通常，我们把物联网设备分为三类：

①无需移动性，大数据量（上行），需较宽频段，比如城市监控摄像头。

②移动性强，需执行频繁切换，小数据量，比如车队追踪管理。

③无需移动性，小数据量，对时延不敏感，比如智能抄表。

**NB-IoT正是为了应对第③种物联网设备而生。**

NB-IoT源起于现阶段物联网的以下几大需求：



•覆盖增强（增强20dB）

•支持大规模连接，100K终端/200KHz小区

•超低功耗，10年电池寿命

•超低成本

•最小化信令开销，尤其是空口。

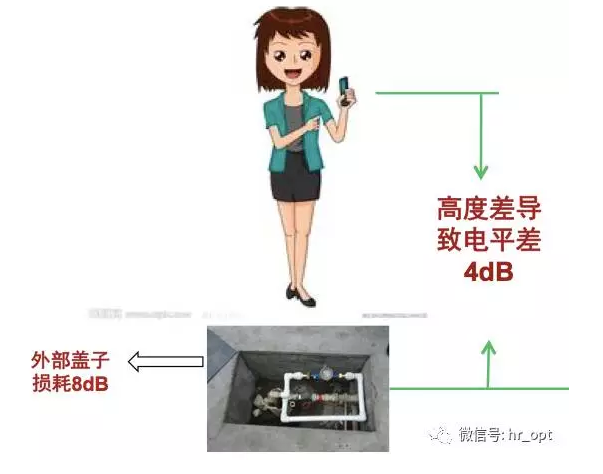
•确保整个系统的安全性，包括核心网。

•支持IP和非IP数据传送。

•支持短信（可选部署）。

对于现有LTE网络，并不能完全满足以上需求。即使是LTE-A，关注的主要是载波聚合、双连接和D2D等功能，并没有考虑物联网。

比如，在覆盖上，以水表为例，所处位置无线环境差，与智能手机相比，高度差导致信号差4dB，同时再盖上盖子，额外增加约10dB左右损耗，所以需要增强20dB。



在大规模连接上，物联网设备太多，如果用现有的LTE网络去连接这些海量设备，会导致网络过载，即使传送的数据量小，可信令流量也够得喝上几壶。

此外，NB-IoT有自己的特点，比如不再有QoS的概念，因为现阶段的NB-IoT并不打算传送时延敏感的数据包，像实时IMS一类的设备，在NB-IoT网络里不会出现。

因此，3GPP另辟蹊径，在Release 13制定了NB-IoT标准来应对现阶段的物联网需求，在终端支持上也多了一个与NB-IoT对应的终端等级——cat-NB1。

尽管NB-IoT和LTE紧密相关，且可集成于现有的LTE系统之上，很多地方是在LTE基础上专为物联网而优化设计，但从技术角度看，NB-IoT却是独立的新空口技术。

今天，我们就来看看这一新空口技术到底有多新？

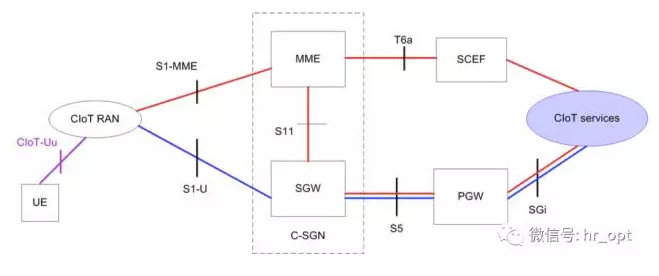
**1 网络**

**1.1 核心网**

为了将物联网数据发送给应用，蜂窝物联网（CIoT）在EPS定义了两种优化方案：

•CIoT EPS用户面功能优化（User Plane CIoT EPS optimisation）

•CIoT EPS控制面功能优化（Control Plane CIoT EPS optimisation）



如上图所示，红线表示CIoT EPS控制面功能优化方案，蓝线表示CIoT EPS用户面功能优化方案。

对于CIoT EPS控制面功能优化，上行数据从eNB（CIoT RAN）传送至MME，在这里传输路径分为两个分支：或者通过SGW传送到PGW再传送到应用服务器，或者通过SCEF（Service Capa- bility Exposure Function）连接到应用服务器（CIoT Services），后者仅支持非IP数据传送。下行数据传送路径一样，只是方向相反。

这一方案无需建立数据无线承载，数据包直接在信令无线承载上发送。因此，这一方案极适合非频发的小数据包传送。

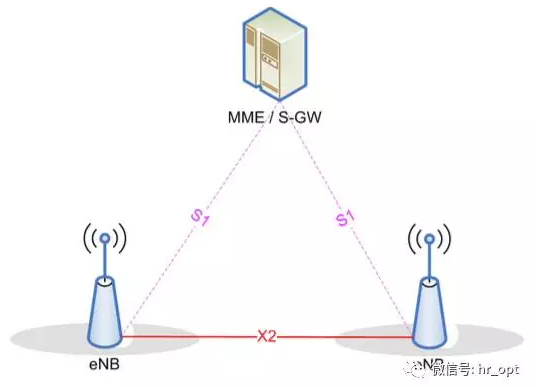
SCEF是专门为NB-IoT设计而新引入的，它用于在控制面上传送非IP数据包，并为鉴权等网络服务提供了一个抽象的接口。

对于CIoT EPS用户面功能优化，物联网数据传送方式和传统数据流量一样，在无线承载上发送数据，由SGW传送到PGW再到应用服务器。因此，这种方案在建立连接时会产生额外开销，不过，它的优势是数据包序列传送更快。

这一方案支持IP数据和非IP数据传送。

**1.2 接入网**

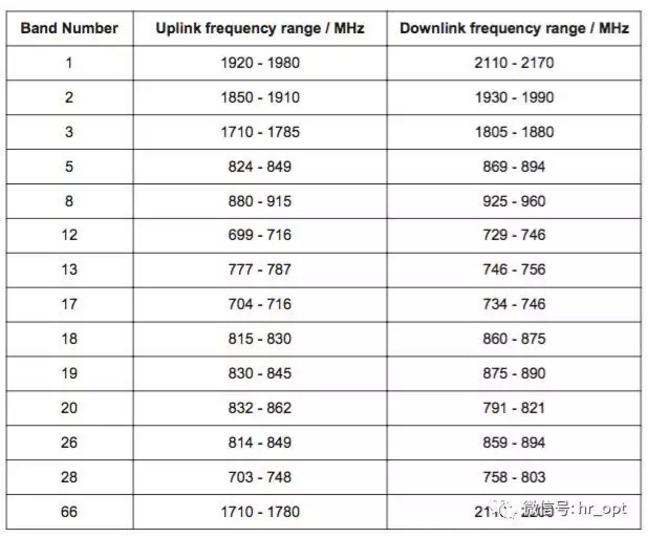
NB-IoT的接入网构架与LTE一样。



eNB通过S1接口连接到MME/S-GW，只是接口上传送的是NB-IoT消息和数据。尽管NB-IoT没有定义切换，但在两个eNB之间依然有X2接口，X2接口使能UE在进入空闲状态后，快速启动resume流程，接入到其它eNB（resume流程将在本文后面详述）。

**1.3 频段**

NB-IoT沿用LTE定义的频段号，Release 13为NB-IoT指定了14个频段。



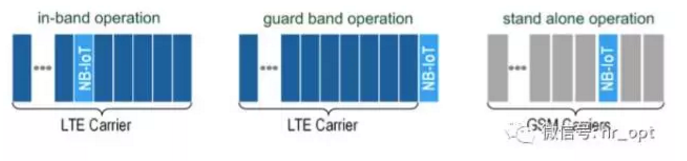
**2 物理层**



**2.1 工作模式**

**部署方式（Operation Modes）**

NB-IoT占用180KHz带宽，这与在LTE帧结构中一个资源块的带宽是一样的。所以，以下三种部署方式成为可能：



1）独立部署（Stand alone operation）

适合用于重耕GSM频段，GSM的信道带宽为200KHz，这刚好为NB-IoT 180KHz带宽辟出空间，且两边还有10KHz的保护间隔。



2）保护带部署（Guard band operation）

利用LTE边缘保护频带中未使用的180KHz带宽的资源块。

3）带内部署（In-band operation）

利用LTE载波中间的任何资源块。

**CE Level**

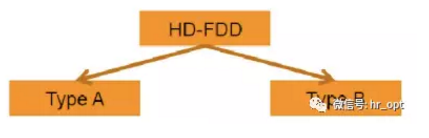
CE Level，即覆盖增强等级（Coverage Enhancement Level）。从0到2，CE Level共三个等级，分别对应可对抗144dB、154dB、164dB的信号衰减。基站与NB-IoT终端之间会根据其所在的CE Level来选择相对应的信息重发次数。

**双工模式**

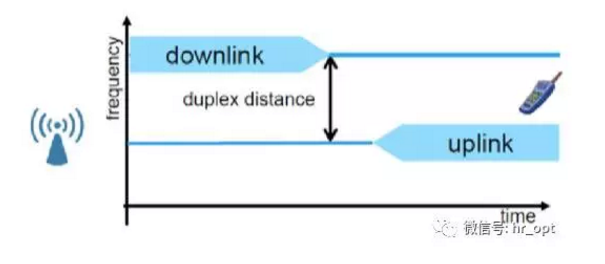
Release 13 NB-IoT仅支持FDD 半双工type-B模式。

FDD意味着上行和下行在频率上分开，UE不会同时处理接收和发送。

半双工设计意味着只需多一个切换器去改变发送和接收模式，比起全双工所需的元件，成本更低廉，且可降低电池能耗。



在Release 12中，定义了半双工分为type A和type B两种类型，其中type B为Cat.0所用。在type A下，UE在发送上行信号时，其前面一个子帧的下行信号中最后一个Symbol不接收，用来作为保护时隙（Guard Period, GP），而在type B下，UE在发送上行信号时，其前面的子帧和后面的子帧都不接收下行信号，使得保护时隙加长，这对于设备的要求降低，且提高了信号的可靠性。



**2.2 下行链路**

对于下行链路，NB-IoT定义了三种物理信道：

1）NPBCH，窄带物理广播信道。

2）NPDCCH，窄带物理下行控制信道。

3）NPDSCH，窄带物理下行共享信道。

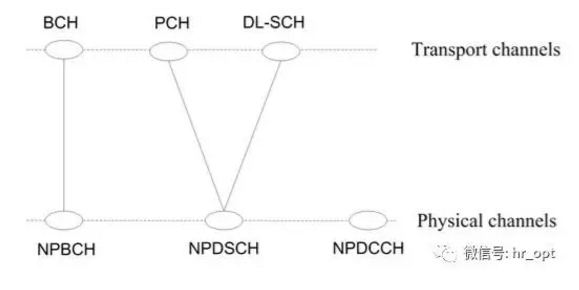
还定义了两种物理信号：

1）NRS，窄带参考信号。

2）NPSS和NSSS，主同步信号和辅同步信号。

相比LTE，NB-IoT的下行物理信道较少，且去掉了PMCH（Physical Multicast channel，物理多播信道），原因是NB-IoT不提供多媒体广播/组播服务。

下图是NB-IoT传输信道和物理信道之间的映射关系。



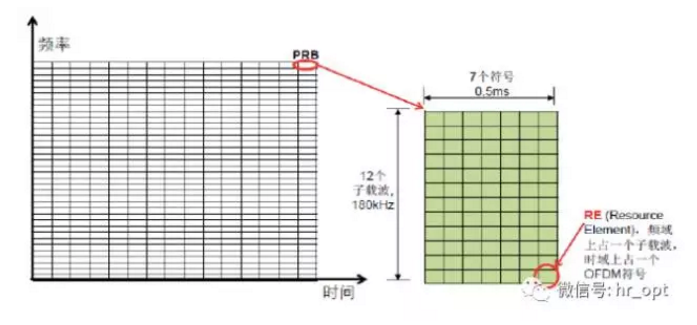
MIB消息在NPBCH中传输，其余信令消息和数据在NPDSCH上传输，NPDCCH负责控制UE和eNB间的数据传输。

NB-IoT下行调制方式为QPSK。NB-IoT下行最多支持两个天线端口（Antenna Port），AP0和AP1。

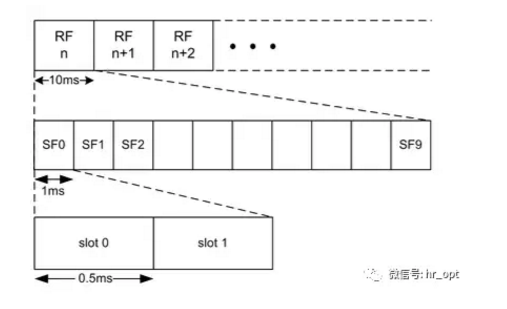
和LTE一样，NB-IoT也有PCI（Physical Cell ID，物理小区标识），称为NCellID（Narrowband physical cell ID），一共定义了504个NCellID。

**帧和时隙结构**

和LTE循环前缀（Normal CP）物理资源块一样，在频域上由12个子载波（每个子载波宽度为15KHz）组成，在时域上由7个OFDM符号组成0.5ms的时隙，这样保证了和LTE的相容性，对于带内部署方式至关重要。



每个时隙0.5ms，2个时隙就组成了一个子帧（SF），10个子帧组成一个无线帧（RF）。

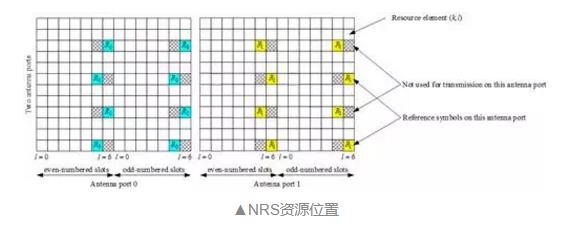


这就是NB-IoT的帧结构，依然和LTE一样。

**NRS（窄带参考信号）**

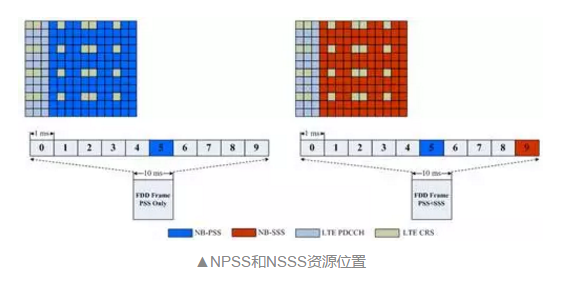
NRS（窄带参考信号），也称为导频信号，主要作用是下行信道质量测量估计，用于UE端的相干检测和解调。在用于广播和下行专用信道时，所有下行子帧都要传输NRS，无论有无数据传送。

NB-IoT下行最多支持两个天线端口，NRS只能在一个天线端口或两个天线端口上传输，资源的位置在时间上与LTE的CRS（Cell-Specific Reference Signal，小区特定参考信号）错开，在频率上则与之相同，这样在带内部署（In-Band Operation）时，若检测到CRS，可与NRS共同使用来做信道估测。



**同步信号**

NPSS为NB-IoT UE时间和频率同步提供参考信号，与LTE不同的是，NPSS中不携带任何小区信息，NSSS带有PCI。NPSS与NSSS在资源位置上避开了LTE的控制区域，其位置图如下：



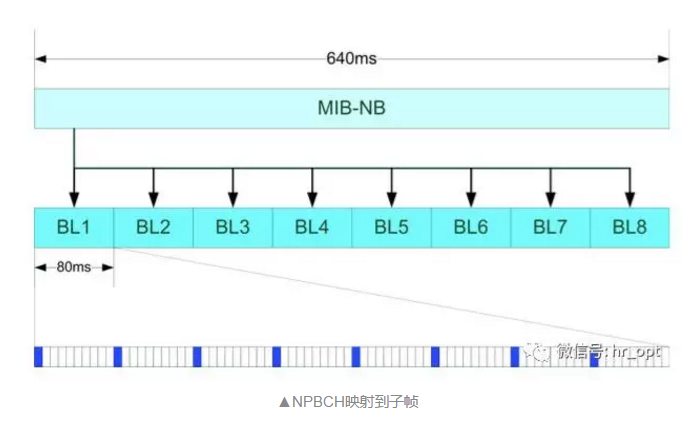
NPSS的周期是10ms，NSSS的周期是20ms。NB-IoT UE在小区搜索时，会先检测NPSS，因此NPSS的设计为短的ZC(Zadoff-Chu)序列，这降低了初步信号检测和同步的复杂性。

**NBPBCH**

NBPBCH的TTI为640ms，承载MIB-NB（Narrowband Master Information Block），其余系统信息如SIB1-NB等承载于NPDSCH中。SIB1-NB为周期性出现，其余系统信息则由SIB1-NB中所带的排程信息做排程。

和LTE一样，NB-PBCH端口数通过CRC mask识别，区别是NB-IOT最多只支持2端口。NB-IOT在解调MIB信息过程中确定小区天线端口数。

在三种operation mode下，NB-PBCH均不使用前3个OFDM符号。In-band模式下NBPBCH假定存在4个LTE CRS端口，2个NRS端口进行速率匹配。

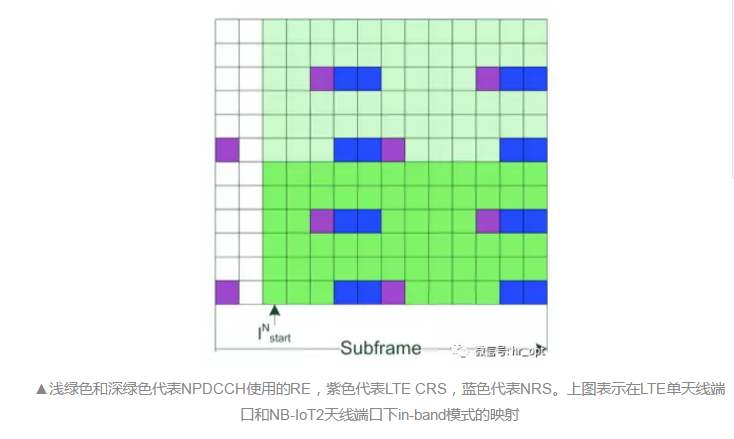




**NPDCCH**

NPDCCH中承载的是DCI（Downlink Control Information），包含一个或多个UE上的资源分配和其他的控制信息。UE需要首先解调NPDCCH中的DCI，然后才能够在相应的资源位置上解调属于UE自己的NPDSCH（包括广播消息，寻呼，UE的数据等）。NPDCCH包含了UL grant，以指示UE上行数据传输时所使用的资源。

NPDCCH子帧设计如下图所示：



NPDCCH的符号起始位置：对于in-band，如果是SIB子帧，起始位置为3，非SIB子帧，起始位置包含在SIB2-NB中；对于stand-alone和Guard band，起始位置统一为0。

NPDCCH有别于LTE系统中的PDCCH的是，并非每个Subframe都有NPDCCH，而是周期性出现。NPDCCH有三种搜索空间(Search Space)，分别用于排程一般数据传输、Random Access相关信息传输，以及寻呼(Paging)信息传输。

各个Search Space有无线资源控制(RRC)配置相对应的最大重复次数Rmax，其Search Space的出现周期大小即为相应的Rmax与RRC层配置的一参数的乘积。

RRC层也可配置一偏移(Offset)以调整Search Space的开始时间。在大部分的搜索空间配置中，所占用的资源大小为一PRB，仅有少数配置为占用6个Subcarrier。

一个DCI中会带有该DCI的重传次数，以及DCI传送结束后至其所排程的NPDSCH或NPUSCH所需的延迟时间，NB-IoT UE即可使用此DCI所在的Search Space的开始时间，来推算DCI的结束时间以及排程的数据的开始时间，以进行数据的传送或接收。

**NPDSCH**

NPDSCH的子帧结构和NPDCCH一样。

NPDSCH是用来传送下行数据以及系统信息，NPDSCH所占用的带宽是一整个PRB大小。一个传输块（Transport Block, TB）依据所使用的调制与编码策略(MCS)，可能需要使用多于一个子帧来传输，因此在NPDCCH中接收到的Downlink Assignment中会包含一个TB对应的子帧数目以及重传次数指示。

**2.3 上行链路**

对于上行链路，NB-IoT定义了两种物理信道：

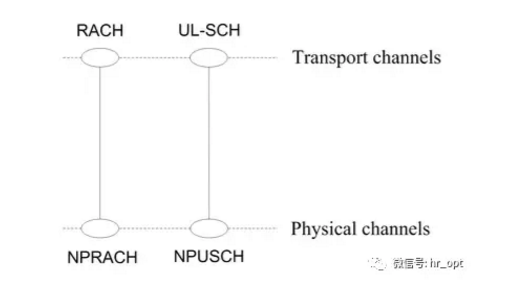
1）NPUSCH，窄带物理上行共享信道。

2）NPRACH，窄带物理随机接入信道。

还有：

1）DMRS，上行解调参考信号。

NB-IoT上行传输信道和物理信道之间的映射关系如下图：

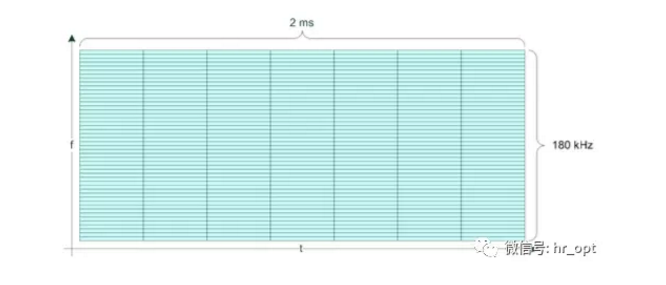


除了NPRACH，所有数据都通过NPUSCH传输。

**时隙结构**

NB-IoT上行使用SC-FDMA，考虑到NB-IoT终端的低成本需求，在上行要支持单频(Single Tone)传输，子载波间隔除了原有的15KHz，还新制订了3.75KHz的子载波间隔，共48个子载波。

当采用15KHz子载波间隔时，资源分配和LTE一样。当采用3.75KHz的子载波间隔时，如下图所示：

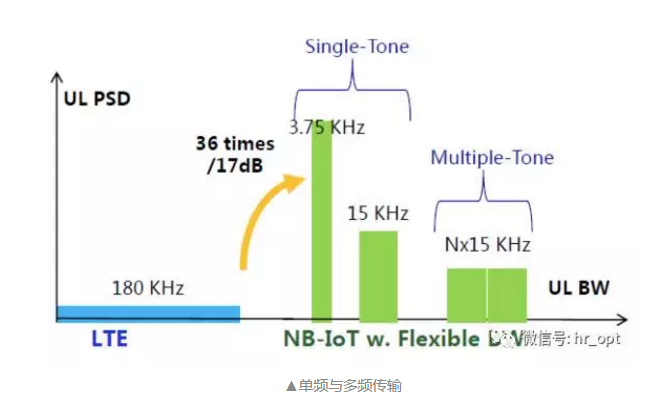


15KHz为3.75KHz的整数倍，所以对LTE系统干扰较小。由于下行的帧结构与LTE相同，为了使上行与下行相容，子载波空间为3.75KHz的帧结构中，一个时隙同样包含7个Symbol，共2ms长，刚好是LTE时隙长度的4倍。

此外，NB-IoT系统中的采样频率(Sampling Rate)为1.92MHz，子载波间隔为3.75KHz的帧结构中，一个Symbol的时间长度为512Ts(Sampling Duration)，加上循环前缀(Cyclic Prefix, CP)长16Ts，共528Ts。因此，一个时隙包含7个Symbol再加上保护区间(Guard Period)共3840Ts，即2ms长。

**NPUSCH**

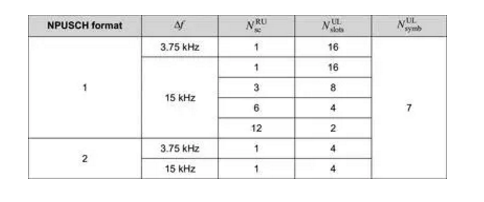
NPUSCH用来传送上行数据以及上行控制信息。NPUSCH传输可使用单频或多频传输。



在NPUSCH上，定义了两种格式：format 1和format 2。NPUSCH format 1 为UL-SCH上的上行信道数据而设计，其资源块不大于1000 bits；NPUSCH format 2传送上行控制信息（UCI）。

映射到传输快的最小单元叫资源单元（RU，resource unit），它由NPUSCH格式和子载波空间决定。

有别于LTE系统中的资源分配的基本单位为子帧，NB-IoT根据子载波和时隙数目来作为资源分配的基本单位，如下表所示：



对于NPUSCH format 1，

当子载波空间为3.75 kHz时，只支持单频传输，一个RU在频域上包含1个子载波，在时域上包含16个时隙，所以，一个RU的长度为32ms。

当子载波空间为15kHz时，支持单频传输和多频传输，一个RU包含1个子载波和16个时隙，长度为8ms；当一个RU包含12个子载波时，则有2个时隙的时间长度，即1ms，此资源单位刚好是LTE系统中的一个子帧。资源单位的时间长度设计为2的幂次方，是为了更有效的运用资源，避免产生资源空隙而造成资源浪费。

对于NPUSCH format 2，

RU总是由1个子载波和4个时隙组成，所以，当子载波空间为3.75 kHz时，一个RU时长为8ms；当子载波空间为15kHz时，一个RU时长为2ms。

对于NPUSCH format 2，调制方式为BPSK。

对于NPUSCH format 1，调制方式分为以下两种情况：

●包含一个子载波的RU，采用BPSK和QPSK。

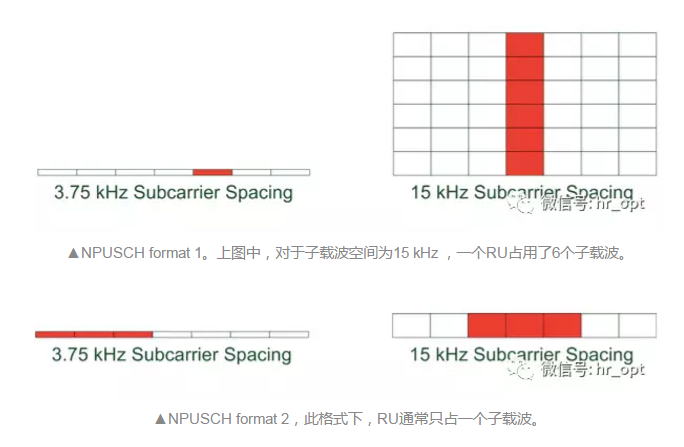
●其它情况下，采用QPSK。

由于一个TB可能需要使用多个资源单位来传输，因此在NPDCCH中接收到的Uplink Grant中除了指示上行数据传输所使用的资源单位的子载波的索引（Index），也会包含一个TB对应的资源单位数目以及重传次数指示。

NPUSCH Format 2是NB-IoT终端用来传送指示NPDSCH有无成功接收的HARQ-ACK/NACK，所使用的子载波的索引(Index)是在由对应的NPDSCH的下行分配(Downlink Assignment)中指示，重传次数则由RRC参数配置。

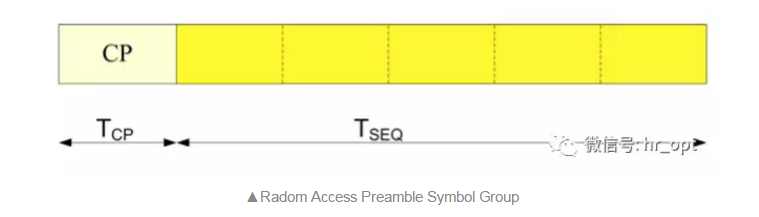
**DMRS**

根据NPUSCH格式，DMRS每时隙传输1个或者3个SC-FDMA符号。



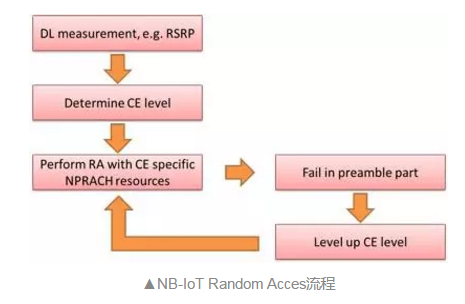
**NPRACH**

和LTE的Random Access Preamble使用ZC序列不同，NB-IoT的Random Access Preamble是单频传输（3.75KHz子载波），且使用的Symbol为一定值。一次的Random Access Preamble传送包含四个Symbol Group，一个Symbol Group是5个Symbol加上一CP，如下图：



每个Symbol Group之间会有跳频。选择传送的Random Access Preamble即是选择起始的子载波。

基站会根据各个CE Level去配置相应的NPRACH资源，其流程如下图：



Random Access开始之前，NB-IoT终端会通过DL measurement（比如RSRP）来决定CE Level，并使用该CE Level指定的NPRACH资源。一旦Random Access Preamble传送失败，NB-IoT终端会在升级CE Level重新尝试，直到尝试完所有CE Level的NPRACH资源为止。

**3 小区接入**

NB-IoT的小区接入流程和LTE差不多：小区搜索取得频率和符号同步、获取SIB信息、启动随机接入流程建立RRC连接。当终端返回RRC\_IDLE状态，当需要进行数据发送或收到寻呼时，也会再次启动随机接入流程。

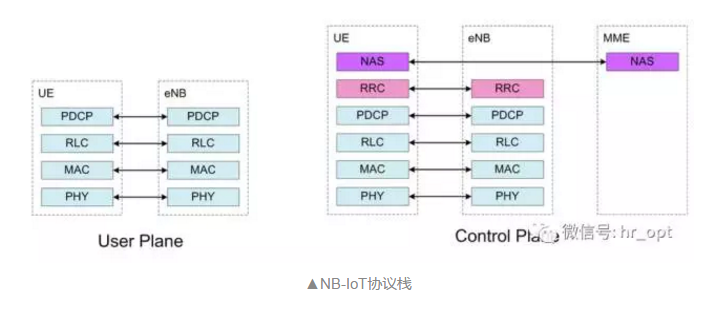
**3.1 协议栈和信令承载**

总的来说，NB-IoT协议栈基于LTE设计，但是根据物联网的需求，去掉了一些不必要的功能，减少了协议栈处理流程的开销。因此，从协议栈的角度看，NB-IoT是新的空口协议。

以无线承载（RB）为例，在LTE系统中，SRB（signalling radio bearers，信令无线承载）会部分复用，SRB0用来传输RRC消息，在逻辑信道CCCH上传输；而SRB1既用来传输RRC消息，也会包含NAS消息，其在逻辑信道DCCH上传输。

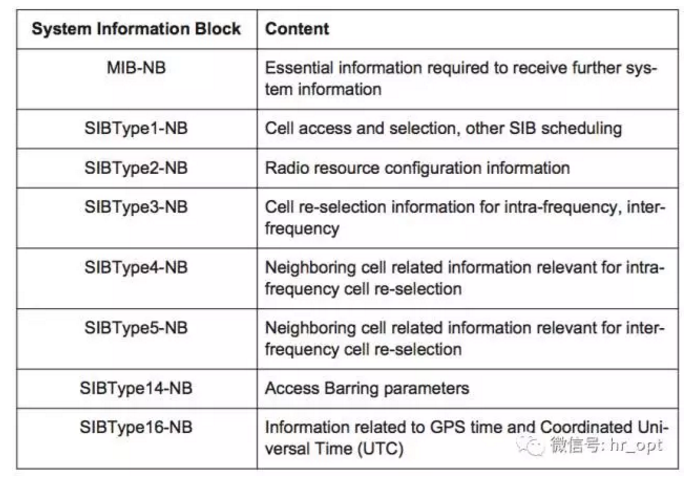
LTE中还定义了SRB2，但NB-IoT没有。

此外，NB-IoT还定义一种新的信令无线承载SRB1bis，SRB1bis和SRB1的配置基本一致，除了没有 PDCP，这也意味着在Control Plane CIoT EPS optimisation下只有SRB1bis，因为只有在这种模式才不需要。



**3.2 系统信息**

NB-IoT经过简化，去掉了一些对物联网不必要的SIB，只保留了8个:



•SIBType1-NB：小区接入和选择，其它SIB调度

•SIBType2-NB：无线资源分配信息

•SIBType3-NB：小区重选信息

•SIBType4-NB：Intra-frequency的邻近Cell相关信息

•SIBType5-NB：Inter-frequency的邻近Cell相关信息

•SIBType14-NB：接入禁止(Access Barring)

•SIBType16-NB：GPS时间/世界标准时间信息

需特别说明的是，SIB-NB是独立于LTE系统传送的，并非夹带在原LTE的SIB之中。

**3.3 小区重选和移动性**

由于NB-IoT主要为非频发小数据包流量而设计，所以RRC\_CONNECTED中的切换过程并不需要，被移除了。如果需要改变服务小区，NB-IoT终端会进行RRC释放，进入RRC\_IDLE状态，再重选至其他小区。

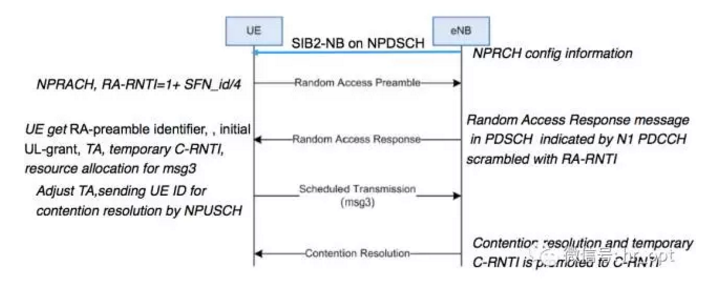
在RRC\_IDLE状态，小区重选定义了intra frequency和inter frequency两类小区，inter frequency指的是in-band operation下两个180 kHz载波之间的重选。

NB-IoT的小区重选机制也做了适度的简化，由于NB-IoT 终端不支持紧急拨号功能，所以，当终端重选时无法找到Suitable Cell的情况下，终端不会暂时驻扎(Camp)在Acceptable Cell，而是持续搜寻直到找到Suitable Cell为止。根据3GPP TS 36.304定义，所谓Suitable Cell为可以提供正常服务的小区，而Acceptable Cell为仅能提供紧急服务的小区。

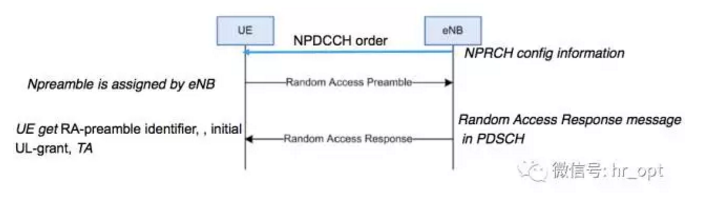
**3.4 随机接入过程**

NB-IoT的RACH过程和LTE一样，只是参数不同。

基于竞争的NB-IOT随机接入过程



基于非竞争的NB-IOT随机接入过程



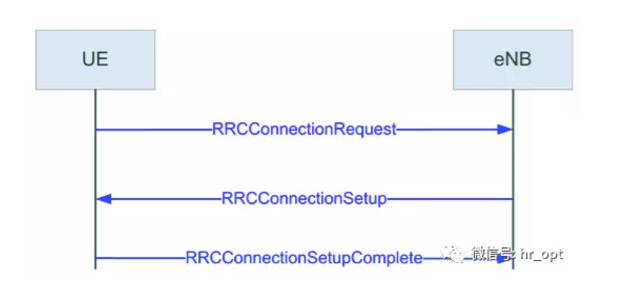
**3.5 连接管理**

由于NB-IoT并不支持不同技术间的切换，所以RRC状态模式也非常简单。



**RRC Connection Establishment**

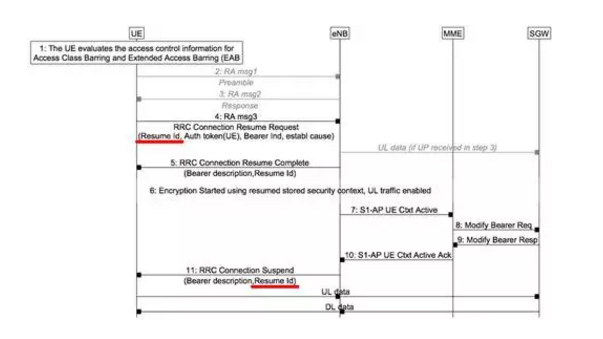
RRC Connection Establishment流程和LTE一样，但内容却不相同。



很多原因都会引起RRC建立，但是，在NB-IoT中，RRCConnectionRequest中的Establishment Cause里没有delayTolerantAccess，因为NB-IOT被预先假设为容忍延迟的。

另外，在Establishment Cause里，UE将说明支持单频或多频的能力。

与LTE不同的是，NB-IoT新增了Suspend-Resume流程。当基站释放连接时，基站会下达指令让NB-IoT终端进入Suspend模式，该Suspend指令带有一组Resume ID，此时，终端进入Suspend模式并存储当前的AS context。



当终端需要再次进行数据传输时，只需要在RRC Connection Resume Request中携带Resume ID（如上图第四步），基站即可通过此Resume ID来识别终端，并跳过相关配置信息交换，直接进入数据传输。

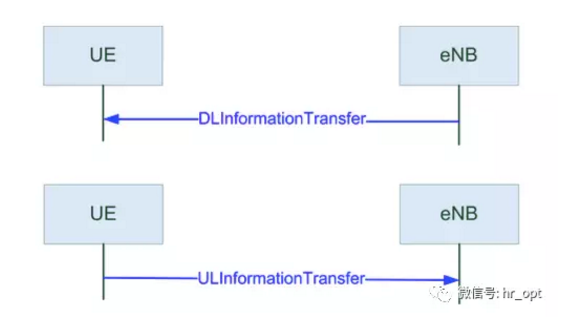
简而言之，在RRC\_Connected至RRC\_IDLE状态时，NB-IoT终端会尽可能的保留RRC\_Connected下所使用的无线资源分配和相关安全性配置，减少两种状态之间切换时所需的信息交换数量，以达到省电的目的。

**4 Data Transfer**

如前文所述，NB-IoT定义了两种数据传输模式：Control Plane CIoT EPS optimisation方案和User Plane CIoT EPS optimisation方案。对于数据发起方，由终端选择决定哪一种方案。对于数据接收方，由MME参考终端习惯，选择决定哪一种方案。

**4.1 Control Plane CIoT EPS Optimisation**

对于Control Plane CIoT EPS Optimisation，终端和基站间的数据交换在RRC级上完成。对于下行，数据包附带在RRCConnectionSetup消息里；对于上行，数据包附带在RRCConnectionSetupComplete消息里。如果数据量过大，RRC不能完成全部传输，将使用DLInformationTransfer和ULInformationTransfer消息继续传送。



这两类消息中包含的是带有NAS消息的byte数组，其对应NB-IoT数据包，因此，对于基站是透明的，UE的RRC也会将它直接转发给上一层。

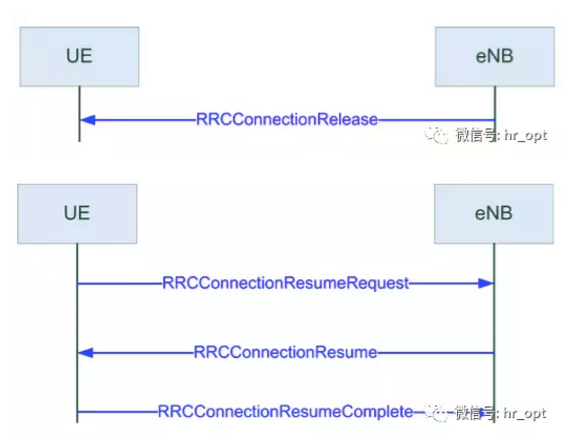
在这种传输模式下，没有RRC connection reconfiguration流程，数据在RRC connection setup消息里传送，或者在RRC connection setup之后立即RRC connection release并启动resume流程。

**4.2 User Plane CIoT EPS optimisation**

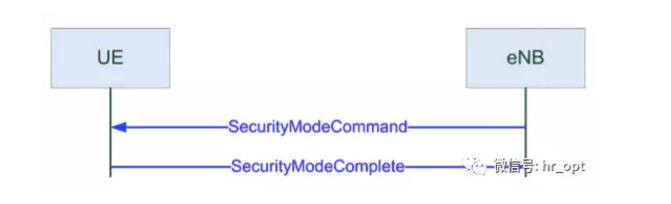
在User Plane CIoT EPS optimisation模式下，数据通过传统的用户面传送，为了降低物联网终端的复杂性，只可以同时配置一个或两个DRB。

此时，有两种情况：

•当RRC连接释放时，RRC连接释放会携带携带Resume ID，并启动resume流程，如果resume成功，更新密匙安全建立后，保留了先前RRC\_Connected的无线承载也随之建立。



•当RRC连接释放时，如果RRC连接释放没有携带携带Resume ID，或者resume请求失败，安全和无线承载建立过程如下图所示：



首先，通过SecurityModeCommand和SecurityModeComplete建立AS级安全。

在SecurityModeCommand消息中，基站使用SRB1和DRB提供加密算法和对SRB1完整性保护。LTE中定义的所有算法都包含在NB-IoT里。

当安全激活后，进入RRC connection reconfiguration流程建立DRBs。



在重配置消息中，基站为UE提供无线承载，包括RLC和逻辑信道配置。PDCP仅配置于DRBs，因为SRB采用默认值。在MAC配置中，将提供BSR、SR、DRX等配置。最后，物理配置提供将数据映射到时隙和频率的参数。

**4.3 多载波配置**

在RRCConnectionReconfiguration消息中，可在上下行设置一个额外的载波，称为非锚定载波（non-anchor carrier）。

基于多载波配置，系统可以在一个小区里同时提供多个载波服务，因此，NB-IoT的载波可以分为两类：提供NPSS、NSSS与承载NPBCH和系统信息的载波称为Anchor Carrier，其余的载波则称为Non-Anchor Carrier。

当提供non-anchor载波时，UE在此载波上接收所有数据，但同步、广播和寻呼等消息只能在Anchor Carrier上接收。

NB-IoT终端一律需要在Anchor Carrier上面Random Access，基站会在Random Access过程中传送Non-Anchor Carrier调度信息，以将终端卸载至Non-Anchor Carrier上进行后续数据传输，避免Anchor Carrier的无线资源吃紧。

另外，单个NB-IoT终端同一时间只能在一个载波上传送数据，不允许同时在Anchor Carrier和Non-Anchor Carrier上传送数据。

好了，一大堆鸟文总算翻译完了，还不算最全，不过已经腰酸痛，累成狗。分享通信知识，共享美好通信未来，我是一个兴趣使然的通信工程师