的需建立/修改的RAB列表；

需释放的RAB列表；

RAB ID在每一个Iu连接内是唯一的。如果RNC收到的消息中包括已经存在的RAB ID，那么RNC认为是修改该RAB（释放除外）。

RNC随时接收释放RAB的消息，并总是响应。如果RNC正在建立/修改某RAB，然后又收到释放该RAB的消息，那么RNC将停止RAB配置过程，释放与该RAB有关的所有资源并返回响应。

UTRAN 侧收到消息后将执行请求的 RAB配置，然后 UTRAN 发送 RABAssignment Response消息给 CN 报告请求结果。在一条 RAB AssignmentResponse消息中可以包含一个或几个RAB的信息，主要是：

成功建立/修改/释放的RABs；

不成功建立/修改/释放的RABs；

排队的RABs。

如果没有RABs被排队，则CN就停止TRABAssgt，然后RAB Assignment过程就结束于UTRAN侧。

当请求建立/修改的RABs被排队后，UTRAN就启动定时器TQUEUING，该定时器指定排队等候建立/修改的最大时间，且监督所有排队的 RABs。排队的RABs有如下可能的结果：

建立或修改成功；

建立或修改失败；

由于定时器TQUEUING超时而失败。

在第一条 RAB Assignment Response响应消息中，UTRAN 报告所有在RAB

ASSIGNMENT Request消息中涉及的RAB的状态。UTRAN接着在随后的RAB Assignment Response响应消息中报告排队的RAB状态，除了TQUEUING超时的RAB。当知道所有排队的RAB建 立/修改已经成功/ 失败后， UTRAN停止TQUEUING，RAB Assignment过程同时结束于CN与UTRAN。

当CN接收到RAB被排队的响应， CN期望在TRABAssgt超时前 UTRAN提供排队RAB的结果；否则，CN认为RAB Assignment过程结束，并且认为没有报告的RAB配置失败。

在定时器TQUEUING超时的情况下,在UTRAN所有的排队RABs都结束排队,UTRAN在一条RAB Assignment Response消息中报告所有的排队RAB状态。同时在CN侧停止该过程。

4. RAB建立流程

图6-23简要的描述了在CN和UE之间经过UTRAN而建立RAB的流程。

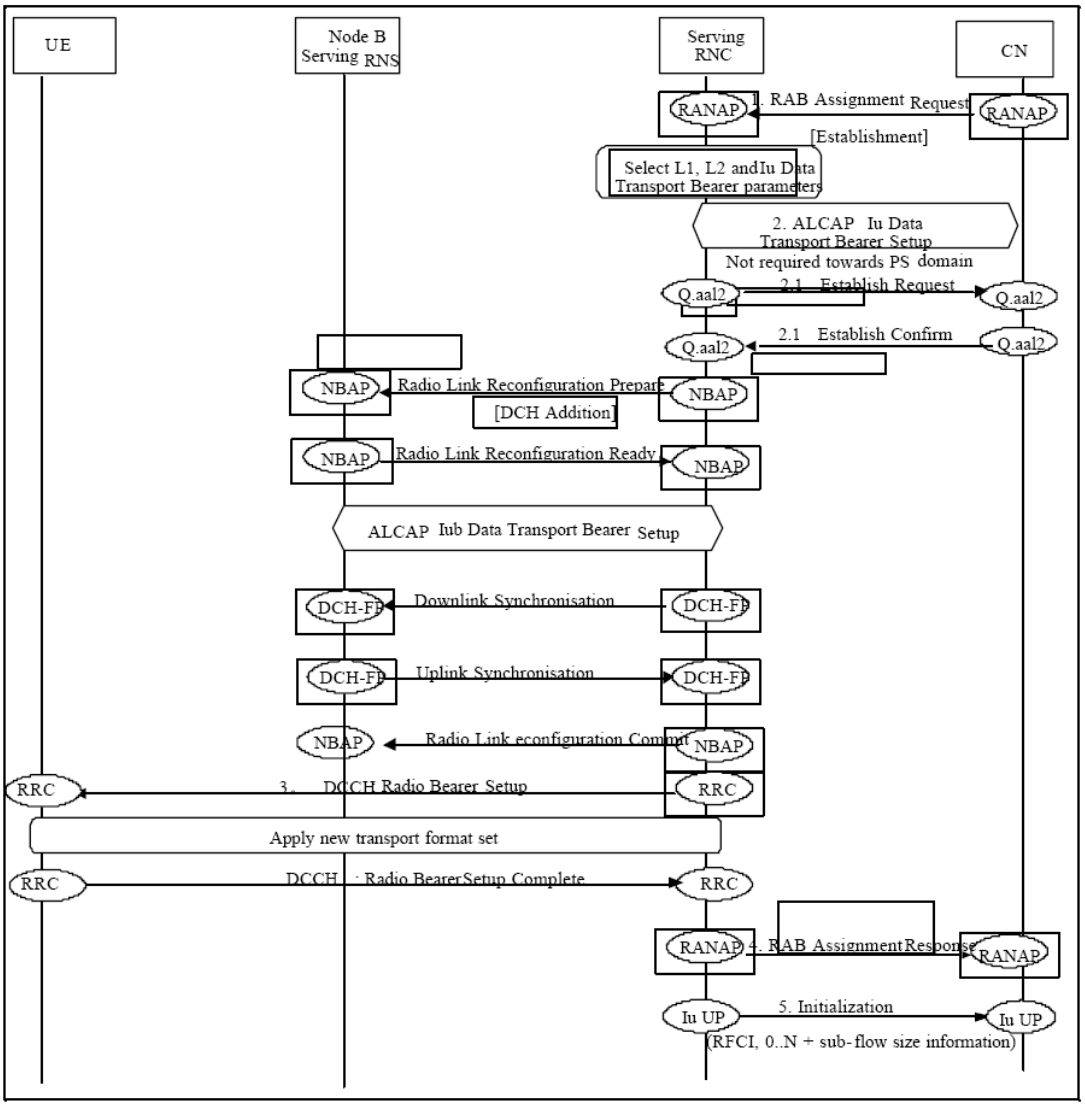


图4-24 无线接入承载建立-（DCH-DCH 同步建立流程）

这个例子说明了当 RRC连接已经建立好以后，在专用传输信道（ DCH）RRC状态下建立无线接入承载RAB（DCH）的过程。

时机：

在电路域，在CN接受UE的业务请求（主叫SETUP，被叫的CALL CONFIRM，CONNECT等消息）后指示需要一条新的 AS的承载通道来承载NAS用户数据时发送RAB Assignment Request消息启动这一过程。

过程描述：

1）CN根据签约用户数据、CN业务能力和UE业务请求的QoS决定采用什末样的RAB。通过RANAP消息Radio Access Bearer Assignment Request（Setup）请求建立RAB。其中的RAB ID根据SI的值来填充，在电路域重要参数有RAB参数，用户面模式，本端用户面ATM地址，IU传输标识（BINDING ID）。

2）服务RNC使用ALCAP协议初始化Iu接口数据传输承载的建立。

在电路域使用AAL2承载的情况下（在PS域这一过程不需要），AAL2连接建立 过 程 如2.1，2.2所述。在AAL2的连接建立请求中使用SUGR参数将BINDING ID透传给CN，用它完成RAB和数据传输承载的绑定，这一消息中的重要参数还有：

对端ATM地址，通路识别（PATH ID），通道识别（CID），通路特性，通道特性等。

3)服务RNC在和Node B等重配置好无线链路，完成上下行链路同步后，通过RRC消息Radio Access Bearer Setup 把RAB参数中的子流和子流组合参数和RAB ID等传给UE。

4）服务RNC在收到UE的成功证实RRC消息Radio Bearer Setup Complete和ALCAP过程的成功建立后向CN证实RAB成功建立。发RANAP消息Radio

Bearer Assignment Response到CN。

5）如果用户面是支持模式，报告结果后UTRAN再通过初始化Iu接口用户面。

说明：

对于其中和Drfit RNC，Drift Node B的交互的流程，图中没有描述。

对于RACH/FACH - DCH，RACH/FACH - RACH/FACH以及分组域的非同步方式，过程类似。

5. RAB释放流程

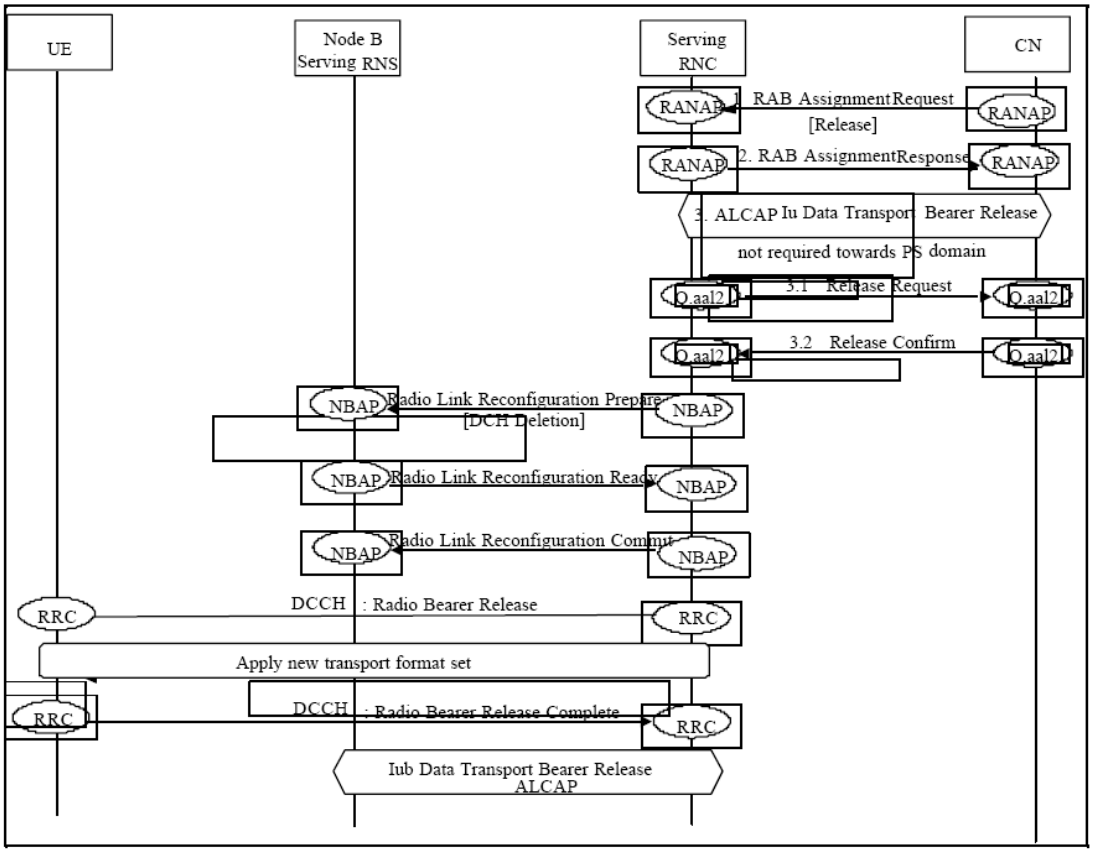


图4-25 无线接入承载释放-（DCH - DCH- 同步释放流程）

启动时机：

在电路域，在 CC层使用该RAB的事物全部结束或RNC请求释放该RAB时启动此过程。

过程描述：

1 ）CN通过发送RANAP消息Radio Access Bearer Assignment Request。（Release)启动RAB释放过程，其中指明是哪一个RAB ID。

2）业务RNC以RANAP消息Radio Access Bearer Assignment Response来证实。

3）业务RNC使用ALCAP协议，如果是 AAL2承载，使用 AAL2 释放消息来启动和CN之间的Iu数据传输承载的释放（在PS域这一过程不需要）。

4）业务RNC在释放了和Node B等的链路后， 发 送 RRC消 息 Radio Bearer Release给UE启动承载释放过程。

5）业务RNC在收到UE的证实RRC消息Radio Bearer Release Complete后。整个释放过程结束。

6. RAB修改流程

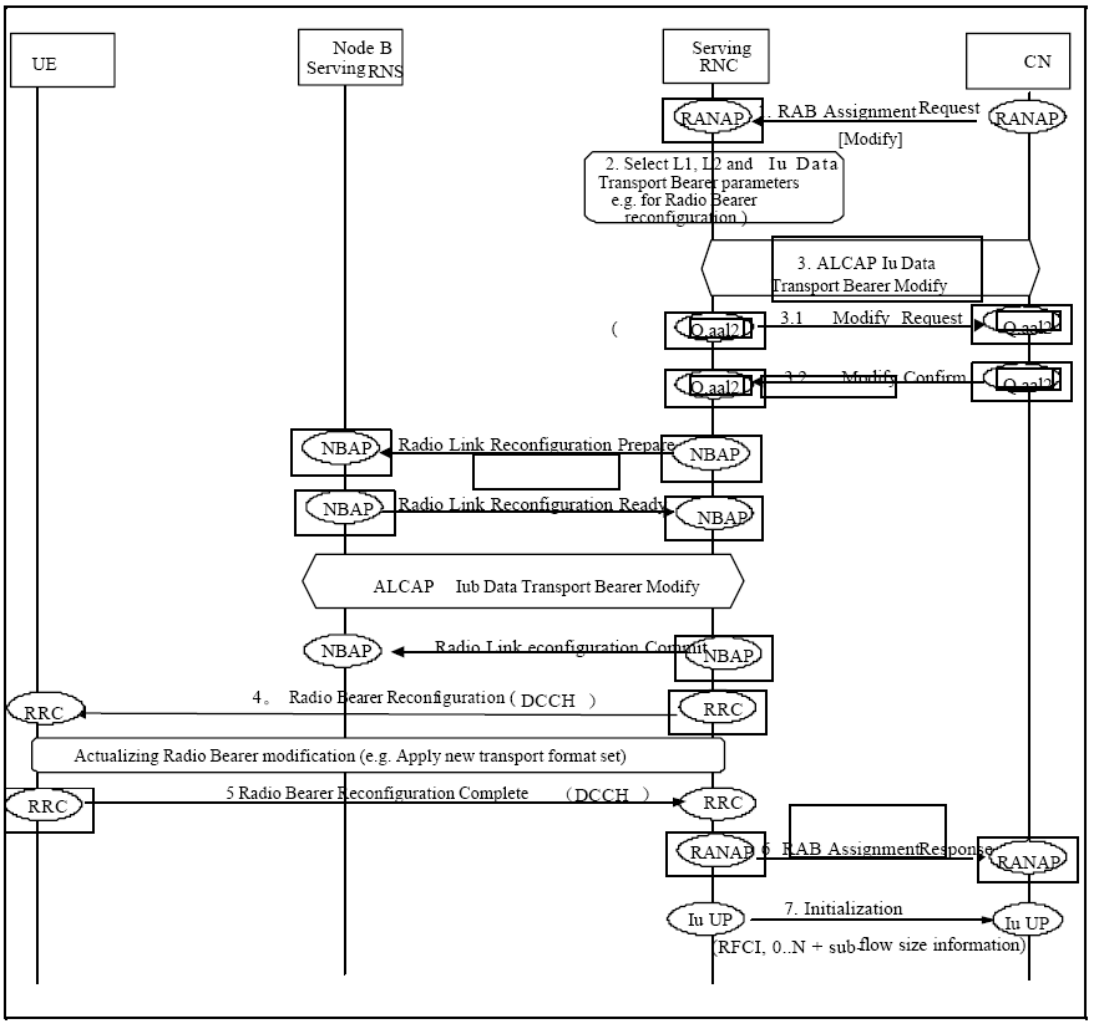


图4-26 无线接入承载修改（DCH-DCH 同步修改）

启动条件：

UE业务切换或速率调整时，CN重配置业务信道以支持业务属性的改变。

过程描述：

1）CN通过RANAP消息Radio Access Bearer Assignment Request（Modify）请求修改RAB。其中的RAB ID根据指明RAB 标识，在电路域重要参数有RAB参数。

2）服务RNC选择哪种参数应该被修改，哪种程序应该被启动。

3）服务RNC使用ALCAP协议修改Iu接口数据传输承载的通道特性。

如果使用AAL2承载，修改过程如3.1，3.2描述。

4)等到Iu接口传输控制面的修改过程成功后，服务RNC在和Node B等修改好无线链路后，通过 RRC消息Radio Bearer Reconfiguration把RAB参数中的子流和子流组合参数和RAB ID等传给UE。

5，6 ）服务RNC在收到UE的成功证实RRC消息Radio Bearer Setup Complete后向CN证实RAB成功建立。发 RANAP消息Radio Bearer Assignment Response到CN。

7 ）如果用户面是支持模式，报告结果后UTRAN再通过初始化Iu接口用户面。

4.5.4 寻呼流程

寻呼过程是CN向被叫发起的寻呼过程，当CN需要向和被叫用户建立连接时，首先需要通过寻呼过程找到被叫，寻呼过程的作用就是使CN能够寻呼到被叫用户，寻呼过程通过无连接信令方式建立。

CN通过向被叫发起PAGING消息来开始寻呼程，PAGING消息应该包含足够的信息以使RNC能够找到被叫，如果一次寻呼不可及，CN负责通过 lu接口重复发寻呼的过程。

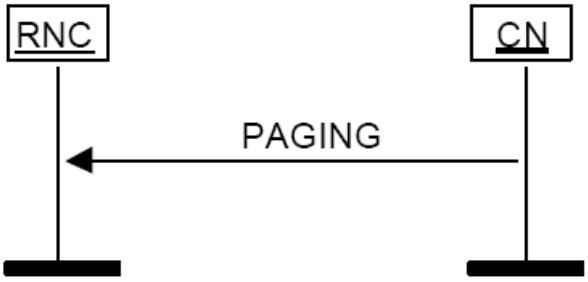


图4-27 成功寻呼流程

1. 寻呼过程

来自主叫的呼叫请求信息CN经过处理后，如果成功的得到了有关被叫用户的信息，寻呼过程就可以开始。CN需要知道被叫所在的位置区信息，并且取得足够的寻呼信息参数，这样，CN就可以向被叫发起寻呼。

如果CN没有得到被叫用户的位置区信息，需要通过广播过程向CN下的所有RNC发起寻呼消息。

CN下发PAGING消息是通过RANAP接口进行的， RANAP接口处理来自CN的PAGING消息，PAGING包含的参数包括寻呼是来自CS域还是PS域的，是何种原因引发的寻呼，以及被叫用户的位置区信息等。由RANAP向被叫所属位置区下RNC发寻呼消息。

当PAGING消息到达RNC后，RNC通过分析寻呼消息的参数取得被叫所在的位置区信，RNC通过PCCH传送寻呼信息给位置区的 UE，如果被叫UE检测到RNC来的寻呼消息， 开始执行NAS信令过程。

如果寻呼成功，CN会得到寻呼响应消息，否则，CN需要通过lu接口重复发送寻呼消息。

以下就两个例子UE在RRC 空闲状态和RRC连接状态下的寻呼过程。

2. UE在RRC 空闲状态的寻呼过程

当RRC处于空闲状态时候，UE 可能会收到来自 CS或者PS的寻呼，因为此时UE处于空闲状态，CN可以知道该UE的位置区（LA)信息，因此，寻呼会通过该位置区来下发，这里列出了LA跨越两个RNC的情况。

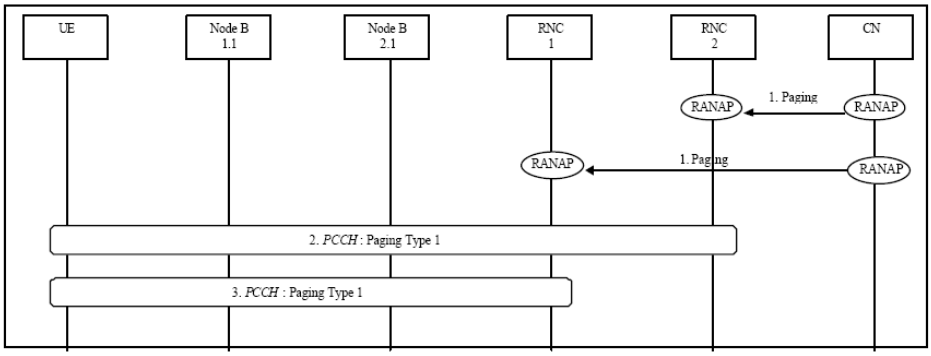


图4-28 RRC空闲状态下寻呼过程

1）CN通过发起的寻呼消息，跨过两个RNC到达被寻呼UE。

2）小区1用Paing Type1发起寻呼。

3）小区2用paging Type 发起寻呼。

PAGING 消息通过RANAP的到达RNC1，RNC2， RNC通过PCCH传送寻呼信息给位置区的 UE，如果被叫UE检测到RNC1或者RNC2来的寻呼消息， 开始执行NAS信令过程。

3. UE在RRC RRC连接状态下的寻呼过程

当RRC处于连接状态时候。这种情况在CN为CS域或者PS域两种情况，由于移动性管理的独立性，有两种可能的解决方案：

1）UTRAN来协调在已存在RRC连接上寻呼请求

2）UE来协调已存在RRC连接上的寻呼请求

以下例子说明在RRC连接状态（CELL_DCH 和 CELL_FACH 状态)执行寻呼UE过程的，由UTRAN在RRC连接的状态下用DCCH协调寻呼请求的情况。

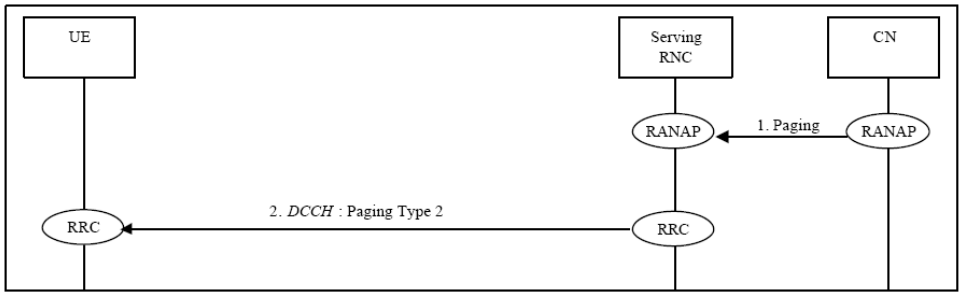


图4-29 在RRC连接状态（CELL_DCH 和CELL_FACH)下寻呼UE过程

1） CN通过RANAP发送PAGING消息来对UE寻呼。

2）SRNC对RRC发送消息 Paging Tyep2。

4.6.5 呼叫释放过程

当移动用户通话完毕，主叫方或被叫方挂机的消息要通知到网络侧，进行呼叫的释放过程。网络侧通过终止GSM PLMN之间或GSM PLMN与别的网络之间的电路交换连接而释放呼叫。

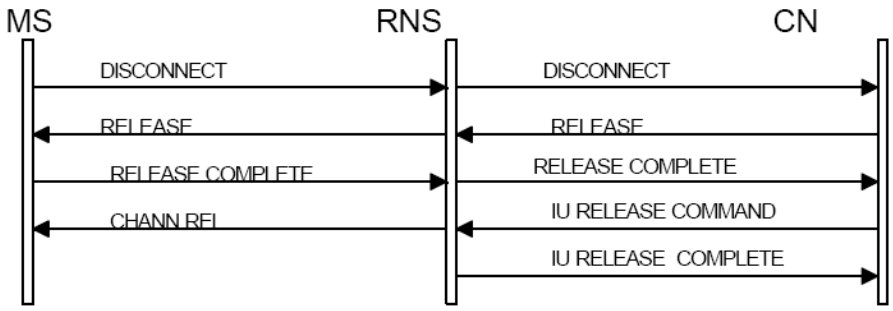


图4-30 移动发起呼叫释放的成功情况

1）移动方挂机之后，移动台通过向网络发送 DISCONNECT消息而发起呼叫清除；

2）网络接收到该消息之后发送一个RELEASE消息给移动台；

3）MS发RELEASE COMPLETE消息给网络，如果此时不再需要通信信道，则要执行信道的释放过程；

4）如果该呼叫是整个Iu连接上的唯一的一个呼叫，则要释放Iu连接。 CN向RNS发送IU RELEASE COMMAND消息请求释放Iu连接。

4.6 分组域会话管理流程

4.6.1 SM基本概念

1. SM功能概述

会话管理是3GPP协议中连接管理层（Connection Management）的一个主要的组成部分。位于移动性管理（Mobile Management）和用户面之间，使用GMM子层提供的无应答数据传送服务，向高层——用户面提供连接管理服务。

它一方面完成核心网络SGSN到GGSN之间的隧道建立、修改和释放的控制功能，另一方面完成SGSN和RNC/MS之间无线接入承载（Radio Access Bearer）建立、修改和释放的控制。

2. 术语

1）PDP CONTEXT

PDP上下文保存了用户面进行隧道转发的所有信息，包括RNC/GGSN的用户面IP地址、隧道标识和QoS等。

2）NSAPI

在MS中NSAPI用于标识一个PDP服务访问点，在SGSN/GGSN中用于表示一个会话。

3）RAB ID

在接入层标识用户的一个RAB，它的取值等于NSAPI。

4）APN解析

Access Point Name，采用标准域名格式。APN包括两部分：网络名和运营商名。在 GGSN

中用于标识一个指定的外部网和一种服务的ISP，在SGSN中可根据APN通过DNS解析得到与此APN对应的GGSN地址。

5）PDP地址匹配和APN选择

一个用户可以使用多个PDP地址和APN，在激活一个会话时，用户请求的PDP地址和APN必须满足签约数据的要求。根据请求的地址和 APN找到满足此要求的签约PDP CONTEXT数据的过程称为PDP地址匹配和APN选择。

6）QoS协商

会话管理在建立分组传输路由的同时，也必须指定此路由满足的QOS，会话管理过程在MS、RNC、SGSN、GGSN之间进行QoS协商，使各节点提供的服务质量保持一致。 QoS协商的算法是在签约的QOS、SGSN能提供的最大QOS和其它节点满足的QOS之间取最小值。

3. SM在协议栈中的位置

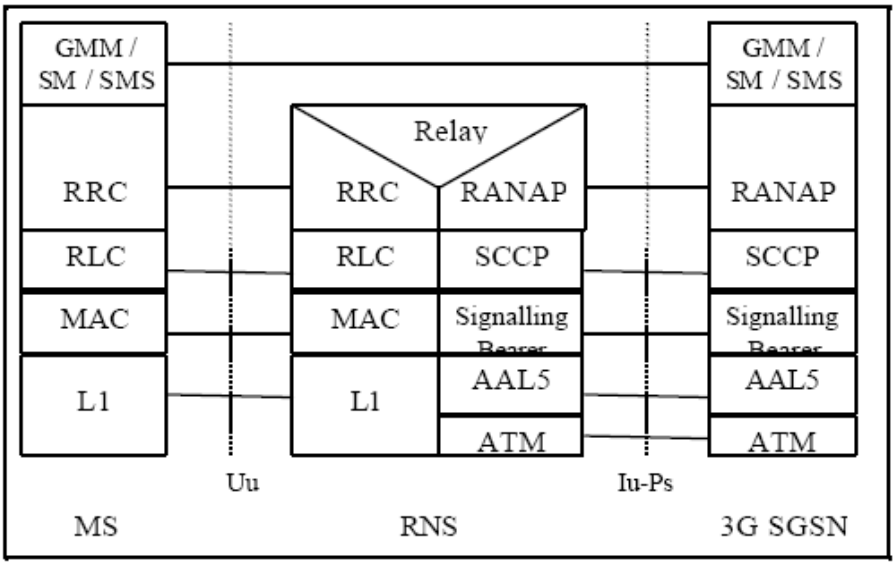


图4-31 UMTS MS-SGSN的控制面协议

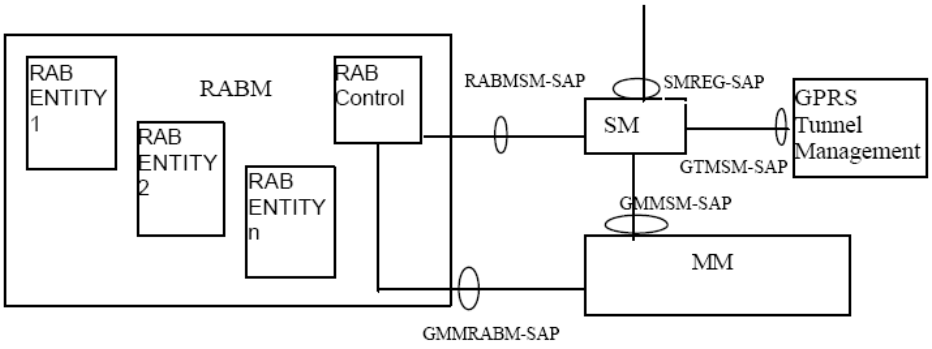


图4-32 SM与各协议单元的关系：

SM与其他协议单元的服务访问点说明：

RABMSM-SAP：

完成RAB激活、修改、去激活的控制功能；接口原语有：

RABMSM-ACTIVATE-IND SM指示RABM指定NSAPI的会话已激活；

RABMSM-ACTIVATE-RSP RABM完成创建RAB后向SM返回响应；

RABMSM-DEACTIVATE-IND SM指示RABM指定NSAPI的会话已去激活；

RABMSM-DEACTIVATE-RSP RABM完成去激活RAB后向SM返回响应；

RABMSM-DEACTIVATE-REQ RABM在指配失败后向SM发起去激活请求；

RABMSM-MODIFY-IND SM指示RABM指定NSAPI的会话已修改；

RABMSM-MODIFY-RSP RABM完成修改RAB后向SM返回响应；

RABMSM-STATUS-REQ RABM通知SM出错；

GMMRABM-SAP:

Service Request过程，通知RABM有上行数据传送，RABM进行RAB重建。

UL-DATA-IND 上行数据传送指示；

GMMSM-SAP：

GMM在次SAP向SM提供无应答数据透传服务，另外在Detach时通知SM释放；

接口原语有：

GMMSM-RELEASE-IND MS Detach时通知SM的释放指示；

GMMSM-UNITDATA-REQ SM的无确认数据传送请求；

GMMSM-UNITDATA-IND GMM向SM发送无确认的数据指示；

GTMSM-SAP ：

SM与隧道管理之间的接口，完成SGSN-GGSN之间的隧道创建、修改、删除的控制功能；

GTMSM-CRT-REQ SM请求GTP隧道管理创建隧道；

GTMSM-CRT-RSP 隧道管理创建GTP隧道之后向SM返回响应；

GTMSM-MDF-REQ SM请求GTP隧道管理修改隧道；

GTMSM-MDF-RSP GTP隧道管理修改隧道之后的响应；

GTMSM-DEL-REQ SM请求GTP隧道管理删除隧道；

GTMSM-DEL-RSP GTP隧道管理删除隧道之后向SM返回响应；

GTMSM-PDU-NTF-IND GTP隧道管理通知SM有下传数据；

GTMSM-PDU-NTF-RSP SM向GTP隧道管理返回数据通知响应；

GTMSM-PDU-NTF-REJ-REQ SM向GTP隧道管理返回数据通知拒绝请求；

GTMSM-PDU-NTF-REJ-RSP GTP隧道管理向SM返回数据通知拒绝响应；

GTMSM-ERR-IND GTP隧道管理通知SM用户面出错；

4. 与SM相关的功能实体

(1) RAB管理

RABM（RAB Management）完成RAB的创建、修改、释放和重建的管理功能。

RAB由两部分组成：RNC和SGSN之间的 GTP隧道以及RNC与MS之间的无线承载（Radio Bearer）。RAB ID唯一标识用户的一个RAB。

RAB的建立、修改、释放和重建都是通过RAB ASSIGNMENT过程完成的。

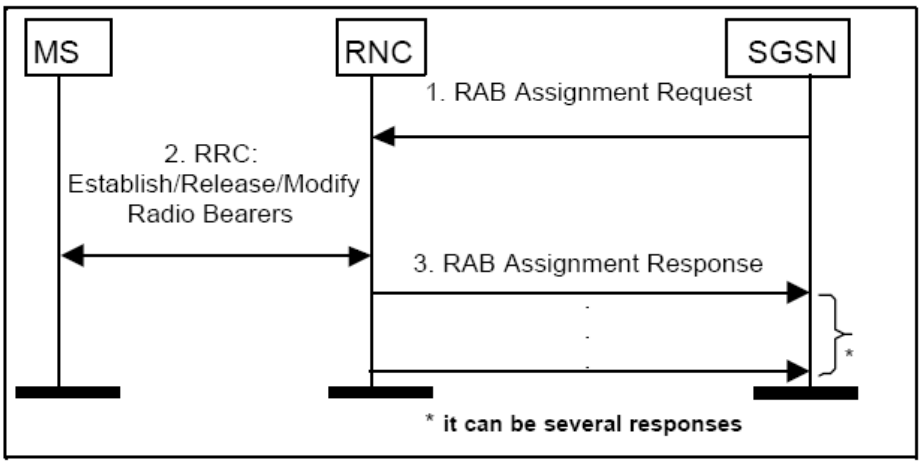


图4-33 RAB管理流程图

流程说明：

1 ） SGSN向RNC发送RABAssignment Request（SGSN ADDR，TEIDs，QOS）消息，请求建立、修改或释放RAB(s)，在指配参数中可指定RAB的无线优先级，是否允许抢占和排队；

2）RNC建立、修改或释放无线承载；

3）RNC向SGSN发送RAB Assignment Response，如果因为 QoS的原因指配失败，则要降低QoS重发指配请求。

如果RAB重建时发生QoS改变，则执行SGSN发起的PDP CONTEXT修改流程，将QoS通知MS和GGSN。

(2) 隧道管理

隧道管理的主要任务是创建SGSN到GGSN之间的GTP隧道。隧道管理包括创建隧道、修改隧道、删除隧道和网络侧发起PDP CONTEXT激活的管理。

PDP CONTEXT的激活、修改、去激活和保留过程

SM通过PDP CONTEXT的激活、修改、去激活信令流程实现会话管理。PDP CONTEXT 激活流程建立用户面的分组传输路由；PDP CONTEXT修改流程修改激活的 PDP CONTEXT 的QOS和TFT，在发生RAU改变时，也需要修改SGSN到GGSN之间的隧道路由；PDP CONTEXT去激活流程用于拆除激活的PDP CONTEXT。SM的状态机模型如下图所示：

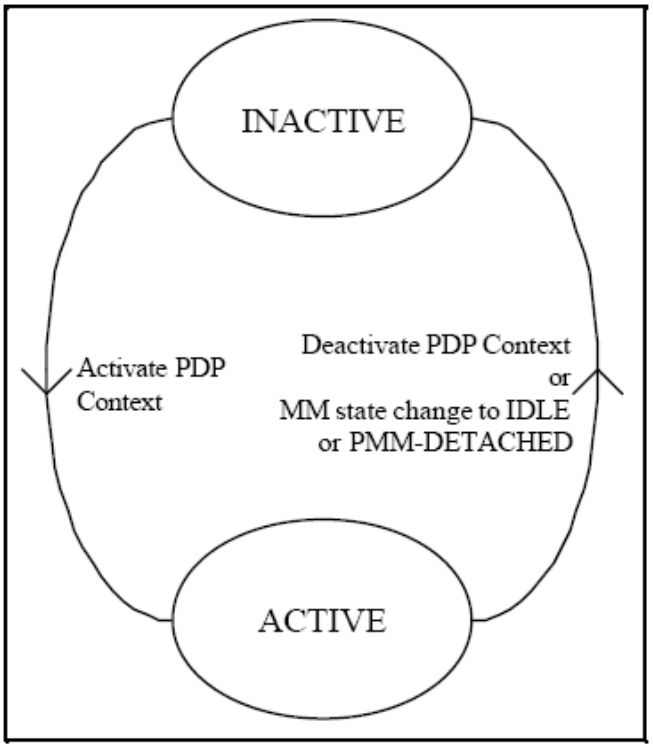


图4-34 PDP状态机模型

在用户进行激活流程之前，SGSN上 的SM必须先进入PMM-CONNECTED状态。

一个用户可以有多个签约的 PDP地址，每一个PDP地址可能包含一个或多个会话，每个对话有两种状态：激活态和非激活态（ACTIVE/INACTIVE）。非激活的会话不包含路由信息，不能进行数据的转发。

二次激活使用和一次激活相同的PDP ADDRESS、APN，但使用不同的QOS，在激活之后，二次激活的PDP CONTEXT和一次激活的PDP CONTEXT是完全对等的。发生 R99到R98/97的路由区更新时，对共享地址和APN的激活的PDP CONTEXT（s），保存QOS最高的PDP CONTEXT，其它的PDP CONTEXT将被去激活。

RNC发起RAB或IU释放之后，SGSN可以保留这些激活的PDP CONTEXT，而不进行去激活。当用户发起SERVICE REQUEST过程时进行RAB的重建，恢复数据传送。

下面将分节讨论各个会话管理流程。

4.6.2 PDP Context激活功能

PDP CONTEXT激活包括MS发起的，网络发起的PDP CONTEXT激活和二次激活。

1. MS发起的PDP Context激活

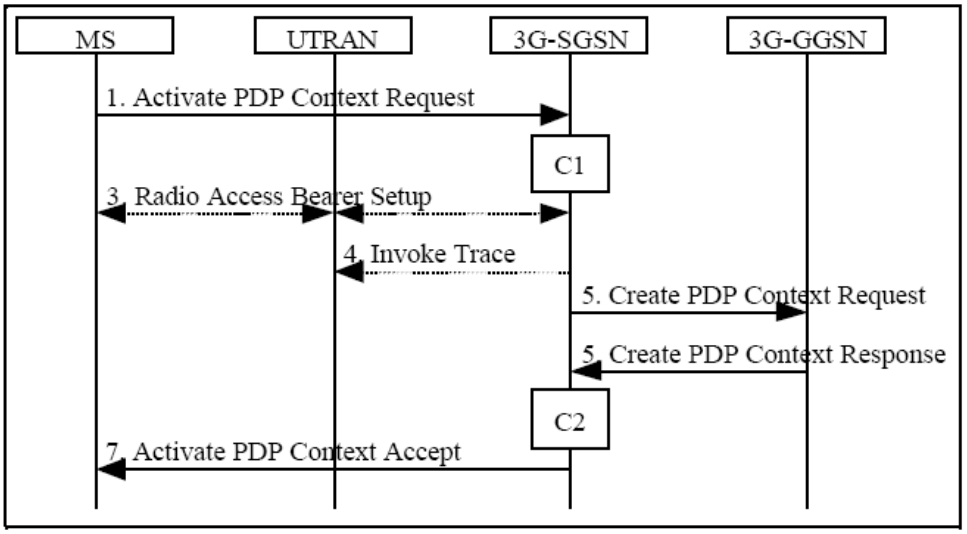


图4-35 M S发起的PDP CONTEXT激活过程

1）MS 向SGSN发送激活请求Activate PDP Context Request（NSAPI，TI ，PDP Type ，PDP Address， Access Point Name ， QoS Requested ）。PDP Address指出是动态地址还是静态地址。如是动态地址，则设为空。

2）执行RAB指配过程；

3）SGSN通过使用PDP Type（optional），PDP Address（optional），Access Point Name（optional）和PDP CONTEXT签约数据来验证Activate PDP Context Request的有效性；

SGSN给PDP Context分配TEID，如果使用动态地址，则要求GGSN分配一个动态地址。SGSN根据一定的算法选择一个APN，SGSN向GGSN发创建PDP Context请求（PDP Type，PDP Address，Access Point Name，QoS Negotiated，TEID，NSAPI，MSISDN，Selection Mode，ChargingCharacteristics，Trace Reference，Trace Type，Trigger Id，OMC Identity，PDP Configuration Options）。

GGSN为PDP context分配动态地址，计费ID，协商QoS。如果MS要求外部网分配IP地址，则设为0.0.0.0，在以后外部网分配地址后，执行GGSN发起的PDP CONTEXT修改过程；

4 ）收到GGSN的CREATE PDP CONTEXT RESPONSE（NSAPI，PDP ADDR，GGSN ADDR，TEID，QOS），SGSN将地址，Qos等信息通过Activate PDP Context Accept 发送给MS。

2. 二次激活

一个PDP地址可对应多个PDP Context，二次激活仅在相同的PDP地址和APN上有激活的PDP Context时才发起。二次激活的PDP Context与已激活的PDP Context只有Qos profile不同，每个PDP context使用唯一的TI和NSAPI。

二次激活执行过程APN选择和地址协商不必执行，流程与PDP contextv Activation过程类似。

在许多PDP Context中，只允许一个PDP Context没有TFT。

传输下行N-PDU时，GGSN按TFT匹配选择合适的PDP context。MS发送数据时，按QOS选择

不同的PDP context。

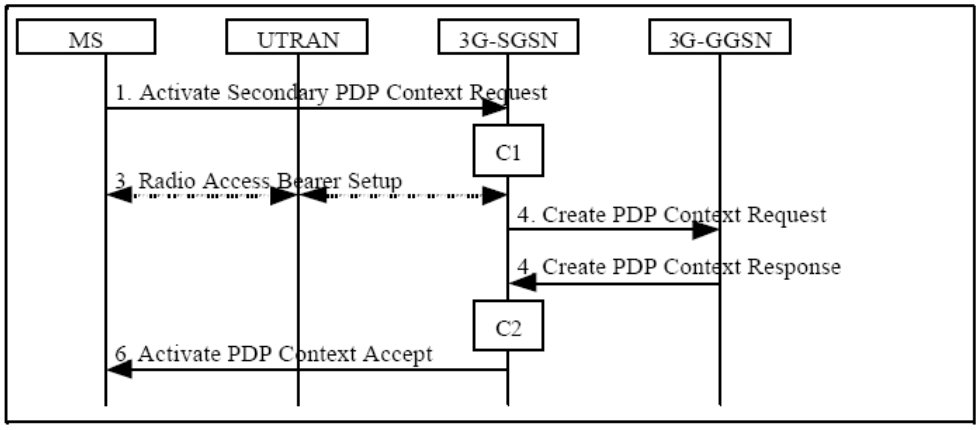


图4-36 二次激活流程

3. 网络发起的PDP Context激活

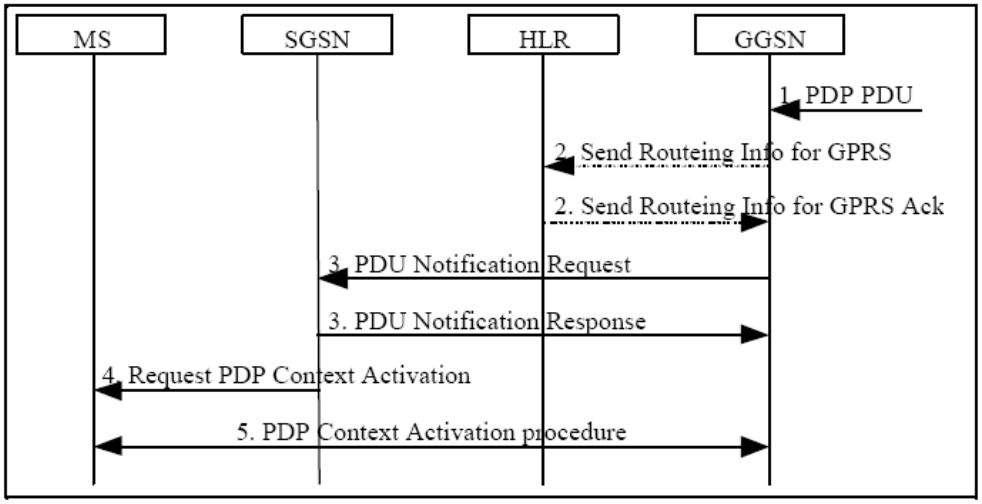


图4-37 网络侧发起的PDP CONTEXT激活过程

1） GGSN收到PDP PDU，向HLR发送Send Routeing Information for GPRS （IMSI），取SGSN的地址

2 ）如果MS可达，则HLR发送Send Routeing Information for GPRS Ack（IMSI，SGSN Address，Mobile Station Not Reachable Reason）返回 SGSN的地址，否则返回错误，如果错误不是“No Paging Response”，HLR将此GGSN添加到该用户的GGSN-List。

3）如SGSN存在或错误是“No Paging Response”，则发送PDU Notification Request（IMSI，PDP Type，PDP Address，APN）通知给SGSN;

4)SGSN返回应答PDU Notification Response(Cause),确认将要请求MS激活PDP context过程。

5）SGSN 向 MS 发 送Request PDP Context Activation（TI ，PDP Type，PDP Address，APN）要求MS发起激活PDP context请求。

6）MS发起PDP CONTEXT激活过程。

4.6.3 PDP Context修改功能

PDP CONTEXT修改过程包括：

MS发起的PDP Context修改过程

SGSN发起的PDP Context修改过程

GGSN发起的PDP Context修改过程

RAB/IU释放，SGSN发起PDP CONTEXT修改流程；

修改参数包括:

QoS Negotiated;

Radio Priority;

Packet Flow Id;

PDP Address （GGSN发起的修改过程 in case of the GGSN-initiated modification procedure）；

TFT（MS发起的修改过程）。

1.SGSN发起的PDP Context修改

SGSN发起的PDP CONTEXT修改过程包括:

HLR向SGSN插入用户数据而且会话处于激活状态，SGSN发起PDP Context修改过程。

RAB重建，发生QOS改变，SGSN发起PDP CONTEXT修改流程；

SGSN 之间的路由区更新过程，如果会话处于激活状态，SGSN 发起PDP CONTEXT 修改流程；

MS、SGSN、GGSN发起的PDP Context修改最主要的过程就是QOS协商和路由的重新建立。

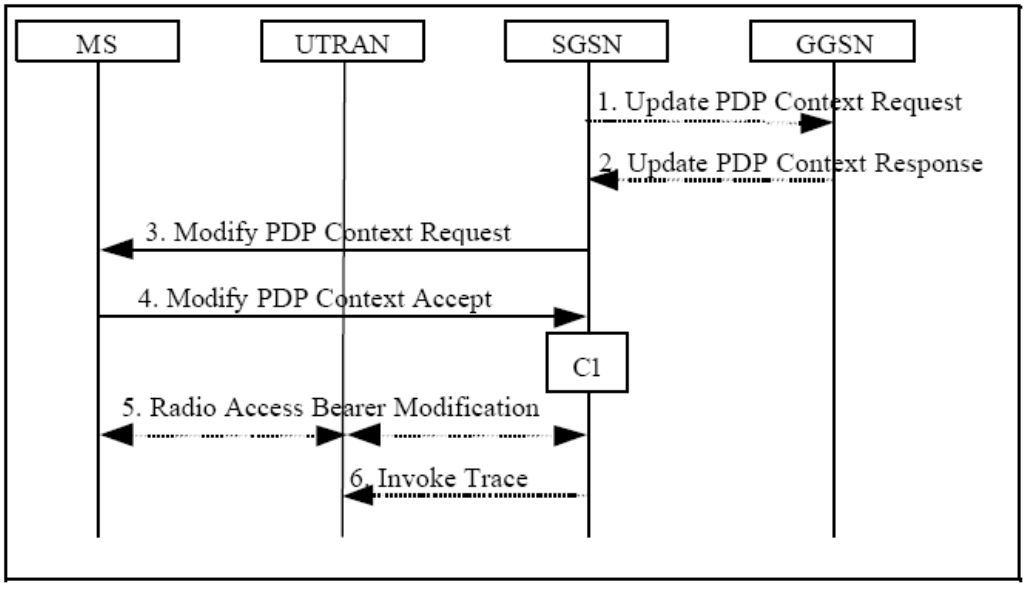


图4-38 SGSN发起的PDP CONTEXT修改过程

1）SGSN发送更新请求Update PDP Context Request(TEID，NSAPI，QoS =Negotiated ，Trace Reference，Trace Type，Trigger Id，OMC Identity）与GGSN协商QOS;

2 ） GGSN 进 行 QOS 协 商 ， 向 SGSN 发 送 Update PDP Context Response（TEID，QoS Negotiated，Cause）；

3） SGSN 按 QOS选择无线优先级和 Packet Flow Id。向MS发送修改请求Modify PDP Context Request（TI，QoS Negotiated，Radio Priority，Packet Flow Id）；

4）MS 接受QOS，则向 SGSN发送Modify PDP Context Accept，如MS 不接受QOS，则发起去活PDP context过程；

5）执行RAB指配过程修改RAB；

6）如果启动 BS跟踪，则要发引用跟踪消息 Invoke Trace（Trace Reference，Trace Type，Trigger Id，OMC Identity）。

2. MS发起的PDP Context修改

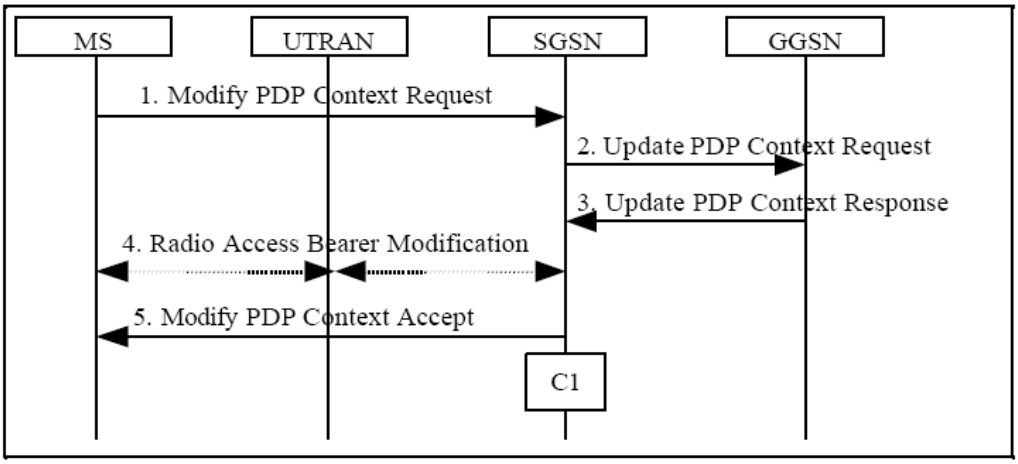


图4-39 MS发起的PDP CONTEXT修改过程

MS发起修改流程的目的是为了改变PDP CONTEXT的QoS或TFT。

1 ）MS向SGSN发送Modify PDP Context Request（TI，QoS Requested，TFT）消息，请求修改PDP CONTEXT；

2）SGSN进行QOS协商，发送更新请求Update PDP Context Request（TEID，NSAPI ， QoS Negotiated，Trace Reference，Trace Type，Trigger Id， OMC Identity）与GGSN协商QOS；

3)GGSN进行QOS协商，向SGSN发送Update PDP Context Response(TEID,QoS Negotiated，Cause）；

4）执行RAB指配过程修改RAB；

5）SGSN向MS发送Modify PDP Context Accept。

3. GGSN发起的PDP Context修改

GGSN的修改流程的目的是改变传输路由的QoS或用户的PDP ADDRESS，有两种情况：

GGSN作为DHCP中继代理，收到外部网给MS分配的IP地址；

GGSN中会话的QOS发生改变；

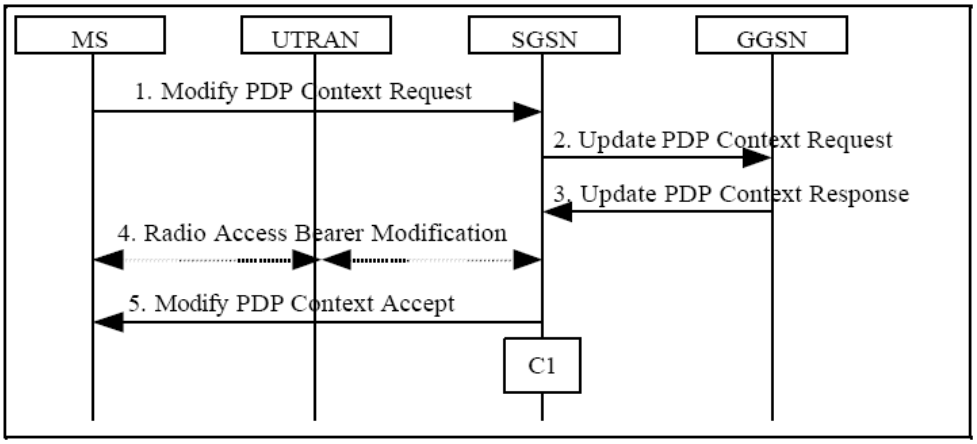


图4-40 GGSN发起的PDP Context 修改

流程说明：

1） GGSN向SGSN发送Update PDP Context Request（TEID，NSAPI，PDP Address，QoS Requested）；

2）SGSN 进行Qos协商，向MS发送修改PDP CONTEXT的请求Modify PDP Context Request（TI ，PDP Address，QoS Negotiated，Radio Priority， Packet Flow Id）；

3）如果MS接受指定的QoS，向SGSN返回修改接受Modify PDP Context Accept消息，如果拒绝接受，发起PDP CONTEXT的去激活过程；

4）执行RAB修改过程；

5）如果SGSN收到Modify PDP Context Accept ，则向GGSN发送Update PDP Context Response（TEID，QoS Negotiated），如果收到Deactivate PDP Context Request，则执行MS发起的去激活过程。

4. IU/RAB释放引起的PDP Context修改

RNC向SGSN 发送IU RELEASE REQUEST或 RAB RELEASE REQUEST，释放Iu/RAB成功之后:

SGSN，对背景级和交互级的通信，PDP Context不改变

SGSN，对流级和实时会话级的通信，PDP Context不改变，但将最大通信速率降到0，同时通知GGSN也将最大传输速率降到0

对MS失去无线覆盖之后:

对背景级和交互级的通信，PDP Context不改变

对流级和实时会话级的通信，当 RRC重建失败后， PDP Context保留，但将最大通信速率降到0，在重新获得覆盖后，利用PDP Context修改过程重建PDP Context和RAB。

4.7.4 PDP Context去激活功能

PDP Context 去激活流程包括MS发起的、SGSN发起的和GGSN发起的PDP Context去激活过程。

1. MS发起的PDP Context去激活

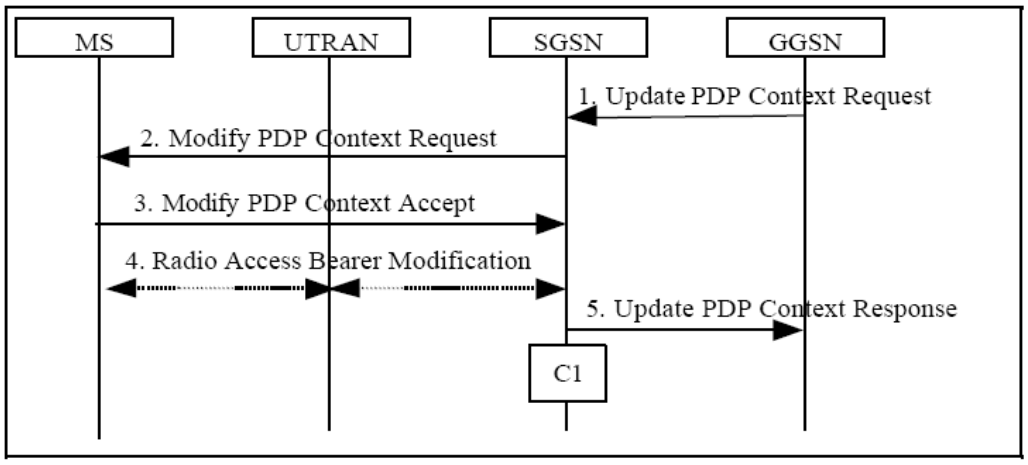


图 4-41 M S 发起的 PDP Context 去激活过程

1）MS向SGSN发送去激活请求Deactivate PDP Context Request（TI，Teardown Ind），Teardown Ind指示是否去激活和指定TI共享地址的激活的PDP CONTEXT。

2）SGSN 收到MS的去激活请求，向GGSN发送Delete PDP Context Request（TEID，NSAPI，Teardown Ind）删除GGSN PDP Context；

3）GGSN向SGSN发送Delete PDP Context Response（TEID）；

4）收到Delete PDP Context Response后，然后向MS发送去激活接受应答；

5）SGSN调用RAB指配过程释放RAB；

2. SGSN发起的PDP Context去激活

SGSN发起的去激活通常由于MM释放或各种异常情况引起，例如MS、SGSN、GGSN之间PDP CONTEXT不一致，RAB重建失败，资源不足等。

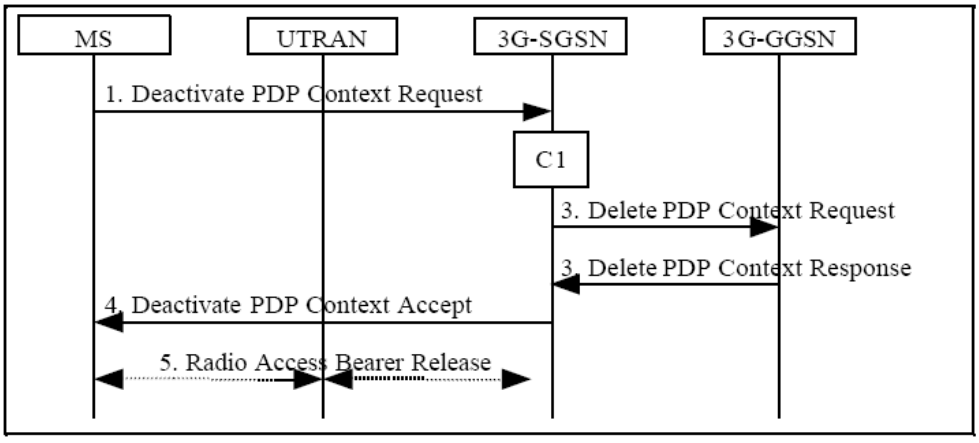


图 4-42 SGSN 发起的 PDP Context 去激活

1）SGSN向GGSN 删除PDP Context 请求，Delete PDP Context Request（TEID， NSAPI ，Teardown Ind），Teardown Ind指示是否去激活和指定TI共享地址的激活的PDP CONTEXT。

2）GGSN向SGSN发送Delete PDP Context Response（TEID）；

3）得到GGSN的删除应答后，向MS发送Deactivate PDP Context Request删除MS PDP

Context，如果是DETACH引起的PDP CONTEXT去激活，不发此消息；

4）收到MS发来Deactivate PDP Context Accept ；

5）SGSN发起RAB assignment procedure释放RAB。

3. GGSN发起的PDP Context去激活

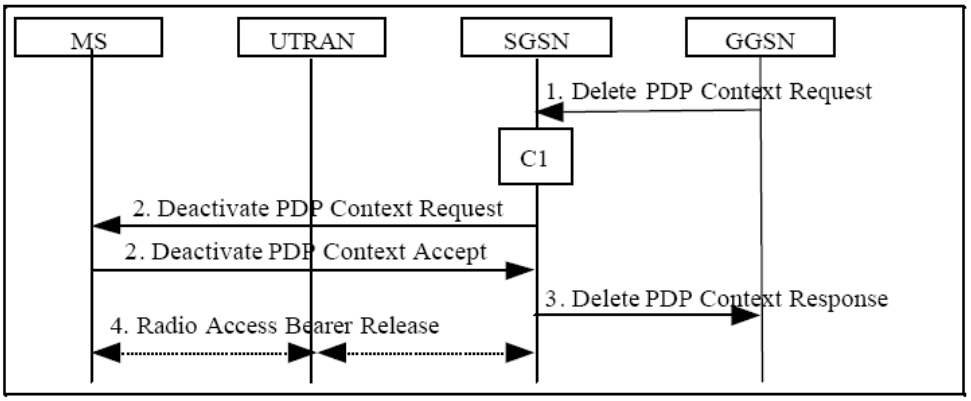


图 4-43 GGSN 发起的 PDP Context 去激活过程

过程说明：

1）GGSN向SGSN发送删除PDP CONTEXT的请求消息Delete PDP Context Request（TEID，NSAPI，Teardown Ind），Teardown Ind指示是否去激活和指定TI共享地址的激活的PDP CONTEXT。

2）SGSN向MS发送去激活请求消息Deactivate PDP Context Request（TI，Teardown Ind）

3）MS删除本地的PDP CONTEXT，向SGSN返回去激活接受消息Deactivate PDP Context Accept（TI，Teardown Ind）；

4)SGSN向 GGSN发送删除 PDP CONTEXT的响应消息Delete PDP Context Response(TEID)，GGSN收到此消息后，如果为MS分配了动态地址，可以释放此动态地址给其他的MS使用，SGSN发送删除PDP CONTEXT响应不必等待收到MS的去激活接受消息；

第五章 IMS体系架构

5.1 IMS体系架构的简介

5.1.1 什么是因特网协议(IP)多媒体子系统(IMS)

固定和移动网络在过去20年里经历了巨大的转变。在移动领域中，第一代 (1G)系统在20世纪80年代中期引入。这些网络为用户提供基本的业务，其重点是话音以及与话音相关的业务。20世纪90年代的第二代(2G)系统为用户带来了一些数据业务和更复杂的辅助业务。现在的第三代(3G)系统使得为用户提供更快的数据传输速率和丰富多彩的多媒体业务成为可能。在固定侧，传统的公共交换电话网(PSTN)和综合业务数字网(ISDN)已经主宰了传统的话音和视频通信。最近几年中，因特网的使用量呈爆炸态势，越来越多的用户使用更快、更便宜的因特网连接，例如非对称数字用户线(ADSL)。这些类型的因特网连接使得持续在线成为可能，这对开始使用实时通信方式的人们而言是非常必要的，如聊天应用、在线游戏、基于IP的话音(VoIP)等。

当前，我们正在经历着固定和移动网络的快速融合，随着移动设备渗透率的逐年递增，全球很快将拥有超过20亿的移动设备用户。这些移动设备拥有巨大、高清晰度的显示屏，有内嵌的相机以及很多用于各种应用的资源。它们是持续在线、持续连接的应用设备。这使得“应用”一词有了新的含义，应用不再是只通过用户界面交换信息的孤立实体。下一代更令人兴奋的应用是对等(peer-to-peer)实体，它使得共享更加容易：共享的浏览、共享的白板、共享的游戏体验、共享的双向无线会话(即基于蜂窝网络的按键通话)。连接状态的概念也被重新进行了定义。拨一个号码并交谈将很快被视为非常狭窄的网络子集。在支持因特网协议(IP)的新设备之间建立点到点连接的能力是这种网络所需的关键因素。这个新的通信范例已经远远超过了传统的老式电话业务(POTS)的能力。

为了实现交互通信，基于IP的应用必须有相应机制能与对端进行沟通。当前的电话网络通过建立点对点连接来完成这个必不可少的工作。通过拨打对方号码，这个网络可以在口网络上的任意两个终端之间建立自组织(ad hoc)连接。提供这种D通道的重要能力只存在于因特网中孤立和单个业务提供商的环境中，封闭系统在用户数量基础上进行竞争，其中网络占有的用户是竞争的关键所在，而业务提供商之间的互连功能并不受欢迎。我们需要一个全球性系统——IP多媒体子系统(IMS)，它允许支持IP设备上的应用能够很容易和安全地建立点对点以及点对内容的连接。

我们对IMS的定义是：IMS是一个全球性的、接入独立并且基于标准的IP通道和业务控制体系，它使得基于普通因特网协议的终端用户使用不同类型多媒体业务成为可能。

话音和数据业务的真正融合提高了生产力和整体效率，而整合话音、数据和多媒体的创新型应用的开发将形成新业务的更多需求，例如在线状态、多媒体聊天、按键通话以及移动会议。将移动性和IP网络合并的能力将是未来业务成功的关键所在。

图1—1给出了固定移动环境下的通信网络融合。IMS不仅在分组交换域引入了多媒体会话控制，同时它还在分组交换域实现了电路交换功能。IMS是这种网络融合的关键技术。

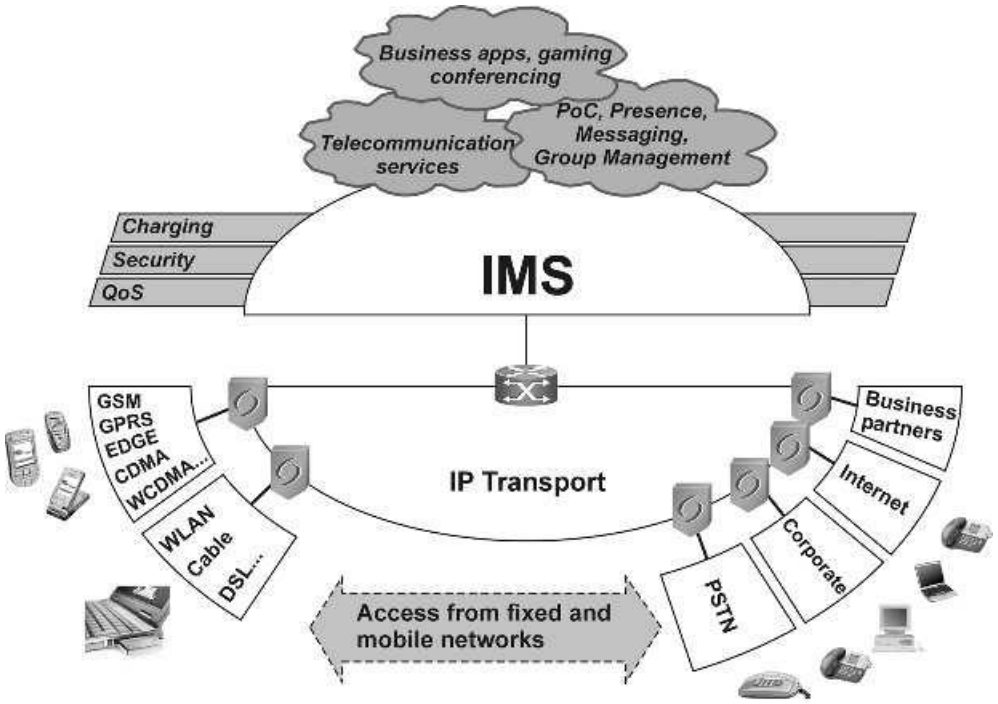


图5-1融合网络中的IMS

5.1.2 IMS业务举例

假设我有一个可以使用因特网协议多媒体子系统(IMS)的设备，打开它之后设备将使用身份验证模块(例如USIM卡)中的信息自动注册到IMS网络。在注册过程中，设备和网络都会被验证，并且设备将从网络获得我的用户身份。在这个惟一的注册之后，我就可以使用所有业务，包括按键通话、在线状态、话音和视频会话、消息和多用户游戏等。而且，在线状态服务器会把有关设备可用的信息更新为“在线”，并且列出当前使用的应用。

当我需要联系我的朋友鲍勃时，我可以从设备的电话本中选择鲍勃，并且基于他的在线状态信息，可以马上看到他是否在线。按下设备上的“绿色按键”(译者注：通话键)，我就可以发起一个“普通”的呼叫。IMS网络将负责在两个设备之间发现并且建立会话初始化协议(SIP)会话，即使呼叫时鲍勃在国外。当呼叫到达鲍勃的终端时，他可以知道这个呼叫来自于我，并且他还将看到我插入的一个文字信息“下周三有免费的电影票”。鲍勃接了电话，但是告诉我他不能确定到时候是否能赶回来。我们决定周日的时候再确认这个问题。在挂电话之前，鲍勃对我说：“你无法相信我今天看到了什么，等一下我展示给你。”鲍勃开始将一个视频流片断发送给我，并且在我观看这个视频的时候，鲍勃详细解释了当天早些时候在动物园发生的事情。

麦克发现今天是自己最好的朋友吉尔的生日。虽然他正在旅行并且无法与她约会，但是他想送给吉尔一条个性化的生日短信。当麦克坐在当地的咖啡馆里的时候，他一边享受咖啡一边使用其崭新的无线局域网(WLAN)设备阅读因特网上的最新新闻，他决定发送给她一个视频片断作为生日礼物。当吉尔听到她的电话振铃的时候，她正在洗澡。她看到手机提示接收到一条消息，于是检查了收件箱并保存了这个视频片断，同时她决定回复这条短信。她知道麦克很了解她所具有的独特的幽默感，于是将她自己正在洗澡的照片发了出去，如图5-2所

示。

图5-2多媒体消息

皮特·辛普森是伦敦人，并且是阿森纳队的铁杆球迷。他非常幸运地拿到了一张阿森纳队和托特纳姆热刺队德比战的球票，并且出发去观看比赛。当比赛过程中他坐在球场内，突然有压制不住的强烈欲望想让他的朋友们知道自己有这种机会。他拿起自己的移动电话并且给他的朋友，一个托特纳姆热刺队球迷，约翰·克拉克打了一个电话。约翰正坐在自己的座位上并接收到了电脑屏幕上弹出的来话提醒，通知他有来自皮特的呼叫。约翰接了电话并且两人开始交谈。皮特无法自制，于是打开了视频共享应用来聚焦比赛现场。约翰收到了视频请求，同意接收这个视频流。PC客户端启动并显示了比赛情况，约翰看到了阿森纳得分了。“美妙的进球，对吧?”皮特问到。“比赛还没有结束呢”，约翰说到，并且关了视频。他们开始在电话里对比赛和他们各自喜欢的球队进行争论。

上述所有通信都需要使用IMS提供的IP通道。IMS不仅提供了选择最好和最合适通信媒体的能力，而且提供了会话过程中自然地改变媒体类型以及在任何IP接入点使用首选(支持SIP的)通信设备的能力。

5.1.3 IMS从何而来

5.1.3.1 从GSM到3GPP版本7

欧洲电信标准化委员会(ETSI)是20世纪80年代末到90年代间制订全球移动通信系统(GSM)规范的标准化组织。ETSl还制订了通用分组无线服务(GPRS)网络体系。最后一个GSM专门规范制订于1998年；同年，欧洲、日本、韩国、美国和中国的标准化机构成立了3GPP来制订由宽带码分多址(WCDMA)和时分／码分多址(TD-

CDMA)无线接入与演进的GSM核心网所构成的第三代移动通信系统(http：／／www．39pp．or9／About／39ppagre．pdf)。其大部分工作和基础规范是从ETSl特别移动小组(SMG)继承而来。3GPP最初决定每年推出一版规范，第一个版本就是版本9913GPP R991。

5.1.3.2 3GPP版本99(3GPP R99)

版本1999的形成仅用了不到一年的时间。除少数基本规范的完成时间推迟到了2001年3月以外，该版本的主体功能于1999年12月冻结。如此快速的完成规范是因为实际工作是由两个组织：3GPP和ETSI SMG分工完成的。3GPP负责完成业务、系统结构、WCDMA和TD．CDMA无线接入和通用核心网。ETSI SMG开发了GSM／全球演进增强数据速率(EDGE)无线接入。

WCDMA无线接入是版本1999的3G系统相对于GSM的最大进步。除WCDMA以外，UTRAN(UMTS陆地无线接入网)还引入了Iu接口。与A接口和Gb接口相比，Iu接口有以下两个明显差别。首先，语音的编码转换在核心网进行。而在GSM网中这是BTS(基站控制器)的逻辑功能之一；其次，Iu接口中加密和小区级移动性管理在RNC进行，而在GSM网中，GPRS业务的这些功能是由GPRS服务支持节点(SGSN)完成的。

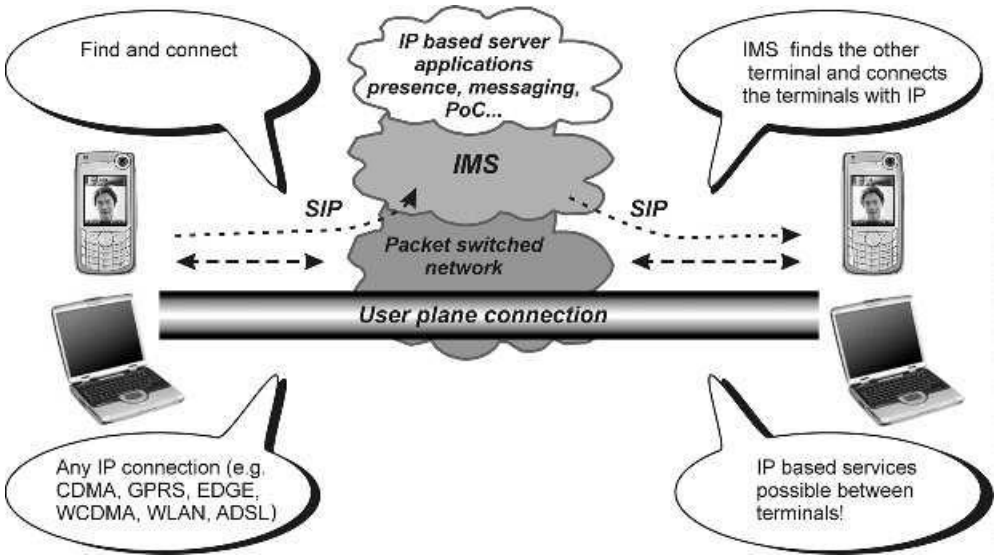


图5-3 IMS在分组交换网络中的作用

该版本在业务生成方面还引入了开放业务体系(OSA)。业务方面规范的目标是不再对新业务进行规范而是转向专注于业务能力，例如各种工具集(CAMEL、SIM应用工具集和OSA)。这一原则得到了良好的贯彻，虽然虚拟归属环境(VHE这一包容了所有业务生成的概念仍缺乏清晰的定义。

5.1.3.3 3GPP版本4

继版本1999之后，3GPP开始定义版本2000，包括所谓的全口网络即后来更名为IMS的部分。在2000年时，人们意识到IMS的开发不可能在2000年一年之内完成，因此版本2000被拆分为版本4和版本5两个阶段。

版本4可以独立于IMS而完成。3GPP版本4最主要的新功能包括移动交换中心(MSC)服务器和媒体网关(MGW)的概念、核心网协议的IP传输、UTRAN的位置业务(LCS)增强、多媒体消息以及Gb用户平面的IP传输。

3GPP版本4功能冻结并正式完成于2001年3月。而对无线接口所必需的用于协议改变的反向兼容性的直到2002年9月才得到增强。

5.1.3.4 3GPP版本5、版本6和版本7

版本5最终将IMS引入到3GPP标准中。IMS是一个独立于接入技术的基于IP的标准体系，它与现存的话音和数据网络都可以互通，不论是固定网络用户(例如PSTN、ISDN、因特网)还是移动用户(例如GSM、CDMA)。IMS的体系使得通过各种类型的客户端都可以建立起对等的

P通信，并可以获得所需要的服务质量。除会话管理之外，IMS体系还涉及完成业务提供所必需的功能(例如注册、安全、计费、承载控制、漫游)。总之，IMS形成了IP核心网的核心。

版本5应包含哪些内容经历了热烈讨论，该版本的功能最终于2002年3月冻结。这一决定的结果是很多特性被推迟到下一个版本，即版本6中，内容冻结后工作仍在继续，到2004年初基本稳定。版本6的IMS弥补版本5中IMS的缺点，并引入新的功能。版本6于2005年9月完成。表1．1列举了版本5和版本6最主要的功能，还给出了版本7的候选功能。

从表5-1中可以看到，3GPP已经为基于SIP的IP多媒体业务集合定义了有限架构体系。它包含了逻辑单元的功能、各单元如何连接的描述、连接所选择的协议和进程的描述。还应注意IMS针对移动通信环境进行了优化，包括基于移动标识的用户认证和授权，以及用户网络接口上用于允许无线丢失与恢复检测的SIP消息压缩、安全和策略控制机制的规则定义。除此之外，从运营商的角度而言，很多重要方面应在体系的进一步发展中得到解决，例如计费体系、策略和业务控制。本书将解释这些方面是如何定义的。

表5-1 IMS特性

版本5	版本6	版本7
体系:网络实体和参考点包含了计费功能	体系：互连(CS、其他口网络、WLAN)，一些新实体和参考点	体系：cs域、Ps域和连接到IMS的固定宽带之间话音呼叫的连续性
倍令：通用路由原则、注册、会话发起、会话变更、会话拆除、网络发起的会话释gUfl!册取消流程 ●UE和IMS网络之间的SIP压缩 ●用户信息存储(Hss)和会话控制实体(CSCF)之间的数据传输 ●用户信息存储(HSs)和应用服务器(AS)之间的数据传输	信令：组身份的路由、多级(MULTIPLE)注册	信令：紧急会话、使用SIP的SMS支持、CS呼叫与IMS会话的合并
安全：对用户和网络进行鉴权的IMS AKA、UE和Ⅱ“S网络之间的SIP消息完整性保护、网络域安全	安全：SIP消息的机密性保护、基于Ⅱ’地址的认证、通用认证体系	安全：宽带接入的适应性调整、TLS支持
服务质量：IMS和GPRS接入网之间的策略控制、先决条件和授权标志	服务质量:基于相同PDP上下文的独立会话媒体流的复用	服务质量:策略和计费控制协调、无标志的QoS授权
业务开通：采用应用服务器和IMS服务控制参考点	业务j在线状态、消息、会议、蜂窝上的按键通话、组管理、本地业务	业务：SIP中的辅助业务
基本：ISⅡ讧		多系统互操作:WLAN-UMTS移动性

5.2 I P多媒体子系统体系

本章向读者介绍因特网协议(IP)多媒体子系统(IMS)。5.1节介绍基本的体系概念，例如，解释为何要对承载进行区分，以及为何要选择归属控制模型等。6．2节是对IMS体系的总体介绍，包括各种不同网络实体和主要功能的介绍。6．3节更深入地阐述各实体如何连接以及相互之间使用何种协议；还包括与其他域的关系描述：IP网络、通用移动通信系统(UMTS)和电路交换核心网(CSCN)。

5.2.1体系上的要求

在IMS体系的创建过程和未来发展中，一系列基本要求起到了指导作用。本节涵盖了中最主要的要求。第三代合作项目(3GPP)的IMS要求参见文件[3GPPTS22．228]。

5.2.1.1 l P多媒体会话

现有的通信网络能够使用电路交换承载提供话音、视频和消息类型的业务，因此，当用户转换到分组交换域并且开始使用IMS的时候，终端用户的业务提。供自然就不应该拒绝这些业务类型。IMS通过提供丰富的通信方式开创了通信的÷新高度。IMS用户能够在单个通信会话期间以他们选择的任何方式将多种基于IP的业务进行混合和匹配。用户能够将语音、视频、文字、内容共享以及在线一状态整合作为他们通信的一部分，并且能够随心所欲地增加或者停止业务提供。例如，两个人可以开始一个语音会话，并且稍后在相同会话中增加游戏或者视频单元。

5.2.1.2 I P连接

正如IP多媒体子系统这个名字所指出的，一个基本要求就是设备必须由IP连接来接入这个系统。点对点应用需要端到端的可到达性，并且这个连接应该非常容易地支持口版本6(IPv6)，因为IPv6不会存在地址短缺的现象。因此，3GPP协商了相关事宜来使得IMS完全支持IPv6[3GPP TS23．221]。不过，早期的IMS实现和配置可能会使用IP版本4(IPv4)。3GPP已经建立了IMS中如何处理IP版本间互连的相关规范[3GPP TS23．981]，从而可以与早期的IMS配置兼容。在3．17节将对此进行进一步介绍。

IP连接可以通过归属网络或拜访网络来获得。图5-4左边的部分表示用户设备(UE)通过拜访网络获得口地址的一种选项。通用移动通信系统(UMTS)网络中，这意味着用户漫游到拜访网络时所使用的无线接入网(黜～N)、GPRS服务支持节点(SGSN)和GPRS网关支持节点(GGSN)都位于拜访网络。图5-4右边部分表示UE从归属网络获得口地址的情况。在UMTS网络中这意味着用户漫游到拜访网络时，RAN和SGSN位于拜访网络。显然，当用户位于归属网络时，所有必需的网元都位于归属网络，IP连接也应该在这个网络中获得。

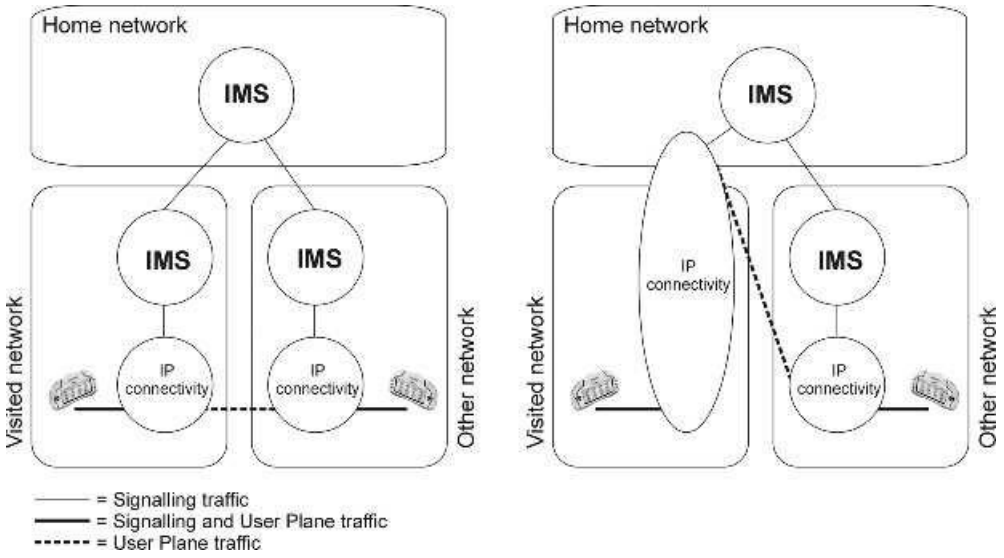


图 5-4 用户漫游时的 IP 连接选项

特别需要注意的是，用户要能够漫游并且能够像图中所示那样从归属网络获得P连接。这使得用户即使漫游到一个没有IMS但是可以提供IP连接的网络中，也可以使用新鲜有趣的IMS业务。从理论上讲，可以在某一个地区或国家建设IMS网络，并通过诸如通用分组无线服务(GPRS)漫游将用户连接到该归属网络。实际上这种方式由于路由效率不够高而无法实用。可以设想将实时传输协议(R11P)话音分组从美国传送到欧洲再返回美国将会是什么后果。但是，当运营商建设IMS网络时，或者在IMS的初期阶段，仅仅提供非实时或准实时多媒体业务时，这种部署方式还是很重要的。

5.2.1.3 IP多媒体服务的服务质量保证

在公众因特网中，时延一般比较高，并且波动也不确定，分组的到达顺序会颠倒，并且有些分组会丢失或被丢弃。在IMS中将不再是这样。底层接入和传输网络与IMS一起提供了端到端服务质量(QoS)。通过IMS，终端通过会话初始化协议(SIP)的会话建立或者会话变更过程来协商它的能力并提出其QoS需求。终端可以协商以下参数：

- ✓ 媒体类型、业务流方向；
- ✓ 媒体类型的比特率、分组大小、分组传输频率；
- ✓ 各媒体类型的RTP净荷的用法；
- ✓ 带宽的自适应。

在应用层协商了这些参数之后，终端在接入网中预留适当的资源。当端到端QoS建立起来之后，终端用适当的协议(例如R1限)将各个媒体类型进行编码和分组，并通过口上的某种传输层协议(例如TCP或IJ1)P)将这些媒体分组传递到接入网和传输网。运营商之间应该协商达成应用级协定，从而在彼此互连的骨干网上保证所需的QoS。在UMTS中，运营商间可使用GPRS漫游交换骨干网。

5.2.1.4 为确保正确使用媒体资源的IP策略控制

IP策略控制是指基于IMS会话中的信令参数，对IMS媒体预计的承载业务的使用进行授权和控制的能力。这要求IP连接接入网与IMS之间的交互。建立交互的方式可以分为三类[3GPP TS22．228，23．207，23．228]：

- ✓ 策略控制单元能够确保按照SIP信令中的参数为媒体流激活承载。这可以使运营商确保其承载资源没有被误用(例如，源IP地址和目的IP地址以及承载级的带宽确实与SIP会话建立时要求的一模一样)；
- ✓ 策略控制单元能够严格遵守SIP会话两端间媒体流的启动和终止时间。这可以防止在会话建立起来之前就使用承载资源；并且使业务流的启动和终止与IMS会话计费的启动和停止相同步。
- ✓ IP连接接入网络中的业务将与会话相关的用户承载进行变更、挂起或释放时，策略控制单元可以得到通知。这使得在例如用户离开覆盖区这类情况发生时，IMS可以将正在进行的会话释放掉。

基于业务的局部策略(SBLP)在1MS中用作IP策略控制的同义词，并且它将在3．9节中进一步说明。

5.2.1.5 通信的安全性

安全性是每个电信系统的基本要求，[MS也不例外。除了接入网络过程(例如，GPRS网络)之外，IMS在UE和IMS网络之间有它自己的鉴权和授权机制。而且，不管向下延伸的核心网(例如，RAN和GPRS)如何，在UE和IMS网络之间以及IMS网络实体之间提供了SIP消息的完整性和可选的保密性。因此，IMS至少提供了与相应的GPRS和电路交换网络相似级别的安全。例如，IMS要确保用户开始使用业务之前都已经进行了鉴权，并且会话中的用户也能够请求隐私保护。3．6节将深入讨论安全特征的细节。图5-5中给出了得到应用的IMS安全解决方案概述。

图 5-5 IMS 安全概述

5.2.1.6 计费的安排

从运营商和业务提供商的角度而言，对用户的计费能力是任何一个网络都必须具备的。IMS体系允许使用不同的计费模型，这也就是说，包括根据传输层所使用的资源，只对主叫方单向计费或者对主被叫双方都计费的能力。在后一种计费方式中，主叫方可以完全基于IMS级会话进行计费，换言之，在传输层和IMS层可以采用不同的计费机制。实际上，运营商可能对在传输和IMS(业务和内容)计费层生成的计费信息进行关联更有兴趣。如果某个运营商使用策略控制参考点，那么就可以具备这个能力。

由于IMS会话可能包含多种媒体元素(例如音频和视频)，这就需要IMS提供一种对每个媒

体元素进行计费的方式。如果被叫方在会话中增加了一个新的媒体元素，这就使得对被叫方计费成为可能，同时也就需要不同的IMS网络能够交换用于当前会话计费的信息[3GPP TS 22．101，TR 23．815]。

IMS体系对在线和离线两种计费能力都支持。在线计费是这样一种计费过程：计费信息可以实时地影响服务的提供，因此直接与会话和服务的控制相配合。实际上，运营商可以在允许用户进行会话之前检查用户账户，也可以在账户内金额全部用完时终止会话。预付费服务就是需要这种在线计费能力的应用。离线计费是计费信息不实时影响服务提供的一种计费过程。这是传统的计费模型，一段时间内的计费信息被收集起来，运营商在这段时间结束时将账单寄给顾客。

图5-6给出了IMS环境中通用计费体系的简单说明。关键性的事实就是：IMS为IP业务增加了从比以前更细小的粒度上进行计费的可能性。

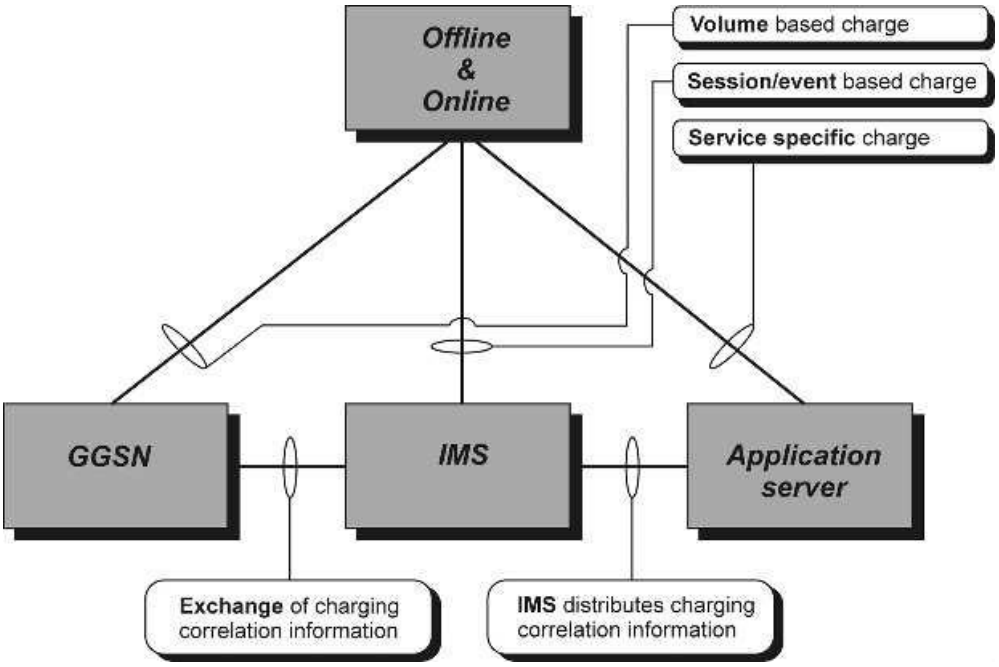


图 5-6 IMS 计费概述

5.2.1.7 对漫游的支持

从用户角度而言，非常重要的一点是，无论他身处何处都要能够访问到所需服务。漫游特征使得用户即使不在归属网络的服务区域内也能正常使用服务。6.1.2节已经描述了两个漫游的例子，分别称为GPRS漫游和IMS漫游。除此之外，还有IMS电路交换(CS)漫游。GPRS漫游是指拜访网络提供SGSN和RAN，而归属网络提供GGSN和IMS的情况下接入IMS的能力。IMS漫游模型是指一种网络配置，此时拜访网络提供IP连接(例如RAN、SGSN、GGSN)和IMS接入点(即P．CSCF)，而归属网络提供IMS功能的剩余部分。和GPRS漫游模型相比，这种漫游模型的主要好处在于它对用户平面的资源进行了最优化的利用。在IMS和CS CN域之间的漫游是指IMS和CS之间的域间漫游。当用户在某个域内没有注册或者无法找到时，会话就可以被转发到另一个域。需要注意的是，CSCN域和IMS域都有自己的服务，这些服务无法被另外一个域所使用；而有些服务则非常相似，并且在两个域内都可以使用(例如IMS中的VoIP和CSCN中的

语音电话)。图5-7给出了IMS / CS漫游的各种情况。

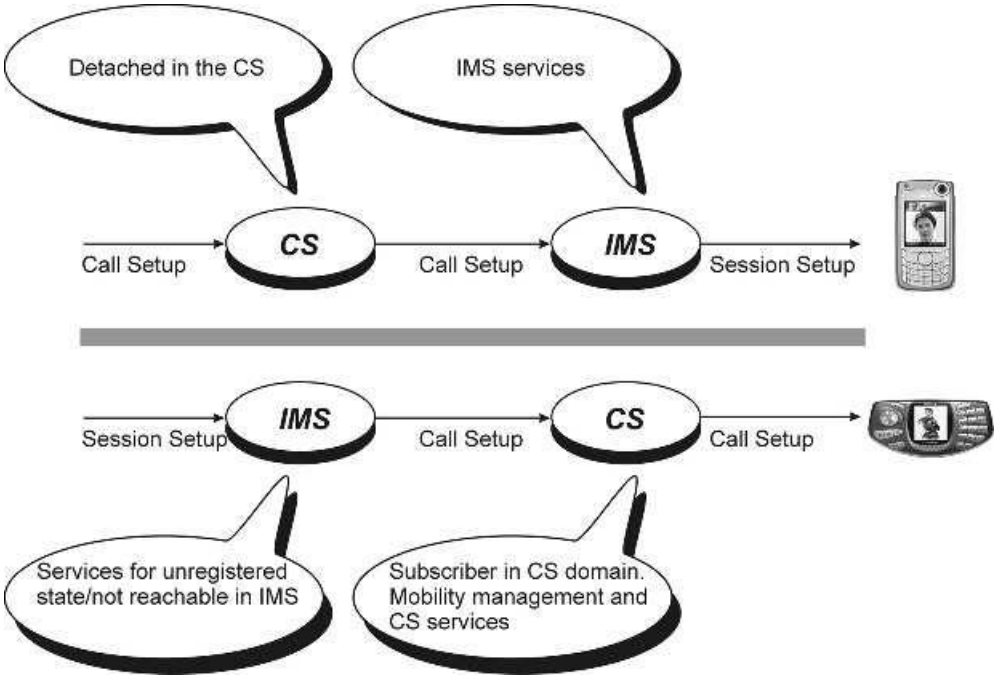


图 5-7 IMS / CS 漫游的各种情况

5.2.1.8 与其他网络的配合

显然，IMS不可能在世界上同时铺设，而且人们也不可能很快地更换他们的终端和签约信息。这就提出了一个问题，即无论人们拥有什么样的终端，也无论他们居住在什么地方，用户信息都是可达的。作为一个新的、成功的通信网络技术和结构，IMS必须连接尽可能多的用户。因此，IMS支持与PSTN、ISDN、移动网和因特网用户间的通信。另外，也可以支持与非3GPP组织开发的因特网应用之间进行会话[3GPP TS 22. 228]。

5.2.1.9 服务控制模型

在2G移动网络中使用了拜访服务控制。这意味着，当一个用户漫游时，拜访网络中的一个实体为用户提供服务并控制业务流。在2G移动网络中，这个实体称作拜访移动服务交换中心。在版本5的早期，对拜访和归属服务控制模型都支持。同时支持两个模型会导致每个问题都有不止一个解决方案，而且由于简单的方案可能无法同时适合两个模型，因而减少了最优体系方案的个数。同时支持两个模型还意味着需要对因特网工程任务组(IETF)协议进行附加扩展，并且会增加注册与会话流程中的工作量。因此，拜访服务控制被放弃。因为与归属服务控制相比，它过于复杂而且不提供任何重要的附加价值，相反还造成了一些限制；它需要运营商之间存在一种多重关系和漫游模型，服务速度会变慢，因为需要拜访网络和归属网络支持相似的服务，否贝IJ漫游用户将会感到服务变差；另外，运营商内部参考点的数目也将增加，这就需要复杂的解决方案(例如在安全和计费方面)。因此，IMS仅采用了归属服务控制，换言之，访问用户数据库并且与服务平台直接交互的实体将总是位于用户的归属网络。

5.2.1.10 服务开发

拥有可扩展的服务平台与快速启动新服务的可能性是非常重要的，这就意味着过去对于全套的电信服务、应用和附加服务进行标准化的旧方法不再合适。因此，3GPP正在进行服务能力的标准化，而不是服务本身的标准化[3GPP TS22. 101]。IMS体系实际上应当包含一个服务框架，该框架提供必要的能力，以便在IMS中支持语音、视频、多媒体、消息、文件共享、数据传输、游戏和基本附加服务。

5.2.1.11 分层设计

3GPP已经决定使用分层的方法来进行体系设计，这意味着传输和承载服务被从IMS信令网和会话管理服务中分离出去，更高层的服务都运行在IMS信令网之上。图5-8描述了这种设计。

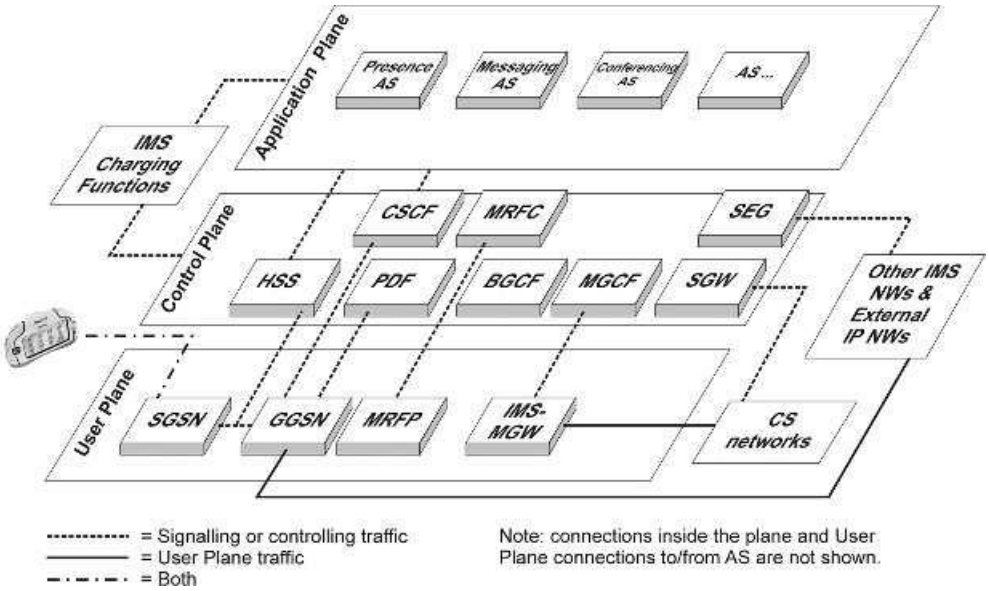


图 5-8 IMS 和分层体系

（注：平面内连接以及用户平面与 AS 的连接没有给出。）

在一些情况下，分辨上层和下层之间的功能是不可能的。分层的方法是为了最小化分层之间的依赖性。这样做的好处是，以后新的接入网加入到 IMS 系统将变得非常容易，在版本 6 中已经增加了无线本地网（WLAN）接入 IMS，而在版本本 7 中固定宽带接入 IMS 也将被标准化。

分层的方法提高了应用层的重要性，因为业务被设计为与具体接入网相独立，网络配备IMS作为业务和接入网两者之间的桥梁。无论用户使用移动电话还是PC客户端进行通信，IMS中都将使用相同的在线状态信息和成组列表功能。不同的业务有不同的需求，这些需求包括：

- ✓ 带宽；
- ✓ 延时；
- ✓ 设备的处理功耗。

这意味着为了让不同的业务能够正确执行，网络必须为多媒体业务配备接入感知(access. aware)控制和业务逻辑。IMS体系结构中嵌入多种接入功能体，以便为固定和移动运营商提供固定网络和移动网络融合解决方案。这也将使得业务提供商能够使用并且动态适

应选定的现有设备的特点和能力及其网络接入方法。

5.2.1.12 接入无关性

IMS最初的设计思想是与具体的接入方式无关，以便IMS业务可以通过任何IP连接网络(例如，GPRS、WLAN、宽带xDSL)提供。遗憾的是，版本5的IMS规范中包含了一些GPRS特有的特性。在版本6中，与接入方式相关(例如GPRS)的问题将从核心的IMS描述中分离出来，并且IMS体系结构将回归到它最初的设计状态(也就是接入独立性)。图5-9说明了IMS可以运行的各种不同类型的接入独立的网络。这些网络包括了固定宽带网络、WLAN、GPRS以及UMTS。本书中将以GPRS为例。

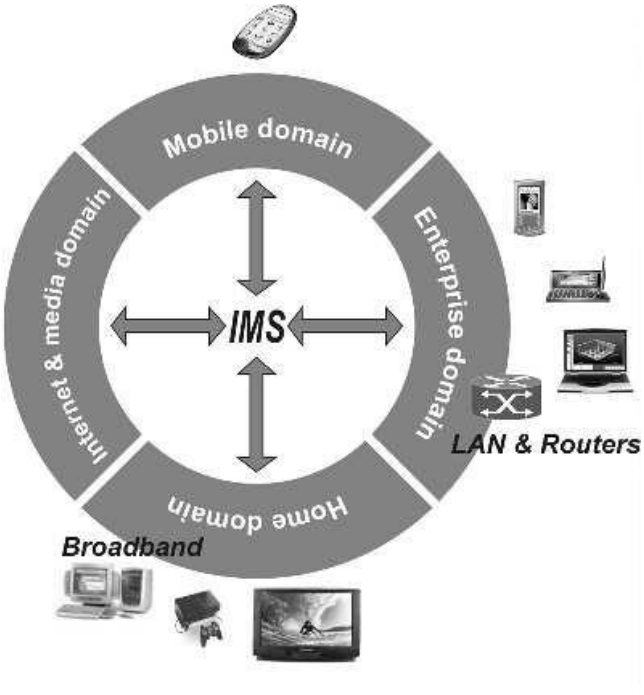


图 5-9 IMS 接入独立性

5.2.2 IMS相关实体和功能的描述

本节讨论 IMS 实体和关键功能。这些实体大体上可以被分为六种主要类别：

- ✓ 会话管理和路由类(CSCF)；
- ✓ 数据库(HSS，SLF)；
- ✓ 服务(应用服务器，MRFC，MRFP)；
- ✓ 网络互连互通功能(BGCF，MGCF，IMS. MGW，SGW)；
- ✓ 支拷}功能(PDF，SEG，THIG)；
- ✓ 计费。

需要理解的重要一点是，建立IMS规范时，并不详细制定网络实体的内部致能规范。相反地，规范定义了实体之间的参考点和参考点支持的功能。例如，CSCt如何从数据库获得用户数据。6.2.3节介绍了各种不同的参考点。另外，本节最后介绍了通用分组无线服务(GPRS)功能。

5.2.2.1 呼叫会话控制功能(CSCF)

呼叫会话控制功能(CSCF，Call Session Control Function)有三种不同类型：代理．CSCF(P-CSCF)、服务．CSCF(S-CSCF)和问询．CSCF(I-CSCF)。每个CSCF都有自己特定的任务，并且这些任务将在随后的章节中进行说明。所有CSCF的共同点就是它们在注册和会话建立过程期间起作用，并且形成SIP路由系统。而且，所有功能都能够发送计费数据给离线计费功能。P．CSCF和S-CSCF能够执行一些共同的功能。这两个实体都能够代表用户释放会话(例如，当S-CSCF监测到会话挂起或者P-CSCF接收到一个媒体承载丢失的通告时)，并且能够检查会话描述协议(SDP)有效负荷的内容以及检查它是否包含不允许提供给用户的媒体类型和编码类型。当被提议的SDP不符合运营商的策略时，这两个CSCF会拒绝该请求并且发送SIP错误消息给UE。

1．代理．CSCF(P-CSCF)

代理呼叫会话控制功能(P-CSCF)是IMS系统中用户接触到的第一个实体。它意味着所有来自用户的SIP信令业务都必须发送给P．CSCF。相似地，所有来自网络的终结SIP信令业务都必须从P-CSCF发送给LIE。有四种独一无二的任务分配给P-CSCF：SIP压缩、IPSec安全关联、与策略决策功能(PDF)交互以及紧急会话检测。

因为SIP协议是基于文字的信令协议，它包含了包括扩展信息和与安全相关的信息在内的大量信元头和头参数，这就意味着整个消息的大小远大于二进制编码的协议。为了加速会话建立过程，3GPP已经强制要求支持UE和P-CSCF之间的SIP压缩。如果UE指示它希望接收到压缩后的信令消息的时候，P-CSCF就需要压缩消息。

P-CSCF负责维持安全关联以及为SIP信令应用完整性和机密性保护。这是在SIP注册期间伴随着UE和P-CSCF协商IPSec SA而完成的。在初始的注册之后，P-CSCF能够应用SIP信令的完整性和机密性保护。

当运营商希望应用SBLP的时候，P-CSCF还被赋予了将会话和媒体相关信息中继转发给PDF的任务。基于接收到的信息，PDF能够得到授权的IP QoS信息，这些信息当GGSN在接受辅助PDP上下文激活之前需要执行基于业务的局部策略(SBLP)的时候会传送给GGSN，这个概念在3．10节进行了阐述。而且，IMS能够通过PDF传递IMS计费相关信息给GPRS网络；类似地，IMS还可以通过PDF接收来自GPRS网络的GPRS计费相关信息。这使得来自IMS和GPRS网络的计费数据记录融合到计费系统中成为可能。

IMS紧急会话还没有完全定义清楚(版本7中还将继续相关工作)，因此IMS网络监测紧急会话尝试并且引导UMTS UE使用CS网络用于紧急会话是非常重要的功能。这种监测是P-CSCF的任务之一。这个功能在支持IMS紧急会话的时候也不会消失，在特定的漫游情况下，可能出现UE本身无法意识到用户已经拨打了一个紧急号码的现象。版本7中规划了P-CSCF能够选择紧急CSCF来处理紧急会话的功能。这样的选择是必须的，因为在IMS漫游情况下，分配的S-CSCF是在归属网络中，而归属S-CSCF无法传送请求给正确的紧急呼叫中心。

2．问询．CSCF

问询CSCF(1．CSCF)是一个运营商网络内部的接触点，所有与这个网络运营商的用户连接都要经过这个实体。分配给I-CSCF有四个独特的任务如下：

- 从归属用户服务器(HSS)获取下一跳的名字(S-CSCF 或者应用服务器)；
- 基于来自 HSS 的接收能力集分配 S-CSCF。当用户注册到网络的时候，或者当用户没有注册到网络但是拥有与非注册状态相关的业务(例如话音邮件)时接收到 SIP 请求的时候，就会分配一个 S-CSCF。
- 发送进入的请求给已经分配的 S-CSCF 或者应用服务器(假设公共业务身份参见 11．11 节)；
- 提供拓扑隐藏网间网关(THIG，Topology Hiding Inter-network Gateway)功能。

3. 服务．CSCF

服务CSCF(S-CSCF)是IMS的核心所在，它负责处理注册过程，进行路由判断，维持会话状态并且存储业务配置。当用户发送一个注册请求的时候，它就会被传送给S．CSCF，S-CSCF将从HSS下载鉴权数据。基于鉴权数据，它会生成一个回应给UE。在接收到响应并确认之后，这个S-CSCF接受这个注册并且开始监督注册状态。在此过程之后，用户就能够发起和接收IMS业务。而且，S-CSCF从HSS下载业务配置作为注册过程的一部分。

业务配置是特定用户信息的集合，它永久性地存储在HSS中。当特定的公共用户身份(例如，joe．doe@ims．example．com)在IMS中进行注册的时候，S-CSCF下载与这个特定公共用户身份相关的业务配置。当用户发送SIP·请求或者接收到来自其他人的请求时，S-CSCF使用包含在业务配置中的信息来决定什么时候联系，以及特别是联系哪个(些)应用服务器。而且，业务配置可能包含有关S-CSCF需要应用的媒体策略类型的进一步说明——例如，它可能指出用户只允许使用音频和应用媒体分量而不允许使用视频媒体分量。

在它接收到所有UE发起或者UE终结的会话和活动的时候，S-CSCF负责关键的路由决策。当S-CSCF接收到通过P-CSCF的UE发起请求的时候，它需要在进一步发送请求之前决定是否联系应用服务器。在可能的应用服务器交互之后，S-CSCF或者继续IMS中的会话或者转换到其他域(CS或者其他IP网络)。而且，如果UE使用移动台ISDN(MSISDN)号寻址找到了被叫方，那么S．CSCF在进一步发送请求之前将MSISDN号(也就是电话URL)转换为SIP通用资源标识符(URJ)格式，此时IMS不会基于MSISDN号传送请求。同样地，S-CSCF接收所有终结于UE的请求。虽然S-CSCF从注册信息中确认了UE的IP地址，但是它通过P-CSCF传送所有请求，此时P-CSCF负责SIP压缩和安全功能。在发送请求给P-CSCF之前，S-CSCF可能传送请求给应用服务器，例如，检查可能的重定向指令。图5-10给出了S-CSCF在路由决策中的角色。

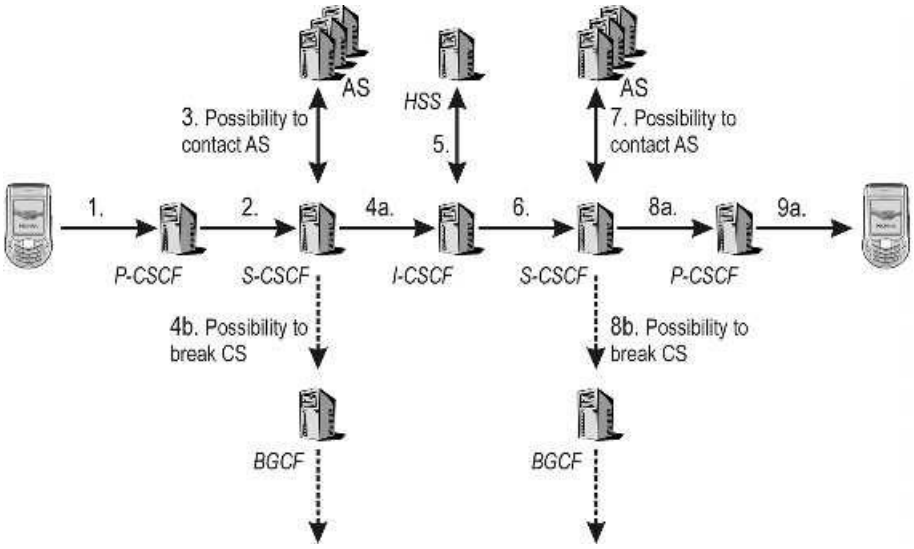


图5-10 S-CSCF路由和基本IMS会话建立

另外，S-CSCF能够发送账号相关信息给在线计费系统(OCS，Online ChargingSystem)进行在线计费(即支持预付费用户)。

5.2.2.2数据库

IMS体系结构中有两个主要的数据库：归属用户服务器(HSS)和订购关系定位功能(SLF)。

HSS是用于所有用户和IMS业务相关数据的主要数据存储单元。存储在HSS中的主要数据包括用户身份、注册信息、接入参数以及业务触发信息[3GPPTS23．002]。用户身份包括两种类型：专用用户身份和公共用户身份。专用用户身份是归属网络运营商分配的用户身份，它用于诸如注册和授权的目的;而公共用户身份是其他用户用于与这个终端用户进行通信请求的用户身份。IMS接入参数用于建立会话，它包括了像用户鉴权、漫游授权和已分配的S-CSCF名字之类的参数。业务触发信息使得SIP业务执行成为可能。HSS还提供了用户对S-CSCF能力方面特定的需求。这个信息被I-CSCF用来为用户选择最适合的S．CSCF。除了与IMS功能体相关的功能之外，HSS还包含了PS域和CS域所需要的归属位置寄存器和鉴权中心(HL刚AUC)功能的子集。HSS的结构如图5-11所示。HSS不同功能之间的通信并没有标准化。

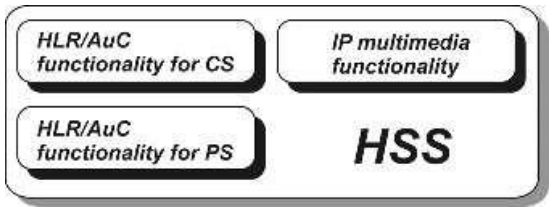


图 5-11 HSS 结构

HLR功能用于提供支持给PS域实体，例如GGSN和SGSN。这就使用户能够接入PS域业务。类似地，HLR也用于提供支持给CS域实体，例如MSC／MSC服务器。这就使用户能够接入CS域业务并且支持向GSM/UMTS的CS域网络的漫游。AUC为每个移动用户存储密钥，密钥用来为每个用户生成动态的安全数据。这些数据可以用于国际移动用户身份(蹦SI)和网络的相互鉴权。安全数据也用于提供LIE与网络之间无线链路上进行通信的完整性保护和加密。在归属网中可能有不止一个HSS，这依赖于移动用户的数目、设备容量和网络的架构。在HSS与其他

网络实体之间有多个参考点。

订购关系定位功能(SLF)作为一种地址解析机制，当网络运营商部署了多个独立可寻址的HSS的时候，这种机制使I-CSCF、S-CSCF和AS能够找到用于给定用户身份的订购关系数据的HSS地址。

5.2.2.3 业务功能

本书中的三项功能归类到IMS业务相关的功能——也就是多媒体资源功能控制器(MRFC)，多媒体资源功能处理器(MRFP)和应用服务器(AS)。

根据前面提到的分层设计思想，应用服务器(AS)并不是纯粹的IMS实体；实际上，它们是IMS之上的功能。不过，我们在这里把AS描述成IMS功能的一部分，因为在IMS中AS是提供增值多媒体业务的实体。AS驻留在用户的归属网络或者在第三方的位置。这里的第三方指网络或者独立的AS。AS主要功能有：

- ✓ 处理和影响从IMS接收到的SIP来话的能力；
- ✓ 发起S口请求的能力；
- ✓ 发送账目信息给CCF和OCS的能力。

提供的业务并不局限于基于SIP的业务，因为运营商能够为其IMS用户基于移动网络增强逻辑的定制应用(CAMEL)业务环境(CSE)和开发业务结构(OSA)提供业务接入[3GPP TS 23.228]。因此，“AS”是一个术语，一般用来捕捉SIP AS、OSA业务性能服务器(SCS)和CAMEL IP多媒体业务交换功能(IM-SSF)的行为。

通过使用OSA，运营商能够利用诸如呼叫控制、用户交互、用户状态、数据通话控制、终端性能、账户管理、计费和策略关联等业务能力特征进行业务的开发[3GPP TS 29. 198]。OSA结构的附加好处就是，它可以用作以安全的方式提供第三方AS给IMS的标准化机制，因为OSA自身就包含了初始接入、鉴权、授权、注册和发现等特征(S. CSCF不能为第三方直接安全地接入到IMS提供鉴权和安全功能)。由于对OSA业务的支持是基于运营商的选择，而不是从结构上就要求在多个实体内支持OSA协议和特征，因此OSA SCS用来终止来自S. CSCF的SIP信令。OSA SCS使用OSA应用程序接口(API)与实际的OSA应用服务器进行通信。

在IMS结构中已经介绍了IM. SSF动能，它支持CAMEL业务环境(CSE)中开发的继承业务。它拥有CAMEL网络特征(触发检测点，CAMEL业务交换有限状态机等等)并且与CAMEL应用部分(CAP)相互配合。

SIP AS是基于SIP的服务器，拥有广泛的增值多媒体业务。SIP AS可以被用于提供在线状态业务、消息、按键通话和会议业务。

图5-12说明了不同功能是如何连接的。从S-CSCF SIP AS的角度看，OSA业务性能服务器和IM. SSF展示了相同的参考点行为。

一个AS可能专用于一个单一业务，而用户可能有多于一个的业务，因此每个用户可能有一个或者多个AS。另外，在一个通话中也可能需要一个或者多个

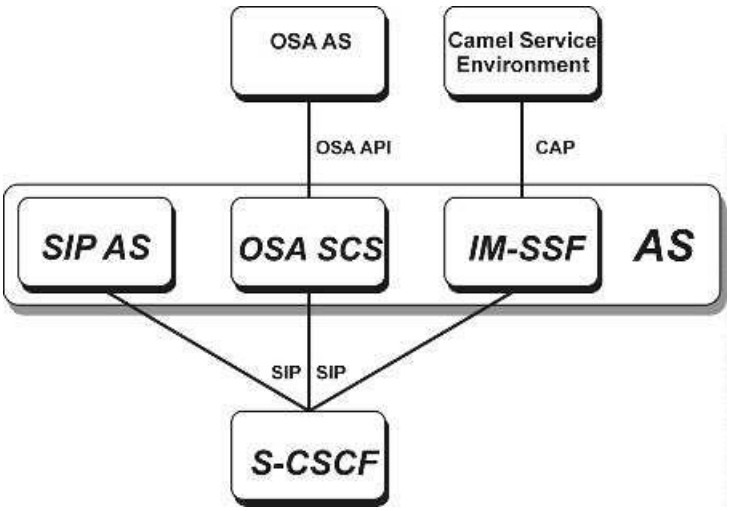


图 5-12 不同 AS 类型之间的关系

AS参与。例如，运营商可能用一个AS根据用户的选择(例如，在下午5点到早上7点之间将所有输入的多媒体通话都定向于应答机)对终止给用户的业务进行控制，使用另外一个AS根据UE的性能(屏幕尺寸、色彩种类等)对及时消息的内容进行自适应调整。

在IMS体系结构中，MRFC和MRFP都可以为与承载相关的业务，例如会议和公告，给用户或承载提供相应的机制进行代码转换。MRFC的任务是处理来自和去往S-CSCF的SIP通信，并且控制多媒体资源功能处理器(MRFP)。随后,MRFP提供MRFC请求和指示的用户平面资源。MRFP完成下列功能：

- ✓ 输入媒体流的混合(例如，为多方通话进行的混合)；
- ✓ 媒体流信源(如多媒体公告信源)；
- ✓ 媒体流处理(例如，音频代码转换，媒体分析)[3GPP TS 23．228，TS23．002]

目前，IMS体系结构中MRFC和MRFP的角色相对次要一些，因为在IMS会议工作[3GPP TS 24．1471中MRFC与AS在同一个位置，而MRFC和MRFP之间的参考点还没有进行很好定义。

5.2.2.4 互连互通功能

本节介绍了四种互连互通功能，这些功能是IMS和CS CN之间信令和媒体交换所必需的。

上一节说明了S-CSCF决定什么时候转换到CS CN。为了进行转换，S-CSCF发送SIP会话请求给出口网关控制功能(BGCF)；它进一步选择CS域出口的位置。所选择的出口既可以与BGCF处于相同网络，也可以位于另外一个网络。如果这个出口位于相同的网络，那么BGCF选择媒体网关控制功能(MGCF)进行进一步的通话处理。如果出口位于另外一个网络，那么BGCF将会话转发到相应网络的BGCF[3GPP TS 23．228]。后一种情况允许接近被叫用户的基于IP的信令和媒体的传输。

当SIP会话请求到达MGCF的时候，它在ISDN用户部分(ISU_P)或者承载独立呼叫控制(BICC)与SIP协议之间进行协议的转换，并且通过信令网关(SGW)发送转换请求给CS CN。SGW在基于m的信令传输(即SCTP／IP和SS7 MTP信令传输之间)和基于七号信令系统(SS7)信令传输之间的传输层进行信令转换(双向)。SGW不对应用层(例如，BICC，ISUP)的消息进行解释

说明，如图5-13所示。MGCF还控制了IMS媒体网关(IMS．MGW)。IMS．MGW提供了CS CN网络和IMS之间的用户平面链路。它终止来自CS网络的承载信道和来自骨干网(例如，IP网络中的RTP流或者ATM骨干网中的AAL2／ATM连接)的媒体流，执行这些终端之间的转换并且在需要时为用户平面进行代码转换和信号处理。另外，IMS．MGW能够提供音调和公告给CS用户。IMS．MGW是受MGCF控制的。

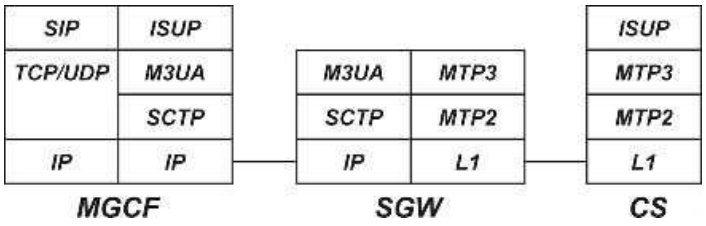


图 5-13 SGW 中的信令转换

类似地，所有从CS用户到IMS用户的来话控制信令都指定到MGCF，它执行必要的协议转换并发送SIP会话请求给I-CSCF用来中止会话。同时，MGCF与IMS．MGW交互，并且在用户平面预留必要的IMS．MGW资源。

5.2.2.5 支撑功能

策略决策功能(PDF)负责根据从P-CSCF获得的会话和媒体相关的信息制定策略。对于SBLP控制而言，它就相当于一个策略决策点。

IMS中的会话建立使用SIP和SDP，它包括了端到端消息交换。在消息交换期间，UE协商媒体特征集(例如，公共编解码器)。如果运营商应用SBLP，那么P-CSCF将转发会话发起者的指示以及相关SDP信息给PDF。随后，PDF分配并返回一个授权标记，这个标记将由P-CSCF传递给UE。PDF通过将SDP参数映射为授权的IP QoS参数，实现对选定媒体类型的IP流进行标记和授权，以便通过GO接口向接入网进行传输——在UMTS／GPRS接入情况下也就是GGSN。在接收到PDP上下文激活或者修改请求时，GGSN就会要求从PDF获取授权信息。PDF比较接收到的绑定信息和存储的授权信息，并且返回授权决定。如果绑定信息是正确的，那么PDF会在这个授权决定中将媒体授权的详细内容发送给GGSN。

除了承载授权决定之外，PDF还接收有关SBLP支配的PDP上下文释放时间或者UE丢失，恢复其无线承载时间的信息，以及有关SBLP支配的PDP何时使用流媒体或者会话业务类型的信息。基于这些信息，PDF能够通知P-CSCF有关发生的事件。这使得P-CSCF能够影响计费，甚至它可能代表用户开始释放IMS会话。而且，PDF能够请求GGSN对特定SBLP支配的PDP上下文进行去激活。

安全网关(SEG)拥有保护安全域之间控制平面业务的功能。安全域指的是由专一管理机构管理的网络。一般来说，它的边界就是运营商的边界。SEG放在安全域的边界，并且它针对目标安全域的其他SEG执行本安全域的安全策略。在IMS中所有的IMS业务都要经过SEG，特别是当业务是不同域间也就意味着业务是由它接收到的不同的安全域发起的时候。当保护域间IMS业务安全的时候，保密性、数据完整性以及鉴权都是必须有的[3GPP TS 33．203]。

THIG功能可以用来对运营商网络之外隐藏配置、容量和网络拓扑。如果运营商希望使用

隐藏功能，那么运营商必须在接收来自其他IMS网络的请求或者响应的时候将THIG功能放置在路由路径上。类似地，在发送请求或者响应给其他IMS网络的时候，THIG也必须放置在路由路径上。THIG执行所有信元头的加密和解密工作，这些信元头揭示了有关运营商IMs网络拓扑信息。

5.2.2.6计费实体

5.2.2.7 GPRS实体

1、 GPRS 业务支持节点

GPRS业务支持节点(sGsN)连接RAN和分组核心网。它负责为PS域进行控制和业务处理功能。控制部分包括两大主要功能：移动性管理和通话管理。移动性管理处理UE的位置和状态并且对用户和UE进行鉴权。控制部分韵通话管理处理连接接纳控制和现有数据连接中的任何变化，它也负责监督管理3G网络业务和资源，而且它还负责业务处理的执行。SGSN是作为用户数据通道的网关，换言之，它是UE和GGSN之间用户业务的中继。作为这个功能的一部分，SGSN也需要保证这些连接接收到适当的QoS。另外，SGSN还生成计费信息。

2、GPRS网关支持节点

GPRS网关支持节点(GGSN)提供与外部分组数据网之间的互连。GGSN的主要功能就是提供UE与外部数据网之间的连接，而外部数据网提供基于IP的应用和业务。例如，外部数据网可以是IMS或者因特网。换句话说，GGSN将包含SIP信令的IP包从UE传送到P. CSCF，反之亦然。另外，GGSN负责将IMS媒体口包转发给目标网络(例如，向通话终点网络的GGSN)。而提供的网络互连业务是作为接入点实现的，接入点是与用户希望连接的不同网络相关的。在大多数情况下，IMS有它自己的接入点。当UE激活和接入点(IMS)承载(PDP上下文)时，GGSN分配一个动态IP地址给UE。这个分配的IP地址用于IMS注册和在LIE初始化通话时作为UE的联系地址。另外，GGSN还为IMS媒体业务监测和管理PDP上下文的使用并且生成计费信息。

5.3 IMS概念

5.3.1 概述

本部分首先对IP多媒体子系统(IMS)的注册和会话建立进行一个比较浅显的说明，描述了有关的IMS实体。其目的并不是为了展示成熟的解决方案，而是通过给出一个概述来帮助读者理解在本章中所解释的各种IMS概念。更详细的注册和会话建立流程将在后续部分中给出并加以阐释。

在即IMS注册之前，用户设备(UE)必须找到它要发送一个REGISTER请求的IMS实体，这个概念被称为代理呼叫会话控制功能(P-CSCF)发现。另外，在注册过程之前，UE需要从身份模块中取出用户身份。在注册过程中，将分配一个服务CSCF(S-CSCF)，并进行认证和建立相应的安全机制，之后用户配置将被下载到所分配的S-CSCF，会话初始化协议(SIP)压缩也得到初始化，并传递隐性注册的公共用户身份。在用户建立一个会话时，因特网协议(IP)策略控

制如何被应用。如何进行服务提供。

5.3.2注册

注册过程使得LIE可以使用IMS服务。在进行IMS注册之前，UE必须获得一个IP连接承载，并且发现IMS系统的入口点P-CSCF。例如，在通用分组无线服务(GPRS)接入中，UE执行GPRS附着过程，并且为SIP信令激活一个分组数据协议(PDP)上下文。

IMS注册包括两个阶段：图5-14的左侧显示了第一阶段——网络如何向UE注册表示异议（Challenge）;图3-1 的右侧展示了第二阶段----UE如何对网络的异议进行响应 ，并完成注册过程 。

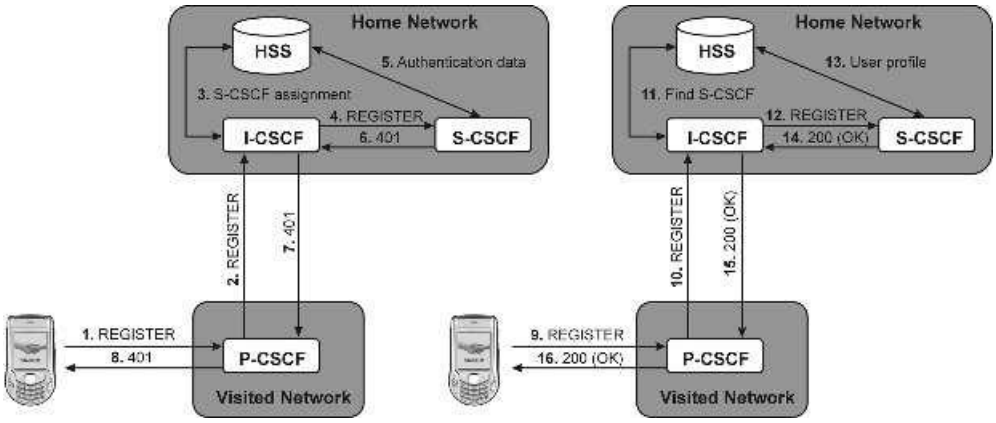


图5-14高层的IMS注册流程

首先，UE发送一个SIP REGISTER(SIP注册)请求给已发现的P-CSCF。这个请求包含要注册的身份和归属域名称(问询CSCF或称I-CSCF的地址)。该P-CSCF处理这个REGISTER请求，并使用所提供的归属域名称来解析I-CSCF的IP地址。随后I-CSCF将会联系归属用户服务器(HSS)，以便为S-CSCF选择过程来获取所需的S-CSCF能力要求。在S-CSCF选定之后，I-CSCF将REGISTER请求转发给选定的S-CSCF。S-CSCF会发现这个用户没有被授权，因此它向HSS索取认证数据，并且通过一个401未授权响应来对该用户的注册表示异议。其次，LIE将计算对这个异议的响应，并且发送另外一个REGISTER请求给P-CSCF。P-CSCF再次找到I-CSCF，并且I-CSCF也将依次找到S-CSCF。最后，S-CSCF检查这个响应，如果这个响应正确，它就从HSS下载用户配置，并且通过一个2000K响应来接受该注册。一旦UE成功被授权，UE就能够发起和接收会话。在注册过程中，UE和P-CSCF会了解到网络中的哪个S-CSCF将要为UE提供服务。

通过周期性的注册更新，UE可以保持其注册处于激活状态，这是UE功能。如果UE没有更新其注册信息，那么在注册定时器超时时，S-CSCF将毫无声息地清除该注册。当UE想要解除在IMS中的注册时，它就简单地发送一个REGISTER请求，该请求中的注册定时器取值为0(过期)。注册过程前后和注册过程期间的信息存储见表5-2。

表5-2 注册过程前后和注册过程期间的信息存储

节点	注册前	注册期间	注册后
UE	P-CSCF地址，归属域名称，证书，公共用户身份，私有用户身份	P-CSCF地址，归属域名称，证书，公共用户身份，私有用户身份，安全联盟	P-CSCF地址，归属域名称，证书，公共用户身份(和隐性注册的公共用户身份)，私有用户身份，安全联盟，服务路由信息(S-CSCF)

P-CSCF	无状态信息	初始网络入口点，LIE的m地址，公共和私有用户III，安全联盟	最终网络入口点(S-CSCF)，LIE地址，公共用户身份(和隐性注册的公共用户身份)，私有用户身份，安全联盟，CDF的地址
I-CSCF	HSS或者SLF地址	HSS或者SLF入口，P-CSCF地址，S-CSCF地址	HSS或者SLF地址
S-CSCF	HSS或者SLF地址	HSS地址/名称，用户配置(有限数量—楣据每个网络场景而不同)，代理地址，名称，公共/私有用户ID，UE IP地址	HSS地址/名字，用户配置(有限数量——根据每个网络场景而不同)，代理地址/名字，公共/私有用户ID，UE IP地址
HSS	用户配置认证数据，S-CSCF选择参数	用户配置，S-CSCF选择参数，如果用户处于漫游状态还包括拜访网络信息	用户配置，S-CSCF选择参数，用户身份注册的相关信息，分配给用户的S-CSCF名字

5.3.3 一次注册多个用户标识符的机制

SIP只允许一次注册一个公共用户身份，因此，如果一个用户有多于一个公共用户身份，那么他必须分别注册每一个公共用户身份。从终端用户的角度来看，这将是让人失望且费时的。显然，在通用移动通信系统(UMTS)中，注册四个公共用户身份所耗费的无线资源将是注册一个公共用户身份情况的四倍。正是出于这些原因，3GPP开发了一种一次注册多个公共用户身份的机制，这个概念称为“隐性注册”。

一个隐性注册集是指通过单条注册请求来注册的一组公共用户身份。当集合内的一个公共用户身份注册后，所有与该隐性注册集合相关联的公共用户身份均同时被注册。同样，当该集合内的一个公共用户身份被注销时，所有已隐性注册的公共用户身份也同时被注销。属于一个隐性注册集合的公共用户身份可能指向不同的服务配置。这些公共用户身份中的一些也可能指向相同的服务配置[3GPPTS 23. 228]。

为了得到隐性注册的公共用户身份，UE必须发送一条SUBSCRIBE(订阅)请求给S-CSCF，来申请一个注册事件包。当S-CSCF收到这个SUBSCRIBE请求后，它将通过一个NOTIFY(通告)请求返回已被隐性注册的公共用户身份。例如，一个用户有四个公共用户身份，它们分属两个隐性注册集。第一个集合包含joe.smith@brandnewcar.com和tel：+358501234567，第二个集合包含joe. smith@irns.example.com和tel：+358503334444。当该用户发送一条包含joe.smith@brandnewcar.com身份的REGISTER请求进行注册时，所指派的S-CSCF将执行正常的注册过程。在授权成功后，S-CSCF下载与该隐性注册集合中的公共用户身份相关联的服务配置(服务配置1)。为了获得隐性注册的公共用户身份，Joe的UE必须发送一条SUBSCRIBE请求给S-CSCF。当S-CSCF接收到该SUBSCRIBE请求时，它将在NOTIFY内返回已隐性注册的公共用户身份，即tel：+358501234567。

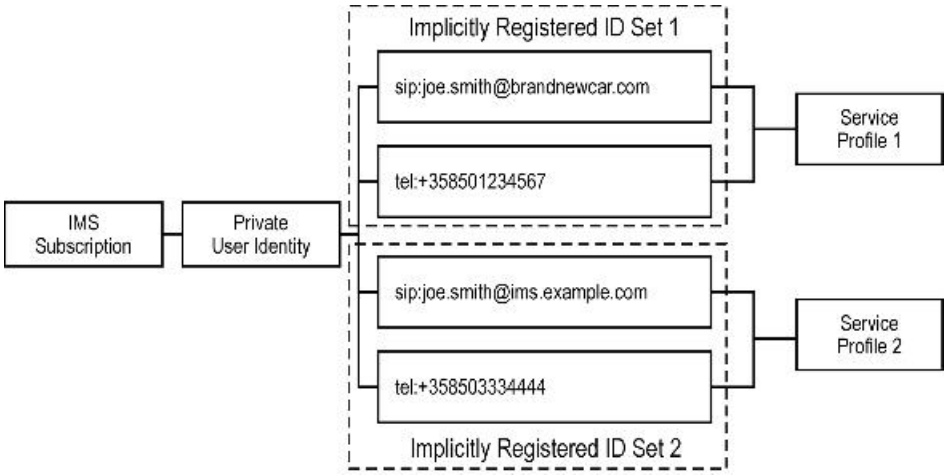


图5-15 隐性注册集举例

5.3.4会话的发起

当用户A想要与用户B进行会话时，UE A就生成一个SIP INVITE请求，并且通过Gm参考点将该请求发送给P-CSCF。P-CSCF会对这个请求进行处理，例如，它在将这个请求通过Mw参考点向S-CSCF转发之前，将其解压缩，并且验证呼叫发起用户的身份。S-CSCF继续处理这个请求，执行服务控制，这可以包括与应用服务器(AS)的交互，并且通过SIP INVITE请求中的用户8的身份最终确定用户8的归属运营商的入口点。I-CSCF会通过Mw参考点收到该请求，并且通过Cx参考点来联系HSS，以找到正在为用户B提供服务的S-CSCF。该S-CSCF负责处理这个终结的会话，这可以包括与应用服务器(AS)的交互，并最终通过Mw参考点将这个请求发送给P-CSCF。经过进一步处理(例如压缩和隐私检查)之后，P-CSCF通过Gm参考点将这个SIP INVITE请求发送给UE B。UE B生成一个响应，即183会话进行中。该响应将按照从UE A到UE B的相同路径反向传回UE A(也就是UE B→P—CSCF→S-CSCF→I-CSCF→S-CSCF→P-CSCF→UE A)(见图5-16)。再经过几次往返之后，两个LIE都完成了会话建立过程，并且能够开始真正的应用了(例如一个棋类游戏)。在会话建立过程期间，运营商可以控制对媒体业务流所用承载的使用。

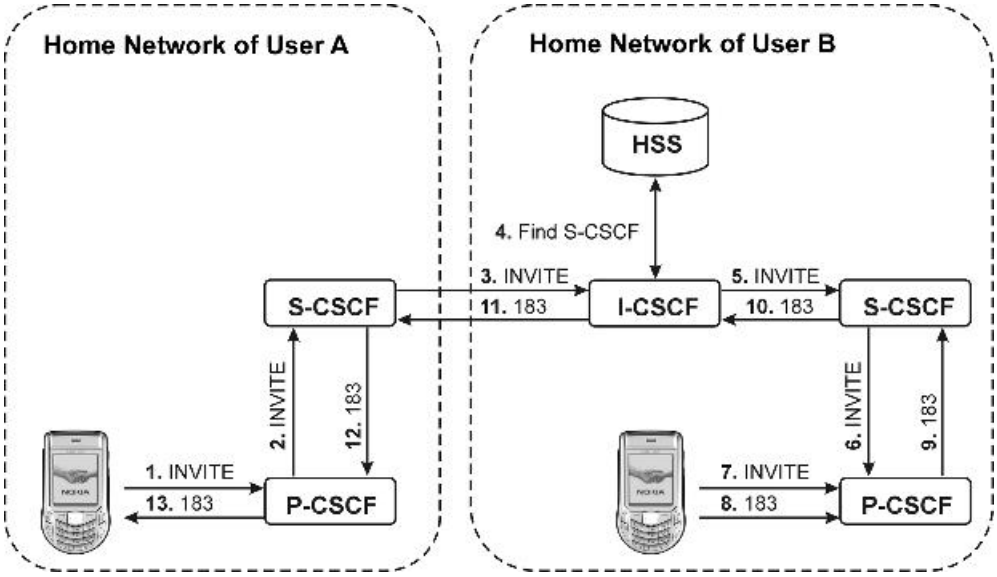


图5-16高层IMS会话建立流程图

为了让读者能够对本书即将介绍的内容先睹为快，表5-3中给出了SIP INVITE请求的高层内容。表中每行给出了被插入、删除或者修改的信息元素。在本书随后的章节中将介绍每个信息元素的含义。

表5-3会话建立过程中SlP lNVITE请求的高层内容

UE(A)	P-CSCF(A)	S-CSCF(A)
用户A身份 用户8身份 联系地址 接入信息 路由信息(Via和Route消息头) 对可靠响应的支持 对前提(Precondition)的支持 安全信息 隐私指示 压缩指示 SDP净荷，反映了用户的终端能力和用户对这个会话的优先选择、MIME子类型“telephone. event”、带宽信息	**插入的信息：** 一条路由信息(Record-Route消息头) IMS计费信息 已确认的A方身份 **删除的信息：** 安全信息 建议的A方身份 **修改的信息：**一路由信息(Route，Via)	**插入的信息：** 运营商之间的标识符 **删除的信息：** 一条路由信息(Route消息头) 接入信息 **修改的信息：** 路由信息(Record-Route，Via) 已确认的A方身份，还包括从现在开始的Tel-URL类型的身份(如果用户有的话)

I-CSCF(B)	S-CSCF(B)	P-CSCF(B)
插入的信息： 一条路由信息(Route消息头) **删除的信息：** 无 **修改的信息：** 路由信息(Via)	**插入的信息：** 无 **删除的信息：** 运营商之间的标识符 **修改的信息：** 路由信息(R-URl,Route,Via,Route. Record)	**插入的信息：** 授权令牌 **删除的信息：** IMS计费信息 一条路由信息(Rout,消息头) 如果要求隐私，则删除A方身份 **修改的信息：** 路由信息(Record-Route，VIa)

5.4 IMS会话举例

5.4.1 概述

本章介绍了一个IMS会话的例子，该会话发生在Tobias和Theresa之间，二者都在各自的归属网络中注册，并且目前都在其他国家漫游。

IMS(IP多媒体子系统)利用SIP(会话初始化协议)和SDP(会话描述协议)来确保Tobias和Theresa之间互相交谈，并且在手机屏幕上看到对方。为了在无线环境下实现上述功能，需要执行以下步骤：

- ✓ Tobias UE需要创建一个INVITE请求，其中包含Theresa注册的公共用户标识，这样才能找到她。
- ✓ 所有的SIP消息都必须经过两人的P．CSCF(代理呼叫会话控制功能)和S．CSCF(服务CSCF)。
- ✓ 所有的SIP消息都要通过在UE和P-CSCF之间建立的IP安全(IPsec)安全联盟(AS)。
- ✓ 所有的SIP消息都以压缩的形式在UE和P-CSCF之间传递。
- ✓ 两个UE要对它们之间即将交换的媒体流达成一致。在本例中，它们将交换一个双向的音频流，以实现两人交谈；还有一个双向视频流，使得他们可以看到对方。
- ✓ 两个UE要采用协商一致的惟一的编解码方案，用于两人交换的每个媒体流。
- ✓ 网络要对会话的媒体进行授权，使得用户可以预留相应的资源。
- ✓ 两个UE都要预留资源(即它们要建立起必要的媒体PDP上下文,用于和网络之间传递媒体流)。
- ✓ 首先两端要成功预留媒体会话所需的资源(即媒体PDP上下文)，然后Theresa UE才能得到指示说弟弟正在呼叫她，这样可以确信媒体会话可以真正的建立起来。
- ✓ 各网元要交换计费信息，使媒体会话能够正确计费。
- ✓ S-CSCF可以为服务对象用户发起高级的服务。
- ✓ 最后Theresa UE开始振铃，并且Theresa会接受这个会话。会话建立阶段到此结束。Tobias和Theresa完成呼叫后，他们将挂机，其中一人的UE将向对方发出BYE请求。举例会话的SIP消息序列如图5-17所示。

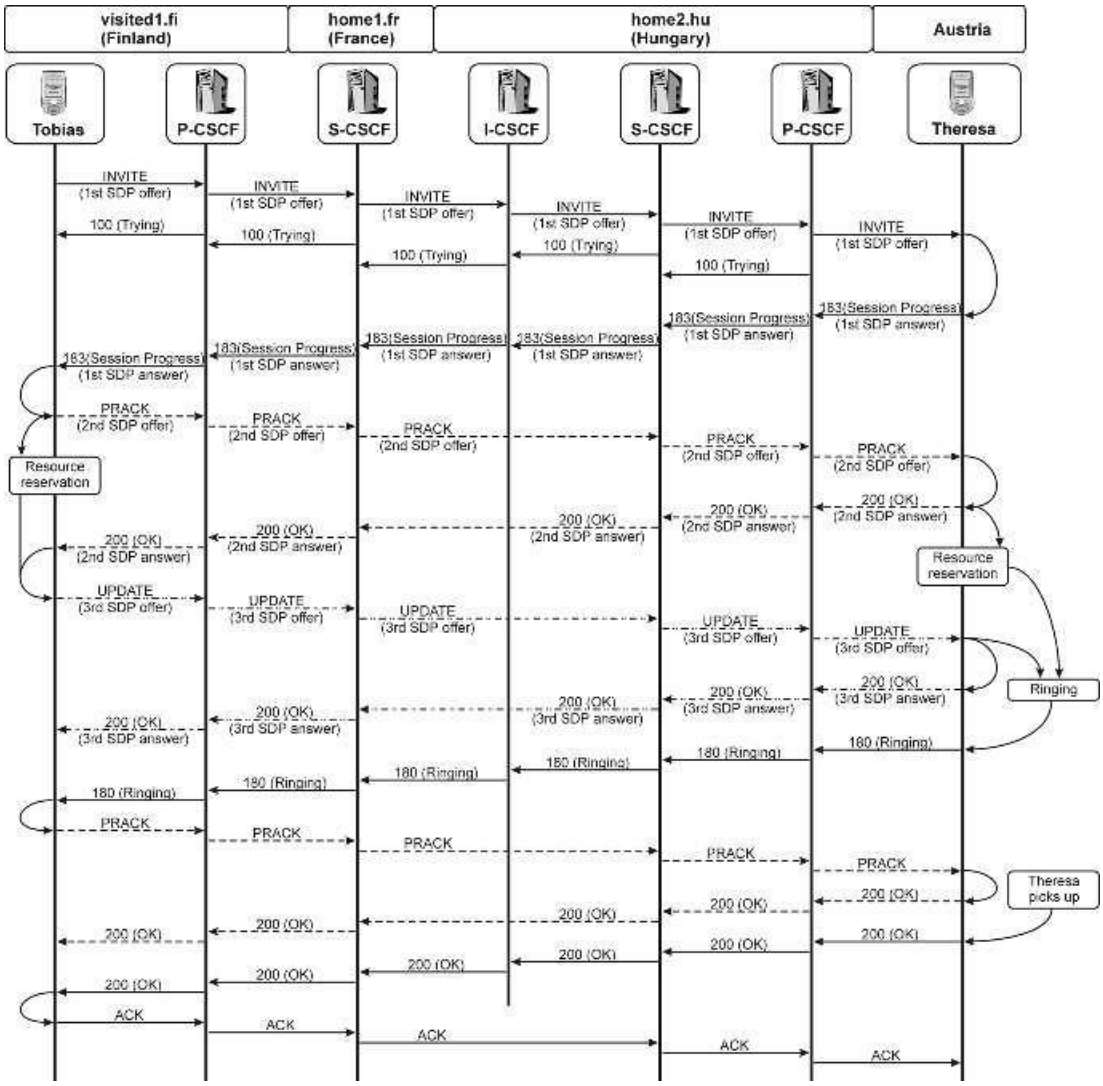


图5-17 IMS会话简历呼叫流程

5.4.2 主叫和被叫标识

5.4.2.1 概述

在注册过程中IMS用户如何得知他能用哪些公共用户标识 ，以及其中哪些标识是已经注册过的。随后，用户——在例子中是Theresa和Tobias——将把这些标识用于各种目的。在每种IMS对话中——本例中为INVITE对话——有两个标识是必须的：

- ✓ 请求中需要给出已注册并已认证的主叫用户(Tobias)的公共用户标识，以便归属网络识别出该用户，并且判断其对于扩展服务的执行权限。该标识位于INVITE请求的P-Asserted-Identity头中。
- ✓ 请求中需要给出已注册并已认证的被叫用户(Theresa)的公共用户标识，以便找到该用户并为其提供服务。该标识位于INVITE请求的请求URI(统一资源标识)以及第一个响应的P-Asserted-Identity头中。

5.4.2.2 From和TO消息头

Tobias UE发给Theresa的INVITE请求中包含以下与他们俩的标识有关的消息头：

INVITE sip:theresa@home2.hu SIP/2.0
From: "Your Brother" <sip:tobi@brother.com>;tag=veli
To: "My beloved Sister" <sip:Theresa@sister.com>
P-Preferred-Identity: <sip:tobias@home1.fr>
Privacy: None

显然，From和TO消息头可以设置为发送者所希望的任何值。本例中选择我们以上词汇是为了清晰地说明：在除REGISTER之外的任何请求消息中，这两个消息头的值都丝毫不会影响IMS路由和安全过程，它们可以随意设置。在这两个消息头中，协议本身惟一需要的信息就是tag参数。

Tobias的归属网络可以对TO消息头中可设置的内容进行一定的限制。这种情况下，如果From和TO消息头中的值不符合运营商的策略，归属网络只能拒绝该请求，因为SIP不允许对这些头中的内容进行任何变更。

5.4.2.3 主叫用户的标识：P-Preferred—Identity和P-Asserted—Identity

1、主叫UE包含的P-Preferred-Identity消息头

上例中,Tobias包含了一个可选的P-Preferred-Identity消息头。如果使用了该消息头，它应该包含该用户的一个已注册的公共用户标识。

如果Tobias希望对他姐姐完全隐藏自己的标识，他必须将Privacy头的值设为“id”。该值迫使Theresa的P-CSCF从INVITE请求中删除P-Asserted-Identity头，这样Theresa只能将From头中的标识作为主叫标识。

2、主叫方P-CSCF包含的P-Asserted-Identity消息头

Tobias UE发出的INVITE请求首先将到达P-CSCF。P-CSCF检查该请求是否来自于一个有效的IPsec SA。如果收到的请求没有受到保护(即没有基于SA)，P-CSCF将拒绝它。

之后，P-CSCF在INVITE请求中添加一个P-Asserted-Identity头；并且如果INVITE请求中包含P-Preferred-Identity，则它会被P-Asserted-Identity头取而代之。在IMS对话中，P-Asserted-Identity头是惟一的、肯定包含了该用户已注册并已认证的公共用户标识的标识。

如果有P-Preferred-Identity头，P-CSCF会检查该消息头中的URI是否是发送方用户的一个当前已注册的公共用户标识0。P-CSCF可以检查所订阅的注册状态信息，得知该公共用户标识是否已经注册。它还可以根据某个请求是通过哪个SA发过来的，从而判断该请求是否来自某个特定用户。如果这两项检查全部通过，P-CSCF就会用P-Asserted-Identity头来替代P-Preferred-Identity头，但内容是相同的。

如果P-Preferred-Identity头中不包含已注册的公共用户标识,P-CSCF就会删除该消息头。在这种情况下，或者在根本不存在P-Preferred-Identity头的情况下，P-CSCF都会添加一个P-Asserted-Identity，其内容为该用户缺省的公共用户标识。

INVITE sip:theresa@home2.hu SIP/2.0
From: "Your Brother" <sip:tobi@brother.com>;tag=veli

To: "My beloved Sister" <sip:Theresa@sister.com>
P-Asserted-Identity: <sip:tobias@home1.fr>
Privacy: None

3、主叫方S-CSCF与P-Asserted-Identity消息头

接收到INVITE请求后，Tobias归属网络的S-CSCF将根据P-Asserted-Identity头中的信息把他识别出来。S-CSCF还会针对该消息头中的公共用户标识，而检查其认证和注册状态。正是由于这些检查，这个消息头成为整个对话中识别该用户的主要标识。应用服务器AS也可以依据这个消息头作为标识识别甚至认证的依据。Tobias的S-CSCF与P-Asserted-Identity消息头

接收到INVITE请求后，Tobias归属网络的S-CSCF将根据P-Asserted-Identity头中的信息把他识别出来。S-CSCF还会针对该信息头中的公共用户标识，而检查其认证和注册状态。正是由于这些检查，这个消息头成为整个对话中识别该用户的主要标识。应用服务器AS也可以依据这个头作为标识识别甚至认证的依据。

Tobias的S-CSCF可以在P-Asserted-Identity头中增加一个附件的URI。本例中它在消息头中增加了Tobias的电话统一资源定位符（tel URL）：

INVITE sip:theresa@home2.hu SIP/2.0
From: "Your Brother" <sip:tobi@brother.com>;tag=veli
To: "My beloved Sister" <sip:Theresa@sister.com>
P-Asserted-Identity: <sip:tobias@home1.fr>, <tel:+44123456789>
Privacy: None

在Tobias归属网络S-CSCF将请求转发到Theresa的归属网络之前，它还要检查该网络是否位于其信任域之内。如果该S-CSCF与Theresa的归属网络不处于相同的信任域，只要Privacy头设置为“id”，那么S-CSCF会从请求中删除P-Asserted-Identity头。在本例中，我们假设两个网络具有信任关系，该消息头可以继续发送。

4、被叫方一侧的P-Asserted-Identity消息头

Theresa的P-CSCF需要检查请求中的Privacy头。如果它的值没有设置为“id”，P-CSCF就可以将P-Asserted-Identity头转发给Theresa UE。

至此，Theresa UE最终收到了P-Asserted-Identity头。它可以利用该消息头中的信息来显示其主叫方的“真实名称”。

5.4.2.4 被叫用户标识

1、请求URI

让我们再看一下Tobias发出的INVITE消息。其第一行，也就是请求URl，如下所示：

INVITE sip:theresa@home2.hu SIP/2.0

请求URl被设置为该请求的最终目的地(即Theresa的SIP URI)。11. 3节将解释SIP和IMS路由过程如何使用该URl。然而，该URl同时还用于在Theresa的归属网络中标识她为被叫用户。这意味着Theresa的S-CSCF会检查这个公共用户标识目前是否已经完成注册并通过认证。如果Theresa现在还没有注册这个公共用户标识，S-CSCF将会对INVITE请求返回一个404(未

发现)响应，宣布呼叫失败，或者将INVITE请求前转到Theresa的语音邮箱，这取决于对未注册用户设置的过滤规则。

在我们的例子中，假设Theresa已经注册了Tobias UE请求URI中的公共用户标识。

2、请求URI和P-Called-Party-ID消息头

当Theresa S-CSCF将请求转发给被叫侧的P-CSCF时，产生了另一个问题：作为Theresa的SIP注册服务器，S-CSCF会用Theresa已注册的联系地址来覆盖请求URI，以便将请求路由到Theresa目前注册的UE上。这样，请求URI中的公共用户标识将会丢失。

但是，Theresa可能有多个公共用户标识，她希望知道这个呼叫是发往其中的哪一个。例如，她可能有一个与工作有关的用户标识，其他的则与其私人生活有关。可能她的UE对于不同的用户标识会响起不同的振铃。

Theresa不能信任请求中的To消息头，因为主叫方可以将其设置为任意值——甚至是与请求URI中的公共用户标识完全不同的内容。

为了不丢失Tobias呼叫姐姐时所使用的公共用户标识,S-CSCF在使用已注册的联系地址覆盖请求URI的同时，还在INVITE请求中增加P-Called-Party-ID头。这个P—Called—Party-ID头中包含了请求URl中的那个公共用户标识：

```
INVITE sip:[5555::5:6:7:8]:1006 SIP/2.0
P-Called-Party-ID: sip:theresa@home2.hu
```

3、P-Asserted-Identity消息头

收到INVITE请求后，Theresa UE在对INVITE请求的第一个响应183(会话进行中)响应中包含P-Preferred-Identity头，其中会包含Theresa的公共用户标识中的某一个。

```
SIP/2.0 183 Session in Progress
From: "Your Brother" <sip:tobi@brother.com>;tag=veli
To: "My beloved Sister" <sip:Theresa@sister.com>;tag=schwester
P-Preferred-Identity: <sip:theresa@home2.hu>
Privacy: None
```

Theresa的P-CSCF会执行与前文Tobias P-CSCF所作的相同检查，并将P-Preferred-Identity头更换为P-Asserted-Identity头。

```
SIP/2.0 183 Session in Progress
From: "Your Brother" <sip:tobi@brother.com>;tag=veli
To: "My beloved Sister" <sip:Theresa@sister.com>;tag=schwester
P-Asserted-Identity: <sip:theresa@home2.hu>
Privacy: None
```

5.4.2.5 相关标准

与5.2节有关的规范有：

- ✓ RFC3323 A Privacy Machanism for the Session Initiation Protocol(SIP).
- ✓ RFC3325 Private Extensions to the Session Initiation Protocol(SIP)for Asserted Identity within Trusted Networks.
- ✓ RFC3455 Private Header(P-Header)Extensions to the Session Initiation

Protocol(SIP)for the 3rd-Generation Partnership Project(3GPP).

5.4.3 路由

5.4.3.1 概述

IMS中最复杂的问题之一就是请求消息的路由，尤其是初始请求的路由。在我们的例子中，Tobias发送初始INVITE请求给Theresa。其结果是，建立了一个SIP对话，并通过它发送若干后续的请求，例如ACK、PRACK、UPDATE和BYE。

Tobias UE发送INVITE请求时并不知道如何才能达到Theresa UE。它所能提供的所有信息仅包括：

- ✓ INVITE请求的最终目的地——即Theresa的SIP URI(她公共用户标识之一)，Tobias必须要提供(例如从他的电话本中选取)。
- ✓ P-CSCF的地址——即Tobias UE的出站代理，也是路由的第一跳。该地址是在SIP注册之前的P-CSCF发现过程中获得的。
- ✓ S-CSCF的地址——这是在注册过程中通过Service-Route消息头发现的。

具备了这些不完整的路由信息之后，INVITE请求就上路了。它先后经过为Tobias选派的P-CSCF和S-CSCF。

Tobias的S-CSCF现在除了最终目的地(即Theresa的公共用户标识：“sip: Theresa@home2.hu”)之外，没有任何进一步的路由信息。由于Tobias的S-CSCF不是Theresa的注册服务器，它只能解析地址的宿主部分“home2.hu”。它将该域名发往域名系统(DNS)服务器，然后将收到一个或多个Theresa归属网络中的问询CSCF(I-CSCF)地址。S-CSCF选择其中之一并把INVITE请求发给它。

I-CSCF仅作为Theresa归属网络的入口。它询问本地HSS为Theresa选派哪个S-CSCF，并把INVITE请求进一步转发到该S-CSCF地址。

现在Theresa的S-CSCF就作为注册服务器，将她的SIP URI更换成她已注册的联系地址。它还不直接将请求发往Theresa UE，因为它还没有和UE建立SA。因此，这个INVITE请求首先被发往Theresa的P-CSCF。S-CSCF知道P-CSCF的地址，因为Theresa注册过程中从Path头收到了该地址。

最终，P-CSCF通过IPsec SA将INVITE请求转发到Theresa UE。以上显示了对于初始的请求，从Tobias到Theresa的路由是一段一段被拼接 起来的，因为主叫UE和各个CSCF都仅仅知道需要经过的下一跳或两跳的信息。为了使得该对话中后续的消息路由更为简单，将使用SIP路由机制：

- ✓ 所有的CSCF都将自己的地址放在Via消息头的顶端——这使得所有对于INVITE请求的响应都可以准确地沿着请求消息所经过的路由发送回去。
- ✓ 除Theresa的I-CSCF以外，所有CSCF将自己的地址放入Record-Route头的顶端——这使得该对话中所有的后续请求都可以根据Record-Route头记录的CSCF而顺序转发。Theresa归属网络的I-CSCF在找到Theresa的S-CSCF地址后 就完成了它的路由功能，因此在后续路由中就不再需要它了。

当发送后续请求时，UE将包含一个Route条目的列表，这将强制该请求沿着已记录的路由转发。

5.4.3.2 会话、对话、事务和分支

在会话建立过程中以及会话保持活跃的过程中，两个UE之间要交换多种不同的信令消息，并建立各种不同的关系。

名词“会话(Session)”描述了两个用户之间的媒体连接。Tobias希望与他姐姐之间交换音频和视频媒体流。这种媒体交换是在所谓“承载层”完成的，这意味着RTP(实时传输协议)数据包从两个UE发往它们的GGSN（网关GPRS支持节点），然后GGSN直接通过骨干网交换彼此之间的这些数据包。这个会话是建立在SIP和SDP信令基础上的，而这些信令通过“控制平面”交换。

SIP对话(Dialog)是两个UE之间用于建立、更改和释放媒体会话的信令关系。对话首先将(通过INVITE请求)建立起来，并且在与相关的会话保持活跃期间一直存在。每个SIP对话通过SIP请求中Call-ID头的值、To和From头中的标签来标识。

From: "Your Brother" <sip:tobi@brother.com>;tag=veli

To: "My beloved Sister" <sip:theresa@home2.hu>;tag=schwester

Call-ID: apb03a0s09dkjdfglkj49555

本例中如下所示：

Tobias和Theresa间多媒体会话的SIP对话起始于INVITE请求，并终止于对BYE请求的200(OK)响应。

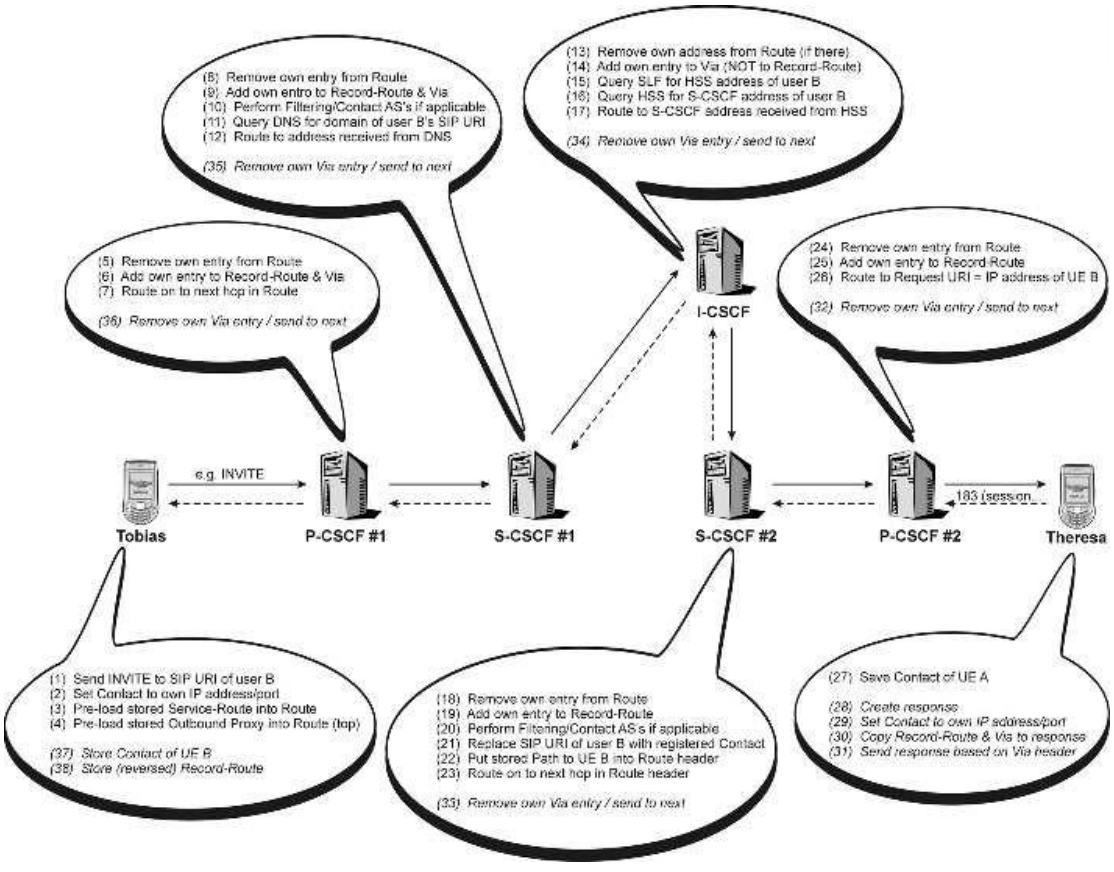


图5-18 初始INVITE请求及其响应的路由

一个SIP事务(transaction)由一个SIP请求和所有对它的响应构成。为建立会话,Tobias UE发送INVITE请求给Theresa UE。首先它会收到P-CSCF对该请求的100(尝试中)响应。之后，Theresa UE返回一个183(会话进行中)、一个180(振铃中)并最终给出一个200(OK)响应。所有这5个消息属于同一个对话，并具有相同的CSeq号。

From: "Your Brother" <sip:tobi@brother.com>;tag=veli
To: "My beloved Sister"
<sip:theresa@home2.hu>;tag=schwester
Call-ID: apb03a0s09dkjdfglkj49555
CSeq: 1112 INVITE

来自同一点(本例是Tobias UE)的每个后续请求都具有比前一个请求更高的CSeq值，例如第一个PRACK请求的CSeq是1113，接下来的UPDATE请求的 CSeq是1114，依此类推。

每个实体，包括UE和CSCF，都基于“分支(branch)”参数把收到的响应与发出的请求相关联起来，branch参数是作为VIa消息头的参数而添加的。例如，Tobias的P—CSCF将下面的Via头加到INVITE请求中：

INVITE sip:theresa@home2.hu SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb

这个branch参数在P-CSCF处标识了INVITE事务(即INVITE请求和及其响应),它的构造是通过请求中的To和From头的标签、Call-ID、Cseq号码以及Via头中最顶端的信息来完成的。

5.4.3.3 INVITE请求的路由

1、从Tobias UE到P. CSCF Tobias UE将在初始的INVITE请求中包含如下与路由相关的消息头：

INVITE sip:theresa@home2.hu SIP/2.0
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Route: <sip:[5555::a:b:c:d]:7531;lr>
Route: <sip:orig@scscf1.home1.fr;lr>
Contact: <sip:[5555::1:2:3:4]:1357>

该请求的目的地是Theresa的SIP URI，如请求URI示。

在注册过程中，Tobias UE到其归属网络S-CSCF之间的路由是通过Service-Route头发现的。UE预先将这部分路由放到Route消息头中，然后把P-CSCF加在上面，因为UE总是需要首先联系气出站代理。

Tobias UE还把自己的IP地址放在请求消息的Contact消息头中，这样对端的UE B就可以直接访问它。它还将其口地址放在Via消息头中，以便可以接收到对该请求的响应。

当已建立的IPsec SA发送请求消息通过时，Tobias UE会：

- ✓ 把Contact消息头的端口值设置为UE的受保护的服务器端口(1357)，因为它希望通过已建立的IPsec SA接收该对话中所有的后续请求。
- ✓ 把Via消息头的端口值设置为UE的受保护的服务器端口(1357)，因为它希望通过已建立的IPsec SA接收对INVITE请求的所有的响应。

- ✓ 把Route消息头中P-CSCF地址的端口值设置为P-CSCF受保护的服务器端口(7531)，因为P-CSCF必须通过已建立的Ipsec SA接收所有来自UE的请求。UE是在SIP安全机制协定过程中得知P. CSCF受保护的服务器端口。

To和From消息头从来不用于路由的目的。

现在INVITE请求将发往Route消息头中最顶端的地址，在本例中就是服务于Tobias的P-CSCF。

2、从Tobias的P-CSCF到S-CSCF

当接收到请求消息时，P-CSCF会：

- ✓ 从Route消息头的顶端删除自己的地址。
- ✓ 检查该请求包含的路由信息是否与在注册过程中所保存的进一步的路由信息相一致(即UE并没有试图违背Service-Route)。
- ✓ 在Via消息头的顶端填入自己的地址，因为它希望接收对INVITE请求的所有的响应。
- ✓ 添加第一个Record-Route消息头并在其中填写它自己的地址——这可以确保该对话中所有后续的请求都会经过该P-CSCF。
- ✓ 在Via和Record-Route头中都不包含受保护的服务器端口号——受保护的服务器端口号仅仅用于接收UE通过已建立的IPsec SA组发来的SIP消息。

完成这些之后，P-CSCF再次将分组路由到Route头最顶端的地址，本例中即是为Tobias提供服务的S-CSCF.

```
INVITE sip:theresa@home2.hu SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Record-Route: <sip:pcscf1.visited1.fi;lr>
Route: <sip:orig@scscf1.home1.fr;lr>
Contact: <sip:[5555::1:2:3:4]:1357>
```

3、从Tobias的S-CSCF到Theresa的归属网络(I-CSCF)

Tobias的S-CSCF把自己的地址从Route消息头的顶端除去；之后Route消息头就空了，可以被删除。之后S-CSCF将自己的地址放在Record-Route和Via头的顶端。

完成这些步骤之后，它就要进一步转发该请求消息。但是，现在出现了一个问题：没有Route消息头来指示下一跳的地址。现在S-CSCF所能做的就是取出请求URl中Theresa的公共用户标识的宿主部分(即“home2. hu”)，并且通过DNS找到该域的一个SIP服务器。作为应答，它会收到Theresa归属网络的一个或多个I-CSCF的地址，它从中选取一个并将请求转发过去。

请注意，当S-CSCF知道这个I-CSCF可以作为宽松路由器时，它惟一能做的就是将I-CSCF地址放入Route消息头。在本例中，S-CSCF和I-CSCF在不同的网络中，因此假设S-CSCF无法知道I-CSCF的路由能力，因此它通过UDP包将初始INVITE请求发往I-CSCF地址。

```
INVITE sip:theresa@home2.hu SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.fr;branch=asctb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Record-Route: <sip:scscf1.home1.fr;lr>
```

Record-Route: <sip:pcscf1.visited1.fi;lr>
Contact: <sip:[5555::1:2:3:4]:1357>

4、从I-CSCF到Theresa的S-CSCF

现在Theresa归属网络的I-CSCF需要找到为Theresa分配的S-CSCF的地址。即便Theresa现在是未注册状态，只要她订阅了某些服务而现在是未注册状态，I-CSCF就能够找到一个缺省的S-CSCF地址。

有关当前为某用户所分配的S-CSCF的信息存储在归属用户服务器(HSS)中；由于网络中可能同时存在多个HSS，I-CSCF首先需要查询订购关系定位功能(SLF)来找到保存Theresa数据的HSS。SLF返回HSS地址后，I-CSCF便查询该HSS最终得到为Theresa提供服务的那个S-CSCF的地址。现在，I-CSCF在Route列表顶端添加一个Route项，并填入所收到的S-CSCF地址。然后，I-CSCF会：

- ✓ 从Route消息头顶端删除它自己的条目，如果存在该项的话(本例中不存在该项)。
- ✓ 把它的地址放入Via列表顶端，以便可以收到对INVITE请求的所有响应。
- ✓ 并不把它的地址放入Record-Route中，由于它不需要再收到该对话中的任何后续请求——I-CSCF的任务就是找到被叫用户的S-CSCF，但是由于这是在初次请求过程中完成的，因此在Route消息头中不再需要保留它。

请求消息再次发往Route消息头最顶端的地址，这次是Theresa的S-CSCF。

INVITE sip:theresa@home2.hu SIP/2.0
Via: SIP/2.0/UDP icscf1.home2.hu;branch=bicth
Via: SIP/2.0/UDP scscf1.home1.fr;branch=asctb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Route: <sip:scscf2.home2.hu;lr>
Record-Route: <sip:scscf1.home1.fr;lr>
Record-Route: <sip:pcscf1.visited1.fi;lr>
Contact: <sip:[5555::1:2:3:4]:1357>

5、从Themsa的S-CSCF到P-CSCF

现在，Theresa的S-CSCF(她的注册服务器)收到了INVITE请求。同样，它也从Route头中删除自己地址的条目，并把自己的地址放入Via和Record-Route列表。然后，它按照11．3．8节中介绍的那样为Theresa提供服务。

做完这些之后，S-CSCF就执行注册服务器的功能(即它把请求URl：Theresa的SIP地址，换成她的已注册联系地址)。已注册联系地址还包含一个受保护的服务器端口(1006)，用于通过建立的IPsec SA将请求从P．CSCF发给Theresa UE。

在Theresa的注册过程中，S-CSCF从P．CSCF处收到了Path消息头。它现在必须把Path消息头中的条目放到INVITE请求的Route消息头中去。如果不做这一步，该请求会被直接发往Theresa UE，但后者无法接收该请求，因为它没有和S-CSCF之间建立IPsec SA。

因此S-CSCF增加一个新的Route消息头，并填入P-CSCF地址，由于现在这就是最顶端的条目了，因此该请求会立刻发往该地址。

INVITE sip:[5555::5:6:7:8]:1006 SIP/2.0

Via: SIP/2.0/UDP scscf2.home2.hu;branch=cscth
Via: SIP/2.0/UDP icscf1.home2.hu;branch=bicth
Via: SIP/2.0/UDP scscf1.home1.fr;branch=asctb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Route: <sip:pcscf2.home2.hu;lr>
Record-Route: <sip:scscf2.home2.hu;lr>
Record-Route: <sip:scscf1.home1.fr;lr>
Record-Route: <sip:pcscf1.visited1.fi;lr>
Contact: <sip:[5555::1:2:3:4]:1357>

6、从P-CSCF到Theresa UE

P-CSCF收到请求之后，它会按照惯例操作：将整个Route头删除i并将自己放入Record-Route和Via头中，并将请求发往最终目的地，也就是请求URI中指示的——Theresa UE。

INVITE sip:[5555::5:6:7:8]:1006 SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.hu:1511;branch=dpcth
Via: SIP/2.0/UDP scscf2.home2.hu;branch=cscth
Via: SIP/2.0/UDP icscf1.home2.hu;branch=bicth
Via: SIP/2.0/UDP scscf1.home1.fr;branch=asctb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Route: <sip:pcscf2.home2.hu:1511;lr>
Record-Route: <sip:scscf2.home2.hu;lr>
Record-Route: <sip:scscf1.home1.fr;lr>
Record-Route: <sip:pcscf1.visited1.fi;lr>
Contact: <sip:[5555::1:2:3:4]:1357>

Via头中的P-CSCF条目还包含受保护的服务器端口的端口号(1511)，该端1：3号是在Theresa注册过程中与TheresaUE协商确定的，与10．7．5节介绍的Tobias注册过程相同。该条目迫使Theresa UE通过已建立的IPsec SA来发送对于该请求的所有响应。

完全相同的受保护服务器端El(1511)也被填入P.CSCF的Record.Route消息头的条目中，P-CSCF希望在这里收到该对话中所有后续的来自Theresa UE的请求。当Theresa UE收到INVITE请求后，它保存所收到的Contact值和Record．Route因为它还要基于这些信息对该对话中的后续请求进行路由。

5.4.3.4 首个响应的路由

1、从Theresa UE到 P-CSCF

现在，Theresa UE根据先决条件对收到的INVITE请求生成一个响应消息：183(会话进行中)响应。UE在Contact消息头中填入自己的IP地址，指示它希望用此地址接收该对话中的后续请求。这个Contact地址还包括Theresa UE受保护的服务器端口(1006)，以确保所有后续请求都是通过已建立IPsec SA来接收的。INVITE请求的Record-Route和Via消息头也会出现在响应中。之后，Theresa UE发送到Via消息头最顶端的地址和端口号，即P-CSCF的受保护

的服务器端口号：

SIP/2.0 183 Session in Progress
Via: SIP/2.0/UDP pcscf2.home2.hu:1511;branch=dpcth
Via: SIP/2.0/UDP scscf2.home2.hu;branch=cscth
Via: SIP/2.0/UDP icscf1.home2.hu;branch=bicth
Via: SIP/2.0/UDP scscf1.home1.fr;branch=asctb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Record-Route: <sip:pcscf2.home2.hu:1511;lr>
Record-Route: <sip:scscf2.home2.hu;lr>
Record-Route: <sip:scscf1.home1.fr;lr>
Record-Route: <sip:pcscf1.visited1.fi;lr>
Contact: <sip:[5555::5:6:7:8]:1006>

Theresa UE对该INVITE请求而发出的所有的其他响应也都会包含与183(会话进行中)响应中相同的Via消息头。

2、从Theresa的P-CSCF到Tobias的P-CSCF

P-CSCF通过Via消息头中自己设定的branch参数来标识该响应属于哪个INVITE事物。它会按照如下的方式来处理183(会话进行中)响应中的路由信息:它将自己的地址从Via头中删除。它重写自己的Record-Route条目。

✓ 它将请求发往Via头顶端的地址，即Theresa归属网络的S-CSCF。

P-CSCF为何要重写它的Record. Route条目呢?它这样做是为了确保除Theresa UE以外，其他任何实体都不会向P-CSCF的受保护的服务器端口发送消息，而这个端口只用于和UE. 之间的IPsec SA。如果Theresa S-CSCF向P-CSCF的受保护服务器端口(1511)发送下一个请求(PRACK)，则该请求会被P-CSCF协议栈的IPsec层丢弃，因为它在发送过程中没有经过IPsec SA的完整性保护。

SIP/2.0 183 Session in Progress
Via: SIP/2.0/UDP scscf2.home2.hu;branch=cscth
Via: SIP/2.0/UDP icscf1.home2.hu;branch=bicth
Via: SIP/2.0/UDP scscf1.home1.fr;branch=asctb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Record-Route: <sip:pcscf2.home2.hu;lr>
Record-Route: <sip:scscf2.home2.hu;lr>
Record-Route: <sip:scscf1.home1.fr;lr>
Record-Route: <sip:pcscf1.visited1.fi;lr>
Contact: <sip:[5555::5:6:7:8]:1006>

从现在开始，直到它达到Tobias的P-CSCF之前，响应消息不会再发生任何重要变化——每一跳仅仅是删掉它自己的Via条目，并把消息发往Via中的下一个条目。Record-Route保持不变。请注意，允许返回途中的其他服务器改写它们的 Record-Route条目，以区分来自不同方向的请求。但是，这在本例中没有这样做，因为这仅是CSCF具体实现中的可选功能。

3、从Tobias的P. CSCF到他的UE

收到l 83(会话进行中)响应后，Tobias P-CSCF执行与Theresa P-CSCF相类似的操作。它也重写Record-Route消息头中关于它自己的条目，但是它不会删除 受保护的服务器端口(与Theresa P-CSCF处理同一响应的方式完全相同)，而是增加该端口(7531)。其结果就是强制Tobias UE必须通过已建立的IPsec SA来发送所有后续的请求。

由于P-CSCF根据Via头来转发响应，它会将该响应发往Tobias UE的受保护的服务器端口(1357)，即通过IPsec SA发送：

SIP/2.0 183 Session in Progress
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Record-Route: <sip:pcscf2.home2.hu;lr>
Record-Route: <sip:scscf2.home2.hu;lr>
Record-Route: <sip:scscf1.home1.fr;lr>
Record-Route: <sip:pcscf1.visited1.fi:7531;lr>
Contact: <sip:[5555::5:6:7:8]:1006>

Tobias UE在收到响应消息后，会：

- ✓ 从Contact头中读出Theresa UE的IP地址并保存起来；
- ✓ 把Record-Route列表中的所有条目的顺序颠倒过来并保存起来。

5.4.3.5 重传INVl TE请求和100(尝试中)响应

发出INVITE 请求之后，Tobias UE会等候来自Theresa UE的响应。它会等候计时器Tl(在IMS中设置为2s)超时。每次超时之后，它就重传一个INVITE请求，直到收到对该请求的响应。如果128s(=64xTI)后还不能收到响应，它就告诉Tobias这次会话建立失败。

由于本例中的INVITE请求要经过欧洲各地的多个CSCF，因此它到达TheresaUE可能已经超过2s了，而且后者还要生成183(会话进行中)响应并沿原路长途跋涉返回芬兰。

为了避免Tobias UE频繁地重发INVITE请求，P-CSCF在收到INVITE请求后会发回一个100(尝试中)响应，这意味着现在开始P-CSCF会负责上述重传工作。

沿途的所有感知呼叫状态的其他SIP代理都会发出相同的100(尝试中)响应(见图11—1)，该响应总是终止于最后一个负责进行重传的SIP代理。例如，Theresa归属网络的S-CSCF发回一个100(尝试中)响应，它首先到达I-CSCF。由于I-CSCF并不是能感知呼叫状态的SIP代理，它只是再次转发(基于Via头)。接下来，响应到达Tobias归属网络的S-CSCF。Tobias的S-CSCF已经向P. CSCF发出过100(尝试中)响应，因此它已经承担起重传INVITE的任务。现在接收到了100(尝试中)响应，说明不需要继续重传INVITE请求，因为这个责任已经转移到Theresa的S-CSCF上。

5.4.3.6 同一对话中后续请求的路由

当两个UE其中之一需要发起这一对话中的后续请求时，它将所存储的Record-Route条目复制到新请求的Route头中，并把对端UE的IP地址放入请求URl中。

这个请求会严格按照Route消息头中的条目路由到对端UE(见图5-19)。途中经过的每个CSCF都把自己的地址放在Via头中，以便得到对于该请求的所有响应。

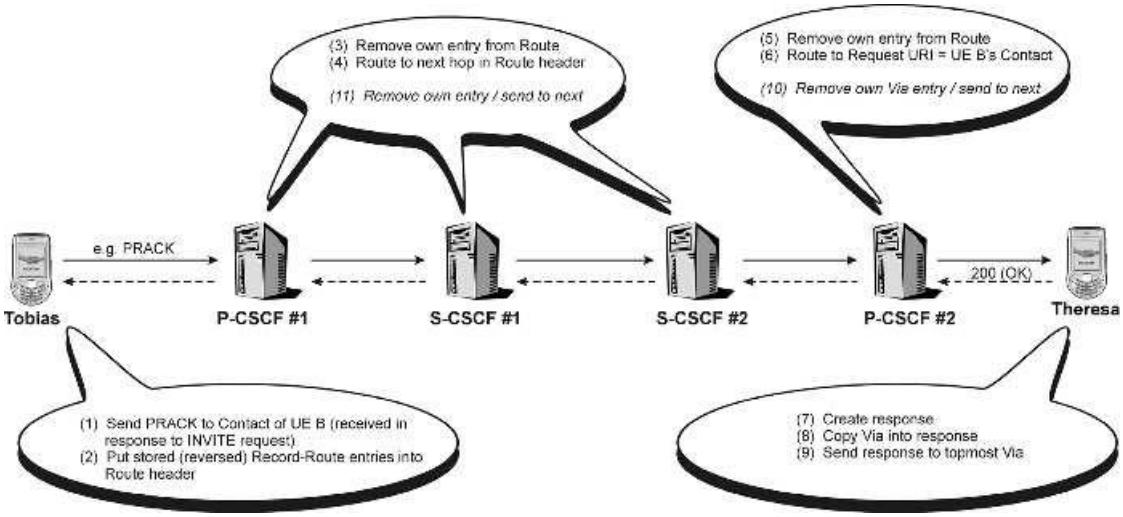


图5-19 后续请求及其响应的路由

由于I-CSCF从一开始就不记录任何路由，因此它不会再收到任何后续请求。例如，Tobias LIE要返回一个PRACK请求来确认已收到183(会话进行中)响应。这个PRACK请求要包含如下路由信息：

PRACK sip:[5555::5:6:7:8]:1006 SIP/2.0
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=82uetb
Route: <sip:pcscf1.visited1.fi:7531;lr>
Route: <sip:scscf1.home1.fr;lr>
Route: <sip:scscf2.home2.hu;lr>
Route: <sip:pcscf2.home2.hu;lr>

因此，该PRACK请求会被按照如下方式路由：

- ✓ 根据Route头，到达Tobias的P-CSCF和S-CSCF，之后是Theresa的S-CSCF和P-CSCF；
- ✓ Theresa的P-CSCF根据请求URI地址，通过IPsec SA，发往Theresa UE；请求URI取自Tobias LIE从183(会话进行中)响应的Contact消息头。

一个对话中的后续请求中不再包含Contact消息头，因为两个UE的地址已经在初始请求及其初始响应的发送和接收过程中交换过了。此外，CSCF也不在请求中放入任何Record-Route头，因为在初始请求中已经记录下了路由。

Theresa UE将对PRACK请求发出一个200(OK)响应，并包含下列路由信息：

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.hu;branch=c2scth
Via: SIP/2.0/UDP scscf1.home1.fr;branch=a2sctb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=92pctb

该响应根据Via消息头中的条目而路由回去，不再返回Record-Route头。

5.4.3.7 两个UE之间的独立事务

对于独立事务，例如MESSAGE和OPTION，将采用与初始请求相同的路由过程，只是不需要记录路由，因为独立事务不会生成对话。

5.4.3.8 与AS之间的路由

1、 S-CSCF上的过滤准则评估

应用服务器(AS)实现了IMS的服务提供，要根据初始过滤准则来联系AS。当Tobias或Theresa的S-CSCF收到一个初始请求时，它会逐个检查这些过滤准则，如果匹配了其中一个或多个，它就会把请求发送给准则中指出的AS。过滤准则是注册过程中由S-CSCF从HSS中下载而来的，作为Tobias和Theresa服务配置的一部分。

在本例中，我们假设有三个AS为来自Tobias的请求设置了过滤准则。Tobias的S-CSCF会针对INVITE请求中收到的信息来逐个检查这些过滤准则。

INVITE sip:theresa@home2.hu SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.fr;branch=asctb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Route: <sip:orig@scscf1.home1.fr;lr>
From: "Your Brother" <sip:tobi@brother.com>;tag=veli
To: "My beloved Sister" <sip:Theresa@sister.com>
P-Asserted-Identity: <sip:tobias@home1.fr>
Privacy: None

表5-4 Tobias S-CSCF中的过滤准则

过滤准则元素	过滤准则1	过滤准则2	过滤准则3.
SPT：会话情况	发起	发起	终止
SPT：公共用户标识	tel：+44.123-456-789	sip：tobias@homl. fr tel：+44-123-456.789	sip：tobias@homel. fr
SPT：SIP方法		Dn，舵	SUBSCRmE
其他SPT			SIP消息头：event：pres
应用服务器	sip：asl. homel. fr；lr	sip：as2. homel. fr；lr	sip：as3. homel. fr；lr

注：星号表示任何值都可以匹配。

过滤准则#1不匹配，因为经检查为公共用户标识而设置的服务点触发器(SPT)，发现P-Asserted-Identity头中没有包含Tobias的tel URL。

过滤准则#2获得了匹配，因为：

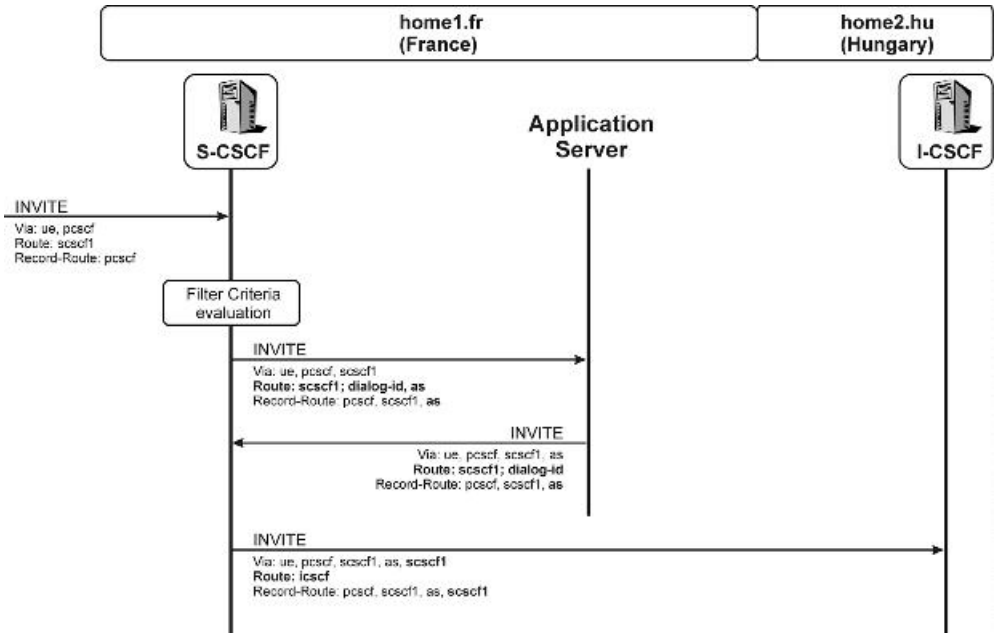
- ✓ 该INVITE请求来自会话发起用户——S-CSCF是通过它当初设置在Service-Route头条目中的用户部分得知这一情况的，并且现在这个用户部分随着Route头返回来了(见10.5.8节)。
- ✓ P-Asserted-Identity的置满足过滤准则的公共用户标识之一(sip:tobias@homel.fr)。
- ✓ SIP方法是INVITE。

2、从S-CSCF到AS

现在，S-CSCF需要将INVITE请求发往过滤准则2中指示的AS(图5-20)。

S-CSCF还需要采取措施，来应付当AS完成操作后自己还会再次收到该INVITE请求，因为S-CSCF还要检查过滤准则3，以便将请求发往Theresa的归属网络。为了达到这个目的，S-CSCF

增加一系列与路由有关的消息头：



- ✓ 将它自己的地址放入Route头最顶端，以便可以接收到从AS发回的INVITE请求；
- ✓ 将AS的地址放入Route头最顶端，以便将AS作为INVITE请求路由的下一跳；
- ✓ 将它自己的地址放入Record-Route头最顶端，这样后续请求都会经过它；
- ✓ 将它自己的地址放入Via头最顶端，以便它可以收到该请求的所有响应。

除此之外，S-CSCF还将Route头自己的条目中添加一个对话标识符，这个Route头是刚刚添加的,对话标识符特定于具体的实现方式。它将此对话标识符设置成某个值，使得它可以识别为此INVITE请求而生成的对话。进行这一操作的目的是什么呢?

AS有可能决定充当一个背靠背用户代理(B2BUA)，在本地终结这个INVITE请求。然后它发出一个新的INVITE请求给S-CSCF，带有新的Call-ID。由于AS要使用Route头中的URI进行下一跳路由，因此S-CSCF将可以重新得到对话标识符。这样，它就可以知道这个新的Call-ID实际上是与早先收到的INVITE请求相关的。S-CSCF这时就可以正确地返回到向AS发出INVITE请求后的位置。

在本例中我们不再进一步分析AS作为B2BUA的情况：

INVITE sip:theresa@home2.hu SIP/2.0
Via: SIP/2.0/UDP sip:scscf1.home1.fr;branch=9sc2as2tb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Route: <sip:as2.home1.fr;lr>
Route: <sip:scscf1.home1.fr;lr>;dia-id=6574839201
Record-Route: <sip:scscf1.home1.fr;lr>
Record-Route: <sip:pcscf1.visited1.fi;lr>

3、 从AS返回S-CSCF

收到INVITE请求后，AS会：

- ✓ 删除Route消息头最顶端的条目，它指向AS。

- ✓ 根据请求中的信息来提供服务。
- ✓ 可能依照[RFC3261]更改请求消息(例如增加另一个消息头)。
- ✓ 把自己的地址放入Via列表的顶端。
- ✓ 决定是否希望接收此对话的后续请求——如果希望，它就将自己的地址放在Record-Route列表的顶端(在本例中，我们假设AS希望将自己保留在Route头中)。
- ✓ 根据Route消息头中最顶端的地址将INVITE请求路由回S-CSCF。

INVITE请求现在如下所示：

```
INVITE sip:theresa@home2.hu SIP/2.0
Via: SIP/2.0/UDP sip:as2.home1.fr;branch=vas2tb
Via: SIP/2.0/UDP sip:scscf1.home1.fr;branch=9sc2as2tb
Via: SIP/2.0/UDP pcscf1.visited1.fi;branch=9pctb
Via: SIP/2.0/UDP [5555::1:2:3:4]:1357;branch=8uetb
Route: <sip:scscf1.home1.fr;lr>;dia-id=6574839201
Record-Route: <sip:as2.home1.fr;lr>
Record-Route: <sip:scscf1.home1.fr;lr>
Record-Route: <sip:pcscf1.visited1.fi;lr>
```

4、 S-CSCF继续评估其他的过滤准则

当再次收到INVITE请求后，S-CSCF检查过滤准则3，因为SIP方法不是SUBSCIBE(如SPT所示)，所以准则3不匹配。因此，S-CSCF继续执行正常路由过程，如11．3．3．3节所介绍(即它将INVITE请求发往Theresa归属网络的I-CSCF)。

由于服务提供会使得路由过程更加复杂，因此本例始终没有过多涉及；此处增加的Via、Rome和Record-Route头也同样不再出现在本例的后续部分。

5.4.3.9 相关标准

IMS服务提供体系的进一步介绍参见：

3GPP TS 23．218：IP Multimedia(IM)session handlin9；IM call model；Stage 2

5.4.4 媒体控制

5.4.4.1概述

由于UE通常是通过无线链路附着到IMS的，带宽资源稀少，因此需要谨慎处理。双方交换对于会话中使用的媒体和编解码方案的倾向意见，直到一致同意媒体流的某个特定组合，并且每个媒体流使用同一种编解码方案。

由于媒体流的路由不经过任何CSCF，因此IMS网络需要对资源的预留进行授权。这样，任何时候当P-CSCF收到对话中第一个发往UE的SIP消息时，它会要求PDF(策略决策功能)生成一个媒体授权令牌(见图5-21)。这个令牌被加入到INVITE请求中并发往Theresa UE。Tobias UE也会在183(会话进行中)响应中得到它的本地令牌。

在SDP提议／应答过程中，本地P-CSCF能够告诉LIE将特定的媒体流聚合成一组填入一个媒体PDP上下文中，或者为某些媒体流保留单独的媒体PDP上下文——这通过SDP媒体行分组

机制实现。

除此之外，网络运营商可能希望限制每个UE可以使用的媒体类型和编解码方案。为了实现这个目的，P-CSCF和S-CSCF检查INVITE请求中的SDP信息。如果某个CSCF认为不允许使用某个媒体类型或编解码方案，它就会给Tobias UE发一个拒绝消息。在本例中，我们假设不会发生这种情况。

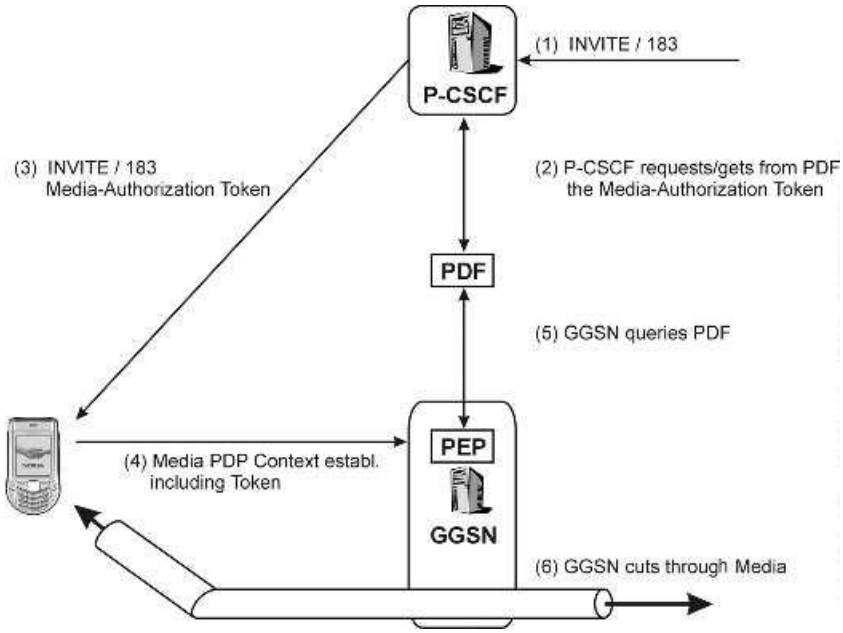


图5-21 媒体授权信息的传输

SDP提议 / 应答过程完成之后，各UE就可以开始为商定的媒体预留资源了。在GPRS中，当使用一个专用的信令PDP上下文时，预留资源意味着每个LIE现在可以为媒体建立一个或多个次PDP上下文。在每个建立媒体PDP上下文的请求中，UE把从P-CSCF处得到的媒体授权令牌包含进来。

GGSN接到一个新的PDP上下文请求，首先把令牌返回给生成它的PDF。它还在给PDF的消息中包含所请求的会话参数。PDF和策略实施点(PEP)对资源预留请求进行检查。接下来，GGSN和UE之间建立起所请求的媒体PDP上下文。

未来其他类型的接入网络也会定义类似的过程，这里只是使用GPRS作为一个例子。

5.4.4.2 媒体授权

当Theresa的P-CSCF收到INVITE请求后，会请求PDF生成媒体授权令牌。

P-CSCF会在INVITE请求中添加一个P-Media-Authorization消息头，包含所收到的令牌，并将请求发往Theresa UE。

```
INVITE sip:[5555::5:6:7:8]:1006 SIP/2.0
P-Media-Authorization: example-auth-token2
```

Theresa UE将使用这个令牌来建立媒体PDP上下文，或者建立双方UE商定的多个媒体流的PDP上下文。

随后，Tobias的P-CSCF将收到183(会话进行中)响应，它也会向它的PDF申请一个媒体授权令牌。它将该令牌包含在P-Media-Authorization消息头中，并发给Tobias UE。

SIP/2.0 183 Session in Progress
P-Media-Authorization: example-auth-token1

由于每个UE的资源预留和授权都是本地事件，这两个令牌是不同的。

每个UE对于由一个INVITE请求而生成的所有媒体会话，只会收到一个令牌。不论UE建立多少个PDP上下文，在请求资源时总是使用这同一个令牌。因此，UE完全不需要了解令牌的内容和编码，它只需要在SIP消息中收到令牌，然后把它放在PDP上下文激活请求(ACTIVE PDP CONTEXT REQUEST)中。

5.4.4.3 媒体行的分组

关于QoS资源授权的一节已经包含了一个媒体行分组的例子。本章的例子中我们假设两端的分组是不同的。

5.4.4.4单一预留流

在PRACK请求里的第二个SDP提议中，Theresa的P-CSCF会向她的UE发送如下与媒体行分组有关的信息：

```
v=0
o=- 1357924 1357924 IN IP6 5555::1:2:3:4
s=-
c=IN IP6 5555::1:2:3:4
t=907165275 0
a=group:SRF 1
m=audio 3458 RTP/AVP 97 98
a=mid: 1
a=rtpmap:97 AMR-WB
a=rtpmap:98 telephone-event
m=video 3400 RTP/AVP 99
a=mid: 1
a=rtpmap:99 H.261
m=video 0 RTP/AVP 98
```

SDP头部的a行定义了一个单一预留流(SRF)组，号码为“1”：即本组中听有的媒体流都进入到同一个PDP上下文中。

两个媒体行(一个音频和一个视频)都跟随了一个a行，指示了媒体流标识(MID)，两处都设置为上述定义的分组号码“1”。这意味着P-CSCF指示Theresa JE将两个媒体流都分组到一个PDP上下文中。

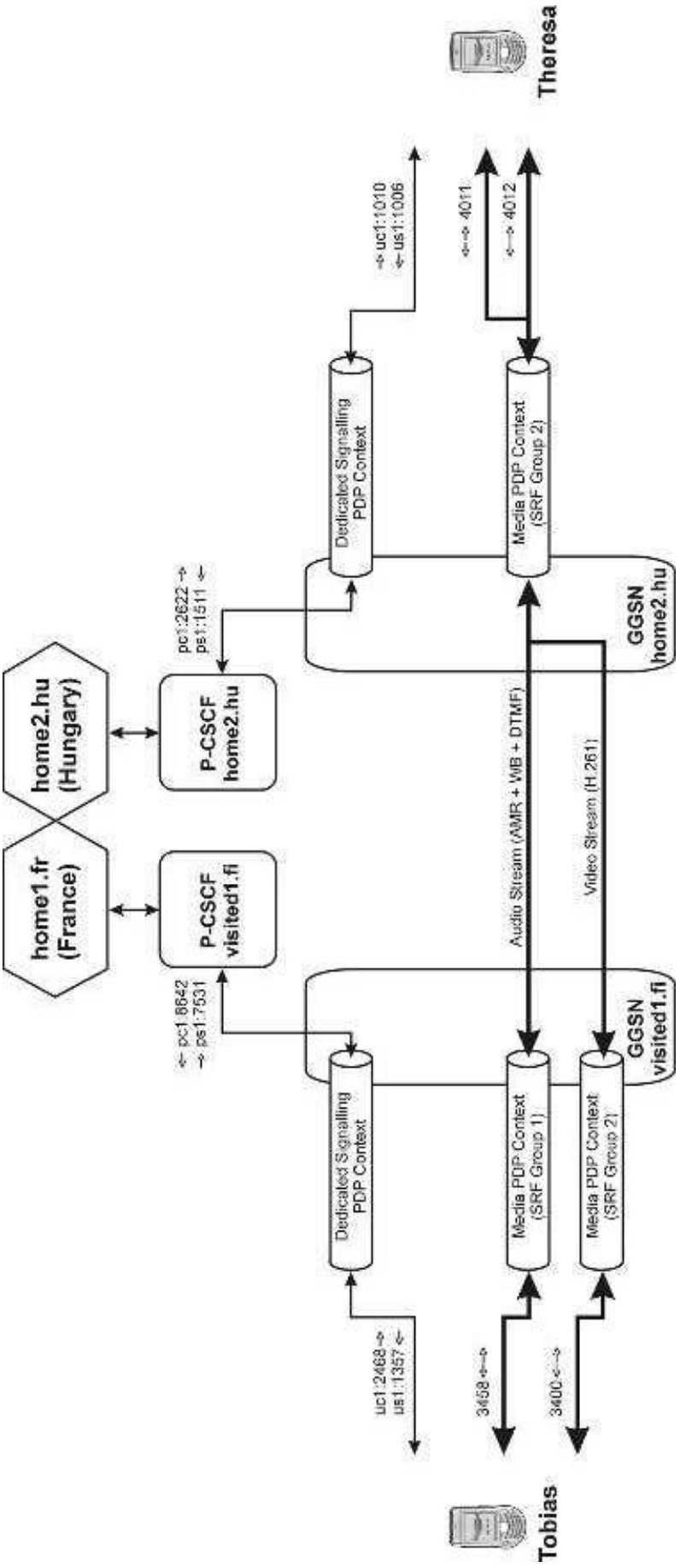
5.4.4.5 分离的流

芬兰的P-CSCF要求分离的媒体流，因此它将如下与媒体行分组有关的信息忝加到SDP应答中，该应答包含在对PRACK请求的200(OK)响应中发往Tobias UE。

```
v=0
o=- 1357924 1357925 IN IP6 5555::5:6:7:8
```

```
s=-
c=IN IP6 5555::5:6:7:8
t=907165275 0
a=group:SRF 1
a=group:SRF 2
m=audio 4011 RTP/AVP 97 98
a=mid: 1
a=rtpmap:97 AMR-WB
a=rtpmap:98 telephone-event
m=video 4012 RTP/AVP 99
a=mid: 2
a=rtpmap:99 H.261
m=video 0 RTP/AVP 98
```

示SRF组为“1”，视频流指示SRF组为“2”，Tobias UE必需为每个媒体流预留单独的媒体PDP上下文(见图5-22 例子情景中的媒体流和传输)。


Theresa
uc1:1010
us1:1006
4011
4012
Dedicated Signalling PDP Context
Media PDP Context (SRF Group 2)
pc1:2622
ps1:1511
home2.hu (Hungary)
P-CSCF home2.hu
GGSN home2.hu
home1.fr (France)
P-CSCF visited1.fi
Audio Stream (AMR + WB + DTMF)
Video Stream (H.261)
pc1:8642
ps1:7531
GGSN visited1.fi
Dedicated Signalling PDP Context
Media PDP Context (SRF Group 1)
Media PDP Context (SRF Group 2)
uc1:2468
us1:1357
3458
3400
Tobias

5.4.4.6 媒体策略

P-CSCF和S-CSCF可以拒绝SDP提议的特定媒体类型或编解码方案。这可能是由于运营商的策略。一个可能的原因是运营商不允许使用任何未知的媒体类型或未知的编解码方案,.因为网络可能无法对这些媒体计费。

如果CSCF发现SDP提议中包含了不支持的媒体类型或编解码方案，它就会使用488(此处不接受)响应来拒绝该请求，并在响应正文中指出所支持的媒体类型。

本例的场景中，假设上述情况都不会发生。图5-23展示了一种最差的情况，路由中每个CSCF都不支持特定的媒体元素，实际中这样的极端情况不太可能发生。

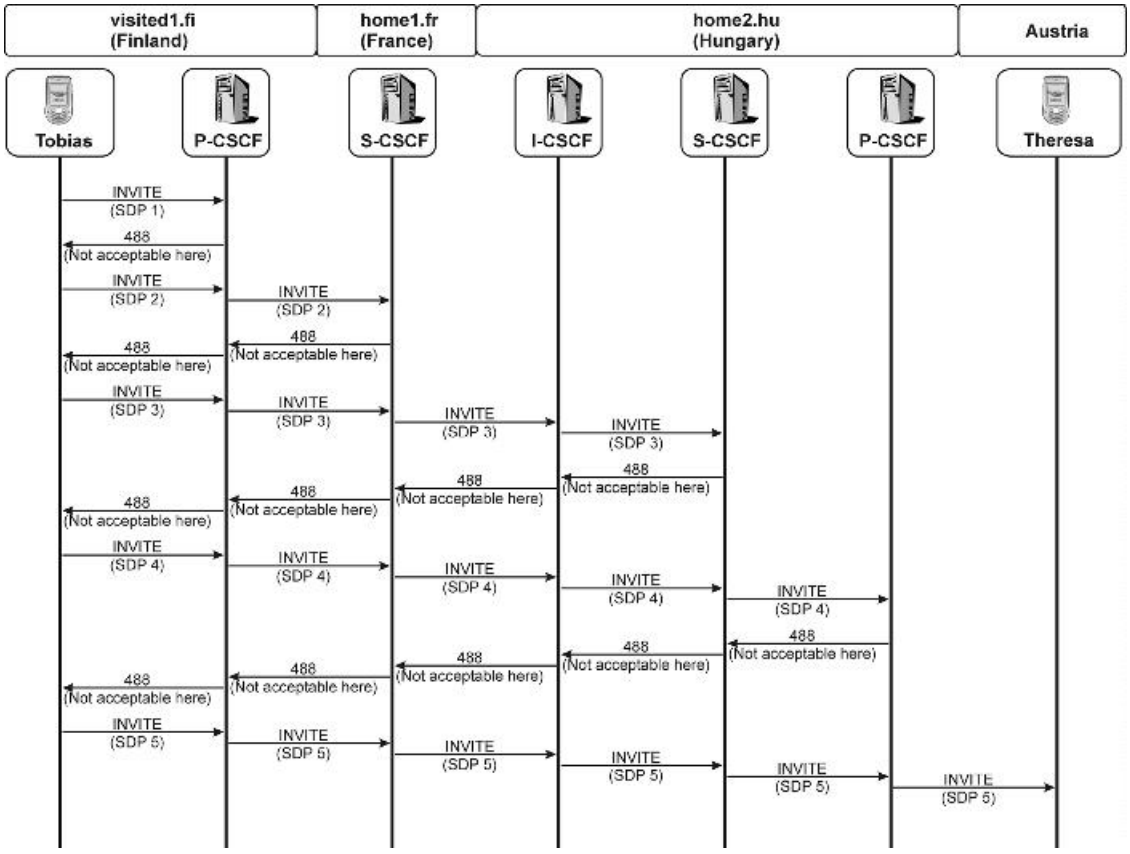


图5-23媒体策略中的最差情况

5.4.4.7 相关标准

与6.4.4节有关的规范有：

- ✓ RFC3313 Private Session Initiation Protocol(SIP)Extensions for Media Authorization.
- ✓ RFC3388 Grouping of Media Lines in the Session Description Protocol(SDP)
- ✓ RFC3524 Mapping of Media Streams to Resource Reservation Flows.

5.4.5 会话的释放

5.4.5.1 用户发起的会话释放

当然，Tobias和Theresa会在某个时间终止他们的交谈。我们假设Theresa在维也纳Stephansdom遇到了一个朋友，因此不得不向她的弟弟告别(见图5-24)。她会按下手机上的红色按键挂掉呼叫。

这样，她的UE会生成一个BYE请求，沿着与其他后续请求相同的路径发给Tobias UE。与此同时，她的UE还会释放为本次会话建立的媒体PDP上下文。

BYE sip:[5555:1:2:3:4]:1357 SIP/2.0
Route: <sip:pcscf2.home2.hu:1511;lr>
Route: <sip:scscf2.home2.hu;lr>
Route: <sip:scscf1.home1.fr;lr>
Route: <sip:pcscf1.visited1.fi;lr>
To: "Your Brother" <sip:tobi@brother.com>;tag=veli
From: "My beloved Sister" <sip:Theresa@sister.com>;tag=schwester

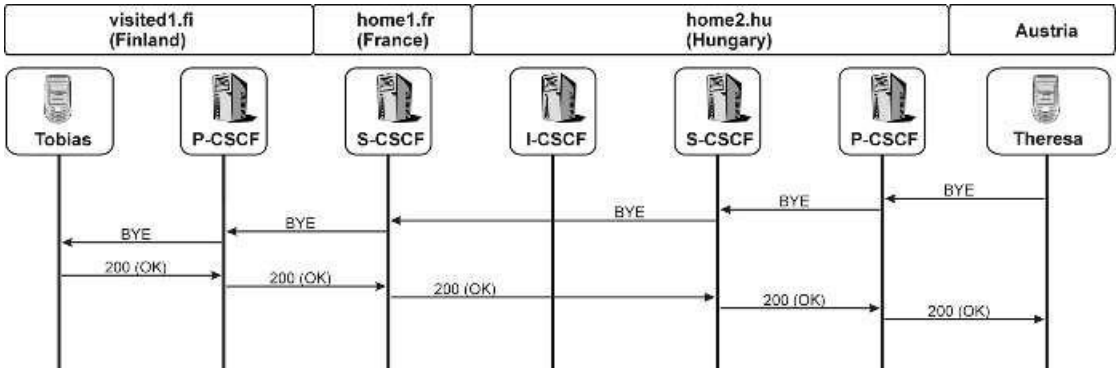


图5-24 Theresa释放会话

我们从这个BYE请求中可以看到，TO和From头中的信息被相互交换了，因为这次请求是从Theresa一侧发出的。

Tobias UE在收到BYE请求后会立刻释放它的PDP上下文，它还会向Theresa返回一个200(OK)响应来应答BYE请求。沿途的四个CSCF和所有AS都会清除与本次会话有关的所有对话状态和信息。

5.4.5.2 P-CSCF执行网络发起的会话释放

有些情况下，CSCF之一有可能需要发起会话释放，而不是由用户发起。

例如，当Theresa的P-CSCF发现Theresa UE已经离开了无线覆盖从而失去了与接入网络的连接时，它需要释放正在进行的会话(见图5-25)。这种情况下P-CSCF需要代表Theresa发出BYE请求。

BYE sip:[5555:1:2:3:4]:1357 SIP/2.0
Route: <sip:scscf2.home2.hu;lr>
Route: <sip:scscf1.home1.fr;lr>
Route: <sip:pcscf1.visited1.fi;lr>
To: "Your Brother" <sip:tobi@brother.com>;tag=veli
From: "My beloved Sister" <sip:Theresa@sister.com>;tag=schwester

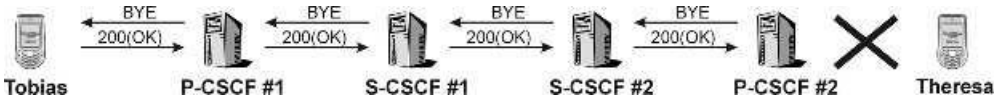


图5-25 P-CSCF终止一个会话

5.4.5.3 S-CSCF执行网络发起的会话释放

有时Tobias的S-CSCF需要停机，如Tobias在使用预付费卡并且余额已经用光。这种情况下，Tobias的S-CSCF需要向Tobias UE发送一个BYE请求来释放会话。

BYE sip:[5555:1:2:3:4]:1357 SIP/2.0
Route: <sip:pcscf1.visited1.fi;lr>
To: "Your Brother" <sip:tobi@brother.com>;tag=veli
From: "My beloved Sister" <sip:Theresa@sister.com>;tag=schwester
S-CSCF 终止一个会话

另一个BYE请求发给Theresa UE。
BYE sip:[5555:1:2:3:4]:1006 SIP/2.0
Route: <sip:scscf2.home2.hu;lr>
Route: <sip:pcscf2.home2.hu;lr>
From: "Your Brother" <sip:tobi@brother.com>;tag=veli
To: "My beloved Sister" <sip:Theresa@sister.com>;tag=schwester

为了正确生成BYE请求中的Route消息头，P-CSCF和S-CSCF需要跟踪任何一个对话建立过程中的所有路由信息。

5.5 SIP

本节并不提供完整的会话初始化协议(SIP)规范，而是旨在指出SIP在应用于IP多媒体子系统(IMS)中时需重点关注的方面。例如，本章并不讨论SIP实体在URI(统一资源标识符)中应如何使用maddr参数，也不解释SIP实体在某个错误发生时所采取的动作。SIP的完整规范请参见[RFC32611]。

5.5.1 背景

SIP是一种在IP网络中建立、修改和终止多媒体会话的应用层协议，它是因特网工程任务组(IETF)在不断进行标准化的多媒体协议体系的一部分。其应用包括但不限于语音、视频、游戏、消息、呼叫控制和在线状态(presence)等。

IP上的会话信令协议思想可以追溯到组播会议概念刚出现的1992年。SIP本身起源于1996年后期，当时是作为IETF Mbone(组播骨干网)的一个组成部分，该网络是架设于公众因特网之上的一个组播实验网。其中SIP被IETF用来发布多媒体内容，包括mTF会议，专题讨论会和大型会议等。由于其简单性和可扩展性，SIP后来被采纳为IP电话(VoIP)的信令协议，并于1999年最终成为IETF标准[RFC2543]。之后SIP在互操作性、设计的优化和新特性等方面

得到了进一步增强。为清晰起见，原文档进行了重写，由此形成的新协议基本上与[RFC25431]保持后向兼容。新文档于2002年取代了 [RFC2543]，成为新标准[RFC3261]。

5.5.2 设计原则

作为IETF工作进程中的一部分，SIP基于超文本传输协议(HTTP)和简单邮件传送协议(SMTP)。图5-26给出了SIP在协议栈中的位置。

SIP的设计旨在实现以下目标:

独立于传输协议——可以在可靠(TCP、SCTP)和不可靠(UDP)的协议上运行。

请求的路由——直接路由(为了性能)或代理路由(为了控制)。

信令和媒体描述相分离——以便可以增加新的应用或媒体。

可扩展性。

个人的移动性。

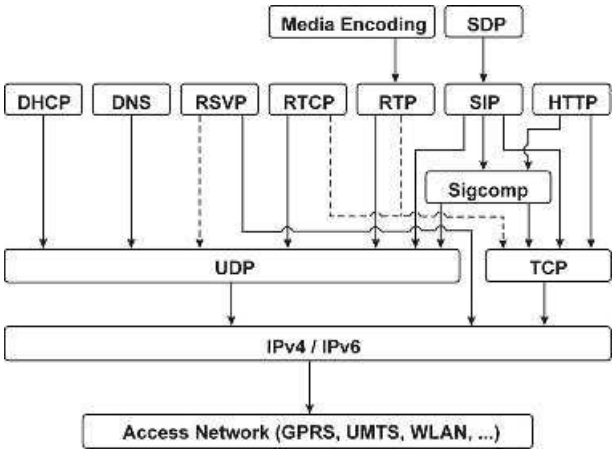


图5-26协议栈

5.5.3 SIP体系结构

SIP中的组成元素可分为用户代理(UA)和中间服务器。在理想情况下，两个端点(或UA)间的通信并不需要中间服务器的参与即可完成。但现实并非总是如此，因为网络管理者和业务提供者可能希望对其网络内的业务流有所了解。

图5-27描述了一种典型的网络结构，称为“SIP梯形(trapezoid)”。

SIP UA或终端构成对话的端点:它发送或接收SIP请求和响应，是多媒体流的终点。此外它通常是用户设备(UE),即终端上的一个应用或一个专用的硬件设备。UA由以下两部分组成:

用户代理客户端(UAC)——发起请求的主叫方应用。

用户代理服务器(UAS)——接受、重定向或拒绝请求，并代表用户给到来的请求发送响应。

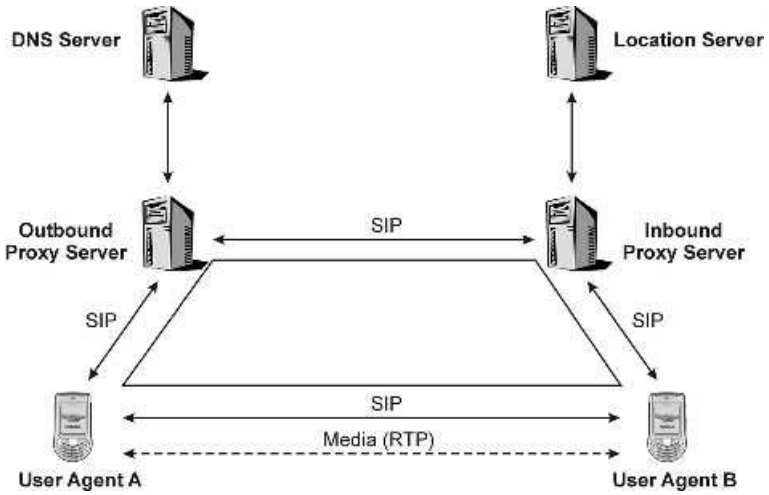


图5-27 SIP梯形

网关是UA的特例。

SIP中间服务器是SIP消息在到达其最终目的地前所经过的逻辑实体,这些中间服务器用于对请求进行路由和重定向。这些服务器包括:

代理服务器(Proxy Server)——接收和转发SIP请求。可解释或重写SIP消息的某些部分，包括消息正文。这些重写不会打乱端点处的请求或对话的状态。代理服务器也可同时向多处发送请求。这样的实体被标识为“分叉代理”。分叉可以是并行的或是串行的。一共有三种代理服务器类型:

对话状态感知代理(Dialog-statefull proxy)——如果一个代理从起始请求(INVITE request)到终止请求(BYE request)期间保持各个对话的状态，则为对话状态感知代理。

事务状态感知代理(Transaction-statefull proxy)——在处理请求的过程中对客户端和服务器的事务状态机进行维护的代理。

无状态代理(Stateless proxy)——将收到的每个请求向下游转发和将收到的每个响应向上游转发的代理。

重定向服务器(Redirect Server)——将请求地址映射为新地址。它对请求进行重定向，但并不参与事务的处理。

位置服务器(Location Server)——跟踪用户的位置。

登记员服务器(Registrar Server)——接受REGISTER请求的服务器。这类服务器用于存储用户登记的地址(SIP地址)与用户当前所在的或用户希望用于接收请求的主机地址之间的明确绑定关系。

此外还有两个给SIP用户提供服务的元素:

应用服务器(Application Server)——AS是在网络中为终端用户提供服务的实体，典型例子如在线状态(presence)和会议服务器。

背靠背用户代理(back-to-back-user-agent)——正如其名字所述，一个B2BUA中的UAS和UAC粘合在一起。UAS和正常的UAS一样终止请求；而UAC发起一个新请求，该请求与UAS端收到的请求具有一定的相关性，但不是任何协议指定的链路。该实体基本上类似于一个代理(Proxy)，但打破了代理(Proxy)修改请求时所遵守的所有准则。

5.5.4 消息格式

如图5-28所示，SIP消息由三部分组成，即:开始行(start line)，消息头(header)和正文(body)。

开始行的内容根据SIP消息是请求还是响应而有所不同。若是请求，则称为“请求行”；若是响应，则称为“状态行”。

SIP请求的例子如下所示:

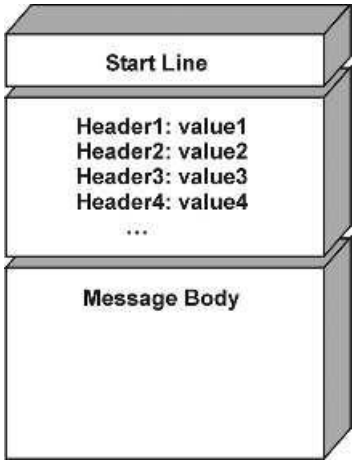


图5-28 SIP消息格式

```
INVITE sip:bob.smith@nokia.com SIP/2.0
Via: SIP/2.0/UDP cscf1.example.com:5060;branch=z9hG4bK8542.1
Via: SIP/2.0/UDP [5555::1:2:3:4]:5060;branch=z9hG4bK45a35h76
Max-Forwards: 69
From: Alice <sip:alice@nokia.com>;tag=312345
To: Bob Smith <sip:bob.smith@nokia.com>
Call-ID: 105637921
CSeq: 1 INVITE Contact: sip:alice@[5555::1:2:3:4]
Content-Type: application/sdp
Content-Length: 159
[body]
```

5.5.4.1 请求

通过开始行可以识别一个SIP消息是请求还是响应。如前所述，请求中的开始行通常被称为请求行，由三个部分组成:方法名、请求URI和协议版本。它们以上述顺序出现并由单个空格符分开。请求行本身以一对回车换行符(CRLF)结束。

方法——方法表示请求的类型。在基本SIP协议[RFC3261]中定义了六个方法:INVITE请求、CANCEL请求、ACK请求和BYE请求用于会话的创建、修改和终止；REGISTER请求用于对用户的联系信息进行注册；OPTIONS请求用于对服务器及其能力进行查询。其他方法都是作为对[RFC3261]的扩展。

请求URI-一请求URI用来标识所请求的资源的SIP或SIPS URI。

协议版本——目前的SIP版本为2.0。所有符合[RFC3261]的请求都必需包含这个版本信

息，形式为“SIP/2.0”。

5.5.4.2 响应

SIP响应可以通过查询开始行来与SIP请求区分。如前所述，响应中的开始行经常被称为状态行，由三个部分组成:协议版本、状态码和原因短语。它们以该顺序出现并由单个空格符分开。状态行本身以一对CRLF符号结束。

版本——与请求行中的协议版本相同。

状态码——状态码是由三个阿拉伯数字组成的码,用来标识响应种类,指示请求的结果。

原因短语一—这是一个自由的文本域，给状态码提供简短的描述，主要针对个人用户。

状态码可以分为六类(从2xx到6xx类是最终响应):

1xx——临时的 / 信息性响应。表明请求已收到，接收方正在继续处理该请求。

2xx——成功响应。请求已成功收到、理解并被接受。

3xx——重定向响应。请求方需要采取进一步动作以完成请求。

4xx——客户端错误响应。该请求包含语法错误，也可指示服务器不能实现请求所提的要求。

5xx——服务器错误响应，服务器在对有效请求进行处理时失败，是服务器的错误。

6xx——全局失败响应。请求不能在任何一个服务器上得到满足，产生该响应的服务器需要知道有关用户的确切信息。

“xx”是表明响应确切种类的两位数字。例如，一个“180”的临时响应表明对端的振铃，而一个“181”临时响应则表明呼叫正在被中转。

5.5.4.3 消息头字段

消息头字段包含与请求有关的信息，例如请求的发起者、请求的接收者和呼叫标识。消息头字段也可指示消息正文的特征。

每个消息头字段以一对CRLF结束。一个SIP消息的整个消息头部分也以CRLF结束。

消息头字段的格式如下:

Header-name: header-value

有些消息头是每个SIP请求和响应都必须具有的，这些消息头及其格式列举如下:

TO消息头	TO:SIP-URI(; 参数)
From消息头	From:SIP-URI(; 参数)
Call-ID消息头	Call-ID:惟一的id
CSeq消息头	CSeq:数字　方法
Via消息头	Via:SIP/2.0/[传输协议] 发送者地址(; 参数)
Max-Forwards消息头	Max-Forwards:数字
Contact消息头	Contact:SIP-URI(; 参数)

Contact头对于创建对话的请求来说是必须的，Max-Forwards头的典型值为70。注意，参数两侧的括号表示参数是可选的，括号不是消息头语法的一部分。凡是(; 参数)出现时即

表明消息头里可以出现多个参数，参数之间用分号隔开。Via头的传输协议可以是用户数据报协议(UDP)、传输控制协议(TCP)或传输层安全(TLS)协议。

5.5.4.4 消息正文

消息正文(有效负荷)可携带任何基于文本的信息，而请求的方法和响应的状态码决定了消息正文该如何解释。

当描述一个会话时，典型的SIP消息正文是一个会话描述协议(SDP)消息。

5.5.5 SIP URI

SIP URI遵从与电子邮件地址相同的格式，即“用户名@域名”。有如下两种URI模式:

Sip:bob.smith@nokia.com是一个SIP URI, 这是最通用的格式，[RFC2543]中有介绍。

sips:bob.smith@nokia.com是一个SIPS URI，这种新模式在[RFC3261]中有介绍，要求使用TCP上的TLS来进行安全的传输。

存在两种SIP和SIPS URI：

记录地址(AOR)——这个SIP地址用于标识一个用户。该地址几乎可以同电话号码一样的方式发布给公众，例如sip:bob.smith@nokia.com(需要DNS SRV记录来定位nokia.com域的SIP服务器)。

主机的全合格域名(FQDN)或IP地址(标识一个设备)----例

如:sip:bob.smith@127.233.4.12或sip:bob.smith@pc2.nmp.nokia.com(不需要路由解析)。

SIP URI的格式为:“sip:用户信息@主机端口[参数][消息头]”，SIPS URI遵从与SIP URI完全相同的语法。

用户信息——用户名或电话号码。

主机端口——域名或数字形式的网络地址和端口。

参数——定义具体的URI参数，例如传输(transport)协议、生存时间等。

消息头——一个很少用到的格式，用来传递额外信息。

下面是一些SIP URJ的例子。

sip:bob.smith@nokia.tom

sip:bob@nokia.corn; transport=tcp

sip:+1-212-555-1234@gw.com; user=phone

sip:root@136.16.20.100:8001

sip:bob.smith@registrar.com; method=REGISTER

5.5.6 tel URI

电话URI(tel URI)用于标识占用了某个电话号码的资源。SIP允许将请求送往tel URI，这就意味着SIP请求的请求URI可以包含一个tel URI。

tel URI可包含一个全球号码或一个本地号码。全球号码遵从E.164号码的规则，以“+”

开始；而本地号码遵从本地私有编号计划。本地号码需要有电话上下文(phone-context)参数，用于标识本地号码的上下文(拥有者)，也就是号码范围。这就使得该号码是全球惟一的。上下文可以用一个全球号码或域名来表示:前者必须包含一个有效的、被本地号码发行者所拥有的全球号码；后者必须包含一个有效的、已授权给本地号码发行者的域名。下面是一些tel URI的举例:

全球号码———-tel:+358-9-123-45678。

具有域名上下文的本地号码———-tel:45678;phone-context=example.com。

具有全球号码上下文的本地号码——tel:45678; phone-context=+358-9-123。

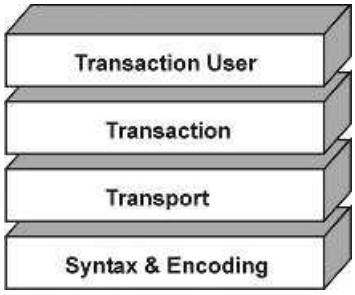
注意，tel URI允许在号码中含有如连字号“-”之类的视觉分隔符，以提高可读性。tel URI的参数之间用分号“；”分隔。[RFC3966]中可以找到所有tel URI的语法。

5.5.7 SIP结构

SIP是一个分层协议，其中不同模块功能相对独立，各层间仅保持松散耦合。图5-29清楚地展示了所采用的分层方法。

5.5.7.1 语法和编码层

协议的第一层(最底层)是语法和编码层。编码采用增强的巴柯斯范式(BNF)语法，[RFC3261]给出了其完整描述。



5.5.7.2 传输层

第二层是传输层。正如其名称所示，该层起到告知客户端如何发送请求和接收响应以及服务器如何接收请求和发送响应的作用。传输层与SIP实体的套接字(socket)层密切相关。

5.5.7.3事务层

第三层是事务层。在SIP术语中，一次事务是指客户端发送到服务器的一条请求，以及从服务器送回客户端的所有对该请求的响应。事务层处理响应与请求之间的匹配。应用层的重传和应用层的事务超时也都在该层处理，并依赖于所使用的传输协议。客户端事务发送请求并接收响应，而服务器事务则接收请求和发送响应。事务层利用传输层来发送和接收请求及响应。

事务层有四个事务状态机，每个事务状态机有其自身的定时器、重传规则和终止规则。

INVITE客户端事务。

非INVITE客户端事务。

INVITE服务器事务。

非INVITE服务器事务。

5.5.7.4 事务用户层

第四层是事务用户(TU)层，该层创建客户端和服务器事务。当TU希望发送SIP请求时，它创建一个客户端事务实例(instance)，并把目的IP地址、端口号和所使用的传输协议等放在请求中一起发送。TU被定义为UAC核和UAS核，或简称为UAC和UAS。UAC使用事务层创建和发送请求并接收响应，而UAS使用事务层接收请求并创建和发送响应。

有两个因素可以影响TU行为:一个是SIP消息中的方法名，另一个是请求的对话状态。

除了这两个因素外，Tu以标准方式工作。相关内容在以下各部分进行介绍。

1、UAC行为

对于在对话以外到达的请求，UAC需要采取的步骤包括填写请求URI、TO消息头、From消息头、Call-ID消息头、CSeq消息头和Via消息头。其他消息头，例如Require头(用于指示UAC要求的SIP扩展)和Supported头(用于指示UAC支持的SIP扩展)，也可以填入其中。如果该请求要创建一个对话或要进行注册绑定，则必须加入Contact消息头。任何其他的内容也可在这一阶段填加，包括消息正文。当SIP请求中出现消息正文时，Content-type和Content-length消息头也必须填加。

TO消息头填写为目标AOR(AOR类似于名片地址)。

From消息头填写为发送者AOR，此外还填加一个标签(tag)参数。标签是用于标识对话的一种手段。

Call-ID消息头填写为一个惟一的标识符。

CSeq消息头用来标识事务的先后顺序。对于对话以外的请求，CSeq号码是任意数值。包含两部分，一个CSeq数值和一个方法名，二者由空格分开。方法部分填写为请求行中的方法。

Max-Forwards消息头用来限制请求所经过的跳数，以避免回环，其典型值为70(表示跳数)。每经过一跳该值递减1。

Via消息头包含两块关键的信息:传输协议和响应消息应该发往的地址。协议名称和版本号总是设为SIP和2.0。Via消息头包含一个标识事务的分支(branch)参数，用于将请求与响应相匹配。该参数必须是惟一的。符合本规范的分支参数值总是以字符串“29hG4bK”开头。

Contact消息头一般填写为发起该请求的主机地址的URI。

请求URI通常与TO消息头中的数值相同。REGISTER请求是一个特例，其中的请求URI填写为登记员地址。UAC可以有一个预置的路由集，即UAC希望请求在到达目的地之前途经的中间节点集合，包括出站代理(outbound-proxy)。该路由集放在请求消息的Route 头中。在这种情况下，请求URI的值可能会根据Route头的最顶端是否包含“宽松路由(loose-route)”参数而有所区别。

UAC还对它所发出的请求的响应进行处理。这些响应可以是超时错误响应或SIP成功或失败响应，包括重定向响应(3xx)。

2、 UAS行为

对于在对话以外到达的请求，UAS检查请求中的方法以进行识别，并检查请求URI和To信息头以确定自己是否为该请求的目的地。如果两个检查中的任意一个失败，则返回一个错误响应。

然后UAS判断是否有扩展的要求，如果它不能满足扩展要求则返回一个错误。如果能够满足，则UAS继续处理该请求，检查和处理请求的内容(消息正文)。

如果以上步骤均成功，UAS就能采用UAC支持的所有扩展(如Supported消息头所指示)。随后的请求处理就取决于具体的方法了。

一旦UAS处理完请求后，它就产生一个响应，该响应可以是临时的或是最终的。针对一个请求可以发送多个临时响应，但最终响应只会发送一个。一般来说，只有在对INVITE请求进行响应时才发送临时响应。

当产生一个响应时，响应中的From消息头、Call-ID消息头、CSeq消息头、Via消息头和TO消息头等都是从请求消息中复制过来的。请求中Via消息头的顺序必须保持不变。

如果请求中包含有TO消息头的标签参数，则不允许再产生新标签。然而，如果请求中的TO消息头不含有标签，则UAS必须在响应中给TO消息头添加一个标签。对于“100”临时响应来说，TO消息头标签并不是必需的。该标签作为标识一个对话的多个组件之一，它还被分叉代理用来标识UAS。

5.5.8 注册

SIP支持用户移动性(user mobility)和发现(discovery)的概念。用户可以通过将自己的AOR与某个主机地址进行明确绑定，使自己可以被联络到。这就使用户移动性成为可能，因为用户可以通过支持SIP的任何设备进行注册，包括个人计算机、无线设备和蜂窝电话。

为一个SIP请求发现其希望到达的接收者，是典型的SIP中间服务器的功能。例如，用户创建一个与登记员之间的绑定,该登记员作为去往存储所有绑定记录的位置服务器的前置单元，当一个代理服务器收到的请求是发往其负责区域内的节点时，它就与这个位置服务器联系，以获取接收者的确切位置。

用户通过在TO消息头中放置其AOR和在Contact消息头中放置主机地址来形成一个绑定。

用户通过从每个设备发送一个REGISTER请求，就可以实现同时从多个设备进行注册。同样,用户可以从同一个设备创建多个绑定,这可以通过发送一个与AOR有多个绑定的REGISTER请求来实现。要做到这一点，用户会在REGISTER请求中加入多个Contact消息头。

用户可以通过一个称为“注册领取”的过程来发现当前其AOR的所有绑定，这是通过发送一个没有Contact消息头的REGISTER请求来实现。登记员在对REGISTER请求的响应中返回当前所有绑定。在响应中，每个绑定都有一个它自己的Contact消息头。

SIP注册从本质上讲是软状态，这意味着注册的绑定必须周期性刷新。一个绑定的过期时间通过注册实体在Contact消息头里使用的过期参数来指示。如果该参数没有出现，则登记员会认为过期时间为lh。若UA没有刷新或明确清除该绑定，则当绑定过期时，登记员将直接将其删除。uA可以通过发送一个REGISTER请求来明确地清除一个绑定，该请求中对要清除

的绑定添加一个Contact消息头，该Contact消息头包含的过期参数值为0。

5.5.9 对话

对话是通信双方之间的一种SIP关系，它提供了在通信双方之间进行路由和消息排序时所依据的必要的状态信息。

对话使用对话ID来标识，UA用它来跟踪属于同一个对话的消息。对话ID由呼叫ID、本地标签和远端标签组成。对于UAC来说，本地标签就是在创建对话的初始请求的From消息头中的标签，远端标签就是创建对话的响应的TO消息头中的标签。对于UAS来说，本地标签就是在创建对话的响应的TO消息头中的标签，远端标签是创建对话的初始请求的From消息头中的标签。对于任意一端发出的该对话中的后续请求，本地标签放在From消息头中，而远端标签放在TO消息头中。

请注意UAS也要接收From消息头中没有任何标签的请求，这时认为标签中包含了一个空值。

在一个对话中创建、发送、接收和处理消息时需要用到对话的状态。该状态由对话ID、本地序列号、远端序列号、本地URI、远端URI、远端目的地、一个称为“安全”标记的布尔标记以及一个路由集组成。

当某个对话处于“早期”状态时，它就称为“早期对话”。这在对初始请求的临时响应到达UAC时发生，这时一个对话就创建起来。当“2xx”成功响应到达时，对话就进入“确定”状态。若“2xx”类响应以外的其他最终响应到达，或根本没有响应到达时，早期对话便终止。

当UAS用表示成功的最终响应对一个请求进行应答时，它必须将出现在请求中的所有Record-Route消息头复制到响应中，并维持它们的顺序不变。然后UAS将Record-Route消息头中的那些URI存储为路由集，并维持其顺序不变。如果没有出现Record-Route消息头，则路由集置为空。该路由集合即使是空的，仍将在对话的后续部分中保持不变。这就意味着本对话中各请求消息的其他Record-Route消息头不会覆盖现有的路由集。

如果消息途径的中间服务器希望对话期间内所有从UAC发往UAS或者从UAS发往UAC的后续请求的信令仍然经过自己，它就在请求消息中添加一个Record-Route消息头。

UAS还必须在响应消息中添加一个Contact消息头，以指示对话内后续请求的目的地址。

UAS处的对话状态构成如下:

如果到来的请求是通过TLS传输的，且请求URI包含一个SIPS URI，则“安全”标记设为真；否则设为假。

远端目的地设置为请求消息中Contact消息头内的URI。

远端序列号设置为请求消息中CSeq头内的序列号。

本地序列号在此阶段保持为空，当远端发送一个属于本对话内的请求时再填写。

远端URI设置为From消息头中的URI。

本地URI设置为TO消息头中的URI。

对话ID如上所示来创建。

路由集如上所示来设置。

UAC必须在创建对话的初始请求中提供一个Contact消息头。当UAC收到一个创建对话的响应时，它根据如下步骤来创建自身的对话状态:

如果请求基于TLS发送并且请求URI包含一个SIPS URI，则“安全”标志设为真；否则设为假。

远端目的地设置为响应消息中Contact消息头的URI。

远端序列号在此阶段设置为空，当远端在对话期间发送一个请求时再填写。

本地序列号设置为请求消息中Cseq头的序列号值。

本地URI设置为From消息头中的URI。

远端URI设置为TO消息头中的URI。

Dialog-ID如上所示来创建。

路由集用Record-Route头中的URI来设置,但其顺序进行了翻转。如果没有Record-Route头出现，则路由集设置为空。该路由集即使为空，仍将保留用于对话的余下部分。这就意味着出现在对话请求中的其他Record-Route消息头不会覆盖现有的路由集。如果路由集是由一个临时响应中的Record-Route头来生成的，则确认对话的2xx最终响应会使用其Record-Route头中的URI来重置路由集，但这次顺序又是翻转的。

对话内的请求填写要用到对话状态。每当对话中产生一个新请求时，本地Cseq消息头的值就加1。如果对话内的请求是目的地刷新请求，则可能更新远端目的地。目的地刷新请求的例子如INVITE请求和UPDTAE请求。

当返回一个非2xx的最终响应时，早期对话便会终止。已确认的对话根据所采用的方法不同，其终止方式也不同。

5.5.10 会话

多媒体会话由一组多媒体发送者和接收者及其彼此之间的数据流组成，会话采用SIP对话并在对话期间发送请求时遵循SIP规则。

SIP在建立多媒体对话中扮演的角色以其在消息正文中携带SDP媒体描述的能力为核心。SDP用来描述会话，并采用提供/应答模型[RFC32641]。

会话由INVITE方法、请求行和消息头发起，这些都由UAC来填写。消息体中填入SDP提供。SDP应答可能在临时响应或2xx响应中到达。

INVITE请求遵循三次握手模型，即UAC在收到对INVITE请求的最终响应后，必须发送一个ACK请求。该ACK请求并不要求响应。实际上，对ACK请求发送响应也是不允许的。

在发送INVITE请求后，如果UAC想取消这次会话邀请，它可以发送一个CANCEL请求。CANCEL请求使用类似方法构造，其请求URI、TO消息头、From消息头、Call-ID消息头以及CSeq消息头的数字部分都是从INVITE请求中复制过来的。CSeq消息头的方法部分的内容为“CANCEL”。收到CANCEL的UAS用200响应对其应答，紧接着对INVITE请求发出一个“487请求终止”响应。需要注意的是所有事务都必须彼此独立地完成，因此UAS不仅需要对CANCEL进行响应，还必须对INVITE请求进行响应。

如果UAC对2xx响应中的SDP应答不满意，就发送一个ACK请求后面跟着一个BYE请求来终止会话。如果UAS对SDP提供不满意，它就用488响应来拒绝该请求。

INVITE请求也可在对话期间发送，以对会话描述进行重新协商。

一个会话通过BYE请求来终止。BYE请求的发送和对话中其他请求的发送方式一样。

SlP中的SDP提供／应答模型

在基本的SIP中，提供和应答只能出现在INVITE请求中以及对INVITE请求和ACK请求的可靠响应中。

如果一个INVITE请求创建多个对话，则每个对话都有自己单独的提供／应答交换。

提供／应答交换的一个通用原则就是，如果前面发出(收到)了一个提供，那么只有该提供已经收到(或发出)了应答，才可以发送下一个提供。该原则将基本SIP限制在以下两种提供／应答交换的可能情形中:

如果提供存在INVITE请求中，则回答必须出现在对INVITE的2xx响应中。

如果INVITE请求没有包含一个提供，则2xx响应包含提供，ACK包含应答。

5.5.11 安全

5.5.11.1威胁模型

SIP可能会遭到以下威胁和攻击:

拒绝服务(Denial of service)——DOS攻击的结果就是遭受攻击的实体变成不可用。这包括如下情况:针对某个UA或代理发送大量请求。组播请求就是另一个例子。

窃听(Eavesdropping)——如果消息以明文发送，任何恶意用户都可以窃听并获取会话信息，从而轻而易举地发动各种拦截类的攻击。

拆除会话(tearing down sessions)——攻击者可插入类似于CANCEL请求之类的消息来阻止呼叫方与他人的通信，也可通过发送BYE请求来终止会话。

注册拦截(registration hijacking)——攻击者伪装成某用户进行注册，从而将所有去往该用户的流量引导到攻击者自己的机器。

会话拦截(session hijacking)——攻击者可在对话中发送NVTIE请求，来请求对发送途中的请求进行修改，通过修改会话描述把媒体流引导到其他地方。会话拦截者也可用3xx-类型的响应来对呼叫者进行应答，从而将会话建立请求重定向到攻击者自己的机器。

冒充服务器(impersonating a server)——假装自己是服务器并伪造一个响应，这样原来的消息就可能被错误地路由。

中间人(man in the middle)——这种攻击中，攻击者篡改发往接收者过程中的消息。

5.5.11.2 安全框架

SIP安全框架包含六个方面:

认证、(Authentication)——识别某实体或用户并确保该用户确实是其自称的用户的方法，典型方法包括用户ID，口令或使用密钥散列进行数字签名。

授权(Authorization)——一旦用户通过认证后，就必须对其授权。授权包括决定是否允许已确认身份的用户访问他所要求的服务，通常使用访问控制列表(ACLs)来实现。

机密性(Confidentiality)——这用于消息必须保持机密并且只允许特定接收者看到消息内容的场合，通常通过加密的方法来实现。

完整性(Integrity)——用户需要确保消息在途中不被篡改。消息完整性检查是确保完整性的方法之一。

隐私性(Pricacy)——用户的匿名是一个关键因素。用户不想其他人知道他是谁，他的通信内容以及他在与谁通信。

不可否认(Non-repudiation)——提供反向保护。

5.5.11.3 机制和协议

1、 逐跳机制

逐跳认证给用户提供了完整的机密性。它包括一个复杂的安全体系，该体系要求每个代理对消息进行解密，因此该体系依赖于各跳之间的信任关系。SIP现在使用两种安全协议，IP安全(IPsec)和传输层安全协议(或称TLS)。

1.SIP、TLS和SIPS URI

TLS可以实现认证、完整性和机密性。正如前面所提到的，SIP消息中若使用TLS要求，则所有SIP实体都要使用SIPS URI。即如果UAC希望进行安全通信，就在TO消息头中放置一个SIPS URI。如果下一跳URI或SIP请求的请求URI包含SIPS UP,则UAC必须在Contact消息头里放置一个SIPS URI。如果请求URI 包含一个SIPS URI，则请求的任何备选目的地也必须用TLS来联系。

用TLS来保证安全的请求必须使用可靠的传输层协议，如TCP或流控制传输协议(SCTP)。发送TLS安全请求和发送TLS安全响应的默认端口都是5061。

当注册一个绑定时，UAC必须在Contact消息头里创建一个SIPS URI，除非它能保证Contact消息头里的主机有其他的安全措施。

当UAS用能创建对话的响应(非失败响应)对能创建对话的请求进行响应时，如果请求URI、Record-route消息头顶端(如果有该消息头)或Contact消息头(如果没有Record-Route消息头)中含有SIPS URI，则UAS要在该响应的Contact消息头里放入一个SIPS URI。如果收到的请求是基于TLS(Via消息头显示传输协议为TLS)的，则UAS必须用TLS来发送响应。

当在对话期间发送请求时，UAC和UAS检查对话状态中的“安全”标志。该标志为真时，则要求UAC和UAS在Contact消息头里放入一个SIPS URI。

对于插入Record-Route消息头的代理而言，如果请求URI或Route消息头顶端(在对请求进行处理后)有SIPS URI，则他们必须在消息头里插入一个SIPS URI。

如果下一跳URI是SIPS URI，所有SIP实体都必须使用TLS。如果初始请求中的请求URI包含SIPS URI，并且收到了对该请求的3xx响应，那么实体在按照3xx响应里的Contact消息头来发送新请求时，不应给其中的非SIPS URI发送新请求。SIP实体在进行下一跳发现过程时，不论使用哪种URI作为过程的输入，只要请求-URI中列出了一个SIPS资源，SIP实体就必

须遵循与输入URI是SIPS URI时相同的过程。

代理对响应进行处理时，如果要将来自非TLS连接的请求转发到TLS连接上时，则它会把放在Record-Route消息头里的URI由SIPS URI改为SIP URI。同样，当代理处理响应时收到从TLS连接来的请求并把它转发到非-TLS连接上，则将它放在Record-Route消息头里的URI由SIP URI改为SIPS URI。

SIPS URI的格式与SIP URI的格式惟一的不同点在于模式(scheme)不同:

SIPS URI以“sips”开头，而SIP URI以“sip”开头。因此SIP URI和SIPS URI是不能等同的。

2.IPsec

IPsec通过在IP层对SIP消息提供安全来实现认证、完整性和机密性，它同时

支持TCP和UDP。

2、用户到用户和代理到用户机制

用户到用户(或端到端)和代理到用户的安全可以被认为是一种更安全的机制,因为只有两个实体可被攻击。SIP中使用两种协议来实现这种机制，即SIP摘要和安全多用途因特网邮件扩展或称S/MIME[RFC2633]。另外，在第三代伙伴计划(3GPP)的IMS中，采用了一种对摘要框架的扩展(即摘要AKA)。

1.摘要认证

SIP摘要认证大部分采用了HTTP摘要[RFC2617]认证机制，只有少量的改动。虽然摘要提供的完整性保护是有限的，但确实能提供客户端认证和阻止重放攻击(replay)。它还能提供一种互相认证的能力，使得客户端能认证服务器。

摘要认证要求共享密钥,这就意味着所有用户间以及用户和代理间都需要有一种先前存在的关系。在公共服务中，这个要求很成问题。

2.摘要AKA认证

IMS的认证采用了UMTS的认证和密钥协商(AKA)协议。该协议需要在SIP信令内传输，这就是摘要AKA的基本思想:将AKA协议和摘要认证框架集成起来。

现实中,这就意味着AKA认证请求被封装在401“未授权”响应的WWW.Authenticate消息头中或407“要求代理认证”响应的Proxy-Authenticate头里。同样，客户端认证响应被封装在请求消息的Authorization消息头或Proxy-Authorization消息头中。

AKA参数(即随机挑战(或RAND)和网络认证标志(AUTN))是串在一起的，并添加在服务器的当前参数之后。响应(RES)可以从响应摘要中计算出来，方法是简单地将RES参数视为摘要密码。使用摘要AKA的正常认证流程如图5-30所示。

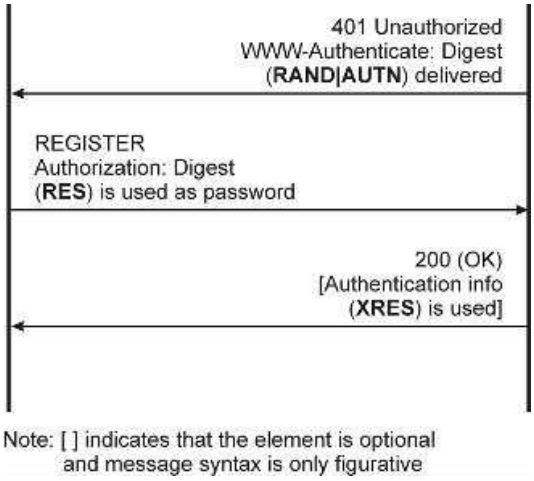


图5-30 正常的摘要AKA消息流程

([]表示该元素可选，且消息语法仅仅是描述性的)

不能完全遵循摘要框架的惟一例外发生在AKA同步失败时。这时，同步失败参数AUTS被包含在扩展的摘要参数中，采用Base64编码:这样做的原因仅仅是没有其他更合适的协议元素来携带该参数(见图5-31)。

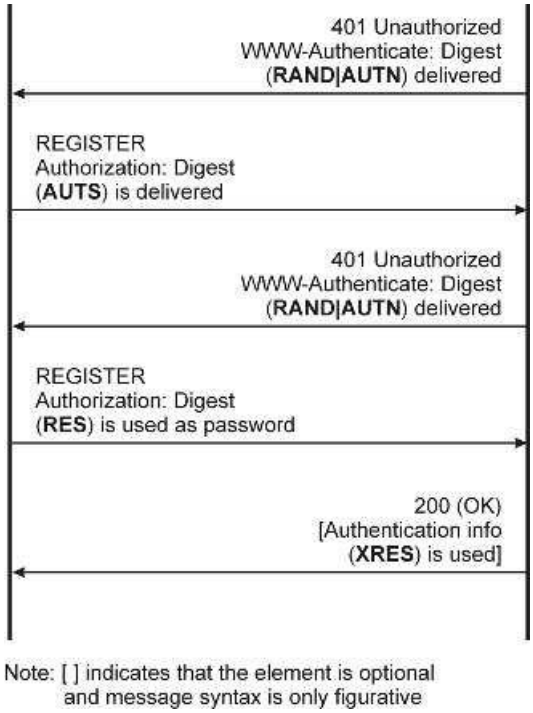


图5-31 同步失败时的摘要AKA消息流程

([]表示该元素可选，且消息语法仅仅是描述性的)

3.S/MIME

安全的多目的互联网邮件扩展(S/MIME)通过加密和/或签名的S/MIME SIP消息正文来保护SIP消息头，从而提供消息的完整性、机密性和认证，该方法不需要共享密钥。