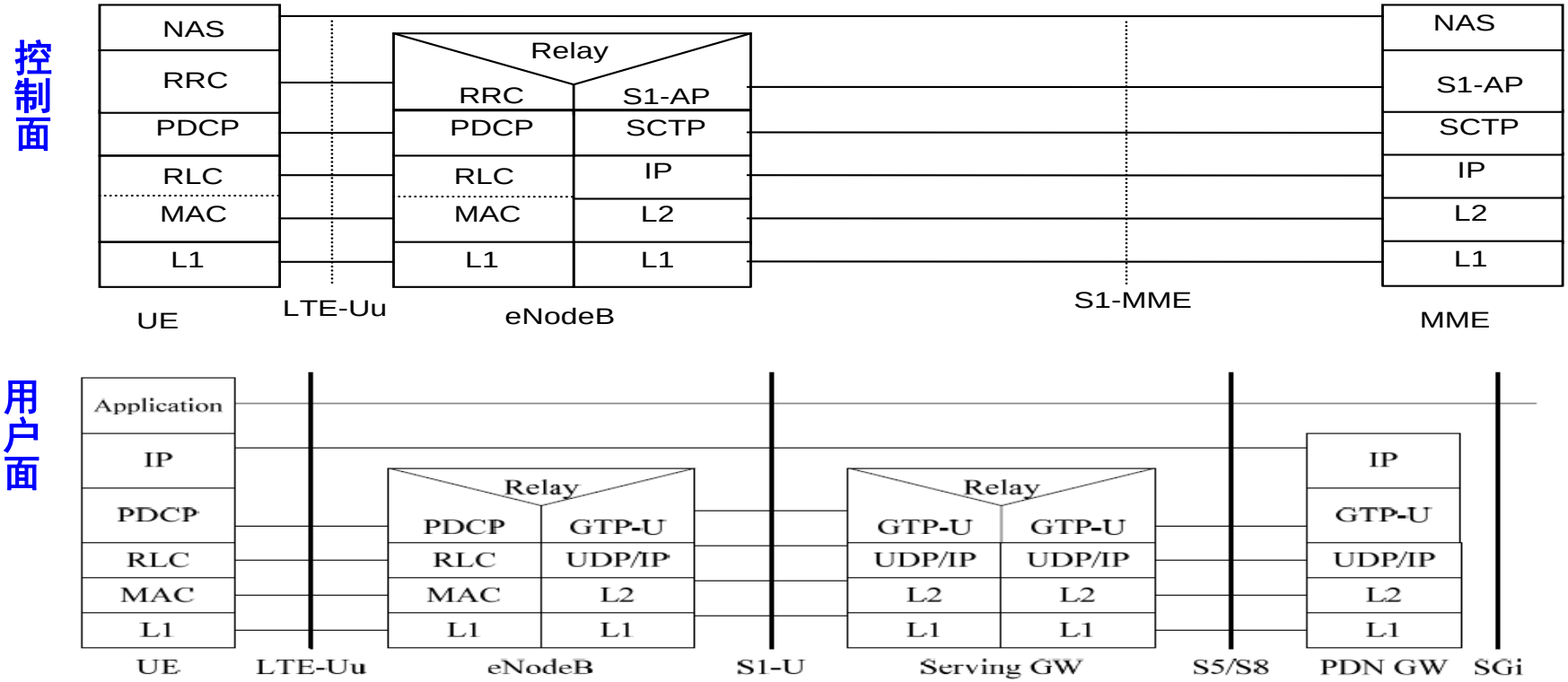
TDD LTE信令流程与分析

www.huawei.com

HUAWEI

目录

网元间控制面整体协议栈



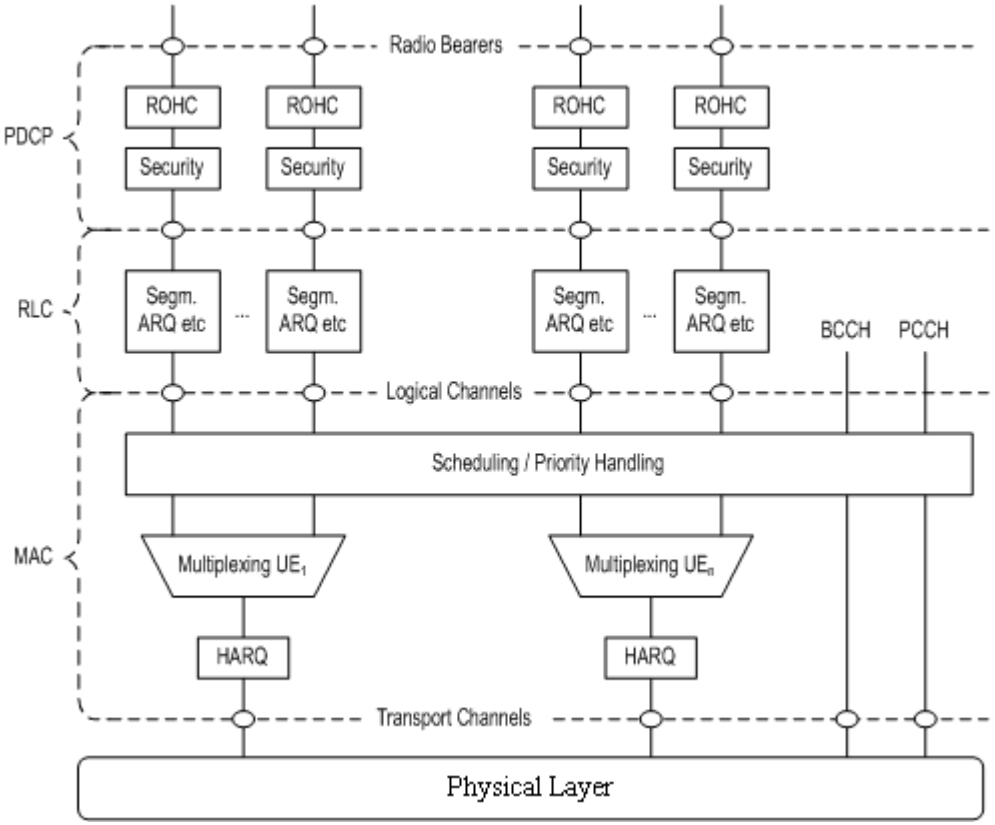
控制面协议栈

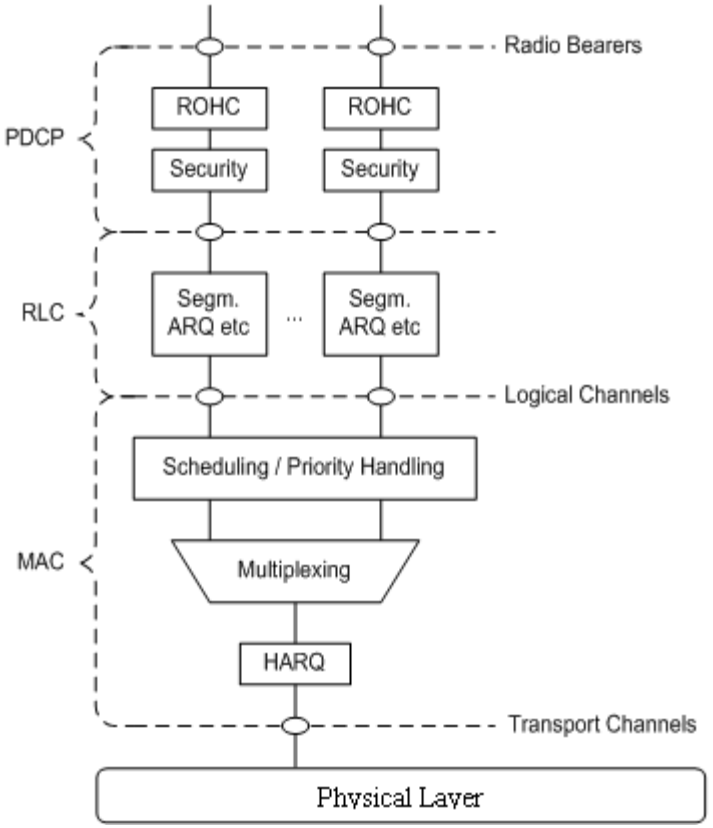
- 没有RNC，空中接口的控制平面（RRC）功能由eNB进行管理和控制

用户面协议栈

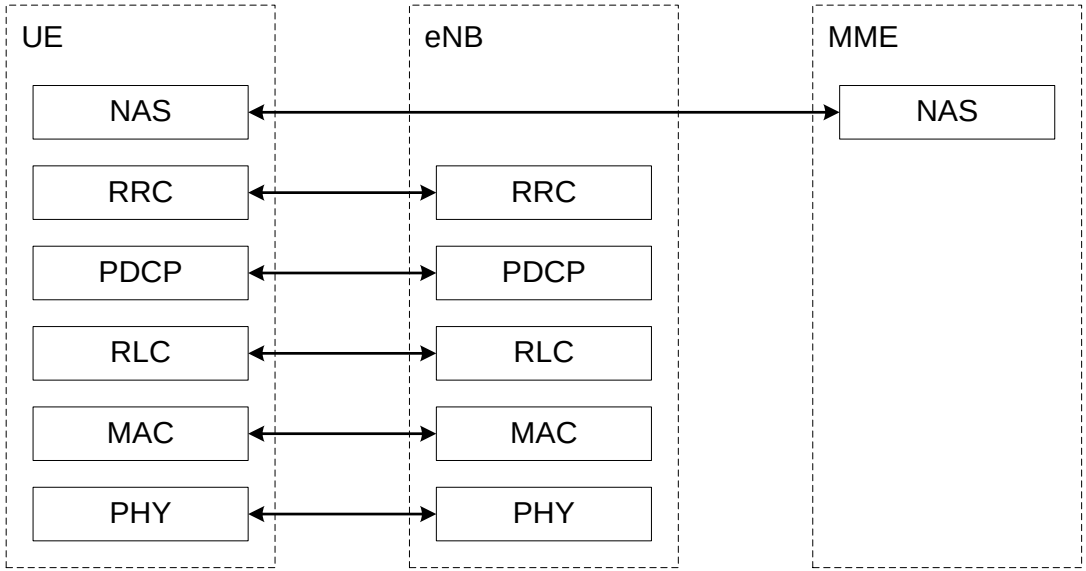
- 用户面和控制面协议栈均包含PHY,MAC,RLC和PDCP层，控制面向上还包含RRC层和NAS层
- 没有了RNC，空中接口的用户平面（MAC/RLC）功能由eNB进行管理和控制

用户面协议内部的关系


Radio Bearers
PDCP
ROHC
ROHC
ROHC
ROHC
Security
Security
Security
Security
RLC
Segm. ARQ etc
Segm. ARQ etc
Segm. ARQ etc
Segm. ARQ etc
BCCH
PCCH
Logical Channels
Scheduling / Priority Handling
MAC
Multiplexing UE1
Multiplexing UEn
HARQ
HARQ
Transport Channels
Physical Layer


Radio Bearers
PDCP
ROHC
ROHC
Security
Security
RLC
Segm. ARQ etc
Segm. ARQ etc
Logical Channels
Scheduling / Priority Handling
MAC
Multiplexing
HARQ
Transport Channels
Physical Layer

Uu口控制面协议栈



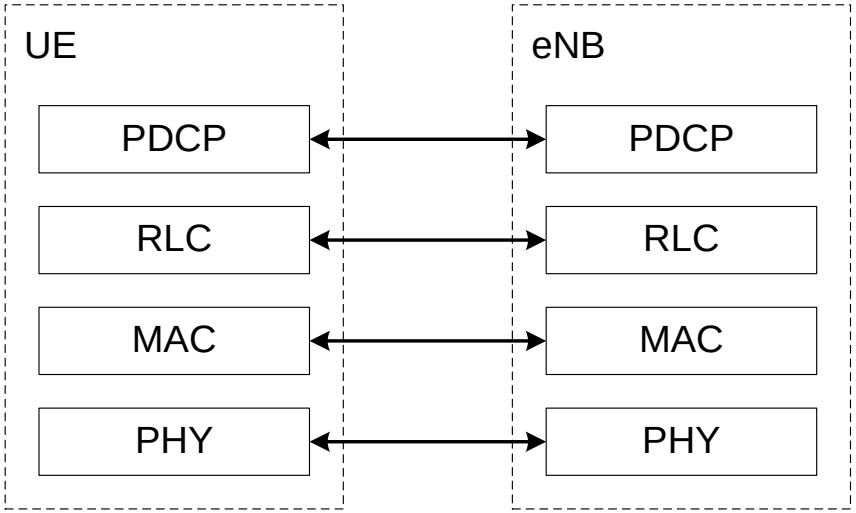
LTE控制面

- 控制平面RRC协议数据的加解密和完整性保护功能，在LTE中交由PDCP层完成
- RRC子层主要承担广播、无线接口寻呼、RRC连接管理、无线承载控制、移动性管理、UE测量上报和控制等功能
- 仅存在一个MAC实体

与3G的异同

- 3G中控制平面不存在PDCP协议栈，由RLC层提供无线信令承载SRB
- RLC层依然提供TM/UM /AM三种传输模式
- 3G中UM/AM传输模式下的加密由RLC层实现，TM模式 下的加密由MAC层实现
- 3G中含有多个MAC实体：MAC-b, MAC-c/sh, MAC-d, MAC-hs

Uu口用户面协议栈



LTE用户面

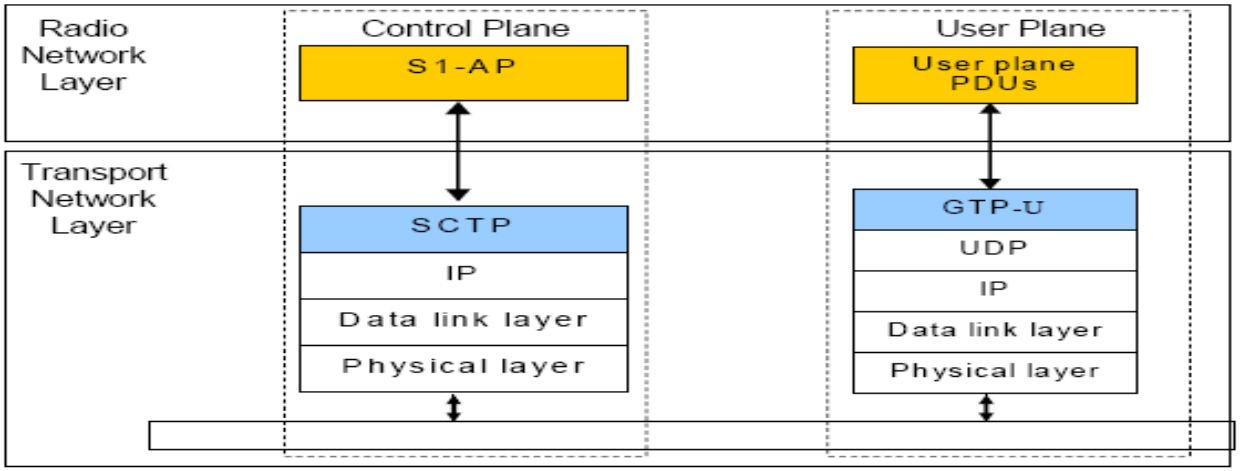
- 安全方面的功能，用户面的加密和解密功能由PDCP子层完成
- 仅存在一个MAC实体

与3G的异同

- 3G中PDCP层仅用于承载PS业务，广播和多播业务由BMC层协议承载
- 3G中用户数据的加密和解密由RLC和MAC层完成
- 3G中含有多个MAC实体：MAC-b, MAC-c/sh, MAC-d, MAC-hs
- RLC层依然提供TM/UM /AM三种传输模式

S1接口协议栈

S1接口

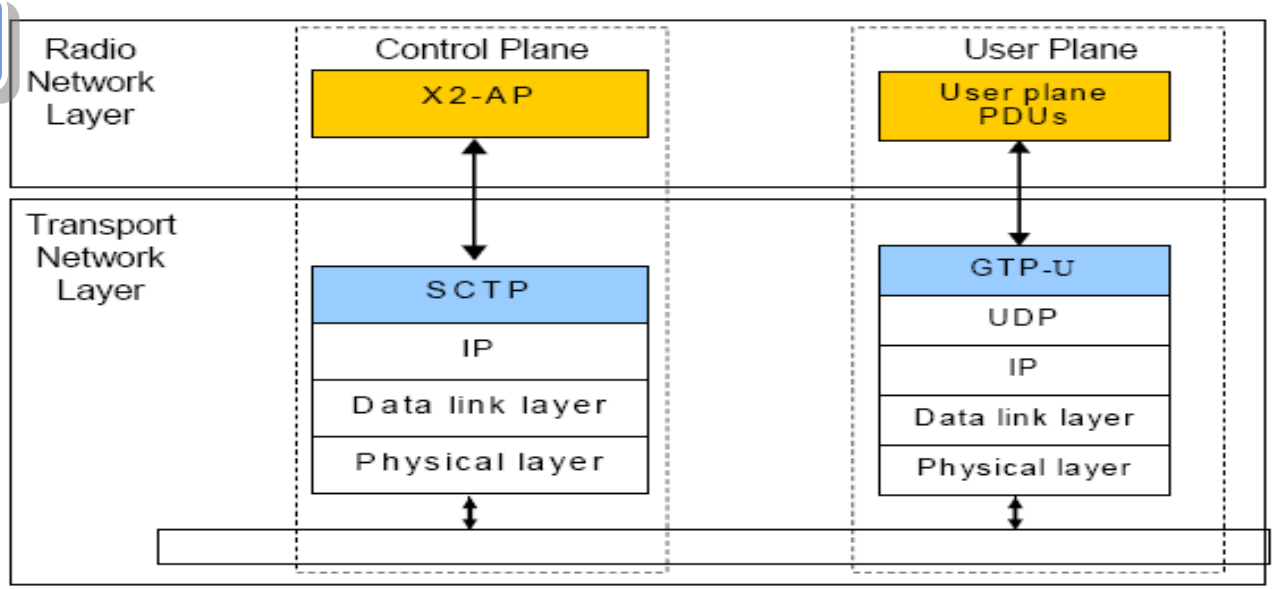


- 控制层为了可靠的传输信令消息，在IP层之上添加了SCTP
- S1控制面主要功能：
  - EPC承载服务管理功能；
  - S1 接口UE上下文释放功能；
  - ACTIVE状态下UE的移动性管理功能
  - S1接口的寻呼；
  - NAS信令传输功能；
  - 漫游于区域限制支持功能；
  - NAS节点选择功能；
  - 初始上下文建立过程；

- UDP/IP之上的GTP-U用来传输S-GW与eNB之间的用户平面PDU
- S1用户面主要功能为：
  - 在S1接口目标节点中指示数据分组所属的SAE接入承载；
  - 移动性过程中尽量减少数据的丢失；
  - 错误处理机制；
  - MBMS支持功能；
  - 分组丢失检测机制；

X2接口协议栈

X2接口



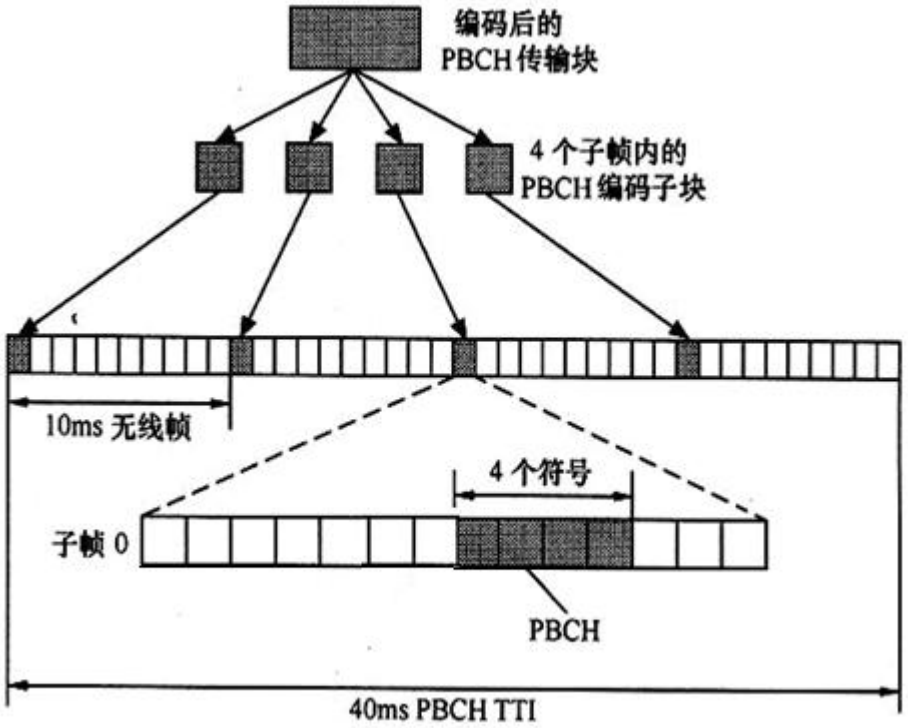
- LTE系统X2接口的定义采用了与S1接口一致的原则
- X2接口应用层协议主要功能：
  - 支持LTE_ACTIVE状态下UE的LTE接入系统内的移动性管理功能；
  - X2接口自身的管理功能，如错误指示、X2接口的建立与复位，更新X2接口配置数据等；
  - 负荷管理功能。

- X2接口用户面提供eNB之间的用户数据传输功能
- X2-U接口协议栈与S1-U接口协议栈完全相同

系统消息（36.331）

LTE系统消息

- **系统消息的组成**
  - MasterInformationBlock(MIB)
  - 多个SystemInformationBlocks (SIBs)
- **MIB**
  - 承载于BCCH → BCH → P-BCH上
  - 包括有限个用以读取其他小区信息的最重要、最常用的传输参数（系统带宽，系统帧号，PHICH配置信息）
  - 时域：在第一个子帧的第二个时隙的前4个符号，以10ms为周期重传4次
  - 频域：位于系统带宽中央的72个子载波



系统消息（36.331）

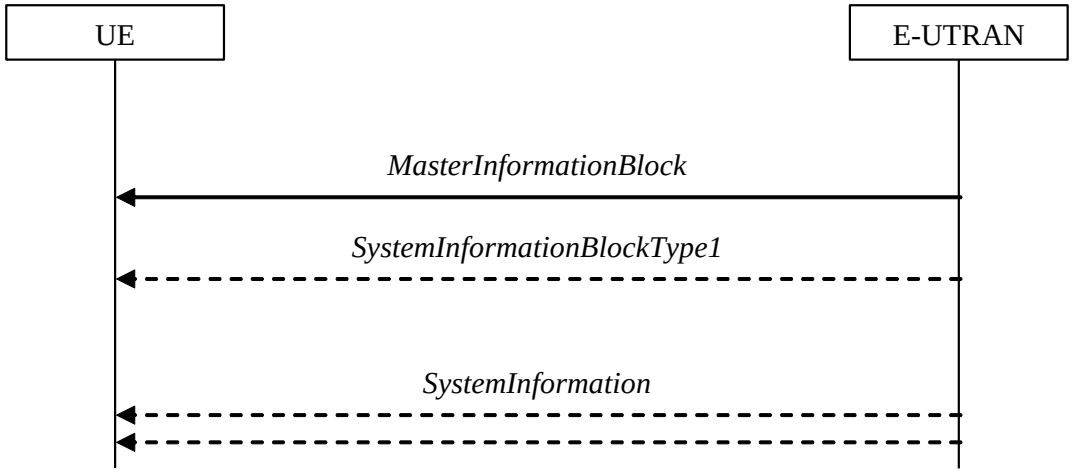
LTE系统消息

- SIBs
  - 除MIB以外的系统消息，包括SIB1-SIB12
  - 除SIB1以外，SIB2-SIB12均由SI (System Information)承载
  - SIB1是除MIB外最重要的系统消息，固定以20ms为周期重传4次，即SIB1在每两个无线帧（20ms）的子帧#5中重传（SFN mod 2 = 0，SFN mod 8 ≠ 0）一次，如果满足SFN mod 8 = 0时，SIB1的内容可能改变，新传一次。
  - SIB1和所有SI消息均传输在BCCH → DL-SCH → PDSCH上
  - SIB1的传输通过携带SI-RNTI（SI-RNTI每个小区都是相同的）的PDCCH调度完成
  - SIB1中的SchedulingInfoList携带所有SI的调度信息，接收SIB1以后，即可接收其他SI消息

各系统消息作用


SystemInformation
系统消息功能说明
MIB
主消息块包括有限个最重要、最常用的传输参数，其需要从该小区中获得其它的信息
SIB1
SIB1 包含了其他 SIB 的调度信息以及其他小区接入的相关信息
SI
SystemInformation (SI)消息中承载的是 SIB，而不是 SystemInformationBlockType1
SIBs
SIB2
SIB2 包含了所有 UE 公共的无线资源配置信息
SIB3
SIB3 包含了同频、异频或不同技术网络的小区重选信息。
SIB4
SIB4 包含了相邻小区相关的仅用于同频小区重选的信息以及小区重选单参数、黑名单小区。
SIB5
SIB5 包含异频 E-UTRA 网络重选的信息。
SIB6
SIB6 包含了异频 UTRA 网络重选的信息。
SIB7
SIB7 包含了异频 GERAN（GSM/EDGE）网络重选的信息。
SIB8
SIB8 包含了异频 CDMA2000 网络重选的信息。
SIB9
SIB9 包含了家庭基站的名字
SIB10
SIB10 包含了 ETWS 主通知的信息
SIB11
SIB11 包含了 ETWS 辅通知的信息
SIB12
SIB12 包含了 CMAS 辅通知的信息。

系统消息获取

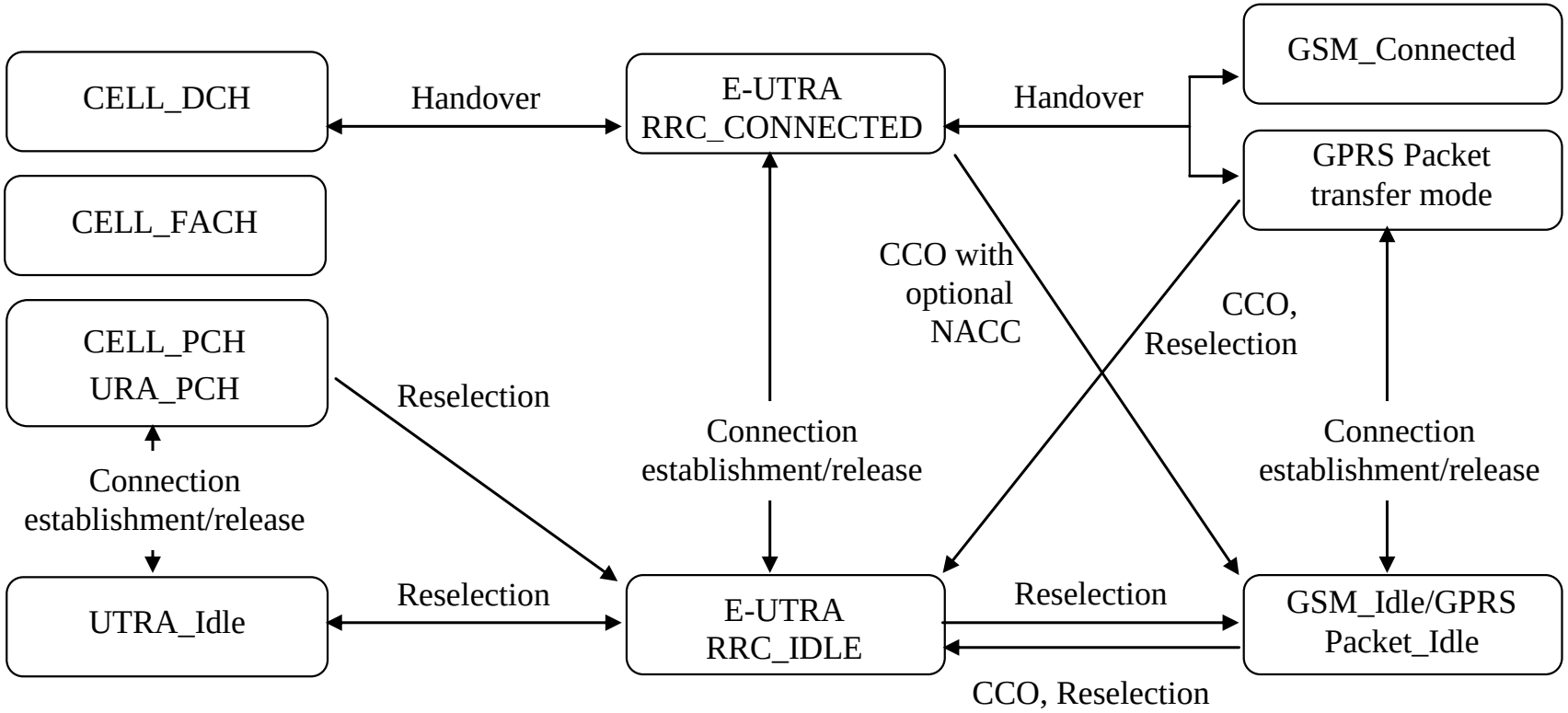


系统消息信令流程

- UE通过E-UTRAN广播消息获取AS和NAS系统消息
- 此过程适用于RRC-IDLE和RRC_CONNECTED状态
  - 开机选网和小区重选时
  - 切换完成或从另一个RAT切换到E-UTRAN时
  - 重新返回覆盖区域时
  - 当系统消息改变时
  - 当出现接收ETWS指示时
  - upon receiving a request from CDMA2000 upper layers
  - upon exceeding the maximum validity duration (3h)

3GPP各状态间转换

各系统状态转移图

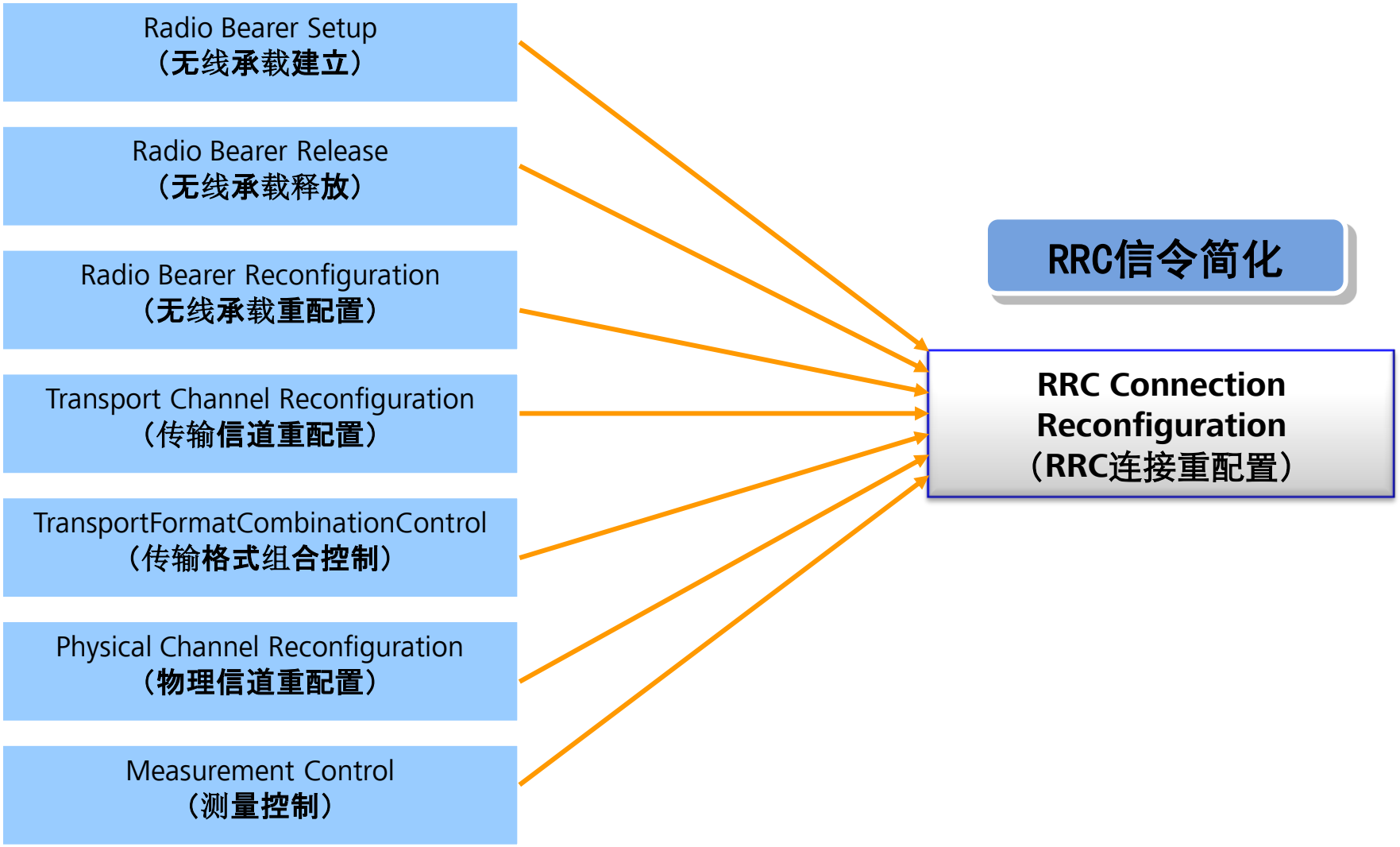


UE各状态说明

RRC状态

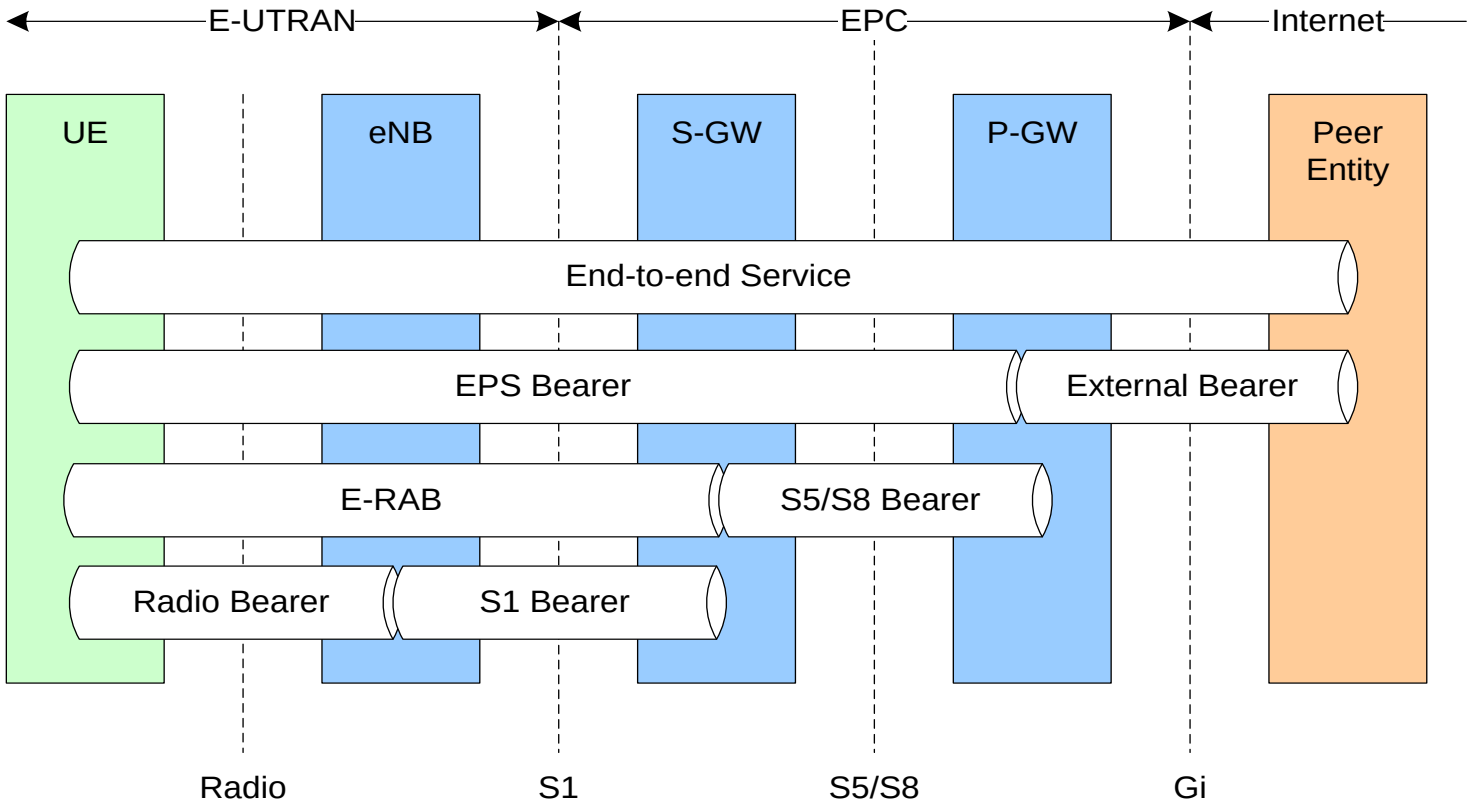
状 态	行 为
RRC_IDLE	PLMN选择
	NAS配置的DRX过程
	系统信息广播和寻呼
	邻小区测量
	小区重选的移动性
	UE获取1个TA区内的唯一标识
	eNodeB内无终端上下文
RRC_CONNECTED	网络侧有UE的上下文信息
	网络侧知道UE所处小区
	网络和终端可以传输数据
	网络控制终端的移动性
	邻小区测量
	存在RRC连接: UE可以从网络侧收发数据 监听共享信道上指示控制授权的控制信令 UE可以上报信道质量给网络侧 UE可以根据网络配置进行DRX

RRC信令消息简化


Radio Bearer Setup
（无线承载建立）
Radio Bearer Release
（无线承载释放）
Radio Bearer Reconfiguration
（无线承载重配置）
Transport Channel Reconfiguration
（传输信道重配置）
TransportFormatCombinationControl
（传输格式组合控制）
Physical Channel Reconfiguration
（物理信道重配置）
Measurement Control
（测量控制）
RRC信令简化
RRC Connection Reconfiguration
（RRC连接重配置）

LTE中的承载

- Radio Bearer承载空口RRC信令和NAS信令
- S1 Bearer 承载eNB与MME间S1-AP信令
- NAS消息也可作为NAS PDU附带在RRC消息中发送



标准QCI属性

QCI是EPS承载最重要的QoS参数之一，它是一个数量等级，代表了EPS应该为这个SDF提供的QoS特性，每个SDF都与且仅与一个QCI相关联。与相同IP-CAN会话相对应的多个SDF，若具有相同的QCI和ARP值，可以作为一个单独的业务集合来处理，这就是SDF集合。下表给出了EPS系统定义的标准QCI属性，所有的QCI属性均可由运营商根据实际需求预配置在eNodeB上，这些参数决定了无线侧承载资源的分配。

QCI	资源类型	优先级	数据包时延	数据包丢包率	典型业务
1	GBR	2	100ms	10^{-2}	会话语音
2		4	150ms	10^{-3}	会话视频（直播要求）
3		3	50ms	10^{-3}	实时游戏
4		5	300ms	10^{-6}	非会话视频（缓冲流要求）
5	Non-GBR	1	100ms	10^{-6}	IMS信令
6		6	300ms	10^{-6}	语音（缓冲流要求）、基于TCP的业务（如：www、e-mail、chat、ftp、p2p file sharing、progressive video等）
7		7	100ms	10^{-3}	语音、视频（直播流要求）、交互式游戏
8		8	300ms	10^{-6}	语音（缓冲流要求）、基于TCP的业务（如：www、e-mail、chat、ftp、p2p文件共享、progressive video等）
9		9			

无线承载分类

根据承载内容分类

- 数据承载为DRB，通过eNB为其分配的PDSCH来承载
- 信令承载通过SRB，LTE中有三类SRB
  - SRB0：承载RRC消息，映射到CCCH信道
  - SRB1：承载RRC消息，也可承载NAS消息，映射到DCCH信道
  - SRB2：承载NAS消息，映射到DCCH信道
  - UE的RRC连接未建立时，由SRB0承载RRC信令；SRB2未建立时，由SRB1承载NAS信令

NAS消息其他承载方式

- 由于带宽增加，数据传输性能增强，LTE的RRC消息的数据携带能力显著提升；
  因此LTE中所有NAS消息可填充在RRC消息中携带传输，进一步精简了信令流程
- NAS消息通过四条RRC消息传递：
  - ULInformation Transfer 和 DLInformation Transfer （由SRB2承载，SRB2未建立时SRB1承载）
  - RRCConnection Setup Complete 和 RRCConnection Reconfiguration （由SRB1承载）
  - RRCConnection Setup Complete（只携带NAS的初始直传消息）

小区内UE标识（1）

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

核心网UE标识（2）

用户标识	名称	来源	作用
IMSI	International Mobile Subscriber Identity	SIM卡	UE在首次ATTACH时需要携带IMSI信息，网络也可以通过身份识别流程要求UE上报IMSI参数
IMEI	International Mobile Equipment Identity	终端	国际移动台设备标识，唯一标识UE设备，用15个数字表示
IMEISV	IMEI and Software Version Number	终端	携带软件版本号的国际移动台设备标识，用16个数字表示
S-TMSI	SAE Temporary Mobile Station Identifier	MME产生并维护	SAE临时移动标识，由MME分配。与UMTS的P-TMSI格式类似，用于NAS交互中保护用户的IMSI
GUTI	Globally Unique Temporary Identifier	MME产生并维护	全球唯一临时标识，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.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；TMSI信息是GUTI的一部分

随机接入过程（36.300）

随机接入实现的基本功能

- 申请上行资源
- 与eNodeB间的上行时间同步

随机接入的使用场景

竞争接入过程

- 从RRC-IDLE状态到RRC-CONNECT的状态转换，即RRC连接过程，如初始接入和TAU更新
- 无线链路失败后的初始接入，即RRC 连接重建过程
- 在RRC-CONNECTED状态，未获得上行同步但需发送上行数据和控制信息或虽未上行失步但需要通过随机接入申请上行资源
- 在RRC-CONNECTED状态，从服务小区切换到目标小区

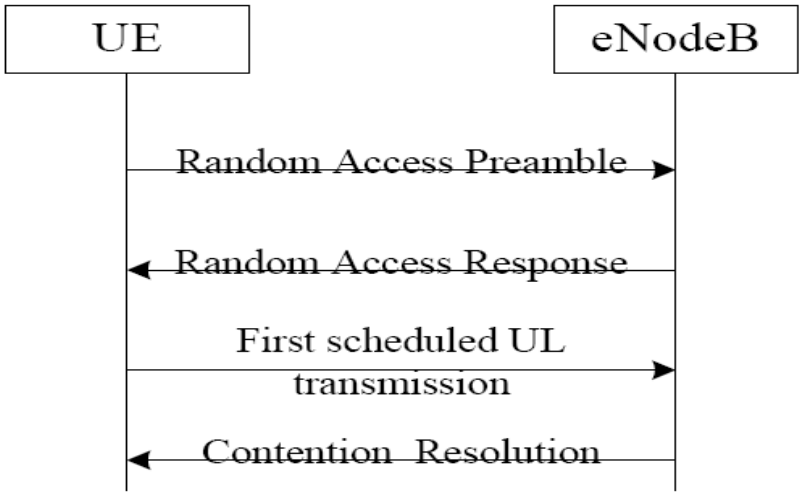
非竞争接入过程

- 在RRC-CONNECTED状态，从服务小区切换到目标小区
- 在RRC-CONNECTED状态，未获得上行同步但需接收下行数据
- 在RRC-CONNECTED状态，UE位置辅助定位需要，网络利用随机接入获取时间提前量（TA: Timing Advance）

基于竞争的随机接入（2-1）

基于竞争的随机接入过程2-1

- UE随机选择preamble码发起
- Msg1：发送Preamble码
  - eNB可以选择64个Preamble码中的部分或全部用于竞争接入
  - Msg1承载于PRACH上
- Msg2：随机接入响应
  - Msg2由eNB的MAC层组织，并由DL_SCH承载
  - 一条Msg2可同时响应多个UE的随机接入请求
  - 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
- Msg3：第一次调度传输
  - UE在接收Msg2后，在其分配的上行资源上传输Msg3



基于竞争的随机接入（2-2）

基于竞争的随机接入过程2-2

- 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
- Msg4：竞争解决

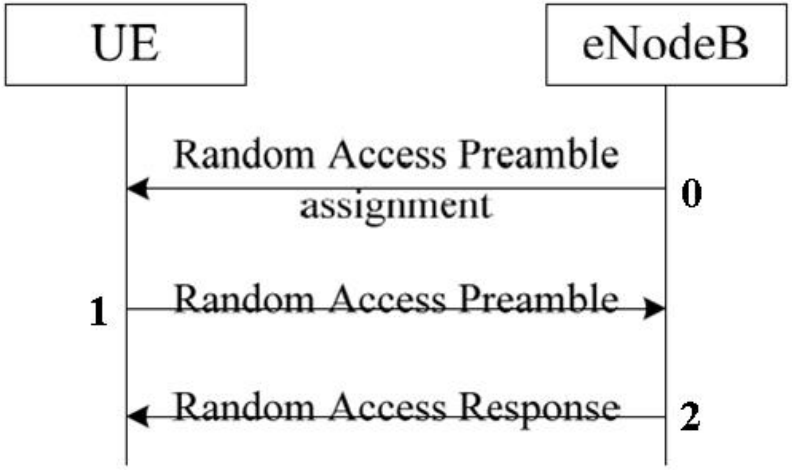
	初始接入和连接重建场景	切换，上/下行数据到达场景
竞争判定	Msg4携带成功解调的Msg3消息的拷贝，UE将其与自身在Msg3中发送的高层标识进行比较，两者相同则判定为竞争成功	UE如果在PDCCH上接收到调度Msg4的命令，则竞争成功
调度	Msg4使用由临时C-RNTI加扰的PDCCH调度	eNB使用C-RNTI加扰的PDCCH调度Msg4
C-RNTI	Msg2中下发的临时C-RNTI在竞争成功后升级为UE的C-RNTI	UE之前已分配C-RNTI，在Msg3中也将其传给eNB。竞争解决后，临时C-RNTI被收回，继续使用UE原C-RNTI

基于非竞争的随机接入

基于非竞争的随机接入过程

- 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
  - 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

控制面协议——RRC协议

RRC协议介绍

- **RRC协议功能**
  - 为NAS层提供连接管理、消息传递等服务
  - 对接入网的底层协议实体提供参数配置的功能
  - 负责UE移动性管理相关的测量、控制等功能

- **RRC协议承载——SRB**

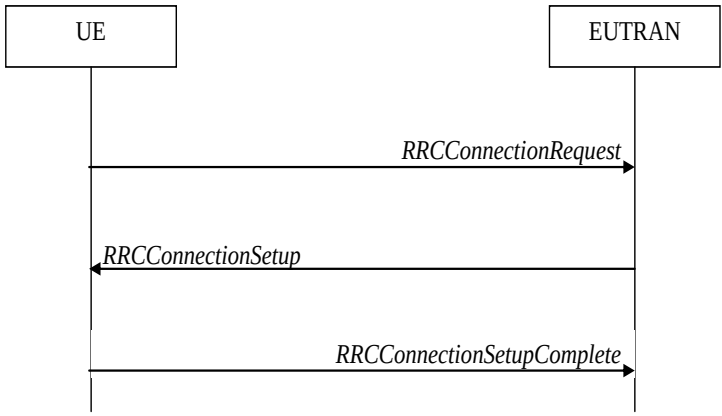
SRB类别	承载逻辑信道	承载消息类别	承载消息内容
SRB0	CCCH	RRC消息	RRC连接请求，RRC连接建立，RRC连接拒绝，RRC连接重建立请求，RRC连接重建立，RRC连接重建立拒绝
SRB1	DCCH	RRC消息 部分NAS消息	RRC连接建立完成，RRC连接重建立完成，RRC连接重配置，RRC连接重配置完成，RRC连接释放等
SRB2	DCCH	NAS消息	上下行直传消息

RRC连接建立过程

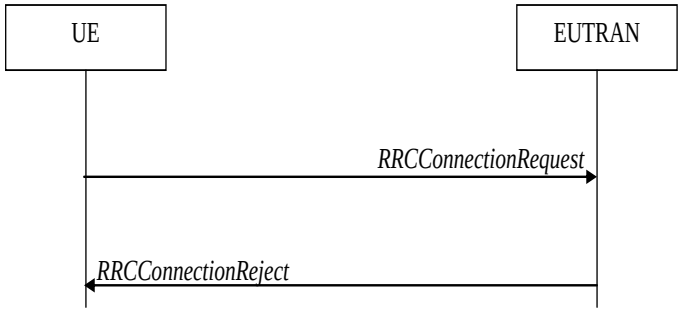
RRC连接建立

- **触发原因：**
  - IDLE态UE需变为连接态时发起该过程，如呼叫、响应寻呼、TAU、Attach等；
- **RRC连接建立成功流程**
  - RRC连接请求：UE通过UL_CCCH在SRB0上发送，携带UE的初始（NAS）标识和建立原因等，该消息对应于随机接入过程的Msg3；
  - RRC连接建立：eNB通过DL_CCCH在SRB0上发送，携带SRB1的完整配置信息，该消息对应随机接入过程的Msg4；
  - RRC连接建立完成：UE通过UL-DCCH在SRB1上发送，携带上行方向NAS消息，如Attach Request、TAU Request、Service Request、Detach Request等，eNB根据这些消息进行S1口建立；
- **RRC连接建立失败**
  - 第二步中，如果eNB拒绝为UE建立RRC连接，则通过DL_CCCH在SRB0上回复一条RRC连接拒绝消息；

RRC连接，建立成功



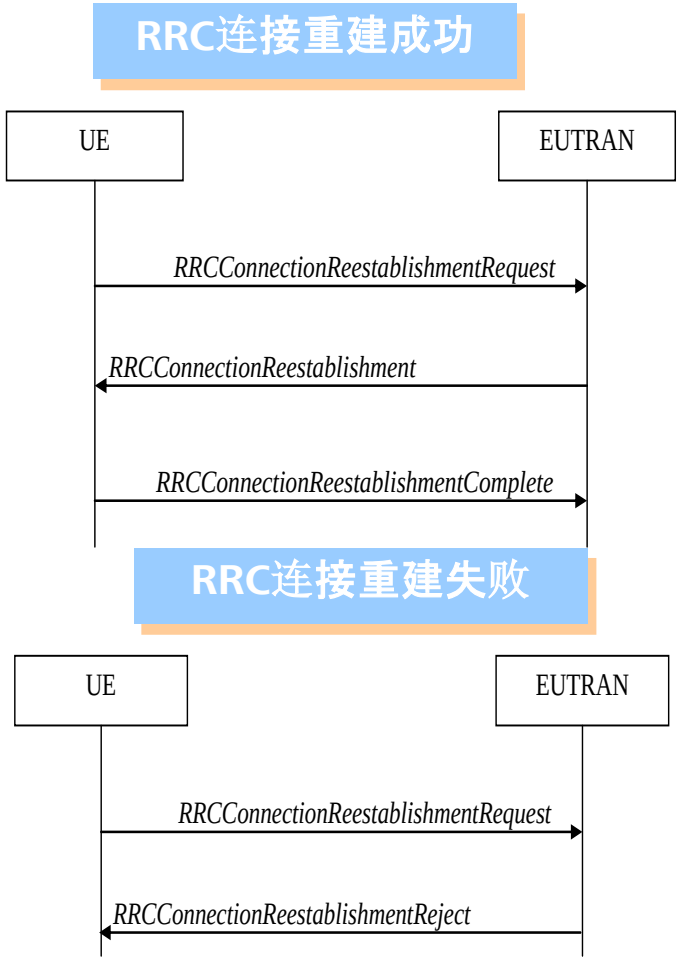
RRC连接，网络侧拒绝



RRC连接重建立过程

RRC连接重建

- **触发原因：**
  - 当处于RRC连接状态但出现切换失败、无线链路失败、完整性保护失败、RRC重配置失败等情况时，触发此过程；
- **RRC连接重建立成功流程**
  - RRC连接重建请求：UE通过UL_CCCH在SRB0上发送，携带UE的AS层初始标识信息及重建立原因，该消息对应随机接入过程的Msg3；
  - RRC连接重建：eNB通过DL_CCCH在SRB0上回复，携带SRB1的完整配置信息，该消息对应随机接入过程的Msg4；
  - RRC连接重建立完成：UE通过UL-DCCH在SRB1上发送，不携带任何实际信息，只起到RRC层确认的功能；
- **RRC连接重建立拒绝流程**
  - 第二步中，如果eNB中没有UE的上下文信息，则拒绝为UE重建RRC连接，则通过DL_CCCH在SRB0上回复一条RRC连接重建立拒绝消息；

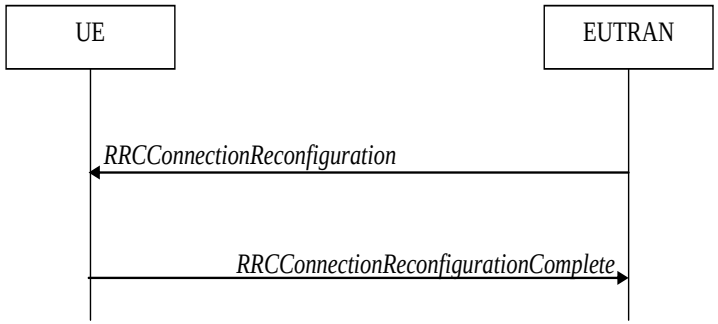


RRC连接重配置过程

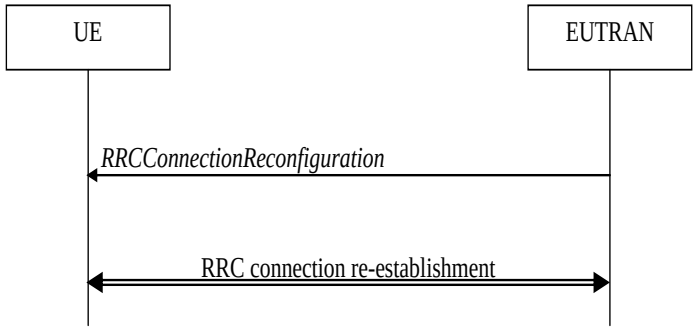
RRC连接重配

- **触发原因：**
  - 当需要发起对SRB和DRB的管理、低层参数配置、切换执行和测量控制时，触发此过程
- **RRC连接重配置过程**
  - RRC连接重配置：eNB通过DL_DCCH在SRB1上发送，根据功能的不同携带不同的配置信息内容，一条消息中可以携带体现多个功能的信息单元
  - RRC连接重配置完成：UE通过UL_DCCH在SRB1上发送，不携带任何实际信息，只起到RRC层确认的功能
- **RRC连接重配置异常流程**
  - 若UE无法执行RRC连接重配置消息中的内容，则UE回退到收到该消息前的配置，并发起RRC连接重建立过程

RRC连接重配置成功



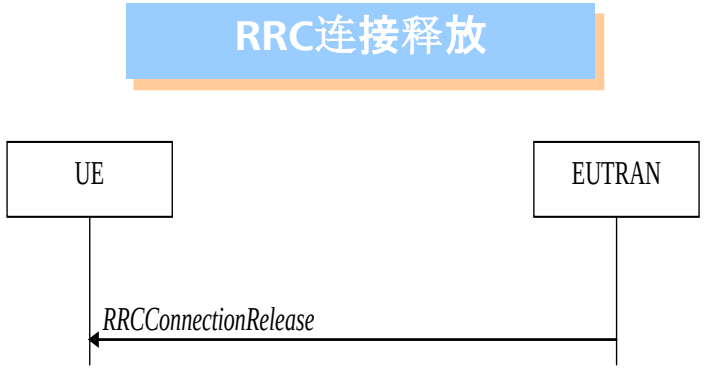
RRC连接重配置异常



RRC连接释放过程

RRC连接释放

- **触发原因：**
  - 网络希望解除与UE的RRC连接时，触发该过程
- **RRC连接释放过程**
  - RRC连接释放：eNB通过DL_DCCH在SRB1
  - 上发送，可选择携带重定位信息和专用优先级分
  - 配信息（用于控制UE的小区选择和小区重选）
- **本地释放**
  - 某些情况下，UE的RRC层根据NAS层的指示主动释放RRC连接，不通知网络侧而主动进入空闲状态，如NAS层鉴权过程中没有通过鉴权检查



RRC过程场景总结

RRC过程总结

	RRC连接建立	RRC连接重建	RRC重配置	RRC释放
场景	➢初始接入Attach时发起； ➢UE从IDLE态至连接态时发起： 发起呼叫； 响应寻呼； Attach Request； TAU Request； Detach Request	➢RRC连接出现异常时发起切换失败； 无线链路失败； 底层完整性保护失败； RRC重配置失败；	➢当需要对SRB和DRB进行管理时发起： E-RAB的建立、修改、删除；请求UE激活SRB2； ➢测量控制下发时发起； ➢切换执行时发起；	➢希望解除与UE的RRC连接，使UE返回IDLE态时；

RRC建立原因

NAS Procedure		RRC Establishment Cause
Attach		Mobile Originating Signalling
Detach		
Tracking Area Update		
Service Request	User plane radio resources request	Mobile Originating Data
	Uplink signalling resources request	
	Paging response for PS core network domain	Mobile Terminating Access
Extended Service Request	Mobile originating CS fallback	Mobile Originating Data
	Mobile terminating CS fallback	Mobile Terminating Access
	Mobile originating CS fallback emergency call	Emergency

测量（36.331）

测量概述

- RRC_IDLE状态下，UE的测量参数信息通过E-UTRAN的广播获得
- RRC_CONNECTED状态下，E-UTRAN通过专属信令向UE下发测量配置（measurement configuration）信息，如*RRCConnectionReconfiguration*消息中可携带
- UE可执行的测量类型
  - 同频测量：测量与当前服务小区下行频点相同的邻小区下行频点
  - 异频测量：测量与当前服务小区下行频点不同的下行频点（同小区或邻小区）
  - 与UTRA的系统间测量
  - 与GERAN的系统间测量
  - 与CDMA2000 HRPD或CDMA2000 1xRTT的系统间测量

测量下达

测量配置下发

- IDLE态，网络侧通过系统消息告知UE需要进行的测量及其参数
  - SIB4：下发同频邻区测量信息（邻区列表）
  - SIB5：下发异频邻区测量信息（邻区列表）
  - SIB6：下发UTRAN邻区信息
  - SIB7：下发GERAN邻区信息
  - SIB8：下发CDMA2000邻区信息
  - SIB9：下发Home eNodeb name
  - SIB10、11： 下发EWTS信息；
  - SIB12: 下发CMAS 信息；
  - SIB13:MBMS信息；

- 连接态，网络侧通过RRC重配消息中携带 MeasConfig 信元给UE下发测量配置
  - 该信元中携带测量对象和测量上报标准

测量报告上报

测量上报

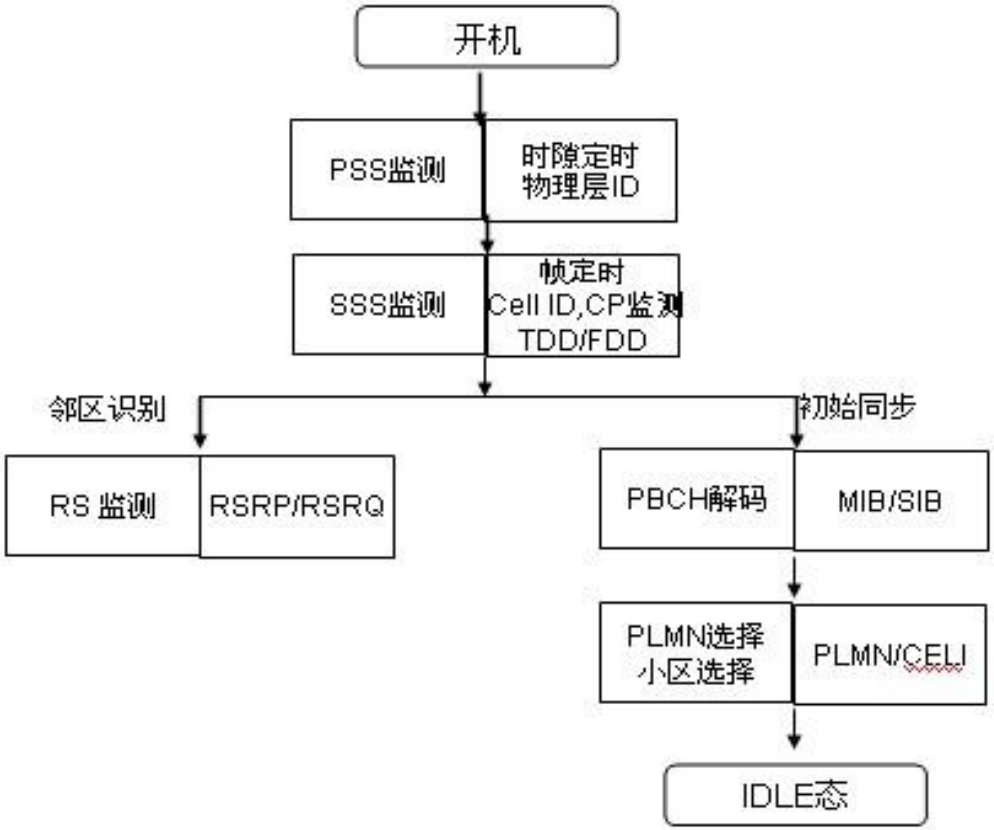
- IDLE态下，UE不上报，仅做小区重选；连接态下UE进行测量上报
- 事件触发一次上报
  - 触发事件有A1—A6，B1，B2
  - 上报次数为一次
  - UE忽略上报间隔配置
- 周期性上报
  - 触发类型为周期，包含上报CGI、上报最强小区、SON目的上报最强小区
  - 如果上报目的为“上报CGI”或上报“SON目的上报最强小区”，则上报次数为1
- 事件触发周期上报（事件触发上报与周期性上报的结合）
  - 触发事件有A1—A6，B1，B2
  - 上报次数为多次
  - 上报间隔配置有效

测 量 事 件	
LTE系统内的同频/异频测量事件	异技术测量事件
– Event A1：服务小区测量值（RSRP或RSRQ）大于门限值 – Event A2：服务小区测量值（RSRP或RSRQ）小于门限值 – Event A3：邻小区测量值优于服务小区测量值一定门限值 – Event A4：邻小区测量值大于门限值 – Event A5：服务小区测量值小于门限1，同时邻小区信道质量大于门限2 – Event A6：邻小区测量值优于SCELL一定门限值	– Event B1：异技术邻小区信道质量大于门限 – Event B2：服务小区信道质量小于门限1，同时异技术邻小区信道质量大于门限2

目录

小区搜索

- 小区搜索过程又称为下行同步过程，主要通过解下行的主同步信号PSS和辅同步信号SSS完成

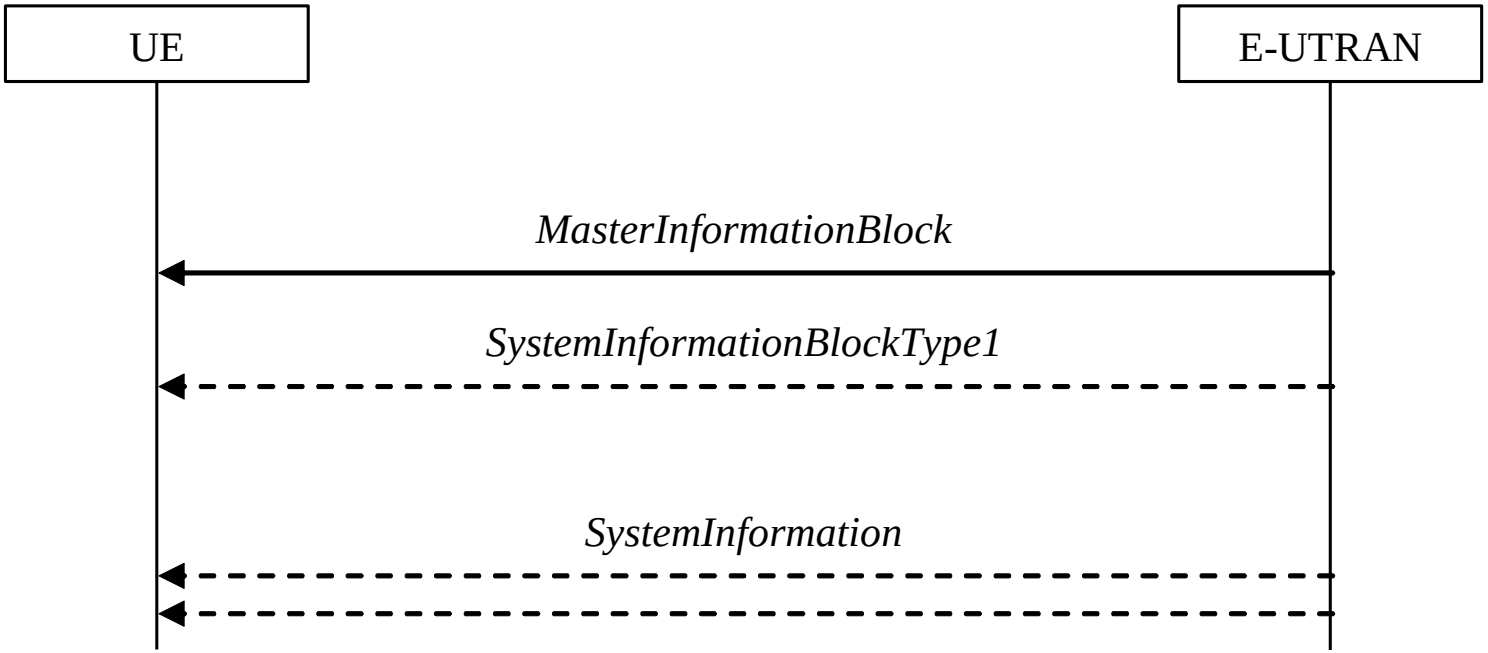


小区搜索

- 对于FDD，PSS在slot0和slot10的倒数第一个OFDM符号上；SSS在slot0和slot10的倒数第二个OFDM符号上。
- 对于TDD，PSS在slot2和slot12的第三个OFDM符号上；SSS在slot1和slot11的倒数第一个OFDM符号上。
- PSS在每个无线帧的2次发送内容一样，SSS每个无线帧2次发送内容不一样，通过解PSS先获得5ms定时，通过解SSS可以获得无线帧的10ms定时；由于FDD和TDD时SSS的时域位置不同，通过解SSS又可以获得系统的制式。
- 通过解PSS可以获得物理层小区ID，再通过解SSS可以获得小区的组ID（504个小区分成168个组），二者组合就可以获得当前小区的小区ID（每个组内又有3个小区ID）；当前小区的PCI = 组ID * 3 + 小区ID

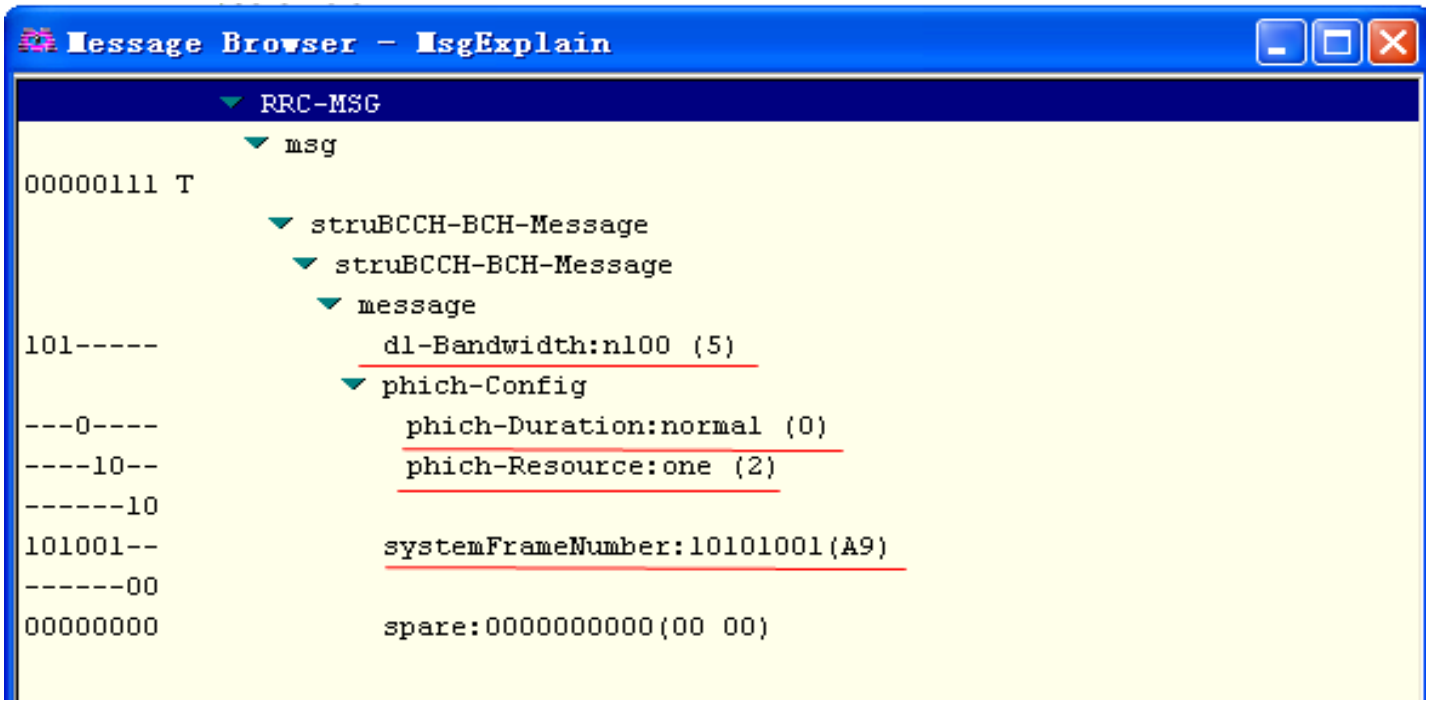
PLMN和小区选择

➢小区搜索完成后，UE会获得当前小区的PCI，UE使用获得的PCI去解当前小区的MIB和SIB消息，通过解MIB消息获得小区的下行同步以及系统带宽等关键信息，完了在SIB信息的时域位置上检测PDCCH，根据PDCCH指示获取小区的SIB1信息，完了再解析其它SIB信息。



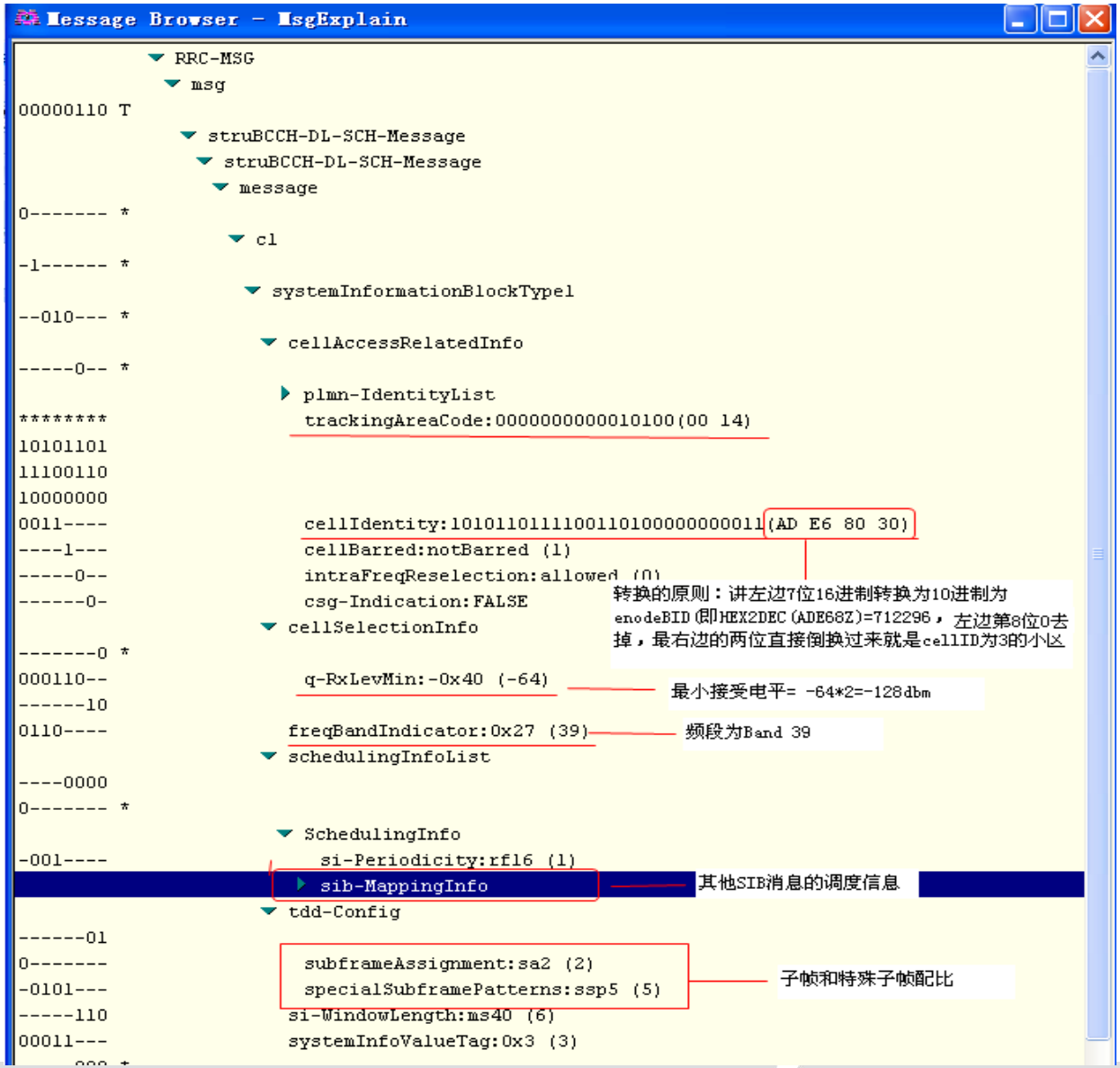
PLMN和小区选择——MIB

➢MIB传输周期为40ms，在一个周期内，PBCH信道分布在每个无线帧的#0子帧内，在每一个#0子帧内，占据第二个slot的前4个符号位置；频域与PSS和SSS信号一样，占据中心的1.08MHz，即频域中心的6RB。



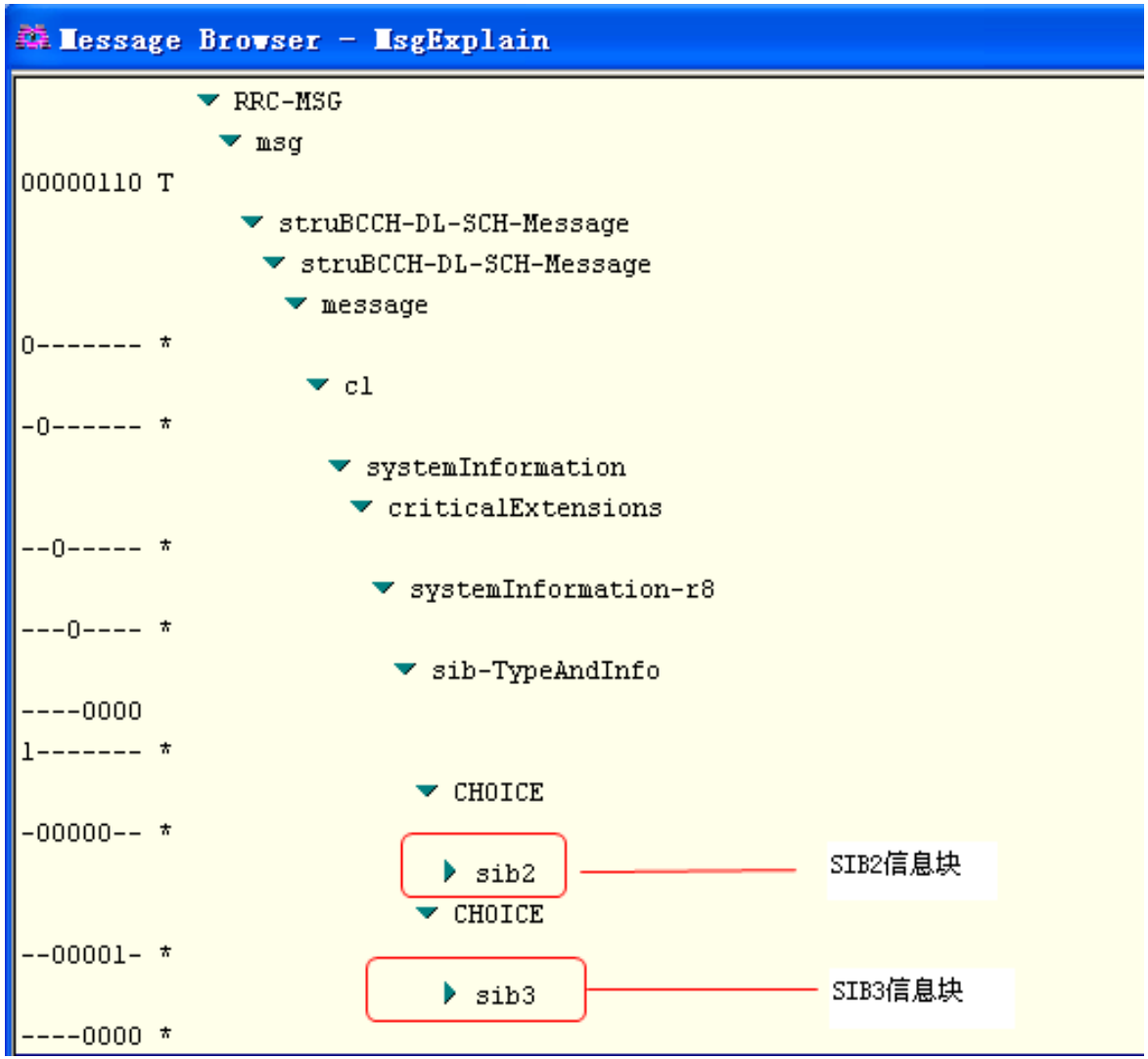
PLMN和小区选择——SIB1

- SIB1传输周期为80ms，传输TTI内的首次传输是在帧号为8的整数倍的无线帧上，重复传输是在TTI内的其它偶数无线帧上；每次传输都是在对应无线帧的#5子帧上，UE在这些子帧内检测PDCCH，如果存在SI-RNTI，则在该子帧内的PDSCH上接收SIB1。



PLMN和小区选择——SIBn

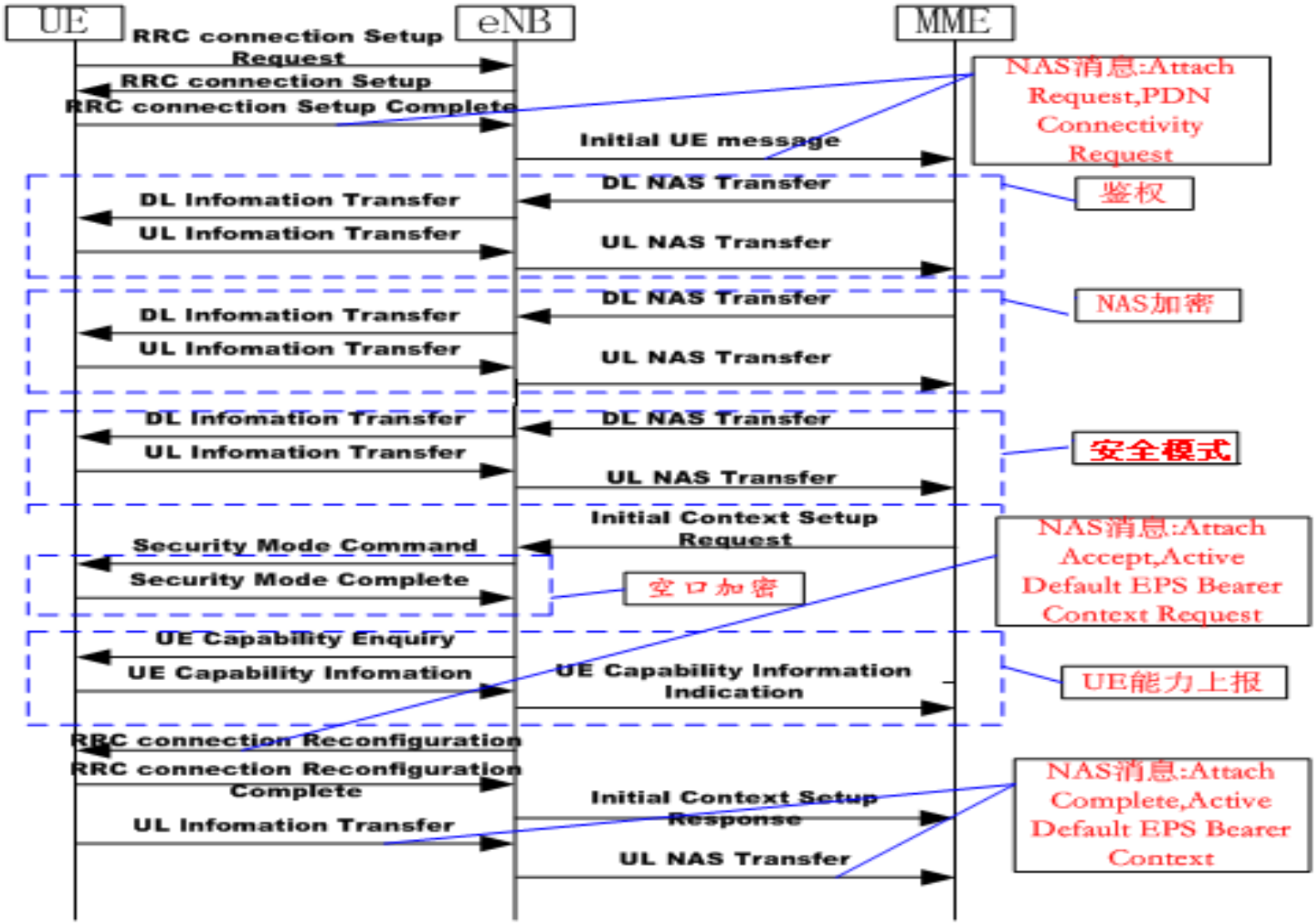
SIBn传输周期为80ms的整数倍，SIB2主要是无线资源相关配置，SIB3~SIB5主要是LTE系统内的小区重选配置；SIB6~SIB8分别为UTRA、GERAN、CDMA2000系统的重选配置，SIB9为HNB配置，SIB10为ETWS的主通知，SIB11为ETWS的辅通知。



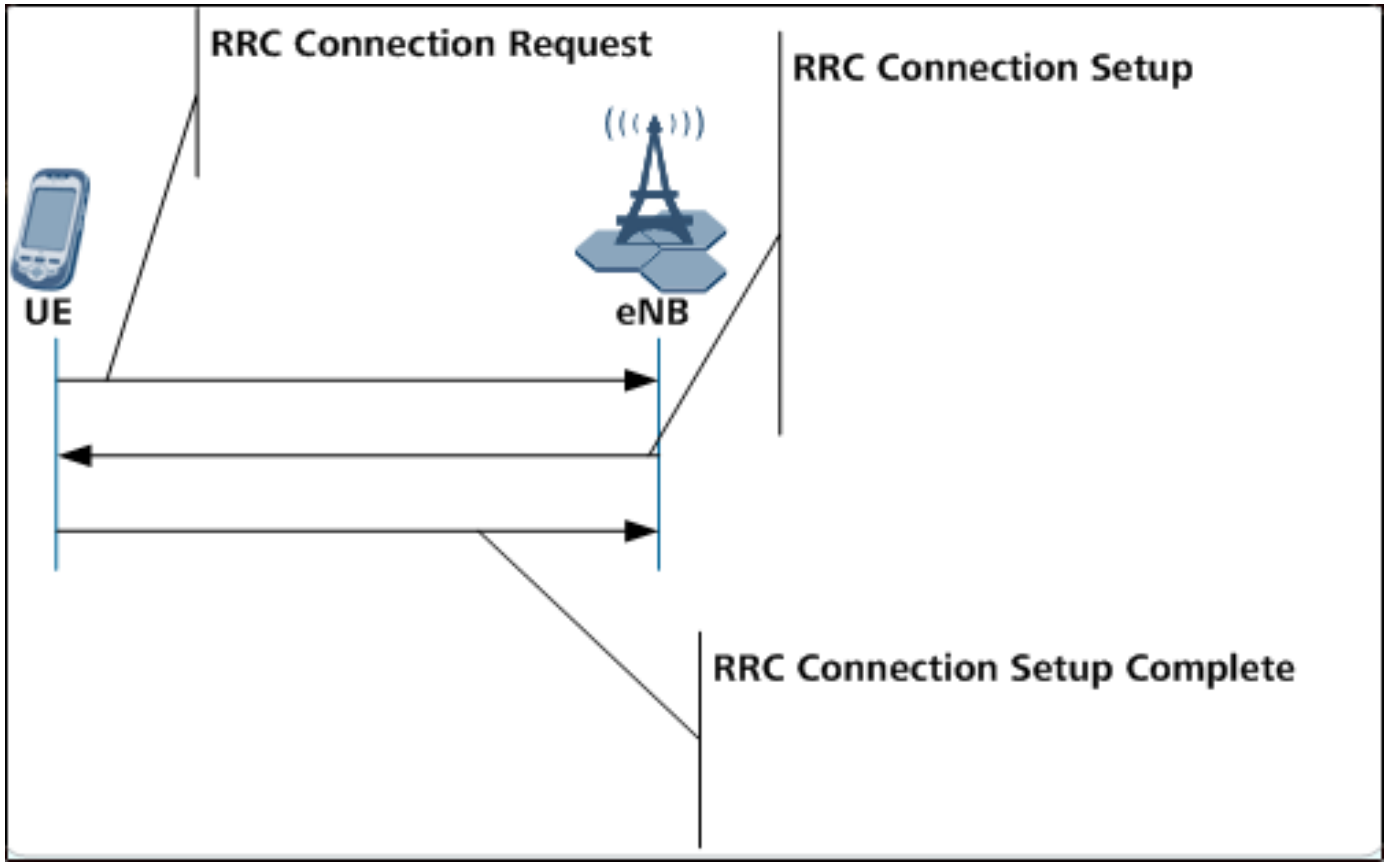
PLMN和小区选择

- 在SIB1信息中会携带网络侧的PLMN列表，UE的接入层AS会把解析的PLMN列表上报自己的非接入层NAS，由NAS层执行PLMN的选择，选择合适的PLMN。
- UE选定PLMN后会在该PLMN下选择合适的小区，小区的选择按照S准则，UE选择该PLMN下信号最强的小区进行驻留。

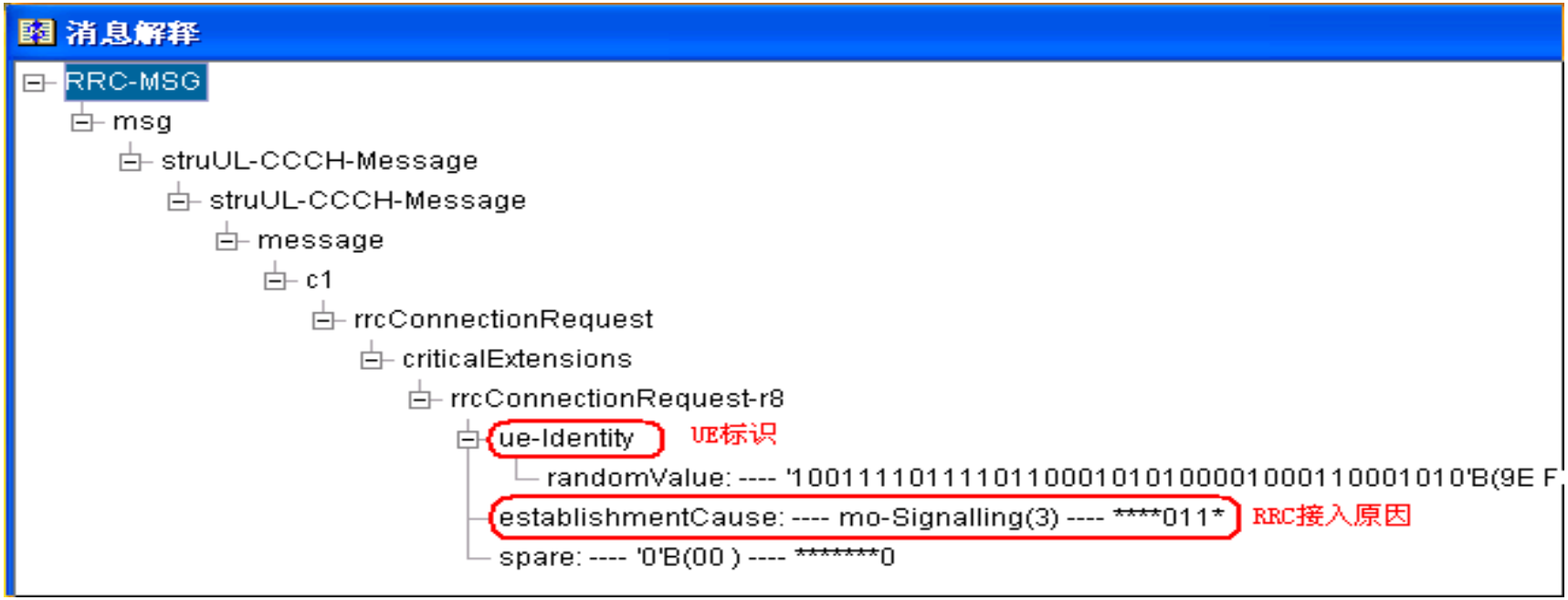
附着流程——ATTACH


UE
eNB
MME
RRC connection Setup Request
RRC connection Setup
RRC connection Setup Complete
Initial UE message
NAS消息:Attach Request,PDN Connectivity Request
DL NAS Transfer
鉴权
DL Infomation Transfer
UL Infomation Transfer
UL NAS Transfer
DL NAS Transfer
NAS加密
DL Infomation Transfer
UL Infomation Transfer
UL NAS Transfer
DL Infomation Transfer
DL NAS Transfer
安全模式
UL Infomation Transfer
UL NAS Transfer
Initial Context Setup Request
Security Mode Command
NAS消息:Attach Accept,Active Default EPS Bearer Context Request
Security Mode Complete
空口加密
UE Capability Enquiry
UE Capability Infomation
UE Capability Information Indication
UE能力上报
RRC connection Reconfiguration
RRC connection Reconfiguration Complete
Initial Context Setup Response
NAS消息:Attach Complete,Active Default EPS Bearer Context
UL Infomation Transfer
UL NAS Transfer

附着流程——RRC连接建立

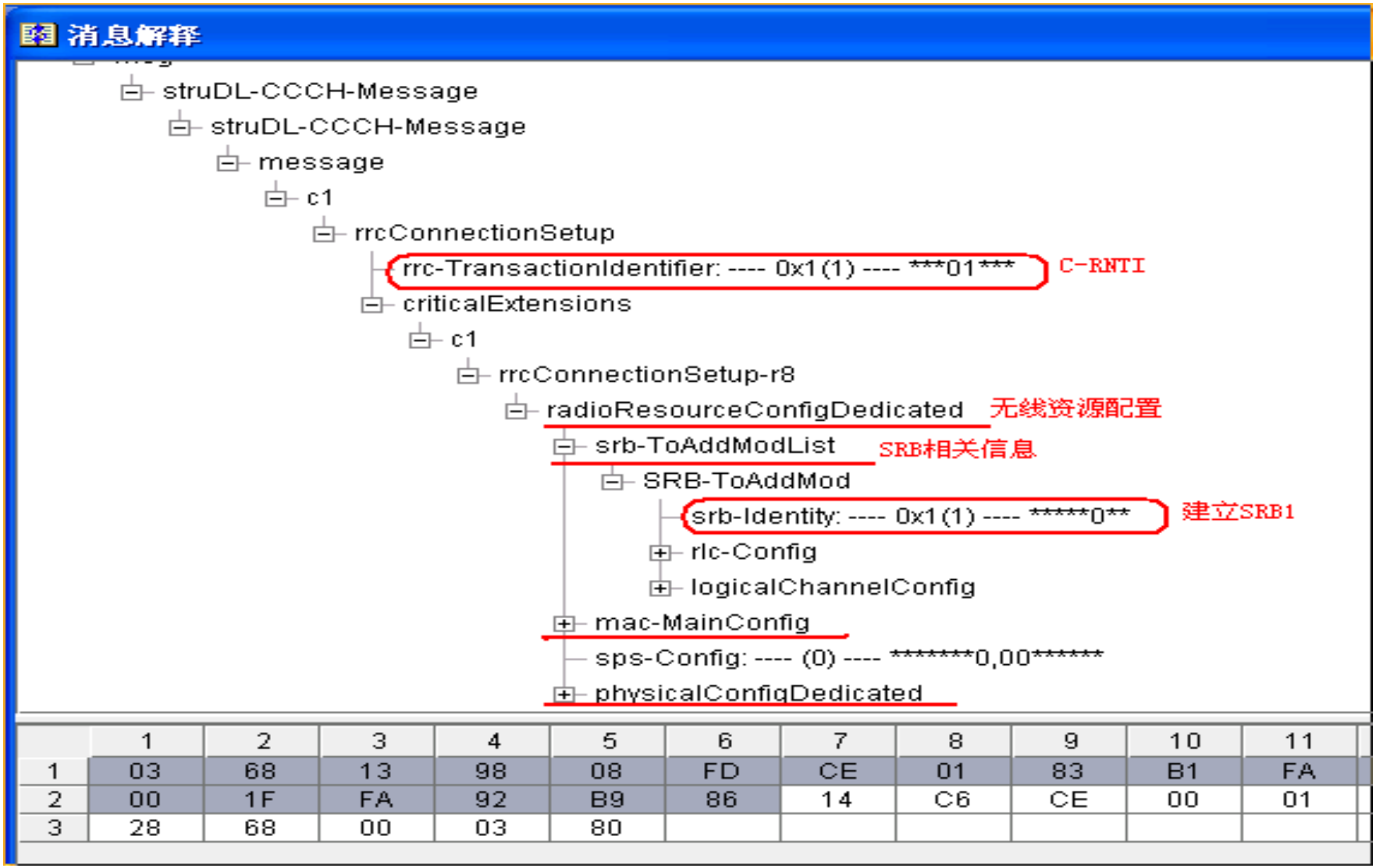


附着流程——RRC Connection Setup Request



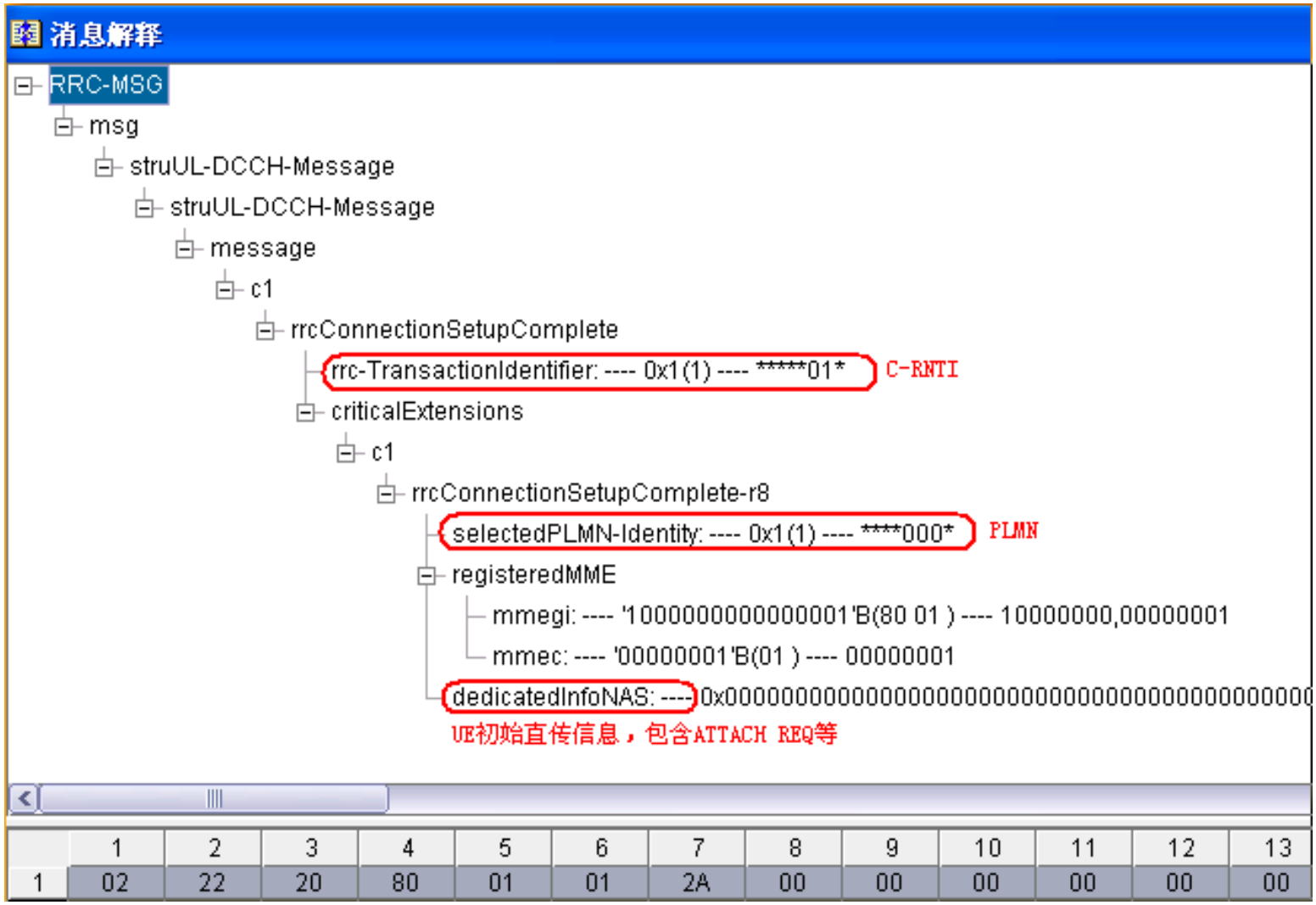
NAS Procedure		RRC Establishment Cause
Attach		Mobile Originating Signalling
Detach		
Tracking Area Update		
Service Request	User plane radio resources request	Mobile Originating Data
	Uplink signalling resources request	
	Paging response for PS core network domain	Mobile Terminating Access
Extended Service Request	Mobile originating CS fallback	Mobile Originating Data
	Mobile terminating CS fallback	Mobile Terminating Access
	Mobile originating CS fallback emergency call	Emergency

附着流程——RRC Connection Setup

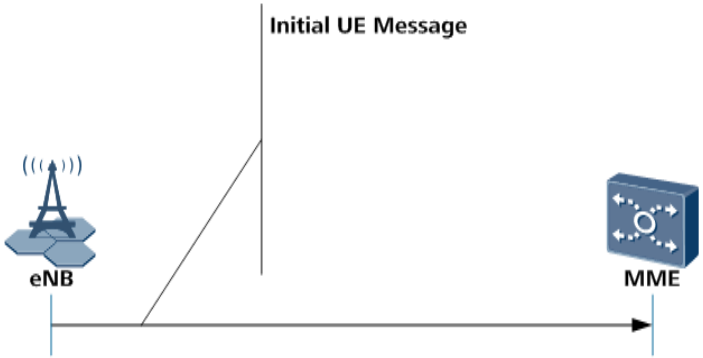


	1	2	3	4	5	6	7	8	9	10	11
1	03	68	13	98	08	FD	CE	01	83	B1	FA
2	00	1F	FA	92	B9	86	14	C6	CE	00	01
3	28	68	00	03	80						

附着流程——RRC Connection Setup Complete



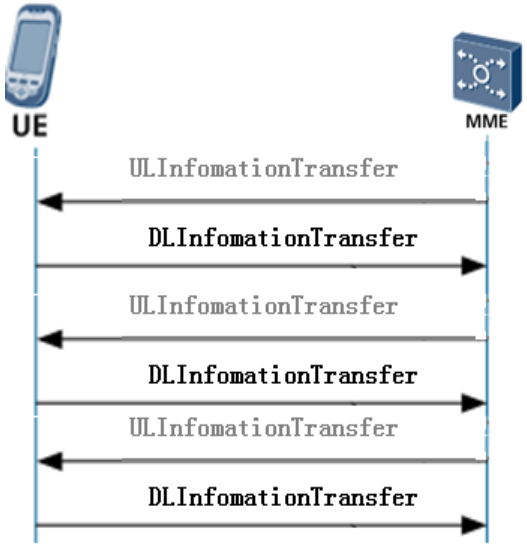
附着流程——Initial UE Message



消息解释 - 4

- S1ap-Msg
  - initiatingMessage
    - procedureCode: ---- 0xc(12) ---- ***00000,00001100
    - criticality: ---- ignore(1) ---- 01******
    - value
      - initialUEMessage
        - protocolIEs
          - SEQUENCE
            - id: ---- 0x8(8) ---- 00000000,00001000
            - criticality: ---- reject(0) ---- 00******
            - value
              - eNB-UE-S1AP-ID: ---- 0x23(35) ---- 00000000,00100011
          - SEQUENCE
          - SEQUENCE
            - id: ---- 0x43(67) ---- 00000000,01000011
            - criticality: ---- reject(0) ---- 00******
            - value
              - tAI
                - pLMNidentity: ---- 0x64F000 ---- 01100100,11110000,00000000
                - tAC: ---- 0x0001 ---- 00000000,00000001
          - SEQUENCE
            - id: ---- 0x64(100) ---- 00000000,01100100
            - criticality: ---- ignore(1) ---- 01******
            - value
              - eUTRAN-CGI
                - pLMNidentity: ---- 0x64F000 ---- 01100100,11110000,00000000
                - cell-ID: ---- '10101010111001101111000011111'B(AA E6 F0 F0) ---- 10101010,11100110,1
          - SEQUENCE
            - id: ---- 0x86(134) ---- 00000000,10000110
            - criticality: ---- ignore(1) ---- 01******
            - value
              - rRC-Establishment-Cause: ---- mo-Signalling(3) ---- 0011****

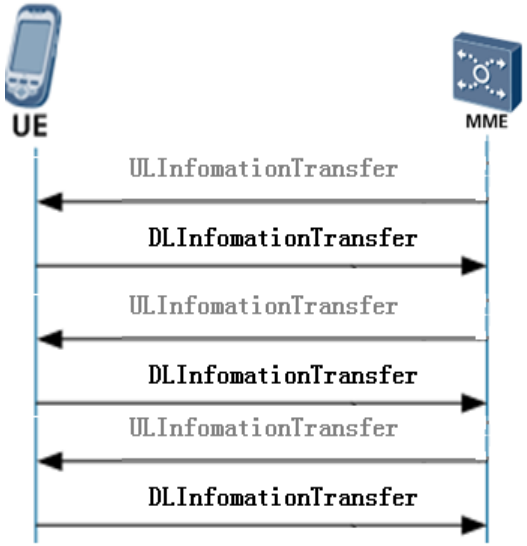
附着流程——鉴权、加密、安全模式（1）



消息解释 - 40

- S1ap-Msg
  - initiatingMessage
    - procedureCode: ---- 0xb(11) ---- ***00000,00001011
    - criticality: ---- ignore(1) ---- 01******
    - value
      - downlinkNASTransport
        - protocolIEs
          - SEQUENCE
            - id: ---- 0x0(0) ---- 00000000,00000000
            - criticality: ---- reject(0) ---- 00******
            - value
              - mME-UE-S1AP-ID: ---- 0x1794a1b(24726043) ---- 11000000,00000001,01111001,01001010,00011011
          - SEQUENCE
            - id: ---- 0x8(8) ---- 00000000,00001000
            - criticality: ---- reject(0) ---- 00******
            - value
              - eNB-UE-S1AP-ID: ---- 0xc6dc(50908) ---- 01000000,11000110,11011100
          - SEQUENCE
            - id: ---- 0x1a(26) ---- 00000000,00011010
            - criticality: ---- reject(0) ---- 00******
            - value
              - nAS-PDU
                - NAS-MESSAGE
                  - no-security-protection-MM-message
                    - msg-body
                      - authenticationRequest
                        - spare-half-octet: ---- 0x0(0) ---- 0000****
                        - key-set-identifier
                          - spare: ---- 0x0(0) ---- ****0***
                          - nAS-key-set-identifier: ---- nas-KSI5(5) ---- *****101
                        - authentication-parameter-RAND: ---- 0xCBF5F6FFFD32650FD77E4BDB1EC02B04 ----
                        - authentication-parameter-AUTN: ---- 0xC32FA5FB446CF24C2C6DA326A98E83A0 ----

附着流程——鉴权、加密、安全模式（2）

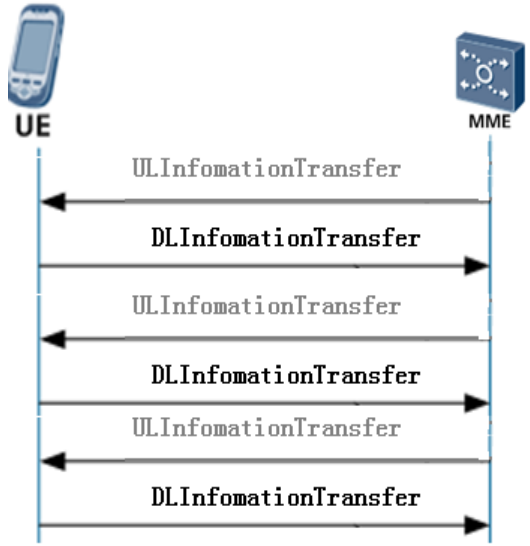


消息解释 - 44

- criticality: ---- ignore(1) ---- 01******
- value
  - downlinkNASTransport
    - protocolIEs
      - SEQUENCE
      - SEQUENCE
      - SEQUENCE
        - id: ---- 0x1a(26) ---- 00000000,00011010
        - criticality: ---- reject(0) ---- 00******
        - value
          - nAS-PDU
            - NAS-MESSAGE
              - security-command-msg
                - message-authentication-code: ---- 0xBF1D8828 ---- 10111111,00011101,10001000,00101000
                - sequence-number: ---- 0x0(0) ---- 00000000
                - nas-message
                - msg-body
                - securityModeCommand
                - selected-NAS-security-algorithms
                - spare1: ---- 0x0(0) ---- 0*******
                - type-of-ciphering-algorithm: ---- ePS-encryption-algorithm-128-EEA2(2) ---- *010****
                - spare2: ---- 0x0(0) ---- ****0***
                - type-of-integrity-protection-algorithm: ---- ePS-integrity-algorithm-128-EIA2(2) ---- *****010
                - spare-half-octet: ---- 0x0(0) ---- 0000****
                - nAS-key-set-identifierASME
                - tsc: ---- native-security-context(0) ---- ****0***
                - nAS-key-set-identifier: ---- nas-KSI5(5) ---- *****101
                - replayed-UE-security-capabilities
                - eEA
                - eIA

加密算法和完整性保护算法： 当前主要是是三类:不加密、Snown 3G、AES算法，分别对应EEA0,EEA1,EEA2和EIA0,EIA1,EIA2;

附着流程——鉴权、加密、安全模式（3）



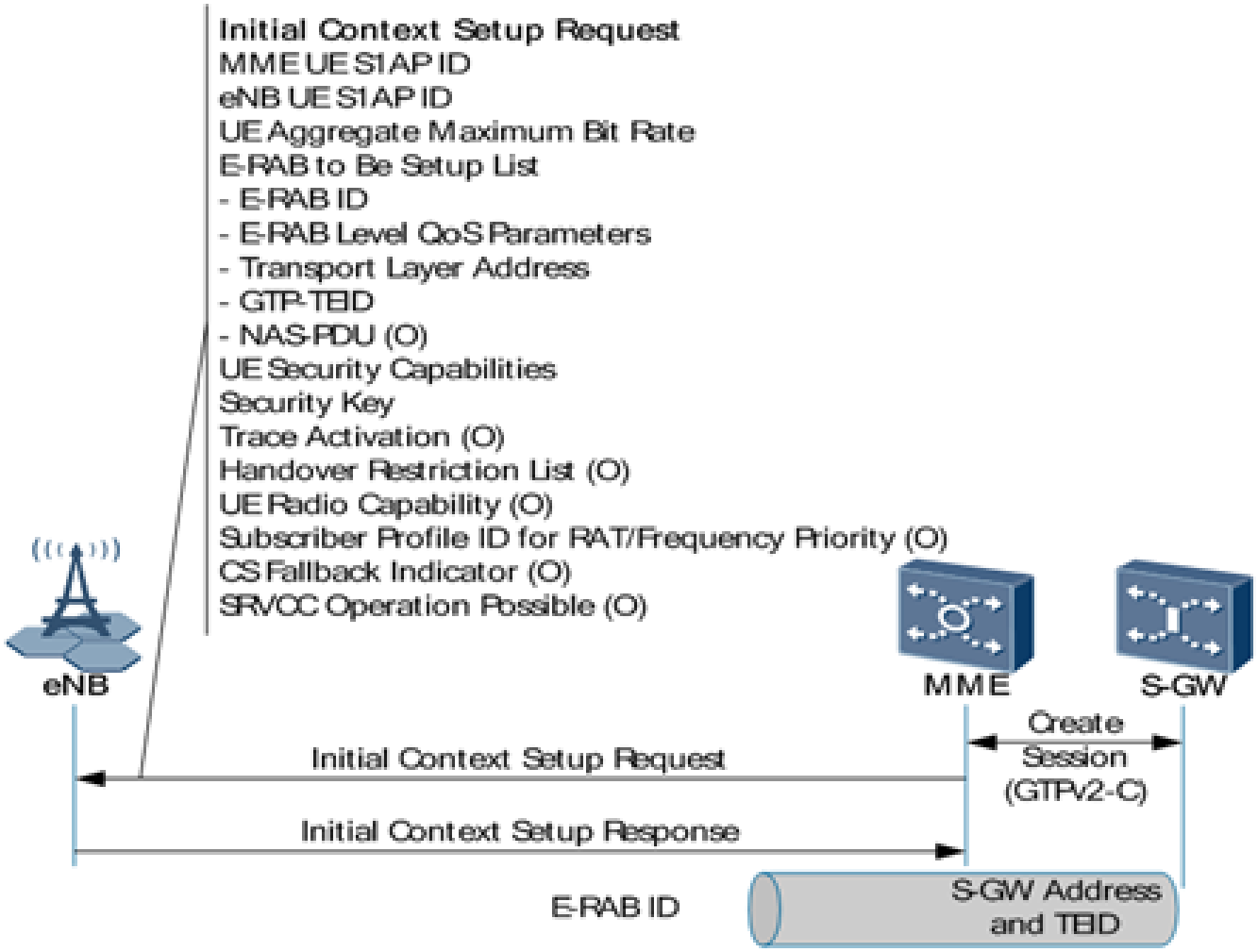
消息解释 - 48

- S1ap-Msg
  - initiatingMessage
    - procedureCode: ---- 0xb(11) ---- ***00000,00001011
    - criticality: ---- ignore(1) ---- 01******
    - value
      - downlinkNASTransport
        - protocolIEs
          - SEQUENCE
            - id: ---- 0x0(0) ---- 00000000,00000000
            - criticality: ---- reject(0) ---- 00******
            - value
              - mME-UE-S1AP-ID: ---- 0x1794a1b(24726043) ---- 11000000,00000001,01111001,01001010,00011011
          - SEQUENCE
            - id: ---- 0x8(8) ---- 00000000,00001000
            - criticality: ---- reject(0) ---- 00******
            - value
              - eNB-UE-S1AP-ID: ---- 0xc6dc(50908) ---- 01000000,11000110,11011100
          - SEQUENCE
            - id: ---- 0x1a(26) ---- 00000000,00011010
            - criticality: ---- reject(0) ---- 00******
            - value
              - nAS-PDU
                - NAS-MESSAGE
                  - security-protected-and-ciphered-NAS-message
                    - message-authentication-code: ---- 0x0D8867F3 ---- 00001101,10001000,01100111,11110011
                    - sequence-number: ---- 0x1(1) ---- 00000001

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

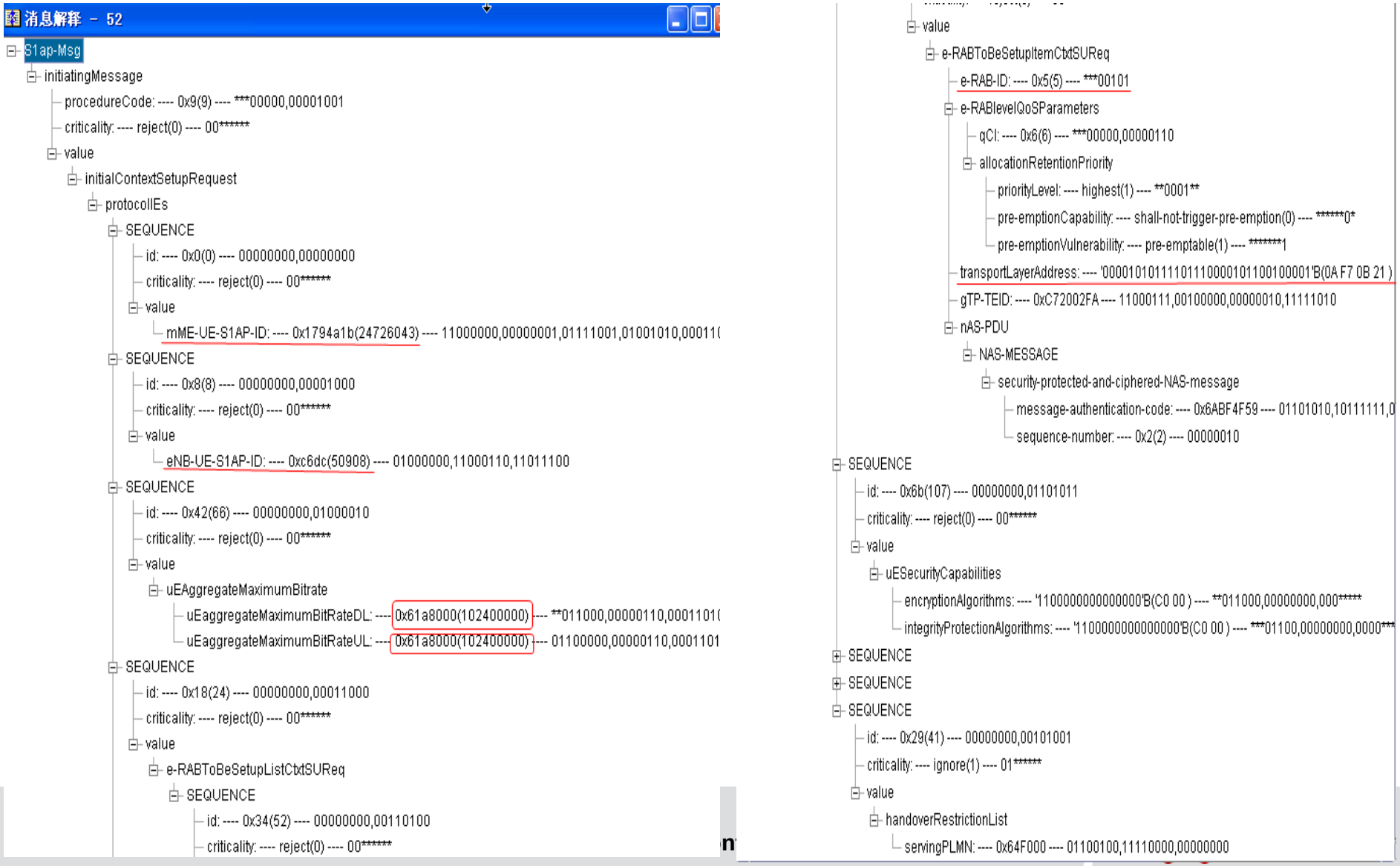
上一条(P) 下一条(N)

附着流程——Initial Context Setup Request（I）

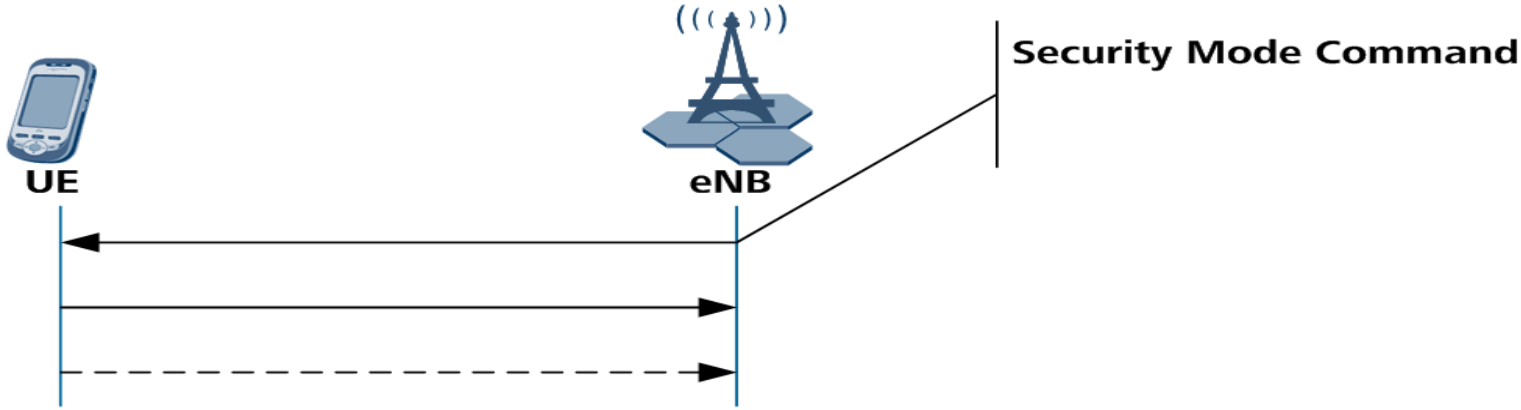


附着流程——Initial Context Setup Request（II）

➢消息解析



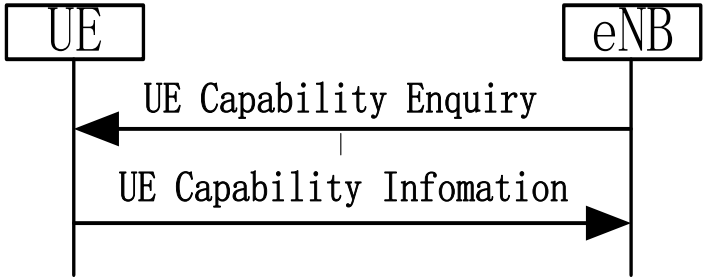
附着流程—RRC Security Mode Command/Complete



RRC-MSG
msg
struDL-DCCH-Message
struDL-DCCH-Message
message
c1
securityModeCommand
rrc-TransactionIdentifier:0x2 (2)
criticalExtensions
c1
securityModeCommand-r8
securityConfigSMC
securityAlgorithmConfig
cipheringAlgorithm:eea0 (0)
integrityProtAlgorithm:spare1 (7)

RRC-MSG
msg
struUL-DCCH-Message
struUL-DCCH-Message
message
c1
securityModeComplete
rrc-TransactionIdentifier:0x2 (2)
criticalExtensions
securityModeComplete-r8

附着流程——UE Capability Enquiry/Infomation




```
ueCapabilityInformation
  rrc-TransactionIdentifier: ---- 0x1 (1) ---- *****01*
criticalExtensions
  c1
    ueCapabilityInformation-r8
      ue-CapabilityRAT-ContainerList
        UE-CapabilityRAT-Container
          rat-Type: ---- eutra(0) ---- 0000****
          ueCapabilityRAT-Container
            ueEutraCap
              UE-EUTRA-Capability
                accessStratumRelease: ---- rel8(0) ---- ******00,00******
                ue-Category: ---- 0x3(3) ---- **010***
                pdcp-Parameters
                phyLayerParameters
                rf-Parameters
                  supportedBandListEUTRA
                    SupportedBandEUTRA
                      bandEUTRA: ---- 0x27(39) ---- ****1001,10******
                      halfDuplex: ---- TRUE(1) ---- **1*****
                    SupportedBandEUTRA
                      bandEUTRA: ---- 0x28(40) ---- ***10011,1*******
                      halfDuplex: ---- TRUE(1) ---- *1******
                    SupportedBandEUTRA
                      bandEUTRA: ---- 0x29(41) ---- **101000
                      halfDuplex: ---- TRUE(1) ---- 1*******
                    SupportedBandEUTRA
                    SupportedBandEUTRA
                measParameters
                featureGroupIndicators: ---- '11100110000011010001100010000000'B(E6 0D 18 80)
                interRAT-Parameters: ---- (0) ---- *******0,000000**
```

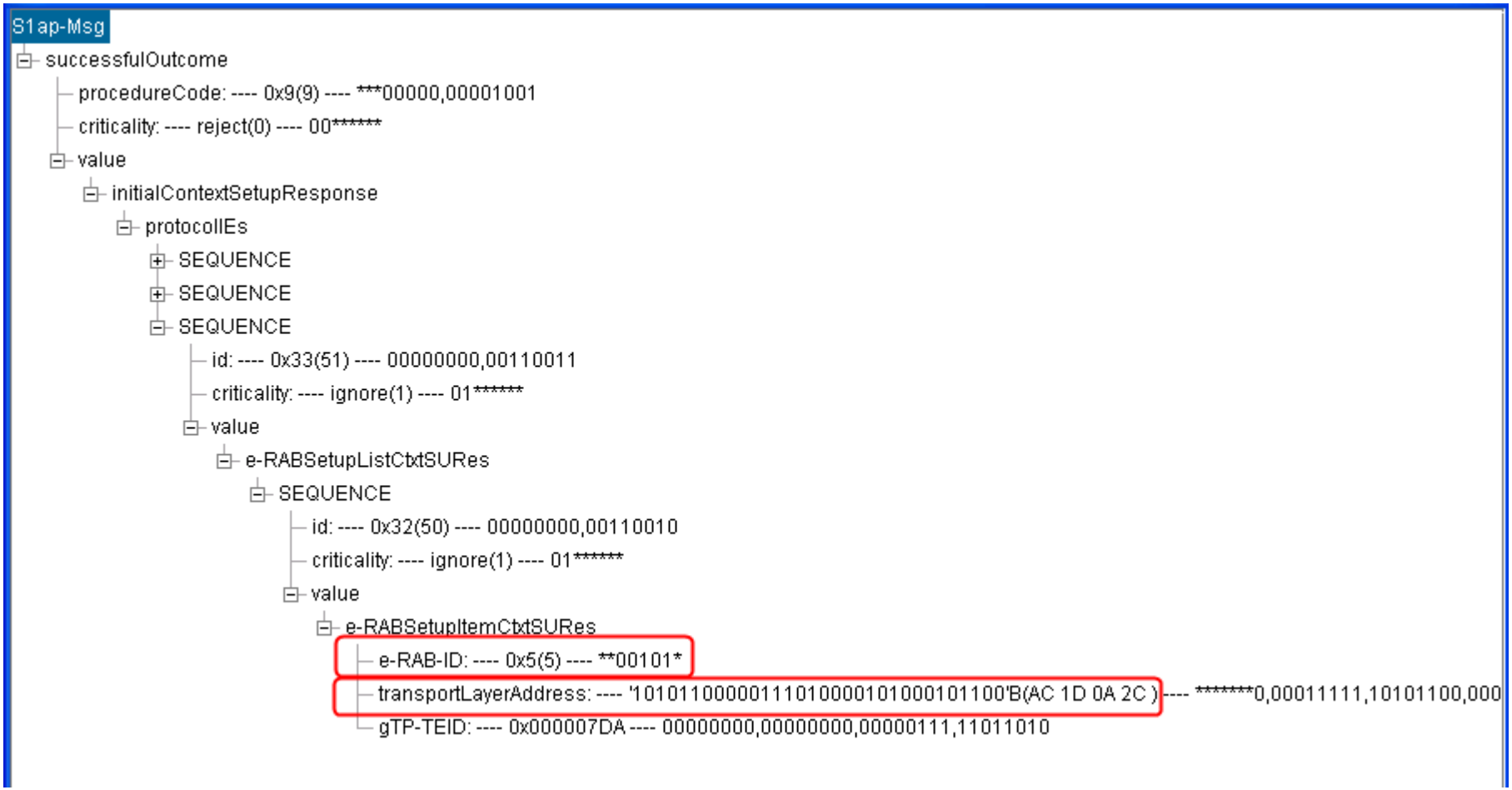
其中，对于featureGroupIndicators，共32bit，每个bit代表不同的功能，具体的功能参加36.331 Annex B

附着流程——RRC Connection Reconfiguration

➢用于建立SRB2和DRB1

- rrcConnectionReconfiguration-r8
  - dedicatedInfoNASList
    - DedicatedInfoNAS: ---- 0x273002A91B0166BF5C9F136147518FA7459188CF22BC17AEC54C5
  - radioResourceConfigDedicated
    - srb-ToAddModList
      - SRB-ToAddMod
    - drb-ToAddModList
      - DRB-ToAddMod
    - mac-MainConfig
    - physicalConfigDedicated
      - cqi-ReportConfig
        - cqi-ReportModeAperiodic: ---- rm30(3) ---- *****011
        - nomPDSCH-RS-EPRE-Offset: ---- 0x0(0) ---- 001*****
        - cqi-ReportPeriodic
          - setup
      - soundingRS-UL-ConfigDedicated
        - setup
      - schedulingRequestConfig
        - setup
          - sr-PUCCH-ResourceIndex: ---- 0x0(0) ---- 00000000,000*****
          - sr-ConfigIndex: ---- 0x11(17) ---- ***00010,001*****
          - dsr-TransMax: ---- n64(4) ---- ***100**

附着流程——Initial UE Context Setup Response



附着流程——虚用户IMSI跟踪信令（有鉴权、加密）

来源	采集时间	Tick/MS	标准接口消息类型	消息方向
TMF文件	07/07/2012 10:31:20	847	RRC_CONN_REQ	接受自UE
TMF文件	07/07/2012 10:31:20	847	RRC_CONN_SETUP	发送到UE
TMF文件	07/07/2012 10:31:20	847	RRC_CONN_SETUP_CMP	接受自UE
TMF文件	07/07/2012 10:31:20	847	S1AP_INITIAL_UE_MSG	发送到MME
TMF文件	07/07/2012 10:31:20	847	S1AP_DL_NAS_TRANS	接收自MME
TMF文件	07/07/2012 10:31:20	847	RRC_DL_INFO_TRANSF	发送到UE
TMF文件	07/07/2012 10:31:20	847	RRC_UL_INFO_TRANSF	接受自UE
TMF文件	07/07/2012 10:31:20	847	S1AP_UL_NAS_TRANS	发送到MME
TMF文件	07/07/2012 10:31:20	847	S1AP_DL_NAS_TRANS	接收自MME
TMF文件	07/07/2012 10:31:20	848	RRC_DL_INFO_TRANSF	发送到UE
TMF文件	07/07/2012 10:31:20	848	RRC_UL_INFO_TRANSF	接受自UE
TMF文件	07/07/2012 10:31:20	848	S1AP_UL_NAS_TRANS	发送到MME
TMF文件	07/07/2012 10:31:20	848	S1AP_DL_NAS_TRANS	接收自MME
TMF文件	07/07/2012 10:31:20	848	RRC_DL_INFO_TRANSF	发送到UE
TMF文件	07/07/2012 10:31:20	848	RRC_UL_INFO_TRANSF	接受自UE
TMF文件	07/07/2012 10:31:20	848	S1AP_UL_NAS_TRANS	发送到MME
TMF文件	07/07/2012 10:31:20	848	S1AP_INITIAL_CONTEXT_SETUP_REQ	接收自MME
TMF文件	07/07/2012 10:31:20	848	RRC_UE_CAP_ENQUIRY	发送到UE
TMF文件	07/07/2012 10:31:20	860	RRC_UE_CAP_INFO	接受自UE
TMF文件	07/07/2012 10:31:20	855	S1AP_UE_CAPABILITY_INFO_IND	发送到MME
TMF文件	07/07/2012 10:31:20	867	RRC_SECUR_MODE_CMD	发送到UE
TMF文件	07/07/2012 10:31:20	868	RRC_CONN_RECFG	发送到UE
TMF文件	07/07/2012 10:31:20	880	RRC_SECUR_MODE_CMP	接受自UE
TMF文件	07/07/2012 10:31:20	889	RRC_CONN_RECFG_CMP	接受自UE
TMF文件	07/07/2012 10:31:20	893	RRC_CONN_RECFG	发送到UE
TMF文件	07/07/2012 10:31:20	885	S1AP_INITIAL_CONTEXT_SETUP_RSP	发送到MME

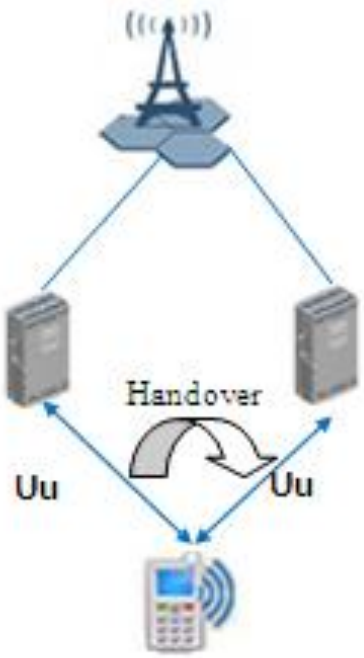
附着流程——虚用户IMSI跟踪信令（无鉴权、加密）

TMF文件	16/05/2012 09:32:09	385	RRC_CONN_REQ	接受自UE	
TMF文件	16/05/2012 09:32:09	385	RRC_CONN_SETUP	发送到UE	
TMF文件	16/05/2012 09:32:09	385	RRC_CONN_SETUP_CMP	接受自UE	
TMF文件	16/05/2012 09:32:09	385	S1AP_INITIAL_UE_MSG	发送到MME	
TMF文件	16/05/2012 09:32:09	385	S1AP_INITIAL_CONTEXT_SETUP_REQ	接收自MME	
TMF文件	16/05/2012 09:32:09	391	RRC_SECUR_MODE_CMD	发送到UE	
TMF文件	16/05/2012 09:32:09	392	RRC_CONN_RECFG	发送到UE	
TMF文件	16/05/2012 09:32:09	407	RRC_SECUR_MODE_CMP	接受自UE	
TMF文件	16/05/2012 09:32:09	418	RRC_CONN_RECFG_CMP	接受自UE	
TMF文件	16/05/2012 09:32:09	419	RRC_UE_CAP_ENQUIRY	发送到UE	
TMF文件	16/05/2012 09:32:09	417	S1AP_INITIAL_CONTEXT_SETUP_RSP	发送到MME	

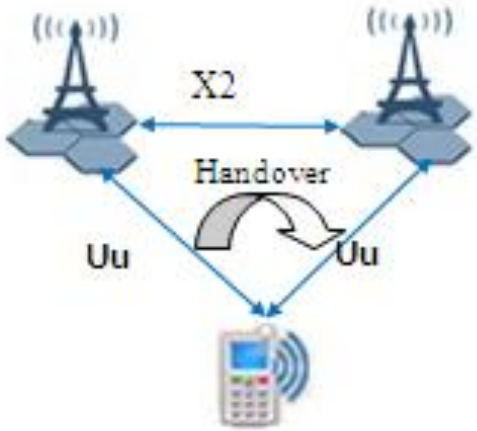
目录

切换概述

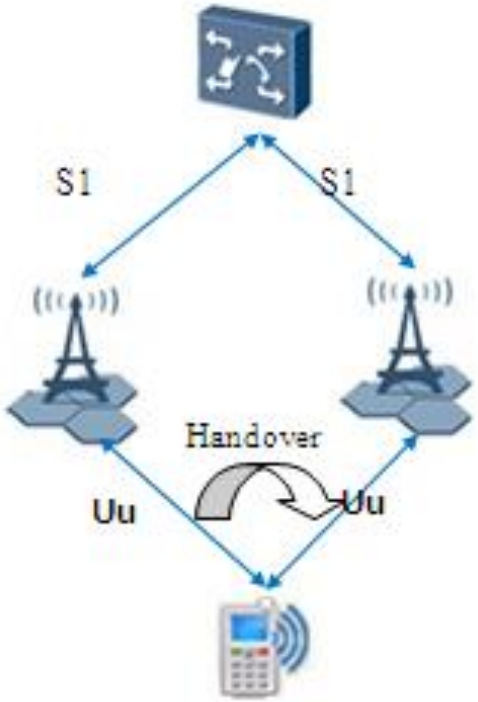
➢LTE系统内切换三种分类



站内切换



站间X2切换



站间S1切换

切换概述——LTE系统

➢切换包括切换测量、切换决策、切换执行三个阶段

- ●测量阶段，UE根据eNB下发的测量配置消息进行相关测量，并将测量结果上报给eNB；
- ●决策阶段，eNB根据UE上报的测量结果进行评估，决定是否触发切换；
- ●执行阶段，eNB根据决策结果，控制UE切换到目标小区，由UE完成切换；

➢**整个切换流程采用UE辅助网络控制的思路，基站下发测量控制，UE进行测量上报，基站执行切换判决、资源准备、切换执行和原有资源释放；**

➢ LTE 事件介绍

● 事件A1表示服务小区质量高于一定门限，满足事件触发条件的小区信息被上报时，eNodeb停止异频/异系统 测量，但在基于频率优化级的切换中，事件A1用于启动异频测量；

● 事件A2表示服务小区质量低于一定门限，满足事件触发条件的小区信息被上报时，eNodeb启动异频/异系统测量；

●事件A3表示当邻区质量高于服务小区质量，满足事件触发条件的小区信息被上报时；

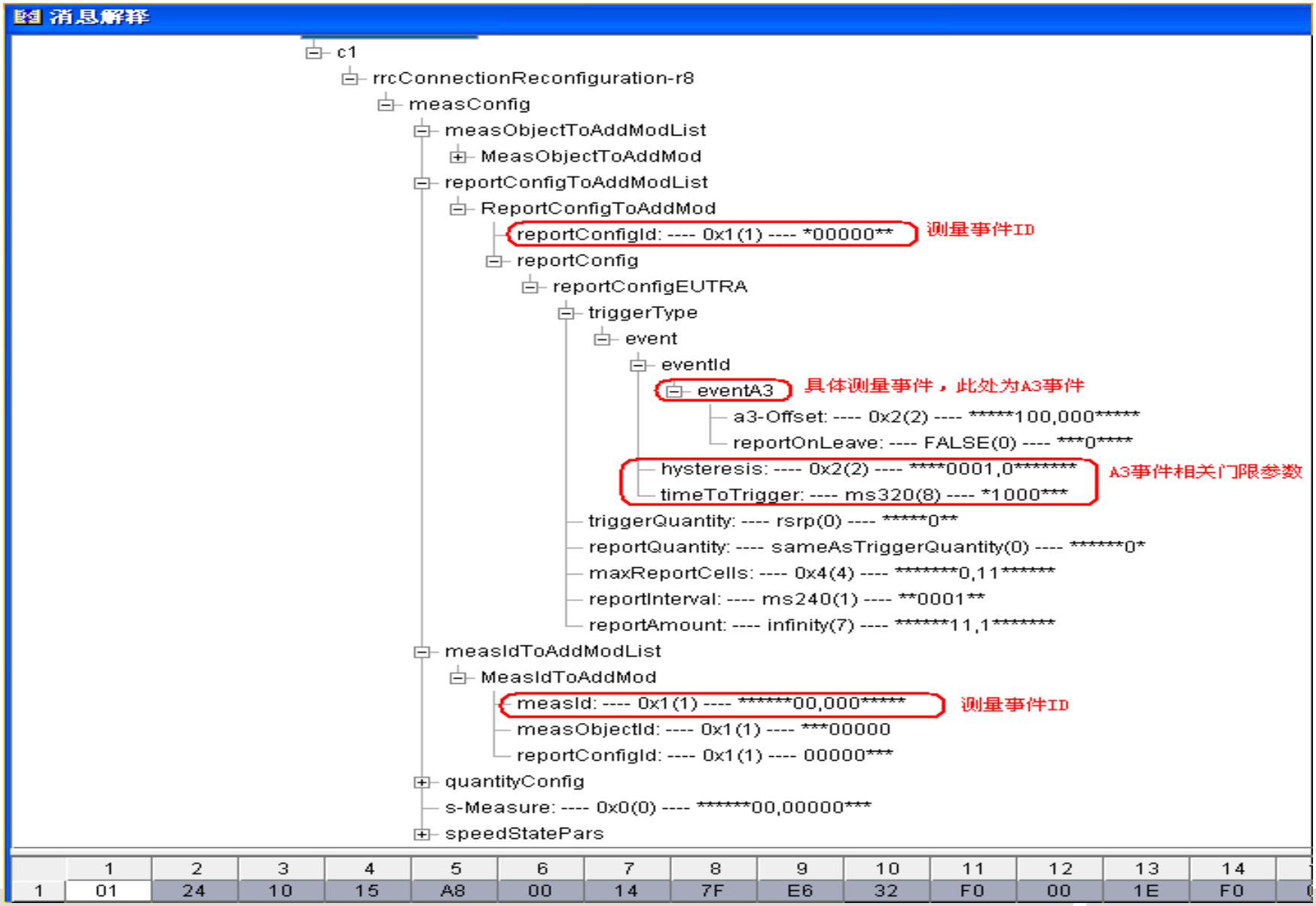
●事件A4表示当异频邻区质量高于一定门限，满足事件触发条件的小区信息被上报时；

● 时间A5表示主服务小区低于某一门限，而邻区高于某一门限；

●事件B1表示异系统邻区质量高于一定门限，满足事件触发条件的小区信息被上报

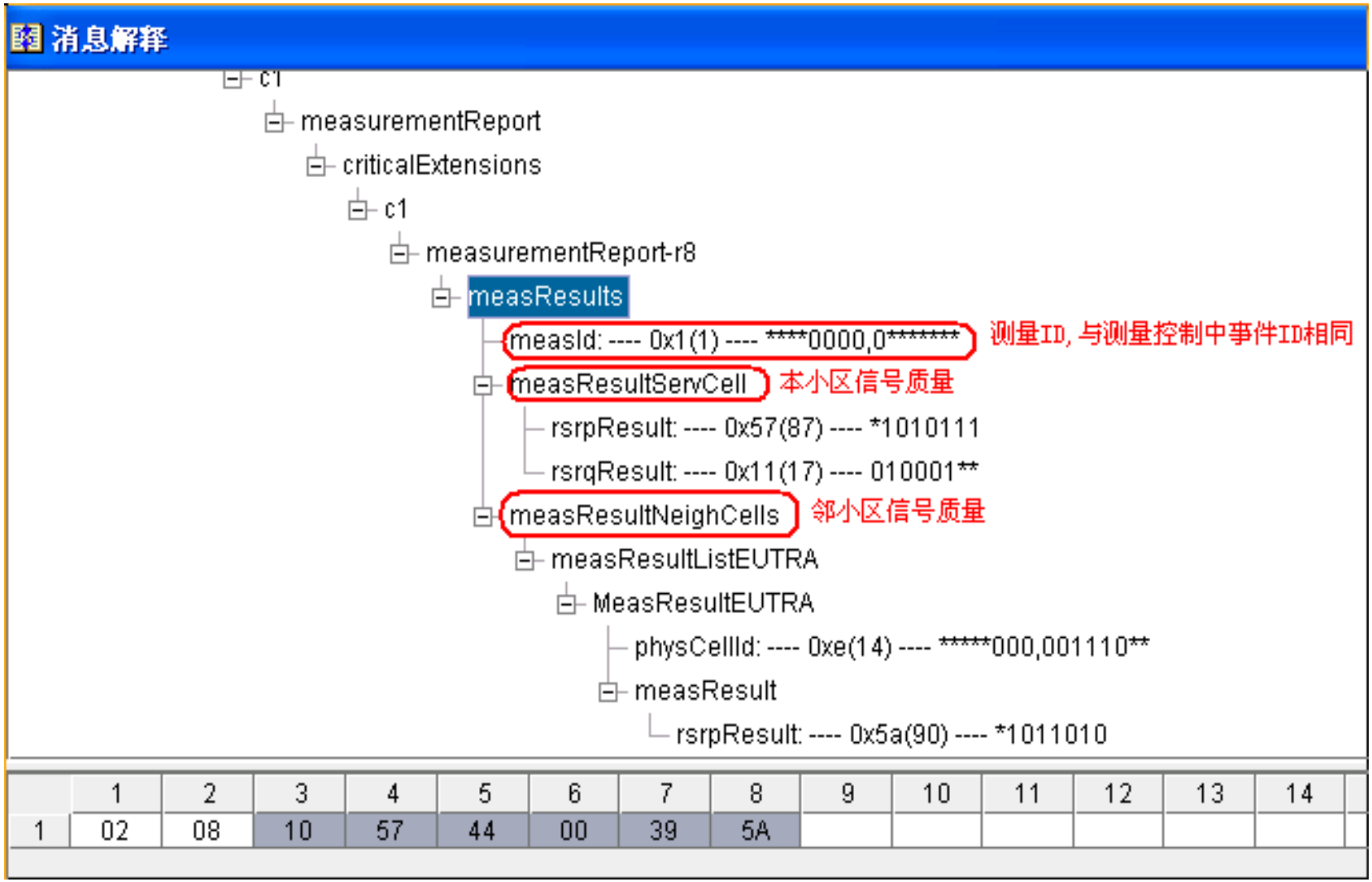
●事件B2表示服务小区差于一定门限，且异系统邻区质量高于一定门限，满足事件触发条件的小区的信息被上报；

切换概述—测量控制



	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	01	24	10	15	A8	00	14	7F	E6	32	F0	00	1E	F0

切换概述—测量报告



	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	02	08	10	57	44	00	39	5A						

切换概述—切换命令

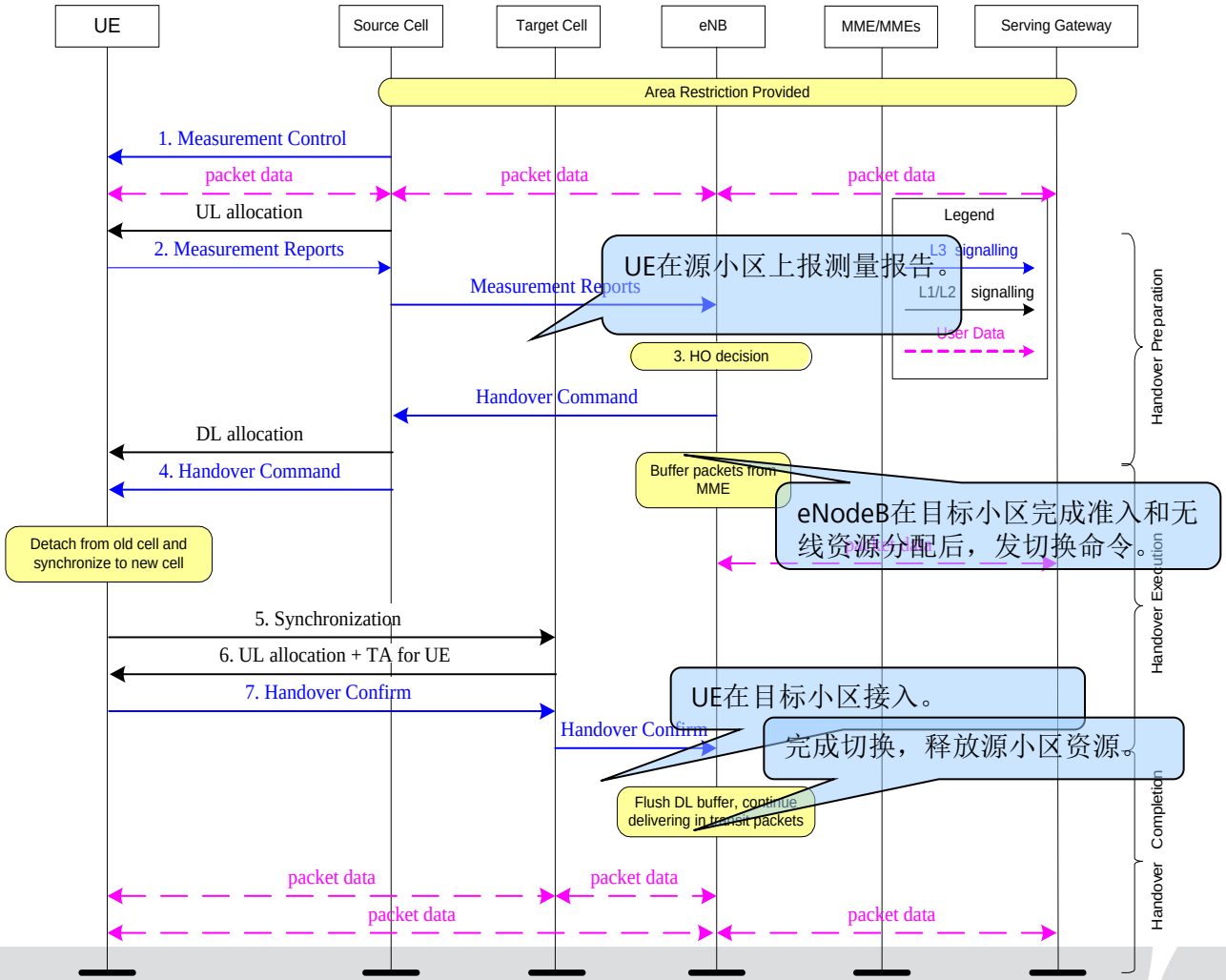

handoverCommand-r8
handoverCommandMessage
DL-DCCH-Message
message
c1
rrcConnectionReconfiguration
rrc-TransactionIdentifier: ---- 0x1(1) ---- **01****
criticalExtensions
c1
rrcConnectionReconfiguration-r8
mobilityControlInfo
targetPhysCellId: ---- 0x39(57) ---- ***00011,1001****
carrierFreq
dl-CarrierFreq: ---- 0x93da(37850) ---- *****100,10011110,11010***
ul-CarrierFreq: ---- 0x93da(37850) ---- *****100,10011110,11010***
carrierBandwidth
dl-Bandwidth: ---- n100(5) ---- ******01,01******
t304: ---- ms500(4) ---- **100***
newUE-Identity: ---- '00000000011011'B(00 5B) ---- *****000,00000010,11011
radioResourceConfigCommon
rach-ConfigDedicated
radioResourceConfigDedicated
securityConfigHO
handoverType
intraLTE

eNB内小区间切换

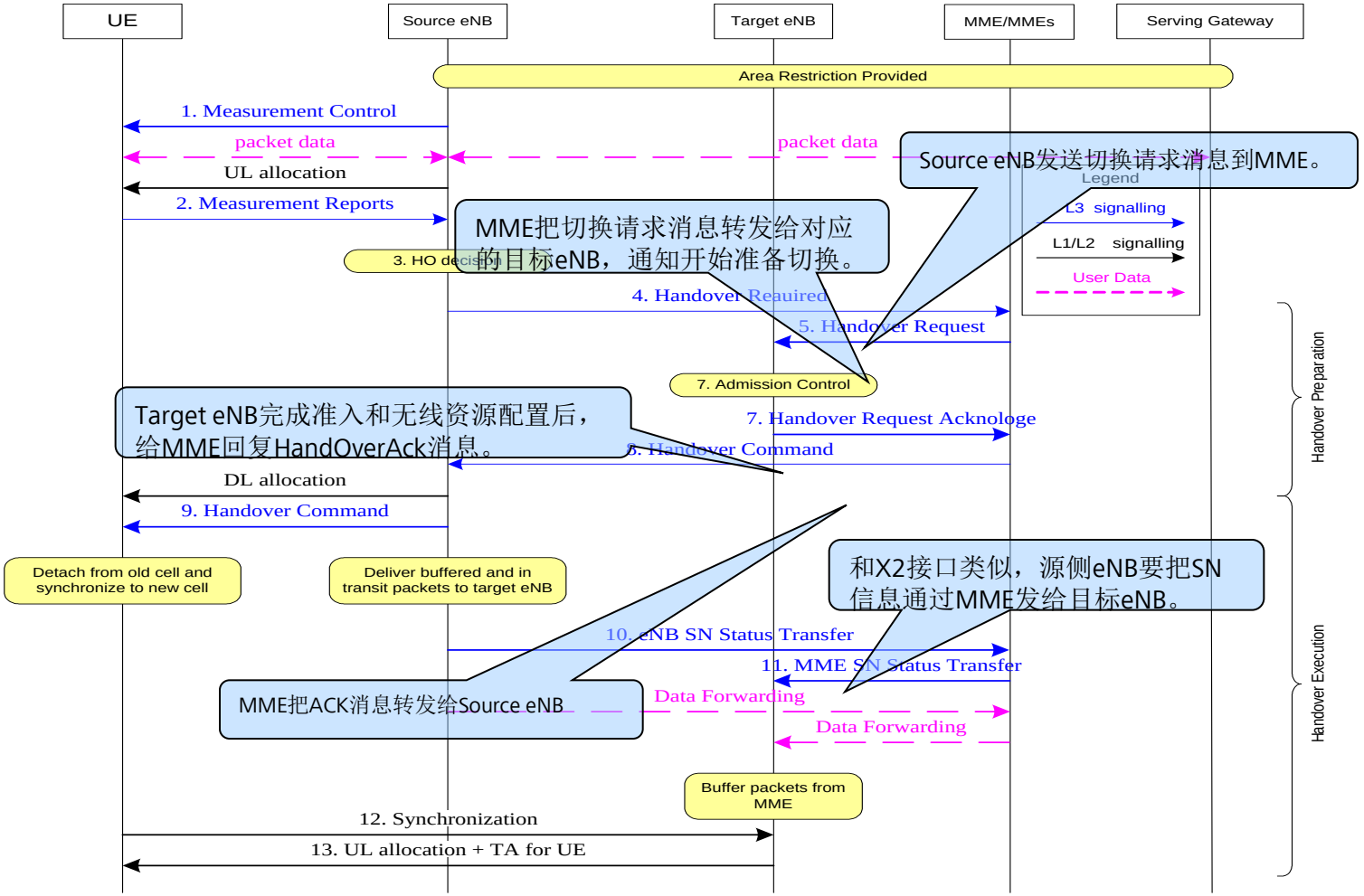
➢eNB内的小区间切换分同频切换和异频切换2种，作用如下

◆切换只是更新Uu口资源，源小区和目标小区的资源申请和资源释放都通过eNB内部消息实现；

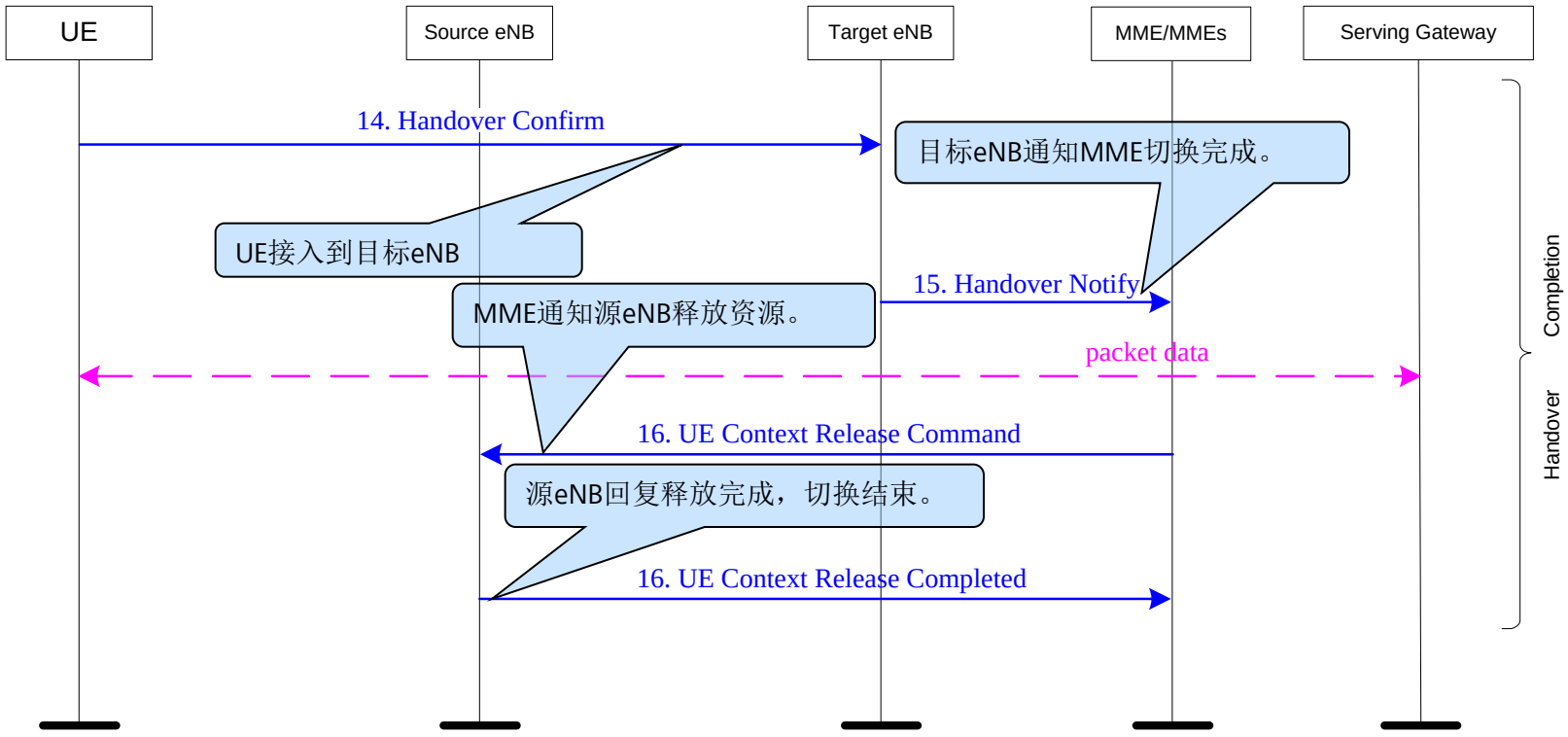
◆没有eNB间的数据转发，同时也没有UE的随机接入过程，也不需要与核心网有信令交互。



eNB间通过S1接口切换流程（I）



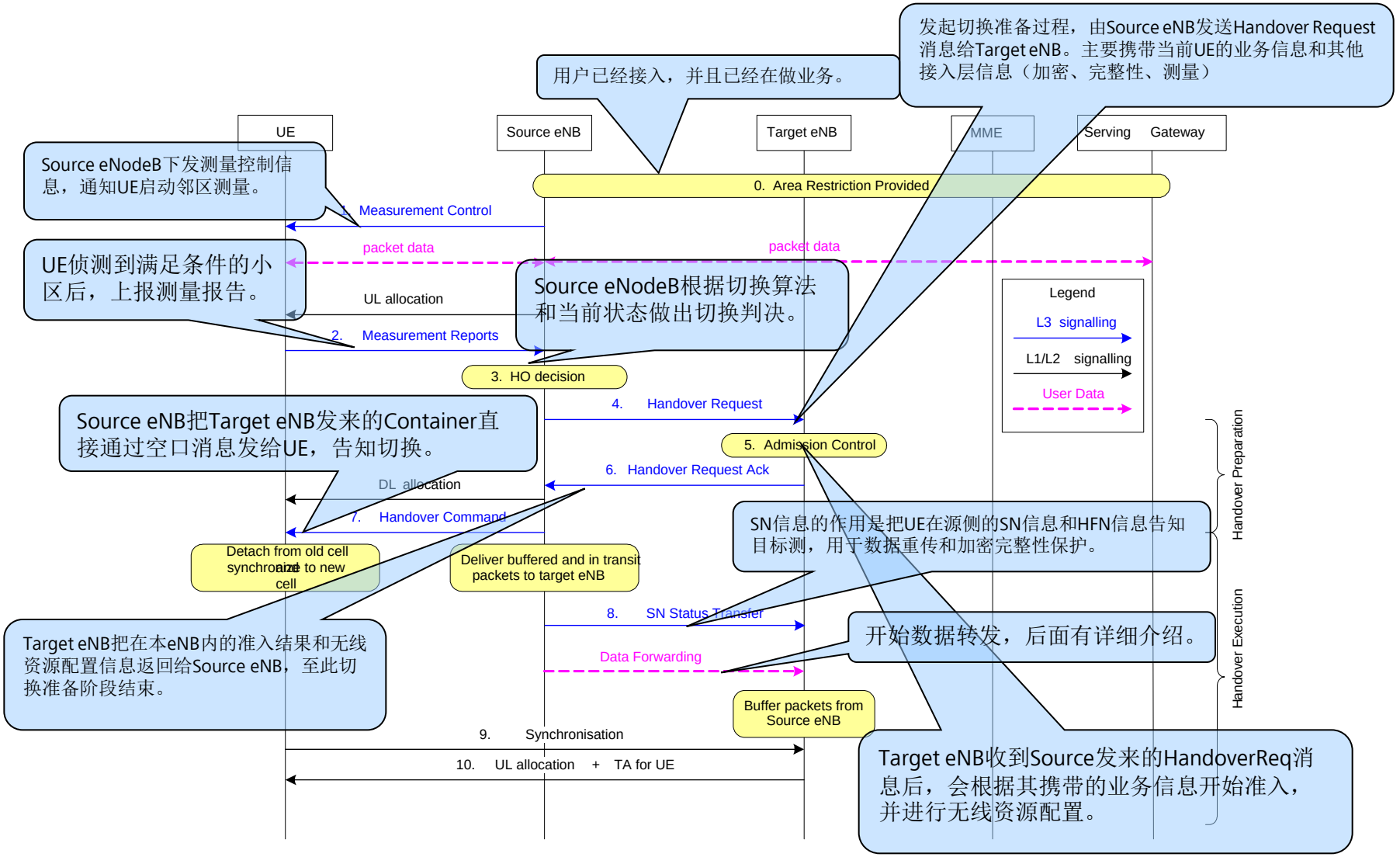
eNB间通过S1接口切换流程（II）



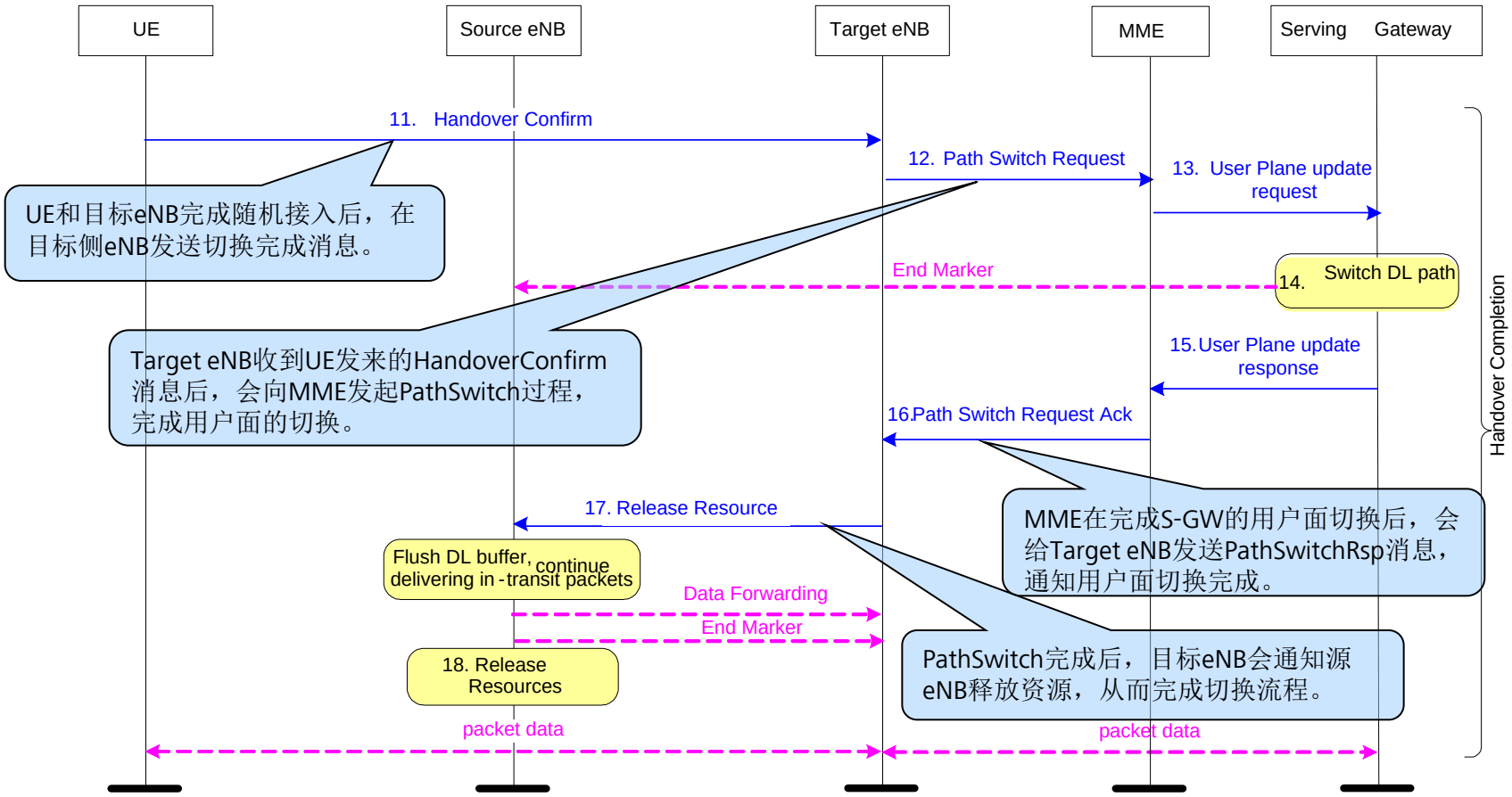
eNB间通过S1接口切换信令流程(I)

TMF文件	16/05/2012 09:32:18	413	RRC_MEAS_RPRT	接受自UE
TMF文件	16/05/2012 09:32:18	413	S1AP_HANDOVER_REQUIRED	发送到MME
TMF文件	16/05/2012 09:32:18	443	S1AP_HANDOVER_CMD	接收自MME
TMF文件	16/05/2012 09:32:18	448	RRC_CONN_RECFG	发送到UE
TMF文件	16/05/2012 09:32:18	447	S1AP_eNB_STATUS_TRANSFER	发送到MME
TMF文件	16/05/2012 09:32:21	源小区	RRC_CONN_RECFG	发送到UE
TMF文件	16/05/2012 09:32:21	19	RRC_CONN_RECFG_CMP	接受自UE
TMF文件	16/05/2012 09:32:28	507	S1AP_UE_CONTEXT_REL_CMD	接收自MME
TMF文件	16/05/2012 09:32:28	509	S1AP_UE_CONTEXT_REL_CMP	发送到MME
TMF文件	16/05/2012 09:32:33	191	S1AP_HANDOVER_REQ	接收自MME
TMF文件	16/05/2012 09:32:33	203	S1AP_HANDOVER_REQ_ACK	发送到MME
TMF文件	16/05/2012 09:32:33	247	S1AP_MME_STATUS_TRANSFER	接收自MME
TMF文件	16/05/2012 09:32:33	317	RRC_CONN_RECFG_CMP	接受自UE
TMF文件	16/05/2012 09:32:33	目标小区	RRC_CONN_RECFG	发送到UE
TMF文件	16/05/2012 09:32:33		S1AP_HANDOVER_NOTIFY	发送到MME
TMF文件	16/05/2012 09:32:33	318	others:2_62	发送到MME
TMF文件	16/05/2012 09:32:33	318	others:2_62	发送到MME
TMF文件	16/05/2012 09:32:33	318	others:2_62	发送到MME
TMF文件	16/05/2012 09:32:33	319	others:2_62	发送到MME
TMF文件	16/05/2012 09:32:33	342	RRC_CONN_RECFG_CMP	接受自UE
TMF文件	16/05/2012 09:32:33	343	RRC_CONN_RECFG	发送到UE
TMF文件	16/05/2012 09:32:33	362	RRC_CONN_RECFG_CMP	接受自UE
TMF文件	16/05/2012 09:32:33	365	RRC_CONN_RECFG	发送到UE
TMF文件	16/05/2012 09:32:33	438	RRC_CONN_RECFG_CMP	接受自UE

eNB间通过X2接口切换流程（I）



eNB间通过X2接口切换流程（II）



eNB间通过X2接口切换信令流程

TMF文件	20/08/2012 10:36:21	450	RRC_MEAS_RPRT	接受自UE
TMF文件	20/08/2012 10:36:21	450	HANDOVER REQUEST	发送到ENodeB
TMF文件	20/08/2012 10:36:21	475	HANDOVER REQUEST ACKNOWLEDGE	接收自ENodeB
TMF文件	20/08/2012 10:36:21	481	RRC_CONN_RECFG	发送到UE
TMF文件	20/08/2012 10:36:21	479	SN STATUS TRANSFER	发送到ENodeB
TMF文件	20/08/2012 10:36:21	559	UE CONTEXT RELEASE	接收自ENodeB
TMF文件	20/08/2012 10:36:21	251	HANDOVER REQUEST	接收自ENodeB
TMF文件	20/08/2012 10:36:21	261	HANDOVER REQUEST ACKNOWLEDGE	发送到ENodeB
TMF文件	20/08/2012 10:36:21	295	SN STATUS TRANSFER	接收自ENodeB
TMF文件	20/08/2012 10:36:21	326	RRC_CONN_RECFG_CMP	接受自UE
TMF文件	20/08/2012 10:36:21	326	S1AP_PATH_SWITCH_REQ	发送到MME
TMF文件	20/08/2012 10:36:21	355	S1AP_PATH_SWITCH_REQ_ACK	接收自MME
TMF文件	20/08/2012 10:36:21	356	UE CONTEXT RELEASE	发送到ENodeB
TMF文件	20/08/2012 10:36:21	357	others:2_62	发送到MME
TMF文件	20/08/2012 10:36:21	362	RRC_CONN_RECFG	发送到UE
TMF文件	20/08/2012 10:36:21	386	RRC_CONN_RECFG_CMP	接受自UE
TMF文件	20/08/2012 10:36:21	388	RRC_CONN_RECFG	发送到UE
TMF文件	20/08/2012 10:36:21	427	RRC_CONN_RECFG_CMP	接受自UE
TMF文件	20/08/2012 10:36:23	898	RRC_CONN_RECFG	发送到UE
TMF文件	20/08/2012 10:36:23	926	RRC_CONN_RECFG_CMP	接受自UE

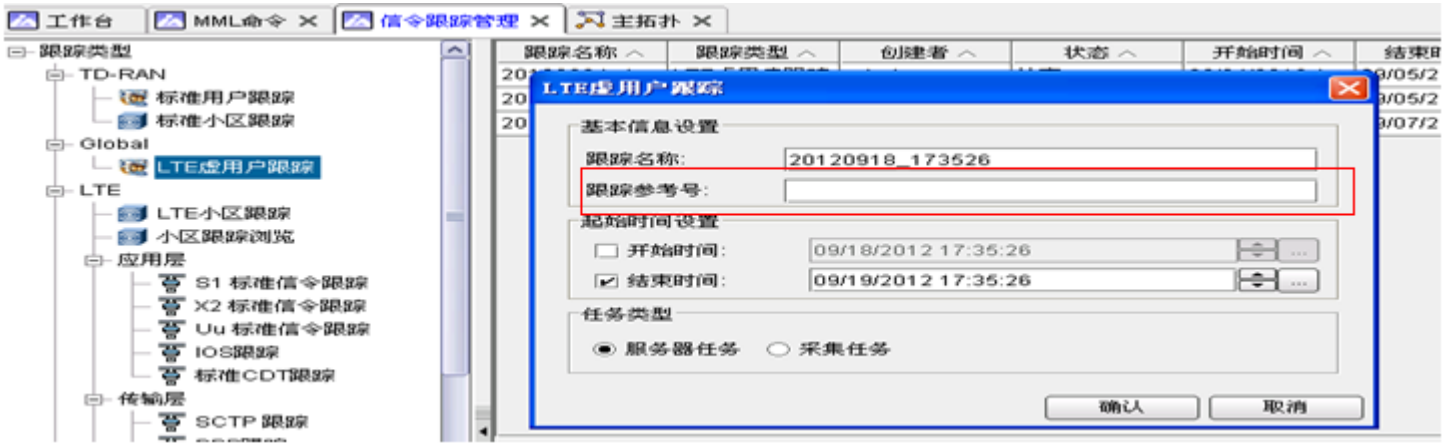
Thank you

www.huawei.com

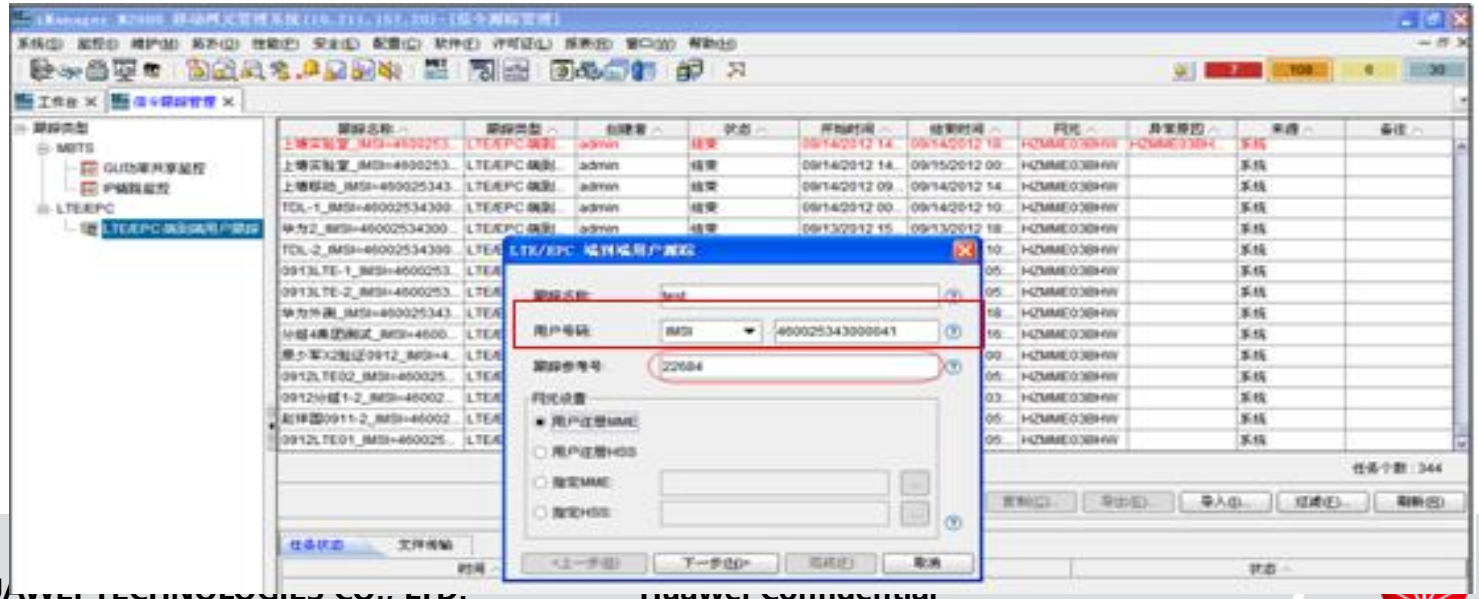
虚用户跟踪操作

Step1：登录M2000服务器，选择 监控->信令跟踪->信令跟踪管理；

Step2：双击左图所示“LTE虚用户跟踪”，填写“跟踪名称”、“跟踪参考号”；



Step3：跟踪参考号从MME的M2000获取，如下图,保存跟踪任务；



LTE信令分析工具

LTE无线侧跟踪的信令主要采用LTE TDD的LMT为Web LMT进行浏览,离线工具需要单独安装。

工具下载的地址（离线工具在SUPPORT网站上，在每个版本的软件包中，向下兼容）

support—软件中心—版本软件—无线—LTE TDD—LTE TDD eNodeB—DBS3900 LTE TDD—具体版本-- 3900 Series LTE eNodeB XXXX offline_tool.rar

解析的信令如下图所示：

171	2012-02-15 17:28:59(4914307)	RRC_CONN_REQ	RECEIVE
172	2012-02-15 17:28:59(4918852)	RRC_CONN_SETUP	SEND
173	2012-02-15 17:28:59(4948974)	RRC_CONN_SETUP_CMP	RECEIVE
174	2012-02-15 17:28:59(4979256)	RRC_SECUR_MODE_CMD	SEND
175	2012-02-15 17:28:59(4994567)	RRC_SECUR_MODE_CMP	RECEIVE
176	2012-02-15 17:28:59(4995260)	RRC_UE_CAP_ENQUIRY	SEND
177	2012-02-15 17:28:59(5008954)	RRC_UE_CAP_INFO	RECEIVE
178	2012-02-15 17:28:59(5014262)	RRC_CONN_RECFG	SEND
179	2012-02-15 17:28:59(5044467)	RRC_CONN_RECFG_CMP	RECEIVE
180	2012-02-15 17:28:59(5047425)	RRC_CONN_RECFG	SEND
181	2012-02-15 17:28:59(5064402)	RRC_UL_INFO_TRANSF	RECEIVE
182	2012-02-15 17:28:59(5074644)	RRC_CONN_RECFG_CMP	RECEIVE
183	2012-02-15 17:29:00(5930218)	RRC_MEAS_RPRT	RECEIVE
184	2012-02-15 17:29:00(5931808)	RRC_CONN_RECFG	SEND
185	2012-02-15 17:29:00(5994286)	RRC_CONN_RECFG_CMP	RECEIVE