第6章 基本信令流程

6.1 概述

6.1.1 流程的分类

在 WCDMA 系统中具有的各种各样的信令流程中，从协议栈的层面来说，可以分为接入层的信令流程和非接入层的信令流程；从网络构成的层面来说，可以分为电路域的信令流程和分组域的信令流程。

所谓接入层的流程和非接入层的流程，实际是从协议栈的角度出发的。在协议栈中，RRC 和 RANAP 层及其以下的协议层称为接入层，它们之上的 MM、SM、CC、SMS 等称为非接入层。简单地说，接入层的流程，也就是指无线接入层的设备 RNC、NodeB 需要参与处理的流程。非接入层的流程，就是指只有 UE 和 CN 需要处理的信令流程，无线接入网络 RNC、NodeB 是不需要处理的。举个形象的比喻，接入层的信令是为非接入层的信令交互铺路搭桥的。通过接入层的信令交互，在 UE 和 CN 之间建立起了信令通路，从而便能进行非接入层信令流程了。

接入层的流程主要包括 PLMN 选择、小区选择和无线资源管理流程。无线资源管理流程就是 RRC 层面的流程，包括 RRC 连接建立流程、UE 和 CN 之间的信令建立流程、RAB 建立流程、呼叫释放流程、切换流程和 SRNS 重定位流程。其中切换和 SRNS 重定位含有跨 RNC、跨 SGSN/MSC 的情况，此时还需要 SGSN/MSC 协助完成。所以从协议栈的层面上来说，接入层的流程都是一些底层的流程，通过它们，为上层的信令流程搭建底层的承载。

非接入层的流程主要包括电路域的移动性管理，电路域的呼叫控制，分组域的移动性管理、分组域的会话管理。

6.1.2 基本信令流程总体介绍

接下来我们对基本的信令流程进行简单的总体介绍。

我们首先看一下用户在不移动的情况下，从开机、进行业务到关机的整个业务流程。

图6-1 主叫业务流程

(1) 用户 UE 开机，首先进行接入层的信令交互。此时首先进行 PLMN 选择，选择某个运营商的网络，接着进行小区选择，驻留一个合适的小区，然后进行 RRC 连接建立，Iu 接口的信令连接建立。至此，通过这些接入层的信令流程，在 UE 和 CN 之间搭建起了一条信令通道，为非接入层的信令流程做好了准备。

(2) 接着 UE 和 CN 之间便开始进行非接入层的移动性管理流程了。此时用户会进行附着流程，其中包括鉴权、加密、位置更新等小流程。

(3) 当通过鉴权等流程后，UE 便进行非接入层的业务相关流程了。包括电路域的呼叫连接流程，分组域的会话管理流程。通过这些流程为进行业务搭建好了业务承载的链路。随后用户就可以开始打电话，上网了。

(4) 当用户结束业务后，同样会进行电路域的呼叫连接流程，分组域的会话管理流程，拆除业务承载链路。

(5) 此时如果用户关机的话，则 UE 和 CN 之间进行非接入层的移动性管理流程，进行电路域、分组域的分离。

(6) 等非接入层的信令交互结束后，系统会进行接入层的信令流程，拆除之前建立的 Iu 信令连接，以及 RRC 信令连接。

至此，一个用户在不移动的情况下，从开机，进行业务，到关机的整个流程便结束了。其中可以看到，这个业务过程是需要接入层的信令流程和非接入层的信令流程互相配合完成的。接入层的流程为非接入层的流程搭建信号承载。

接下来我们再看一下用户进行被叫的一个业务流程。

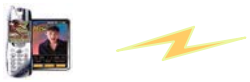


图6-2 被叫业务流程

(1) 用户 UE 处在待机状态。此时从网络侧对其进行寻呼；
(2) 如果没有现存的 UE 与 CN 之间的信令连接，则 UE、RNC、CN 之间会进行接入层的信令流程，建立 RRC 连接和 Iu 接口信令连接；
(3) 接下来可能会进行移动性管理的鉴权加密流程；
(4) 随后通过电路域的呼叫连接流程、分组域的会话管理流程，建立其业务的承载链路，从而就可以进行业务了。
(5) 结束业务后，再拆除相关的业务承载链路。
(6) 接着释放接入层的信令连接，包括 Iu 接口的信令连接和 RRC 连接。

上面的两个流程主要从总体上介绍了用户在不产生位置变化的情况下进行业务的情况。这只是一个总体上的简单描述。详细的各种流程将在后续章节中进行描述。

由于移动通信具有移动性的特点，所以由此就产生了很多处理移动性相关的流程。比如，当用户不进行业务的时候产生了位置改变，由此便产生了位置更新等移动性管理的流程；当用户进行业务的时候发生了位置变化，由此便产生了切换、SRNS 重定位等流程。

6.2 UE 的状态与寻呼流程

6.2.1 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。

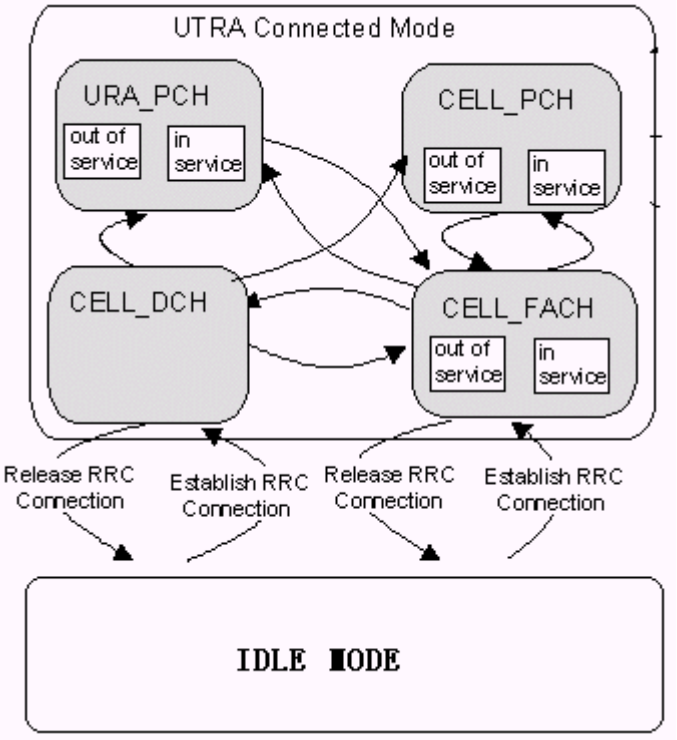


图6-3 UE 运行模式

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。

6.2.2 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。

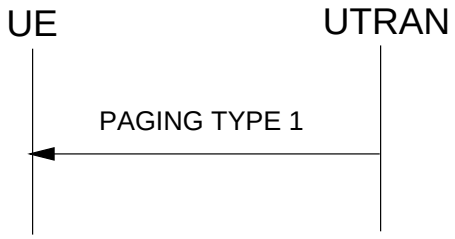


图6-4 寻呼空闲模式和 PCH 状态下的 UE

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。

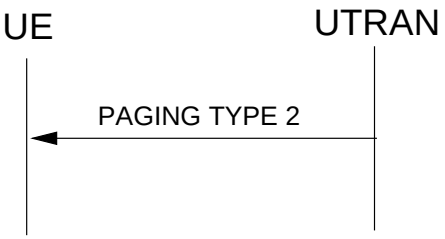


图6-5 寻呼 CELL_DCH 或 CELL_FACH 状态下的 UE

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 消息来发起寻呼过程。这种寻呼也叫做专用寻呼过程。

6.3 空闲模式下的 UE

6.3.1 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下图所示。

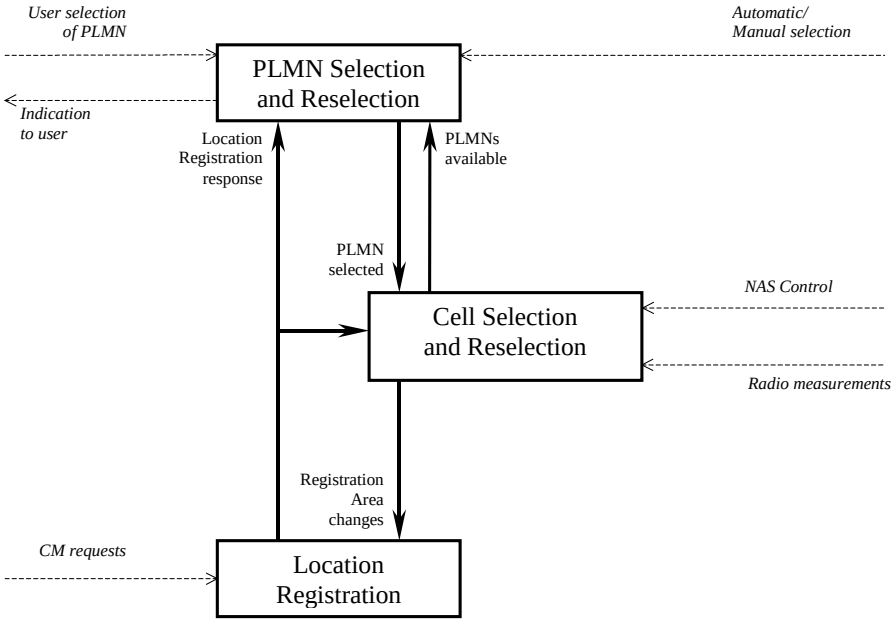


图6-6 空闲模式下的 UE

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 就驻留在这个小区中了。驻留的作用有 4 个：

- 使 UE 可以接收 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 通过系统广播信息中的 SIB1 发现 LA 或者 RA 的变化。

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。

6.3.2 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 会维护一个 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。

6.3.3 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）：

通过 primary SCH，UE 获得时隙同步。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。这一过程同时也确定了这个小区的扰码组。然后， UE 通过对扰码组中的每一个扰码在 CPICH 上相关，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，比如使用哪个频率，甚至主扰码，上述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。

- 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）。
- 如果当前 PLMN 是 UE 要找的 PLMN，UE 读 SIB3，取得“Cell selection and re-selection info”，通过获取这些信息，UE 计算是否满足小区驻留标准。如果满足，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，获取临区消息，这样 UE 就可以算出并判断临区是否满足小区选择驻留标准。

如果 UE 发现了任何一个临区满足小区驻留标准，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小区驻留标准。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）。如果在 Treselection 时间内，小区重选条件得到满足，UE 就选择这个小区，驻留下来，读它的广播消息。 小区重选结束。

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。

6.3.4 位置登记

这些过程请参见 MM，GMM 的过程。

6.4 无线资源管理流程

6.4.1 RRC 连接建立流程

UE 处于空闲模式下，当 UE 的非接入层请求建立信令连接时，UE 将发起 RRC 连接建立过程。每个 UE 最多只有一个 RRC 连接。

当 SRNC 接收到 UE 的 RRC CONNECTION REQUEST 消息，由其无线资源管理模块（RRM）根据特定的算法确定是接受还是拒绝该 RRC 连接建立请求，如果接受，则再判决是建立在专用信道还是公共信道。对于 RRC 连接建立使用不同的信道，则 RRC 连接建立流程也不一样。

1. RRC 连接建立在专用信道上

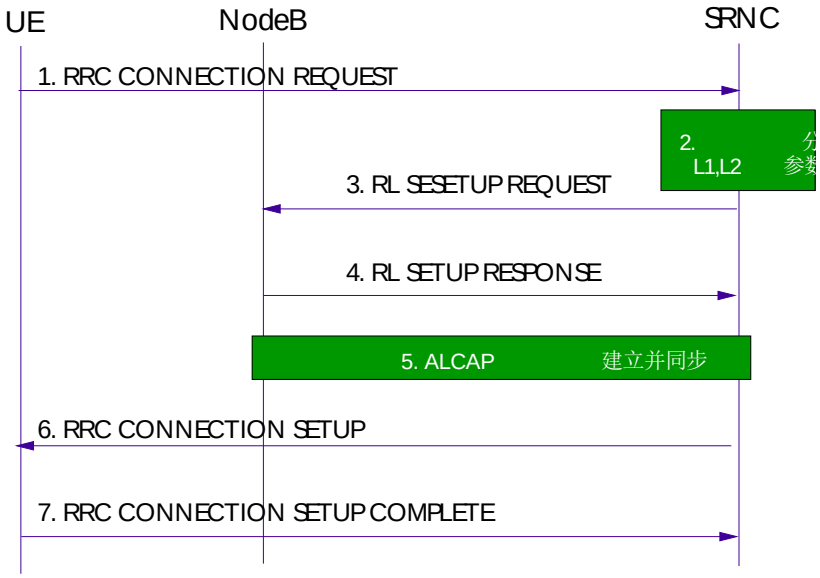


图6-7 RRC 连接建立在专用信道上

信令流程说明：

1）UE 在上行 CCCH 上发送一个 **RRC Connection Request** 消息，请求建立一条 RRC 连接；

2）SRNC 根据 RRC 连接请求的原因以及系统资源状态，决定 UE 建立在专用信道上，并分配 RNTI 和 L1、L2 资源；

3）SRNC 向 Node B 发送 **Radio Link Setup Request** 消息，请求 Node B 分配 RRC 连接所需的特定无线链路资源；

4）Node B 资源准备成功后，向 SRNC 应答 **Radio Link Setup Response** 消息；

5)SRNC 使用 ALCAP 协议发起 Iub 接口用户面传输承载的建立，并完成 RNC 于 Node B 之间的同步过程；

6）SRNC 在下行 CCCH 向 UE 发送 **RRC Connection Setup** 消息；

7）UE 在上行 DCCH 向 SRNC 发送 **RRC Connection Setup Complete** 消息。

至此，RRC 连接建立过程结束。

2. RRC 连接建立在公共信道上

当 RRC 连接建立在公共信道上时，因为用的是已经建立好的小区公共资源，所以这里无需建立无线链路和用户面的数据传输承载，其余过程与 RRC 连接建立在专用信道相似。

6.4.2 信令建立流程

信令建立流程是在 UE 与 UTRAN 之间的 RRC 连接建立成功后，UE 通过 RNC 建立与 CN 的信令连接，也叫“NAS 信令建立流程”，用于 UE 与 CN 的信令交互 NAS 信息，如鉴权、业务请求、连接建立等。

UE 与 CN 的交互的信令，对于 RNC 而言，都是直传消息。RNC 在收到第一条直传消息时，即：初始直传消息（Initial Direct Transfer），将建立与 CN 之间的信令连接，该连接建立 SCCP 之上。流程如下图所示：

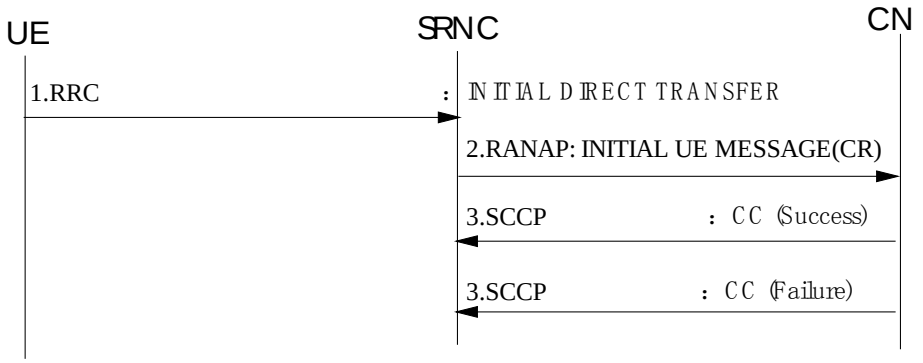


图6-8 信令建立过程

具体流程如下：

1）RRC 连接建立后，UE 通过 RRC 连接向 RNC 发送初始直传消息（Initial Direct Transfer），消息中携带 UE 发送到 CN 的 NAS 信息内容。

2）RNC 接收到 UE 的初始直传消息，通过 Iu 接口向 CN 发送 SCCP 连接请求消息（CR），消息数据为 RNC 向 CN 发送的初始 UE 消息（Initial UE Message），该消息带有 UE 发送到 CN 的消息内容。

3）如果 CN 准备接受连接请求，则向 RNC 回 SCCP 连接证实消息（CC），SCCP 连接建立成功。RNC 接收到该消息，确认信令连接建立成功。

4）如果 CN 不能接受连接请求，则向 RNC 回 SCCP 连接拒绝消息（CJ），SCCP 连接建立失败。RNC 接收到该消息，确认信令连接建立失败，则发起 RRC 释放过程。

信令连接建立成功后，UE 发送到 CN 的消息，通过上行直传消息（Uplink Direct Transfer）发送到 RNC，RNC 将其转换为直传消息（Direct Transfer）发送到 CN；CN 发送到 UE 的消息，通过直传消息（Direct Transfer）发送到 RNC，RNC 将其转换为下行直传消息（Downlink Direct Transfer）发送到 UE。

6.4.3 RAB 建立流程

RAB 是指用户平面的承载，用于 UE 和 CN 之间传送语音、数据及多媒体业务。UE 首先要完成 RRC 连接建立，然后才能建立 RAB。

RAB 建立是由 CN 发起，UTRAN 执行的功能，基本流程为：

- 首先由 CN 向 UTRAN 发送 RAB 指配请求消息，请求 UTRAN 建立 RAB；
- UTRAN 中的 SRNC 发起建立 Iu 接口与 Iub 接口（Iur 接口）的数据传输承载；
- SRNC 向 UE 发起 RB 建立请求；
- UE 完成 RB 建立，向 SRNC 回应 RB 建立完成消息；
- SRNC 向 CN 应答 RAB 指配响应消息，结束 RAB 建立流程。

当 RAB 建立成功以后，一个基本的呼叫即建立，UE 进入通话过程。

根据无线资源使用情况（RRC 连接建立时的无线资源状态与 RAB 建立时的无线资源状态），可以将 RAB 的建立流程分成以下三种情况：

1）DCH-DCH：RRC 使用 DCH，RAB 准备使用 DCH；

2）RACH/FACH-RACH/FACH：RRC 使用 CCH，RAB 准备使用 CCH；

3）RACH/FACH-DCH：RRC 使用 CCH，而 RAB 准备使用 DCH。

下面给出以上第一种情况下的 RAB 建立流程的具体过程描述。

1. DCH-DCH

UE 当前的 RRC 状态为专用传输信道（DCH）时，指配的 RAB 只能建立在专用传输信道上。根据无线链路（RL）重配置情况，RAB 建立流程可分为同步重配置 RL（DCH-DCH）与异步重配置 RL（DCH-DCH）两种情况，二者的区别在于 Node B 与 UE 接收到 SRNC 下发的配置消息后，能否立即启用新的配置参数：

- 同步情况下，Node B 与 UE 在接收到 SRNC 下发的配置消息后，不能立即启用新的配置参数，而是从消息中获取 SRNC 规定的同步时间，在同步时刻，同时启用新的配置参数；
- 异步情况下，Node B 与 UE 在接收到 SRNC 下发的配置消息后，将立即启用新的配置参数。

(1) 同步重配置 RL

在 DCH-DCH 同步情况下，需要 SRNC 、Node B 与 UE 之间同步重配置 RL：

- Node B 在接收到 SRNC 下发的重配置 RL 消息后，不能立即启用新的配置参数，而是准备好相应的无线资源，等待接收到 SRNC 下发的重配置执行消息，从消息中获取 SRNC 规定的同步时间；
- UE 在接收到 SRNC 下发的配置消息后，也不能立即启用新的配置参数，而是从消息中获取 SRNC 规定的同步时间；
- 在 SRNC 规定的同步时刻，Node B 与 UE 同时启用新的配置参数。

下面给出 RAB 建立流程中 DCH-DCH 同步重配置 RL 的过程。

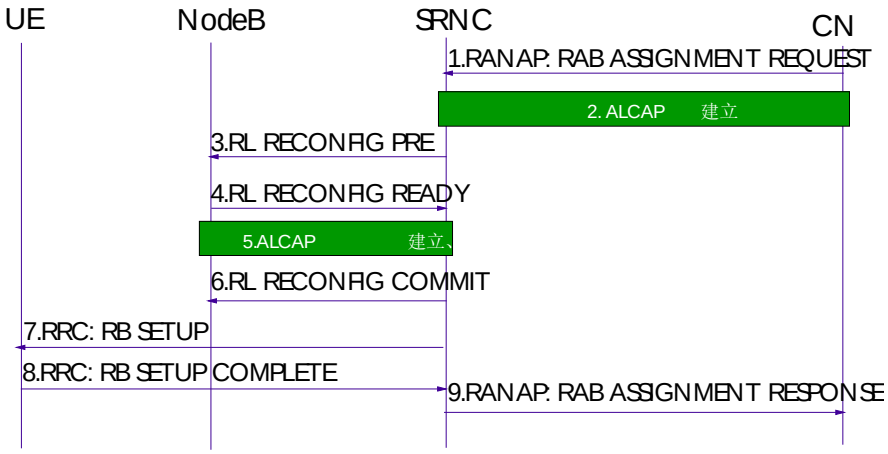


图6-9 RAB 建立流程（DCH-DCH，同步）

信令流程说明：

1）CN 向 UTRAN 发送 RANAP 协议的 RAB 指配消息 Radio Access Bearer Assignment Request，发起 RAB 建立请求；

2）SRNC 接收到 RAB 建立请求后，将 RAB 的 QoS 参数映射为 AAL2 链路特性参数与无线资源特性参数，Iu 接口的 ALCAP 根据其中的 AAL2 链路特性参数发起 Iu 接口的用户面传输承载建立过程；

3)SRNC 向属下的 Node B 发送 NBAP 协议的无线链路重配置准备 Radio Link Reconfiguration Prepare 消息，请求属下的 Node B 准备在已有的无线链路上增加一条（或多条）承载 RAB 的专用传输信道（DCH）；

4）Node B 分配相应的资源，然后向所属的 SRNC 发送 Radio Link Reconfiguration Ready 消息，通知 SRNC 无线链路重配置准备完成；

5）SRNC 中 Iub 接口的 ALCAP 发起 Iub 接口的用户面传输承载建立过程，Node B 与 SRNC 通过交换 DCH 帧协议的上下行同步帧建立同步；

6）SRNC 向属下的 Node B 发送无线链路重配置执行消息 Radio Link Reconfiguration Commit；

7）SRNC 向 UE 发送 RRC 协议的 RB 建立消息 Radio Bearer Setup；

8）UE 执行 RB 建立后，向 SRNC 发送无线承载建立完成消息 Radio Bearer Setup Complete；

9）SRNC 接收到无线承载建立完成的消息后，向 CN 回应 RAB 指配响应消息 Radio Access Bearer Assignment Response，结束 RAB 建立流程。

(2) 异步重配置 RL

在 DCH-DCH 异步情况下，不要求 SRNC 、Node B 与 UE 之间同步重配置 RL：Node B 与 UE 在接收到 SRNC 下发的配置消息后，将立即起用新的配置参数。

下面给出 RAB 建立流程中 DCH-DCH 异步重配置 RL 的例子。

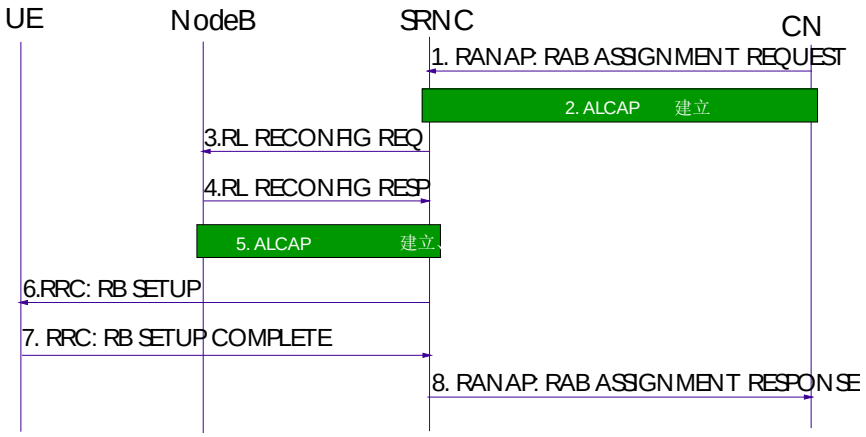


图6-10 RAB 建立流程（DCH-DCH， 异步）

信令流程说明：

1）CN 向 UTRAN 发送 RANAP 协议的 RAB 指配消息 Radio Access Bearer Assignment Request，发起 RAB 建立请求；

2）SRNC 接收到 RAB 建立请求后，将 RAB 的 QoS 参数映射为 AAL2 链路特性参数与无线资源特性参数，Iu 接口的 ALCAP 根据其中的 AAL2 链路特性参数发起 Iu 接口的用户面传输承载建立过程；

3）在异步情况下，无线重配置无需同步，SRNC 向属下的 Node B 发送 NBAP 协议的无线链路重配置请求 Radio Link Reconfiguration Request 消息，请求属下的 Node B 在已有的无线链路上建立新的专用传输信道（DCH）；

4）Node B 接收到无线链路重配置请求消息后，即分配相应的资源，然后向所属的 SRNC 发送 Radio Link Reconfiguration Response 消息，通知 SRNC 无线链路重配置完成；

5）SRNC 中 Iub 接口的 ALCAP 发起 Iub 接口的用户面传输承载建立过程，Node B 与 SRNC 通过交换 DCH 帧协议的上下行同步帧建立同步；

6）SRNC 向 UE 发送 RRC 协议的无线承载建立消息 Radio Bearer Setup；

7）UE 执行 RB 建立后，向 SRNC 发送无线承载建立完成消息 Radio Bearer Setup Complete；

8）SRNC 接收到无线承载建立完成的消息后，向 CN 回应 RAB 指配响应消息 Radio Access Bearer Assignment Response，结束 RAB 建立流程。

6.4.4 呼叫释放流程

呼叫释放流程也就是 RRC 连接释放流程。RRC 连接释放流程分为两种类型：UE 发起的释放和 CN 发起的释放。两种释放类型的区别主要在于高层的呼叫释放请求消息由谁先发出，但最终的资源释放都是由 CN 发起的。

当 CN 决定释放呼叫后，将向 SRNC 发送 IU RELEASE COMMAND 消息。SRNC 收到该释放命令后，有如下操作步骤：

1 ）向 CN 返回 IU RELEASE COMPLETE 消息；

2 ）发起 IU 接口用户面传输承载的释放；

3 ）释放 RRC 连接。

RRC 释放就是释放 UE 和 UTRAN 之间的信令链路以及全部无线承载。根据 RRC 连接所占用的资源情况，可进一步划分为两类：释放建立在专用信道上的 RRC 连接和释放建立在公共信道上的 RRC 连接。

1. 释放建立在专用信道上的 RRC 连接

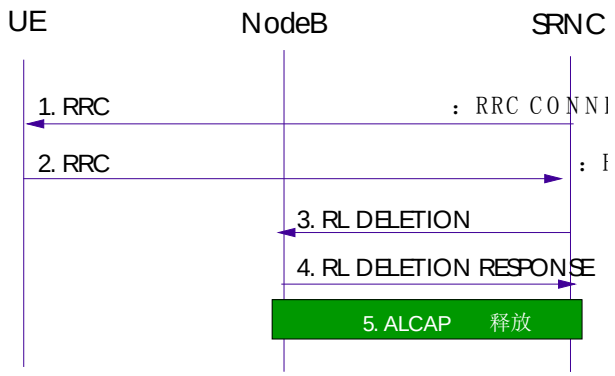


图6-11 释放建立在专用信道上的 RRC 连接

流程描述：

1) RNC 向 UE 发送 RRC 连接释放消息 **RRC Connection Release**；
2) UE 向 RNC 返回释放完成消息 **RRC Connection Release Complete**；
3) RNC 向 Node B 发送无线链路删除消息 **Radio Link Deletion**，删除 Node B 中的无线链路资源；
4) Node B 资源释放完成后，向 RNC 返回释放完成消息 **Radio Link Deletion Response**；
5) RNC 使用 ALCAP 协议发起 IUB 接口用户面传输承载的释放。

最后 RNC 再发起本端 L2 资源的释放。至此，RRC 释放过程结束。

2. 释放建立在公共信道上的 RRC 连接

释放建立在公共信道上的 RRC 连接时，因为此时用的是小区公共资源，所以直接释放 UE 就可以了，无需释放 Node B 的资源，当然也没有数据传输承载的释放过程。

6.4.5 切换流程

切换过程是移动通信区别于固定通信的一个显著特征之一， 当 UE 使用的小区或制式（FDD ， TDD）发生变化时，我们就说 UE 发生了切换。 WCDMA 支持的切换包括软切换，硬切换，前向切换和系统间切换。软切换和硬切换主要是由网络侧发起，前向切换主要是 UE 发起，而系统间切换既有网络侧发起的情况，又有 UE 发起的情况。发生切换的原因包括 UE 的移动，资源的优化配置，人为干预等。

1. 软切换

在 WCDMA 中，由于相邻小区存在同频的情况，UE 可以通过多条无线链路与网络进行通信，在多条无线链路进行合并的时候，通过比较，选取信号较好的一条，从而达到优化通信质量的目的，只有 FDD 制式才能进行软切换。根据小区之间位置的不同，软切换可以分为几种情况。第一种情况， Node B 内不同小区之间。这种情况，无线链路可以在 Node B 内，也可以到 SRNC 再进行合并，如果在 Node B 内部就完成了合并，我们称之为更软切换；第二种情况，同一 RNC 内不同 Node B 之间；还有不同 RNC 之间。

软切换中一个重要问题就是多条无线链路的合并，WCDMA 中使用宏分集（MACRO DIVERSITY）技术对无线链路进行合并，就是根据一定的标准（如误码率）对来自不同无线链路的数据进行比较，选取质量较好的数据发给上层。

在软切换中，关于邻近小区有几个重要的概念：

1 ）活动集，指的是 UE 当前正在使用的小区的集合，软切换的执行结果就表现在活动集中小区增加或减少。

2 ）观察集，UE 根据 UTRAN 给的邻近小区信息，正在观察但不在活动集中的小区，UE 对观察集中的小区进行测量，当测量结果符合一定的条件时，这些小区可能被加入活动集，所以有时也称为候选集；

3 ）已检测集，UE 已检测到，但既不属于活动集也不属于观察集的小区，UTRAN 可以要求 UE 报告已检测集的测量结果；由于它们不属于邻近小区列表，所以有时也称之为未列出集。

软切换的过程可以分为以下几个步骤：

1 ）UE 根据 RNC 给的测量控制信息， 对同频的邻近小区进行测量，测量结果经过处理后，上报给 RNC；

2 ）RNC 对上报的测量结果和设定的阈值进行比较，确定哪些小区应该增加，哪些应该删除；

3 ）如果有小区需要增加，先通知 Node B 准备好；

4 ）RNC 通过活动集更新消息，通知 UE 增加和/或删除小区；

5 ）在 UE 成功进行了活动集更新后，如果删除了小区，则通知 Node B 释放相应的资源。

在进行软切换的过程中，原来的通信不受影响，所以能够完成从一个小区到另一个小区的平滑切换。

2. 硬切换

当邻近小区属于异频小区时，不能进行软切换，这时可以进行硬切换，硬切换过程就是先中断跟原来小区的通信，然后再从新的小区接进来，因此它的性能不如软切换，所以一般在不能进行软切换的时候，才会考虑硬切换。

硬切换的目标小区可以没有经过测量，适合于紧急情况下的硬切换，失败率较高；更常见的硬切换同样也要对目标小区先进行测量，但一般 UE 只配一个解码器，不能同时对两个频点的信号进行解码，所以为了 UE 能进行异频测量，在 WCDMA 中引入了压缩模式技术。

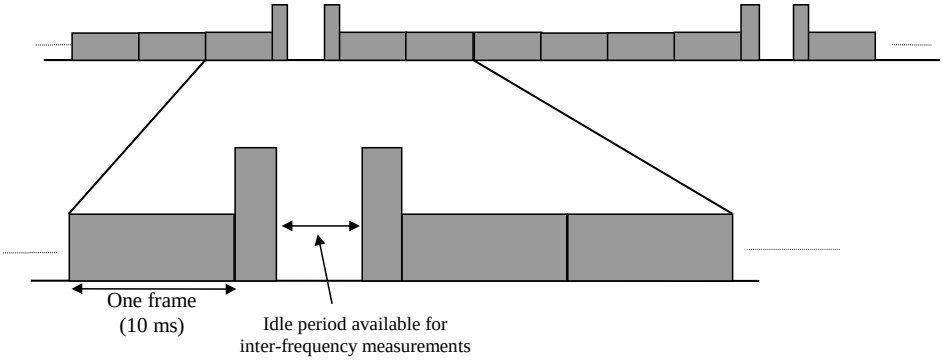


图6-12 压缩模式原理图

压缩模式技术的基本原理就是，Node B 在发送某些帧（每 10ms 发送的数据为一帧）的时候，加大发送速率，用少于 10ms 的时间发送完原来需要 10ms 的数据，那么空出来的时间，就让 UE 进行异频测量。具体采用什么方式和什么时间来加大发送速率，由 RNC 进行控制。

跟软切换类似，硬切换根据原小区和目标小区的位置关系，分为以下几种：

1）同一个小区内，FDD 和 TDD 方式之间的硬切换；

2 ） Node B 内的小区之间；

3 ）同一 RNC 内不同 Node B 的小区之间；

4 ）不同 RNC 的小区之间。

通常不同 RNC 之间发生硬切换时，两个 RNC 之间都存在 IUR 接口，否则就需要通过伴随迁移（RELOCATION）来完成硬切换。

Uu 接口有 5 个信令过程都能够完成硬切换：

1 ）物理信道重配置（PHYSICAL CHANNEL RECONFIGURATION ）；

2 ）传输信道重配置（TRANSPORT CHANNEL RECONFIGURATION）；

3 ）RB 建立过程（RADIO BEAR SETUP ）；

4 ）RB 释放过程（RADIO BEAR RELEASE）；

5 ）RB 重配置过程（RADIO BEAR RECONFIGURATION）。

下图以物理信道重配置为例给出不同 Node B 之间小区硬切换的信令过程：

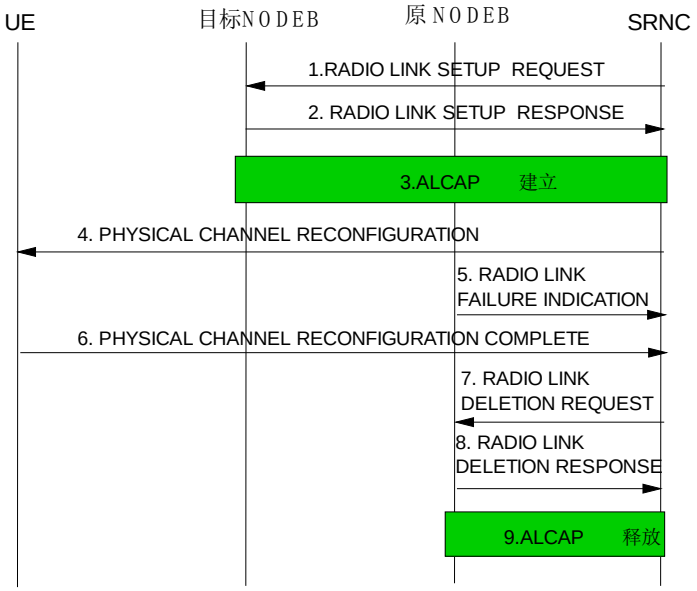


图6-13 硬切换流程图

信令流程描述：

1）SRNC 向目标小区所在的 Node B 发送消息 Radio Link Setup Request，要求其建立一条无线链路；

2）目标小区所在的 Node B 向 SRNC 应答消息 Radio Link Setup Response，表明无线链路建立成功；

3)SRNC 采用 ALCAP 协议建立 SRNC 和目标 Node B 的 IUB 接口传输承载，并且进行 FP 同步；

4）SRNC 通过下行 DCCH 信道向 UE 发送消息 Physical Channel Reconfiguration，消息中给出目标小区的信息；

5）在 UE 从原小区切换到目标小区后，原小区 Node B 会检测到无线链路失去联系，于是向 SRNC 发消息 Radio Link Failure Indication，指示无线链路失败；

6）UE 在成功切换到目标小区后，通过 DCCH 向 SRNC 发送消息 Physical Channel Reconfiguration Complete，通知 SRNC 物理信道重配置完成；

7）SRNC 向原小区所在的 Node B 发送消息 Radio Link Deletion Request，删除原小区的无线链路；

8）原小区所在的 Node B 完成无线链路资源删除后，向 SRNC 应答消息 Radio Link Deletion Response；

9）SRNC 采用 ALCAP 协议释放 SRNC 和原小区所在 Node B 的 IUB 接口的传输承载。

3. 前向切换

RRC 连接移动性管理中，前向切换是其中的一部分。前向切换分为小区更新和 URA 更新，主要用于当 UE 位置发生改变时及时更新 UTRAN 侧关于 UE 的信息，还可以监视 RRC 的连接、切换 RRC 的连接状态，另外还有错误通报和传递信息的作用。不管是小区更新还是 URA 更新，更新过程均是由 UE 主动发起的。

(1) 小区更新

处于 CELL_FACH、CELL_PCH 或 URA_PCH 状态的 UE 都可能发起小区更新过程，对不同的连接状态，会有不同的小区更新原因，小区更新流程也不同。

- 如果小区更新原因是周期性小区更新，且 UTRAN 侧不给 UE 分配新的 CRNTI 或 URNTI，其流程如图所示：

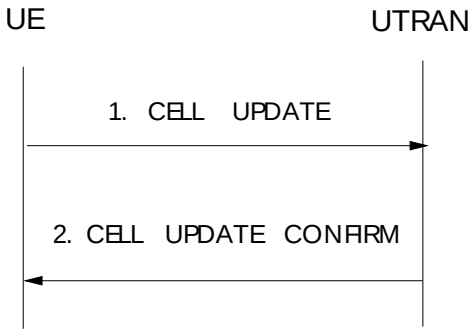


图6-14 小区更新过程

具体流程如下：

1）UE 从 CCCH 向 UTRAN 发送 CELL UPDATE 消息。

2）UTRAN 收到 UE 的 CELL UPDATE 消息处理完成后给 UE 发应答消息 CELL UPDATE CONFIRM。UTRAN 侧结束本次小区更新。UE 收到 CELL UPDATE CONFIRM 消息后结束本次小区更新。

- 如果小区更新的原因是因为有上行数据传输，或者是对寻呼的响应，UTRAN 侧没有给 UE 分配 CRNTI 或 URNTI，也没有指示相关物理信道信息，并且 UE 中保存的 TFS/TFCS 与系统信息中广播的 PRACH/SCCPCH 的 TFS/TFCS 相同；如果小区更新的原因是因为有上行数据，或者是对寻呼的响应，或者是小区重选，UTRAN 侧给 UE 分配了 CRNTI 或 URNTI，但没有指示相关物理信道信息，并且 UE 中保存的 TFS/TFCS 与系统信息中广播的 PRACH/SCCPCH 的 TFS/TFCS 相同，其流程中伴随有物理信道重配置。
- 如果小区更新的原因是因为有上行数据传输，或者是对寻呼的响应，UTRAN 侧没有给 UE 分配 CRNTI 或 URNTI，也没有指示相关物理信道信息，并且 UE 中保存的 TFS/TFCS 与系统信息中广播的 PRACH/SCCPCH 的 TFS/TFCS 不同；如果小区更新的原因是因为有上行数据，或者是对寻呼的响应，或者是小区重选，UTRAN 侧给 UE 分配了 CRNTI 或 URNTI，但没有指示相关物理信道信息，并且 UE 中保存的 TFS/TFCS 与系统信息中广播的 PRACH/SCCPCH 的 TFS/TFCS 不同，则其流程中伴随有传输信道重配置。
- 如果小区更新原因是周期性，UTRAN 侧给 UE 分配了 CRNTI 或 URNTI，但没有指示相关物理信道信息，UE 将更新其标识，即流程中伴随有 RNTI 重分配。

(2) URA 更新

URA 更新过程的目的是处于 URA_PCH 状态下的 UE 经过 URA 再选择后用现在的 URA 更新 UTRAN；在没有 URA 再选择发生时该过程也可以用来监视 RRC 连接。一个小区中可以广播几个不同的 URA ID，在一个小区中不同的 UE 可以属于不同的 URA。当 UE 处于 URA_PCH 状态时有且仅有一个有效的 URA。处于 URA_PCH 状态时，如果分配给 UE 的 URA 不在小区中广播的 URA ID 列表中，则 UE 将发起 URA 更新过程。或者 UE 在服务区内，但 T306 超时，则 UE 将发起 URA 更新过程。

- 如果 URA 更新过程中 UTRAN 没有给 UE 分配新的 CRNTI 或 URNTI 其流程如图所示：

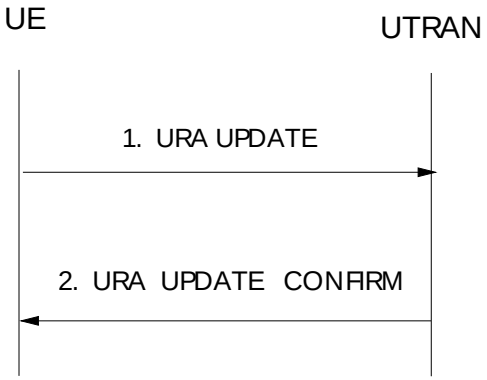


图6-15 URA 更新过程（没有分配新的 CRNTI 或 URNTI）

具体流程如下：

1）UE 从 CCCH 向 UTRAN 发起 URA UPDATE 消息。

2)UTRAN 收到 UE 的 URA UPDATE 消息处理完成后给 UE 发应答消息 URA UPDATE CONFIRM，并结束 UTRAN 侧本次 URA 更新。UE 收到 URA UPDATE CONFIRM 消息后，结束本次 URA 更新。

- 如果 URA 更新过程中 UTRAN 给 UE 分配了新的 CRNTI 或 URNTI 则其流程中伴随有 UE 发给 UTRAN 的 RNTI REALLOCATION COMPLETE 消息。

4. 系统间切换

WCDMA 支持 UE 在 UTRAN 和现存系统（如 GSM/GPRS）之间进行切换，可以分为网络控制下的切换（如 GSM）和 UE 的小区重选（如 GPRS）二种情况，它们各自又可分为入 UTRAN 和出 UTRAN 两种情况；这里仅以网络控制下的切换入 UTRAN 为例详细介绍流程。这里只介绍 UTRAN 中的信令。

- 迁入 UTRAN

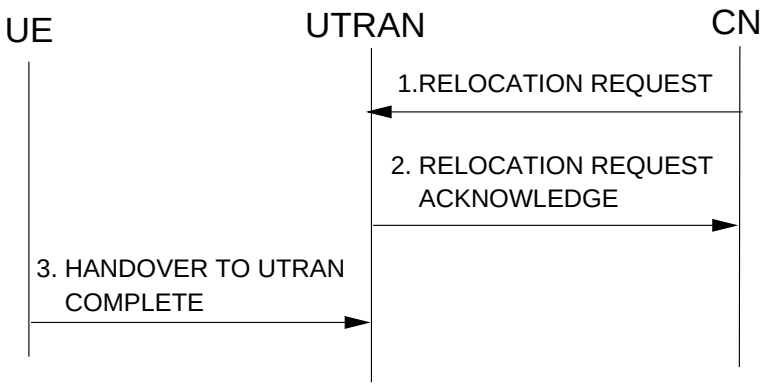


图6-16 迁入 UTRAN 流程图

具体流程如下：

1）CN 用 Relocation Request 消息通知 UTRAN 有 UE 需要迁入；

2）UTRAN 在准备好资源之后，向 CN 发送 Relocation Request Acknowledge 消息，在这条消息中又带着 Handover To UTRAN Command 消息，由对方系统把 Handover To UTRAN Command 消息发送给 UE；

3）UE 在成功接入 UTRAN 之后， 向 UTRAN 发送 Handover To UTRAN Complete 消息。

6.4.6 SRNS 重定位

RNC 重定位指 UE 的 SRNC 从一个 RNC 变成另一个 RNC 的过程，根据发生迁移时 UE 所处位置的不同可以分为静态迁移和伴随迁移两种情况，或者说 UE 不涉及的（UE Not Involved）和 UE 涉及的（UE Involved）。

1. 静态迁移

发生静态迁移的条件是 UE 从一个 DRNC，而且只从一个 DRNC 中接入。由于迁移过程不需要 UE 的参与，所以也称之为 UE 不涉及的（UE Not Involved）迁移，下面给出一个存在两条无线链路的例子。发生迁移之后，原来的 DRNC 变成了 SRNC，IUR 接口的连接被释放，IU 接口发生迁移，如图所示。

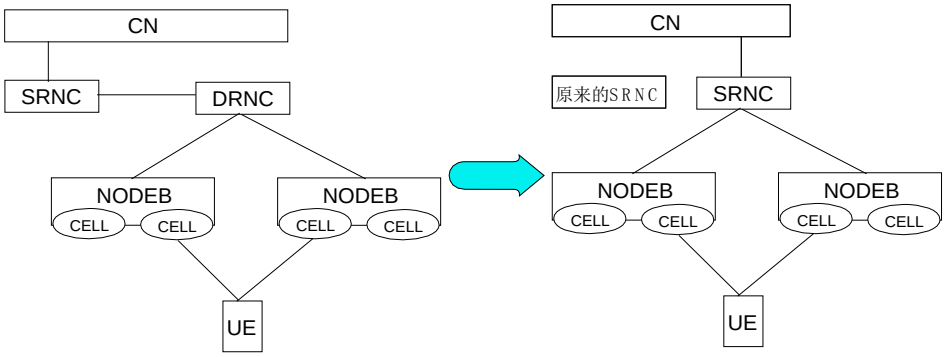


图6-17 静态迁移过程

在 WCDMA 中由于存在两个 CN 域，如果在发生迁移的时候，UE 和两个域都有连接，那么这两个域必须同时迁移。

2. 伴随迁移

伴随迁移指 UE 从 SRNC 硬切换到目标 RNC，同时 IU 接口发生变化的过程。由于迁移过程需要 UE 的参与，所以也称之为 UE 涉及的（UE Involved）迁移。其连接变化情况如图所示：

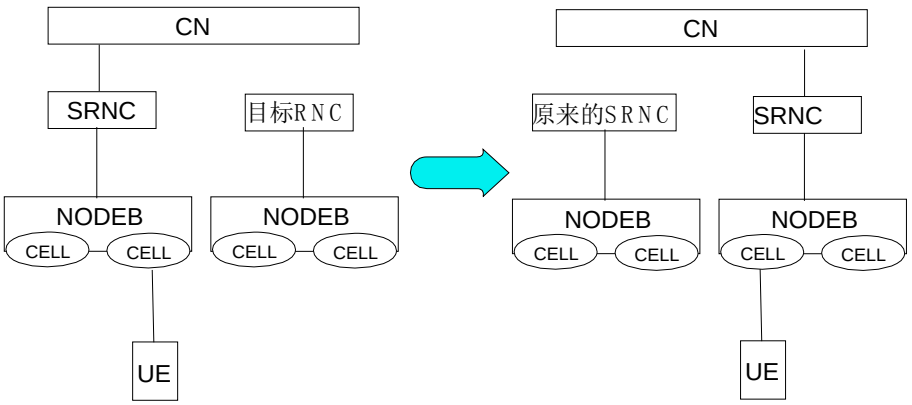


图6-18 伴随迁移过程

能够完成硬切换的 5 个信令过程都可以用来完成伴随迁移。

6.5 电路域移动性管理

6.5.1 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过程，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。

1. 位置登记

执行 MAP 操作里的 Update Location 操作，可以通过 Update Location Request 消息里的 Update Location Type 来区分不同类型的位置登记。

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。其中移动设备开机时 Update Location Type 指示为 IMSI Attach，漫游时 Update Location Type 指示为 Normal Updating。

移动设备主要是通过自身记录的 LAI 与收到的广播消息里的 LAI 对比，相同则发起 IMSI Attach 过程，不同则发起 Normal Updating 操作。

2. 周期性位置登记

执行 MAP 操作里的 Update Location 操作，此时 Update Location Request 消息里的 Update Location Type 指示为 Periodic Updating。

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。

3. 用户数据删除

执行 MAP 操作里的 Cancel Location 操作。

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。

用途是位置更新时 HLR 删除前 VLR 的用户信息，或用户数据修改引发的独立位置删除，以及操作人员删除用户位置信息。

下图是一个典型的位置更新流程图，基本包含了上述三个过程。

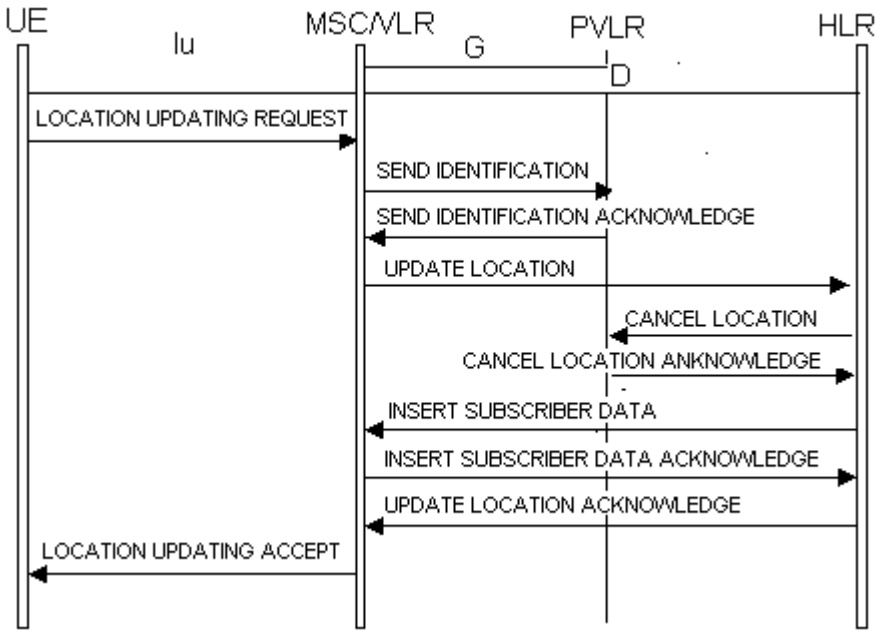


图6-19 位置更新流程图

(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：

A、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，参见上图中的 SEND IDENTIFICATION 流程；

B、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，上图中没有列出该流程，要求手机提供 IMSI 的流程参见下面章节。

(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。否则直接进入 LOCATION UPDATING ACCEPT 流程。

(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。

6.5.2 分离

分离过程即移动用户关机，UE 发起 IMSI Detach 的过程，MSC/VLR 置用户状态为 IMSI 分离，值得注意的是该过程不通知 HLR。这和 Purge 过程不同，因为在 HLR 中是没有用户 Detach/Attach 状态指示位的，但是 Purge 有，这可以参见后面对于 Purge 操作的详细描述。

如果该用户做被叫，则 HLR 会通过 Provide Roaming Number 过程到 VLR 取漫游号码，此时因为用户为 Detach 状态，所以取 Roaming Number 失败，返回原因值为 Absent Subscriber，主叫 MSC 根据该原因值给主叫 UE 放用户已关机提示音。

流程图如图

图6-20 关机流程图

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 过程。

6.5.3 身份识别

身份识别过程在 Iu 接口发生，用于网络向移动设备要求提供 IMEI 或 IMSI 信息，身份识别执行 Identity 过程。

Identity 过程有两种：

- VLR 里没有移动设备的 IMEI 时，将强制执行一个 Identity 过程，网络侧通过 Identity Request 向移动设备发起请求 IMEI 的操作，移动设备在 Identity Response 里给网络侧提供 IMEI。
  典型的情况有用户的第一次位置更新、VLR 记录的用户 IMEI 无效（注意由于目前没有使用 IMEI 鉴权，所以不会影响用户使用）。
- 由于位置更新时 TMSI 不识别，将强制执行一个 Identity 过程， 网络侧通过 Identity Request 向移动设备发起请求 IMSI 的操作，移动设备在 Identity Response 里给网络侧提供 IMSI。
  典型的情况有用户漫游到不使用 TMSI 的区域等。

图6-21 IDENTITY 流程图

6.5.4 用户清除

用户清除就是 VLR 发起移动用户删除过程，即 MAP 的 PurgeUE 过程，用于 VLR 向 HLR 报告 VLR 的用户删除操作。和上一节的 IMSI Detach 过程不同，PurgeUE 过程要通知 HLR，收到 PurgeUE 消息以后，在 HLR 中将把该用户的 UE Purge Flag 标志置位，指示该用户已经在 VLR 中清除了。

如果该用户做被叫，则当主叫 UE 通过 Send Routing Information 过程到 HLR 时，HLR 会查询 UE Purge Flag 标志，由于是置位状态，所以 HLR 将会给 MSC 返回 Absent Subscriber 的失败原因值，主叫 MSC 根据该原因值给主叫 UE 放用户已关机提示音。该过程没有 HLR 到 VLR 的 Provide Roaming Number 操作。

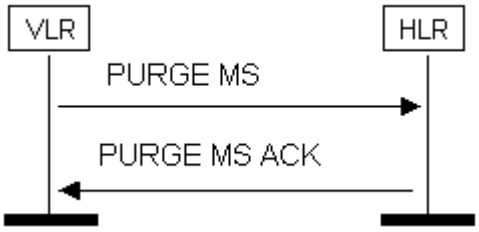


图6-22 PURGE 流程图

6.5.5 鉴权流程

一个成功的鉴权过程可以用流程图来表示，如图所示。

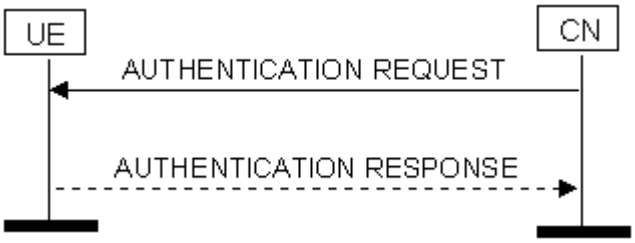


图6-23 鉴权成功

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。

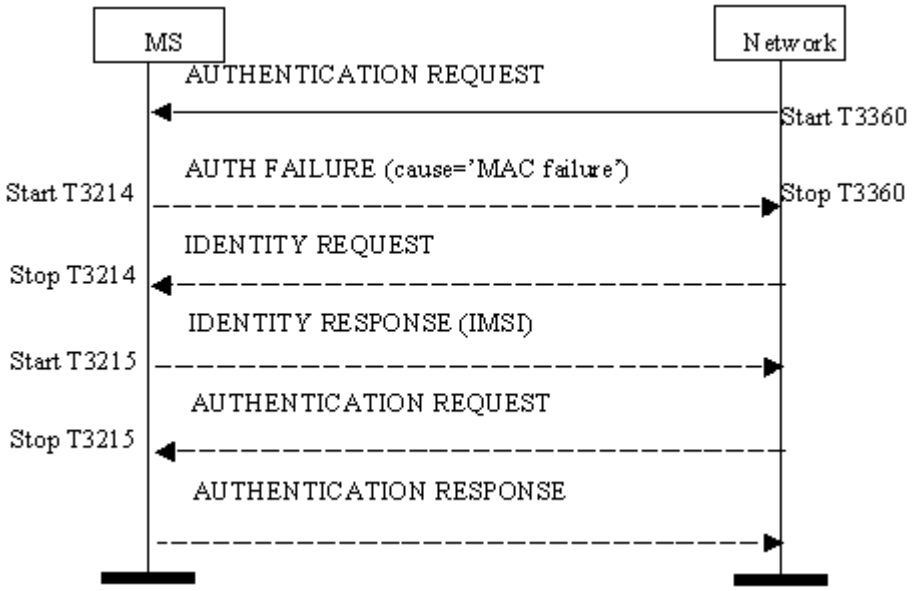


图6-24 鉴权失败（失败原因为 MAC Failure）

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）

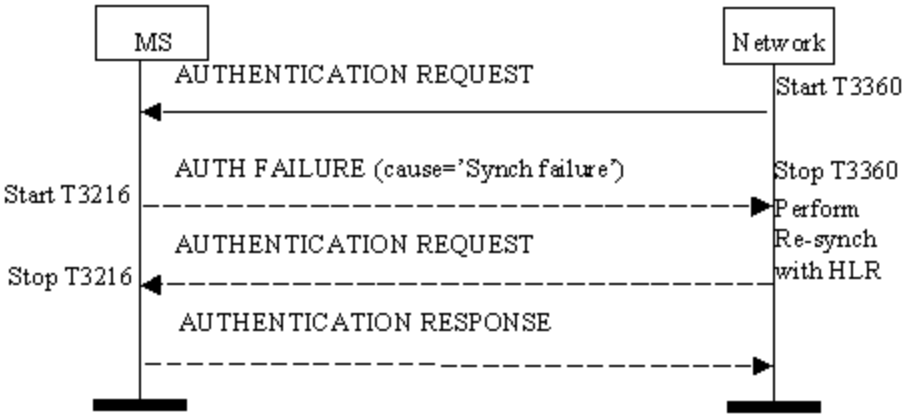


图6-25 鉴权失败（原因值为 Synch failure）

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。

6.5.6 安全模式控制

安全模式控制过程是由网络侧用来向无线接入网侧发送加密信息的。在此过程中，核心网的网络侧将与无线接入网协商对用户终端进行加密的算法，使得用户在后续的业务传递过程中使用此加密算法；并且在终端用户发生切换后，尽可能的仍使用此加密算法——即用于加密的有关参数会送到切换的目的 RNC。

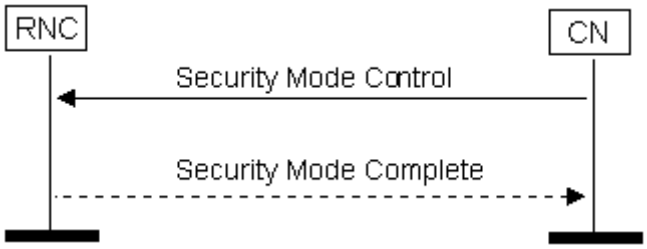


图6-26 安全模式控制

6.5.7 TMSI 重分配

TMSI，临时移动用户识别码，是由和临时分配给指定用户的一串数字（4 个 BYTE）组成。TMSI 由 MSC/VLR 管理，一般来说是当用户首次在一个位置区注册时分配给它，并在用户离开该位置区时注销。TMSI 被用来唯一识别一个位置区的移动台，取代 IMSI 在无线信道中传输，从而防止第三方通过窃听无线信道上的信号而识别并跟踪移动用户。所以其主要作用就是增加移动台的安全性。

TMSI 与 IMSI（国际移动终端设备标识）的对应关系存放在管理移动台当前访问位置区的 VLR 中，最新分配的 TMSI 也存放于移动台的 SIM 卡中。所以 TMSI 是 VLR 和 SIM 卡里两处保存的。

TMSI 重分配的实现在用户位置更新和呼叫建立及补充业务等业务过程都可以执行。这在 MSC 的 MAP 功能流程里选择是否执行 TMSI 的重新分配流程即可实现。

在位置更新时进行的 TMSI 重分配流程，是与位置更新接受融合在一起的。其流程图如图所示：

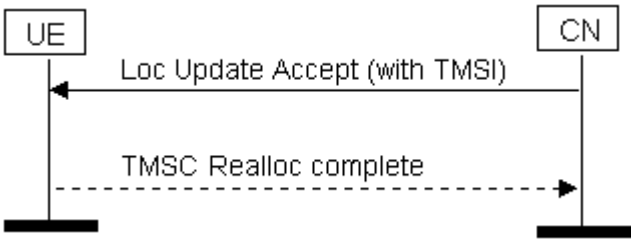


图6-27 位置更新时的 TMSI 重分配

& 说明：

在移动性管理过程中，鉴权、安全模式控制、TMSI重分配等几项过程属于可选过程。这些过程可以由网络运营商来决定是否激活或提供。

如MSC9800里是通过MAP功能流程配置参数来实现的。

6.5.8 联合位置更新

当用户终端所处的位置区与路由区都发生改变时，将发起联合位置更新过程：同时在 CS 域、PS 域发起位置更新。网络侧的 CS 域与 PS 域通过 Gs 接口相连（核心网的电路域、分组域分离组网时，下面的描述中将用 MSC 来代表 CS 域，SGSN 来代表 PS 域）。Gs 接口采用 No.7 信令上中的 BSSAP+协议，借助 Gs 接口，CS 域和 PS 域可互相更新数据库里保存的移动台的位置信息，这样可减少空中信令，而且有助于 MSC 通过 Gs 接口寻呼到正在进行 GPRS 业务的 B 类手机。

下图是一个典型的联合位置更新的流程图：

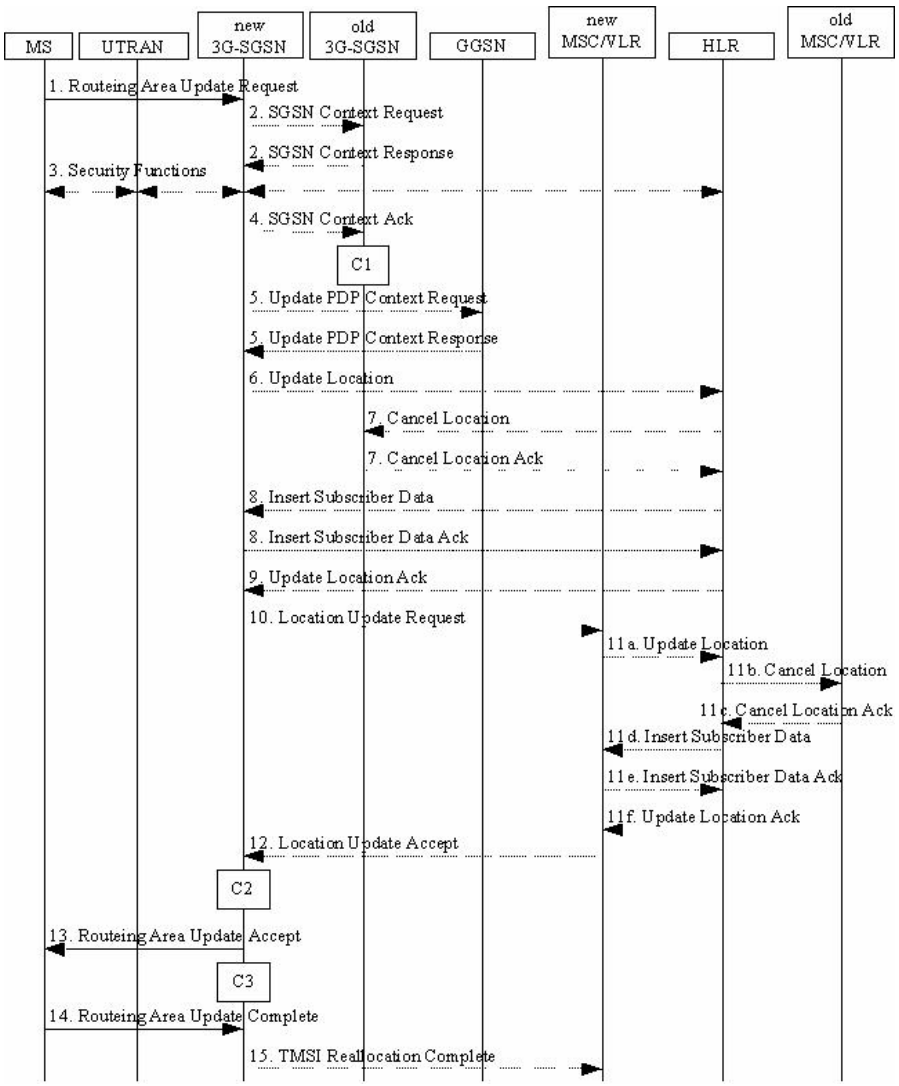


图6-28 联合位置更新

(1) SGSN 接收到手机的路由区更新请求后，如果需要则发起到 HLR 的位置更新。

(2) 如果 SGSN 和 MSC/VLR 之间配置有 Gs 接口，则 SGSN 发起到 MSC/VLR 的联合位置更新，否则直接下发路由区更新接受。

(3) MSC/VLR 接收到 SGSN 的位置更新请求后，执行 MSC/VLR 的位置更新处理和并记录关联数据。

(4) MSC/VLR 接收到 HLR 的位置更新接受后，通过 Gs 接收向 SGSN 发出位置更新接受消息。

(5) SGSN 接收到 MSC/VLR 的位置更新接受消息后，置关联数据，下发路由区更新接受。如果进行了 TMSI 重分配，则 SGSN 把手机上报的 TMSI 重分配完成转发给 MSC/VLR 完成联合位置更新流程。

6.6 分组域移动性管理流程

6.6.1 MM 功能概述

移动性管理（MOBILITY MANAGEMENT）的主要作用就是为了在本 PLMN 或是其他 PLMN 中，对用户的当前位置进行跟踪。比如用户想登录到 GPRS 网络，就必需首先执行附着（ATTACH）过程（它移动性管理的一个基本流程），使之相关信息在核心网络中进行注册。MM 和会话管理 SM（SESSION MANAGEMENT）、短消息 SMS（SHORT MESSAGE SERVICES）共同组成了 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。它的其他功能还包括用户的分离、安全流程、路由区更新、位置更新等。

1. 术语介绍

- GMM/PMM

GMM：GPRS Mobility Management GPRS 移动性管理（主要用来区别于 CMM Circuit Mobility Management）

PMM：Packet Mobility Management 分组移动性管理

在这里，我们可以简单认为 GMM 和 PMM 分别指的是 GSM 和 UMTS 系统中的移动性管理，本文主要介绍 UMTS 系统中分组域的移动性管理特性。

- RANAP

Radio Access Network Application Part 无线接入网络应用部分。RANAP 协议层封装、传输更高层的信令，处理 3G-SGSN 和 UTRAN 之间的信令，管理 IU 接口的 GTP 连接。

- MM CONTEXT

MM 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所示。

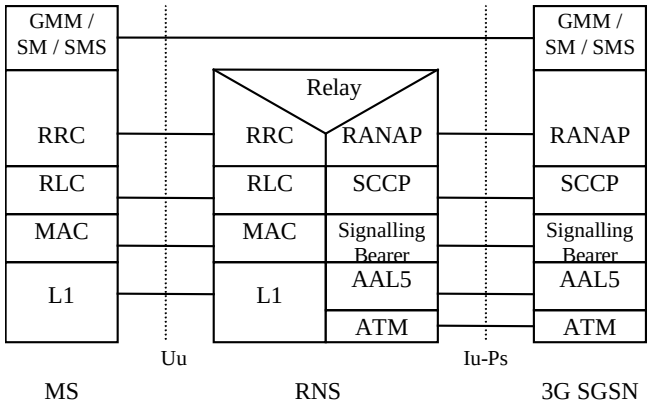


图6-29 UMTS 系统分组域手机和网络侧的控制面协议

6.6.2 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。

- PMM DETACHED State

在该状态下，MS 和 3G-SGSN 之间没有通讯，没有有效的位置信息和路由信息。MS 不可达，MS 位置不可知。

- PMM IDLE State

MS 位置可知，但处于空闲状态

- PMM CONNECTED State

MS 位置可知，PS 信令连接已经被建立。

具体 PMM 的状态迁移关系描述如下图所示。从图中，我们还可以看出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。也就是说 MM 状态只与 GPRS 的移动性管理活动有关，和 PDP 上下文的状态、数量没有任何联系。

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。

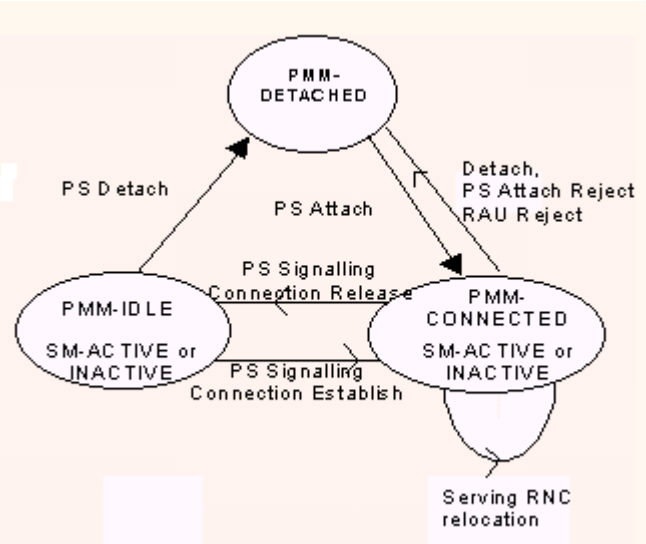


图6-30 UMTS 系统分组域移动性管理的状态迁移图

6.6.3 SGSN 和 MSC/VLR 之间的联系

在 UMTS 系统中，规定了 SGSN 和 MSC/VLR 之间的 Gs 接口。他们之间的关联关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）。

建立了 Gs 接口的联系后，系统便可以进行以下流程：

(1) 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。

(2) 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。

(3) 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。

(4) 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。

6.6.4 联合的 GPRS / IMSI 附着过程

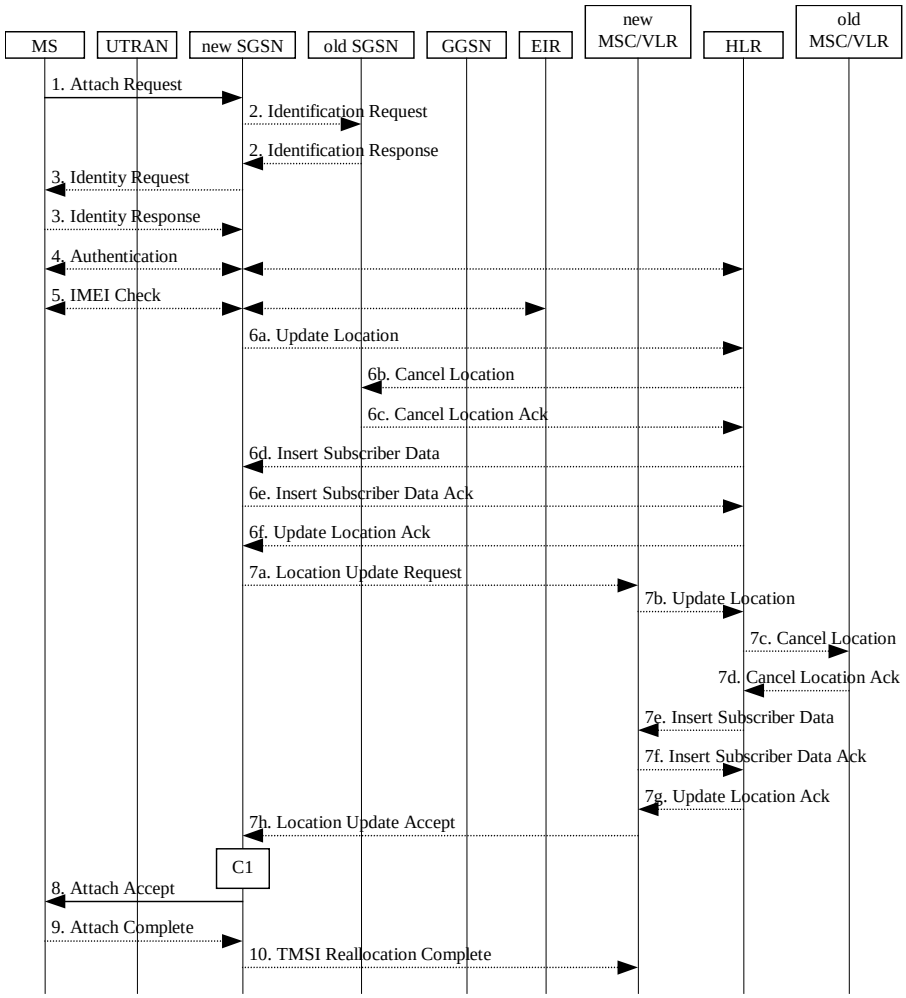


图6-31 附着流程

注：图中的 C1 为 CAMEL 点，可触发或进行智能业务。本章以下流程图中出现的 C1、C2、C3 等均为 CAMEL 点，不再注释。

1）用户通过发送附着请求消息发起附着流程。用户在附着请求消息中携带有 IMSI or P-TMSI and old RAI，Attach Type， old P-TMSI Signature， Follow On Request 等参数，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。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。具体过程如下：

SGSN 发送一条 UpdateLocation 消息（带有 SGSN 号码、SGSN 地址、IMSI）给 HLR；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；老 SGSN 以 Cancel Location Ack（带有 IMSI）消息确认收到 HLR 的 Cancel Location；HLR 发送插入用户签约数据消息（带有 IMSI、GPRS 签约数据）给新 SGSN；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）。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，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。

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。

6.6.5 分离功能

分离过程包括 MS 发起的、SGSN 发起的和 HLR 发起的分离过程（本文只介绍 MS 发起和 SGSN 发起的分离过程）。

1. MS 发起的分离

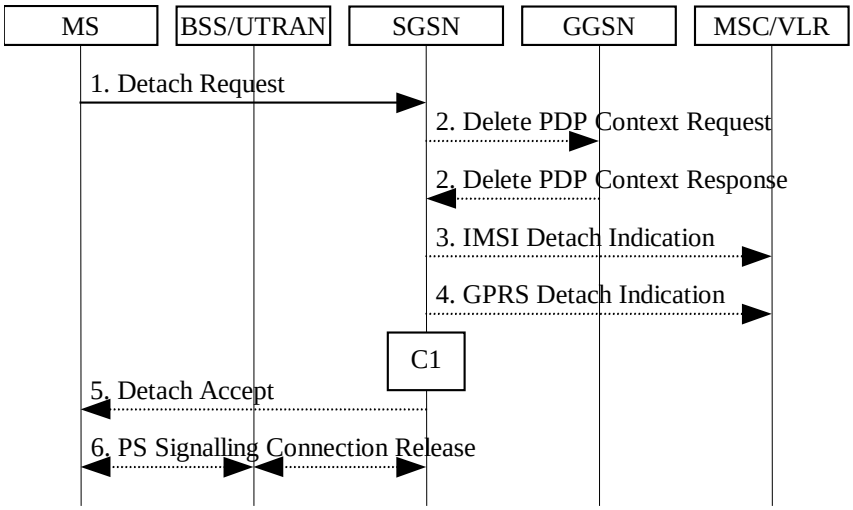


图6-32 MS 发起的分离

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. SGSN 发起的分离

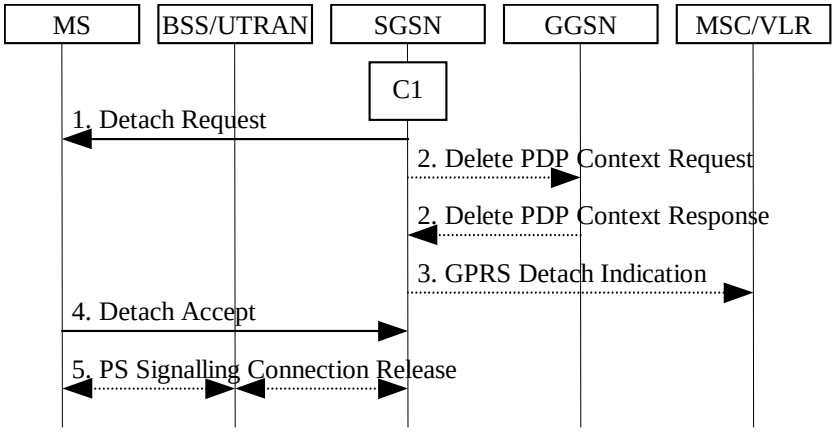


图6-33 SGSN 发起的分离过程

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。

6.6.6 安全流程（鉴权加密）

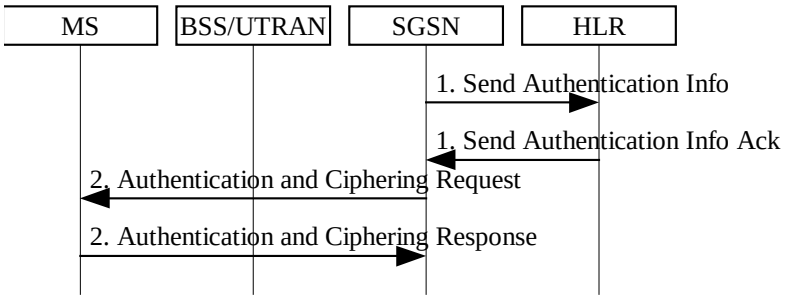


图6-34 鉴权加密

1）如果 SGSN 没有以前存储的 UMTS 五元鉴权组，向 HLR 发出一条发送鉴权信息（IMSI）消息。收到此消息，HLR/AUC 以鉴权信息确认消息给予回应，包含顺序排放的五元组。每一个五元组包含 RAND、XRES、AUTN、CK 和 IK。五元鉴权组的产生见 3G TS 33.102。

2）在对 UMTS 用户进行鉴权时，SGSN 选择下一组五元组并且包含属于这个五元组的 RAND 和 AUTN 于鉴权和加密请求消息中给用户。SGSN 还选择一个 CKSN 包含于消息中。

3）在收到这个消息时，用户手机中的 USIM 验证 AUTN，如果接受，根据协议 33.102 计算出 RAND 的签名 RES。如果 USIM 认为鉴权成功，用户返回鉴权和加密响应消息（RES）给 SGSN。同时，手机中的 USIM 也计算出 CK、IK，这些密钥同 CKSN 一起保存，直到 CKSN 在下一次鉴权后被更新。

如果 USIM 认为鉴权不成功，例如鉴权同步错误，用户返回鉴权和加密失败消息给 SGSN。

6.6.7 位置管理功能（路由区更新）

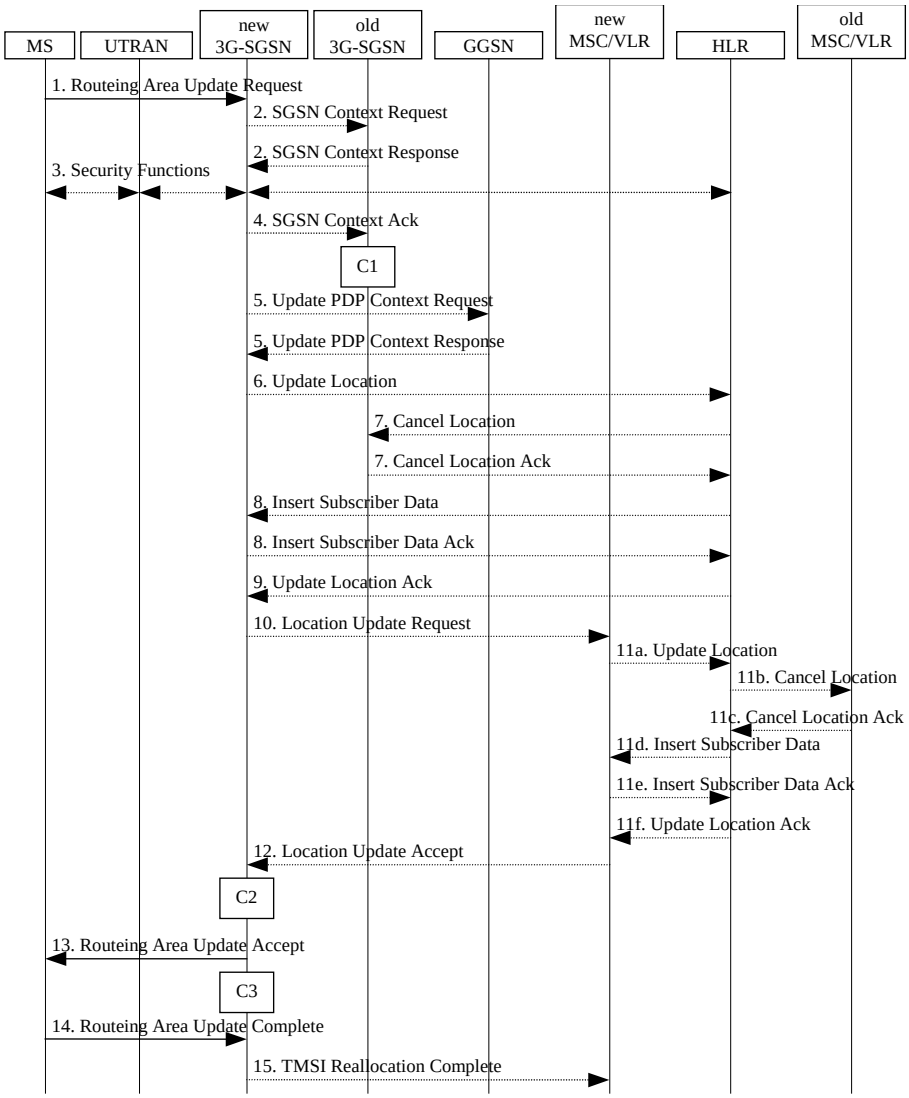


图6-35 路由区更新

1）如果没有 RRC 连接，先建立 RRC 连接。用户发送路由区更新请求消息（带有 P-TMSI、老 RAI、老 P-TMSI 签名、路由更新类型、跟随请求等）给新的 SGSN。如果用户有上传的信令或数据，跟随请求应该被置上。作为实现上的选择，SGSN 可以根据跟随请求标志，决定在路由更新流程结束后是否释放 Iu 连接。路由区更新类型应该指示：

路由区更新－－如果流程因为路由区改变引起；

周期性路由区更新－－如果流程因为周期性路由区更新定时器超时引起；

联合路由区更新－－如果用户是 IMSI 附着的，并且位置区更新应该在网络操作模式 I 情况下进行；

联合路由区更新伴随 IMSI 附着－－如果用户想要在网络操作模式 I 下进行 IMSI 附着；

服务RNC应该在将消息转发给SGSN前加上用户所在位置所属的路由区标识（包括路由区编码和位置区编码）。

2）如果路由区更新是跨越 SGSN 间的，并且用户处于 PMM-IDLE 状态，新 SGSN 发送 SGSN 上下文请求消息（带有用户老的 P-TMSI、老的 RAI、老的 P-TMSI 签名）给老的 SGSN，以得到用户的 MM 上下文和 PDP 上下文。老 SGSN 检验用户的 P-TMSI 和签名，如果不匹配回应合适的原因值。这将导致新 SGSN 发起安全流程。如果安全流程鉴权用户通过，新 SGSN 应该发送 SGSN 上下文请求消息（带有 IMSI、老的 RAI、用户已经验证标志）给老的 SGSN。用户已经验证标志指示新 SGSN 已经对用户进行鉴权。如果用户的签名合法或者经过新 SGSN 鉴权成功，老 SGSN 回应 SGSN 上下文响应消息（Cause、IMSI、MM 上下文、PDP 上下文）。如果用户在老 SGSN 中为未知，老 SGSN 回应以适当的原因值。老 SGSN 启动定时器。

3）安全流程可以在此处进行。如果鉴权失败，路由更新请求将被拒绝，新 SGSN 应该发送拒绝指示给老 SGSN。老 SGSN 应该继续如同没有收到过 SGSN 上下文请求消息一样。

4）如果是 SGSN 间的路由区更新，新 SGSN 应该发送 SGSN 上下文确认消息给老的 SGSN。老的 SGSN 在它的上下文中标记 MSC/VLR 关联、GGSN 和 HLR 中的信息为非法。如果在未完成正在进行的路由更新前，用户发起路由更新回到老 SGSN，这将引起 MSC/VLR、GGSN、HLR 被刷新。

5）如果是 SGSN 间的路由更新，并且用户处于 PMM-IDLE 状态，新 SGSN 发送修改 PDP 上下文请求消息（新 SGSN 地址、协商的 QoS、TEID）给相关的 GGSN。GGSN 更新它的 PDP 上下文，回应修改 PDP 上下文响应消息（TEID）给 SGSN。

6）如果是 SGSN 间的路由区更新，SGSN 以 Update Location 消息（SGSN 号码、SGSN 地址、IMSI）通知 HLR SGSN 的改变。

7）如果是 SGSN 间的路由区更新，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。老的 SGSN 以 Cancel Location Ack 消息（带有 IMSI）向 HLR 进行确认。

8)如果是 SGSN 之间的路由区更新，HLR 发送插入签约数据消息(带有 IMSI、GPRS 签约数据）给新 SGSN；新 SGSN 证实用户存在于新的路由区中，如

果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，同时可以回应插入用户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 插入用户签约数据确认消息（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 插入用户签约数据确认消息（带有 IMSI）。

9）如果是 SGSN 间的路由区更新，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。

10）如果路由更新类型是联合路由更新伴随 IMSI 附着，或者位置区发生改变，SGSN 和 VLR 之间的关联必须建立。新 SGSN 发送 Location Update Request 消息（带有新的位置区标识、IMSI、SGSN 号码、位置区更新类型）给 VLR。如果路由区更新类型是联合路由区更新伴随 IMSI 附着，位置区更新类型应该指示 IMSI 附着。否则，位置区更新类型应该指示正常位置区更新。VLR 的号码是通过以 RAI 查询 SGSN 中的表得到。SGSN 在上面的步骤 8，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。通过存储 SGSN 号码，VLR 创建或者更新同 SGSN 的关联。

11）如果在 VLR 中的用户签约数据被标记为未被 HLR 证实，新 VLR 将通知 HLR。HLR 删除老的 VLR 的数据，插入用户签约数据到新的 VLR。

12）新 VLR 分配新的 TMSI，回应 Location Update Accept（带有 VLR 号码、TMSI）消息给 SGSN，如果 VLR 没有改变，TMSI 分配是可选的。

13）新 SGSN 证实用户存在于新的路由区中，如果签约数据限制用户在此路由区附着或者签约数据检查失败，SGSN 应该拒绝用户附着请求，带上合适的原因值。如果所有签约数据检查通过，SGSN 为用户构造 MM 上下文。新 SGSN 回应用户路由更新接受消息（带有 P-TMSI、VLRTMSI、P-TMSI 签名）。

14）用户以附着完成消息给 SGSN 确认新分配的 TMSI。

15）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。

注：步骤 11、12 和 15 仅当步骤 10 发生时才发生。

6.6.8 服务请求

1. 手机发起的服务请求

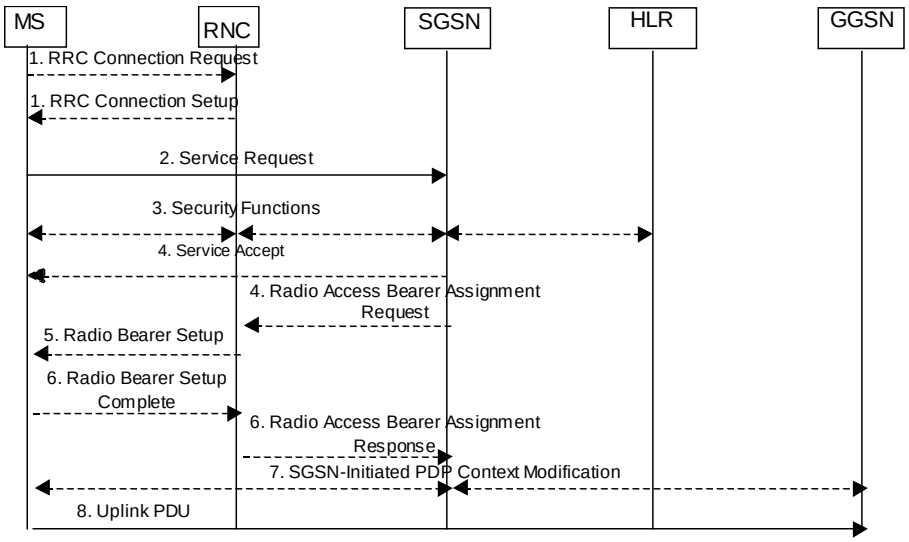


图6-36 手机发起的服务请求

1）如果没有 CS 通路，MS 建立 RRC 连接。

2）MS 发送 Service Requset （P-TMSI，RAI，CKSN，Service Type）消息给 SGSN。服务类型定义了所需要的服务。服务类型是数据和信令中的一个。此时，SGSN 可能会发起一个鉴权过程。

如果服务类型指明是数据：那么 MS 和 SGSN 之间的信令连接将被建立，同时为激活的 PDP 预留资源。

如果服务类型指明是信令：那么为上层信令传送的 MS 和 SGSN 之间的信令连接将被建立 。

3）如果 MS 在 PMM-IDLE 状态发起服务请求，SGSN 将发起安全流程。

4)如果网络侧在 PMM-CONNECTED 状态，并且服务类型是数据，如果 SGSN 接受服务请求，SGSN 将回应 Service Accept 消息给 MS，如果指明是数据类型，SGSN 发送 Radio Access Bearer Assignment Request （NSAPIRAB ID(s)，TEID(s)，QoS Profile(s)，SGSN IP Address(es)）消息重建无线接入承载给每一个激活的 PDP 上下文。

5）RNC 指示 MS 已经建立新的无线接入承载标识和相应的 RAB ID 。

6）SRNC 发送消息 Radio Access Bearer Assignment Response （RAB ID(s)， TEID(s)，QoS Profile(s)，RNC IP Address(es)）消息响应。GTP 隧

道已经在 Iu 接口上建立，如果 RNC 回应 Radio Access Bearer Assignment Response 消息，其中的原因值指明无法提供要求的 QoS，“Requested Maximum Bit Rate not Available”，那么 SGSN 将会再发送一个 Radio Access Bearer Assignment Request 消息带有不同的 QoS。重试的次数和新 QoS 的值与实现相关。

7）对每一个 RAB 重建修改了的 QoS，SGSN 发起一个 PDP 上下文修改过程通知 MS 和 GGSN 新的协商过的 QoS。

8）MS 发送上行包。

服务接受消息并不意味着 RAB(s)重建成功。

无论任何服务类型，如果服务请求不能被接受，网络侧将会回应一个服务拒绝消息并带上合适的原因给 MS。

当服务类型为数据时：如果 SGSN 重建 RAB(s)失败，SGSN 将会发起修改过程或者将 PDP 去激活，具体情况根据 QoS 协商决定。

2. 网络侧发起的服务请求

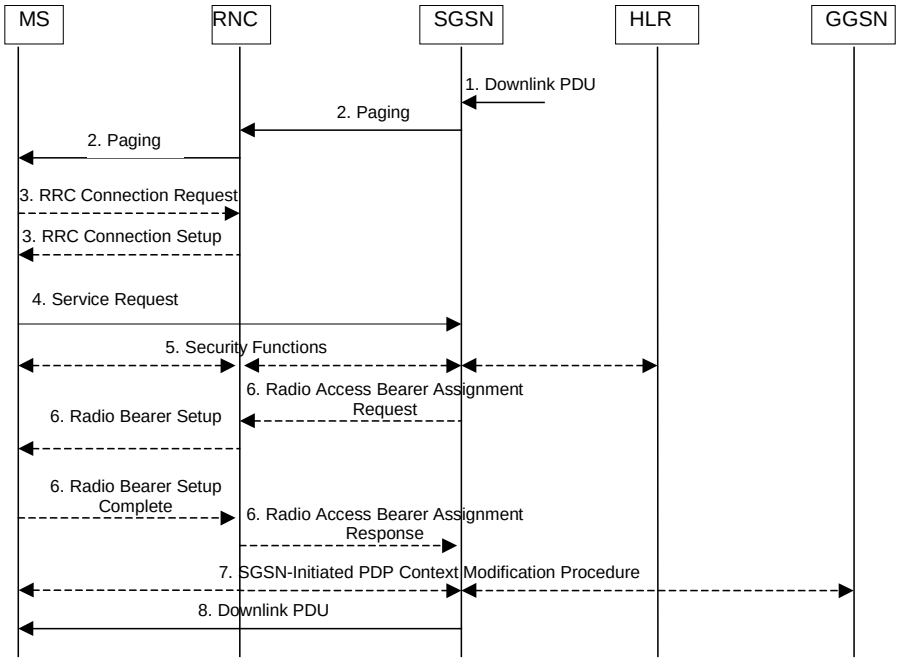


图6-37 网络侧发起的服务请求

1）SGSN 收到处在 PMM-IDLE 的 MS 的下行 PDP PDU。

2）SGSN 发送寻呼消息给 RNC，RNC 寻呼通过发送寻呼消息寻呼 MS。

3）如果没有 CS 通路 MS 建立 RRC 连接。

4）MS 发送 Service Request（P-TMSI，RAI，CKSN，Service Type）消息给 SGSN。服务类型为寻呼响应。此时，SGSN 可能发起一个鉴权。SGSN 知道下行包是否需要 RAB 重建。

5）SGSN 指定加密模式。

6）如果 PDP 上下文的资源重建，SGSN 发送 Radio Access Bearer Assignment Request （RAB ID(s)，TEID(s)，QoS Profile(s)，SGSN IP Address(es)）消息给 RNC。RNC 发送 Radio Bearer Setup （RAB ID(s)）消息给 MS。MS 发送 Radio Bearer Setup Complete 消息给 RNC。RNC 发送 Radio Access Bearer Assignment Response（RAB ID(s)，TEID(s)，RNC IP Address(es)）消息给 SGSN，指明 GTP 隧道已经建立在 Iu 接口，并且无线接入承载已经在 RNC 和 MS 之间建立。如果 RNC 回应的 Radio Access Bearer Assignment Response 消息中的原因值是要求的 QoS 无法提供。“Requested Maximum Bit Rate not Available”，那么 SGSN 将发送新的 Radio Access Bearer Assignment Request 消息携带 不同的 QoS。重试的次数与新的 QoS 参数和产品实现相关 。

7）对于每一个 RAB 重建修改 QoS，SGSN 会发起一个 PDP 上下文修改过程通知 MS 和 GGSN 新的 QoS。

8）SGSN 发送下行包。

如果服务类型为寻呼响应，MS 在收到 RRC 的安全模式控制消息后，认为服务请求已经被 SGSN 成功的收到了。

如果 SGSN 重建 RAB(s)失败，SGSN 将会发起一个修改过程。

6.7 呼叫控制

6.7.1 移动起始呼叫建立

当 UE 想发起一个呼叫时，UE 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，即 Iu 接口上的 SETUP 消息。CN 将建立一个到该 UE 的通信信道，并使用取到的被叫方 UERN 创建一个 IAM/IAI 消息发送到被叫方（值得注意的是本局内呼叫无 IAM/IAI，该消息只存在于 E 接口）。

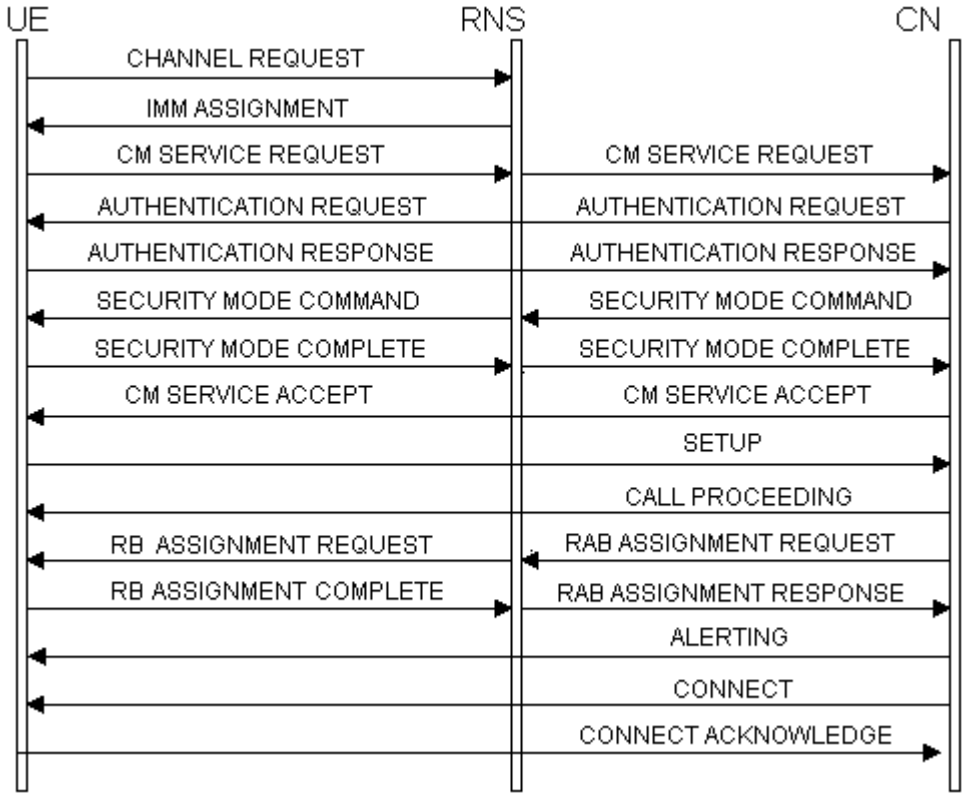


图6-38 移动起始呼叫建立过程

1）UE 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 UE 可占用指定的专用信道。

3）UE 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，UE 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 UE 分配一个通信信道。

8）当被叫振铃时，网络收到被叫的振玲消息 ALERTING 以后，则要向主叫 UE 发一个 ALERTING 消息，同时给主叫送回铃音。

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 UE 回 CONNECT ACKNOWLEDGE 消息之后即完成了呼叫建立的过程。

6.7.2 移动终止呼叫的建立

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。

若 CN 收到 IAM/IAI 消息或在本局内取到 MSRN 以后，如果允许该到来的呼叫建立，则 CN 要使用无线接口信令寻呼 UE。当 UE 以 PAGING RESPONSE 消息回应，CN 收到后即建立一个到 UE 的通信信道。

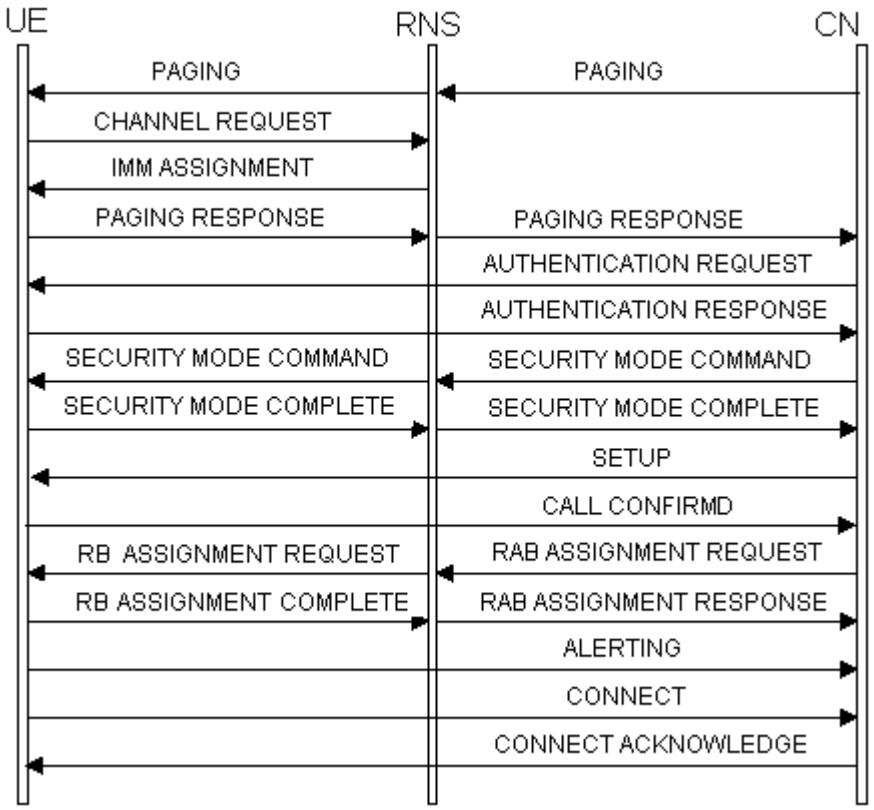


图6-39 移动终止建立过程

1）CN 向 RNS 发送一个 PAGING 消息，RNS 在寻呼信道上广播该寻呼消息。可以参考 6.6.4 的寻呼过程。

2）被叫 UE 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 UE 使用指定的信令信道。

3）然后 UE 将在该信令信道上发送一个寻呼响应消息，CN 收到 UE 的寻呼响应消息后，将发起鉴权和加密的安全过程（请注意这两个安全过程是可选的，可以由 MAP 功能流程进行配置）。

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及发起此次呼叫的主叫号码。

5）当 UE 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 UE 发指配消息命令 UE 调节到一个指定的通信信道上，UE 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 RESPONSE 消息。

8）UE 发送 ALERTING 消息指示被叫用户振铃。

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

10）CN 将给 UE 回应 CONNECT ACKNOWLEDGE 消息，呼叫建立过程结束。

6.7.3 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。

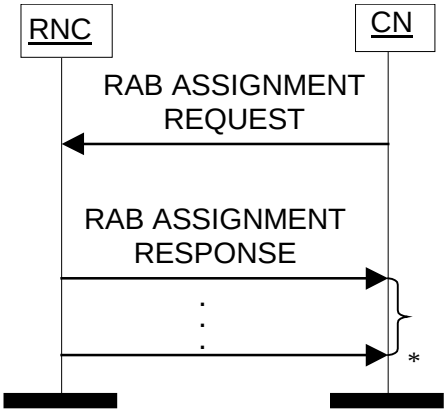
RAB 的优先级由 CN 根据签约信息、QoS 信息等内容决定。CN 在请求 RAB 建立、修改消息中指定优先级、预占能力和排队特性。UTRAN 执行 RAB 排队和资源预占。

2. RAB 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. RAB 建立，释放，修改控制流程



* it can be several responses

图6-40 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 RAB Assignment Response 消息给 CN 报告请求结果。在一条 RAB Assignment Response 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

下图简要的描述了在 CN 和 UE 之间经过 UTRAN 而建立 RAB 的流程。

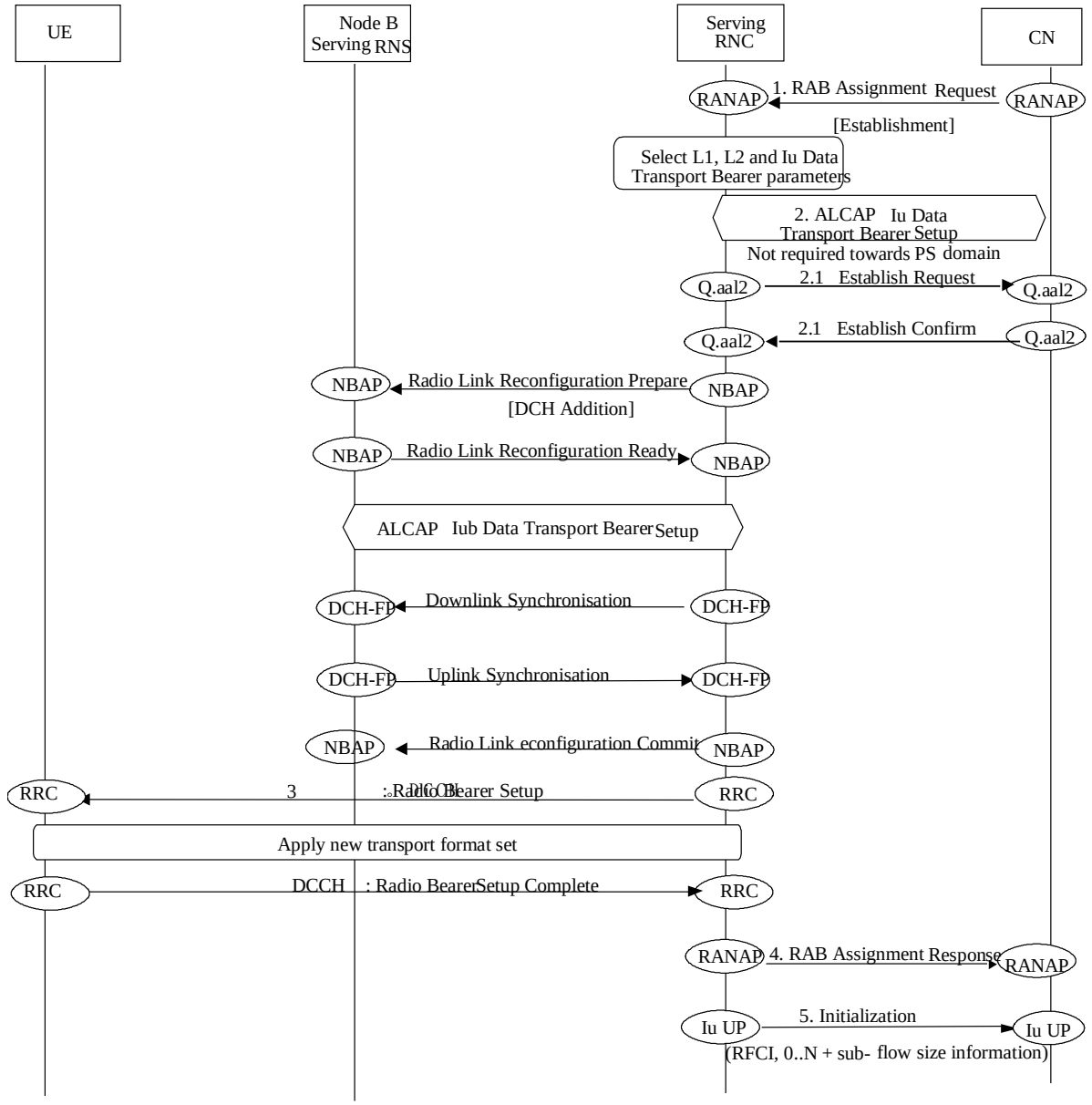


图6-41 无线接入承载建立-（DCH-DCH 同步建立流程）

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）。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

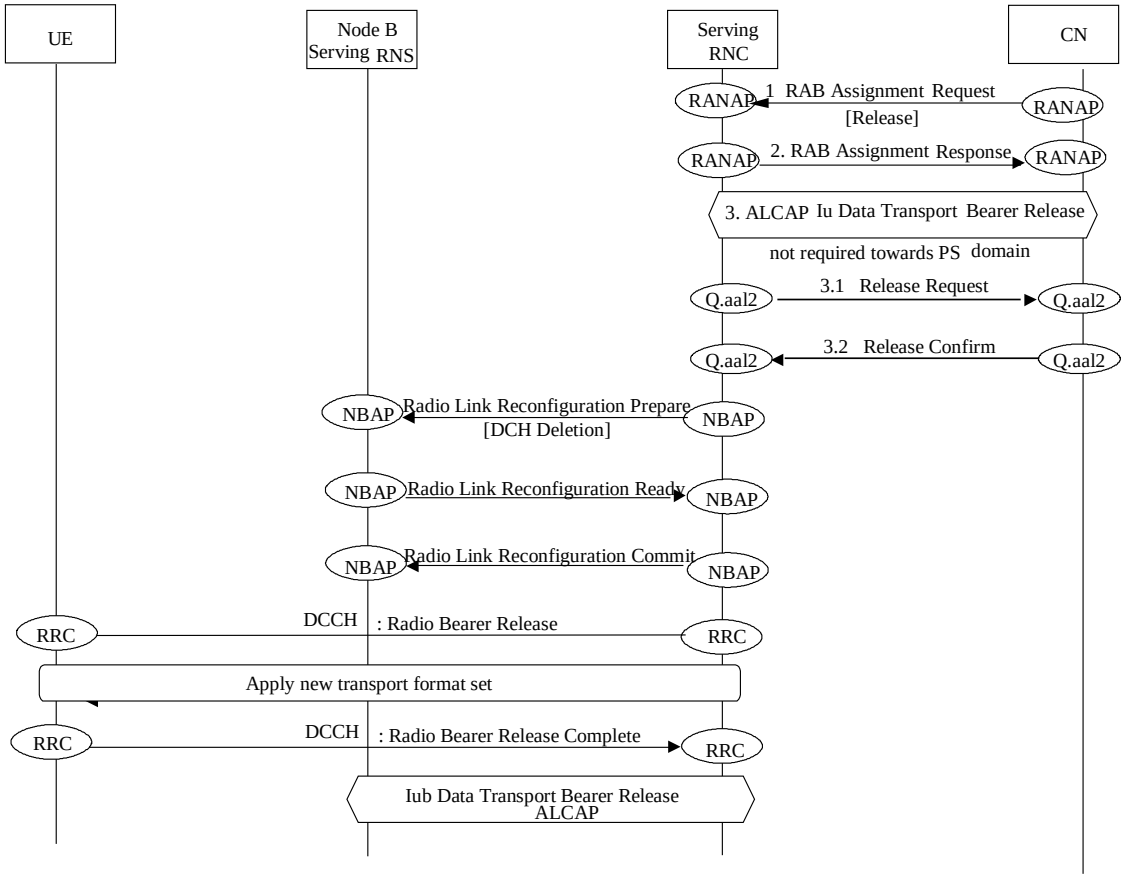


图6-42 无线接入承载释放-（DCH - DCH- 同步释放流程）

- 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

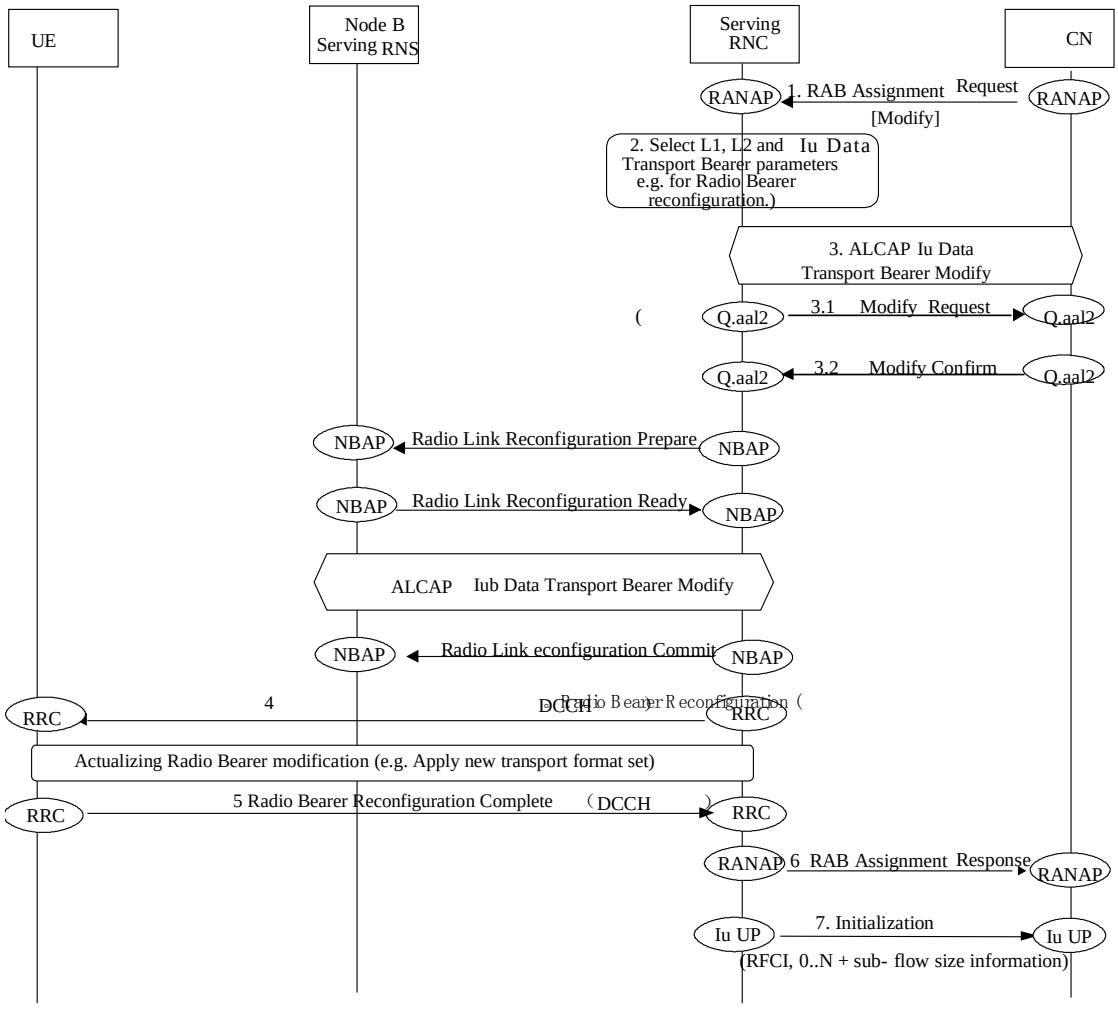


图6-43 无线接入承载修改（DCH-DCH 同步修改）

- 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。

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。

6.7.4 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 Iu 接口重复发寻呼的过程。一般来说，重复发寻呼的次数已经他们之间的时间间隔可以在 CN 处控制。

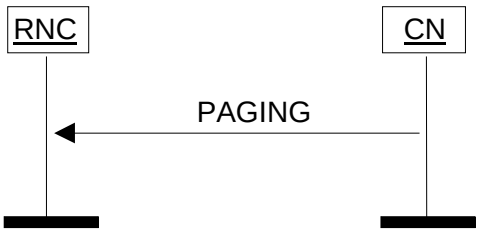


图6-44 成功寻呼流程

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 Iu 接口重复发送寻呼消息。

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（LAI)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。

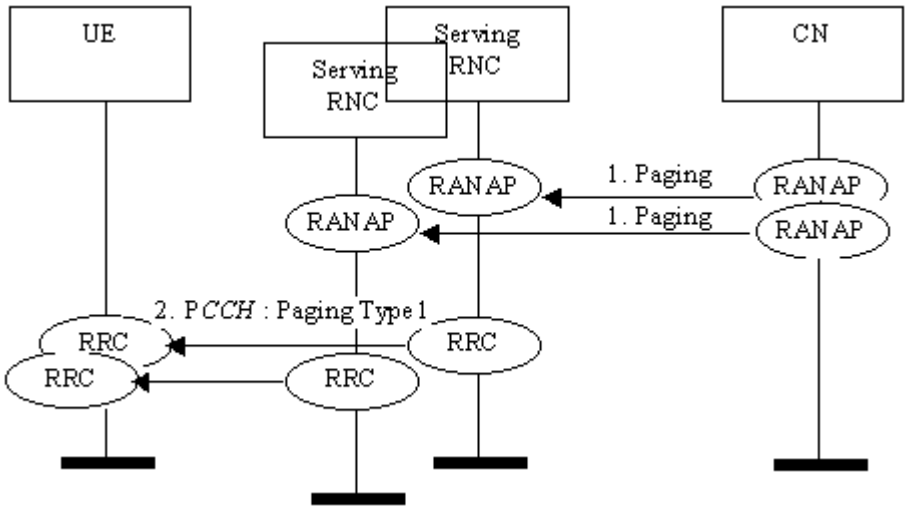


图6-45 RRC 空闲状态下寻呼过程

1）CN 通过发起的寻呼消息，跨过两个 RNC 到达被寻呼 UE。注意此时在 IU 接口上看到的就是 CN 连续发两条 PAGING 消息，里面所携带的 LAI 都是一样的，只是 DPC 分别为两个 RNC 而已。

2）小区 1 用 Paging　Type 1 发起寻呼。

3）小区 2 用 Paging Type 1 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 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。

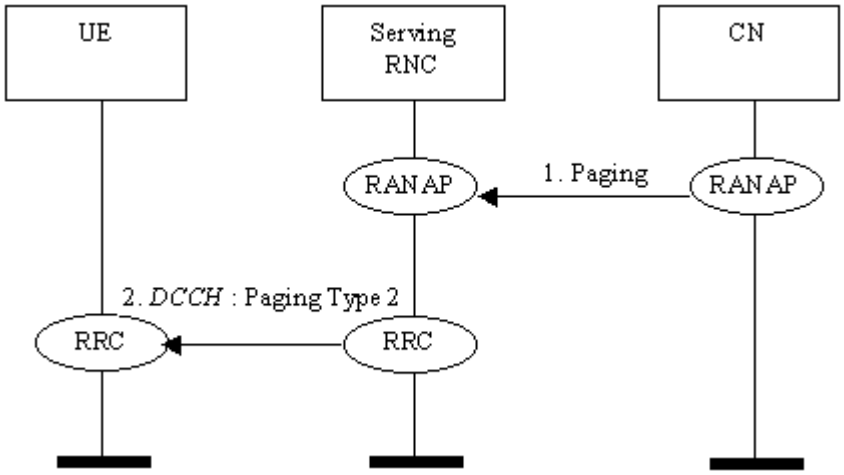


图6-46 在 RRC 连接状态（CELL_DCH 和 CELL_FACH)下寻呼 UE 过程

1）CN 通过 RANAP 发送 PAGING 消息来对 UE 寻呼。

2）SRNC（Sercing RNC）对 RRC（UE）发送消息 Paging Type 2。

& 说明：

Paging Type 1**是用于UE空闲时从PCCH上下发**；Paging Type 2是用于RRC连接状态时从DCCH下发，**典型情况如UE在PS业务时下发CS的寻呼消息就用**Paging Type 2，**不过**Paging Type**是由RNC控制的**，CN**无需知道。**

6.7.5 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 PLMN 之间或 PLMN 与别的网络之间的电路交换连接而释放呼叫。

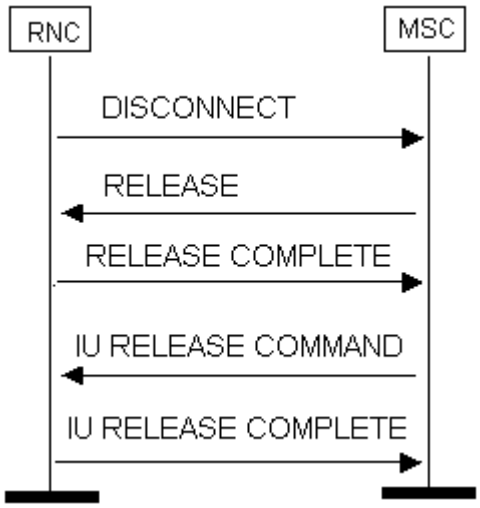


图6-47 移动发起呼叫释放的成功情况

1）移动台挂机之后，移动台通过向网络发送 DISCONNECT 消息而发起呼叫清除；此时消息里的释放原因是：Normal Call Clearing。

2）网络接收到该消息之后发送一个 RELEASE 消息给移动台；

3）移动台发 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。

6.8 分组域会话管理流程

6.8.1 SM 基本概念

1. SM 功能概述

会话管理（SM）的主要目的就是建立、修改和释放分组域承载。它是 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 ADDRESS

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。

每个 GPRS 签约数据包含一个或多个 PDP 地址，每个 PDP 地址由 MS、SGSN、GGSN 中的一个或多个 PDP Context 描述，每个 PDP Context 存在两种状态（INACTIVE 状态和 ACTIVE 状态），其状态转换关系见下图。PDP 状态指示该 PDP 地址的数据是否可以传送。 非激活的会话不包含路由信息，不能进行数据的转发。用户的所有 PDP Context 都与该用户的 MM Context 相关联。

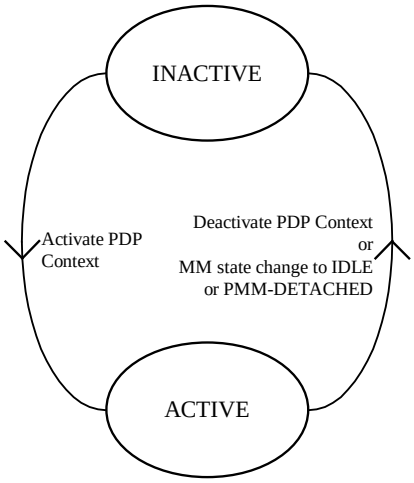


图6-48 PDP 状态机模型

2）NSAPI

在 MS 中 NSAPI 用于标识一个 PDP 服务访问点，在 SGSN/GGSN 中用于标识一个会话。其取值等于接入层用来标识用户 RAB 的 RAB ID

4）APN 解析

Access Point Name，采用标准域名格式。APN 包括两部分：网络名（NI）和运营商名（OI）。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）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

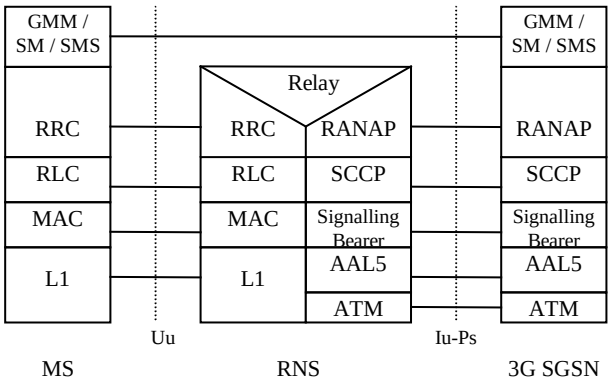


图6-49 UMTS MS-SGSN 的控制面协议

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。

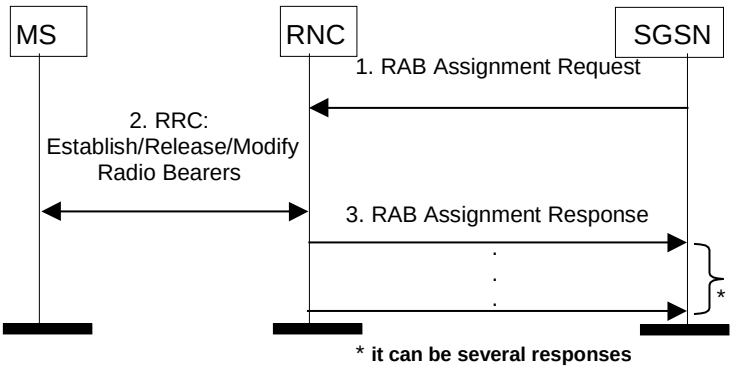


图6-50 RAB 管理流程图

流程说明：

1）SGSN 向 RNC 发送 RAB Assignment 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。

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。

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 过程进行 RAB 的重建时，可以立刻恢复数据传送。

6.8.2 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（本文只介绍 MS 发起的 PDP 激活流程）。

1. MS 发起的 PDP Context 激活

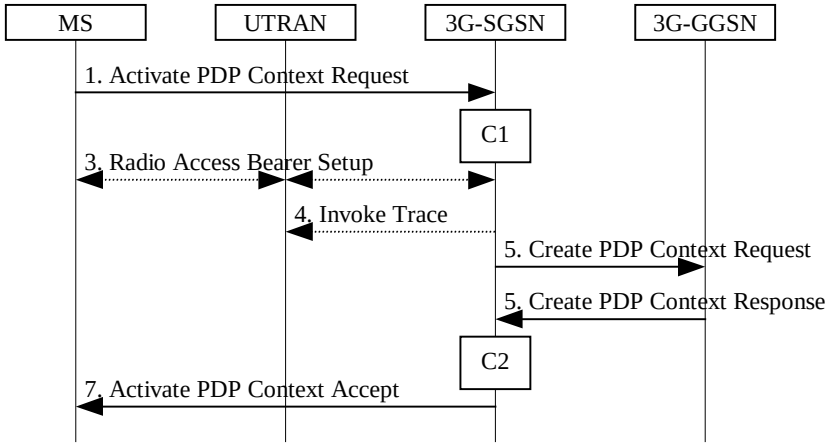


图6-51 MS 发起的 PDP CONTEXT 激活过程

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，然后向 GGSN 发创建 PDP Context 请求。

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。

注：在 R99 的激活流程中，如果 GGSN 已经降低 Qos，并不通知 RNC，那么在 SGSN 的两侧资源使用并不一致，空口处的资源可能比网络分配的资源

还要高，造成空口资源浪费。R4 中，SGSN 先与 GGSN 交互，创建 GTP 隧道，然后再建立 RAB，建完 RAB 后，是一个可选的更新 GGSN 流程（如果在 RAB 中建立过程中降低 QOS，则发起更新流程，将 SGSN 两侧的资源同步）。

6.8.3 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 修改过程和由于 RAB/IU 释放，SGSN 发起 PDP CONTEXT 修改流程（本文只介绍 MS 发起的 PDP Context 修改过程和 SGSN 发起的 PDP Context 修改过程）；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）和 TFT（MS 发起的修改过程）。

1. SGSN 发起的 PDP Context 修改

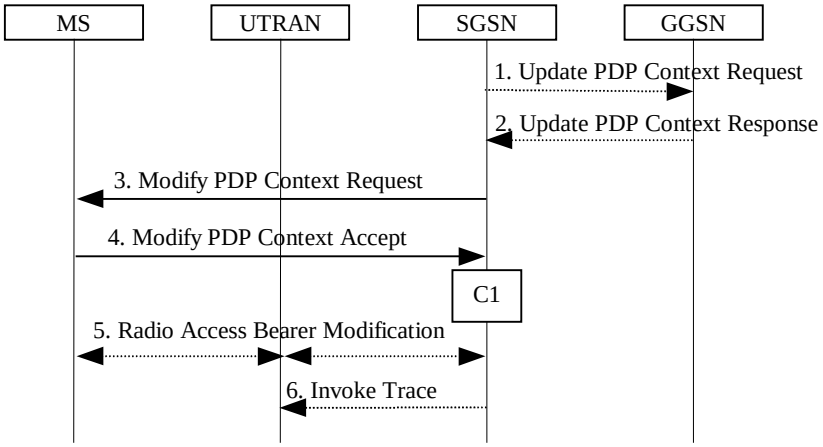


图6-52 SGSN 发起的 PDP CONTEXT 修改过程

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 BSS 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

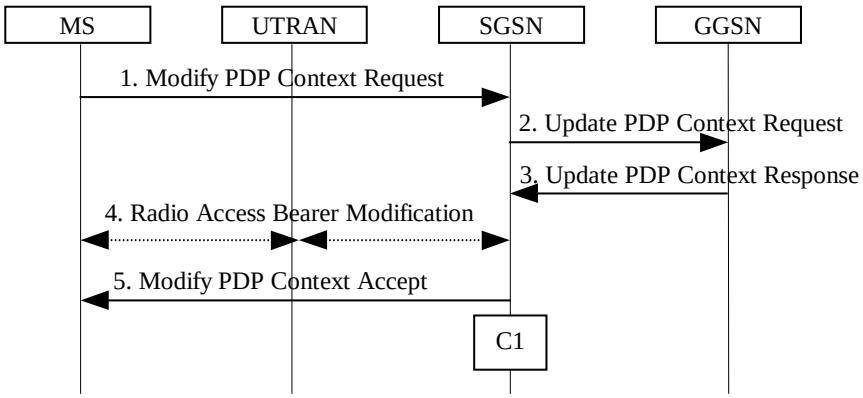


图6-53 MS 发起的 PDP CONTEXT 修改过程

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。

6.8.4 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（本文只介绍 MS 发起的 PDP Context 去激活过程和 SGSN 发起的 PDP Context 去激活过程）。

1. MS 发起的 PDP Context 去激活

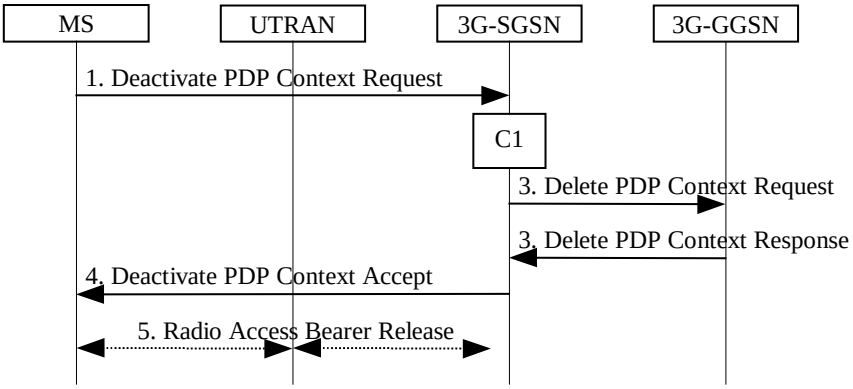


图6-54 MS 发起的 PDP Context 去激活过程

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。

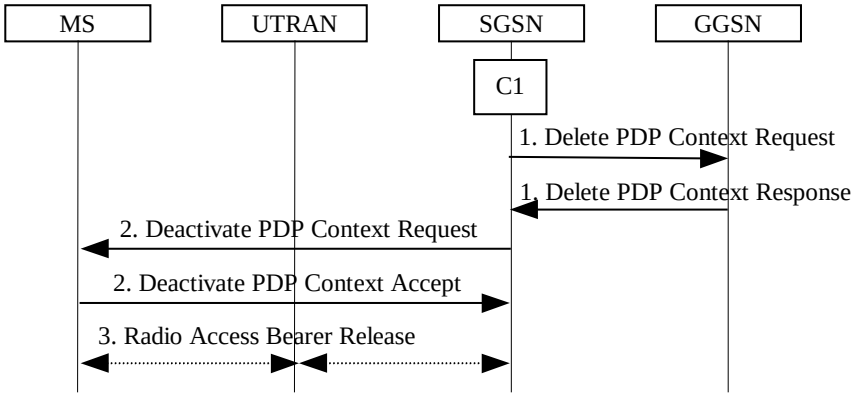


图6-55 SGSN 发起的 PDP Context 去激活

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。

6.8.5 保留过程和 RAB 重建

在 RNC 发起的 RAB 释放和 IU 释放时，可以不释放 PDP CONTEXT，而是把 PDP CONTEXT 保留下来，不做任何更改，RAB 将在以后的 Sevice Request 过程中重建。

1. MS 发起 Service request 进行 RAB 重建

当 MS 有上行的数据传输需求，PDP CONTEXT 处于激活状态而 RAB 不存在时，MS 发起 Sevice Request 过程为激活的 PDP CONTEXT 重建 RAB。过程描述如下：

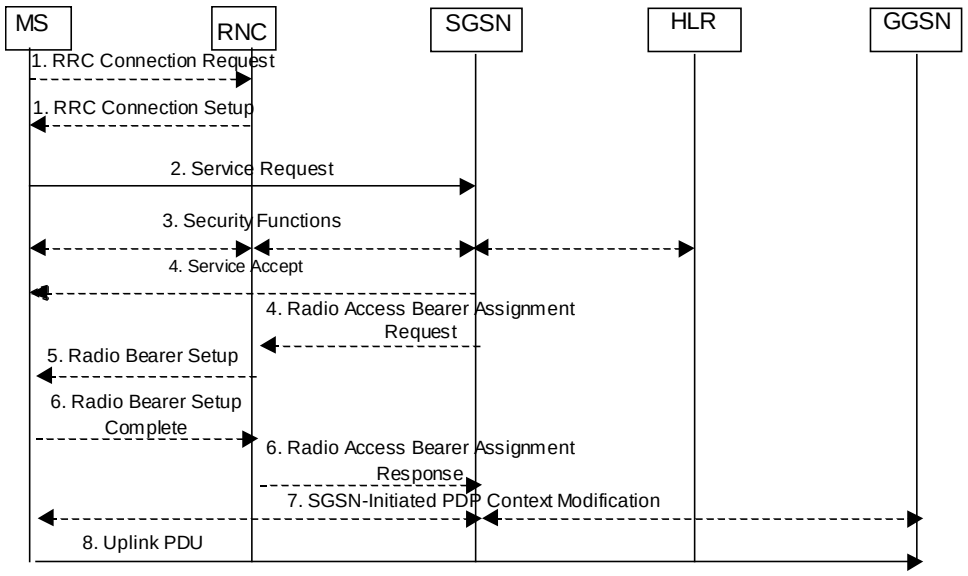


图6-56 MS 发起 Service request 进行 RAB 重建

1）如果没有 RRC 连接，建立 RRC 连接；

2）MS 向 SGSN 发送 Service Request（P-TMSI，RAI，CKSN，Service Type）消息，Service Type=data；

3）执行安全流程；

4）SGSN 向 MS 发送 Service Accept，对用户每个处于激活状态但 RAB 已释放的 PDP CONTEXT 进行 RAB 的重新建立；

5）如果建立的 RAB 的 QoS 发生改变，执行 SGSN 发起的 PDP CONTEXT 修改流程将 QoS 通知 MS 和 GGSN；

6）MS 进行上行数据传送。

2. SGSN 发起 Service Request 过程进行 RAB 重建

当 SGSN 收到下行的信令或数据包后，发现用户处于 PMM-IDLE 状态，则要发起寻呼。MS 在收到寻呼后，发送 Sevice Request 请求，sevice type="paging response"。如果是由于 SGSN 收到数据包引起的 Service Request 过程，则要调用 RAB Assignment 过程 进行 RAB 重建。

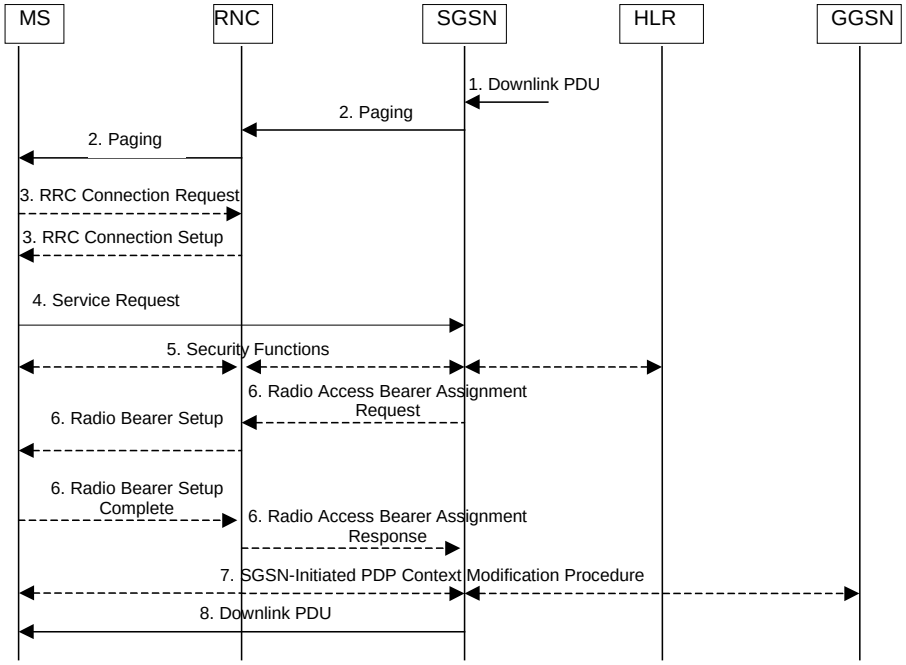


图6-57 SGSN 发起 Service Request 过程进行 RAB 重建