第 3 章

LTE 信令流程

信令是控制和保障整个通信过程的一套机制，贯穿于整个通信过程。信令的功能类似人类的大脑和神经系统，是通信的重要组成部分，在通信过程中扮演着不可替代的管控角色。在网络优化过程中，通常遇到的问题具有一定的模糊性，无法精确定位问题所在。对于从事网络优化的工程师来讲，在断定复杂问题（Trouble Shooting）过程中，遇到的部分网络问题已经无法用常规的经验去分析和解决，需要依靠信令分析进行辅助去定位原因。信令分析的过程，由于其数据采集的充分性、全面性和精确性，能够高效地进行问题定位。因此，掌握信令及流程分析对于网优工作尤其是判断复杂网优问题起着举足轻重的作用。

本章首先介绍 LTE 系统中关于信令的一些基本概念，然后按照基本信令流程、端到端信令流程和移动性管理流程三个维度，对各类信令及流程做了详细的分析和解释。建议读者把本章介绍的信令流程和上一章相应的业务过程进行比对，在对常见信令流程有清晰认识的基础上，可以更加深入地理解 LTE 网络的业务过程。

3.1 信令相关的基本概念

在描述信令流程之前，首先介绍与信令相关的几个基本概念，包括控制面与用户面、UE 的 6 种不同网络标识、无线承载和信令承载，以便于读者理解相关信令构成。

3.1.1 控制面与用户面

第 2 章已经就 LTE 的系统架构和通信协议进行了相关介绍，在 LTE 无线通信系统中，协议分为控制面和用户面两类。用户面协议负责解决传送“什么内容”的问题，具体对应传送和处理用户的数据流，如语音数据和分组业务数据；而控制面协议负责如何把数据通过网络传递到对方，具体对应传送和处理系统的信令。

从协议栈的角度看，信令分为接入层（AS）信令和非接入层（NAS）信令。RRC 和 RANAP 层及其以下的协议层统称接入层，接入层流程中 eNodeB 需要参与处理。RRC 之上的移动性管理（Mobility Manangement，MM）、会话管理（Session Management，SM）、呼叫控制（Call Control，CC）、短消息服务（Short Message Service，SMS）等称为非接入层，非

接入层的流程中只有 UE 和 CN 需要处理信令。即接入层信令是为非接入层信令的交互铺路搭桥的，通过接入层的信令交互，在 UE 和 CN 之间建立起信令通路，从而让 UE 和 CN 进行非接入层的直接沟通。

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

通过图 3-1 可以了解数据流和信令流在协议栈中的不同走向和各自的通道。例如，信令流在控制面协议栈，从 UE 侧始于 NAS，然后通过 RRC、PDCP、RLC、MAC、PHY 层到达 eNodeB，最终止于 MME 的 NAS。

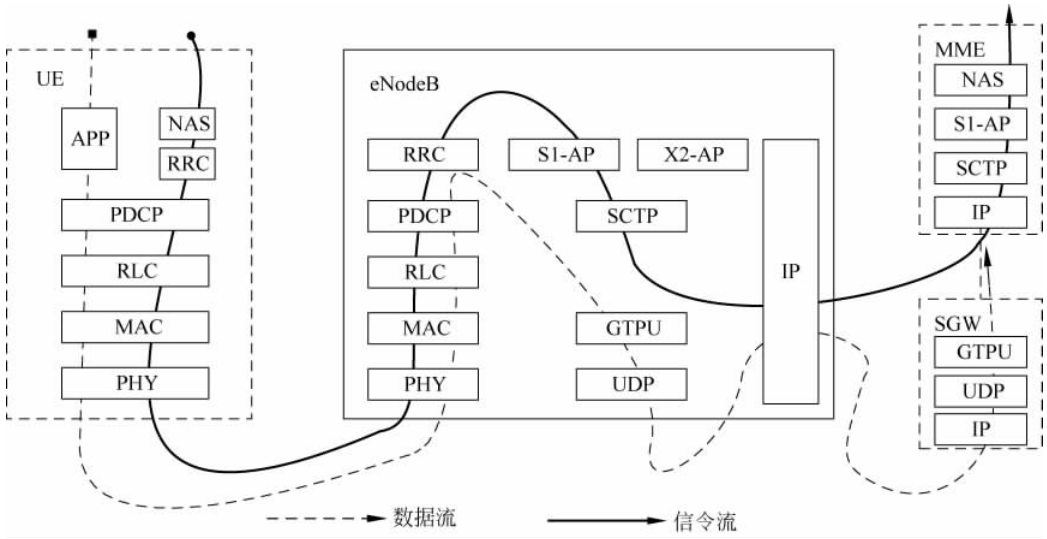

图 3-1　数据流、信令流与协议栈

3.1.2　UE 的不同网络标识

在 EPC 中，UE 一共有 6 种不同的标识，包括国际移动用户识别码(International Mobile Subscriber Identity，IMSI)、国际移动设备识别码(International Mobile Equipment Identity，IMEI)、SAE 临时移动台识别码(SAE Temporary Mobile Station Identifier，S-TMSI)、国际移动设备识别码和软件版本号(IMEI and Software Version Number，IMEISV)、全球唯一临时 UE 标识(Globally Unique Temporary UE Identifier，GUTI)和 IP，各个标识的生命期、有效期、功能和分配方式均不相同。这些标识用户身份的 ID 在建立 RRC 连接时发送到 eNodeB 进行用户身份识别。

(1) IMSI 是运营商给 UE 分配的一个永久标识，开户就有，IMSI 存储在 SIM 卡和 HSS 中，是 3GPP 的 PLMN 中全球唯一标识。

(2) IMEI 是由设备(手机)制造商给 UE 设备分配的一个永久标识，IMEI 存储在 SIM

卡和 HSS 中，可防止不法手机的再使用等，目前中国未使用。

(3) S-TMSI 是临时的 UE 识别号，由 MME 产生并分配，用于 NAS 交互过程中保护用户的 IMSI 不暴露，其中 S 代表 SAE，与 M-TMSI 一致。

(4) IMEISV 是携带软件版本号的国际移动台设备标识，用 16 位数字表示。

(5) GUTI 在网络中唯一标识 UE 终端，可以减少 IMSI、IMEI 等用户私有参数暴露在网络传输中。GUTI 是由核心网分配的一个动态标识，存储在 UE 和 MME 中。只有在 EPC 注册同时附着 MME 的 UE，GUTI 才有效。

(6) IP 地址是 PGW 分配的一个动态的标识。在上下文本存在时有效。

在小区(eNodeB)内，UE 的标识如表 3-1 所示。其中，C-RNTI(Cell Radio Network Temporary Identifier)是小区无线网络临时标识，是由 eNodeB 分配给 UE 的一个动态标识，唯一标识了一个小区空中接口下的 UE，只有处于连接态下的 UE，C-RNTI 才有效。而 T-RNTI 是临时的 C-RNTI，连接态建立后 T-RNTI 会晋升为正式的 C-RNTI。RA-RNTI (Random Access Radio Network Temporary Identifier)是随机接入无线网络临时标识，接收端 UE 知道自己之前的 Preamble 发送位置，通过计算可以检测 PDCCH 上是否有自己对应的 RA-RNTI；如有，则说明接入被响应。RA-RNTI 对于 FDD-LTE 系统是 10 个，对于 TDD-LTE 系统最多 60 个。

表 3-1　eNodeB 内 UE 的标识

标识类型	应用场景	获得方式	有效范围	是否与终端/卡相关
RA-RNTI	随机接入中用于指示接收随机接入响应消息	根据占用的时频资源计算获得(0001～003C)	小区内	否
T-CRNTI	随机接入中，没有进行竞争裁决前的 C-RNTI	eNodeB 在随机接入响应消息中下发给终端(003D～FFF3)	小区内	否
C-RNTI	用于标识 RRC Connect 状态的 UE	初始接入时获得(T-CRNTI 升级为 C-RNTI) (003D～FFF3)	小区内	否
SPS-CRNTI	半静态调度标识	eNodeB 在调度 UE 进入 SPS 时分配(003D～FFF3)	小区内	否
P-RNTI	寻呼	FFFE(固定标识)	全网相同	否
SI-RNTI	系统广播	FFFF(固定标识)	全网相同	否

3.1.3　承载的定义及分类

在 LTE 系统中，把 UE 和 P-GW 之间具有相同 QoS 的业务数据流的逻辑聚合称为一个 EPS 承载(Bearer)。

如图 3-2 所示，端到端的服务可以分为 EPS 承载和外部承载，EPS 承载又包括 E-RAB 和 S5/S8 承载。E-RAB 分为无线承载和 S1 承载。无线承载(Radio Bearer，RB)是 UE 到

eNodeB 空中接口之间的一段，用于承载空中接口 RRC 信令和 NAS 信令。S1 承载是 eNodeB 到 S-GW 之间的一段，主要承载 eNodeB 与 MME 间 S1-AP 信令。另外，NAS 消息也可作为 NAS PDU 附带在 RRC 消息中发送。S5/S8 是 S-GW 和 P-GW 的接口，S5/S8 承载用于在 S-GW 和 P-GW 间传输 EPS 承载的分组包。

EPS 承载旨为在 UE 和 PDN 之间提供某种特性的 QoS 传输保证，分为默认承载和专用承载。默认承载是一种满足默认 QoS 的数据和信令的用户承载，可简单地理解为一种提供尽力而为的 IP 连接的承载。默认承载随着 PDN 链接的建立而建立，随着 PDN 链接的拆除而销毁。专用承载是在 PDN 链接建立的基础上建立的，为了提供某种特定的 QoS 传输需求而建立的。一般情况下，专用承载的 QoS 比默认承载的 QoS 要求高。

在一个 PDN 链接中，只有一个默认承载，但可以有多个专用承载。一般来说，一个用户最多可建立 11 个承载。每当 UE 请求一个新的业务时，S-GW/P-GW 将从 PCRF 收到策略和计费控制(Policy and Charging Control，PCC)规则，其中包括业务所要求的 QoS。如果默认承载不能提供所要求的 QoS，则需要建立专用承载以提供服务。

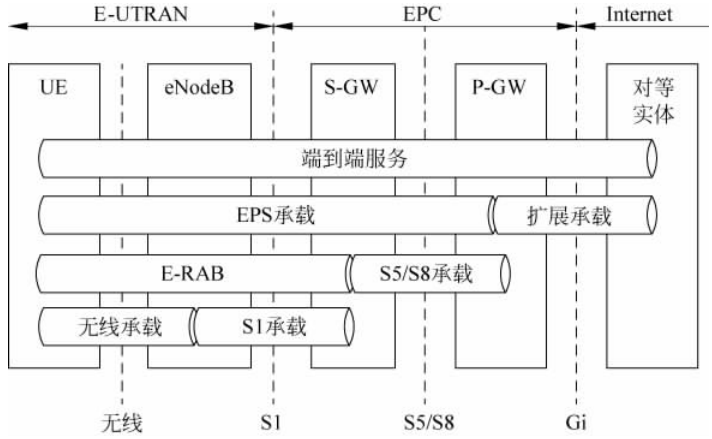

图 3-2　承载的位置关系

无线承载根据用户业务需求和 QoS 的不同，可以分为保证比特速率(Guaranteed Bit Rate，GBR)和不保证比特速率(Non-GBR)承载。GBR 是保证比特速率承载，在承载建立或修改过程中通过例如 eNode B 的接纳控制等功能永久分配给某个承载。这个承载在比特速率上要求能够保证不变。否则，如果不能保证一个承载的速率不变，则是一个 Non-GBR 承载。对同一用户同一链接而言，专用承载可以是 GBR 承载，也可以是 Non-GBR 承载。而默认承载只能是 Non-GBR 承载。

无线承载根据承载的内容不同，分为信令无线承载(Signaling Radio Bearer，SRB)和数据无线承载(Data Radio Bearer，DRB)。DRB 承载用户面数据，通过 eNodeB 为其分配的 PDSCH 来承载。根据 QoS 的不同，UE 与 eNodeB 之间可能最多建立 8 个 DRB。

SRB 根据承载的信令不同分为 SRB0、SRB1 和 SRB2 三类，如表 3-2 所示。

（1）SRB0：承载 RRC 连接建立之前的 RRC 信令，通过 CCCH 逻辑信道传输，在 RLC 层采用 TM 模式。

（2）SRB1：承载 RRC 信令（可能会携带 NAS 信令）和 SRB2 建立之前的 NAS 信令，通过 DCCH 逻辑信道传输，在 RLC 层采用 AM 模式。

（3）SRB2：承载 NAS 信令，通过 DCCH 逻辑信道传输，在 RLC 层采用 AM 模式，SRB2 优先级低于 SRB1，安全模式完成后才能建立 SRB2。

UE 的 RRC 连接未建立时，由 SRB0 承载 RRC 信令；SRB2 未建立时，由 SRB1 承载 NAS 信令。

表 3-2　SRB 承载信道及承载消息

SRB 类型	承载逻辑信道	承载消息类别	承载消息内容
SRB0	CCCH	RRC 消息	RRC 连接请求、连接建立、拒绝、重建请求、重建成功和重建拒绝等
SRB1	DCCH	RRC 消息和部分 NAS 消息	RRC 连接建立完成、重建完成、重配、重配完成以及 RRC 连接释放等
SRB2	DCCH	NAS 消息	上下行直传消息

3.2　基本信令流程

对网优工程师来说，需要熟悉掌握的基本信令流程包括随机接入、RRC 建立、RRC 释放、RRC 重建、RRC 重配置、寻呼、语音的电路域回落、紧急呼叫以及 LTE 测量等流程。

3.2.1　随机接入流程

随机接入使 UE 终端与网络建立通信连接成为可能，简单来讲就是确保 UE 与 eNodeB 建立无线链路，获取或恢复上行同步。用户的随机性和无线环境的复杂性决定了接入的发起以及分配的资源具有随机特征，因此，随机接入的成功率取决于随机接入流程是否顺利完成。

随机接入发起的目的主要包括：①请求初始接入；②从空闲状态向连接状态转换；③支持 eNodeB 之间的切换过程；④取得或恢复上行同步；⑤向 eNodeB 请求 UE-ID；⑥向 eNodeB 发出上行发送的资源请求。

在第 2 章中提到，随机接入分为竞争性随机接入和非竞争性随机接入两类。前者是 UE 从基于冲突的随机接入前缀中依照一定算法随机选择一个随机前导序列，后者是基站侧通过下行专用信令给 UE 指派非冲突的随机接入前导序列。

基于竞争模式的随机接入包括三种场景：①RRC_IDLE 状态下的初始接入；②无线链路失败以后的初始接入；③RRC_CONNECTED 状态下，当有上行数据需要传输时存在上行失步 non-synchronised，或者没有 PUCCH 资源用于发送调度请求消息的场景。第③种场景，除了通过随机接入的方式外，此时没有其他途径告诉 eNodeB，UE 存在上行数据需要发送。

基于非竞争模式的随机接入包括两种情况：

（1）RRC_CONNECTED 状态下，当下行有数据需要传输时，此时发生上行失步 non-synchronised 的情况。因为数据的传输除了接收外，还需要确认，如果上行失步，eNodeB 无法保证能够收到 UE 的确认信息。此时下行还是同步的，因此可以通过下行消息告诉 UE 发起随机接入需要使用的资源，如前导序列以及发送时机等，这些资源都是双方已知的，不需要通过竞争的方式接入系统。

（2）切换过程中的随机接入，在切换的过程中，目标 eNodeB 可以通过服务 eNodeB 来告诉 UE 它可以使用的资源。

如图 3-3 所示，基于竞争的随机接入流程包括：

（1）MSG1：UE 在 RACH 上发送随机接入前缀，携带前导码（Preamble）。

（2）MSG2：eNodeB 接收到 MSG1 后，在 DL-SCH 上发送随机接入响应（Random Access Response，RAR），RAR 中携带了 TA 调整、上行授权指令和 T-CRNTI。

（3）MSG3（连接建立请求）：UE 收到 MSG2 后，通过 preamble ID 核对，判断是否属于自己的 RAR 消息。如果是，则发送 MSG3 消息，携带 UE-ID。UE 的 RRC 层产生 RRC Connection Request 并映射到 UL-SCH 上的 CCCH 逻辑信道上发送。

（4）MSG4（RRC 连接建立）：竞争解决消息 RRC Contention Resolution 由 eNodeB 的 RRC 层产生，并在 CCCH 或 DCCH（FFS）逻辑信道上发送，UE 正确接收 MSG4 完成竞争解决。

如图 3-4 所示，非竞争性随机接入流程包括：

（1）MSG1：eNodeB 通过下行专用信令给 UE 指派非竞争的随机接入前缀（Preamble），这个前缀不在 BCH 上广播的集合中。

（2）MSG2：UE 在 RACH 上发送指派的随机接入前缀。

（3）MSG3：eNodeB 的 MAC 层产生随机接入响应，并在 DL-SCH 上发送。对于非竞争随机接入过程，Preamble 码由 eNodeB 分配，随机接入响应（RAR）消息正确接收后接入流程结束。

图 3-3　竞争性随机接入流程

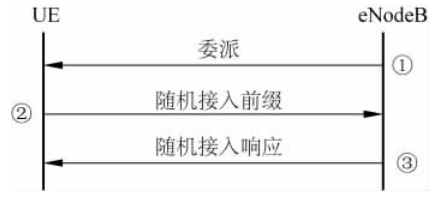

图 3-4　非竞争性随机接入流程

3.2.2 RRC 信令流程

RRC 连接在 UE 与 E-UTRAN 之间传输无线网络信令，在呼叫建立之初 RRC 连接建立，在通话结束后释放，并在期间一直维持。每个 UE 最多只有一个 RRC 连接。RRC 信令流程是信令分析的重点，具体包括 RRC 连接建立、连接释放、连接重建和连接重配置。

1. RRC 连接建立

RRC 连接的建立通常有两种触发原因：一是 UE 初始接入网络，进行 Attach 时发起；二是 UE 从 RRC_IDLE 状态进入到连接状态时发起，如发起呼叫、响应寻呼、跟踪去更新(TAU)或者去附着(Detach)等操作。如图 3-5 所示，RRC 连接建立包括以下步骤：

(1) RRC 连接请求：UE 通过上行 CCCH(UL_CCCH)信道在 SRB0 上发送 RRC Connection Request 消息，消息中携带了 UE 的初始(NAS)标识和建立原因等信息。该消息对应于随机接入过程中的 MSG3，是 UE 向 eNodeB 发送的第一条 RRC 信令消息，目的是请求建立一条 RRC 连接。建立 RRC 连接的目的是进行冲突解决和建立 SRB1，同时 RRC 连接建立时也可以让 UE 向 E-UTRAN 发送初始的 NAS 专用消息。E-UTRAN 通过该过程仅能建立 SRB1。

(2) RRC 连接建立：eNodeB 通过下行 CCCH 信道(DL_CCCH)在 SRB0 上发送 RRC Connection Setup 消息，消息中携带了 SRB1 的完整配置信息。该消息对应于随机接入过程中的 MSG4。

(3) RRC 连接建立完成：UE 通过 UL_DCCH 在 SRB1 上发送 RRC Connection Setup Complete 消息，该消息携带了上行 NAS 消息，如 Attach Request、TAU Request、Service Request、Detach Request 等，eNodeB 根据这些消息进行 S1 口建立。

RRC 连接建立失败的流程如图 3-6 所示。在 RRC 连接建立流程的第二步中，如果 eNodeB 拒绝为 UE 建立 RRC 连接，则会通过 DL_CCCH 在 SRB0 上回复 RRC Connection Reject 消息给 UE。

图 3-5　RRC 连接建立流程

图 3-6　RRC 连接建立失败

2. RRC 连接重建

当 UE 处于 RRC 连接状态但是出现切换失败、无线链路失败、完整性保护失败、RRC

重配置失败等事件时，UE 会发起 RRC 连接重建流程。如图 3-7 所示，RRC 连接重建步骤如下：

（1）RRC 连接重建请求：UE 通过 UL_CCCH 在 SRB0 上发送 RRC Connection Restablishment Request 消息，消息中含有 UE 的 AS 层初始标识信息及重建原因，该消息对应随机接入过程中的 MSG3。

（2）RRC 连接重建立：eNodeB 收到重建请求后，通过 DL_CCCH 在 SRB0 上回复 UE RRC Connection Reestablishment 消息，消息中携带 SRB1 的完整配置信息，该消息对应随机接入过程的 MSG4。

（3）RRC 重建完成：UE 通过 UL_DCCH 在 SRB1 上发送 RRC Connection Reestablishment Complete 消息，该消息并不携带任何实质性信息，仅实现重建完成确认并通知 eNodeB。

图 3-7　RRC 连接重建流程

在 RRC 重建过程中的第 2 步，如果 eNodeB 没有 UE 的上下文信息，则拒绝为 UE 重建 RRC 连接。eNodeB 通过下行 CCCH 信道回复一条 RRC 重建拒绝的指令 RRC Connection Reestablishment Reject 给 UE，如图 3-8 所示。

图 3-8　RRC 连接重建失败

3. RRC 连接重配置

当需要发起对 SRB 和 DRB 的管理、底层参数配置、切换执行和测量控制时，会触发 RRC 连接重配置流程。如图 3-9 所示，RRC 连接重配置流程包括以下步骤：

（1）RRC 连接重配置：eNodeB 通过 DL_DCCH 在 SRB1 上发送 RRC Connection

Reconfiguration 消息给 UE，根据携带的不同配置信息，一条消息中可以携带体现多个功能的信息单元。

（2）RRC 连接重配置完成：UE 通过 UL_DCCH 在 SRB1 上发送 RRC Connection Reconfiguration Complete 消息给 eNodeB，该消息中不含实质性信息，仅仅实现 RRC 层的确认功能。

图 3-9　RRC 连接重配置流程

在 RRC 连接重配置流程的第 2 步，如果 UE 无法执行 RRC 连接重配置消息中的内容，UE 会回退到收到重配消息前的配置，并发起 RRC 重建流程，如图 3-10 所示。

图 3-10　RRC 连接重配置失败

4. RRC 连接释放

当网络希望解除与 UE 的 RRC 连接时，会触发 RRC 连接释放流程。如图 3-11 所示，在 RRC 连接释放时，eNodeB 通过 DL_DCCH 在 SRB1 上发送 RRC Connection Release 消息给 UE，该消息中可选择携带重定位信息和专用优先级分配信息（用于控制 UE 的小区选择和重选）。在某些情况下（如 NAS 层鉴权过程中没有通过鉴权检查），UE 的 RRC 层根据 NAS 层的指示可以主动释放 RRC 连接，不通知网络侧而主动进入空闲状态，称为本地释放。

图 3-11　RRC 连接释放

表 3-3 对 RRC 连接建立、连接重建、重配置和连接释放这几个典型场景进行了总结。

表 3-3　典型的 RRC 场景列表

RRC 连接建立	RRC 连接重建	RRC 重配置	RRC 连接释放
① 初始接入附着时发起。 ② UE 从 RRC_IDLE 态至连接态时发起： • 发起寻呼； • 响应寻呼； • 附着请求； • 位置更新请求(TAU)； • 去附着请求	RRC 连接发生异常时发起： • 切换失败； • 无线链路失败； • 底层完整性保护失败； • RRC 重配置失败	① 当需要对 SRB 和 DRB 进行管理时发起： • E-RAB 的建立、修改和删除； • 请求 UE 激活 SRB2。 ② 测量控制下发时发起。 ③ 切换执行时发起	网络希望解除 UE 的 RRC 连接，使 UE 返回 RRC_IDLE 状态时

3.2.3　寻呼流程

寻呼是网络寻找 UE 时进行的信令流程，当网络告知 UE 有些信息要下发给它，UE 必须通过解析寻呼消息、发起相应寻呼流程来响应，才能确保通信的正常进行。

在 LTE 网络中，寻呼被触发的条件有三种：①UE 被叫(MME 发起)；②系统消息改变时(eNodeB 发起)；③地震告警(ETWS，小概率事件)。寻呼过程的实现依靠跟踪区(TA)来进行(相当于 2/3G 系统的 LAC)，寻呼的范围在 TAC 内进行，并不是在 TAC 列表的范围内进行寻呼。TAC 列表的设计只是减少了位置更新次数，从而降低信令负载。

从信令角度可以把寻呼流程分为两类：S_TMSI 寻呼和 IMSI 寻呼。一般情况下，优先使用 S_TMSI 寻呼，当网络发生错误需要恢复时(如 S_TMSI 不可用)，才发起 IMSI 寻呼。

从寻呼发起原因来分，也可以分为被叫寻呼和小区系统消息改变时寻呼(暂不考虑地震寻呼)，区别在于被叫寻呼是由 EPC 发起，经 eNodeB 透传；而小区系统消息改变时寻呼由 eNodeB 发起。通常所说的寻呼，主要指被叫寻呼。

1. S-TMSI 寻呼

当 UE 在 RRC_IDLE 模式时，网络若需要给 UE 发送数据(业务或信令)，则发起 S_TMSI 寻呼过程，S_TMSI 寻呼流程如图 3-12 所示。

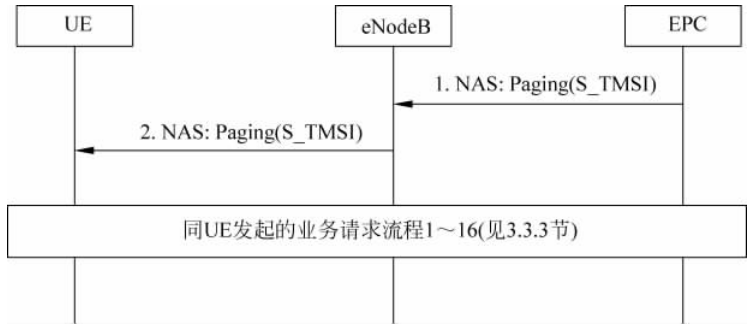

图 3-12　S_TMSI 寻呼流程

2. IMSI 寻呼

当网络发生错误需要恢复时(如 S-TMSI 不可用),可发起 IMSI 寻呼,UE 收到后执行本地去附着(Detach)过程,然后再开始附着请求(Attach),如图 3-13 所示。

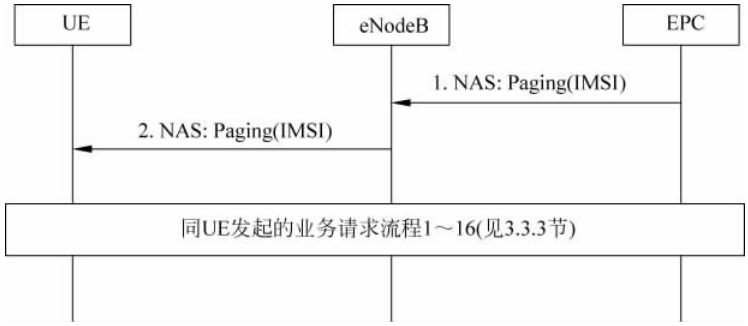

图 3-13　IMSI 寻呼流程

3.2.4　语音的电路域回落流程

当 4G 网络覆盖不完全或 VoLTE 网络尚未完全建好时,LTE 用户的语音要回落到 2G(GSM EDGE Radio Access Network,GERAN)或 3G (UMTS Terrestrial Radio Access Network,UTRAN)网络上进行,称为电路域回落(Circuit Switch Fallback,CSFB)。作为一种过渡性解决方案,CSFB 较好地解决了语音电话的可靠性问题,同时可以在一定程度上通过延长 2G/3G 网络的服务年限来保护运营商的前期投资。CSFB 的流程分为主叫流程和被叫流程。

1. 主叫 CSFB 流程

如图 3-14 所示,主叫 CSFB 流程包括以下步骤:

(1) UE 发起 CS Fallback 语音业务请求。当用户拨打语音电话时,UE 会发一条 Extended Service Request 消息,该消息里会携带 CSFB 信息。

(2) MME 发送 Initial Context Setup Request 消息给 eNodeB,包含 CS Fallback Indicator,该消息告知 eNodeB,UE 因 CS Fallback 业务需要回落到 UTRAN/GERAN。

(3) eNodeB 要求 UE 启动系统小区测量,并获取 UE 上报的测量报告,确定重定向的目标系统小区。然后向 UE 发送目标系统具体的无线配置信息,并释放 RRC 连接。LTE 网络通过 RIM 流程(无线消息管理流程)提前获取 2G 目标小区的广播信息,将其填充至 RRC Connection Release 消息中下发,省去了终端读取 2G 广播信息的时间。

(4) UE 接入目标系统小区,发起 CS 域的业务请求消息 CM Service Request。如果 CM 业务请求消息中有 CSMO 字样,则说明本次呼叫是移动终端发起的 CSFB 呼叫。

(5) 如果目标系统小区归属的 MSC Server 与 UE 附着 EPS 网络时登记的 MSC Server 不同,则该 MSC Server 收到 UE 的业务请求时,并没有该 UE 的信息。若 MSC Server 可以

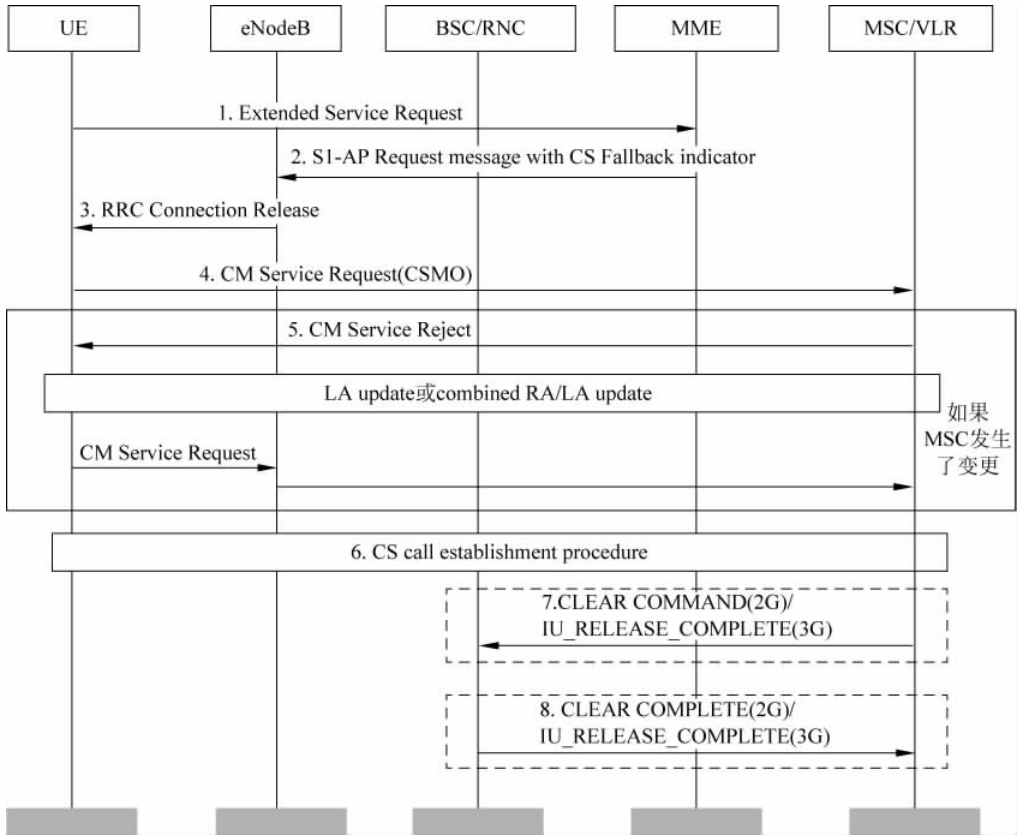

图 3-14　主叫 CSFB 流程

采取隐式位置更新流程，则接受用户请求。若 MSC Server 不支持隐式位置更新，则会拒绝用户的请求。MSC Server 拒绝用户的业务请求会导致 UE 发起一个 CS 域的位置更新。如果位置更新请求消息中携带了 CSMO 标识，且该标识有效，则 MSC Server 会记录本次呼叫是 CSFB 呼叫。

（6）完成位置更新后 UE 再次尝试在 CS 域建立语音呼叫流程。

（7）通话结束后，MSC Server 向主叫回落到的 BSC 发送的 Clear Command 消息中携带 CSFB Indication 信元，指示 BSC 拆除空口连接并通知 UE 回到 LTE 网络。或者 MSC Server 向主叫回落到的 RNC 发送 Iu Release Command 消息，携带 End Of CSFB 信元，指示 RNC 拆除空口连接并指示 UE 回到 LTE 网络。

（8）MSC 收到 BSC 的 Clear Complete 消息或者 RNC 的 Iu Release Complete 消息，表示呼叫结束，A 口连接拆除完成。接入侧在指示终端重选网络时只针对 CSFB 用户通话前携带的 LTE 频点，实现终端快速返回 LTE 网络。

2. 被叫 CSFB 流程

如图 3-15 所示，被叫 CSFB 流程包括以下步骤：

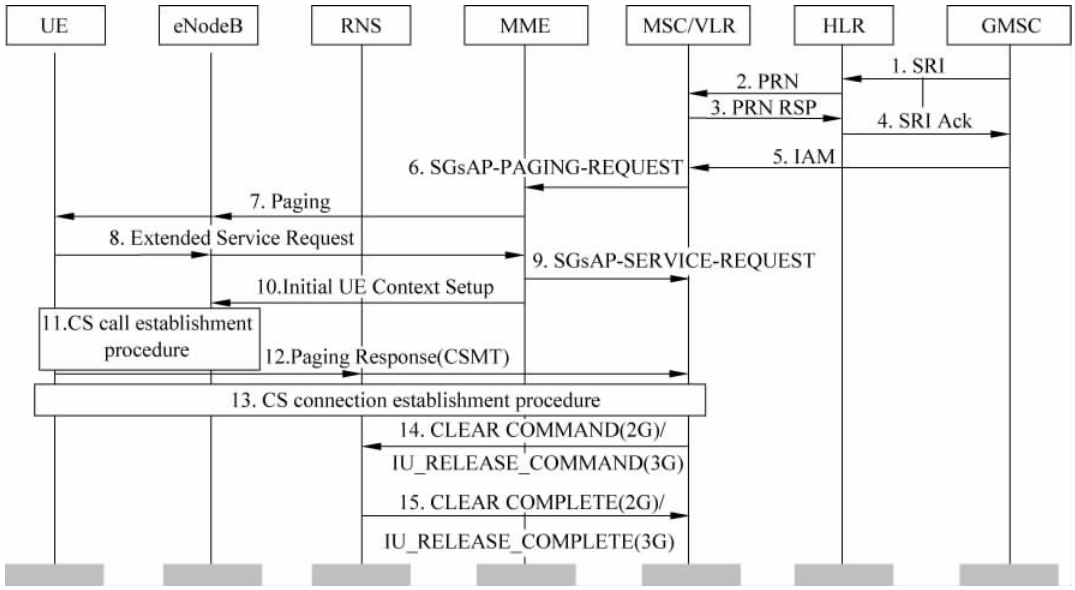

图 3-15　被叫 CSFB 流程

(1) GMSC Server 向被叫用户归属 HLR 发送取路由信息 SRI。

(2) HLR 收到该 SRI 消息后,向被叫用户当前附着的 MSC Server 获取漫游号码。

(3) MSC Server 为该次呼叫分配漫游号码 MSRN1,并返回给 HLR。

(4) HLR 将漫游号码反馈给 GMSC。

(5) GMSC 收到漫游号码后,对号码进行分析,并根据分析结果把呼叫路由发给 MSC Server。

(6) MSC Server 收到 IAM 入局消息后,发送 SGsAP-PAGING-REQUEST(含 IMSI、TMSI、Service indicator、CLI、LAC 等信息)消息给 MME。

(7) MME 发送寻呼消息给 eNodeB,eNodeB 发起空口的寻呼流程。

(8) UE 建立连接并发送 Extended Service Request 消息给 MME。

(9) MME 发送 SGsAP-SERVICE-REQUEST 消息给 MSC Server。为避免主叫等待时间过长,MSC Server 收到包含空闲态指示的 SGsAP-SERVICE-REQUEST 消息后,先通知主叫,呼叫正在进行中。

(10) MME 发送 Initial UE Context Setup 消息(包含 CS Fallback Indicator)给 eNodeB,通知 eNodeB,UE 因 CSFB 业务需要回落到 UTRAN/GERAN。

(11) UE 回落到 CS 域后,若检测到当前的位置区信息和存储的位置区不同,将发起位置更新,MSC Server 会收到 UE 发送的位置更新(Location Update Request)消息。如果位置更新消息中携带 CSMT 字样,则 MSC Server 会标识本次呼叫为 CSFB 呼叫。

(12) 随着空口、A/Iu-CS 等连接的建立,UE 发送 Paging Response 消息给 MSC Server。该消息中携带 CSMT 标识,即使 BSC/RNC 没有向该 UE 发起过寻呼请求,也需要

能处理 UE 的寻呼响应。如果寻呼响应消息中的位置区信息和 VLR 中保存的不一致，则 VLR 在业务接入成功之后将 SGs 关联置为非关联。

（13）建立 CS 呼叫。

（14）通话结束后，告知 BSC/RNC 拆除空口连接并指示 UE 返回 LTE 网络。

（15）MSC 收到 BSC 的 Clear Complete 消息或 RNC 的 Iu Release Complete 消息表示呼叫结束。接入侧在指示终端重选网络时只针对 CSFB 用户携带的 LTE 频点，可以让 CSFB 终端快速返回 E-UTRAN。

3.2.5　紧急呼叫流程

在 VoLTE 尚未商用之前，当使用 USIM 卡的用户发起紧急呼叫（例如用手机拨打 112、110、119、120 之类的报警或求救号码）时，MME 会指示 eNodeB 将 UE 回落到 GERAN/UTRAN 网络上进行。与普通的语音呼叫相比，紧急呼叫业务流程无须进行位置更新处理。当非 USIM 卡用户发起紧急呼叫时，由于 SIM 卡类型的原因，其紧急呼叫流程与 GERAN/UTRAN 网络的呼叫流程是一样的。

如图 3-16 所示，LTE 网络紧急呼叫流程包括以下步骤：

（1）UE 发起电路域回落（CS Fallback）呼叫业务请求，向 eNodeB 发送 Extended Service Request 消息（其中的 service-type 信元指示业务类型为紧急呼叫），eNodeB 再把该消息发给 MME。

（2）MME 收到请求后，指示 eNodeB 需要将 UE 回落到 CS 域。

（3）CS 域回落完成后，UE 向 2G/3G MSC 发起 CM Service Request 消息（消息中携带紧急呼叫标识）。

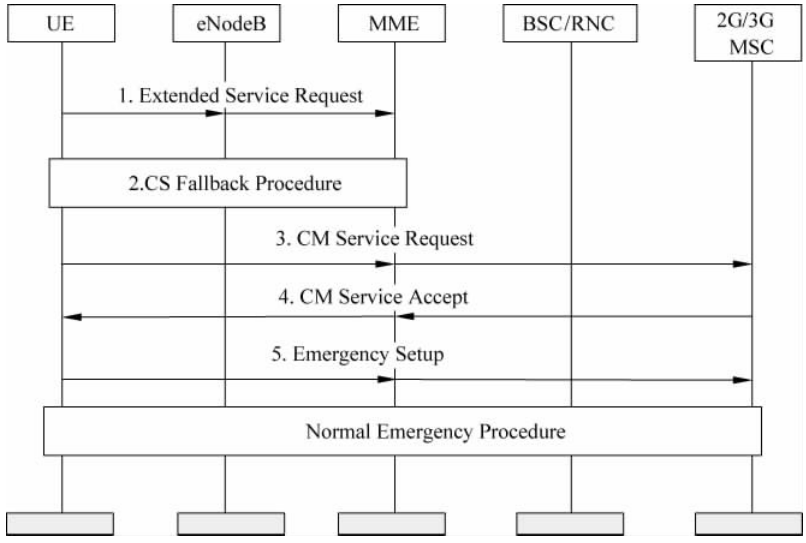

图 3-16　紧急呼叫流程

(4) MSC 通过 eNodeB 向 UE 返回 CM Service Accept 消息。

(5) UE 向 2G/3G MSC 发送 Emergency Setup 消息,并发起紧急呼叫。

3.2.6 LTE 测量过程

在移动通信系统中,测量过程作为实现移动性管理的先决条件,为移动台的切换和重选等操作提供数据来源。LTE 的测量过程分为两个动作:eNodeB 的测量控制消息下发和 UE 的测量数据上报。

当 UE 处于 RRC_IDLE 状态下时,UE 通过 E-UTRAN 的广播获得测量参数信息。小区重选是空闲模式中最重要的一项操作,UE 端通过对具体测量量(如 RSRP 或 RSRQ)进行测量,获取当前服务小区和邻近小区的质量。通过小区重选,可以确保 UE 驻留在优质的小区中。

当 UE 处于 RRC_CONNECTED 状态下,E-UTRAN 通过 RRC 连接重配置(RRC Connection Reconfiguration)消息,提供测量配置信息(Measurement Configuration)给 UE,具体流程可参考 RRC 的连接重配置信令流程。

关于小区重选及切换的测量准则、测量过程等相关内容,将在本书第 5 章结合小区重选和切换算法进行详细描述。

3.3 端到端业务流程

下面完整描述整个端到端的业务流程,由 UE 开机附着开始,到业务请求、专用承载建立,包含了去附着和专用承载释放等流程。

3.3.1 附着流程

当移动用户刚开机或者手机因异常原因重启后,UE 处于空状态(NULL)。UE 首先要进行物理下行同步并通过搜索测量,进行 PLMN 选择和小区选择。当 UE 选择到一个合适或者可接纳的小区后,就驻留在该小区并启动附着(Attach)流程。

当 UE 完成在 E-UTRAN 网络的附着后,网络端会建立 UE 的上下文,并在 UE 和网络之间建立一个默认的 EPS 承载,该承载使 UE 获得一个总是在线的 IP 连接。UE 只有成功附着到网络,才能与网络进行正常的业务交互。如图 3-17 所示,附着流程包括以下步骤:

(1) 处在 RRC_IDLE 态的 UE 开始启动 Attach,发起随机接入过程,即 UE 发送 MSG1 消息。

(2) eNodeB 检测到 MSG1 消息后向 UE 发送随机接入响应消息,即 MSG2 消息。

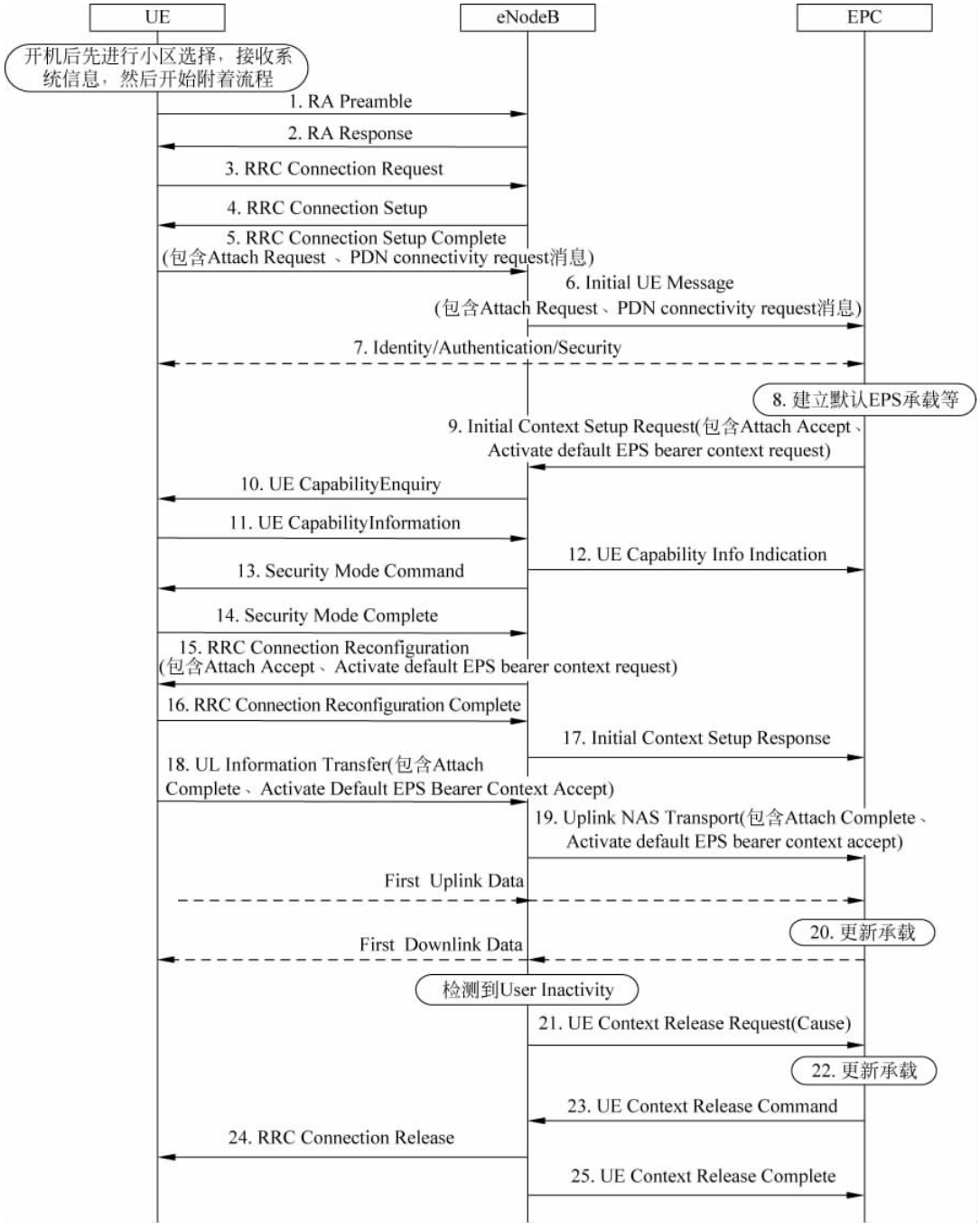
UE
eNodeB
EPC
开机后先进行小区选择，接收系统信息，然后开始附着流程
1. RA Preamble
2. RA Response
3. RRC Connection Request
4. RRC Connection Setup
5. RRC Connection Setup Complete
(包含Attach Request 、PDN connectivity request消息)
6. Initial UE Message
(包含Attach Request、PDN connectivity request消息)
7. Identity/Authentication/Security
8. 建立默认EPS承载等
9. Initial Context Setup Request(包含Attach Accept、Activate default EPS bearer context request)
10. UE CapabilityEnquiry
11. UE CapabilityInformation
12. UE Capability Info Indication
13. Security Mode Command
14. Security Mode Complete
15. RRC Connection Reconfiguration
(包含Attach Accept、Activate default EPS bearer context request)
16. RRC Connection Reconfiguration Complete
17. Initial Context Setup Response
18. UL Information Transfer(包含Attach Complete、Activate Default EPS Bearer Context Accept)
19. Uplink NAS Transport(包含Attach Complete、Activate default EPS bearer context accept)
First Uplink Data
20. 更新承载
First Downlink Data
检测到User Inactivity
21. UE Context Release Request(Cause)
22. 更新承载
23. UE Context Release Command
24. RRC Connection Release
25. UE Context Release Complete

图 3-17　附着流程

（3）UE 收到随机接入响应后，根据 MSG2 的 TA 调整上行发送时机，向 eNodeB 发送 RRC Connection Request 消息，申请建立 RRC 连接。

（4）eNodeB 向 UE 发送 RRC Connection Setup 消息，包含建立 SRB1 信令承载信息和无线资源配置信息。

（5）UE 完成 SRB1 信令承载和无线资源配置，向 eNodeB 发送 RRC Connection Setup Complete 消息，包含 NAS 层的 Attach Request 信息。

（6）eNodeB 选择 MME，向 MME 发送 Initial UE Message 消息，包含 NAS 层的 Attach Request 消息。

（7）UE 与 EPC 间执行鉴权流程；UE 刚开机第一次附着时，使用的 IMSI，无 Identity 过程；后续如果有有效的 GUTI，则使用 GUTI 附着，EPC 才会发起 Identity 过程。

（8）建立默认的 EPS 承载。

（9）MME 向 eNodeB 发送 Initial Context Setup Request 消息，包含 NAS 层的 Attach Accept 消息。该消息是 MME 向 eNodeB 发起的初始上下文建立请求，请求 eNodeB 建立承载资源。UE 的安全能力参数是通过 Attach Request 消息带给 EPC 的，EPC 再通过该消息传给 eNodeB。

（10）eNodeB 接收到 Initial Context Setup Request 消息后，如果 eNodeB 没有 UE 的能力信息，则 eNodeB 会发送 UE Capability Enquiry 消息，向 UE 查询其能力；如果 MSG9 中包含 UE Radio Capability，则 eNodeB 不会发送 UE Capability Enquiry 消息给 UE。

（11）UE 向 eNodeB 发送 UE Capability Information 消息，报告 UE 的能力。

（12）eNodeB 向 MME 发送 UE Capability Info Indication 消息，更新 MME 中的 UE 能力信息。

（13）eNodeB 向 UE 发送 Security Mode Command 消息，进行安全激活。

（14）UE 向 eNodeB 发送 Security Mode Complete 消息，表示安全激活完成。

（15）eNodeB 根据 Initial Context Setup Request 消息中的 ERAB 建立信息，向 UE 发送 RRC Connection Reconfiguration 消息进行资源重配，包括重配 SRB1 信令承载信息和无线资源配置，建立 SRB2、DRB 等。

（16）UE 向 eNodeB 发送 RRC Connection Reconfiguration Complete 消息，表示无线资源配置完成。

（17）eNodeB 向 MME 发送 Initial Context Setup Response 响应消息，表明 UE 的上下文建立完成。

（18）UE 向 eNodeB 发送 UL Information Transfer 消息，包含 NAS 层的 Attach Complete、Activate Default EPS Bearer Context Accept 等消息。

（19）eNodeB 向 MME 发送上行直传 Uplink NAS Transport 消息，包含 NAS 层的 Attach Complete 消息。

第 20～25 步对应 UE 的上下文释放过程。

3.3.2　去附着流程

去附着(Detach)流程往往是伴随着用户进入覆盖盲区(或接入受限区域)或用户关机发生的,该流程通过 UE 执行并与附着流程互逆。去附着流程通常可以分为关机去附着和非关机去附着两种。

1. 关机去附着

当用户的手机终端关机时,需要发起去附着流程,来通知网络释放其保存的该 UE 的所有资源。空闲状态下关机去附着流程如图 3-18 所示。具体步骤包括:

(1) UE 在 RRC_IDLE 状态下,先发起随机接入过程和 RRC 连接建立过程,然后 UE 向 eNodeB、EPC 发送的消息中携带 NAS 层的 Detach Request 消息(类型为 Switch off)。

(2) MME 向 eNodeB 发送 UE Context Release Command 消息,请求 eNodeB 释放 UE 上下文信息。UE 侧清空所有的 EPS 承载和 RB 承载,EPC 侧清空所有的 EPS 承载和 TEID(Tunnel Endpoint ID)资源,其中隧道端点标识符(TEID)是标识 S1 承载使用的,用于标识 UE 和核心网隧道的两端。

(3) eNodeB 释放 UE 上下文信息完成后发送 UE Context Release Complete 消息通知 EPC。

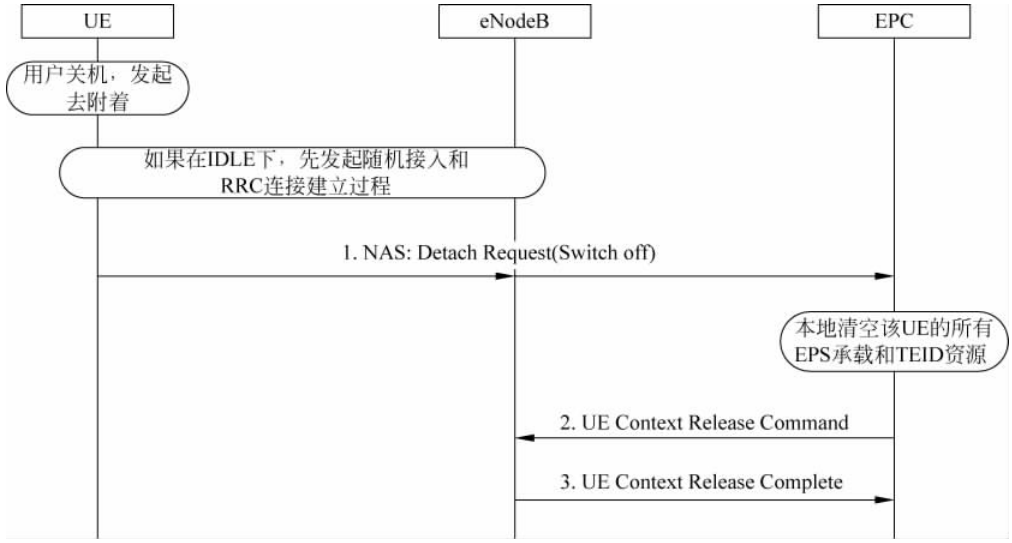

图 3-18　空闲状态下关机去附着流程

连接状态下关机去附着流程如图 3-19 所示。具体步骤包括:

(1) 第 1～4 步中,UE(在 RRC_CONNECTED 状态下,EPS 能力被禁用)向 eNodeB 发送上行传输消息(其中携带 NAS 层的去附着请求消息)。

(2) eNodeB 向 MME 发送上行直传 Uplink NAS Transport 消息,包含 NAS 层的

Detach Request 信息。

(3) 第 3、4 步中,EPC 侧清除 EPS 承载和 RB 资源,MME 向 eNodeB、eNodeB 向 UE 发送 DL InformationTransfer 消息,该消息中包含 NAS 层的 Detach Accept 消息(含 Switch off 信息)。

(4) 第 5～7 步中,MME 向 UE 发起 UE 文本释放和 RRC 连接释放信息,完成去附着流程。

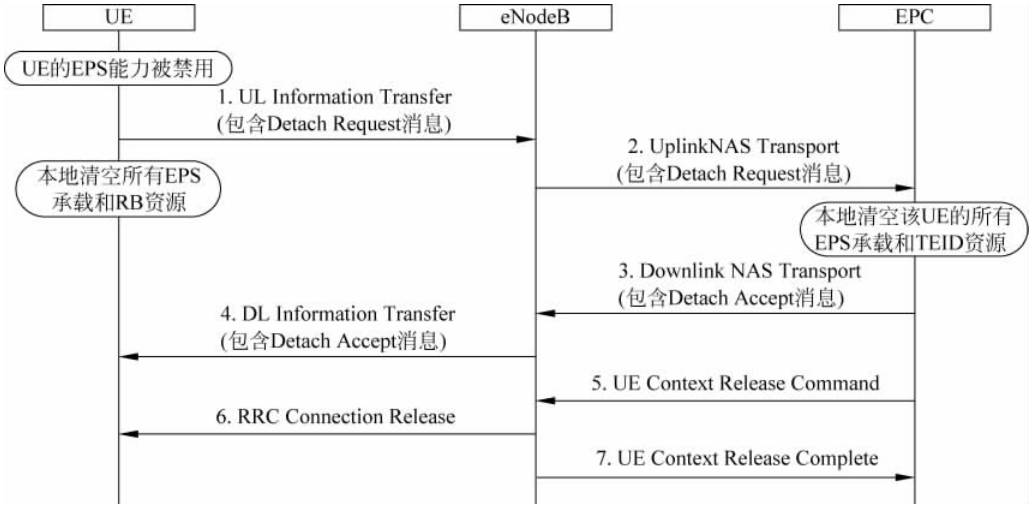

图 3-19　连接状态下关机去附着流程

2. 非关机去附着

RRC_IDLE 状态下非关机去附着流程如图 3-20 所示。主要步骤包括:

(1) 第 1～5 步是 RRC 连接的建立过程,RRC 建立完成消息中会附带去附着请求。

(2) 第 6～9 步是 UE 和 EPC 进行相互安全验证的过程,验证完成后,EPC 侧执行清除 EPS 承载和 RB 资源并向 UE 发送去附着接受消息。

(3) 第 10～12 步则是 EPC 向 UE 发起文本释放和连接释放信息。

3.3.3　业务请求流程

UE 在 RRC_IDLE 模式下需要发送或接收业务数据时,会发起业务请求 Service Request 过程,这个过程通常是在随机接入流程之后发生的。业务请求流程的目的是建立初始上下文信息 Initial Context Setup,在 S1 接口上建立 S1 承载,在 Uu 接口上建立数据无线承载,打通 UE 到 EPC 之间的路由,为后面的数据传输做好准备。

当业务请求由 UE 主动发起时,需先发起随机接入过程,Service Request 消息由 RRC Connection Setup Complete 携带,整个流程类似于主叫过程。当下行数据达到时,网络侧先对 UE 进行寻呼,随后 UE 发起随机接入过程,在下行数据到达时发起业务请求,整个流

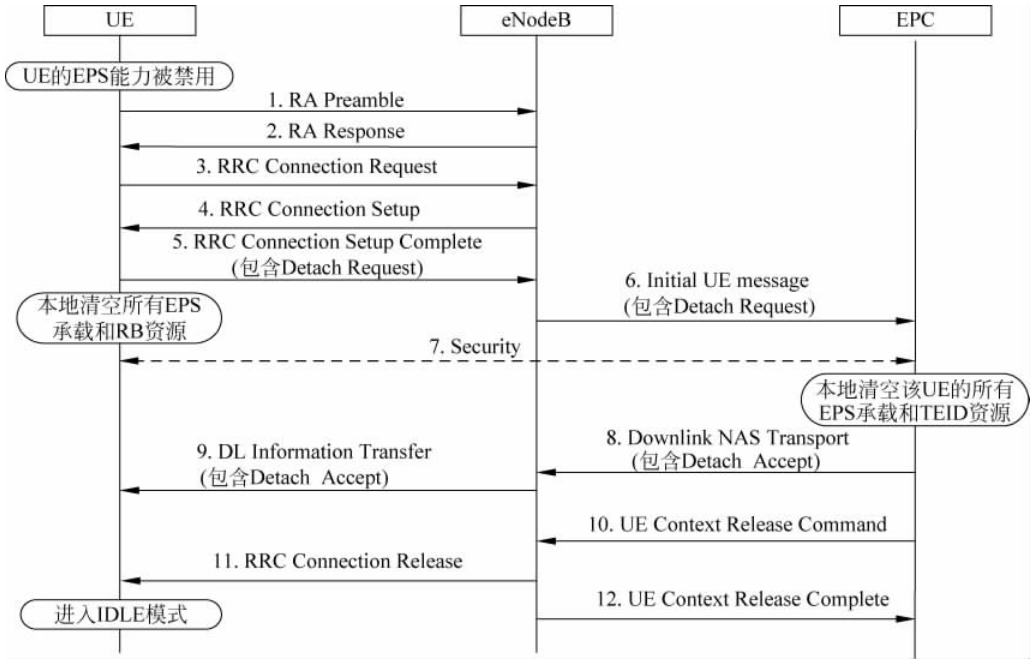

图 3-20　RRC_IDLE 状态下非关机去附着流程

程类似于被叫接入。如图 3-21 所示，详细的业务请求流程说明如下：

（1）处在 RRC_IDLE 态的 UE 启动业务请求过程，发起随机接入，即 MSG1 消息。

（2）eNodeB 接收到 MSG1 消息后，向 UE 发送随机接入响应消息，即 MSG2 消息。

（3）UE 收到随机接入响应后，根据 MSG2 的 TA 调整上行发送时机，向 eNodeB 发送 RRC Connection Request 消息，即 MSG3 消息。

（4）eNodeB 向 UE 发送 RRC Connection Setup 消息，包含建立 SRB1 承载信息和无线资源配置信息。

（5）UE 完成 SRB1 承载和无线资源配置后，向 eNodeB 发送 RRC Connection Setup Complete 消息，包含 NAS 层 Service Request 信息。

（6）eNodeB 选择 MME，向 MME 发送 Initial UE message 消息，包含 NAS 层 Service Request 消息。

（7）UE 与 EPC 间执行鉴权流程，4G 的鉴权是双向鉴权流程，以提高网络安全能力。

（8）MME 向 eNodeB 发送 Initial Context Setup Request 消息，请求建立 UE 上下文信息。

（9）eNodeB 接收到 Initial Context Setup Request 消息，如果不包含 UE 能力信息，则 eNodeB 向 UE 发送 UE Capability Enquiry 消息，查询 UE 能力。

（10）UE 向 eNodeB 发送 UE Capability Information 消息，报告 UE 能力信息。

（11）eNodeB 向 MME 发送 UE Capability Info Indication 消息，更新 MME 的 UE 能

力信息。

(12) eNodeB 根据 Initial Context Setup Request 消息中 UE 支持的安全信息,向 UE 发送 Security Mode Command 消息,进行安全激活。

(13) UE 向 eNodeB 发送 Security Mode Complete 消息,表示安全激活完成。

(14) eNodeB 根据 Initial Context Setup Request 消息中的 E-RAB 建立信息,向 UE 发送 RRC Connection Reconfiguration 消息进行 UE 资源重配,包括重配 SRB1 和无线资源配置,建立 SRB2 信令承载、DRB 业务承载等。

(15) UE 向 eNodeB 发送 RRC Connection Reconfiguration Complete 消息,表示资源配置完成。

(16) eNodeB 向 MME 发送 Initial Context Setup Response 响应消息,表明 UE 上下文建立完成。至此业务请求流程完成,随后进行数据的传输。

(17) 图 3-21 中第 17～20 步发送的消息是数据传输完毕后,对 UE 进行的去激活过程,涉及 UE 上下文信息释放(UE Context Release)流程。

3.3.4 专用承载的建立

专用承载可以是 GBR 类型,也可以是 Non-GBR 类型,专用承载建立流程可以为专用承载分配相关资源。专用承载的建立可以由 UE 或 EPC 在 UE 处于 RRC_CONNECTED 状态下主动发起,不能由 eNodeB 主动发起。

当 UE 发起专用承载建立需求时,EPC 仅将其作为参考,有权接受或拒绝。若 EPC 接受,可回复承载建立、修改流程。

专用承载建立的过程包括:①P-GW 根据 QoS 策略制定该 EPS 承载的 QoS 参数;②S-GW 向 eNodeB 发送承载建立请求,包含 IMSI、QoS、TFT、TEID、LBI 等信息;③MME 向 eNodeB 发送 E-RAB 建立请求,包含 E-RAB ID、QoS、S-GW TEID 等信息;④eNodeB 接收建立请求消息后,建立数据无线承载;⑤eNodeB 返回 E-RAB 建立响应消息,E-RAB 建立列表信息中包含成功建立的承载信息,E-RAB 建立失败列表消息中包含没有成功建立的承载消息。

如图 3-22 所示,专用承载建立流程包括以下步骤:

(1) 连接状态下的 UE 向 eNodeB 发出 UL Information Transfer 消息(含 Bearer Resource Allocation Request 消息或 Bearer Resource Modification Request 消息)。

(2) eNodeB 接收到 UE 的消息后,向 MME 发送上行 NAS 消息,其中包含了 Bearer Resource Allocation Request 消息。

(3) MME 收到承载分配请求消息后,进行相应的承载资源申请处理。

(4) MME 向 eNodeB 发送 E-RAB 建立/修改消息,其中包含激活/修改专用 EPS 承载消息。

(5) eNodeB 通过向 UE 发送重配消息,将 NAS 消息 Activate Dedicated EPS Bearer Context Request 告知 UE。

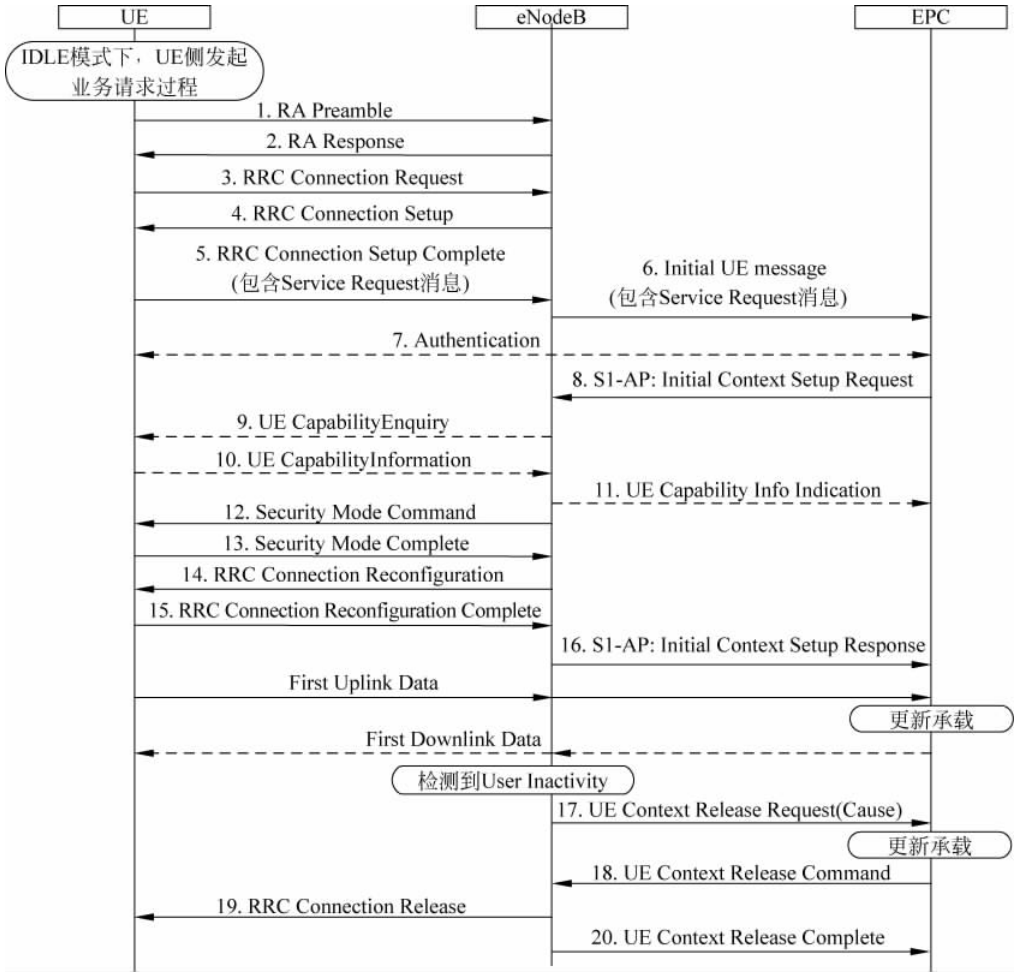

图 3-21　业务请求流程

(6) UE 建立专用承载完成后，向 eNodeB 发送 RRC Connection Reconfiguration Complete 消息，表明建立承载成功。

(7) eNodeB 回应 E-RAB Setup/Modify Response 消息给 MME，表明无线承载建立成功；

(8) UE 在发送完成重配完成消息后，通过上行传送消息告知 eNodeB Activate/Modify Dedicated EPS Bearer Context Accept 消息。

(9) eNodeB 通过 NAS 消息传送把 Activate/Modify Dedicated EPS Bearer Context Accept 消息传递给 MME。

(10) UE 与 MME 可以通过 eNodeB 开始传输上下行数据，MME 反馈承载资源分配响应。

如果是 MME 主动发起的承载建立流程，则省略步骤 1 和 2。

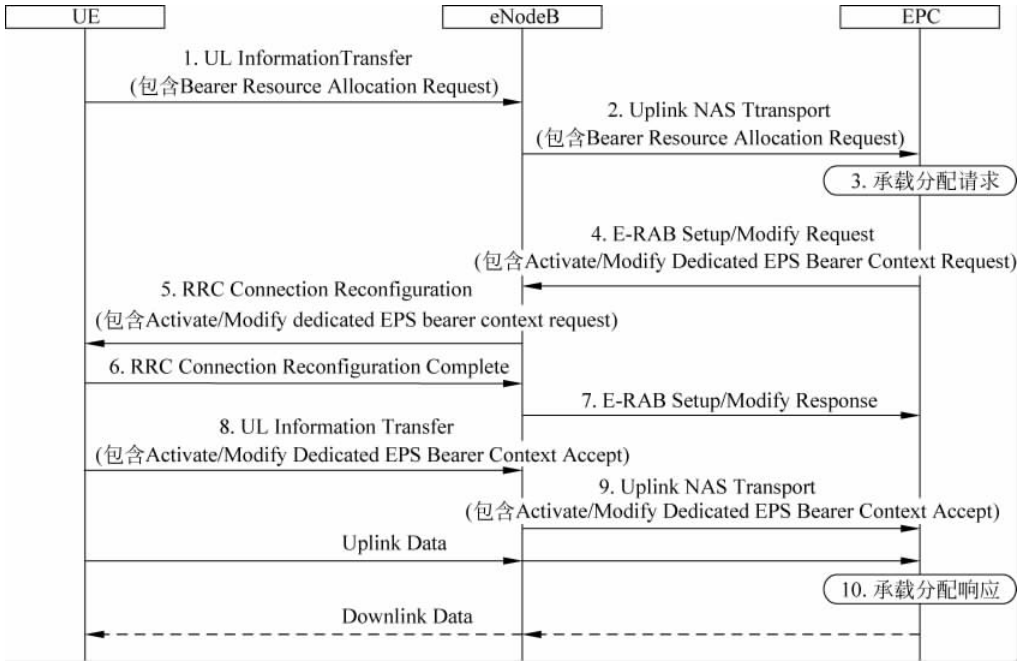

图 3-22　专用承载建立流程

3.3.5　专用承载的修改

专用承载的修改过程可以由 UE 或 MME 主动发起，用于修改已经建立承载的配置，不能由 eNodeB 主动发起，E-RAB 的修改只能在连接状态下发起该流程。

E-RAB 专用承载的修改过程可以分为修改 QoS 和不修改 QoS 两种类型。若由 UE 发起时，EPC 可回复承载建立、修改、释放流程。

专用承载修改流程如图 3-23 所示。具体步骤包括：

（1）连接状态下的 UE 通过 UL Information Transfer 消息将 Bearer Resource Modification Request 消息传递给 eNodeB。

（2）eNodeB 通过 Uplink NAS Transport 消息将 Bearer Resource Modification Request 发送给 MME。

（3）MME 收到承载修改请求消息后，进行相应的承载资源修改处理。

（4）MME 通过 E-RAB Modify Command 传递 Modify EPS Bearer Context Request 消息告知 eNodeB。

（5）eNodeB 通过重配消息，将 Modify EPS Bearer Context Request 消息传递给 UE。

（6）UE 建立专用承载完成后，向 eNodeB 发送 RRC Connection Reconfiguration Complete 消息，表明建立承载成功。

(7) eNodeB 发送 E-RAB Modify Response 消息给 MME,表明无线承载修改成功。

(8) UE 通过 UL Information Transfer 消息将 Modify EPS Bearer Context Accept 消息告知 eNodeB。

(9) eNodeB 通过 Uplink NAS Transport 消息发送 Modify EPS Bearer Context Accept 消息给 MME。

(10) UE 与 MME 可以通过 eNodeB 开始进行上下行数据传输,EPC 进行承载资源修改响应。

若 MME 主动发起的承载修改流程,则省略步骤 1 和 2; 若 eNodeB 主动发起的专用承载释放流程,则无步骤 1,步骤 2 改为发送 E-RAB Release Indication 消息给 MME。

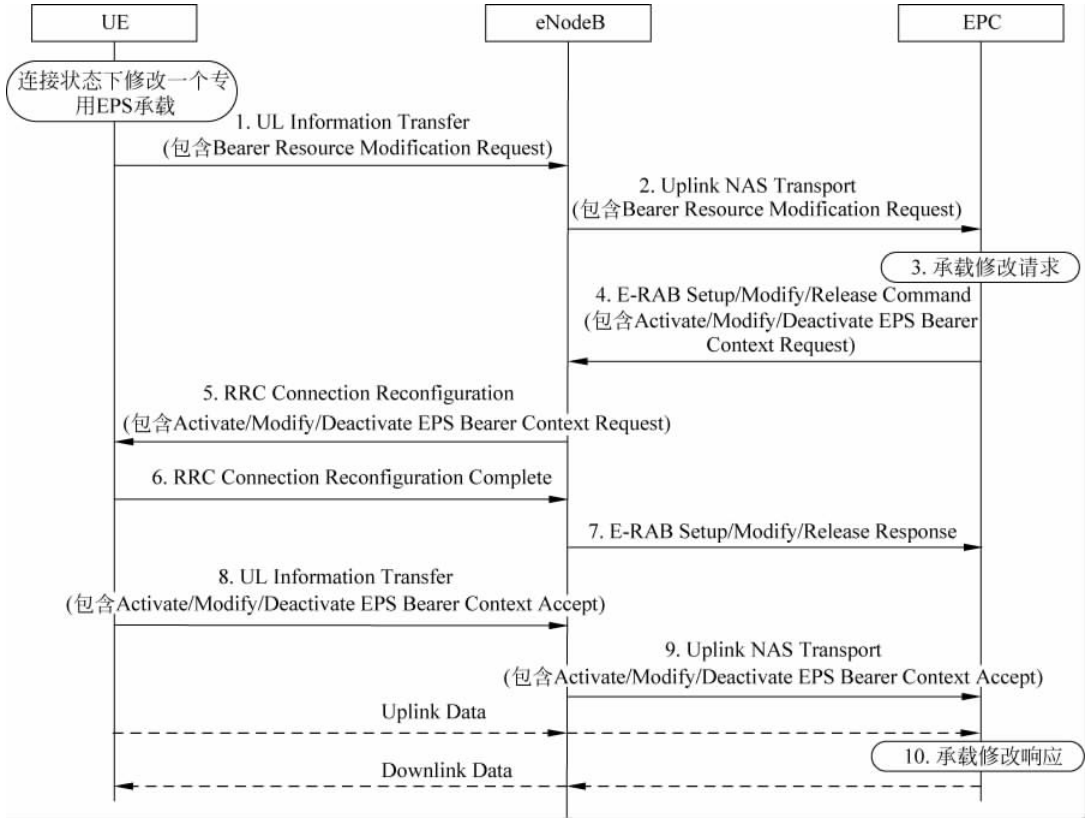

图 3-23　专用承载修改流程

3.3.6　专用承载的释放

专用承载的释放只能在连接状态下由 UE 或 EPC 侧(MME 或 P-GW)主动发起。P-GW 和 MME 均可发起对 E-RAB 的释放流程,由 P-GW 发起的承载释放,可释放某一专用承载或该 PDN 地址下的所有承载; 而由 MME 发起的承载释放,可释放某一专用承载,但

不能释放该 PDN 下的默认承载。

无论 UE 发起还是 EPC 侧发起，专用承载的释放过程均由 EPC 侧向 eNodeB 发送 E-RAB 释放命令消息，释放一个或多个承载的 S1 和 Uu 接口资源；eNodeB 接收到 E-RAB 释放命令消息后，释放每一个承载的 S1 接口资源，Uu 接口上的资源和数据无线承载。如图 3-24 所示，专用承载释放流程包括如下步骤：

（1）EPC 发起承载释放过程，可能是 UE 启动，也可能是 EPC 侧启动的。

（2）EPC 发送 E-RAB Release Command 消息给 eNodeB，其中包含 NAS 消息 Deactivate EPS Bearer Context Request。

（3）eNodeB 收到 E-RAB Release Command 消息后，启动承载释放流程，并且发送重配消息给 UE，其中包含 NAS 消息 Deactivate EPS Bearer Context Request。

（4）UE 释放相关承载资源后，发送返回 RRC Connection Reconfiguration Complete 消息，表明无线承载释放成功。

（5）eNodeB 收到 RRC Connection Reconfiguration Complete 消息后，返回 E-RAB Release Response 消息给 EPC。

（6）UE 在发送重配置完成消息后，通过 UL Information Transfer 消息将 NAS 层 Deactivate EPS Bearer Context Accept 消息告知 eNodeB。

（7）eNodeB 发送 Uplink NAS Transport 消息，包含 Deactivate EPS Bearer Context Accept，告知 EPC 进行 EPS 承载删除完成。

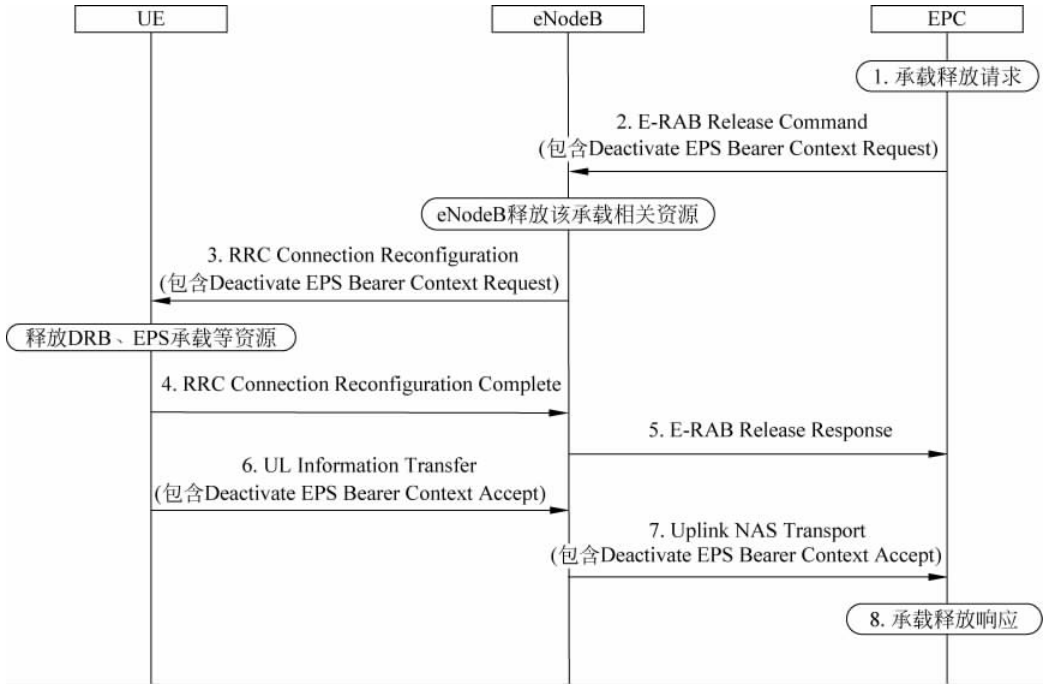

图 3-24　专用承载的释放流程

3.4　跟踪区更新流程

网络移动性管理是对移动终端的位置信息、安全性以及业务连续性方面的管理，其主要目的是保障用户与网络的连接达到最佳状态。移动性管理主要包括位置管理和切换管理两个方面，具体涉及的业务流程有 PLMN 选择、小区选择与重选、跟踪区更新和切换等。本节重点介绍跟踪区更新流程，关于 PLMN 选择、小区选择与重选以及切换流程，将在第 5 章中结合具体算法进行详细描述。

在 LTE 网络中，为了确认 UE 的地理位置，将基站的覆盖区域分为多个跟踪区(Tracking Area，TA)。TA 的功能与 3G 网络中的位置区(Location Area，LA)和路由区(Routing Area，RA)类似，是 LTE 系统中位置更新和寻呼的基本单位，一个 TA 中可包含一个或多个小区。

在 LTE 网络中，用跟踪区码(Tracking Area Code，TAC)来标识不同的 TA，TAC 在小区的 SIB1 消息中广播。实际网络中，TAI(Tracking Area Identity)是 TA 的全球唯一标识，TAI 由移动国家码(MCC)、移动网络码(MNC)和跟踪区码(TAC)共同组成，总计 6 字节。

根据跟踪区更新(Tracking Area Update，TAU)发生的时机，可以把 TAU 分成连接态的更新和空闲态的更新。空闲态更新又可以分为激活和不激活两种位置更新方式。激活的位置更新是 UE 在位置更新后可立即进行数据传输。

根据更新内容的不同，也可以把 TAU 分成联合 TAU(更新 TAI 列表和 LAU)和非联合 TAU(只更新 TAI 列表)。例如，在实现电路域回落(CSFB)的过程中，附着和位置更新都是联合进行的。

TAU 的成功率直接关系到寻呼的成功率，UE 在以下场景会启动 TAU：

(1) 当前服务小区的跟踪区不在原有的 TAI 列表里。

(2) 周期性地进行跟踪区更新，按照既定周期定期触发，无论 UE 在空闲状态还是在连接状态。

(3) 当 UE 从服务区外返回服务区时，且周期性 TAU 到期。

(4) MME 负载均衡时，可要求 UE 发起 TAU。

(5) ECM-IDLE 状态下 UE 的 GERAN 和 UTRAN Radio 能力发生变化。

(6) 从 UTRAN PMM Connected 或 GPRS READY 状态通过小区重选进入 E-UTRAN。

1. 空闲态不激活的 TAU 流程

在空闲态不激活的 TAU 过程中，UE 不进行任何业务操作，仅仅是进行位置更新。例如周期性位置更新和移动性位置更新等，都属于此类。如图 3-25 所示，空闲态不激活的 TAU 流程包括以下步骤：

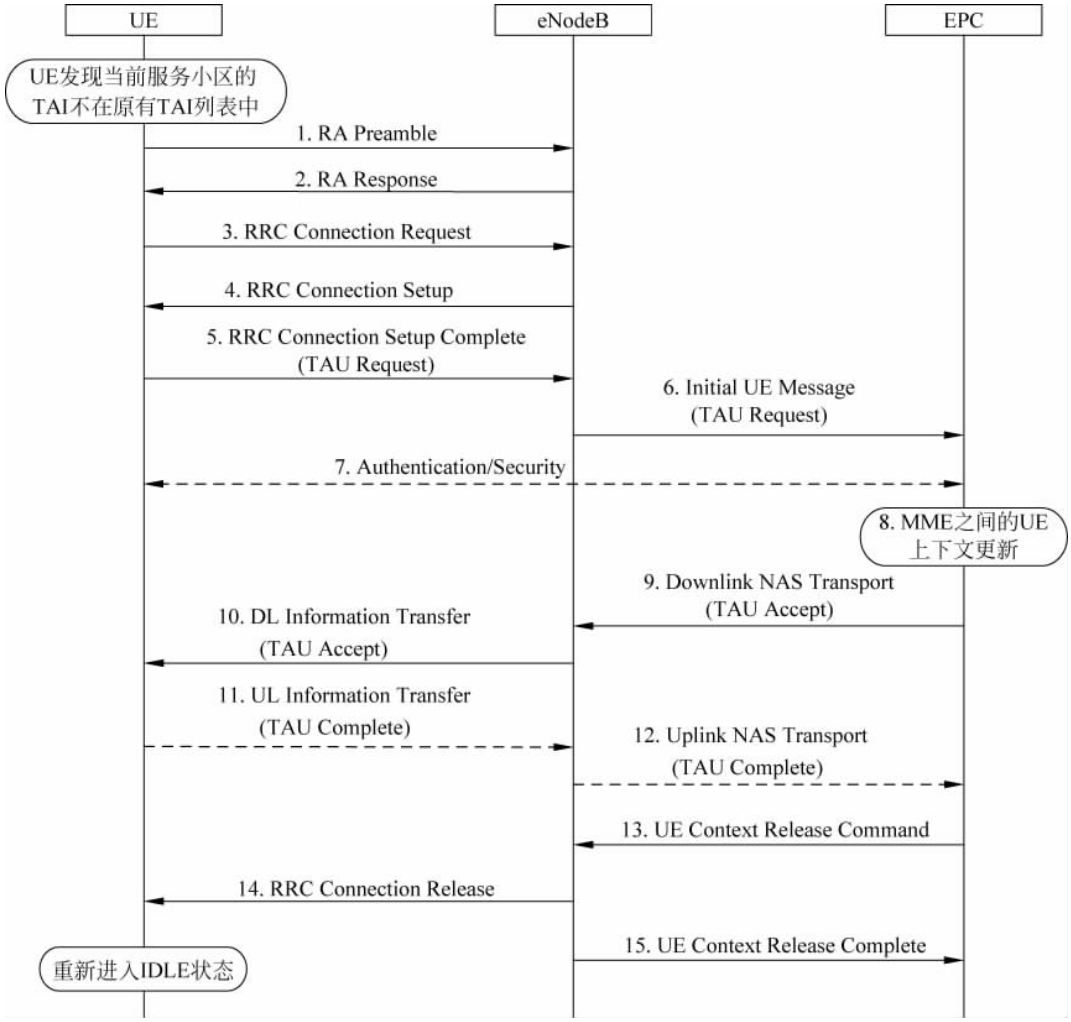

图 3-25　空闲态不激活的 TAU 流程

（1）处在 RRC_IDLE 状态的 UE 监听当前小区广播中的 TAI，若其不在原有的 TAI 列表中时，就发起随机接入过程，即 MSG1 消息。

（2）eNodeB 接收到 MSG1 消息后，向 UE 发送随机接入响应消息，即 MSG2 消息。

(3) UE 收到随机接入响应后，根据 MSG2 的 TA 调整上行发送时机，向 eNodeB 发送 RRC Connection Request 消息。

(4) eNodeB 向 UE 发送 RRC Connection Setup 消息，其中包含建立 SRB1 承载信息和无线资源配置信息。

(5) UE 完成 SRB1 承载和无线资源配置，向 eNodeB 发送 RRC Connection Setup Complete 消息，包含 NAS 层的 TAU Request 信息。

(6) eNodeB 向 MME 发送 Initial UE Message 消息，其中包含 NAS 层 TAU Request 消息。

(7) UE 与 EPC 间执行双向鉴权流程。

(8) MME 之间进行 UE 上下文更新。

(9) MME 向 eNodeB 发送 Downlink NAS Transport 消息，包含 NAS 层 TAU Accept 消息。

(10) eNodeB 接收到 Downlink NAS Transport 消息，向 UE 发送 DL Information Transfer 消息，包含 NAS 层 TAU Accept 消息。

(11) 在 TAU 过程中，如果分配了 GUTI，UE 就会向 eNodeB 发送 UL Information Transfer，包含 NAS 层 TAU Complete 消息。

(12) eNodeB 向 MME 发送 Uplink NAS Transport 消息，包含 NAS 层 TAU Complete 消息。

(13) TAU 过程完成，释放链路，MME 向 eNodeB 发送 UE Context Release Command 消息，指示 eNodeB 释放 UE 上下文。

(14) 图 3-25 中第 14、15 步，eNodeB 向 UE 发送 RRC Connection Release 消息，指示 UE 释放 RRC 链路；并向 MME 发送 UE Context Release Complete 消息进行响应。

2. 空闲态激活的 TAU 流程

空闲态激活的 TAU 流程对应数据传输前或承载发生修改时正好有位置更新发生。如图 3-26 所示，空闲态激活的 TAU 流程包括以下步骤：

(1) 第 1～12 步与空闲状态不激活的 TAU 流程相同。

(2) 第 13 步，UE 向 EPC 发送上行数据。

(3) 第 14 步，EPC 进行下行承载数据发送地址更新。

(4) 第 15 步，EPC 向 UE 发送下行数据。

3. 连接态 TAU 流程

如图 3-27 所示，连接态 TAU 流程包括以下步骤：

(1) 处在 RRC_CONNECTED 状态的 UE 进行去附着过程，向 eNodeB 发送 UL Information Transfer 消息，包含 NAS 层 TAU Request 信息。

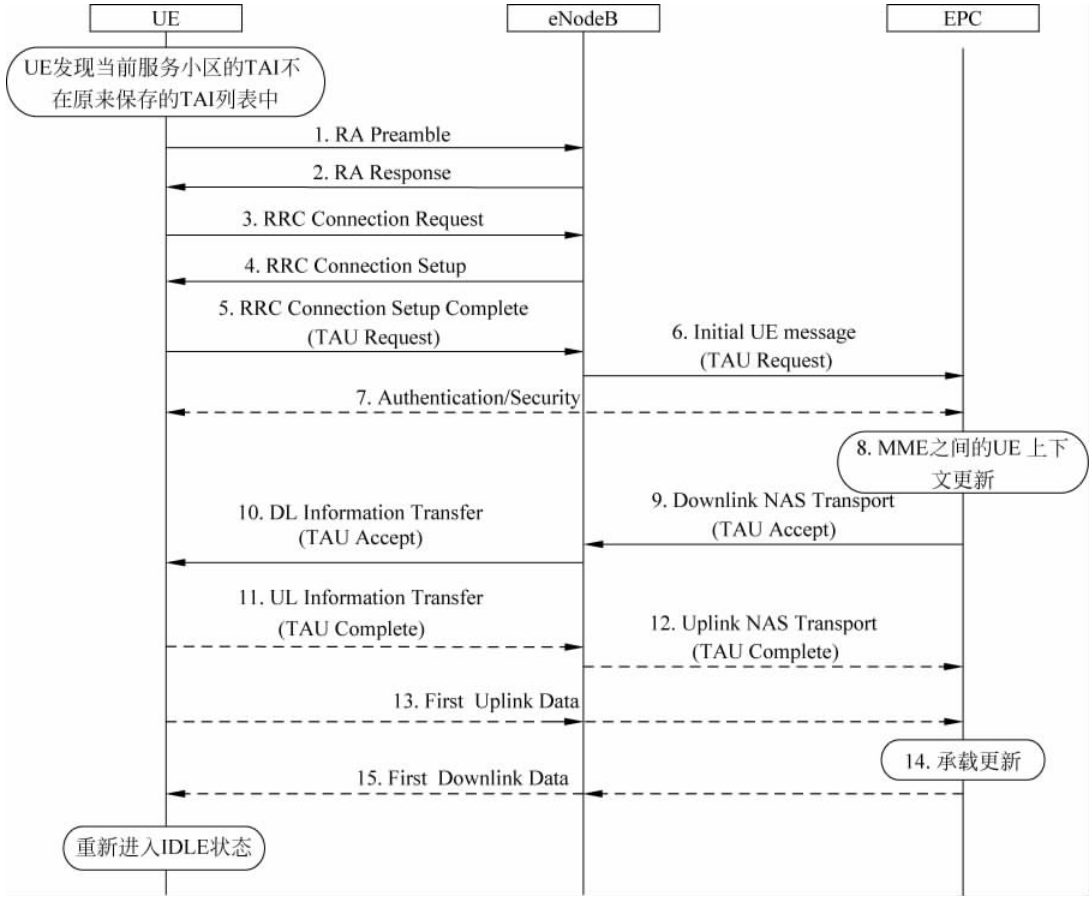

图 3-26　空闲态激活的 TAU 流程

(2) eNodeB 向 MME 发送上行直传 Uplink NAS Transport 消息,包含 NAS 层 TAU Request 信息。

(3) MME 更新 UE 上下文。

(4) MME 向基站发送下行直传 Downlink NAS Transport 消息,包含 NAS 层 TAU Accept 消息。

(5) eNodeB 向 UE 发送 DL Information Transfer 消息,包含 NAS 层 TAU Accept 消息。

(6) UE 向 eNodeB 发送 UL Information Transfer 消息,包含 NAS 层 TAU Complete 信息。

(7) eNodeB 向 MME 发送上行直传 Uplink NAS Transport 消息,包含 NAS 层 TAU Complete 信息。

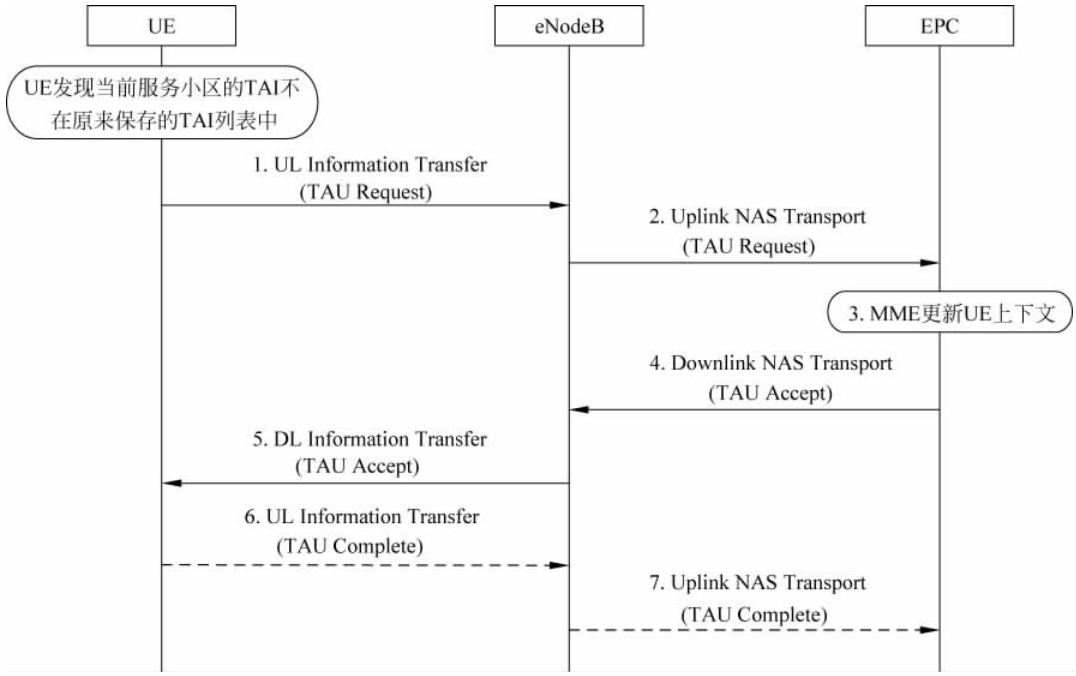

图 3-27　连接态 TAU 流程