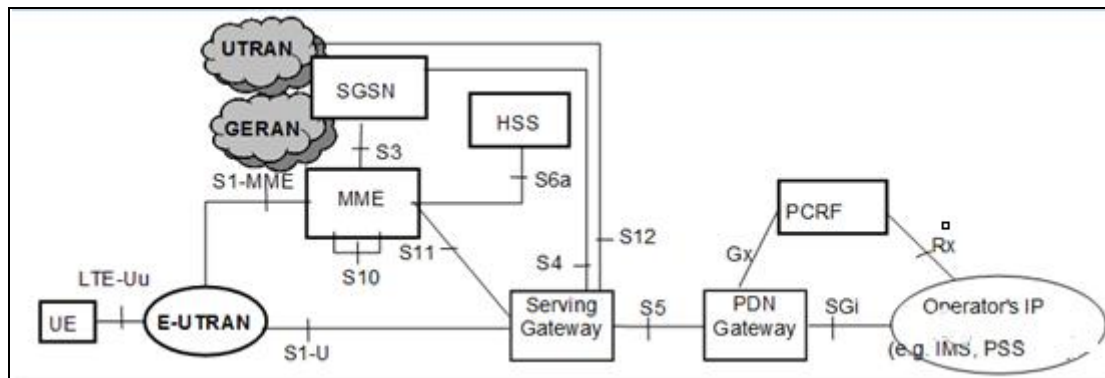


核心网关键技术流程



3GPP 23.401 中对于蜂窝物联网 (Cellular Internet of Things, CIoT) 是短短一句话定义的，蜂窝网络支持低复杂度和低吞吐率的物联网设备。蜂窝物联网同时支持 IP 业务和非 IP 业务 (非 IP 的业务指的是站在 EPS 的角度来看的一些非结构化数据，尽管还是会被分配 APN) 。

对于物联网，小包数据业务传输将成为应用的典型特征。因此，对于核心网而言，基于物联网的这种小数据，短时延传输模式进行了一些协议流程方面的优化。这种优化方式包含了两种模式，一种是基于用户面传输用户数据，而另一种是将用户数据封装在了 NAS 层消息里的控制面传输方式，这种方式减少很多控制面的信令开销。PDN 连接可以采取控制面 CIoT 核心网承载优化方式处理，或者也可以采取用户面 CIoT 核心网承载优化方式处理。相比传统 PDN 连接需要使用 S1-U 接口进行传输，这里 S11-U 也可以被用来传输小包数据。

CIoT 的数据可以包括物联网应用的状态信息以及测量数据。

5G 当中支持物联网数据通信的 MME 可能有这么几种支持数据传输的模式，

MME 支持控制面 CIoT 数据优化传输模式，

MME 支持用户面 CIoT 数据优化传输模式，

支持传统的 S1-U 数据传输模式。

同时也包括了一些特殊的核心网功能，比如

是否支持无需联合附着的 SMS 消息传输，

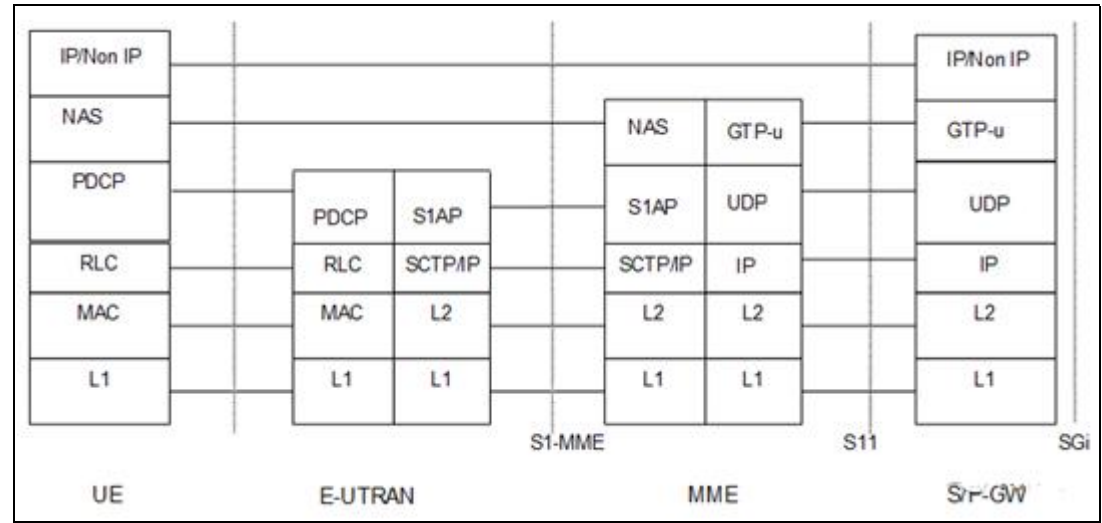
是否支持没有 PDN 连接的附着，

是否支持控制面 CIoT 数据优化传输模式的包头压缩。

对于支持 NB-IoT 的终端，网络侧应该提供控制面 CIoT 数据优化传输模式的功能，对于 S1-U 传统用户面数据传输模式并不属于 CIoT 的数据优化传输模式范畴，但是支持用户面 CIoT 数据优化传输模式功能的 UE 也需要能够支持 S1-U 模式。

UE 会通过 ATTACH/TAU 请求中附带消息体 Preferred and Supported Network Behaviour 与网络能力进行协商。值得一提的是，这种核心网对于数据传输的优化机制并不仅仅限于低复杂度，低吞吐率的物联网应用。

用户面 CIoT 核心网优化功能可以无需像传统 LTE 大网数据业务请求建立一样，通过 NAS 层消息 Service Request 触发一系列的接入网流程作为数据业务传输的承载。但是这里有个前提，就是 UE 与网络之间的 RRC 连接处于挂起状态，这也意味着 UE 与网络侧的接入网承载和接入网安全上下文已经协商分配好了。通过挂起流程，在 UE 转为 ECM-IDLE 过程中，UE 与 eNodeB 分别存储了接入层相关信息以及承载上下文，同时 MME 存储了与 S1AP 和核心网承载相关的上下文，可以说“挂起”流程是一种“睡眠”机制，并不把 UE 连接建立相关信息删除。

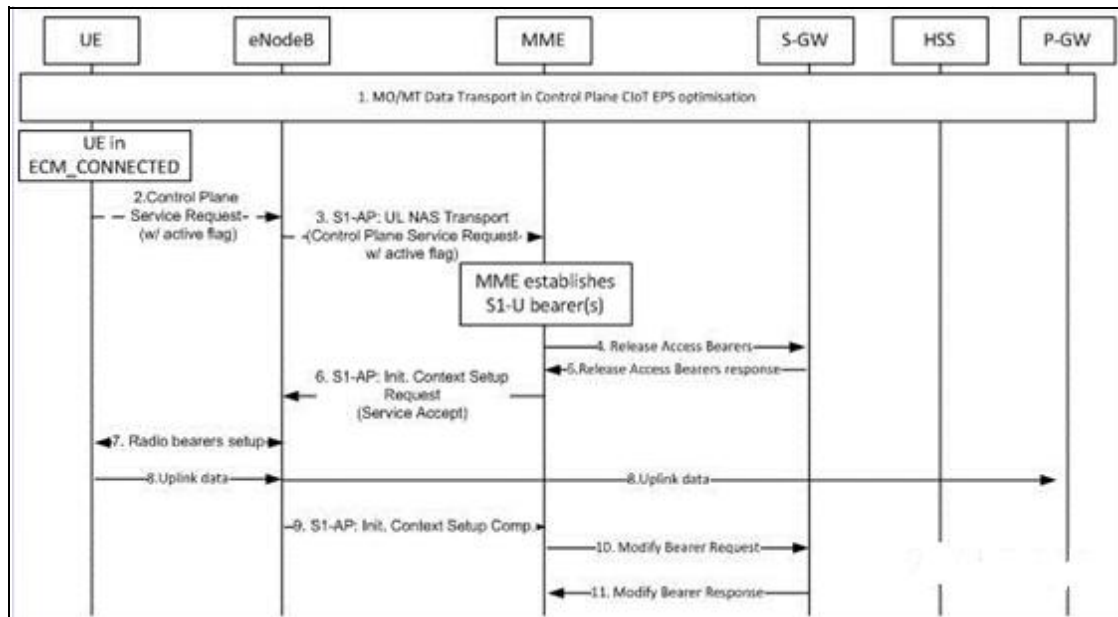


控制面优化数据传输模式下的用户面协议栈

从核心网控制面优化数据传输模式下的用户面协议栈结构中可以看出与典型 LTE 系统网络中用户面传输数据在协议架构中的不同。UE 与 MME 之间通过 NAS 层信令之间传输数据，而 LTE 系统中 S1 接口的 GTP-u 传输隧道协议后移到 S11 接口中作为用户面数据传输协议。

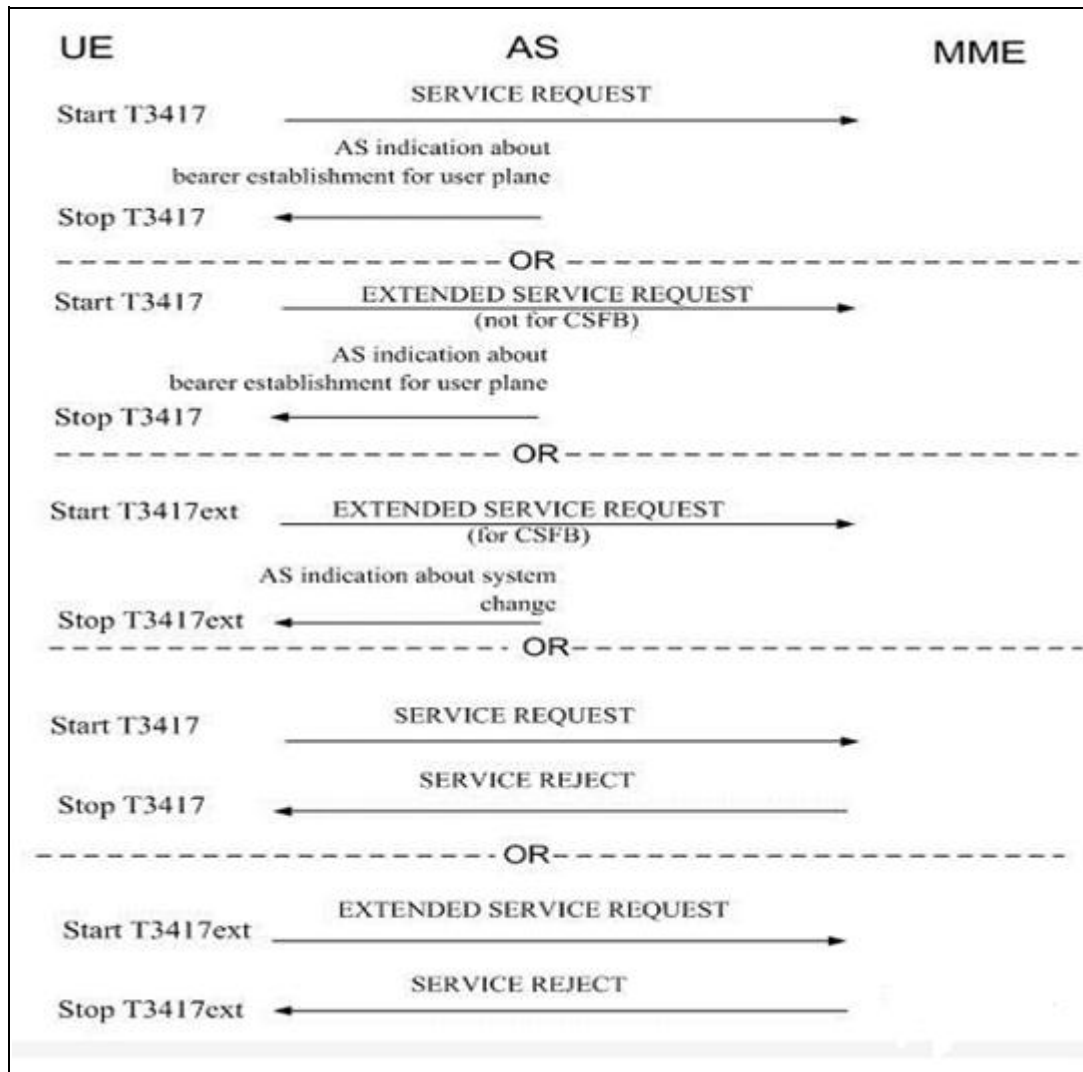
在控制面数据传输模式下，UE 上行数据包和相应的 EPS Bearer ID (EBI) 被封装在 NAS DATA PDU 中，通过 S1-AP 初始 UE 消息传递，MME 在收到了初始消息后可以与 SGW/PGW 协商传递上行数据，同时并行的触发核心网移动性以及会话管理流程，比如鉴权和安全涉及流程。相对比而言，如果此时有来自于 SGW/PGW 的下行数据，则需要先在 MME 缓存，等待 EMM 和 ESM 流程完毕之后进行传递。对于接入侧通过 NB-IoT 技术建立连接，并且触发原因是 MO Exception Data，MME 需要将此触发原因告知 SGW。这里其实表达了一层逻辑，上行 NAS PDU 数据和上行 NAS 信令流程可以在 MME 进行分离，数据通过 S11 接口传出去，NAS 鉴权安全流程可以并发进行，而下行的 NAS PDU 数据则需要等待 NAS 鉴权安全流程结束之后才能继续下发 eNodeB。

在 UE 与 MME 采取控制面优化数据传输模式下，即 UE 处于连接态下，如果需要通过建立用户面传输数据，可以采取传统 S1-U 模式进行数据传输或者采取用户面优化数据传输模式。如果 MME 决定采取 S1-U 模式进行数据传输，UE 就不需要重新发起 Service Request，并通过后续的初始上下文请求告知 eNodeB 相关承载信息，包括安全上下文，信令连接 ID，EPS 承载 QoS 参数，S1 连接标识等。如果采取用户面优化数据传输模式，UE 需要发起控制面 Service Request 申请 S1-U 承载。不管控制面优化数据传输模式，用户面优化数据传输模式，还是 S1-U 数据传输模式，相应的 PDN 连接需要建立，而与之相应的 EPS bearer 也需要有 MME 进行分配建立。

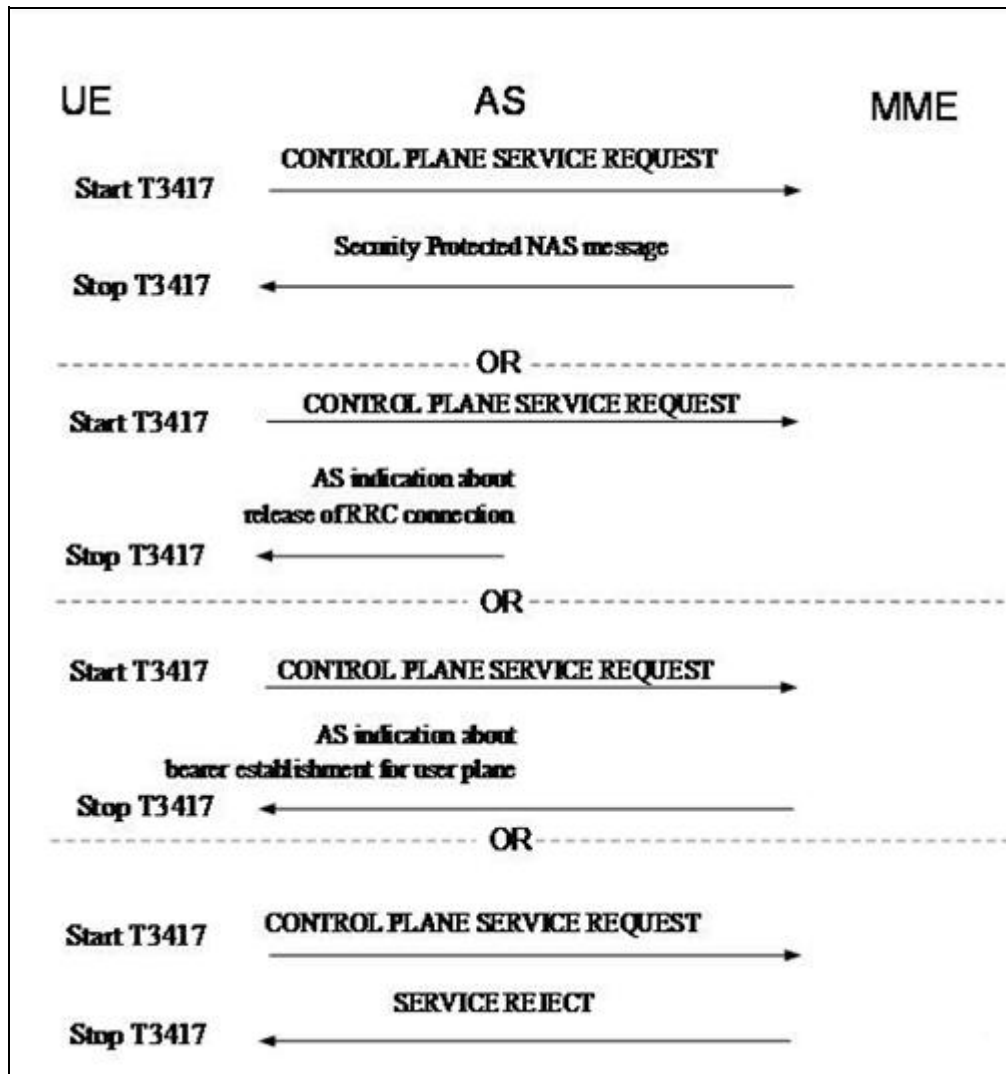


处于 CP 数据传输模式下的连接态 UE 转为 UP 模式或者 S1-U 模式进行数据传输

NAS 信令流程



像 Service Request 这样的 NAS 层服务请求信令在目前的 LTE 网络问题日常分析中很常见，它主要在于处于空闲态终端为了主/被叫 UE 申请接入侧和核心网侧网络资源，由它触发了一系列的接入网信令流程建立，这样的数据传输模式是 S1-U 数据传输模式。什么时候使用 SR，什么时候使用 ESR（Extended Service Request，这里是针对非 CSFB 的数据业务）这个取决一个 UE 设备侧 NAS 控制消息中所带的标识 NAS signalling low priority，如果该标识置为 1，且 MME 通过最近一次的 Attach Accept/TAU Accept 消息告知 UE 网络侧支持 ESR，那么流程由 ESR 发起，否则由 SR 发起。该标识其实告知 MME 在核心网信令拥塞时优先对哪些信令进行处理响应。



对于采取控制面或者用户面的 CIoT 数据传输模式，则是通过 CONTROL PLANE SERVICE REQUEST 进行，区别在于对于 CP 模式，CPSR 中包括了 UE 中需要通过 NAS 信令封装传送的数据，以 ESM DATA TRANSPORT 消息的形式封装在 ESM message container IE 中传送。而对于之前提及到的在 CP 模式连接态下转为 UP 模式数据传输的过程或者 UE 在 IDLE 态有数据需要传送，可以通过 CPSR 发起建立用户面数据传输优化模式，与 CP 模式区别的是，NAS 消息不携带任何与数据相关的消息体，既不包含 ESM message container IE 也不包含 NAS message container IE，同时将 active flag 置为 1。如果 MME 接受该流程，在完成一些 EMM（核心网移动性管理）公共流程后（比如鉴权，安全模式等等），将 EPS bear 上下文相关信息关联，向 UE 发送 SERVICE ACCEPT 消息，表示该流程

成功完成。可以概括的理解 SERVICE ACCEPT 是对通过 NAS 层控制面传输数据的确认，如果需要为 UE 的上下行数据再建立用户面承载，则不需要通过任何 NAS 信令再予以确认。在 MME 发送 SERVICE ACCEPT 之前如果有下行数据需要通过控制面进行发送，则先保证下行数据传递出去。

从这里 NAS 信令流程可以归纳几点核心网对于物联网技术的优化设计思路

- 1、数据优先，如果通过控制面承载，先于确认信息将待发数据发送出去；**
- 2、新增 SERVICE ACCEPT 是为了确认 CPSR 请求的，对于通过用户面承载发送数据，则无需 SERVICE ACCEPT 再确认，应为两个为不同的面（控制面，用户面），可以没有严格的时间顺序；**
- 3、相比 LTE 大网的设计思路，一切都由网络控制调度，为了保证数据传输的时延，物联网的终端在一定程度上参与发起数据传输模式选择，这对 UE 设计更多了一些灵活性。而相比 LTE 网络单一的交互流程则更加丰富，为了物联网低时延，大容量的设计目标更加契合，但是站在解读协议或者分析网络实际问题的角度来看，可能会觉得更加复杂多变。**

为了应对大量物联网连接对于核心网络的负荷带来的冲击，核心网对设备的上下行数据包还进行了流控机制。这里包含两种两种流控，一种是服务 PLMN 网络流控，另一种是 APN 流控，这二者的区别在于前一种流控机制主要为了由于 NAS 数据 PDU 引起的对于 MME 以及接入层相关信令冲击，而后一种机制在于运营商策略为了规定用户一天之内最多可以发送多少消息或者消耗多少数据流量，一般认为后者所规定的消息限额要小于前者，而且二者都可以在逻辑网元 PGW 或者 SCEF 上具体实现，不过 APN 流控机制一般会先于服务 PLMN 流控机制应用触发在用户数据上。

微信扫码以下二维码，免费加入【5G 俱乐部】，还赠送整套：5G 前沿、NB-IoT、4G+ (VoLTE) 资料。

