LTE信令流程解析

loseblue

Version 0.1, 2015年7月29日 14

系统信息

概述

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，　　都会接收系统信息(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信息有种: MIB, SIB1和SI, 其作用分别如下.

- 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.
    - 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.(WCDMA)
    - 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.

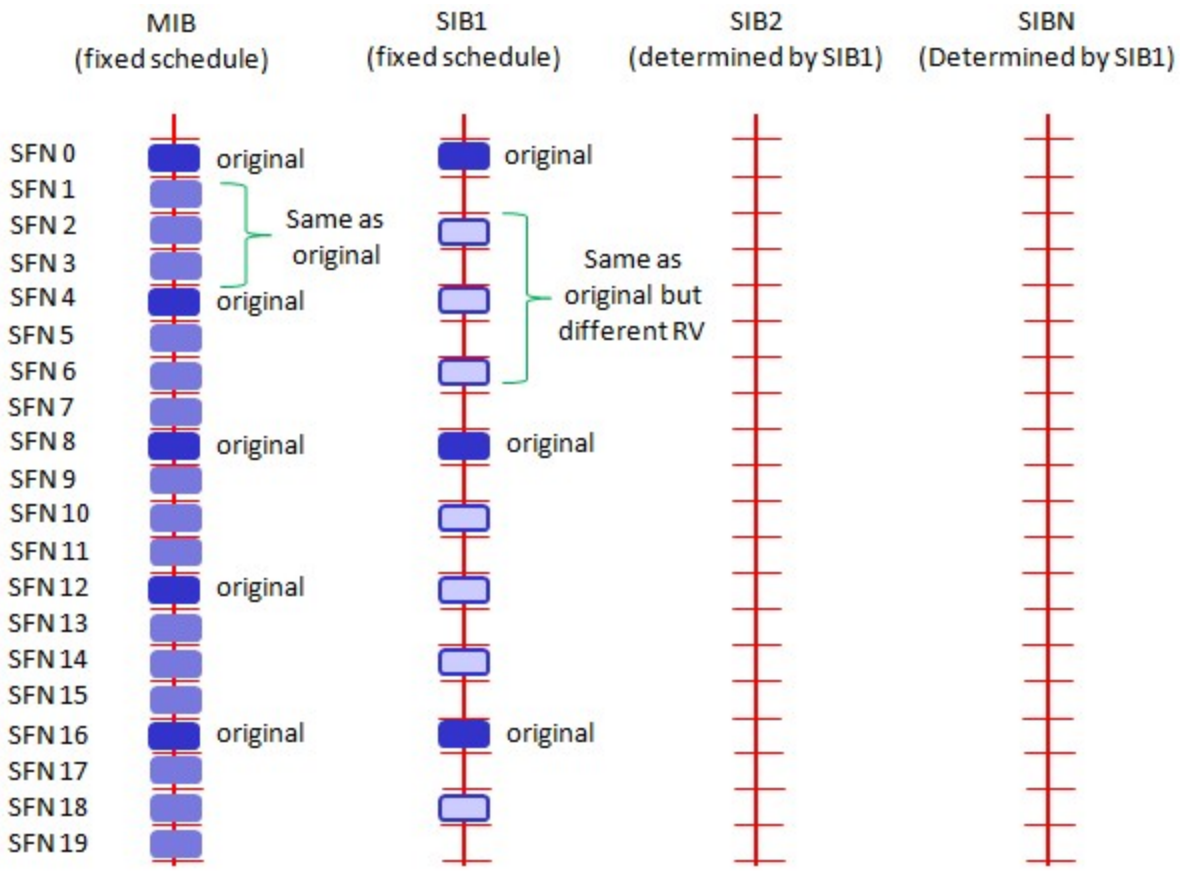


Figure 1. 系统信息时序图

系统信息(System Information)解析

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)

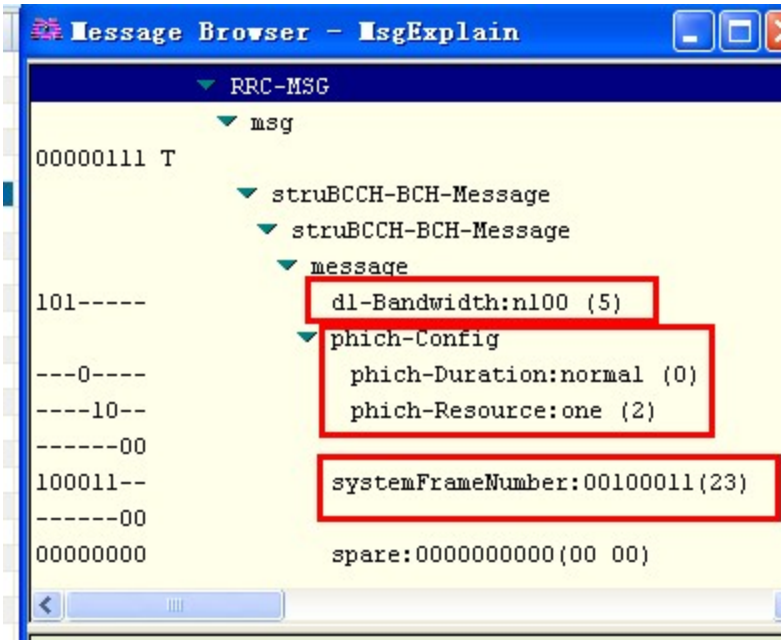


Figure 2. mib

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_Config

- 参见 PHICH分析一
- 参见 PHICH分析二

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.

Table 1. Phich_Duration

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

PHICH-Resource

该参数用于计算小区PHICH信道的资源;

SystemFrameNumber

系统帧号. 系统帧号, 用于UE获取系统时钟. 实际SFN位长为10bit, 也就是取值从0-1023循环. 在PBCH的MIB广播中只广播前8位，剩下的两位根据该帧在PBCH 40ms周期窗口的位置确定，第一个10ms帧为00，第二帧

为01, 第三帧为10, 第四帧为11. PBCH的40ms窗口手机可以通过盲检确定.

Spare

预留的, 暂时未用

SIB1 (System Information Block 1) 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信息的调度信息. 主要包括4部分:

- 小区接入相关信息(cell Access Related Info)
  - PLMN Identity List, PLMN Identity, TA Code, Cell identity & Cell Status
- 小区选择信息(cell Selection Info)
  - Minimum Receiver Level
- 调度信息(scheduling Info List)
  - SI message type & Periodicity, SIB mapping Info, SI Window length
- TDD配置信息(tdd-Config)

SIB1

```
MS1
System Information Block Type1 (DL-BCCH-SCH)

Time : 15:57:43.004
Vendor Header
  Length : 47
  Log Code (Hex) : 0xB0C0
  HW Timestamp : (63622381.25 ms) 17:40:22.381
    1.25 ms fraction : 0.00
    CFN : 136
    1.25 ms counter : 867576017905
  RRC Signaling Header
    Log Packet Version : 2
    RRC Release Number : 9.5.0
    Radio Bearer Id : 0
    Physical Cell Id : 2
    E-ARFCN : 39150
    System Frame Number
      System frame number : N/A
      Sub frame number : N/A
    Message Type : BcchSchDownlink
    Message Length : 22
plmn-IdentityList                                                    ①
  PLMN-IdentityList :
    [0 ] :
      plmn-Identity
        mcc
          MCC :
            [0 ] : 0
            [1 ] : 0
            [2 ] : 1
```

```
        mnc
          MNC :
            [0 ] : 0
            [1 ] : 1
      cellReservedForOperatorUse : notReserved
trackingAreaCode : 12594 (0x3132)                                    ②
cellIdentity : 2 (0x2)                                               ③
cellBarred : notBarred                                               ④
intraFreqReselection : allowed                                       ⑤
csg-Indication : False                                               ⑥
q-RxLevMin : -65                                                     ⑦
q-RxLevMinOffset : 1                                                 ⑧
p-Max : 23                                                           ⑨
freqBandIndicator : 40                                               ⑩
schedulingInfoList                                                   ⑪
  SchedulingInfoList :
    [0 ] :
      si-Periodicity : rf16                                          ⑫
      sib-MappingInfo
        SIB-MappingInfo :
          [0 ] :
            extensionBit0 : 0
            Optionalitem : sibType3                                  ⑬
          [1 ] :
            extensionBit0 : 0
            Optionalitem : sibType5
    [1 ] :
      si-Periodicity : rf128
      sib-MappingInfo
        SIB-MappingInfo :
          [0 ] :
            extensionBit0 : 0
            Optionalitem : sibType6
          [1 ] :
            extensionBit0 : 0
            Optionalitem : sibType7
tdd-Config
  subframeAssignment : sa2                                           ⑭
  specialSubframePatterns : ssp7                                     ⑮
si-WindowLength : ms20                                               ⑯
systemInfoValueTag : 0                                               ⑰


Message dump (Hex):
    70 40 04 03 31 32 00 00 00 29
    14 6B 38 48 80 28 21 91 3D 00
    00 00
```

① PLMN标识列表(0-6)

② TAC跟踪区(0-65546) 消息中(0x3132)为16进制数, 转换成十进制为12594

③ 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

④ 小区禁止: 小区是否禁止UE驻扎, notBarred表示不禁止

⑤ 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

⑥ 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.

⑦ 指示小区要求的最小接收功率RSRP(-140..-44)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: $Q_{rxlevmin}$ = IE value * 2[dB]

⑧ 小区选择所需要的最小接收电平偏移,(2-16)dB

⑨ 小区支持UE允许的最大发射功率,如果eNB配置大于UE支持最大值, UE就设置为UE支持的最大值. 例如Cat3 UE支持最大23db

⑩ 频带指示, 表示当前系统的使用40频段

⑪ 调度信息表

⑫ SI消息的调度周期, 以无线帧为单位. 如rf16表示周期为16个无线帧

⑬ 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.

⑭ 用于指示上下行子帧的配置, sa2对应配置2. 详见 TD LTE uplink-downlink configuration

⑮ 特殊子帧配比. 详见 TD LTE uplink-downlink configuration

⑯ 系统消息调度窗口,20ms

⑰ 指示其它SIB是否发生了改变 详见 systemInfoValueTag解析

Table 2. TD LTE uplink-downlink configuration

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

Table 3. TD LTE uplink-downlink configuration

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	0	3	2
7	10	2	2
8	11	1	2
9	6	6	2

systemInfoValueTag解析

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SI已经更新, 重新读取SI.
2. 当重新获取得的systemInfoValueTag3与systemInfoValueTag1相同, 而systemInfoValueTag2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systemInfoValueTag2与重新接收的systemInfoValueTag3相同, 而与寻呼消息中的systemInfoValueTag1不同的话, 认为MIB还没有广播下来, 等下一个MIB.

SIB2 (System Information Block 2) 解析

- SIB2包含对所有UE适用的无线资源配置信息
- SIB2包含通用和共享信道配置, RACH相关配置, 定时器, 上行功控
- 没有SIB2会导致UE无法初始化ATTACH流程
- SIB2消息不一定显式的包含在SIB1调度信息中, 但是它总是映射在IB1消息中schedulingInfoList的第一个实体

SIB2

```
MS1
System Information Block 2

Time : 17:45:31.000
ac-BarringForEmergency : False
ac-BarringForMO-Signalling
  ac-BarringFactor : p95
  ac-BarringTime : s8
  ac-BarringForSpecialAC : 00000
    [0 ] : 0
    [1 ] : 0
```

```
    [2 ] : 0
    [3 ] : 0
    [4 ] : 0
ac-BarringForMO-Data
  ac-BarringFactor : p95
  ac-BarringTime : s8
  ac-BarringForSpecialAC : 00000
    [0 ] : 0
    [1 ] : 0
    [2 ] : 0
    [3 ] : 0
    [4 ] : 0
radioResourceConfigCommon
  rach-ConfigCommon                                                    ①
    numberOfRA-Preambles : n52                                         ②
    sizeOfRA-PreamblesGroupA : n44                                     ③
    messageSizeGroupA : b56                                            ④
    messagePowerOffsetGroupB : dB5                                     ⑤
    powerRampingStep : dB2                                             ⑥
    preambleInitialReceivedTargetPower : dBm-90                        ⑦
    preambleTransMax : n20                                             ⑧
    ra-ResponseWindowSize : sf10                                       ⑨
    mac-ContentionResolutionTimer : sf48                               ⑩
    maxHARQ-Msg3Tx : 8                                                 ⑪
  bcch-Config
    modificationPeriodCoeff : n4                                       ⑫
  pcch-Config
    defaultPagingCycle : rf64                                          ⑬
    nB : oneT                                                          ⑭
  prach-Config
    rootSequenceIndex : 22                                             ⑮
    prach-ConfigInfo
      prach-ConfigIndex : 0                                            ⑯
      highSpeedFlag : False                                            ⑰
      zeroCorrelationZoneConfig : 1                                    ⑱
      prach-FreqOffset : 10                                            ⑲
  pdsch-ConfigCommon
    referenceSignalPower : -10                                         ⑳
    p-b : 1                                                            (1)
  pusch-ConfigCommon
    n-SB : 2                                                           (2)
    hoppingMode : interSubFrame                                        (3)
    pusch-HoppingOffset : 6                                            (4)
    enable64QAM : True                                                 (5)
    ul-ReferenceSignalsPUSCH
      groupHoppingEnabled : False                                      (6)
      groupAssignmentPUSCH : 0                                         (7)
      sequenceHoppingEnabled : False                                   (8)
      cyclicShift : 0                                                  (9)
  pucch-ConfigCommon
    deltaPUCCH-Shift : ds1                                             (10)
    nRB-CQI : 2                                                        (11)
    nCS-AN : 0                                                         (12)
    n1PUCCH-AN : 2                                                     (13)
  soundingRS-UL-ConfigCommon
    SoundingRS-UL-ConfigCommon : release
  uplinkPowerControlCommon
    p0-NominalPUSCH : -80                                              (14)
    alpha : al1                                                        (15)
    p0-NominalPUCCH : -100                                             (16)
```

```
    deltaFList-PUCCH
      deltaF-PUCCH-Format1 : deltaF-2                          (17)
      deltaF-PUCCH-Format1b : deltaF3
      deltaF-PUCCH-Format2 : deltaF-2
      deltaF-PUCCH-Format2a : deltaF2
      deltaF-PUCCH-Format2b : deltaF2
    deltaPreambleMsg3 : 4                                      (18)
  ul-CyclicPrefixLength : len1                                 (19)
ue-TimersAndConstants
  t300 : ms1000                                                (20)
  t301 : ms1000                                                1.
  t310 : ms1000                                                2.
  n310 : n1                                                    3.
  t311 : ms1000                                                4.
  n311 : n8
additionalSpectrumEmission : 1                                 5.
timeAlignmentTimerCommon : infinity                            6.
```

① 随机接入配置

② 保留给竞争模式使用的随机接入前导码个数, n52即52个

③ 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前导码, 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.n44:前导码组A包含44个前导码, B组52-44=8个前导码

④ Msg3消息块大小门限, 针对Preamble码集合A. 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 – preambleInitialReceivedTargetPower–deltaPreambleMsg3 – messagePowerOffsetGroupB的门限值, 则选择Group B; 否则就选择Group A. b56表示56bit.

⑤ 用于配合判决UE随机接入Preamble B组的选择

⑥ 随机前导码的发射功率调整步长. dB2表明2个dB

⑦ eNodeB期望接收到的初始随机前导码的功率.当PRACH前导格式为0时, 在满足前导检测性能时, eNodeB所期望的目标功率水平.

⑧ 随机接入前导最大重发次数. 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

⑨ 随机接入响应窗大小. 若在窗口期未收到RAR, 则上行同步失败.Sf10表示10个子帧的长度. 响应窗起点与Msg1间隔10ms(发送了接入前导序列以后, UE需要监听PDCCH信道,是否存在ENODEB回复的RAR消息, (Random Access Response), RAR的时间窗是从UE发送了前导序列的子帧 + 3个子帧开始, 长度为Ra-ResponseWindowSize个子帧)

⑩ RA过程中UE等待接收Msg4的有效时长. 当UE初传或重传Msg3时启动. 在超时前UE收到Msg4或Msg3的NACK反馈, 则定时器停止. 定时器超时, 则随机接入失败, UE重新进行RA. 当前参数设置sf48, 即48个子帧长度.

⑪ Msg3的HARQ最大传输次数, 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

⑫ 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 = modificationPeriodCoeff * defaultPagingCycle.

⑬ 默认的寻呼周期. 当前参数设置rf128, 即128个无线帧长度

⑭ 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

⑮ 用于生成Signature的逻辑Za-doff序列索引，每一个逻辑索引对应一个物理Zadoff-chu序列. 该值一般是按网络规划配置设置的. 当前参数设置为7, 对应物理Zadoff-chu序列为629.见36.211 Table 5.7.2-4

⑯ 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. 见36.211 Table 5.7.1-2

⑰ 高速移动小区指示. 即是否是覆盖高速移动场景, 当前参数设置为False, 表示非覆盖高速移动场景

⑱ 零自相关区配置索引. 随机接入前导是由具有CAZAC(恒幅零自相关)的Zadoff-chu序列生成的，通过逻辑根序列获取物理根序列, 然后对物理根序列进行循环移位获得. 零自相关区配置索引与Ncs的选择直接相关. 取值范围0～15, 当前参数设置为2, 即对应Ncs=15(无限集)或Ncs=22(有限集), 见36.211 Table 5.7.2-2

⑲ 该参数用于广播PRACH所占用的频域资源起始位置的偏置值码当前参数设置为10, 即在第10个PRB位置

⑳ 每逻辑天线(port)的小区参考信号功率. 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.参数设置值为-10, 即RS信号功率为-10dbm

⑴ 表示PDSCH上EPRE(Energy Per Resource Element)的功率因子比率指示, 它和天线端口共同决定了功率因子比率的值,P-b实际表征的是有RS的PDSCH符号功率与没有RS的PDSCH符号的功率偏移量 见36.213 Table 5.2-1

⑵ 给定跳频模式下, 用于跳频的PUSCH子带个数. 该参数与跳频偏置决定了子带的大小, 而子带大小与跳频偏置, Vrb数一起决定PUSCH信道PRB的分配. 该参数设置为2, 即子带数为2.

⑶ PUSCH跳频模式选择. 该参数设置为interSubFrame, 表示采用子帧间跳频模式. 还有另一种模式为子帧内跳频. 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

⑷ PUSCH信道的跳频偏移. 与FDD/TDD模式, 子帧配置, CP长度相关. 参与决定PUSCH信道资源分配.

⑸ 上行PUSHC是否使用64QAM调制方式. CAT5类终端支持. 当前参数设置为TRUE, 表示上行支持64QAM使用.

⑹ 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

⑺ PUSCH信道的分组指派; 一个eNodeB下所有小区的GroupAssignPUSCH取0时, 这些的PUSCH上的UL RS由不同的base序列组生成, 每个小区在生成UL RS时可以使用全部的CS(Cyclic Shift)取值, 可用的CS越多, 能够支持配对的V-MIMO用户越多.

⑻ 是否允许USCH信道的序列跳频; 当不执行Group hopping时, 允许支持sequence hopping

⑼ PUSCH信道的循环移位; 当一个eNodeB下的所有小区使用相同的base序列组生成PUSCH上的UL RS时, 为了保证在半静态调度时这些小区使用不同的CS(Cyclic Shift)取值, 需要为这些小区配置不同的CyclicShift取值

⑽ PUCCH信道的循环移位间隔. 在组网时根据环境类型获得小区的平均时延扩展, 然后根据小区的平均时延扩展得到PUCCH信道的循环移位间隔. 与硬件处理能力相关.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.

⑾ 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.RRC层给CQI配置的RB总数. 当PUCCH资源调整开关关闭时, CQI RB个数才能够进行手动配置. 参数设置为1, 表示1个RB用于承载CQI.该参数定义与36.211 5.4章节描述不一致.规范中定义为不同PUCCH格式下一个Slot可用带宽, 即RB数

⑿ 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. 是delta PUCCH Shift的整数倍

⒀ PUCCH占用RB数索引, 表示PUCCH 使用的RB 个数.

⒁ PUSCH的标称P0值, 应用于上行功控过程. 与p0-NominalPUCCH含义一致

⒂ 即α, 路径损耗补偿因子, 应用于上行功控过程. 是一个 3bit 的小区专用参数, 01代表0.1

⒃ 正常进行PUCCH解调, eNodeB所期望的PUCCH发射功率水平; P0NominalPUCCH设置的过高, 会增加本小区的吞吐量, 但是会降低整网的吞吐量; P0NominalPUCCH设置偏低, 降低对邻区的干扰, 导致本小区的吞吐量的降低, 提高整网吞吐量.

⒄ PUCCH格式1的Delta值; 用于计算PUCCH信道功率, 相当于对每种PUCCH格式补偿值. 当前设置值deltaF-2, 表示-2dB

⒅ 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

⒆ 小区的上行循环前缀长度, 分为普通循环前缀和扩展循环前缀, 扩展循环前缀主要用于一些较复杂的环境, 如多径效应明显, 时延严重等. 当前参数设置为len1, 即采用扩展循环前缀.

⒇ RRC连接建立定时器. 开始于RRCConnectionRequest发送, 在收到RRCConnectionSetup或RRCConnectionReject消息, cell re-selection或连接放弃后停止, 定时器超时后,则认为本次 RRC 建立失败, UE直接进入RRC_IDLE态. 参数设置值为1000ms.

1. RRC连接重建定时器. 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(适合小区定义参见3GPP TS 36.331), 则停止该定时器. 定时器超时后, UE进入RRC_IDLE态. 参数设置为1000ms.
2. 无线链路失败定时器.在收到底层连续N310个失步指示后启动, 若在定时器时间内收到连续N311个同步指示, 无线链路恢复, 否则定时器超时, 即意味着无线链路失败. 参数设置值为1000ms
3. 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.
4. 无线链路失败恢复定时器. 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 进行小区重选或者TA更新, 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.
5. 附加频率散射, 限制UE功率在相应信道带宽内的水平. 即用于计算ue的上行发射功率. 这个参数对应一个Additional Maximum Power Reduction (A-MPR), 该值可以计算对应频带的上行发射功率. 该参数与Additional Maximum Power Reduction (A-MPR)的对应关系, 见 TS 36.101 Table6.2.4-1和TS 36.521 Table 6.2.4.3-1.当前参数设置值为1, 对应NS_01, 即A-MPR为NA.
6. 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

SIB3 (System Information Block 3) 解析

- SIB3包含了用于同频, 异频, 异系统间小区重选的基本共用信息
- 除临区相关信息之外的同频小区重选信息

SIB3

```
MS1
System Information Block 3                                  ①

Time : 17:45:36.299
q-Hyst : dB3                                                ②
s-NonIntraSearch : 22                                       ③
threshServingLow : 15                                       ④
cellReselectionPriority : 7                                 ⑤
q-RxLevMin : -60                                            ⑥
p-Max : 23                                                  ⑦
s-IntraSearch : 19                                          ⑧
allowedMeasBandwidth : mbw100                               ⑨
presenceAntennaPort1 : False                                ⑩
neighCellConfig                                             ⑪
  Binary string (Bin) : 01
    [0 ] : 0
    [1 ] : 1
t-ReselectionEUTRA : 1                                      ⑫
```

① 小区重选信息

② 小区重选迟滞. 用于作用在(在服务小区测量RSRP值上加上该值)服务小区后作为重选判决依据

③ 异频搜索门限. 低于22dB开启

④ 由服务频率向低优先级重选时门限. 实际值=7*2=14dB

⑤ 小区重选优先级.Value is between 0-7 where 0 means: lowest priority.

⑥ 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: $Q_{rxlevmin}$ = IE value * 2, -60为-120dBm

⑦ 同频临小区上行传输功率最大值. 如果缺省, UE采用自己的传输功率最大值.

⑧ If the field s-IntraSearchP is present, the UE applies the value of s-IntraSearchP instead. Otherwise if neither 09s-IntraSearch nor s-IntraSearchP is present, the UE applies the (default) value of infinity for SIntraSearchP.

⑨ [later]

⑩ [later]

⑪ 用于提供临小区MBSFN和上下行配比信息. 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.

⑫ EUTRA小区重选定时器, 1s

SIB4 (System Information Block 4) 解析

- SIB4仅包含同频临小区重选信息
- SIB4包括具有特定重选参数以及黑名单小区
- SIB4包含的所有内容均是可选项, 因为UE可以自动探测和完成同频临小区监测

SIB4

```
MS1
System Information Block 4                                    ①

Time : 10:01:27.846
intraFreqNeighCellList                                        ②
  IntraFreqNeighCellList :
    [0 ] :
      physCellId : 14                                         ③
      q-OffsetCell : dB0                                      ④
    [1 ] :
      physCellId : 201
      q-OffsetCell : dB0
```

① 同频临小区重选信息

② 同频临小区重选列表, 最多16个

③ 临小区ID

④ 定义两小区间的偏移. Value -24 ~ +24dB

SIB5 (System Information Block 5) 解析

- SIB5仅包含LTE异频小区重选相关的信息
- SIB5包含普通的频率小区重选参数以及特定的小区重选参数

SIB5

```
MS1
System Information Block 5                                          ①

Time : 17:45:36.299
interFreqCarrierFreqList                                            ②
  InterFreqCarrierFreqList :                                        ②
    [0 ] :
      dl-CarrierFreq : 38950                                        ③
      q-RxLevMin : -65                                              ④
      t-ReselectionEUTRA : 1                                        ⑤
      threshX-High : 12                                             ⑥
      threshX-Low : 11                                              ⑦
      allowedMeasBandwidth : mbw100                                 ⑧
      presenceAntennaPort1 : False                                  ⑨
      cellReselectionPriority : 7                                   ⑩
      neighCellConfig                                               ⑪
        Binary string (Bin) : 00
          [0 ] : 0
          [1 ] : 0
```

① 异频临小区重选信息

② 异频临小区重选列表,最多8个

③ 异频临小区频点

④ 异频临小区最小的RSRP. Value -70 ~ -22 dBm.

⑤ 定义了小区重选时间 0 ~ 7 s

⑥ # Threshold (in dB) used by UE for cell re-selection to a HIGHER priority # The Srxlev of the candiate cell is greater then threshX_High # Value 0 to 31 dB. Actual value= Signaled value * 2

⑦ # Threshold (in dB) used by UE for cell re-selection to a LOWER priority # Cell re-selection is allowed only when Srxlev of the candiate cell is greater then threshX_Low and RSRP of serving cell is less than the value of ThreshServingLow singalled within SIB3 # Value 0 to 31 dB. Actual value= Signaled value * 2

⑧ 异频临小区带宽

⑨ [later]

⑩ 异频临小区优先级

⑪ 用于提供临小区MBSFN和上下行配比信息. 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.

SIB6 (System Information Block 6) 解析

- SIB6仅包含WCDMA小区重选信息

SIB7 (System Information Block 7) 解析

- SIB7仅包含2G小区重选信息

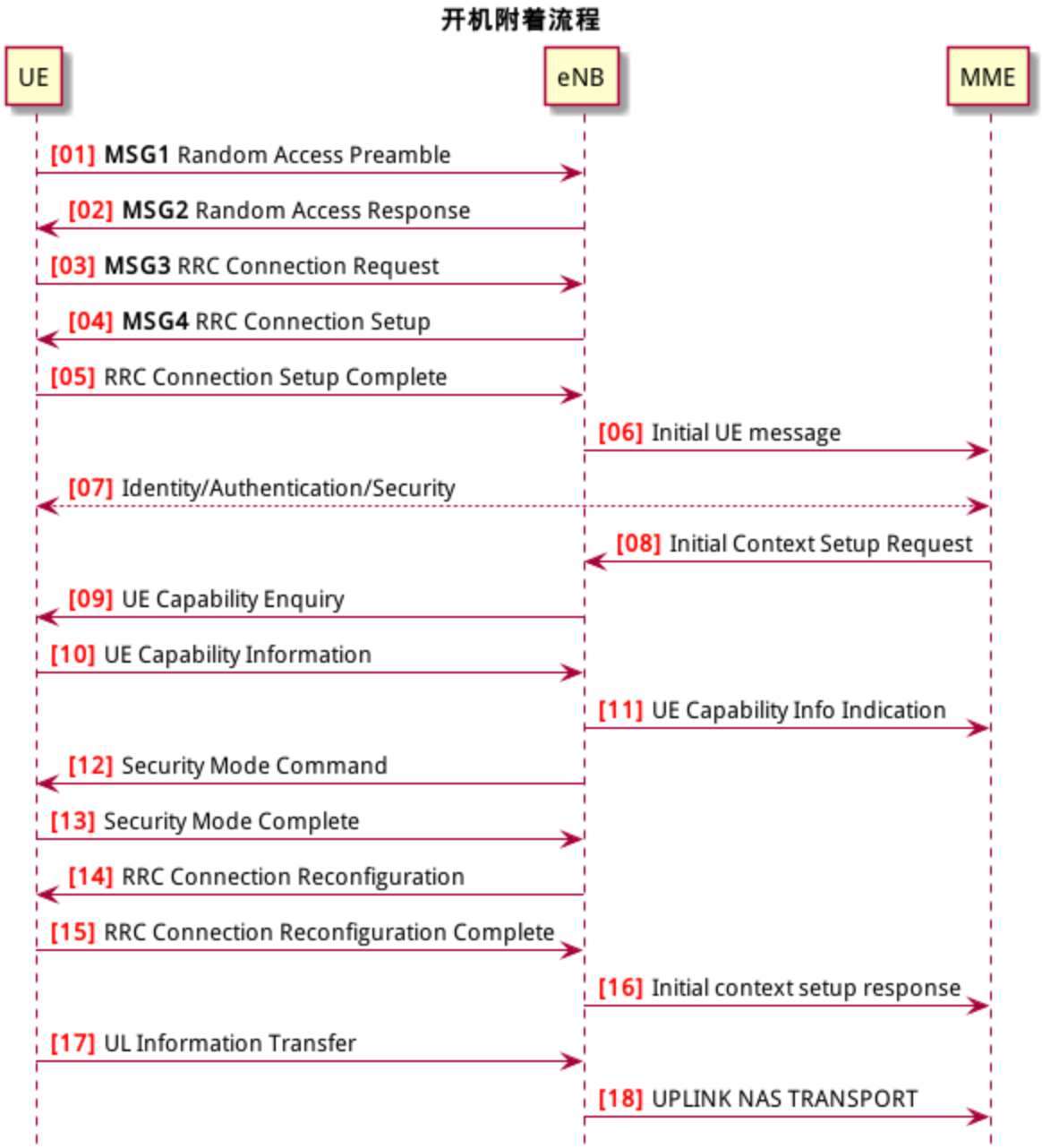
SIB8 (System Information Block 8) 解析

SIB9 (System Information Block 9) 解析

主要信令流程

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:



1. 处在RRC_IDLE态的UE进行Attach过程, 首先发起随机接入过程, 即MSG1消息; [Random Access Request]
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;[Random Access Response]
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;[RRC Connection Request]
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; [RRC Connection Setup]
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Attach request信息; [RRC Connection Setup Complete]
6. eNB选择MME, 向MME发送INITIAL UE MESSAGE消息, 包含NAS层Attach request消息; [InitialUEMessage]

7. NAS message
8. MME向eNB发送INITIAL CONTEXT SETUP REQUEST消息, 请求建立默认承载, 包含NAS层Attach Accept, Activate default EPS bearer context request消息;
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, DRB(包括默认承载)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;
17. UE向eNB发送ULInformationTransfer消息, 包含NAS层Attach Complete, Activate default EPS bearer context accept消息;
18. eNB向MME发送上行直传UPLINK NAS TRANSPORT消息, 包含NAS层Attach Complete, Activate default EPS bearer context accept消息.

随机接入

信令解析

空口信令

Random Access Request

Random Access Request

```
MS1
ML1 Random Access Request

Time : 18:02:58.666
Length : 40
Log Code (Hex) : 0xB167
HW Timestamp : (71192875.00 ms) 19:46:32.875
  1.25 ms fraction : 0.00
  CFN : 0
  1.25 ms counter : 868618874300
Version : 5
Preamble Sequence : 41
Physical Root Index : 1
Cyclic Shift : 533
PRACH Tx Power : -25
Beta PRACH : 242
PRACH Frequency Offset : 10
Preamble Format : 0
Duplex Mode : TDD
Frequency Resource Index : 0
Resource reoccurring in : All Even Radio Frames
Random access resource located in : First Half Frame
UL Subframe number where preamble starts : 0
Density per 10 ms : 0.5
PRACH Timing SFN : 848
PRACH Timing Sub-fn : 2
PRACH Window Start SFN : 848
PRACH Window Start Sub-fn : 5
PRACH Window End SFN : 849
PRACH Window End Sub-fn : 5
RA RNTI : 3
PRACH Actual Tx Power : 231
```

Random Access Response

Random Access Response

```
MS1
ML1 Random Access Response

Time : 18:02:58.666
Length : 24
Log Code (Hex) : 0xB168
HW Timestamp : (71192886.25 ms) 19:46:32.886
  1.25 ms fraction : 0.00
  CFN : 0
  1.25 ms counter : 868618874309
Version : 1
PRACH Response Timing SFN : 848
PRACH Response Timing Sub-fn : 9
Timing Advance : 0
Timing Advance Included : Included
RACH Procedure Type : Contention Based
RACH Procedure Mode : Initial Access
RNTI Type : TEMP_C_RNTI
RNTI Value : 107
```

RRC Connection Request

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.

RRC Connection Request

```
MS1
RRC Connection Request (UL-CCCH)

Time : 18:02:58.476
Vendor Header
  Length : 31
  Log Code (Hex) : 0xB0C0
  HW Timestamp : (71192783.75 ms) 19:46:32.784
    1.25 ms fraction : 0.00
    CFN : 0
    1.25 ms counter : 868618874227
  RRC Signaling Header
    Log Packet Version : 2
    RRC Release Number : 9.10.0
    Radio Bearer Id : 0
    Physical Cell Id : 2
    E-ARFCN : 39150
    System Frame Number
      System frame number : N/A
      Sub frame number : N/A
    Message Type : CcchUplink
    Message Length : 6
criticalExtensions : rrcConnectionRequest-r8                    ①
rrcConnectionRequest-r8                                         ②
  ue-Identity                                                   ③
    Initial UE Identity : Random Value
    Random Value : 197823733579
  establishmentCause : mo-Signalling                            ④
  spare : 0                                                     ⑤
    [0 ] : 0


Message dump (Hex):
    52 E0 F3 69 F4 B6
```

① 关键字扩展

② RRC连接请求, R8版本

③ 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.

④ 接入原因 //参考mt-Access(2)

⑤ 预留值为以后的网络扩展做准备

RRC Connection Setup

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 Connection Setup

```
MS1
```

```
RRC Connection Setup (DL-CCCH)

Time : 18:02:58.666
Vendor Header
  Length : 49
  Log Code (Hex) : 0xB0C0
  HW Timestamp : (71192916.25 ms) 19:46:32.916
    1.25 ms fraction : 0.00
    CFN : 0
    1.25 ms counter : 868618874333
  RRC Signaling Header
    Log Packet Version : 2
    RRC Release Number : 9.10.0
    Radio Bearer Id : 0
    Physical Cell Id : 2
    E-ARFCN : 39150
    System Frame Number
      System frame number : N/A
      Sub frame number : N/A
    Message Type : CcchDownlink
    Message Length : 24
rrc-TransactionIdentifier : 1                                   ①
criticalExtensions : c1                                         ②
c1 : rrcConnectionSetup-r8                                      ③
rrcConnectionSetup-r8
  radioResourceConfigDedicated                                  ④
    srb-ToAddModList
      SRB-ToAddModList :                                        ⑤
        [0 ] :
          srb-Identity : 1                                      ⑥
          rlc-Config : explicitValue                            ⑦
          explicitValue
            RLC-Config : am                                     ⑧
            ul-AM-RLC                                           ⑨
              t-PollRetransmit : ms80                           ⑩
              pollPDU : p128                                    ⑪
              pollByte : kB125                                  ⑫
              maxRetxThreshold : t16                            ⑬
            dl-AM-RLC                                           ⑭
              t-Reordering : ms80                               ⑮
              t-StatusProhibit : ms15                           ⑯
          logicalChannelConfig : explicitValue                  ⑰
          explicitValue
            priority : 1                                        ⑱
            prioritisedBitRate : infinity                       ⑲
            bucketSizeDuration : ms300                          ⑳
            logicalChannelGroup : 0                             (1)
    mac-MainConfig : explicitValue                              (2)
    explicitValue
      maxHARQ-Tx : n5                                           (3)
      periodicBSR-Timer : infinity                              (4)
      retxBSR-Timer : sf2560                                    (5)
      ttiBundling : False                                       (6)
      drx-Config
        DRX-Config : release                                    (7)
      timeAlignmentTimerDedicated : infinity                    (8)
      phr-Config : setup                                        (9)
      periodicPHR-Timer : sf200                                 (10)
      prohibitPHR-Timer : sf100                                 (11)
      dl-PathlossChange : dB3                                   (12)
```

```
    physicalConfigDedicated                                    (13)
      pdsch-ConfigDedicated                                    (14)
        p-a : dB0                                              (15)
      pucch-ConfigDedicated                                    (16)
        ackNackRepetition : release                            (17)
        tdd-AckNackFeedbackMode : bundling                     (18)
      pusch-ConfigDedicated                                    (19)
        betaOffset-ACK-Index : 9                               (20)
        betaOffset-RI-Index : 5                                1.
        betaOffset-CQI-Index : 15                              2.
      uplinkPowerControlDedicated                              3.
        p0-UE-PUSCH : 0                                        4.
        deltaMCS-Enabled : en0                                 5.
        accumulationEnabled : True                             6.
        p0-UE-PUCCH : 0                                        7.
        pSRS-Offset : 3                                        8.
        extensionBit0 : 0                                      9.
        filterCoefficient : fc0                                10.
      cqi-ReportConfig                                         11.
        nomPDSCH-RS-EPRE-Offset : 0                            12.
      antennaInfo : explicitValue                              13.
      explicitValue
        transmissionMode : tm2                                 14.
        ue-TransmitAntennaSelection : release                  15.
      schedulingRequestConfig                                  16.
        SchedulingRequestConfig : setup                        17.
        sr-PUCCH-ResourceIndex : 0                             18.
        sr-ConfigIndex : 72                                    19.
        dsr-TransMax : n64                                     20.

Message dump (Hex):
    68 12 98 0F A9 A0 19 83 B0 FA
    73 3E 45 E5 C9 2B F8 60 C0 10
    A0 01 22 00
```

① RRC消息ID

② 关键扩展c1 //c1是什么意思?

③ RRC连接建立, R8版本

④ 无线资源配置专用

⑤ 添加SRB

⑥ 建立SRB1

⑦ ?

⑧ SRB采用AM接收模式. 关于模式: 透明模式™, 非确认模式(UM)和确认模式(AM)

⑨ 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

⑩ 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.

⑪ 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p128对应为128个PDU

⑫ PollByte为AM PDU侦测字节数. 触发每个pollByte字节的一个轮询. 此处kB125对应125kB

⑬ 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. t16对应16次重传输.

⑭ UE侧的下行RLC配置, 主要配置RLC数据接收状态上报规则.

⑮ 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ms80表示80ms.

⑯ 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. ms15表示15ms.

⑰ SRB1的逻辑信道配置

⑱ SRB1逻辑信道优先级, 值越小优先级越高. 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.

⑲ 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.

⑳ SRB1 bucket size调整持续时间, 300ms

⑴ 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

⑵ MAC层主要配置

⑶ UL HARQ的最大传输次数.

⑷ 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.

⑸ SR重传定时器(子帧).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. ENUMERATED {sf320, sf640, sf1280, sf2560, sf5120,sf10240, spare2, spare1}

⑹ 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.

⑺ RX-Config : release

⑻ 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)

⑼ 功率余量报告配置, PHR(power headroom report)

⑽ 功率余量报告周期定时器

⑾ 禁止上报功率剩余报告定时器

⑿ 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

⑬ 物理层配置专用

⑭ PDSCH配置专用

⑮ PA=0 //?

⑯ PUCCH配置专用

⑰ 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.

⑱ TDD-确认非确认反馈模式 绑定模式

⑲ PUSCH配置专用

⑳ ACK随路偏置索引, 该参数表示ACK随路偏置索引. INTEGER (0..15)

1. RI随路偏置索引, 该参数表示RI随路偏置索引. INTEGER (0..15)
2. CQI随路偏置索引, 该参数表示RI随路偏置索引. INTEGER (0..15)
3. 上行链路功控专用
4. INTEGER (-8..7) //?
5. 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)
6. 累积使能, (0:不能够; 1:能够) //?
7. INTEGER (-8..7) //?
8. SRS相对PUSCH的功率偏置, INTEGER (0..15)
9. //?
10. 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.
11. CQI配置
12. //?
13. 天线配置
14. 传输模式TM2, 标识UE所使用的传输模式
15. 终端UE传输天线选择, Setup或release. Setup表示开环或者闭环. //?
16. 调度请求配置信息
17. 调度请求配置信息类型setup
18. 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.

19. //?

20. //?

RRC Connection Setup Complete

RRC Connection Setup Complete

```
MS1
RRC Connection Setup Complete (UL-DCCH)

Time : 18:02:58.666
Vendor Header
  Length : 101
  Log Code (Hex) : 0xB0C0
  HW Timestamp : (71192920.00 ms) 19:46:32.920
    1.25 ms fraction : 0.00
    CFN : 0
    1.25 ms counter : 868618874336
  RRC Signaling Header
    Log Packet Version : 2
    RRC Release Number : 9.10.0
    Radio Bearer Id : 1
    Physical Cell Id : 2
    E-ARFCN : 39150
    System Frame Number
      System frame number : N/A
      Sub frame number : N/A
    Message Type : DcchUplink
    Message Length : 76
rrc-TransactionIdentifier : 1
criticalExtensions : c1
c1 : rrcConnectionSetupComplete-r8
rrcConnectionSetupComplete-r8                                    ①
  selectedPLMN-Identity : 1                                      ②
  registeredMME                                                  ③
    mmegi : 0000000000000010
      [0 ] : 0
      [1 ] : 0
      [2 ] : 0
      [3 ] : 0
      [4 ] : 0
      [5 ] : 0
      [6 ] : 0
      [7 ] : 0
      [8 ] : 0
      [9 ] : 0
      [10] : 0
      [11] : 0
      [12] : 0
      [13] : 0
      [14] : 1
      [15] : 0
    mmec
      MMEC : (0x1) : 1
  dedicatedInfoNAS                                               ④
    Protocol Discriminator : 7 (EMM)
    Message Type : Attach Request
```

```
    Message Contents : 17 71 ...


Message dump (Hex):
    22 20 00 02 01 46 17 71 87 86
    9D 04 07 41 02 0B F6 00 F1 10
    00 02 01 01 00 00 33 05 E0 F0
    00 00 01 00 05 02 02 D0 31 D1
    52 00 F1 10 31 32 5C 0A 00 13
    FF FF FF FF FE 90 11 03 4F 18
    A6 40 08 04 02 60 04 00 02 1F
    02 F1 5D 01 02 E0
```

① RRC连接建立完成消息

② 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

③ //?

④ 传输UE和网络层的NAS层消息. eNB层透传此消息给MME.

网络层信令

Initial UE Message

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.

InitialUEMessage

```
S1 Application Protocol
  S1AP-PDU: initiatingMessage (0)
    initiatingMessage
      procedureCode: id-initialUEMessage (12)                    ①
      criticality: ignore (1)
      value
        InitialUEMessage                                         ②
          protocolIEs: 5 items
            Item 0: id-eNB-UE-S1AP-ID                            ③
              ProtocolIE-Field
                id: id-eNB-UE-S1AP-ID (8)
                criticality: reject (0)
                value
                  ENB-UE-S1AP-ID: 1                              ④
            Item 1: id-NAS-PDU                                   ⑤
              ProtocolIE-Field
                id: id-NAS-PDU (26)
                criticality: reject (0)
                value
                  NAS-PDU: 177187869d04074102...
                  Non-Access-Stratum (NAS)PDU
            Item 2: id-TAI                                       ⑥
              ProtocolIE-Field
                id: id-TAI (67)
                criticality: reject (0)
                value
                  TAI
                    pLMNidentity: 00f110                         ⑦
                    Mobile Country Code (MCC): Unknown (1)
                    Mobile Network Code (MNC): Unknown (01)
                    tAC: 3132                                    ⑧
            Item 3: id-EUTRAN-CGI                                ⑨
              ProtocolIE-Field
                id: id-EUTRAN-CGI (100)
                criticality: ignore (1)
                value
                  EUTRAN-CGI
                    pLMNidentity: 00f110
                    Mobile Country Code (MCC): Unknown (1)
                    Mobile Network Code (MNC): Unknown (01)
                    cell-ID: 00000020                            ⑩
            Item 4: id-RRC-Establishment-Cause                   ⑪
              ProtocolIE-Field
                id: id-RRC-Establishment-Cause (134)
                criticality: ignore (1)
                value
                  RRC-Establishment-Cause: mo-Signalling (3)     ⑫
```

① procedureCode

② UE初始消息

③ id-eNB-UE-S1AP-ID

④ eNB侧的用户标识

⑤ id-NAS-PD

⑥ id-TAI

⑦ PLMN值

⑧ TAC值

⑨ id-EUTRAN-CGI

⑩ 此值为ECI

⑪ id-RRC-Establishment-Cause

⑫ RRC建立原因值, 移动终端接入. 此值与[RRC Connection Request]携带的原因值一致

Initial Context Setup Request

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.

Initial Context Setup Request

```
S1 Application Protocol
 S1AP-PDU: initiatingMessage (0)
  initiatingMessage
   procedureCode: id-InitialContextSetup (9)
   criticality: reject (0)
   value
     InitialContextSetupRequest                                    ①
       protocolIEs: 6 items
         Item 0: id-MME-UE-S1AP-ID
           MME-UE-S1AP-ID: 33554442                                ②
         Item 1: id-eNB-UE-S1AP-ID
           ENB-UE-S1AP-ID: 1                                       ③
         Item 2: id-uEaggregateMaximumBitrate
           UEAggregateMaximumBitrate                               ④
             uEaggregateMaximumBitRateDL: 20480000                 ⑤
             uEaggregateMaximumBitRateUL: 4096000                  ⑥
         Item 3: id-E-RABToBeSetupListCtxtSUReq                    ⑦
           E-RABToBeSetupListCtxtSUReq: 1 item
             Item 0: id-E-RABToBeSetupItemCtxtSUReq                ⑧
               E-RABToBeSetupItemCtxtSUReq
                 e-RAB-ID: 5                                       ⑨
                 e-RABlevelQoSParameters
                   qCI: 7
                   allocationRetentionPriority
                     priorityLevel: highest (1)
                     pre-emptionCapability: may-trigger-pre-emption (1)
                     pre-emptionVulnerability: pre-emptable (1)
                   gbrQosInformation
                     e-RAB-MaximumBitrateDL: 0
                     e-RAB-MaximumBitrateUL: 0
                     e-RAB-GuaranteedBitrateDL: 0
                     e-RAB-GuaranteedBitrateUL: 0
                 0... .... Extension Present Bit: False
                 transportLayerAddress: 0a5878cc
                   transportLayerAddress(IPv4): 10.88.120.204
```

```
                gTP-TEID: 0000048a
                nAS-PDU: 27dac5cd...
                Non-Access-Stratum (NAS)PDU
                  0010 .... = Security header type: Integrity protected and ciphered
(2)
                  .... 0111 = Protocol discriminator: EPS mobility management messages
(7)
                  Message authentication code: 0xdac5cd60
                  Sequence number: 2
                  0000 .... = Security header type: Plain NAS message, not security
protected (0)
                  .... 0111 = Protocol discriminator: EPS mobility management messages
(7)
                  NAS EPS Mobility Management Message Type: Attach accept (0x42)
                  0000 .... = Spare half octet: 0
                  .... 0... = Spare bit(s): 0x00
                  .... .010 = Attach result: Combined EPS/IMSI attach (2)
                  GPRS Timer - T3412 value
                    GPRS Timer: 54 min
                      010. .... = Unit: value is incremented in multiples of decihours
(2)
                      ...0 1001 = Timer value: 9
                  Tracking area identity list - TAI list
                    Length: 6
                    0... .... = Spare bit(s): 0x00
                    .10. .... = Type of list: list of TAIs belonging to different
PLMNs (2)
                    ...0 0000 = Number of elements: 0 [+1 = 1 element(s)]
                    Mobile Country Code (MCC): Unknown (1)
                    Mobile Network Code (MNC): Unknown (01)
                    Tracking area code(TAC): 0x3132
                  ESM message container
                    Length: 73
                    ESM message container contents: 5202c10507fff...
                      0101 .... = EPS bearer identity: 0x05
                      .... 0010 = Protocol discriminator: EPS session management
messages (2)
                      Procedure transaction identity: 2
                      NAS EPS session management messages: Activate default EPS bearer
context request (0xc1)
                      EPS quality of service
                        Length: 5
                        Quality of Service Class Identifier (QCI): QCI 7 (7)
                        Maximum bit rate for uplink : 0 kbps
                        Maximum bit rate for downlink : 0 kbps
                        Guaranteed bit rate for uplink : 0 kbps
                        Guaranteed bit rate for downlink : 0 kbps
                      Access Point Name
                        Length: 6
                        APN: cmnet
                      PDN address
                        Length: 5
                        0000 0... = Spare bit(s): 0x00
                        PDN type: IPv4 (1)
                        PDN IPv4: 70.0.0.1 (70.0.0.1)
                      APN aggregate maximum bit rate
                        Element ID: 94
                        Length: 4
                        APN-AMBR for downlink : 8640 kbps
                        APN-AMBR for uplink : 4096 kbps
```

```
                        APN-AMBR for downlink (extended) : 20 Mbps
                        Total APN-AMBR for downlink : 20.000 Mbps
                        Use the value indicated by the APN-AMBR for uplink
                        Total APN-AMBR for uplink : 4.096 Mbps
                      ESM cause
                        Element ID: 88
                        Cause: PDN type IPv4 only allowed (50)
                      Protocol Configuration Options
                        Element ID: 39
                        Length: 41
                        [Link direction: Network to MS (1)]
                        1... .... = Ext: 0x01
                        Configuration Protocol: PPP (0)
                        Protocol or Container ID: IP Control Protocol (32801)
                        Length: 0x10 (16)
                        PPP IP Control Protocol
                          Code: Configuration Ack (0x02)
                          Identifier: 0x00
                          Length: 16
                          Options: (12 bytes)
                            Primary DNS server IP address: 8.8.8.8
                            Secondary DNS server IP address: 4.2.2.1
                        Protocol or Container ID: Challenge Handshake Authentication
Protocol (49699)
                        Length: 0x04 (4)
                        PPP Challenge Handshake Authentication Protocol
                          Code: Success (3)
                          Identifier: 0
                          Length: 4
                        Protocol or Container ID: DNS Server IPv4 Address (13)
                        Length: 0x04 (4)
                        Data (4 bytes)

00008 08 08 08                    ....
                          Data: 08080808
                          [Length: 4]
                        Protocol or Container ID: DNS Server IPv4 Address (13)
                        Length: 0x04 (4)
                        Data (4 bytes)

00004 02 02 01                    ....
                          Data: 04020201
                          [Length: 4]
                    EPS mobile identity - GUTI
                      Element ID: 80
                      Length: 11
                      .... 0... = odd/even indic: 0
                      .... .110 = Type of identity: GUTI (6)
                      Mobile Country Code (MCC): Unknown (1)
                      Mobile Network Code (MNC): Unknown (01)
                      MME Group ID: 2
                      MME Code: 1
                      M-TMSI: 0x01000032
                    EMM cause
                      Element ID: 83
                      Cause: CS domain not available (18)
                    GPRS Timer - T3402 value
                      Element ID: 23
                      GPRS Timer: 12 min
                        001. .... = Unit: value is incremented in multiples of 1 minute
```

```
(1)
                        ...0 1100 = Timer value: 12
                    GPRS Timer - T3423 value
                      Element ID: 89
                      GPRS Timer: 54 min
                        010. .... = Unit: value is incremented in multiples of decihours
(2)
                        ...0 1001 = Timer value: 9
                    EPS network feature support
                      Element ID: 100
                      Length: 1
                      000. .... = Spare bit(s): 0x00
                      ...0 0... = CS-LCS: no information about support of location
services via CS domain is available (0)
                      .... .0.. = EPC-LCS: location services via EPC not supported
                      .... ..1. = EMC BS: emergency bearer services in S1 mode supported
                      .... ...1 = IMS VoPS: IMS voice over PS session in S1 mode
supported
          Item 4: id-UESecurityCapabilities
            ProtocolIE-Field
              id: id-UESecurityCapabilities (107)
              criticality: reject (0)
              value
                UESecurityCapabilities
                  ..0. .... Extension Present Bit: False
                  encryptionAlgorithms: c000 [bit length 16, 1100 0000  0000 0000
decimal value 49152]
                  ...0 .... Extension Present Bit: False
                  integrityProtectionAlgorithms: c000 [bit length 16, 1100 0000  0000
0000 decimal value 49152]
          Item 5: id-SecurityKey
            ProtocolIE-Field
              id: id-SecurityKey (73)
              criticality: reject (0)
              value
                SecurityKey: dc1e1efe6156ecc43e94fc0f46a96f1eb3ec055fe0dce418... [bit
length 256]
```

① 初始化上下文建立请求

② 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不同

③ 基站侧用户标识

④ 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.

⑤ 下行AMBR, EPC开户配置

⑥ 上行AMBR, EPC开户配置

⑦ 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. 因此只有一项.

⑧ 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. <9> <10> <11> <12> <13> <14> <15> <16>

Inital Context Setup Response

Inital Context Setup Response

```
S1 Application Protocol
  S1AP-PDU: successfulOutcome (1)
    successfulOutcome
      procedureCode: id-InitialContextSetup (9)
      criticality: reject (0)
      value
        InitialContextSetupResponse
          protocolIEs: 3 items
            Item 0: id-MME-UE-S1AP-ID
              ProtocolIE-Field
                id: id-MME-UE-S1AP-ID (0)
                criticality: ignore (1)
                value
                  MME-UE-S1AP-ID: 33554442
            Item 1: id-eNB-UE-S1AP-ID
              ProtocolIE-Field
                id: id-eNB-UE-S1AP-ID (8)
                criticality: ignore (1)
                value
                  ENB-UE-S1AP-ID: 1
            Item 2: id-E-RABSetupListCtxtSURes
              ProtocolIE-Field
                id: id-E-RABSetupListCtxtSURes (51)
                criticality: ignore (1)
                value
                  E-RABSetupListCtxtSURes: 1 item
                    Item 0: id-E-RABSetupItemCtxtSURes
                      ProtocolIE-SingleContainer
                        id: id-E-RABSetupItemCtxtSURes (50)
                        criticality: ignore (1)
                        value
                          E-RABSetupItemCtxtSURes
                            e-RAB-ID: 5
                            .... ...0 Extension Present Bit: False
                            transportLayerAddress: 0a58788c [bit length 32, 0000 1010
0101 1000  0111 1000  1000 1100 decimal value 173570188]
                              transportLayerAddress(IPv4): 10.88.120.140
(10.88.120.140)
                            gTP-TEID: 0200000a

----
```