# LTE基础LTE信令流程解析

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中重要的信令流程，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，将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 。

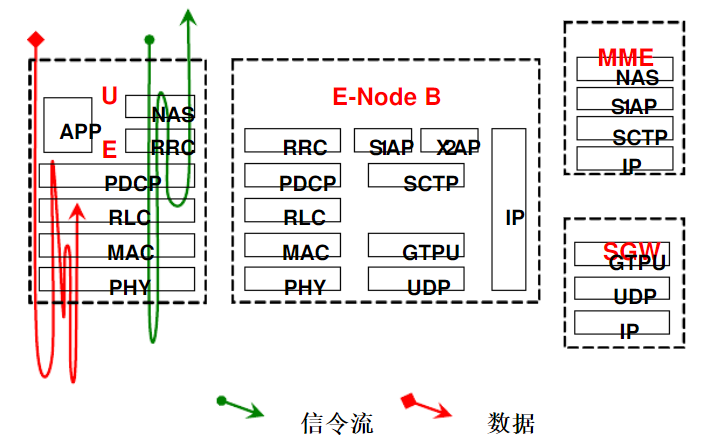


图1 子层、协议栈与流



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 PCC H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 |
|  |  |

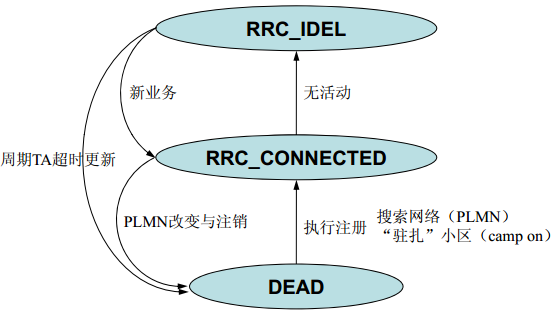


图3 状态的转换过程

## 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。

UE ID: 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。

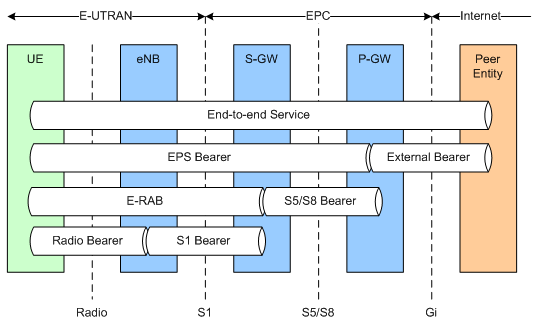


图4 承载的位置关系

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：



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：

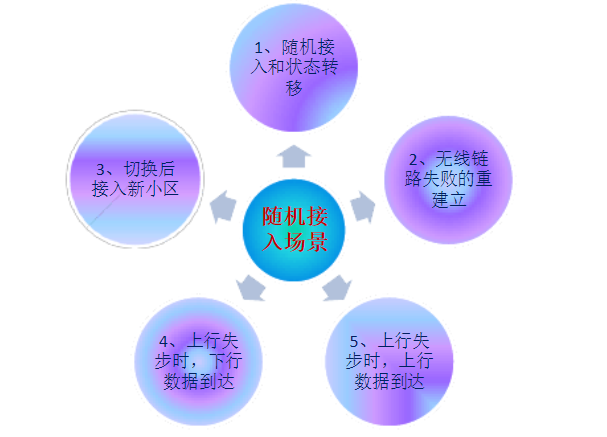


图6 随机接入场景

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M SG 2后，在其分配的上行资源上传输MSG3

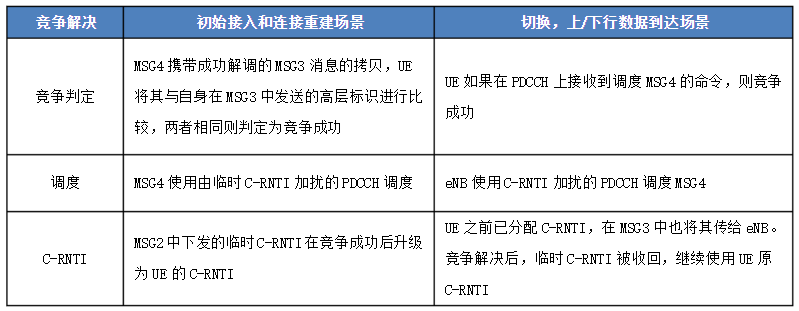
 针对不同的场景，Msg3包含不同的内容:

● 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；



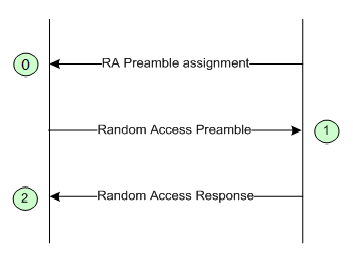


图8 基于非竞争的随机接入

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 I nitial 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。

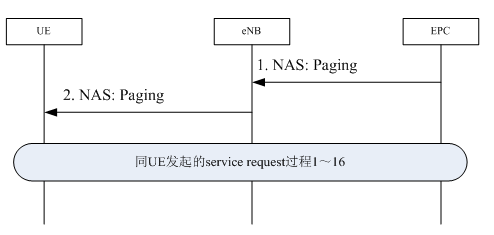


图10 寻呼流程

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 。

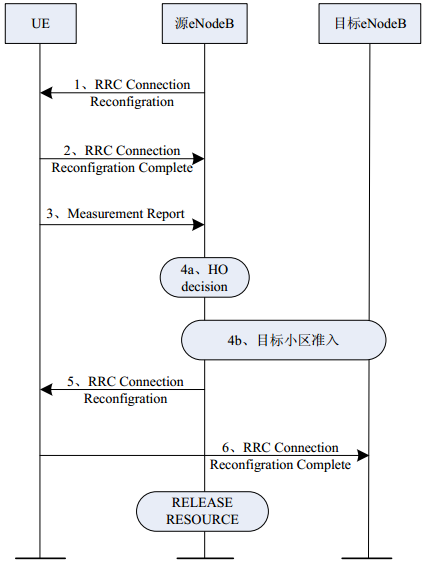


图11 站内切换流程

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 。

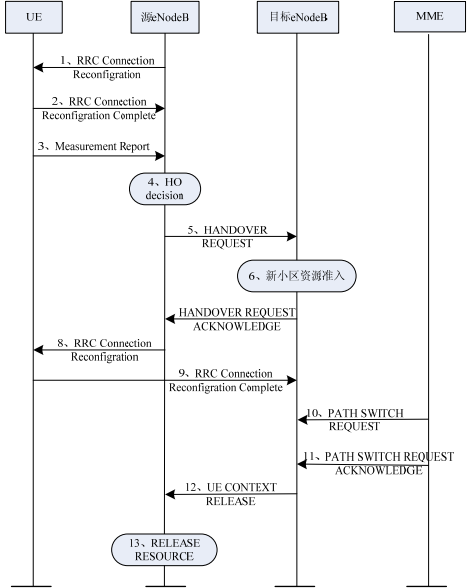


图1 2 X2 切换流程

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。

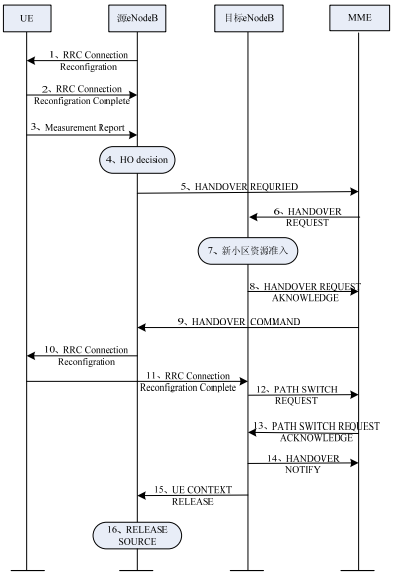


图1 3 S1 切换流程

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 SWITCH REQUEST 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， V oIP 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

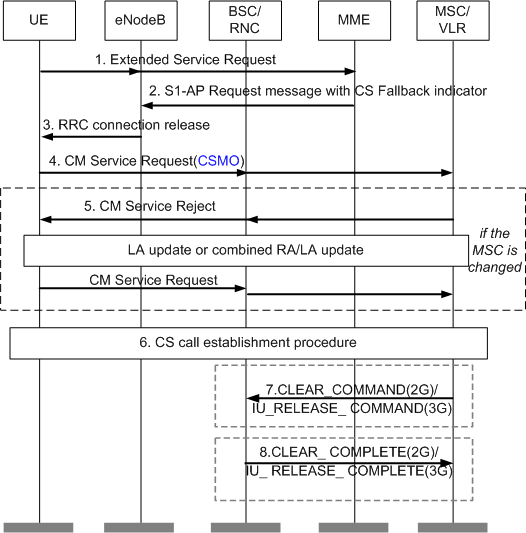


图14 主叫CSFB流程

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FastR e turn （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。

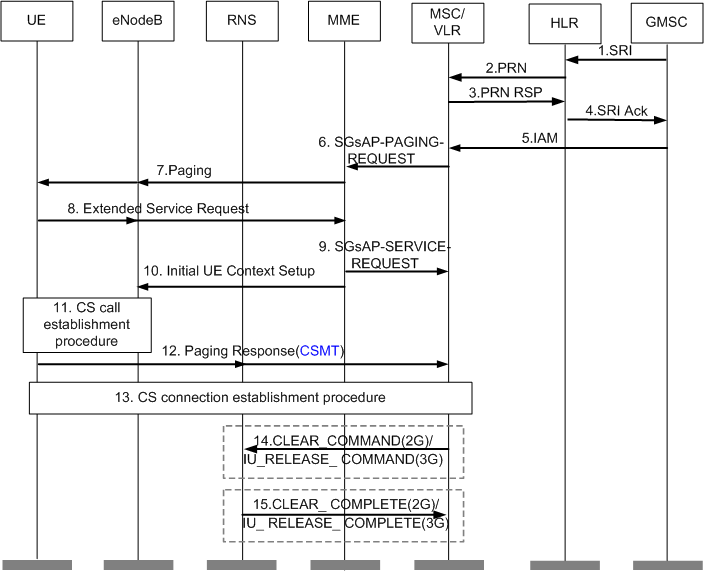


图15 被叫CSFB流程

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。

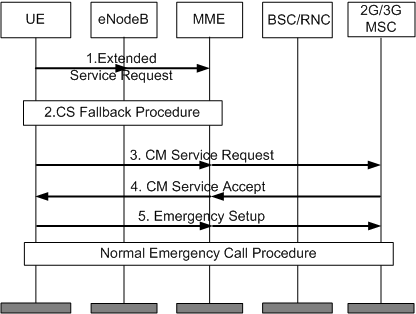


图1 6 LTE网络紧急呼 叫流程

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1 7 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1 8 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1 9 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2 1 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S 1 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2 2 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2 3 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2 4 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2 5 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。

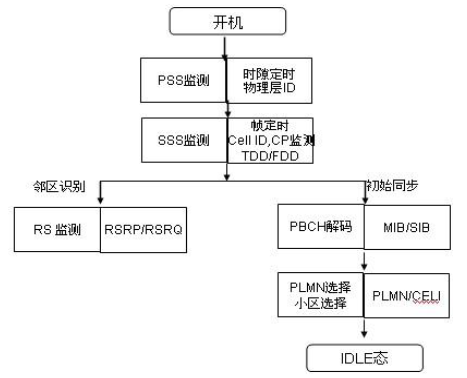


图 26 小区搜索 流程 图

### 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。

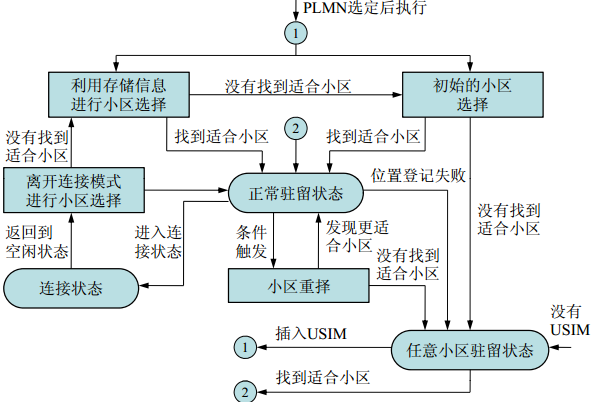


图 27 小区选择 流程 图

### 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

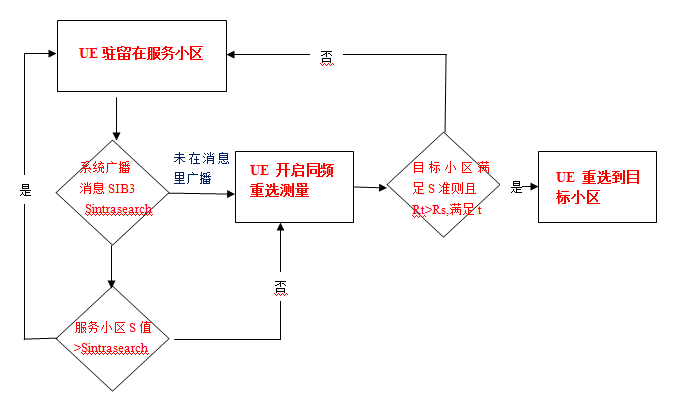


图28同频/同优先级重选流程

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

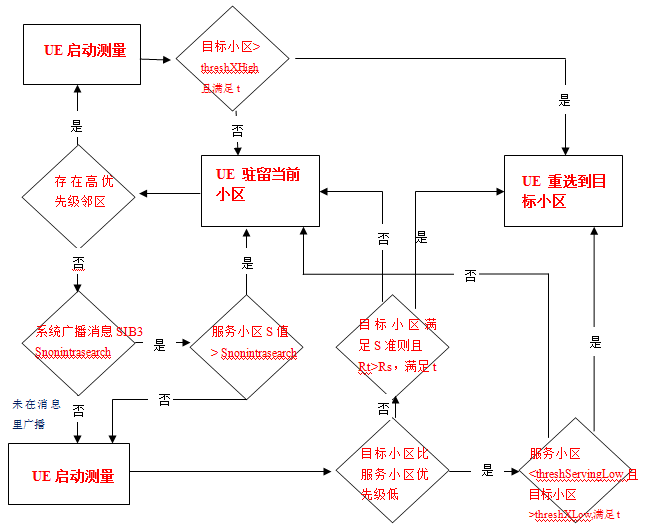


图2 9 同频/同优先级重选流程

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3 4 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 RRC Connection Reconfiguration 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 RRC Connection Reconfiguration 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3 5 eNB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3 6 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3 7 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3 8 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3 9 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。

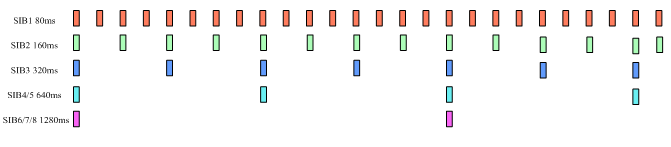
 SIB9:Home eNodeB的名称。

 SIB10:ETWS主信息（primary notification）。

 SIB11:ETWS辅信息（secondary notification）。

 SIB12:CMAS信息（CMAS notification）。

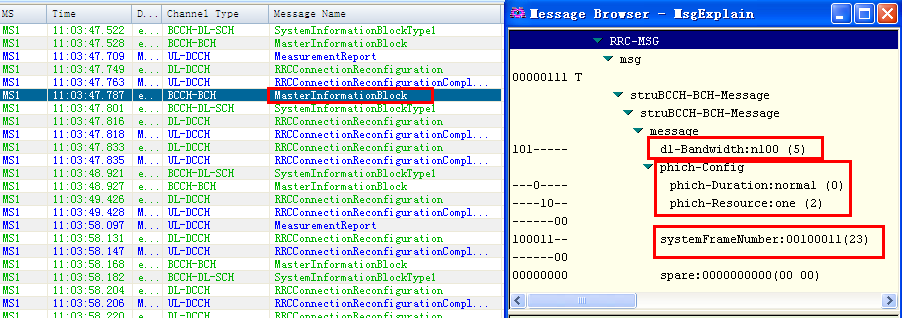
 SIB13:请求获取跟一个或多个MBSFN区域相关的MBMS控制信息的信息。



## 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。

 S pare：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:1000100100000101010100001010(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。 S f 10 表示 10 个子帧的长度。响应窗起点与Msg1间隔 10 ms【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 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 , 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 ，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 ，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 ，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 3 bit 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 deltaF 3

..............................deltaF-PUCCH-Format2:deltaF1 (2) // {deltaF-2, deltaF0, deltaF1, deltaF2} ，2表示 deltaF 1

..............................deltaF-PUCCH-Format2a:deltaF2 (2) // {deltaF-2, deltaF0, deltaF2} ，2表示 deltaF 2

..............................deltaF-PUCCH-Format2b:deltaF2 (2) // {deltaF-2, deltaF0, deltaF2} ，2表示 deltaF 2

............................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 | ERA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，侧该值为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) // SRB1 bucket 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) // CQ I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 --- '1000100100000011000100011111'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 --- '1010010111011111110000001000001000110101000111000101011010011000001111111110101011001101010101110010001101011100010000001101010001111011011101011010101111011001100111110010010011001110100100111011110111101000100100101000001000111110011100111101100000111111'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

..............handoverRestrictionLis t //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3 9

....................................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 UT RAN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 --- 0x400012A8CAAB541A955AA8452A299F9E9080001000230200072557122B64828401D4B000C694A99380

......................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) // SRB 2 逻辑信道优先速率

................................bucketSizeDuration --- ms300(3) // SRB 2 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I sr

............................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0.5 Db ,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1 Db ,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 --- '1000100100000011000100011111'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2 4 -140=-11 6 dbm

### 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 --- '1000100100000011000100011111'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。