1 基础知识

1.1 E-RAB 在 LTE 系统中的位置和组成

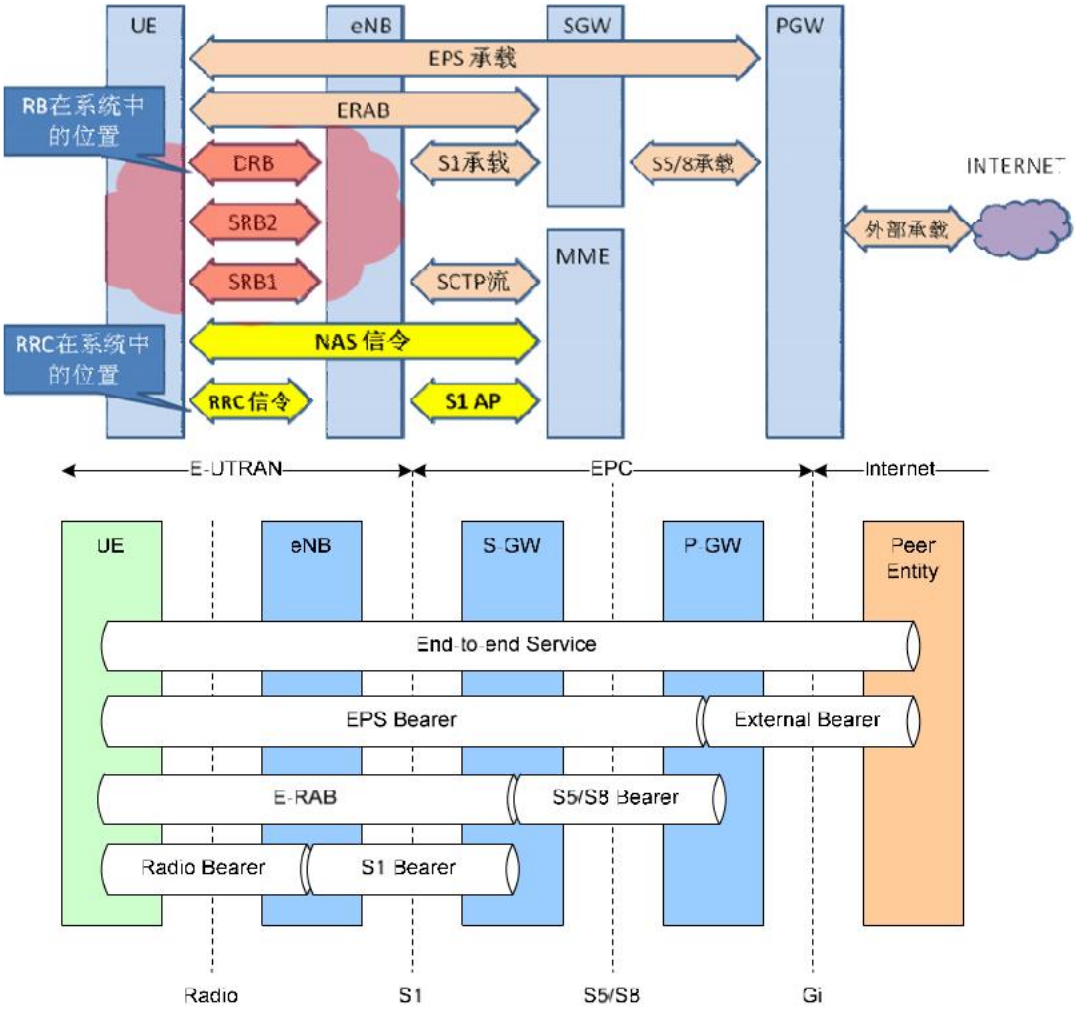


图1 TD-LTE EPS的承载管理架构

延续3GPP的一贯定义，RAB(Radio Access Bearer)为用户提供从核心网到UE的数据连接能力，但是在LTE中RAB更名为E-RAB。如图1所示，LTE的E-RAB从SGW开始到UE结束，由S1-U承载和DRB(Data Radio Bearer)串联而成，进入LTE系统的业务数据主要通过E-RAB进行传输，因此LTE对于业务的管理主要是在E-RAB层次上进行的。为了管理E-RAB，在LTE系统内需要相应的信令连接传输网元间的控制信令来完成，LTE的信令主要包括三个部分，就是NAS信令、RRC信令和S1 AP信令以及用来传输信令的各种实际的承载。另外ERAB的管理主要体现在S1接口的信令中，包括ERAB的建立、修改和释放，对于RB的管理也就是空口连接的管理可以看做是ERAB管理过程的子过程。

其中DRB是数据无线承载的简称，在UE和ENodeB之间传输ERAB数据包，在DRB和ERAB之间有点到点的映射，是属于空口（Uu接口）的内容，同时在Uu口还包括SRB(Signal Radio Bearer,信令无线承载）。作为eNodeB和UE之间数据传输的通道，RB是通过RRC信令来进行管理的，eNodeB和UE通过RRC信令的交互，完成各种RB的建立、重配和释放等功能。

S1-U承载在ENodeB和SGW之间传输数据，通过S1AP信令来进行管理的，包括S1承载的建立、修改和释放。S1-AP有专门建立、修改和释放信令完成这几个功能。

1.2 RB 的功能

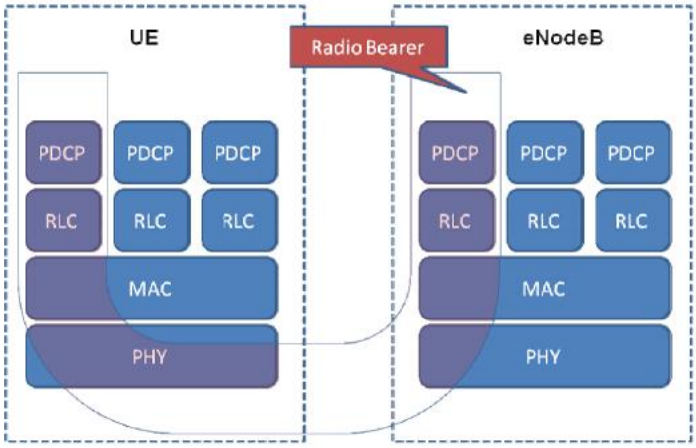
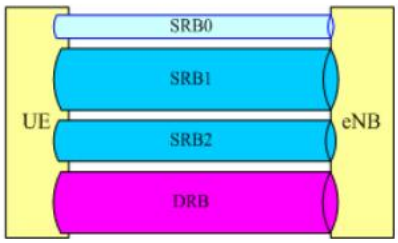


图 2 RB 的构造

RB 是 eNodeB 为 UE 分配的一系列协议实体及配置的总称，包括 PDCP 协议实体、RLC 协议实体以及 MAC 和 PHY 分配的一系列资源等。RB 是 Uu 接口连接 eNodeB 和 UE 的通道，在协议架构由下到上包括 PHY、MAC、RLC 和 PDCP 协议，任何在 Uu 接口上传输的数据都要经过 RB。

RB 包括 SRB 和 DRB，SRB 是系统的信令消息实际传输的通道，DRB 是用户数据实际传输的通道。



SRB0	缺省承载，UE在RRC_IDLE时，该承载已经存在	传输CCCH信道上的消息（RRC连接建立,重建相关消息）
SRB1	RRC连接建立时，建立该承载	传输DCCH信道上的消息大部分的RRC消息
SRB2	一般在安全性激活后，建立该承载，优先级较低，且最后建立	只传输NAS消息
DRB	根据用户业务需要建立	传输用户面数据

图3 RB的分类

1.2.1 DRB

“数据无线承载”DRB是用于传输用户数据的无线承载，DRB只有一种，协议规定每个UE可以最多有8个DRB用来传输不同的业务。

1.2.2 SRB

“信令无线承载”（SRB）定义为仅仅用于RRC和NAS消息传输的无线承载（RB）。更具体地讲，定义如下三种SRB：

- SRB0 用于 RRC 消息，使用 CCCH 逻辑信道；message3、4 均使用 SRB0。
- SRB1 用于 RRC 消息（可能包括含有 NAS 消息），SRB1 先于 SRB2 的建立，所有使用 DCCH 逻辑信道；message5 使用 SRB1。
- SRB2 用于 NAS 消息，使用 DCCH 逻辑信道。SRB2 要后于 SRB1 建立，并且总是由 E-UTRAN 在安全激活后进行配置。

下行捎带 NAS 消息仅仅用于一个依附的流程（即在连接成功/失败的时候使用）：建立/修改/释放承载。上行捎带 NAS 消息仅仅用于在建立连接的过程中传输初始的 NAS 消息。

一旦安全被激活，在SRB1和SRB2上所有的RRC消息，包括那些包含NAS或非3GPP消息，都由PDCP进行完整型保护和加密。NAS各自独立采用完整性保护和加密生成NAS消息。

2 RB 的管理

RB的管理主要是在RRC连接的信令传输上完成的，Uu口上的RB包括SRB0、SRB1、SRB2和DRB。接下来介绍RRC连接相关内容。

2.1 RRC 连接管理

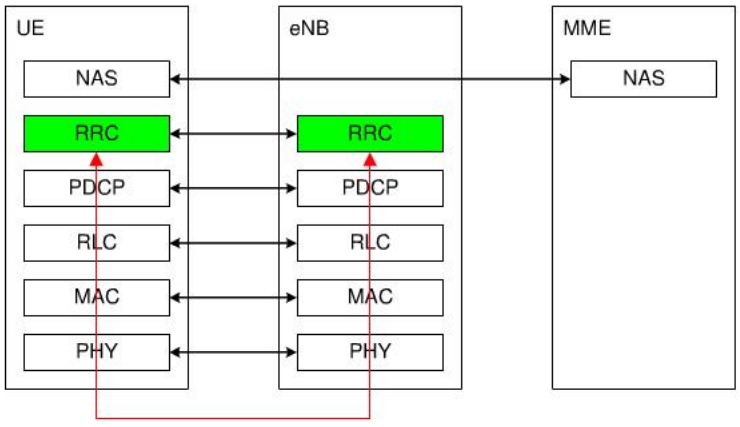


图 4 RRC 协议架构

如上所述，RRC是管理RB的协议实体，通过RRC信令的交互完成RB的建立、修改以及释放等功能。通俗的讲RRC连接指的是UE和eNodeB之间建立的SRB1，因为标准规定SRB0是不需要建立的，UE在RRC_IDLE状态就可以获得SRB0的配置和资源，如果需要可以直接使用。系统中业务发起的过程是通过SRB0上传输信令建立SRB1，SRB1建立之后UE就进入RRC_Connected状态；进而通过SRB1传输信令建立SRB2用来传输NAS信令；利用SRB1传输信令建立DRB来传输用户数据，在业务进行过程中通过SRB1进行管理；当业务结束后，SRB1上传输的信令可以将所有的DRB、SRB释放，使得UE进入到RRC_IDLE状态，在需要时UE唯一可以使用的资源就是SRB0，而且需要在完成随机接入之后进行。

RRC 连接建立包括SRB1的建立。E-UTRAN在完成S1连接建立过程前，即在接收EPC发出的UE上下文信息之前，完成RRC连接的建立。因此，在RRC连接的初始阶段，SRB1的建立不需要同核心网进行信息的交互，AS安全将不会被激活。

当接收到EPC发出的UE上下文后，E-UTRAN使用初始安全激活过程来激活安全（包括加密和完整性保护）。激活安全的RRC消息（命令与成功响应）会得到完整性保护，而加密只有当此过程完成后才开始。也就是说，激活安全消息的响应没有被加密，只有随后的消息有完整性保护和加密，比如建立SRB2和DRB的消息。

初始安全激活过程启动后，E-UTRAN 发起 SRB2 和 DRB 的建立，也就是在接收到 UE 发出的初始安全激活确认前 E-UTRAN 可以发起 SRB2 和 DRB 的建立。在任何情况下，E-UTRAN 会对用于建立 SRB2 和 DRB 的 RRC 连接重配消息进行加密和完整性保护。如果初始安全激活和/或无线承载建立失败，E-UTRAN 应释放 RRC 连接。

2.1.1 RRC 连接建立过程

与RRC连接建立相关的信令包括RRCConnectionSetupRequest，RRCConnectionSetup，RRCConnectionReject，RRCConnectionSetupComplete。

其中RRCConnectionSetup消息用于建立SRB1，无线承载是SRB0,RCL-SAP是TM，逻辑信道是CCCH,是从E-UTRAN到UE的消息

***RRCConnectionSetup* 消息**

```
-- ASN1START

RRCConnectionSetup ::=              SEQUENCE {
    rrc-TransactionIdentifier       RRC-TransactionIdentifier,
    criticalExtensions              CHOICE {
```

```
        c1                                          CHOICE {
            rrcConnectionSetup-r8                   RRCConnectionSetup-r8-IEs,
            spare7 NULL,
            spare6 NULL, spare5 NULL, spare4 NULL,
            spare3 NULL, spare2 NULL, spare1 NULL
        },
        criticalExtensionsFuture                    SEQUENCE {}
    }
}


RRCConnectionSetup-r8-IEs ::=           SEQUENCE {
    radioResourceConfigDedicated        RadioResourceConfigDedicated,
    nonCriticalExtension                SEQUENCE {}                         OPTIONAL    -- Need
OP
}


-- ASN1STOP
```

2.1.2 RRC 连接重配置过程

该过程旨在修改RRC连接，包括增加、删除、修改各种RB；进行切换，这是由于LTE没有单独定义Intra-LTE的切换信令，对于UE的切换信令是通过RRC重配消息完成的；这条消息还可以的修改和释放测量的配置。在SRB2建立之前，NAS消息还可以通过这个过程捎带给UE。

发起RRC连接重配的前提必须是UE已经建立SRB1进入RRC连接状态，并且已经建立了AS安全上下文。

该过程包括RRCConnectionReconfigurationComplete和RRCConnectionReconfiguration消息，信令无线承载是SRB1，RLC-SAP是AM，逻辑信道是DCCH。RRCConnectionReconfiguration 消息是命令消息，用来修改RRC 连接。其可以传送测量配置、移动控制、包含任何相关专用NAS信息的无线资源配置（包含RBs、MAC主要配置以及物理信道配置）、安全配置。

RRCConnectionReconfiguration 消息

```
-- ASN1START

RRCConnectionReconfiguration ::=        SEQUENCE {
        rrc-TransactionIdentifier                RRC-TransactionIdentifier,
        criticalExtensions                       CHOICE {
                c1                                       CHOICE{
                        rrcConnectionReconfiguration-r8          RRCConnectionReconfiguration-r8-IEs,
                        spare7 NULL,
                        spare6 NULL, spare5 NULL, spare4 NULL,
                        spare3 NULL, spare2 NULL, spare1 NULL
                },
                criticalExtensionsFuture                 SEQUENCE {}
        }
}

RRCConnectionReconfiguration-r8-IEs ::= SEQUENCE {
        measConfig                                       MeasConfig                                      OPTIONAL,       --
Need ON
        mobilityControlInfo                      MobilityControlInfo                     OPTIONAL,       -- Cond HO
        dedicatedInfoNASList                     SEQUENCE (SIZE(1..maxDRB)) OF
                                                         DedicatedInfoNAS                OPTIONAL,       -- Cond
nonHO
        radioResourceConfigDedicated             RadioResourceConfigDedicated    OPTIONAL, -- Cond HO-toEUTRA
        securityConfigHO                         SecurityConfigHO                        OPTIONAL,       -- Cond HO
        nonCriticalExtension                     SEQUENCE {}                             OPTIONAL        -- Need OP
}

SecurityConfigHO ::=                     SEQUENCE {
```

```
    handoverType                        CHOICE {
        intraLTE                            SEQUENCE {
            securityAlgorithmConfig             SecurityAlgorithmConfig     OPTIONAL,    -- Need
OP
            keyChangeIndicator                  BOOLEAN,
            nextHopChainingCount            NextHopChainingCount
        },
        interRAT                            SEQUENCE {
            securityAlgorithmConfig             SecurityAlgorithmConfig,
            nas-SecurityParamToEUTRA        OCTET STRING (SIZE(6))
        }
    },
    ...
}

-- ASN1STOP
```

2.1.3 RRC 连接重建立过程

该过程旨在重建 RRC 连接，包括 SRB1 操作的恢复，以及安全的重新激活。

处于 RRC_CONNECTED 状态的 UE，安全已被激活，可发起该过程继续 RRC 连接。仅当相关小区是具有 UE 上下文的小区时，连接重建才会成功。假使 E-UTRAN 认可重建，SRB1 的操作会恢复，而其它 RB 将继续保持挂起。如果 AS 安全没有被激活，UE 不会发起该过程，而直接转到 RRC_IDLE 状态。

E-UTRAN 在如下情况使用此过程：

- 重配 SRB1，且仅为其恢复数据传输；
- 重新激活AS安全不改变算法。

RRCConnectionReestablishment 消息用于解决竞争和建立 SRBs。

信令无线承载： SRB0

RLC-SAP: TM

逻辑信道：CCCH

方向：从 E-UTRAN 到 UE

RRCConnectionReestablishment 消息

```
-- ASN1START
RRCConnectionReestablishment ::=        SEQUENCE {
        rrc-TransactionIdentifier                RRC-TransactionIdentifier,
        criticalExtensions                       CHOICE {
                c1                                       CHOICE{
                        rrcConnectionReestablishment-r8          RRCConnectionReestablishment-r8-IEs,
                        spare7 NULL,
                        spare6 NULL, spare5 NULL, spare4         NULL,
                        spare3 NULL, spare2 NULL, spare1         NULL
                },
                criticalExtensionsFuture                 SEQUENCE {}
        }
}

RRCConnectionReestablishment-r8-IEs ::= SEQUENCE {
        radioResourceConfigDedicated            RadioResourceConfigDedicated,
        nextHopChainingCount                     NextHopChainingCount,
        nonCriticalExtension                     SEQUENCE {}                                    OPTIONAL        -- Need
OP
}

-- ASN1STOP
```

其中radioResourceConfigDedicated来源于ENodeb已经存储的UE上下文。

2.1.4 RRC 连接释放过程

该过程旨在释放该RRC连接，包括建立的无线承载以及所有无线资源的释放。这个过程如果由EUTRAN发起，需要通过RRC连接释放命令通知UE释放RRC连接。

该过程不涉及专用无线资源的释放。