LTE 信令流程

目录

概述

本文通过对重要概念的阐述，为信令流程的解析做铺垫，随后讲解 LTE 中重要信令流程，让大家熟悉各个物理过程是如何实现的，其次通过异常信令的解读让大家增强对异常信令流程的判断，再次对系统消息的解析，让大家了解系统消息的特点和携带的内容。最后通过实测信令内容讲解，说明消息的重要信元字段。

第一章协议层与概念

1.1 控制面与用户面

在无线通信系统中，负责传送和处理用户数据流工作的协议称为用户面；负责传送和处理系统协调信令的协议称为控制面。用户面如同负责搬运的码头工人，控制面就相当于指挥员，当两个层面不分离时，自己既负责搬运又负责指挥，这种情况不利于大货物处理，因此分工独立后，办事效率可成倍提升，在 LTE 网络中，用户面和控制面已明确分离开。

1.2 接口与协议

接口是指不同网元之间的信息交互时的节点，每个接口含有不同的协议，同一接口的网元之间使用相互明白的语言进行信息交互，称为接口协议，接口协议的架构称为协议栈。在 LTE 中有空中接口和地面接口，相应也有对应的协议和协议栈。

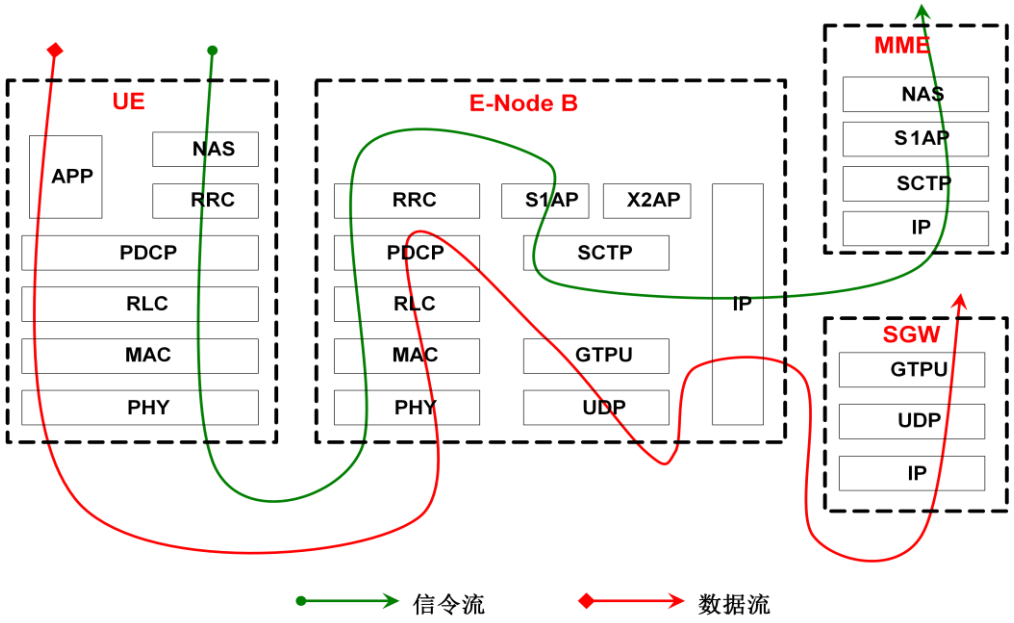


图 1 子层、协议栈与流

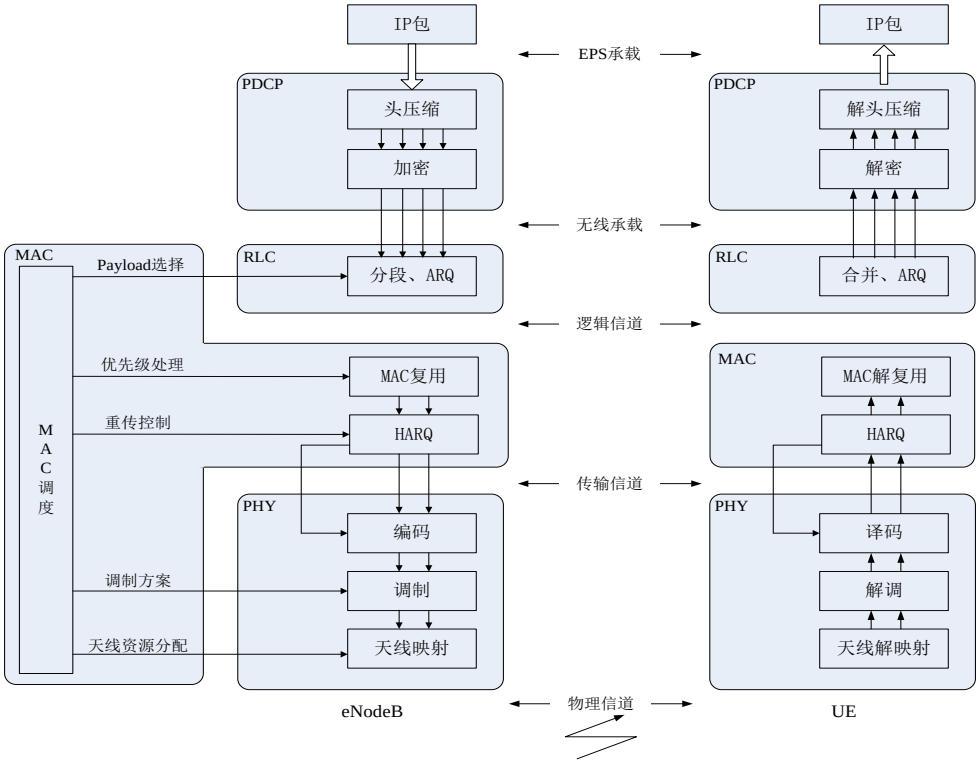


图 2 子层运行方式

LTE 系统的数据处理过程被分解成不同的协议层。简单分为三层结构：物理层、数据链路层 L2 和网络层。图 1 阐述了 LTE 系统传输的总体协议架构以及用户面和控制面数据信息的路径和流向。用户数据流和信令流以 IP 包的形式进行传送，在空中接口传送之前，IP 包

将通过多个协议层实体进行处理，到达 eNodeB 后，经过协议层逆向处理，再通过 S1/X2 接口分别流向不同的 EPS 实体，路径中各协议子层特点和功能如下：

1.2.1 NAS 协议（非接入层协议）

处理 UE 和 MME 之间信息的传输，传输的内容可以是用户信息或控制信息（如业务的建立、释放或者移动性管理信息）。它与接入信息无关，只是通过接入层的信令交互，在 UE 和 MME 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。

NAS 层功能如下：

- 会话管理：包括会话建立、修改、释放及 QoS 协商
- 用户管理：包括用户数据管理，以及附着、去附着
- 安全管理：包括用户与网络之间的鉴权及加密初始化
- 计费

1.2.2 RRC 层（无线资源控制层）

RRC 层是支持终端和 eNodeB 间多种功能的最为关键的信令协议。RRC 的功能包括：

- 广播 NAS 层和 AS 层的系统消息
- 寻呼功能（通过 PCCH 逻辑信道执行）
- RRC 连接建立、保持和释放，包括 UE 与 E-UTRAN 之间临时标识的分配、信令无线承载的配置
- 安全功能，包括密钥管理
- 端到端无线承载的建立、修改与释放
- 移动性管理，包括 UE 测量报告，以及为了小区间和 RAT 间移动性进行的报告控制、小区间切换、UE 小区选择与重选、切换过程中的 RRC 上下文传输等

- MBMS 业务通知，以及 MBMS 业务无线承载的建立、修改与释放
- QoS 管理功能
- UE 测量上报及测量控制
- NAS 消息的传输
- NAS 消息的完整性保护

1.2.3 PDCP 层（分组数据汇聚协议层）

负责执行头压缩以减少无线接口必须传送的比特流量。头压缩机制基于 ROHC。在接收端，PDCP 协议将负责执行解密及解压缩功能。对于一个终端每个无线承载有一个 PDCP 实体。一个 PDCP 实体是关联控制平面还是用户平面，主要取决于它为哪种无线承载携带数据。PDCP 层在控制面对 RRC 和 NAS 层消息进行完整性校验，在用户面不进行完整性校验。

PDCP 层功能

- IP 包头压缩与解压缩
- 数据与信令的加密
- 信令的完整性保护。

1.2.4 RLC 层（无线链路控制层）

负责分段与连接、重传处理，以及对高层数据的顺序传送。RLC 层以无线承载的方式为 PDCP 层提供服务，其中，每个终端的每个无线承载配置一个 RLC 实体。主要目的是将数据交付给对端的 RLC 实体。所以 RLC 提出了三种模式：透明模式（Transparent Mode，TM）、非确认模式（Unacknowledged Mode，UM）和确认模式（Acknowledged Mode，AM）。

TM 模式最简单，它对于上层数据不进行任何改变，这种模式典型地被用于 BCCH 或 PCCH 逻辑信道的传输，该方式不需对 RLC 层进行任何特殊的处理。RLC 的透明模式实体从上层接收到数据，然后不做任何修改地传递至下面的 MAC 层，这里没有 RLC 头增加、数据分割及串联。

UM 模式可以支持数据包丢失的检测，并提供分组数据包的排序和重组。UM 模式能够用于任何专用或多播逻辑信道，具体使用依赖于应用及期望 QoS 的类型。数据包重排序是指对不按顺序接收到的数据进行排序。

AM 模式是一种最复杂的模式。除了 UM 模式所支持的特征外，AM RLC 实体能够在检测到丢包时要求它的对等实体重传分组数据包，即 ARQ 机制。因此，AM 模式仅仅应用于 DCCH 或 DTCH 逻辑信道。

一般来讲，AM 模式典型地用于 TCP 的业务，如文件传输，这类业务主要关心数据的无错传输；UM 模式用于高层提供数据的顺序传送，但是不重传丢失的 PDU，典型地用于如 Voip 业务，这类业务最主要关心传送时延；TM 模式则仅仅用于特殊的目的，如随机接入。

1.2.5 MAC 层（媒体接入层）

负责处理 HARQ 重传与上下行调度。MAC 层将以逻辑信道的方式为 RLC 层提供服务。其主要目的是为 RLC 层业务与物理层之间提供一个有效的连接。从这个角度看，MAC 层支持的主要功能包括：

- 逻辑信道与传输信道之间的映射；
- 传输格式的选择，例如通过选择传输块大小、调制方案等作为输入参数提供给物理层；

- 一个 UE 或多个 UE 之间逻辑信道的优先级管理；
- 通过 HARQ 机制进行纠错；
- 填充（Padding）；
- RLC PDU 的复用与解复用；
- 业务量的测量与上报。

MAC 层提供给上层的业务主要包括：数据传送及无线资源分配。物理层提供给 MAC 层的业务包括：数据传送、HARQ 反馈信令、调度请求信令以及测量。

在上行链路发送中，终端侧的 MAC 层只是复用自己的多个上行链路数据流，并且决定是发送上行链路调度请求还是发送上行链路数据。然而在下行链路共享信道，eNodeB 必须考虑小区内发往所有用户的数据流（或逻辑信道）。这就涉及到优先级处理过程，优先权处理是 MAC 层的一个主要功能。优先权处理过程是指从不同的等待队列选出一个分组，将其传递到物理层，并通过无线接口发送的过程。因为要考虑到不同信息流的发送，包括纯用户数据、E-UTRAN 信令和 EPC 信令，这个过程非常复杂。当已传数据没有正确接收时，是否重传也与优先权处理有关，所以优先权处理过程还是与 HARQ 密切相关的，HARQ 是 MAC 的另一个主要功能。此外，网络侧的 MAC 层要负责上行链路优先权处理，因为它必须从共享 UL-SCH 传输信道的多个终端的所有上行链路调度请求消息中进行选择。

1.2.6 PHY 层（物理层）

负责处理编译码、调制解调、多天线映射以及其它电信物理层功能。物理层以传输信道的方式为 MAC 层提供服务。

物理层将包含如下功能：

- 传输信道的错误检测并向高层提供指示。

- 传输信道的前向纠错编码（FEC）与译码。
- 混合自动重传请求（HARQ）软合并。
- 传输信道与物理信道之间的速率匹配及映射。
- 物理信道的功率加权。
- 物理信道的调制与解调。
- 时间及频率同步。
- 射频特性测量并向高层提供指示。
- MIMO 天线处理。
- 传输分集。
- 波束赋形。
- 射频处理。

以上为 LTE 网络架构中各层的主要功能和作用，其中 MAC、RLC、PDCP 三个子层组成数据链路层，称为 L2。子层与子层之间使用服务接入点（Service Access Points， SAP）作为端到端通信的接口。PDCP 层向上提供无线承载服务，并提供可靠头压缩（Robust Header Compression， ROHC）与安全保护功能；物理层与 MAC 层之间的 SAP 为传输信道，MAC 层与 RLC 层之间的 SAP 为逻辑信道。物理信道，执行信息的收发；传输信道，区分信息的传输方式；逻辑信道，区分信息的类型。MAC 层主要负责提供逻辑信道到传输信道之间的映射，同时执行将几个逻辑信道（例如无线承载）复用到统一传输信道（例如传输块）。

LTE 系统的上下行架构各子层实现功能是基本相同的，它们的主要区别在于下行反映网络侧情况，处理多个用户；上行反映终端侧的情况，只处理一个用户。

1.3 空闲态和连接态

EPS 中有两种管理模型：移动性管理 EMM 和连接性管理 ECM。EMM 状态描述的是 UE 在网络中的注册状态，表明 UE 是否已经在网络中注册。注册状态的转变是由于移动性管理过程而产生的，比如附着过程和 TAU 过程。EMM 分为已注册和为注册两种状态。而 ECM 描述的是 UE 和 EPC 间的信令连接性，也有两种状态：空闲态 ECM-IDLE 和连接态 ECM-CONNECTED。空闲态和连接态是 RRC 子层中的两种状态，建立了 RRC 连接就是连接态，释放了 RRC 连接就是空闲态，如果是脱网、关机、DETACHED 就是 DEAD 态（在 RRC 中描述为 NULL）。

表 1 空闲态和连接态的特征

空闲状态（RRC-IDLE）的特征	连接状态（RRC-CONNECTED）的特征
PLMN 选择； 系统信息广播； 不连续接收寻呼； 小区重选移动性； UE 和网络之间没有信令连接，在 E-UTRAN 中不为 UE 分配无线资源，并且没有建立上下文。 UE 和网络之间没有 S1-MME 和 S1-U 连接。 UE 在由下行数据到达时，上述应终止在 S-GW，并由 MME 发起寻呼。 网络对应 UE 位置所知的精度为 TA 级别。 当 UE 进入未注册的新 TA 时，应执行 TA 更新。 应使用 DRX 等具有省电的功能	UE 有一个 RRC 连接； UE 在 E-UTRAN 中具有通信上下文； E-UTRAN 知道 UE 当前属于哪个小区； 网络和终端之间可以发送和接收数据； 网络控制的移动性管理，包括切换或者网络辅助小区更改（NACC）到 GERAN 小区； 可以测量邻小区； 终端可以监听控制信道以便确定网络是否为它配置了共享信道资源； eNodeB 可以根据终端的活动情况配置不连续接收（DRX）周期，节约电池并提高无线资源的利用率

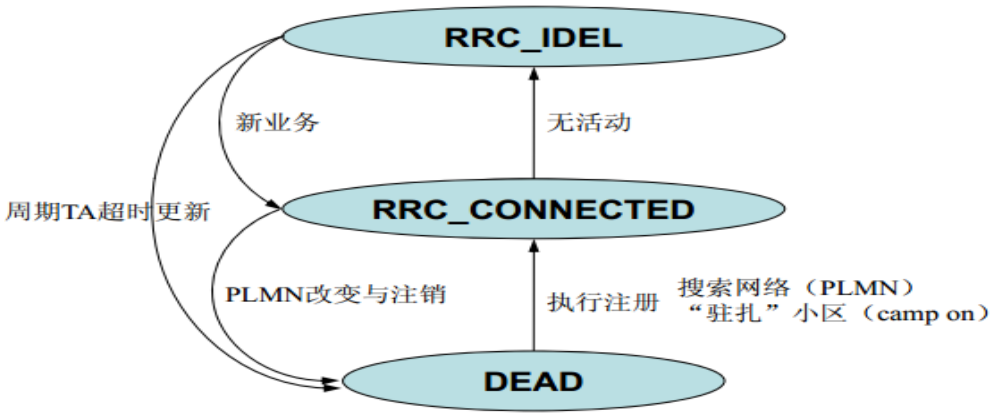


图 3 状态的转换过程

1.4网络标识

在 EPS 网络中，一共有 6 种不同的 UE 标识，包括 IMSI、IMEI、S-TMSI、C-RNTI、GUTI 和 IP，各个标识的生命周期、有效周期、功能作用和分配方式各不相同，在 LTE 信令分析中要懂得区分和查找。

C-RNTI:小区无线网络临时标识，由基站分配给 UE 的一个动态标识，唯一标识了一个小区空口下的 UE，只有处于连接态下的 UE，C-RNTI 才有效。（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:接入用-无线网络临时标识，收端 UE 知道自己之前 Preamble 的发送位置，通过计算可以检测 PDCCH 上是否有自己对应的 RA-RNTI；有，则说明接入被响应。RA-RNTI 可由 UE\eNodeB 根据公式计算而得（发生时刻、频域资源、前导格式等决定），无需通过信令来传送。对于 FDD，RA-RNTI 和 preamble 发送的子帧号一一对应，对于 TDD 同时要考虑频率资源。所以 RA-RNTI 对于 FDD 是 10 个，对于 TDD 最多 60 个。此标识在这里与其他标识对比，是接入用的标识。

IMEI:是由设备制造商给 UE 设备分配的一个永久标识，IMEI 存储在 SIM 卡和 HSS 中，同时 IMEI 可防止不法手机的再使用等，目前中国未使用。

IMSI:国际移动用户识别码，由 SP（service provider）给 UE 分配的一个永久标识，开户就有。只要 UE 能够使用 SP 提供的服务就一直有效，IMSI 存储在 SIM 和 HSS 中，是 3GPP 的 PLMN 中全球唯一标识。

S-TMSI:S-TMSI 是临时 UE 识别号，由 MME 产生并维护，用于 NAS 交互中保护用户的 IMSI，其中 S 代表 SAE，与 M-TMSI 一致。而在小区级识别 RRC 连接时，C-RNTI 提供唯一的 UE 识别号。

UEID:UE 标识，用于识别 UE。这些标识用户身份的 ID 在建立 RRC 连接时发送到 eNB

进行用户身份识别。UE ID 可以是 IMEI、IMSI、S-TMSI，另外 UE ID 不仅用于基站进行用户识别，在 SAE 侧同样需要使用 UE ID 进行用户识别。

GUTI: 在网络中唯一标识UE ,可以减少IMSI、IMEI等用户私有参数暴露在网络传输中。GUTI 由核心网分配的一个动态标识。只有在 EPC 注册同时附着 MME 的 UE，GUTI 才有效。存储在 UE 和 MME 中。在 attach accept, TAU accept, RAU accept 等消息中带给 UE。第一次 attach 时 UE 携带 IMSI，而之后 MME 会将 IMSI 和 GUTI 进行一个对应，以后就一直用 GUTI ,通过 attachaccept 带给 UE。在同一个 MME 下,GUTI 与 M-TMSI 一致。

IP 地址：是有 PGW 分配的一个动态的标识。在上下文本存在时有效。

1.5 承载概念

在 LTE 系统中 ,一个 UE 到一个 PGW 之间 ,具有相同 Qos 待遇的业务流称为一个 EPS 承载。EPS 承载中 UE 到 eNB 空口之间的一段称为无线承载 RB；eNB 到 SGW 之间的一段称为 S1 承载。无线承载与 S1 承载统称为 E-RAB。

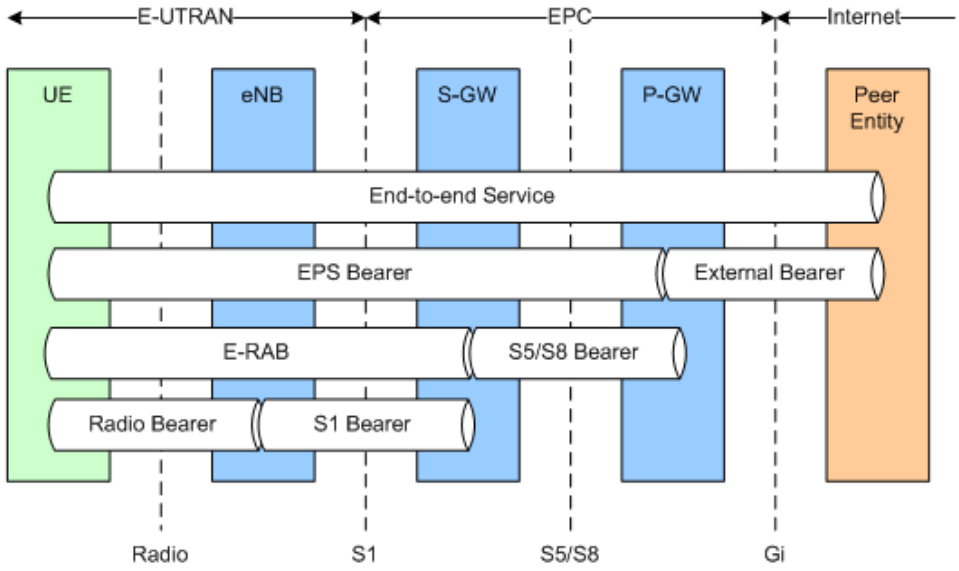


图 4 承载的位置关系

无线承载根据承载的内容不同分为 SRB (signaling radio bearer) 和 DRB (data radio

bearer）

SRB 承载控制面（信令）数据，根据承载的信令不同分为以下三类 SRB：

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。

SRB1 承载 RRC 信令（可能会携带一些 NAS 信令）和 SRB2 之间之前的 NAS 信令，通过 DCCH 逻辑信道传输，在 RLC 层采用 AM 模式。

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。

DRB 承载用户面数据，根据 Qos 不同，UE 与 eNB 之间可能最多建立 8 个 DRB。

根据用户业务需求和 Qos 的不同可以分为 GBR/ Non-GBR 承载，默认承载\专用承载，对承载的概念可以理解为“隧道”、“专有通道”、“数据业务链路”。

GBR/ Non-GBR 承载：在承载建立或修改过程中通过例如 eNode B 接纳控制等功能永久分配专用网络资源给某个保证比特速率（Guaranteed Bit Rate，GBR）的承载，可以确保该承载的比特速率。否则不能保证承载的速率不变则是一个 Non-GBR 承载

默认承载（Default Bearer）：一种满足默认 QOS 的数据和信令的用户承载，提供“尽力而为”的 IP 连接。默认承载为 Non-GBR 承载。默认承载为 UE 接入网络时首先建立的承载，该承载在整个 PDN 连接周期都会存在，为 UE 提供到 PDN 的“永远在线”的 IP 连接。

专用承载：对某些特定业务所使用的 SAE 承载。一般情况下专用承载的 QOS 比默认承载高，专用承载可以是 GBR 或 Non-GBR 承载。

第二章主要信令流程

2.1 开机附着流程

UE 刚开机时，先进行物理下行同步，搜索测量进行小区选择，选择到一个合适或者可接纳的小区后，驻留并进行附着过程。附着流程图如下：

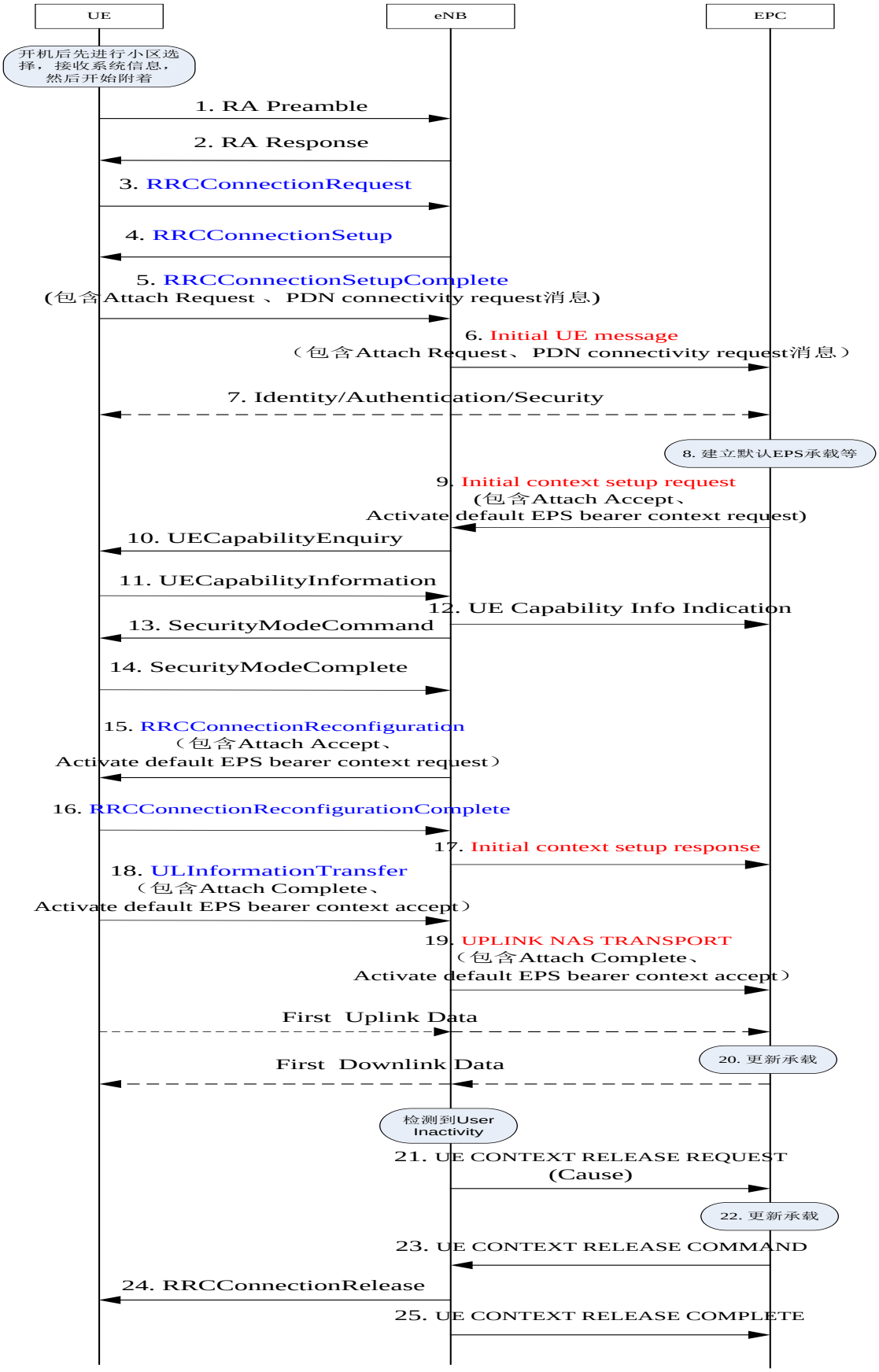

UE
eNB
EPC
开机后先进行小区选择，接收系统信息，然后开始附着
1. RA Preamble
2. RA Response
3. RRCConnectionRequest
4. RRCConnectionSetup
5. RRCConnectionSetupComplete
(包含Attach Request 、 PDN connectivity request消息)
6. Initial UE message
（包含Attach Request、 PDN connectivity request消息）
7. Identity/Authentication/Security
8. 建立默认EPS承载等
9. Initial context setup request
(包含Attach Accept、
Activate default EPS bearer context request)
10. UECapabilityEnquiry
11. UECapabilityInformation
12. UE Capability Info Indication
13. SecurityModeCommand
14. SecurityModeComplete
15. RRCConnectionReconfiguration
（包含Attach Accept、
Activate default EPS bearer context request）
16. RRCConnectionReconfigurationComplete
17. Initial context setup response
18. ULInformationTransfer
（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
First Downlink Data
20. 更新承载
检测到User Inactivity
21. UE CONTEXT RELEASE REQUEST
(Cause)
22. 更新承载
23. UE CONTEXT RELEASE COMMAND
24. RRCConnectionRelease
25. UE CONTEXT RELEASE COMPLETE

图 5 正常开机附着流程

开机附着流程说明：

1）步骤 1～5 会建立 RRC 连接，步骤 6、9 会建立 S1 连接，完成这些过程即标志着 NAS signalling connection 建立完成，见 24.301。

2）消息 7 的说明：UE 刚开机第一次 attach，使用的 IMSI，无 Identity 过程；后续，如果有有效的 GUTI，使用 GUTI attach，核心网才会发起 Identity 过程（为上下行直传消息）。

3）消息 10~12 的说明：如果消息 9 带了 UE Radio Capability IE，则 eNB 不会发送 UECapabilityEnquiry 消息给 UE，即没有 10~12 过程；否则会发送，UE 上报无线能力信息后，eNB 再发 UE Capability Info Indication，给核心网上报 UE 的无线能力信息。

为了减少空口开销，在 IDLE 下 MME 会保存 UE Radio Capability 信息，在 INITIAL CONTEXT SETUP REQUEST 消息会带给 eNB，除非 UE 在执行 attach 或者"first TAU following GERAN/UTRAN Attach" or "UE radio capability update" TAU 过程（也就是这些过程 MME 不会带 UE Radio Capability 信息给 eNB，并会把本地保存的 UE Radio Capability 信息删除，eNB 会问 UE 要能力信息，并报给 MME。注："UE radio capability update" TAU is only supported for changes of GERAN and UTRAN radio capabilities in ECM-IDLE.）。在 CONNECTED 下，eNB 会一直保存 UE Radio Capability 信息。UE 的 E_UTRAN 无线能力信息如果发生改变，需要先 detach，再 attach。

4） 发起 UE 上下文释放（即 21～25）的条件：

---

eNodeB-initiated with cause e.g. O&M Intervention, Unspecified Failure, User Inactivity, Repeated RRC signalling Integrity Check Failure, Release due to UE generated signalling connection release, etc.; or-MME-initiated with cause e.g. authentication failure, detach, etc.

5）eNB 收到 msg3 以后，DCM 给 USM 配置 SRB1，配置完后发送 msg4 给 UE；eNB 在发送 RRCConnectionReconfiguration 前，DCM 先给 USM 配置 DRB/SRB2 等信息，配置完后发送 RRCConnectionReconfiguration 给 UE，收到 RRCConnectionReconfigurationComplete 后，控制面再通知用户面资源可用。

6）消息 13~15 的说明：eNB 发送完消息 13，并不需要等收到消息 14，就直接发送消息 15。

7）如果发起 IMSI attach 时，UE 的 IMSI 与另外一个 UE 的 IMSI 重复，并且其他 UE 已经 attach，则核心网会释放先前的 UE。如果 IMSI 中的 MNC 与核心网配置的不一致，则核心网会回复 attach reject。

8）消息 9 的说明：该消息为 MME 向 eNB 发起的初始上下文建立请求，请求 eNB 建立承载资源，同时带安全上下文，可能带用户无线能力、切换限制列表等参数。UE 的安全能力参数是通过 attach request 消息带给核心网的，核心网再通过该消息送给 eNB。UE 的网络能力（安全能力）信息改变的话，需要发起 TAU。

2.2 随机接入流程

随机接入是蜂窝系统应具有的最基本的功能，它使终端与网络建立通信连接成为可能，由于用户的随机性、无线环境的复杂性决定了这种接入的发起以及采用的资源也具有随机性，因此随机接入的成功率取决于随机接入流程是否能够顺利完成。

从随机接入发起的目的来看主要有：

- 请求初始接入
- 从空闲状态向连续状态转换
- 支持 eNB 之间的切换过程
- 取得/恢复上行同步
- 向 eNB 请求 UE ID
- 向 eNB 发出上行发送的资源请求

总体来说随机接入就是 UE 与 eNB 建立无线链路，获取/恢复上行同步

从随机接入流程发起的场景来看，主要有以下几种情况：

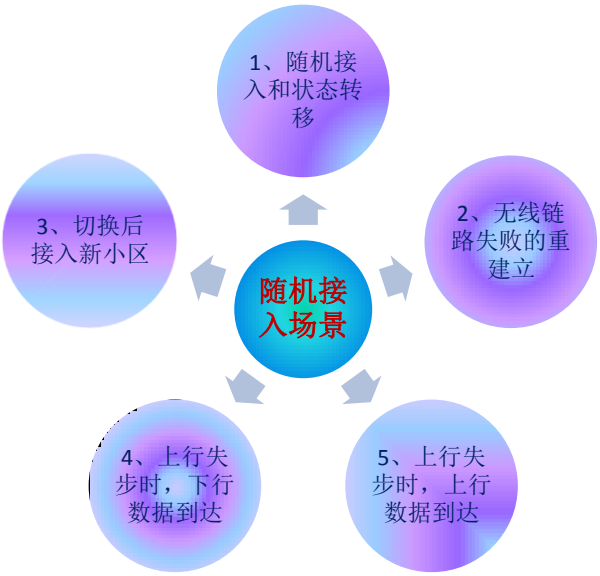


图 6 随机接入场景

随机接入分为基于竞争的（可应用于上述所有场景）、基于非竞争的(只应用于切换和下行数传场景)两种流程接入网络。其区别为针对两种流程选择随机接入前缀的方式不同。前

者为 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缀；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缀。

基于竞争模式的随机接入：

RRC_IDLE 状态下的初始接入；

无线链路出错以后的初始接入；

RRC_CONNECTED 状态下，当有上行数据传输时，例如在上行失步后“non-synchronised”， 或者没有 PUCCH 资源用于发送调度请求消息，也就是说在这个时候除了通过随机接入的方式外，没有其它途径告诉 eNB，UE 存在上行数据需要发送

基于非竞争模式的随机接入：

RRC_CONNECTED 状态下，当下行有数据传输时，这时上行失步“non-synchronised”，因为数据的传输除了接收外，还需要确认，如果上行失步的话，eNB 无法保证能够收到 UE 的确认信息，因为这时下行还是同步的，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，比如前导序列以及发送时机等，因为这些资源都是双方已知的，因此不需要通过竞争的方式接入系统；

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

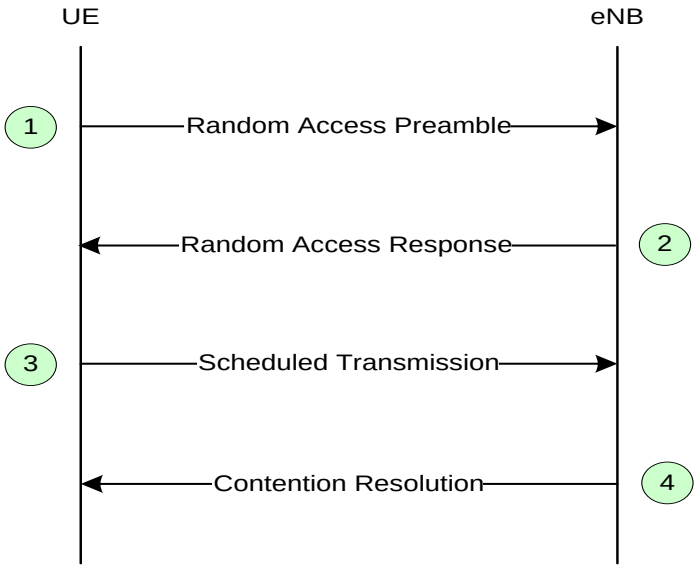


图 7 基于竞争的随机接入流程

基于竞争随机接入流程说明

1) MSG1：UE 在 RACH 上发送随机接入前缀，携带 preamble 码；

2) MSG2：eNB 侧接收到 MSG1 后，在 DL-SCH 上发送在 MAC 层产生随机接入响应（RAR），RAR 响应中携带了 TA 调整和上行授权指令以及 T-CRNTI（临时 CRNTI）；

3) MSG3（连接建立请求）：UE 收到 MSG2 后，判断是否属于自己的 RAR 消息（利用 preamble ID 核对），并发送 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)：RRC Contention Resolution 由 eNB 的 RRC 层产生，并在映射到 DL －SCH 上的 CCCH or DCCH(FFS)逻辑信道上发送，UE 正确接收 MSG4 完成竞争解决。

- 在随机接入过程中，MSG1 和 MSG2 是低层消息，L3 层看不到，所以在信令跟踪上，UE 入网的第一条信令便是 MSG3(RRC_CONN_REQ)
- MSG2 消息由 eNB 的 MAC 层产生，并由 DL_SCH 承载，一条 MSG2 消息可以同时对应多个 UE 的随机接入请求响应。
- eNB 使用 PDCCH 调度 MSG2，并通过 RA-RNTI 进行寻址，RA-RNTI 由承载 MSG1 的 PRACH 时频资源位置确定；
- MSG2 包含上行传输定时提前量、为 MSG3 分配的上行资源、临时 C-RNTI 等；
- UE 在接收 MSG2 后，在其分配的上行资源上传输 MSG3
- 针对不同的场景，Msg3 包含不同的内容：
  - 初始接入：携带 RRC 层生成的 RRC 连接请求，包含 UE 的 S-TMSI 或随机数；
  - 连接重建：携带 RRC 层生成的 RRC 连接重建请求，C-RNTI 和 PCI；
  - 切换：传输 RRC 层生成的 RRC 切换完成消息以及 UE 的 C-RNTI；
  - 上/下行数据到达：传输 UE 的 C-RNTI；

竞争解决	初始接入和连接重建场景	切换，上/下行数据到达场景
竞争判定	MSG4 携带成功解调的 MSG3 消息的拷贝，UE 将其与自身在 MSG3 中发送的高层标识进行比较，两者相同则判定为竞争成功	UE 如果在 PDCCH 上接收到调度 MSG4 的命令，则竞争成功
调度	MSG4 使用由临时 C-RNTI 加扰的 PDCCH 调度	eNB 使用 C-RNTI 加扰的 PDCCH 调度 MSG4
C-RNTI	MSG2 中下发的临时 C-RNTI 在竞争成功后升级为 UE 的 C-RNTI	UE 之前已分配 C-RNTI，在 MSG3 中也将其传给 eNB。竞争解决后，临时 C-RNTI 被收回，继续使用 UE 原 C-RNTI

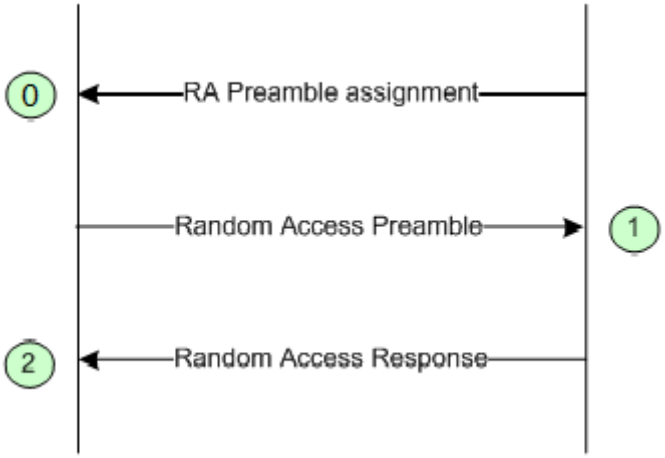


图 8 基于非竞争的随机接入

基于非竞争随机接入流程说明

1） MSG0：eNB 通过下行专用信令给 UE 指派非冲突的随机接入前缀（non-contention Random Access Preamble ），这个前缀不在 BCH 上广播的集合中。

2）MSG1：UE 在 RACH 上发送指派的随机接入前缀。

3） MSG2：ENB 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 ENB 分配，到 RAR 正确接受后就结束。

- UE 根据 eNB 的指示，在指定的 PRACH 上使用指定的 Preamble 码发起随机接入
- MSG0：随机接入指示消息

  对于切换场景，eNB 通过 RRC 信令通知 UE；

  对于下行数据到达和辅助定位场景，eNB 通过 PDCCH 通知 UE；
- MSG1：发送 Preamble 码

  UE 在 eNB 指定的 PRACH 信道资源上用指定的 Preamble 码发起随机接入
- MSG2：随机接入响应

  MSG2 与竞争机制的格式与内容完全一样，可以响应多个 UE 发送的 MSG1

2.3 UE 发起的 service request 流程

UE 在 IDLE 模式下，需要发送或接收业务数据时，发起 service request 过程（值得强调的是这流程之前是随机接入流程）。

当 UE 发起 service request 时，需先发起随机接入过程，Service Request 由 RRC Connection Setup Comlete 携带上去，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，并发起 service request 过程，在下行数据达到发起的 service request 类似于被叫接入。

service request 流程就是完成 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。

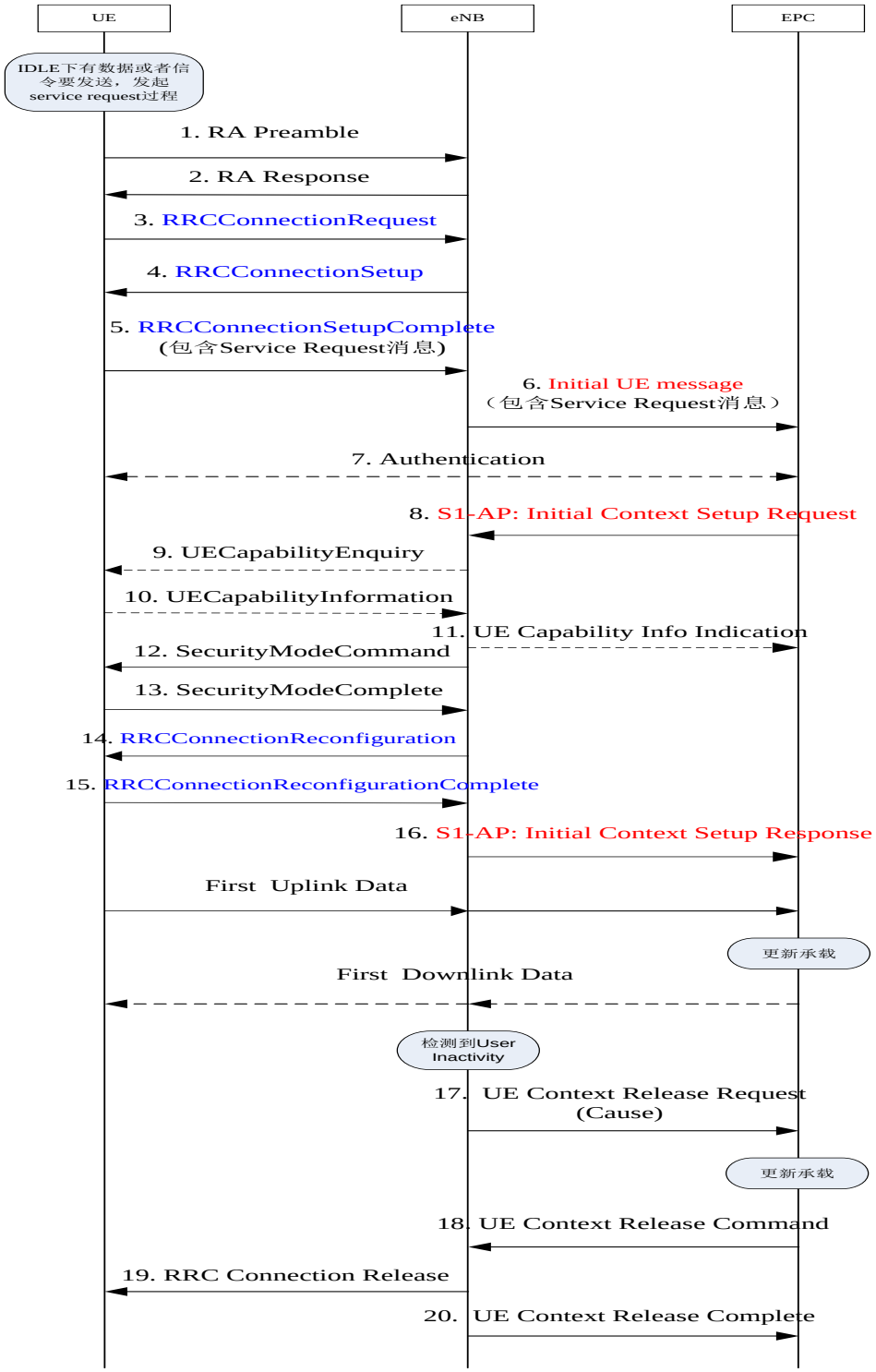


图 9 service request 流程

Service Request 流程说明：

1） 处在 RRC_IDLE 态的 UE 进行 Service Request 过程，发起随机接入过程，即 MSG1 消息；

2） eNB 检测到 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 eNB 发送 RRCConnectionRequest 消息，即 MSG3 消息；

4) eNB 向 UE 发送 RRCConnectionSetup 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,向 eNB 发送 RRCConnectionSetupComplete 消息,包含 NAS 层 Service Request 信息；

6) eNB 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，与 GSM 不同的是：4G 鉴权是双向鉴权流程，提高网络安全能力。

8) MME 向 eNB 发送 INITIAL CONTEXT SETUP REQUEST 消息，请求建立 UE 上下文信息；

9) eNB 接收到 INITIAL CONTEXT SETUP REQUEST 消息，如果不包含 UE 能力信息，则 eNB 向 UE 发送 UECapabilityEnquiry 消息，查询 UE 能力；

10) UE 向 eNB 发送 UECapabilityInformation 消息，报告 UE 能力信息；

11) eNB 向 MME 发送 UE CAPABILITY INFO INDICATION 消息，更新 MME 的 UE 能力信息；

12) eNB 根据 INITIAL CONTEXT SETUP REQUEST 消息中 UE 支持的安全信息，向 UE 发送 SecurityModeCommand 消息，进行安全激活；

13) UE 向 eNB 发送 SecurityModeComplete 消息，表示安全激活完成；

14) eNB 根据 INITIAL CONTEXT SETUP REQUEST 消息中的 ERAB 建立信息，向 UE 发送 RRCConnectionReconfiguration 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 eNB 发送 RRCConnectionReconfigurationComplete 消息，表示资源配置完成；

16) eNB 向 MME 发送 INITIAL CONTEXT SETUP RESPONSE 响应消息,表明 UE 上下文建立完成。流程到此时完成了 service request，随后进行数据的上传与下载。

17) 信令 17~20 是数据传输完毕后，对 UE 去激活过程，涉及 UE context release 流程。

2.4 寻呼流程

寻呼是网络寻找 UE 时进行的信令流程，网络中被叫必须通过寻呼来响应，才能正常通信。为减少信令负荷，在 LTE 中寻呼触发条件有三种：UE 被叫（MME 发起）；系统消息改变时（eNB 发起）；地震告警（Etws，不常见）。寻呼过程的实现依靠 TA 来进行（相当于 2/3G 的 LAC），需要说明的是寻呼的范围在 TAC 区内进行，不是在 TAC LIST 的范围内进行寻呼，TA LIST 只是减少了位置更新次数，从另一个方面降低信令负荷。

寻呼指示在 PDCCH 信道上通知 UE 响应自己的寻呼消息(PDCCH 通知上携带 P-RNT1，表示这是个寻呼指示），空口进行寻呼消息的传输时，eNB 将具有相同寻呼时机的 UE 寻呼内容汇总在一条寻呼消息里 ,寻呼消息内容被映射到 PCCH 逻辑信道中 ,并根据 UE 的 DRX 周期在 PDSCH 上发送，UE 并不是一次到位找到属于自己的寻呼消息，而是先找到寻呼时机，如果是自己的寻呼时机就在 PDSCH 信道上查询并响应属于自己的寻呼内容。

为了降低 IDLE 状态下的 UE 的电力消耗，UE 使用非连续接收方式（DRX），接收寻呼消息。IDLE 状态下的 UE 在特定的子帧里面根据 P-RNTI 监听读取 PDCCH，这些特定的子帧称为寻呼时机（Paging Occasion），这些子帧所在的无线帧称为（Paging Frame），UE 通过相关的公式来确定 PF 和 PO 的位置。计算出 PF 和 PO 的具体位置后，UE 开始监听 PDCCH，如果发现有 P-RNT1，那么 UE 在响应的位置上（PDSCH 信道）获取 Paging 消息,Paging message 中携带具体的被寻呼的 UE 标识(IMSI 或 S-TMSI)。若在 PCH 上未找到自己的标识，UE 再次进入 DRX 状态。

如果按寻呼方式不同，可以有 STMSI 寻呼和 IMSI 寻呼，一般情况下，优先使用 STMSI 寻呼，当网络发生错误需要恢复时（例如 S-TMSI 不可用），才发起 IMSI 寻呼。

寻呼发起原因不同也可分为被叫寻呼和小区系统消息改变时寻呼（地震寻呼不考虑），区别在于被叫寻呼由 EPC 发起，经 ENB 透传；而小区系统改变时寻呼由 ENB 发起。我们常

说的寻呼，主要还是指被叫寻呼。

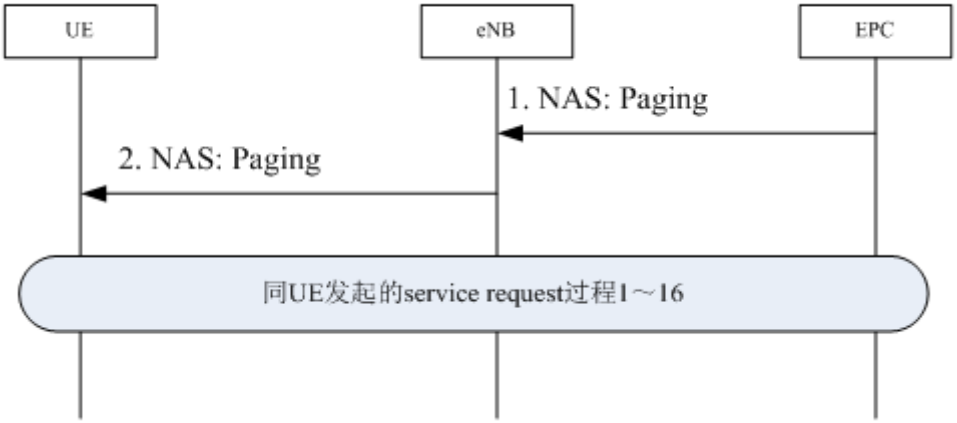


图 10 寻呼流程

被叫寻呼流程说明：

1）当 EPC 需要给 UE 发送数据时，则向 eNB 发送 PAGING 消息；

2）eNB 根据 MME 发的寻呼消息中的 TA 列表信息，在属于该 TA 列表的小区发送 Paging 消息，UE 在自己的寻呼时机接收到 eNB 发送的寻呼消息。

2.5 切换流程

2.5.1 切换的含义及目的

当正在使用网络服务的用户从一个小区移动到另一个小区，或由于无线传输业务负荷量调整、激活操作维护、设备故障等原因，为了保证通信的连续性和服务的质量，系统要将该用户与原小区的通信链路转移到新的小区上，这个过程就是切换。

本文中所描述的均为 LTE 系统内切换，系统间切换需要 UE 支持，并不做详细描述。在 LTE 系统中，切换可以分为站内切换、站间切换（或基于 X2 口切换、基于 S1 口切换），当 X2 接口数据配置完善且工作良好的情况下就会发生 X2 切换 ,否则基站间就会发生 S1 切换。一般来说 X2 切换的优先级高于 S1 切换。

2.5.2 切换发生的过程

切换判决准备—测量报告控制和测量报告上报

基站根据不同的需要利用移动性管理算法给 UE 下发不同种类的测量任务，在 RRC 重配消息中携带 MeasConfig 信元给 UE 下发测量配置；UE 收到配置信息后，对测量对象实施测量，并用测量上报标准进行结果评估，当评估测量结果满足上报标准后向基站发送相应的测量报告，比如 A2\A3 等事件。基站通过终端上报的测量报告判决是否执行切换。

当判决条件达到时，执行以下步骤：

- 切换准备：目标网络完成资源预留
- 切换执行：源基站通知 UE 执行切换；UE 在目标基站上连接完成
- 切换完成：源基站释放资源、链路，删除用户信息

值得注意的是 LTE 系统中，切换命令封装在消息 RRC_CONN_RECFG 信令消息中。

2.5.3 站内切换

当 UE 所在的源小区和要切换的目标小区同属一个 eNB 时，发生 eNB 内切换。eNB 内切换是各种情形中最为简单的一种，因为切换过程中不涉及 eNB 与 eNB 之间的信息交互，也就是 X2、S1 接口上没有信令操作，只是在一个 eNB 内的两个小区之间进行资源配置，所以基站在内部进行判决，并且不需要向核心网申请更换数据传输路径。

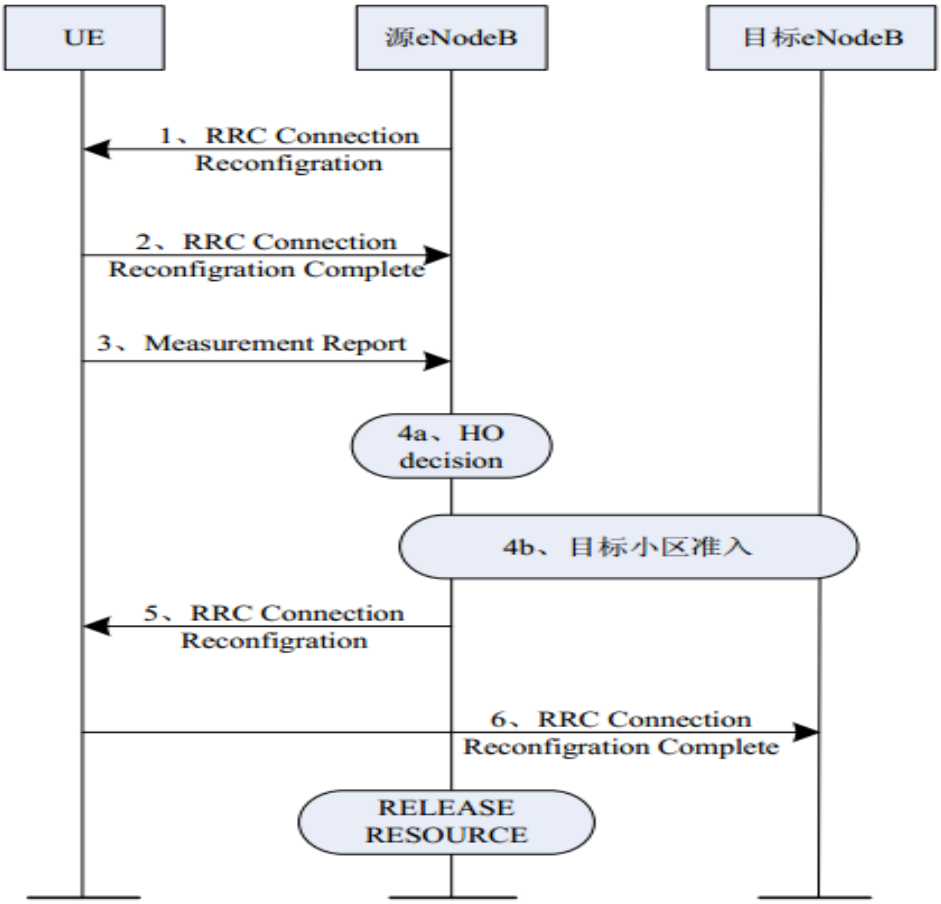


图 11 站内切换流程

站内切换流程说明：

其中步骤 1、2、3、4 为切换准备阶段，步骤 5、6 为切换执行阶段，步骤 7 为切换完成阶段。

1) eNodeB 向 UE 下发测量控制，通过 RRC Connection Reconfigration 消息对 UE 的测量类型进行配置；

2) UE 按照 eNodeB 下发的测量控制在 UE 的 RRC 协议端进行测量配置，并向 eNodeB 发送 RRC Connection Reconfigration Complete 消息表示测量配置完成；

3) UE 按照测量配置向 eNodeB 上报测量报告；

4) eNodeB 根据测量报告进行判决，判决该 UE 将发生 eNodeB 内切换，在新小区内进行资源准入，资源准入成功后为该 UE 申请新的空口资源；

5) 资源申请成功后 eNodeB 向 UE 发送 RRC Connection Reconfigration 消息，指示 UE 发起切换动作；

6) UE 接入新小区后 eNodeB 发送 RRC Connection Reconfigration Complete 消息指示 UE 已经接入新小区；

7）eNodeB 收到重配置完成消息后，释放该 UE 在源小区占用的资源。

2.5.4 X2 切换流程

当 UE 所在的源小区和要切换的目标小区不属于同一 eNodeB 时，发生 eNodeB 间切换，eNodeB 间切换流程复杂，需要加入 X2 和 S1 接口的信令操作。X2 切换的前提条件是目标基站和源基站配置了 X2 链路，且链路可用。

- 在接到测量报告后需要先通过 X2 接口向目标小区发送切换申请（目标小区是否存在接入资源）；
- 得到目标小区反馈后（此时目标小区资源准备已完成）才会向终端发送切换命令，并向目标侧发送带有数据包缓存、数据包缓存号等信息的 SNStatus Transfer 消息；
- 待 UE 在目标小区接入后，目标小区会向核心网发送路径更换请求，目的是通知核心网将终端的业务转移到目标小区，更新用户面和控制面的节点关系；
- 在切换成功后，目标 eNB 通知源 eNB 释放无线资源。X2 切换优先级大于 S1 切换，保证了切换时延更短，用户感知更好。

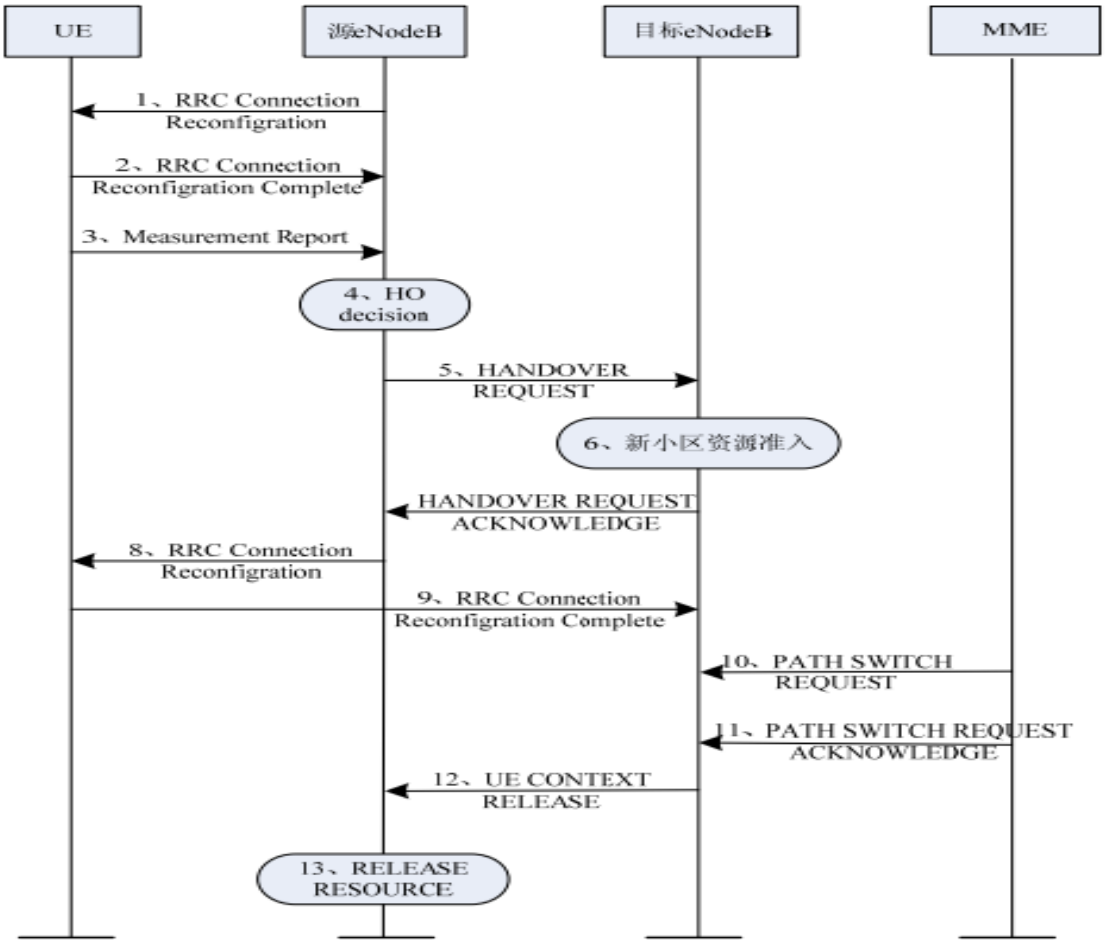


图 12 X2 切换流程

X2 切换流程说明

其中步骤 1、2、3、4、5、6、7 为切换准备阶段，步骤 8、9 为切换执行阶段，步骤 10、11、12、13 为切换完成阶段:

1) 源 eNodeB 向 UE 下发测量控制，通过 RRC Connection Reconfigration 消息对 UE 的测量类型进行配置；

2) UE 按照 eNodeB 下发的测量控制在 UE 的 RRC 协议端进行测量配置，并向 eNodeB 发送 RRC Connection Reconfigration Complete 消息表示测量配置完成；

3) UE 按照测量配置向 eNodeB 上报测量报告；

4) 源 eNodeB 根据测量报告进行判决，判决该 UE 发生 eNodeB 间切换，也有可能负荷分担的原因触发切换；

5) 源 eNodeB 向目标 eNodeB 发生 HANDOVER REQUEST 消息，指示目标 eNodeB 进行切换准备，切换请求消息包含源 eNB 分配的 Old eNB UE X2AP ID，MME 分配的 MME UE S1AP ID，需要建立

的 EPS 承载列表以及每个 EPS 承载对应的核心网侧的数据传送的地址。目标 ENB 收到 HANDOVER REQUEST 后开始对要切换入的 ERABs 进行接纳处理。;

6) 目标小区进行资源准入，为 UE 的接入分配空口资源和业务的 SAE 承载资源;

7) 目标小区资源准入成功后，向源 eNodeB 发送“切换请求确认”消息，指示切换准备工作完成，“切换请求确认”消息包含 New eNB UE X2AP ID、Old eNB UE X2AP ID、新建 EPS 承载对应在 D 侧上下行数据传送的地址、目标侧分配的专用接入签名等参数;

8) 源 eNodeB 将分配的专用接入签名配置给 UE，向 UE 发送 RRC Connection Reconfigration 消息命令 UE 执行切换动作;

9) UE 向目标 eNodeB 发送 RRC Connection Reconfigration Complete 消息指示 UE 已经接入新小区，表示 UE 已经切换到了目标侧。同时，切换期间的业务数据转发开始进行;

10) 目标 eNodeB 向 MME 发送 PATH SWITCH REQUEST 消息请求，请求 MME 更新业务数据通道的节点地址，通知 MME 切换业务数据的接续路径，从源 eNB 到目标 eNB，消息中包含原侧侧的 MME UE S1AP ID、目标侧侧分配的 eNB UE S1AP 、EPS 承载在目标侧将使用的下行地址;

11) MME 成功更新数据通道节点地址，向目标 eNodeB 发送 PATH SWITCHREQUEST ACKNOWLEDGE 消息，表示可以在新的 SAE bearers 上进行业务通信;

12) UE 已经接入新的小区，并且在新的小区能够进行业务通信，需要释放在源小区所占用的资源，目标 eNodeB 向源 eNodeB 发送 UE CONTEXTRELEASE 消息;

13) 源 eNodeB 释放该 UE 的上下文，包括空口资源和 SAE bearers 资源。

2.5.5 S1 切换流程

S1 切换流程与 X2 切换类似，只不过所有的站间交互信令及数据转发都需要通过 S1 口到核心网进行转发，时延比 X2 口略大。协议 36.300 中规定 eNodeB 间切换一般都要通过 X2 接口进行，但当如下条件中的任何一个成立时则会触发 S1 接口的 eNodeB 间切换：

（1）源 eNodeB 和目标 eNodeB 之间不存在 X2 接口；

（2）源 eNodeB 尝试通过 X2 接口切换，但被目标 eNodeB 拒绝。

从 LTE 网络结构来看，可以把两个 eNodeB 与 MME 之间的 S1 接口连同 MME 实体看

做是一个逻辑 X2 接口。相比较于通过 X2 接口的流程，通过 S1 接口切换的流程在切换准备过程和切换完成过程有所不同。S1 切换的前提条件：目标基站和源基站没有配置 X2 链路，或是配置的 X2 链路不可用。如果同时配置了 X2 和 S1 链路，优先走 X2 切换。下图中的流程没有跨 MME 和 SGW，相对简单。即使涉及跨 MME，主流程差异不大，主要在核心网的信令会更多一点而已。

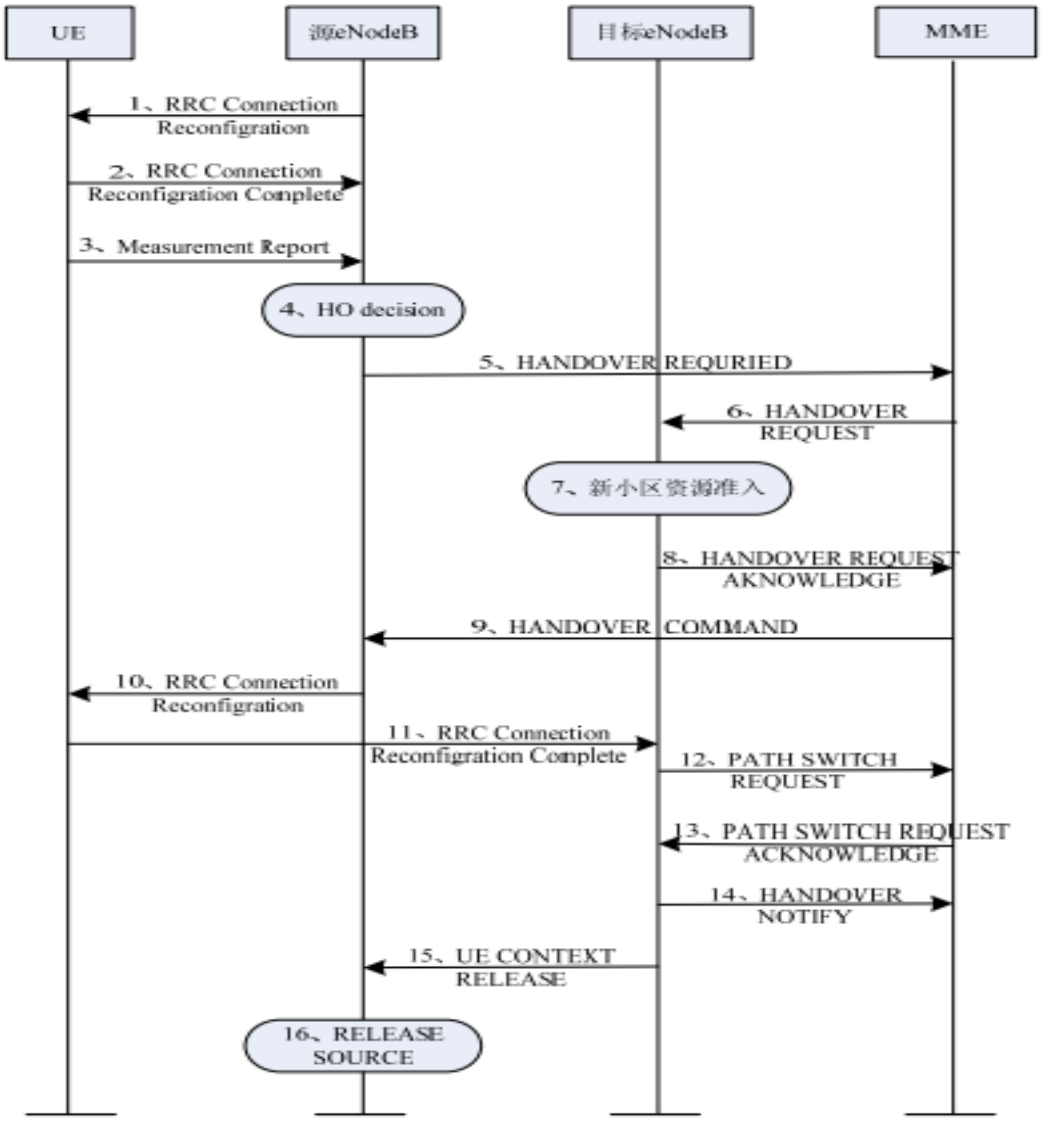


图 13 S1 切换流程

S1 切换流程说明

其中步骤 1 到 9 为切换准备过程，步骤 10、11 为切换执行过程，步骤 12 到 16 为切换完成过程。

1~4) 图中 1~4 步骤与 X2 切换相同，不做累述；

5) 源 eNB 通过 S1 接口的 HANDOVER REQUIRED 消息发起切换请求，消息中包含 MME UE S1AP ID、源侧分配的 eNB UE S1AP ID 等信息。

6) MME 向目标 eNB 发送 HANDOVER REQUEST 消息，消息中包括 MME 分配的 MME UE S1AP ID、需要建立的 EPS 列表以及每个 EPS 承载对应的核心网侧数据传送的地址等参数。

7~8) 目标 eNB 分配后目标侧的资源后，进行切换入的承载接纳处理，如果资源满足，小区接入允许就给 MME 发送 HANDOVER REQUEST ACKNOWLEDGE 消息，包含目标侧侧分配的 eNB UE S1AP ID，接纳成功的 EPS 承载对应的 eNodeB 侧数据传送的地址等参数。

9) 源 eNB 收到 HANDOVER COMMAND，获知接纳成功的承载信息以及切换期间业务数据转发的目标侧地址 。

10) 源 eNB 向 UE 发送 RRCConnectionReconfiguration 消息，指示 UE 切换指定的小区.

11) 源 eNB 通过 eNB Status Transfer 消息，MME 通过 MME Status Transfer 消息 ，将 PDCP 序号通过 MME 从源 eNB 传递到目标 eNB。目标 eNB 收到 UE 发送的 RRC Connection Reconfiguration Complete 消息，表明切换成功。

12) 目标 eNodeB 向 MME 发送 PATH SWITCH REQUEST 消息请求，请求 MME 更新业务数据通道的节点地址，通知 MME 切换业务数据的接续路径，从源 eNB 到目标 eNB，消息中包含原侧侧的 MME UE S1AP ID、目标侧侧分配的 eNB UE S1AP 、EPS 承载在目标侧将使用的下行地址；

13) MME 成功更新数据通道节点地址，向目标 eNodeB 发送 PATH SWITCHREQUEST ACKNOWLEDGE 消息，表示可以在新的 SAE bearers 上进行业务通信；

14) 目标侧 eNB 发送 HANDOVER NOTIFY 消息，通知 MME 目标侧 UE 已经成功接入。

15) 源 ENB 收到“UE CONTEXT RELEASE COMMAND”消息后，开始进入释放资源的流程。

2.5.6 异系统切换简介

E-UTRAN 的系统间切换可以采用 GERAN 与 UTRAN 系统间切换相同的原则。

E-UTRAN 的系统间切换可以采用以下的原则。

(1) 系统间切换是源接入系统网络控制的。源接入系统决定启动切换准备并按目标系统要求的格式提供必要的信息。也就是说，源系统去适配目标系统。真正的切换执行过程由源系

统控制。

(2) 系统间切换是一种后向切换，也就是说，目标 3GPP 接入系统中的无线资源在 UE 收到从源系统切换到目标系统的切换命令前已经准备就绪。

(3) 为实现后向切换，当接入网（RAN）级接口不可用时，将使用核心网（CN）级控制接口。

异系统切换的情形发生在 UE 在 LTE 小区与非 LTE 小区之间的切换，切换过程中涉及到的信令流主要集中在核心网。以 UE 从 UTRAN 切换到 E-UTRAN 为例说明，UE 所在的 RNC 向 UTRAN 的 SGSN 发送切换请求，SGSN 需要与 LTE 的 MME 之间进行消息交互，为业务在 E-UTRAN 上创建承载，同时需要 UE 具备双模功能，使 UE 的空口切换到 E-UTRAN 上来，最后再由 MME 通知 SGSN 释放源 UTRAN 上的业务承载。

2.6 CSFB 流程

在 LTE 系统里，CSFB 技术是针对 TD-LTE 多模单待终端提供语音服务的临时解决方案，大意是数据业务和短信业务由 LTE 承载，电话业务回落到 CS 网络，回落过程数据业务中断，电话业务结束后返回 LTE 网络。

在中国移动 CSFB 流程中，由于 GSM 网覆盖率较好，网络相对成熟，因此回落到 2G。其主要思想是终端驻留在 LTE，呼叫建立前先重选回 2/3G，由 CS 域网络提供语音服务，VoIP 成熟后，该方案会被替换，主要是因为 CSFB 用户不可及时长太长（R9 方案为 6~7 秒），本文介绍其流程为投诉人员处理 CSFB 问题时提供参考，可以不做重点学习。CSFB 技术方案的实现需要 UE 终端支持多种网络制式（换句话说，终端要支持 CSFB），通过联合附着/联合位置更新的方式响应网络。

2.6.1 CSFB 主叫流程

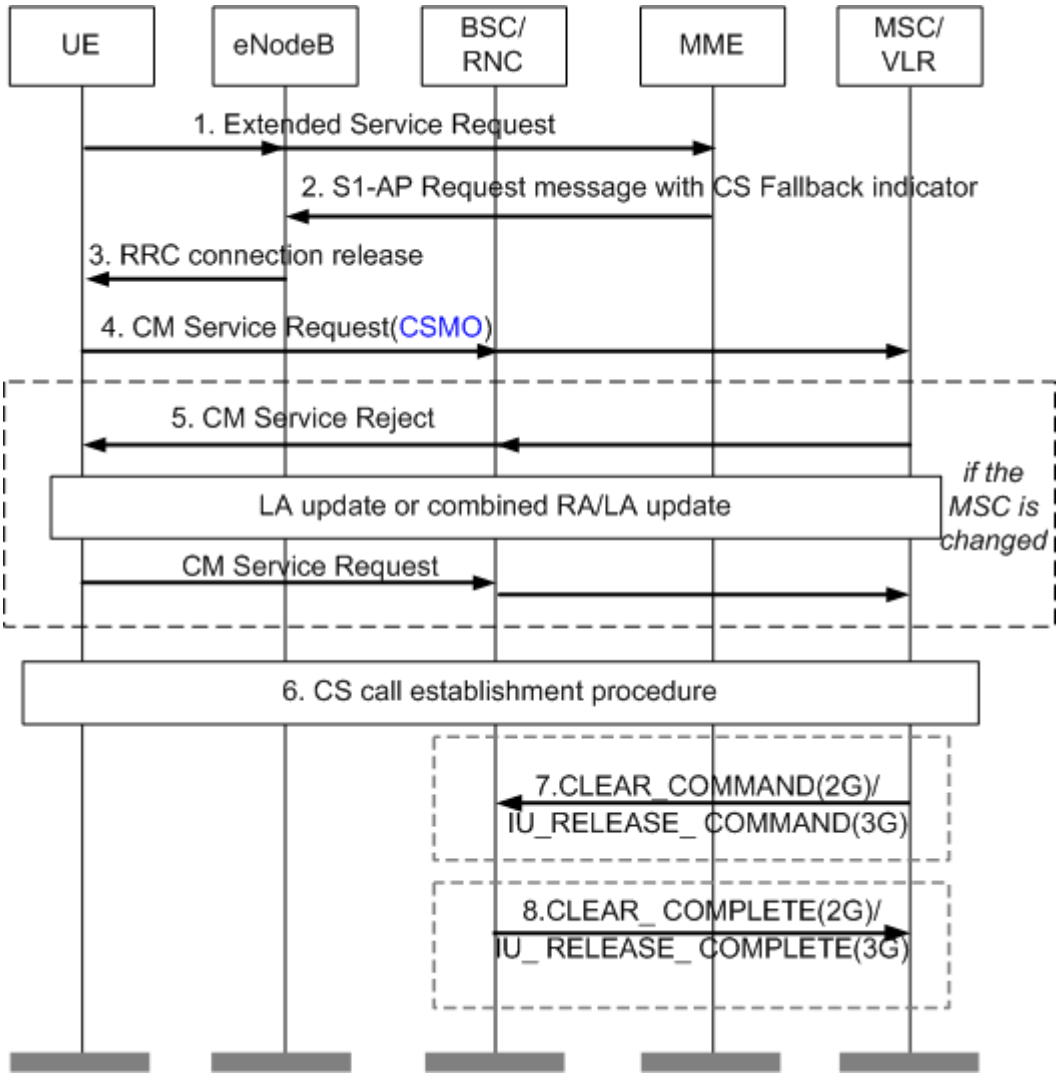


图 14 主叫 CSFB 流程

主叫 CSFB 流程说明

1） UE 发起 CS Fallback 语音业务请求。UE 语音拨打时，会发一条 extended service request，消息里会携带 CSFB 信息。其中 service-type 信元指示业务类型为始发 CSFB 语音业务，同时携带该 UE 在联合附着过程中 CS 域给它分配的 TMSI。之后会在基站的辅助下回落至 2G。

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

3） eNodeB 要求 UE 开始系统的小区测量，并获得 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 目标小区广播信息，将 2G 网络的广播信息一并填充至 RRC Release 消息中下发，省去终端读取 2G 广播信息的时间（约省 1.83 秒）

4） UE 接入目标系统小区，发起 CS 域的业务请求 CM Service Request。如果 CM 业务请求消息中携带“CSMO”标志，则 MSC Server 记录本次呼叫是移动始端 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，由于没有该 UE 的信息，可以采取隐式位置更新流程，接受用户请求。如果 MSC Server 不支持隐式位置更新，且 MSC Server 没有用户数据，则拒绝该用户的业务请求。如果 MSC Server 拒绝用户的业务请求会导致 UE 发起一个 CS 域位置更新流程。终端发起位置更新请求，且位置更新请求消息中的 Additional update parameters 信元中携带 CSMO 标识，同时该标识有效，则 MSC Server 会记录本次呼叫是 CSFB 呼叫。(CS fallback 紧急呼叫流程中，CM_SERVICE_REQUEST 消息前无需位置更新。)

6）完成位置更新后 UE 再次在 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 发送的拆线消息 CLEAR_COMMAND 消息中携带 CSFB Indication 信元，指示 BSC 拆除空口连接并指示 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/RNC 的 IU_RELEASE_COMPLETE 消息表示呼叫结束，A 口拆链完成。接入侧在指示终端重选网络时只针对 CSFB 用户通话前携带 LTE 频点，实现 CSFB 终端快速返回 LTE，快速回落过程也称为 FastReturn（用户不可及时间可缩短为 1-2 秒。)。

2.6.2 CSFB 被叫流程

MSC Server 收到对 UE 的被叫语音请求，通过存在的 SGs 关联和 MME 信息，向该 MME 发起寻呼请求。MME 通过 eNodeB 在空口寻呼该 UE，并指示 UE 回落到目标

GERAN/UTRAN 网络。UE 接入到目标网络后，在电路域继续进行语音呼叫。

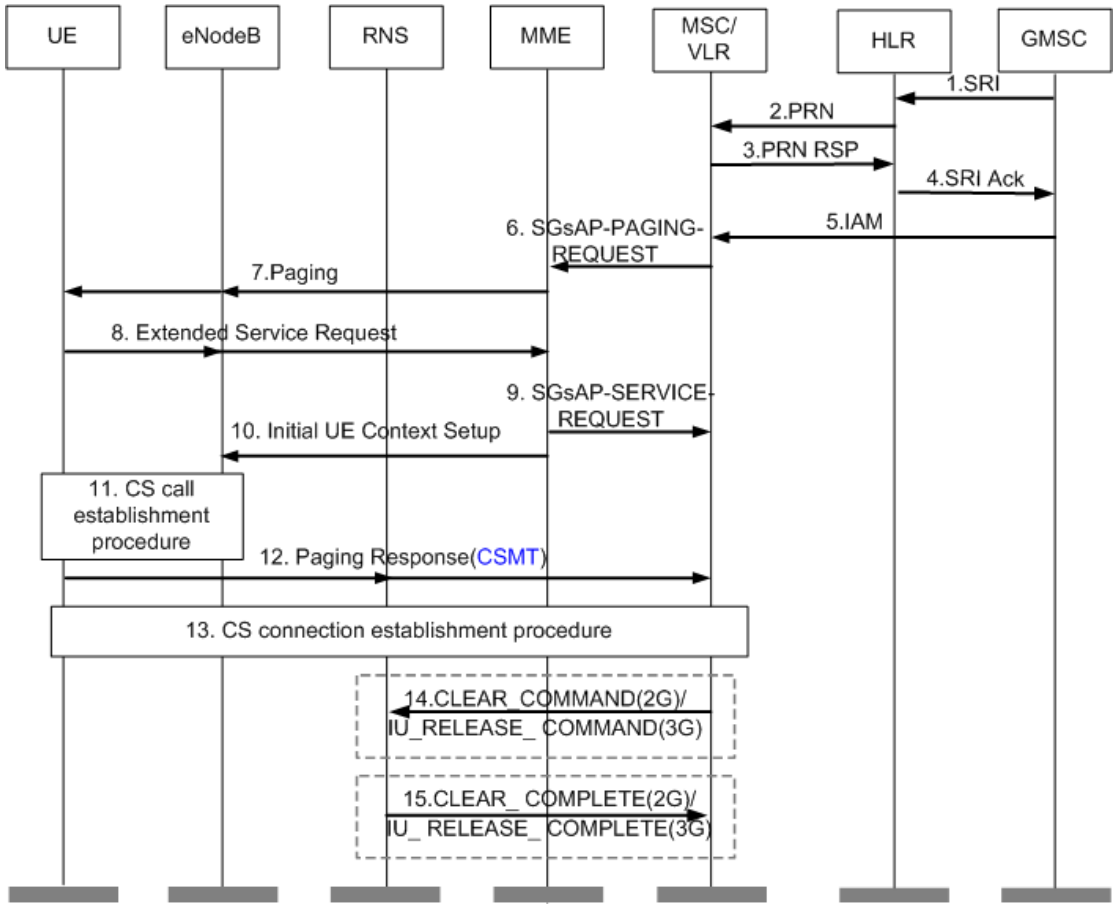


图 15 被叫 CSFB 流程

被叫 CSFB 流程说明

1） GMSC Server 向被叫用户归属 HLR 发送取路由信息请求。

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

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

4） HLR 将该漫游号码发送给 GMSC。

5） GMSC 收到该漫游号码后，进行号码分析，根据分析结果将呼叫路由到 old MSC Server。

6） MSC Server 收到 IAM 入局（例如中继 ISUP 入局）消息后，根据存在的 SGs 关联和 MME 信息，发送 SGsAP-PAGING-REQUEST(携带 IMSI，TMSI，Service indicator ，CLI，LAC)消息给 MME。

7） MME 发送 Paging 消息给 eNodeB。eNodeB 发起空口的 Paging 流程。

8） UE 建立连接并发送 Extended Service Request 消息给 MME（消息中携带“CSMT”移动终端标识）。

9） MME 发送 SGsAP-SERVICE-REQUEST 消息给 MSC Server。MSC Server 收到此消息，不再向

MME 重发寻呼请求消息。为避免呼叫接续过程中，主叫等待时间过长，MSC Server 收到包含空闲态指示的 SGs Service Request 消息，先通知主叫，呼叫正在接续过程中。

10） MME 发送 Initial UE Context Setup 消息给 eNodeB，包含 CS Fallback Indicator。该消息指示 eNodeB，UE 因 CSFB 业务需要回落到 UTRAN/GERAN。

11） UE 回落到 CS 域之后，UE 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 收到 UE 发送的 LOCATION_UPDATE_REQUEST 消息。这种情况下，UE 不需要回 Paging Response 给 MSC Server，UE 直接发送 SETUP 消息建立呼叫。如果位置更新消息中携带“CSMT”标志，则 MSC Server 记录本次呼叫是 CSFB 呼叫。

12） 伴随着空口、A/Iu-CS 接口连接的建立，UE 回 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，指示 BSC/RNC 拆除空口连接并指示 UE 回到 LTE 网络。

15） MSC 收到 BSC 的 CLEAR_COMPLETE 消息/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 LTE 频点，实现 CSFB 终端快速返回 E-UTRAN。FastReturn 方案也需要网络的支持，如果网络不支持，则通过网络优先级的方式返回 LTE（一般为最高优先级）。

2.6.3 紧急呼叫流程

带 USIM 卡的 UE 用户发起紧急呼叫时，MME 指示 eNodeB 需要将 UE 回落到 GERAN/UTRAN 网络。与普通语音呼叫相比，紧急呼叫业务流程无需进行位置更新流程处理。不带 USIM 卡的 UE 用户发起紧急呼叫时，由于卡类型以及也未在具体网络附着，此时的紧急呼叫流程与普通 RAN/UTRAN 网络的呼叫流程一样。

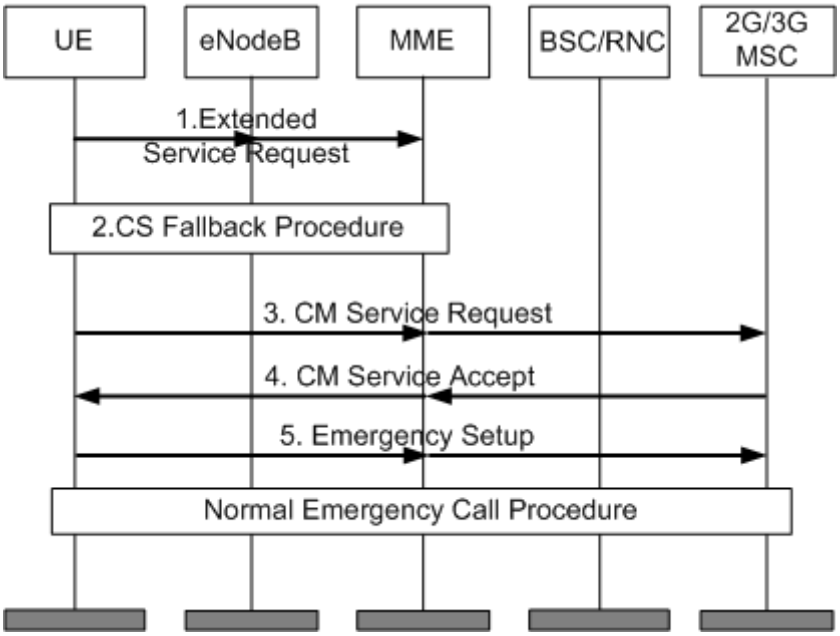


图 16 LTE 网络紧急呼叫流程

LTE 网络紧急呼叫流程说明

1） UE 发起 CS Fallback 呼叫业务请求。Extended Service Request 消息中的 service-type 信元指示业务类型为紧急呼叫业务。

2） MME 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

4） MSC 向 UE 返回 CM Service Accept 消息。

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

2.7 TAU 流程

为了确认移动台的位置，LTE 网络覆盖区将被分为许多个跟踪区(Tracking Area) TA 功能与 3G 的位置区(LA)和路由区(RA)类似，是 LTE 系统中位置更新和寻呼的基本单位。TA 用 TA 码标识，一个 TA 可包含一个或多个小区，TAC 在这些小区的 SIB1 中广播与 LAC、RAC 类似，网络运营时用 TAI 作为 TA 的唯一标识，TAI 由 MCC、MNC 和 TAC 组成，共计 6 字节。TAI LIST 长度为 8~98 字节，最多可包含 16 个 TAI，UE 附着成功时获取一组

TAI LIST(具体与 UE 关机前的状态有关)，移动过程中只要进入的 TAI LIST 中没有的 TA 就发生位置更新，把新的 TA 更新到 TAI LIST 中，如果表中已经存在 16 个 TA,则替换掉最旧的那个；如果 UE 在移动过程中进入一个 TAI list 表单中的 TA 时，不发生位置更新。TA 更新成功与否直接关系到寻呼成功率问题，在 LTE 网络中为了实现 CSFB 流程，附着和位置更新都是联合的。根据位置更新发生的时机，空闲态一般有设置激活和不设置激活的两种位置更新。设置激活就是位置更新后可立即进行数据传输。

2.7.1 空闲态不设置“ACTIVE”的 TAU 流程

这种状态就是 UE 不做业务，只是位置更新，比如周期性位置更新、移动性位置更新等；

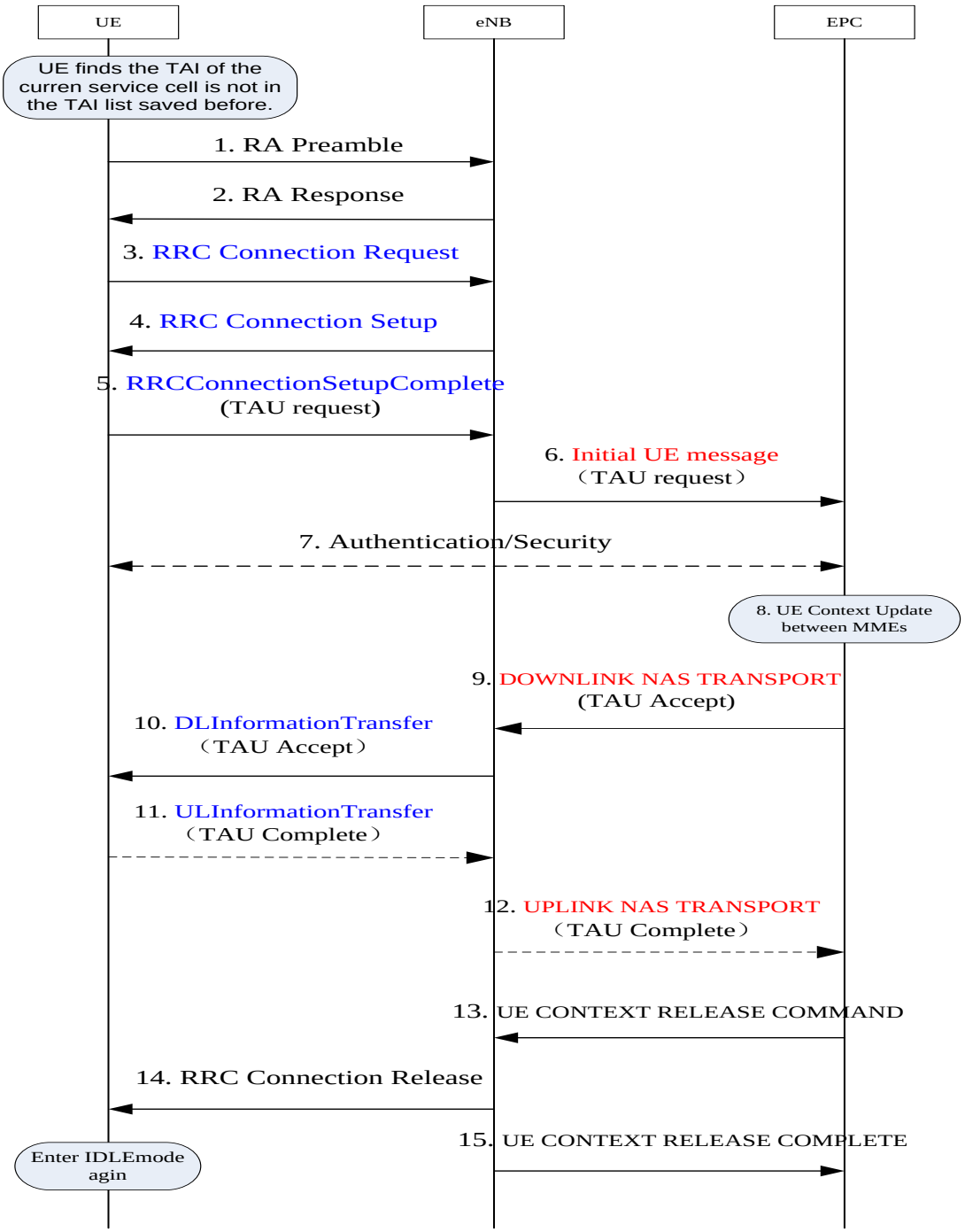


图 17　空闲态不设置“ACTIVE”的 TAU 流程

空闲态不设置“ACTIVE”的 TAU 流程说明

1) 处在 RRC_IDLE 态的 UE 监听广播中的 TAI 不在保存的 TAU List 时，发起随机接入过程，即 MSG1 消息；

2) eNB 检测到 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 eNB 发送 RRCConnectionRequest 消息；

4) eNB 向 UE 发送 RRCConnectionSetup 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，向 eNB 发送 RRCConnectionSetupComplete 消息，包含 NAS 层 TAU request 信息；

6) eNB 选择 MME，向 MME 发送 INITIAL UE MESSAGE 消息，包含 NAS 层 TAU request 消息；

7) MME 向 eNB 发送 Downlink NAS Transport 消息，包含 NAS 层 TAU Accept 消息；

8) eNB 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；

9) 在 TAU 过程中，如果分配了 GUTI，UE 才会向 eNB 发送 ULInformationTransfer，包含 NAS 层 TAU Complete 消息；

10) eNB 向 MME 发送 Uplink NAS Transport 消息，包含 NAS 层 TAU Complete 消息；

11) TAU 过程完成释放链路，MME 向 Enb 发送 UE CONTEXT RELEASE COMMAND 消息指示 eNB 释放 UE 上下文；

12) eNB 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。

2.7.2 空闲态设置“ACTIVE”的 TAU 流程

这种状态恰好为做业务前或承载发生改变时正好有位置更新命令；

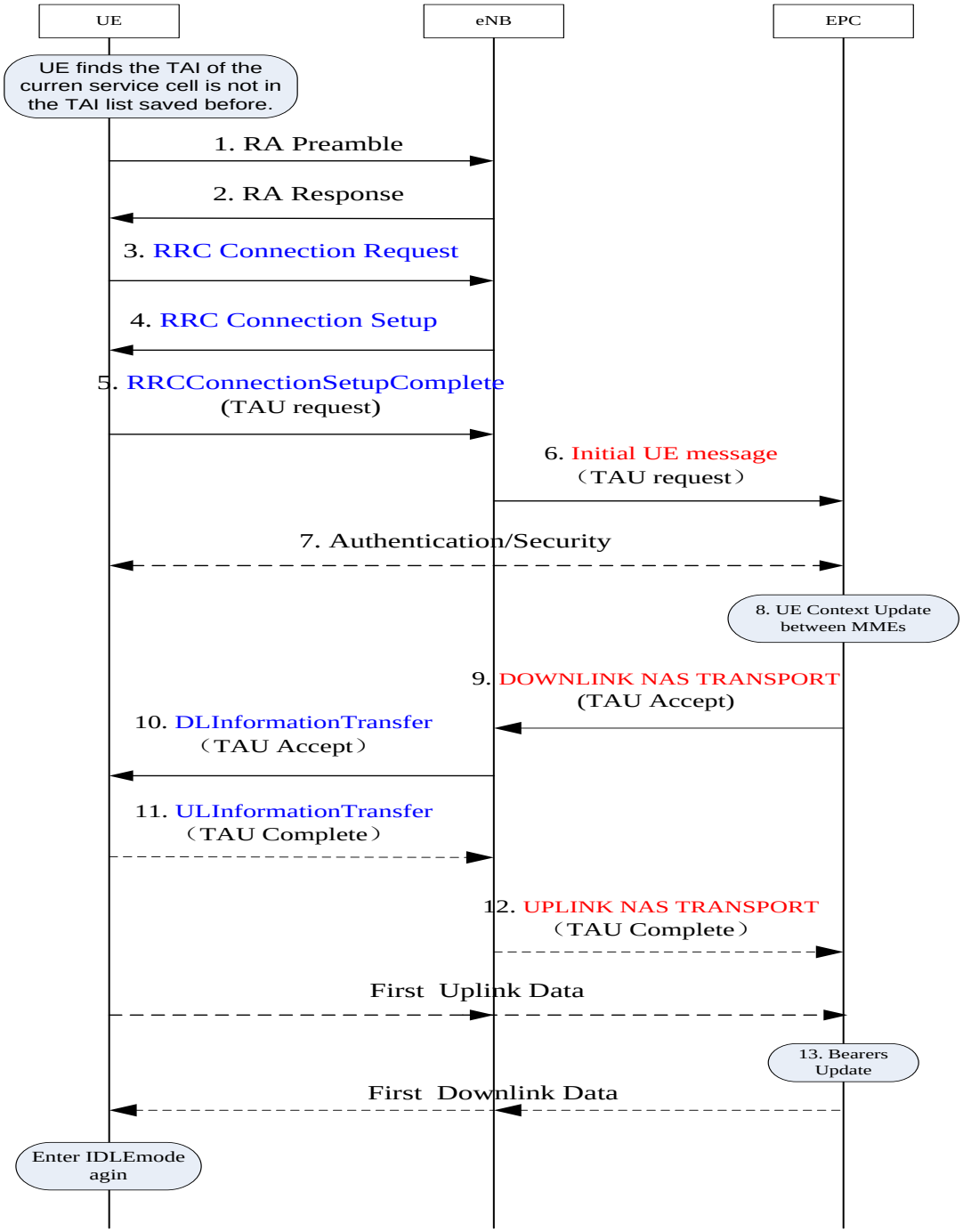


图 18　空闲态设置“ACTIVE”的 TAU 流程

空闲态设置“ACTIVE”的 TAU 流程说明：

1~12）同 IDLE 下发起的不设置"active"标识的正常 TAU 流程相同；

13）　UE 向 EPC 发送上行数据；

14）　EPC 进行下行承载数据发送地址更新。

15）　EPC 向 UE 发送下行数据。

2.7.3 连接态 TAU 流程

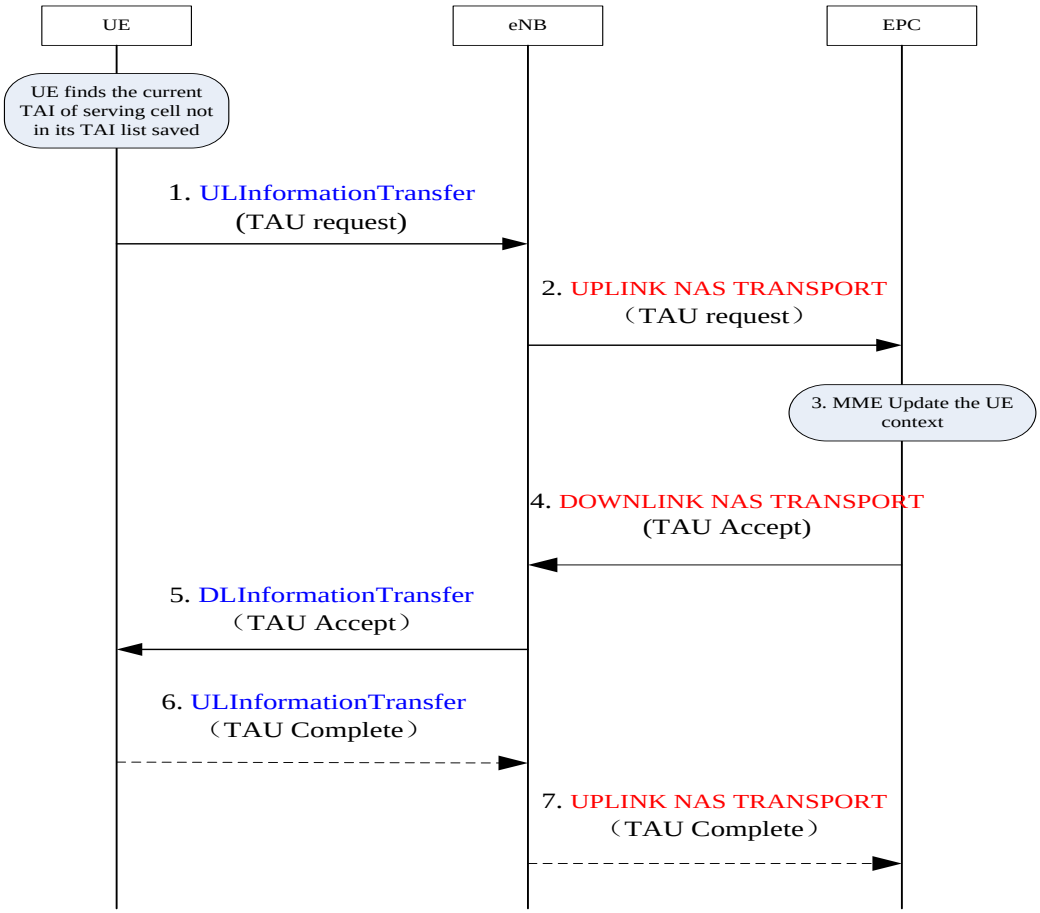


图 19　连接态 TAU 流程

连接态 TAU 流程说明：

1）处在 RRC_CONNECTED 态的 UE 进行 Detach 过程，向 eNB 发送 UL InformationTransfer 消息，包含 NAS 层 Tau request 信息；

2）　eNB 向 MME 发送上行直传 UPLINK NAS TRANSPORT 消息，包含 NAS 层 Tau request 信息；

3）　MME 向基站发送下行直传 DOWNLINK NAS TRANSPORT 消息，包含 NAS 层 Tau accept 消息；

4）　eNB 向 UE 发送 DLInformationTransfer 消息，包含 NAS 层 Tau accept 消息；

5）　UE 向 eNB 发送 ULInformationTransfer 消息，包含 NAS 层 Tau complete 信息；

6）　eNB 向 MME 发送上行直传 UPLINK NAS TRANSPORT 消息，包含 NAS 层 Tau complete 信息。

2.8 专用承载流程

2.8.1 专用承载建立流程

专用承载可以是 GBR 承载也可以是 Non-GBR 承载，专用承载建立流程可以为专用承载分配资源。E-RAB 承载必须在 UE RRC CONNECTED 态下执行 ;UE 和 EPC 均可发起 ,eNB 不可发起；UE 发起时，EPC 仅将其作为参考，有权接受或拒绝。当 EPC 接受时，可回复承载建立、修改流程。

专用承载建立过程：

- PDN-GW 根据 QoS 策略制定该 EPS 承载的 QoS 参数
- S-GW 向 eNB 发送承载建立请求，包含（IMSI, QoS, TFT, TEID, LBI 等）
- MME 向 eNB 发送 E-RAB 建立请求，包含 E-RAB ID,QoS,S-GW TEID
- eNB 接收建立请求消息后，建立数据无线承载
- eNB 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

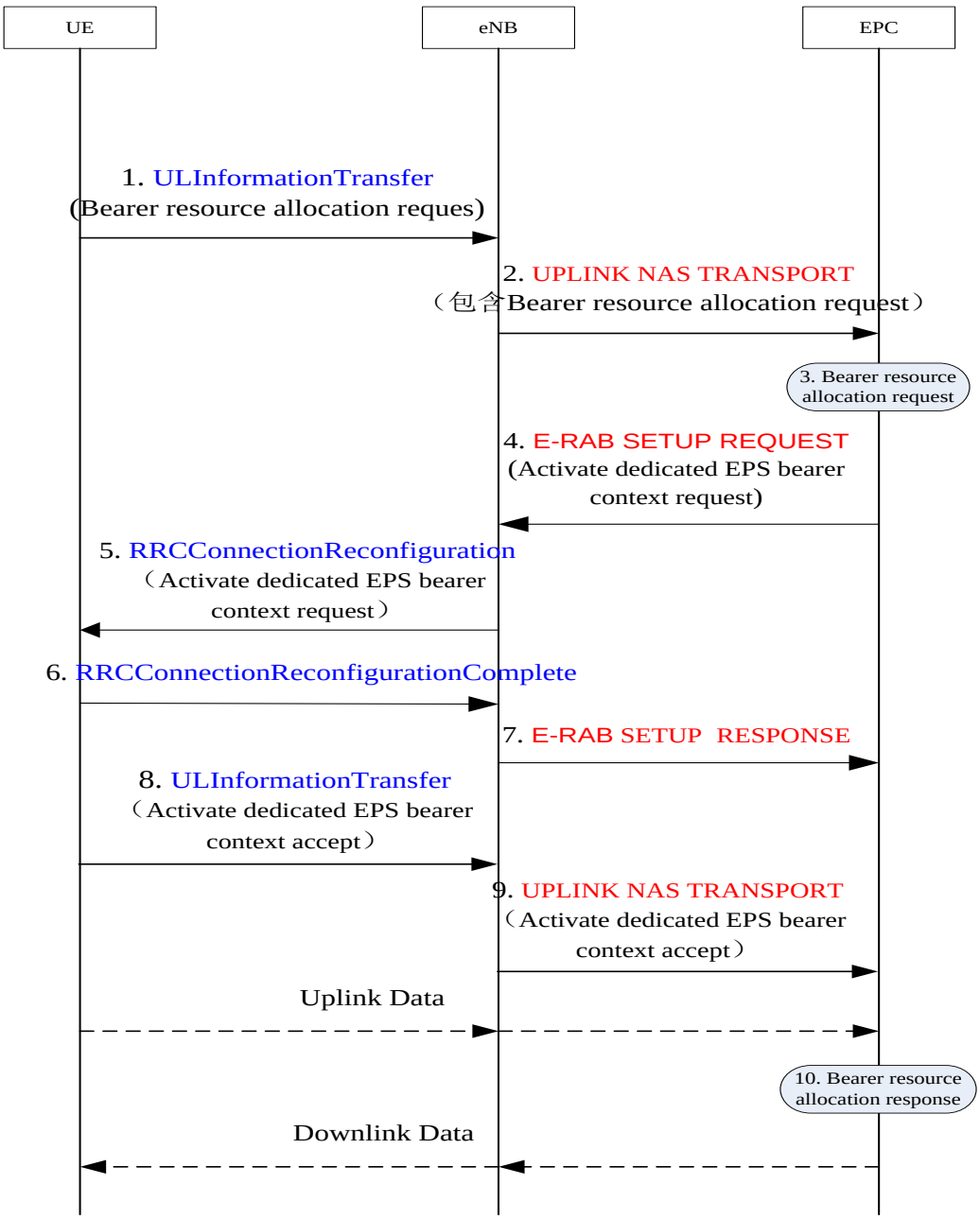


图 20 专用承载建立流程

专用承载建立流程说明：

1）连接状态下的 UE 通过 UL informationTransfer 消息将 Bearer resource allocation Request 消息传递给 eNB。(也可以是发送 Bearer resource modification request 消息)

2）eNB 通过 UPLINK NAS TRANSPORT 消息将 Bearer resource allocation Request（或者是 Bearer resource modification request）发送给 EPC。

3） EPC 通过进行承载资源申请处理。

4）EPC 通过 E-RAB SETUP REQUEST 传递 Activate dedicated EPS bearer context request 消息

告知 eNB。

5）eNB 通过重配消息，将 NAS 消息 Activate dedicated EPS bearer context request 传递给 UE。

6) UE 建立专用承载成功，返回 RRCConnectionReconfigurationComplete 消息，表明承载建立成功。

7）eNB 发送 E-RAB SETUP RESPONSE 消息给 EPC，表明无线承载建立成功。

8）UE 在发送完成重配完成后，通过 ULinformationTransfer 消息将 Activate dedicated EPS bearer context accept 消息告知 eNB。

9）eNB 发送 UL NAS TRANSPORT 消息 Activate dedicated EPS bearer context accept 告知 EPC。

10）此时，上下行数据已经可以进行发送。

11）EPC 通过进行承载资源申请响应。

2.8.2 专用承载修改流程

E-RAB 修改过程由 MME 发起，用于修改已经建立承载的配置。E-RAB 修改也必须在 CONNECTED 态下执行；UE 和 EPC 均可发起，eNB 不可发起；分为修改 Qos 和不修改 Qos 两种类型；UE 发起时，EPC 可回复承载建立、修改、释放流程。

专用承载修改过程：

- P-GW 发起承载修改请求，S-GW 将其发给 MME；
- MME 向 eNB 发送 E-RAB 修改请求消息，修改一个或多个承载，E-RAB 修改列表信息包含每个承载的 QoS；
- eNB 接收到 E-RAB 修改请求消息后，修改数据无线承载；
- eNB 返回 E-RAB 修改响应消息， E-RAB 修改列表信息中包含成功修改的承载信息，E-RAB 修改失败列表消息中包含没有成功修改的承载消息；

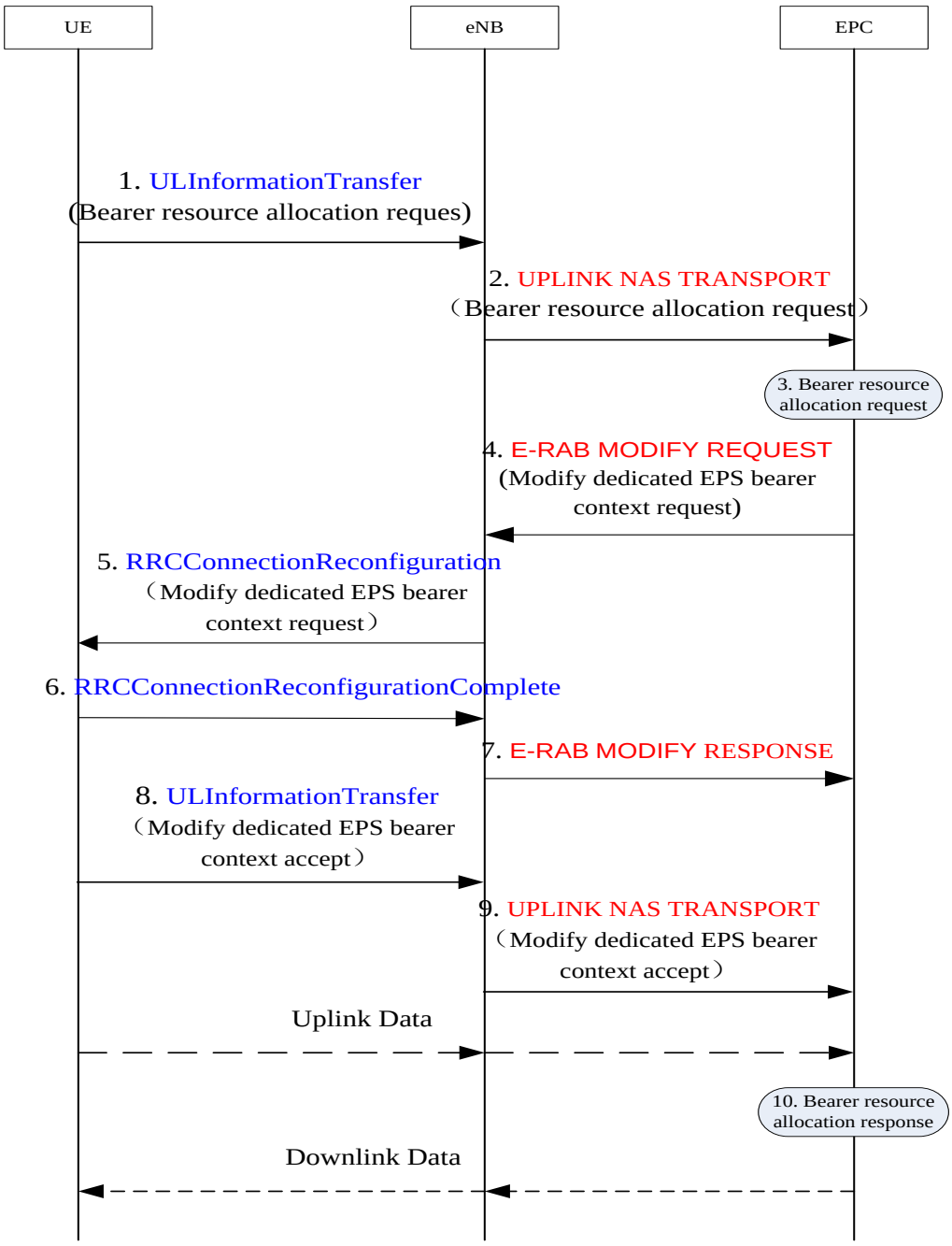


图 21 专用承载修改流程

专用承载修改流程说明：

1) 连接状态下的 UE 通过 ULinformationTransfer 消息将 Bearer resource allocation Request 消息传递给 eNB。(也可以是发送 Bearer resource modification request 消息)

2) eNB 通过 UPLINK NAS TRANSPORT 消息将 Bearer resource allocation Request（或者是 Bearer resource modification request）发送给 EPC。

3) EPC 通过进行承载资源申请处理。

4) EPC 通过 E-RAB MODIFY RESPONSE 传递 Modify dedicated EPS bearer context request 消息告知 eNB。

5) eNB 通过重配消息，将 NAS 消息 Modify dedicated EPS bearer context request 传递给 UE。

6) UE 建立专用承载成功,返回 RRC Connection Reconfiguration Complete 消息,表明承载修改成功。

7) eNB 发送 E-RAB MODIFY RESPONSE 消息给 EPC，表明无线承载修改成功。

8) UE 在发送完成重配完成后，通过 UL information Transfer 消息将 Modify dedicated EPS bearer context accept 消息告知 eNB。

9) eNB 发送 UL NAS TRANSPORT 消息 Modify dedicated EPS bearer context accept 告知 EPC。

10) 此时，上下行数据已经可以进行发送。

11) EPC 通过进行承载资源申请响应。

2.8.3 专用承载释放流程

UE 或 MME 均可发起对 PDN 连接释放的请求 ,此时可以删除该 PDN 下的专用承载(不包括默认承载)。PDN GW 和 MME 均可发起对 E-RAB 的释放流程；对于 PDN GW 发起的承载释放，可释放专用承载或该 PDN 地址下的所有承载；对于 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 P-GW 或 MME 发起的释放过程，由 MME 向 eNB 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；eNB 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。

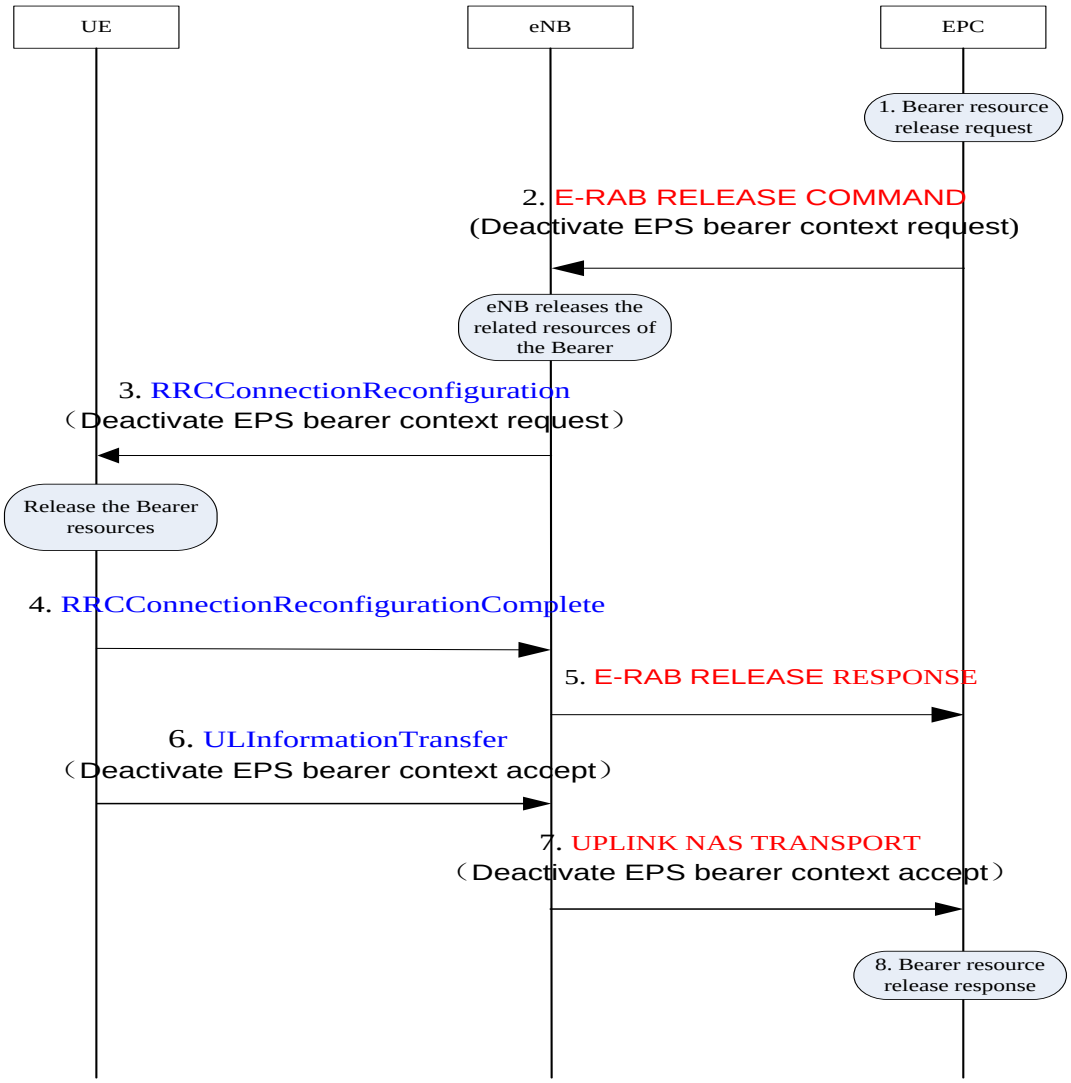


图 22 专用承载释放流程

专用承载释放流程说明

1) EPC 发起承载释放过程。这个过程可能是 UE 申请的，也可能是 EPC 侧启动的。

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

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

4) UE 收到重配消息 RRCConnectionReconfiguration 中的 NAS 消息（Deactivate EPS Bearer Context Request）后释放相关承载资源。

5) UE 发送返回 RRCConnectionReconfigurationComplete 消息，表明无线承载释放成功。

6) eNB 收到 RRCConnectionReconfigurationComplete 消息后，返回 E-RAB Release Response 消息给 EPC。

7) eNB 发送 E-RAB MODIFY RESPONSE 消息给 EPC，表明无线承载建立成功。

8) UE 在发送完成重配完成后，通过 ULinformationTransfer 消息将 NAS 层 Deactivate EPS bearer context accept 消息告知 eNB。

9) eNB 发送 UL NAS TRANSPORT 消息 Deactivate EPS bearer context accept 告知 EPC，告知 EPC 进行 EPS 承载删除完成。

2.9 去附着流程

去附着往往为用户进入覆盖盲区（接入受限）或用户关机，UE 执行的流程，与附着流程是逆过程。

2.9.1 关机去附着流程

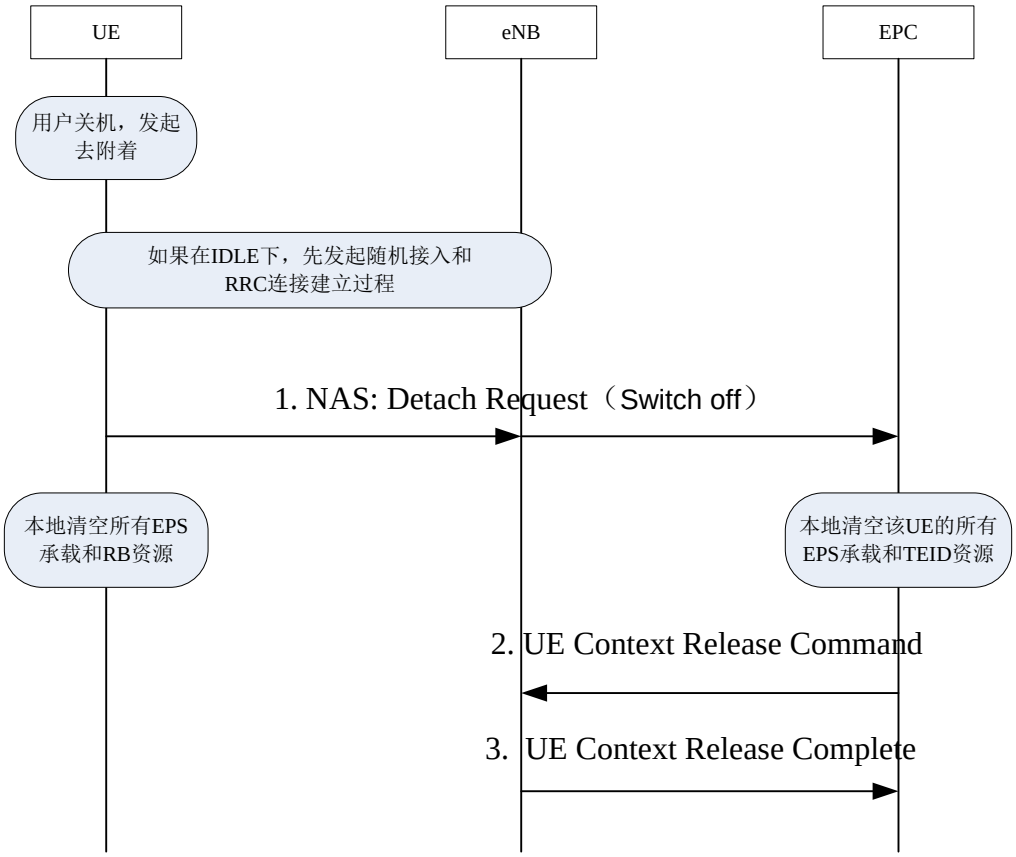


图 23 关机去附着流程

关机去附着流程说明：

UE 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，其流程较为简单

1） 用户关机，发起去附着流程，若在 IDLE 状态下有 RRC 连接建立的过程，UE 向 EPC 发送消息中携带 NAS 消息（类型为关机）。

2） 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 资源,EPC 通知 ENB 释放 UE 文本信息。

3） ENB 释放 UE 文本信息并通知 EPC。

2.9.1 非关机去附着流程

空闲态发起的非关机去附着流程

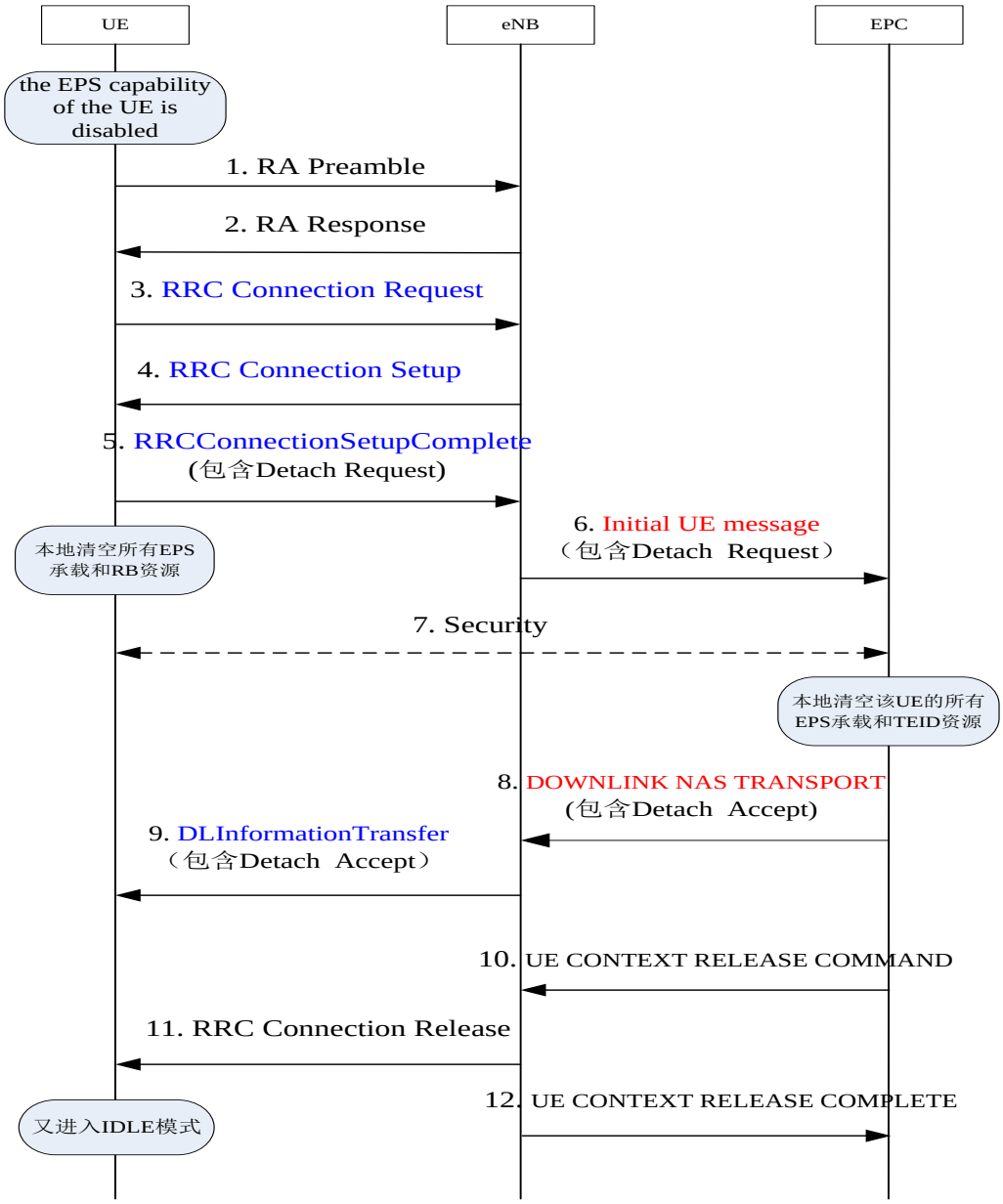


图 24 空闲态非关机去附着流程

空闲态非关机去附着流程说明：

1~5）（UE 的 EPS 能力被禁用）RRC 连接建立过程，建立完成消息中附带去附着请求。

6~9）UE 和 EPC 相互安全验证后，执行清除 EPS 承载和 RB 资源，EPC 向 UE 发送去附着接受消息。

10~12） 网络向终端发起 UE 文本释放和连接释放信息。

连接态发起的非关机去附着流程

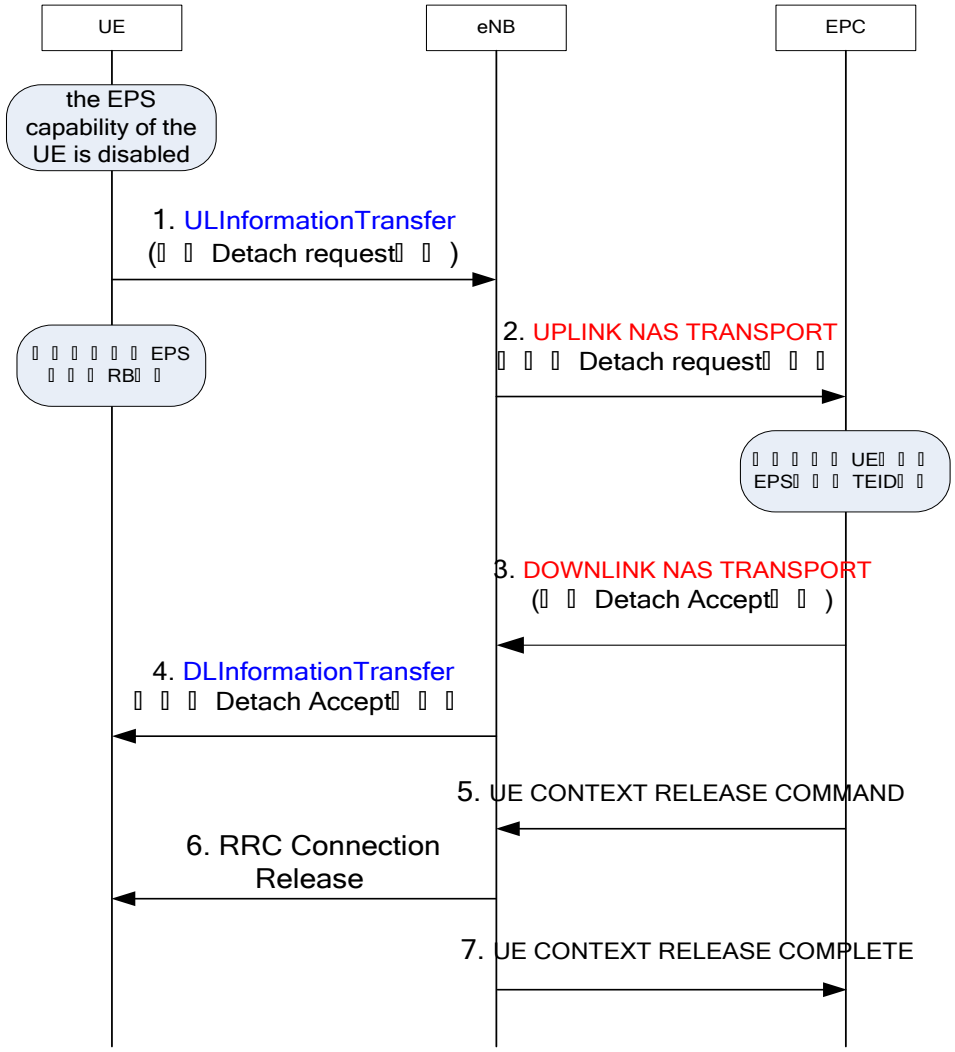


图 25 连接态非关机去附着流程

连接态非关机去附着流程说明：

1~4）（UE 的 EPS 能力被禁用）UE 在上行传输块中携带去附着请求消息，执行清除 EPS 承载和 RB 资源，EPC 向 UE 发送去附着接受消息。

5~7） 网络向终端发起 UE 文本释放和连接释放信息。

2.10 小区搜索、选择和重选

2.10.1 小区搜索流程

小区搜索过程是 UE 和小区取得时间和频率同步，并检测小区 ID 的过程。E-UTRA 系统

的小区搜索过程与 UTRA 系统的主要区别是它能够支持不同的系统带宽（1.4~20MHz）。小区搜索通过若干下行信道实现，包括同步信道（SCH）、广播信道（BCH）和下行参考信号（RS）。SCH 又分成主同步信道（PSCH）和辅同步信道（SSCH），BCH 又分成物理广播信道（PBCH）和动态广播信道（DBCH）。BCH 直接映射到物理信道 PBCH 上，PSCH 和 SSCH 是纯粹的物理信道，不用来传送 L2/L3 控制信令，而只用于同步和小区搜索过程；DBCH 最终承载在下行共享传输信道（DL-SCH），没有独立的信道。

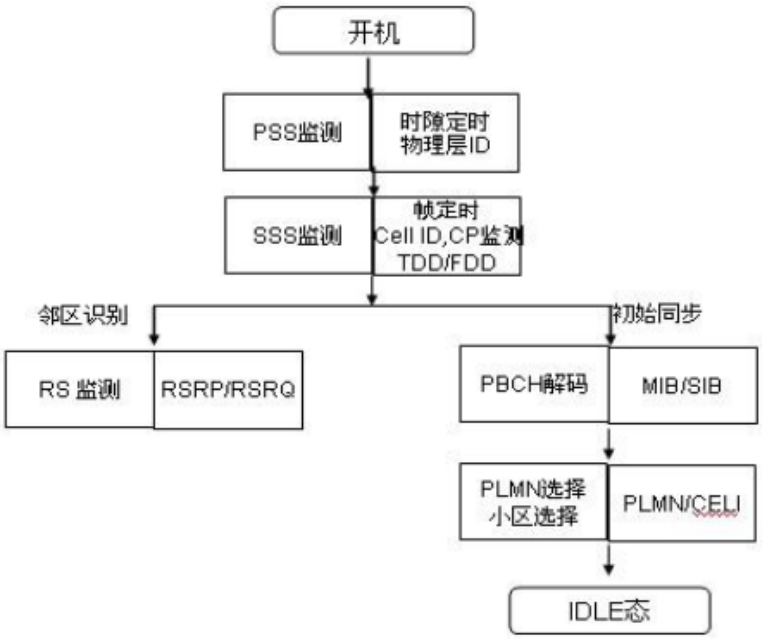


图 26 小区搜索流程图

2.10.1 小区选择流程

小区选择的类型（S 准则）

- 不同场景（初始小区选择；存储信息的小区选择）
- 不同时机（UE 开机；从连接态返回到空闲态模式；重新进入服务区）

S 算法

1、小区选择 S 值，大于 0

2、小区选择 S 值=测量小区的 RSRP 值-（小区中 RSRP 最低接收电平+当驻留在 VPLMN 上搜索高优先级小区防止乒乓响应设置的偏移值）-max（（小区允许 UE 的最大上行发射功率-UE 能力支撑的最大上行发射功率），0）

公式简化为：

当 UE 最大允许发射功率大于 UE 能力支持最大发射功率时，S=测量小区电平值-（最低接收电平+最低接收电平偏置）-（（UE

最大允许发射功率-UE 能力支持最大发射功率）

当 UE 最大允许发射功率小于等于 UE 能力支持最大发射功率时，S=测量小区电平值-（最低接收电平+最低接收电平偏置）

UE 最大允许发射功率：本小区允许 UE 的最大发射功率 UePowerMax，应用于小区选择准则（S 准则）的判决，用于计算功率补偿值。如果该参数不配置，则 UE 的最大发射功率由 UE 自己的能力决定。该值在 LST CELL 命令中。该参数设置的越大，UE 的发射功率也越大，增强本小区覆盖的同时会增加对邻区的干扰；该参数设置的越小，UE 的发射功率也越小，减少本小区覆盖的同时会减少对邻区的干扰。

小区中 RSRP 最低接收电平：在 LST CELLSEL 中，增加某小区的该值，使得该小区更难符合 S 规则，更难成为适当小区，UE 选择该小区的难度增加，反之亦然。该参数的取值应使得被选定的小区能够提供基础类业务的信号质量要求。

最低接收电平偏置：在 LST CELLSEL 中，该参数表示小区最低接收电平偏置，应用于小区选择准则（S 准则）公式，仅当 UE 驻留在 VPLMN 且由于周期性的搜索高优先级 PLMN 而触发的小区选择时，才使用本参数（防止乒乓效应）。增加某小区的该值，使得该小区更容易符合 S 规则，更容易成为适当小区，选择该小区的难度减小，反之亦然。

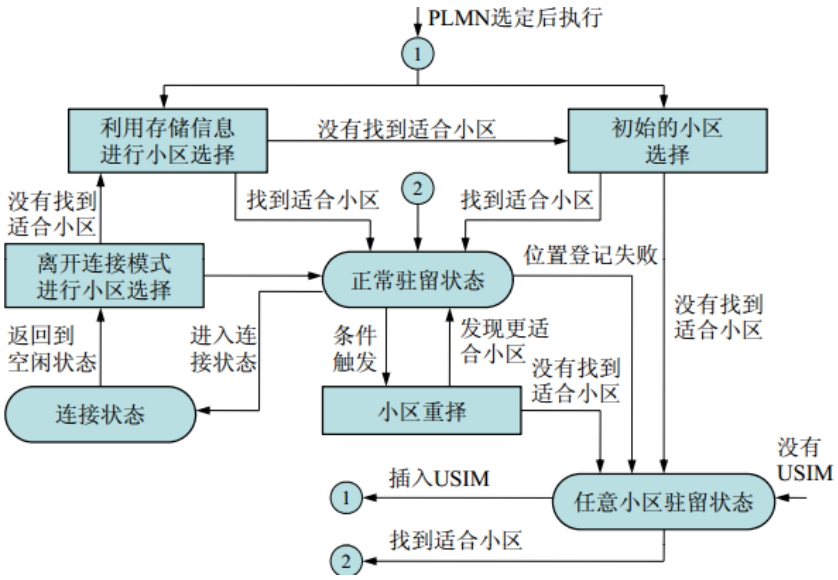


图 27 小区选择流程图

2.10.3 小区重选流程

小区重选（cell reselection）指 UE 在空闲模式下通过监测邻区和当前小区的信号质量以选择一个最好的小区提供服务信号的过程。当邻区的信号质量及电平满足 S 准则且满足一定重选判决准则时，终端将接入该小区驻留。UE 驻留到合适的 LTE 小区停留 1s 后，就可以进行小区重选的过程。小区重选过程包括测量和重选两部分过程，终端根据网络配置的相关参数，在满足条件时发起相应的流程。重选测量启动准则：UE 成功驻留后，将持续进行本小区测量。RRC 层根据 RSRP 测量结果计算 Srxlev，并将其与 Sintrasearch 和

Snonintrasearch 比较，作为是否启动邻区测量的判决条件。

- 对于重选优先级高于服务小区的载频，UE 始终对其测量
- 对于重选优先级等于或者低于服务小区的载频

同频/同优先级重选流程

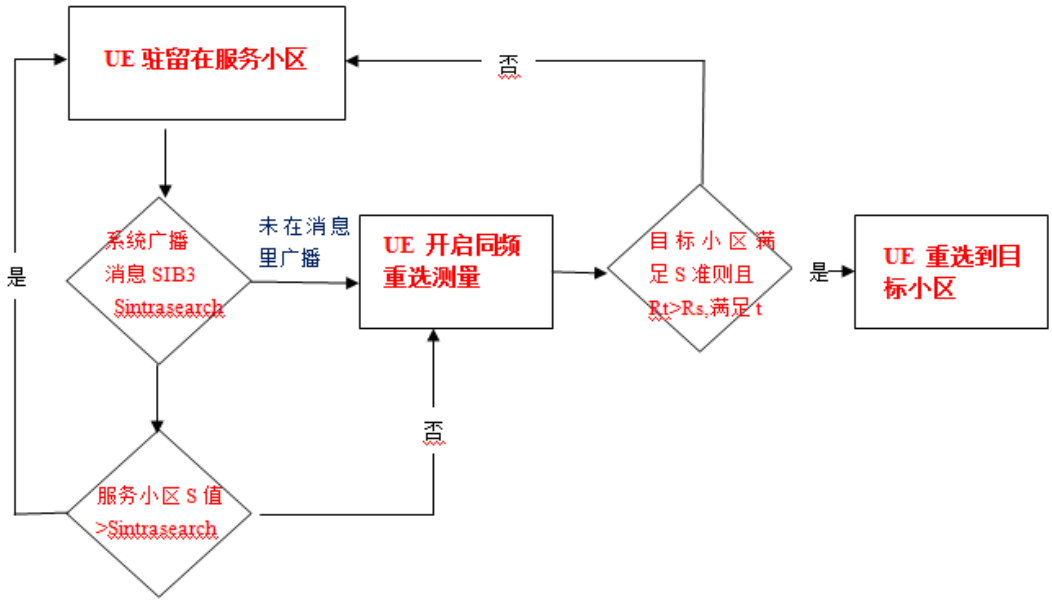


图 28 同频/同优先级重选流程

为了最大化 UE 电池寿命，UE 不需要在所有时刻都进行频繁的邻小区监测（测量），除非服务小区质量下降为低于规定的门限值。具体来说，仅当服务小区的参数 S(S 值的计算方法与小区选择时一致)大于系统广播参数 S-intrasearch 时 UE 才启动同频测量。

小区排序使用 R 准则：对于同频的小区，或者异频但具有同等优先级的小区，UE 采用 R 准则对小区进行重选排序。所谓 R 准则，是指对于服务小区的 Rs 和目标小区的 Rt 分别满足：

服务小区:Rs = Qmeas,s +Qhyst

目标小区:Rt = Qmeas,t - Qoffset

其中 Qmeas 是测量小区的 RSRP 值，Qhyst 表示小区重选迟滞值。同频小区和同优先级小区重选迟滞，用于调整重选难易程度，减少乒乓效应；其它参数一定的情况下，增加迟滞，即增加同频小区或异频同优先级重选的难度，反之亦然。

Qmeas,t 是目标小区的 RSRP 值；Qoffset 定义了目标小区的偏移值，（目标候选小区与当前驻留小区间的偏置量）对于具有同等优先级的异频小区来说，包括基于小区的偏移值和基于频率的偏移值两个部分。其它参数一定的情况下，增加偏置量，即增加同频或异频同优先级小区重选的难度，反之亦然。

如果目标小区在 Treselection 时间内（同频和异频的 Treselection 可能不同），Rt 持续超过 Rs

那么 UE 就会重选到目标小区。

与小区重选有关的参数来源于服务小区的系统消息 SIB3，SIB4 和 SIB5。

Sintrasearch 用于进行同频小区重选时，判断是否进行同频小区重选的门限参数。当 LTE 服务小区的 S 值小于等于 Sintrasearch 时，就要执行同频小区重选测量；另外如果此 Sintrasearch 参数没有在系统消息内广播，也要执行同频小区重选测量。除此之外，UE 可以选择不进行测量。

SIB4 中包含了同频小区重选有关的小区相关信息： 在 intraFreqNeighborCellInfo 中定义了用于同频重选的小区物理 ID 列表

以及对应的偏移量值。偏移量值用于进行小区重选排序 R 准则（下面将会介绍）的公式计算，目的是为了减少重选振荡。在 SIB4 中也定义了不能用于同频重选的小区黑名单列表。

同频小区重选的对象可以是邻小区列表中的小区也可以是通过重选过程检测到到的小区。排队和选择的过程需要满足以下几个约束条件：

1、新目标小区的信道质量在排序中要比当前服务小区的质量好，且持续时间不短于 T(重选时间)

2、如果 UE 处于非普通移动状态（如中速或高速移动状态），则需要考虑对重选参数 t 和 Qhyst 进行缩放。

3、UE 驻留在原小区的时间超过 1s。

异频/异系统/不同优先级重选流程

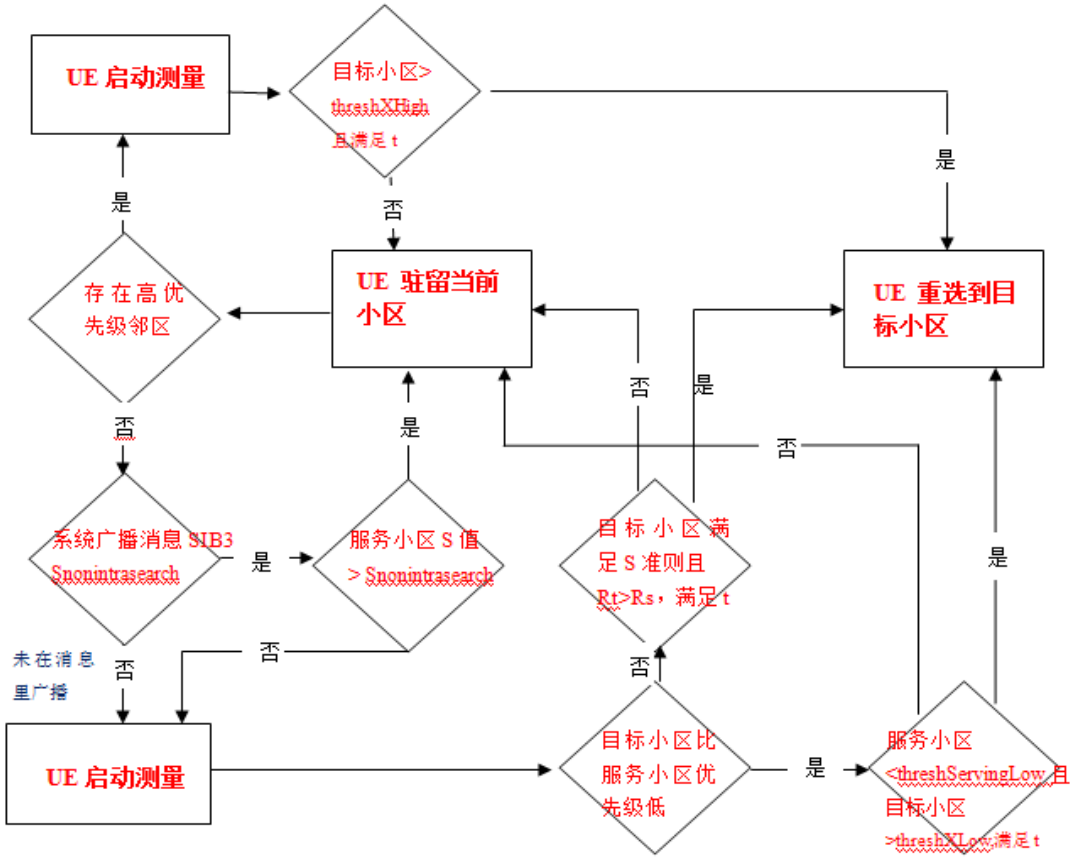


图 29 同频/同优先级重选流程

---

cellReselectionPriority 定义了服务频率在异频小区重选的优先级，在 0 到 7 之间取值，其中 0 代表优先级最低。异频的小区切换基于优先级值的大小， UE 通常总是会尝试驻留在优先级高的小区。相邻小区的优先级在 SIB5 中广播。除此之外， LTE 还可以通过 RRC 层的信令，定义针对每个 UE 特定的小区频率优先级。

Snonintrasearch 用于进行/异频小区重选时，判断是否进行异频小区重选测量的门限参数。在异频重选的情况下，如果相邻小区的优先级高于服务小区，UE 需要进行异频小区重选测量。另外，如果此 Snonintrasearch 参数没有在系统消息内广播，UE 也需要进行异频小区的重选测量。否则，UE 可以选择，只有当服务小区的 S 值小于等于 Snonintrasearch 时，才进行异频小区的重选测量；

threshServingLow 定义了 UE 在重选优先级较低的小区时，服务小区的测量门限，在此情况下，目标小区也必须满足一定的测量门限

SIB5 中包含了异频小区重选有关的小区信息， 包括异频小区列表， 频率等

其中， priority 定义了异频小区的重选优先级，在进行小区重选时，UE 可以只考虑定义了优先级的频率小区。不同接入技术的小区（inter－RAT）之间，其优先级是不相等的。UE 基于小区频率的优先级，进行小区重选。如果目标小区的优先级比当前服务小区的优先级高，并且目标小区的 S 值在时间 ReselectionTimer 内持续超过门限参数 threshXHigh， 那么不管当前小区的 S 值是多少， UE 都会重选到目标小区。否则，如果目标小区的优先级比当前服务小区的低，那么只有服务小区的 S 值小于 threshServingLow （在 SIB3 中定义），并且目标小区的 S 值大于门限参数 threshXLow，而且持续的时间超过 Reselection Timer 后， UE 才会重选到目标小区。

测量准则：

对于系统消息指出的优先级高于当期频率优先级的小区，UE 总是执行对这些高优先级小区的测量；对于系统消息指出优先级低于当期优先级的小区，UE 测量的准则如下：1、如果服务小区的 S 值（与小区选择的 S 值相同）大于门限值 s-NonIntraSearch，不执行测量；2、若服务小区的 S 值（与小区选择的 S 值相同）低于或等于 s-NonIntraSearch，执行测量；3、若 s-NonIntraSearch 参数没有在系统消息内广播，UE 开启异频小区测量。

优先级处理：

UE 可通过广播消息获取频点的优先级信息（公共优先级），或者通过 RRC 连接释放消息获取。若消息中提供专用优先级，则 UE 将忽略所有的公共优先级。若系统消息中没有提供 UE 当前驻留小区的优先级信息，UE 将把该小区所在的频点优先级设置为最低。UE 只在系统消息中出现的并提供优先级的频点之间，按照优先级策略进行小区重选。

小区重选准则：

对于高优先级频点的小区重选，并满足以下条件后进行

1、高优先级频率小区的 S 值大于预设的门限，且持续时间超过重选时间参数 T；2、UE 驻留原小区时间超过 1s。

如果最高优先级上多个邻小区符合条件，则选择最高优先级频率上的最优小区。对于同等优先级频点（或同频），采用同频小区重选的 R 准备。对于低优先级频率的小区重选，则满足以下条件后进行。

1、没有高优先级频率的小区符合重选要求条件。

2、没有同等优先级频率的小区符合重选要求条件。

3、服务小区的 S 值小于预设的门限，并且低优先级频率小区的 S 值大于预设的门限，且持续时间超过重选时间参数值。

4、UE 驻留原小区的时间超过 1s。

第三章异常信令流程

上一章主要讲了正常流程，通过对正常流程的学习有助于我们在实际优化工作中发现流程的异常和不完整性，从而判断出网络问题的症结所在。下面对几个异常流程进行举例，强化大家理论联系实际的能力。实际在处理问题中，信令流程分析一项非常复杂的工作，需要大家对知识的掌握达到相当高的水平才能有所斩获。

3.1 附着异常流程

3.1.1 RRC 连接失败

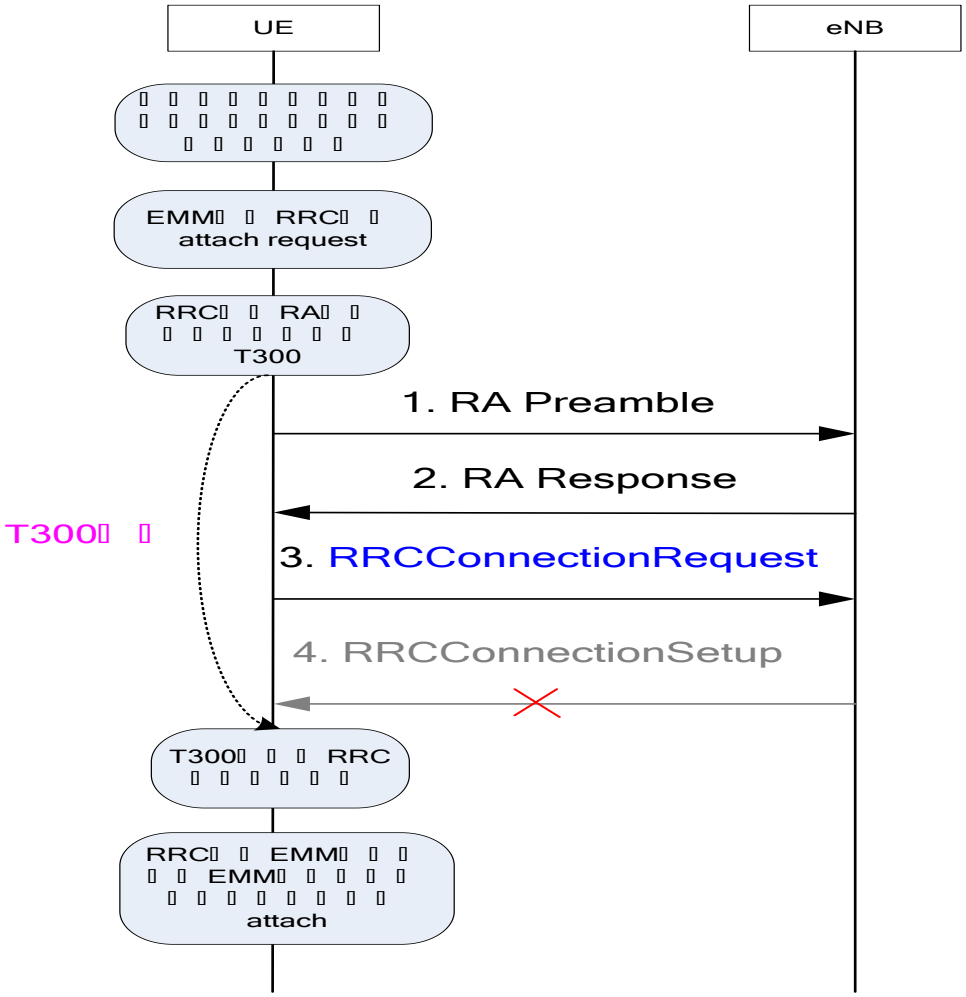


图 30 RRC 连接失败异常流程

3.1.2 核心网拒绝

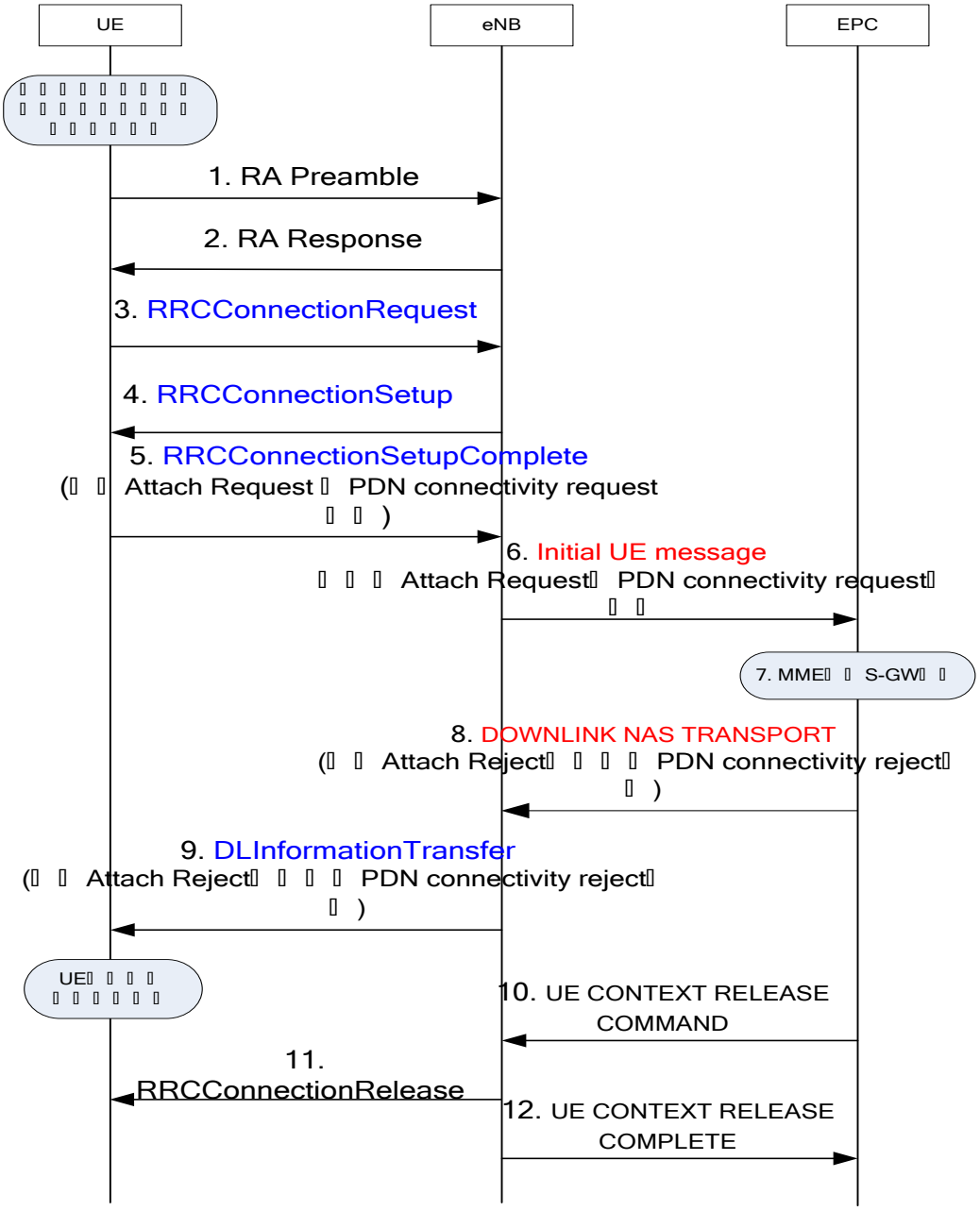


图 31 核心网拒绝异常流程

1）如果是 ESM 过程导致的拒绝（比如默认承载建立失败），才会带 PDN CONNECTIVITY REJECT 消息，EMM 层拒绝，只有 ATTACH REJECT 消息。

2）常见的拒绝原因有：IMSI 中的 MNC 与核心网配置的不一致。

3.1.3 eNB 未等到 Initial context setup request 消息

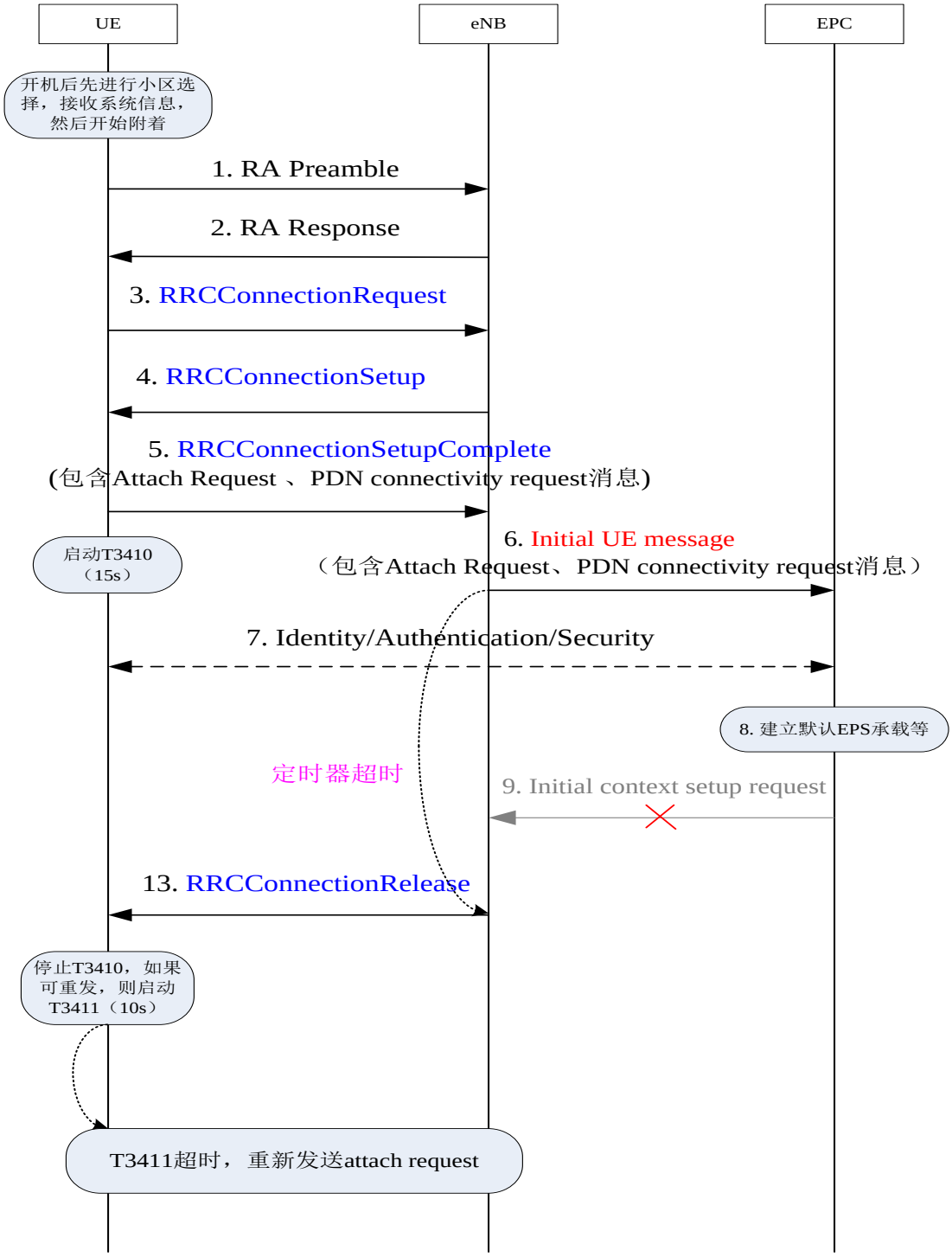


图 32 eNB 未等到 Initial context setup request 消息异常流程

3.1.4 RRC 重配消息丢失或 eNB 内部配置 UE 的安全参数失败

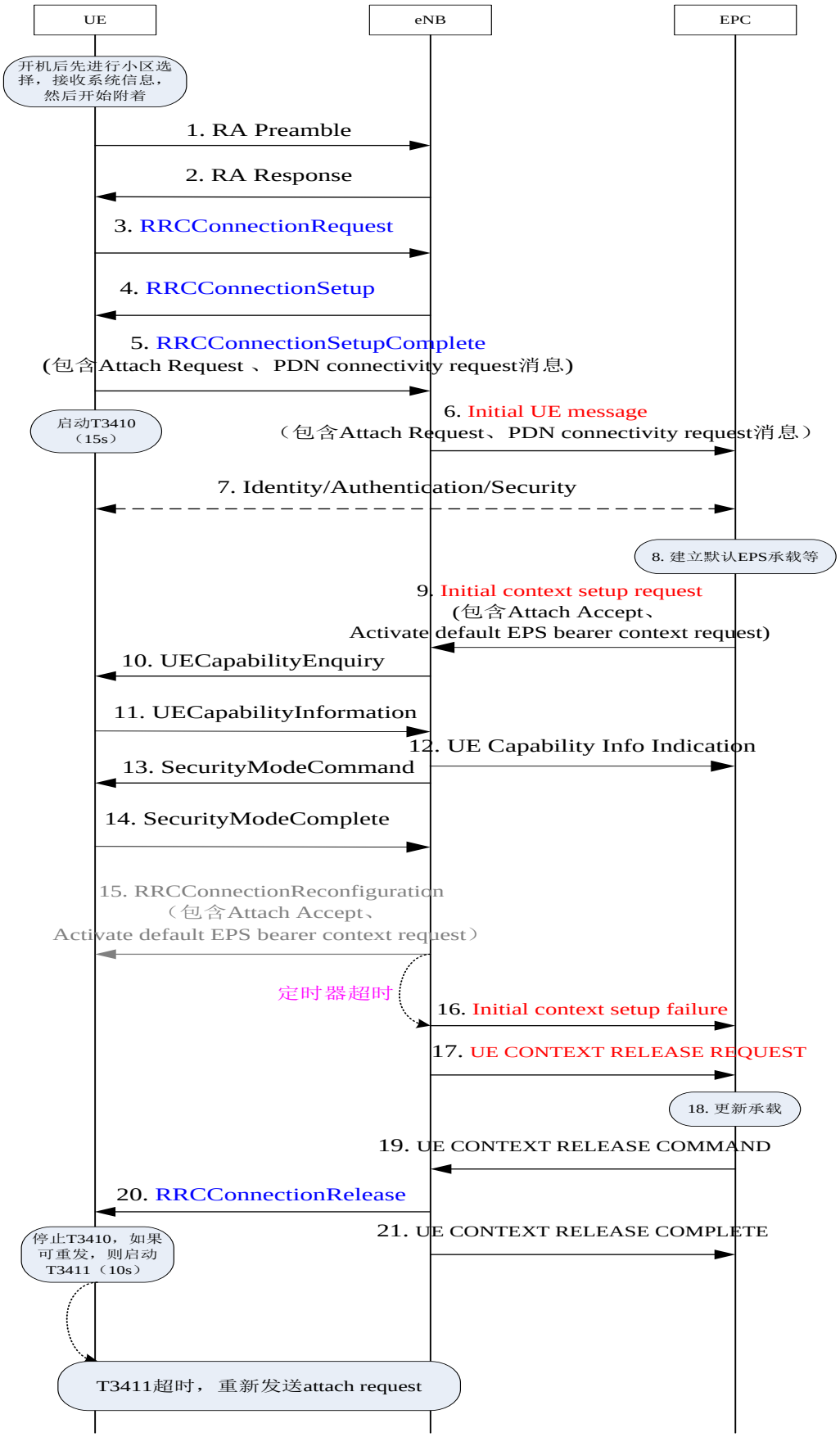


图 33 RRC 重配消息丢失或 eNB 内部配置 UE 的安全参数失败异常流程

3.2 ServiceRequest 异常流程

3.2.1 核心网拒绝

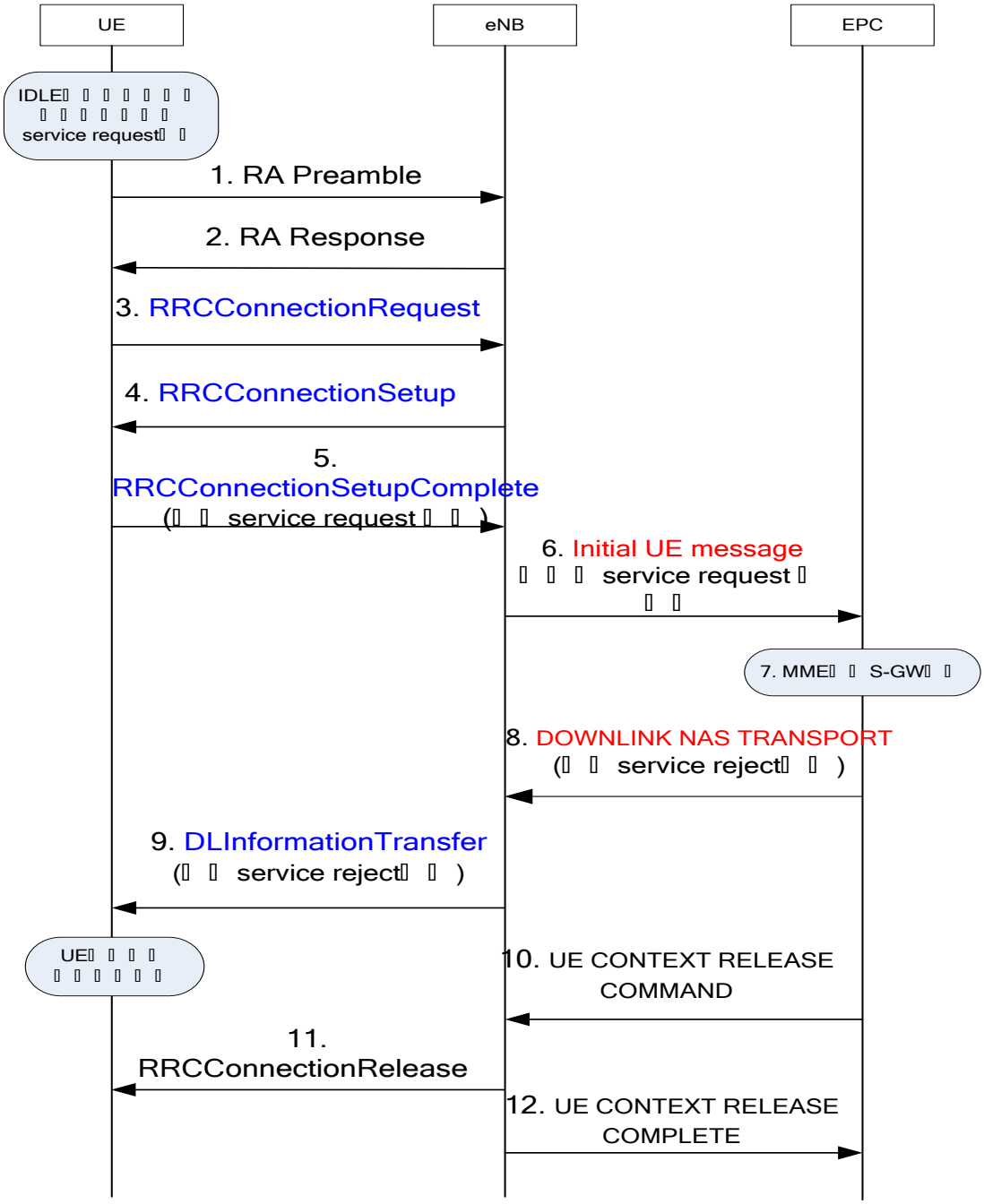


图 34 核心网拒绝异常流程

3.2.2 eNB 建立承载失败

当 attach 成功，建立一个专用承载后，如果 RRC 连接释放进入了 IDLE，下次 UE 发起数据时会发起 service request ,该过程会为默认承载和专用承载建立对应的 DRB 等参数。如果 eNB 建立专用承载失败，则回复给核心网 Initial context setup response，带失败列表，告知核心网专用承载建立失败，核心网会本地去激活该专用承载；同时 RRCConnectionReconfiguration 消息也不会带该专用承载的 DRB，UE 收到后发现该专用承载对应的 DRB 没有建立起来，也会本地去激活该承载，这样 UE 和核心网承载保持一致。另一种情况，当建立的这个专用承载也为非 GBR 承载时，eNB 可能会成功建立该专用承载，而失败建立默认非 GBR 承载，这样回复给核心网 Initial context setup response，带失败列表，核心网发现默认承载建立失败时，会本地 detach 该 UE；同时 RRCConnectionReconfiguration 消息也不会带该默认承载的 DRB，UE 收到后发现默认承载对应的 DRB 没有建立起来，也会本地去激活该默认承载，以及关联的专用承载，从而本地 detach（只有一个默认承载时），这样 UE 和核心网承载保持一致。

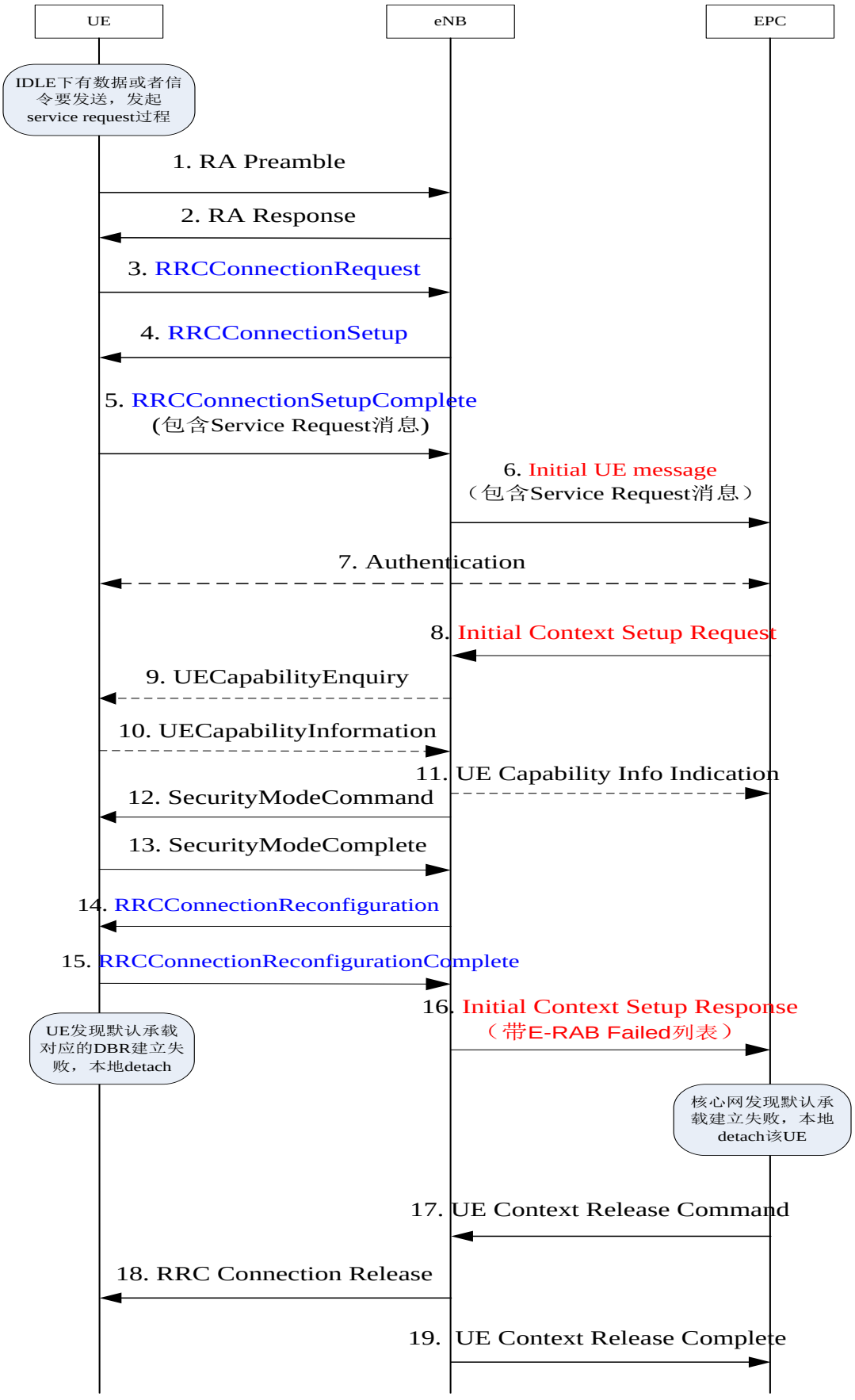


图 35eNB 建立承载失败异常流程

3.3 承载异常流程

3.3.1 核心网拒绝

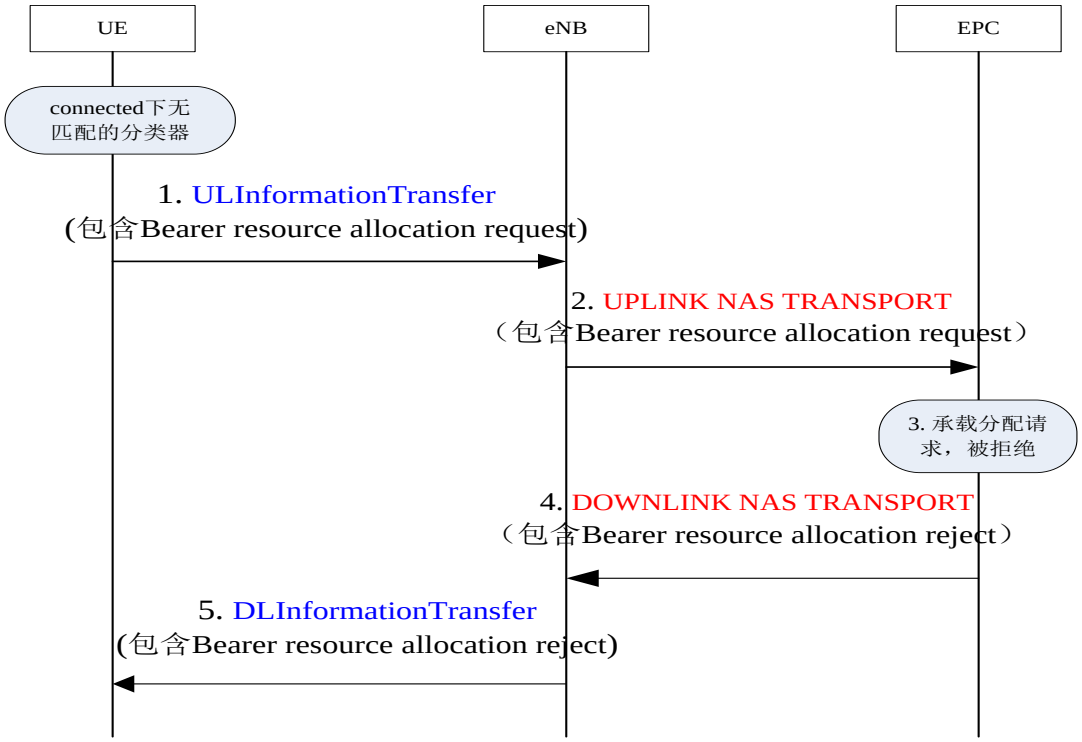


图 36 核心网拒绝异常流程

如果拒绝原因值是"unknown EPS bearer context"，UE 会本地去激活存在的默认承载或专用承载。

3.3.2 eNB 本地建立失败（核心网主动发起的建立）

如果 eNB 建立失败，会回复 E-RAB SETUP RESPONSE，带失败建立的承载列表，并带原因值，核心网应该根据原因值处理（目前 eNB 的实现是： 如果 eNB 本地建立失败，即还没有给 UE 发送 RRC 重配消息，这时 eNB 会发送 NAS NON DELIVERY INDICATION

给 MME)。但目前核心网没有查看原因值 ,都给 UE 下发了 Deactivate EPS bearer context request 消息(与协议不符) , UE 查找不到该承载 , 也回复 Deactivate EPS bearer context accept。

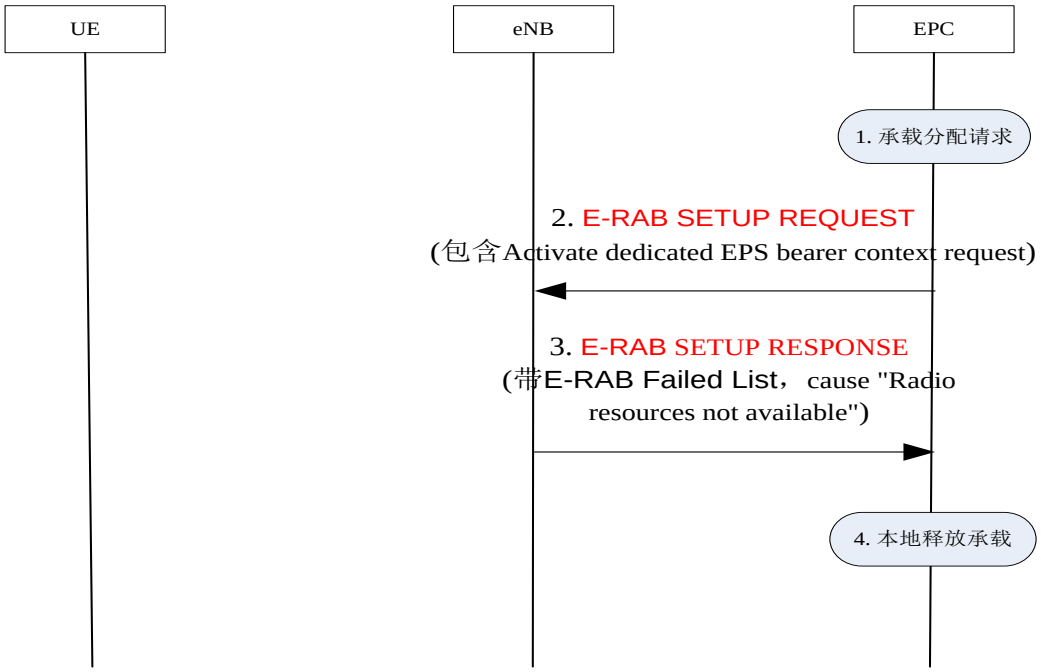


图 37 本地建立失败异常流程

3.3.3 eNB 未等到 RRC 重配完成消息，回复失败

eNB 回复失败区分为 : eNB 本地失败 , 没有给 UE 发送 RRC 重配消息 ; eNB 未收到 RRC 重配完成消息，回复失败。

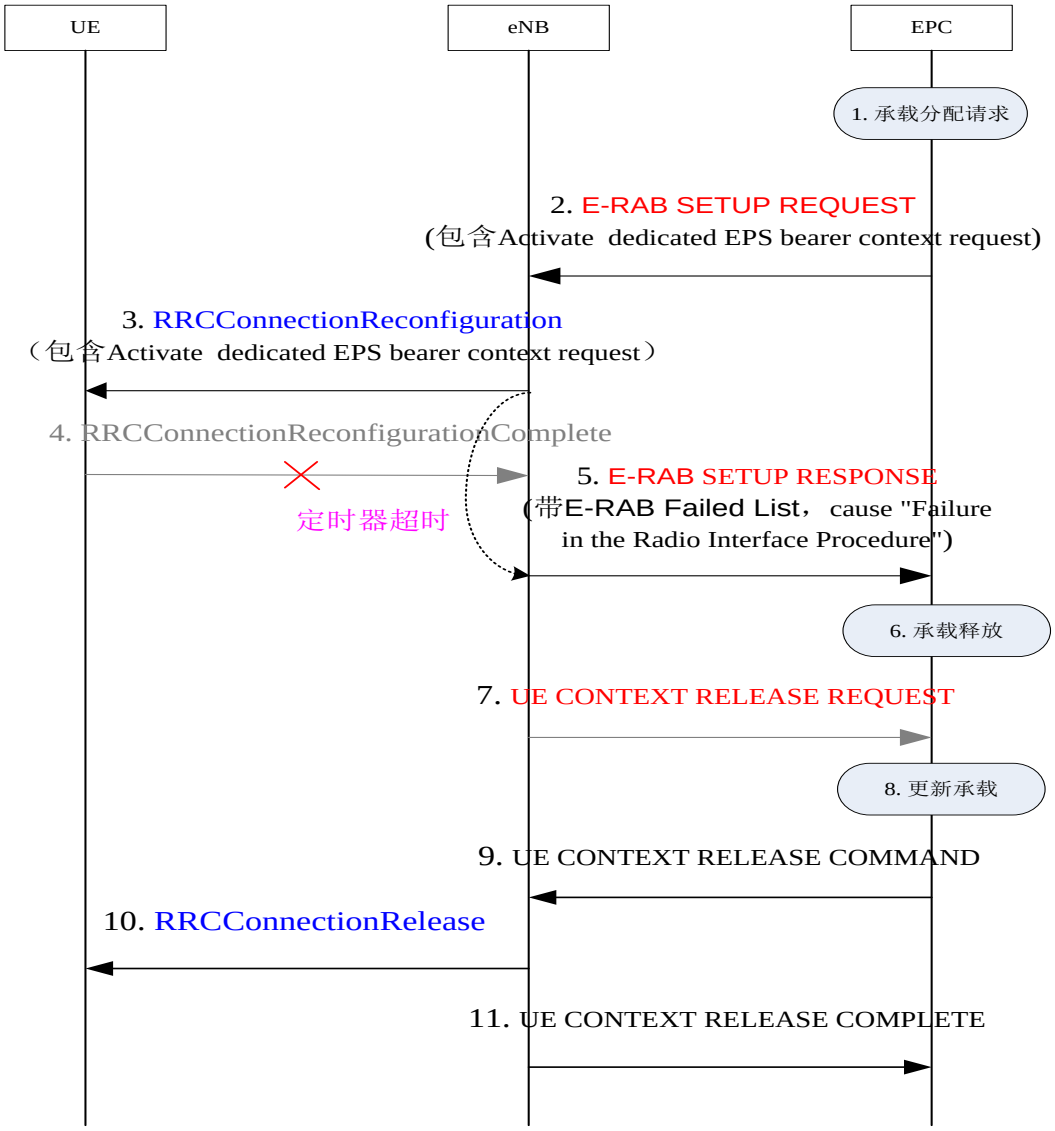


图 38 eNB 未等到 RRC 重配完成消息，回复失败异常流程

3.3.4 UE NAS 层拒绝

如果是 UE 的 NAS 层拒绝，则核心网收到后会给 eNB 发送 E-RAB 释放消息，来释放刚刚建立的 S1 承载，此时不带 NAS PDU。eNB 收到消息后，发 RRC 重配给 UE 来释放刚建立的 DRB 参数。

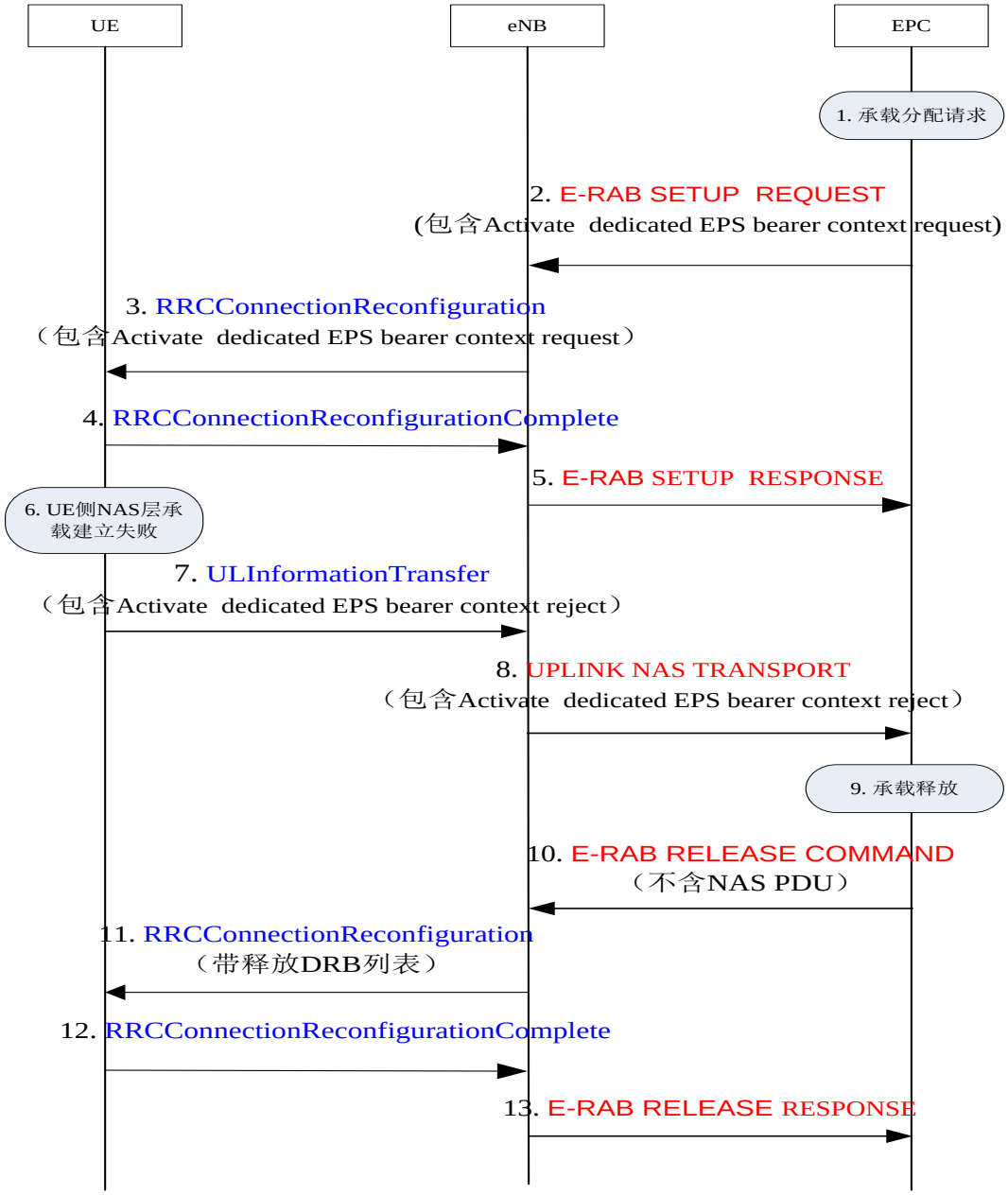


图 39 UE NAS 层拒绝异常流程

3.3.5 上行直传 NAS 消息丢失

若核心网没有收到 UE 回复的 NAS 消息，会重发请求消息，重发 4 次后，如果还没收到应答则放弃。

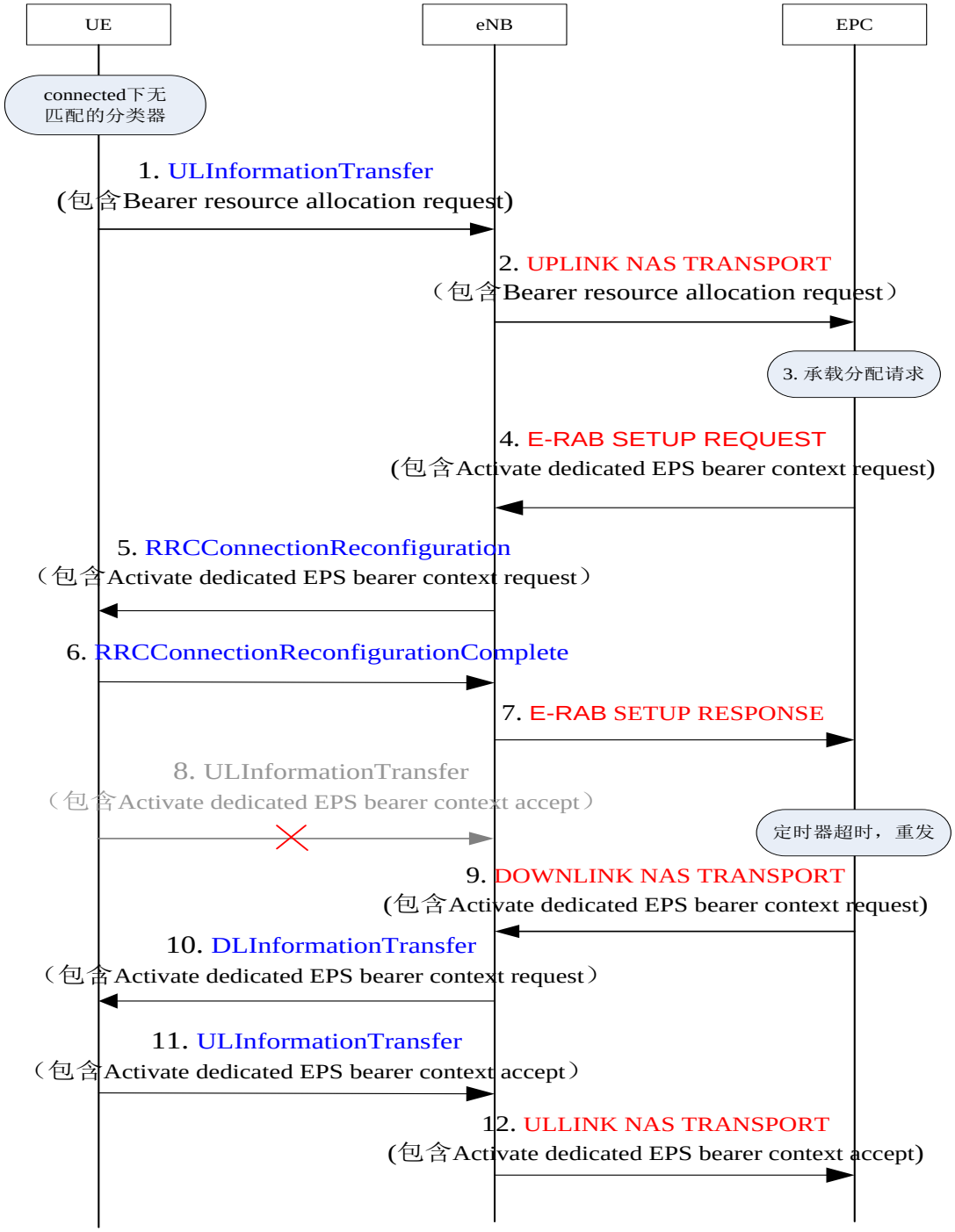


图 40 上行直传 NAS 消息丢失

第四章系统消息解析

本章讲解系统消息和层 3 信令部分，学习完本章后，要了解每个系统消息的作用、会查询消息内容里重要信息；要了解信元内容的主要部分，查询信元内的重要信息为定位问题提

供帮助。

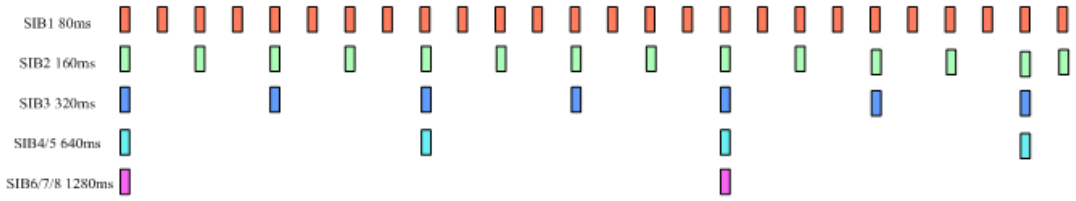
在涉及到具体信息里的信元时，每个厂家对 3GPP 规范有不同的执行方式，这需要大家去了解、去熟悉，比如对于系统消息 MIB 中关于系统带宽，华为设备的定义为 dL-Bandwidth：n100（5），中兴设备的定义为 dL-Bandwidth=5（n100），可谓是形式不同，内容一致。大家不必细究，明白一种方式就行。

4.1 系统消息

LTE 系统内分为 MIB 和 SIB 系列消息，对于 UE 当新接入一个小区或广播消息发生改变时，都会接收系统消息（MIB\SIB），以帮助更新或纠正 UE 当前的状态，完成相应的通信业务和物理过程。在系统路测中可以观察的系统消息有种：MIB、SIB1 和 SI，其作用分别如下，其中 SI 消息里包含了 SIB2~SIB13。

- MIB:用于系统接入。MIB 上传输几个比较重要的系统信息参数，如小区下行带宽、PHICH 配置参数、无线系统帧号 SFN（包含 SIB1 消息的位置），在 PBCH 上发送，表现为“RRC_MASTER_INFO_BLOCK”。
- SIB1:广播小区接入与小区选择的相关参数以及 SI 消息的调度信息（包含了一个或多个 SIB2~13 消息），在 PDSCH 上发送，表现为“RRC_SIB_TYPE1”。
- SI:SI 消息中承载的是 SIB2~SIB13，在 PDSCH 上发送，表现为“RRC_SYS_INFO”。
  - SIB2:小区内所有 UE 共用的无线参数配置，其它无线参数基本配置。
  - SIB3:小区重选信息，主要关于服务小区重选参数以及同频小区重选参数。
  - SIB4:同频邻区列表以及每个邻区的重选参数、同频白/黑名单小区列表。
  - SIB5:异频相邻频点列表以及每个频点的重选参数、异频相邻小区列表以及每个邻区的重选参数、异频黑名单小区列表。
  - SIB6:UTRA FDD 邻频频点列表以及每个频点的重选参数、UTRA TDD 邻频频点列表以及每个频点的重选参数。

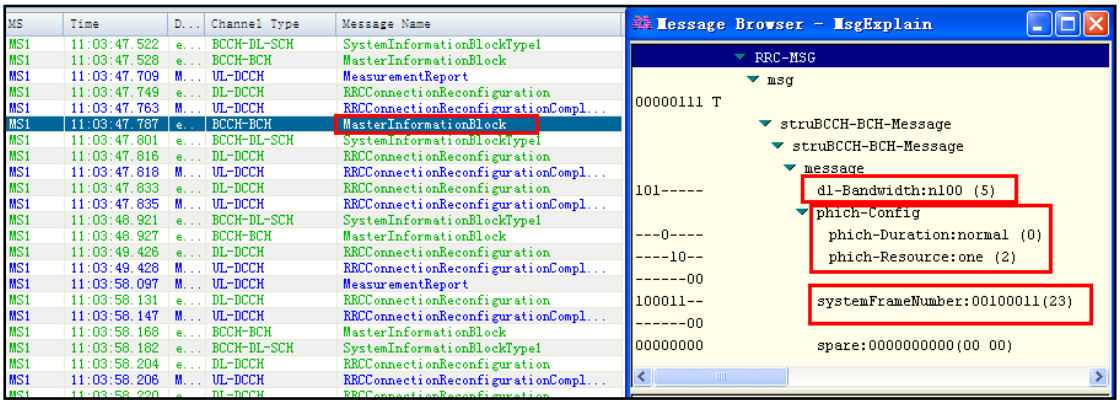
- SIB7:GERAN 邻频频点列表以及每个频点的重选参数。
- SIB8:CDMA2000 的预注册信息、CDMA2000 邻频频段列表和每个频段的重选参数、CDMA2000 邻频频段的邻区列表。
- SIB9:Home eNodeB 的名称。
- SIB10:ETWS 主信息（primary notification）。
- SIB11:ETWS 辅信息（secondary notification）。
- SIB12:CMAS 信息（CMAS notification）。
- SIB13:请求获取跟一个或多个 MBSFN 区域相关的 MBMS 控制信息的信息。



4.2 系统消息解析

4.2.1 MIB （Master Information Block）解析

MIB 主要包含系统带宽、PHICH 配置信息、系统帧号。（下图为实测信令）



- DL_Bandwidth 系统带宽，范围 enumerate(1.4M(6RB，0)，3M(15RB,1)，5M(25RB,2)，10M(50RB,3)，15M(75RB,4)，20M(100RB,5))，上图为 n100，对应的系统带宽为 20M（100RB，带宽索引号为 5）。

- Phich_Duration 当该参数设置为 normal 时，PDCCH 占用的 OFDM 符号数可以自适应调整；当该参数设置为 extended 时，若带宽为 1.4M，则 PDCCH 占用的 OFDM 符号数可以取 3 或 4，对于其他系统带宽下，PDCCH 占用的符号数只能为 3。

PHICH持续时间	非MBSFN子帧		MBSFN子帧
	帧结构类型2中的子帧1和子帧6	其他情况	同时支持PDSCH和PMCH的载波
Normal	1	1	1
Extended	2	3	2

- PHICH-Resource 该参数用于计算小区 PHICH 信道的资源；
- SystemFrameNumber 系统帧号。系统帧号，用于 UE 获取系统时钟。实际 SFN 位长为 10bit，也就是取值从 0-1023 循环。在 PBCH 的 MIB 广播中只广播前 8 位，剩下的两位根据该帧在 PBCH 40ms 周期窗口的位置确定，第一个 10ms 帧为 00，第二帧为 01，第三帧为 10，第四帧为 11。PBCH 的 40ms 窗口手机可以通过盲检确定。
- Spare：预留的，暂时未用

4.2.2 SIB1 （System Information Block Type1）解析

SIB1 上主要传输评估 UE 能否接入小区的相关信息及其他系统消息的调度信息。

主要包括 4 部分：

- 小区接入相关信息（cell Access Related Info）
- 小区选择信息（cell Selection Info）
- 调度信息（scheduling Info List）
- TDD 配置信息（tdd-Config）

SIB1 消息解析（UE 侧）:
RRC-MSG
..msg
....struBCCH-DL-SCH-Message
......struBCCH-DL-SCH-Message
........message
..........c1
............systemInformationBlockType1
..............cellAccessRelatedInfo//小区接入相关信息
................plmn-IdentityList//PLMN 标识列表
..................PLMN-IdentityInfo
....................plmn-Identity

.....mcc//460
.....MCC-MNC-Digit:0x4 (4)
.....MCC-MNC-Digit:0x6 (6)
.....MCC-MNC-Digit:0x0 (0)
.....mnc//00
.....MCC-MNC-Digit:0x0 (0)
.....MCC-MNC-Digit:0x0 (0)
.....cellReservedForOperatorUse:notReserved (1)
.....trackingAreaCode:1000100100001100(890C)
//TAC 跟踪区（890C）为 16 进制数，转换成十进制为 35084，查 TAC 在该消息中可以查到，此条信元重要。
.....cellIdentity:100010010000010101010100001010(08 90 55 0A)
//小区 ID 实际是 ECI，与核心网中的数据相同，其中 089055 为 ENB ID 标识，0A 为小区标识（此数字必须是 2 位 16 进制数，才能与 16 进制的 ENB ID 进行组合成 ECI），如果 ENB ID 和小区 ID 都是十进制数的话，ECI=10 进制的 ENB ID * 256+ 10 进制 cell ID
.....cellBarred:notBarred (1)//小区禁止：不禁止，1 表示不禁止，0 表示禁止；
.....intraFreqReselection:allowed (0)//同频重选：允许；用来控制当更高级别的小区禁止接入时，能否重选同频小区。
.....csg-Indication:FALSE//指示这个小区是否为 CSG 小区。当 csg-Indication 设置为 1（true）时，只有当消息中的 CSG（Closed Subscriber Group 关闭用户组）标识和 UE 中存储的 CSG 列表中的一项匹配时，此 UE 才能接入小区。这个主要是用在 R9 的家庭基站中的概念，用于家庭基站对用户接入的控制。FALSE 表示不启用。
.....cellSelectionInfo//小区选择信息
.....q-RxLevMin:-0x40 (-64)// 小区要求的最小接收功率 RSRP 值[dBm]，即当 UE 测量小区 RSRP 低于该值时，UE 是无法在该小区驻留的。实际的值为：Qrxlevmin = IE value * 2
.....freqBandIndicator:0x27 (39)// 频带指示，表示当前系统的使用 39 频段
.....schedulingInfoList//调度信息表
.....SchedulingInfo
.....si-Periodicity:rf16 (1)// SI 消息的调度周期，以无线帧为单位。如 rf8 表示周期为 8 个无线帧，rf16 表示周期为 16 个无线帧。
.....sib-MappingInfo
.....SIB-Type:sibType3 (0)// 系统消息中所含的系统信息块映射表。表中没有包含 SIB2，它一直包含在 SI 消息中的第一项。该字段决定了该小区能下发的 sib（3 到 11）类型。以上调度信息表示 SIB3 的周期和位置。
.....SchedulingInfo
.....si-Periodicity:rf32 (2)
.....sib-MappingInfo
.....SIB-Type:sibType5 (2)// 以上调度信息表示 SIB3 的周期和位置。
.....tdd-Config
.....subframeAssignment:sa2 (2)// 用于指示上下行子帧的配置，sa2 对应配置 2。

Uplink-downlink configuration	Downlink-to-Uplink Switch-point periodicity	Subframe number									
		0	1	2	3	4	5	6	7	8	9
0	5 ms	D	S	U	U	U	D	S	U	U	U
1	5 ms	D	S	U	U	D	D	S	U	U	D
2	5 ms	D	S	U	D	D	D	S	U	D	D
3	10 ms	D	S	U	U	U	D	D	D	D	D
4	10 ms	D	S	U	U	D	D	D	D	D	D
5	10 ms	D	S	U	D	D	D	D	D	D	D
6	5 ms	D	S	U	U	U	D	S	U	U	D

.....specialSubframePatterns:ssp5 (5)//特殊子帧配比

特殊子帧配置	Normal CP（常规CP）1ms14个码		
	DwPTS	GP	UpPTS
0	3	10	1
1	9	4	1
2	10	3	1
3	11	2	1
4	12	1	1
5	3	9	2
6	9	3	2
7	10	2	2
8	11	1	2
9	6	6	2

.....si-WindowLength:ms40 (6)// 系统消息调度窗口，以毫秒为单位,40ms

.....systemInfoValueTag:0x5 (5)// 指示其它 SIB 是否发生了改变,对于除 MIB、SIB1、SIB10 和 SIB11 之外的所有系统信息块的公共值，范围（0~31）；SI 每变化一次，systemInfoValueTag 值就加 1【或减 1：移动研究院测试华为网络机制是减 1】。举例：UE 将寻呼消息 PAGING TYPE1 中的 MIB value tag1 与自己保存的 MIB value tag2 进行比较：

1、如果这两个 Tag 不同的话，认为 MIB 已经更新，重新读取当前 BCH 上广播的 MIB。

2、当重新获取得 MIB 的 MIB value tag3 与 MIB value tag1 相同，而与 MIB value tag2 不同的话，读取 MIB 中的调度内容，进行系统消息更新。

3、如果自己保存的 MIB value tag2 与重新接收的 MIB value tag3 相同，而与寻呼消息中的 MIB value tag1 不同的话，认为 MIB 还没有广播下来，等下一个 MIB。

4.2.3 SystemInformation 消息

SIB2~SIB13 不会单独存在，它们会组合成 SI 消息进行下发，S2 消息为 SI 消息中第一项内容不可或缺，其他消息下发时机由 SIB1 消息进行调度指示。此条消息为 UE 侧跟踪

得到,仅包含了 SIB2 和 SIB3 消息
RRC-MSG
..msg
....struBCCH-DL-SCH-Message
......struBCCH-DL-SCH-Message
........message
..........c1
............systemInformation
..............criticalExtensions
................systemInformation-r8//系统消息版本 R8
..................sib-TypeAndInfo
....................CHOICE
......................sib2
........................radioResourceConfigCommon//无线资源配置 SIB
..........................rach-ConfigCommon//随机接入配置
............................preambleInfo
..............................numberOfRA-Preambles:n52 (12)// 该小区用于随机接入前导码个数（竞争）ENUMERATED{n4, n8, n12, n16 ,n20, n24, n28,n32, n36, n40, n44, n48, n52, n56, n60, n64},n52，即 52 个。
..............................preamblesGroupAConfig
................................sizeOfRA-PreamblesGroupA:n28 (6)//随机接入前导码组 A 的大小。对于所有用于竞争随机接入的 Preamble 码，eNodeB 可以选择性的将其分为两组，称为集合 A 和集合 B。触发随机接入时，UE 首先根据待发送的 Msg3 大小和路损大小确定使用哪个集合。集合 A 用于 Msg3 较小或路损较大的场景；集合 B 用于 Msg3 较大且路损较小的场景。ENUMERATED{n4, n8, n12, n16 ,n20, n24, n28,n32, n36, n40, n44, n48, n52, n56, n60},n28:前导码组 A 包含 28 个前导码。
................................messageSizeGroupA:b56 (0)//Msg3 消息块大小门限，针对 Preamble 码集合 A。b56 表示 56bit.如果 Group B 存在，则在选择 Preamble 码的集合时，考察：如果 Msg3 的大小大于该门限，同时满足 UE 的路损小于：PCMAX 【配置的 UE 发射功率：位置需核实（SIB1 的 P-max。这个是可选项，现网可能没开。)】 - preambleInitialReceivedTargetPower - deltaPreambleMsg3 - messagePowerOffsetGroupB 的门限值，则选择 Group B；否则就选择 Group A ENUMERATED { b56, b144, b208, b256}
................................messagePowerOffsetGroupB:dB10 (4) //用于配合判决 Preamble 码集合的选择。ENUMERATED { minusinfinity, dB0, dB5, dB8, dB10, dB12, dB15, dB18}
............................powerRampingParameters
..............................powerRampingStep:dB2 (1)//随机前导码的发射功率调整步长。ENUMERATED {dB0, dB2,dB4, dB6},dB2 表明 2 个 dB
..............................preambleInitialReceivedTargetPower:dBm-104 (8)//eNodeB 期望接收到的初始随机前导码的功率。ENUMERATED{dBm-120, dBm-118, dBm-116, dBm-114, dBm-112, dBm-110, dBm-108, dBm-106, dBm-104, dBm-102, dBm-100, dBm-98, dBm-96, dBm-94, dBm-92, dBm-90}
............................ra-SupervisionInfo//随机接入监测信息

.....preambleTransMax:n10 (6)//preamble 码最大发送次数。如果初始接入过程失败，但是还没有达到最大尝试次数 preambleTransMax，则可以继续尝试。如果达到最大次数，则本次随机接入过程结束。ENUMERATED { n3, n4, n5, n6, n7,n8, n10, n20, n50, n100, n200}

补充知识：两次尝试之间时间间隔：在 RAR 消息中，还可能存在一个 backoff 指示，指示了 UE 重传前导的等待时间范围. 如果 UE 在规定的时间范围以内，没有收到任何 RAR 消息，或者 RAR 消息中的前导序列索引与自己的不符，则认为此次的前导接入失败.UE 需要推迟一段时间，才能进行下一次的前导接入. 推迟的时间范围，就由 backoff indictor 来指示，UE 可以在 0 到 BackoffIndicator 之间随机取值. 这样的设计可以减少 UE 在相同时间再次发送前导序列的几率

.....ra-ResponseWindowSize:sf10 (7)//随机接入响应窗大小。Sf10 表示 10 个子帧的长度。响应窗起点与 Msg1 间隔 10ms【发送了接入前导序列以后，UE 需要监听 PDCCH 信道,是否存在 ENODEB 回复的 RAR 消息，(Random Access Response)，RAR 的时间窗是从 UE 发送了前导序列的子帧 + 3 个子帧开始，长度为 Ra-ResponseWindowSize 个子帧】,ENUMERATED { sf2, sf3, sf4, sf5, sf6, sf7, sf8, sf10}

.....mac-ContentionResolutionTimer:sf64 (7)//MAC 竞争解决定时器。UE 在发送 Msg3 后启动该定时器，并在每次 Msg3 重传时重启该定时器。如果直到该定时器超时都没有完成竞争解决，则认为此次竞争解决失败，根据相关时延后发起下一次请求，直到 preambleTransMax 达到最大次数。ENUMERATED { sf8, sf16, sf24, sf32, sf40, sf48, sf56, sf64},sf40，即 200ms,sf64 为 320ms。

.....maxHARQ-Msg3Tx:0x5 (5)//Msg3 的传输支持 HARQ 过程，该参数即表示自动重传次数。取值为整数 1~8，该参数与 preambleTransMax 的区别，该参数是在一次 preamble 码接入成功的基础上 Msg3 可以自动重传的次数。

.....bcch-Config

.....modificationPeriodCoeff:n2 (0)//系统消息更新周期系数，n2 就是 2。在 UE 没有得到其他通知的情况下, LTE 规定 UE 存贮的系统信息的有效期为 3 小时。LTE 中，系统信息的改变只能在特定的系统帧上进行，这些特定的帧满足条件：SFN 帧号 mod 系统消息更新周期 = 0；其中系统消息更新周期 = 系统消息更新周期系数 * 默认寻呼周期.

.....pcch-Config

.....defaultPagingCycle:rf128 (2)//默认的寻呼周期。ENUMERATED { rf32, rf64, rf128, rf256}，rf128，即 128 个无线帧，也就是 1280ms

.....nB:oneT (2)//默认寻呼周期的系数。oneT，即生效的默认寻呼周期=1*默认寻呼周期,ENUMERATED { fourT, twoT, oneT, halfT, quarterT(1/4), oneEighthT(1/8) , oneSixteenthT(1/16), oneThirtySecondT(1/32) }

.....prach-Config

.....rootSequenceIndex:0x158 (344) //根序列索引，344（十进制）

.....prach-ConfigInfo

.....prach-ConfigIndex:0x3 (3)//PRACH 配置索引，用于指示无线帧中的 PRACH 时频位置，取值范围为 0~63，不同的取值对应不同个数个 PRACH 信道。对于 TDD，由于上行子帧较少，一个 subframe 可以有多个 PRACH，但最多为 6 个。

.....highSpeedFlag:FALSE//标志位，决定前导生成的循环移位值 N_{CS}

是取限制集还是取非限制集，false 即取非限制集的值

.....zeroCorrelationZoneConfig:0x8 (8)//零相关区配置，决定前导生成的循环移位值 N_{CS},取值范围 0~15

.....prach-FreqOffset:0x8 (8)//该参数用于广播 PRACH 在频域上的位置，prach-FreqOffset 的值代表的是物理块资源的号码。由 MAC 层触发的随机接入前导序列，只能在特定的时频资源上发送。PRACH 在频域上的位置由上层半静态设定的，通过 SIB2 中的参数 prach-FreqOffset 广播。

.....pdsch-ConfigCommon

.....referenceSignalPower:0xc (12)//参考信号功率。下行参考信号传输功率定义为系统带宽内所有承载小区专用参考信息的资源粒子功率的线性平均,取值 INTEGER (-60..50)

.....p-b:0x1 (1)//P_B 是 Type A 和 Type B 的 PDSCH 资源元素的 offset. 当等于 1 时且为 2/4 天线端口的情况下，A 类符号和 B 类符号的功率相等。

.....pusch-ConfigCommon

.....pusch-ConfigBasic

.....n-SB:0x4 (4)//pusch 物理资源映射中用于计算子带（sub-band）长度，即子带数目

.....hoppingMode:interSubFrame (0)//跳频模式。不同跳频模式下 pusch 发送信号使用的资源块获得方式不一样。ENUMERATED {interSubFrame, intraAndInterSubFrame}

.....pusch-HoppingOffset:0x1a (26)//跳频偏移

.....enable64QAM:TRUE//是否支持 64QAM 调制

.....ul-ReferenceSignalsPUSCH

.....groupHoppingEnabled:FALSE//是否允许组跳频。所谓序列组跳，是指小区在不同的时隙内，使用不同序列组内的参考序列。在非序列组跳转的情况下，也就是说，在不同的时隙内，小区的参考序列都来自同一个参考序列组。在 PUCCH 的情况下，序列组的序号是小区的 PCI 模 30 后的余值。其中，PCI 在 0 到 503 之间取值。对于 PUSCH 使用的序列组是通过 SIB2 中的参数“groupAssignmentPUSCH”来显式通知 UE 的。这样做的目的是允许相邻的小区使用相同的参考信号根序列。通过相同根序列的不同循环移位来使相邻小区的不同 UE 之间的 RS 相互正交。false，则表示不支持

.....groupAssignmentPUSCH:0x0 (0)//组分配 PUSCH ，用于定义 pusch 不用的位移序列样式

.....sequenceHoppingEnabled:FALSE//是否允许序列跳频

.....cyclicShift:0x0 (0)// 循环移位

.....pucch-ConfigCommon

.....deltaPUCCH-Shift:ds1 (0)//协助计算 pucch 格式 1、1a、1b 时的循环移位及正交序列索引的确定。ENUMERATED {ds1, ds2, ds3}

.....nRB-CQI:0x1 (1)// 即 $N_{RB}^{(2)}$，表示每个时隙中可用于 PUCCH 格式 2/2a/2b 传输的物理资源块数.

.....nCS-AN:0x0 (0)// 即 $N_{cs}^{(1)}$，表示的是 PUCCH 格式 1/1a/1b 和格式 2/2a/2b 在一个物理资源块中混合传输时格式 1/1a/1b 可用的循环移位数

.....n1PUCCH-AN:0x48 (72)// 即 $N_{PUCCH}^{(1)}$，用于传输 PUCCH 格式 1/1a/1b 的资源的非负索引值
.....soundingRS-UL-ConfigCommon
.....setup
.....srs-BandwidthConfig:bw0 (0)//探测参考信号带宽。
.....srs-SubframeConfig:sc0 (0)// 探测参考信号子帧配置
.....ackNackSRS-SimultaneousTransmission:TRUE//决定了 UE 是否配置支持在同一个子帧中进行 PUCCH ACK/NACK 和 SRS 的传输
.....srs-MaxUpPts:true (0)
.....uplinkPowerControlCommon
.....p0-NominalPUSCH:-0x43 (-67)//该参数只用于非持续调度，用于 pusch 功率计算
.....alpha:al07 (4)// 即α，是一个 3bit 的小区专用参数，用于 pusch 功率计算，07 代表 0.7
.....p0-NominalPUCCH:-0x69 (-105)// 用于 pucch 功率计算
.....deltaFList-PUCCH
.....deltaF-PUCCH-Format1:deltaF0 (1)//{deltaF-2, deltaF0, deltaF2}，1 表示 deltaF0
.....deltaF-PUCCH-Format1b:deltaF3 (1)//{deltaF1, deltaF3, deltaF5}，1 表示 deltaF3
.....deltaF-PUCCH-Format2:deltaF1 (2)//{deltaF-2, deltaF0, deltaF1, deltaF2}，2 表示 deltaF1
.....deltaF-PUCCH-Format2a:deltaF2 (2)//{deltaF-2, deltaF0, deltaF2}，2 表示 deltaF2
.....deltaF-PUCCH-Format2b:deltaF2 (2)//{deltaF-2, deltaF0, deltaF2}，2 表示 deltaF2
.....deltaPreambleMsg3:0x4 (4)//用于随机接入响应许可的 PUSCH 的功率计算。实际值= IE value * 2 [dB],4*2=8
.....ul-CyclicPrefixLength:len1 (0)// 循环前缀长度 。len1 表示常规循环前缀，len2 表示扩展循环前缀
.....ue-TimersAndConstants//UE 定时器常数
.....t300:ms1000 (5)//RRC 连接建立定时器。启动时间：RRCConnectionRequest 发出后；停止时间：收到 RRCConnectionSetup or RRCConnectionReject 。如果在超时时还未收到 RRCConnectionSetup or RRCConnectionReject，则认为本次 RRC 建立失败。
.....t301:ms200 (1)// UE 在发送 RRCConnectionReestabilshmentRequest 时启动该定时器。定时器超时前，如果 UE 收到 RRCConnectionReestablishment 或者 RRCConnectionReestablishmentReject 或者被选择小区变成不适合小区，则停止该定时器。定时器超时后，UE 进入 RRC_IDLE 态。
.....t310:ms1000 (5)// UE 在检测到物理层故障时，启动该定时器。在定时器超时前，如果 UE 检测到物理层故障恢复，或者触发切换流程，或者 UE 发起连接重建流程，则停止该定时器。定时器超时后，如果没有激活安全模式，UE 进入 RRC_IDLE 态；

否则，发起连接重建流程。改小此参数，RRC 重建增多。改大此参数可能无法及时检测到下行失步，影响用户业务时延感受，可以减少重建次数。
.....n310:n10 (6)// 该参数表示接收到底层的连续"失步"指示的最大数目。改小，可能增加重建次数，改大可能无法及时检测到下行失步，影响用户业务时延感受。
.....t311:ms10000 (3)// UE 在发起 RRC 连接重建流程时启动该定时器。定时器超时前，如果 UE 选择了一个 EUTRAN 小区或者异系统小区后，停止此定时器。定时器超时后，UE 进入 RRC_IDLE 态。改小此参数对掉话率有负增益。改大此参数影响用户业务时延感受，可以减少掉话次数。
.....n311:n1 (0)//该参数表示接收到底层的连续"同步"指示的最大数目，改小可以减少 RRC 重建，可能无法及时检测到下行故障，影响用户业务时延感受；改大，RRC 重建次数增多。
.....freqInfo
.....additionalSpectrumEmission:0x1 (1)// UE 射频参数，需要查表
.....timeAlignmentTimerCommon:sf1920 (3)//时间调整定时器，上行同步成功后启动，失步后重启。这个参数是 MAC 层过程参数，是对 UE 上行同步状态进行维护的一个定时器。UE 上行需要保持和 eNodeB 的同步 ，同步是利用 Rach 信道和过程获得的。但是 UE 一次做完一次 Rach，获得同步以后，可能由于 UE，eNodeB 双方的时钟偏移，或者信道情况改变，而又变成失步状态。在 Time Alignment Timer 超时的时间内，eNodeB 必需对 UE 的上行定时做一次调整(eNB 会给 UE 发 Timing Advance Command 来调整上行同步)，或者确认，否则 UE 认为上行失步，需要重新 Rand Access。例如：在随机接入过程的 Msg2 中，基站通常会返回给 UE 一个 TA（时间提前量），这是为了保证 Msg3 的同步，sf1920，子帧为单位，即 1920 个子帧长度
.....CHOICE
.....sib3
.....cellReselectionInfoCommon//小区重选信息
.....q-Hyst:dB4 (4)//小区重选迟滞。用于作用在（在服务小区测量值上加上该值）服务小区后作为重选判决依据
.....cellReselectionServingFreqInfo//小区重选服务频率信息
.....s-NonIntraSearch:0xe (14)// 异频搜索门限。实际值=配置值*2
.....threshServingLow:0x4 (4)// 由服务频率向低优先级重选时门限。实际值=配置值*2
.....cellReselectionPriority:0x7 (7)// 小区重选优先级。
.....intraFreqCellReselectionInfo//同频小区重选信息
.....q-RxLevMin:-0x40 (-64)// 小区要求的最小接收功率 RSRP 值[dBm]，即当 UE 测量小区 RSRP 低于该值时，UE 是无法在该小区驻留的。实际的值为：Qrxlevmin = IE value * 2，-64 为-128dBm
.....s-IntraSearch:0x1d (29)// 同频搜索门限。实际值=配置值*2
.....presenceAntennaPort1:FALSE//用于指示是否所有的邻区均使用天线端口 1，FALSE 表示不使用。
.....neighCellConfig:01(01)// 相邻小区配置。00：不是所有邻区均和当前服务小区有相同的 MBSFN 子帧配置。10：所有邻区均和当前服务小区有相同的 MBSFN 子帧配置。01：所有邻区均没有 MBSFN 子帧配置。11：相对于服务小区的 UL/DL 配置，邻区中存在不同的 UL/DL 配置。对于 TDD，00、10、01 只用于服务小区和邻区的 UL/DL 配置相同情况。

.....t-ReselectionEUTRA:0x2 (2)// EUTRA 小区重选定时器。
.....t-ReselectionEUTRA-SF//对应速度状态下的 t-ReselectionEUTRA 的比例系数。
.....sf-Medium:lDot0 (3)// 中速状态下的比例系数。
.....sf-High:oDot75 (2)// 高速状态下的比例系数。
.....s-IntraSearch-v920
.....s-IntraSearchP-r9:0x1d (29)// R9 下同频搜索 rsrp 门限。实际值=配置值*2
.....s-IntraSearchQ-r9:0x5 (5)// R9 下同频搜索 rsrq 门限。实际值=配置值*2
.....s-NonIntraSearch-v920
.....s-NonIntraSearchP-r9:0xe (14)// R9 下异频搜索 rsrp 门限。实际值=配置值*2
.....s-NonIntraSearchQ-r9:0x4 (4)// R9 下异频搜索 rsrq 门限。实际值=配置值*2
.....q-QualMin-r9:-0x12 (-18)// R9 下小区驻留要求的最小 rsrq

其他系统消息也是与 SIB2 组合在一起在 SI 消息中下发，SI 系统消息可能会包含多个 SIB，这里不详细列举，对信元的理解需要多查询资料。华为 eNodeB 设备，在同频邻区 CIO 设置为 0 时，系统不会向终端下发 SIB4，即同频邻区列表信息。

第五章信令案例解析

通过前几章信令流程和系统消息的学习，我们对信令有了一些基本认识。本章我们以一个实测案例来分析各个信元消息的作用和重要信元内容，帮助我们加深信令的理解和学习，下面的案例是在华为设备 OM920 上 LTE 虚用户跟踪采集到的信令，信令中包含了 RRC 的建立过程、文本建立过程、安全模式、ERAB 承载修改、UE 文本修改、CSFB 在 4G 网的过程等。这个信令流程是多个物理过程的组合，一般在问题定位时，主要看物理过程的流程是否完善，去判断流程的异常性，比如 RR 有建立请求没有建立完成消息就说明 RRC 在建立过程中异常。

5.1 实测案例流程

采集时间	标准接口消息类型	消息中文名称	消息方向
18:12:32 (972)	RRC_CONN_REQ	RRC 连接请求	接受自 UE
18:12:32 (973)	RRC_CONN_SETUP	RRC 连接建立	发送到 UE
18:12:32 (973)	RRC_CONN_SETUP_CMP	RRC 连接建立完成	接受自 UE
18:12:32 (973)	S1AP_INITIAL_UE_MSG	初始直传消息	发送到 MME
18:12:32 (973)	S1AP_INITIAL_CONTEXT_SETUP_REQ	初始文本建立请求	接收自 MME
18:12:32 (973)	RRC_UE_CAP_ENQUIRY	UE 能力查询	发送到 UE
18:12:32 (993)	RRC_UE_CAP_INFO	UE 能力信息	接受自 UE
18:12:32 (993)	S1AP_UE_CAPABILITY_INFO_IND	UE 能力信息指示	发送到 MME
18:12:32 (998)	RRC_SECUR_MODE_CMD	RRC 安全模式命令	发送到 UE
18:12:32 (999)	RRC_CONN_RECFG	RRC 连接重配置	发送到 UE
18:12:33 (13)	RRC_SECUR_MODE_CMP	RRC 安全模式完成	接受自 UE
18:12:33 (23)	RRC_CONN_RECFG_CMP	RRC 连接重配置完成	接受自 UE
18:12:33 (23)	S1AP_INITIAL_CONTEXT_SETUP_RSP	初始文本建立完成	发送到 MME
18:12:33 (47)	S1AP_ERAB_MOD_REQ	ERAB 修改请求	接收自 MME
18:12:33 (50)	RRC_DL_INFO_TRANSF	RRC 下行直传消息	发送到 UE
18:12:33 (50)	S1AP_ERAB_MOD_RSP	ERAB 修改完成	发送到 MME
18:12:33 (67)	RRC_CONN_RECFG	RRC 连接重配置	发送到 UE
18:12:33 (68)	RRC_UL_INFO_TRANSF	RRC 上行直传消息	接受自 UE
18:12:33 (68)	S1AP_UL_NAS_TRANS	上行 NAS 信息传输	发送到 MME
18:12:33 (83)	RRC_CONN_RECFG_CMP	RRC 连接重配置完成	接受自 UE
18:12:33 (649)	RRC_CONN_RECFG	RRC 连接重配置	发送到 UE
18:12:33 (673)	RRC_CONN_RECFG_CMP	RRC 连接重配置完成	接受自 UE
18:12:33 (753)	RRC_MEAS_RPRT	RRC 测量报告	接受自 UE
18:12:34 (354)	RRC_UL_INFO_TRANSF	RRC 上行信息传输	接受自 UE
18:12:34 (354)	S1AP_UL_NAS_TRANS	上行 NAS 信息传输	发送到 MME
18:12:34 (360)	S1AP_UE_CONTEXT_MOD_REQ	UE 文本更改请求	接收自 MME
18:12:34 (361)	S1AP_UE_CONTEXT_MOD_RSP	UE 文本更改响应	发送到 MME
18:12:34 (371)	RRC_CONN_REL	RRC 连接释放	发送到 UE
18:12:34 (394)	S1AP_UE_CONTEXT_REL_REQ	UE 文本释放请求	发送到 MME
18:12:34 (408)	S1AP_UE_CONTEXT_REL_CMD	UE 文本释放命令	接收自 MME
18:12:34 (409)	S1AP_UE_CONTEXT_REL_CMP	UE 文本释放完成	发送到 MME

上表采用超链接方式，Ctrl+鼠标左键点击　可迅速进入对应的信令解析

5.2 流程中各信令消息解析

通过信令消息内容的解析，来熟悉每条信息携带的内容和重要信元。

5.2.1 RRC_CONN_REQ:RRC 连接请求

RRC 连接请求。终端由 IDLE 态转为 CONNECT 态，或者终端有数据需要发送时，会发送建立 RRC 连接的请求。由 UL_CCCH 信道发送上来，在 SRB0 上承载。

UE 上行发送一条 RRC Connection Request 消息给 eNB,请求建立一条 RRC 连接，该消息携带主要IE有 :ue-Identity :初始的UE标识。如果上层提供S-TMSI ,则该值为S-TMSI；否则从 0...240-1 中抽取一个随机值，设置为 ue-Identity 。

establishmentCause ：建立原因。该原因值有 emergency(紧急呼叫), highPriorityAccess（高优先级接入）, mt-Access（移动终端接入，如响应寻呼）, mo-Signalling（移动始端信令，如附着、位置更新、随机接入等）, mo-Data（移动始端数据，上行有需要传送时，如发生视频、图片）, spare3, spare2, spare1。其中“mt”代表移动终端，理解成“被叫”，“mo”代表移动始端，理解成“主叫”。

RRC-MSG
..msg
....struUL-CCCH-Message
......struUL-CCCH-Message
........message
..........c1
............rrcConnectionRequest
..............criticalExtensions//关键扩展
................rrcConnectionRequest-r8//RRC 连接请求原因，R8 版本
..................ue-Identity//UE ID，包含 randomValue 和 S-TMSI 两种。
UE 接入时，如果已经获取过 TMSI，并判断驻留 cell 的 TA 在 UE 的 TAI list 里，即 MME 中保存了 UE 的上下文信息,会使用 TMSI 作为 UE ID;其他情况使用随机数 randomValue。
....................s-TMSI//值得说明的是对于华为后台跟踪，需要核心网提供随机接入值或 STMSI 才能跟踪，但是核心网未必有时间查询，因此需要我们前台兄弟提供 STMSI 值就可立即进行信令跟踪，前台测试中在 RRC 连接请求消息中携带 STMSI 值。
....................mmec --- '00001000'B//如果是终端测试此信元会解析为十进制（8）
....................m-TMSI --- '11000011000001010100010000100111'B
..................establishmentCause --- mt-Access(2)//接入原因值：移动终端接入，如响应寻呼
..................spare --- '0'B//预留值为以后的网络扩展做准备

5.2.2 RRC_CONN_SETUP:RRC 连接建立

RRC 连接建立消息包含建立 SRB1 承载和无线资源配置信息，主要目的为建立 SRB1，该消息通过 DL_CCCH 信道发送，承载在 SRB0 上。

RRC-MSG
..msg
....struDL-CCCH-Message
......struDL-CCCH-Message
........message
..........c1
............rrcConnectionSetup
..............rrc-TransactionIdentifier --- 0x1(1)//RRC 消息 ID
..............criticalExtensions
................c1
..................rrcConnectionSetup-r8
....................radioResourceConfigDedicated//无线资源配置专用
......................srb-ToAddModList
........................SRB-ToAddMod
..........................srb-Identity --- 0x1(1)//只建立 SRB1
..........................rlc-Config
............................explicitValue
..............................am//SRB 为保证信令的正确接收配置为 AM 模式，关于模式：透明模式（TM）、非确认模式（UM）和确认模式（AM）
..............................ul-AM-RLC//UL-AM-RLC 为针对 UE 侧的上行 RLC 配置，主要配置 RLC 数据接收侦测规则。SRB1 上下行采用 AM RLC 模式
................................t-PollRetransmit --- ms45(8)//AMD PDU 重传检测定时器时长。发送端发送某个 Poll 的 AMD PDU 后，如果在该定时器超时后，还没有收到响应，则重新触发 Poll.
................................pollPDU --- pInfinity(7)//UE 触发 Polling 的 PDU 字节数据量门限。轮询间隔 SDU 数，该参数给出了一个触发轮询的门限值，发送了 PollSDU 个 SDU 后触发一次轮询。此处的 pInfinity 对应为无穷多个 PDU。
................................pollByte --- kBinfinity(14)//PollByte 为 AM PDU 侦测字节数。触发每个 pollByte 字节的一个轮询。此处 kBinfinity 对应无穷多个 kByes
................................maxRetxThreshold --- t32(7)//UE AM 模式 RLC ARQ 最大重传次数。该参数用于配置 UE，表示 RLC ARQ 最大重传次数，用于限制一个 AM PDU 的重传次数。当等于该值时，将向高层上报不可恢复的错误，触发 RRC 连接重建。t32 对应 32 次重传输。
..............................dl-AM-RLC//DL-AM-RLC 为针对 UE 侧的下行 RLC 配置，主要配置 RLC 数据接收状态上报规则。
................................t-Reordering --- ms35(7)//UE AM 模式接收端重排序定时器，用于触发 RESET PDU 的重传。该参数用于配置 UE，表示 AM 模式接收端重排序定时器的大小。此处 ms35 表示 35ms。

.....t-StatusProhibit --- ms0(0)//UE 禁止发送状态报告定时器。该参数用于配置 UE，表示 AM 模式接收端禁止发送状态报告的定时器大小。即在本时长内不允许上报状态报告。ms0 表示 0ms。
.....logicalChannelConfig//SRB1 逻辑信道配置
.....explicitValue
.....ul-SpecificParameters
.....priority --- 0x1(1)//SRB1 逻辑信道优先级，值越小，优先级越高。华为 eNB 实现 SRB1 的优先级为 1，SRB2 为 3。UE 调度器按逻辑信道优先级由高到低优先速率；所有业务优先速率保证后，按逻辑信道优先级由高到低依次分配资源。
.....prioritisedBitRate --- infinity(7)//SRB1 逻辑信道优先速率。UE 调度器按逻辑信道优先级由高到低依次保证逻辑信道的优先速率。Infinity 仅仅适用于 SRB1 和 SRB2.
.....bucketSizeDuration --- ms300(3)//SRB1bucket size 调整持续时间，300ms。
.....logicalChannelGroup --- 0x0(0)//根据业务的不同，UE 可能建立大量的无线承载（radio bearer，每个 bearer 对应一个逻辑信道），如果为每一个逻辑信道上报一个 BSR，会带来大量的信令开销。为了避免这种开销，LTE 引入了 LCG（Logical Channel Group）的概念，并将每个逻辑信道放入一个 LCG（共 4 个）中。UE 基于 LCG 来上报 BSR，而不是为每个逻辑信道上报一个 BSR。某个逻辑信道所属的 LCG 是在逻辑信道建立时通过 IE: LogicalChannelConfig 的 logicalChannelGroup 字段来设置的 。CCCH、SRB1、SRB2 默认属于 LCG 0
.....mac-MainConfig//MAC 层主要配置
.....explicitValue//确切的值
.....ul-SCH-Config//上行 SCH 信道配置
.....maxHARQ-Tx --- n5(4)//UL HARQ 的最大传输次数。BSR 报告定时器：用子帧表示，sf2560 表示 2560 个子帧。如果 retxBSR-Timer 超时并且 UE 在逻辑信道组中任意一个逻辑信道有可传数据，则触发缓存状态报告。而这样的 BSR 称为常规 BSR；如果 periodicBSR-Timer 超时，则触发缓存状态报告。而这样的 BSR 称为周期 BSR。ENUMERATED {n1, n2, n3, n4, n5, n6, n7, n8,n10, n12, n16, n20, n24, n28, spare2, spare1}
.....periodicBSR-Timer --- sf10(1)//周期性 BSR 上报定时器(子帧)。ENUMERATED {sf5, sf10, sf16, sf20, sf32, sf40, sf64, sf80,sf128, sf160, sf320, sf640, sf1280, sf2560,infinity, spare1},infinity 表示去使能。
.....retxBSR-Timer --- sf320(0)//BSR 重传定时器（子帧）。ENUMERATED {sf320, sf640, sf1280, sf2560, sf5120,sf10240, spare2, spare1}为提高 BSR 的健壮性，LTE 提供了一个重传 BSR 的机制：这是为了避免 UE 发送了 BSR 却一直没有收到 UL grant 的情况。eNodeB 通过 IE:MAC-MainConfig 的 retxBSR-Timer 字段为 UE 配置了一个 timer，当该 timer 超时且 UE 的任意一个 LCG 的任意一个逻辑信道里有数据可以发送时，将会触发 BSR。
.....ttiBundling --- FALSE(0)// TTI 捆绑只对 FDD 有效，对 TDD 仅仅适用于配置为 0，1 以及 6 的情况。FALSE 不绑定，TURE 表示 TTI 捆绑有效。
.....timeAlignmentTimerDedicated --- sf1920(3)//上行时间对齐定时器，该参数表示 UE 上行时间对齐的定时器长度，该定时器超时，则认为 UE 上行失步。取值范围：SF500(500 个子帧)，SF750(750 个子帧)，SF1280(1280 个子帧),

SF1920(1920 个子帧), SF2560(2560 个子帧), SF5120(5120 个子帧), SF10240(10240 个子帧), INFINITY(无穷大)
.....phr-Config//功率余量报告配置，PHR(power headroom report)
.....setup
.....periodicPHR-Timer --- sf1000(6)//功率余量报告周期定时器。ENUMERATED {sf10, sf20, sf50, sf100, sf200,sf500, sf1000, infinity}
.....prohibitPHR-Timer --- sf100(4)//禁止上报功率剩余报告定时器。ENUMERATED {sf0, sf10, sf20, sf50, sf100,sf200, sf500, sf1000}
.....dl-PathlossChange --- dB3(1)//PHR 报告的下行路径损耗变化。ENUMERATED {dB1, dB3, dB6, infinity}
什么时候报告功率余量？功率余量报告定时器：当 UE 有传输新数据的上行资源，prohibitPHR-Timer 超时或者已经超时且在上次传输功率余量报告之后，路径损耗的变化值大于 dl-PathlossChange dB。触发功率余量报告（PHR）；periodicPHR-Timer 超时，触发功率余量报告。
.....physicalConfigDedicated//物理层配置专用
.....pdsch-ConfigDedicated//PDSCH 配置专用
.....p-a --- dB-3(2)//PA=3
.....pucch-ConfigDedicated//PUCCH 配置专用
.....ackNackRepetition
.....release --- (0)//此处“release”为清除此配置以及停止使用相关资源。若设置为“setup”，采用相应的接收配置以及开始使用相关的资源。
.....tdd-AckNackFeedbackMode --- bundling(0)//TDD-确认非确认反馈模式----绑定模式。
.....pusch-ConfigDedicated//PUSCH 配置专用
.....betaOffset-ACK-Index --- 0x9(9)//ACK 随路偏置索引，该参数表示 ACK 随路偏置索引。INTEGER (0..15)
.....betaOffset-RI-Index --- 0x5(5)//RI 随路偏置索引，该参数表示 RI 随路偏置索引。INTEGER (0..15)
.....betaOffset-CQI-Index --- 0xc(12)//CQI 随路偏置索引，该参数表示 RI 随路偏置索引。INTEGER (0..15)
.....uplinkPowerControlDedicated//上行链路功控专用
.....p0-UE-PUSCH --- 0x0(0)//INTEGER (-8..7)
.....deltaMCS-Enabled --- en0(0)//根据不同 MCS 格式调整 UE 发射功率的开关。取值范围（0:不能够；1:能够）
.....accumulationEnabled --- TRUE(1)//累积使能，(0:不能够；1:能够)
.....p0-UE-PUCCH --- 0x0(0)//INTEGER (-8..7)
.....pSRS-Offset --- 0x5(5)//SRS 相对 PUSCH 的功率偏置，INTEGER (0..15)
.....filterCoefficient --- fc6(6)//RSRP 滤波系数。该参数表示 UE 估算路损过程中，对 RSRP 测量值进行滤波的 alpha 滤波系数。
.....tpc-PDCCH-ConfigPUCCH
.....release --- (0)
.....tpc-PDCCH-ConfigPUSCH
.....release --- (0)

.....cqi-ReportConfig//CQI 配置
.....cqi-ReportModeAperiodic --- rm30(3)//CQI 不定期上报模式，如果 CQI 周期自适应开关打开，则采用周期自适应相关配置。
.....nomPDSCH-RS-EPRE-Offset --- 0x0(0)
.....cqi-ReportPeriodic//CQI 周期上报相关参数
.....setup
.....cqi-PUCCH-ResourceIndex --- 0x0(0)//CQI-PUCCH 资源索引
.....cqi-pmi-ConfigIndex --- 0x12(18)//CQI-PMI 配置索引,确定上报周期 NP 和偏移量 NOFFSET.
.....cqi-FormatIndicatorPeriodic//
.....widebandCQI --- (0)//宽度 CQI。CQI 测量是针对 k 个连续的 PRB（即子带）进行的。如果在所有子带内反馈一个 CQI 值，则称为宽带 CQI；如果对每一个子带反馈不同的 CQI 值，称为子带反馈。
.....simultaneousAckNackAndCQI --- FALSE(0)//确认非确认及 CQI 是否同时，PUCCH CQI 反馈类型，取决于传输模式。FALSE 为不同时。
.....soundingRS-UL-ConfigDedicated//上行 RS 参考信号配置专用
.....setup
.....srs-Bandwidth --- bw2(2)//SRS 带宽
.....srs-HoppingBandwidth --- hbw0(0) //SRS 跳频带宽
.....freqDomainPosition --- 0x0(0)//SRS 频率范围位置
.....duration --- TRUE(1)//持续的
.....srs-ConfigIndex --- 0xf(15)//SRS 配置索引
.....transmissionComb --- 0x0(0)
.....cyclicShift --- cs4(4)
.....antennaInfo//天线信息
.....explicitValue
.....transmissionMode --- tm2(1)//传输模式,TM2，标识 UE 所使用的传输模式
.....ue-TransmitAntennaSelection//终端 UE 传输天线选择，Setup 或 release。Setup 表示开环或者闭环。
.....setup --- openLoop(1)//开环。
.....schedulingRequestConfig//调度请求配置信息
.....setup
.....sr-PUCCH-ResourceIndex --- 0x2(2)//SR PUCCH 资源索引，SR（资源调度请求），BSR（上行数据缓冲域状态报告过程）根据规范 BSR 过程：UE 在收到网络端的逻辑信道配置信息后，根据其中的逻辑信道标识号、优先级、逻辑信道组等信息，将每个逻辑信道归属于固定的逻辑信道组。BSR 主要功能是向 eNB 报告 UE 端上行数据缓冲域中的数据量，从而能够从 eNB 获取上行资源来传输缓冲域中的数据。MAC 层触发了 BSR 过程之后，如果没有传输 BSR 的资源则立即触发 SR 过程，向 eNB 申请至少 4 字节的上行资源以便能够传输 BSR 及其对应的 MAC 字头。两者关系可类似于一阶段接入和二阶段接入的关系。
.....sr-ConfigIndex --- 0x7(7)
.....dsr-TransMax --- n64(4)

5.2.3 RRC_CONN_SETUP_CMP:RRC 连接建立完成

通过连接建立消息，SRB1 建立起来，建立完成消息就 SRB1 承载在 UL_DCCH 信道上发送。RRC 连接建立完成消息中带有 NAS 层信息 ,NAS 消息基站侧不解析 ,直传到 MME。

RRC-MSG
..msg
....struUL-DCCH-Message
......struUL-DCCH-Message
........message
..........c1
............rrcConnectionSetupComplete//RRC 连接建立完成消息
..............rrc-TransactionIdentifier --- 0x1(1)//RRC 消息 ID
..............criticalExtensions
................c1
..................rrcConnectionSetupComplete-r8
....................selectedPLMN-Identity --- 0x1(1)//指示 UE 选择的 PLMN,如果是 1，表示在 SIB1 消息里面的第一个 PLMN，如果是 2，表示在 SIB1 消息里面的第二个 PLMN。以此类推
....................dedicatedInfoNAS --- 0xC71D63BD.....//传输 UE 和网络层的 NAS 层消息。eNB 层透传此消息给 MME。

5.2.4 S1AP_INITIAL_UE_MSG:初始直传消息

初始直传消息。基站把从 UU 口收到的 NAS 消息发往核心网 ,初始 ATTACH 时 ,该 Nas 消息一般包含 ATTACH REQ，请求在核心网创建上下文。

S1ap-Msg
..initiatingMessage
....procedureCode --- 0xc(12)
....criticality --- ignore(1)
....value
......initialUEMessage//UE 初始消息
........protocolIEs
..........SEQUENCE
............id --- 0x8(8)
............criticality --- reject(0)
............value
..............eNB-UE-S1AP-ID --- 0x513c35(5323829)//eNB 侧的用户标识。
..........SEQUENCE
............id --- 0x1a(26)
............criticality --- reject(0)

.....value
.....nAS-PDU
.....NAS-MESSAGE
.....service-request-message//服务请求消息
.....kSI-and-sequence-number
.....kSIasme --- 0x0(0)//MME 根据 KSIasme 可以找到 Kasme。之所以 MME 不直接用 Kasme，应该是一个安全性考虑。
.....sequence-number --- 0x1d(29)
.....message-authentication-code//消息鉴权码
.....short-MAC-value --- 0x63bd(25533)
.....SEQUENCE
.....id --- 0x43(67)
.....criticality --- reject(0)
.....value
.....tAI
.....pLMNidentity --- 0x64F000//PLMN 值
.....tAC --- 0x890A//TAC 值
.....SEQUENCE
.....id --- 0x64(100)
.....criticality --- ignore(1)
.....value
.....eUTRAN-CGI
.....pLMNidentity --- 0x64F000
.....cell-ID --- '100010010000001100010001111'B//此值为 ECI
.....SEQUENCE
.....id --- 0x86(134)
.....criticality --- ignore(1)
.....value
.....rRC-Establishment-Cause --- mt-Access(2)//RRC 建立原因值，移动终端接入，如响应寻呼等。此值与 RRC 连接请求携带的原因值一致。
.....SEQUENCE
.....id --- 0x60(96)
.....criticality --- reject(0)
.....value
.....s-TMSI
.....mMEC --- 0x08//接入的 MMEC
.....m-TMSI --- 0xC3054427//分配的 TMSI

5.2.5 S1AP_INITIAL_CONTEXT_SETUP_REQ:初始化文本建立请求

初始上下文建立请求。由核心网发往基站，包含 Nas 消息 ATTACH ACCEPT，指示基站为该 UE 分配资源建立数据承载。

S1ap-Msg
..initiatingMessage
....procedureCode --- 0x9(9)
....criticality --- reject(0)
....value
......initialContextSetupRequest//初始文本建立请求
........protocolIEs
..........SEQUENCE
............id --- 0x0(0)
............criticality --- reject(0)
............value
..............mME-UE-S1AP-ID --- 0x250ff2e(38862638)//核心网侧 UE 用户标识。在 eNodeB 保存的 UE 上下文释放之前，S1 接口都是用同样的一对 MME-eNodeB S1AP ID 来识别 UE。此值与“eNB-UE-S1AP-ID --- 0x513c35(5323829)”不同
..........SEQUENCE
............id --- 0x8(8)
............criticality --- reject(0)
............value
..............eNB-UE-S1AP-ID --- 0x513c35(5323829)//基站侧用户标识
..........SEQUENCE
............id --- 0x42(66)
............criticality --- reject(0)
............value
..............uEAggregateMaximumBitrate//AMBR (Aggregate Maximum Bit Rate)是集合最大比特速率，在 UE 开户时设置，系统通过限制流量方式禁止一组数据流集合的比特速率超过 AMBR，多个 EPS 承载可以共享一个 AMBR。对于 UE AMBR 带宽管理是限制一个 UE 的所有 Non-GBR 承载的速率之和不会超过 UE AMBR。如果开户时 AMBR 设置为 0，则初始上下文建立失败，会回复 INITIAL CONTEXT SETUP FAILURE 消息且原因值可能为“Semantic Error”。（因为协议没有完全对应的原因值，所以原因值和产品实现有关。）该值定义了用户 SIM 的最大下载速率，分为下行和上行。
................uEaggregateMaximumBitRateDL --- 0x61a8000(102400000)// 下行 AMBR,EPC 开户配置
................uEaggregateMaximumBitRateUL --- 0x61a8000(102400000) // 上行 AMBR,EPC 开户配置
..........SEQUENCE
............id --- 0x18(24)
............criticality --- reject(0)
............value
..............e-RABToBeSetupListCtxtSUReq//需要建立的 E-RAB 的列表，初始接入时只包含默认承载的信息。
................SEQUENCE
..................id --- 0x34(52)
..................criticality --- reject(0)
..................value

.....e-RABToBeSetupItemCtxtSUReq
.....e-RAB-ID --- 0x5(5)//eNodeB 分配的管理 E-RAB 的标识。默认承载建立时，E-RAB-ID 默认为 5。专用承载为其它值。ERAB-ID 的有效范围也同样是 5-15；故我们看到的默认承载建立其 ERAB-ID 都是从 5 开始编号的。
.....e-RABlevelQoSParameters//ERAB Qos 参数等级
.....qCI --- 0x6(6)//终端开户的 CQI。不同 QCI 的 SDF 映射到不同的 EPS 承载。默认承载只能是 Non-GBR 类型，而 QCI5 用于 IMS 信令，所以默认承载只能在开户时选择 QCI6-9。
.....allocationRetentionPriority//分配资源的优先级配置（包括优先级和抢占指示器）
.....priorityLevel --- 0x6(6)//此处为优先级 6，如果配置为“no priority”，则不考虑下面两个参考的配置。
.....pre-emptionCapability --- shall-not-trigger-pre-emption(0)//配置为 " may-trigger-pre-emption " ，表示分配可触发抢占过程。若配置为“shall-not-trigger-pre-emption”表示分配不可触发抢占过程。
.....pre-emptionVulnerability --- pre-emptable(1)//表示某 ERAB 的资源能否被其他 ERAB 抢占。此处设置为"pre-emptable"，表示该 E-RAB 应该包含在抢占过程中。
.....transportLayerAddress---
'01100100010110110111101100001000'B//UGW 分配的 GTPU 对端地址(传输层地址)，应该等于 eNodeB IPPATH 中设置的 UGW 业务地址。如果地址不相等，则 eNodeB 传输资源申请失败，会回复 INITIAL CONTEXT SETUP FAILURE 消息且原因值为“Transport Resource Unavailable”。
.....gTP-TEID --- 0xD178B68C//GTP 遂道终结点，此处指的是上行 GTP 遂道终结点，或者说 UGW 分配的 GTPU 对端端口。eNodeB 在申请传输资源并分配本端的地址和端口后，建立 GTPU 实体。默认承载和专有承载实际上使用的是不同的 GTPU 隧道。
.....SEQUENCE
.....id --- 0x6b(107)
.....criticality --- reject(0)
.....value
.....uESecurityCapabilities//UE 的安全能力，在 NAS Attach Request 中包含了网络能力。这里主要体现了加密算法和完全性保护算法。
.....encryptionAlgorithms --- '1100000000000000'B//加密算法：比特映射中每一个位置表示一种加密算法："所有比特为 0" - UE 支持 EEA0，不支持其它算法； "first bit" - 128-EEA1,； "second bit" - 128-EEA2，其它比特保留以备以后使用。值 ‘1’ 表示支持，值 '0'表示不支持该算法。
.....integrityProtectionAlgorithms --- '1100000000000000'B//完整性算法：比特映射中每一个位置表示一种完整性保护算法："all bits equal to 0" – UE 只支持 EIA0 ([15])； "first bit" - 128-EIA1；"second bit" - 128-EIA2。其它比特保留以备以后使用。值 ‘1’ 表示支持，值 '0'表示不支持该算法
.....SEQUENCE
.....id --- 0x49(73)
.....criticality --- reject(0)

.....value
.....securityKey ---
'10100101110111111100000010000010001101010001110001010110100110000011111111110101011001101010101110010001101011100010000000110101000011110110111010110101011110110011001111100100100110011101001001110111011110100010010010100000100011111001110011111011000001111111'B//安全密钥。核心网和 UE 之间 NAS 层的鉴权和安全过程之后，通过初始密钥生成的 KeNodeB，eNodeB 收到后会导出 AS 层的安全密钥。
.....SEQUENCE
.....id --- 0x19(25)
.....criticality --- ignore(1)
.....value
.....traceActivation//跟踪启动消息(跟踪激活)
.....e-UTRAN-Trace-ID --- 0x64F000003C090000//eNB 跟踪 ID:其组成为：PLMN(高 3 字节,如 64F000）+ Trace ID(中间 3 字节,如 003C09）+ Trace Recording Session Reference（低 2 字节，MDT 中使用，多个 UE 共用，如 0000），M2000 启动跟踪时填写.
.....interfacesToTrace --- '11100000'B//比特中每一位代表一个 eNB 接口 第一个比特=S1-MME，第二个比特 =X2，第三个比特 =Uu 其它比特保留以备以后使用..值“1”表示‘应该被跟踪’值“0”表示‘不应该被跟踪’.M2000 启动跟踪时选择
.....traceDepth --- maximum(2)//跟踪深度，参考协议 32.422/423。根据协议最低要求，eNB 目前只支持 Maximum，跟踪编码后的消息，不单独上报消息名称。
.....traceCollectionEntityIPAddress ---
'00000000000000000000000000000000'B//跟踪收集实体 IP 地址(TCE IP 地址),M2000 启动跟踪时填写
.....SEQUENCE
.....id --- 0x29(41)
.....criticality --- ignore(1)
.....value
.....handoverRestrictionList//切换限制列表
.....servingPLMN --- 0x64F000//当前服务网络

5.2.6 RRC_UE_CAP_ENQUIRY:UE 能力查询

UE 能力查询请求消息，由基站发往终端。查询 UE 在不同网络的接入能力。

RRC-MSG
..msg
....struDL-DCCH-Message
.....struDL-DCCH-Message
.....message
.....c1
.....ueCapabilityEnquiry//UE 能力查询
.....rrc-TransactionIdentifier --- 0x1(1)

.....criticalExtensions
.....c1
.....ueCapabilityEnquiry-r8
.....ue-CapabilityRequest//UE 能力查询的制式列表
.....RAT-Type --- eutra(0)
.....RAT-Type --- utra(1)
.....RAT-Type --- geran-cs(2)
.....RAT-Type --- geran-ps(3)
.....RAT-Type --- cdma2000-1XRTT(4)

5.2.7 RRC_UE_CAP_INFO:UE 能力信息

UE 根据前一个消息会把自己的无线接入能力上报给上层网络，并与网络 MME 中存储的能力进行比对更新，以应备后续的通信服务需求。

RRC-MSG
..msg
....struUL-DCCH-Message
.....struUL-DCCH-Message
.....message
.....c1
.....ueCapabilityInformation//UE 能力信息
.....rrc-TransactionIdentifier --- 0x1(1)
.....criticalExtensions
.....c1
.....ueCapabilityInformation-r8
.....ue-CapabilityRAT-ContainerList//UE 支持网络制式的列表，该列表中优先介绍 LTE 的支持能力，然后介绍是否包含 3G 能力，如果包含就会介绍，最后介绍包含 2G 的能力。
.....UE-CapabilityRAT-Container
.....rat-Type --- eutra(0)//系统类型---支持 EUTRAN 系统
.....ueCapabilityRAT-Container
.....ueEutraCap
.....UE-EUTRA-Capability
.....accessStratumRelease --- rel9(1)//UE 的协议版本，R8/9/10
.....ue-Category --- 0x3(3)//UE 能力等级，协议规定取值范围 1～5，一般商用终端为 CAT3(E392 等)或 CAT4(E5375)，TUE 可以支持 CAT5
.....pdcp-Parameters//PDCP 层参数
.....supportedROHC-Profiles// 支持 ROHT 协议情况。ROHC（RObust Header Compression）是一种专为无线链路设计的数据包头压缩机制，以适应无线链路高误码率和长环回时间的链路特性。一般应用于 VOIP 业务。
.....profile0x0001 --- TRUE(1)//Profile：在 ROHC 的框架下，针对不同的协议的数据流，有不同的头部压缩算法。Profile 定义了针对特定协议层数据流的

压缩方式。Profile ID 用于标识 Profile。Profile ID 为 0x0000 表示不压缩。如果信令中有这一条： maxNumberROHC-ContextSessions --- cs2(0)表示为 UE 支持的并发激活 ROHC 上下文的最大数量。CS2 表示 2 个上下文。如果终端不支持 ROHC profiles,网络侧会忽略此值。
.....profile0x0002 --- TRUE(1)
.....profile0x0003 --- FALSE(0)
.....profile0x0004 --- FALSE(0)
.....profile0x0006 --- FALSE(0)
.....profile0x0101 --- FALSE(0)
.....profile0x0102 --- FALSE(0)
.....profile0x0103 --- FALSE(0)
.....profile0x0104 --- FALSE(0)
.....phyLayerParameters//物理层参数
.....ue-TxAntennaSelectionSupported --- FALSE(0)// 该值如果为 TURE，则表示 UE 有能力支持 TS 36.213[8.7]中所描述的 UE 传输天线选择。FALSE 则表示能力不支持该传输天线选择。
.....ue-SpecificRefSigsSupported --- FALSE(0)//标识是否支持 UE 特定参考信号。该信号在天线端口 5 上传输。FALSE 表示不支持
.....rf-Parameters//RF 参数，目前只有支持的频段
.....supportedBandListEUTRA
.....SupportedBandEUTRA
.....bandEUTRA --- 0x26(38)//支持频段 38
.....halfDuplex --- FALSE(0)// 半双工标识，如果为 TURE，那么该频带仅仅支持半双工操作，否则支持全双工操作。此条消息表示支持全双工操作。
.....SupportedBandEUTRA
.....bandEUTRA --- 0x27(39) //支持频段 39
.....halfDuplex --- FALSE(0)
.....SupportedBandEUTRA
.....bandEUTRA --- 0x28(40) //支持频段 40
.....halfDuplex --- FALSE(0)
.....measParameters//测量参数
.....bandListEUTRA//条目列表，对应于每一个支持 EUTRA 频带，其排列的顺序与 supportedEUTRA-BandList.的排列顺序一样。
.....BandInfoEUTRA
.....interFreqBandList//支持异频测量的列表
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)// 表示当在 bandListEUTRA 以及在 interFreqBandList 中所给出的 E-UTRA 频带上进行测量时，是否需要测量间隔。TRUE 表示需要测量间隔。
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....interRAT-BandList//支持异系统测量的列表

.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)//异系统测量间隔，即当在 eutraBandList 中条目所给出的 E-UTRA 频带上，以及在 interRAT-BandList 中条目所给出的 interRAT 频带上进行测量时，需要的测量间隔。
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....BandInfoEUTRA
.....interFreqBandList
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....interRAT-BandList
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....BandInfoEUTRA
.....interFreqBandList
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....interRAT-BandList

.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....featureGroupIndicators ---
'01111110000011011111100010000010'B//功能组指示，每个 BIT 表示一个功能，共 32bit,具体的定义可以参考 36331 协议的 Table B.1-1: Definitions of feature group indicators
.....interRAT-Parameters//异系统支持能力
.....utraTDD128//支持互操作的 utraTDD128，也就是 TDSCDMA 频段
.....supportedBandListUTRA-TDD128
.....SupportedBandUTRA-TDD128 --- a(0)//支持 A 频段 2010~2025
.....SupportedBandUTRA-TDD128 --- f(5)//F 频段 1880~1920
.....geran//支持互操作的 GSM 频段
.....supportedBandListGERAN
.....SupportedBandGERAN --- gsm850(5)//支持 850M GSM
.....SupportedBandGERAN --- gsm900E(7)//支持 900E GSM
.....SupportedBandGERAN --- gsm1800(9)//支持 1800M GSM
.....SupportedBandGERAN --- gsm1900(10)//支持 1900M GSM
.....interRAT-PS-HO-ToGERAN --- FALSE(0)//异系统 Ps 切换到 GSM---不支持
.....nonCriticalExtension//非关键扩展参数
.....phyLayerParameters-v920 --- (0)//R9 协议新增的物理层能力参数
.....interRAT-ParametersGERAN-v920//R9 协议新增的 GERAN 异系统互操作参数
.....e-RedirectionGERAN-r9 --- supported(0)//R9 协议 e 重定向到 GSM 系统-----支持。
.....interRAT-ParametersUTRA-v920//R9 协议新增的 UTRAN 异系统互操作参数
.....e-RedirectionUTRA-r9 --- supported(0)//R9 协议 e 重定向到 UTRA 系统-----支持。

.....csg-ProximityIndicationParameters-r9 --- (0)//R9 协议新增的CSG(关闭用户组)接入指示参数。只有归属于该 CSG 的用户才允许接入该小区。目前产品不支持 CSG 小区。
.....neighCellSI-AcquisitionParameters-r9 --- (0)//邻区系统消息获得参数。
.....son-Parameters-r9 --- (0)//R9 协议新增的 SON 能力参数
.....nonCriticalExtension//非关键扩展参数
.....lateNonCriticalExtension
.....UE-EUTRA-Capability-v9a0-IEs
.....featureGroupIndRel9Add-r9 ---
'10000000000000000000000000000000'B//R9 协议增加的特征组指示版本
.....UE-CapabilityRAT-Container
.....rat-Type --- utra(1)//支持 utra 系统
.....ueCapabilityRAT-Container
.....ueRATCap ---
0x400012A8CAAB541A955AA8452A299F9E90800010002302000725571 22B64828401D4B000C694A99380
.....UE-CapabilityRAT-Container
.....rat-Type --- geran-cs(2) //支持 GSM 系统电路域
.....ueCapabilityRAT-Container
.....ueRATCap --- 0x33035758A66014046F650061E24140
.....UE-CapabilityRAT-Container
.....rat-Type --- geran-ps(3) //支持 GSM 系统 PS 域，EDGE
.....ueCapabilityRAT-Container
.....ueRATCap ---
0x1953432AA556461E40004DD8C63230F2000268C4B19187900012

5.2.8 S1AP_UE_CAPABILITY_INFO_IND:UE 能力信息指示

UE 能力上报消息，由基站发往核心网，将 RRC_UE_CAP_INFO 中的内容转发到核心网。

这条消息与上一条消息是基站透传的结果，上一条消息是 UE 向基站上报无线接入能力，这条消息是基站把 UE 的无线接入能力透传给 MME。

S1ap-Msg
..initiatingMessage
....procedureCode --- 0x16(22)
....criticality --- ignore(1)
....value
......uECapabilityInfoIndication
........protocolIEs
..........SEQUENCE
............id --- 0x0(0)

.....criticality --- reject(0)
.....value
.....mME-UE-S1AP-ID --- 0x250ff2e(38862638)
.....SEQUENCE
.....id --- 0x8(8)
.....criticality --- reject(0)
.....value
.....eNB-UE-S1AP-ID --- 0x513c35(5323829)
.....SEQUENCE
.....id --- 0x4a(74)
.....criticality --- ignore(1)
.....value
.....uERadioCapability
.....UERadioAccessCapabilityInformation//UE 无线接入能力信息。
.....criticalExtensions
.....c1
.....ueRadioAccessCapabilityInformation-r8
.....ue-RadioAccessCapabilityInfo
.....UECapabilityInformation
.....rrc-TransactionIdentifier --- 0x1(1)
.....criticalExtensions
.....c1
.....ueCapabilityInformation-r8
.....ue-CapabilityRAT-ContainerList
.....UE-CapabilityRAT-Container
.....rat-Type --- eutra(0)//支持 EUTRAN
.....ueCapabilityRAT-Container
.....ueEutraCap
.....UE-EUTRA-Capability
.....accessStratumRelease --- rel9(1)
.....ue-Category --- 0x3(3)
.....pdcp-Parameters
.....supportedROHC-Profiles
.....profile0x0001 --- TRUE(1)
.....profile0x0002 --- TRUE(1)
.....profile0x0003 --- FALSE(0)
.....profile0x0004 --- FALSE(0)
.....profile0x0006 --- FALSE(0)
.....profile0x0101 --- FALSE(0)
.....profile0x0102 --- FALSE(0)
.....profile0x0103 --- FALSE(0)
.....profile0x0104 --- FALSE(0)
.....phyLayerParameters
.....ue-TxAntennaSelectionSupported --- FALSE(0)

.....ue-SpecificRefSigsSupported --- FALSE(0)
.....rf-Parameters
.....supportedBandListEUTRA
.....SupportedBandEUTRA
.....bandEUTRA --- 0x26(38)
.....halfDuplex --- FALSE(0)
.....SupportedBandEUTRA
.....bandEUTRA --- 0x27(39)
.....halfDuplex --- FALSE(0)
.....SupportedBandEUTRA
.....bandEUTRA --- 0x28(40)
.....halfDuplex --- FALSE(0)
.....measParameters
.....bandListEUTRA
.....BandInfoEUTRA
.....interFreqBandList
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....interRAT-BandList
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....BandInfoEUTRA
.....interFreqBandList
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....interRAT-BandList

.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....BandInfoEUTRA
.....interFreqBandList
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....InterFreqBandInfo
.....interFreqNeedForGaps --- TRUE(1)
.....interRAT-BandList
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....InterRAT-BandInfo
.....interRAT-NeedForGaps --- TRUE(1)
.....featureGroupIndicators ---
'01111110000011011111100010000010'B
.....interRAT-Parameters
.....utraTDD128
.....supportedBandListUTRA-TDD128
.....SupportedBandUTRA-TDD128 --- a(0)
.....SupportedBandUTRA-TDD128 --- f(5)
.....geran
.....supportedBandListGERAN
.....SupportedBandGERAN --- gsm850(5)
.....SupportedBandGERAN --- gsm900E(7)

.....SupportedBandGERAN --- gsm1800(9)
.....SupportedBandGERAN --- gsm1900(10)
.....interRAT-PS-HO-ToGERAN --- FALSE(0)
.....nonCriticalExtension
.....phyLayerParameters-v920 --- (0)
.....interRAT-ParametersGERAN-v920
.....e-RedirectionGERAN-r9 --- supported(0)
.....interRAT-ParametersUTRA-v920
.....e-RedirectionUTRA-r9 --- supported(0)
.....csg-ProximityIndicationParameters-r9 --- (0)
.....neighCellSI-AcquisitionParameters-r9 --- (0)
.....son-Parameters-r9 --- (0)
.....nonCriticalExtension
.....lateNonCriticalExtension
.....UE-EUTRA-Capability-v9a0-IEs
.....featureGroupIndRel9Add-r9 ---
'10000000000000000000000000000000'B
.....UE-CapabilityRAT-Container
.....rat-Type --- geran-cs(2)
.....ueCapabilityRAT-Container
.....ueRATCap ---
0x33035758A66014046F650061E24140
.....UE-CapabilityRAT-Container
.....rat-Type --- geran-ps(3)
.....ueCapabilityRAT-Container
.....ueRATCap ---
0x1953432AA556461E40004DD8C63230F2000268C4B19187900012

5.2.9 RRC_SECUR_MODE_CMD:RRC 安全模式命令

安全加密及完整性算法配置消息，由基站发送给终端。之后，终端和基站将应用该算法加密 RRC 消息和上层消息；终端和核心网将应用该算法加密 NAS 消息。

RRC-MSG
..msg
....struDL-DCCH-Message
.....struDL-DCCH-Message
.....message
.....c1
.....securityModeCommand//安全模式命令
.....rrc-TransactionIdentifier --- 0x1(1)
.....criticalExtensions
.....c1

.....securityModeCommand-r8
.....securityConfigSMC
.....securityAlgorithmConfig//用于配置完整性保护（SRB）以及加密（SRB 和 DRB）
.....cipheringAlgorithm --- eea2(2)//加密算法，对 SRB 和 DRB 都有效，R9 协议规定 eea2 表示 AES 算法，eea1 表示 snow 3G 算法，eea0 表示为 NULL；R8 协议未对空算法进行定义和设置标志位。，当前采用的是 eea2.
.....integrityProtAlgorithm --- eia2(2)//完整性保护算法,仅对 SRB 生效，协议规定 eia2 表示 AES 算法，eia1 表示 snow 3G 算法。UE 协议版本 R9 是 eia0-v920 为空算法加密；R8 协议的 spare（7）为空算法加密。UE 会首先验证本条 SecurityModeCommand 消息的完整性保护。

5.2.10 RRC_CONN_RECFG:RRC 连接重配置

RRC 建立阶段的 RRC 连接重配消息，要求 UE 进行相关无线资源重配，为建立 SRB2 和 DRB。

RRC-MSG
..msg
....struDL-DCCH-Message
.....struDL-DCCH-Message
.....message
.....c1
.....rrcConnectionReconfiguration//RRC 连接重配置
.....rrc-TransactionIdentifier --- 0x1(1)
.....criticalExtensions
.....c1
.....rrcConnectionReconfiguration-r8
.....radioResourceConfigDedicated//无线资源配置专用
.....srb-ToAddModList//SRB 增加模式列表
.....SRB-ToAddMod//增加 SRB 模式
.....srb-Identity --- 0x2(2)//增加 SRB2,SRB2：用于传传 NAS 消息的，它必须在安全激活后才能被建立起来。确保信令的安全性。SRB1 是传送 RRC 信令的，在 SRB2 建立前也传 NAS 消息，SRB2 建立后 SRB1 就只用于传 RRC 信令了。重配置等消息就是在 SRB1 上传送的。
.....rlc-Config//SRB2 的 RLC 配置,这是系统定义的。
.....explicitValue
.....am//SRB 为保证信令的正确接收配置为 AM 模式
.....ul-AM-RLC//UL-AM-RLC 为针对 UE 侧的上行 RLC 配置，主要配置 RLC 数据接收侦测规则。
.....t-PollRetransmit --- ms45(8)//AM PDU 重传检测定时器时长。
.....pollPDU --- pInfinity(7)//UE 触发 Polling 的 PDU 字节数据量门限。此处配置为无限大

.....pollByte --- kBinfinity(14)//PollByte 为 AMD PDU 侦测字节数。此处配置为无限大。
.....maxRetxThreshold --- t32(7)//UE AM 模式 RLC ARQ 最大重传次数。该参数用于配置 UE，表示 RLC ARQ 最大重传次数，用于限制 AM PDU 的重传次数。达到最大重传次数时会触发 RRC 连接重建。
.....dl-AM-RLC//下行确认 RLC 模式
.....t-Reordering --- ms35(7)//UE AM 模式接收端重排序定时器。该参数用于配置 UE，表示 AM 模式接收端重排序定时器的大小。
.....t-StatusProhibit --- ms0(0)//UE 禁止发送状态报告定时器。该参数用于配置 UE，表示 AM 模式接收端禁止发送状态报告的定时器大小。即在本时长内不允许上报状态报告。
.....logicalChannelConfig//SRB2 的逻辑信道配置
.....explicitValue
.....ul-SpecificParameters//以下消息的字段定义请参阅 RRC 建立请求消息中 SRB1 的建立过程。
.....priority --- 0x3(3)//SRB2 优先级
.....prioritisedBitRate --- infinity(7)//SRB2 逻辑信道优先速率
.....bucketSizeDuration --- ms300(3)// SRB2 bucket size 调整持续时间
.....logicalChannelGroup --- 0x0(0)//SRB2 逻辑信道组
.....drb-ToAddModList//DRB 增加模式列表
.....DRB-ToAddMod//增加 DRB
.....eps-BearerIdentity --- 0x5(5)//由 MME 分配，端到端的承载，EPS 承载 ID 为 5
.....drb-Identity --- 0x1(1)//DRB 的 ID,由 eNB 分配，无线侧数据承载
.....pdcp-Config//PDCP 层配置
.....discardTimer --- infinity(7)//PDCP 层丢弃定时器,根据 QCI 的不同，设置值不同，比如 QCI6/8/9 是无限长、QCI2/7 是 150ms。此处为无限大
.....rlc-AM//保证数据的可靠传输，采用确认模式
.....statusReportRequired --- TRUE(1)//AM 模式切换时 PDCP 状态报告反馈指示。如果配置为 False，目标 eNodeB 将传输所有源 eNodeB 转发的数据，其中某些数据 UE 可能已收到，造成空口资源的浪费。如果为 TRUE 需要发一个状态报告。
.....headerCompression//头压缩
.....notUsed --- (0)//头压缩，一般只在 VoIP、视频类的业务中才会根据 eNB 侧的配置决定是否启用。该值默认关闭。
.....rlc-Config//RLC 配置
.....am//确认模式
.....ul-AM-RLC//上行 RLC 确认模式，针对 UE 侧的配置
.....t-PollRetransmit --- ms40(7)//UE Polling PDU 重传定时器大小。该定时器设置过小会触发过多的 Polling PDU，且连续多次触发 PDU 重传使 ARQ 重传达到最大次数，从而导致 RRC 重建；设置过大会导致状态报告不能及时的反馈。40ms(QCI4/5/6/8/9)
.....pollPDU --- p32(3)//UE 触发 Polling 的 PDU 字节数据量门限。表示触发 Polling 的 PDU 数据量门限。当 PDU 发送数据量达到该值时，将在 PDU 头部设

置 Poll 标志位。(满足个数或字节数其中一个条件就会启动 POLL 机制)。该参数是发送端为了防止等待确认队列太长导致缓冲区溢出，根据发送 PDU 的数据量主动触发状态报告。取值过小可能增加 Polling PDU 的触发次数；取值过大则缓冲占用越大，且会减慢发送窗的移动。QCI4/6/8/9 为 2 万 5 千字节；QCI5 为无限长

.....pollByte --- kB25(0)//PollByte 为 AMD PDU 侦测字节数。QCI4/6/8/9 为 32PDU；QCI5 为无限长

.....maxRetxThreshold --- t32(7)//UE AM 模式 RLC ARQ 最大重传次数。该参数用于配置 UE，表示 RLC ARQ 最大重传次数，用于限制 AM PDU 的重传次数。达到最大重传次数时会触发 RRC 连接重建。32(QCI4/5/6/8/9)

.....dl-AM-RLC//为针对 UE 侧的下行 RLC 配置，主要配置 RLC 数据接收状态上报规则。

.....t-Reordering --- ms50(10)//UE AM 模式接收端重排序定时器。如果该定时器配置较小，则导致发送端无效的 HARQ 重传及接收端触发重复的状态报告，浪费资源；如果配置过大，则导致接收端判断乱序包传输失败延时较大，不能及时的触发状态报告，从而造成业务延时和吞吐量下降。默认 50ms

.....t-StatusProhibit --- ms50(10)//UE 禁止发送状态报告定时器。即在本时长内不允许上报状态报告。该定时器影响 AM 模式下状态报告的发送。如果状态报告发送不频繁，可以减少状态报告的频繁调度，但容易导致发送端发送窗口为 0，降低发送速率；如发送频繁，则可以保证发送端发送窗口数据及时得到确认，保证发送速率，但容易导致数据状态报告的频繁调度和重复发送，浪费资源。默认值 50ms

.....logicalChannelIdentity --- 0x3(3)//逻辑信道 ID

.....logicalChannelConfig//DRB 逻辑信道配置

.....ul-SpecificParameters

.....priority --- 0x9(9)//逻辑信道优先级。UE 调度器按逻辑信道优先级由高到低依次保证逻辑信道的优先速率；所有业务优先速率保证后，按逻辑信道优先级由高到低分配资源，仅在 QCI 为 6、7、8、9 时该参数有效。取值范围 9~16，默认值 QCI6：9；QCI7：10；QCI8：11；QCI9：12

.....prioritisedBitRate --- kBps8(1)//逻辑信道优先速率。UE 调度器按逻辑信道优先级由高到低保证逻辑信道的优先速率，仅在 QCI 为 2、3、4、6、7、8、9 时有效。PBR_8_KBps(8 千字节/秒)

.....bucketSizeDuration --- ms300(3)//bucket size 调整持续时间

.....logicalChannelGroup --- 0x3(3)//逻辑信道组.CCCH、SRB1、SRB2 默认属于 LCG 0；RRC 消息在 SRB 上传输且 SRB 默认属于 LCG 0，比 LCG 2 的优先级要高。

.....physicalConfigDedicated//物理信道配置专用，此过程与 RRC 建立消息里相似，以下字段大家可以参看前面的消息，此不复述。

.....cqi-ReportConfig

.....cqi-ReportModeAperiodic --- rm30(3)//CQI 不定期上报模式，如果 CQI 周期自适应开关打开，则采用周期自适应相关配置。

.....nomPDSCH-RS-EPRE-Offset --- 0x0(0)

.....cqi-ReportPeriodic

.....setup

.....cqi-PUCCH-ResourceIndex --- 0x6(6)//CQI-PUCCH 资源索引

.....cqi-pmi-ConfigIndex --- 0x17(23)//CQI-PMI 配置索引,确定上报

周期 NP 和偏移量 NOFFSET.
.....cqi-FormatIndicatorPeriodic
.....widebandCQI --- (0)// 宽度 CQI。CQI 测量是针对 k 个连续的 PRB（即子带）进行的。如果在所有子带内反馈一个 CQI 值，则称为宽带 CQI；如果对每一个子带反馈不同的 CQI 值，称为子带反馈。
.....simultaneousAckNackAndCQI --- TRUE(1)//确认非确认及 CQI 是否同时，PUCCH CQI 反馈类型，取决于传输模式。FALSE 为不同时。
.....antennaInfo//天线信息
.....explicitValue
.....transmissionMode --- tm2(1)
.....ue-TransmitAntennaSelection//终端 UE 传输天线选择，Setup 或 release。Setup 表示开环或者闭环。
.....release --- (0)
.....schedulingRequestConfig//调度请求配置
.....setup
.....sr-PUCCH-ResourceIndex --- 0x2(2)// sr-PUCCH 资源索引
.....sr-ConfigIndex --- 0x11(17)// SR 配置索引参数 Isr
.....dsr-TransMax --- n64(4)// SR 传输最大次数，当超过最大次数时，通知 RRC 释放 PUCCH/SRS，发起一次随机接入过程。本消息表明最大次数为 64 次。

5.2.11 RRC_SECUR_MODE_CMP:RRC 安全模式完成

安全加密及完整性配置完成

RRC-MSG
..msg
....struUL-DCCH-Message
......struUL-DCCH-Message
.....message
.....c1
.....securityModeComplete
.....rrc-TransactionIdentifier --- 0x1(1)
.....criticalExtensions
.....securityModeComplete-r8 --- (0)

5.2.12 RRC_CONN_RECFG_CMP:RRC 连接重配置完成

RRC 连接重配完成消息与连接重配置消息是一对对存在的，总是对应前一个重配消息。信令中没有重配失败消息，如果重配失败，则直接发起 RRC 连接重建。该消息表示建立 SRB2 和 DRB 已完成。

RRC-MSG
..msg
....struUL-DCCH-Message
......struUL-DCCH-Message
........message
..........c1
............rrcConnectionReconfigurationComplete//RRC 连接重配置完成
..............rrc-TransactionIdentifier --- 0x1(1)
..............criticalExtensions
................rrcConnectionReconfigurationComplete-r8 --- (0)

5.2.13 S1AP_INITIAL_CONTEXT_SETUP_RSP:初始化文本建立完成

初始上下文建立成功响应，如果文本建立失败可能的原因，从大类上分为无线、传输、NAS、协议、其他。

S1ap-Msg
..successfulOutcome
....procedureCode --- 0x9(9)
....criticality --- reject(0)
....value
......initialContextSetupResponse//初始文本建立响应
........protocolIEs
..........SEQUENCE
............id --- 0x0(0)
............criticality --- ignore(1)
............value
..............mME-UE-S1AP-ID --- 0x250ff2e(38862638)//MME 侧用户标识
..........SEQUENCE
............id --- 0x8(8)
............criticality --- ignore(1)
............value
..............eNB-UE-S1AP-ID --- 0x513c35(5323829)//enb 侧用户标识
..........SEQUENCE
............id --- 0x33(51)
............criticality --- ignore(1)
............value
..............e-RABSetupListCtxtSURes
................SEQUENCE
..................id --- 0x32(50)
..................criticality --- ignore(1)
..................value
....................e-RABSetupItemCtxtSURes

.....e-RAB-ID --- 0x5(5)//ERAB ID 为 5.
.....transportLayerAddress ---
'01100100010110110000000100000010'B
.....gTP-TEID --- 0x00003723//此处的 GTP-TEID 为下行 GTP-TEID

5.2.14 S1AP_ERAB_MOD_REQ:ERAB 修改请求

对比初始文本建立时的承载 ,此处承载修改请求变更的内容是承载分配资源的优先级发生了改变 , 以前是“priorityLevel --- 0x6(6)”, 现在更改为“priorityLevel --- highest(1)”。

S1ap-Msg
..initiatingMessage
....procedureCode --- 0x6(6)
....criticality --- reject(0)
....value
......e-RABModifyRequest
.....protocolIEs
.....SEQUENCE
.....id --- 0x0(0)
.....criticality --- reject(0)
.....value
.....mME-UE-S1AP-ID --- 0x250ff2e(38862638)
.....SEQUENCE
.....id --- 0x8(8)
.....criticality --- reject(0)
.....value
.....eNB-UE-S1AP-ID --- 0x513c35(5323829)
.....SEQUENCE
.....id --- 0x1e(30)
.....criticality --- reject(0)
.....value
.....e-RABToBeModifiedListBearerModReq
.....SEQUENCE
.....id --- 0x24(36)
.....criticality --- reject(0)
.....value
.....e-RABToBeModifiedItemBearerModReq
.....e-RAB-ID --- 0x5(5)
.....e-RABLevelQoSParameters
.....qCI --- 0x6(6)
.....allocationRetentionPriority

.....priorityLevel --- highest(1)//优先级最高
.....pre-emptionCapability --- shall-not-trigger-pre-emption(0)
.....pre-emptionVulnerability --- pre-emptable(1)
.....nAS-PDU
.....NAS-MESSAGE//NAS 消息
.....security-protected-and-ciphered-NAS-message//安全保护和加密 NAS 消息
.....protected-nas ---
0x2624558B07E228660B86640CD8C0173419340702F1C55F6EF4B76E6997F121EA514F078FB372EC8E18//保护的 NAS 内容

5.2.15 RRC_DL_INFO_TRANSF:RRC 下行直传消息

目的：传送 NAS 消息

RRC-MSG
..msg
....struDL-DCCH-Message
.....struDL-DCCH-Message
.....message
.....c1
.....dlInformationTransfer
.....rrc-TransactionIdentifier --- 0x2(2)
.....criticalExtensions
.....c1
.....dlInformationTransfer-r8
.....dedicatedInfoType
.....dedicatedInfoNAS ---
0x272624558B07E228660B86640CD8C0173419340702F1C55F6EF4B76E6997F121EA514F078FB372EC8E18//NAS 消息专用

5.2.16 S1AP_ERAB_MOD_RSP:ERAB 修改完成

该条消息表示 ERAB 模式修改已经得到 MME 的认可，并完成修改，承载的优先级发生了变更。

S1ap-Msg
..successfulOutcome
....procedureCode --- 0x6(6)
....criticality --- reject(0)
....value
.....e-RABModifyResponse

.....protocolIEs
.....SEQUENCE
.....id --- 0x0(0)
.....criticality --- ignore(1)
.....value
.....mME-UE-S1AP-ID --- 0x250ff2e(38862638)
.....SEQUENCE
.....id --- 0x8(8)
.....criticality --- ignore(1)
.....value
.....eNB-UE-S1AP-ID --- 0x513c35(5323829)
.....SEQUENCE
.....id --- 0x1f(31)
.....criticality --- ignore(1)
.....value
.....e-RABModifyListBearerModRes
.....SEQUENCE
.....id --- 0x25(37)
.....criticality --- ignore(1)
.....value
.....e-RABModifyItemBearerModRes
.....e-RAB-ID --- 0x5(5)

5.2.17 RRC_CONN_RECFG:RRC 连接重配置

RRC-MSG
..msg
....struDL-DCCH-Message
.....struDL-DCCH-Message
.....message
.....c1
.....rrcConnectionReconfiguration//RRC 连接重配置
.....rrc-TransactionIdentifier --- 0x3(3)
.....criticalExtensions
.....c1
.....rrcConnectionReconfiguration-r8
.....measConfig//测量配置
.....measObjectToAddModList
.....MeasObjectToAddMod
.....measObjectId --- 0x1(1)
.....measObject
.....measObjectEUTRA//目标系统：EUTRA eNodeB 只下发 UE 能力

支持测量的目标系统，UE 能力不支持测量的目标系统，则不进行对应系统的测量。
.....carrierFreq --- 0x940c(37900)//测量频点(若与当前服务频点相同，则为同频测量对象，否则为异频测量对象。若携带有异频点测量对象，则测量控制中会携带有 GAP 周期的配置)。eNodeB 根据选择的测量目标系统，从相应配置的邻区列表中获取测量频点。
.....allowedMeasBandwidth --- mbw100(5)//测量带宽，同频时可不配置，默认为本小区带宽，以 RB 数来标识。异频时必须配置。
.....presenceAntennaPort1 --- FALSE(0)//用于指示是否所有邻近的小区使用天线端口 1。设置为 true 时，UE 可以假定至少两个特殊小区天线端口用于所有邻近的小区。
.....neighCellConfig --- '01'B//同频邻区配置信息。00: 表示部分邻区具有相同的 MBSFN 子帧配置；01: 表示所有邻区不具有 MBSFN 子帧配置；10: 所有邻区的 MBSFN 子帧配置与服务小区相同或为子集；11: TDD 服务小区具有不同上下行配比的邻区
.....offsetFreq --- dB0(15)//频率偏置
.....cellsToAddModList//增加的测量小区:主要作用就是配置小区偏移，小区偏移在做测量评估时使用。对于 UE 测量到的，但邻区列表中又没有指示的小区，UE 默认该小区的小区偏移为 0。对于 UE 测量到的任何小区，无论是否存在于邻区列表中，LTE 协议要求 UE 都需要进行评估、上报处理。因此对于 E-UTRAN 来说，只有当对应小区的 CIO 不为默认值（0dB）时，eNodeB 才下发对应的测量小区，否则不下发测量小区。
.....CellsToAddMod
.....cellIndex --- 0x1(1)
.....physCellId --- 0x1(1)//PCI=1
.....cellIndividualOffset --- dB0(15)//CIO 小区偏移量。用于控制同频/异频测量事件发生的难易程度，该值越大，越容易触发测量报告和切换，提高切换次数。设置过大或过小都会降低切换成功率。
.....reportConfigToAddModList
.....ReportConfigToAddMod
.....reportConfigId --- 0x1(1)//报告配置 ID，每个报告配置由相应的报告配置 Id 来唯一标识
.....reportConfig
.....reportConfigEUTRA
.....triggerType//触发类型
.....event
.....eventId
.....eventA3//A3 事件，同频切换

事件类型	触发含义	使用场景	白话表达
A1	服务小区高于门限	取消异频/异系统的 GAP 测量	我信号很好
A2	服务小区低于门限	启动异频/异系统的 GAP 测量	我信号不行了
A3	邻区比服务小区好	触发同频/同优先级异频切换	别人比我好

A4	异频邻区高于门限	触发高优先级异频切换	别人信号很好
A5	异频邻区高于门限且服务小区低于门限	触发低优先级异频切换	我信号不行了，别人很好
B1	RAT 邻区高于门限	触发高优先级 RAT 切换	别人（异系统）信号很好
B2	RAT 邻区高于门限且服务小区低于门限	触发低优先级 RAT 切换	我信号不行了，别人（异系统）很好

事件	A1	A2	A3	A4	A5	B1	B2
同频	-	-	判决切换	-	-	-	-
异频	停止测量	启动测量	-	判决切换	-	-	-
异系统	停止测量	启动测量	-	-	-	判决切换	-

A5、B2 事件类型目前华为设备没有应用

.....a3-Offset --- 0x2(2)//A3 事件的偏置，单位 0.5Db,2 为 1dB

.....reportOnLeave --- FALSE(0)//指示小区触发列表里的小区满足触发条件时是否应启动 UE 的测量报告程序。

.....hysteresis --- 0x2(2)//A3 事件的幅度迟滞，单位 0.5dB，默认 1Db,2 表示 1dB。

.....timeToTrigger --- ms320(8)//A3 事件的时间迟滞（ms0~ms5120），默认 320ms

.....triggerQuantity --- rsrp(0)//A3 测量触发类型,分 RSRP/RSRQ，默认 RSRP

.....reportQuantity --- sameAsTriggerQuantity(0)//A3 切换事件触发后上报类型。A3 事件（同频或异频）触发后上报类型，可配置为与 A3 测量触发类型相同，或者 RSRP 和 RSRQ 都上报。

.....maxReportCells --- 0x4(4)//最大上报小区数（1~8）。系统内同频、异频切换事件测量或快速 ANR 周期测量触发上报时，允许上报的最大小区数。默认为 4

.....reportInterval --- ms240(1)//周期上报两条测量报告的间隔（ms120~min60,离散取值）。对于同频测量,按照协议当前 UE 实现为物理层按照 200ms 的周期进行周期性上报。

.....reportAmount --- infinity(7)//同频或者异频切换事件触发后周期上报测量报告的次数.Infinity(无限)

.....ReportConfigToAddMod

.....reportConfigId --- 0x2(2)//报告配置 ID 2

.....reportConfig

.....reportConfigEUTRA

.....triggerType

.....event

.....eventId

.....eventA1//A1 事件，取消异频测量事件

.....a1-Threshold

.....threshold-RSRP --- 0x23(35)//异频切换测量的 A1 事件的 RSRP 触发门限。如果 RSRP 测量值超过该触发门限,将上报测量报告。增大门限 Thresh，将增加 A1 事件触发的难度，即延缓停止异频测量。根据不同的切换算法，可以有不同的配

置。
.....hysteresis --- 0x2(2)//异频 A1A2 幅度迟滞,默认 1dB（2）
.....timeToTrigger --- ms640(11)//异频 A1A2 时间迟滞,默认 640ms
.....triggerQuantity --- rsrp(0)//触发类型--RSRP
.....reportQuantity --- both(1)//上报类型，RSRP 和 RSRQ 都上报
.....maxReportCells --- 0x1(1)//最大上报小区数（1~8）。
.....reportInterval --- ms480(2)//周期上报两条测量报告的间隔
.....reportAmount --- r1(0)//同频或者异频切换事件触发后周期上报测量报告的次数
.....ReportConfigToAddMod
.....reportConfigId --- 0x3(3)//报告配置 ID 3
.....reportConfig
.....reportConfigEUTRA
.....triggerType//触发类型
.....event
.....eventId
.....eventA2//事件类型 2,启动异频测量。（A1A2 测量触发类型）
.....a2-Threshold
.....threshold-RSRP --- 0x1f(31)//异频切换的 A2 事件的 RSRP 触发门限。如果 RSRP 测量值低于触发门限，将上报测量报告。减小门限 Thresh，将增加 A2 事件触发的难度，即延缓启动异频测量。根据不同的切换算法，可以有不同的配置。
.....hysteresis --- 0x2(2)//异频 A1A2 幅度迟滞
.....timeToTrigger --- ms640(11)//异频 A1A2 时间迟滞
.....triggerQuantity --- rsrp(0)//触发类型
.....reportQuantity --- both(1)//上报类型
.....maxReportCells --- 0x1(1)//最多上报小区数。该参数减小，则减少切换候选小区数目，减少每次测量报告触发的切换的成功率，但是节省了空口资源。反之亦然。默认值为 4
.....reportInterval --- ms480(2)//周期上报两条测量报告的间隔
.....reportAmount --- r1(0)//同频或者异频切换事件触发后周期上报测量报告的次数
.....ReportConfigToAddMod
.....reportConfigId --- 0x4(4)//报告配置 ID 4
.....reportConfig
.....reportConfigEUTRA
.....triggerType//触发类型
.....event
.....eventId
.....eventA2//A2 事件，与上一个 A2 有差异，此处应该为基于频率优先级的 A1A2 测量触发类型
.....a2-Threshold
.....threshold-RSRP --- 0x13(19)

.....hysteresis --- 0x2(2)
.....timeToTrigger --- ms640(11)
.....triggerQuantity --- rsrp(0)
.....reportQuantity --- both(1)
.....maxReportCells --- 0x1(1)
.....reportInterval --- ms480(2)//周期上报两条测量报告的间隔
.....reportAmount --- r1(0)//同频或者异频切换事件触发后周期上报测量报告的次数
.....measIdToAddModList//增加的测量列表
.....MeasIdToAddMod
.....measId --- 0x1(1) //ID 1
.....measObjectId --- 0x1(1)
.....reportConfigId --- 0x1(1)
.....MeasIdToAddMod
.....measId --- 0x2(2) //ID 2
.....measObjectId --- 0x1(1)
.....reportConfigId --- 0x2(2)
.....MeasIdToAddMod
.....measId --- 0x3(3) //ID 3
.....measObjectId --- 0x1(1)
.....reportConfigId --- 0x3(3)
.....MeasIdToAddMod
.....measId --- 0x4(4) //ID 4
.....measObjectId --- 0x1(1)
.....reportConfigId --- 0x4(4)
.....quantityConfig//数量配置
.....quantityConfigEUTRA
.....filterCoefficientRSRP --- fc6(6)//RSRP 高层滤波系数，即 L3 滤波系数，L3 滤波公式如下：Fn = (1-a)•Fn-1 + a•Mn 其中，Fn：第 n 个滤波后的测量值；Fn-1：第 n-1 个滤波后的测量值；Mn：从物理层接收到的第 n 个测量值；
a= 1 / (2 的(k/4)次幂)，是当前测量量的一个权重系数。k 就是对应的 L3 滤波系数。当 k 为 0，即 a=1 时，则不进行 L3 滤波。从上述算法可以看出，RSRP 高层滤波系数对切换性能会有较大影响：RSRP 高层滤波系数越大，对信号平滑作用越强，抗快衰落能力越强，但对信号变化的跟踪能力变弱，可能出现切换不及时导致掉话；该值设置过小，会增加不必要的切换以及乒乓切换。默认值 FC6
.....filterCoefficientRSRQ --- fc6(6)//RSRQ 高层滤波系数
.....s-Measure --- 0x0(0)//物理小区质量阈值控制 UE 是否在同频、异频和异系统邻区间执行测量。值“0”表示禁止的措施。
.....speedStatePars
.....release --- (0)

5.2.18 RRC_UL_INFO_TRANSF:RRC 上行直传消息

目的：传送上行 NAS 消息，这是 RRC 层（空口）跟踪的消息内容

RRC-MSG
..msg
....struUL-DCCH-Message
......struUL-DCCH-Message
........message
..........c1
............ulInformationTransfer
..............criticalExtensions
................c1
..................ulInformationTransfer-r8
....................dedicatedInfoType
......................dedicatedInfoNAS --- 0x2750ABAE001EDC0342//NAS 消息专用

5.2.19 S1AP_UL_NAS_TRANS:上行 NAS 直传消息

直传 NAS 消息，这是基站透传 UE 消息给 MME，S1 接口跟踪的消息内容

S1ap-Msg
..initiatingMessage
....procedureCode --- 0xd(13)
....criticality --- ignore(1)
....value
......uplinkNASTransport
........protocolIEs
..........SEQUENCE
............id --- 0x0(0)
............criticality --- reject(0)
............value
..............mME-UE-S1AP-ID --- 0x250ff2e(38862638)
..........SEQUENCE
............id --- 0x8(8)
............criticality --- reject(0)
............value
..............eNB-UE-S1AP-ID --- 0x513c35(5323829)
..........SEQUENCE
............id --- 0x1a(26)
............criticality --- reject(0)
............value
..............nAS-PDU
................NAS-MESSAGE

.....security-protected-and-ciphered-NAS-message//安全保护和加密 NAS 消息
.....protected-nas --- 0x50ABAE001EDC0342
.....SEQUENCE
.....id --- 0x64(100)
.....criticality --- ignore(1)
.....value
.....eUTRAN-CGI
.....pLMNidentity --- 0x64F000//PLMN ID 460 00
.....cell-ID --- '10001001000000110001000111111'B//服务小区的 ECI
.....SEQUENCE
.....id --- 0x43(67)
.....criticality --- ignore(1)
.....value
.....tAI
.....pLMNidentity --- 0x64F000
.....tAC --- 0x890A//服务小区的 TAC

5.2.20 RRC_CONN_RECFG_CMP:RRC 连接重配置完成

该条消息是针对上面的连接重配命令的反馈和确认。

RRC-MSG
..msg
....struUL-DCCH-Message
.....struUL-DCCH-Message
.....message
.....c1
.....rrcConnectionReconfigurationComplete
.....rrc-TransactionIdentifier --- 0x3(3)
.....criticalExtensions
.....rrcConnectionReconfigurationComplete-r8 --- (0)

5.2.21 RRC_CONN_RECFG:RRC 连接重配置

RRC-MSG
..msg
....struDL-DCCH-Message
.....struDL-DCCH-Message
.....message
.....c1

.....rrcConnectionReconfiguration//RRC 连接重配置
.....rrc-TransactionIdentifier --- 0x0(0)
.....criticalExtensions
.....c1
.....rrcConnectionReconfiguration-r8
.....radioResourceConfigDedicated
.....mac-MainConfig
.....explicitValue
.....drx-Config//不连续接收配置
.....setup
.....onDurationTimer --- psf4(3)//DRX 持续时间定时器，单位 PDCCH 子帧，DRX 状态下的激活时长
.....drx-InactivityTimer --- psf3(2)//DRX 非激活定时器，单位 PDCCH 子帧，UE 连续无调度时间超过该定时器后才会进入 DRX 状态
.....drx-RetransmissionTimer --- psf8(4)//DRX 等待重传数据的定时器的长度。超过该定时器后，UE 尚未接收到重传数据，即进入休眠期。
.....longDRX-CycleStartOffset
.....sf40 --- 0x1b(27)//针对 ANR 测量的 DRX 长周期时，为了保证 CGI 的读取成功率，建议配置大于等于 256ms 的 DRX 长周期，且配置 DRX 长周期越大，则 CGI 读取时延就越大，对系统时延的影响也越大。
.....shortDRX
.....shortDRX-Cycle --- sf5(1)//该参数表示 DRX 短周期长度。由于受 SRS 带宽及 TimeAlignmentTimer(TA 周期)的约束，配置给 UE 的 LongDrxCycle 值可能小于对应的 MML 配置值，以及协议上规定的 DRX 长周期必须为 DRX 的短周期整数倍的约束，则配置给 UE 的 ShortDrxCycle 值可能小于界面配置值。当其他 DRX 参数固定时，该参数配置的越小，则 UE 耗电量会越高，但会减少系统时延；该参数配置的越大，则 UE 耗电量会越低，但会增加系统时延。
.....drxShortCycleTimer --- 0x8(8)//DRX 短周期定时器。该参数表示短周期 DRX 的生命周期。值为 1，对应 1 * shortDRX-Cycle；值为 2，对应 2 * shortDRX-Cycle。当该参数设置的比较长时，UE 在配置了短周期 DRX 的情况下，处于短周期 DRX 的时间就会比较长。该参数设置不同会影响 DRX 操作机制，但不是影响 DRX 操作机制的唯一参数，以下各种 DRX 参数组合共同影响 DRX 操作机制：LongDrxCycle、OnDurationTimer、DrxInactivityTimer、ShortDrxCycle、DrxShortCycleTimer、DrxReTxTimer。当其他 DRX 参数固定时，该参数配置的越小，则 UE 耗电量会越低，但会增加系统时延；该参数配置的越大，则 UE 耗电量会越高，但会减少系统时延。
.....timeAlignmentTimerDedicated --- sf1920(3)//上行时间对齐定时器，该参数表示 UE 上行时间对齐的定时器长度，该定时器超时，则认为 UE 上行失步。取值范围：SF500(500 个子帧)，SF750(750 个子帧)，SF1280(1280 个子帧)，SF1920(1920 个子帧)，SF2560(2560 个子帧)，SF5120(5120 个子帧)，SF10240(10240 个子帧)，INFINITY(无穷大)
.....physicalConfigDedicated//物理信道配置指示
.....cqi-ReportConfig
.....cqi-ReportModeAperiodic --- rm30(3)
.....nomPDSCH-RS-EPRE-Offset --- 0x0(0)

.....cqi-ReportPeriodic
.....setup
.....cqi-PUCCH-ResourceIndex --- 0x6(6)//CQI-PUCCH 资源索引
.....cqi-pmi-ConfigIndex --- 0x17(23)//CQI-PMI 配置索引，确定上报周期 NP 和偏移量 NOFFSET.
.....cqi-FormatIndicatorPeriodic
.....widebandCQI --- (0)// 宽度 CQI。CQI 测量是针对 k 个连续的 PRB（即子带）进行的。如果在所有子带内反馈一个 CQI 值，则称为宽带 CQI；如果对每一个子带反馈不同的 CQI 值，称为子带反馈。
.....simultaneousAckNackAndCQI --- FALSE(0)//确认非确认及 CQI 是否同时，PUCCH CQI 反馈类型，取决于传输模式。FALSE 为不同时。

5.2.22 RRC_CONN_RECFG_CMP:RRC 连接重配置完成

RRC-MSG
..msg
....struUL-DCCH-Message
.....struUL-DCCH-Message
.....message
.....c1
.....rrcConnectionReconfigurationComplete//RRC 连接重配置完成消息
.....rrc-TransactionIdentifier --- 0x0(0)
.....criticalExtensions
.....rrcConnectionReconfigurationComplete-r8 --- (0)

5.2.23 RRC_MEAS_RPRT:RRC 测量报告

测量报告消息。终端上报给源小区，消息中携带测量事件 ID、本小区信号质量、邻小区信号质量。

RRC-MSG
..msg
....struUL-DCCH-Message
.....struUL-DCCH-Message
.....message
.....c1
.....measurementReport//测量报告消息
.....criticalExtensions

.....c1
.....measurementReport-r8
.....measResults
.....measId --- 0x2(2)//测量事件 ID
.....measResultPCell//本小区信号质量
.....rsrpResult --- 0x46(70)
.....rsrqResult --- 0x1b(27)
.....measResultNeighCells//邻小区测量（这里只列了一个，实际可能多个）
.....measResultListEUTRA
.....MeasResultEUTRA
.....physCellId --- 0x2d(45)//邻小区的 PCI
.....measResult
.....rsrpResult --- 0x18(24)//邻小区信号质量 RSRP,实际值=上报值-140，单位 dBm。 本例中 24-140=-116dbm

5.2.24 RRC_UL_INFO_TRANSF:RRC 上行信息传输

传输 NAS 消息

RRC-MSG
..msg
....struUL-DCCH-Message
.....struUL-DCCH-Message
.....message
.....c1
.....ulInformationTransfer
.....criticalExtensions
.....c1
.....ulInformationTransfer-r8
.....dedicatedInfoType
.....dedicatedInfoNAS --- 0x27EB0985D51F74DAA820FC0CF0B473AE9D5BFE

5.2.25 S1AP_UL_NAS_TRANS:上行 NAS 信息传输

S1 接口跟踪得到的消息，传输 NAS 消息

S1ap-Msg
..initiatingMessage
....procedureCode --- 0xd(13)
....criticality --- ignore(1)
....value
.....uplinkNASTransport

.....protocolIEs
.....SEQUENCE
.....id --- 0x0(0)
.....criticality --- reject(0)
.....value
.....mME-UE-S1AP-ID --- 0x250ff2e(38862638)
.....SEQUENCE
.....id --- 0x8(8)
.....criticality --- reject(0)
.....value
.....eNB-UE-S1AP-ID --- 0x513c35(5323829)
.....SEQUENCE
.....id --- 0x1a(26)
.....criticality --- reject(0)
.....value
.....nAS-PDU
.....NAS-MESSAGE
.....security-protected-and-ciphered-NAS-message
.....protected-nas ---
0xEB0985D51F74DAA820FC0CF0B473AE9D5BFE
.....SEQUENCE
.....id --- 0x64(100)
.....criticality --- ignore(1)
.....value
.....eUTRAN-CGI
.....pLMNidentity --- 0x64F000
.....cell-ID --- '100010010000001100010001111 1'B
.....SEQUENCE
.....id --- 0x43(67)
.....criticality --- ignore(1)
.....value
.....tAI
.....pLMNidentity --- 0x64F000
.....tAC --- 0x890A

5.2.26 S1AP_UE_CONTEXT_MOD_REQ:UE 文本更改请求

此时文本更改请求的目的是为了拨打电话，这是 S1 接口跟踪到的 CSFB 开始流程。

S1ap-Msg
..initiatingMessage
....procedureCode --- 0x15(21)
....criticality --- reject(0)
....value

……uEContextModificationRequest
……..protocolIEs
……..SEQUENCE
……..id --- 0x0(0)
……..criticality --- reject(0)
……..value
……..mME-UE-S1AP-ID --- 0x250ff2e(38862638)
……..SEQUENCE
……..id --- 0x8(8)
……..criticality --- reject(0)
……..value
……..eNB-UE-S1AP-ID --- 0x513c35(5323829)
……..SEQUENCE
……..id --- 0x6c(108)
……..criticality --- reject(0)
……..value
……..cSFallbackIndicator --- cs-fallback-required(0)//此时为 CSFB 拨打电话的请求

5.2.27 S1AP_UE_CONTEXT_MOD_RSP:UE 文本更改响应

核心网接到 CSFB 的请求后进行文本更改应答。接收 CSFB 请求。随后进行的过程应该为

RRC 连接释放，文本释放，然后回落到 CS 域进行拨打电话。

S1ap-Msg
..successfulOutcome
….procedureCode --- 0x15(21)
….criticality --- reject(0)
….value
……uEContextModificationResponse
……..protocolIEs
……..SEQUENCE
……..id --- 0x0(0)
……..criticality --- ignore(1)
……..value
……..mME-UE-S1AP-ID --- 0x250ff2e(38862638)
……..SEQUENCE
……..id --- 0x8(8)
……..criticality --- ignore(1)
……..value
……..eNB-UE-S1AP-ID --- 0x513c35(5323829)

5.2.28 RRC_CONN_REL:RRC 连接释放

释放 RRC 连接消息，携带了 RRC 释放原因值，如果是 CSFB 呼叫，还会携带重定向信息。

（RIM 流程要求）

RRC-MSG
..msg
....struDL-DCCH-Message
......struDL-DCCH-Message
........message
..........c1
............rrcConnectionRelease//RRC 连接释放消息
..............rrc-TransactionIdentifier --- 0x0(0)
..............criticalExtensions
................c1
..................rrcConnectionRelease-r8//RRC 连接释放
....................releaseCause --- other(1)//RRC 连接释放原因包含 loadBalancingTAUrequired,other, cs-FallbackHighPriority, spare1
....................redirectedCarrierInfo//重定向携带的信息
......................geran//gsm 信息
........................startingARFCN --- 0x28(40)//开始启测频点
........................bandIndicator --- dcs1800(0)//频段指示
........................followingARFCNs
..........................explicitListOfARFCNs//测量频点列表
............................ARFCN-ValueGERAN --- 0x3d(61)
............................ARFCN-ValueGERAN --- 0x3c(60)
............................ARFCN-ValueGERAN --- 0x3b(59)
............................ARFCN-ValueGERAN --- 0x3a(58)
............................ARFCN-ValueGERAN --- 0x39(57)
............................ARFCN-ValueGERAN --- 0x38(56)
............................ARFCN-ValueGERAN --- 0x37(55)
............................ARFCN-ValueGERAN --- 0x36(54)
............................ARFCN-ValueGERAN --- 0x35(53)
............................ARFCN-ValueGERAN --- 0x34(52)
............................ARFCN-ValueGERAN --- 0x33(51)
............................ARFCN-ValueGERAN --- 0x32(50)
............................ARFCN-ValueGERAN --- 0x31(49)
............................ARFCN-ValueGERAN --- 0x30(48)
............................ARFCN-ValueGERAN --- 0x2f(47)
............................ARFCN-ValueGERAN --- 0x2e(46)
............................ARFCN-ValueGERAN --- 0x2d(45)
............................ARFCN-ValueGERAN --- 0x2c(44)
............................ARFCN-ValueGERAN --- 0x2b(43)

.....ARFCN-ValueGERAN --- 0x2a(42)
.....ARFCN-ValueGERAN --- 0x29(41)

5.2.29 S1AP_UE_CONTEXT_REL_REQ:UE 文本释放请求

文本释放请求消息，这条消息与上一条消息位置上可能有前后不同的地方，都是有 ENB 发出，RRC 连接释放发送到 UE，文本释放发送到 MME。

S1ap-Msg
..initiatingMessage
....procedureCode --- 0x12(18)
....criticality --- ignore(1)
....value
......uEContextReleaseRequest
........protocolIEs
.........SEQUENCE
...........id --- 0x0(0)
...........criticality --- reject(0)
...........value
.............mME-UE-S1AP-ID --- 0x250ff2e(38862638)
.........SEQUENCE
...........id --- 0x8(8)
...........criticality --- reject(0)
...........value
.............eNB-UE-S1AP-ID --- 0x513c35(5323829)
.........SEQUENCE
...........id --- 0x2(2)
...........criticality --- ignore(1)
...........value
.............cause
...............radioNetwork --- ue-not-available-for-ps-service(24)//UE 数据业务服务不可用，这条消息与 UE 的终端类型也有关系，本次不可用不是由于 UE 不支持，而是在做 CS 业务。常见释放原因 Normal Release”，“Detach”，“User Inactivity”，“CS Fallback triggered”，“UE Not Available for PS Service”，“Inter-RAT Redirection”，“Time Critical Handover”，“Handover Cancelled，详细原因见协议 36413-9.2.1.3

5.2.30 S1AP_UE_CONTEXT_REL_CMD:UE 文本释放命令

核心网收到基站侧发送的文本释放请求消息后进行确认，并返回释放文本的命令，返回值中携带释放原因（文本释放请求中的原因值）

S1ap-Msg
..initiatingMessage
....procedureCode --- 0x17(23)
....criticality --- reject(0)
....value
......uEContextReleaseCommand
........protocolIEs
..........SEQUENCE
............id --- 0x63(99)
............criticality --- reject(0)
............value
..............uE-S1AP-IDs
................uE-S1AP-ID-pair
..................mME-UE-S1AP-ID --- 0x250ff2e(38862638)
..................eNB-UE-S1AP-ID --- 0x513c35(5323829)
..........SEQUENCE
............id --- 0x2(2)
............criticality --- ignore(1)
............value
..............cause
................radioNetwork --- ue-not-available-for-ps-service(24)//携带文本释放请求中的原因值

5.2.31 S1AP_UE_CONTEXT_REL_CMP:UE 文本释放完成

UE 收到本文释放命令后,执行文本释放。

S1ap-Msg
..successfulOutcome
....procedureCode --- 0x17(23)
....criticality --- reject(0)
....value
......uEContextReleaseComplete
........protocolIEs
..........SEQUENCE
............id --- 0x0(0)
............criticality --- ignore(1)
............value
..............mME-UE-S1AP-ID --- 0x250ff2e(38862638)//S1 信令都会携带此信元。
..........SEQUENCE
............id --- 0x8(8)
............criticality --- ignore(1)
............value
..............eNB-UE-S1AP-ID --- 0x513c35(5323829) //S1 信令都会携带此信元。