深入浅出4G网络
——LTE/EPC

张明和 著

- 本书源于华为Hi社区博客频道超级热帖“纵横4海：深入浅出EPC原理”
- 本书作者博客的总点击量突破200 000次
- 《大话无线通信》作者丁奇鼎力推荐，盛赞本书是很好的通俗类技术图书

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

深入浅出4G网络

——LTE/EPC

张明和◎著

人民邮电出版社
北京

图书在版编目（CIP）数据

深入浅出4G网络 : LTE/EPC / 张明和著. -- 北京 : 人民邮电出版社, 2016.1
ISBN 978-7-115-40959-1

Ⅰ. ①深… Ⅱ. ①张… Ⅲ. ①无线电通信－移动网－研究 Ⅳ. ①TN929.5

中国版本图书馆CIP数据核字(2015)第262550号

◆ 著　　张明和
责任编辑　刘　洋
责任印制　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷
◆ 开本：787×1092　1/16
印张：17.25　　2016 年 1 月第 1 版
字数：334 千字　　2016 年 1 月北京第 1 次印刷

定价：59.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第 0021 号

内容提要

ABSTRACT

本书是一本介绍4G网络内容的图书。本书首先介绍了4G核心网（EPC）的概念、接口和演进特点，然后从用户状态和基本的附着流程介绍EPC网络的流程和业务——包括日常4G网络运维工作中常见的切换、服务请求和跟踪区更新等流程，并对鉴权和网络拓扑选择等难点进行深入讲解；紧接着，本书探讨了CDMA网络的历史、特点、CDMA与3GPP移动数据核心网的区别，以及CDMA如何演进到3GPP架构下的4G网络；然后，本书针对4G网络3个技术难点——CSFB语音方案、QoS、VoLTE和SRVCC进行了深入分析和讲解。在本书的最后一章，对全球移动数据网络国际漫游架构进行了分析。

本书来源于作者在公司内部社区的博客连载。本书在讲解流程知识的过程中，尝试探究技术方案产生的背后原因，使读者不但“知其然”，更“知其所以然”。作者相信“一图胜千言”，因此本书采用大量图表来说明复杂的技术原理。另外，本书注重理论结合实践，图中采用大量消息讲解流程原理，为读者呈现关键信元如何在消息中封装，具有很强的实际网络运维工作指导意义。

本书可供无线通信技术初学者用来“从无到有”建立移动数据核心网的完整知识框架，也可作为4G相关网络设计、优化、维护人员进行问题处理的参考书，另外还可作为移动通信行业管理人员了解4G网络原理和业务的读物。

博友赞誉

PRAISE

语言不晦涩，易懂。真正的专家，佩服！大侠热心分享，对我们的帮助太大了，非常感谢！

——姚婷

作为一个核心网的同学，一直对于无线侧的原理都是一知半解的。看了大师的文章，受益很多。

——周二强

将复杂的事情解构出来并以通俗易懂的语言描述之，这就是大师的所谓庖丁解牛吧。

——陈春华

知其然，知其所以然，从无线通信两个受限的资源：空口、终端电量出发开始讲，让大家更容易理解为什么这么设计。

——唐新亭

大师就是能将复杂的问题简单讲出来，必须点赞。

“纵横 4 海”这个专题太好了，根本停不下来，一口气读下去。

——马力

从第 1 章学习到现在，获益匪浅，以前只是停留在 eNodeB 以下层面对 LTE 的典型流程的理解，现在终于对全流程有了一个了解，多谢！

——张丙龙

通过拜读张大师的著作使我对前一段时间处理的一个现网问题有了比较深入的理解，感谢张大师哈。

——罗玉才

张老师文章写得很清晰，平时模拟 CSFB 业务流程，由于自己不理解 4G 和 2G 的位置对应关系，以至于 TAI 配置出错导致业务流程失败。通过学习此文章，领悟了 CSFB 业务流程原理，结合文章中的消息跟踪内容，以后面对此类问题就有定位思路了。

——李波余

谢谢大侠，文章通俗易懂，连我这个门外汉，都学习了解到了一些 LTE 的相关业务流程，对我们的业务有很大的帮助，期待大侠出书。

——张鹏飞

这是我看过最好的介绍 EPS 的文章了。

——何飞鹏

世间的万事都是一个道理，最深刻的领悟，就是看破具体事物的表象，把内在的、通用的道理总结出来。比如技术是为了更好地分配资源，技术的复杂性是因为资源的稀缺性决定的，等等。系列文章中有很多深层次的理解，赞一个，感谢专家。

——刘伟

真正的、少有的专家，故事讲得好，道理讲得明。大格局，大智慧，致敬！

——冯立坤

前言

PREFACE

4G LTE 是目前通信行业的热点领域。在中国，3 家移动通信运营商都在快速建设 4G 网络。越来越多的终端用户在享受着 4G 高速网络带来的美好业务体验。

通信网络是一个极其复杂的系统。通信网络所承载的业务也过于抽象，理解起来并不容易。本书主要讲解 4G 网络结构和业务流程，并对无线的概念有所涉及。

本书内容覆盖 EPC 网络当前商用阶段的全部原理和业务，包括 4G 网络的基本结构、4G 网络附着、安全流程、承载建立、基于 DNS 的拓扑选择、移动性相关的切换流程、4G 和传统 2G、3G 网络的互操作、CDMA 网络和 eHRPD 网络、eHRPD 网络和 LTE 网络的互操作、CSFB 语音业务、4G 网络 QoS 机制、VoLTE 业务、国际漫游。本书以通俗的语言解构 4G 网络核心网，探究技术协议产生背后的驱动力，详细分析各个信令流程，并深入到信元级。

工程师通过学习本书可以具备解决复杂网络问题的能力。本书同样适合需要对 4G 网络具备概要性了解的管理人员，以及需要了解 4G 核心网和 4G 业务的无线工程师、网络优化工程师、IMS 工程师，还有维护 4G 承载网和传送网的数据通信工程师。

我必须感谢公司知识管理部谭新德、王楠斌和张希杰 3 位老师，感谢他们在本书写作和出版过程中给予的帮助；更要感谢部门周震、翁奇、易多亮、唐运虞、俞春辉等领导的认可和鼓励，是他们的鼓励使得我能够坚持写完本书；还有更多同事在本书写作过程中给予过帮助，无法一一列举，在此一并表示衷心的感谢。

感谢家人的理解和支持，使得我在工作之外有时间完成本书。

这本书是我根据自己学习理解的 4G 网络的知识，结合自己十余年在移动数据网络方面的工作经验所做的总结性阐述和思考，其中难免有偏颇和疏漏之处，欢迎大家批评指正。

特别声明：虽然作者供职于华为，但本书所述内容并不意味着是华为实现，不能作为理解华为设备机制的依据。

2015 年 11 月

张明和

目录

Contents

第 1 章 ■ 概述 1

1.1 关于 4G 的几个概念 1

1.2 长期演进，演进到哪里了 2

1.3 认识 EPC 网络的网元 5

1.4 移动宽带网络的本质 7

1.5 EPC 网络的接口 8

1.6 EPC 网络的协议 11

1.7 EPC 网络的业务 14

第 2 章 ■ EPC 网络基本流程 19

2.1 历史从未走远 19

2.2 为什么会有状态 21

2.3 需要澄清的概念 22

2.4 EPC 网络中有哪些状态 22

2.5 协议对附着流程的描述 25

2.6 关于 4G 网络的承载 31

2.7 分解附着过程 32

2.8 S1 接口信令连接的建立和获取用户标识 35

2.8.1 S1 接口信令连接的建立 35

2.8.2 获取用户身份标识 38

2.9 鉴权流程和安全流程 42

2.10 Diameter 选路 48

2.10.1 七号链路时代的 Gr 接口选路 49

2.10.2 IP 时代的 S6a 接口选路 49

2.11 位置更新流程 52

2.11.1 注册用户当前所在 MME 52

2.11.2 不只是响应的响应 54

2.12 承载的创建 56
2.12.1 先澄清几个概念 56
2.12.2 默认承载创建流程 57
2.12.3 承载建立过程消息分解 59
2.13 DNS 和网络拓扑选择 65
2.13.1 DNS 域名 65
2.13.2 DNS 解析类型 67
2.13.3 当域名遇到解析类型 69
2.13.4 本地优先的实现 70
2.13.5 拓扑选择的实现 71

第 3 章 ■ 移动状态下的流程 73
3.1 第一件事，统一语言 73
3.2 位置标识 78
3.3 TAU 流程 83
3.4 Service Request 流程 89
3.5 Handover 流程 94
3.5.1 Handover 流程概述 94
3.5.2 基于 X2 接口的切换 97
3.5.3 基于 SI 接口的切换 99

第 4 章 ■ 3GPP 内的互操作 103
4.1 基于 UE 能力选择网关 105
4.1.1 选择的烦恼 105
4.1.2 什么是基于 UE 能力选择网关功能 106
4.1.3 SGSN 设备如何实现网关选择功能 108
4.2 对等网元选择 109
4.2.1 以别人的方式 109
4.2.2 来自哪里 110
4.2.3 MME 还是 SGSN 111
4.3 互操作消息流程 114

第 5 章 ■ CDMA 网络和 LTE 互操作 120
5.1 CDMA 的历史 120
5.2 通往分组的路 121
5.3 CDMA 分组网网元和接口 123

目录

Contents

5.4 移动网络面对的问题 124
5.5 CDMA 的问题解决之道 125
5.5.1 鉴权 126
5.5.2 连接无线 126
5.5.3 移动性 128
5.5.4 QoS 129
5.5.5 计费 130
5.6 过渡者 eHRPD 131
5.6.1 eHRPD 如何“e” 131
5.6.2 eHRPD 网络接口 133
5.7 4G 终端在 eHRPD 接入 135
5.8 切换——优化和非优化 144
5.9 CL 切换流程例解 146

第 6 章 ■ LTE 网络中的语音业务 150
6.1 语音方案概述 150
6.1.1 SVLTE 151
6.1.2 CSFB 152
6.1.3 VoLTE 和 SRVCC 153
6.1.4 OTT 155
6.2 CSFB 详解 155
6.2.1 CSFB 主叫流程 156
6.2.2 CSFB 被叫业务 159
6.2.3 回落方式的选择 164
6.2.4 返回方式的选择 166
6.2.5 CSFB 几个关键问题 168

第 7 章 ■ QoS 和 PCC 架构 169
7.1 QoS，以业务为本 169
7.2 4G QoS 3 个关键参数 174
7.2.1 QCI，量化转发质量 174
7.2.2 ARP：有，还是没有？ 177
7.2.3 GBR/MBR，路有多宽 179

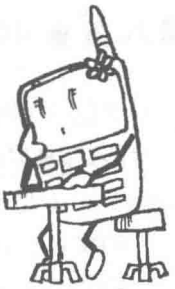
7.3 端到端 QoS 的实现 181
7.4 从业务到承载 184
7.5 QoS 的决策 190
7.5.1 网络侧协商：互相妥协 191
7.5.2 网络侧控制：独断决定 193
7.5.3 网络侧控制加 MME 限制：一票否决 195

第 8 章 ■ VoLTE 语音 197
8.1 语音通信简史：从面对面到软交换 197
8.2 认识 SIP 协议 205
8.2.1 软交换最简呼叫流程 205
8.2.2 一次典型的 FTP 流程 206
8.2.3 SIP 的功能 208
8.2.4 SIP 协议结构 210
8.2.5 SIP 呼叫流程 215
8.3 语音的承载 216
8.3.1 默认 APN 的选择 217
8.3.2 IMS 默认承载的建立 218
8.3.3 IMS 专有承载的建立 221
8.4 主叫域选 225
8.5 被叫域选 228
8.6 呼叫流程中的 EPC 230
8.6.1 建立 IMS 默认承载 230
8.6.2 VoLTE 的 IMS 域注册 234
8.6.3 建立 VoLTE 专有承载 236
8.7 SRVCC 和 eSRVCC 239

第 9 章 ■ 数据业务的国际漫游 247
9.1 数据业务漫游类型 247
9.2 三通，国际漫游的条件 249
9.3 签约信息互通 250
9.4 DNS 互通 252
9.5 IP 互通 255

缩略语 257

参考文献 263



第1章 概述

Chapter 1

《旧约》创世纪一章记载：人类在远古时代一度变得自以为是，联合起来建造通往天堂的巴别塔。上帝为此大逆不道的行为震怒，摧毁了巴别塔。为了削弱人类的力量，使得人类无法再干这种事，上帝让人类说不同的语言，使人类相互之间不能沟通，增加隔阂。

为了有效沟通、消除误解，在本书的一开始，我们先统一技术术语。在以后每一章的开始，我们都尽量去规范术语的使用，以便各种背景的人都可以使用一致的术语描述4G网络。

1.1 关于4G的几个概念

4G从概念阶段到商用阶段，走过了不短的路程。4G范畴内的概念，先后出现LTE、SAE、EPC、EPS、E-UTRAN等名字，它们都存在于各自的历史阶段，并且有着独特的含义。

早期的移动数据网络核心网部分（指PS，Packet Switching，分组交换）资料都冠以SAE前缀。SAE全称是**系统架构演进（System Architecture Evolution）**，是PS网络核心网网络架构向4G演进的工作项目。

与SAE对应的概念是LTE。LTE全称是**长期演进（Long Term Evolution）**，是无线接口部分向4G演进的工作项目。

SAE和LTE都是工作项目（Work Item）的名称，是3GPP为达成某种目标而聚集了一群人、在某个时间开展的一项工作。所以，SAE和LTE是一群人从事的一个**工作、一项事业**。

而SAE和LTE所研究的对象，分别被称为EPC和E-UTRAN。这两个概念构成我

们看到的 4G 网络。

E-UTRAN：演进的 UMTS 陆地无线接入网（Evolved UMTS Terrestrial Radio Access Network），是 3GPP 4G 的空中接口部分。

EPC：演进分组核心网（Evolved Packet Core），即 4G 核心网。

EPC 和 E-UTRAN，以及用户终端（UE）共同构成了 EPS（演进的分组系统）。EPS 代表了整个端到端的 4G 网络。EPS 和 LTE 以及 SAE 的关系如图 1-1 所示。

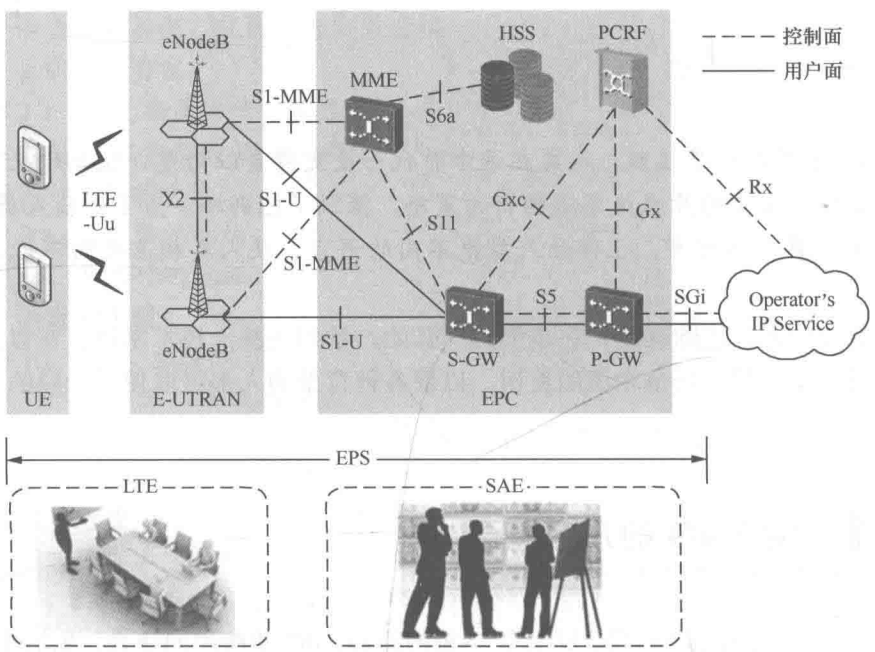


图 1-1　LTE、EPS、EPC、SAE 概念

由于整个通信业，特别是终端行业，在宣传 4G 网络时往往以 LTE 来指代 4G，造成 LTE 这个词在今天成了整个 4G 网络的代名词。

1.2　长期演进，演进到哪里了

在 4G 时代，LTE 的 EPC 部分演进到架构扁平化、承载控制分离、全 IP 组网的形态（如图 1-2 所示）。

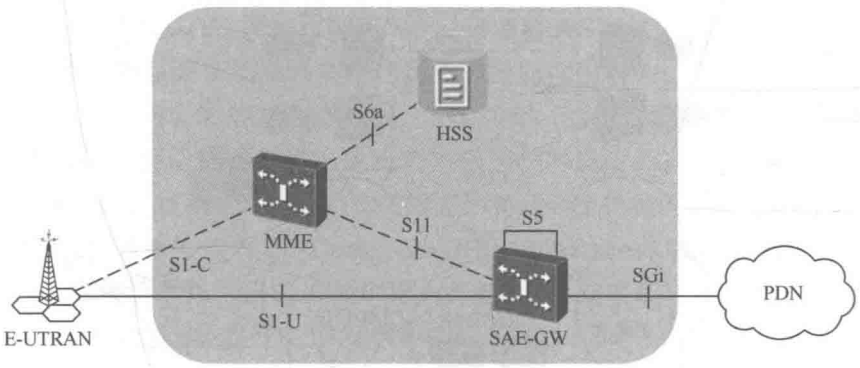


图 1-2　承载和控制分离

网络架构扁平化：无线接入部分从 3G 时代的 RNC 与 NodeB 两个设备演进为 eNodeB 一个节点。用户面在核心网网络部分只经过 SAE-GW 一个节点，不再经过对等 2G、3G 网络 SGSN 的 MME 网元。MME 只处理信令相关流程。通过这种结构，移动数据网络在 4G 时代实现了“承载控制分离”。

承载控制分离这种架构，大约 10 年前的语音软交换时代就已经在电路域实现了。软交换架构的电路域如图 1-3 所示。

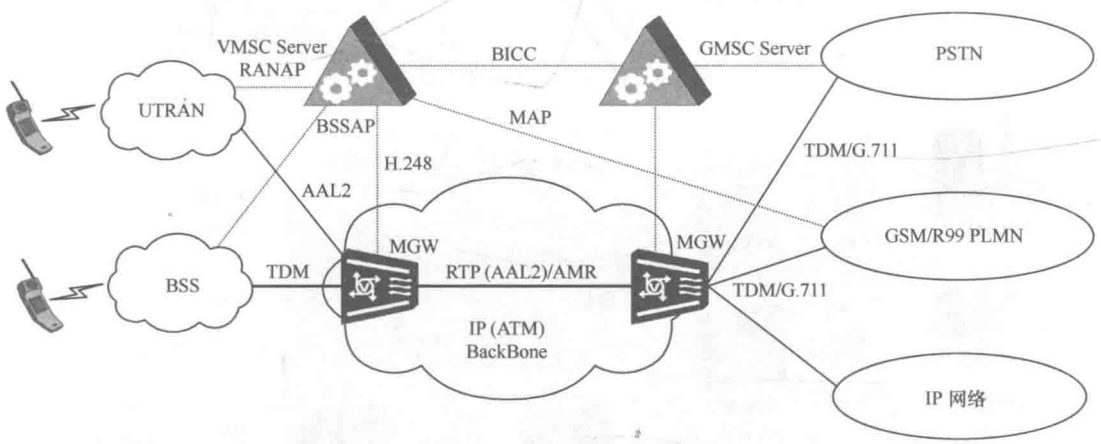


图 1-3　软交换网络结构

这张图的结构和现在的 EPC 网络结构完全相同。

EPC 网络的另一个特点是全面 IP 化：整个移动数据网络除空口部分外的其他全部接口均已经实现 IP 化、分组化（如图 1-4 所示）。

4G 网络的网络架构更加简化。但是，在相当长一段时间里工程师面对的将是如图 1-5 所示的各种制式共存并逐步实现全面互操作的网络。所以，对于工程和维护人员而言，面对的将是一个更加复杂的各种制式共存的移动数据网络。

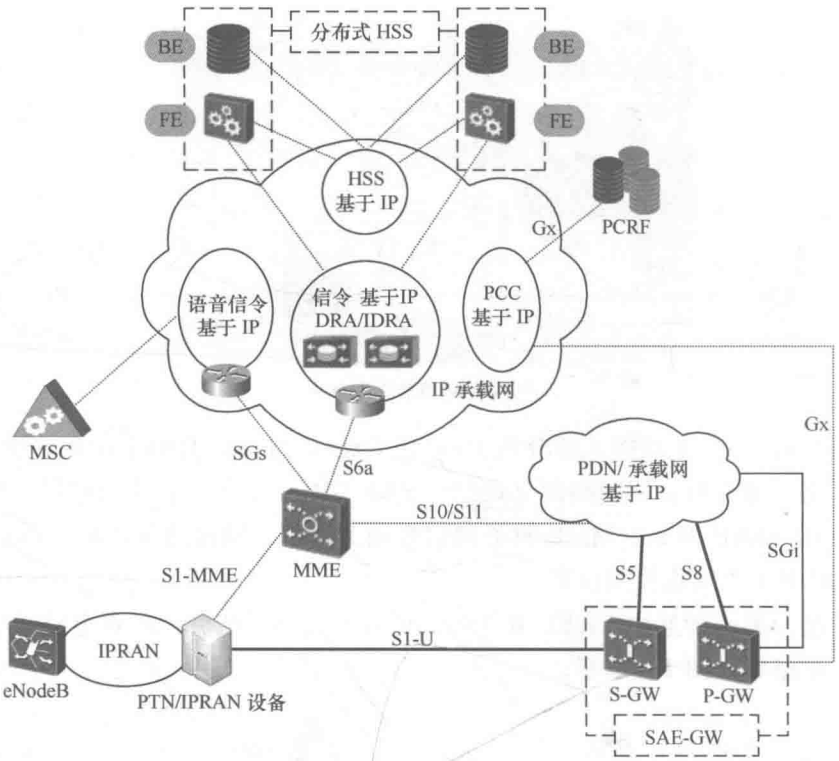


图 1-4　4G 网络各接口 IP 化情况

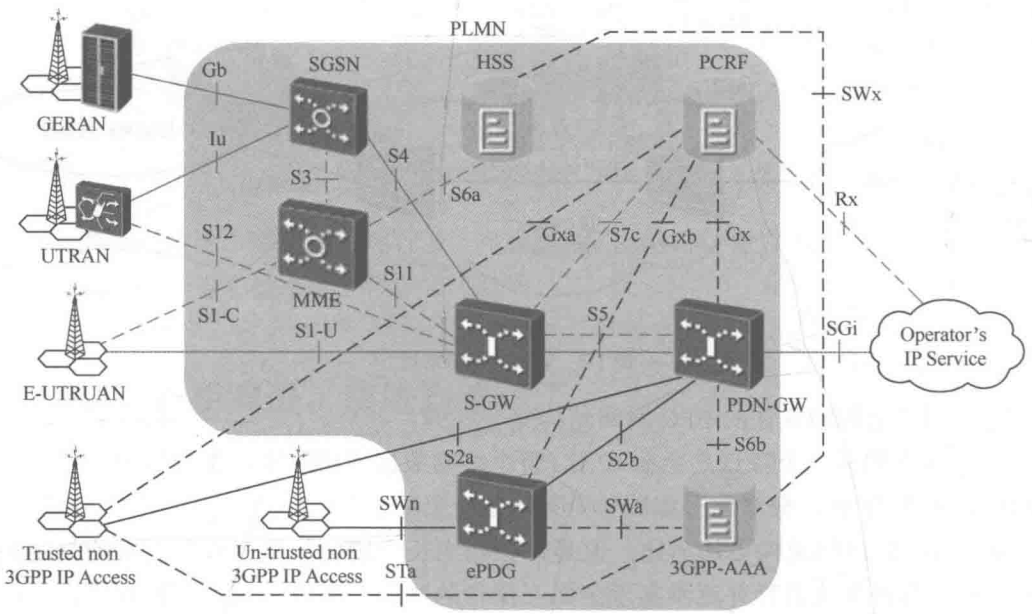


图 1-5　各种接入条件 4G 接口示意

（1）为了从现有 2G/3G 网络过渡到 4G，与 GERAN（2G 无线接入网）和 UTRAN（3G 无线接入网）的互操作场景将会在相当长一段时间内存在。

（2）为了接管 3GPP2 的 CDMA 的网络，在 CDMA 运营商网络里，E-UTRAN 和 Trusted non-3GPP 的 CDMA 网络的互操作场景将会在相当长时间内存在。

（3）Wi-Fi 架构、移动宽带和固定宽带融合，将是未来数据网络的发展方向。3GPP 的 4G 网络在可预见的未来会接入 Un-Trusted non-3GPP IP Access 网络的接入部分（如 Wi-Fi）。

同时，4G 网络给运维带来的挑战也更大。4G 网络扁平化，4G 网络取消 BSC/RNC 控制器节点，海量 eNodeB 直连 MME/SAE-GW（如图 1-6 所示）。

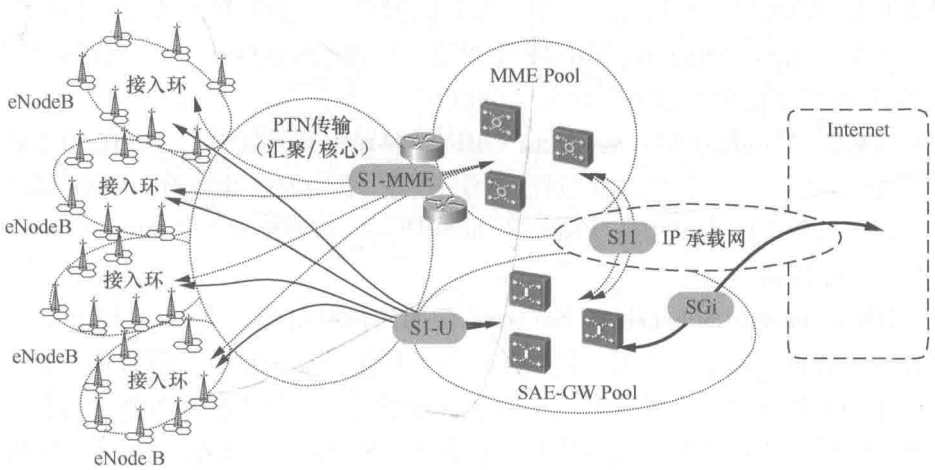


图 1-6　网络扁平化带来的 eNodeB 集中接入

扁平化的网络架构给核心网带来更多的切换信令、寻呼信令。核心网设备直接承担无线基站汇聚节点功能对 MME 和 SAE-GW 的维护和业务冲击大，风险更加集中。

4G 网络业务多样化，并承载语音业务。在 4G 时代，移动互联网深入每个人的生活；4G 网络所承载的业务更加贴近生活，更加影响生产。每个字节所承载的价值更多，用户对移动数据通信的要求更高，因此对 4G 网络的可靠性、业务质量控制提出更高的要求。

全网 IP 化。从 eNodeB 到业务服务器端到端路径均经由 IP 承载。IP 网络单节点故障影响的范围大，问题定界困难，对网络的维护带来很大挑战。

1.3　认识 EPC 网络的网元

LTE 网络所完成的工作是将移动终端以分组的方式连接到外部分组数据网络。

这里面的关键词是**移动**和**分组**。

移动的特性决定了终端是通过空中接口和网络侧连接，并且网络结构必须有能力保证终端在移动过程中业务的连续。

分组的特性要求网络中所有网元和接口必须支持分组方式的转发。分组（主要是 IP 协议）技术具备统计共享的特点。共享的另一层意思是资源抢占。因此，网络必须能够保证优先级较高的业务优先分配到资源（QoS 控制）。

根据以上特点，LTE 网络的设计包括的主要网元有：

（1）**eNodeB（evolved Node B，演进的节点 B）**。eNodeB 是 LTE 网络中的基站，是 LTE 网络 E-UTRAN 的主要网元，负责无线资源管理、上下行数据分类和 QoS 执行、空口的数据压缩和加密。eNodeB 同 MME 完成信令处理，与 S-GW 一起完成用户面数据转发。eNodeB 相当于面向终端的一个汇聚节点。

（2）**MME（Mobility Management Entity，移动性管理实体）**。MME 负责控制面的移动性管理、用户上下文和移动状态管理、分配用户临时身份标识等。MME 相当于 LTE 网络总的管家，所有的内部事务（Intra System 切换）和外部事务（Inter System 互操作）均由 MME 总体协调完成。

（3）**HSS（Home Subscriber Server，归属用户服务器）**。HSS 存储了 LTE 网络中用户所有与业务相关的签约数据，提供用户签约信息管理和用户位置管理。类似于 2G、3G 网络中的 HLR 网元。运营商是一个营利性组织，不能任由任何人都使用运营商的网络，谁可以使用？这些签约、鉴权信息都保存在 HSS 中。通常情况下，4G 网络的 HSS 与 2G、3G 网络的 HLR 融合在一起。

（4）**S-GW（Serving Gateway，服务网关）**。S-GW 是 3GPP 内不同接入网络间的用户锚点，负责用户在不同接入技术之间移动时用户面的数据交换，以屏蔽 3GPP 内不同接入网络的接口。S-GW 承担 EPC 的网关功能，终结 E-UTRAN 方向的接口。

（5）**P-GW（PDN Gateway）**。**PDN 是 Packet Data Network 的缩写**，指采用分组协议（基本是 IP 协议）的数据网络，泛指移动终端访问的外部网络。P-GW 被称为 PDN 网关，是 3GPP 接入网络和非 3GPP 接入网络之间的用户锚点。P-GW 与外部 PDN 连接的网元，终结与 PDN 相连的 SGi 接口。P-GW 承担 EPC 的网关功能。一个终端可以同时通过多个 P-GW 访问多个 PDN。

S-GW 和 P-GW 通常是物理网元合一部署，被称为 SAE-GW。

（6）**PCRF（Policy and Charging Rules Function，策略和计费规则功能）**。PCRF 完成动态 QoS 策略控制和动态的基于流的计费控制功能，同时还提供基于用户签约信息的授权控制功能。P-GW 识别业务流，通知 PCRF。PCRF 再下发规则，决定业务是否可用，以及提供给该业务的 QoS。