接入网协议流程

5G 是什么？目前业内已经达成了基本共识，它的一个重要属性是支持万物互联，也就意味着下一代通信网络构建的目的不仅是为用户提供更高的速率，同时也需要有效提供支持物联网的系统架构。这在协议标准里就进行了体现，3GPP 的标准并没有直接为 NB-IoT（NarrowBand Internet of Things，窄带物联网），eMTC 等物联网技术单独立书作传，但是在 LTE 的接入网，核心网等协议中进行了融合升级，这样其实也表明了一种态度，物联网的核心技术（例如物理层的调制/解调技术）与 LTE 的是大体一致的，同时又是 LTE 技术的某种方向上的演进，与 LTE 网络技术长远来看是和谐共存的。

在开始这篇文章的阅读之前，我们先简单澄清一个概念。目前蜂窝物联网技术（CIoT）是一个总体的范畴，当然还有 sidelink 这样的物物数据传输技术，可以说 CIoT 又细分成了窄带物联网（NB-IoT）和非 NB-IoT 两个领域（非 NB-IoT 包括 eMTC 或 BL UE 或支持物联网技术的 LTE 终端等），NB-IoT 技术相对比较独立，承接了某些 GSM 标准化组织早期的研究基因，这里我们不去天花乱坠的叙述物联网技术的前世今生，我们直接从协议标准的角度来理解物联网技术。

从接入网来看，NB-IoT 等终端的工作状态与 LTE 一样，基本是两种，RRC_IDLE,RRC-CONNETED,但也有一些不同的细节，例如 NB-IoT 没有互操作的属性，意味着 NB-IoT 的终端无法切换，重定向，CCO（cell change order）到 2,3G 网络，NB-IoT 终端只具备 E-UTRA 状态（只有一种工作模式）；NB-IoT 终端在连接态下不读系统消息，而 4G 终端在连接态下可以获取系统消息；NB-IoT 终端在连接态不提供任何信道反馈（没有 QoS 管控），同时也不提供测量报告（Measurement Reporting）；另外在 NB-IoT 里关于上行速率调度机制也不具备，相比较而言 MTC 终端由于根源自 LTE，因此这些基本的机制还和 LTE 大网技术保持一致，但也有一些细微的区别，我们慢慢会提及到。

信令承载和系统消息

相较于 LTE，NB-IoT 没有 SRB2，NB-IoT 使用 SRB1 bis 作为专属逻辑信道的承载。

在 LTE 系统中，UE 想要正常小区驻留，获取系统消息，首先需要获取 MIB 消息块，为了保证 MIB 的正确解读，LTE 系统以 40ms 作为周期，每个周期之内重复发送 4 次 MIB 的方式提高 MIB 获取的可靠性。而相比之下，NB-IoT 更加保守，不仅以 640ms 作为周期，每个周期内重发发送 64 次 MIB-NB，同时每 80ms 子周期内 MIB-NB 被分别独立编码了 8 次，并在每个无线帧的 0 号子帧中进行下发，这样每 80ms 都重复着这样的编码循环，提升了 MIB-NB 的获取和解读的可靠性。

LTE 系统中以 80ms 作为周期发送 SIB1 消息，每个周期之内重复发送 4 次 SIB1 消息，起始位置在 SFNmod8=0 的 5 号子帧中发送（即无线帧 0,8,16,24.....）。NB-IoT 里面的 SystemInformationBlockType1-NB (SIB1-NB) 以 2560ms 为周期进行发送，SIB1-NB 以 16 个连续的无线帧作为基本发送单位，在 4 号子帧上固定发送。在一个 2560ms 周期内等时间间隔的重复发送，可以分别按照 4,8,16 循环次数发送。SIB1-NB 的传输块大小以及 2560ms 内的循环次数在

MIB-NB 中的 *schedulingInfoSIB* 指明。

至于其他的 SI 消息的相关调度信息（SI 时/频资源占用，SI 窗长，SI 周期）在由 SIB1-NB 消息解码获取。

MasterInformationBlock

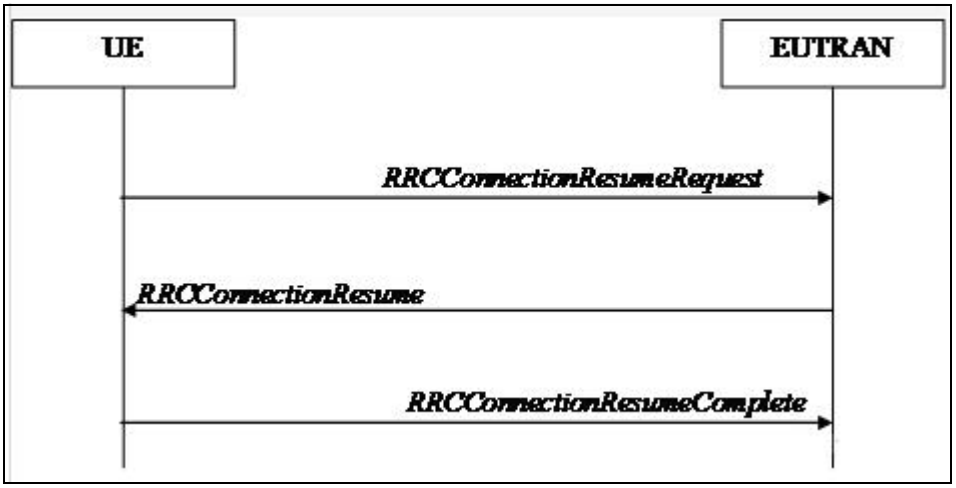
```
-- ASN1START
MasterInformationBlock ::=          SEQUENCE {
    dl-Bandwidth                        ENUMERATED {
                                            n6, n15, n25, n50, n75, n100},
    phich-Config                        PHICH-Config,
    systemFrameNumber                   BIT STRING (SIZE (8)),
    schedulingInfoSIB1-BR-r13           INTEGER (0..31),
    spare                               BIT STRING (SIZE (5))
}


-- ASN1STOP
```

层 3 协议流程

涉及 NB-IoT 终端的协议流程大体与 LTE 的终端协议流程类似，不过也有几点更新以及需要关注的方面。

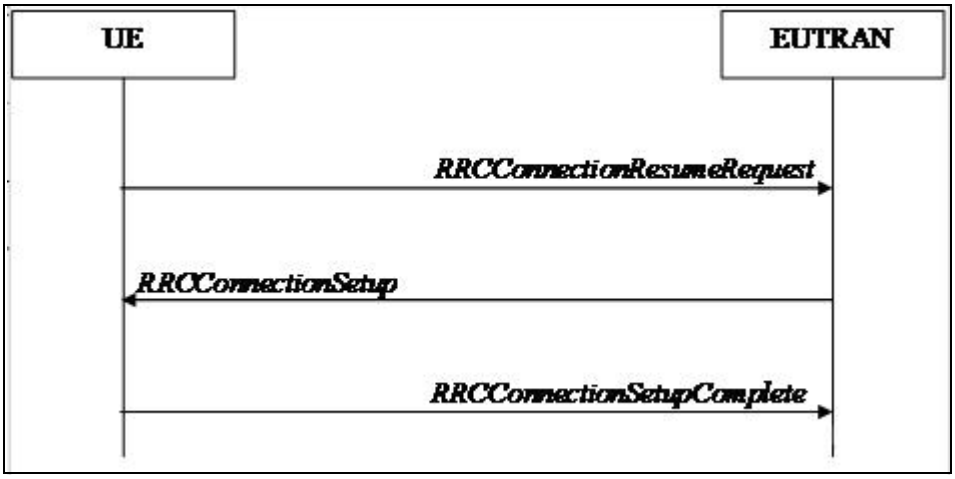
目前暂时不确定未来 NB-IoT 终端的形态，按照协议的设计，大致分为纯 NB-IoT 终端，以及和 LTE 公网接入混合类型终端，而纯 NB-IoT 终端从技术标准又分为两种，一种是通过 NAS 层协议栈传送小数据，不建立 DRB。另外一种如同传统的 E-UTRAN 协议栈，通过建立 DRB 传输数据。对于后者，在 RRC 的专用信令承载 SRB1 建立之时，SRB1 bis 同时被隐式的建立起来，但是需要等到安全指令模式之后才被真正使用。这里通过不同逻辑信道标识实现，SRB1 采用标识 1，SRB1 bis 采用标识 3。

相比 LTE 接入网信令流程，NB-IoT 多出了一个 RRC connection resume（RRC 连接恢复流程），而该流程不适用于 NAS 层控制面协议栈传送小数据的 CIoT 终端（挂起针对 RRC 层已建立至少 1 个 DRB）。



恢复是针对“挂起”流程而言的，为了使得 NB-IoT 终端更加省电，协议设计了“挂起-恢复”流程（当然该流程也可以适用大网），网络侧通过 *RRCConnectionRelease* 消息中的 *rrc-Suspend* 字段告诉 UE，RRC 连接被挂起，UE 存储接入层协议栈上下文和 *resumeIdentity（恢复 ID 身份）*，同时从连接态转变为 RRC_IDLE（空闲态），挂起针对 RRC 层已建立的至少 1 个 DRB，这也意味着对于 NAS 层协议栈传送小数据的 NB-IoT 终端，“挂起-恢复”流程是不适用的。恢复流程会重新激活安全模式和重新建立信令和数据承载，相比 *RRCConnectionRequest*,不需要有后续安全模式控制流程了。这样可以使得终端快速“恢复”与网络侧的连接。另外，相比 R13 之前的协议版本中 *RRCConnectionRequest* 的触发原因，*RRCConnectionResumeRequest* 多出一条 mo-VoiceCall（R13 中两者是中所含的触发原因是保持一致的）。如果触发原因是多媒体电话视频业务请求，并且驻留小区 SIB2 消息中包含 *voiceServiceCauseIndication*,那么 RRC 接入/恢复的触发原因就可以设置为 mo-VoiceCall，值得注意的是现网 VoLTE 主叫触发原因是 mo-Data。从这里看出，窄带物联网也不仅仅是传输数据，还可以传送语音。

对于终端的“恢复”请求，网络侧可能会恢复之前“悬挂”起的 RRC 连接，或者拒绝恢复请求，或者建立一个新的 RRC 连接。



当 UE 发出 *RRCConnectionResumeRequest*,而网络侧的响应消息为 *RRCConnecionSetup*,此时意味着网络侧建立一个新的 RRC 连接，那么 UE 需要将之前存贮的 AS 上下文以及 *resumeIdentity* 丢弃，并且通知高层 UE 连接恢复被“回退”成新的 RRC 连接了。如同 RRC 连接请求一样，RRC 连接恢复请求也同样受 T300 控制，T300 超时后底层清空，RRC 连接流程终止，后续行为由终端决定。

接入层对于终端的挂起一般是由处于 EMM-CONNECTED 模式下的网络侧高层（NAS 层）触发的，而恢复 NAS 信令连接则对应的由 UE 触发，这与接入层的“挂起-恢复”流程是对应的，可以看到接入层的“挂起”是由 NAS 层的“挂起”触发的，而 NAS 层的“恢复”则是由接入层的“恢复”触发的。这里要提到 CIoT 的两种数据传输模式，一种是传统的由 NAS 用户面承载数据（user plane CIoT EPS optimization），另一种是由 NAS 控制面承载数据（control plane CIoT EPS optimization）。以上的“挂起-恢复”流程只和 NAS 用户面承载数据模式相关，并不适用 NAS 控制面承载数据。NAS 控制面模式只能通过 NAS 信令连接释放的方式进行资源释放和优化。UE 通过在 TAU REQUEST 中设置“signalling active"标签来指明释放通过 NAS 控制面信令进行数据传输。

对于 NB-IoT 终端来讲，control plane CIoT EPS optimization（简称 CP）模式是必选项，而 user plane CIoT EPS optimization（简称 UP 模式）是可选项，因此在 *RRCConnectionSetupComplete-NB* 消息体中只含 UP 模式的可选项。

***RRCConnectionSetupComplete-NB* message**

```
-- ASN1START

RRCConnectionSetupComplete-NB ::=   SEQUENCE {
    rrc-TransactionIdentifier              RRC-TransactionIdentifier,
    criticalExtensions                     CHOICE{
            rrcConnectionSetupComplete-r13      RRCConnectionSetupComplete-NB-r13-IEs,
            criticalExtensionsFuture            SEQUENCE {}
    }
}

RRCConnectionSetupComplete-NB-r13-IEs ::= SEQUENCE {
    selectedPLMN-Identity-r13              INTEGER (1..maxPLMN-r11),
    s-TMSI-r13                             S-TMSI                          OPTIONAL,
    registeredMME-r13                      RegisteredMME                   OPTIONAL,
    dedicatedInfoNAS-r13                   DedicatedInfoNAS,
    attachWithoutPDN-Connectivity-r13      ENUMERATED {true}               OPTIONAL,
    up-CIoT-EPS-Optimisation-r13           ENUMERATED {true}               OPTIONAL,
    lateNonCriticalExtension               OCTET STRING                    OPTIONAL,
    nonCriticalExtension                   SEQUENCE {}                     OPTIONAL
}

-- ASN1STOP
```

而对那些非 NB-IoT 的终端，比如 eMTC 终端，或者 LTE 更新版本的终端，UP 模式和 CP 模式都是可选项，RRCConnectionSetupComplete 消息体里根据高层指示，选填这两个字段进行上报。这个取决于网络设备商如何实现了。

```
    nonCriticalExtension                RRCConnectionSetupComplete-v1320-IEs
    OPTIONAL
}

RRCConnectionSetupComplete-v1320-IEs ::= SEQUENCE {
    ce-ModeB-r13                        ENUMERATED {supported}          OPTIONAL,
    s-TMSI-r13                              S-TMSI                          OPTIONAL,
    attachWithoutPDN-Connectivity-r13       ENUMERATED {true}               OPTIONAL,
    up-CIoT-EPS-Optimisation-r13            ENUMERATED {true}               OPTIONAL,
    cp-CIoT-EPS-Optimisation-r13            ENUMERATED {true}               OPTIONAL,
    nonCriticalExtension                RRCConnectionSetupComplete-v1330-IEs                OPTIONAL
}

RRCConnectionSetupComplete-v1330-IEs ::= SEQUENCE {
    ue-CE-NeedULGaps-r13                    ENUMERATED {true}               OPTIONAL,
    nonCriticalExtension                    SEQUENCE {}                     OPTIONAL
}

RegisteredMME ::=                   SEQUENCE {
    plmn-Identity                           PLMN-Identity                   OPTIONAL,
    mmegi                                   BIT STRING (SIZE (16)),
    mmec                                    MMEC
}
```

再来最后聊一个小问题，对于 UP 模式下的物联网终端的恢复请求 *RRCConnectionResumeRequest*，网络侧什么时候会直接响应 *RRCConnectionSetup*,一般理解是网络侧找不到用户上下文时会指示终端建立新的 RRC 连接，但一般什么时候网络侧会找不到用户上下文呢，根据前面分析提到的一个概念，恢复是对应挂起的，而挂起源自于核心网 MME 的触发，因此一般 MME 内部基站间切换都可以进行上下文的传递，而当跨 MME 切换的时候，由可能由于网络侧找不到用户上下文而直接响应用户建立新的 RRC 连接。这只是我们初步用力拍脑袋的一个理论分析，更多的实例有待于我们去发现。