

通 信 标 准 类 技 术 报 告

YDB 072—2012

下一代网络（NGN）支持泛在网应用的需求

Requirements for support of Ubiquitous Network applications and services in the
NGN environment

2012 - 03 - 25 印发

中国通信标准化协会 发 布

目 次

前言	III
1 范围	1
2 术语、定义和缩略语	1
2.1 术语和定义	1
2.2 缩略语	1
3 泛在网典型应用场景分类及特征分析	2
3.1 概述	2
3.2 监控报警类	2
3.3 数据收集类	2
3.4 信息推送类	3
3.5 视频监控类	3
3.6 远程控制执行器类	3
4 参考业务架构模型	4
5 泛在网应用对NGN的业务需求	5
5.1 概述	5
5.2 网络管理	5
5.3 数据组织管理	5
5.4 开放业务环境	5
5.5 标识、认证与授权管理	6
5.6 移动性支持	6
5.7 基于位置的业务支持	6
5.8 安全性	6
5.9 服务质量	6
5.10 私密性	6
5.11 结算与计费	7
6 为了支持泛在网应用及业务的NGN网络能力需求	7
6.1 概述	7
6.2 传送层功能需求	7
6.3 业务层功能需求	8
6.4 终端功能需求	15
6.5 管理功能需求	15
7 安全需求	16
7.1 概述	16
7.2 传送层安全需求	17
7.3 业务层安全需求	17
7.4 终端安全需求	17
附录A（资料性附录） 泛在网应用典型场景	18
参考文献	22

前 言

本技术报告使用重新起草法参考ITU-T Y. 2221: 2010《下一代网络支持泛在网应用和业务的需求》和3GPP TS 22.368-a10: 2010《支持机器类应用的网络增强》编制，与ITU-T Y. 2221: 2010和3GPP TS 22.368-a10: 2010的一致性程度为非等效。

本技术报告按照GB1.1-2009给出的规则起草。

为适应信息通信业发展对通信标准文件的需要，在工业和信息化部统一安排下，对于技术尚在发展中，又需要有相应的标准性文件引导其发展的领域，由中国通信标准化协会组织制定“通信标准类技术报告”，推荐有关方面参考采用。有关对本技术报告的建议和意见，向中国通信标准化协会反映。

本技术报告由中国通信标准化协会提出并归口。

本技术报告起草单位：中国电信集团公司、工业和信息化部电信研究院、中国移动通信集团公司。

本技术报告主要起草人：黄倩、张园、史敏锐、李健、王亚晨、邓桓。

下一代网络（NGN）支持泛在网应用的需求

1 范围

本技术报告规定了下一代网络（NGN）支持泛在网应用的参考业务架构模型、业务需求、能力需求、安全需求。

本技术报告适用于下一代网络（NGN）环境。

2 术语、定义和缩略语

2.1 术语和定义

下列术语和定义适用于本技术报告。

2.1.1

泛在网Ubiquitous Network

基于个人和社会的需求，实现人与人、人与物、物与物之间按需进行的信息获取、信息传递、信息存储、信息处理，具有环境感知、内容感知能力和智能性，为个人和社会提供泛在的、无所不含的信息服务和应用的网络。

2.2 缩略语

下列缩略语适用于本技术报告。

AKA	Authentication and Key Agreement	认证和密钥协商
ANI	Asynchronous Network Interface	异步网络接口
AS	Application Server	应用服务器
CDR	Charging Data Record	计费数据
FTTx	Fiber-to-the-x	光纤接入
GPS	Global Positioning System	全球卫星导航系统
IM	Instant Message	即时消息
IMEI	International Mobile Equipment Identity	国际移动设备身份码
IMSI	International Mobile Subscriber Identifier	国际移动用户识别
IP	Internet Protocol	网络之间互连的协议
LTE	Long Term Evolution	长期演进
M2M	Machine-to-Machine	机器对机器
MSISDN	Mobile Subscriber International ISDN/PSTN number	移动用户综合业务数字网号码
NAT	Network Address Translation	网络地址翻译

YDB 072—2012

NGN	Next Generation Network(s)	下一代网络
PDP	Packet Data Protocol	分组数据协议
POC	PTT Over Cellular	无线一键通
PSTN	Public Switched Telephone Network	公共交互电话网络
QoS	Quality of Service	服务质量
SIP	Session Initiation Protocol	会话初始协议
UNI	User Network Interface	用户网络接口
VoIP	Voice over Internet Protocol	IP 电话
XDM	XML Document Management	XML 文档管理
xDSL	X Digital Subscribe Line	多种数字用户线路

3 泛在网典型应用场景分类及特征分析

3.1 概述

泛在网应用包含丰富的终端设备类型，能够带来大量的人机互动的新型应用，泛在网应用与下一代网络（NGN）的结合，有可能带来杀手级业务，促进第三代移动通信技术（3rd-generation，以下简称 3G）和 NGN 的发展。

每一个泛在网应用都是由多种基本的通信过程组成的。结合终端上下行传输数据量、频度、移动性，时间窗、QoS 等多方面的需求，根据泛在网典型应用场景将泛在网应用大致划分为五类：监控报警类、数据收集类、信息推送类、视频监控类、远程控制执行器类等。

3.2 监控报警类

监控报警类产品，主要是指泛在网的传感器本地监测数据，当发生不符合预期的数据变化时通过网络通知应用层进行报警。应用场景及典型应用特征分析如下：

- a) 应用场景包括：烟雾温度火警信息监控报警、河流流量监控报警、商店银行门窗监测报警、电梯远程监控、井盖监控报警系统、医疗人体机能监测报警等。
- b) 典型应用特征分析：以电梯远程监控为例，从数据流量特征来看，属于低频次实时应用的泛在网应用，每次传输的数据比较少，具备机器到机器的自动化通信特征，与现有的人上网行为不同。且电梯远程监控终端属于前装市场，通信模块在电梯出厂前就已预装完毕，销售到全国各地，因此在制定业务资费、系统计费、出账等业务环节，终端管理、维护等支撑环节方面具有集中、便捷、高效的优势，但也涉及到漫游等问题。参见附录 A.1。

3.3 数据收集类

数据收集类产品，主要是指泛在网的传感器收集本地数据，但并不进行实时处理，部分应用会实时上传服务器进行后续处理，部分应用采用周期性上传发送。应用场景及典型应用特征分析如下：

- a) 应用场景包括：电力抄表信息收集、气象信息采集、火灾现场数据收集、交通路况信息采集、农业大棚数据采集、环境监测等。
- b) 典型应用特征分析：以电力抄表系统为例，目前电网公司，有以下三个方面的应用场景：分别是台区监控（远程实时的监测小区台变的工作状态的系统平台）、大用户负控（使用智能电表，实时地将专变的工作状态和用电量等信息通过泛在网终端远程传输到电力公司监控平台）、居民小区集抄（通过抄表集中器和采集器将若干小区电表集中一处，周期性收集小区居民电能表

数据)。从这三类电力应用的数据流量特征来看,大用户负控和小区居民集抄属于低频次实时应用的泛在网业务,台区监控则具有低频次非实时应用泛在网业务的特征,每次传输的数据比较少,具备机器到机器的自动化通信特征,与现有的人通过上网卡的上网行为不同。另外,采集器无需持续与网络保持连接,网络侧按照预先设定的日期和时间主动向智能电表终端发起通信,激活电表终端设备与网络的链接,实现采集电表信息的通信即可。参见附录 A.2。

3.4 信息推送类

信息推送类产品,主要用于网络侧向泛在网终端发送用户已订阅的有用信息。应用场景及典型应用特征分析如下:

- a) 应用场景包括: 交通状况信息发布系统、智能博物馆、交通信息发送等。
- b) 典型应用特征分析: 以车载信息应用为例,汽车生产厂商在车辆销售前就在汽车中预装车载系统,可以提供的功能包括结合了 GPS 数据的保障汽车和用车人安全,以及车内的通讯、娱乐、信息整合等,并可通过设置门户网站及与内容提供者合作的方式,从事移动电子商务等增值服务。从数据流量特征来看,兼有低频次实时和低频次非实时泛在网业务的特点,每次传输的数据比较少,具备机器到机器的自动化通信特征,与现有的人上网行为不同。且车辆具有移动性的特点,汽车生产厂家在车载终端预装时 UIM 卡归属于 A 地电信公司而销售到 B 地电信公司业务区域,用户在使用时将产生异地漫游。参见附录 A.3。

3.5 视频监控类

视频监控类产品,是指本地侧为泛在网视频捕捉终端,通过实时采集数据并上传到服务器,实现在线监控。应用场景及典型应用特征分析如下:

- a) 应用场景包括: 金融行业(各银行网点、信用社、邮政储蓄的远程集中联网监控)、公安、交通系统(城市道路监控、高速路监控、城市治安联防监控、“数字城管”“平安城市”监控系统)、教育系统(考场监控、校园保安监控、远程教学等)、油田、煤矿系统(油井、输油管道、矿井、排污口水流的远程集中联网监控)、电信、水利、电力行业(机房、无人值守基站的联网监控)、跨省市的大型企、事业单位、连锁经营店铺、娱乐商业场所(歌舞厅、网吧、酒吧、夜总会)、军队、医院等。
- b) 典型应用特征分析: 以自助银行监控为例,目前无人值守自助银行内主要是 ATM 提款机,要求自助银行内监控设备具备防暴和不可搬运,能够 24 小时稳定工作,能够提供精确的报警检测和强大的报警联动等功能。从 ATM 监控设备的数据流量特征来看,具有持续的多媒体流的特征,传输数据量比较大。监控设备一般固定地点,不发生移动。但由于无人值守,24 小时提供金融服务的营业场所,其相关设备和客户交易过程的安全性非常重要,防范各种针对 ATM 的犯罪行为是一个亟待解决的问题。当发生视频丢失,局部遮挡,信号报警时,及时准确的做出响应。报警事件可以触发本地警号输出,触发拨号器,也可以通过网络传输到监控中心,由监控中心做出相应的处理,要监督和防止不法之徒的恶意破坏、诈骗、抢盗,以便为事后公安机关的取证提供有效依据。

3.6 远程控制执行器类

远程控制执行类产品,广泛应用于远程操作以及自动化系统,通过服务器端下发的控制信令对各种类型的终端进行实时远程控制。应用场景及典型应用特征分析如下:

- a) 应用场景包括: 工业自动化、智能家居远程控制、未来的远程医疗等。
- b) 典型应用特征分析: 以智能家居业务为例,智能家居可以通过远程控制,控制家庭中各种设备的运行状况,如电灯的灭/亮和亮度控制,空调的启/停以及温度和风量的控制,家庭安防系统

的信号采集和执行, 各种开关量的输入, 电动窗帘的开启/关闭控制, 室内各种物理量的探测 (如温度、湿度, 各种气体含量等), 四表 (煤气表、电表、水表和暖气的热量表) 数据的输出与指示等。从智能家居的数据流量特征来看, 传输的信息主要是控制信息以及一些物理量的参数, 具有低频次小数据量的特征, 一般在数十 kbps 就可满足要求, 但是信息传输的可靠性要求比较高。这是因为它传输的信息是各种设备的控制信息, 它的错误不仅可能导致设备的非正常工作, 而且可能导致设备的损坏, 因此需要通过一定的技术保证数据传输的可靠性。参见附录 A. 4。

4 参考业务架构模型

基于泛在网应用和业务的NGN参考业务架构模型图如图1所示:

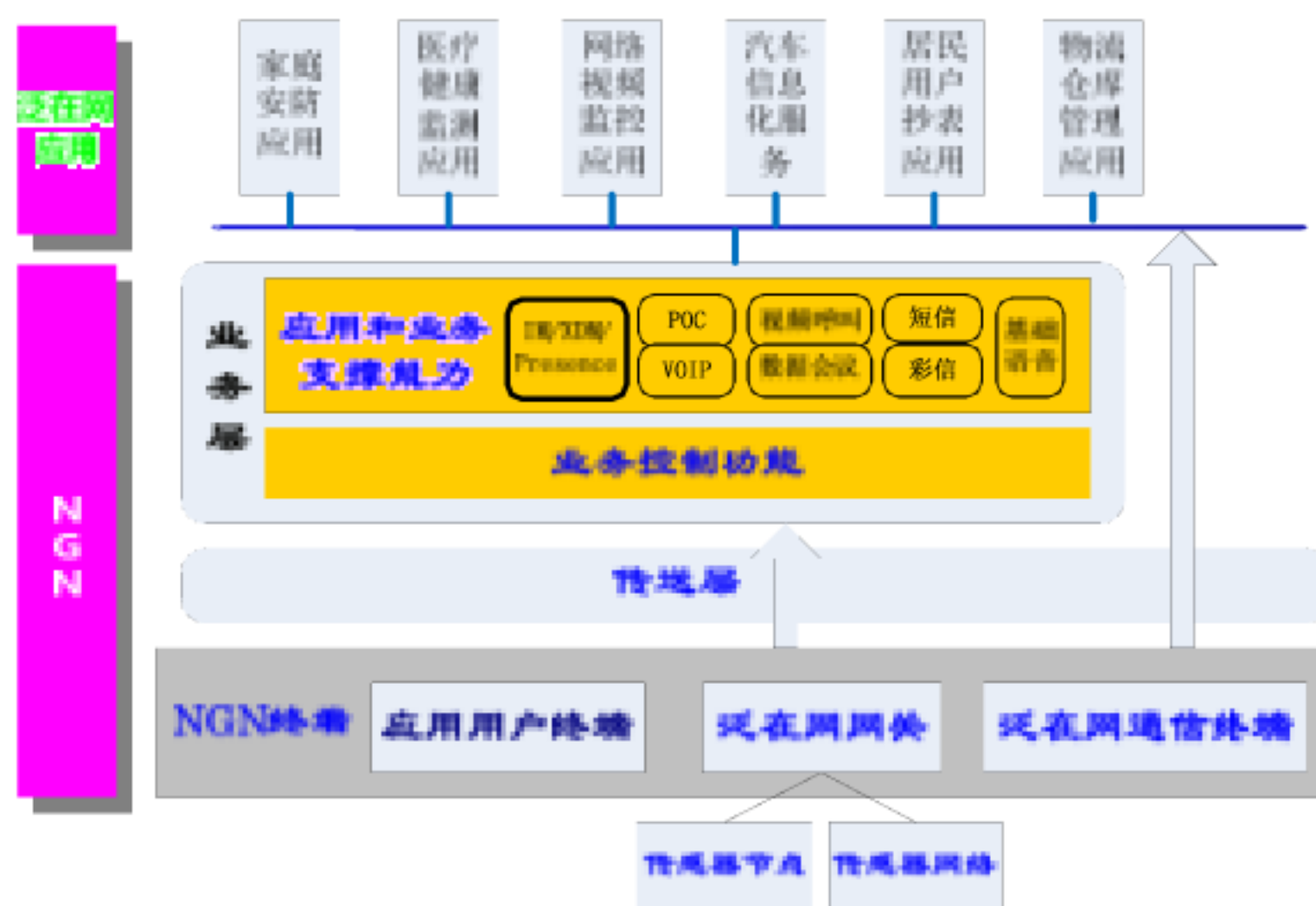


图1 下一代网络基于泛在网应用和业务的参考业务架构模型图

其中，下一代网络（NGN）为ITU-T Y. 2001定义，是一个基于分组的提供电信业务的网络，它能够利用多种宽带和具有QoS机制的传送技术，实现与底层传送技术无关的业务相关的功能。NGN是一个电信级和企业级的全业务网，能满足新的通信需求，不仅能够满足人与人之间的多媒体通信，也能够为大量的机器服务，可以满足基于泛在网应用的机器与机器，人和机器，人与人的3大类通信需求的和谐共存。

NGN 由运营商网络和终端组成。运营商网络分为传送层和业务层（业务层包括业务控制功能、应用和业务支撑能力部件，能够为泛在网应用提供丰富的基础业务能力和运营维护能力）。

用于泛在网应用的NGN终端类型包括:

- a) 具备 NGN 通信模块的泛在网网关, 即泛在网接入终端。是传感器网络中的汇聚节点, 负责与 NGN 网络相连, 能够将传感器节点及传感器网络的数据进行汇聚, 并上传到泛在网应用; 泛在网网关可以实现传感器节点及传感器网络之间的互通; 完成传感器节点及传感器网络的配置与组网、协议转换、地址映射和数据转发等功能, 也可以集成安全和计费等功能。
- b) 具备 NGN 通信模块的泛在网通信终端, 即泛在网智能处理终端。一般通过 RFID 技术、IP 传输或其他技术获取信息, 并直接与 NGN 网络发生交互, 将获取的信息通过 NGN 网络传输到泛在网应用或通信对端。
- c) 具备 NGN 通信模块的泛在网应用用户终端。订购泛在网应用的用户可使用应用用户终端来获取泛在网信息, 也可使用该终端对泛在网通信终端、泛在网网关进行数据配置和业务控制等已授权的操作。

对于非IP连接的传感器网络（需通过泛在网网关与NGN及上层泛在网应用通信）、不具备NGN通信模块的传感器节点等，因为不能直接与NGN通信，不属于NGN终端范畴。

另外，泛在网应用是指基于个人和社会的需求，在人与人、人与物、物与物之间按需进行的信息获取、信息传递、信息存储、信息处理的应用。泛在网应用类型丰富，可包括家庭安防、医疗健康监测、网络视频监控、汽车信息化服务、居民用户抄表、物流仓库管理等不同领域。不同的泛在网应用对移动性、通信模式、鉴权、处理模式、数据速率、安全性、可靠性、交互性等业务交互特征和需求存在差异。

NGN网络能够为泛在网应用提供丰富的基础业务能力和运营维护能力，用于泛在网应用的NGN终端可以通过NGN接入到泛在网应用，也可以直接通过传送层直接与泛在网应用通信。

5 泛在网应用对 NGN 的业务需求

5.1 概述

在第4章对泛在网典型应用场景和特征进行了分析，可以发现部分泛在网应用在数据传输模式上，区别于普通的个人通过手机/上网卡上网的模式，同时在移动终端和卡的漫游结算和计费、业务的计费套餐、用户管理、终端维护等方面，均有别于普通个人上网业务的支撑要求，因此泛在网应用的发展对NGN网络提出了一些特殊的需求，需要NGN网络提供特别的资源和支撑。

5.2 网络管理

泛在网应用允许多种NGN终端设备类型的接入，如使用有线或无线的连接手段，这些NGN终端设备需能够共存于NGN网络中。

用于泛在网应用时，NGN网络主要管理用于泛在网应用的NGN终端，其中包含泛在网通信终端、泛在网网关、应用用户终端等。同时，NGN应支持基于泛在网应用的业务层和传送层的运营维护管理功能，包括连通性、异构网络、网络资源、基础网络、故障等。

5.3 数据组织管理

用于泛在网应用的NGN终端和它的感应数据通常会被多个不同的泛在网应用所使用。根据不同的业务需求或用户需求，感应数据的使用也有所区别。

用于泛在网应用时，NGN的数据组织管理可以包含泛在网业务数据组织（service profile）和泛在网设备数据组织（device profile）。其中：

- a) 泛在网业务数据组织：由泛在网应用和业务的信息组成，包含泛在网应用标识、泛在网数据类型、泛在网应用服务提供商、位置信息等组成。
- b) 泛在网设备数据组织：由用于泛在网应用的NGN终端设备等信息组成，包含所属网络标识、设备标识、设备类型、设备能力、群组标识、QoS策略等组成。

其中，泛在网设备数据组织可以与泛在网业务数据组织相关联。

5.4 开放业务环境

泛在网应用应预先进行注册，以保证应用和业务的正常进行。用于泛在网应用的NGN终端也需要进行注册和发现。为了提供设备发现机制，设备应该注册一系列的属性。如果泛在网应用用户，即NGN终端的归属用户，不希望终端设备被其他人或应用接入，设备就需要注册私有属性。另外，需要提供泛在网应用描述语言以支持业务注册和发现机制。

YDB 072—2012

NGN需简化业务生成机制，利用资源及业务的组合和协调来创建和支撑更多的泛在网应用及业务。另外，新的泛在网应用和业务应与NGN提供的基础业务能力相结合，如IM业务、短信业务、基础语音业务等，并提供较好的业务生成环境。

5.5 标识、认证与授权管理

NGN网络及泛在网应用需要通过不同的标识来区分NGN终端，以便对业务及应用进行管理、认证及授权，如禁止未授权的网络资源使用，禁止未授权的信息流及应用接入，对接入泛在网获取感应数据的用户进行鉴权等。

在泛在网应用中，数据可以有不同级别的授权需求。例如，对于军事系统而言，原始感应数据与提炼出来的业务数据同样重要，因为可能数据将在其他业务中使用，如医疗系统。因此，泛在网应用提供者或者NGN网络运营商应该同时支持对于原始数据使用授权，以及提炼数据使用授权等。

5.6 移动性支持

NGN实现泛在网应用和业务的移动性支持，关键在于NGN终端中使用的技术。满足低功耗的IP移动机制的需求还是面临较大的挑战。

关于移动性需求的一个典型应用场景是在交通应用领域。例如，用户的车载终端可以在汽车移动时，为驾乘人员提供发送和接收多媒体短消息功能，并且利用GPS、基站定位等定位技术，通过车载终端为驾乘人员提供信息查询、位置显示、实时路况和在线更新地图等服务。当驾乘人员忘记车辆停放地点，可以拨打呼叫中心的电话，呼叫中心人员通过身份认证后可以远程操作让指定的车辆鸣号或启动双跳灯，提醒停车位置。移动性支持需求也适用于很多的其他场景。

5.7 基于位置的业务支持

用于泛在网应用的NGN终端，如泛在网通信终端、泛在网网关等的位置需要被NGN网络获取，并实施相应的管理，便于实施泛在网应用中的基于位置信息的上下文感知。另外，也可以通过位置信息促使业务发现及设备发现。

5.8 安全性

泛在网应用需要高安全性保障，因为传感数据通常是具备敏感性的数据。但由于系统限制、成本等方面的原因，对于一个小的传感器节点可能不会提供所有的安全机制。因此，在不同系统架构之间传输的感应数据可能无法实施较高的加密技术及安全保护。

NGN应提供一定的安全机制以保证泛在网应用的数据安全。

5.9 服务质量

建立QoS级别和数据优先机制，保障基于泛在网的一些关键任务、关键数据能够优先提供QoS保障，如保证火灾告警通过可靠方式及时传递到国家灾害预警系统。

NGN的应用层应具备一定的流量控制机制。通常泛在网应用和业务的通信量较大，高效率的泛在网流量控制及资源管理可以提高泛在网应用和业务的QoS。

5.10 私密性

泛在网应用允许通过远程连接的手段收集一些具备时间范围或位置限制的大量感应数据。在大量数据的传递过程中，可能被一些未授权的用户获取或破坏。另外，数据在多个节点间进行传输会使用大量资源和位置，以及造成时延，一些中间节点可能会因此获取到一些敏感信息。也会危及到NGN网络及泛在网应用用户的安全，例如智能小区、智能家庭等应用。

因此，一些重要的信息应在NGN网络中被标识为“Private”，即保持私密性，这些信息只能在相互信任的多方间进行共享。另外，NGN网络同时支撑多个泛在网应用场景下，也应采取一定机制保证不同应用间的数据的私密性。

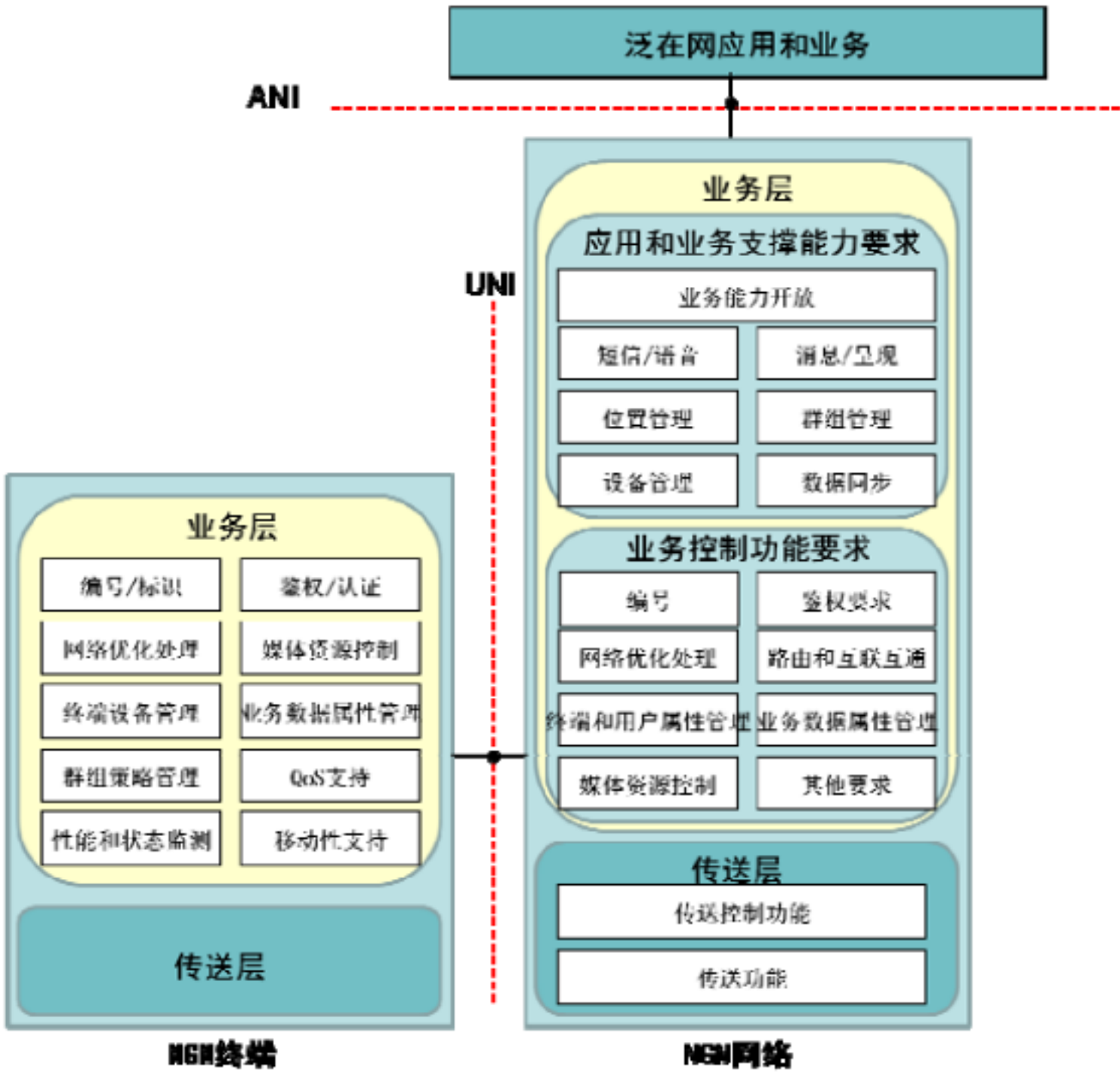
5.11 结算与计费

NGN应支持多样化的计费策略和计费方式。针对不同的泛在网应用场景可能存在不同的计费需求。如可能会有一系列的用于泛在网应用的NGN终端部署在同一个地理区域内，有的部署在企业网内，有的部署在公网内。某些应用可能长时间内只传输了一次数据，某些应用可能不停的传输流媒体数据。因此这些应用应实施不同的计费策略。

6 为了支持泛在网应用及业务的 NGN 网络能力需求

6.1 概述

为支持基于泛在网应用和业务，NGN网络应在传送层功能、业务层功能、终端用户功能和管理功能等方面均具备相应的能力。图2为NGN支持泛在网应用的功能架构模型图。



注：图中NGN终端主要指用于泛在网应用的具备NGN通信模块的泛在网通信终端、泛在网网关、应用用户终端等。

图2 NGN 支持泛在网应用的功能架构模型图

6.2 传送层功能需求

NGN传送层功能应具备以下能力，以满足泛在网应用和业务对于多种接入方式、QoS控制和位置管理的相关需求：

- a) NGN 应能支持各种基于泛在网应用的接入技术、传送技术，包括无线接入、固定接入，支持对无线接入网络的空口优化，及 IP 与承载网的 IP 网增强与优化等；

- b) NGN 应能够满足基于泛在网应用的机器与机器，人和机器，人与人的 3 大类通信需求的和谐共存；
- c) 所有 NGN 接入传送技术应能够在用于泛在网应用的 NGN 终端与业务层之间提供传送层面的 IP 连接；
- d) NGN 应支持在接入网层面的登记，初始化用于泛在网应用的 NGN 终端设备功能，包括接入 NGN 业务以及管理接入网 IP 地址空间，包括 NAT 功能；
- e) NGN 应支持 IPv4 和 IPv6 地址，应在不影响业务的前提下支持多个传送层地址互通情景，包括 IPv4 和 IPv6 地址不同，并在不影响业务的前提下支持传送层、业务层不同地址格式的变换；
- f) NGN 需要提供满足处于公网地址空间的泛在网应用可以向处于私网地址空间的 NGN 终端设备发送数据的需求的机制；
- g) NGN 应支持传送层鉴权和授权，用于泛在网应用的 NGN 终端设备属性应包含泛在网接入鉴权数据和网络接入配置相关的信息；
- h) 当用于泛在网应用的 NGN 终端设备游牧时，NGN 应支持可用业务的再配置，并据要提供的业务分配资源。
- i) NGN 应支持基于泛在网应用的策略管理能力，依据不同的应用服务质量需求提供不同的 QoS；
- j) NGN 应能管理由不同泛在网应用和业务引发的相关事务量；
- k) NGN 应可避免集中接入某单一资源；

6.3 业务层功能需求

6.3.1 业务控制功能要求

6.3.1.1 编号

NGN 应支持以下编号要求：

- a) NGN 需要为用于泛在网应用的 NGN 终端、用户、泛在网应用等提供有效、安全和可信任的编号、命名、寻址和标识环境。
- b) NGN 应支持动态和静态的地址分配机制，可以支持不同的泛在网应用使用单独的地址映射方案，或所有业务使用同一机制进行地址分配和命名。
- c) NGN 应唯一标识用于泛在网应用的 NGN 终端设备，标识应支持可携带、独立性、泛在网应用订购者和终端绑定、多终端关联等能力。
- d) NGN 应提供管理标识的机制，包括：设备标识的转换、标识映射关系的存储等。
- e) 可根据不同接入类型的 NGN 终端设备区别进行标识，如：
 - 1) 每个通过 2G/3G 接入的 NGN 终端设备都应具备通信模块，并与传统移动终端一样占用实际用户号码，具备 IMSI、IMEI 和 MSISDN 等参数，计费系统通过用户的 IMSI、MSISDN、群组标识等参数标识计费。根据运营商方案不同，也可采用独立建网的虚拟号码（虚拟号码+IMSI）进行标识和计费；
 - 2) 通过 xDSL、FTTx、宽带无线接入、卫星/微波接入、LTE 接入的 NGN 终端设备，可以以互联网号码或实际号码的形式进行标识，互联网号码包括 SIP URI 等形式，并能够在运营商的运营系统进行计费及管理；
 - 3) NGN 应支持多种不同的编号方法，除 ITU-T E.164 Tel URI（全球号码），非 ITU-T E.164 编号（本地号码），SIP URI 等之外，还应允许国内标号计划内的短号码、允许私有和行业号码。当使用非 ITU-T E.164 编号（本地号码）或拨号序列时，NGN 寻址应提供本地号码的有效范围。应支持区分字母数字的能力；

- f) NGN 应支持用于泛在网应用的 NGN 终端设备的群组标识机制，如对于位于相同区域，或具备同样泛在网应用特征，或归属于同一个泛在网应用订购者的 NGN 终端设备，可以将这些 NGN 终端设备标识为一个群组。

6.3.1.2 鉴权要求

NGN 应支持以下鉴权要求：

- a) NGN 应支持业务层鉴权和授权，并支持对不同类型标识的用于泛在网应用的 NGN 终端设备的认证，验证终端的有效性。对于具备群组标识的用于泛在网应用的 NGN 终端设备，NGN 应支持对群组标识的鉴权和授权。
- b) NGN 应支持适用于底层接入网络技术的各种网络鉴权机制，泛在网应用鉴权应与 NGN 接入网技术无关，并保持业务鉴权机制的一致性。
- c) NGN 应支持硬件或软件鉴权方式，允许使用设备属性信息进行 NGN 终端设备鉴权。
- d) NGN 应提供用于泛在网应用的 NGN 终端设备与泛在网应用服务器之间的双向鉴权。
- e) NGN 应提供个人用户与用于泛在网应用的 NGN 终端之间通信的双向鉴权，防止未授权的个人用户接入，保护 NGN 终端设备的数据的安全性。
- f) NGN 应支持根据业务数据的安全等级对用户的访问进行认证和鉴权；
- g) NGN 应支持用于泛在网应用的 NGN 终端设备的位置保密机制，能够对非信任实体隐藏位置信息。
- h) NGN 应支持按照应用和业务需求对不同类型的数据进行多级认证；
- i) NGN 应支持根据接入权限、泛在网属性、QoS 属性和网络策略提供已鉴权 NGN 终端设备的业务接入。

6.3.1.3 网络优化处理

NGN 应支持以下网络优化处理要求：

- a) NGN 需要提供减少终端执行移动性管理流程的机制；
- b) NGN 需要提供根据时间可控属性对 NGN 终端设备执行接入控制；
- c) 泛在网应用种类多，跨行业领域广，应用趋向多样性，终端种类多，因此 NGN 应有能力可控地对不同泛在网应用提供不同的业务等级。业务等级可考虑最大平均数率，峰值速率和丢包率三个方面作为划分维度，支持对泛在网应用依据业务等级进行高、低优先级处理的机制；
 - 1) 最大平均数率（以超过一小時间隔计）：考虑四种的最大平均速率范围为业务等级划分标准，速率范围是：小于等于 1kbps，1kbps 到 10kbps 之间，10kbps 到 100kbps 之间，大于等于 100kbps。
 - 2) 峰值速率：考虑四种峰值速率作为业务等级划分标准，速率是：10kbps，100kbps，1Mbps，大于 1Mbps。
 - 3) 丢包率：考虑是否丢包这两种情况作为业务等级划分标准。
- d) 当离线、干扰、中断、盗窃等监控中的紧急事件发生时，NGN 需启动相应告警处理流程，具备提供此类事件上报给泛在网应用用户的机制，并能够提供对 NGN 终端设备执行控制的机制；
- e) NGN 应支持对低数据流量泛在网应用执行优化传输的机制；
- f) 泛在网应用用户有能够控制用于泛在网应用的 NGN 终端的通信的需求，不允许 NGN 终端随机访问泛在网应用，同时在泛在网应用中，NGN 终端不需要持续与网络保持连接，或者不需要永远和网络建立 PDP/PDN 连接。因此，NGN 应支持对休眠终端的网络唤醒，按照一定的规律（如预先设定的日期和时间）主动向 NGN 终端发起通信，并启动终端发送/接收数据的机制；
- g) NGN 应支持触发在一定区域内的 NGN 终端设备发起业务的机制；

- h) NGN 应支持群组策略管理的机制, 如对一个群组的 NGN 终端设备执行最大带宽限制, 触发一个群组的 NGN 终端设备发起业务, 支持群组内安全的通信机制;
- i) NGN 应支持对 NGN 终端设备的远程设备管理机制。支持终端监测, 如监测终端设备和 SIM/UM 卡是否对应, 监测终端的业务功能是否和终端的权限相符, 监测终端的位置信息, 监测终端是否连接掉线等。当 NGN 检测到这些事件时, 将触发相应的后续动作, 如: 拒绝终端接入, 断开连接等。
- j) NGN 应提供针对泛在网应用的拥塞控制的能力, 针对设备故障, 同一时间触发等造成大量终端同一时间附着/连接网络的情况, 一方面是如何避免拥塞, 一方面是在拥塞的场景下, 如何执行拥塞控制;
- k) NGN 应提供流量控制机制, 网络应支持拒绝从某 APN 申请接入的用户的能力, 支持拒绝某个 NGN 终端群组用户接入网络的能力, 支持高优先级用户优先接入的能力, 支持对大量漫游的 NGN 终端设备的管控等;

6.3.1.4 路由和互联互通

NGN 应支持以下路由和互联互通要求:

- a) NGN 应能支持各种基于泛在网应用的接入技术、传送技术, 包括无线接入、固定接入, 支持对无线接入网络的空口优化, 及 IP 与承载网的 IP 网增强与优化等;
- b) NGN 应支持带有 NAT/NAPT 和防火墙的 NGN 终端设备接入。
- c) 泛在网应用需要的 IP 地址数量将极大增加, 预计需要 20 亿个 NGN 终端地址, 现有 IPv4 对应的 32 位 IP 地址远不能满足泛在网地址需求, 因此, NGN 应支持 IPv4 和 IPv6 地址;
- d) NGN 应支持业务注册和业务发现, 并至少支持一种业务描述语言和执行框架;
- e) NGN 应支持 NGN 终端设备不同编号规则的号码之间的通信, 如 ITU-T E.164 号码 和非 ITU-T E.164 号码 (如 SIP URI 号码等) 之间的通信;
- f) NGN 应能与其他非 NGN 网络之间基于泛在网应用进行互通, 并支持路由、信令互通、编号命名寻址互通、记账计费相关信息的交换、安全性互通、QoS 互通、NGN 终端设备属性信息的交换、媒体互通、管理互通、策略管理互通能力。
- g) NGN 应支持各种路由方案, 并提供选择最合适的路由路径的能力: (1) 支持静态和动态的泛在网应用路由方案。(2) 支持 NGN 网内和网间有效运行的路由方案, 以保证泛在网应用互操作。

6.3.1.5 终端和用户属性管理

NGN 应支持用于泛在网应用的 NGN 终端设备数据的集中管理。NGN 网络中存储的 NGN 终端设备数据应包括基本数据、认证数据、位置数据、业务签约数据、优化管理数据、安全数据等。

- a) 用于泛在网应用的 NGN 终端设备基本数据, 至少包括:
 - 1) NGN 终端设备的终端标识、号码、寻址信息、所属网络标识;
 - 2) 泛在网应用用户标识、号码等信息;
 - 3) NGN 终端设备的公/私有信息;
 - 4) NGN 终端设备与泛在网应用用户的归属关系, NGN 终端设备信息向泛在网应用用户的授权属性;
 - 5) NGN 终端设备的设备属性, 如设备标识、设备类型、终端能力、终端的资源限制、NGN 终端设备标识 (如 IMSI/IMEI) 与 UICC 的关联关系等;

- 6) NGN 终端设备群组属性, 对于属于同一个地区, 属于同一个应用用户, 具备同样的特征等的 NGN 终端设备进行群组标识; 允许同一个 NGN 终端设备归属于不同群组; 群组特性对所有群组成员适用;
- b) 用于泛在网应用的 NGN 终端设备认证数据至少包括:
 - 1) NGN 终端设备的认证方式;
 - 2) 与认证方式对应的认证信息: 如 AKA 方式的认证密钥、序列号等; HTTP Digest (MD5) 方式的用户名/密码等;
 - 3) 漫游属性, 如是否允许 NGN 终端设备漫游, 允许漫游/游牧的拜访网络;
 - 4) 时间可控 (Time Controlled) 属性, 如网络限制 NGN 终端设备在允许的时间范围发起业务或接收数据;
- c) 用于泛在网应用的 NGN 终端设备位置数据至少包括:
 - 1) NGN 终端设备的位置信息;
 - 2) 终端寻呼区域参数, 如对于具备低移动性 (Low Mobility) 属性的终端;
 - 3) 位置保密属性, 能够对非信任实体隐藏位置信息;
- d) 用于泛在网应用的 NGN 终端设备的业务签约数据至少包括:
 - 1) 为 NGN 终端设备提供业务的泛在网应用地址, 及其他应用信息;
 - 2) NGN 终端设备签约业务的触发条件, 业务触发优先级, 及触发失败的默认处理机制;
 - 3) 共享 iFC 签约指针集, 这些 iFC 被多个用户共用;
 - 4) 不透明的应用数据;
 - 5) 计费实体名称;
- e) 用于泛在网应用的 NGN 终端设备的优化管理数据至少包括:
 - 1) 低移动性 (Low Mobility) 属性, 如限制终端不移动、游牧或者在一定区域移动, 以便 NGN 减少对该类终端执行移动性管理流程;
 - 2) 时延不敏感 (Time Tolerant) 属性: 标识实时性要求不高/时延不敏感的终端。NGN 可以允许一定的时延, 以便在网络繁忙时采取一定的优先级处理机制;
 - 3) 低数据利用率 (Low Data Usage) 属性: 标识发送或接收的数据量比较小的终端;
 - 4) 只发不收 (Mobile Originated Only) 属性: 标识仅作为业务发起端 (MO), 无业务接收端 (MT) 的终端。对于此类终端, 网络侧不会主动向 NGN 终端设备发起业务, 以便 NGN 减少对该类终端执行移动性管理流程;
 - 5) 业务接收不频繁 (Infrequent Mobile Terminated) 属性: 标识以 MO 业务为主, 少量 MT 业务的终端。以便 NGN 减少对该类终端执行移动性管理流程;
 - 6) 网络激活属性: 标识平时休眠, 并由网络唤醒并启动业务发送/接收的终端;
 - 7) 低频率传输 (Infrequent Transmission) 属性: 标识 MO/MT 业务均很少量/频率很低的终端;
 - 8) 低功耗 (Extra Low Power Consumption) 属性: 标识低功耗终端;
- f) 用于泛在网应用的 NGN 终端设备安全数据至少包括:
 - 1) 保障 NGN 终端设备数据安全的必要机制, 如备份和容灾;
 - 2) 离线提示 (Offline Indication) 属性, 如终端离线时, NGN 需将此类事件上报给泛在网应用用户;
 - 3) 干扰提示 (Jamming Indication) 属性, 如终端被干扰掉线时, NGN 需将此类事件上报给泛在网应用用户;
 - 4) 安全连接 (Secure Connection) 属性, 如终端安全连接中止时, NGN 需将此类事件上报给泛在网应用用户;

- 5) 终端监控 (MTC Monitoring) 属性, 如 NGN 需对终端进行定时的监控, 当终端被盗或被破坏时, NGN 需启动相应告警处理流程, 并能对 NGN 终端设备执行一定控制;
- 6) 优先告警 (Priority Alarm Message) 属性: 如终端被盗时, 被破坏的情况时产生的上报信息, NGN 需优先启动紧急告警处理流程;

6.3.1.6 媒体资源控制

NGN 应支持以下媒体资源控制要求:

- a) NGN 应支持泛在网应用涉及媒体资源管理的需求, 如涉及语音、视频、图片、文字、其他数据等业务和应用。NGN 应具备处理各种媒体资源的能力, 如编解码、播放、媒体转换、录制、语音识别、音频/视频/数据会议桥、监控等。
- b) NGN 应支持 NGN 终端设备和泛在网应用服务器之间编解码端到端协商。
- c) NGN 应支持 NGN 终端设备之间的编解码协商, 如个人用户终端与泛在网通信终端/网关之间。

6.3.1.7 其他要求

NGN 应支持以下补充要求:

- a) NGN 应支持对泛在网应用终端和业务用户数据提供隐私管理的处理能力;
- b) NGN 应支持基于流、基于会话、基于群组、基于应用用户类别、基于应用类型的 QoS 控制粒度; 支持动态 QoS 行为; 支持 QoS 资源控制; 支持接纳控制和拥塞控制机制, 并具备一定的数据缓冲能力; 保证信令和控制包及时可靠传送的机制; 优先传送紧急通信和优先通信的机制;
- c) NGN 应支持针对泛在网应用的多播能力, 以实现有效、可扩展的数据分发, 提供在 NGN 网内或多个 NGN 网间实现广播/多播业务的能力;
- d) NGN 应支持保护切换能力、重选路由能力、业务恢复能力, 保证泛在网应用的可靠性、安全性和生存性;
- e) NGN 应支持基于蜂窝移动网络的 NGN 终端设备的无缝移动和漫游, 支持 NGN 网内和 NGN 网间的移动性, 以及 NGN 网在基础网络间的移动需要;
- f) NGN 应支持移动终端定位能力以及基于位置的泛在网应用, 可以对泛在网、NGN 终端设备的位置信息进行静态或动态的注册和更新;
- g) NGN 应支持加强私密性保护的多跳路由机制, 源节点标识、位置、时间等私密性信息不应向中间节点展示; 提供必要的匿名和标识转换机制;
- h) 电信网络和泛在网应用的运营要考虑到国家 and 地区的管制和法律的需求, NGN 应支持针对泛在网应用的紧急通信、合法拦截、恶意监听跟踪、恶意盗窃时设备控制、NGN 终端设备标识呈现和限制等能力;
- i) 泛在网应用开发方应具备保护 NGN 基础设施的能力, 防止恶意攻击, 例如用户信息盗取、篡改数据和消息、伪造等;
- j) 在法律法规允许的情况下, 泛在网应用提供者应防止将 NGN 终端设备信息或业务用户信息通过 NNI 接口泄露给其他实体;
- k) 在法律法规允许的情况下, NGN 应支持在泛在网应用提供者之间交换 NGN 终端设备相关的信息, 以便业务互操作;
- l) NGN 可根据业务需求支持离线计费、在线计费等多种计费形式, 以及多样化的计费元素和计费事件类型, 如群组计费;

6.3.2 应用和业务支撑能力要求

6.3.2.1 概述

NGN业务层可为泛在网应用提供丰富的通信能力，并与行业进行深度融合，对泛在网和社会发展将具有积极而广泛深远的影响。NGN可提供的通信能力包括：GPRS、短信、语音、消息、呈现、位置管理、群组管理、设备管理、数据同步、数据业务等。

6.3.2.2 短信

NGN可以为泛在网应用提供短信能力：

- a) 泛在网应用中在线低频率小数据传输（Online Small Data Transfer）的业务需求，且实时性要求不高的。较适合于采用短信进行承载，相对于分组域数据传输会减少系统负荷。
- b) 对于具备网络激活属性的 NGN 终端设备，可通过系统短信唤醒终端发送/接收功能；
- c) 可利用短信来进行远程 NGN 终端设备配置管理，如设备管理、OTA 配置等。

6.3.2.3 语音

NGN可以为泛在网应用提供语音能力：

- a) NGN 应为泛在网应用提供建立、维护及终止端到端业务会话的能力，包括 NGN 终端设备之间、NGN 终端设备与泛在网服务器之间，可用于固定和移动融合网络环境。主要功能包括：会话建立与连接，会话协商，会话控制等；
- b) NGN 应支持带有多种媒体类型的泛在网应用会话；
- c) NGN 应支持基于指定 QoS 等级和安全的会话接纳控制；
- d) 对于具备网络激活属性的 NGN 终端设备，可通过 CS 电话/彩信链接唤醒发送/接收功能；

6.3.2.4 消息

NGN可以为泛在网应用提供消息能力：

- a) NGN 应为泛在网应用提供建立、维护及终止端到端实时消息通信的能力，用于基于实时消息的泛在网应用。提供的能力包括 IM 即时消息、IM Chat，其中 IM 即时消息包含小数据寻呼模式聊天、基于连接的大消息通信等；
- b) NGN 应支持为泛在网应用提供建立、维护及终止端到端非实时消息通信的能力，用于基于对消息的传送时间并不敏感的泛在网应用。提供的能力包括，离线即时消息，电子邮件，短信，彩信等。非实时消息也可被 NGN 网络保存并在随后的某个时间递送。
- c) NGN 提供在不同 NGN 终端设备之间传递消息的服务，传递的内容可以是文本、图像、音频或视频等。

6.3.2.5 呈现

NGN可以为泛在网应用提供呈现能力：

- a) NGN 可以将 Presence 呈现业务由人与人之间的沟通扩展到泛在网应用，可以实现呈现任何 NGN 终端设备状态变化。任何一个有状态变化的 NGN 终端设备都可以作为呈现体（Prentity），并将自己的状态变化发布到 NGN 呈现业务平台，供其他 NGN 终端设备或应用订购。
- b) NGN 应支持收集 NGN 终端设备连接状态、位置的信息
- c) NGN 应支持向其它 NGN 终端设备或应用通知该终端的状态，同时其它业务或应用也可接入获取 NGN 终端设备的呈现信息。
- d) NGN 应支持对收集到的泛在网应用的呈现信息进行管理，并根据隐私性要求和接入规则对呈现信息进行接入控制，支持只提供部分呈现信息。呈现管理还应支持 NGN 终端设备间可发送呈现信息接收请求，并对其他 NGN 终端设备的请求进行处理（如接受或拒绝其他 NGN 终端设备/应用的请求）。

6.3.2.6 位置管理

NGN可以为泛在网应用提供位置管理能力：

- a) NGN 应提供基于泛在网应用位置管理能力，以确定和报告 NGN 终端设备和用户的位置信息。
- b) NGN 应提供附加功能，确保位置信息正确合法使用。
- c) NGN 提供基于位置的业务和应用时，应需考虑隐私保护。
- d) NGN 应提供根据 NGN 终端设备/用户属性发布位置信息的手段。

6.3.2.7 群组管理

NGN可以为泛在网应用提供群组管理能力：

- a) NGN 应支持以群组为特征的泛在网应用，如 VPN、远程设备管理、群组终端网络唤醒、触发群组业务发起、群组业务推送（Push）、紧急通知等，并支持对于群组执行策略管理，如执行最大带宽限制等；
- b) NGN 应支持基于群组的标识、配置操作、策略管理和计费；
- c) NGN 应支持 NGN 终端设备群组管理，并提供安全的群组通信机制。

6.3.2.8 设备管理

NGN可以为泛在网应用提供设备管理能力：

- a) NGN 应具备提供 NGN 终端设备管理和控制的网络能力，用于 NGN 终端设备硬件/软件配置管理；
- b) NGN 应支持的功能包括：远端软件升级/自动配置；远端故障诊断；支持收集 NGN 终端连接信息，如 IP 地址和位置；支持 NGN 终端设备信息的注册、管理和更新；支持远程查询 NGN 终端设备状态、确认状态变迁及升级，并支持诊断报告的创建；根据业务需求，允许安装泛在网应用用户喜好的程序或应用；

6.3.2.9 数据同步

NGN可以为泛在网应用提供数据同步能力：

- a) NGN 应具备实现 NGN 终端设备与网络设备之间数据同步的能力，并支持多种类型的数据同步。
- b) NGN 应支持多种不同的数据同步机制，如同步网络数据至 NGN 终端设备、同步 NGN 终端设备至网络、NGN 终端设备之间的数据同步；
- c) NGN 数据同步应独立于传送协议；
- d) NGN 应支持基于泛在网应用的强制网络数据同步；
- e) NGN 应了解 NGN 终端设备的资源限制；

6.3.3 业务能力开放需求

NGN可以面向泛在网应用适当的开放网络业务能力：

- a) NGN 应提供应用和业务能力的协调，应能追踪不同泛在网应用提供者的能力或业务成分，以及这些能力与业务成分之间的关系；
- b) NGN 开放业务环境应允许业务生成环境与应用和业务网络实体之间的互通；
- c) NGN 应面向泛在网应用适当的开放 NGN 业务网络实体的业务能力，并且方便地为用户生成个性化的业务逻辑，以吸引更多的泛在网应用开发者加入到泛在网应用开发中来，用以简化泛在网应用开发流程，促进泛在网应用的大发展；

- d) NGN 开放业务环境可以为第三方泛在网应用提供更多的业务能力，如语音/视频呼叫、多方通话、点对点短信、点对点彩信、点击拨号、呼叫转移、IM、呈现、位置信息以及终端状态信息等；
- e) NGN 开放业务环境可面向泛在网应用开发者、以及行业应用集成商等提供包括 widget、JS 脚本、插件以及 SOAP、Web Service、REST 等多种形式的业务开发接口以灵活适应各层次开发者的需求；
- f) NGN 开放业务环境应可以支持在有线及无线网络环境的互操作，提供跨网络的一致性的用户体验，支持业务组合技术、支持应用扩展性，不降低 NGN 可靠性；
- g) NGN 开放业务环境应提供基于泛在网应用的管理能力、业务和应用登记的手段，保证业务登记、取消登记，包括配置、激活、公布等；

6.4 终端功能需求

NGN终端应满足以下功能需求：

- a) 泛在网通信终端应支持以 2G 移动通信、3G 移动通信、xDSL、FTTx、宽带无线接入等接入方式的一种或多种，将终端感知数据传输到泛在网应用或通信对端；泛在网网关应支持以 2G 移动通信、3G 移动通信、xDSL、FTTx、宽带无线接入等接入方式的一种或多种，将终端感知数据传输到泛在网应用或通信对端；
- b) NGN 终端设备应支持 NGN 网络、泛在网应用或远程管理服务器对节点的设备认证和用户认证；
- c) NGN 终端设备应支持 NGN 网络、泛在网应用和远程管理服务器对终端的参数和软件配置；
- d) NGN 终端设备应支持支持用户/设备认证和业务安全、设备管理安全机制；
- e) NGN 终端设备应支持 NGN 网络、泛在网应用或远程管理服务器节点的性能和状态监测；
- f) NGN 终端设备应支持基于 QoS 策略对业务流进行优先级分类和调度；
- g) NGN 终端设备应支持不同传输速率、时延要求、传输间隔、数据包大小的数据可靠传输；
- h) NGN 终端设备应支持 NGN 网络唤醒功能，根据网络触发消息启动终端数据发送/接收；
- i) NGN 终端设备应支持 NGN 群组策略管理机制，根据群组广播消息启动终端数据发送/接收等操作；
- j) NGN 终端设备应根据时间可控属性遵守执行接入控制机制，并在接入时间窗到来时，启动数据发送/接收等操作；
- k) 当离线、干扰、中断、盗窃等监控中的紧急事件发生时，NGN 终端设备需启动相应告警处理流程，并根据网络指示对终端设备进行自我管控；

6.5 管理功能需求

6.5.1 概述

为支持基于泛在网的应用和业务，NGN管理功能应具备对泛在网网关、泛在网通信终端、和泛在网应用用户进行管理的能力，包括网络运营维护管理、计费管理等。

6.5.2 网管需求

NGN 应支持基于泛在网应用的NGN业务层和传送层的运营维护管理功能。

- a) NGN 应支持泛在网应用或网络提供商选择运营维护管理功能的能力。
- b) NGN 应支持连通性管理，如支持从泛在网应用到 NGN 网络及其终端设备、基础网络及其设备的连通性测试；连通性状态能实时向 NGN 业务层或向应用平台提供检测报告；

- c) NGN 应具备异构网络管理能力, 如对基于 IP 技术与非 IP 技术泛在网应用的管理; 对业务路径上各类异构网络及其设备的无缝管理, 形成端到端性能监测能力; 异构网络间 QoS 的统一配置等;
- d) NGN 应支持网络资源管理能力, 如提供对各种异构网络资源描述机制 (如: 不同类型泛在网应用的描述、NGN 基础网络的描述、端到端业务路径的描述、拓扑描述、链路带宽等); 提供网络资源使用方式 (授权) 的可配置能力; 提供泛在网应用流量对 NGN 网络资源的占用状况报告 (如占用信道、消耗带宽、占用链路等); 提供对 NGN 网络中被占用资源的可溯源能力, 记录业务的发起者和目的地等;
- e) NGN 应支持对 NGN 终端的网络管理, 如支持基于 IP 连接的泛在网应用及其终端的管理; 支持非 IP 连接传感器网络及终端通过网关进行管理的能力; 支持对不同能力的传感器网络本地化管理与远程信息采集和管理;
- f) NGN 应支持基础网络管理, 如泛在应用支持能力配置 (在网络和设备中配置、部署和管理泛在应用相关能力, 包括按照业务需要对流量进行调度与 QoS 控制、设备监控及其管理、业务链路监控及其管理); 管理域配置 (管理域的划分和配置, 满足跨管理域的业务流量调度的需要); QoS 配置与管理 (支持网络中泛在应用的端到端 QoS 的网络配置能力); 性能管理 (支持泛在业务承载网络性能的全程监测);
- g) NGN 应支持故障管理, 如支持为泛在网业务提供保护/备份链路并提供配置能力; 支持对基础网络和泛在网应用中的设备和链路的故障提示告警, 进行远程诊断、故障定位以及故障恢复操作; 支持故障通知功能; 支持自动检测丢失数据、丢失连接、错误数据、不期望的数据自复制、曲解数据等异常情况;

6.5.3 计费需求

NGN 应支持基于泛在网应用业务层和传送层的计费管理功能。

- a) NGN 需要提供有效、多样的计费方式满足运营商针对泛在网的行业用户不同的情况和需求进行计费;
- b) NGN 应支持离线 (即后处理 CDR 收集) 和在线 (即会话中计费) 的计费功能;
- c) NGN 支持开放的计费管理机制;
- d) NGN 应支持基于泛在网应用的各种计费策略, 如固定费率或基于会话的业务费率;
- e) NGN 应支持基于泛在网应用的多播业务的使用进行记账, 如记录哪个 NGN 终端设备在何时段接收了何种信息;
- f) NGN 应支持 NGN 终端设备、泛在网应用用户、网络运营商、泛在网应用提供商之间的计费和账单功能;
- g) NGN 可利用时间可控特性对 NGN 终端设备或行业用户进行区分计费 (在终端允许的时间范围之内和之外使用网络资源进行区分计费);

7 安全需求

7.1 概述

泛在网应用从信息世界延伸到物理世界, 可能会带来一系列安全问题。一些用于泛在网应用的 NGN 终端通过射频识别 (RFID)、红外感应器、全球定位系统、激光扫描器等信息传感设备, 按约定的协议, 把任意物品与网络连接起来, 进行信息交换和通信, 以实现智能化识别、定位、跟踪、监控和管理。由

此分析，泛在网应用的整个环节中容易受到安全攻击的节点非常多。NGN网络应支持泛在网应用特殊的安全性需求。

7.2 传送层安全需求

NGN网络支持泛在网应用对传送层有如下安全需求：

- a) 通讯网络接入认证安全要求：用于泛在网应用的NGN终端应经过严格的认证才能接入NGN网络，运营商应通过网络安全地验证NGN终端的标识，确认NGN终端身份，并通过授权控制其对NGN网络的访问。
- b) 密钥管理机制：密钥管理可以使用现有NGN网络中的密钥管理机制。
- c) 机密性、完整性保护：通信信息的机密性、完整性保护可以使用现有NGN网络中的机密性完整性保护机制。

7.3 业务层安全需求

NGN网络支持泛在网应用对业务层有如下安全需求：

业务认证：NGN业务层对用于泛在网应用的NGN终端进行业务认证的安全要求。为防止假冒用户使用未授权的业务或者合法用户使用未定制的业务，用户请求使用泛在网业务前应经过严格的业务认证，业务认证可在NGN业务层或者泛在网应用上执行，具体认证主体由具体业务场景确定。

群组认证要求：泛在网应用通常对应大量的终端节点，这些节点将构成一个组，具有相同的应用属性和行为能力，并且用于执行同样的任务。因此，NGN业务层需要提供对这些终端节点提供群组认证的能力。

用户隐私保护：泛在网中的有些应用不需要应用用户终端的参与，但某些业务的使用会涉及到个人隐私，如个人的身份信息、所在地理位置、兴趣爱好等信息，这些隐私信息可能会被攻击者有意或无意的获取，因而NGN需加强用户的隐私保护。

端到端的机密性，完整性保护：NGN业务层需要通过多种异构网络与用于泛在网应用的NGN终端进行通讯，这些网络间的安全机制相互独立且并不一致，因此需要为NGN业务层与NGN终端之间的应用通讯提供端到端的机密性和完整性保护。机密性，完整性保护的密钥变更周期由具体泛在网业务场景确定。

7.4 终端安全需求

下一代网络支持泛在网中对NGN终端有如下安全需求：

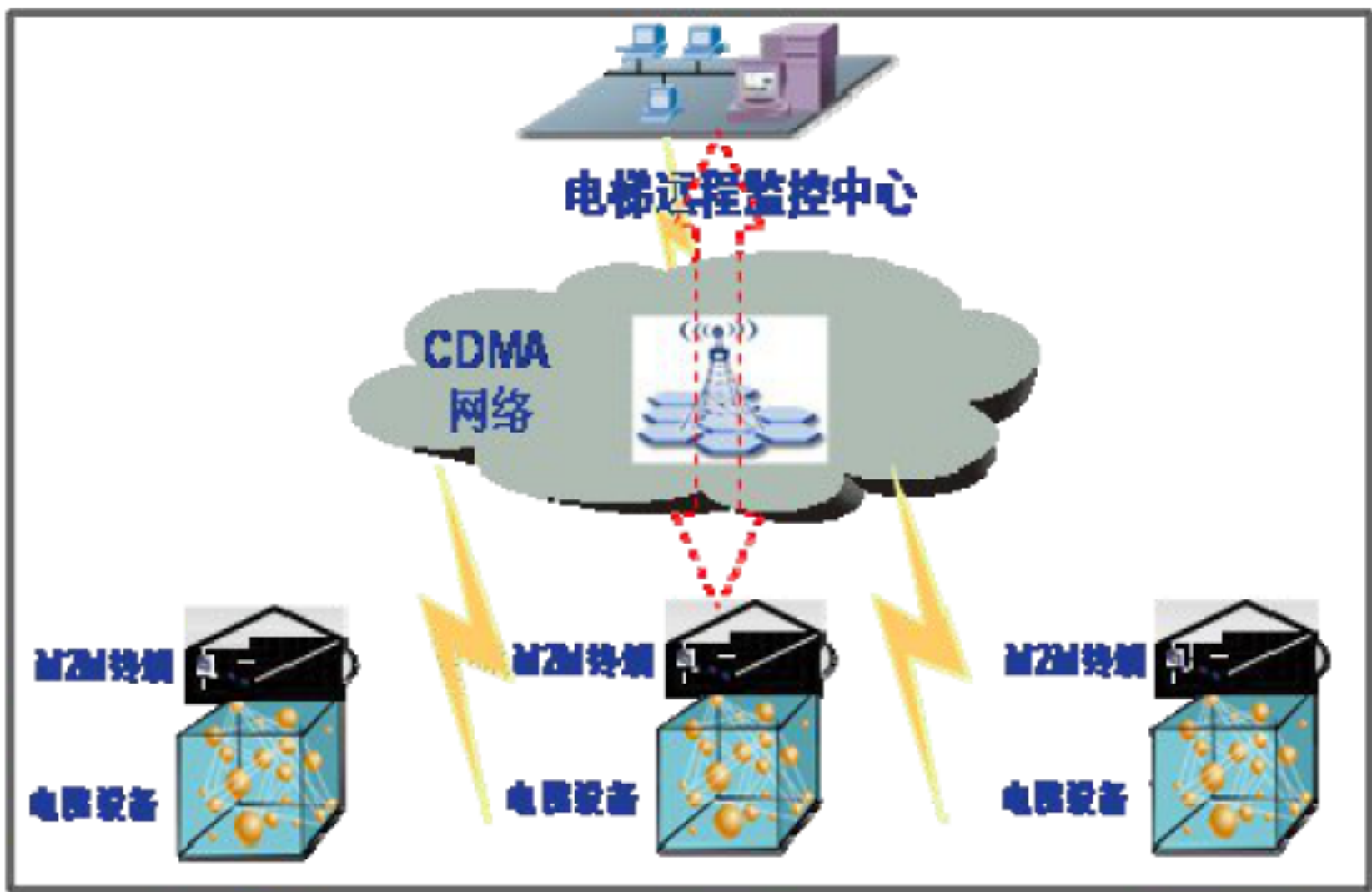
- a) 接入认证机制：用于泛在网应用的NGN终端节点应经过严格的认证和相关功能的授权才能接入NGN网络，运营商应通过网络安全地验证一个节点的标识，确认节点身份，并通过授权控制对本地资源和服务的访问；
- b) 密钥管理功能：用户的认证密钥是接入网络所需的关键信息，其衍生密钥将用于信息的机密性和完整性保护，因而NGN终端应有相应的安全功能来保证密钥安全产生与管理，同时防止密钥通过其他方式向未授权的第三方泄露，从而防止未授权的用户接入网络，以及机器间通信信息的安全；
- c) 设备完整性检查机制：设备完整性检查能够保证合法的设备接入网络，防止设备被恶意破坏或应用程序被更改等威胁，并且能防止用户识别卡非法插拔。
- d) 位置锁定机制：对于泛在网中有些业务中的终端节点具有低移动性或不移动的特点，位置锁定机制可以确保其不被盗用或非法移动，同时需要考虑移动性要求的便利。

附 录 A
(资料性附录)
泛在网应用典型场景

A. 1 电梯远程监控—监控报警类

A. 1.1 业务场景

电梯生产厂商出售电梯后,希望能够通过无线的方式,对其出售到全国各地的电梯的一些运行情况、运行状态、故障信息等能够及时的了解和收集。如图A. 1所示。



图A. 1 案例分析-电梯远程监控

因此电梯生产厂商,期望在电梯出厂前,在电梯中内置泛在网络终端(CDMA通信),泛在网络终端可按需将电梯运营的相关参数上报给电梯远程监控平台进行分析和处理。实现对电梯运行状况的实时监控,可以及时发现电梯故障隐患,并在故障发生时可以迅速派赴工程人员到现场进行设备维护修理,从而降低故障几率,提高售后服务响应速度并增加客户满意度。

目前全国电梯保有量近100万台,而且每年将增加18-20万部。

A. 1.2 业务特征

从电梯远程监控的数据流量特征来看,属于低频次实时应用的泛在网业务,每次传输的数据比较少,具备机器到机器的自动化通信特征,与现有的人上网行为不同。

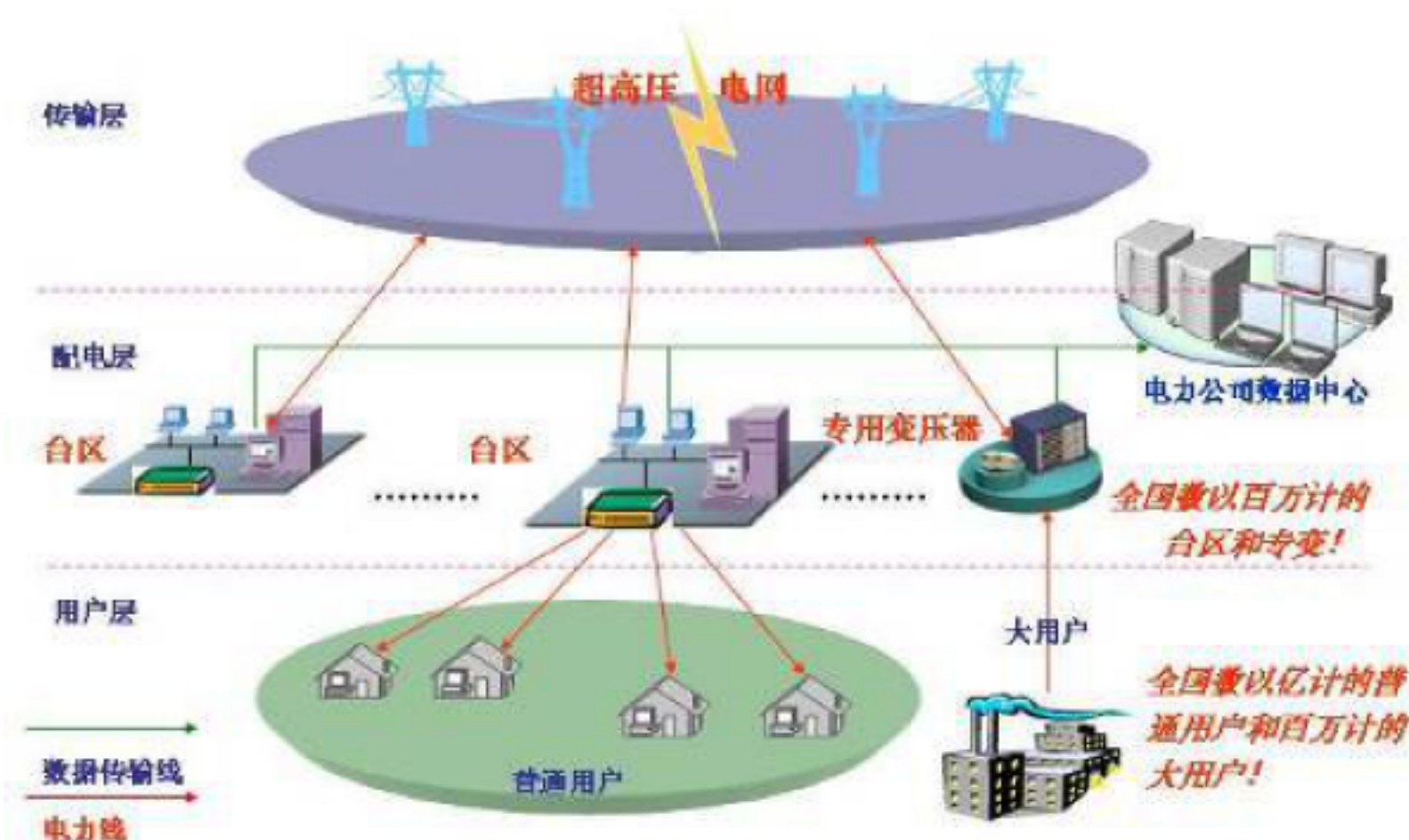
电梯远程监控终端在电梯出厂前就已预装完毕,销售到全国各地,如果能够给电梯厂家预先分配一批区别于现有133/189的号段资源,那么在制定业务资费、系统计费、出账等业务环节,终端管理、维护等支撑环节方面具有集中、便捷、高效的优势。但因为是前装市场应用,因此会涉及到漫游问题。

A. 2 电力抄表—数据收集类

A. 2.1 业务场景

随着电网公司智能电网发展的需要，电网公司需要能够及时，通过无线网络的方式，监控到小区电表的用电情况、大用户电表的用电情况，以及希望能够实时的掌握诸如台区变压器等电力设备的运营情况。目前电网公司，有以下三个方面的应用场景：

- a) 台区监控：远程实时的监测小区台变的工作状态的系统平台，通过安装在台变一侧的泛在网络终端将台变负荷、油温、电压、电流、是否偷漏电等信息远程传送到电力公司监控平台；
- b) 大用户负控：使用智能电表，实时地将专变的工作状态和用电量等信息通过泛在网络终端远程传输到电力公司监控平台；
- c) 居民小区集抄：通过抄表集中器和采集器将若干小区电表集中一处，每隔一定周期（如以每月一次的频率）统一收集小区居民电能表数据，并通过泛在网络终端远程传送到电力公司数据中心。而其他大部分时间，抄表集中器和采集器无需持续与网络保持连接，网络侧按照预先设定的日期和时间主动向智能电表终端发起通信，激活电表终端设备与网络的链接，实现采集电表信息的通信即可。



图A.2 案例分析-电力抄表

图A.2为电子抄表的案例分析。按照国家电网规划，预计到2011年底，国内电力无线抄表连接数规模在420万，其中2009-2011三年新增市场规模为310万。其中台区配变监测将新增200万，大用户专变负荷监测将新增为110万。大中用户用电量占整个电力用户用电量的60%~80%，电高峰期，对大企业用电的有序管理及监管，是电力的投资重点。

A.2.2 业务特征

从这三类电力应用的数据流量特征来看，大用户负控和小区居民集抄属于低频次实时应用的泛在网业务，台区监控则具有低频次非实时应用泛在网业务的特征，每次传输的数据比较少，具备机器到机器的自动化通信特征，与现有的人通过上网卡的上网行为不同。

每个地区电力公司的应用系统都包含成千上万的终端，如果能够给电力用户预先分配一批区别于现有133/189的号段资源，那么在制定业务资费、系统计费、出账等业务环节，终端管理、维护等支撑环节方面具有集中、便捷、高效的优势。

A.3 车载信息应用（Telematics）—信息推送类

A.3.1 业务场景

Telematics是Telecommunication（通信）和Informatics（信息科学）的合称，指利用无线通信和GPS卫星导航技术给在车里的人提供所需信息的服务，主要包含位置、交通、娱乐、互联网、车辆诊断、保安等服务。

汽车生产厂商在车辆销售前就在汽车中预装车载系统，可以提供的功能包括结合了GPS数据的保障汽车和用车人安全，以及车内的通讯、娱乐、信息整合等，并可通过设置门户网站及与内容提供者合作的方式，从事移动电子商务等增值服务。



图A.3 案例分析-车载信息应用（Telematics）

图A.3为车载信息应用的案例分析。据中国汽车工业协会的统计，2008年我国乘用车产销673.77万辆和675.56万辆；2009年1至6月，我国乘用车生产440.55万辆、销售452.34万辆，同比增长均超过20%，为前装车载信息服务市场提供了很大的空间。而在后装市场，截止2008年末，全国共有私人轿车1947万辆，Telematics也具有强大的发展潜力和空间。

A.3.2 业务特征

从Telematics的数据流量特征来看，兼有低频次实时和低频次非实时泛在网业务的特点，每次传输的数据比较少，具备机器到机器的自动化通信特征，与现有的人上网行为不同。且车辆具有移动性的特点，汽车生产厂家在车载终端预装时UIM卡归属于A地电信公司而销售到B地电信公司业务区域，用户在使用时将产生异地漫游；由于车辆市场达上千万的巨大容量，如果能够给该业务用户预先分配一批区别于现有133/189的号段资源，那么在制定业务资费、系统计费、出账等业务环节，终端管理、维护等支撑环节方面具有集中、便捷、高效的优势。

A.4 智能家居——远程控制执行类

A.4.1 业务场景

智能家居是通过统一的网络总线和控制平台将家庭的电器设备、灯光控制系统、安全控制系统、能源管理系统等连成一体。目前智能家居的发展趋势是由集中控制到分布控制，与集中式控制相比，分布式控制不仅能减少布线，而且能提高系统的可靠性，当某一个节点出现故障时，只需将该节点从网络中拿走，而其它节点不受影响。

智能家居可以通过远程控制，控制家庭中各种设备的运行状况，如电灯的灭/亮和亮度控制，空调的启/停以及温度和风量的控制，家庭安防系统的讯号采集和执行，各种开关量的输入，电动窗帘的开启/关闭控制，室内各种物理量的探测（如温度、湿度，各种气体含量等），四表（煤气表、电表、水表和暖气的热量表）数据的输出与指示等。

例如：当小张下班回家时，大门的门禁设备识别他的脸，并探测到他口袋里的电子钥匙将门自动打开。当小张进入或者离开一个房间时家庭控制中心，就会相应地自动打开或者关闭这个房间的电灯。家庭控制中心结合室内外温度、网上的天气预报以及用户的偏好等信息触发并自动调节暖气系统。

当家庭控制中心检测到异常情况，比如煤气泄露就会向小张的移动终端同时向他发送警告消息，并将电源自动切断。小张在办公室收到这一警告消息，他连接上家庭控制中心并点击“家庭维修”按钮，煤气公司就会收到家庭控制中心提供的详细信息。煤气公司派来的修理工带有专业的无线ID卡，家庭控制中心检测到这一信息并识别出无线卡的合法性才让修理工进入小张的房子，修理工可以通过冰箱上的视频面板与小张进行交流。当修理工完成修理以后保险公司会自动接收到来自家庭控制中心的损坏报告。

未来的智能家居不再是信息孤岛，由智能家电构成的家庭传感器网络与各服务提供商的应用系统建立连接，通过标准化的接口协议请求服务。

例如，冰箱可根据存储食物的剩余容量，按照预设的清单向食品超市订购食品，而超市又通过和专业的物流企业联网，向用户提供食品配送服务。通过不同应用之间的相互融合，逐步形成一个泛在的服务环境，为用户提供周到的服务。

A. 4. 2 业务特征

智能家居中控制网络的特点是：在这个网络上传输的信息主要是控制信息以及一些物理量的参数。信号的频率相对较低，因此传输的速率可以比较低，一般在数十kbps就可满足要求，但是信息传输的可靠性要求比较高。这是因为它传输的信息是各种设备的控制信息，它的错误不仅可能导致设备的非正常工作，而且可能导致设备的损坏。因此控制网络在技术上主要解决的问题是传输的可靠性。

参 考 文 献

- [1] ITU-T Y.2001 General overview of NGN
 - [2] ITU-T Y.2221 ITU-T Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment
 - [3] ITU-T Y.2011 General principles and general reference model for next generation networks
 - [4] ITU-T Y.2012 Functional requirements and architecture of the NGN
 - [5] 3GPP TS 22.368 Network Improvements for Machine-Type Communications (NIMTC), stage 1
 - [6] 3GPP TS 23.888 Network Improvements for Machine-Type Communications (NIMTC), stage 2
-