

# 5G无线网络信令流程

在NSA组网下，gNodeB不需要广播RMSI,RMSI中的内容通过RRC信令（由LTE发送）在UE开始接入NR前发生给UE。

作者：5G信令 来源：前景理论 | 2019-09-28 23:30

[收藏](#)

[分享](#)

## 一、5G初始接入

### 1. 开机入网概述

初始无线接入：当UE开机后，它的首要任务就是要找到无线网络并与无线网络建立连接，需要如下步骤：

获得上下行同步：侦听网络获得下行同步;随机接入，获取上行同步;  
收发消息，建立连接

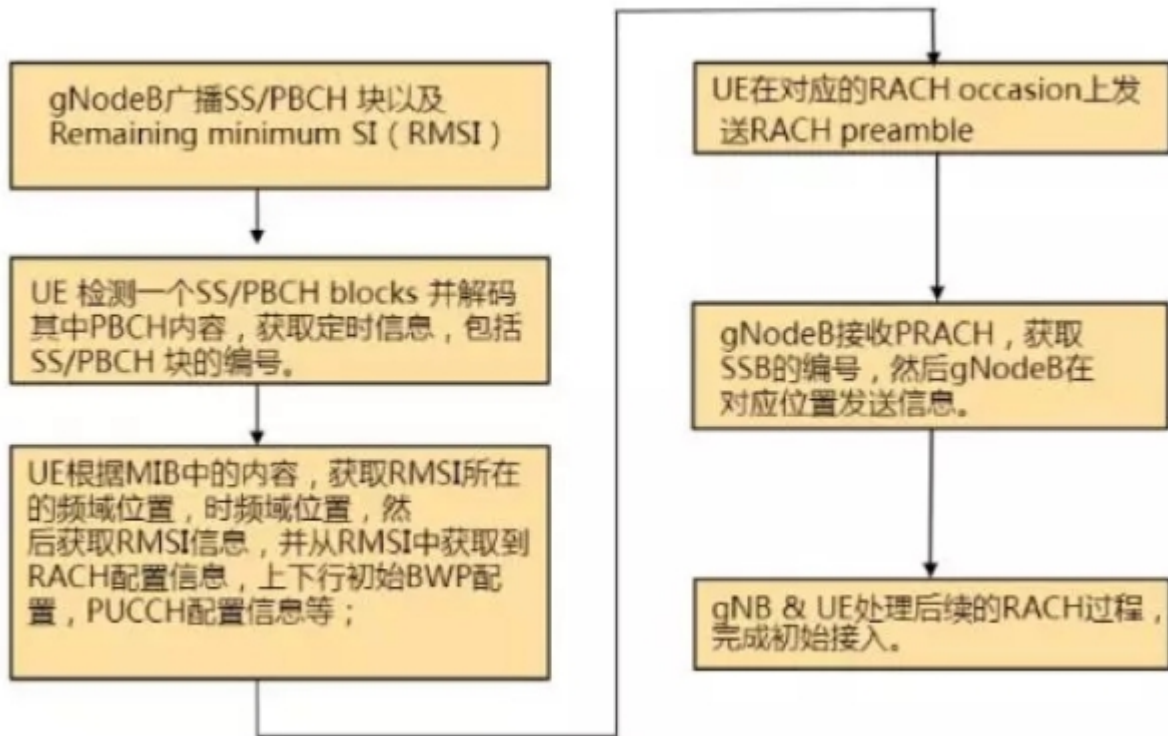
ATTACH：

建立UE与核心网之间相同的移动性上下文;  
建立UE与核心网之间的缺省承载  
通过EPS ATTACH流程，UE还可以获取到网络分配的IP地址

公共流程：

鉴权过程和安全模式过程

### 2. 初始接入流程概述



在NSA组网下, gNodeB不需要广播RMSI,RMSI中的内容通过RRC信令(由LTE发送)在UE开始接入NR前发送给UE;

### 3. 系统消息广播概述

NR同步和系统消息广播包括: PSS/SSS,PBCH,RMSI和QSI等;

PSS/SSS用于UE进行下行时钟同步, 并获取小区的Cell ID

PBCH(携带了MIB)用于UE获取接入网络的最基本信息, 主要是通知UE在何处接收RMSI消息;

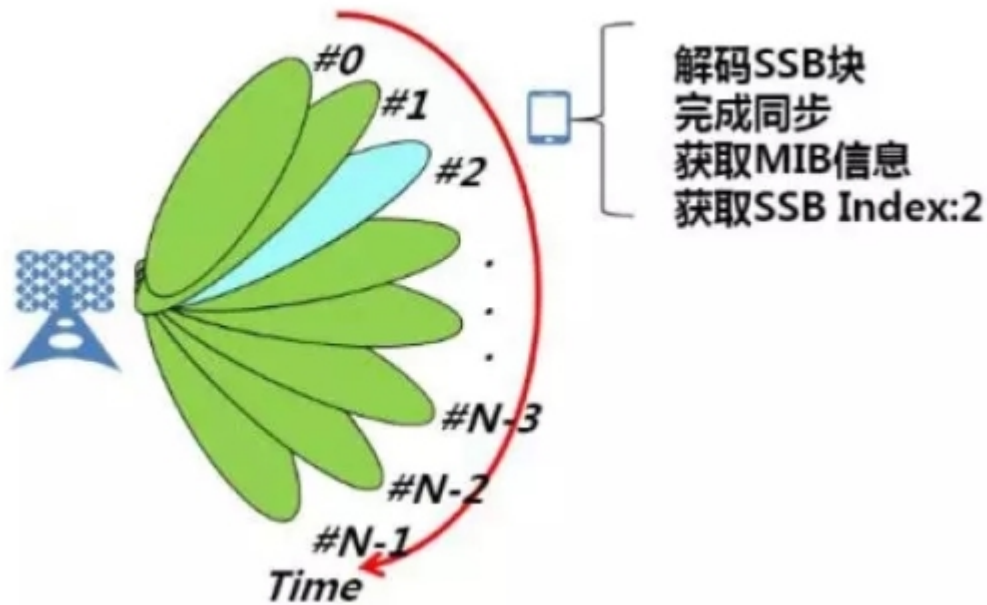
RMSI(SIB1)用于广播初始BWP信息, 初始BWP中的信道配置, TDD小区的半静态配比已经其他UE接入网络的必要信息等。

OSI, 用于其他小区信息的广播(目前NSA组网下没有用到这里的内容)

为了支持massive MIMO, 所有的广播信道和信号都支持进行波束扫描。

### 4. 广播信道波束扫描

广播波束最多设计为N个方向固定的波束。通过在不同时刻发送不同的波束完成小区的广播波束覆盖, UE通过扫描每一个波束, 获得最优波束, 完成同步和系统消息的解调。



## 5. MIB的信息内容

```

--- EXAMPLE:
--- The MIB-SSB-
MIB ::= SEQUENCE {
  -- The 4 most significant bits (MSB) of the 16 bit System Frame Number. The 4 LSBs of the SFN are contained in the SSB payload block.
  systemFrameNumber BIT STRING (SIZE=16),
  -- Subcarrier spacing for SSB, see 3.1.1 for initial access and broadcast of messages.
  -- If the UE acquires this MIB on a carrier frequency <600, the values 15 and 30 kHz are applicable.
  -- If the UE acquires this MIB on a carrier frequency >600, the values 60 and 120 kHz are applicable.
  ssbSubcarrierSpacing ENUMERATED {scs15kr60, scs30kr120},
  -- The frequency domain offset between SSB and the overall resource block grid in number of subcarriers. (See 3.1.1)
  -- Note: the frequency <600 is a fifth, this field may contain only the 4 least significant bits of the sub-carrier offset.
  -- The optional "FTS-START" indicates that this cell does not provide SSB and that there is hence no common CORESET.
  ssbSubcarrierOffset INTEGER (0..15),
  -- Position of SSB in DL DM-BM. Corresponds to 3GPP parameter "DL-DMB-type0-p0" from 3G.111, section 5.4.1.1.1)
  dmbs-type0-position ENUMERATED {pos0, pos1},
  -- Determine a bandwidth for PDSCH/SSB, a common ControlResourceSet (CORESET) a common search space and a common PDSCH resource.
  -- Corresponds to 3GPP parameter "PDSCH-Config" from 3GPP Specification, section 3.1.1.1.1.
  pdsch-config CORESET (0..255),
  -- Indicates that UE shall not camp on this cell.
  cellBarred ENUMERATED {barred, notBarred},
  -- Controls cell reselection in intra-frequency cells when the highest ranked cell is barred, or treated as barred by the UE.
  -- as specified in 3G.304.
  intraFreqReselection ENUMERATED {allowed, notAllowed},
  spare BIT STRING (SIZE=1)
};
--- The MIB-SSB-
--- ASN1 DEFINITION

```

系统帧号，共10bit，低4bit直接编码PBCH payload中

用于指示RMSI，MSG2/4使用的子载波间隔：  
低频只允许使用15KHz和30KHz，  
高频只允许用60KHz和120KHz，

用户指示RMSI所在的CORESET的时频域位置和相关。  
其中MSB (4bit) 用于指示RMSI的CORESET时频域位置；  
LSB (4bit) 用于指示CORESET的周期；  
该参数间接指示了初始BWP的相关信息。

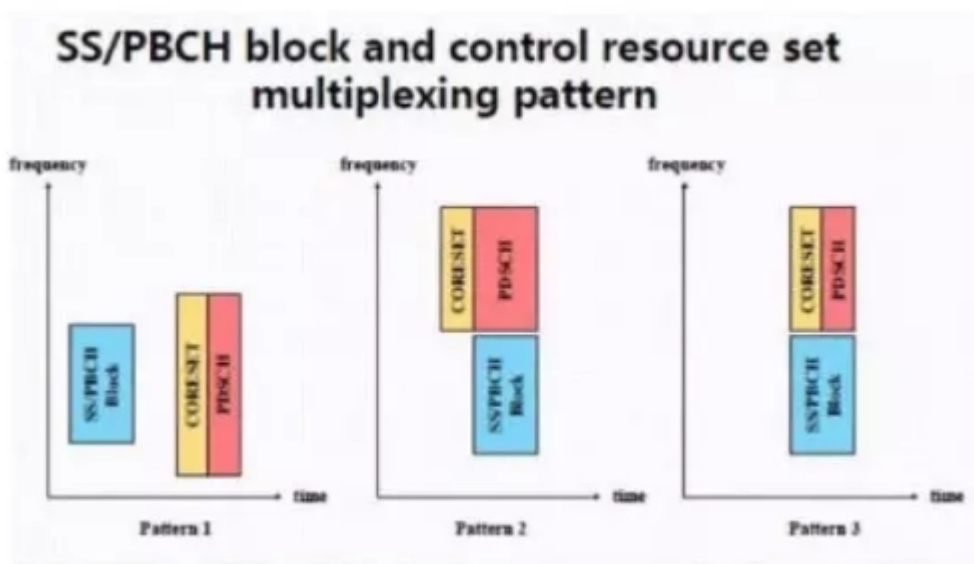
5G的MIB一个最重要的作用就是通知UE如何获取SIB1消息。

## pdccch-ConfigSIB1中高4bit对应表格

• Table 13-4: Set of resource blocks and slot symbols of control resource set for Type0-PDCCH search space when {SS/PBCH block, PDCCH} subcarrier spacing is {30, 30} kHz with minimum channel bandwidth 5 MHz or 10 MHz.

Index	SS/PBCH block and control resource set multiplexing pattern	Number of RBs $N_{\text{CORESET}}^{\text{RB}}$	Number of Symbols $N_{\text{CORESET}}^{\text{sym}}$	Offset (RBs)
0	1	24	2	0
1	1	24	2	1
2	1	24	2	2
3	1	24	2	3
4	1	24	2	4
5	1	24	3	0
6	1	24	3	1
7	1	24	3	2
8	1	24	3	3
9	1	24	3	4
10	1	48	1	12
11	1	48	1	14
12	1	48	1	16
13	1	48	2	12
14	1	48	2	14
15	1	48	2	16

在 38.213 中定义了 10 张表，UE 需要根据 SSB 的子载波间隔，MIB 中的 SubcarrierSpaceCommon 参数，以及频段对应的小区的最小带宽来确定选择哪张表，然后通过 pdccch-ConfigSIB1 中的高 4bit 选择表中的哪一行。



Number of RB CORESET: 该参数定义了初始BWP中CORESET的RB数，同时也定义了初始BWP的带宽。目前协议之定义了三种带宽：24，48和96RB。Number of Symbols CORESET: 该参数定义了初始BWP中CORESET的符号数，取值范围为1-3;

offset(RBs)该参数定义了初始BWP中CORESET的起始RB与SSB的RB0之间的偏移，见解定义初始BWP的频域位置。

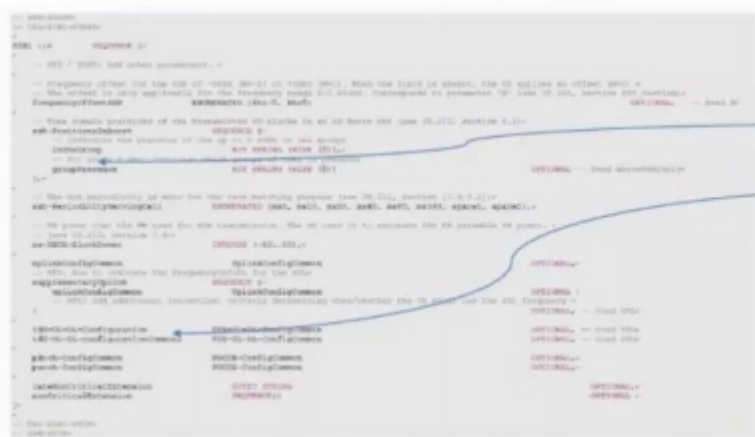
## 6. MIB的信元

Index	MS	Date	Time	Direction	Channel Type	Message Name	Message Data
50	MS1	201	15:03:58.788	gNodeB->MS	BCCH-BCH	MasterInformationBlock	01 DE 18 84 00
51	MS1	201	15:29:39.577	gNodeB->MS	BCCH-BCH	MasterInformationBlock	01 56 98 84 00
52	MS1	201	15:40:36.680	gNodeB->MS	BCCH-BCH	MasterInformationBlock	01 82 98 84 00
53	MS1	201	15:41:58.098	gNodeB->MS	BCCH-BCH	MasterInformationBlock	01 76 18 84 00
54	MS1	20	-0				00
55	MS1	20	-0				00
56	MS1	20	-0				00
57	MS1	20	-0				00
58	MS1	20	-0				00
59	MS1	20	-0				00
60	MS1	20	0				00
61	MS1	20	-0				00
62	MS1	20	-0				00
63	MS1	20	7				00
64	MS1	20	0				00
65	MS1	20	0				00
66	MS1	20	0				00
67	MS1	20	0				00
68	MS1	20	-0				00

RRC-Msg
mag
struBCH-BCH-Message
struBCH-BCH-Message
bchmessage
systemFrameNumber:011011000(76 00)
commonResourceControl
searchSpace-Bandwidth:rb48 (1)
numerologyForCCE:0x1 (1)
symbolIndices:s0 (0)
rmsiPeriodicity:ms20 (1)
ssBlockTimeIndex:0x0 (0)
halfFrameIndication:firstHalf (0)
cellBarredFlag:notBarred (1)
dmrsPosition:s3 (0)
prbGridOffset:0x0 (0)
spare:00000(00)

00000001 I
01110110
00-----
--01----
--1-----
-----00-
-----0
1-----
-000----
-----0
-----1-
-----0-
-----0
000-----
---00000

## 7. SIB1信元解析



- SIB1消息主要广播UE初始接入网络时需要的基本信息，包括初始SSB相关的信息，初始BWP信息，下行信道配置等。
- SIB1中会广播实际中发送的SSB的数目；UE需要根据这个信息对SSB进行Rate Matching；
- 此外，SIB1中还广播Cell-specific的配比信息。
- UE需要根据自己搜索到的SSB index的位置，获取对应位置上的SIB1消息。
- 在NSA中，不广播SIB1消息；SIB1中承载的内容，在RRC重配置消息中通过LTE下发给UE。

## 8. SIB1消息

SIB1消息主要广播UE初始接入网络时需要的基本信息，包括初始SSB相关信息，初始BWP信息，下行信道配置等。

SIB1中会广播实际中发送的SSB的数目；UE需要根据这个信息对SSB进行rate matching；

此外，SIB1中还广播cell-specific的配比信息。

UE需要根据自己搜索到的SSB index的位置，获取对应位置上的SIB1消息。

在NSA中，不广播SIB1消息;SIB1承载的内容，在RRC重配置消息中通过LTE下发UE。

## 9. 其他广播消息

包括SIB2-SIBn

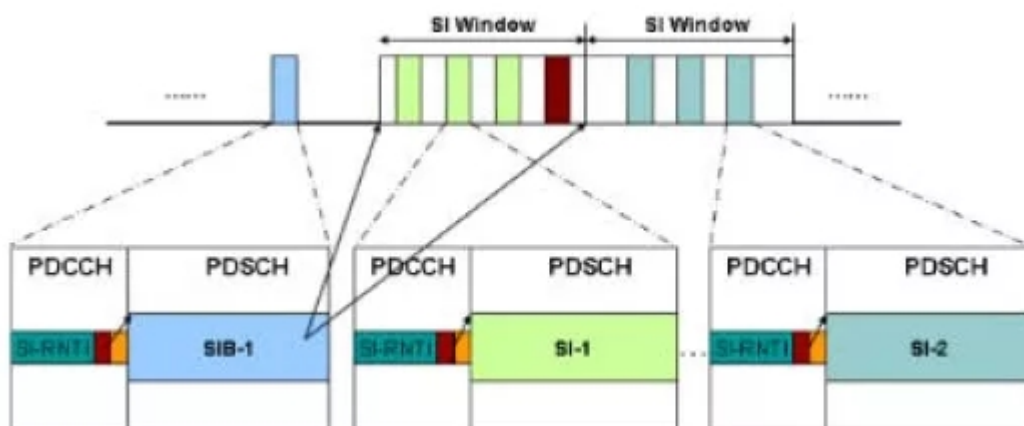
QSI承载在PDSCH

支持周期性广播

具有相同传输周期的SIBs，映射到相同的SI message中。

不同传输周期的SIBs不能映射到同一个SI message中。

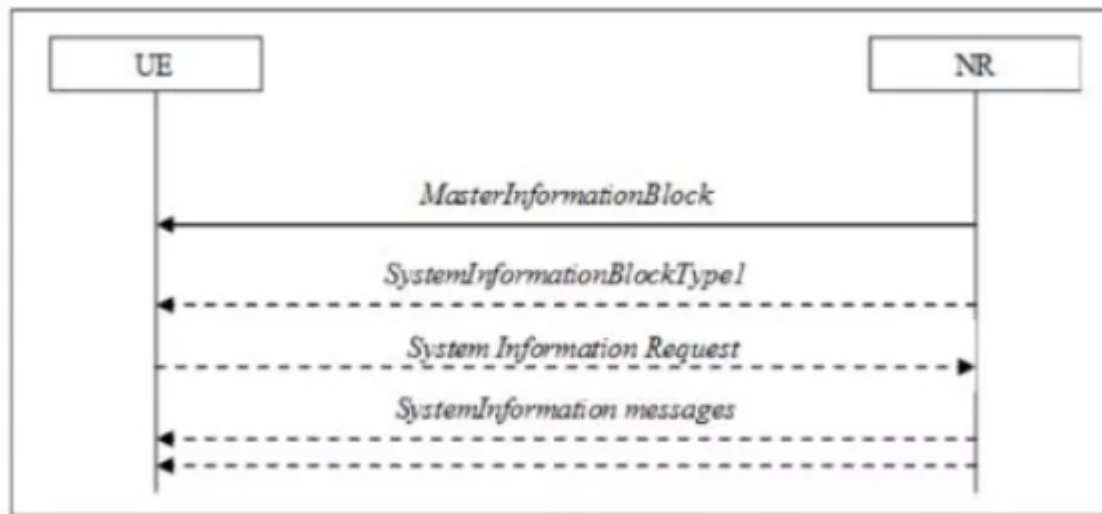
具有相同传输周期的SIBs可以映射到不同的SI message中。



支持ODOSI广播

在RRC CONNECTED状态的UE，通过专用信令来请求和传递OSI，具体流程待协议明确

在RRC IDLE或RRC INACTIVE状态的UE;如果SIB1中指示支持ODOSI，则通过MSG1请求OSI，否则，通过MSG3请求OSI，具体细节待协议明确;



## 10. 随机接入

触发RA的事件有如下几类：

初始RRC连接建立

RRC连接重建

切换

失步状态下行数据到达

失步状态上行数据到达。

NSA接入。UE在LTE小区接入后，添加NR小区时，在NR发起RA。

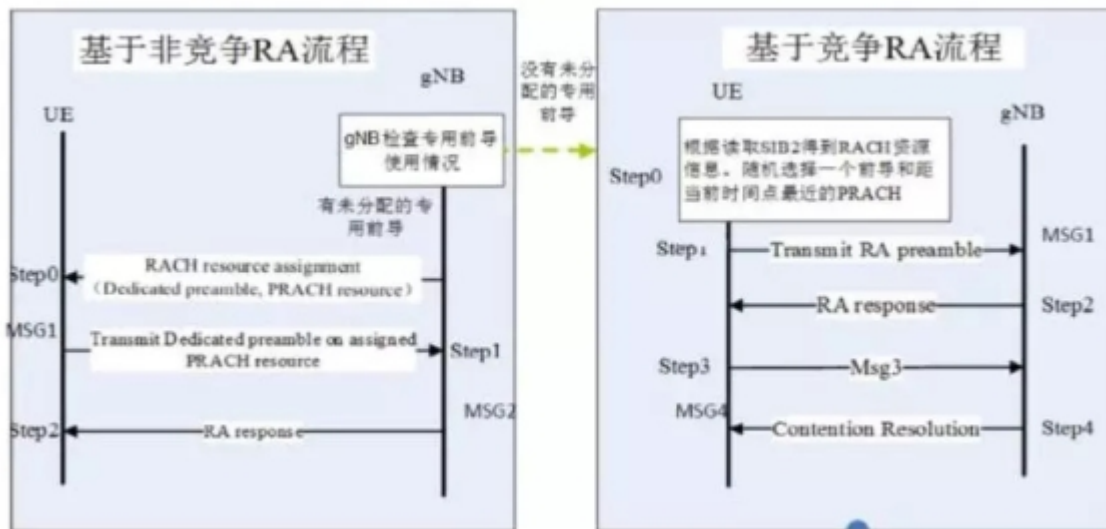
基于RA请求SI(系统消息)。UE需要请求特定SI时会发起RA。

UE从RRC\_INACTIVE到RRC\_CONNECTED状态。

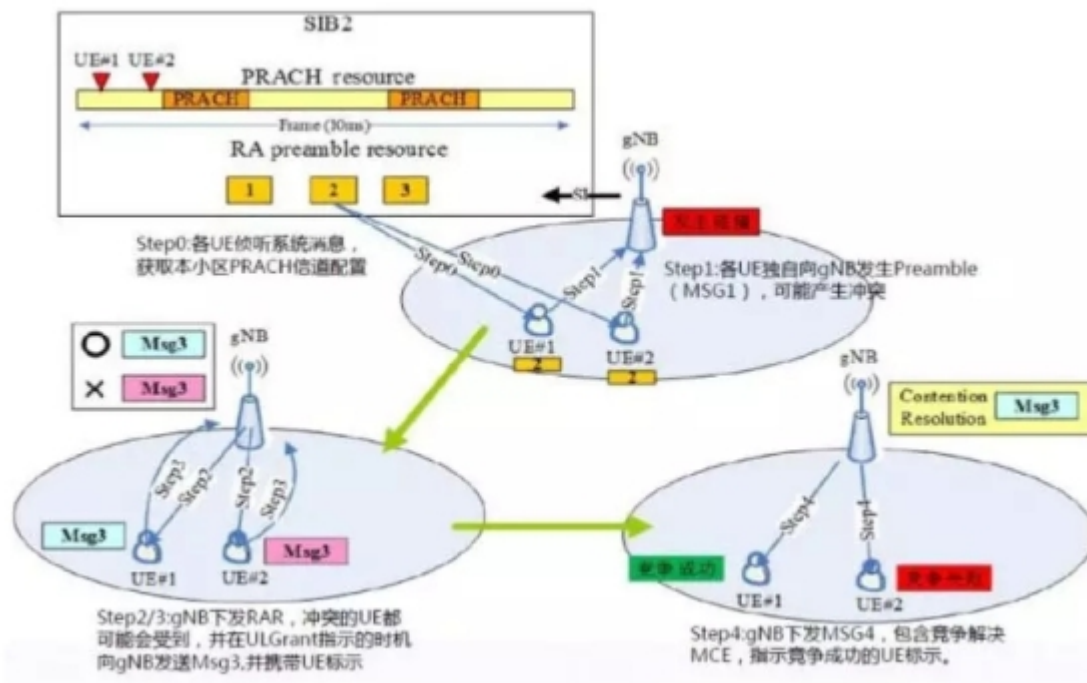
波束恢复，当UE PHY层检测到波束失步时，会通知UE MAC发起RA。

NR中的随机接入流程与LTE的基本相同，通过发送preamble启动接入过程，接入过程也分为竞争接入和非竞争接入(通过使用不同类型的preamble来区分)





## 11. 随机接入冲突解决

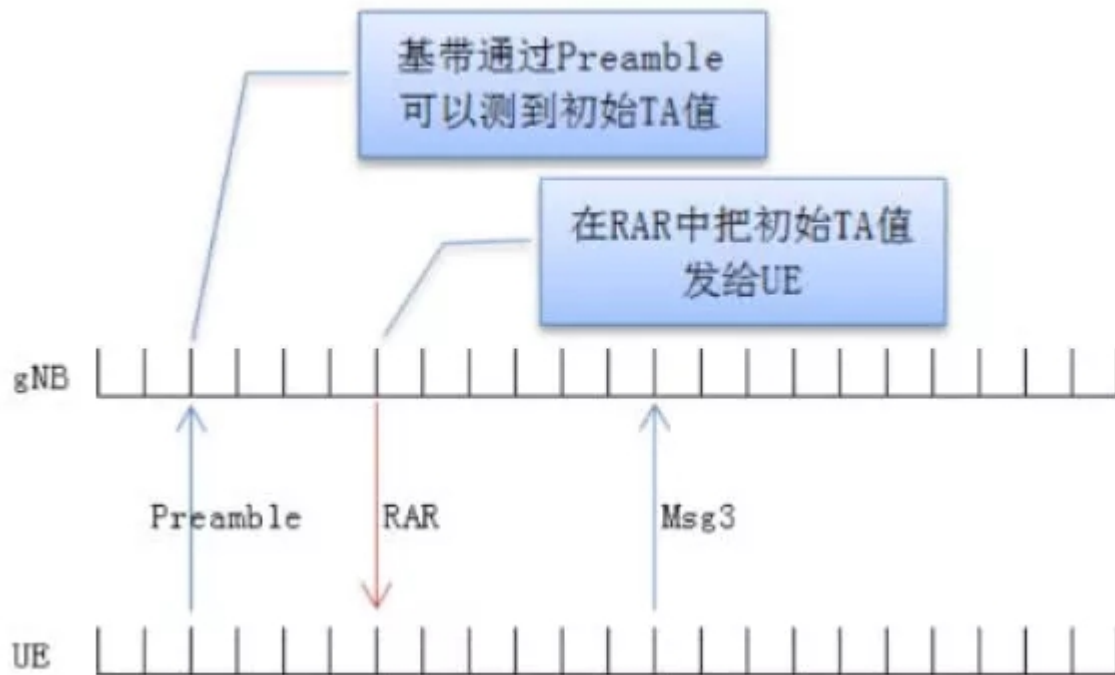


## 12. 随机接入中的上行同步

UE通过随机接入建立或恢复上行同步，新开机，空闲态UE，失步态UE以切换入UE都通过随机接入完成和gNodeB的上行同步，进入同步态。

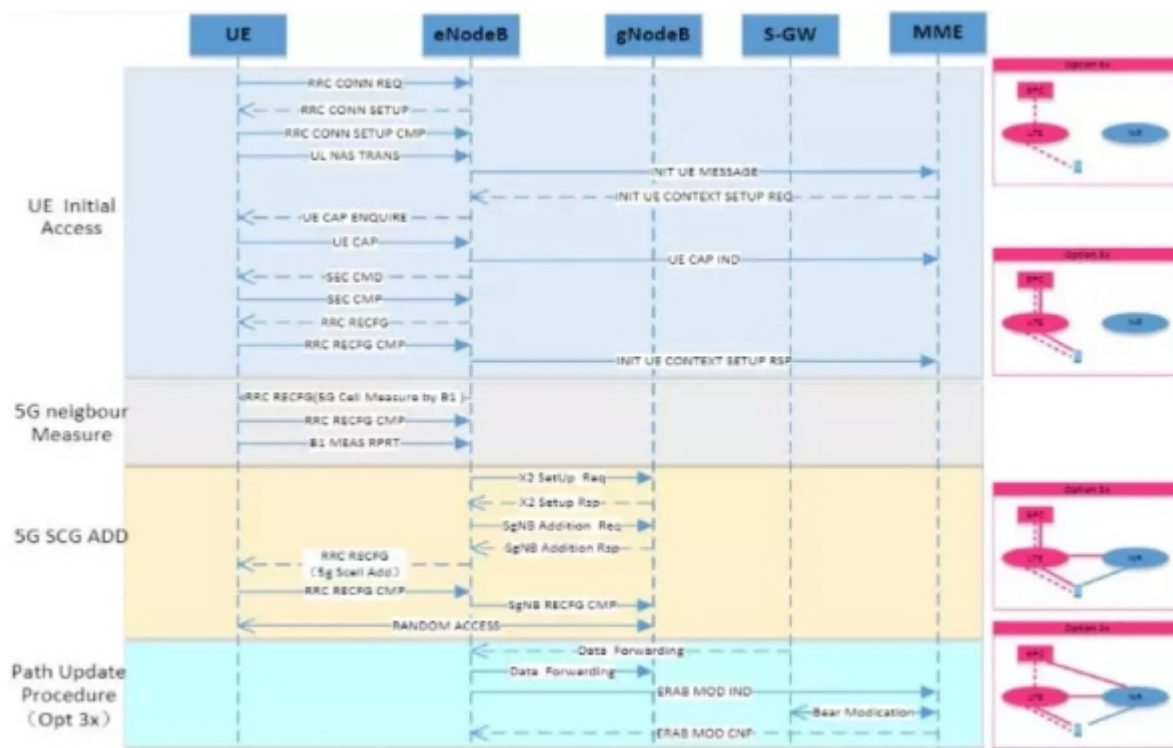
gNodeB根据Random Access Preamble测量得到UE侧的定时偏移，通过RAR消息携带给UE。



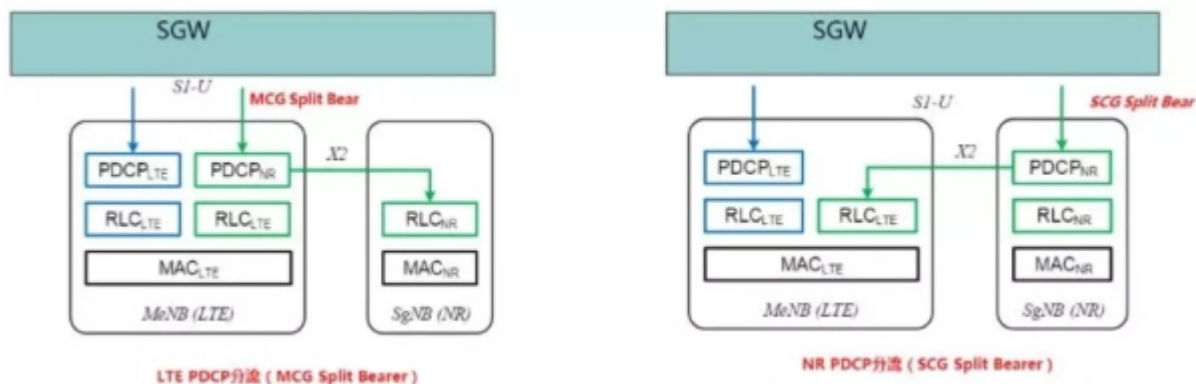


## 二、5G NSA信令流程

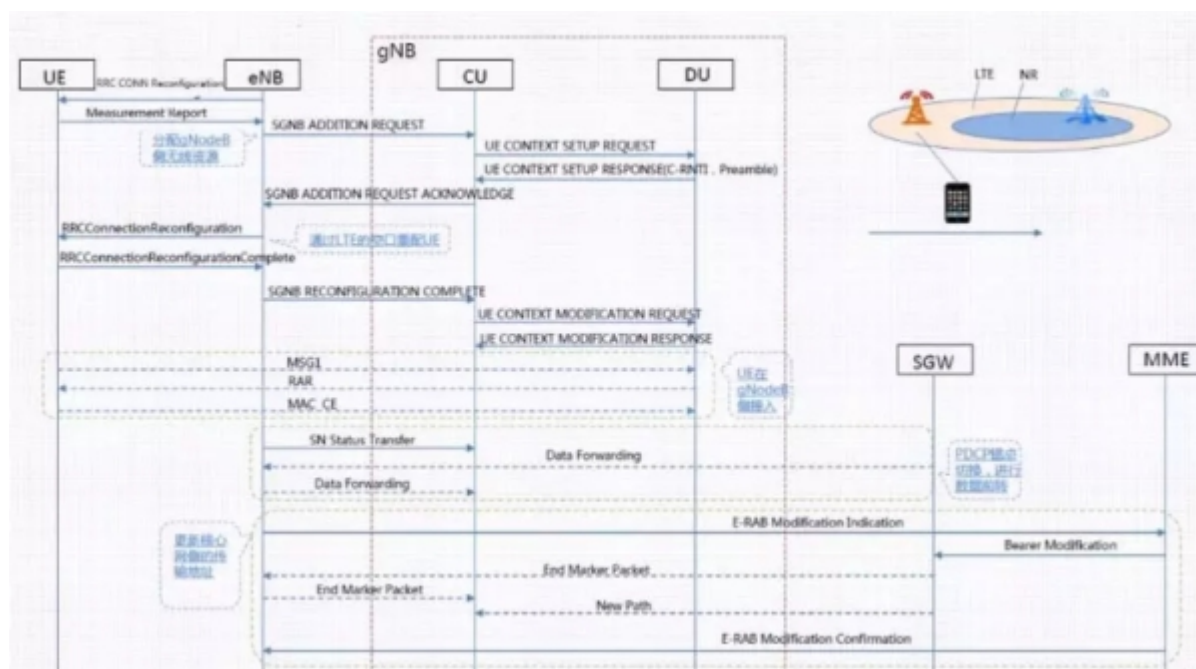
### 1. NSA总流程



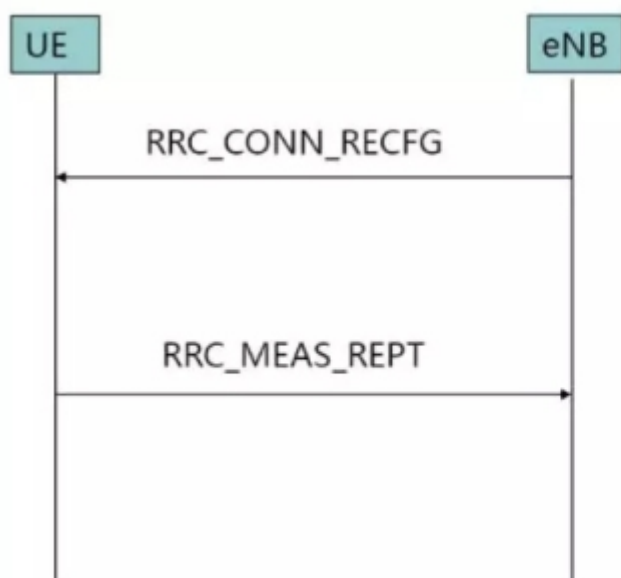
### 2. NSA下行数据分流



### 3. NSA辅站添加流程



### 4. 测量控制及测量报告上报



1. UE成功接入LTE后，eNB会通过“RRC\_CONN\_RECFG”下发NR的测量控制：包括测量事件B1及相关门限，NR的绝对频点号等
2. UE启动测量，当发现满足条件的NR小区后，通过测量报告上报NR小区的PCI及RSRP

The screenshot shows the 'Process Explorer' tool with the 'Process List' window open. The process list includes:

Name	PID	PPID	Name	Path
NRC_CONN_RECV_CMP	24	1594	NRC	C:\Program Files\NRC\NRC.exe
NRC_CONN_RECV_CMP	26	1594	NRC	C:\Program Files\NRC\NRC.exe
NRC_CONN_RECV_CMP	28	1594	NRC	C:\Program Files\NRC\NRC.exe
NRC_CONN_RECV_CMP	30	1594	NRC	C:\Program Files\NRC\NRC.exe

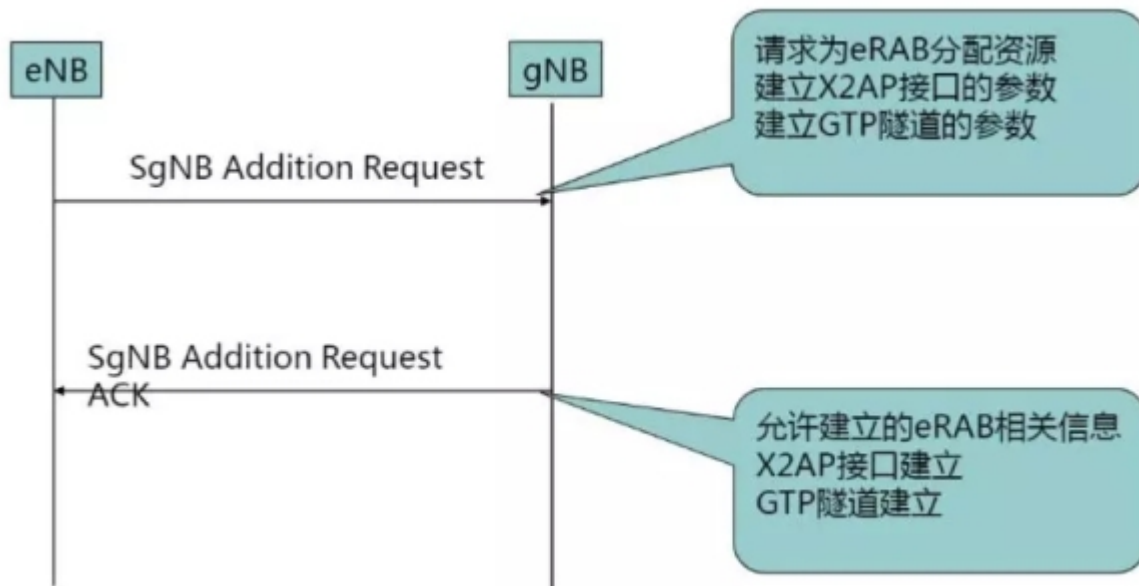
The 'Process List' window is open, showing the process details for 'NRC\_CONN\_RECV\_CMP'.

[illegible]

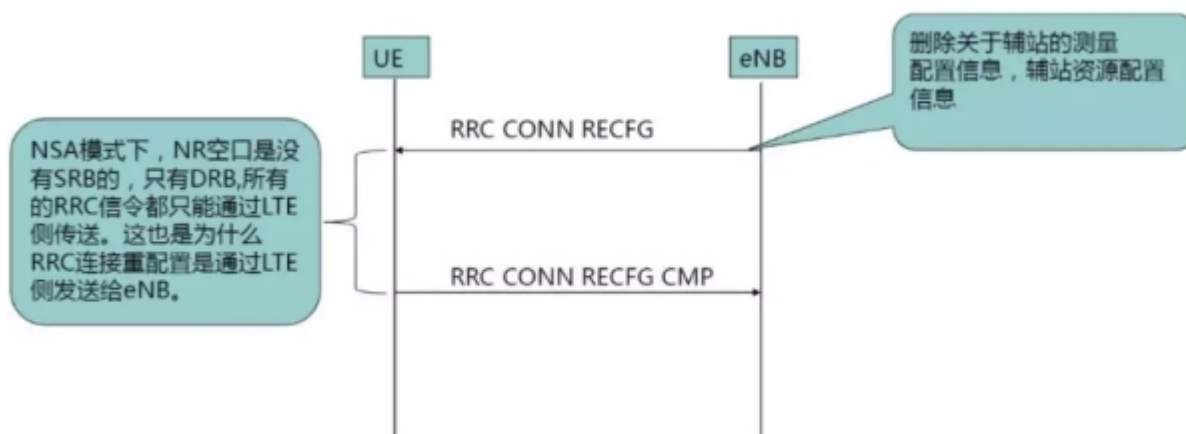
The screenshot displays the Wireshark interface for analyzing an RRC\_Meas\_Req message. The left pane shows the packet list with RRC\_Meas\_Req selected. The right pane shows the message structure tree, with the 'measResults' field expanded to show measurement results for various cells, including 'cellMeasResult-r15' for 'physCellId-r15'.

### ▼网管信元

## 5. 辅站添加



## 6. 空口辅站添加信令流程

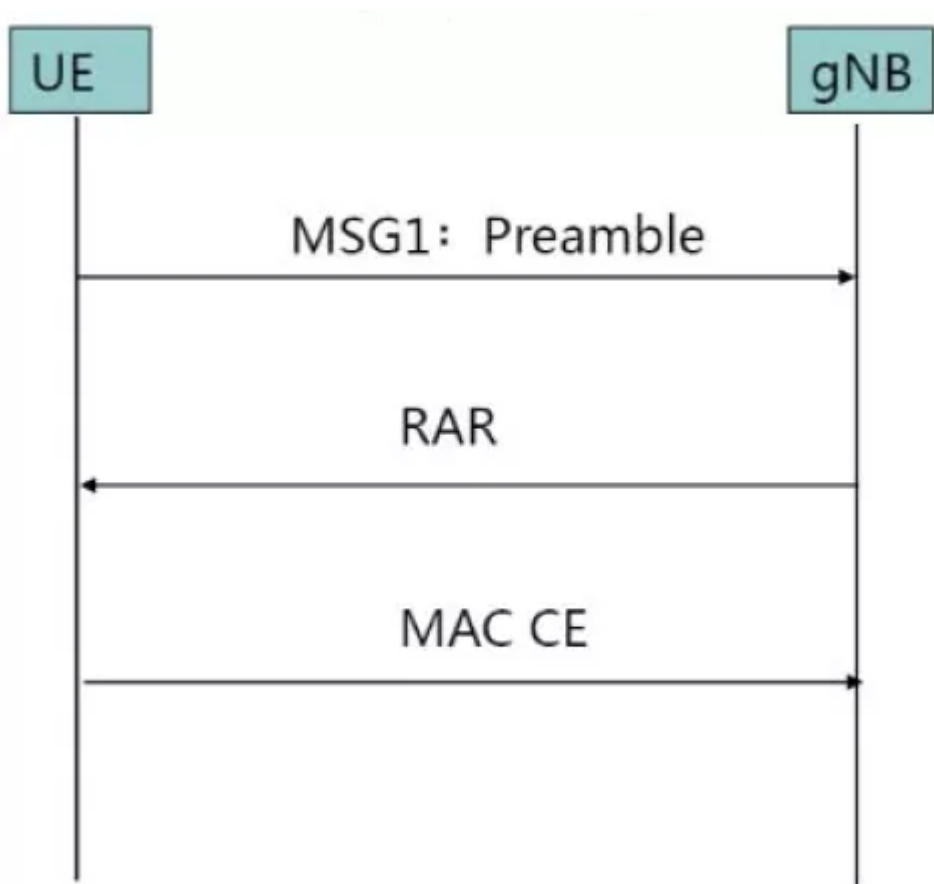


## 7. gNR侧的随机接入

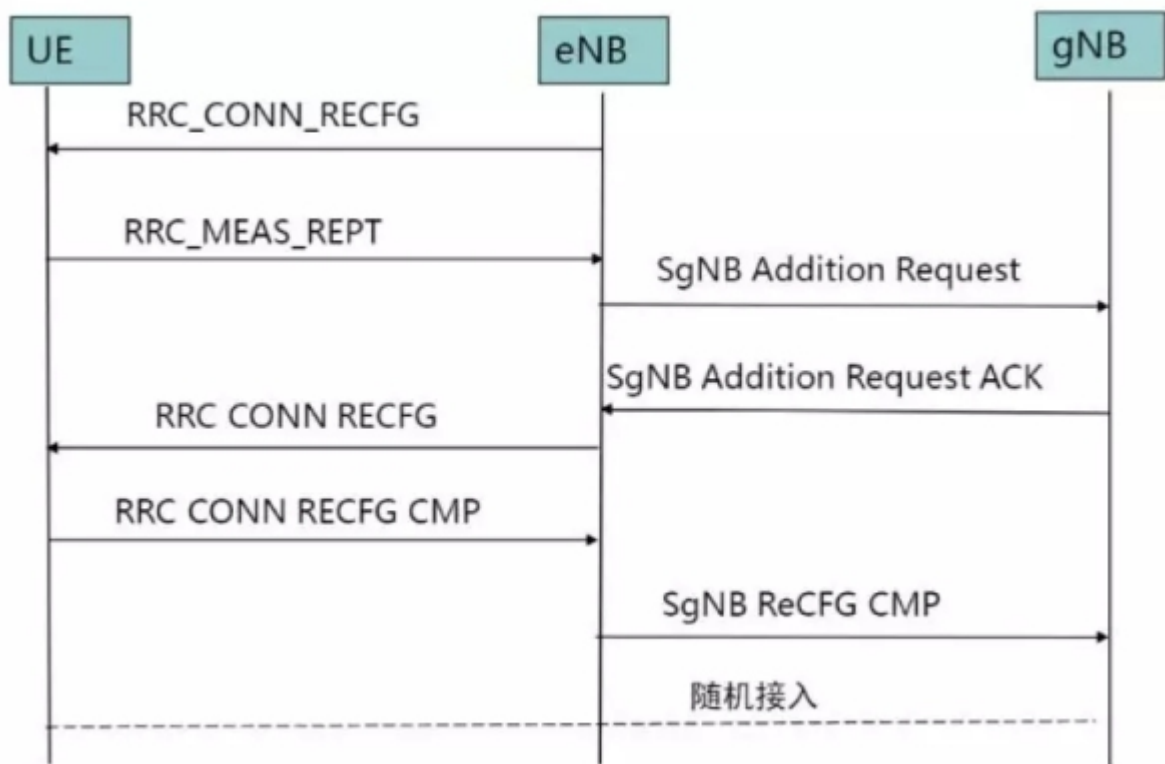
UE在LTE侧发送RRC连接重配置完成后, 就会尝试接入NR;

以下三条信令因为是层1信令, 所以无法通过LMT进行跟踪。

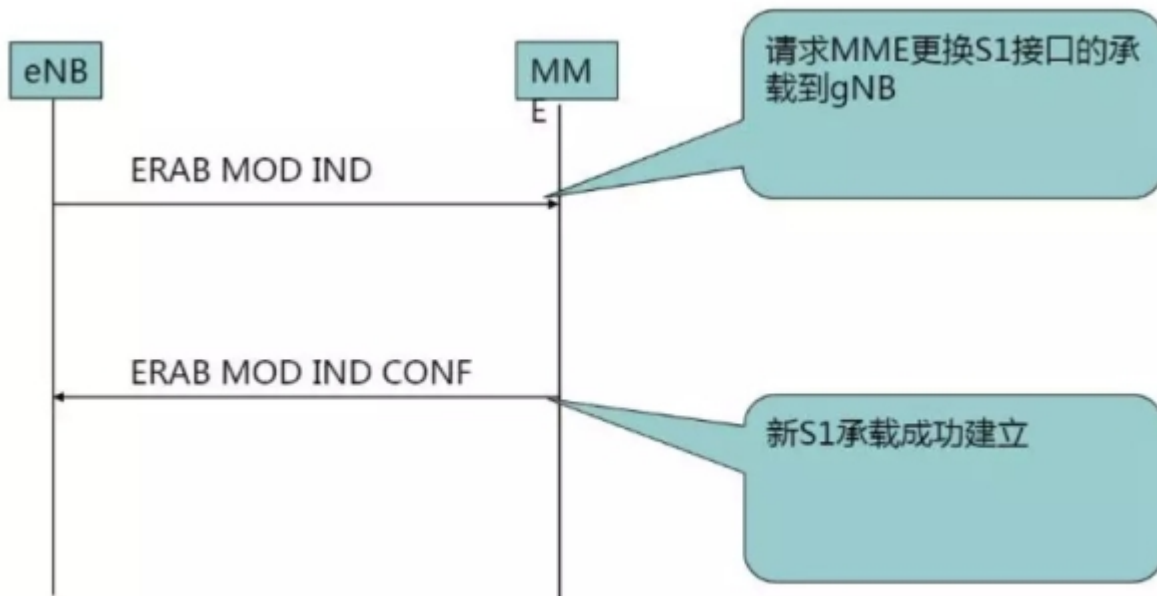
NSA模式下, NR空口是没有SRB的, 只有DRB, 所有的RRC信令只能通过LTE传送。下图MSG3, 只有MAC CE, 是不包含RRC信令的。



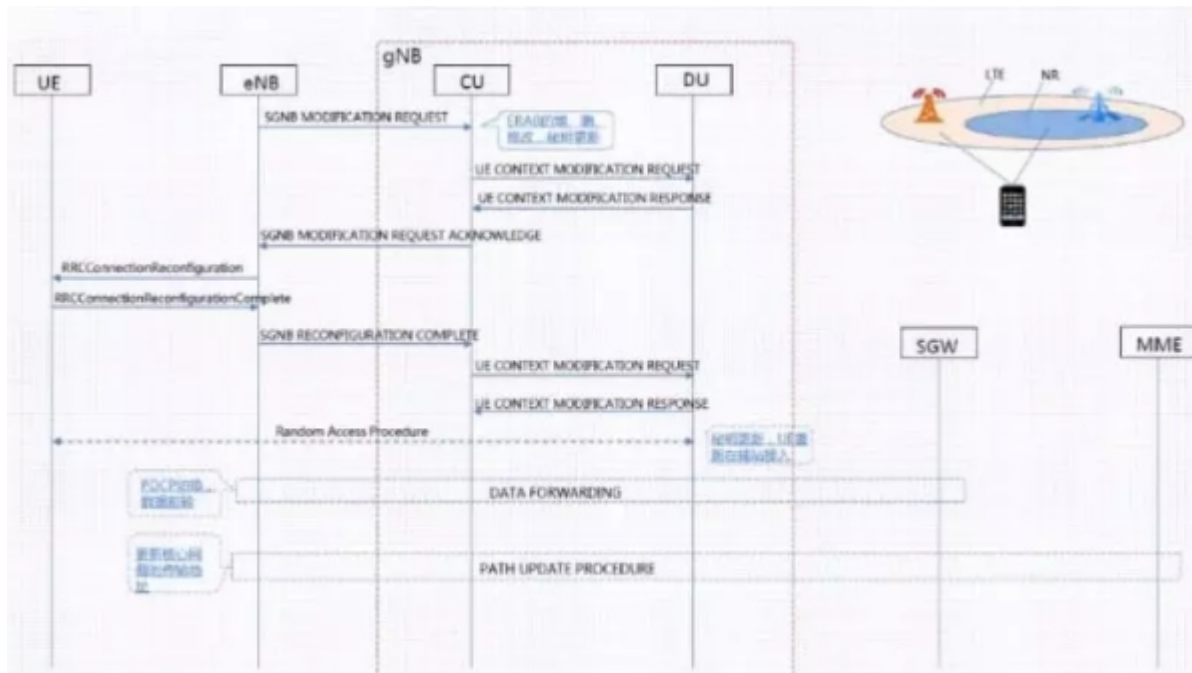
## 8. 辅站添加流程



## 9. 核心网侧的传输地址更新

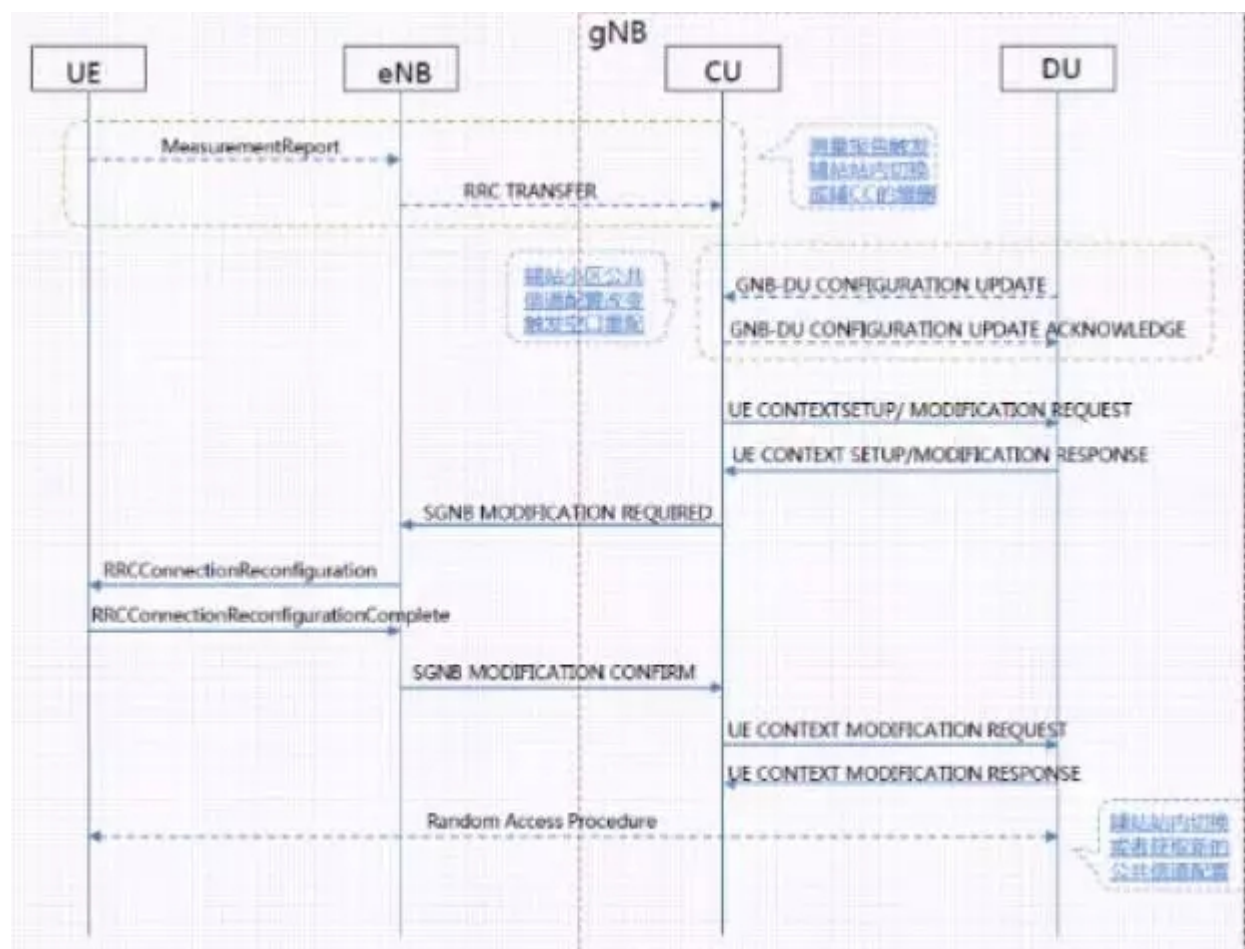


## 10. NSA辅站修改(主站触发)

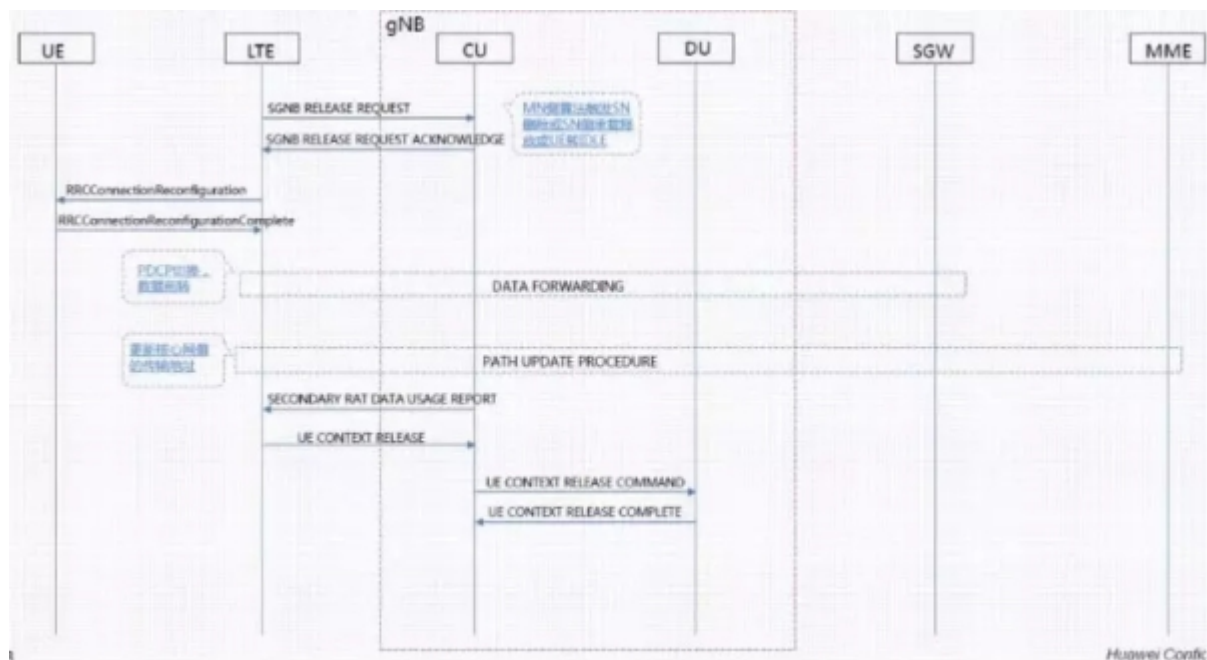


## 11. NSA辅站修改(辅站触发)

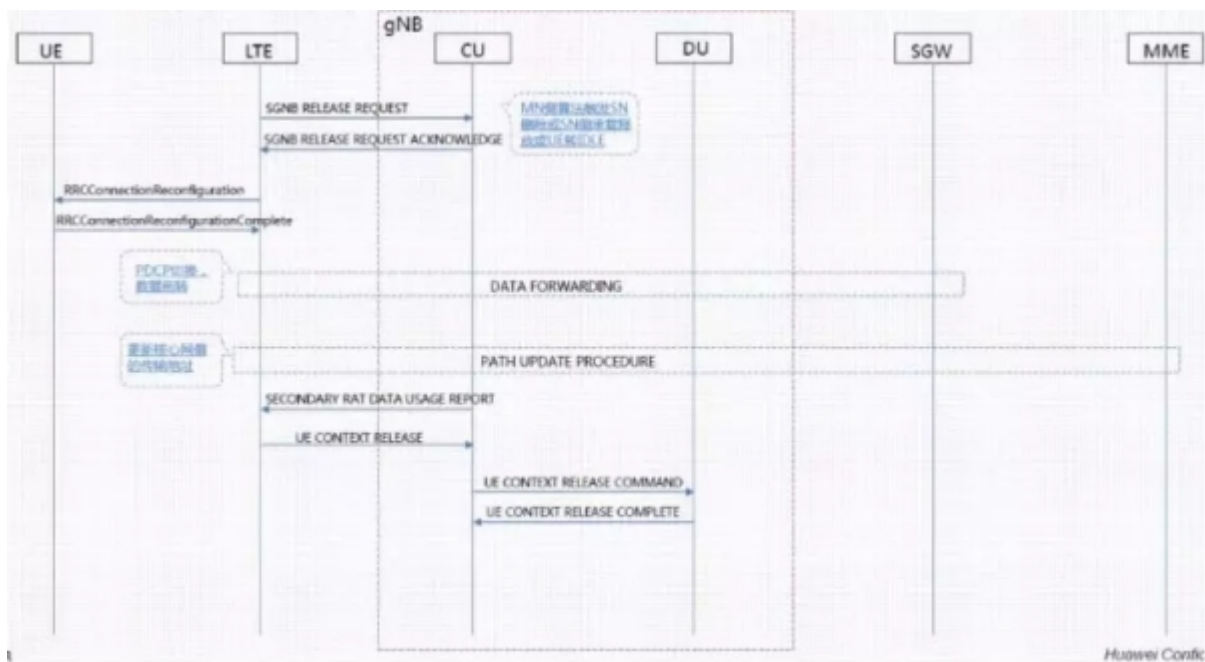




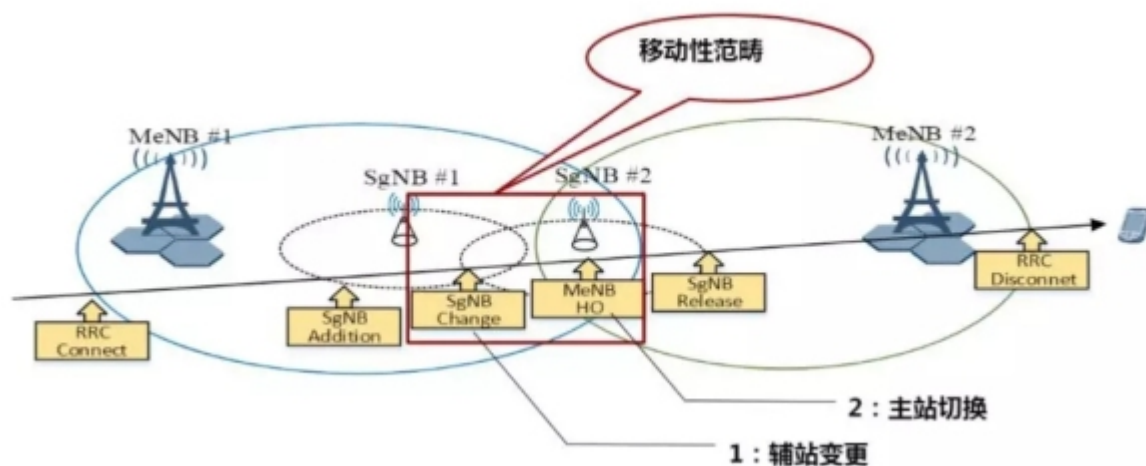
## 12. 主站触发的辅站释放



## 13. 辅站触发的辅站释放

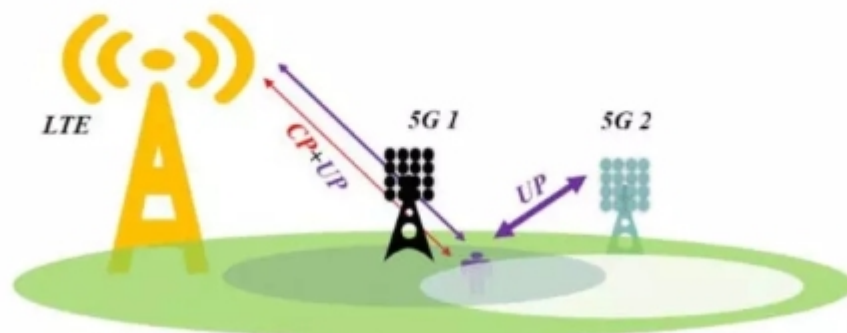


### 三、5G移动性信令流程



### 概念-辅站变更

- 辅站变更是一种在NSA场景下将UE的PSCell从NR侧一个小区转移到另一个小区的过程，
- NSA场景下NR辅站的测量事件在LTE侧下发。NR有测量控制模块，NR测量控制模块的测量控制信息通过X2口传递到LTE。LTE将测量控制信息下发给UE，UE的测量信息上报给LTE，LTE通过X2口将测量上报信息传递给NR。



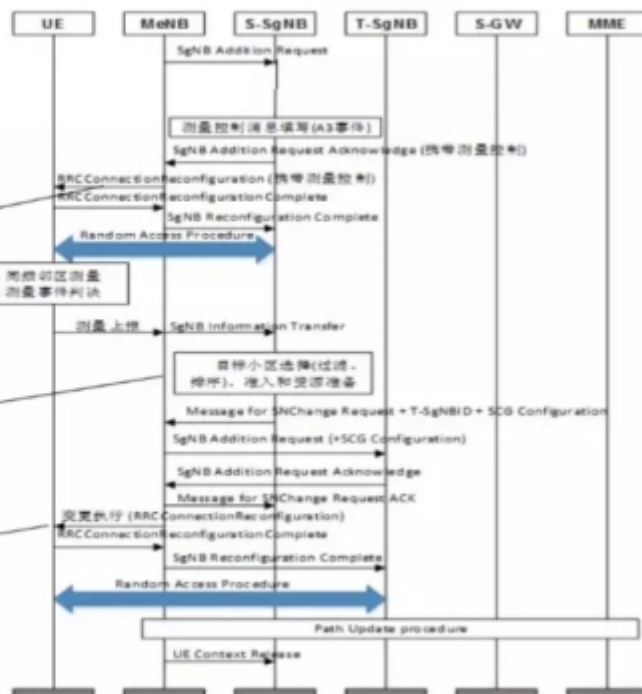
## 流程-辅站变更

1: 测量控制信息下发

2: UE进行邻区测量  
并上报测量结果

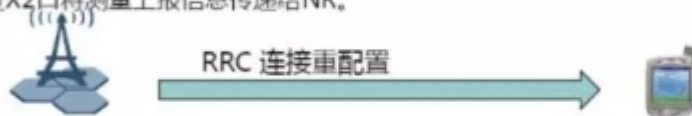
3: 辅站变更判决

4: 辅站变更命令下发



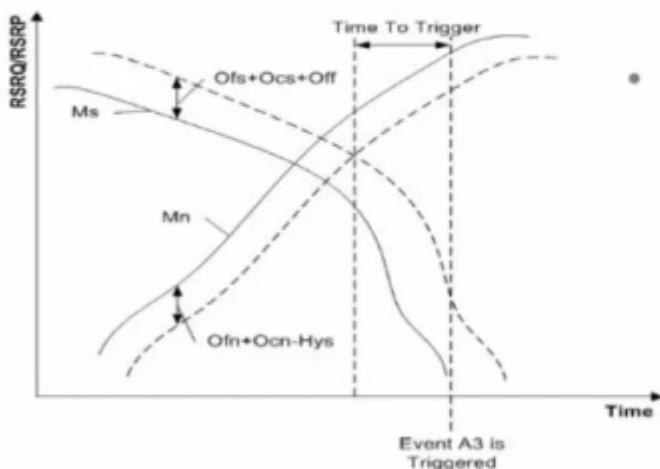
## 测量控制下发

- 5G RAN1.0中，NSA场景下NR辅站的测量事件全部在LTE侧下发。NR有测量控制模块，NR测量控制模块的测量控制信息通过X2口传递到LTE。LTE将测量控制信息下发给UE，UE的测量信息上报给LTE，LTE通过X2口将测量上报信息传递给NR。



- 测量配置参数主要由SgNB管理配置，在EN-DC UE建立无线承载后，SgNB通过SgNB Addition Request Acknowledge消息将测量控制信息转发给MeNB，而MeNB通过RRC Connection Reconfiguration下发该测量配置信息给UE。
- 测量配置信息主要由测量对象、测量任务的测量事件及其参数（报告配置）以及测量消息中的公共配置构成。
- 5G RAN1.0，辅站变更中仅支持A3同频测量

## 测量控制下发 - A3



- 同频辅站变更通过事件A3触发，且事件上报方式采用事件转周期的上报方式

- 触发条件：

- $Mn + Ofn + Ocn - Hys > Ms + Ofs + Ocs + Off$

- 取消条件：

- $Mn + Ofn + Ocn + Hys < Ms + Ofs + Ocs + Off$

## 测量事件 - 事件报告配置

### reportConfigNR

#### triggerType

##### event

##### eventId

##### eventA3

a3-Offset:0x2 (2)

reportOnLeave:FALSE

hysteresis:0x2 (2)

timeToTrigger:ms160 (6)

triggerQuantity:rsrp (0)

reportQuantity:sameAsTriggerQuantity (0)

maxReportCells:0x4 (4)

reportInterval:ms240 (1)

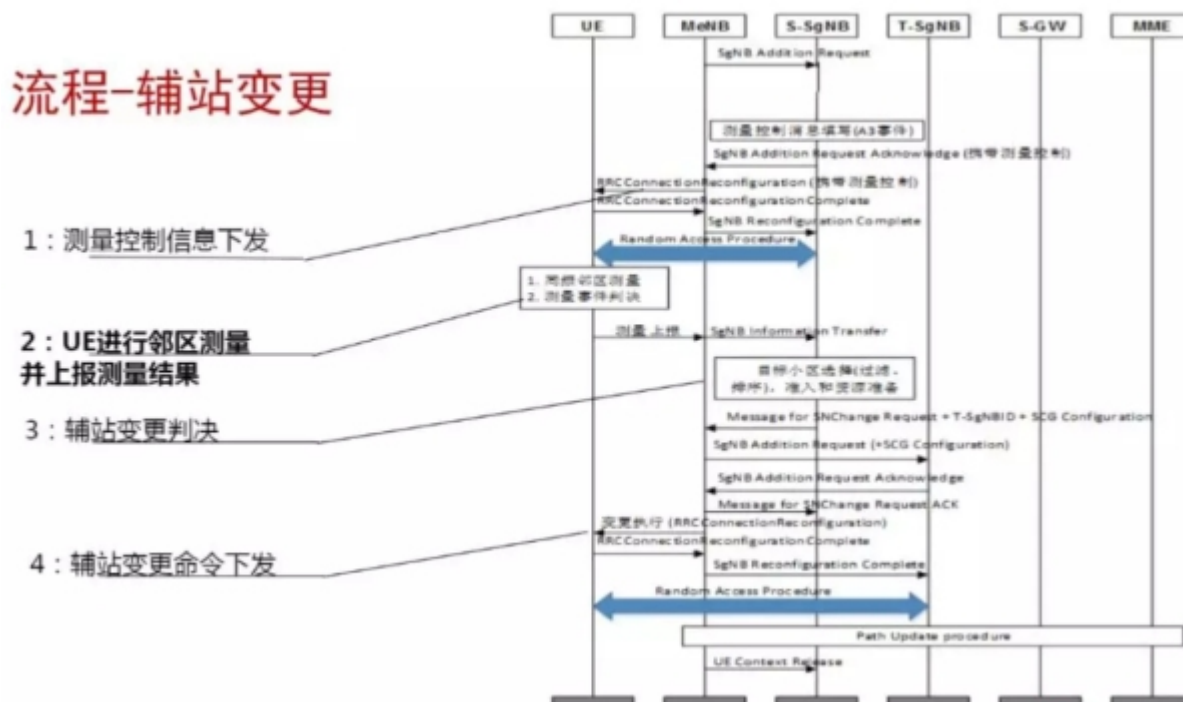
reportAmount:infinity (7)

Off

Hys

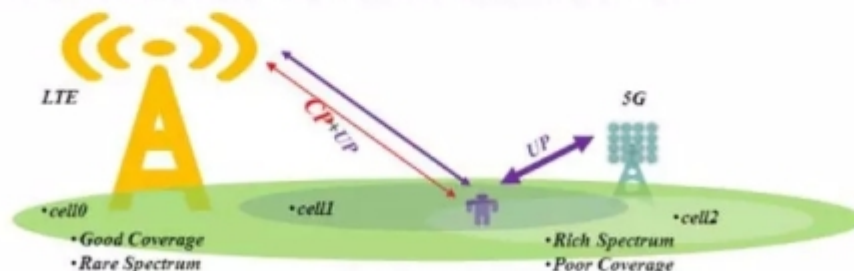
Time to  
Trigger

## 流程-辅站变更



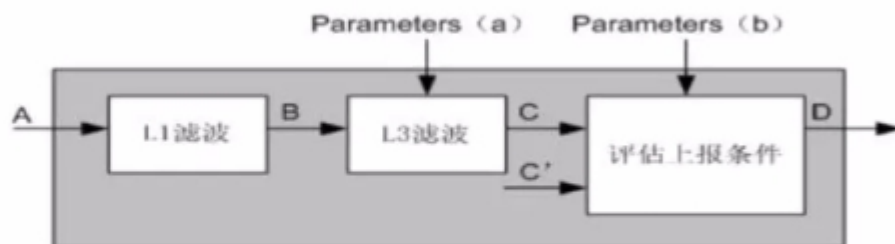
## UE测量上报

- 根据基站下发的测量控制消息，UE进行测量，当同频邻区质量满足所配置的A3事件的触发条件，UE将向基站侧上报测量结果
- UE的测量信息上报给LTE MeNB，LTE通过X2口将测量上报信息传递给NR侧的SgNB。
- 默认配置下，UE上报的邻区的小区级测量结果即为邻区的最佳波束测量结果。



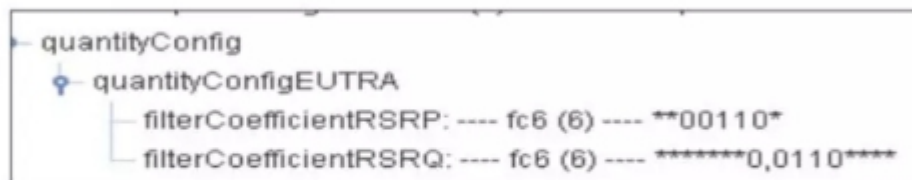


## UE测量- 滤波配置



- A为TUE侧的物理层的直接测量结果
- B是经过L1滤波的物理层的测量结果，即向高层提供的测量结果
- C是经过L3滤波后的测量值

## UE测量-滤波配置（续）



- 该参数表示NR的RSRP、RSRQ高层滤波系数
- 该参数越大，对信号平滑作用越强，抗快衰落能力越强，但对信号变化的跟踪能力变弱



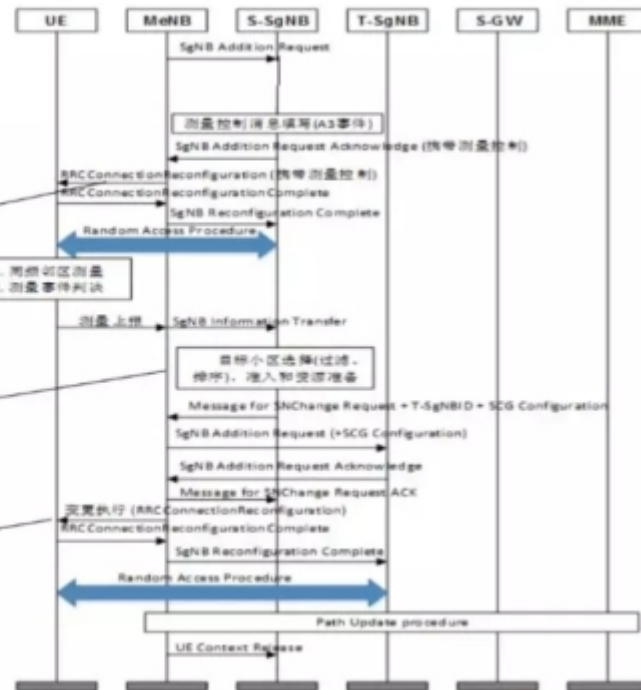
## 流程-辅站变更

1: 测量控制信息下发

2: UE进行邻区测量  
并上报测量结果

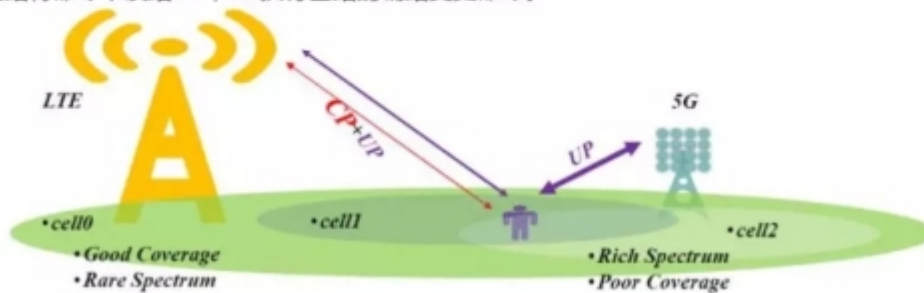
3: 辅站变更判决

4: 辅站变更命令下发



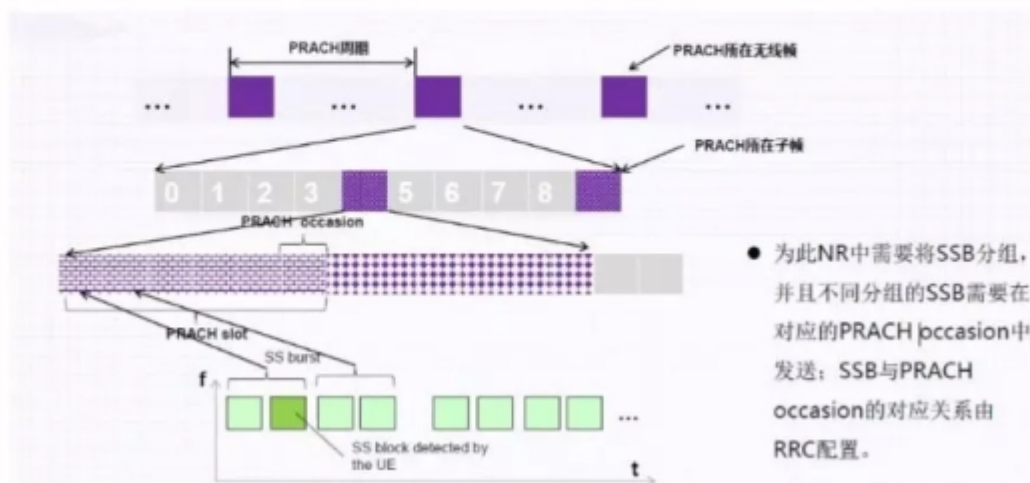
## 基站判决和命令下发

- MeNB将测量结果发给SgNB后，sgNB对测量结果进行评估判决：MeasId的正确性、上报邻区为可知邻区，将满足要求的小区生成辅站变更的目标小区列表。
- gNodeB将对目标小区列表中选一个质量最好小区发起辅站变更尝试。
- MeNB基站将命令下发给UE，UE执行基站的辅站变更命令。

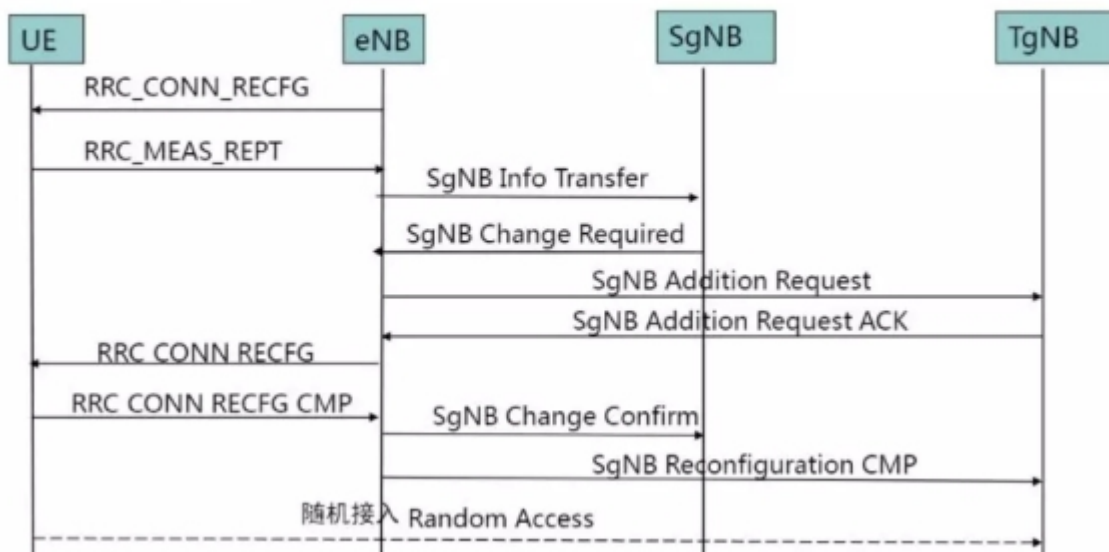


## 随机接入的波束管理

- NR中支持波束，因此随机接入过程需要支持波束扫描机制，此外NR中还需要将UE扫描到的下行波束信息反馈给gNodeB



## 辅站变更流程



## 流程-主站站内切换

18B版本MeNB站内切换时，当源MeNB没有收到源SgNB的释放请求时，则需SgNB做站内切换：

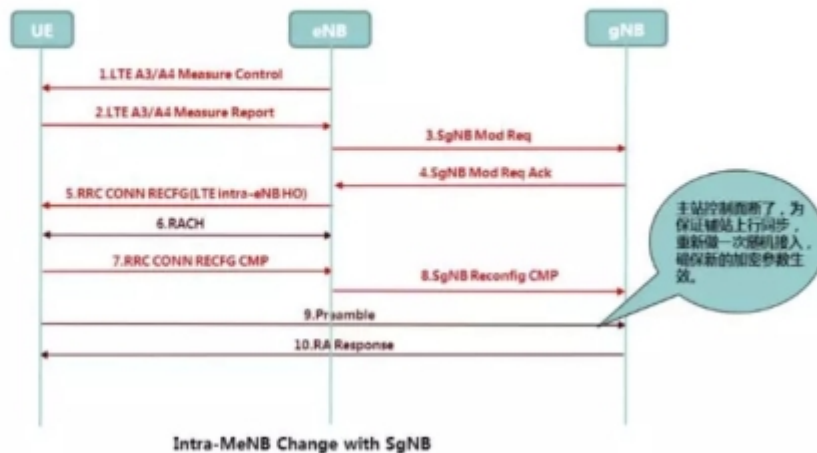
1~2:eNB下发LTE 同频/异频测量控制，UE上报同频/异频测量报，eNodeB收到测量报告判断触发站内切换。

3~4：eNB发送SgNB Modify Request消息，其中包括了LTE小区切换后加密参数等用户上下文信息的变更，通知辅站SgNB更新加密参数，SgNB重新完成配置并响应。

5~7：UE完成切换到新的LTE主小区。

9~10：UE根据eNB下发的重配置信息随机接入到目标eNB和原辅站小区。

若MeNB在站内切换时，辅站已经释放，则在切换时不需要辅站切换，切换完成或重新发起辅站添加流程。



## 流程-主站站间切换

1.当前18B不支持：MeNB跨站切换带SCG

2. 18B版本MeNB跨站切换时，只能将SCG删除后，重新在目标MeNB添加辅站。

