最后报告
ITU-D第2研究组

第26/2号课题

发展中国家从现有网络向下一代网络过渡：技术、监管和政策方面

2010-2014年第5研究期
电信发展部门

联系我们

网站：	www.itu.int/ITU-D/study_groups
国际电联电子书店：	www.itu.int/pub/D-STG/
电子邮件：	devsg@itu.int
电话：	+41 22 730 5999

第 26/2 号课题

发展中国家从现有网络向下一代网络过渡：技术、监管和政策方面

ITU-D 研究组

作为电信发展局知识共享和能力建设议程的后盾，ITU-D 研究组支持各国实现其发展目标。通过推动为减贫和经济社会发展进行 ICT 知识的创建、共享和运用，ITU-D 研究组鼓励为成员国创作条件，利用知识更有效地实现其发展目标。

知识平台

ITU-D 研究组通过的输出成果和相关参考资料，被用于 193 个国际电联成员国的政策、战略、项目和特别举措的落实工作。这些活动还有助于巩固成员的知识共享基础。

信息交换和知识共享中枢

共同关心议题的共享是通过面对面会议、电子论坛和远程与会，在鼓励公开讨论和信息交流的气氛中实现的。

信息存储库

研究组成员根据收到的供审议的输入文件起草报告、导则、最佳做法和建议书。信息通过调查、文稿和案例研究采集，并通过内容管理和网络发布工具提供成员方便地使用。

第 2 研究组

第 2 研究组由 WTDC-10 受命研究涉及信息通信基础设施和技术发展、应急通信和适应气候变化等领域的九项课题。着重为在规划、发展、实施、运营、维护和持续提供电信服务过程中能够优化用户得到的服务价值，并能最合适、最成功地提供服务的方法和方式。该工作包括将具体工作重点放在宽带网络、移动无线电通信和农村与边远地区的电信/ICT、发展中国家对频谱管理的需要、ICT 在缓解气候变化对发展中国家的影响中的使用、用于减轻自然灾害和赈灾的电信/ICT、合规性和互操作性测试及电子应用，特别强调通过电信/ICT 手段支持的应用。该项工作还研究探讨信息通信技术的实施，同时兼顾 ITU-T 和 ITU-R 开展研究的成果以及发展中国家的优先事宜。

第 2 研究组与 ITU-R 第 1 研究组一道共同负责涉及第 9 号决议（WTDC-10，修订版）问题的研究 – 各国，特别是发展中国家对频谱管理的参与。

本报告是由来自不同主管部门和组织的众多志愿人员编写的。文中提到了某些公司或产品，但这并不意味着它们得到了国际电联的认可或推崇。文中表述的仅为作者的意见，与国际电联无关。

目录

页码

页码

图目录

页码

页码

表目录

页码

第 26/2 号课题
发展中国家从现有网络向下一代网络过渡：
技术、监管和政策方面

1 向 NGN 过渡

1.1 为什么需要过渡？

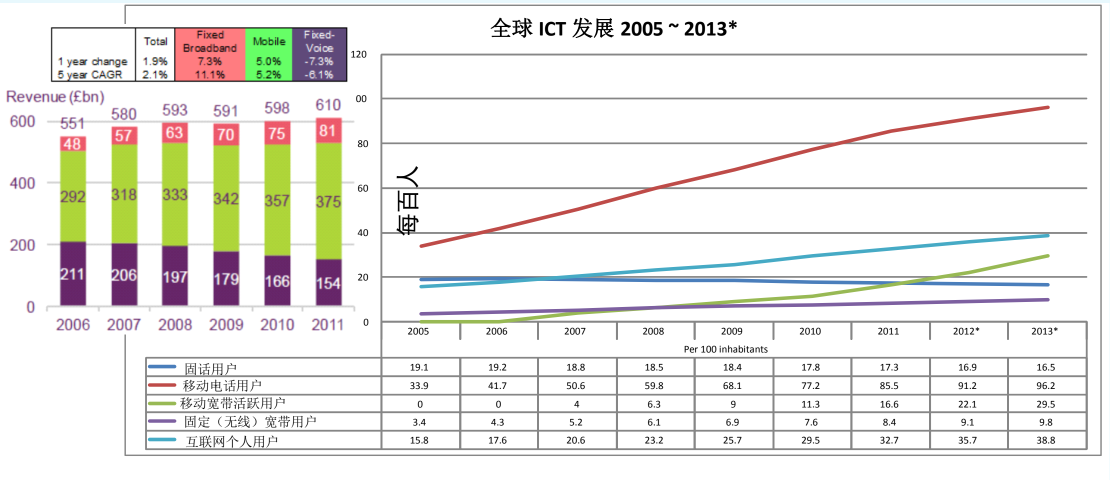
本节介绍从传统网络基础设施向新的网络基础设施过渡的动机。根据不同的观点，如业务方面，技术方面等，这有几个原因。

1.1.1 过渡的总动力

考虑向如NGN之类的新的网络基础设施过渡的重要因素之一就是跟随业务流量所造成的趋势。

业务流量的一个关键点是语音业务从传统的基于固话（例如，PSTN和ISDN）向移动和基于IP过渡。如下图1-1所示，这种趋势自2003年触发以来还在持续。这种趋势带来两个方向：一是固定语音业务收入的降低（2006年和2011年之间固定语音业务收入下降-6%左右），另一个是在其网络上要求更多面向移动的业务和固定和/或移动宽带上基于IP的容量，这要求除传统网络基础设施外的额外投资（例如，在2006年至2011年期间，移动和宽带收入分别增长了5.2%和11%左右）。

图1-1：ICT发展状况



	Total	Fixed Broadband	Mobile	Fixed-Voice
1 year change	1.9%	7.3%	5.0%	-7.3%
5 year CAGR	2.1%	11.1%	5.2%	-6.1%

	2005	2006	2007	2008	2009	2010	2011	2012*	2013*
	Per 100 inhabitants								
固话用户	19.1	19.2	18.8	18.5	18.4	17.8	17.3	16.9	16.5
移动电话用户	33.9	41.7	50.6	59.8	68.1	77.2	85.5	91.2	96.2
移动宽带活跃用户	0	0	4	6.3	9	11.3	16.6	22.1	29.5
固定（无线）宽带用户	3.4	4.3	5.2	6.1	6.9	7.6	8.4	9.1	9.8
互联网个人用户	15.8	17.6	20.6	23.2	25.7	29.5	32.7	35.7	38.8

应对这些趋势有几种方法，可分为两种途径：补偿收入的减少和寻找新的收入来源。

对于收入减少的补偿，通过共享网络基础设施和系统来降低成本应该是除降低网络和服务基础设施部署的成本外最重要的一点。以下是在这个意义上的要求，并导致了对向NGN过渡的考虑：

- 降低运营成本和改进程序操作；
- 提供各类服务和应用的集成平台；
- 包括综合维护和培训的集成操作平台；
- 集中管理和控制。

在一般情况下，从寻找新的收入来源的角度，以经济的方式提供商业多媒体服务应该是强有力的选项之一。在这方面，以下应被视为提供多媒体服务时的高层次要求，并将导致向NGN过渡的原因：

- 补偿语音收入的减少，并增加宽带相关业务；
- 提供服务创新（如 VPN）；
- 减少引入任何新的服务和应用类型的上市时间。

1.1.2 运营商对过渡的看法

适应行业趋势对于运营商也是非常重要的问题，因为他们处于这些趋势的中心位置。也就是说，运营商应尽快做好准备，以使他们的业务配置和运营足够弥补他们的收入来源的减少。当他们在其基础设施中引入新系统和任何元素时，它们应足以及时提供新的收入。

运营商有意引进新的基础设施时要考虑以下问题：

- 支持保持主要业务的持续和需要运营商级服务的客户所需的业务连续性；
- 纳入现有的新业务，并对实时出现的新业务迅速作出反应的灵活性（充分利用 IP 模式的主要优点）；
- 能够实现投资的可行回报和具有市场价值最佳实践的可盈利性；
- 在故障和外部突发事件的情况下确保服务的存续能力；
- 服务质量，以在不同的流量混合、条件和超负荷下保证服务水平协议；
- 网络之间的互操作性，以对不同网络域中的流量实现端到端服务。

人们普遍认为，NGN是能够满足这些要求的主要选项之一。因此，许多运营商开始将其传统基础设施向NGN过渡，甚至其中有些已经过渡到NGN。

1.1.3 技术上对过渡的看法

关于当今的互联网，甚至IP技术的使用有很多技术问题，NGN中也使用该技术。这些技术问题对解决网络运营商和服务提供商的要求造成了一定困难。此外，更多的技术问题来自对如IPTV之类的媒体的有效处理。因此，在使用IP时必须在当前IP之上开发全新的技术或额外功能。

关键的技术问题的概要如表1所示。

根据ITU-T Y.2001建议书给出的定义，NGN虽然不能解决所有这些技术问题，但是解决其中许多问题的最佳选择之一。所以大多数行业正在开发NGN系统，运营商正在将其传统电信基础设施向基于NGN过渡。

表1-1：过渡的技术性问题

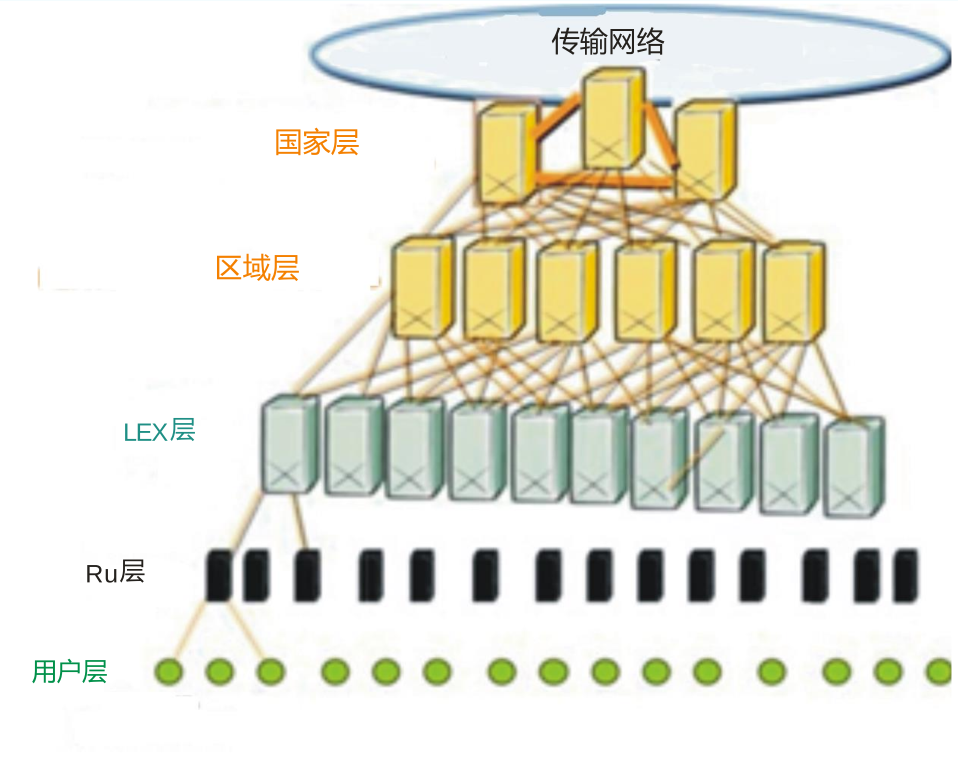
技术领域	问题
管理	可扩展性 计费
服务质量（QoS）和安全性	更高的可靠性 较高的弹性 安全系统 鲁棒性 性能 应用性能 认证，授权和结算
泛在性	使用户保持连接的泛在的网络，总是保持连接，无时不在、无所不在、以任何方式 存在意识
内容	数字版权管理（DRM） 有条件访问 安全和高效的传送
网络优化	公共服务基础设施 更少的网络节点 更少的开关操作 更简化的服务部署 更高的容量
互操作性	所有厂商设备的互操作性
多种接入网络	固定、移动、铜缆、光纤、无线... 支持多个连接 覆盖有线和无线的透明的移动性
资源共享	语音和数据传输资源的共享 服务平台的尽可能共享
传统和互联网服务的混合	将传统通信服务和基于 IP 的服务相结合的能力
互联	端到端的互联（例如，个性化的互动多媒体通信等） 客户端—服务器的交互（例如，游戏：高性能和低延迟） 用户控制的交互性（例如任播、M 对 N 的交互性等）
存储	业务连续性 公共（如 NPVR 和云计算）和私有（如 PVR）存储共享 数据保留
符合标准	实施符合标准的设备 标准化的协议和接口

1.1.4 架构上的考虑

传统电信是在几个层次上构建的。这有两个方面：一方面是技术基础，如物理网络，传输网络和服务网络等，另一方面是几何分布基础，如远程接入网络、接入网络、区域网络和国家网络等。这些层次一般不仅对建设和运营，对系统开发也非常有帮助。这些层次结构在识别方面很适于基于传统电话的服务提供和网络操作，也就是基于E.164号码。

然而，这些层次结构正成为瓶颈，尤其是正确地提供端到端连接和有效处理路由，考虑到如采用统一地址和动态路由等各种IP功能。因此，传统的层次结构是IP基础设施准备的课题。图1-2显示了传统电信网络的架构模型。

图1-2：传统电信网络的一般架构模式



以下是对传统架构模式组成主要特点的总结：

- 分 4 到 5 层的层次拓扑结构，到上一层的连接，以及每一层中的经济优化功能；
- 作为输出数据流量功能的节点数目和节点容量；
- 所有交换节点的媒体、信令、控制和管理处理服务；
- 具有明确定义的服务质量标准和标准化的工程规则的运营商级质量。

在尽量保持现有基础设施的良好功能的同时，需要改善某些功能，以满足变化趋势。对此，应考虑到以下几个方面：

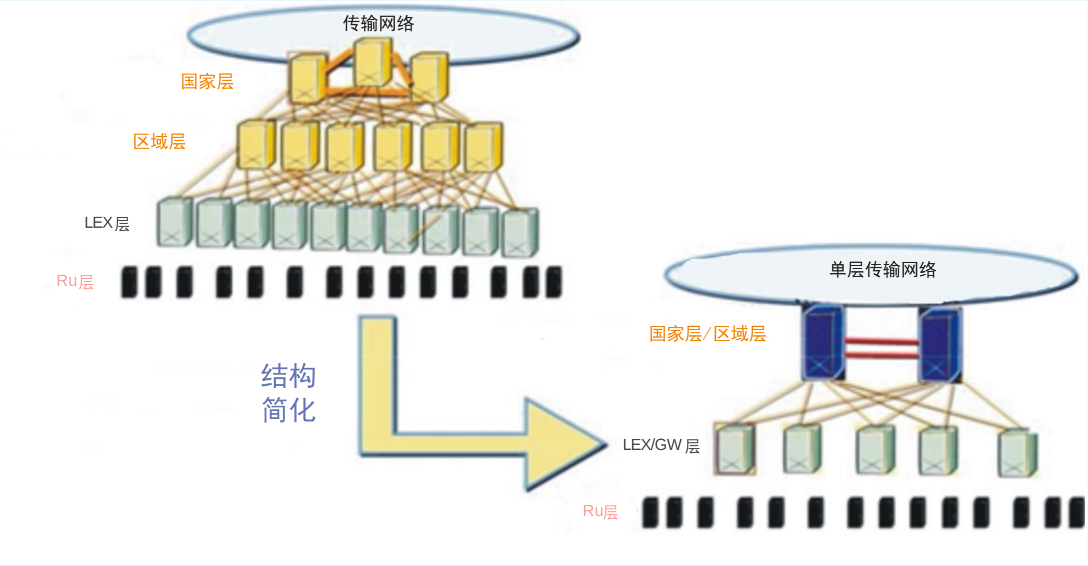
- 由于系统容量扩大，减少网络节点和链路（一个数量级）；
- 由于相同的用户位置，接入层面的结构相同；
- 由于安全，高容量节点和路径的拓扑连接更高；
- 所有高容量系统中在功能和物理层面要有高保护的水平和多样化的路径/来源。

考虑到上述原因，预计新的基础设施的构造结构应比现有基础设施更加简单。以下图1-3是这种预计的例子之一。

这种更为简单的架构除了解决传统电信基础设施中存在的问题外，还会带来许多好处。其中一个重要的好处是解决了接入网络中的主要问题：物理基础设施成本和部署时间。这个好处是通过比传统网络更短的本地环路长度获得的，为高带宽多媒体服务铺平了道路。

这种简单的架构允许在实施新的外部设备或改造现有设备时，使用xDSL和/或更靠近用户的光纤来实现宽带能力的快速部署。此外，这也将给为低密度用户引入新的无线技术提供灵活性。所有这些配备了固定和移动宽带能力的接入网络的增强功能，将为各种多媒体服务的供应，包括固定和移动融合的情况，提供非常灵活的方式。

图1-3：改进架构方面的方式



1.2 NGN 作为过渡途径

1.2.1 NGN 的特点

NGN的全称是“下一代网络”，因此这个名字本身并没有提供足够的信息来了解整体情况。好在ITU-T制定了明确的定义和各主要特点来更加详细地确定NGN，包括服务和功能方面。ITU-T Y.2001和Y.2011建议书为我们提供了在已达成全球共识的意义上的NGN的定义及其特点。

ITU-T Y.2001建议书确定了NGN的全球定义，如“能够提供电信业务并能够利用多宽带、启用QoS的传输技术的基于分组的网络，其服务相关功能独立于底层传输相关技术。它使用户能够不受限制地接入到网络以及相互竞争的服务提供商和/或他们所选择的服务。它支持通用移动性，能够为用户提供一致的和泛在的服务。”

此外，Y.2001建议书确定了NGN的如下基本特征：

- 基于分组的传输；
- 承载能力、呼叫/会话，和应用/服务之间的控制功能分离；
- 将服务提供从传输中的脱离，并提供开放接口；
- 基于服务构建模块（包括实时/流/非实时和多媒体服务）支持各种各样的服务，应用和机制；
- 带端到端 QoS（服务质量）的宽带能力；
- 通过开放接口与传统网络互联；
- 通用移动性；
- 用户可以不受限制地访问不同的服务提供商；
- 多种识别方案；
- 对于相同业务，用户感知统一的服务特性；
- 固定/移动之间的融合服务；
- 服务相关功能独立于底层传输技术；
- 支持多种最后一英里技术；
- 符合所有监管规定，例如关于应急通信、安全、隐私、合法拦截等。

根据NGN的定义和特点，得出NGN以下主要特点，这些应该是理解和使用NGN的一个框架：

- 开放式架构：开放支持服务创建，服务更新，和对由第三方提供的服务逻辑的包容，并且还支持“分布式控制”以及增强的安全性和保护。
- 独立提供：通过采用分布式、开放式控制机制，将提供服务的过程从网络运营中分离出来，以促进竞争。
- 多重性：NGN 功能架构应提供支持多种接入技术所需的配置灵活性。

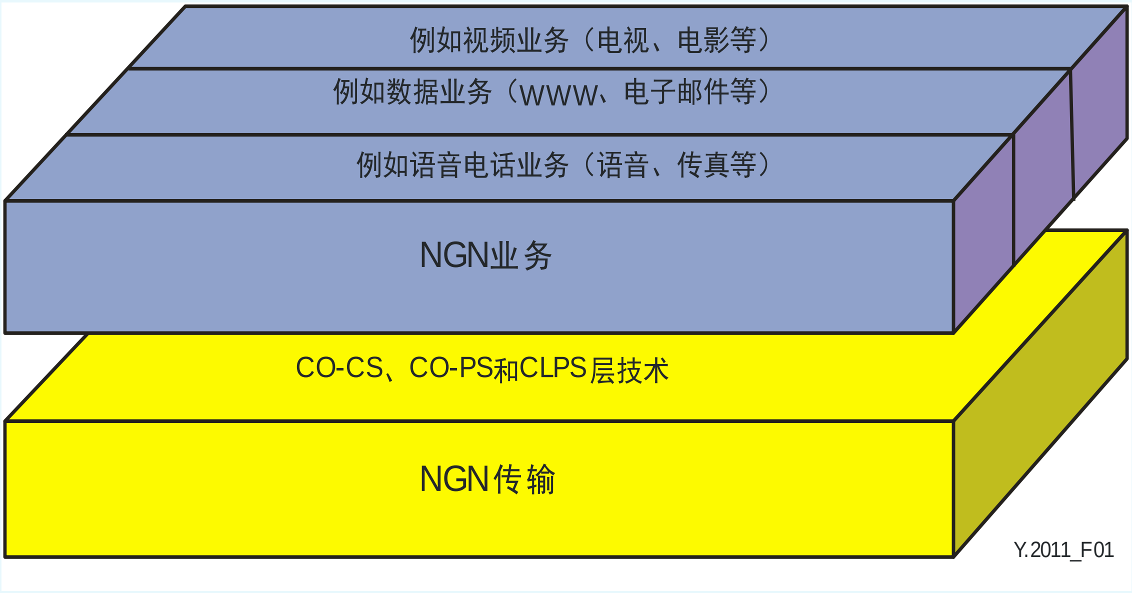
对这些从ITU-T定义的NGN定义和特点中得出的主要特点进行比较，人们认识到这些特点将为解决满足第1章中描述的业务趋势带来的困难提供一定的条件。

1.2.2 NGN 架构的基本参考模型

NGN的优点和最大挑战之一是服务与底层传输技术之间的分离。NGN的基本参考模型如图1-4（ITU-T Y.2011建议书）所示。该图显示服务从底层传输中分离时的特点。

一般情况下，任何和所有类型的网络技术可以部署在标识为“NGN传输”的传输层中，包括面向连接的电路交换（CO-CS），面向连接的分组交换（CO PS）和根据ITU T G.805和G.809建议书的无连接分组交换（CLPS）层技术。直到今日，IP被认为是用来支持NGN业务以及支持传统服务的首选的传输协议。“NGN服务”为用户提供如电话服务，Web服务之类的用户服务。因此，“NGN服务”可能涉及一套复杂的地理分布的服务平台，或者在简单的情况下，仅是两个终端用户网站之间的服务功能。

图1-4：(图1/Y.2011) NGN业务从传输中分离

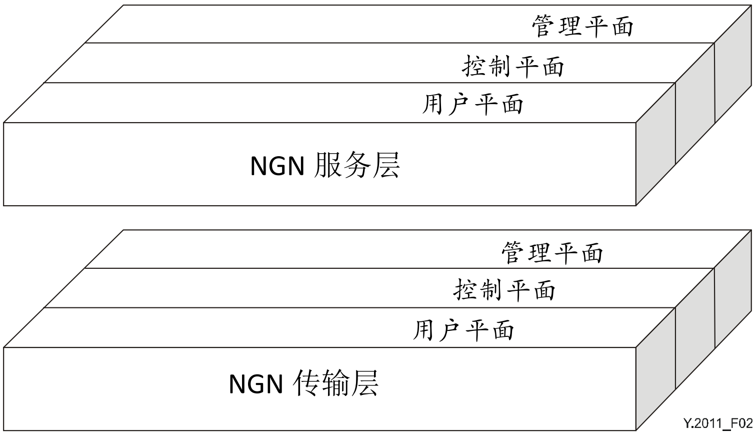

例如视频业务（电视、电影等）
例如数据业务（WWW、电子邮件等）
例如语音电话业务（语音、传真等）
NGN业务
CO-CS、CO-PS和CLPS层技术
NGN传输
Y.2011_F01

ITU-T Y.2011建议书用一段文字来确定这两个重要方面，分别以“NGN业务层”和“NGN传输层”的名字，如图1-5所示，并提供了以下概述来总体了解这两个方面：

- **NGN 业务层**：NGN 中为用户提供传输服务相关数据的功能和控制管理服务资源和网络服务的功能，以实现用户服务和应用的部分。用户服务可能通过业务层内多个服务层递归来实现。NGN 业务层关心的是应用及其在对等实体之间进行操作的服务。例如，服务可能与语音、数据或视频应用相关，单独排列或在多媒体应用的情况下，以某种组合排列。从架构的角度来看，业务层中的每一层被认为是有它自己的用户、控制和管理平面。

- **NGN 传输层**：NGN 中为用户提供传输数据功能和控制管理传输资源功能，以在终端实体之间承载数据的部分。如此承载的数据本身可以是用户，控制和/或管理信息。可以建立动态或静态的关联来控制和/或管理这种实体之间的信息传递。一个 NGN 传输层可以通过如 ITU-T G.805 和 G.809 建议书中所描述的多层网络的递归来实现。从构架的角度来看，传输层中的每一层都被认为是有它自己的用户、控制和管理平面。

图1-5：(图 2/Y.2011) NGN基本参考模型(NGN BRM)

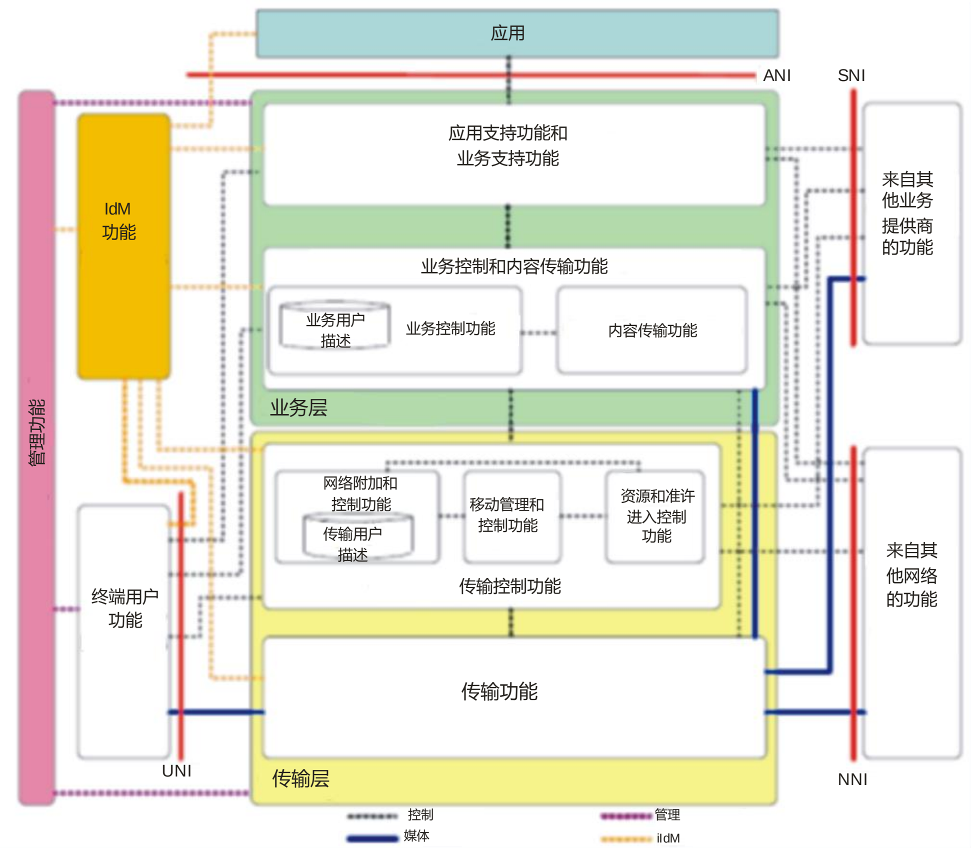


基于上述NGN的架构基本，ITU-T制定了具有详细功能的NGN架构模型，并在ITU-T Y.2012建议书中公布，如图1-6所示。

ITU-T Y.2012建议书中的NGN架构的制定饱含了以下原则：

- 支持多种接入技术：NGN 功能架构应提供支持多种接入技术所需要的配置灵活性。
- 分布式控制：这将能够实现对基于包网络的分布式处理性质的适用，并支持分布式计算的位置透明性。
- 开放控制：网络控制接口应是开放的，以支持服务创建、服务更新，和对由第三方提供的服务逻辑的包容。
- 独立服务提供：通过使用上述分布式、开放式控制机制，服务提供过程应从传输网络运营中分离。这是为了促进 NGN 发展的竞争环境，以加快提供多元化的 NGN 业务。
- 支持融合网络服务：这是产生灵活的，易于使用的多媒体服务所需的，通过发掘 NGN 的融合、固定-移动功能架构的技术潜力。
- 增强的安全性和保护：这是开放架构的基本原则。通过在相关层提供安全机制和存续能力来保护网络基础设施是至关重要的。
- 功能实体的特点：功能实体应包含以下原则：
  - 功能实体可能没有分布在多个物理单位，但可能会有多个实例。
  - 功能实体与分层架构没有直接关系。但是，类似的实体可位于不同的逻辑层。

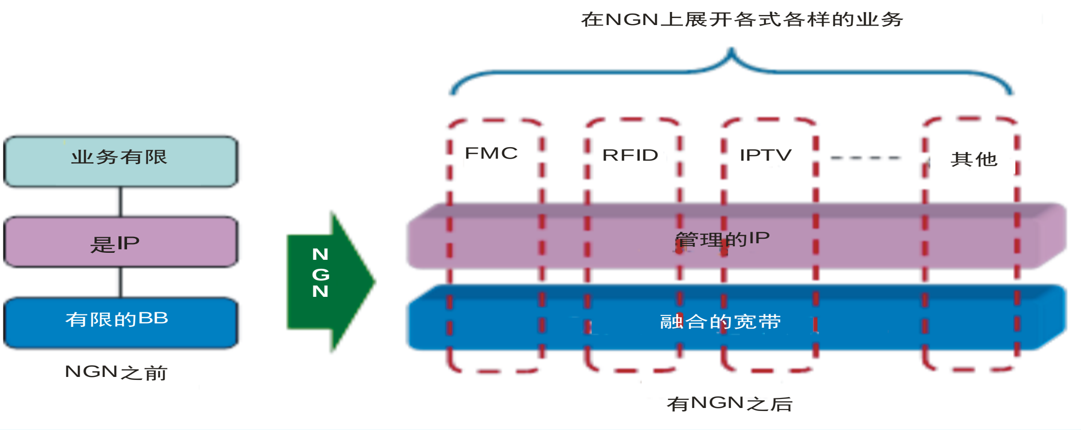
图1-6：(图7-1/2012) NGN架构概述



1.2.3 NGN 架构的好处

NGN架构的最大好处之一是支持在共同传输平台上提供各种服务的方式。固定和移动接入网络域上的各种宽带技术，将提供更多利用这个好处的机会，如在固定和移动融合传输网络上提供各种宽带业务和融合业务。图1-7显示了NGN架构将如何支持各种服务。

图1-7：NGN架构的好处



使用IP的优点之一是提供第3层和第4层之间的简单连接，在一般情况下，这是服务和传输之间的关键临界点。在NGN之前（如左侧图所示），IP只能提供一种被称为“尽力而为”的能力，不能支持足够的质量和安全性考虑。此外，底层传输一直依赖XDSL提供的非常有限的宽带容量，对满足业务趋势造成一定的限制。这种情况可能无法提供足够的平台来利用融合服务和业务。

NGN之后，具有融合宽带能力的IP（称为“可管理的IP”）和底层传输容量的扩大，将为在公共传输上支持各种业务（如IPTV、无线射频识别、FMC等）的同时保持3层和4层之间的简单链路提供一种方式。因此，这将带来不同的商业模式和市场参与者，鼓励多样化和灵活的业务关系。

1.2.4 NGN 应用的增强 IMS

IMS规范制定用于蜂窝接入网络，并基于对接入网络的一定假设，如可用带宽。不同类型的接入网络之间的本质差异将对IMS规范有实质影响。这种影响的例子是：

- 为支持基于 xDSL 的接入网络，IMS 可能还需要接口到 IP-CAN 的网络附着功能，以实现对位置信息访问。在基本 IMS 规范中不存在相应的接口。
- 要考虑对 IPv4 的支持，这会带来对支持 NAPT 功能的要求。这里至少有两个原因：
  - 一些运营商已经（或将要）面临 IPv4 地址短缺问题。
  - 媒体流 IP 地址隐私不能像 IPv6 的情况那样，依靠于 RFC 3041（IPv6 无状态地址自动配置的隐私扩展）。NAPT 提供了隐藏终端地址的另一种方法。

支持NAPT功能包含在NGN功能架构中。IMS规范中需要提供IMS的扩展，以处理包含NAPT的配置。

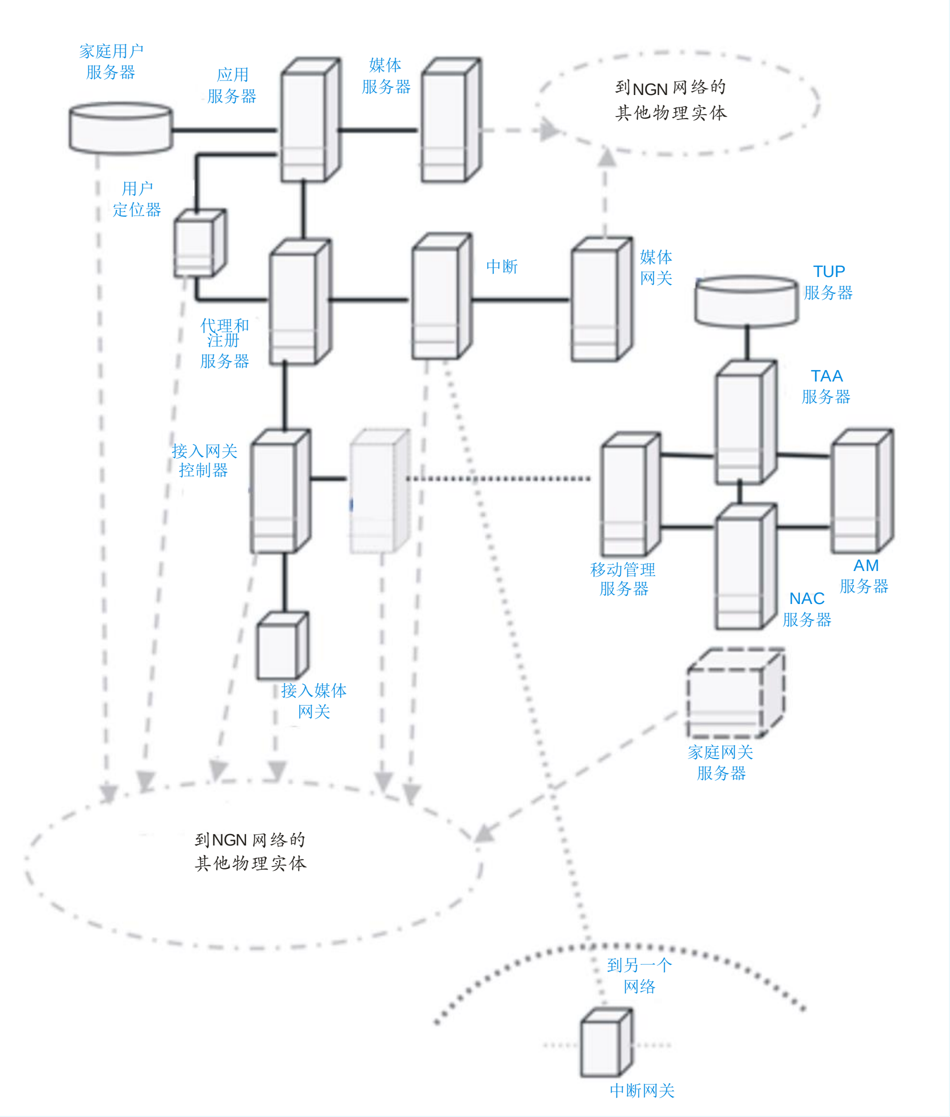
- 放宽带宽稀缺的限制，可能会导致考虑将目前被认为是强制性的一些功能变为可选支持的（例如 SIP 压缩）。
- 位置管理的差异将影响到传送这一信息的各种协议，无论是在信令接口还是在充电接口。
- 接入网络中资源预留程序的差异将要求改变 IMS 资源授权和预留程序，因为 xDSL 接入网络的资源预留程序将通过网络实体（在基于 SIP 服务的情况下，即 P-CSCF）来代表最终用户终端发起。

各个标准组织正在研究上述这些扩展，以支持NGN中IMS的使用。

1.2.5 NGN 的物理架构

NGN的物理架构确定了广义NGN的功能架构中对应的功能实体或一组功能实体的物理实体。通过物理架构，可以确定物理实体之间的互操作点，以实现NGN网络中不同的物理实体之间的互操作性。一个可能的NGN物理架构实现如图1-7所示：

图1-8：NGN可能采用的物理架构



1.3 向 NGN 过渡的方式

1.3.1 向 NGN 过渡的考虑

在制定向新的基础设施过渡的计划时，要仔细研究许多看法和考虑，因为这将影响到相关实体以及社区的许多方面。如 PSTN/ISDN 之类的传统网络基础设施向 NGN 过渡也将对整个通信基础设施产生巨大的影响。

为了跟上技术发展和市场预期，需要对系统进行定期升级或用新技术来更替系统，同时又不妨碍该服务。更替和升级现有设备到更新更先进的技术，不仅是提供新服务的要求，而且往往时间都花在从制造商获得硬件和软件支持。制造商通常进行这些改进以配合技术过渡，过时的设备必须更换为更高效、紧凑和可靠的设备，并希望其为用户提供更优质的服务。

特别是在农村偏远地区的业务扩展，向 NGN 的过渡最好不是间断性的，老的和新的技术应该共存一段合理时间。从消费者的角度，不能因为他们的服务提供商已经将自己的系统“升级”到 NGN 就强迫他们更换终端设备。

考虑到这些，ITU-T Y.2261 建议书为运营商建立过渡计划时提供指导。

对于PSTN/ISDN向NGN的过渡，要考虑以下所确定的方面。

1.3.1.1 信令和控制

PSTN/ISDN 使用诸如模拟线路信令，如信令系统 R1 [Q.310-Q.332]、R2 [Q.400-Q.490]的信道相关信令（CAS），如 SS7 或 DSS1[Q.931]的公共信道信令（CCS）之类的信令系统。所有这些信令系统都是用于电路交换网络的。由于 NGN 运输是基于分组的（呼叫与承载是分离的），可能需要其他合适类型的信令（如 BICC，SIP-I [Q.1912.5]等）。此外，信令功能和呼叫控制功能可以位于多个 NGN 组件中。

由于 NGN 需要与 PSTN/ISDN 和其他网络共同工作，NGN 信令系统和传统网络的信令系统之间的互通是必需的。下一代企业网络内的信令方面应与 NGN 接入或核心网络的信令保持独立。

据进一步预计，接入和核心网的信令方面是独立的，为分步向NGN过渡的方法提供了可能性。

1.3.1.2 管理

NGN 管理系统是由 3 个平面组成，即网络管理平面，网络控制平面和业务管理平面。三个平面中的每一个都实现 NGN 分层模型中的每一层对应的管理功能。

PSTN/ISDN管理（即操作，行政及管理）系统的过渡需要支持PSTN/ISDN通过中间阶段向NGN过渡的能力。

1.3.1.3 服务

通过传统 PSTN/ISDN 交换机提供的 PSTN/ISDN 服务可以通过 NGN 中的应用服务器（AS）来提供。预计部分或全部传统服务将通过 NGN 提供。由于 PSTN 业务的语音质量被认为是“最好的”，任何从这个“最好”的服务过渡到基于 IP 的 NGN 需要保证其服务可与那些传统 5 级（或 TDM）基础设施所提供的相媲美。

然而，无法保证所有的服务可通过 PSTN/ISDN 模拟来提供。

为了支持现有服务，预计要使用通过调适到NGN的传统终端。

- 承载业务：在从 PSTN/ISDN 向 NGN 过渡的同时，应提供承载业务的连续性。使用 NGN 来连接 PSTN/ISDN 对于所有承载服务应是透明。NGN 应提供具有相同的或更好的服务质量的 PSTN/ISDN 承载服务。
  - PSTN/ISDN 仿真提供与现有的 PSTN/ISDN 承载业务相似但不完全相同的功能。
  - PSTN/ISDN 仿真应能够提供 PSTN/ISDN 所提供的所有承载服务。然而，没有要求 NGN 支持国际电联 T I.230 系列建议书中所确定的所有 N-ISDN 承载服务。

- 补充服务：在从 PSTN/ISDN 向 NGN 过渡的同时，应在实用程度上提供补充业务的连续性。PSTN/ISDN 仿真应提供对 PSTN/ISDN 提供的所有补充服务的支持，同时 PSTN/ISDN 仿真提供与现有 PSTN/ISDN 服务相似但不完全相同的功能。NGN 不需要支持 ITU-Ti.250 系列建议书中确定的所有 ISDN 补充业务。NGN 在用于连接 PSTN/ISDN 网络之间的补充服务时应看上去是透明的。

- 操作，管理和维护（OAM）：OAM 功能是用来验证网络性能，通过尽可能减少服务中断、服务质量下降和操作的停机时间来降低运营。作为最低要求，在进行 PSTN/ISDN 向 NGN 过渡时，应提供检测如丢失、错误或误插入包之类的故障、缺陷和失败的能力。此外，应该有机制来指示连接状态，并为性能监控提供支持。

- 命名、编号和寻址：根据 ITU-T Y.2001 建议书，NGN 命名、编号和寻址机制应能够与现有的 E.164 编号方案互通。在从 PSTN/ISDN 向 NGN 过渡的过程中，应确保国际电联成员国在国家代码编号、命名、寻址和识别计划方面的主权得到充分的维护。此外，作为最低要求，还应该支持互联网 IP 寻址方案，其中包括 E.164 电话统一资源标识符（TEL URI），例如，电话：+98 765 4321 和/或 SIP 统一资源标识符（SIP URI），例如，SIP：my.name@company.org。

- 结算，收费和计费：在过渡期内，可能需要在可用的程度上维持现有的结算，收费和计费程序。从现有网络向 NGN 过渡也将意味着替换现有的结算数据生成来源。NGN 应支持离线和在线收费。

- 互通：互通用于表达网络之间、终端系统之间，或部件之间的相互作用，其目的是提供能够支持端到端通信的功能性实体。PSTN/ISDN 向 NGN 过渡应考虑以下问题：

  – 与传统的网络，如 PSTN/ISDN 和互联网互通的能力

  – 基于 IMS 的或基于呼叫服务器的网络互通的能力；

  – 域间，区域间或以太网互通的能力；

  – 支持身份验证和授权；

  – 执行呼叫许可控制的能力；

  – 支持[Y.1541]中定义的网络性能参数的能力；

  – 支持结算、收费和计费。

- 呼叫路由：当 NGN 与 PSTN/ISDN 共存时，路由方案应使运营商能够控制他们的流量进入和离开 NGN。这将使得运营商有可能优化他们的网络资源的使用，以避免 NGN 和 PSTN/ISDN 之间沿介质路径的多点互通。

- 国家监管机构的服务要求：国家/地区的法规或法律要求中作出以下要求，这意味着 NGN 服务提供商在互通的情况下应提供：

  – 具有与现有 PSTN / ISDN 相同或更好的质量和可用性的基本电话服务；

  – 精确结算和计费能力；

  – 精确结算和计费能力；

– 提供 PSTN/ISDN 和 NGN 用户的电话号码查询服务；

– 支持应急通信；

– 对所有用户的支持，包括残疾人。应提供至少与现有 PSTN/ISDN 相同的功能的支持。NGN 为更高级的支持提供了机会，如文本到语音的网络能力；

– 支持合法拦截和监控电信语音、数据、视频、电子邮件、短信等各种媒体类型的机制。这种机制可能要求网络提供商提供对电信内容（CT）的访问，并由执法机构（LEA）拦截相关信息（IRI），以满足主管部门和国际条约的要求；

– NGN 和其他网络，如 PSTN/ISDN 和 PLMN 之间的互操作性。

1.3.2 总体过渡程序

从一个到另一个过渡并不是件容易或简单的任务，因为很多东西都涉及不同的方面。特别是网络基础设施的过渡需要非常周密的计划，研究各个方面。总之，没有一个统一的或最佳的向NGN过渡的方式，因为过渡应根据每个国家的情况，以及各运营商给定的条件。

在制定传统网络向NGN基础设施过渡的计划时，建议考虑以下步骤：

1 除了现有网络外，向宽带用户提供新的通信服务。

2 很大一部分用户转移到这些服务。真正的 PSTN/ISDN 使用量的减少显现出来。

3 保持两个系统并行的成本成为一个重要因素。**决定开始更换基础设施**。

4 用新的基础设施替换部分基础设施（如本地交换机），**无需强制要求所有用户过渡**。

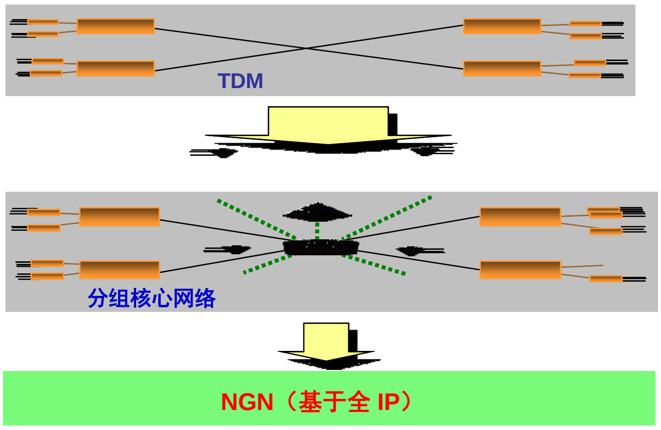
5 完全改变到新的基础设施。

6 其余用户过渡到 NGN。

1.3.3 过渡的总体方式

过渡的结果应成为“全IP环境”，这是一个关键的NGN技术，因此从技术的角度，过渡应该被解释为从“基于TDM”到“基于IP”的变化。考虑到每个国家在“接入网络域”和“核心网络域”之间的组成部分，过渡过程应首先应用到其中一个域。通常的理解是制定“核心网络域”的过渡计划更容易一些。核心过渡比“接入网络域”的过渡对服务提供的影响更小。图1-9显示了核心网络向NGN过渡的总体描述。

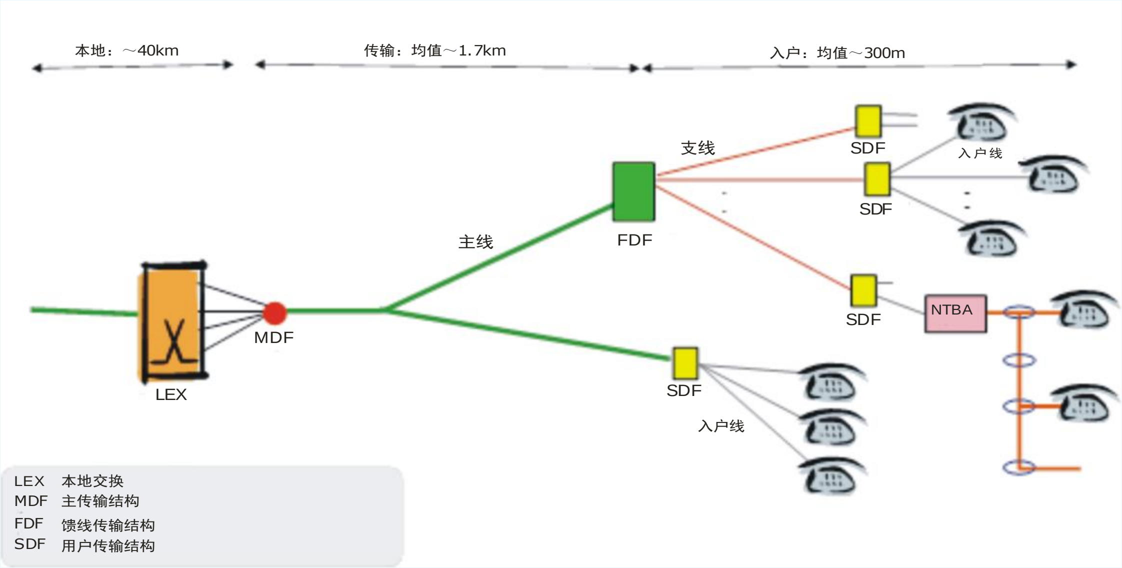
图1-9：核心网络向NGN过渡的总体描述



接入网络域的情况相当复杂，不仅是技术方面，而且在地域差异上，不建议选择一个特定的技术来替代任何传统接入网络系统。而是建议考虑不同技术之间的协调，以更为灵活和经济的方式来满足用户的要求。许多不同的接入技术是利用支持宽带的固定和移动连接开发的。大多数技术还提供了IP连接，这是满足NGN要求的关键技术功能（如基于分组的传输）。

对于固定接入网络的情况，如今xDSL技术主要用于提供宽带。固定网络中的最终目标是要部署基于光纤的基础设施。xDSL提供了尽可能利用现有的基于铜缆的接入基础设施，以经济的方式部署宽带基础设施的可能性，但其容量有限（最大几十Mbps）。光纤是固定网络领域的一种目标技术，其具有的无限容量，不仅是对于核心网络，但有接入网络，包括家庭网络。唯一的考虑是相关的成本和施工难度。这两个问题将要面临技术的快速发展。因此，建议在接入网络同时使用xDSL和光纤，作为向NGN过渡的准备，包括准备足够的宽带容量。图1-10显示了考虑到地理距离，如何建设接入网络的一个例子。

图1-10：接入网络（固定）向NGN过渡的总体描述



另一个重要领域应该是利用移动技术（包括无线WiFi和WiMAX等）来提供宽带连接。这方面也是非常重要的，因为许多人，尤其是在发展中地区，使用手机作为他们的生活通信，移动将为人们提供移动性。有很多的技术可以为移动接入网络包括IP连接，提供宽带容量，但在提供带宽方面仍然有一定限制（大约为10 Mbps）。各标准组织都在努力开发新技术以提供更好的带宽，但这需要时间。下图1-11显示了如何在接入网络中使用不同的移动通信技术，图1-12显示了移动和固定之间混合的图。

图1-11：不同移动接入结构的应用

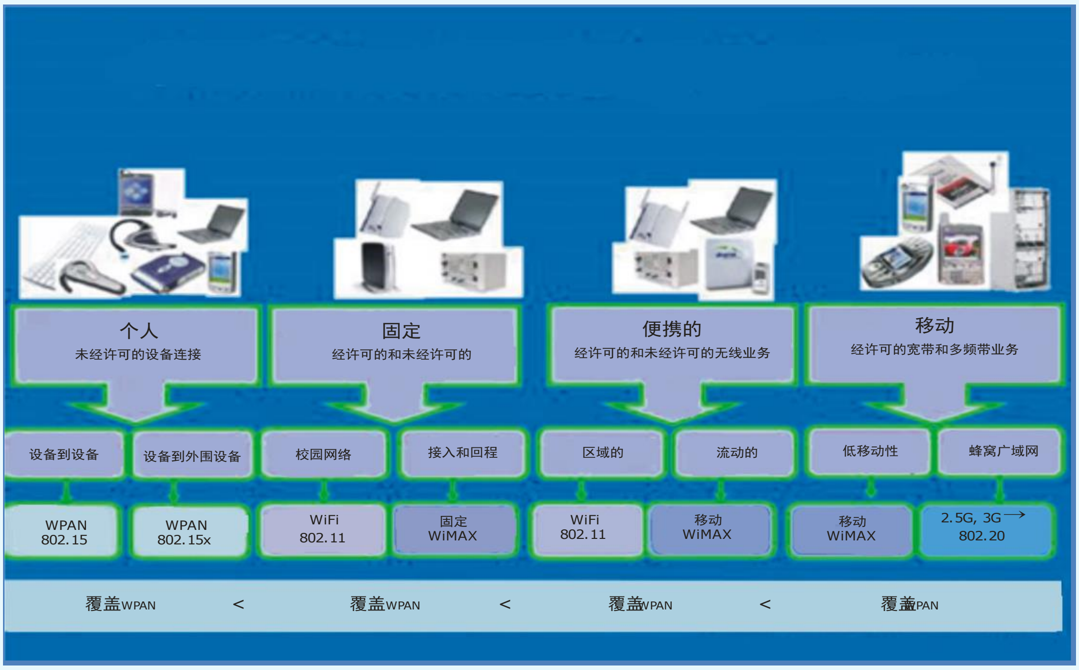
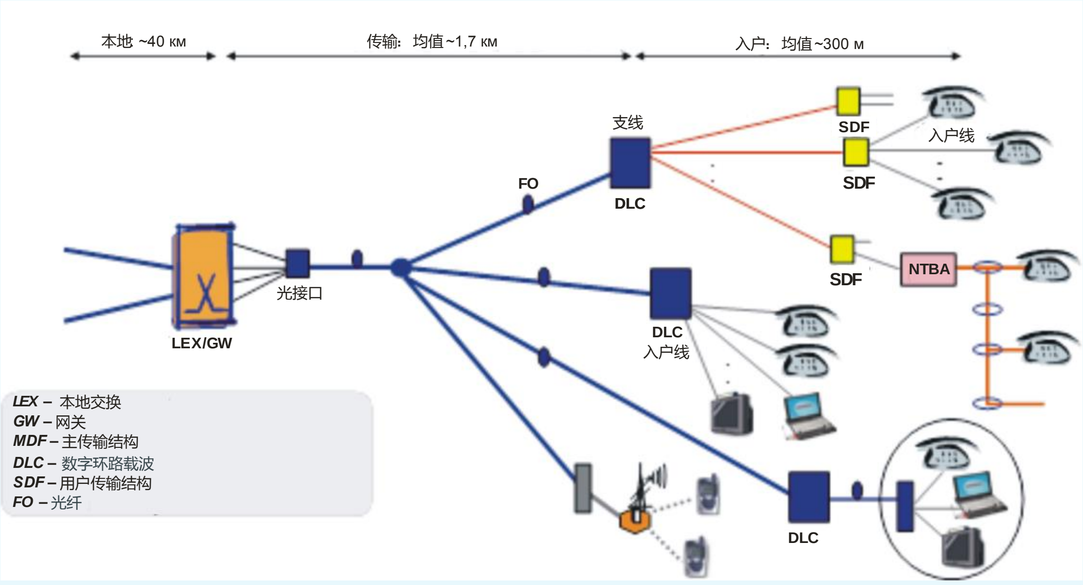


图1-12：接入网络（混合）向NGN过渡的总体描述



1.3.4 支持过渡的 NGN 技术

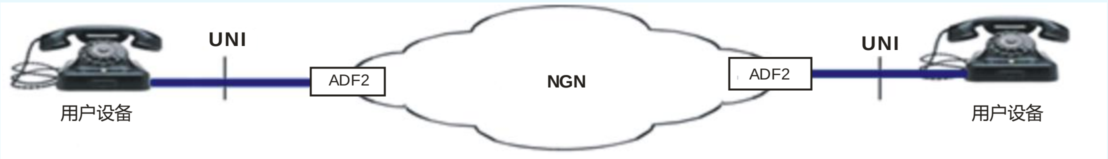
为帮助传统网络，至少是基于语音的服务向NGN过渡，NGN提供了两种功能。其中一种是“仿真”，它支持提供PSTN/ISDN服务的能力和适用于使用IP的NGN基础设施的接口。另一种是“模拟”，它使用在IP接口和基础设施上的进程控制，支持提供类似PSTN/ISDN服务的能力。

1.3.4.1 仿真场景

下图1-13显示了对仿真场景高层面的描述。使用提供“适配功能（ADF）”的NGN仿真能力，如黑手机之类的传统终端设备连接到NGN网络，使用以下几个方面的服务：

- 封装处理。
- PSTN/ISDN 用户可用的所有服务。
- 用户体验不会因网络改造而改变。

图1-13：PSTN/ISDN的NGN模拟



1.3.4.2 模拟场景

模拟用于向 NGN 用户提供 PSTN/ISDN 类似服务。因此，NGN 用户将使用这种仿真功能与 PSTN/ISDN 用户通信。NGN 模拟的主要特点总结如下：

- PSTN/ISDN 类的服务。
- 可以使用可能的新服务。
- 用户体验会因网络改造而改变。

图1-14：PSTN/ISDN的NGN模拟图-1

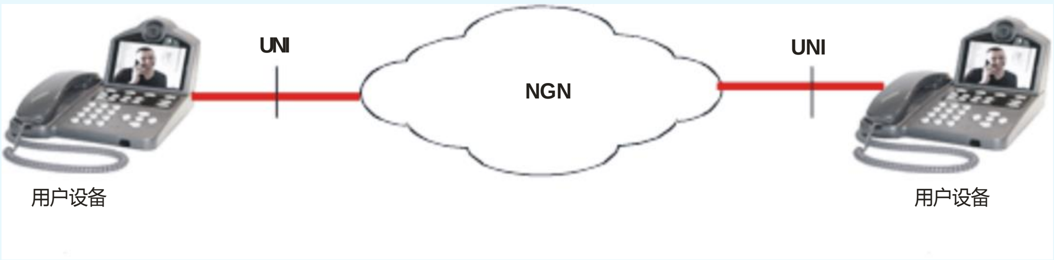
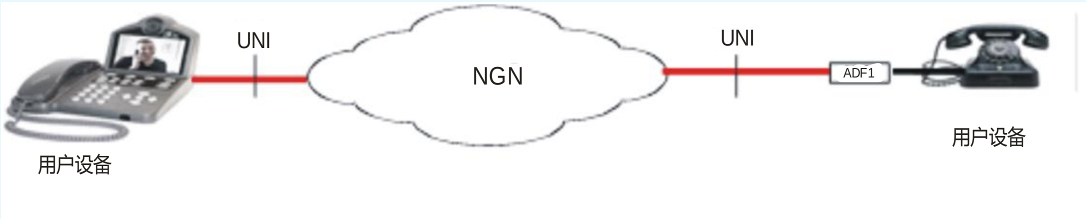


图1-15：PSTN/ISDN的NGN模拟图-2



1.3.4.3 使用仿真和模拟的互通

考虑到语音服务的重要性，面向 NGN 语音的服务应与 PSTN/ISDN 环境中的语音服务相连。为了支持这一要求，仿真和模拟要共同用于 NGN 和 PSTN/ISDN 等传统网络之间的互通。将根据互通情况来决定何种技术将被用于哪个区域。

图 1-16 显示了 NGN 与传统 PSTN/ISDN 之间互通的一个例子。NGN 侧使用仿真，同时与传统侧互通使用模拟。在这种情况下，服务功能的特点如下：

- 服务需要在 NGN 和 PSTN/ISDN 之间互通；
- 只能使用 PSTN/ISDN 类的服务；
- 对于端到端的连接无法满足传统终端的用户体验。

图1-16：NGN仿真与模拟之间的互联-1

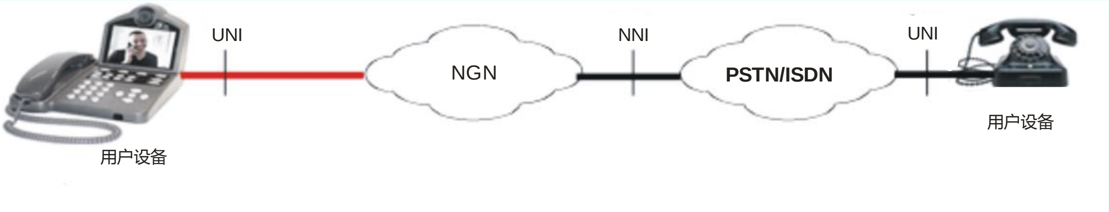
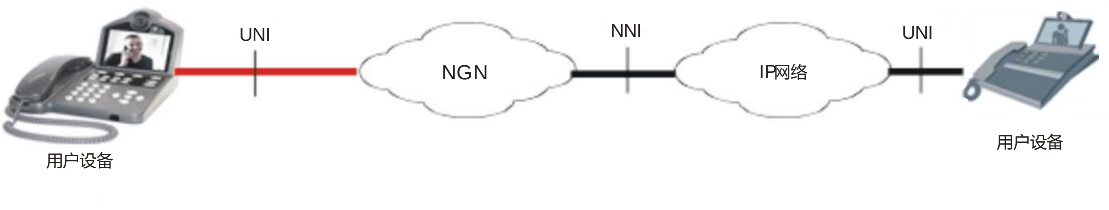


图 1-17 显示了 NGN 和支持语音服务（如 VoIP）的传统基于 IP 的网络之间互通的另一个例子。NGN 侧使用了仿真，同时与传统侧互通使用模拟。在这种情况下，服务功能的特点如下：

- 要求 NGN 和 IP 网络之间的服务互通；
- 端到端的连接可能无法满足 NGN 和 IP 网络的用户体验。

图1-17：NGN仿真与模拟之间的互联-2

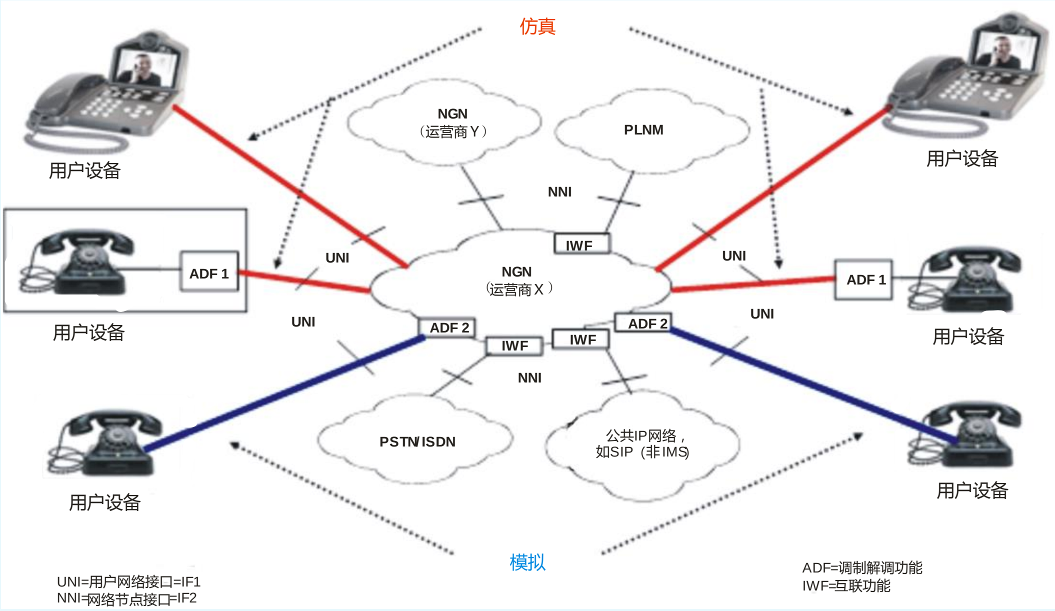


1.3.4.4 利用仿真和模拟做出的总配置

仿真与仿真技术的重点要求是支持面向语音的服务。如今PSTN/ISDN是支持语音服务，包括在ISDN情况下各种各样的补充服务的主要网络基础设施。此外，越来越多的终端用户在传统IP环境中使用语音服务。

因此，NGN应支持语音相关功能，如覆盖PSTN/ISDN和基于传统的IP网络的仿真和模拟。因此，结合这些功能与适当的互通方案将有助于支持在终端用户设备连接到固定、移动和传统基于IP网络情况下的终端用户语音业务要求，无论终端用户身在何处都能够覆盖到语音服务。下图1-18显示了使用仿真和模拟的总体配置模型，并指出了混合互通的情况。

图1-18：使用NGN仿真与模拟的总体描述



UNI=用户网络接口=IF1
NNI=网络节点接口=IF2

ADF=调制解调功能
IWF=互联功能

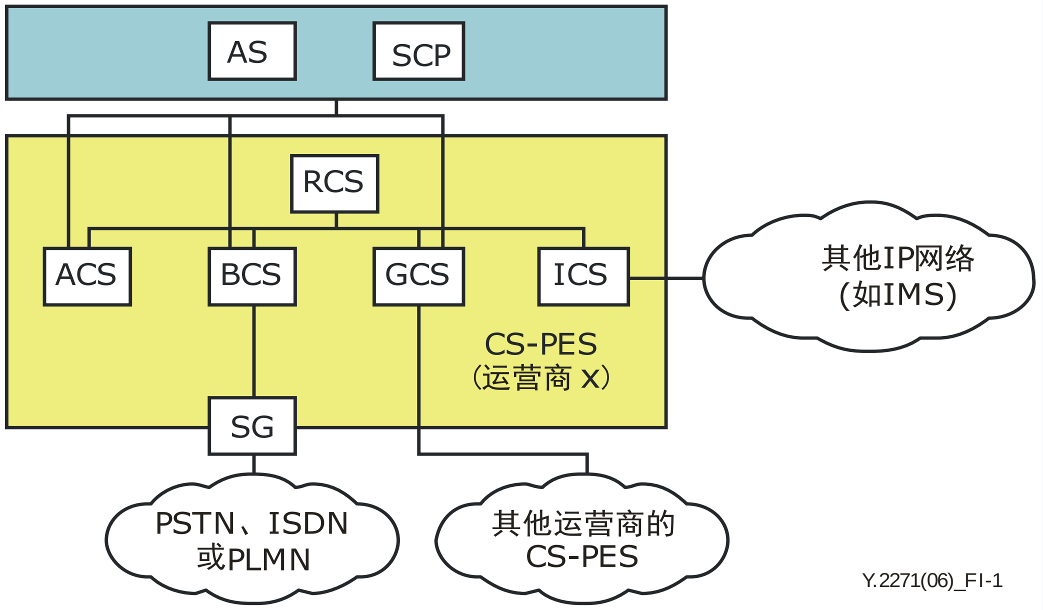
1.3.4.5 支持向 NGN 过渡的呼叫服务器

呼叫服务器是 PSTN/ISDN 仿真的核心要素，负责呼叫控制、网关控制、媒体资源控制、路由、用户配置文件和用户认证、授权和结算。呼叫服务器可提供 PSTN/ISDN 的基本业务和补充服务，并可能通过与外部服务控制点（SCP）和/或在服务/应用层中的应用服务器的服务交互来提供增值服务。

呼叫服务器可以执行ITU-T建议书Y.2271中确定的以下一个或多个功能，图1-19显示了一个示例部署：

- 接入呼叫服务器（ACS）– 实现接入网关控制和媒体资源控制功能，从而提供 PSTN/ISDN 的基本业务和补充服务；
- 出口呼叫服务器（BCS）– 履行互通职能，实现与 PSTN/ISDN 网络的互连；
- IMS 呼叫服务器（ICS）– 提供单一 NGN 域内的 PSTN/ISDN 仿真组件和 IP 多媒体组件之间的互操作性；
- 网关呼叫服务器（GCS）– 提供来自各个业务提供者的不同 NGN 域之间的互操作性；
- 路由呼叫服务器（RCS）– 提供呼叫服务器之间的路由功能。

图1-19：(图 1/Y.2271) 呼叫服务器部署实例

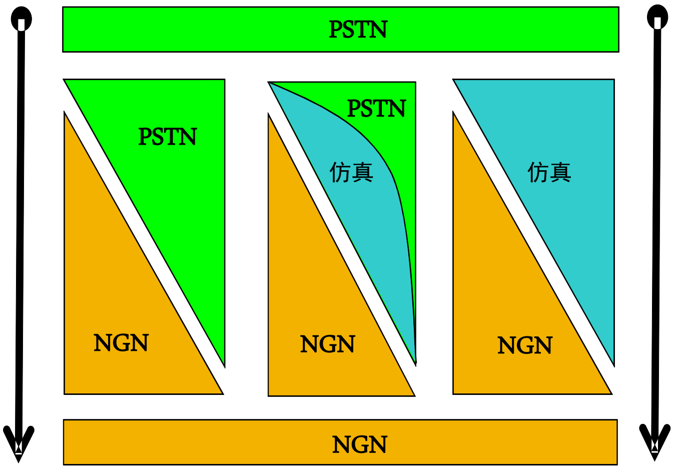


* AS：应用服务器；SCP：服务控制点；SG：信令网关；PES：PSTN仿真服务部分。

1.4 过渡情景

使用NGN的仿真和/或模拟组件可以有各种方式从原有的网络过渡到NGN，视各国或各提供商的情景而定。本报告中介绍了三种不同类型的过渡场景，可作为提纲挈领式的考虑，但并不排除有其他的可能性。下图1-20通过图画的形式解释了从PSTN/ISDN向NGN过渡的三种类型。

图1-20：总体过渡情况



三个情景如下：

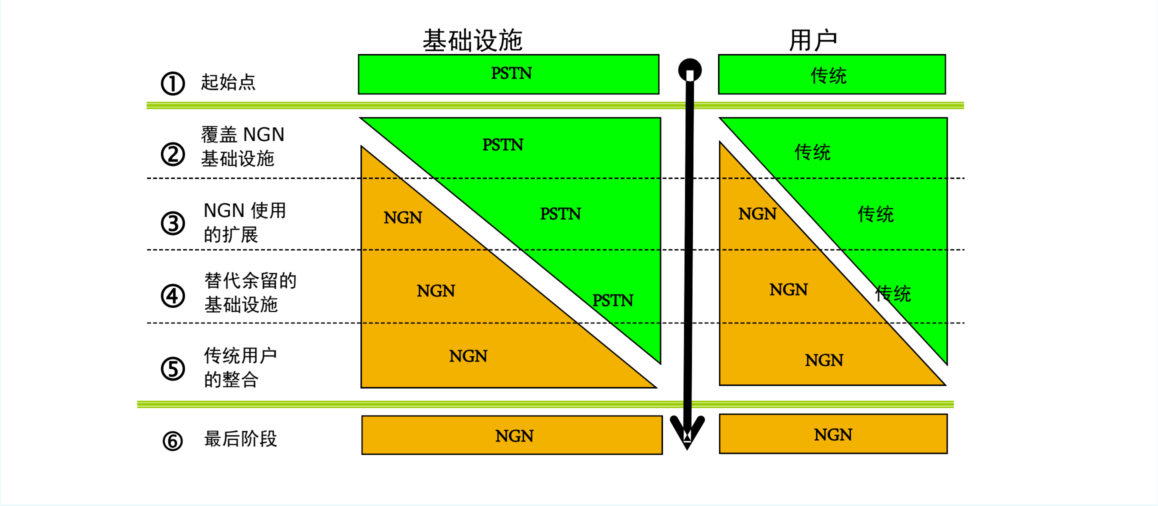
- 叠加情景（图 1-20 左侧）：NGN 与 PSTN/ISDN 共同部署并运营。NGN 将逐渐占领更多的份额，而 PSTN/ISDN 的份额逐渐减少，最终演进到 NGN。
- 替换情景（图 1-20 右侧）：广泛使用 NGN 仿真组件支持面向话音的业务，但是保留原有的终端，如黑电话。这样最终用户不会意识到在其终端背后所发生的技术变化。
- 混合情景（图 1-20 中间）：这一场景中同时使用了叠加和仿真，这样最初某些 PSTN 用户连接可以由 NGN 仿真组件替换，而其他 PSTN 用户可以保留其 PSTN 连接。随着 NGN 部署、仿真的增多，PSTN 用户将被 NGN 用户取代。

1.4.1 叠加情景

国家或运营商没有足够的 PSTN/ISDN 的基础设施，那里已经是缺乏连接，以支持语音服务的情况下，这种情况将是有益的。在这种情况下，这是很难继续 PSTN/ISDN 设备的部署，因为这也将需要新的投资，同时为 NGN 的投资也将是必要的。但是，在这种情况下，即使使用当前用户的 PSTN/ISDN 将继续支持他们的终端没有任何变化，如果可能的话。

通过这种情况下，运营商将停止其部署的 PSTN/ISDN，但取代向 NGN 的投资。然后，操作员将提供自动进稿器（适配功能），到目前的 PSTN/ISDN 用户的语音服务提供连续的使用，表示 NGN 仿真功能的扩展，如图 1-22 所示。根据越来越多的用户希望使用先进的功能，那么运营商将扩大 NGN 的覆盖面和因此将减少谁使用仿真服务的客户。终于有一天，所有用户都将被完全覆盖 NGN 能力。下图 1-21 显示了此方案的步骤。

图1-21：覆盖过渡的情况

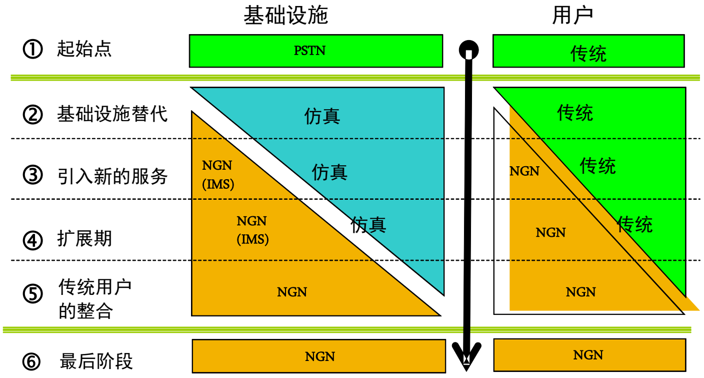


1.4.2 基础设施替换情景

在某国或某个运营商不具备足够的 PSTN/ISDN 基础设施、缺乏支持话音业务的连接的情形下，这一场景是有效的。在此情形下，很难继续部署 PSTN/ISDN 设备，因为此举需要新的投资，而 NGN 的投资也是必不可少。但是在此情形下，当前用户即使使用 PSTN/ISDN，亦可继续获得服务支持而无需改变所用的终端。

通过实施这一场景，运营商可以不再部署 PSTN/ISDN，转而投资 NGN。运营商将向当前的 PSTN/ISDN 用户提供 ADF（适配功能），使他们可以继续使用话音业务，这就意味着 NGN 仿真能力的扩大，见图 1-22。随着越来越多的用户希望使用先进的业务功能，运营商可以扩大 NGN 的覆盖范围，从而减少使用仿真业务的用户。最终 NGN 的业务功能将覆盖所有用户。此场景的几个步骤见下图 1-22。

图1-22：基础设施替代过渡的情况

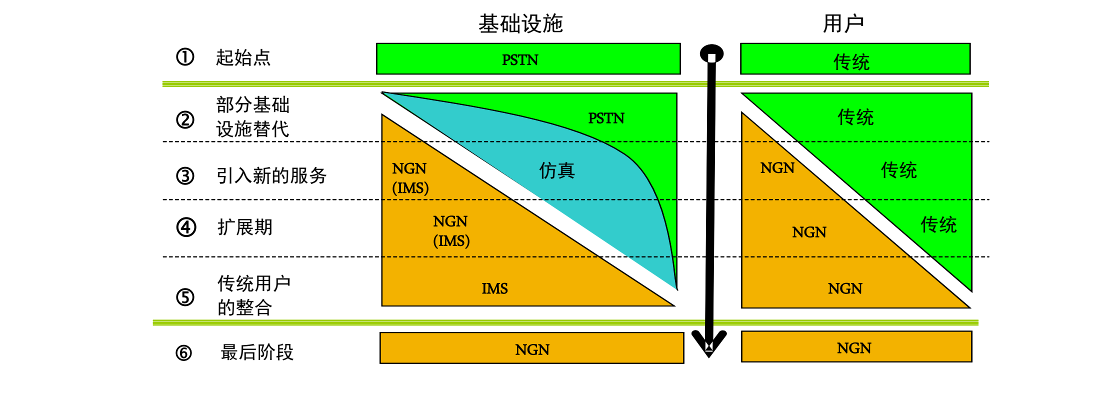


1.4.3 混合场景

当某国或某个运营商处于网络发展的中间阶段时，即，PSTN/ISDN 的某些部分需要替换，但其他部分因为使用的是新的 PSTN/ISDN 基础设施所以仍处在良好且稳定的状态下，这一场景是有效的。在此情形下，既应考虑叠加场景又应考虑替换场景。运营商应维持对有关用户的 PSTN/ISDN 网络，直至获得投资回报，或直至 PSTN/ISDN 的状态需要付出重大的成本进行运营、管理和维护包括故障管理，此时即为替换之时。另一方面，运营商同时着手部署 NGN 基础设施来替换那些已该替换的 PSTN/ISDN 部件。此场景的几个步骤见下图 1-23。

通过实施这一场景，运营商将逐渐积累足够的资源进行下一步新的投资，同时维持了 PSTN/ISDN 的用户服务。此外，运营商还可以通过新部署的 NGN 满足用户使用先进业务功能的要求。随着越来越多的用户希望使用先进的业务功能，运营商可以扩大 NGN 的覆盖范围，从而减少原有网络的客户。最终解决方案就是 NGN 将得到全面部署，覆盖所有用户。

图1-23：混合过渡的情况



2 用于 NGN 过渡的技术发展

过去10年或者更长的时间已经见证了信息和通信日益快速地整合，包括设备和网络，某种程度上由于移动电话的日益普及和业务由电话网络转移到公众互联网，传统的公众网络运营商已经看到了其公共交换电信网络中话务量在减少。

在过去的几年中，新的综合宽带网络的概念已经得到发展，被称为“下一代网络：NGN”。

由网络运营商面临的问题就能确定NGN的基本特性：需要通过宽带接入提供服务（以增加收入）；需要合并各种网络业务-数据（网页浏览）、音频、电话、多媒体和新兴“受欢迎的”互联网业务例如即时消息、网真和广播类型业务；客户需要能够从任何地方（固有的移动性）接入他们的业务。下一代业务所需要的不是一个提供特定解决方案的网络（例如PSTN），而是一系列能够支持服务提供灵活平台的网络。

2.1 业务方面

了解业务需求应该是所有电信发展的第一步，就此而言，确定媒体特性应是确定业务的最初阶段，随着处理器的发展提高处理能力，以及半导体技术实现足以安装在板上的小型化，产生了以不同方式使用各种多媒体的需求，这就需要在任何固定或移动情况下的宽带连接。

表2-1所示的是带宽和QoS方面的媒体要求的高度抽象化视图，除一般语音以外的许多业务都需要至少2 Mb/s的带宽和确保满足QoS要求的高优先级处理。为支持这种业务趋势，网络必须具有足以进行业务（如会议、流量等）管理等能力，无论提供的宽带连接过多还是恰到好处。下一代网络提供了一个在运营商级妥善满足这些需求的途径。

表2-1：媒体业务要求

业务	带宽（下行链路）	QoS要求
广播电视 (MPEG-2)	2 至 6 Mb/s	参数化
高清电视 (MPEG-4)	6 至 12 Mb/s	参数化
PPV 或 NVoD	2 至 6 Mb/s	按优先排序
VoD	2 至 6 Mb/s	按优先排序
画中画 (MPEG-2)	高达 12 Mb/s	参数化的
PVR	2 至 6 Mb/s	按优先排序
交互式 TV	高达 3 Mb/s	尽力而为
高速互连网	3 至 10 Mb/s	尽力而为
视频会议	300 至 750 Kb/s	按优先排序
语音/可视电话	64 至 750 Kb/s	按优先排序

2.2 接入传输技术

正如前面所述，支持不同类型的多媒体需要网络具有足够的带宽和流量管理能力，确保必要的带宽是满足这些业务（和媒体）要求的第一步。提供带宽有两种形式：固定和移动。

移动网络仍在持续发展，具有移动性优势的移动接入，是商务人士和学生等游牧用户不可或缺的接入方式，使他们无论在静止或移动中都能使用连接。

近几年，对于用于无线通信应用的57至134 GHz之间的频率范围的关注已显著地增加，由于其可能用于较宽带宽的设备，这些设备可满足正在增长的对于数百Mbit/s范围内高速数据应用的需求，包括最后一英里连接。可以预期各种短距离链路配置会在这些波段，包括高密度应用。

目前是可以使用60/70/80/95 GHz波段的无线解决方案的，但系统成本还不能与较低频率的技术进行竞争，这些频率上的设计挑战仍然存在，对于将要与较低频率的那些系统进行竞争的60/70/80/95/120 GHz波段范围的系统，所部署系统的容量必须很大。

60/70/80/95/120 GHz波段内非常高的工作频率允许设计具有定向波束的小尺寸高增益天线，因此，对于距离很近的通信设备，可以将实际的天线设计成能构成具有最小干扰的小型无线网状网。

可能受益于60/70/80/95/120 GHz波段的室外/室内应用例子包括：

- 无线局域网（WLAN）和无线个人区域网（WPAN）；
- 微蜂窝和频率复用体系结构，例如：用于移动的固定链路；
- 高分辨率游牧多媒体业务；
- 无线视频分发系统；
- 用于地下隧道和大型会议厅的无线通信；
- 数据速率达到和大于 10 Gbit/s 的无线链路。

使用 60/70/80/95/120 GHz 波段的优点包括：

- 密集区内频率复用时能减少潜在的不需要干扰；
- 使用更小尺寸的天线（天线增益与天线的尺寸和波长成正比）；
- 小型无线电设备可以支持游牧应用；
- 狭窄的天线波束宽度（天线波束宽度与工作频率成反比），这可以减少干扰、增加频率复用；
- 潜在的与其它无线业务共享频率的可行性；
- 支持高容量传输，由于其较宽的可用带宽（香农定律）。

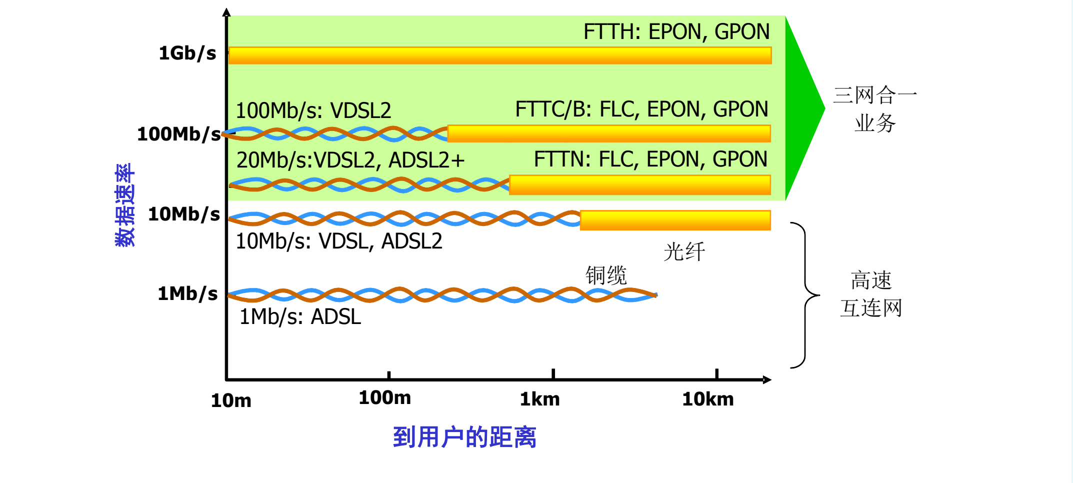
这些波段的缺点包括：

- 由物体或人体引起的信号遮挡；
- 在 60 GHz 范围内的氧吸收；
- 在大雨和降雪地区对中断的敏感性；
- 不适合长距离传输。

在固定网络领域，由于提供的xDSL是世界上非常受欢迎的宽带接入（实际上是当今最好的宽带建设技术），各国现在都正在部署基于光纤的宽带，实现FTTC（光纤到路边）和FTTH（光纤到户）。随着PON（无源光网络）的发展，每个人都可以经济地享用100Mb/s的速率。因此，在许多发达国家，光网正将企业用户和一些家庭纳入自己的覆盖范围。

如图2-1所示，基于光纤的技术能够以足够的带宽提供比传统接入更远的距离，这种特性非常有助于扩展正在提供的宽带连接，包括农村地区。特别地，光纤和xDSL的结合能够支持经济地实现到最终用户的宽带距离延伸，而且保持宽带容量，例如，FTTC和VDSL能提供30 Mb/s到户。

图2-1：传输技术发展

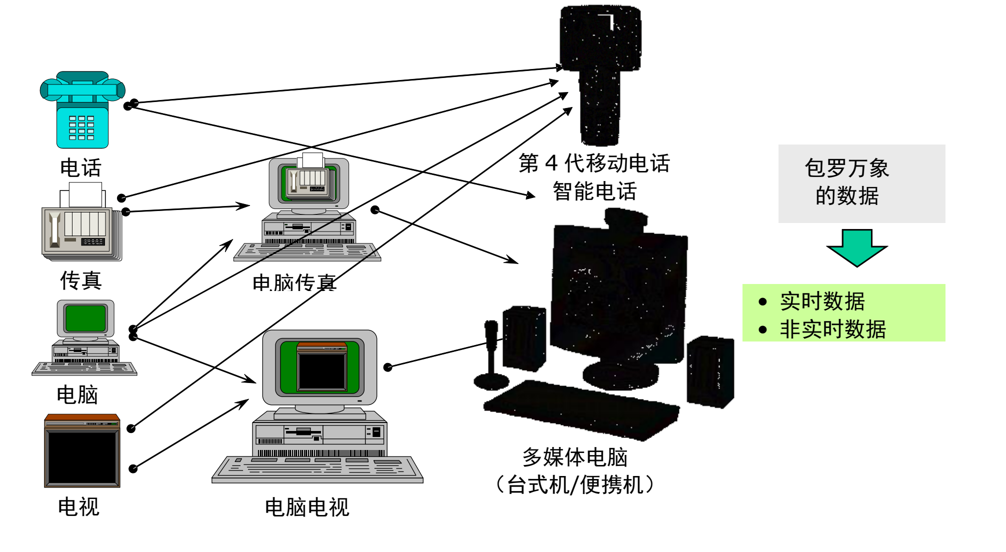


2.3 终端业务发展

处理技术的发展极大推动了终端设备的发展，而且这一趋势方兴未艾。在过去十年中，终端设备特别是便携电脑和手机包括智能电话（如 PDA）已经在大多数电信业务发展中保持了领先地位。便携和智能是这一发展的主题。

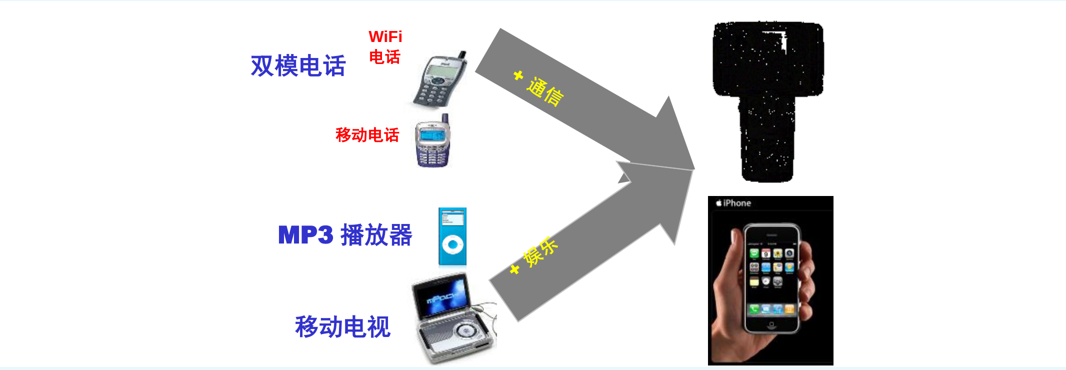
如图2-2所示，终端原有的图形、文本和视频功能，被集成到一个基于电脑或基于移动的物理设备之中。语音服务功能也得到了很好地开发，被集成到被称为手机的小巧装置中，而这一功能也被纳入由集成的多媒体终端设备组成的电脑。通过这种整合，包括语音在内的各类业务都变成了“数据”，因此终端设备的输出信号应是“以实时或非实时划分的数据”。这些集成到便携电脑的各种功能，正使得象移动个人办公室等这样一类的游牧生活成为现实。

图2-2：终端业务发展



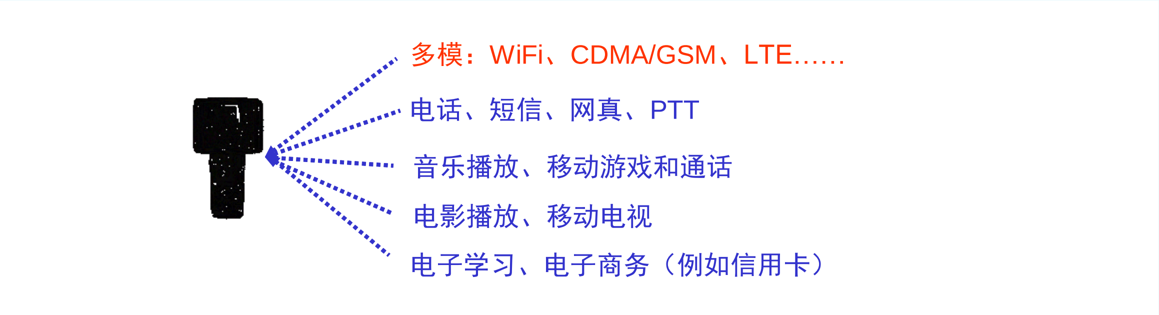
在这些发展当中，移动终端设备是强化我们信息通信生活的主要力量。手机已不再只是电话，它已成为使人们能够随时随地沟通，包括享受个人娱乐的智能手持设备（图2-3）。

图2-3：移动终端业务发展



由于它的发展，最终用户终端设备，甚至智能移动电话这类单一设备，现已能够支持大多数图2-4所示的多媒体业务。

图2-4：多功能终端设备上的各种业务



2.4 电信网络发展

许多技术不仅是为移动网络，也是为固定网络开发和使用的。以本报告的简短篇幅很难对这些发展作出详细地分析。因此，本报告试图分析电信网络现在和未来发展的大趋势。

引领电信网络发展的一大变化或趋势，是从"电路"向"分组"的转变。直到80年代末，模拟向数字的转变是启动ISDN等电信网络发展的最重要主题。但由于IP技术在20世纪90年代中期得到采用，基于电路的网络向基于分组的网络的过渡成为发展的重中之重。图2-5以概括的方式显示了技术发展取得的成就以及未来的方向。

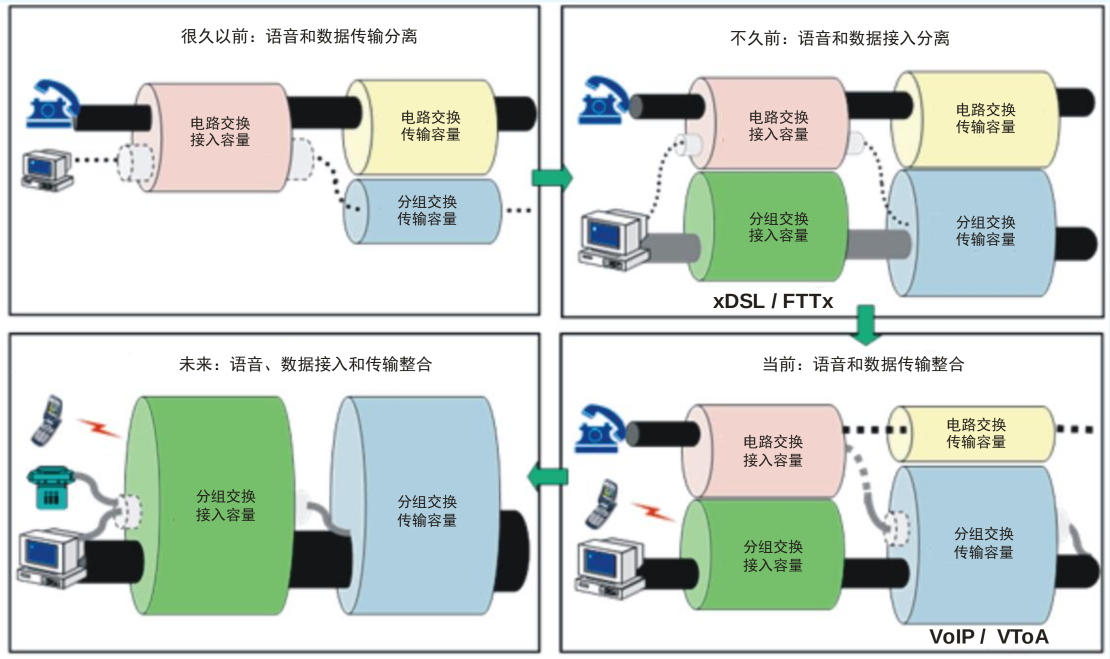
- 很久以前：电信网络是按照业务例如语音和数据完全分离的，因此，PSTN 是为语音业务开发的，包括话带数据例如传真，PSDN 是为数据通信开发的，但两个网络均采用电路技术进行网络接入。

- 不久前：广泛部署于大多数网络的分组技术不仅像很久以前的情况那样用于核心网，而且用于接入网。这主要是通过支持 xDSL 的 IP 技术实现的，并对建立全球连接起到了巨大的推动作用。有几种数据业务仍在使用调制解调器等电路接入。

- 当前：分组能力是电信网络的主要能力，无论语音、数据甚至移动通信都是如此。受益于宽带接入的分组基础设施涵盖了包括语音在内的多项多媒体业务。但基于电路的网络依然占据提供语音业务主要网络的地位，尽管采用电路接入的语音业务也开始利用分组核心网络进行传输。

- 未来：预计该分组能力将涵盖包括接入网和核心网在内的所有网络领域。它将不仅支持多媒体，还支持固定和移动的语音业务以及宽带功能。

图2-5：电信网络发展的趋势



注：V：语音；D：数据

2.5 编号和路由选择方面

2.5.1 编号和命名

各个用户将通过名称或号码来识别，名称/号码解析系统将用于把一个给定的名称/号码转换成网络中可以路由的地址。由于 NGN 和传统网络在将来的一段时间内将并存，NGN 必须能够支持用于固定和移动网络的现有的命名、编号和寻址方案。ITU-T E.164 建议书定义了适用于电话的国际命名方案，而 ITU-T Y.2001 建议书“NGN 概述”致力于 NGN 中编号、命名和寻址的课题，地址是一个用于特定端点的标识符，用于寻找到该端点，路由选择是分发和收集与拓扑有关的信息，计算路由，建立并维护网络中路由表的过程（Y.2612），在传统的模拟网络中，号码用于寻址网络部件，在数字交换网络中，寻址与编号是相互分离的，然而，编号体制会被相当长时间地使用，因为客户知道号码并使用号码，CPE 也合并了号码。

但是在 NGN 情况下，也可能会想到另一个 URI 即 SIP URI。在 VoIP 情况下，呼叫 TEL URI 或者 SIP URI 将会经过 DNS（域名系统）被转换为 IP 地址，SIP URI 可以在服务提供商域内或者自我供给的域内。SIP URI 的一些例子如下所示：

SIP: 911125368781@<dummy>	> 仅 E.164 格式
SIP: 911125368781@opr1.in	> E.164 +服务提供商域
SIP: abc@opr2.in	> 名称＋服务提供商域

因此，现有的编号体制也可以用于 NGN，对于网络和最终用户，在编号体制方面并没有区别。软交换和 SIP 服务器将负责以 E.164 号码为基础的呼叫的路由选择，所有的 SIP 用户将被指配一个 E.164 号码，软交换的 SIP 服务器功能将会为所有这些 SIP 用户建立一个数据库，在该数据库中会存储相对于 E.164 号码的 IP 地址分配，从 PSTN 到 SIP 用户的呼叫的路由选择将基于这个数据库表格来完成，这种方法的最大优点是保持与现有相同的编号体制，最终用户不会被网络中传输语音的新技术的采用所迷惑。

号码/名称解析通常采用各个数字交换机中的路由表来完成，在互联网中，域名系统（DNS）用于号码/名称解析，由于 NGN 是分组交换网络、采用的是 IP 协议，DNS 可能是 NGN 中号码/名称解析机制的合理选择。

E.164 编号（ENUM）是电话号码到采用域名系统（DNS）的统一资源标识符（URI）的映射，ENUM 能够实现 PSTN 和 IP 之间的融合，使用的是 DNS，因此可以节约资本支出。

各个服务提供商将会需要内部的、支持编号和路由选择的 ENUM DNS， 它位于该运营商的公共骨干网中。利用这类概念，运营商能够使用他们现有的编号体制，以及现有的运营商标识码，如下所示：

(区号：2 到 4 位数字) + (运营商标识码：1 位数字) + (用户号码：5 到 7 位数字)

所有的 PSTN 和 IP 交换均应端接在该运营商的公共 IP 骨干网上，DNS 也连接在该网上，DNS 导出目的地的可路由地址，并端接该呼叫。在多运营商、多业务网络的情况下，通过使用全局 DNS，路由选择和交换也是可能的。

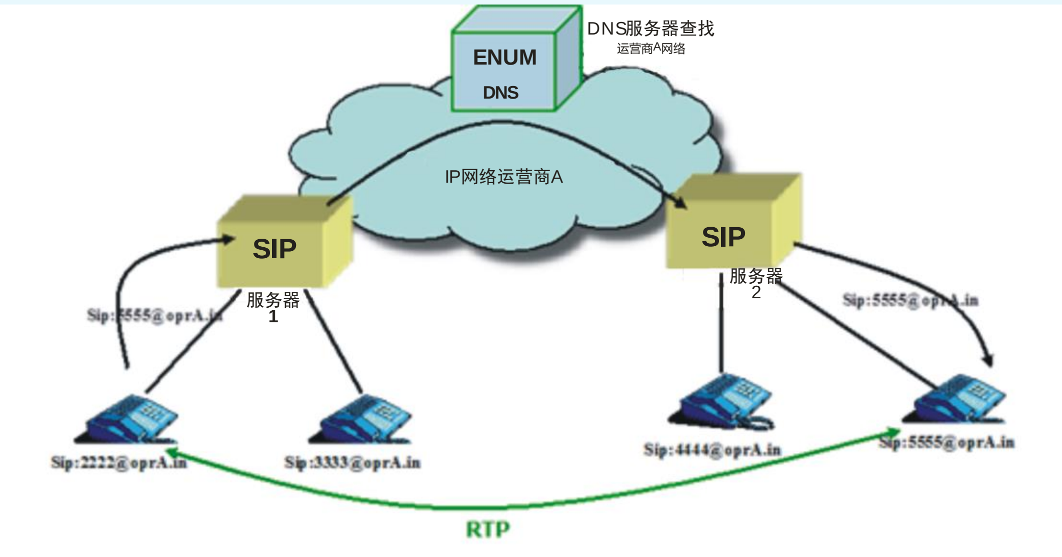
对于从 IP 到 PSTN 的呼叫，目的地的电话号码可以用 SIP URI 表示，对于这些呼叫，网关会去掉电话号码，并用它发起采用 ISUP 信令的呼叫。

这就允许一个 E.164 号码表示为一个 URI，DNS 能够将 URI 解析为 IP 地址。主要的行政上的讨论集中在用于电话号码的树，可以设想对一个世界范围内的树（被称为“黄金树”）取得一致意见，然而，e164.arpa 树只是当前实现的可选项之一。黄金树讨论的上下文是寻找一个适合于 ENUM 的商业模型， ENUM 的最初版本是一个全球公用的、目录似的数据库，具有 e164.arpa 域内国家代码级的用户选择的权力和授权，这也称被称作用户 ENUM，然而，适用于用户 ENUM 概念的切实可行的商业案例还没有出现。

ENUM 的技术概念是可行的，当前实现的主要是运营商 ENUM，运营商或通信业务提供商团体同意通过专用对等关系中的 ENUM 共享用户信息，但是运营商自已控制用户信息。运营商 ENUM 也被称为基础设施 ENUM。

ENUM 还用于将号码解析为 GSMA 提出的 IMS 技术要求和 IPX 技术要求中的地址，因此，实现 IMS 需要实现运营商 ENUM。

图2-6：互操作性和ENUM



2.5.2 路由选择

路由选择是分发和收集与拓扑有关的信息，计算路由，建立并维护网络中路由表的过程（Y.2612），基于 IP 网络中的路由选择由各个路由器中的信息决定，网络之间的路由信息采用边界网关协议(BGP)进行通告，在传统网络中，路由选择是在一个网络内部完成的，如果确定一个特定的地址不在该网络内，则连接会迂回到一个适当的互连点，路由选择可能还与负责网络中断或者拥塞的溢出或流量管理机制有关。

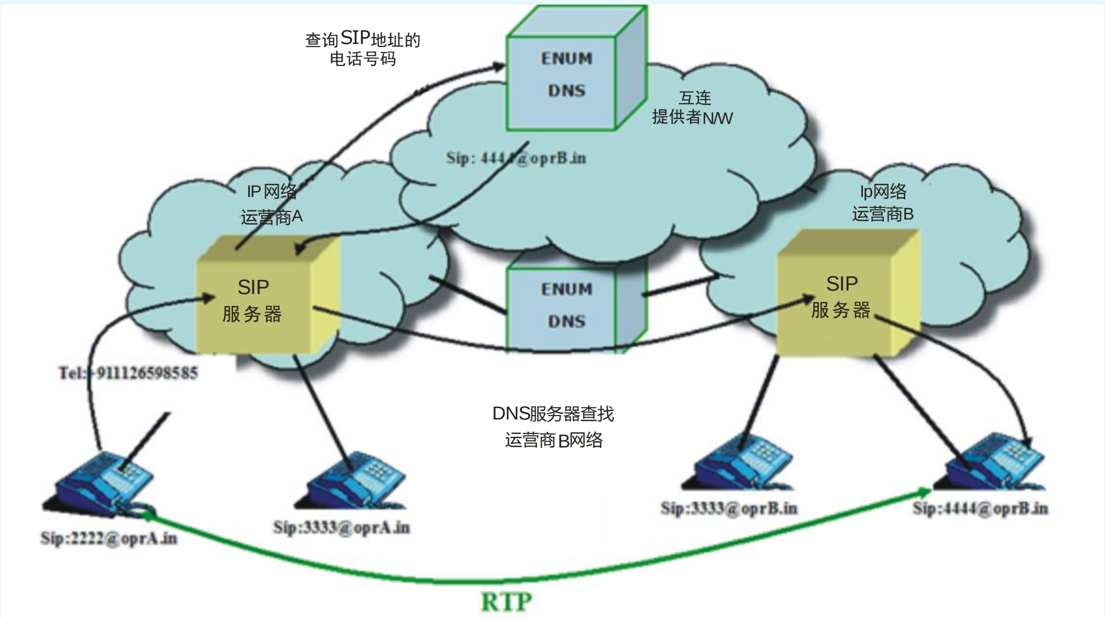
核心网体系结构将采用 OSPF、BGP 等众所周知的 IP 协议用于路由更新，采用 MPLS 用于流量工程，用于将 IP 流量一个运营商移交到另一个运营商的路由选择程序和配置将取决于这两个运营商是如何互连的，除了两个运营商之间的 IP 连通性和路由协议以外，NGN 会需要特殊的设备以便将语音和视频从一个网络顺利地传送到另一个网络，将会存在与两个网络中防火墙穿越、安全性、SLA、协议转换（互操作性）以及对呼叫的合法侦听等相关的问题，为了处理这些问题，在两个 NGN 运营商之间的边界上将会需要会话边界控制器（SBC）之类的设备， 核心网和边界网络中路由器和交换机之类的网络设备应支持 IPV4 以及 IPV6 协议，以便将来容易地过渡到 IPV6。

移动网络已经实现了漫游的概念，这意味着用户能够在所访问的网络中发起呼叫和接收呼叫，并接收来自他们本地网络的帐单，根据 GSM 技术要求，对一个漫游用户的呼叫要途经本地网络，本地网络决定漫游路程的收费。漫游用户的主动呼叫会被直接安排去往目的地，而不需要经过本地网络迂回。受访的运营商记载该呼叫的详细记录，经过由 GSMA 规定的所谓的传输帐务过程（TAP）将它们发送到本地网络。在任何情况下，漫游用户的移动互联网使用情况均会发送到本地网络，由本地网络控制对互联网的接入。

下一代网络中的路由选择和漫游将采用 IP 机制，预计运营商将保持他们对漫游流量的影响，并将包含在对漫游用户的呼叫路径中，从技术的角度来看，也能从其它的网络访问提供的 HLR 信息将不是必需的，IMS 技术要求包含了路由选择和路由信息交换的解决方案。

在基于 IP 的网络中，借助全局 ENUM DNS 建立 SIP 会话的过程如下：

图2-7：借助全局ENUM DNS建立SIP会话



3 向 NGN 过渡带来的监管挑战

某种程度上，NGN带来的监管挑战是与服务提供和网络接入级别的融合过程联系在一起的，本节从管理的角度讨论了许多与NGN有关的监管挑战，这些挑战包括开放接入、市场定义、QoS和互连。

在本讨论中，重要的一点是记住NGN将继承在PSTN上强制执行的诸如合法侦听和使用应急服务之类的监管职责。3GPP和TISPAN均已考虑了使用应急服务的需求，然而，只是计划在之后的版本7才第一次引入3GPP IMS体系结构内的应急服务，而最初的IMS版本R5和R6只允许通过电路交换域使用应急服务，原有的GSM核心基础设施用于语音呼叫。

2G移动网络中的GPRS已经实现了对分组模式业务的合法侦听，GPRS具有发送某一个用户在PDP上下文交换的所有分组的副本，以及通过这个上下文接入实体的地址的能力，合法侦听从最初的3GPP IMS R5技术要求就被引入。

3.1 高级监管考虑事项

尽管NGN及其业务看来呈现出许多的优点，但是期望可以更好地了解所有可用的选项以及与NGN有关的所有优点和缺点，下列问题能有助于确定这些考虑事项：

- 什么网络用于什么业务？
- 管理者设想什么行动可以促进向 NGN 的过渡而对消费者有利？

- 过渡到 NGN 会怎样修改主要运营商的规章制度？
- 引入 NGN 网络对于互连、服务资费设置、编号、频谱管理等的影响是什么？

着眼于准备从现有电信环境向NGN的转变，对NGN可能产生的例如互连、消费者保护、普遍接入的重新定义、技术中立、服务质量、编号和许可等问题应予以认真地考虑。为了确定正确的过渡时间，对向NGN网络过渡的准备工作进行技术、经济和监管方面的研究是非常重要的。重要的一点是要注意到管理者应确保从转变显现出的市场是公平、公开和竞争性的，另一方面，要向管理者阐明向NGN网络转变会产生的所有技术、经济和监管方面的问题，尽早确定与其活动有关的关注领域。

基于这些目的，已经对以下研究课题进行了考虑：

- 回顾法律上的和管理上的电信制度，确定那些为了适应融合可能需要修改的部分；
- 收集运营商和服务提供商对于 NGN 网络的期望；
- 调查主要的固定和移动电话运营商关于核心网和接入网段的过渡策略；
- 确定会妨碍或推动向 NGN 过渡的因素（在技术、经济和监管层面）；
- 确定将与 NGN 及其适用性、耐久性有关的新经济模型；
- 拟定适合于固定和移动电话网络向 NGN 过渡的策略；
- 提出雄心勃勃的可适应新技术变化的过渡路线图以及预算、实际的实现最后期限和监控其实施的指标/机制；

应根据以下提议的阶段开展研究：

1 收集、分析有关电信的法律和管理体制的信息；

2 组织对电信和 ICT 部门所有成员开放的 NGN 研讨会/讲习班；

3 收集来自固定和移动电话运营商以及互联网接入和服务提供商的数据；

4 分析和利用关于各个国家情况的数据，与其它国家的经历进行比较；

5 制定路线图、产生向 NGN 转变的最终研究报告和策略文档。

拥有管理洞察力的方法之一可能集中在方法论框架内分析NGN监管问题的必然性。在这个意义上，关于NGN是否是公共商品的问题是一个很好的检验诸如供给方面的非排斥性、消费方面的非竞争和外部因素等许多方面的主题，研究这些方面可能会直接给NGN的非常高级的管理制度提供有价值的输入，可能会采用新的、拥有不同于原有电信的规章制度的管理方法。

以下是关于上述方面的关键方面的概述：

- 供给方面的非排斥性：这个决定意味着相关产品的供给应涵盖所有的人，不采取排除的方式。已经在一个国家或社会的市场中供应的产品应为那里所有的个体都能获得，市场参与者不能从事市场运行层面的供给，这里的基本假设之一是所供应的产品尚未按要求被提供过，已经给某一个人提供过的产品同时已经为社会中每一个人或者参与者提供过。相关产品的供给应是相同质量的，供给本身应是一个同质的产品。

- 消费方面的非竞争：这个决定意味着某一个人消费相关的产品不会对另一个人消费该产品造成妨碍。个体的消费偏爱不是相同的，而是各不相同的。另一方面，消费偏爱的这种各不相同的性质不会产生消费方面的竞争或者对抗。
- 外部因素：这是与产品有关的其它单元的利益和成本之间的比例关系，与自由市场的功能不同，已经作为公共商品被提供的产品不会在利益成本平衡的框架内有效地运行，公共商品形成了一个负面的外部因素，因而在公开市场方面是无效的。

ITU-D已经起草了一系列有关管理、成本计算和政策做法的文件，并召开了研讨会，以帮助各国开发电信业务，近年来的一大重点是下一代网络，它与新电信/ICT技术所带来的挑战和益处尤其相关。为在此议题上向国际电联成员提供帮助，已经起草了一份题为《在宽带环境中部署NGN的战略——监管和经济方面》（“Strategies for the deployment of NGN in a broadband environment - Regulatory and economic aspects”）的报告[1]。报告从更高的层面审视与向NGN过渡相关的战略议题以及经济及基本方面。报告的目的是为提供意见，帮助制定宽带方面的国家战略和监管做法，使电信行业、消费者和使用电信业务的所有企业受益。

3.2 下一代接入网

根据上面的3.1节，下一代网络已经开始改变电信部门中例如业务、网络结构和网络结构功能模型等基本要素，因此，需要一种新的监管方法，而不是在以前的电信网络中已采用的常规监管方法，主要原因之一在于由NGN结构中特有的技术进步产生的这种特许权，因此，国家监管机构应考虑现有的规定如何能够适应这种与当前市场结构一致的新环境。

首先，关注NGA（下一代接入）网络这一设施是否必不可少是有意义的，原有的网络中只有一个接入网基础设施，因此它必须要到达本地环路的入口，然而，在不依靠特定接入网的NGN范畴内，甚至光纤接入也不是NGN业务不可或缺的设施，因为为了确保光纤是必需的设施，就必须不存在其它的接入网。在向IP网络过渡期间，基于原有电话的网络可以作为NGN网络的一个备选，因此，对于基于原有电话的网络结构而言，可以将NGN看作是提供更多基于IP的新业务（虚拟呼叫、宽带、IPTV和智能业务等）的技术设施，此外，由于NGN是电信部门的一种新途径，市场结构和需求选择尚不成熟，由于NGN和NGA在特性和功能方面不同于原有电信网络结构，这些新网络之上的市场结构尚不明确。

因此，如上所述，在向NGN过渡的过程中，需要新的监管方法。虽然鼓励投资NGN接入网，但促进竞争的关键问题之一是光纤环境下本地环路分拆（LLU）问题。目前，本地环路分拆规则集中在最后一英里。但是向FTTH、FTTB和FTTC过渡意味着焦点是最后四分之一英里或更少。给定相关的成本和其它资源的情况下，适合于传统铜线的LLU模型可能必须为光纤或者确定的不同补救方式而进行修改。管理者授权LLU的地点的一种选择可能是在中央办公室层面提供比特流，此处接入网的特性是完全透明。其它的选择可能包括要求在街道机柜层面进行配置和从机柜到运营商节点的回程。此外，在NGN过渡期间，会有新的方法实现LLU，不同于对原有网络中LLU的传统看法。在向NGN过渡的过程中，没有关于NGN的LLU的规则可以被看作是一种新方法，因为在过渡过程中将LLU置于管理的范畴会不利于分配效率和公平竞争的形成。在支出成本收回和服务市场形成竞争环境之前，NGA网络中部署的公司不应受到LLU的影响。收回投资的时间取决于公司的商业模型、市场结构和社会福利，然而通常可以接受是它应该至少长达4年或5年。NGA网络的LLU职责可能会导致市场中出现免费享用资源

[1] 此报告可在网站免费查阅：http://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Studies.aspx。

的问题，这个问题必须要予以考虑，不仅是为了收回投资，而且为了参与到NGN的各个提供商的公平和服务差异。

在竞争市场结构形成之后，过渡阶段就完成了，除了LLU外还有其它的设备会受益于光纤的部署，例如比特流接入、交换和虚拟分拆。除此之外，还应确定竞争市场对于零售服务市场或者批发接入市场而言是否是所期望的。然而，除非共享管道，否则那些具有竞争性的运营商自己提供回程是很困难的。

还有许多困难与新光纤的部署有关，长期土木工程费用包括公共领域内被动的基础设施改造，例如管沟挖掘和管道安装，私人领域内分支线缆连接，例如室内和住宅线缆敷设等，均耗资不菲。这些费用还与相当高的谈判复杂性有关，任何个体服务提供商单独承担将会被禁止。出于这些原因，需要被动的基础设施共享是管理者正在探索的一个方案。

另一个因FTTx而产生的问题和当前的运营商移除总配线架（MDF）的问题联系在一起，因而使得适用于铜线的LLU “旧”体制至少在其完全拆分和共享线路的情况下显得过时，因为在传统的LLU情形下，LLU发生在MDF。在互连点被撤销的情况下，向NGN过渡的过程中不用支付额外的费用，可以保持继续提供目前服务的能力，不会面对“投资搁浅”的问题，这些对于竞争的运营商来说非常重要。例如[2]，荷兰当前的运营商KPN宣布它将移除其所有的MDF作为其向NGN过渡的一步，从而将其网络整合为数量削减后的多个交换节点和只在街道机柜内部的移动DSLAM。KPN希望通过出售存放其MDF的建筑筹集10亿欧元，然后可以为其推出FTTx提供资金。KPN和荷兰国家监管机构OPTA正在讨论KPN移除MDF的计划，其中包括逐步淘汰MDF接入的条件，以及KPN提出的为街道机柜提供“次环路分拆（SLU）”以及在本地、区域和国家交换层面提供“批发宽带接入（WBA）”的建议。随着运营商不断地推出他们的NGN接入网，其他国家的监管机构可能希望追随欧洲等地监管的进展。

事实上，在向NGN过渡的过程中经济的里程碑不是在基础设施市场形成竞争，而是在业务市场建立竞争。这种竞争市场或许会给经济带来很多的创新。因此，希望建立在基于NGN业务之上的市场竞争，不是完全没有NGA范畴内光缆的分布，光纤分布是基于NGN业务的竞争的一种重要设施。

3.3 市场定义

在许多国家，特别是欧盟国家，相关市场的确定和定义是用于预先监管建立的竞争分析的基础，由于技术和业务之间的界限模糊不清，采用NGN后这项任务将会变得更为复杂。这种复杂性可能是监管机构和市场参与者之间产生争端的源头。

德国电信部署NGN的案例及其与监管机构就向其竞争对手提供网络接入的义务所产生的争端就恰恰证实了NGN对监管体系所带来的新的挑战。实现NGN的有利环境，但是其技术方面的因素更值得重点关注。德国电信和监管机构之间的争端核心在于对光纤接入和DSL接入之间的定性差异的解释存在分歧。在德国电信看来，光纤带来的额外带宽将使业务发生质的改变，例如，高清电视业务的提供将产生一个不同于目前指定具备SMP的DSL业务的市场。但是，监管机构则认为这一项目主要是德国电信对其DSL业务的升级，旨在留住其现有的DSL用户。

[2] 见 http://erg.eu.int/doc/whatsnew/kpn_van_den_beukel_erg_17_apr_07.pdf

如果当前运营商威胁要冻结其投资，那么此类争端的结果可能会是戏剧性的。但是，考虑到潜在的回报因素，欧洲的监管机构似乎对运营商继续投资类似项目充满信心。

3.4 服务质量

NGN的统一业务传输产生了与IP传输无连接特性有关的问题，特别是对于包丢失、时延或者抖动敏感的实时交互式语音或多媒体通信流业务。但是，已经有许多技术能够保证IP网的QoS。这些技术可以大致分为：以与相对优先级有关的过度配置为基础的技术途径和以明确的端到端资源预留为基础的技术途径。

必须注意到，互联网中大量使用的是没有QoS保证的“尽力而为”模式，互联网上的很多应用都使用传输控制协议（TCP），该协议在拥塞的情况下会减少用户的流量。但是，TCP并不适用于实时应用，像视频流、语音或多媒体通信业务就不能在拥塞的情况下限制数据包的发送速率。最近，更多的实时应用正在代表大部分的互联网核心流量，例如语音电话或者视频流等，不仅来自固定而且来自移动网络环境，目前，过度配置的核心网，和许多互联网骨干网的情况一样，处理这种业务会面临严峻的挑战，包括关于公平使用网络资源和数据爆炸的问题。

然而，下一代网络不同于互联网，即使他们使用相同的IP传输技术。NGN依赖网络给其最终用户提供的明确保证来实现对质量敏感的应用，如IPTV和有保证的VoIP。此类应用有望构成NGN流量的主体。

但是，下一代网络是有管理的、封闭的网络。因此，许多由于可伸展性和成本的原因还没有在互联网上得到广泛使用的、涉及差异化优先级和资源预留的QoS技术能够在下一代网络中得到应用。此外，在NGN的体系结构中，传输域处于业务域的控制下，这样就确保了在网络提供特定业务的期间，传输域会进行恰当的资源分配。这样的情形在互联网中不会存在，因为“控制”是端到端的，不是在网络的内部。

剩下的关键问题就是需要确保不同的下一代网络之间的协调，以便提供端到端的QoS。有一个一般性的误解，即，PSTN中端到端的QoS与沿途穿越网络中的64 Kbit/s TDM电路的预留有关。虽然这个理解不错，但是端到端的PSTN QoS也依赖于通过国际电联七号信令系统（SS7）所提供的恰当的端到端的信令。同样的端到端信令原则也可以适用于任何分组传输承载网，改编自SS7的国际电联的承载网独立呼叫控制（BICC）协议规范对这一可能性进行了论证。

通过定义和设计，IMS体系结构采用SIP协议完成呼叫（会话）信令。SIP本质上是一个互联网的端到端协议；但是3GPP和ETSI TISPAN将其进行了延伸，使其可以用于NGN语音和多媒体呼叫的网络控制功能，这类似于原有基于SS7的智能网络体系结构中的呼叫和业务控制功能。国际电联正在开发基于逐个呼叫进行资源预留的NGN信令协议，该协议将应用于网络内部，特别是在网络互连点上使用。这项工作正在与3GPP和ETSI TISPAN的密切配合下积极推进。国际电联已经产生了一些有关资源预留的NGN信令协议的建议书，而进一步的工作正在由ITU-T第11研究组开展。

当然，监管机构的责任不是要切入NGN内部提供QoS的详细技术细节。但是，为了支持如交互式语音等基本业务的提供，监管机构可以对定义网络互联点所需的基本要求有所贡献，就像当前对电话网络之间所作的工作一样。

3.5 互连

电信网络之间的互连需求通常源于最重要的完成业务的需要，NGN也不例外；事实上，与原有电话网络相比，NGN业务接入的泛在性使其对互连的要求更胜一筹。

除原有的为完成业务而要求在不同的下一代网络之间以及一个下一代网络和其他语音网络之间实现互连之外，还必须允许用户具备以下的能力：

- 从任何其他网络实现连接，并能从其本地网络获得业务资料以便享有相应的服务。这一概念类似移动漫游，但是适用于所有类型的宽带分组接入；
- 优先接入属于自己网络的业务，而不是到访网络的业务。这一特性目前在移动网络上通过移动网络增强逻辑的定制应用（CAMEL）IN 接口可以呈现，例如，该接口允许漫游用户接收采用其母语的网络信息报文并使用增值服务；以及
- 使用第三方服务提供商的增值服务，这一概念目前在 2.5 代和 3 代内容服务方面是可用的，例如接入备选的无线应用协议（WAP）门户，或 I-模式服务。

NGN的互连要求使得定义多媒体呼叫的构成很有必要，这一问题在选择呼叫方付费（CPP）方式还是账单-保留体制的时候可能十分关键。基于IP的NGN环境下的互连，但是将CPP制度与电路交换传输联系在一起这一误解必须得到澄清，这一点很重要。CPP制度更多地归功于两个网络域之间特定呼叫的业务完成协议，而不是为特定呼叫所作的实际资源预留。事实上，在原有的话音电话系统中，这就意味着预留了一条专用电路，这仅是一个技术细节，而且会随着网络向着分组传输的发展而不断演进。在NGN中，只有处于网络域边界上的各自的控制实体之间存在或认为有必要存在信令交互，这样的确保业务完成的协议对于各个多媒体呼叫来说才是有意义的。要使得上述信令存在，就必须对这些多媒体呼叫的要求给出共同的定义，就像已经存在的对话音呼叫要求的定义一样。

NGN 中的漫游问题很可能会更为复杂。目前，移动业界已经就相互漫游协议达成一致，无需监管介入。监管机构只干预漫游资费的问题。在 NGN 的环境下，监管机构将不得不考虑授权漫游是否有必要。例如，是否应要求 NGN 移动接入运营商允许任何 NGN 光纤接入运营商的客户在其接入网漫游？反之亦然。

接入第三方服务的问题也很重要。过去，移动运营商试图将其客户锁定在自己的业务提供平台上。幸运的是，这些做法已不复存在，甚至实际上大多数的第三方服务提供是通过运营商的门户来完成的。同样，监管机构应密切监督第三方接入NGN环境下的服务。即使IMS体系结构和NGN采用NGN-OSE和NGN-SIDE，以书面形式昭示第三方接入服务提供商的平台，但是实际的执行可能会是相当复杂的，这也许给技术争论背后隐藏的非竞争性行为留下了一定的空间。

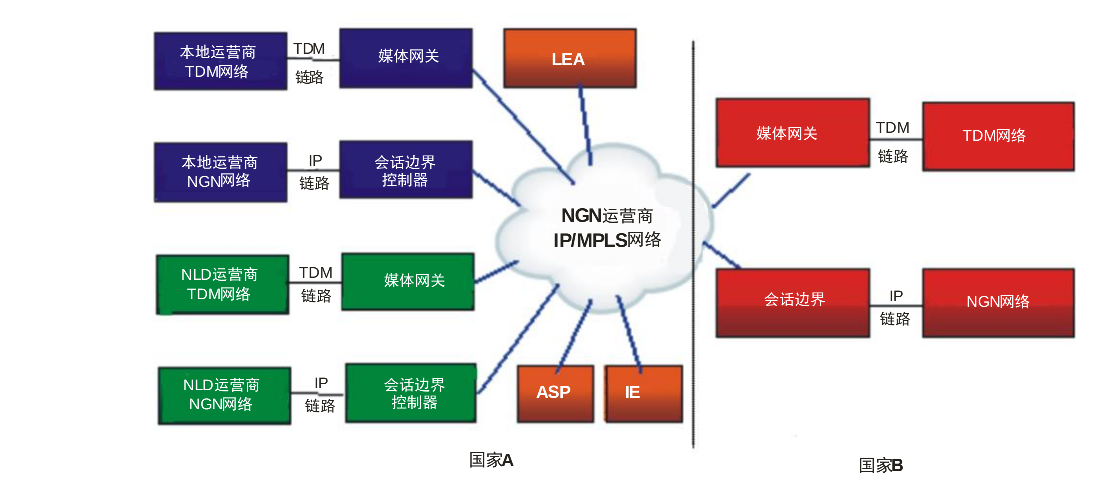
3.5.1 互连体系结构

在过去几年期间建立的许多网络都包含了大多数的NGN部件，向互连的推进工作已变缓展开，即便在技术已经成熟或者接近成熟的情况下。由于IP技术的效率和灵活性，大多数正在建设的新网络都是基于IP的。

NGN环境下运营商之间的情况如图3-1所示。

注意到基于ISDN用户协议（ISUP）的传统PSTN和移动网络，可以通过IP到TDM或者TDM到IP转换的媒体网关，以及在IP之上传输SS7的信令网关进行互连。

图3-1：NGN情况下运营商环境之间互连体系结构



注：　LEA：执法机构

ASP：应用服务提供商

如图3-1所示，NGN网络通过会话边界控制器（SBC）进行互连，该设备位于网络的管理边界，对多媒体会话强制执行策略，会话策略可能定义成管理安全性、服务级别协定、网络设备资源、网络带宽、网络之间的互通和协议互操作性。

SBC能够完成许多功能，例如：

- 网络安全
- 拒绝服务攻击和过载控制
- 网络地址转换和防火墙
- 合法地侦听
- 服务质量（QoS）管理
- 协议转换
- 呼叫记帐。

图3-1所示的MGW（媒体网关）将由NGN中PSTN/移动运营商部署的软交换控制，SGW（信令网关）能够集成到MGW之中，或者也可以是一台独立的设备。

3.5.2　接口

3.5.2.1　物理接口

会话边界控制器SBC提供到其它NGN网络的IP接口，物理接口包括：

- 吉比特以太网接口；
- 10/100 Base-T 快速以太网接口。

SBC提供冗余信令和媒体控制子系统，每一个具有冗余网络接口。SBC子系统相互之间可通过任何有效的IP接口进行通信。

3.5.2.2 信令接口

假设已经定义了信令接口的网络模型是一个全IP下一代网络（NGN），这种情况下网络中的控制点可能是：

- 软交换或者
- IMS（IP 多媒体业务）核心网。

信令的标准化主要是ITU-T的任务，因此不在本问题的范畴之内，然而，由采用特殊类型的接口而产生的监管问题是很重要的，尽管ITU-T对协议和信令进行了标准化，仍应指出这个问题：管理者是应该强制实施一个特定的标准以确保互操作性，还是把它留给运营商、冒缺乏互操作性的风险。

ITU-T 第13研究组已经转发了两个建议书，作为对与这个问题相关论述的响应，ITU-T Y.2701和Y.2201建议书提供了下一代网络的接口安全性要求以及对服务和容量的高级要求，除了这些建议书以外，还有一系列NGN发布的建议书。

ITU-T还批准了管理者可能希望使用的信令建议书Q.3401、NGN信令简介。

3.5.3 互连点

在转变期间，主要的运营商可能会被要求保持传统的PSTN互连能力，假设竞争者有可能通过传统互连到达基于主要NGN的最终用户，提供新的基于NGN互连能力可能不一定是一项管理的义务。在转变期间，主要的运营商会在某些点提供基于IP的互连。当转变过程结束时，他们可能会撤消传统的互连，在这个意义上，他们仍具有市场支配力，他们应毫无疑问有管理上的义务以基于成本的价格提供与NGN的互连。在互联网的世界，绝大多数互连采取的是对等或是转接的形式，在NGN市场情况下，参与者可以优选对等、变换或者其它的互连模型。实际上，对等方式可提供仅仅在主要客户和对等用户之间业务的交换，但不提供接入第三方，相反地，在典型的转接关系中，转接用户能够利用转接提供者的网络到达互联网上任何地方的终端。不大可能推动主要服务提供商为小的竞争运营商提供对等配置，有可能给少数几个国内最大的竞争对手提供对等配置。此时，小的国内竞争者只能进行有限的选择，他们可以坚持PSTN互连，或者可以从主要运营商之一购买转接服务，过多的问题会阻碍适合基于IP的NGN的健壮互连框架的实现以及要出现的这种框架的成功运行。建立并维系与另一个公司的互连配置需要大量的工作。取决于环境，技术上的努力有时是必不可少的，经常被忽视的是建立IP互连时的管理成本和合同成本。当运营商之间没有对等配置时，可以探索一种可能的建立基于IP的互连交换的方法，该方法缺省地将所有的IP流量转接到所有的运营商。

3.5.3.1 互连交换（IE）

互连交换的基本概念是使不同的运营商能够互连到一个公共点，从而高效地交换相互的流量，互连交换也许是一种选择，管理者可能希望将其作为适合于NGN互连的一个模型。

互连交换的作用

- 运营商之间记帐

  当前，运营商之间记帐是各个服务提供商之间争论的一个主要问题，如果不采取补救措施，这个问题很可能会进一步升级。使用互连交换，同时也作为运营商之间票据清算，可能提供这个主要挑战的一个解决方案。运营商之间的收费可能会随传输业务到互连交换的时候所使用的：

  a) 服务等级；

  b) 内容；和

  c) 网络部件而变化。

- 智能网络业务

  通过互连交换/运营商之间记帐票据清算的结合，能够实现多运营商多业务情况下的智能网络业务。

- 号码可携带

  通过一个集中式用于互连交换/运营商之间记帐票据清算的数据库，也可解决多运营商多业务情况下的号码可携带。

- 简化

  采用互连交换/运营商之间记帐票据清算还可使网络体系结构简化，减少互连点（POI）的数量的点数，简化互连使用费用的结算，以及缩短互连能力的等待时间。

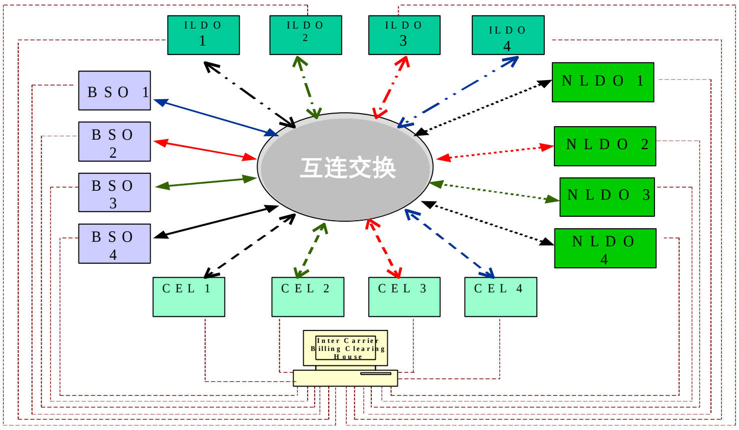
当前互连体制造成的挑战

在多运营商、多服务的环境中，当前的双边互连配置会产生如下问题：

- 高互连成本和端口费用
- 由于模棱两可和不公平竞争环境导致不对称的互连协议和申诉。
- 由于容量限制导致提供互连的时延
- 资源的非最优化利用
- 低效的呼叫处理
- 管理运营商之间结算的高运行成本
- 运营商之间记帐
- 互连使用费用结算的复杂性
- 智能网络平台的共享

- 号码可携带的实现
- CAPEX 和 OPEX 增加导致操作不可行。

图3-2：互连交换



注：　BSO表示基本业务提供商/固定线路业务提供商

　　　CEL表示移动网络

3.5.3.2　互连点的位置

当前，运营商在相互达成一致的POI相互对等连接，在运营商不能实现对等连接的领域，可采用其他运营商的网络进行转接。

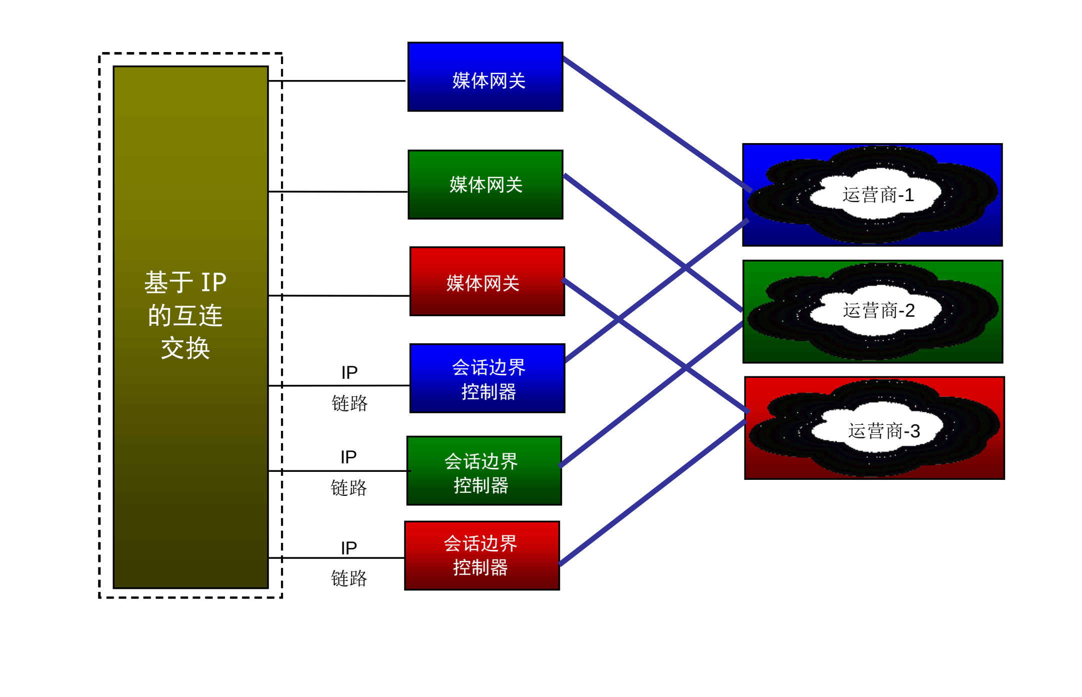
当前，对等双方必须在POI位置拥有基于TDM的交换机，随着MPLS网络的实现，相对于距离的运费概念不再恰当，NGN及其控制和媒体功能分离、分布式架构的NGN消除了这个限制，NGN环境下提议采用下面的方法：

i)　可能会允许运营商选择控制分布式媒体网关的网络中的一个集中式控制点，或者服务区域内的 SBC；

ii)　应允许运营商将媒体网关/SBC 放在国内的任何地方，需要 POI 的任何地方；

iii)　提议将互连交换用于在 NGN 环境下不同运营商之间的互连，如图 3-3 所示。

图3-3：互连交换模型



在大多数运营商都会存在的地方，根据流量的需求可以在服务区级别建立一个或多个互连交换。

这个模型的优点是它可以使得网络规划更加高效，每个运营商都了解物理位置，在那里必须提供能够以更好规划的方式实现传输网络转出的POI。

NGN中互连体系结构应与当前的PSTN/ISDN/移动网络服务可比拟或者更为健壮，因为随着时间的过去，NGN应取代这些网络。因此，这个体系结构的一个重要的目标是：在互连失败的情况下它能以最短的故障时间让服务恢复，这意味着必须要采用一个有弹性的多节点体系结构，以及为了满足严苛要求特别配置的IP协议和网络技术。

NGN环境下的互连应在两个逻辑层面进行–信令层和媒体层，为了使互连的成本和复杂度最小化，第二层连接可能比采用逻辑VLAN/VPN（虚拟局域网/虚拟专用网络）的第三层互连更为可取。

NGN环境下的互连应提供一个安全、低等待时间的环境，在那里可以确保所有运营商之间批发互连的质量。

3.5.4 互连计费

PSTN/移动网络环境中互连计费目前的概念是以呼叫的距离和时间/持续时间为基础的，在基于IP的NGN领域，网络提供者在大多数情况下依然是服务提供商，但他们不一定是唯一的服务提供商。Vonage、Skype和SIPgate都是有竞争力公司的例子，它们能够在不运行自己网络的情况下提供服务，在可以预见的未来，综合的和独立的服务提供者很可能会同时存在，会为了相同的最终端用户客户而竞争，这种功能分离对于网络提供者和服务提供商均有

着深远的影响，在理论上，基于IP领域中的网络提供者不知道或不关心网络上传送的应用业务流的性质，在这种情况下，语音只是另一种应用。

在NGN情况下，互连计费可以采取各种模型，包括账单和保持模型，或者在收取费用的情况下，则费用可以依据带宽、应用使用情况、所提供的服务质量、所使用网络部件的数量、会话期间交换数据量、时间等。

NGN网络可能需要更多的用于收费的特性，如下所示：

- 基于呼叫时间、承载者容量、时间和日期类型等的收费；
- 基于 QoS、带宽和应用等的收费；
- 支付方（主叫、被叫或第三方）；
- 附加的和增值的服务的收费。

应具有产生CDR（呼叫数据记录）、用户记帐、中继线记帐、自动备份以及格式转换功能。

为了将相关信息发送到记帐中心，需要标准的接口和协议。

在NGN环境下，开发互连计费体制是十分重要的，该体制能够为运营商结算提供可信度，并促进互连协定，例如，印度目前采用了基于成本的互连使用计费（IUC），包括发起方计费、运费和终端计费，然而，在基于NGN的网络中至少有四种可能的互连计费模型。它们是：

1. 主叫方网络付费；
2. 账单和保留；
3. 基于服务质量的计费；以及
4. 成批记账。

确定互连计费可能包括评估与NGN环境下建立一个呼叫有关的不同网络部件所产生的各种成本项目，或者以易货的方式进行，或者通过测量发送的流量（容量、提供的QoS级别等），即使采用帐单和保留模型时，一些国家可能会继续采用运营商付费，由发起的运营商到接入提供商。在互连计费以网络部件为基础的情况下，根据各个运营商提供的输入，准确地评估相关的网络部件的成本需要付出非常大的努力。重要的问题是确定与多运营商环境下完成从起点到目的地的长距离运输有关的网络部件。

向NGN的过渡将深刻地影响网络成本以及运输业务的成本和传送业务所经过距离之间的关系，NGN和互联网的相似性已经引发了这样一个问题：向NGN过渡是否会导致互连计费中“距离的消亡”，在互联网计费典型地与数据传输的距离无关的情况下，NGN环境下与距离有关的网络成本可能会变得越来越小，因此，基于成本的互连计费将有助于产生正确的规章制度，从而推动NGN在市场更加快速地部署。

NGN 体制下互连计费的四个主要基础：

在互联网环境下，一些事情在应用层面或服务层面是已知的，而截然不同的事情在网络层面则是已知的。以VoIP为例，实现类似于SIP协议的服务器会知道会话发起的时间，可能会知道会话结束的时间，但差不多对在这期间消耗的网络资源一无所知，会知道起点和终点的拓扑位置（网络中的逻辑位置），但并不一定知道它们的地理位置。除此之外，基于IP的网

络将会处理比仅仅传统语音广泛得多的大批应用。呼叫发起方应被看作费用的产生者这一观念通常不再成立，一般来说，对于如何在最终用户之间分配成本这一问题，并没有显而易见的“正确答案”。基础网络知道截然不同的事情，在基于IP的环境中，每个IP数据报都是独立编址的，基本上都可以被独立地寻找到（尽管路由选择实际上要比暗示的稳定得多），相对简单的应用就能产生非常大量的IP数据报，为了记账，对数据进行概括是必需的，否则，记账系统将会被处理不了的数据量所淹没。出于类似的原因，测量一个给定的点对点数据传输链路上的流量是微不足道的，但是开发一个基于端到端流量目标的总的流量矩阵既昂贵又麻烦。

3.5.4.1 主叫方的网络付费（CPNP）

CPNP-发起呼叫的网络为本次呼叫付费，通常是根据呼叫时间；一般来说，接收（终止）呼叫方不支付任何费用。在基于IP的网络中，收费可以根据所传送数据包的数量，而不是呼叫时间。这可以采取基于部件计费（EBC）或者基于容量计费（CBC）的方式，这两个系统构成了基于成本的系统。

限制：

- 在 EBC 模式下，互连费用取决于网络部件的数量，IP 网络实现 EBC（或 CBC）会产生处理成本（例如，为了确定互连的 IP 点）；
- 终端垄断。

3.5.4.2 帐单和保留

采用该体制时，终端无需付费，帐单和保留从本质上说是一种易货交换，在这种模式下网络运营商A在它自己的网络中终止来自网络B的流量，反之亦然。由于流量可能在进出两个方向上达到平衡，因此就不存在付费流量。运营商A获得其终止在运营商B网络中的流量的价格包括为终止来自B的流量提供网络容量，从这个意义上来说，互连服务不是免费提供的。

采用账单和保留模式，可以降低交易费用，在账单和保留模式下不存在终端垄断问题。在终端服务不付费的情况下，套利的问题也得以避免。

限制：

- 采用账单保留模式时，服务提供商有动力尽早将他们的流量转交给适用于终端的另一个网络，这就产生了“烫手山芋”现象。为了遏止这一问题，制定关于互连点的最小数量和位置的要求可能是适当的，可以让帐单和保留模式适合于特定的网络运营商。

3.5.4.3 基于服务质量

如果两个提供商希望以较好的服务质量相互补偿运输的各自的时延敏感流量，则每一方都希望检验另一方实际上已经做了其承诺去做的。

在QoS的情况下，看来必须要测量：

(1) 两个提供商之间在每个方向上交换的每一级服务流量的总数；以及

(2) 所提供的服务质量的度量。

测量服务质量是非常复杂的，无论是从技术层面来说，还是从商业层面上来说。

限制：

- 提供商之间的承诺主要是在平均时延和时延的方差方面，首先，重要的一点是记住这种测量活动暗示着网络运营商之间的协作程度，对于相同的最终用户客户而言，网络运营商是直接的竞争对手，每个运营商都会比较敏感将其网络的内部性能特性揭示给竞争对手。两者都不希望另一方向预期的用户揭示自己网络的局限性。

- 其次，可能需要关注测量服务器–在运营商自己的网络内运行，为了竞争对手的利益 – 可能会变成操作上的恶梦，或者可能暴露自己网络周边的安全问题。

3.5.4.4 以批量为基础（也可称为“互连旅馆”）

原有的互连计费体制即按分钟计费，无疑会使顺利的理赔复杂化，原因是 NGN产品是以容量、服务质量和服务等级为基础的。由于流量聚集出现在公共节点上，因此有必要批准适用的NGN互连费用计费以成批使用为基础，而不是以当前流行的每分钟为基础。在NGN环境下，总的网络成本和运费相对于业务量会变得非常小，因此，与每业务量单元有关的平均网络费用会下降，以批量为基础的互连费用计费将在运营商之间建立一个完全公平的竞争环境，有助于从不必要的诉讼和结算争论中节约诉讼费和时间。

在这一点上，确定什么应该被监管、什么可以留作相互协商也是十分必要的。

3.5.5 互连方案的经济影响

NGN承诺简单网络架构、更高的带宽、较少的网络部件、更低的成本和更多的功能性。而且传输和服务之间的区别将允许商业模式、网络部件和应用独立地发展。因此，下一代网络意味着技术的变革，产品和服务提供的变化，最终是由下一代（接入）网络引入导致的市场结构的变化，进一步（NGN和NGA）也会影响费用计算的方式，原因是新的成本驱动和成本/容量关系（CVR）。监管成本计算和计费体制应反映这些发展。显然，过去在电信网络中建立的以语音为中心的成本观点必须考虑数据日益增长的作用，以及语音成为“另外一种形式的数据通信”的事实。这意味着NGN环境下成本观点和分析方面的实质性变化。

当关注市场发展时，新的零售资费结构（特别是由批发收费和按时计价收费方面的增加引起的）和新形式应用，尤其是在移动宽带和IPTV方面的增长，改变了期望的网络体系结构，并影响了运营商的成本水平和成本结构。随着全IP网络中数据流量增加以及多个业务共享网络，固定成本的更少部分被分配给了语音服务，这意味着数据业务驱动的规模经济减少了语音服务的成本。

实现IP和NGN网络意味着网络正在变得比现在更为集中，这很可能会激发更少数量PoI的实现，重要的一点是规章制度例如关于资费结构和水平，正在考虑这种发展。

NGN产生的对网络经济的进一步影响是IP网络中网络层和服务层的分离，这意味着新的成本-容量 – 关系（CVR）作为传输成本将会下降（由于全IP网络，获得了规模经济和范围经济的好处），但是控制层和服务平台的成本增加了（由于在软交换和IMS平台方面的额外投资）。由于控制层和服务层将全部的网络负载、活动最终用户的数量、呼叫建立的数量以及信令作为成本驱动，这种分离可能会推动新计费体制的实现。

通过放弃技术中立原则并强迫运营商在IP基础上互连可能会加快向IP互连的过渡，这可以通过以下要求当作寻求者/提供者体制的一部分来实现，当寻求者请求IP连接时，其他的运营商会被迫提供上述的连接。这种配置的优点是IP互连将会受到最高级运营商需求的驱动，否则，向IP互连过渡不会大规模出现直到主要的运营商确认感兴趣，然而，强制执行IP互连会产生许多问题，包括如何设立一个参考报价以及如何管理互连使用费用和互连链路费用。

从目前大量的PoI来看，一些运营商愿意看到NGN中PoI的减少，因为这肯定会影响现有运营商的状况以及将来QoS的管理，但是出于某些担心，这不应通过迅速改变PoI的数量和体系结构来实现。

目前，大多数服务提供商正在向基于IP的网络过渡，尽管语音业务在内部是通过IP传送的，但互连仍然是基于TDM和CS#7技术。由于会在基于分组和基于电路的网络之间产生多个会话以便由两个或多个网络处理业务，呈现出很低的效率。只要当前采用多层互连点的互连结构保持不变，呼叫路由选择的效率就不会高，另一个负面影响是NGN的所有优点，包括新服务创建和新商业模型建立等都会被取消。

将来，为了提高效率，将不得不实现基于IP的互连以取代基于TDM的互连。当前，现有的服务提供商已经实现了基于TDM的互连，如果这些网络过渡到IP互连，则需要额外的投资。因此，一方面必须要从TDM向IP互连过渡的过程中，找到一次性投资之间的平衡点，而且必要要从这种过渡中获得潜在的静态和动态效率增益，由于成本主要由原有的服务提供商承担，向IP互连过渡的动力受限。

3.6 适合 NGN 的法律框架

NGN部署将需要大量预先支付的费用，投资者在进行如此巨大的投资之前需要稳定的监管和法律环境。与向NGN过渡有关的监管挑战和障碍、新型服务提供商的出现、改变商业模型、网络安全风险、竞争和公平竞争环境等都需要优先加以考虑。除非适当地重新定义许可条件和规则，否则向NGN平滑过渡将会非常困难。考虑到所有上述问题，假定各个国家处于快速网络和基础设施发展的阶段，是时候提出与NGN有关的监管和许可的问题了。这不仅有助于更近地查看许可证发放和规章制度，而且将有助于降低运营商的投资风险。不同国家的规章制度起初面对的是接入服务提供商的（即基本服务运营商和蜂窝移动电信服务运营商）远距离服务和互联网服务提供商（ISP）。每个许可下的服务都被严格定义，在其他电信许可下的任何特殊服务重叠的可能性非常小。后来的统一访问许可，在该许可下一个许可证能够提供不同的接入服务，即固定移动网络和互联网。有效演进的许可框架带来了电信部门的大量投资，从而导致大幅增长、更好的服务质量、竞争、用户的选择权，最重要的是覆盖广泛地理区域和人口的电信服务的可用性。电信部门的快速增长已经公平地见证了快速的技术进步。当服务严格绑定部署的交换类型时，先进的网络架构和体系已经轻易地促进了新服务和应用的提供，这在以前是不可能的，那时服务与安装的交换（交换机）类型是严格绑定的。这些新进展正在推动大量的增值服务和应用，这些服务和应用能够由模糊了不同许可之间界线的不同平台提供。例如，宽带对于互联网服务提供商是允许的，但相同的平台也能支持互联网电话。IPTV和许多按照惯例在接入服务提供商许可之下的第三方业务，从技术上说都能由ISP通过宽带服务提供。监管机构面临的挑战是如何在现有的规章制度和电信部门出现的快速技术发展之间保持平衡，坚持现有的规章制度可能会限制技术进步的成果，使其沦为平庸；然而，允许新技术和应用以及鼓励采用IP网络，会与现有的法律规定相矛盾，可能会影响公平的竞争环境。尽管某一学派主张鼓励向NGN过渡，因为NGN是用户友好的，使得用户能以较低的费用使用高级的服务和应用，但是其他人认为NGN只不过是技术进步而已，因此，他们觉得不存在法律上的关注点，是否向NGN平台过渡的决定是商业性的，因而他们觉得这可以留给服务提供商来决定，按照他们的说法，不应该篡改现有的经受时间考验的许可框架。

向NGN过渡意味着不同的商业模型、服务和市场之间的界线正在消失，为了应对这种情况，许可制度必须包含给网络运营商的通用许可，使这些运营商能够提供单一全IP网络的任何基于IP的服务和应用。

修改许可证时要考虑的一个主要问题是委托IP互连的问题，此外，存在一些轻微的与许可证发放有关的问题，该问题可能会对服务提供商造成负面影响，但这些不会成为向NGN过渡的主要障碍。

完全技术中立许可制度的变化对于向NGN过渡非常重要，这些是技术中立的，不需要等待进一步的技术或者即将出现的市场发展。

讨论规章制度对于实现和促进NGN的作用是一个有趣的问题，NGN显著地改变了由技术和经济过程引发的市场，在竞争的环境下，NGN需要一个特定的框架，然而，问题是这样的框架是否能够和是否应该被预先确定，或者市场力量是否应该占上风，当竞争受到阻碍时规则是否应该介入。

规则的作用是在市场失败的情况下介入，例如：滥用市场支配力或者丧失市场准入等。这看起来是市场开放时期的“自然”发展，期间尽管是正规的市场开放也存在合法垄变为事实垄断的风险。现在的情形已然不同，需要用市场失败证实规则是有效的。向NGN过渡不会立即显示市场失败、竞争扭曲或丧失准入，这些结果都是可能的，取决于当地的情况，但是向NGN过渡和例如市场支配力之间并没有固有的联系。因此，任何“规划”向NGN过渡的方法从监管的角度来说都必须慎重考虑。可选的方法是让市场力量先发挥作用，只在市场不能履行其功能时才进行干预，这也意味着向NGN过渡应遵循技术和市场定义的“路线图”而不是监管路线图。

4 NGN 部署的回顾

4.1 NGN 部署的目标

过渡的场景和计划应该根据每个国家或运营商的情况而定。总体而言，要求迁移时需要考虑两个层次的观点。

首先一个观点是认为向 NGN 过渡是改进基础设施的一种方式。在这种情况下，过渡计划应该关注于通过包括扩张“宽带”部署等所谓的“全 IP”取代原有的电信。

另外一个观点是认为向 NGN 过渡是他们社会的推动者，例如鼓励电子社会，在这种情况下，过渡计划应该关注于支持融合，例如固定移动融合以及支持各种应用（例如电子健康，USN 等）。

建议将这两种观点平衡结合起来，这种平衡将会因每个国家或者运营商的情况而不同。

4.2 学习以前的经验

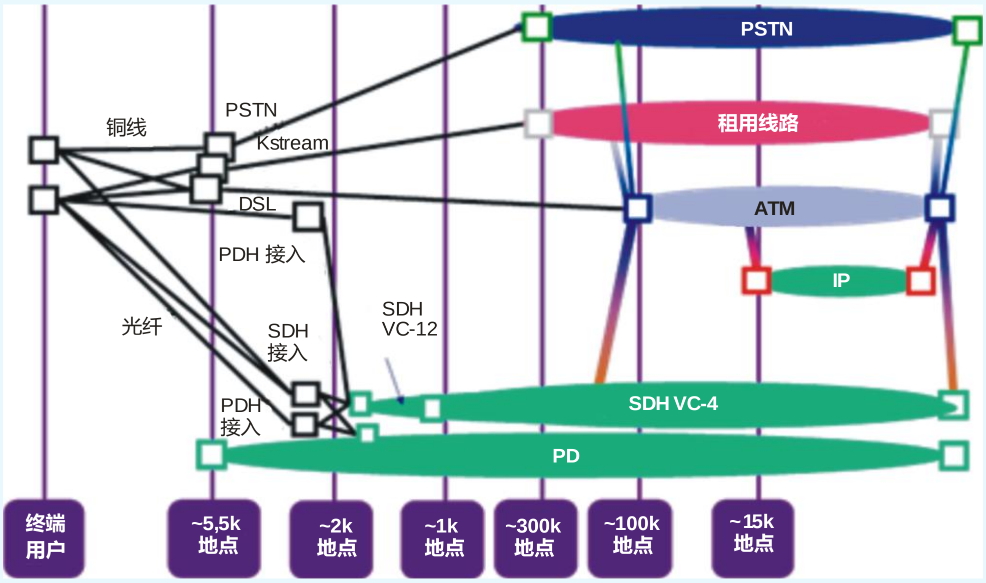
4.2.1 *改善基础设施*

BT 已经发布了向 NGN 过渡的先进经验，名为“21 世纪网络”，它将对 BT 网络 21 世纪的业务发挥重要作用。BT 的 21 世纪网络计划有趣之处在于将目前的网络结构和 21 世纪网络的结构进行了对比。这给我们传递了一个重要的信息，即 NGN 会带来什么好处，尤其是对网络运营商而言。

下图 41 为目前 BT 的网络结构，包括各种传输网络和各种不同的节点，它们根据负责的业务和地理位置发挥不同的作用。就核心网而言，也有根据业务具体特点支持不同路由选择的不同网络。

这种面向服务的结构和网络配置引起了基础设施要素的重复，例如传输节点或路由节点。此外，它还要求复杂的业务和网络运营，因为具体业务会涉及不同的系统。这些方面需要更多的投资，可能会引起供应重复，可能会要求额外的运营和维护资源，从而需要更多的人力费用和资金。

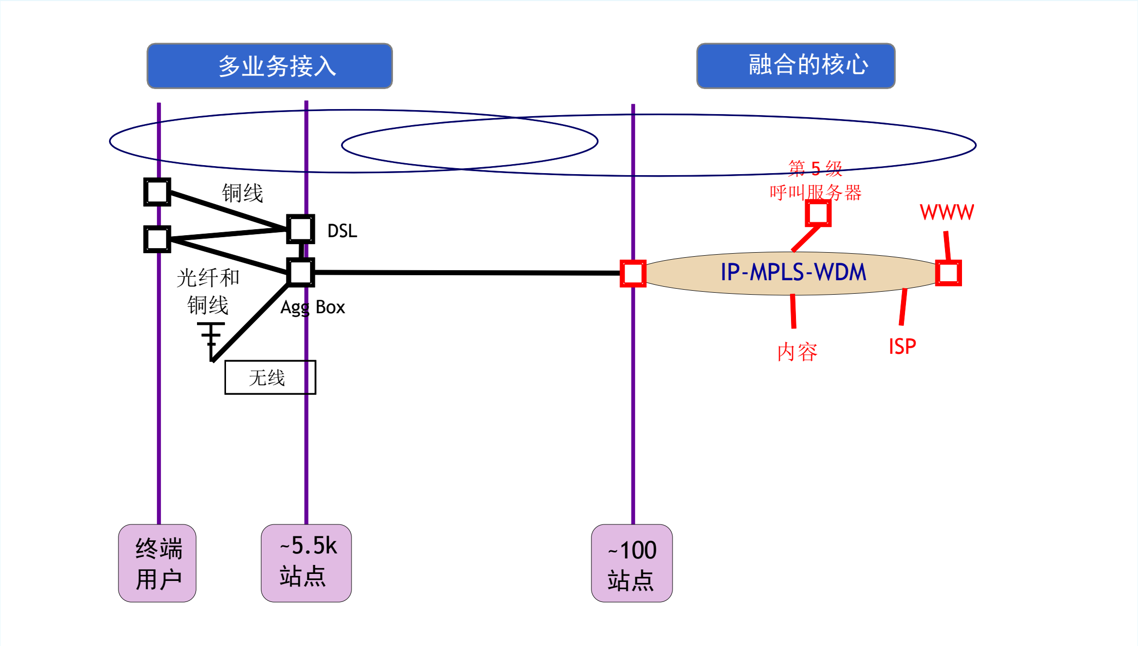
图4-1：BT原有的网络结构及节点数



对比目前BT的网络配置，21世纪网络的结构更为简单，但是能力更强，无论是语音业务还是宽带业务。图4-2是21世纪网络的简单的配置模型。图4-1显示了结构的简化，尤其是在保持客户全覆盖的同时大幅减少节点数。该结构取自“全IP”特性的优点，使核心网的配置更为简单，因此所有服务都经过不同流量的IP核心网传递，从流量管理和服务提供角度来看，对不同流量的处理不同，但是使用相同的系统。

该结构的另一优点是缩短并延伸客户的接触点，使网络覆盖离客户更近。这就是为什么该结构能在客户方保持最大数量的节点，而又能从以前的结构中去掉其他的节点。

图4-2：BT的21世纪网络结构及节点数



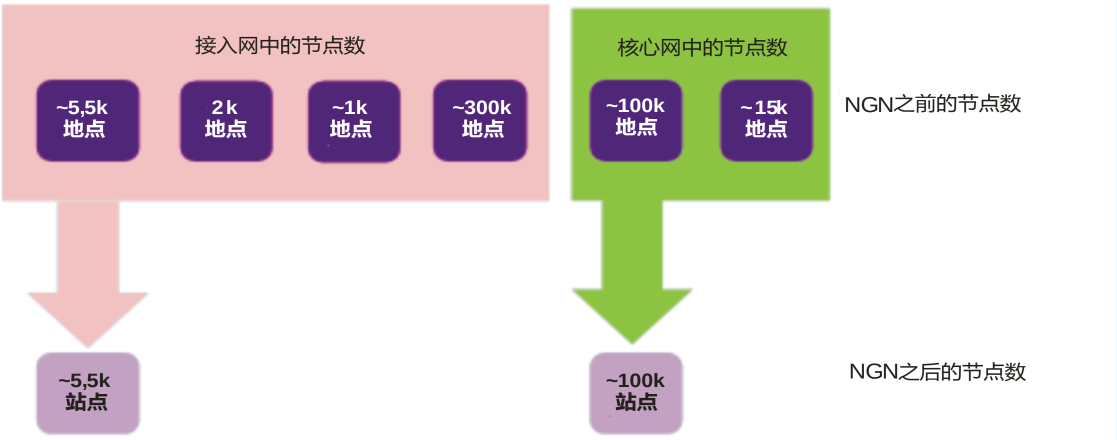
在BT的网络中采用NGN被称为“21世纪网络”，显示了如何改进基础设施以满足未来的商业趋势和用户/运营商的要求，需要仔细地研究BT实现NGN的情况，从基础设施改进方面获取更多的知识。

其中一份报告告诉我们这种新的结构将有助于减少30~40%的温室气体排放，温室气体排放目前已经成为全世界面临的严重问题，下面简单的计算可以为这份报告提供支持：

- 减少接入节点：从 8.8 K 个站点到 5.5K 个站点（减少 37.5 %）；
- 减少核心节点：从 115 个站点到 100 个站点（减少 14%）。

本报告不打算从成本方面评估这个结果，但如果包含每个站点的运行成本的话，通常可以推断节约了大量的成本。

图4-3：BT得益于21世纪网络



4.2.2 促进社会发展

其它类型的向NGN过渡是提供建立新社会例如电子社会的基础设施，这种方式已经在韩国公布，被称为“BcN：宽带融合网络”，目前正在韩国部署。

韩国案例的不同之处在于他们在宽带部署的几乎最后阶段才启动这项计划，因此，他们对BcN的愿景已经完全不同于BT的案例研究。主要包括以下几点：

- 建立全世界当前技术发展水平的信息基础设施；
- 创建一个使用高质量多媒体业务的环境；
- 根据 IT 行业市场成长制定核心计划。

如同这些设想描述的一样，韩国更关注于建立他们的新社会基础设施，而BT关注于改善他们的基础设施，因此韩国采用了任务共享模型类型，其中每个部门承担不同的任务，据此，政府的作用是鼓励发展将用于建立电子社会例如电子教学、电子健康、USN等的新业务和应用，网络运营商更关注于升级他们的基础设施，以便在持续提高接入网容量、提供更大的带宽给客户的同时，支持例如FMC和IPTV等融合业务。

5 案例研究

5.1 关于 LLU 和光纤投资的案例研究

土耳其国家监管机构（NRA）ICTA做出了光纤投资的决定，根据ICTA的标注日期为2011年03月10日的决议，运营商的光纤投资在5年期间或者直到零售互联网用户的比例达到总的宽带用户的25%水平的时候，不会受到任何限制，这意味着光纤业务在这段时间内不会在任何市场定义中被评估，土耳其仍处于由现有网络向NGN过渡的过程之中，在过渡过程开始时，依托固定线路业务的当前运营商土耳其电信的应用，ICTA对形势进行了深入的分析，在评估期间，ICTA还考虑到了如何以最佳的方式促进光纤基础设施部署，以及通过鼓励运营商投资将其在最短的时间内展开。

在这5年期间，土耳其电信还将以转售的方式提供大量基于光纤基础设施的业务，在平等条款和没有歧视情况下的比特流接入客户，另一方面，光纤部署领域中的规则不应与准许的应用相矛盾，施行的法律必须支持光纤免税。

为鼓励运营商进行光纤投资并且在最短且合理的时间限内获得投资利润，可以设想土耳其 NRA 的光纤免税决定是一个备选的方法。然而，毫无疑问应该对这个免税决定的效果和结果进行监督。我们应记住到新情况所需的所有方法都包含了一些风险，可能会导致负面的结果。但是，我们相信土耳其 NRA 的上述免税决定可以作为其它的具有和土耳其类似市场结构的国家的榜样。

这个规则旨在保护投资而不是阻碍光纤分配。总之，各个国家在部署光纤时应该分析他们自己的市场结构和基础设施，各个国家自己的监管机构应该根据其市场结构、基础设施特性以及国家的福利情况决定一种保护投资的方式。

5.2 关于 NGN 部署的案例研究

国际电联最近启动了一个针对亚太地区发展中国家的项目，根据特定国家的经历对向 NGN 过渡的技术和管理方面进行评估，其目标是：通过亚太地区有关 NGN 问题的讲习班和培训，有助于在向 NGN 环境过渡的过程中培养能力，同时通过促进合作机制宣传与 NGN 有关的案例研究，关于亚太地区实现 NGN 的最佳实践的报告—关于印度、菲律宾、斯里兰卡和孟加拉国的案例研究可以通过以下地址在线找到：http://www.itu.int/ITU-D/tech/NGN/CaseStudies/CaseStudies.html

6 适合有前途技术的方法以及 NGN 部署的状况

6.1 确定最具前景的 NGN 构建技术的方法

该技术是以信息通信网络构造或重组的仿真原理为基础，以便评估使用某些满足网络所有者全部要求的技术集的成本和转变时间。

图 6-1 所示的是该方法的一般算法，该算法包括平行的（独立的）四个准备过程，其中的结果进一步用于决定在信息通信网络构造的成本和施工工期（重新组织）方面最有希望的技术。

四个步骤的第一步（用图 6-1 中的数字 1 表示）由两个基本步骤组成：输入现有的或规划的网络的结构信息，分配要建立的独立部分。这两个步骤的第一步包括每个网络部件（硬件或者通信信道）到升级或建立应考虑的那些层次信息的逐步介绍，这一步除了每个部件的类型和技术要求以外，也应输入有关部件相互之间通过特殊接口（既有相同层次的，也有和其它层次的设备）互连的信息。

并确定独立网络部件的位置信息。起初的这两个步骤需要有关于每个网络要素（硬件或通信信道）的逐渐深入的信息介绍。除此之外，每个要素的类型、具体说明、各要素通过特定接口进行互连的相关信息等都必需输入。

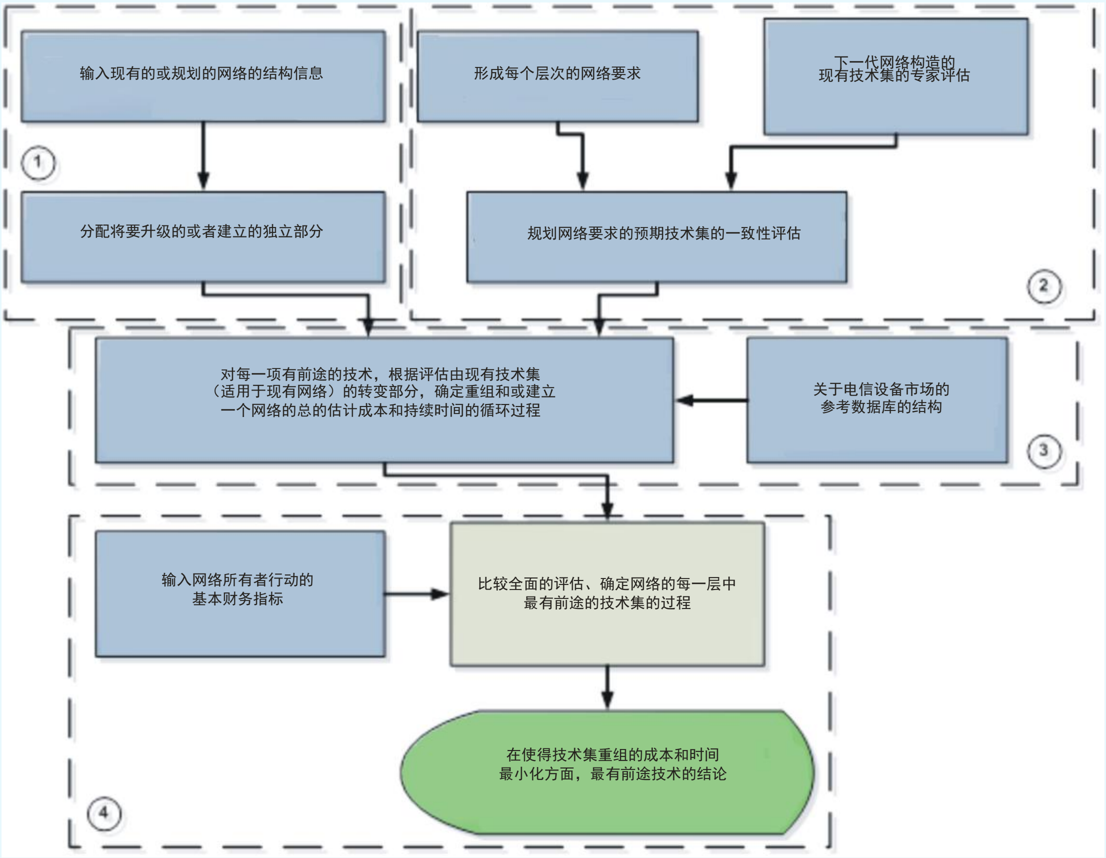
第二个步骤（用图 6-1 中的数字 2 表示）旨在从总的当前看来比较有希望用于升级或构造信息通信网络的技术集中，指定那些能够满足网络所有者需求的技术集。这一步骤主要由三步组成：形成各个层次的网络要求，对用于信息通信网络构造的现有技术集进行专家评估，对有前途的技术集与所规划网络要求的一致性进行评估。这个步骤的结果是获得那些能够完全满足网络所者对该网络的要求的技术集列表（对于网络的每一个层次），向这些技术集的转变在其中每项技术的费用和重构时间方面，将与本方法的后续步骤相匹配。

第三个步骤（用图 6-1 中的数字 3 表示）就操作的步数而言是最复杂的，这个步骤包括对所有选择的独立部分（正在升级或者建立）循环评估转换为新的具有前途技术集（或者采用这些技术集的组合）后的一致性。升级现有网络和建立新的网络的主要区别在于：当升级现有网络时，要考虑拆除现有设备和/或现有通信信道的附加时间和费用。这个步骤的基础是专门形成的关于电信设备市场的信息数据库，包含了模型相互之间可能的互换性信息，这个步骤的结果一个在采用有前途技术集基础上的费用和网络（依据其层次）现代化（或构造）时间的向量。

算法的最后步骤（用图 6-1 中的数字 4 表示）包括根据比较成本和现代化（或构造）期限，考虑到网络所有者运行活动的基本财务指标（例如，通过规定电信网络运营商的资金回收期），确定每个层次网络最有前途的技术集。

应注意到图 6-1 所示的算法只显示了确定有前途技术集的一般原则，特殊条件下（建立一个新的网络或者重新组织现有的网络，不同层次网络的构造等）的详细说明涉及到了具体算法的使用。

图6-1：方法的一般化算法


输入现有的或规划的网络的结构信息
分配将要升级的或者建立的独立部分
1
形成每个层次的网络要求
下一代网络构造的现有技术集的专家评估
规划网络要求的预期技术集的一致性评估
2
对每一项有前途的技术，根据评估由现有技术集（适用于现有网络）的转变部分，确定重组和或建立一个网络的总的估计成本和持续时间的循环过程
关于电信设备市场的参考数据库的结构
3
输入网络所有者行动的基本财务指标
比较全面的评估、确定网络的每一层中最有前途的技术集的过程
在使得技术集重组的成本和时间最小化方面，最有前途技术的结论
4

6.2 NGN 部署的状况

国际电联数据库，特别是资费政策数据库显示了各种有用的统计数字。这个数据库的目的是跟踪和显示与不同国家中定价、成本/资费模型、分析会计、互连计费、通用业务管理和价格控制有关的资费政策应用的趋势。数据每年由电信监管机构和网络运营商提供，这反映了各个地区在完成调查表时的状况，下面的图 6-2 到图 6-4 显示的是来自国际电联世界资费策略数据库的、专门与下一代网络有关的统计数字。[3]

[3] 更多信息见国际电联的“ICT-Eye”，http://www.itu.int/icteye。

图6-2：运营商引进NGN系统的阶段，2012

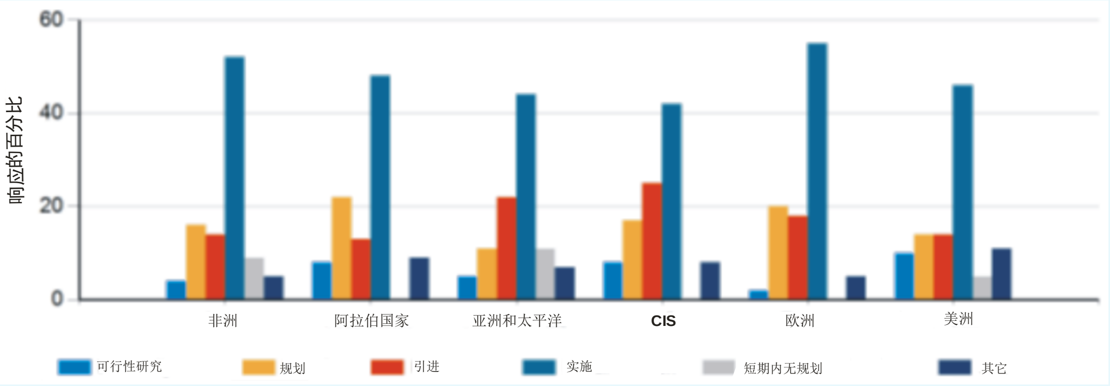


图6-3：NGN：IP网络用于语音业务的管理规定，2012

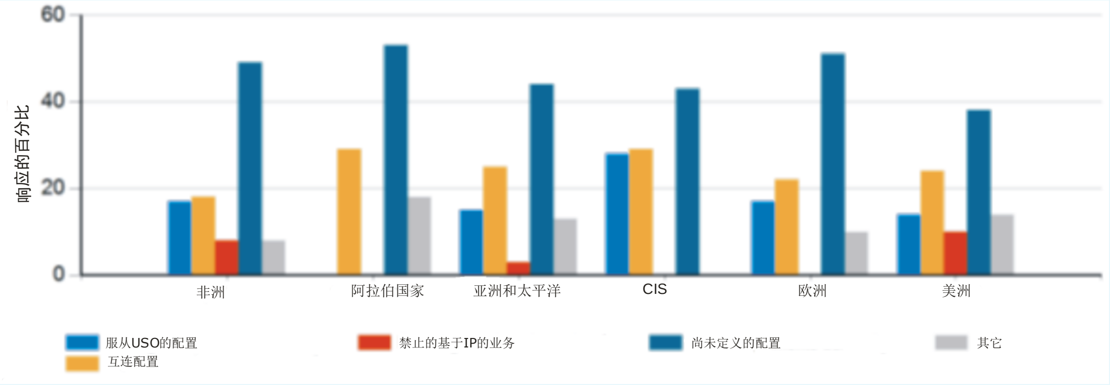
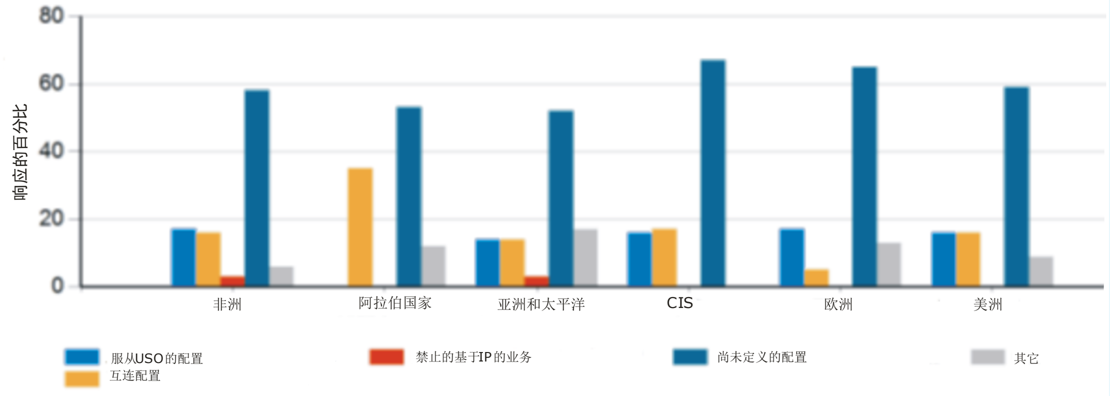


图6-4：NGN：IP网络用于数据业务的管理规定，2012



Annexes

Annex 1: Trends in Telecommunications

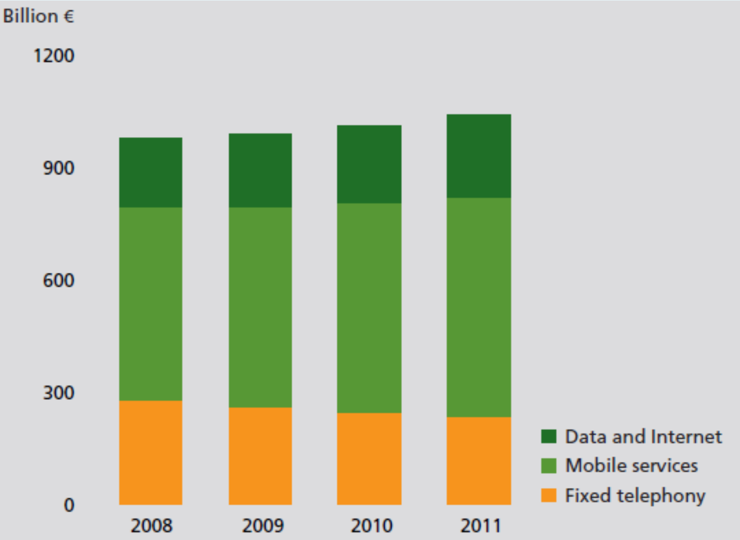
1 Market Trends

1.1 Overall Telecom Market Trends

General analysis of telecom market trend is rather positive in many of countries. Many of reports informed their last year analysis results. This report makes references to various reports: the analysis from Ofcom, United Kingdom published as "The International Communications Market 2012", ITU reports on "Measuring the information society: 2012" and "ICT Facts and Figures: 2011 and 2013" . These reports do not cover all areas on the world but give certain information to look at overall trend of telecom businesses.

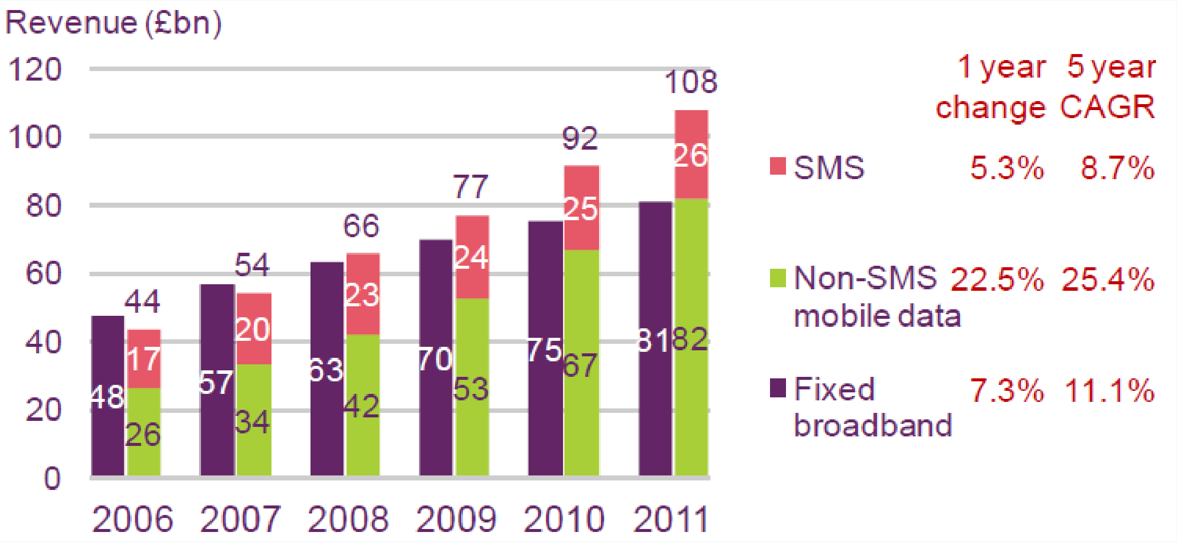
Figures from the ITU show that by the end of 2011 2.3 billion people (around a third of the world's population) accessed the internet globally, almost double the 1.2 billion figures recorded in 2006. Over this period growth in internet use was fastest among developing countries, and by 2011 62% of internet users were located in developing countries, an increase from 44% in 2006. This trend is lead by expansion in mobile and broadband services for data and internet as the key telecommunication market while fixed voice oriented services are continuously diminishing as shown in Figure 1-1.

Figure 1-1: Global telecom services market growth by segment (IDATE)



The report by Ofcom, United Kingdom indicated that there was rapid growth in the take-up of fixed broadband services across the 17 countries in the five years to 2011, during which time fixed broadband take-up almost doubled to reach 42 connections per 100 homes. Increasing take-up of fixed broadband and mobile voice and data services have contributed to an accelerating decline in the use of traditional fixed telephony services in most of the countries. Despite significant growth in fixed broadband take-up, revenues from mobile data services exceeded those from fixed broadband connections for the first time among surveyed 17 countries in 2011 as shown in Figure 1-2.

Figure 1-2: Fixed broadband and mobile data revenues (2006 ~ 2011) (IDATE)



As a total in the survey of Ofcom, mobile data has seen the fastest growth rate (CAGR) of 25.4% between 2006 and 2011 meaning that, for the first time in 2011, mobile data revenues (£82bn) exceeded fixed broadband revenues (£81bn, CAGR of 11.1%). The report analyzed that this growth in mobile data revenue has been driven by a rapid increase in the adoption of smartphones, from which it is much easier and quicker to access the internet. SMS revenues increased at a slower CAGR of 8.7% between 2006 and 2011. Although SMS volumes are still growing but revenues have failed to keep pace as operators have started to offer large bundles of SMS messages as part of subscription packages; this has stimulated use but caused revenue pressure for SMS in many markets. However, much of the revenue growth in fixed broadband in developed countries was realised towards the start of the five-year period when take-up was growing rapidly. Fixed broadband may now be approaching market saturation in many European countries, as the majority of households subscribe to fixed broadband services – limiting revenue growth for the year 2011.The Ofcome report identified three of the key developments which are transforming the global telecoms market, both in terms of industry structures and consumer behaviour:

- The mobile data explosion: the growth in mobile data, with key volume, subscriber and revenue statistics, and sheds some light on the transition from large-screen PCs to small screen smartphone mobile data use.
- Continued growth in superfast broadband networks: the deployment of superfast technologies across countries, and the extent to which consumers are migrating to these services.
- Increased use of text messaging: the contrasting levels of use and expenditure related to texting, and examine attitudes towards texting.

1.2 Trends in the Voice Service Market

The Ofcom report indicated that the fixed voice call volumes continuously fell in most of countries for which figures were available in 2011 except France, where they increased by 0.6% to 113 billion minutes during the year (Figure 1-3). The resilience of the fixed voice market in France is largely as result of high take-up of managed VoIP services, often provided as part of a triple-play bundle of fixed broadband and IPTV services over naked DSL. Naked-DSL-based broadband services do not require a standard fixed line, so VoIP over naked-DSL provides a low-cost alternative to voice calls made over traditional fixed networks, as no line rental is paid. It is this which is the primary driver of the 13.1% fall in fixed voice revenues in France in 2011, despite call volumes increasing during the year. In the UK, fixed voice call volumes fell by 10.0% to 116 billion minutes in 2011, this rate of decline being the fourth highest among 15 countries.

It is noted that the major drivers behind declining fixed call volumes are the low cost of mobile voice and text services and high smartphone take-up, which has contributed to the increasing use of alternative forms of communication such as email and instant messaging. France and the Netherlands (where VoIP use is widespread) were the only countries compared where fixed call volumes increased in the five years to 2011 (up by 1.8% and 0.4% a year on average, respectively). Conversely, the highest average annual rate of decline over the period (13.0%) was in Australia, where fixed call volumes halved over the period, largely due to the increasing use of mobile voice services. As a consequence, fixed voice revenues continuously fell in 2011, the fastest rates of decline, with revenues falling by 17.8% in China and 15.3% in India during the year.

Figure 1-3: Fixed line call volumes and revenue, 2006 and 2011

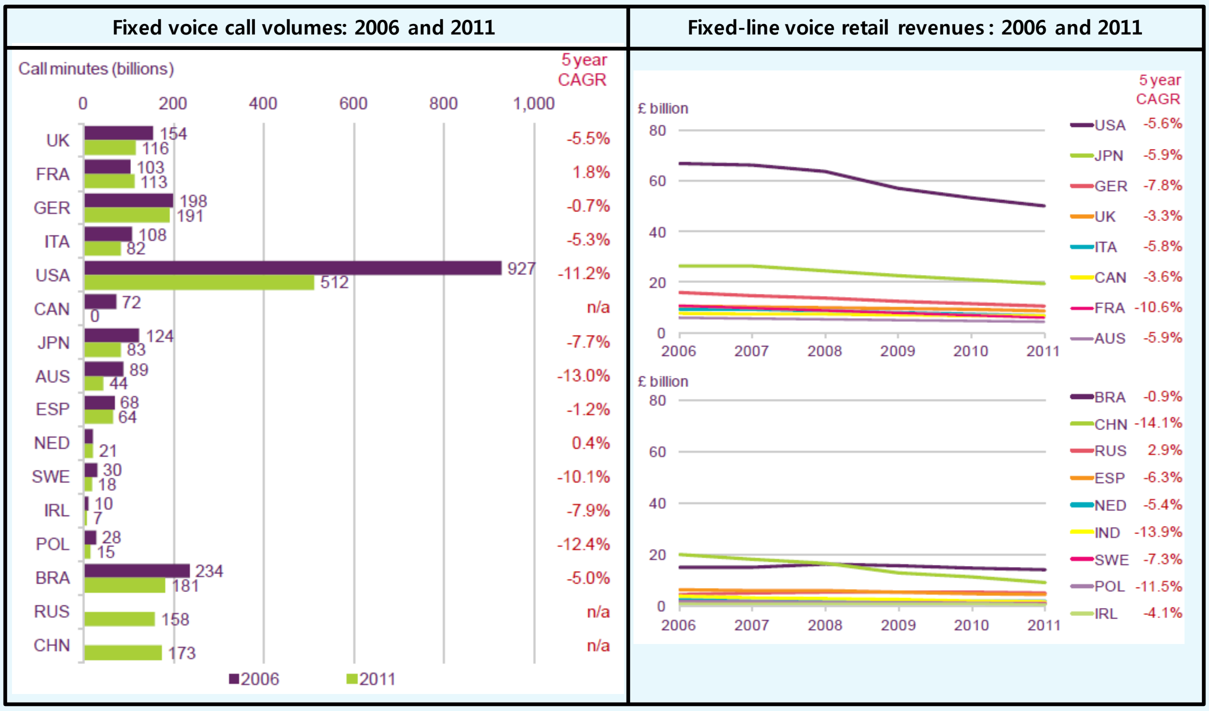
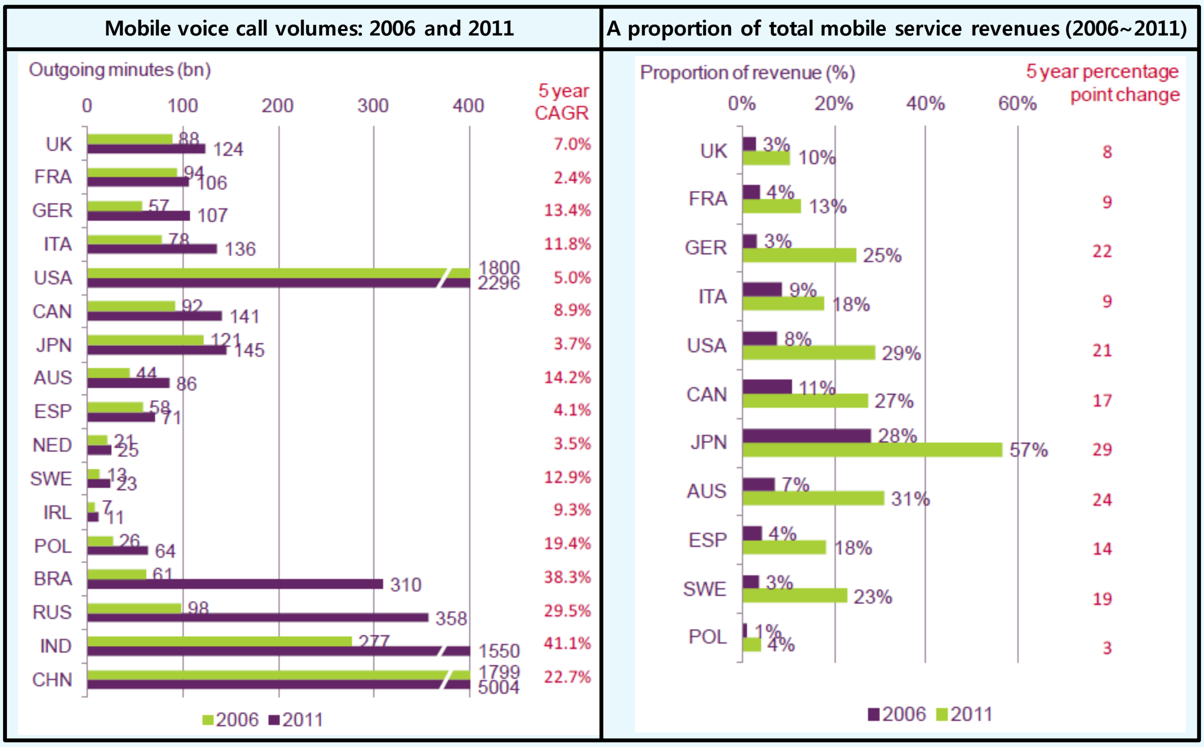


Figure 1-4 shows the status of mobile voice call minutes and revenues by Ofcom report. The countries where the highest proportion of calls originated on mobiles in 2011 were China (97%), the United States (82%) and Poland (81%). In China and Poland this is partly due to the limited availability of fixed telephony networks, while the proportion of calls that are mobile-originated will be overstated in China, the US and Canada as the mobile call volumes used in the calculation include incoming call minutes. Germany and France were the only comparator countries where less than half of voice call minutes originated on mobile networks in 2011 (36% of voice call minutes were mobile-originated in Germany in 2011, while the figure was 49% in France).

Figure 1-4: Mobile call volumes and revenue, 2006 and 2011



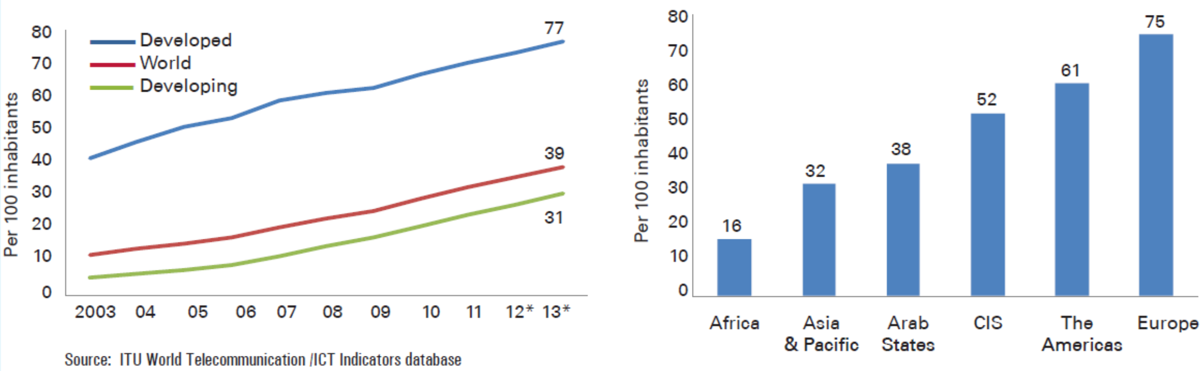
Mobile voice call volumes: 2006 and 2011

A proportion of total mobile service revenues (2006~2011)

1.3 Broadband Market Trends

Benefitting fixed broadband and mobile, especially smartphones, internet users (use of more data including information) is increasing as shown in Figure 1-5 (by ITU, ICT facts and figures 2013).

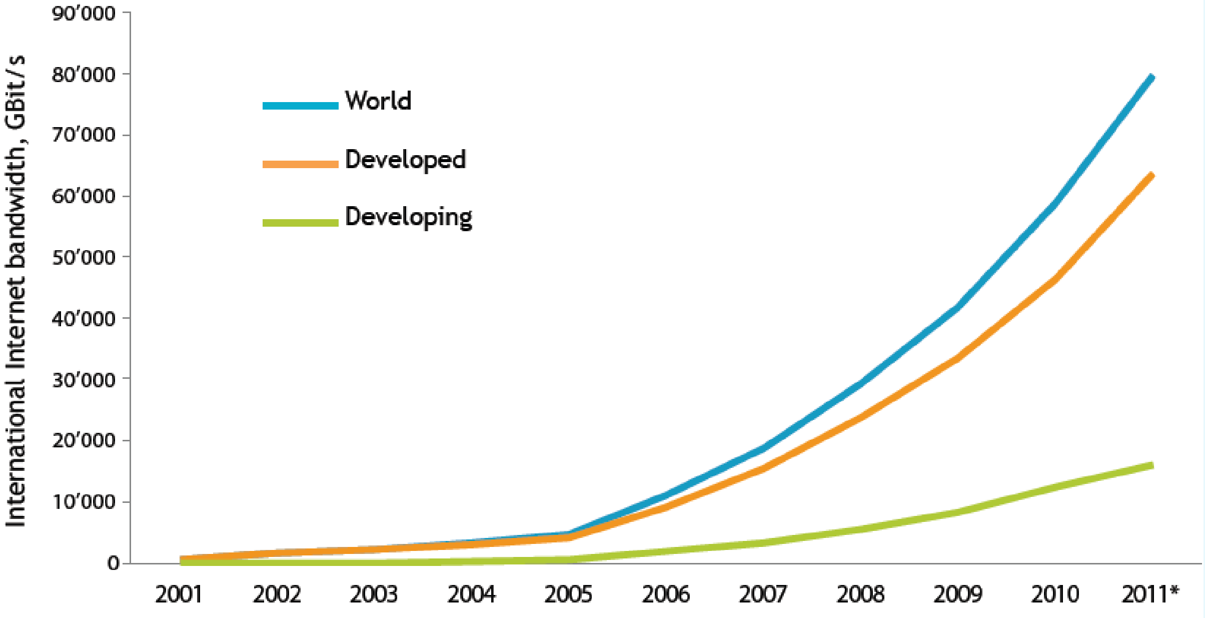
Figure 1-5: Internet users by development level and region



Source: ITU World Telecommunication /ICT Indicators database
Note: * Estimate

As a consequence, bandwidth consumption of the world continuously increased as shown in the Figure 1-6 below (by ITU, ICT facts and figures 2011).

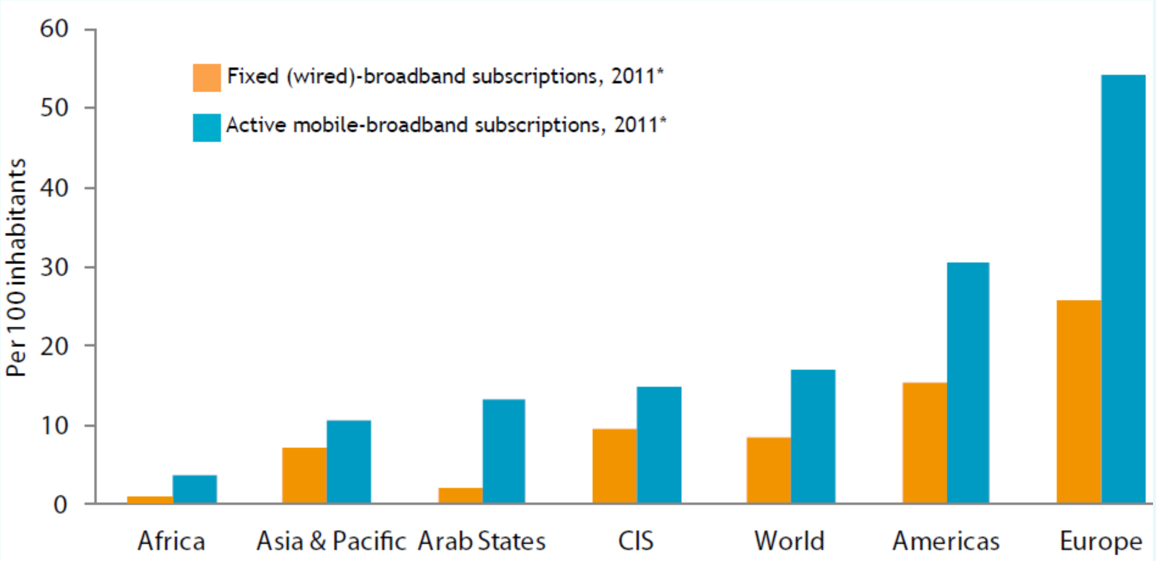
Figure 1-6: Growth of bandwidth



Note: * Estimate
Source: ITU World Telecommunication/ICT Indicators database

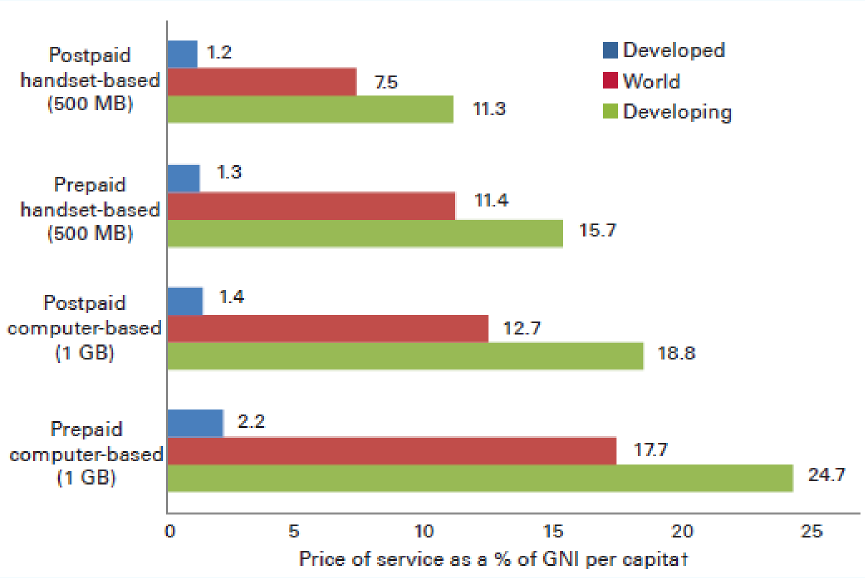
One interesting phenomena is that mobile broadband users are exceed fixed broadband users as shown in Figure 1-7 (ITU, ICT facts and figures 2013). This phenomena is apparent in all of the regions, in both developed or developing countries, which in turn means users enjoyed connectivity over mobile environments.

Figure 1-7: Status of broadband in 2011



Following the analysis by ITU as shown in Figure 1-8, it is noted that mobile broadband is more expensive in developing countries but considerably cheaper than fixed broadband services. By early 2013, the price of an entry-level mobile-broadband plan represents between 1.2-2.2% of monthly GNI p.c. in developed countries and between 11.3-24.7% in developing countries, depending on the type of service. However, in developing countries, mobile broadband services costs are considerably lower than fixed-broadband services costs: 18.8% of monthly GNI p.c. for a 1 GB postpaid computer-based mobile-broadband plan compared to 30.1% of monthly GNI p.c. for a postpaid fixed-broadband plan with 1 GB of data volume. Among the four typical mobile-broadband plans offered in the market, postpaid handset-based services are the cheapest and prepaid computer-based services are the most expensive, across all regions.

Figure 1-8: Price of mobile-broadband services, early 2013



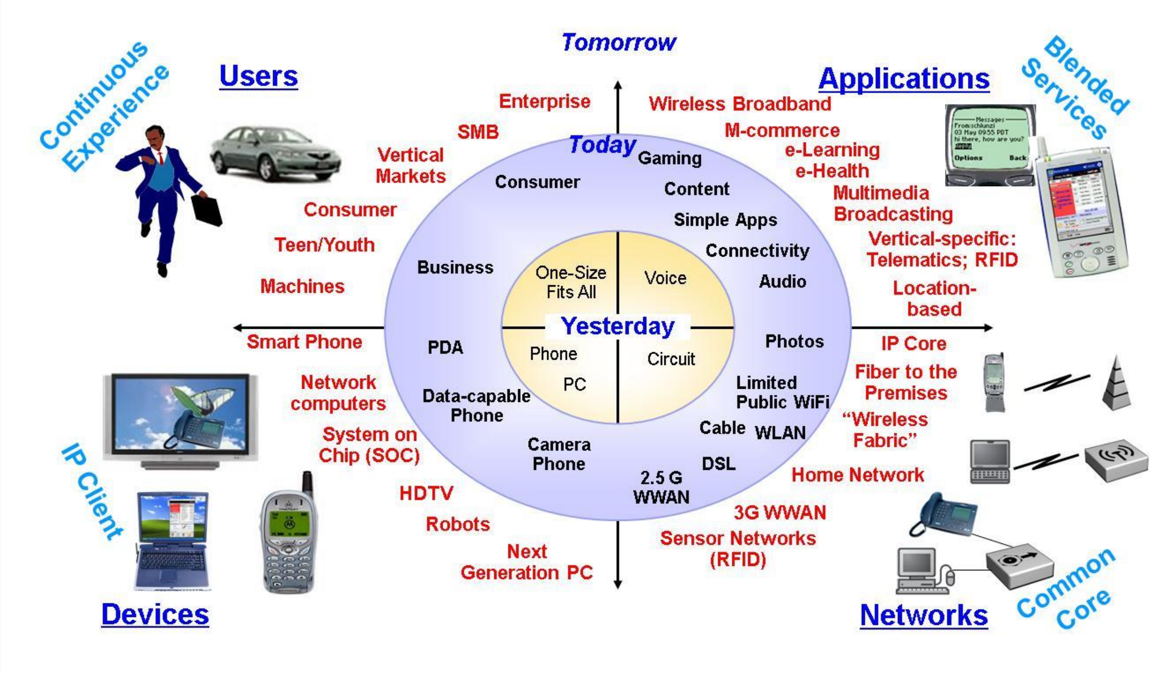
2 Overall Trends in Telecommunications

2.1 Overall Development Trends

There are various angles to look at trends of development in telecommunication such as users' aspects, services/applications' aspects, devices' aspects and networks' aspects etc. Because of the recent developments in telecommunication (should be included with the concept of ICT), this is not an easy task with short sentences like in this report. Therefore this report broadly looks at the development trend from these four different aspects.

In this regard, following Figure 2-1 provided an overview of technology development, taking into account the evolving trends related to users and services/applications.

Figure 2-1: Abstraction of development trends



- **User perspective:** Previous users were quite well-fitted with fixed types of services e.g. a black phone for voice service and a facsimile terminal for graphic service. So it featured as one size service fits all kinds of users. However, users today request more dynamic types of services depending on their lifestyle, and whether they are using the service as a consumer or for their business, etc. This is likely to continue developing in the future and as a result their usage of telecommunication services and applications with require services at anytime, anywhere and on any device.

- **Service/Application perspective:** Voice services have been the key service for telecommunication providers during more than 100 years. This has is now expanding to cover more other services than just voice, including multimedia services with broadband connectivity which are available today. It is further anticipated to expand to cover various services/applications mixed together, which sometimes is called convergence and other the provision of blending services.

- **Network perspective:** Previous circuit oriented networks have evolved to the packet networks of today (mainly using internet protocol (IP)), including continuously increasing bandwidth using xDSL and fibre optics and wireless technologies such as WiFi and WiMAX. This will be leveraged by common core networks in the near future, which will be IP-based but enhanced by other elements such as Quality of Service (QoS) and security.

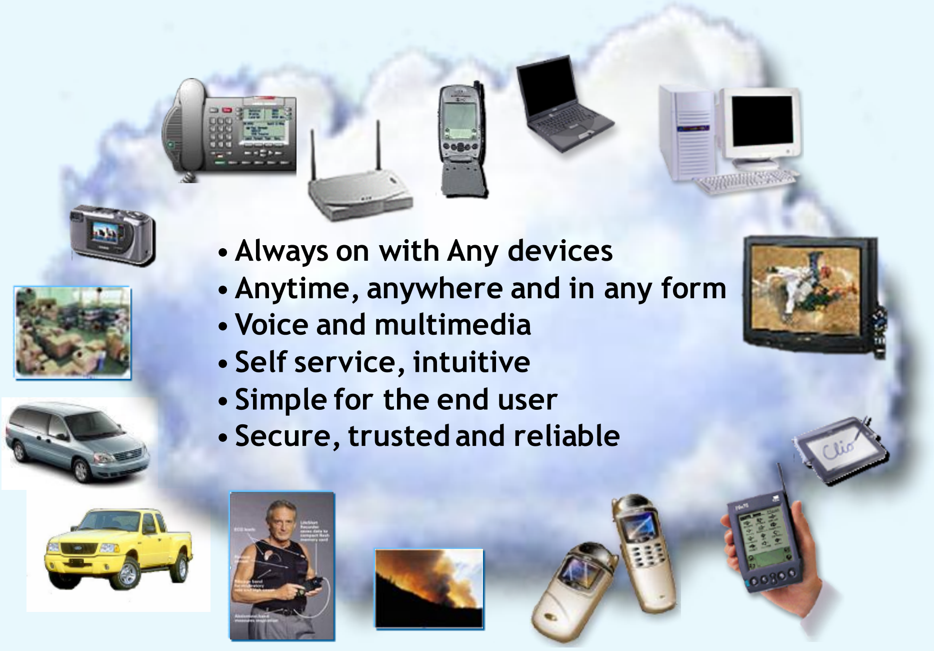
- **Device perspective:** The area which has seen the most remarkable development is the device area. The key themes in the development of devices include the need for them to be portable, multi-functional and smart. Moreover, as the use and growth of IP is expected also for the near future, devices should be IP-enabled.

2.2 Convergences

During the past several years, the ICT domain has continuously developed to support various types of convergences with a vision of "Any Time, Any Where, Any Services and Any Devices." This trend has been led by the development of the associated technology and the notion of "any information/service over any transport infrastructure." One traditional example of this is VoDSL (Voice over DSL). DSL was developed to provide broadband connectivity but today this is used for voice services such as VoIP. Another example is TVoMobile (TV service over Mobile). Mobile was developed to provide voice services while users move around, but today mobile is also used for watching TV.

Especially with development of NGN, fixed mobile convergence (FMC) is now becoming the first instance of converged fixed and mobile services, and IPTV is also following with the convergence between telecom and broadcasting. Moreover, convergences using ICT are rapidly expanding to cover many of the industrial areas.

Figure 2-2: High level view of the converged environment


• Always on with Any devices
• Anytime, anywhere and in any form
• Voice and multimedia
• Self service, intuitive
• Simple for the end user
• Secure, trusted and reliable

Convergence can be classified into two main groups:

- **Internal Convergence** (within the same industry): This means the convergence between different services and/or networks but within the same industries, such as FMC and IPTV. FMC is the convergence between fixed and mobile, but both two belong to the same industry, the telecom industry. IPTV is the convergence between telecom and broadcasting but they also belong to telecom industry in their wider interpretation.
- **External Convergence** (between different industries): This means the convergence between/amongst different industries, e.g., Telematics/ITS, USN, e-Health, Networked Robotics and others. This type of convergence requires more complicated processing not only from the technical aspect but also from regulatory and political aspects.

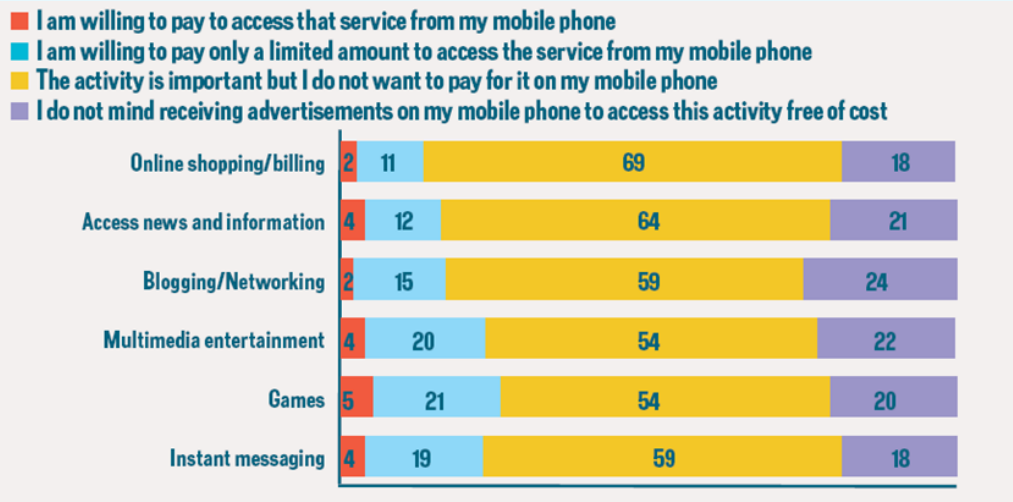
Whether internal or external convergences, the high level view of how services are used in a converged environment can be show as in Figure 2-2 above. Networks will then look like a cloud which allows for the provision of connectivity to the devices anywhere, anytime and where any service can be delivered to any device. Consequently, end users can make use of the services they wish to use in close relation to their real life using handy smart terminal devices and sensors (e.g. USN), even while driving a vehicle.

2.3 Trend of User Willingness

As technology develops further (or maybe even the other way round), end user willingness to pay for specific telecommunication services are also continuously changing. Actually it is better to say "expanding" or "increasing."

Figure 2-3 shows some interesting results of users' willingness to pay for services. All types of services shown in the figure (such as online shopping, accessing news online, etc.) have been identified as important activities for end users, which they are not willing to pay for, especially when they are using their mobile phones. However, there is a certain amount of willingness to use the services, even using the mobile phone, when advertisements cover the associated costs. Both these two cases show that there are potential customers who are willing to use such services if they are made available in an economically beneficial way, such as using flat-rates for the fixed-mobile convergence access.

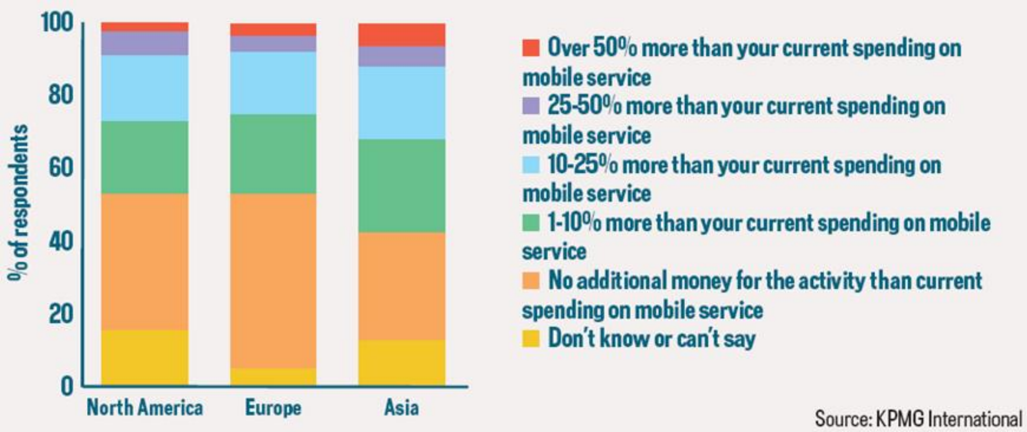
Figure 2-3: Customers' willingness to pay for services



Source: KPMG International

Figure 2-4 shows the results of research done on end user willingness to pay for convergence services. One can see that people in Asia show more interest in converged services than those living in other regions.

Figure 2-4: Customers' willingness to increase spending on converged services



Source: KPMG International

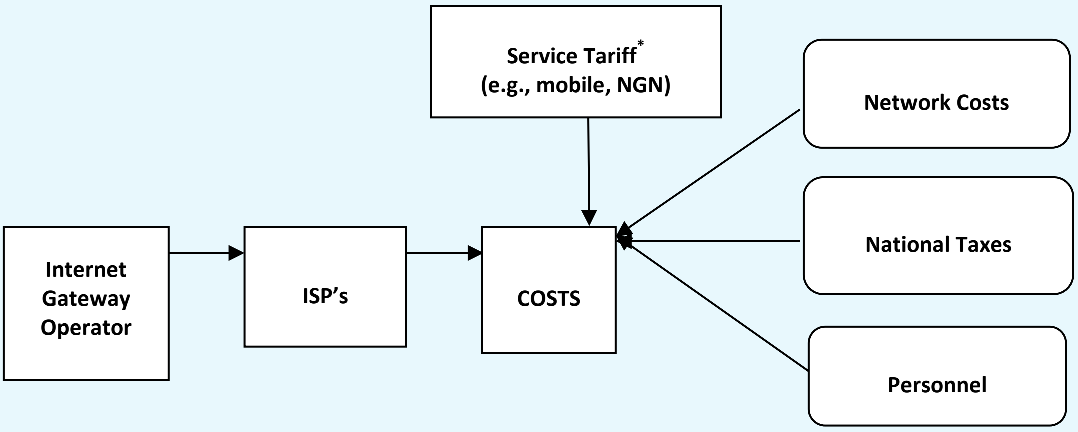
Annex 2: Tariff Considerations for Data Services including NGN

In the voice market, the tariffs are determined by competition. The Regulator sets a uniform interconnection rate across all networks and allows the operators to come up with their own end user rates which are to a large extent determined by competition allowing price differences between the operators. However, tariffs for data services with the advent of NGN's is different, since data services are, in general today, supported by internet interconnected through the gateway.

[Note: In some countries (for example The Gambia), the gateway is still in a monopoly under the incumbent, thus other providers such as mobile operators still need to go through an ISP to get connected to the gateway.]

As regards voice services each operator has the liberty to charge as low as possible to be competitive in price without having to worry much about covering costs. In the case of data services it is not that easy. The extent to which data service prices can be lowered is constrained by the price of bandwidth from the incumbent to the ISP and from the ISP to the other operators, such as mobile operator, in addition to all other network operational costs. The following figure shows this relationship for pricing of data services.

Figure 2-1: An example of pricing on data services



* *This block has been modified from "GSM/NGN tariff" to "service Tariff (e.g., mobile and NGN), because this block shows an input to the costs from other service aspects.*

Annex 3: NGN Functional Architecture/Security

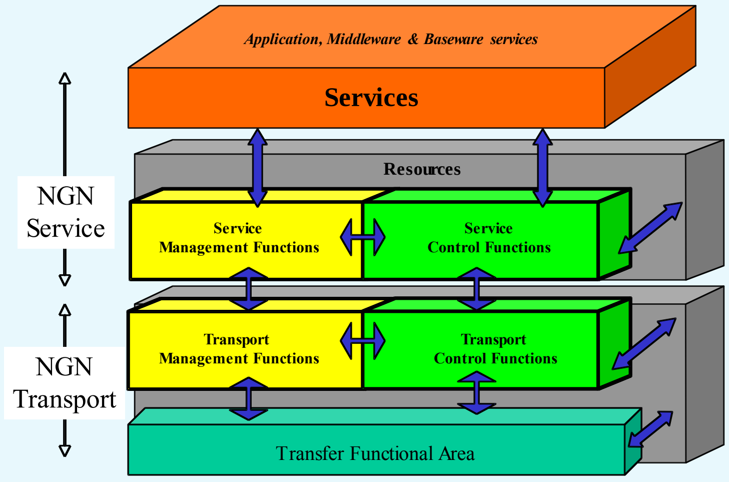
1 NGN Functional Architecture

1.1 General Principles and Reference Architecture Model

As far as NGN systems (non-OSI systems) are concerned, all or some of the following situations may be encountered when considering the OSI 7-layer basic reference model (OSI BRM):

- The number of layers may not equal seven;
- The functions of individual layers may not correspond to those of the OSI BRM;
- Certain prescribed or proscribed conditions/definitions of the OSI BRM may not be applicable;
- The protocols involved may be other than OSI protocols (one notable example being the IP);
- The compliance requirements of the OSI BRM may not be applicable.

Figure 1-1: General functional model of NGN


Application, Middleware & Baseware services
Services
Resources
NGN Service
Service Management Functions
Service Control Functions
NGN Transport
Transport Management Functions
Transport Control Functions
Transfer Functional Area

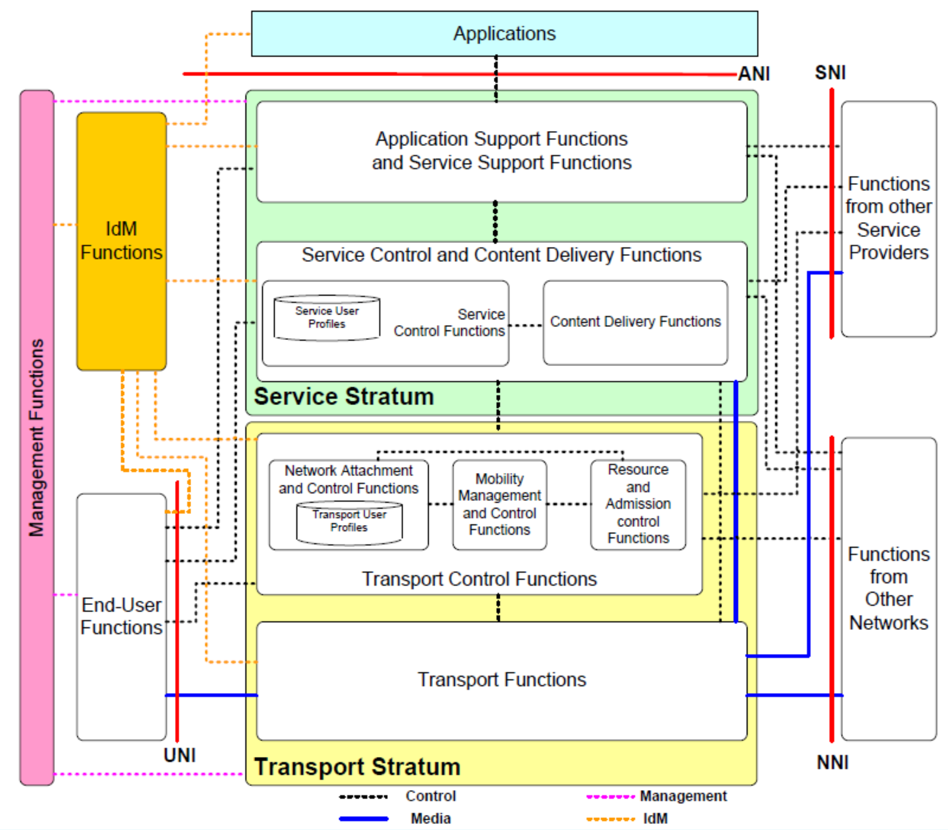
The services and functions are related to each other, since functions are used to build services. It is convenient to assemble functions into two distinct groups, or planes, one comprising all control functions and the other comprising all management functions. The grouping of functions of the same type (i.e., control or management) allows the functional inter-relationships within a given group to be defined, as well as the information flows between functions in the given group.

With this in mind, ITU-T Recommendation Y.2011 goes on to consider the functional aspects of systems implementation. In particular, it develops the following high-level model, which shows how functions may be grouped for the purposes of systems development. The functional blocks shown in Figure 1-1, can then be further decomposed in sub-groups to represent grouping convenient for implementation and distributed system depiction.

1.2 NGN Functional Architecture

NGN services include session-based services, such as IP telephony, video conferencing, and video chatting, and non session-based services, such as video streaming and broadcasting. Moreover, NGN supports PSTN/ISDN replacement.

Figure 1-2: Abstracted NGN functional architecture


Applications
ANI
SNI
Management Functions
IdM Functions
Application Support Functions and Service Support Functions
Service Control and Content Delivery Functions
Service User Profiles
Service Control Functions
Content Delivery Functions
Service Stratum
Functions from other Service Providers
Network Attachment and Control Functions
Transport User Profiles
Mobility Management and Control Functions
Resource and Admission control Functions
Transport Control Functions
End-User Functions
Transport Functions
Functions from Other Networks
UNI
NNI
Transport Stratum
Control
Media
Management
IdM

The NGN architectural overview shown in Figure 1-2 comes from ITU-T Recommendation Y. 2012. The NGN functions are divided into service functions and transport functions. According to ITU-T Recommendation Y.2011, it is called the functional categories strata.

Customer networks and terminals are connected by UNI. Other networks are interconnected through NNI. Clear identification of UNI and NNI is important to accommodate a wide variety of off-the-shelf customer equipment while maintaining business boundaries and demarcation points for the NGN environment.

1.2.1 Transport Stratum Functions

Transport stratum functions identified in ITU-T Recommendation Y.2012 provide connectivity for all components and physically separated functions within the NGN. IP is recognized as the most promising technology for NGN. Thus, the transport stratum provides IP connectivity for both end-user equipment outside the NGN and controllers and enablers, which usually reside on the servers inside the NGN. The transport stratum is responsible for providing end-to-end QoS, which is a desirable feature of the NGN. The transport stratum is divided into access networks and the core network, with a function linking the two transport network portions.

- **Transport functions**: The transport functions provide the connectivity for all components and physically separated functions within the NGN. These functions provide support for the transfer of media information, as well as the transfer of control and management information. Transport functions include access network functions, edge functions, core transport functions, and gateway functions.

- **Transport control functions**: The transport control functions include Resource and Admission Control Functions, Network Attachment Control Functions and Mobility management and Control Functions.

  a) Network attachment control functions (NACF): The network attachment control functions provide registration at the access level and initialization of end-user functions for accessing NGN services. The functions provide network level identification/authentication, manage the IP address space of the access network, and authenticate access sessions. The functions also announce the contact point of the NGN Service/Application functions to the end user. That is, the functions assist end-user equipment to register and start the use of the NGN.

  b) Resource and Admission Control Functions (RACF): In the NGN Architecture, the RACF provides QoS control (including resource reservation, admission control and gate control), NAPT and/or FW traversal control Functions over access and core transport networks. Admission control involves checking authorization based on user profiles, SLAs, operator specific policy rules, service priority, and resource availability within access and core transport. Within the NGN architecture, the RACF act as the arbitrator for resource negotiation and allocation between Service Control Functions and Transport Functions.

  c) Transport User Profile functions: These functions take the form of a functional database representing the combination of a user’s information and other control data into a single "user profile" function in the transport stratum. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

  d) Mobility Management and Control Functions (MMCF): The MMCF provide functions for the support of IPbased mobility in the transport stratum. These functions allow the support of mobility of a single device. The MMCF provides mechanisms to achieve seamless mobility if network conditions permit, but does not provide any mechanism to deal with service adaptation if the post-handover quality of service is degraded from the quality of service before handover. The MMCF assumes that mobility is a service, explicitly specified by parameters in the user service profile. The MMCF is not dependent on specific access technologies, and supports handover across different technologies.

1.2.2 Service Stratum Functions

The service stratum functions provide session-based and non session-based services including subscribe/notify for presence information and the message method for instant message exchange.

- **Service control and content delivery functions** (SC&CDF): The SC&CDF includes service control functions and content delivery functions

  a) Service Control Functions (SCF): The SCF includes resource control, registration, and authentication and authorization functions at the service level for both mediated and non-mediated services.. They can also include functions for controlling media resources, i.e., specialized resources and gateways at the service-signalling level. Regarding the authentication, mutual authentication between end user and the service is performed. The service control functions accommodate service user profiles which represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of functional databases. These functional databases may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

  b) Service user profile functions: The service user profile functions represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of a functional database. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

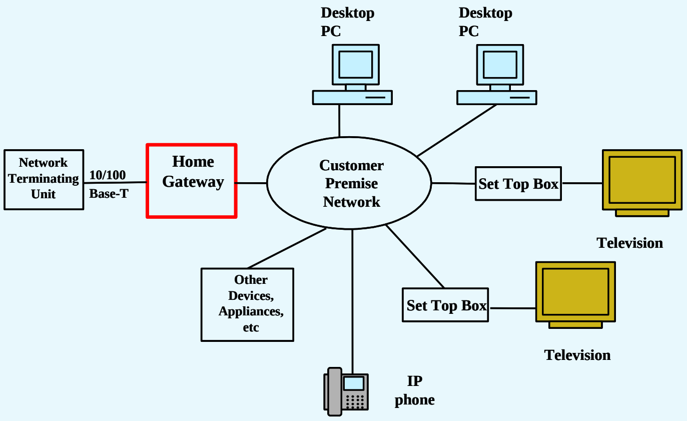
  c) Content Delivery Functions (CDF): The CDF receives content from the application support functions and service support functions, store, process, and deliver it to the end-user functions using the capabilities of the transport functions, under control of the service control functions.

- **Application/Service support functions**: The application/service support functions include functions such as the gateway, registration, authentication and authorization functions at the application level. These functions are available to the “Third-Party Applications” and “End-User” functional groups. The Application/Service support functions work in conjunction with the SCF to provide end-users and third party application providers with the value added services they request. Through the UNI, the Application/Service support functions provide a reference point to the end-user functions. The Third-party applications’ interactions with the Application/Service support functions are handled through the ANI reference point.

1.2.3 End User Functions

No assumptions are made about the diverse end-user interfaces and end-user networks that may be connected to the NGN access network. Different categories of end-user equipment are supported in the NGN, from single-line legacy telephones to complex corporate networks. End-user equipment may be either mobile or fixed.

Figure 1-3: Overall configurations of end systems in NGN



1.2.4 *Management Functions*

Support for management is fundamental to the operation of the NGN. These functions provide the ability to manage the NGN in order to provide NGN services with the expected quality, security, and reliability. These functions are allocated in a distributed manner to each functional entity (FE), and they interact with network element (NE) management, network management, and service management FEs. Further details of the management functions, including their division into administrative domains, can be found in ITU-T recommendation M.3060. Management functions apply to the NGN service and transport strata. For each of these strata, they cover the FCAPS.

The accounting management functions also include charging and billing functions (CBF). These interact with each other in the NGN to collect accounting information, in order to provide the NGN service provider with appropriate resource utilization data, enabling the service provider to properly bill the users of the system.

2 Security in NGN

2.1 Security threats and risks

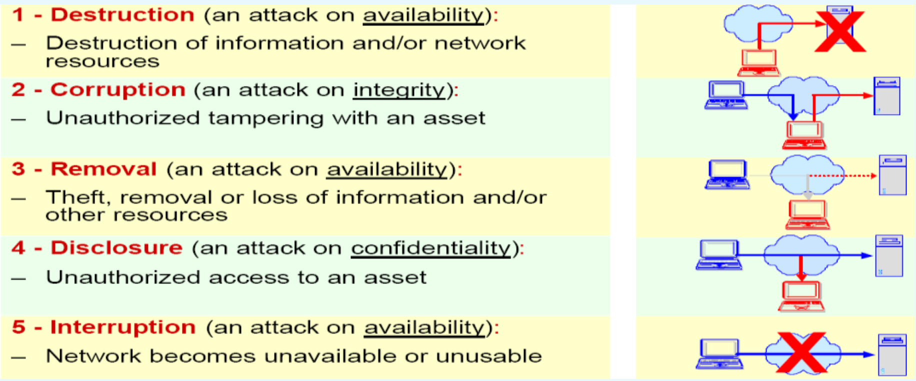
The systems, components, interfaces, information, resources, communications (i.e., signalling, management and data/bearer traffic) and services that make up an NGN will be exposed to a variety of security threats and risks. Those threats and risks will depend on a variety of factors. In addition, end users will also be exposed to certain threats (e.g., unauthorized access to private information). Figure 2-1 illustrates threat model based on Rec. X.800.

Threats to the NGN:

- unauthorized reconnaissance, such as the remote analysis of the system to determine points of weakness (these may include scans, sweeps, port interrogation, route tables, etc.);
- break-in/device takeover resulting in loss of control of the device, anomalies and errors in the configuration audits;
- destruction of information and/or other resources;
- corruption or modification of information;
- theft, removal or loss of information and/or other resources;
- disclosure of information; and

- interruption of services and denial of services.

Figure 2-1: X.800 threat model



1 - **Destruction** (an attack on availability):
— Destruction of information and/or network resources

2 - **Corruption** (an attack on integrity):
— Unauthorized tampering with an asset

3 - **Removal** (an attack on availability):
— Theft, removal or loss of information and/or other resources

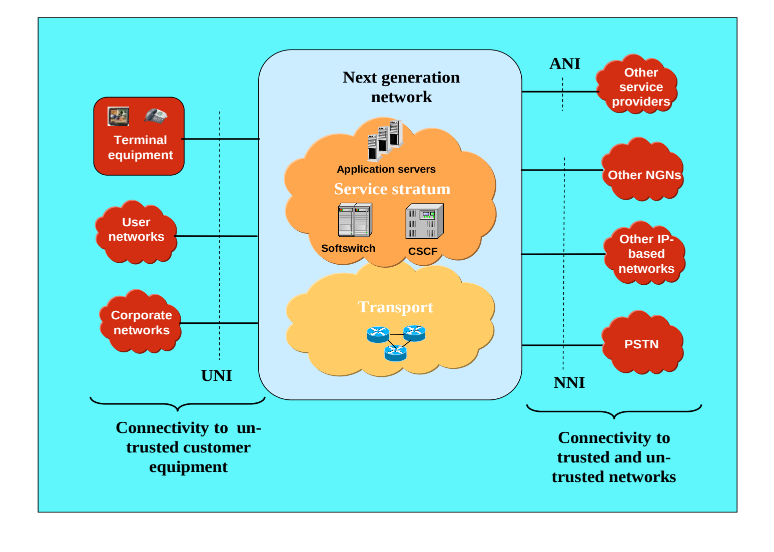
4 - **Disclosure** (an attack on confidentiality):
— Unauthorized access to an asset

5 - **Interruption** (an attack on availability):
— Network becomes unavailable or unusable

Further, it is clear that NGNs will be operating in an environment different from the PSTN environment and may therefore be exposed to different types of threats and attacks from within or externally. NGNs will have direct or indirect connectivity to un-trusted and trusted networks and terminal equipment, and therefore will be exposed to security risks and threats associated with connectivity to un-secure networks and customer premises equipment. For example, a provider's NGN may have direct or indirect (i.e., through another network) connectivity to the following as shown in Figure 2-2.

- other service providers, and their applications;
- other NGNs;
- other IP-based networks;
- public switched telephone network (PSTN);
- corporate networks;
- user networks;
- terminal equipment;
- other NGN transport domains.

Figure 2-2: Connectivity to networks and users



In the evolving environment, security across multiple network provider domains relies on the aggregation of what all providers elect to do for securing their networks. Unauthorized network access into one provider's network can easily lead to exploitation of an interconnected network and its associated services. This is an example of the exploitation of the weakest link that can threaten a provider network's integrity and service continuity along with a host of various types of attacks.

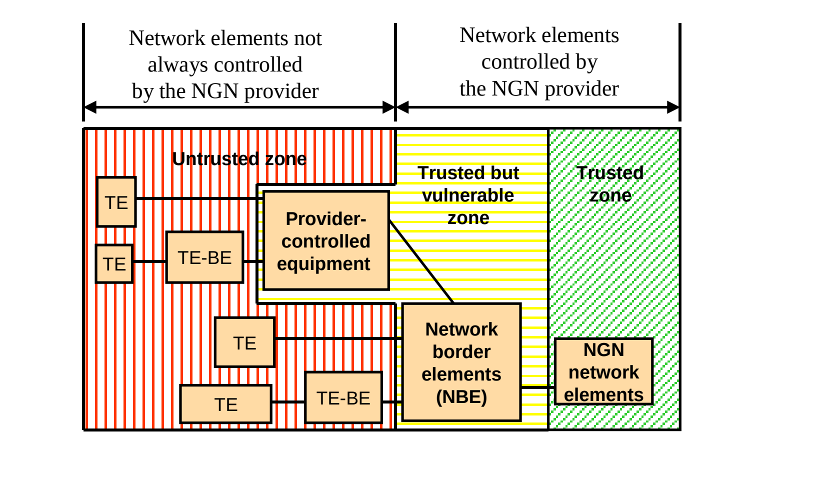
Each NGN provider is responsible for security within its domain. Each NGN provider is responsible for designing and implementing security solutions using network specific policy for trust relations, to meet its own network-specific needs and to support global end-to-end security objectives across multiple network provider domains.

2.2 Security trust model

The NGN functional reference architecture defines functional entities (FEs). However, since network security aspects depend heavily on the way that FEs are bundled together, the NGN security architecture is based on physical network elements (NEs), i.e., tangible boxes that contain one or more FEs. The way these FEs are bundled into NEs will vary, depending on the vendor.

- **Single network trust model**: Three security zones (trusted, trusted but vulnerable, and un-trusted) are dependent on operational control, location, and connectivity to other device/network elements. These three zones are illustrated in the security trust model shown in Figure 2-3.

Figure 2-3: Security trust model


Network elements not always controlled by the NGN provider
Network elements controlled by the NGN provider
Untrusted zone
Trusted but vulnerable zone
Trusted zone
TE
TE
TE-BE
Provider-controlled equipment
TE
TE
TE-BE
Network border elements (NBE)
NGN network elements

a) "trusted network security zone" or "trusted zone": It is a zone where a NGN provider's network elements and systems reside and never communicate directly with customer equipment or other domains. The "trusted zone" will be protected by a combination of various methods. Some examples are physical security of the NGN network elements, general hardening of the systems, use of secure signalling, security for OAMP messages separate VPN within the (MPLS/)IP network for communication within the "trusted" zone and with NGN network elements in the "trusted-but-vulnerable" zone.

b) "trusted but vulnerable network security zone", or "trusted but vulnerable zone": It is a zone where the network elements/devices are operated (provisioned and maintained) by the NGN provider. The equipment may be under the control by either the customer/subscriber or the NGN provider. In addition, the equipment may be located within or outside the NGN provider's premises. Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone.

c) "un-trusted zone": It includes all network elements of customer networks or possibly peer networks or other NGN provider domains outside of the original domain, which are connected to the NGN provider's network border elements. In the "un-trusted zone", comprised of terminal equipment, equipment may not be under the control of NGN providers and it may be impossible to enforce provider's security policy on user.

- **Peering network trust model**: When an NGN is connected to another network, the trust depends on:

a) physical interconnection, where the interconnection can range from a direct connection in a secure building to via shared facilities;

b) peering model, where the traffic can be exchanged directly between the two NGN service providers, or via one or more NGN transport providers;

c) business relationships, where there may be penalty clauses in the SLA agreements, and/or a trust in the other NGN provider's security policy;

d) in general, NGN providers should view other providers as un-trusted.

2.3 Design Principles for NGN Security

2.3.1 Objectives and requirements

- **General security objectives**: The following is a list of general security objectives used to guide the requirements in this Recommendation.

  a) NGN security features should be extensible, and flexible enough to satisfy various needs.

  b) Security requirements should take the performance, usability, scalability and cost constraints of NGN into account.

  c) Security methods should be based on existing and well-understood security standards as appropriate.

  d) The NGN security architecture should be globally scalable (within network provider domains, across multiple network provider domains, in security provisioning).

  e) The NGN security architecture should respect the logical or physical separation of signalling and control traffic, user traffic, and management traffic.

  f) NGN security should be securely provisioned and securely managed.

  g) An NGN should provide security from all perspectives: service, network provider and subscriber.

  h) Security methods should not generally affect the quality of provided services.

  i) Security should provide simple, secure provisioning and configuration for subscribers and providers (plug & play).

  j) Appropriate security levels should be maintained even when multicast functionality is used.

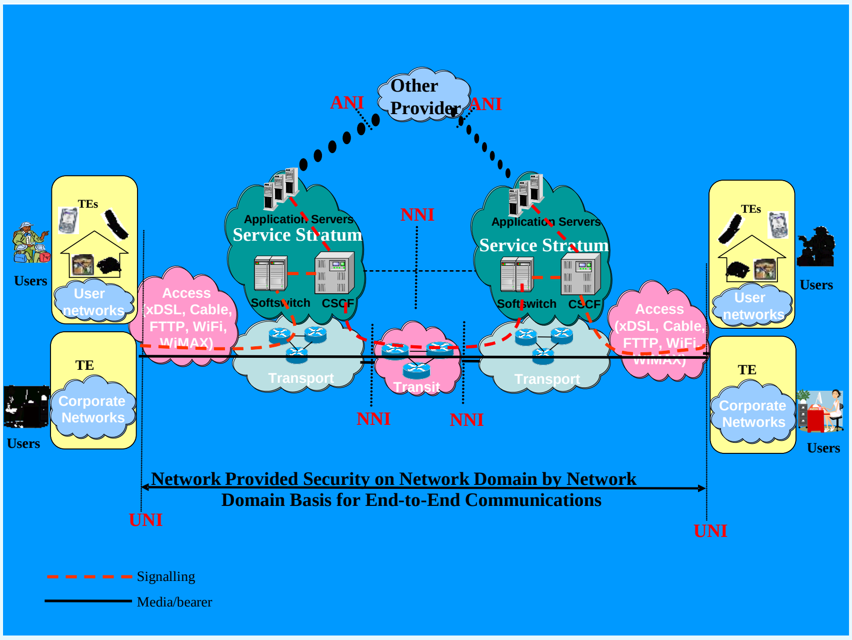
  k) The service discovery capabilities should support a variety of scoping criteria (e.g., location, cost, etc.) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy.

  l) The address resolution system should be a special system used only by this network, and certain security measures are required to be in place. This system may use databases that are internal or external of a domain.

  m) The principles and general security objectives for secure TMN management should be followed.

- **Objectives for security across multiple network provider domains**: The general objective is to provide network-based security for end-to-end communications across multiple provider domains. This is achieved by providing security of the end-to-end communication on a hop-by-hop basis across the different provider's domains. Figure 2-4 shows the general concept of network provided security for end-to-end communications between end users. Each network segment has specific security responsibilities within its security zone to facilitate security and availability of NGN communications across multiple networks.

Figure 2-4: Security of communications across multiple networks



- **Requirements specific for security dimensions**: The objectives described here are specific to particular security dimensions, such as authentication. They are common to all interfaces.

a) Access control: NGN providers are required to restrict access to authorized subscribers. Authorization may be given by the provider providing the access or by other providers after validation by an authentication and access control processes. The NGN is required to prevent unauthorized access, such as by intruders masquerading as authorized users.

b) Authentication: NGN providers are required to support capabilities for authenticating subscribers, equipment, network elements and other providers.

c) Non-repudiation: This document does not specify any non-repudiation security requirements.

d) Data confidentiality: NGN providers are required to protect the confidentiality of subscriber traffic by cryptographic or other means. NGN providers are required to protect confidentiality of control messages by cryptographic or other means if security policy requests it. NGN providers are required to protect the confidentiality of management traffic by cryptographic or other means.

e) Communication security: NGN providers are required to provide mechanisms for ensuring that information is not unlawfully diverted or intercepted.

f) Data integrity: NGN providers are required to protect the integrity of subscriber traffic by cryptographic or other means. NGN providers are required to protect integrity of control messages by cryptographic or other means if security policy requests it. NGN providers are required to protect the integrity of management traffic by cryptographic or other means.

g) Availability: NGN is required to provide security capabilities to enable NGN providers to prevent or terminate communications with the non-compliant end-user equipment. These capabilities may be suspended to allow emergency communications. NGN internal network elements may also be susceptible to viruses, worms and other attacks. Similar measures to quarantine network components are also required. An NGN should provide provision of security capabilities to enable a NGN provider to filter out packets and traffic that is considered harmful by the respective security policy. NGN is required to provide capabilities for the support of disaster recovery functions and procedures.

h) Privacy: NGN is required to provide capabilities to protect the subscriber's private information such as location of data, identities, phone numbers, network addresses or call-accounting data according to national regulations and laws. Specific requirements for privacy are a national matter and are outside the scope of this Recommendation.

2.3.2 Specific security requirements

This clause introduces the specific requirements for security for each of the network elements within the NGN infrastructure.

- **Common security requirements for NGN elements**

  a) Security policy: NGN providers shall prepare appropriate security policy and shall be responsible for applying it to all NEs and devices under its control.

  b) Hardening and service disablement: All NGN elements are required to be capable of being configured to support the minimum services needed to support the NGN provider NGN infrastructure. Any service or transport layer port that is not required for the correct operation of the NGN element is required to be disabled on all systems and network elements. In addition, applications are required to run under minimum privileges (e.g., on "UNIX/Linux" platforms applications should not run as root if root privileges are not indispensable). The base operating system (OS) supporting any NGN element is required to be capable of being specifically configured for security and appropriately hardened. No "backdoors" are permitted (software access which would circumvent usual access control mechanisms) into any NGN element. In addition to hardening, physical and logical access controls are required to be put in place to meet industry best-practices.

  c) Audit trail, trapping and logging: All NGN elements are required to be capable of creating an audit trail that maintains a record of security related events in accordance with NGN provider's security policy. Mechanisms to prevent unauthorized or undetected modification are required. The audit trail is required to be capable of being managed and is required to allow old data in the audit trail to be placed on other media, e.g., removable media, for long-term storage. This interface is required to allow authorized administrators to move old data out of the audit trail onto removable media. This ability is required to be protected by a specific authorization to manage the audit trail.

  d) Time stamping and time source: The NGN element is required to support the use of a trusted time source for both system clock and audit trail item stamping. A trusted time source in this case means a time source that can be verified to be resistant to unauthorized modification. Transitive trust is acceptable, i.e., a time source that relies on a trusted time source is itself an acceptable trusted time source.

  e) Resource allocation and exception handling: Each NGN element is required to provide the capability to limit the amount of its own important resources (e.g., memory allocation) it allocates to servicing requests. Such limits can minimize negative effects of denial of service attacks. Resources used to service requests compete with other resource utilization requests on the system. In addition, each specific NGN application is required to have the ability to limit its own usage of important resources that it allocates for satisfying requests.

f) Code and system integrity and monitoring: The network element is required to be capable of monitoring 1) its configuration and software and 2) any changes to detect unauthorized changes, both based on the security policy. Any unauthorized changes are required to create a log entry and cause an alarm to be generated. Based on the security policy, the network element is required to do the following. The element is required to be capable of periodically scanning its resources and software for malicious software, e.g., a virus. The element is required to generate an alarm if malicious software is discovered during a scan.

g) Patches, hotfixes and supplementary code: To trust signals generated by NGN provider NGN elements within un-trusted networks, say terminal. It is a requirement that software on the system is not compromised. NGN provider network elements and systems are required to provide a capability to verify and audit all their software. The audit results are to be accessible to an OSS. This would allow for an analysis of the security posture of the NGN provider NGN infrastructure and provide guidance to administrators and providers with respect to where mitigation is necessary.

h) Access to OAMP functions in devices: In order to safeguard the OAMP infrastructure, each internal NGN network element is required to be managed through a separate IP address allocated from a separate address block. The NGN network element is required to silently discard all packets received over the non-OAMP interface with source addresses assigned to OAMP traffic. Access to OAMP functions is required to be capable of being controlled by authentication. OAMP traffic is required to be securely protected.

- **Requirements for NGN elements in the trusted zone**: The NGN Release 1 element in the "trusted" zone is to be assigned an IP address in the block reserved for internal NGN elements. All signalling is required to use this address. The NGN Release 1 element is also required to be assigned an IP address in the block reserved for OAMP, and all OAMPs are required to use this address.

- **Requirements for NGN border elements in the "trusted-but-vulnerable" domain**: The network border element is required to support multiple IP addresses, or multiple network interfaces. The NBE is required to silently discard any media packets received that do not correspond to an active session. The NBE is also required to verify that the packet rate is consistent with the negotiated session parameters. The NBE is required to authenticate all requests if required by the service agreement with the customer.

- **Requirements for TE border elements in the "un-trusted" domain**: Physical security is a challenge for equipment placed on customer site. Ultimately, it must be accepted that, to a large extent, the security of these devices is dependent on the customer. In order to preserve the confidentiality of customer communication against eavesdropping on the signalling traffic, signalling messages are required to use a secure signalling connection between the TE-BE and the NBE.

- **Security recommendations for terminal equipment in the "un-trusted" domain**: The terminal equipment (TE) is often outside the control of the NGN provider. Therefore it is not required for the NGN provider to place requirements on its security features or policies, rather it is the function of the various network border elements to adapt to whatever policies are chosen by the customer and to provide the best service under those conditions. Media traffic should be protected from eavesdropping or modification.

2.3.3 NGN security mechanisms and procedures

This clause highlights some important security mechanisms that can be used to realize the requirements in ITU-T Recommendation Y.2701 in each NGN Network Element, and specifies a suite of options to be used for the mechanisms to avoid the mismatch of options.

- **Identification, Authentication and Authorization**: There are identification, authentication and authorization mechanisms, in particular, those concerning SIP-based services.
- **Transport Security for Signaling and OAMP**: Transport security is used in the NGN infrastructure to achieve confidentiality and integrity guarantees of the signalling data and the OAMP messages. It is required to specify profile of TLS and IPsec to be used by the NGN infrastructure network elements as two of the important mechanisms.
- **Media Security**: Media encryption is not required within the NGN infrastructure, but it may be required to be supported for customers that desire its use. Such support may include the support of media encryption protocols, SRTP [RFC3711]. Network Border Elements (i.e., the edge of the network provider's domain) are assumed to implement encryption/decryption although it is possible to do the same in a separate platform shared among NBEs. In either case, the encryption and decryption is required to be collocated with other media processing capabilities such as Dual-Tone Multi-Frequency (DTMF) detection and transcoding.
- **Audit Trail, Trapping, and Logging Systems**: An audit trail is taken all OAMP access attempts (whether successful or not), all OAMP changes made, and all OAMP signoffs. In addition events considered significant by the NGN provider's policy are logged.
- **Provisioning of equipment in untrusted zone**: All customer premise equipments are configured by the TE Provisioning Element. TE Provisioning Element resides in the trusted zone and may only communicate with the TEs via the Network Border Element (NBE). A TE or TE-BE may authenticate and establish a security association with the NBE before it can obtain configuration file from TE Provisioning Element. NBE may support both TLS and IPsec for establishing SA with the TEs (including TE-BE).

2.3.4 Application model for AAA in NGN

Based on security requirements for NGN in Y.2701 and the NGN authentication reference model in Y.2702, the NGN authentication reference model (Figure 2-5) depicts eight authentication reference points. Reference points (1) and (4) refer to transport of user traffic and may be viewed as depending on "horizontal" access control at the transport control level, whereas reference points (2) and (8) may be viewed as depending on control data between the transport and service control layers and therefore as being "vertical." This relationship is displayed in Figure 2-6.

Figure 2-5: End-to-end Reference Architectural Model (Y.2702 NGN Authentication)

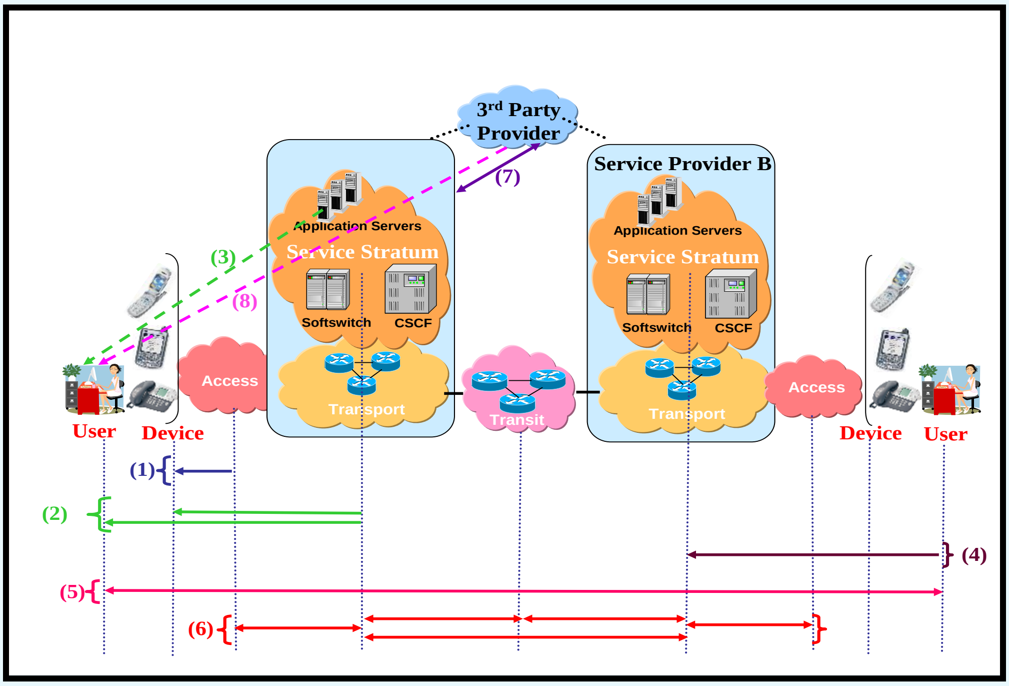
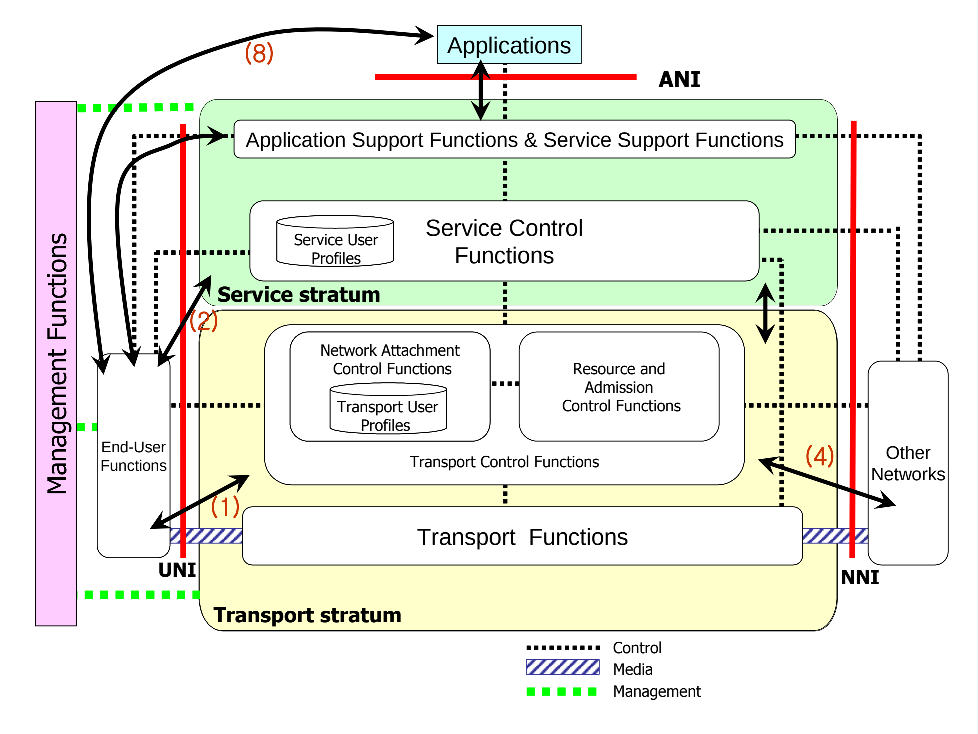


Figure 2-6: NGN Architecture and AAA related domains (Y.2702 NGN Authentication)

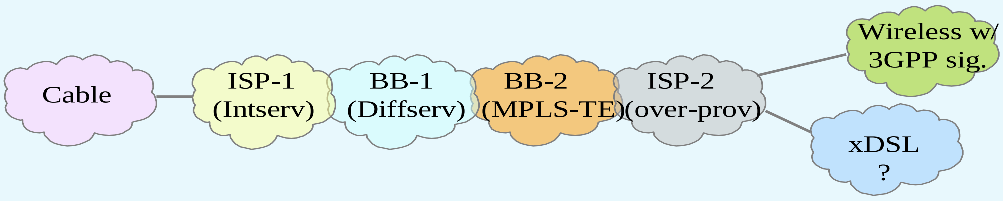


Annex 4: Quality of Service in NGN

1 Overview of QoS and NP in NGN

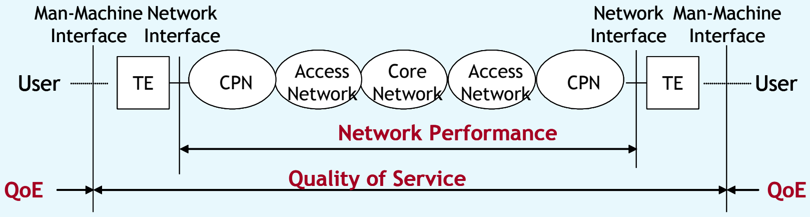
One of the key elements of NGN, which should be based on IP, is the guaranteeing of requested Quality of Services (QoS). The NGN have access and transport agnostic features which should be assumed in heterogeneous environments, so complexity of supporting the QoS is much more complicated. Figure 1-1 shows an example of this complexity.

Figure 1-1: QoS Complexity in Heterogeneous Network Environment



The general aspects of Quality of Service and network performance in NGN are developed to provide descriptions of NGN Quality of Service, Network Performance and Quality of Experience. Figure 1-2 shows the meaning and scope of QoS, QoE and NP with brief explanation about their features.

Figure 1-2: QoE, QoS and NP in NGN environment



Quality of Experience	Quality of Service	Network Performance
User oriented		Provider oriented
User behavior attribute	Service attribute	Connection/Flow element attribute
Focus on user-expected effects	Focus on user-observable effects	Focus on planning, development (design), operations and maintenance
User subject	Between (at) service access points	End-to-end or network elements capabilities

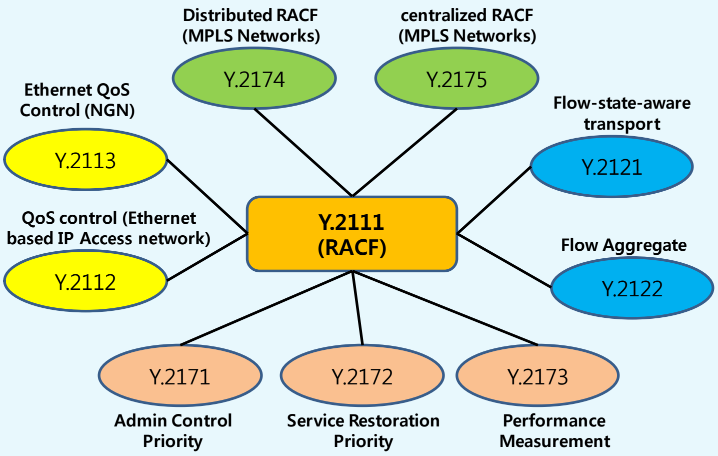
The NGN illustrates how these descriptions are applied in an NGN environment, describe performance aspects of NGN (including performance of service and transport stratum) and provide a basis for common understanding of performance concepts (useful to users and to the industries that compose the NGN – e.g., Fixed & mobile telecommunications, broadcasting, etc.). NGN defines the application QoS classes of the NGN.

The NGN determines the requirements to support QoS across multiple heterogeneous service providers. Existing standards specify several metrics and measurement methods for point to point performance. Notable are ITU-T Recommendations, Y.1540 and Y.1541 standards and the IETF IP Performance Metrics (IPPM) Working Group standards. The NGN considers the options and parameters left unspecified, taking into account the concatenation of performance over multiple network segments, allocation of impairment budgets, mapping between IP and non-IP metrics, accuracy, and data handling.

The network performance parameters of non-homogeneous networks in NGN are developed through the description of performance aspects of the transport layer in NGN. The NGN identifies general performance principles and frameworks that can be applied to the development of specific performance descriptions to support continuing evolution of the NGN. NGN defines the relationship among individual networks' performance which may be observed at physical interfaces between a specific network and associated terminal equipment, and at physical interfaces between specific networks.

A QoS Framework for IP based access networks is also developed in ITU-T through NGN-GSI. Reference architecture for IP access networks for QoS support is provided as well as detailed QoS requirements and validation procedures. The reference model would be part of the overall NGN framework with the service and transport layers, functional entities in each layer, and interfaces between the functional entities, in particular, the functional entities to facilitate interworking with the QoS functionality in the core network as well as that specific to each type of access networks.

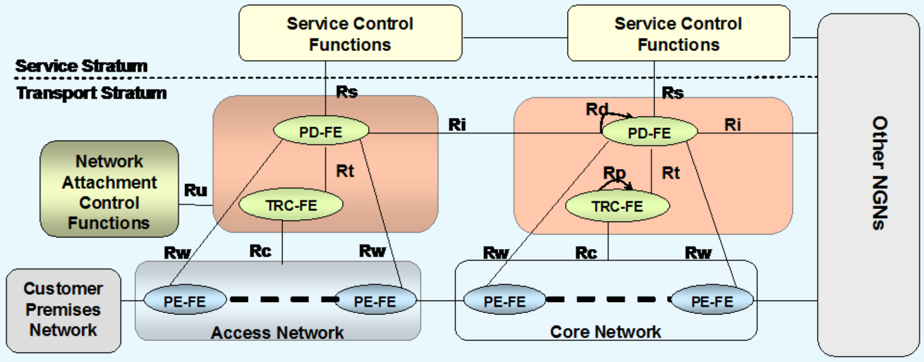
Figure 1-3: ITU-T NGN QoS related standards


Distributed RACF (MPLS Networks)
Y.2174
centralized RACF (MPLS Networks)
Y.2175
Ethernet QoS Control (NGN)
Y.2113
Flow-state-aware transport
Y.2121
QoS control (Ethernet based IP Access network)
Y.2112
Y.2111 (RACF)
Flow Aggregate
Y.2122
Y.2171
Admin Control Priority
Y.2172
Service Restoration Priority
Y.2173
Performance Measurement

2 Resource and Admission Control in NGN

Functional requirements and architecture for resource and admission control in NGN are developed to provide high-level requirements, scenarios and functional architecture. The decomposition to functional entities is specified to provide reference points and interfaces for the control of Quality of Service (QoS), Network Address and Port Translator (NAPT) and/or Firewall (FW) traversal are described.

Figure 2-1: Resource and Admission Control architecture model of NGN



- **QoS capability of CPE**: According to the capability of QoS negotiation, the CPE can be categorized as follows:

  a) Type 1 – CPE without QoS negotiation capability (e.g., vanilla soft phone, gaming consoles)

  The CPE does not have any QoS negotiation capability at either the transport or the service stratum. It can communicate with the SCF for service initiation and negotiation, but cannot request QoS resources directly.

  b) Type 2 – CPE with QoS negotiation capability at the service stratum (e.g. SIP phone with SDP/SIP QoS extensions)

  The CPE can perform service QoS negotiation (such as bandwidth) through service signalling, but is unaware of QoS attributes specific to the transport. The service QoS concerns characteristics pertinent to the application.

  c) Type 3 – CPE with QoS negotiation capability at the transport stratum (e.g. UMTS UE)

  The CPE supports RSVP-like or other transport signalling (e.g. GPRS session management signalling, ATM PNNI/Q.931). It is able to directly perform transport QoS negotiation throughout the transport facilities (e.g. DSLAM, CMTS, SGSN/GGSN).

  Note that the SCF shall be able to invoke the resource control process for all types of CPE.

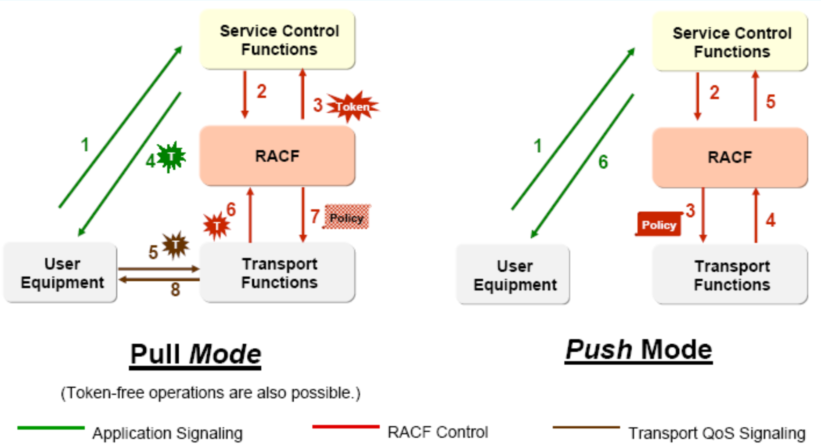
- **Resource control modes**: In order to handle different types of CPE and transport QoS capabilities, the RACF shall support the following QoS resource control modes as part of its handling of a resource request from the SCF:

  a) Push Mode: The RACF makes the authorization and resource control decision based on policy rules and autonomously instructs the transport functions to enforce the policy decision.

  b) Pull Mode: The RACF makes the authorization decision based on policy rules and, upon the request of the transport functions, re-authorizes the resource request and responds with the final policy decision for enforcement.

The Push mode is suitable for the first two types of CPE. For type 1 CPE, the SCF determines the QoS requirements of the requested service on behalf of the CPE; for type 2 CPE, the SCF extracts the QoS requirements from service signalling. The Pull mode is suitable for type 3 CPE, which can explicitly request QoS resource reservation through transport QoS signalling.

Figure 2-2: Pull and Push mode of RACF operation



- **Resource control states**: Regardless of the QoS negotiation capability of a particular CPE and the use of a particular resource control mode, the QoS resource control process consists of three logical states:

  a) Authorization (Authorized): The QoS resource is authorized based on policy rules. The authorized QoS bounds the maximum amount of resource for the resource reservation.

  b) Reservation (Reserved): The QoS resource is reserved based on the authorized resource and resource availability. The reserved resource can be used by best effort media flows when the resource has not yet committed in the transport functions.

  c) Commitment (Committed): The QoS resource is committed for the requested media flows when the gate is opened and other admission decisions (e.g. bandwidth allocation) are enforced in the transport functions.

  d) The general resource control criteria shall be:

  e) The amount of committed resources is not greater than the amount of reserved resources.

  f) The amount of reserved resources is not greater than the amount of authorized resources.

Note that the amount of committed resources typically equals the amount of reserved resources.

- **Resource control schemes**: Given the variety of application characteristics and performance requirements, the RACF supports three resource control schemes:

  a) Single-Phase Scheme: Authorization, reservation and commitment are performed in a single step. The requested resource is immediately committed upon successful authorization and reservation. The Single-Phase Scheme is suitable for client-server-like applications to minimize the delay between the service request and the ensuing reception of content.

  b) Two-Phase Scheme: Authorization and reservation are performed in one step, followed by commitment in another step. Alternatively authorization is performed in one step, followed by reservation and commitment in another step. The Two-Phase Scheme is suitable for interactive applications, which have stringent performance requirements and need to have sufficient transport resources available.

  c) Three-Phase Scheme: Authorization, reservation and commitment are performed in three steps sequentially. The Three-Phase Scheme is suitable for network-hosted services in an environment where transport resources are scarce.

- **Information for resource control**: The RACF shall perform the resource control based on the following information:

  a) Service Information: A set of data provided by the SCF for a resource control request, derived from service subscription information, service QoS requirement and service policy rules.

  b) Transport Network Information: A set of data collected from the transport networks, which may consist of transport resource admission decisions and network policy rules.

  c) Transport Subscription Information: A set of data for the transport subscription profile such as the maximum transport capacity per subscriber.

- **Policy rules for the enforcement of resource control results**: The RACF may assist the installation of two types of policy rules related to the enforcement of resource control results:

  a) Policy Decision: A set of policy conditions and actions for the enforcement of resource control results on a per flow basis, which is produced dynamically upon the individual resource request from the SCF. The RACF shall make policy decisions based on the information for resource control described in above paragraph and install the policy decisions to the transport functions autonomously or upon the request of the transport functions. The policy decision can be modified and updated within the lifetime of a resource control session.

  b) Policy Configuration: A set of static policy rules for default network resource configuration. The policy configuration is pre-defined by network operators and does not vary from the individual resource request. The policy configuration can be pre-provisioned statically in transport functions, e.g. mapping rules of the IP layer QoS to link layer QoS. In some cases, the RACF may help install the initial policy configuration for resource control, such as default resource control configuration (e.g. default gate setting).

Note that the RACF may use the soft-state (state that has a lifetime and requires renewal to keep alive) or hard-state (state that is persistent until explicitly removed) approach in support of transport resource control.

Annex 5: NGN Management

1 Objectives of NGN Management

The objectives of the management is to facilitate the effective interconnection between various types of Operations Systems (OSs) and/or resources for the exchange of management information using an agreed architecture with standardized interfaces including protocols and messages. Many network operators and service providers have a large infrastructure of OSs, telecommunications networks and equipment already in place, and which must be accommodated within the architecture in terms of managements. Management also provides capabilities for end-users with access to, and display of, management information, and end-user-initiated business processes. By considering these, it is noted that a management framework contributes to increase customer satisfaction and at the same time underpins a significant reduction in operating costs through new technologies and operational methods.

Within the context of NGN, management functionality refers to a set of management functions to allow for exchanging and processing of management information to assist network operators and service providers in conducting their business efficiently. NGN management (NGNM) provides management functions for NGN resources and services, and offers communications between the management plane and the NGN resources or services and other management planes.

This document introduces summary information about the NGN management based on Recommendation ITU-T M.3060 developed by SG2. M.3060 identifies the management architecture needs to address followings:

- Administrative boundaries amongst operator domains;
- Processes amongst operators across the domain boundaries;
- Processes between Operators and their suppliers' equipments;
- Reference points between the logical functions for Provider and Consumer;
- Provider and Consumer Interfaces between the physical entities used to realize the provider and consumer reference points;
- Information model concepts used to support logical functions.

In addition to this, M.3060 also identifies objectives of NGN management as following:

- minimize mediation work between different network technologies through management convergence and intelligent reporting;
- minimize management reaction times to network events;
- minimize load caused by management traffic;
- allow for geographic dispersion of control over aspects of the network operation;
- provide isolation mechanisms to minimize security risks;
- provide isolation mechanisms to locate and contain network faults;
- improve service assistance and interaction with customers;
- layering of services to enable a provider to provide the building blocks for services and others to bundle the services and its implications on the management architecture;
- business processes as defined in the M.3050.x series and how they would be used in NGN;
- support of applications, both on the same distributed computing platform and those distributed throughout the network.

The following areas are identified for further study issues.

- implications of the need to manage end-to-end services;
- implications of home networks and customer premises equipment.

2 Architecture of NGN Management

2.1 NGN Management Requirements

NGN management supports the monitoring and control of the NGN services and relevant resources for the service and transport via the communication of management information across interfaces between NGN resources and management systems, between NGN-supportive management systems, and between NGN components and personnel of service providers and network operators. NGN management supports the aims of the NGN based on Recommendation ITU-T Y.2201. Followings are key summary of NGN management requirements:

- Providing the ability to manage NGN system resources, both physical and logical including resources in the core network, access networks, interconnect components, and customer networks and their terminals;
- Providing the ability to manage NGN Service Stratum resources and enabling organizations offering NGN end-user services including the ability to personalize end-user services and customer self-service (e.g., provision of service, reporting faults, online billing reports);
- Supporting eBusiness Value Networks based upon concepts of business roles including support of B2B processes;
- Allowing an enterprise and/or an individual to adopt multiple roles in different value networks and also multiple roles within a specific value network;
- Integrating an abstracted view on Resources (network, computing and application);
- Supporting the collection of charging data for the network operator regarding the utilization of resources in the network;
- The ability to provide survivable networks in the event of impairment and proactive trend monitoring;
- Enable service providers to reduce the time-frame for the design, creation, delivery, and operation of new services;
- The ability to manipulate, analyse and react to management information in a consistent and appropriate manner.

2.2 NGN Management Architecture

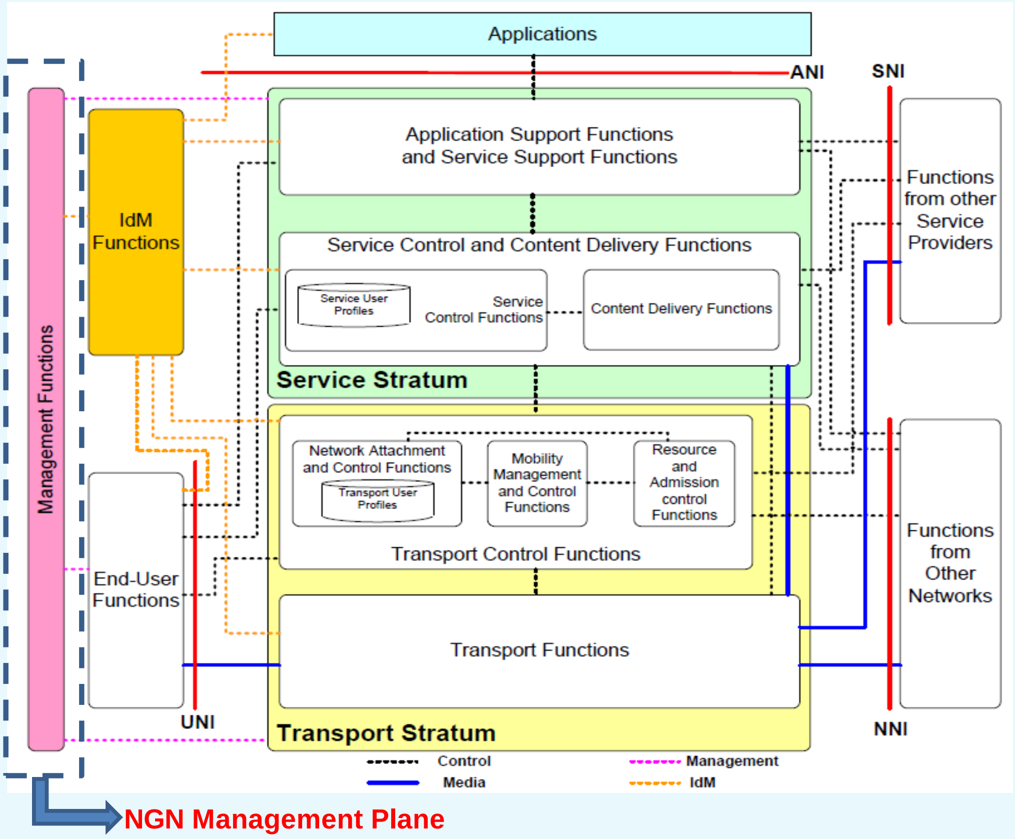
The NGN management plane is the union of the NGN service stratum management plane and the NGN transport stratum management plane following the basis of NGN functional architecture. It may include joint management functions, i.e., functions used to manage entities in both strata plus functions required to support this management.

Referring to Recommendation ITU-T Y.2011 as shown in Figure 2-1, NGN management plane places to cover both transport and service strata as well as other functions such as IdM functions and End-user functions.

The NGN Management architecture will be divided into four different architectural views as shown in Figure 2-2 as followings:

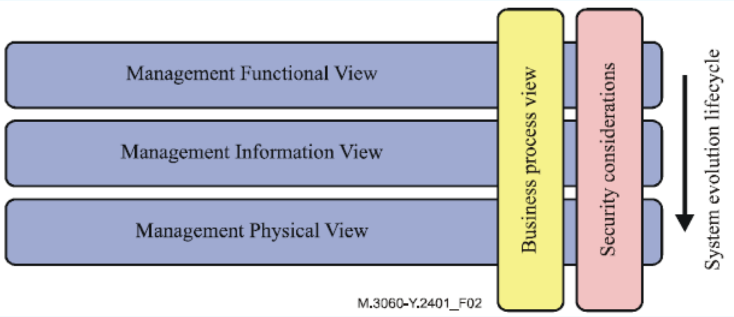
- Business Process View: The business process view, based on the eTOM model (ITU-T Rec. M.3050.x-series), provides a reference framework for categorizing the business activities of a service provider;
- Management Functional View: The functional view permits the specification of what functions have to be achieved in the management implementation;
- Management Information View: The information view characterizes the management information required for communication between the entities in the functional view to enable the performance of the functions to be achieved in the management implementation;
- Management Physical View: The physical view describes the varied ways that management functions can be implemented. They may be deployed in a variety of physical configurations using a variety of management protocols.

Figure 2-1: NGN management plane in the NGN architecture


Applications
ANI
SNI
Application Support Functions
and Service Support Functions
Functions from other Service Providers
IdM Functions
Service Control and Content Delivery Functions
Service User Profiles
Service Control Functions
Content Delivery Functions
Service Stratum
Management Functions
Network Attachment and Control Functions
Transport User Profiles
Mobility Management and Control Functions
Resource and Admission control Functions
Transport Control Functions
End-User Functions
Functions from Other Networks
Transport Functions
UNI
NNI
Transport Stratum
Control
Media
Management
IdM
NGN Management Plane

Each view shows a different perspective into the architecture. These four architecture views also take security into consideration. Figure 2-2 describes the workflow in the creation of management specifications, where first the functional view is defined, followed by the information view and finally the physical view. The Business Process is an influence throughout the lifecycle. Note that, in practice, this process is iterative to enable all aspects of the architecture to evolve over time as required.

Figure 2-2: NGN management architecture



2.3 Relationship to service-oriented architecture (SOA)

One of the architectural principles used in the management architecture for NGN is that of being a Service-Oriented Architecture (SOA). A SOA is software architecture of services, policies, practices and frameworks in which components can be reused and repurposed rapidly in order to achieve shared and new functionality. This enables rapid and economical implementation in response to new requirements thus ensuring that services respond to perceived user needs.

SOA uses the object-oriented principle of encapsulation in which entities are accessible only through interfaces and where those entities are connected by well-defined interface agreements or contracts.

Major goals of an SOA in comparison with other architectures used in the past are to enable:

- faster adaptation to changing business needs;
- cost reduction in the integration of new services, as well as in the maintenance of existing services.

SOA provides open and agile business solutions that can be rapidly extended or changed on demand. This will enable NGN Management to support the rapid creation of new NGN services and changes in NGN technology.

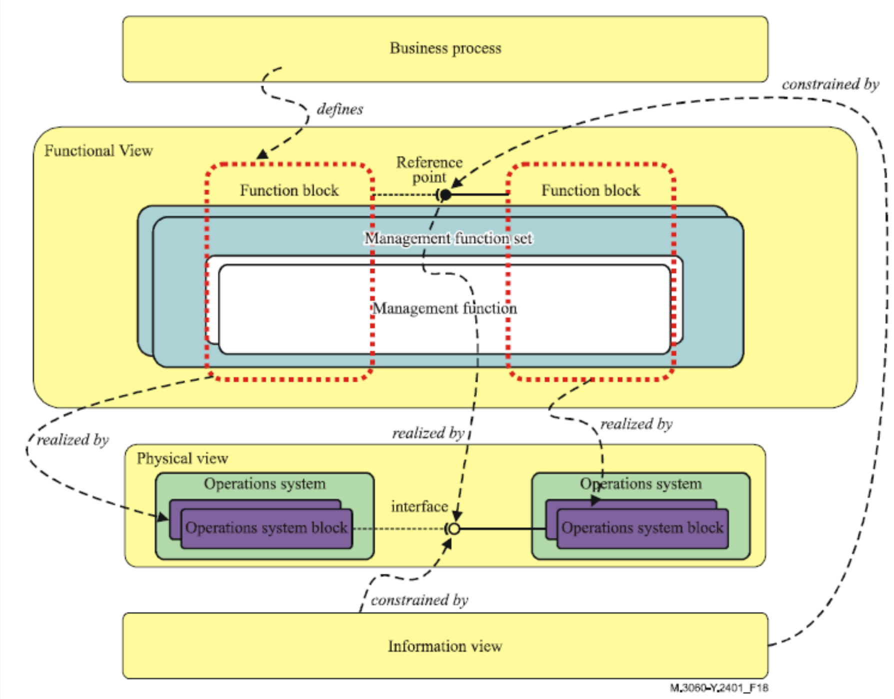
The main features of SOA are:

- loosely coupled, location independent, reusable services;
- any given service may assume a client or a server role with respect to another service, depending on situation;
- the "find-bind-execute" paradigm for the communication between services;
- published contract-based, platform and technology-neutral service interfaces. This means that the interface of a service is independent of its implementation;
- encapsulating the lifecycle of the entities involved in a business transaction; and exposing a coarser granularity of interfaces than OOA.

3 Relationships between management views

A business process provides a set of requirements that defines management functionality in the functional view. This management functionality is composed of management function sets that are composed of management functions. Operations systems realize a number of functional blocks, deployable units of management functionality, in the physical view. The functional view defines reference points that involve interaction between functional blocks. The information view constrains the data and interaction patterns of the interface between operations systems components that are physical realizations of functional blocks. Figure 3-1 shows this relationship between management views and their components.

Figure 3-1: Relationship of management views and their constructs



The management implementation is realized from four different, but interrelated views. These are the business process, functional, information and physical views. Three of these views (business process, functional and information) provide a framework that allows requirements to be documented about what a management implementation should do. The business process view, based on the eTOM model, provides a reference framework for categorizing the business activities of a service provider. The functional view framework permits the specification of what functions have to be achieved in the management implementation. The information view permits the specification of what information (i.e., data) has to be stored so that the functions defined in the functional view can be achieved in the management implementation. The management implementation, that meets the requirements of the management functional and information specifications, may vary greatly from one management solution to another. Management implementations are not currently a subject for standardization.

Annex 6: NGN Testing

1 Background

According to the transition of public telecommunication networks migration from digital circuit-switched to packet switching networks, especially aiming for IP-based network infrastructure, the testing of NGN including equipment testing become of primary importance. Ideally the operator expects to be offered equipment of high quality from the industry. But rapid growth of new technologies and the increase of equipment complexity, it is not easy to confirm the satisfaction of interesting in both operators and industries. However integral testing performed on operator networks is quite costy and it would not be reasonable to wait for external events like incidents affecting the operator networks in order to test them. It seems that the methodology of integral testing may be complemented and updated by the creation of model networks to perform equipment compatibility tests, followed by subsequent resource integration of the model networks to ensure full-fledged integral testing taking into account the interworking testing results.

By considering above, it is required that the study should be covered both compatibility and interoperability testing of various vendors' NGN equipment including new services with the existing ones in the process of NGN equipment operation. ITU-T, especially SG11 is being involved in this study as well as ETSI. This annex introduces summary information about the NGN testing based on Recommendations ITU-T Q.3900 (2006) and Q.3909 (2011) developed by SG11.

2 Technical means and functions to be tested

2.1 NGN technical means to be tested

NGN technical means which identifies as the NGN basic equipment to serve for building NGN solutions including for application shall be implemented taking into account the mandatory NGN function set. It is noted that, at the same time, the composition and number of protocols and interfaces in the specified functionality may be implemented by the manufacturer. For the purposes of standards development, the technical means functionality implemented by the manufacturer, including the requirements for the protocols and interfaces to be implemented in the specified functionality, are assumed to be in complete conformance with the functionality and purpose defined in the NGN requirements (see [ITU-T Y.2012] and [ITU-T Y.2201]).

Recommendation ITU-T Q.3900 introduces following classifications of NGN technical means in public networks as shown in Table 2-1.

Table 2-1: Classification of NGN technical means

System	NGN Technical Means
Call session control system	Media gateway controller (MGC)
	Proxy server SIP (PS)
	IP multimedia subsystem (IMS)
Voice and signalling transmit system	Media gateway (GW)
	Signalling gateway (SG)
	Transport network environment (TNE)
Application servers	Application server (AS)
	Media server (MDS)
	Messaging server (MeS)

System	NGN Technical Means
Management and billing system	NGN management system (NMS)
	Billing system (BS)
Access environment	NGN integrated access devices (NGN-IAD)
	Media gateway for legacy terminal equipment (GW-LTE)

Recommendation ITU-T Q.3900 identifies more details about functionality of the key NGN technical means from above means used in public networks as shown in Table 2-2.

Table 2-2: Functionality of key NGN technical means to be tested

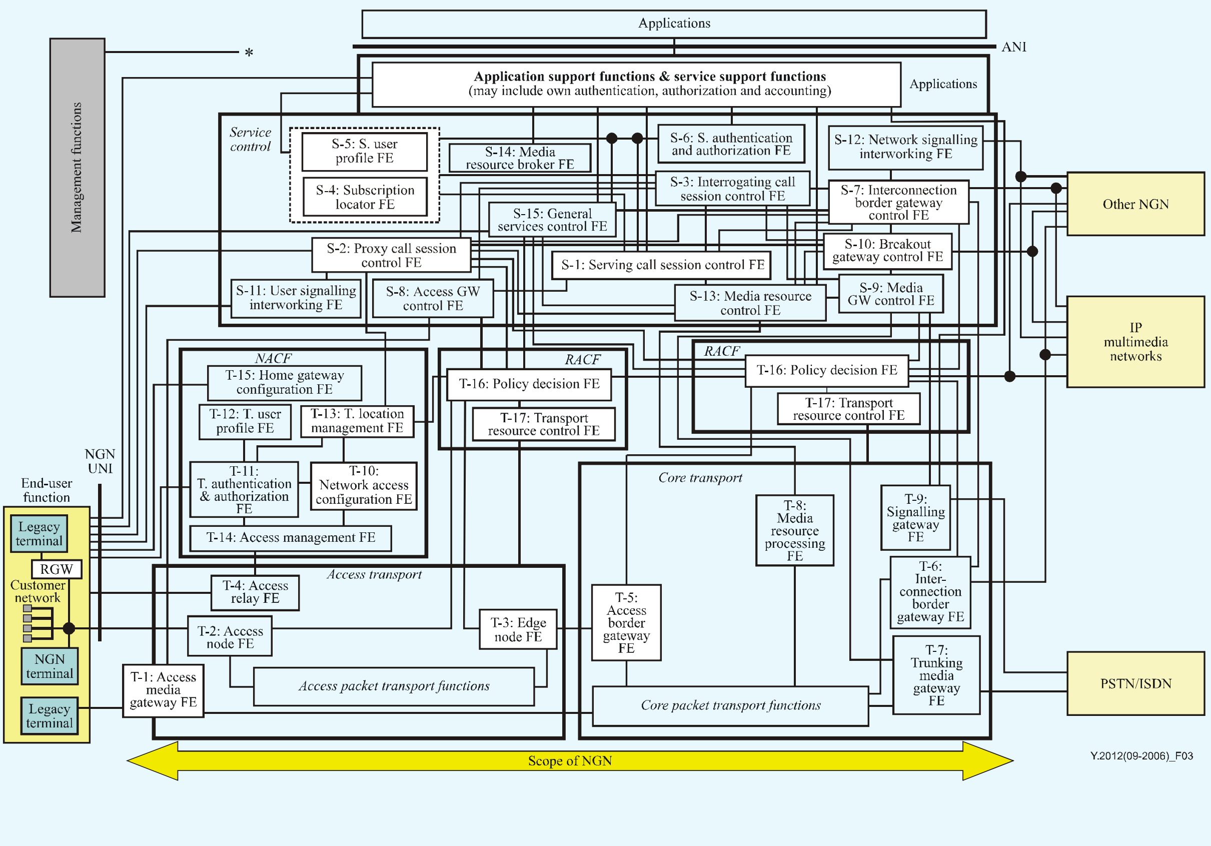
Technical means	Functionality
Media gateway controller (MGC)	• controls the calls among the PSTN subscribers; • provide for a basic part of functionality while controlling the communication sessions (transfer of routing tables, reconfiguring the numbering systems among various numbering plan formats, Media Gateway controlling by means of the signalling protocols (MGCP, H.248/Megaco, H.323, SIP) and etc; • is a main component of softswitch as a part of main switching device in the NGN.
Application server (AS)	• a software server providing new services to the users; • provisioning of new services, for example, e-commerce and electronic trade; • functionally perform as most of the NGN network components in the field of COMMUNICATION SESSION AND SERVICES CONTROL AREA; • a more flexible management of network capabilities and the creation of new and promising network scenarios.
Media server (MDS)	• provides services of interaction between the user and application or other additional communication services by means of voice and DTMF instructions. The MDS architecturally may be divided into: 1) A Media Resource Control Unit ensuring DTMF recognition, speech synthesis, speech recognition, etc; 2) A Service Control Unit ensuring forwarding messages into the message line, message recording, transfer of facsimile services, arranging conference communication, etc; • may be implemented on various software and hardware platforms based on the VoiceXML languages and so on.
Messaging server (MeS)	• responsible for message saving and message transfer to the users; • provide users with additional communication services.
Media gateway (GW)	• provides the functions of transforming the voice information into a digital format and its transfer through the NGN; • performs coding of the amplitude-frequency signals through integrated codecs (G.711, G.723, G.726, G.729, etc.), as well as transfer of digitized signals with the aid of transport protocols RTP/RTCP; • implemented, at least, one of the assortment of protocols (H.323, MGCP, H.248/Megaco, SIP) to establish connection within the GW; • used for the arrangement of interaction on the level of voice circuits between a Circuit Switched Network and NGN.

Technical means	Functionality
Signalling Gateway (SG)	• allows to convert and send a signalling load of the PSTN network to the MGC and converts such signalling types as ISDN, SS7, etc; • transfer of the SIGTRAN-stack protocols is effected over the SCTP transport protocol; • used at the boarder of the NGN and the PSTN including the arrangement of interaction.
Configuration and management system (MS)	• provide management and control of all the NGN technical means; • construct with the use of distributed and object-oriented structure with multi-protocol; • interfaces should be open using standard protocols (IIOP, CMIP, SNMP, FTP, FTAM, etc.) and the usage of formal languages for description of standard interfaces (CORBA IDL, JAVA, GDMO, ASN.1, etc.).

2.2 NGN functions to be tested

The main NGN functions to be tested as mandatory are classified as Transport stratum functions, Service stratum functions, End-user functions and Management functions. To test such functions, it is necessary to understand in more detail their internal functionality, to determine the purpose and degree of their responsibility (see Recommendation ITU-T Y.2012). An NGN functional architectures showing the detailed functionality is given in Figure 2-1.

Figure 2-1: NGN functional architecture


Applications
ANI
*
Management functions
Application support functions & service support functions
(may include own authentication, authorization and accounting)
Applications
Service control
S-5: S. user profile FE
S-4: Subscription locator FE
S-14: Media resource broker FE
S-6: S. authentication and authorization FE
S-12: Network signalling interworking FE
S-3: Interrogating call session control FE
S-7: Interconnection border gateway control FE
S-15: General services control FE
S-2: Proxy call session control FE
S-1: Serving call session control FE
S-10: Breakout gateway control FE
S-11: User signalling interworking FE
S-8: Access GW control FE
S-13: Media resource control FE
S-9: Media GW control FE
Other NGN
IP multimedia networks
NACF
T-15: Home gateway configuration FE
T-12: T. user profile FE
T-13: T. location management FE
T-11: T. authentication & authorization FE
T-10: Network access configuration FE
T-14: Access management FE
RACF
T-16: Policy decision FE
T-17: Transport resource control FE
RACF
T-16: Policy decision FE
T-17: Transport resource control FE
NGN UNI
End-user function
Legacy terminal
RGW
Customer network
NGN terminal
Legacy terminal
Access transport
T-4: Access relay FE
T-2: Access node FE
T-3: Edge node FE
T-1: Access media gateway FE
Access packet transport functions
Core transport
T-8: Media resource processing FE
T-9: Signalling gateway FE
T-5: Access border gateway FE
T-6: Inter-connection border gateway FE
T-7: Trunking media gateway FE
Core packet transport functions
PSTN/ISDN
Scope of NGN
Y.2012(09-2006)_F03

The presented NGN technical means may implement, within their composition, several functions at a time. The function sets implemented in particular technical means will be defined as following:

1) Transport functions:

- User connection to the NGN (Access Transport Functions (ATF): T-1, T-2, T-4);
- Transfer of traffic from the access network to the common transport network with the support of ATF and an additional routing capability (Edge&Access Border Gateway Functions: T-3, T-5);
- Transfer and management of all types of information (media streams, signalling messages and control system signals) being transmitted over the transport network (Core Transport Functions: T-8, T-9, T-6, T-7).

2) Transport control functions:

- QoS management including resource management, management of Network Address and Port Translation (NAPT) and NAPT Traversal at the access and transport layer. Testing should be divided for each layer separate with tests both for Access Transport Resource Control (ATRC) and for Core Transport Resource Control (CTRC). Testing of the resource control function should incorporate: packet filtering, traffic classification, service priority policies, passband reservation, network address translation, Firewall (RACF: T-17 for both access and core);
- Control of user access to the network resources (Admission Control Function) such as user authorization based on the profile should be checked (SLA, service priority, access policies determined by the type of the model network used for testing) and the access and/or transport resources available to the user (RACF: T-16 for both access and core);
- Control of user access to NGN services such as dynamic allocation of IP addresses and additional configuration parameters needed for user identification/authentication, at the network layer, for access to the network and user localization (NACF: T-10, T-11, T-13, T-14) ;
- Control of home gateway (HGW) configuration functionality such as configuration of a firewall internally in the HGW, QoS marking of IP packets, etc. (NACF: T-15).

3) Transport user profile functions: checking the possibility of configuring and modifying the information contained in the user profile at the transport layer (Transport stratum: T-12);

4) Service control functions:

- User registration and authorization at the service layer (S-6);
- Management media streams, terminal equipment and gateways (S-1, S-11, S-8, S-2, S-3, S-12, S-7, S-10, S-9, S-13).

5) Application/Service support functions:

- User registration and authorization at the application layer, for user access to the telecommunication services provided by application servers (S-4, S-5, S-6);
- Management of media streams and telecommunication services (S-14, S-15).

6) Service user profile functions: checking the capability of configuring and modifying the information contained in the user profile at the service control layer and checking the capability of interaction with the user-profile databases of other NGN architecture layers;

7) End-user functions: checking the capabilities of the terminal equipment from the gateway, to which conventional telephone sets are connected, to the multipurpose sets designed specifically for NGN networks include checking codecs, echo-cancellation systems, signalling systems and functions of interaction with the relevant NGN layers;

8) Management functions:

- Error processing management;
- Equipment configuration management;
- Billing system management;
- Service management;
- Security management.

2.3 Conformance of NGN functions to NGN technical means to be tested

The technical means used in NGN networks may implement the functionalities within their composition as shown in Table 2-3.

Table 2-3: Conformance of NGN technical means into NGN functionality

NGN technical means	NGN functionality
Call session control system	
Media gateway controller (MGC)	S-3, S-7, S-9, S-10, S-12 T-10, T-11, T-12, T-13
Proxy server SIP (PS)	S-2, S-3, S-7, S-11, S-12 T-10, T-11, T-12, T-13
IP multimedia subsystem (IMS)	S-1, S-3, S-6, S-7, S-8, S-10, S-12, S-13 T-10, T-11, T-12, T-13, T-14, T-15, T-16, T-17
Voice and signalling transmit system	
Media gateway (GW)	T-7, T-8
Signalling gateway (SG)	T-8, T-9
Transport network environment (TNE)	T-5, T-6, T-8
Application servers	
Application server (AS)	S-4, S-5, S-6, S-14, S-15
Media server (MDS)	S-4, S-5, S-6, S-14, S-15
Messaging server (MeS)	S-4, S-5, S-6, S-14, S-15
Management and billing system	
Management system (MS)	– Error processing management – Equipment configuration management – Billing system management – Service management – Security management
Billing system (BS)	
Access environment	
NGN integrated access devices (NGN-IAD)	T-2, T-4, T-3, T-5, T-15, T-14
Media gateway for legacy terminal equipment (GW-LTE)	T-1, T-2, T-3, T-4, T-5

3 Model networks for NGN testing

There are two types of model networks for NGN testing: dedicated model and distributed model networks. It should be noted that, although creation of model networks appears to be a promising testing method, not all countries are in a position to implement them to the necessary extent desired. Hence, it is reasonable to create regional model networks whose resources could be employed for testing by various countries located in the given region.

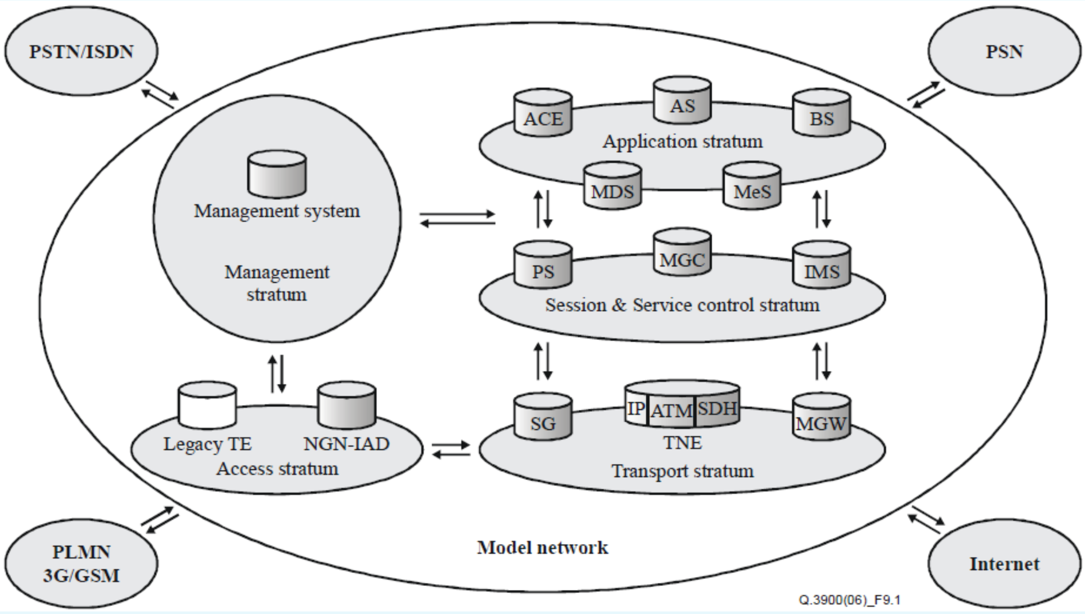
Device Under Test (DUT) may be accessed by the NGN test lab through dedicated model or distributed model. One basic requirement for such a remote testing is that the DUT must appear to the tester as it is connected directly. This is possible by creating a tunnel between the tester and the DUT using appropriate tunneling technology. Tunneling technology can be used, along with pseudo –wire capability in routers, to send the test packets directly to the remotely placed DUT. The available test suits thus become suitable for remote testing.

3.1 Dedicated model network

A dedicated model is a fragment network which is not connected to other model networks and used to perform testing for compatibility and, if possible, for interaction with the technical means employed prior to the NGN development period. The dedicated model network can be connected to a public telecommunication network and/or corporate network.

The basic architecture of a dedicated model network is shown following Figure 3-1.

Figure 3-1: Basic architecture of a model network (form of a dedicated model)



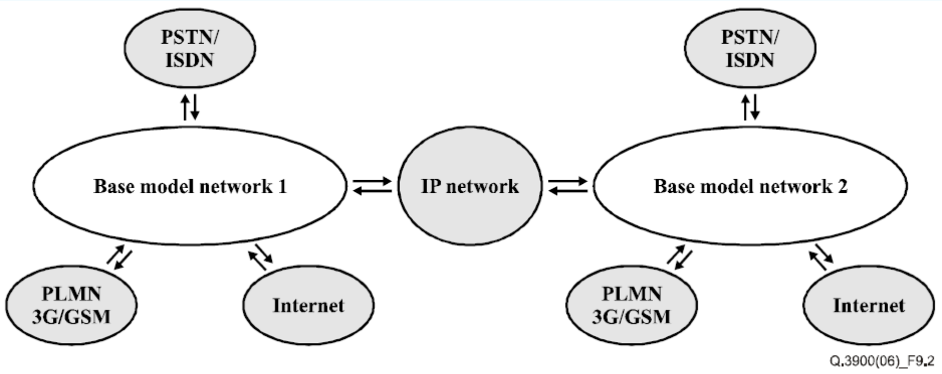
3.2 Distributed model network

A distributed model network is composed of several dedicated model networks, two as a minimum, and should be interconnected by the dedicated Intranet network such as VPN. The distributed model networks can also be connected to public telecommunication networks and/or corporate networks. The distributed model networks are used to perform complex tests for compatibility and interworking as well as to check quality of service parameters, information security requirements and interworking with the technical means. The minimum-size configuration of the model network should have:

- four nodes of the public telecommunication network (three of them should be of different types and two, as a minimum, should originate from different vendors);
- the communication networks inside the dedicated model networks provide internal communication (of the SDH, ATM or IP level) without limitation in types and manufacturers;
- four media gateways, the minimum of three of which should be of different types and the minimum of two should come from different manufacturers;
- four signalling gateways meeting the same different-type and manufacture brand requirements;
- four application servers, out of which at least two should be of different types;
- additional NGN technical means.

The basic architecture of a distributed model network is shown in Figure 3-2.

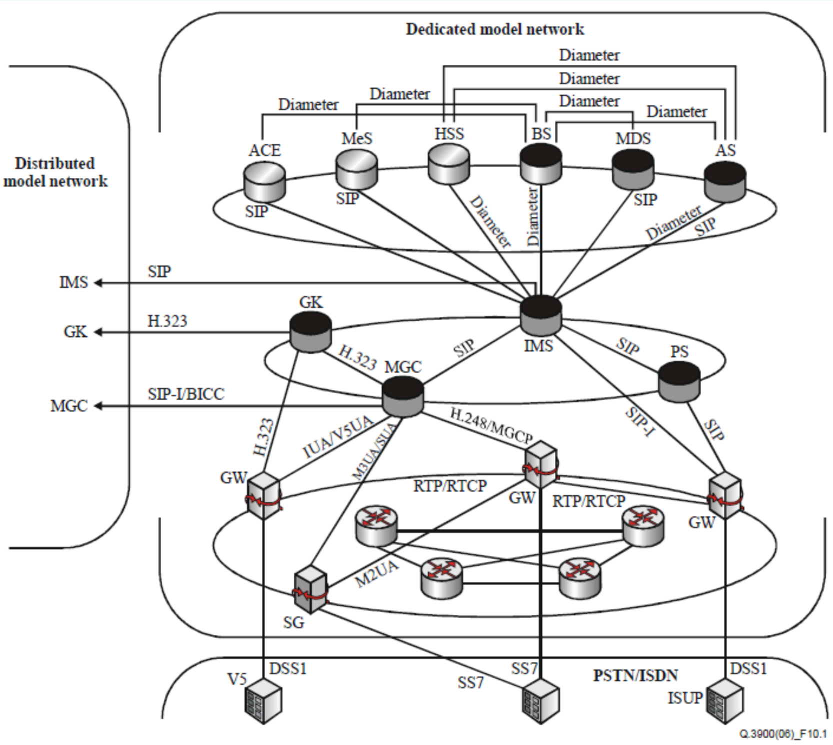
Figure 3-2: Architecture of a distributed model network in minimum-size configuration



3.3 Protocol configuration of model network

The protocols scheme of dedicated and distributed model networks must be realized in accordance with the scheme illustrated in Figure 3-3.

Figure 3-3: Protocol configuration of model network

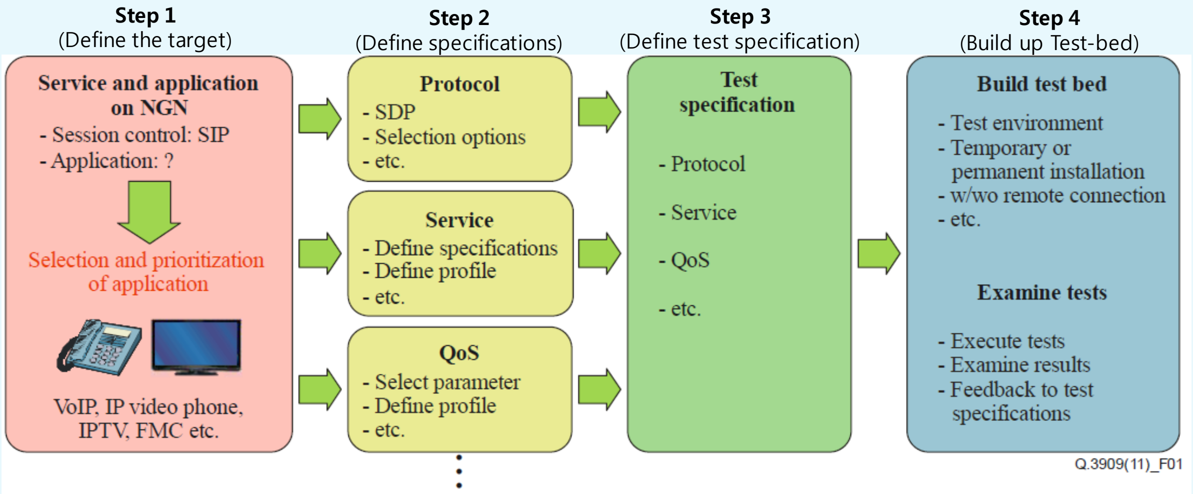


4 NGN conformance testing and interoperability testing

There are two tests to confirm the function of NGN standards: one is for conformance testing and the other is for interoperability testing. NGN conformance testing is able to show that a particular implementation complies with the protocol requirements specified in the associated base standard. However, it is difficult for such testing to be able to prove that the implementation will interoperate with similar implementations in other products. On the other hand, NGN interoperability testing can clearly demonstrate that two or more implementations will cooperate to provide the specified end-to-end functions, but cannot easily prove that either of them conforms to the detailed requirements of the protocol specification. The purpose of interoperability testing is not only to show that target products from different manufacturers can work together, but also to show that these products can interoperate using a specific protocol.

Figure 4-1 shows a four-step approach on the specification process for NGN conformance testing and interoperability testing.

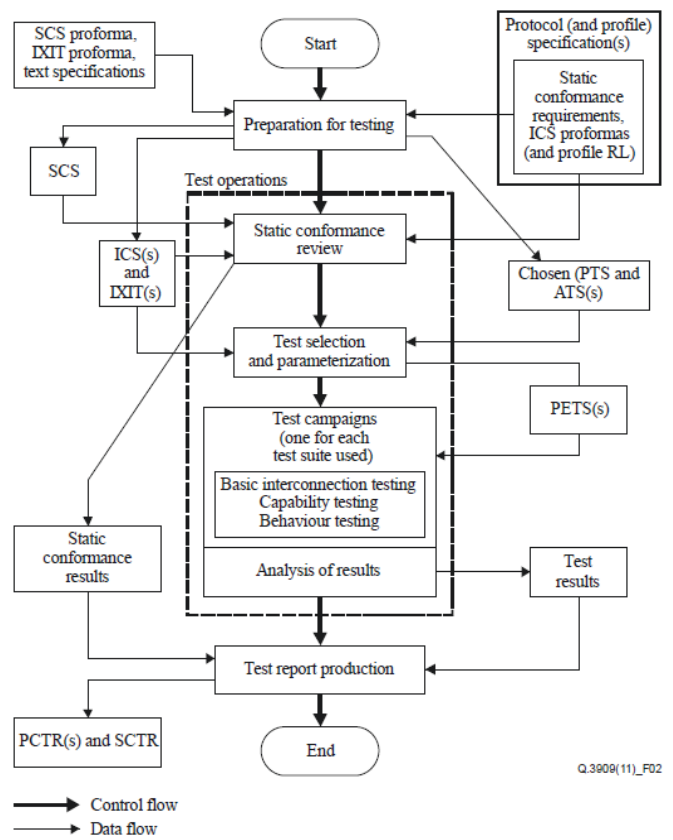
Figure 4-1: Typical NGN conformance and interoperability test specification process



4.1 NGN conformance testing

A conformance testing is performed on a product or a system to confirm that the protocol implemented in the target product (or system) is in accordance with the protocol specification described in specific Recommendations. Therefore NGN conformance testing is performed on NGN systems with relevant Recommendations. It is possible to refer to part of a procedure of the ITU-T X.29x-series as a procedure for NGN conformance testing. Figure 4-2 illustrates the overview of conformance testing of the execution procedure in [ITU-T X.290].

Figure 4-2: ITU-T X.290 conformance assessment process overview



NGN conformance testing should consider specifications on:

- the test subject which is connected to the tester or reference machine and examines conformity with reference Recommendations;
- certifications or the type of approval which may be given to the products passed by the testing authority (this is not a mandatory function of conformance testing);
- test specifications for the conformance testing which are specified in the test specification language (e.g., PICS, PIXIT).

The conformance assessment process involves following three phases: preparation, operation and reporting.

1st phase is the preparation for testing as following step:

1-1) Set the test object, target interface and target Recommendations,

1-2) Set the physical configuration and target products, and

1-3) Define the test scenarios.

2nd phase is for test operations with following step:

2-1) Static conformance review,

2-2) Test selection and parameterization, 2-3) Test campaigns (examine the conformance testing according to the scenarios) and,

2-4) Analysis of results.

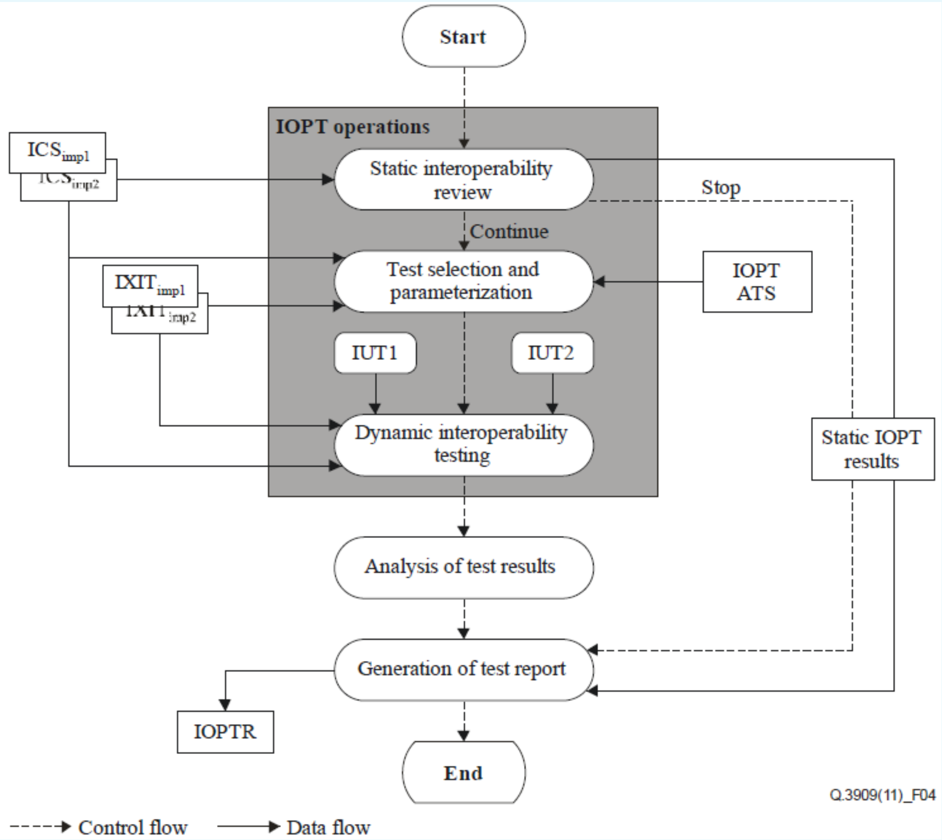
Finally 3rd phase is production of the test report.

4.2 NGN interoperability testing

Interoperability testing for NGNs is performed on two or more products. Its objective is to check the ability and performance of the products implemented by mutually exchanging information. The interoperability testing procedures of [ITU-T X-Sup.4] and [ITU-T X-Sup.5] may be referenced when undertaking NGN interoperability testing,

Figure 4-3 shows the overview of the execution procedure for interoperability testing which identified in [ITU-T X-Sup.4] and [ITU-T X-Sup.5].

Figure 4-3: Interoperability testing procedure



The execution procedure of interoperability testing in [ITU-T X-Sup.4] and [ITU-T X-Sup.5] is described as follows:

- The test operator should receive the information conformance statement (ICS) and implementation extra information for testing (IXIT), described in the applicable reference Recommendations;
- A static interoperability review is executed according to the content described in the ICSs and IXITs;
- If after review of the static interoperability test results, it is judged that interoperability testing does not need to be executed, then the test operation will be ended;
- When it is necessary to execute the tests, the settings of the test method, the test environment architecture and the test specification will be explained in detail during the process of test selection and parameterization;
- Dynamic interoperability testing is executed according to the procedure of the prepared test specification that is built in two or more implementations under test (IUTs) which, as target products, connected mutually;
- The test output in dynamic interoperability testing would be analyzed and the test result report would be generated.

Interoperability testing for NGNs should consider specifications on multiple products from multiple vendors that are connected and tested for interoperability at the service and transport level, or both. And NGN interoperability testing should be conducted in the following steps:

1) Preparation for testing

    1-1) Set the test object, target interface and target Recommendations

    1-2) Set the physical configuration and target products

    1-3) Define the test scenarios.

2) IOPT operations

    2-1) Static interoperability review

    2-2) Test selection and parameterization

    2-3) Dynamic interoperability testing (examine the interoperability testing according to the test scenarios).

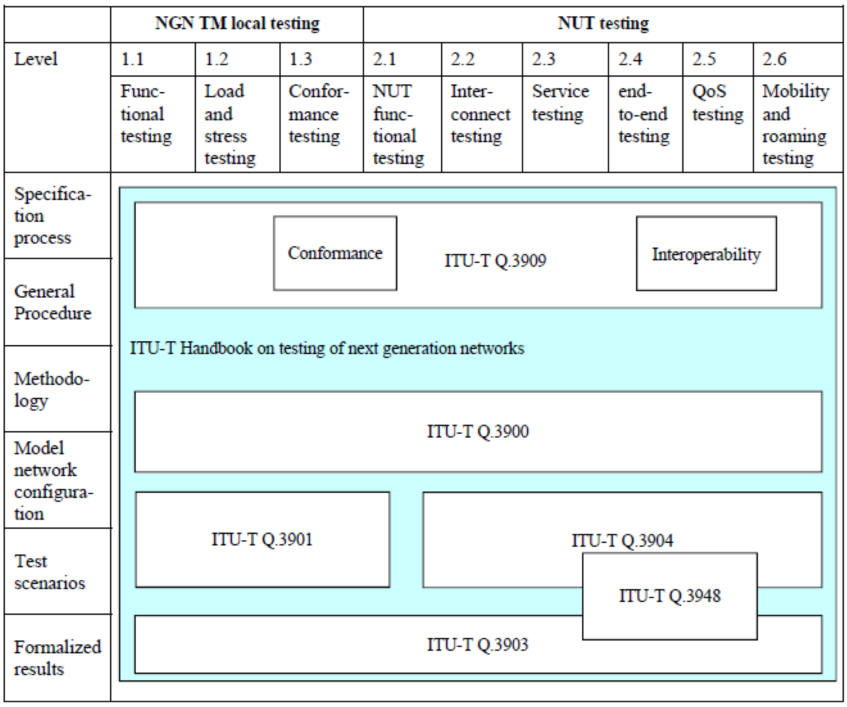
3) Analysis of test results.

4) Generation of test report.

4.3 Positioning map of NGN testing specification documents

A number of ITU-T Recommendations contain NGN testing specifications. Following Table 4-4 shows the relationship between the ITU-T Handbook on testing of NGN and ITU-T Recommendations specifying NGN testing.

Table 4-4: Recommendations for NGN tests



	NGN TM local testing			NUT testing					
Level	1.1	1.2	1.3	2.1	2.2	2.3	2.4	2.5	2.6
	Functional testing	Load and stress testing	Conformance testing	NUT functional testing	Interconnect testing	Service testing	end-to-end testing	QoS testing	Mobility and roaming testing
Specification process									
General Procedure									
Methodology									
Model network configuration									
Test scenarios									
Formalized results									

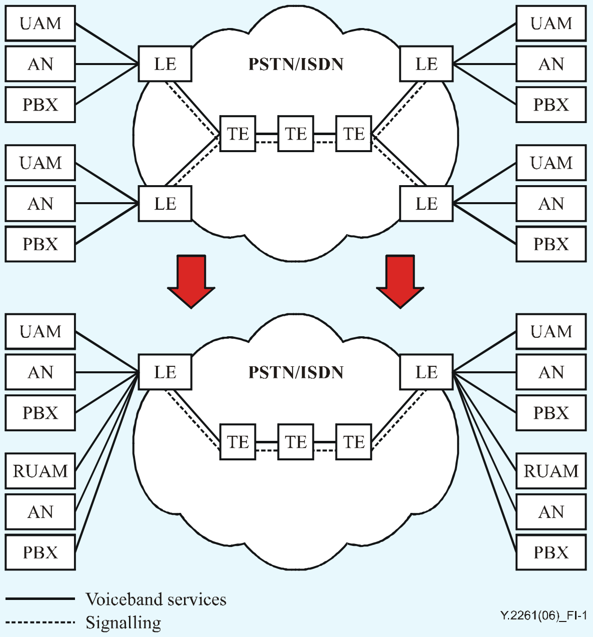
Annex 7: Examples of Migration Scenarios

1 Core Network migration to NGN

1.1 Consolidation of local and remote exchanges for migration to NGN

In order to prepare the PSTN/ISDN for the migration to a NGN, and as an initial step, some of the LEs (Local Exchanges) can be removed and all their functionalities such as control, accounting, etc. transferred to those remaining LEs. The affected UAMs (User Access Modules), PBXs, and ANs (Access Networks) are connected to the remaining LEs. Further consolidation occurs when UAMs become RUAMs (Remote UAMs), which are connected to the remaining LEs. Figure 1-1 shows this preparatory step.

Figure 1-1: Preparation for migration to NGN

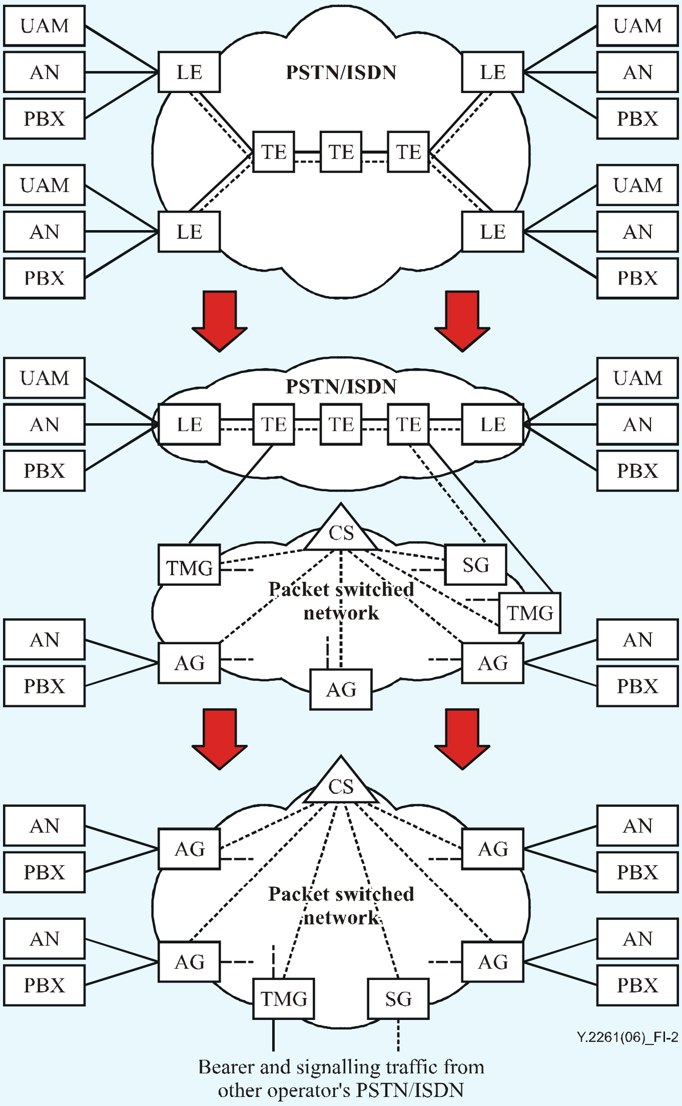


1.2 Scenario 1 – PSTN/ISDN and NGN initially co-exist

In the most likely initial approach for migration of PSTN/ISDN to the NGN, the PSTN/ISDN will co-exist with the NGN during a transition period. There are two steps in this scenario.

- Step 1: In this step, some of the LEs are replaced by AGs (Access Gateways). Functions originally provided by the removed LEs are now provided by the AGs and the CS. In addition, some of the access elements such as UAMs, RUAMs, and PBXs, which were originally connected to the removed LEs, are now directly connected to AGs. Additional AGs may also be deployed to support new subscribers that directly connect to them. The TMGs (Trunking Media Gateways) and SGs (Signaling Gateways) are deployed for interconnection between the NGN and the TEs of the legacy network as well as other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by the CS.
- Step 2: In this step, the remaining LEs are replaced by the AGs, and the TEs are removed and their control functions are performed by CS. The TMGs and SGs are deployed for interconnection between PSN and other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by the CS.

Figure 1-2: Realization of scenario 1



——— Voiceband services
------------ Signalling
– – – – – Data

NOTE – Data indicate packetized voiceband services.

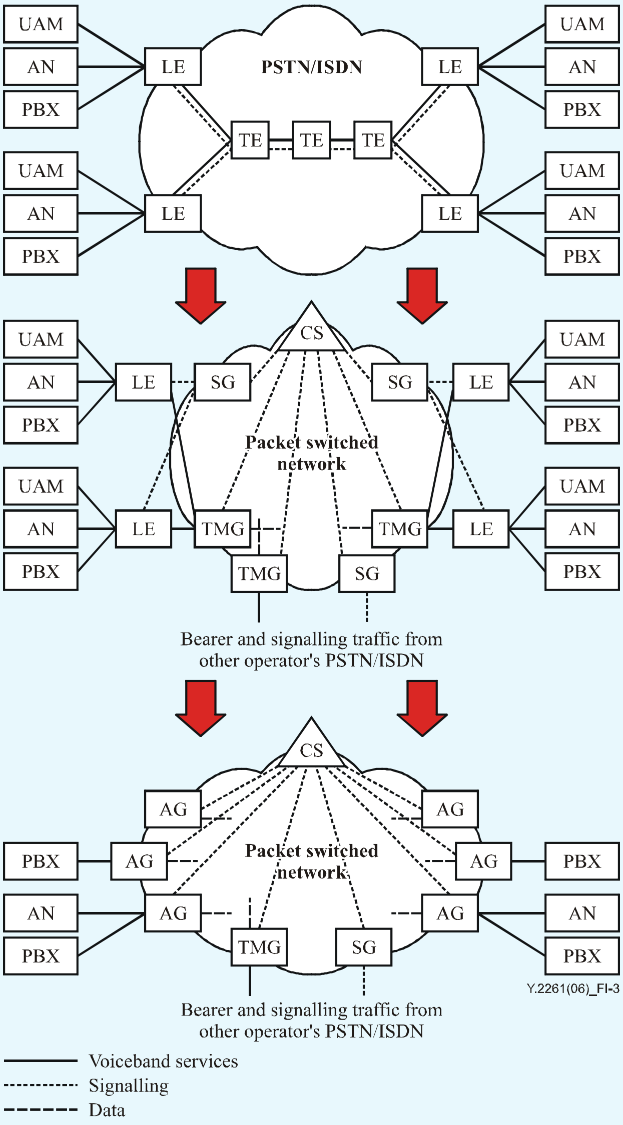
1.3 Scenario 2 – Immediate use of NGN, initially via SGs and TMGs

In this scenario, the PSTN/ISDN is immediately replaced by the NGN. As a first step, the LEs are connected to SGs and TMGs, while later on they are eliminated.

- Step 1: In this step, PSTN/ISDN is replaced by NGN and the TE functions are performed by the TMGs and the SGs under the control of the CS. The LEs are connected to the NGN via TMGs and SGs. The TMGs and SGs are also deployed for interconnection between NGN and other operators' PSTNs/ISDNs.

- Step 2: In this step, the LEs and some of the access elements such as UAMs and RUAMs are removed and their functions are provided by the AGs and CS. The PBXs are directly connected to the AGs. The ANs are either replaced by the AGs or are connected to the AGs. The TMGs and SGs are deployed for interconnection between NGN and other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by CS.

Figure 1-3: Realization of scenario 2

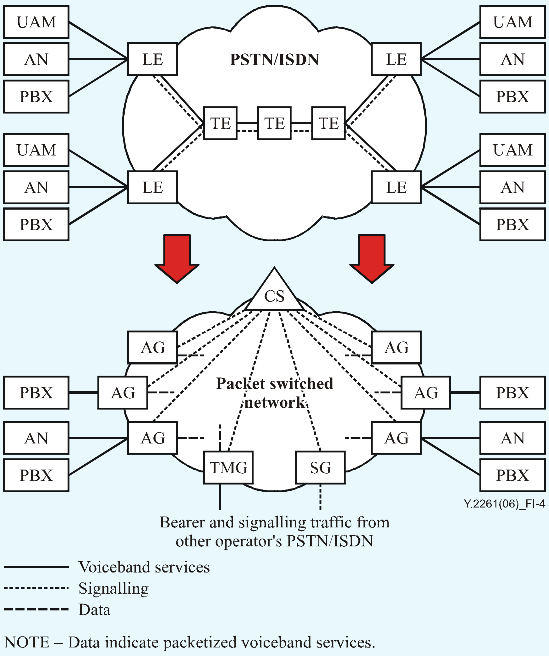


NOTE – Data indicate packetized voiceband services.

1.4 Scenario 3 – The one-step approach

In this scenario, the PSTN/ISDN is replaced with NGN in only one step. The LEs are replaced by AGs and their functions are divided between the AGs and the CS. Specifically, the call control and accounting functions are all transferred to the CS. All access elements such as UAMs, RUAMs, and PBXs are connected to AGs. The ANs are either replaced by the AGs or are connected to NGN through the AGs. The TMGs under the control of the CS, and the SGs, are deployed to replace the TE functions and provide interconnection between NGN and other operators' PSTNs/ISDNs.

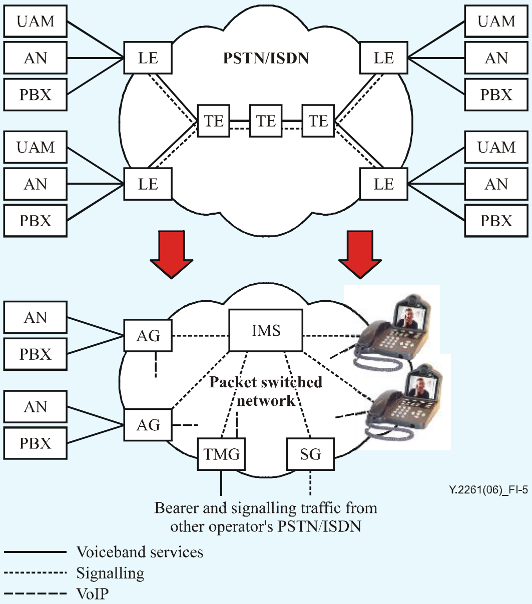
Figure 1-4: Realization of scenario 3


UAM
AN
PBX
LE
PSTN/ISDN
TE
CS
AG
Packet switched network
TMG
SG
Y.2261(06)_FI-4
Bearer and signalling traffic from other operator's PSTN/ISDN
Voiceband services
Signalling
Data
NOTE – Data indicate packetized voiceband services.

1.5 IMS-based migration to NGN

In the case of where PSTN/ISDN evolves directly to a NGN based on the IMS core network architecture, the end-users access the network using NGN user equipment or legacy user equipment connected via an AG. The TMGs and SGs are deployed for interconnection between the NGN and other operators' PSTNs/ISDNs.

Figure 1-5: IMS-based PSTN/ISDN migration to NGN

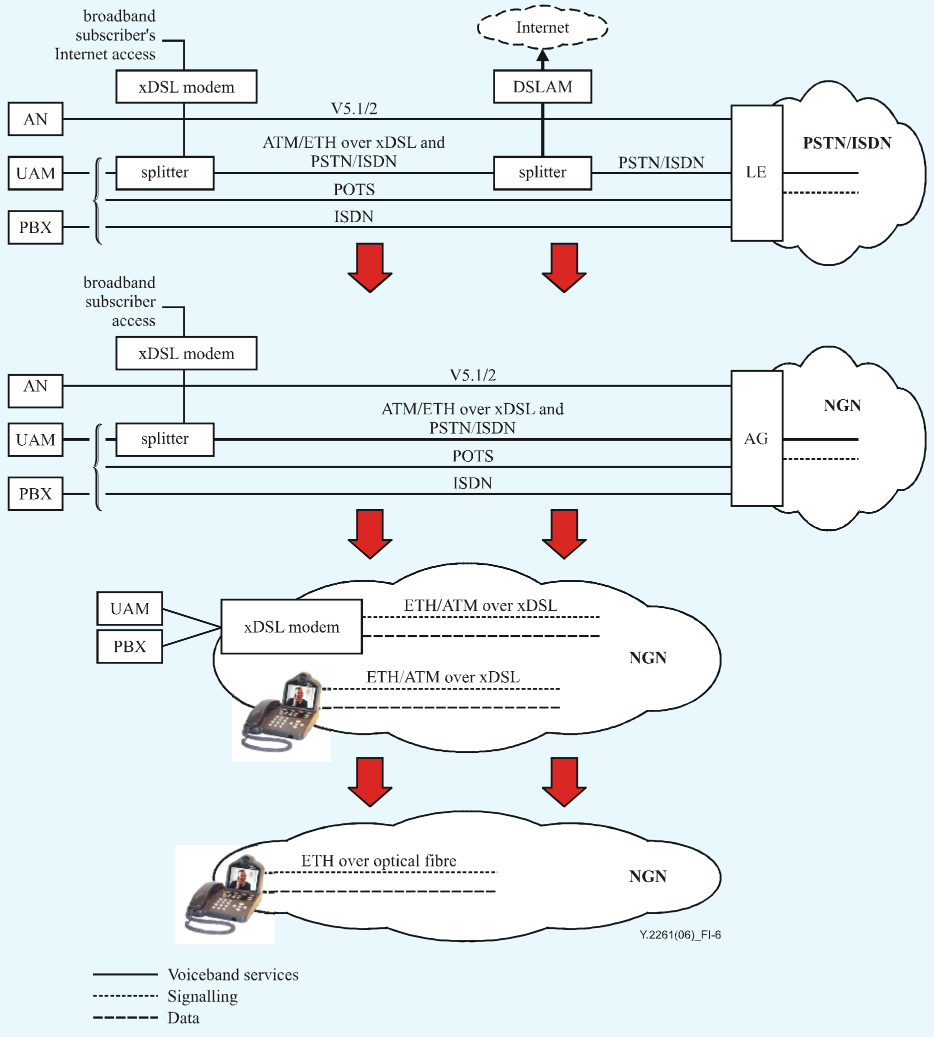


2 Access network migration to NGN

Legacy voice users may also have access to broadband services for example via xDSL (see [G.995.1]). In this case, the customer-located equipment is an xDSL modem and the service provider equipment is a digital subscriber line access multiplexer (DSLAM). Since xDSL interfaces enable users to connect to the Internet, these interfaces may be utilized to connect such users to NGNs. AN, for another user domain with V5.x [G.964] and [G.965] interface can be left as it is shown in Figure 5-6 or it can be completely replaced by AG connected to NGN directly. Migration of access network is shown in three possible steps.

- Step 1: Traditional AN/UAM interfaces include: POTS, ISDN and V5.1/2 [G.964] and [G.965]. Such interfaces connect subscribers to the core PSTN/ISDN via LE.
- Step 2: An IP user may also use xDSL interface as the transport medium to an NGN. Protocol for xDSL interface may be Ethernet which enables broadband data flows and services, e.g., VoD, IPTV, VoIP and Internet.
- Step 3: In this step, the legacy end systems are replaced by NGN end systems and twisted copper lines are replaced by optical fibre, either fibre-to-the-curb (FTTC) or fibre-to-the-home (FTTH) to increase transmission speed.

Figure 2-1: Migration of xDSL access to NGN



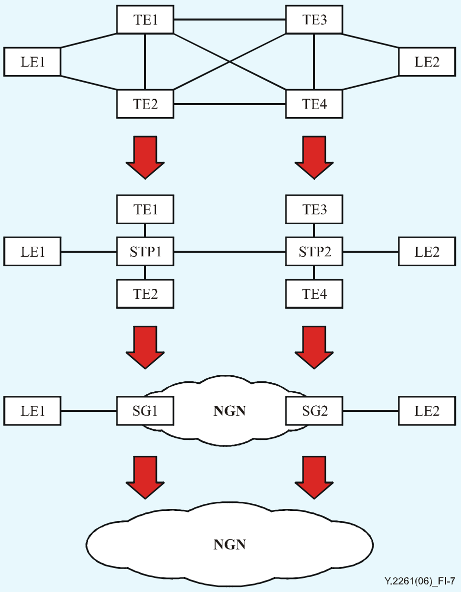
NOTE – Data indicate packetized voiceband services.

3 Signaling and control scenarios

A possible scenario for migration of signalling in the core network consists of following three steps.

- Step 1: In this step, signalling functions are transferred from the TEs to the independent units creating an STP mesh network (partial or complete).
- Step 2: In this step, STPs are upgraded to the SGs and are placed on the edge between PSTN/ISDN and NGN. In this case, both the legacy network and NGN co-exist with each other.
- Step 3: In this step, all LEs and TEs are replaced by NGN.

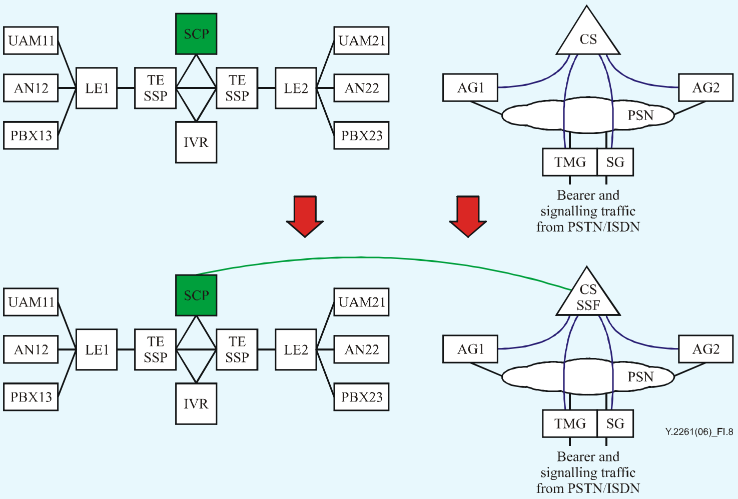
Figure 3-1: Realization of signalling migration scenario



4 Services migration scenarios

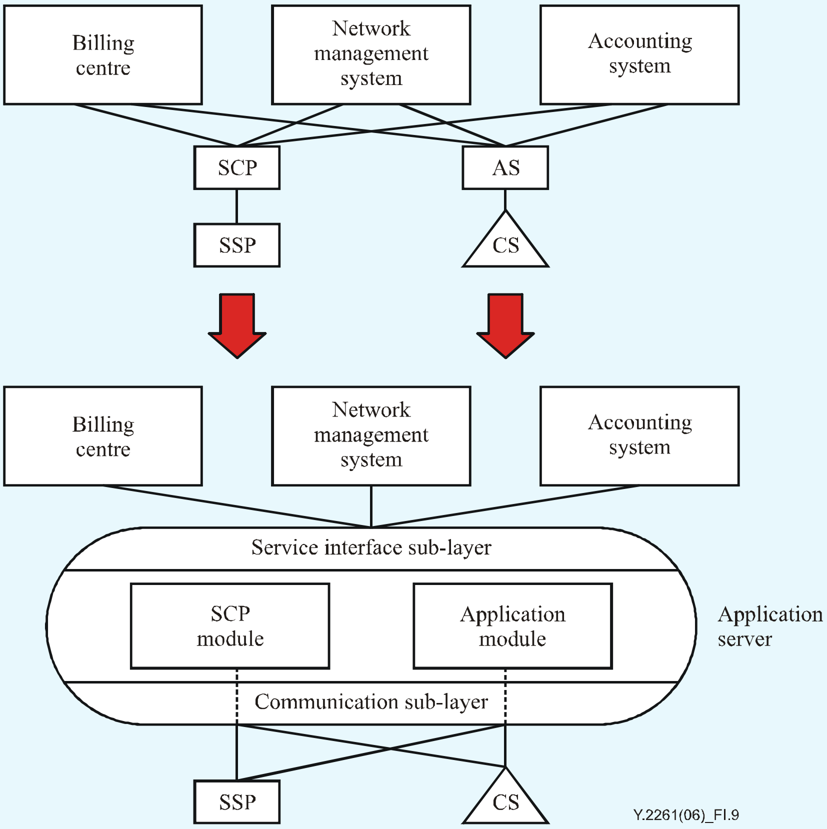
- Scenario 1: In this scenario, existing IN services are reused in NGN by implementing SSF in the CS. Both PSTN/ISDN and NGN exist.

Figure 4-1: Realization of scenario 1



- Scenario 2: In this scenario, the SCP is integrated to the application server. The communication sub-layer is a uniform communication layer which may provide connection between SSP, CS, SCP and the application server. The services created by the service creation environment (SCE) in the IN may be directly loaded into the SCP module of the AS. The SCP and the application module may be connected through a service interface sub-layer to operation and maintenance and external systems (e.g., billing centre, network management centre, accounting system).

Figure 4-2: The SCP is integrated to the application server as a whole

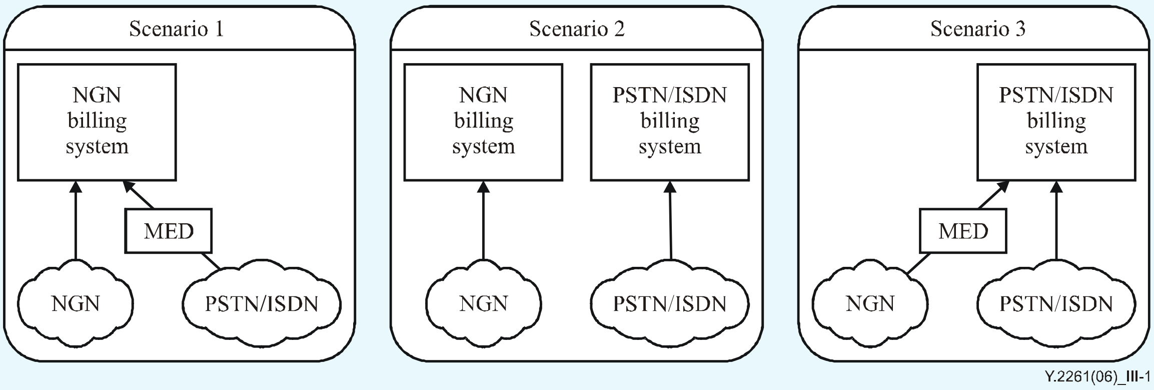


5 Billing system migration scenarios

The following three scenarios are considered when migration to NGN. The timing or preference for selection of these scenarios is service provider dependent. Mediation (MED) is an entity which allows transfer and processing of call detail records (CDRs) from the PSTN/ISDN to the NGN billing system, or from the NGN to the PSTN/ISDN billing system.

- Scenario 1: For this scenario, an NGN billing system is considered to handle both the PSTN/ISDN and the NGN. For this case, all accounting aspects are affected.
- Scenario 2: For this scenario, a new billing system is developed for the NGN, while keeping the existing PSTN/ISDN billing system. For this case, all accounting aspects are to be considered for NGN.
- Scenario 3: For this scenario, a legacy billing system is considered to handle both the PSTN/ISDN and the NGN. For this case, all accounting aspects are affected.

Figure 5-1: Billing system migration scenarios



Annex 8: NGN Issues

NGN should continuously evolve to build up "Connected World" providing more convenient ways to use services and application including to use of relevant network resources allowing from other providers such as 3rd party providers. Another important aspect is that NGN should support Ubiquitous Networking which will represent the situation of "Connect to Anything" in other words called IoT “Internet of Things”. For these, service platform aspects and capabilities to support ubiquitous networking of NGN have been seriously considered and developed during the last few years, especially in ITU-T NGN-GSI.

1 Service Integration and Delivery Environments in NGN

NGN-GSI in ITU-T studied on service platform aspects which should support multi-fold telecommunication business model and through this, NGN enhances NGN end-users access to applications. ITU-T Recommendation Y.2240 (approved at January 2011, formerly known as Y. NGN-SIDE) identifies service delivery platform called NGN-SIDE can be viewed as the next generation service delivery platform (SDP) and its framework can conceptually be applicable to other telecommunication environments (e.g. mobile networks).

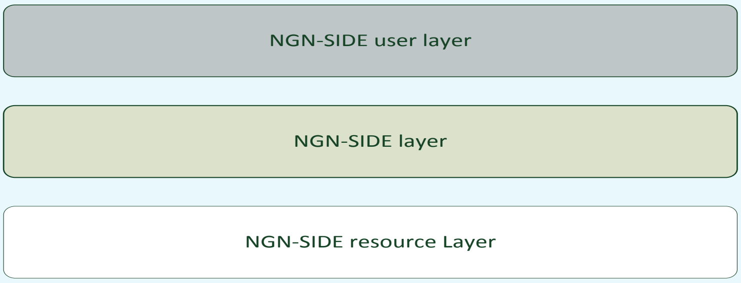
NGN-SIDE is defined as “an open environment in NGN integrating resources from different domains and delivering integrated services to applications over NGN.” Here, domains include, but are not limited to, telecommunication domain (e.g. fixed and mobile networks), Internet domain, Broadcasting domain and Content Provider domain.

The following main functionalities are supported in the NGN-SIDE ecosystem:

- integration of resources from different domains (e.g. telecommunication domain (fixed and mobile networks), broadcasting domain, internet domain or content provider domain) over NGN;
- adaptation, including abstraction and virtualization, of resources from different domains;
- resource brokering for mediation among applications and resources;
- support of application development environment for application developers;
- support of different service interfaces across ANI, UNI, SNI and NNI for exposure of NGN-SIDE capabilities and access to resources in different domains;
- provision of mechanisms for the support of diverse applications including cloud services, machine to machine, and ubiquitous sensor network applications;
- provision of mechanisms for the support of applications making usage of context based information;
- provision of mechanisms for content management.

NGN-SIDE has a layered architecture as shown in the following Figure 1-1:

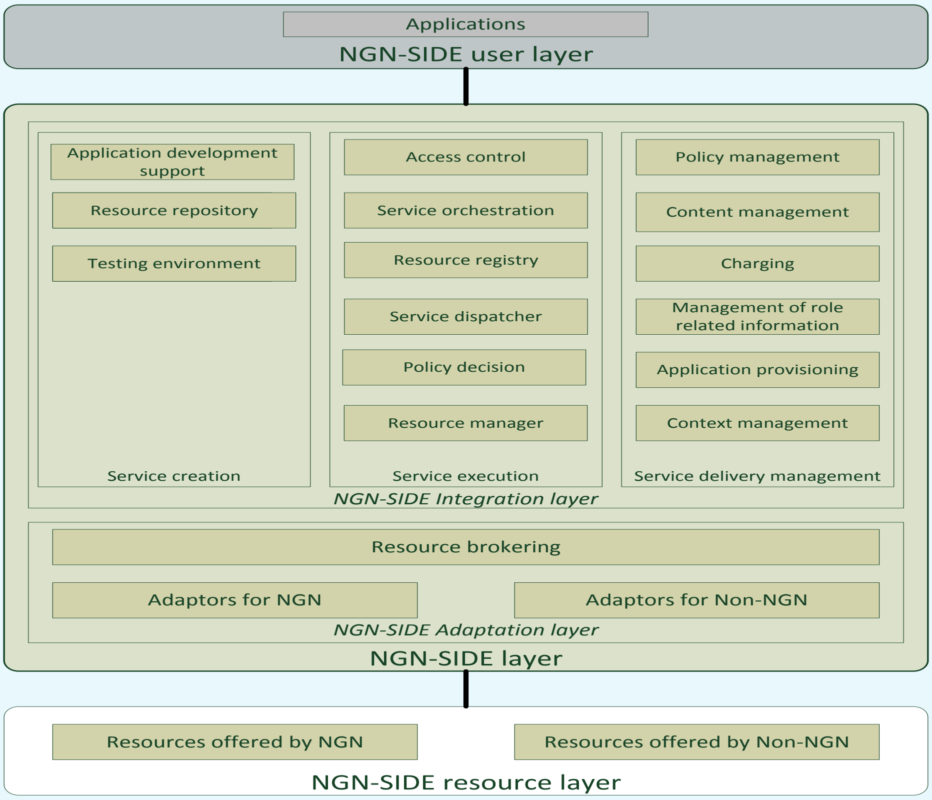
Figure 1-1: Layered View of NGN-SIDE



- The NGN-SIDE user layer uses the services offered by the NGN-SIDE layer, including resource exposure. It includes users accessing the NGN-SIDE, such as applications and other users.
- The NGN-SIDE layer corresponds to NGN-SIDE.
- The NGN-SIDE resource layer includes resources accessible by NGN-SIDE, such as applications, service enablers, network capabilities, connectivity, computing, storage, and content.

The following Figure 1-2 shows a functional view of NGN-SIDE according to the above described layers, the NGN-SIDE layer being comprised of the NGN-SIDE integration layer and the NGN-SIDE adaptation layer:

Figure 1-2: Functional View of NGN-SIDE



In order to reduce the complexity of integrating resources, the NGN-SIDE integration layer provides a unified way for the NGN-SIDE users to access the resources offered by NGN and Non-NGN. It supports the service creation functional group, the service execution functional group and the service delivery management functional group:

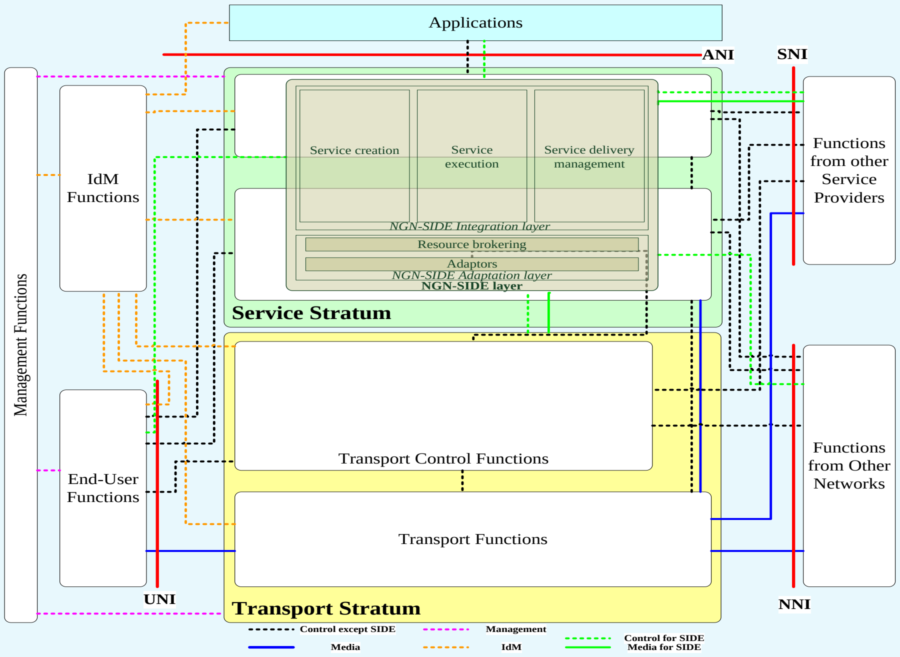
- the service creation functional group provides capabilities to realize an application development environment for application developers;
- the service execution functional group provides capabilities to support the service execution environment;
- the service delivery management functional group provides capabilities to realize the management of different aspects, provisioning of applications and charging for ensuring proper functioning of the service creation and service execution functional groups and providing associated delivery functionalities.

The NGN-SIDE adaptation layer adapts resources offered by NGN-SIDE resource providers such as their own service logic and service control, and related protocols, in order to provide uniformly adapted resources (e.g. control and media format) for interaction with the NGN-SIDE integration layer. NGN-SIDE resource providers use standardized or proprietary interfaces called “NGN-SIDE resource interfaces” to offer resources to NGN-SIDE and these interfaces are adapted by NGN-SIDE.

NGN-SIDE positioning within the NGN reference architecture is shown in the following Figure 1-3:

The NGN-SIDE functional components are positioned inside the NGN service stratum. The NGN-SIDE adaptation layer enables the abstraction of resources, including the resources of the NGN transport stratum (e.g. transport control functions and transport functions related resources) and the NGN service stratum (e.g. service control functions and content delivery functions related resources).

Figure 1-3: NGN-SIDE positioning within the NGN reference architecture



2 Open Service Environments in NGN

Another important aspect of NGN in the sense of services is that enabling new capabilities and supports a wide range of emerging services with advanced and complex functionalities for application providers such as 3rd party providers. In response to a drive from application providers and/or developers to develop new applications and capabilities accessible via standard interfaces, NGN providers should cooperate in the development of standard application network interfaces (ANI) including software reusability and portability. An open service environment (OSE) within NGN aims to provide efficient and flexible capabilities based on the use of standard interfaces to NGN applications thereby enabling applications to take full advantage of the NGN capabilities. Two ITU-T Recommendations address this OSE as follows:

- ITU-T Recommendation Y.2234 (approved at 2008): defines the requirements that are divided into service requirements and functional requirements.
- ITU-T Recommendation Y.2020 (2011): defines the OSE architecture for NGN based on ITU-T Y.2234 and ITU-T Y.2201.

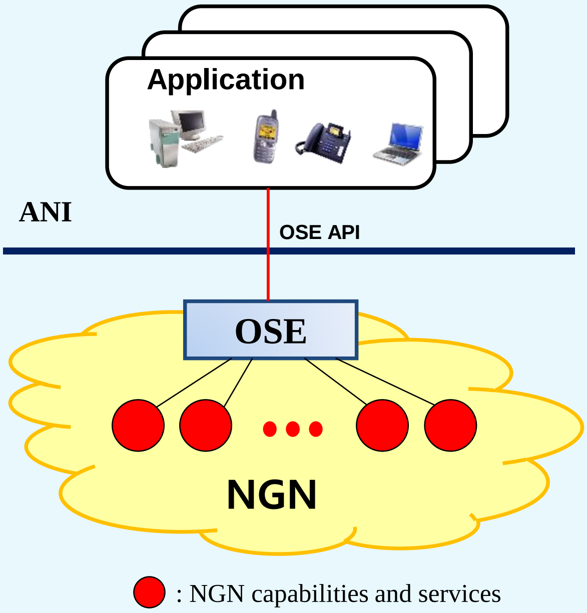
Open service environment provides capabilities to enable flexible and agile service creation, execution and management based on the use of standards interfaces. The use of standard interfaces will ensure NGN OSE based service reusability and portability across networks, as well as accessibility by application providers and/or developers.

OSE capabilities have the following characteristics:

- Flexible development of applications and capabilities by NGN providers, application providers, and other service providers;
- Exposure of capabilities via standard application network interfaces (ANI);
- Portability and re-usability of capabilities across networks (and from other network to NGN or from NGN to other network);
- Leveraging new capabilities enabled by technologies from non-NGN environments

The OSE allows applications to make use of NGN capabilities and/or services offered through the application network interface (ANI) as shown in Figure 2-1. Application providers and/or developers will be able to create and provide new applications via standard interfaces at the ANI as shown OSE API regardless of the type of underlying network and/or equipment.

Figure 2-1: Open service environment capabilities in NGN



Service requirements of NGN-OSE capabilities are defined as followings:

- Provide standard APIs for application providers and/or developers to create and introduce applications quickly and seamlessly;
- Provide the service level interoperability among different networks, operating systems and programming languages (e.g. Web Services are an example of enabling technology for providing service level interoperability);
- Support service independence from NGN provider and manufacturers [ITU-T Y.2201]:
- Support OSE capabilities based on NGN providers' capabilities. However, OSE capabilities based on application providers' capabilities are not supported in this version of the document;
- Support location, network and protocol transparency [ITU-T Y.2201]:
- Provide capabilities for coordinating services among themselves and services with applications;
- Support service discovery capabilities to allow users and their devices to discover the services, applications, and other network information and resources of their interest [ITU-T Y.2201]. In addition, discovery mechanisms for services or components of multiple application providers are recommended to be provided;
- Provide the means to manage the registration of capabilities, services and applications. The technology choice is required to ensure functions for service registration and deregistration, including configuration, activation, publication [ITU-T Y.2201];
- Provide the service management capabilities such as service tracking, update management, auditing, version control, logging, e.g. provide a record of the history of services, access control management, statistical analysis of service registration and utilization.
- Support NGN services reuse by providing service composition capability;
- Support of a service composition language;

- Offer a development support environment which supports construction, trialing, deployment, and removal of applications [ITU-T Y.2201];
- Allow interworking with service creation environments and network entities for creation and provisioning of applications and services [ITU-T Y.2201];
- Provide a secure access to the NGN capabilities in alignment with the general NGN security requirements as specified in clause 5.13 of [ITU-T Y.2201];
- Support policy enforcement capability for resources protection and management, and service personalization.

The functions to support of the NGN-OSE are consisted with service coordination, service discovery, service registration, service management, service composition, service development support, interworking with service creation environments and policy enforcement. In each function has more detail requirements as following:

The NGN service coordination functions are required to:

- Provide coordination of applications and services with capabilities;
- Provide the tracking of NGN capabilities or service components from various application providers, and the relationship between these capabilities or service components;
- Support the information on state change of capabilities or service components for applications and services.

The NGN service discovery functions are required to:

- Provide service discovery for physically distributed NGN services;
- Support a variety of discovering criteria (e.g. specific field based discovery, classification system based discovery). An example of discovering criteria is implemented in the Universal Discovery, Description and Integration (UDDI) specification of Web Services framework;
- Use user and device profile information for discovering the proper service;
- Allow users to discover user-interest services, device-interest services and network information;
- Support a variety of scoping criteria (e.g. location and cost) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy (This allows support of customized discovery for a wide range of scenarios.);
- Use a variety of approaches for discovering services such as client-server, P2P, combination of client-server and P2P;
- Support appropriate mechanisms to ensure security and privacy;
- Take into account scalability (e.g. broadcast mechanisms are recommended to be avoided).

The NGN service registration functions are required to:

- Provide service registration, including configuration, activation, publication and service deregistration;
- Provide a variety of service registration features (e.g. manual, autonomous) for NGN services;
- Support a variety of registration parameters, including mandatory and optional parameters.

The NGN service registration functions may support:

- Registration services in centralized and de-centralized ways;
- Multiple concurrent service registrations.

The NGN service management functions are required to:

- Provide a monitoring function of registered services for availability and predicted response time. NGN services and user applications might need to use monitoring information for the availability or predicted response time of target services before executing services;
- Provide managing functions of QoS information about registered NGN services such as accessibility, performance, integrity, reliability, etc.;
- Provide a version management function to NGN services for interoperability;
- Provide notification service functions for updated services;
- Provide failure detection and recovering functions for unexpected failures;
- Provide service tracking management functions to capture and log all relevant information for each component within a service chain. Service tracking is recommended to allow for an association among the captured data associated with a specific service. Service tracking is required to enable tracking of capabilities or components of multiple third parties, and the relationships between these capabilities or components;
- Provide a service substitution function that considers various kinds of factors to users. It is required to provide mechanisms to capture a set of information including terminal capability, network situation, user preference and substitution policy; and judge whether to substitute the service or not based on the captured information. If there is a need to substitute the service, this function will substitute it;
- Provide service access control functions to control the accessibility of a specific service by applications. (The service access control function provides the necessary authentication and authorization actions required to ensure that the application has appropriate access rights for the requested service.);
- Provide statistical analysis functions to analyze service registration and utilization information (e.g. number of registered services, utilization frequency of registered services, and number of applications using registered services.);
- Provide an auditing function to review the overall operations of open service environment capabilities during a specific period required by the auditor.

The NGN service composition functions are required to:

- Provide a composition language that describes the interaction among services. Additionally, the composition language is recommended to support expression capabilities for describing the composition logic among services;
- Support the composition of services statically or dynamically (i.e. for the static type, the services are composed during service design; while for the dynamic type, the services are composed during service runtime).

The NGN service development support functions are required to:

- Support services re-use and allow for services interchangeability;
- Support mixing-and-matching of services by management of interfaces and consistent semantics of shared data/schema across these services
- Support the full life cycle of services, ranging from installation, configuration, administration, publishing, versioning, maintenance and removal;
- Support delivery-agnostic application designs to allow applications to be implemented without requiring re-design for each subsequent development scenario;
- Support tracking of dependencies among services.

The NGN service creation environment interworking functions are required to:

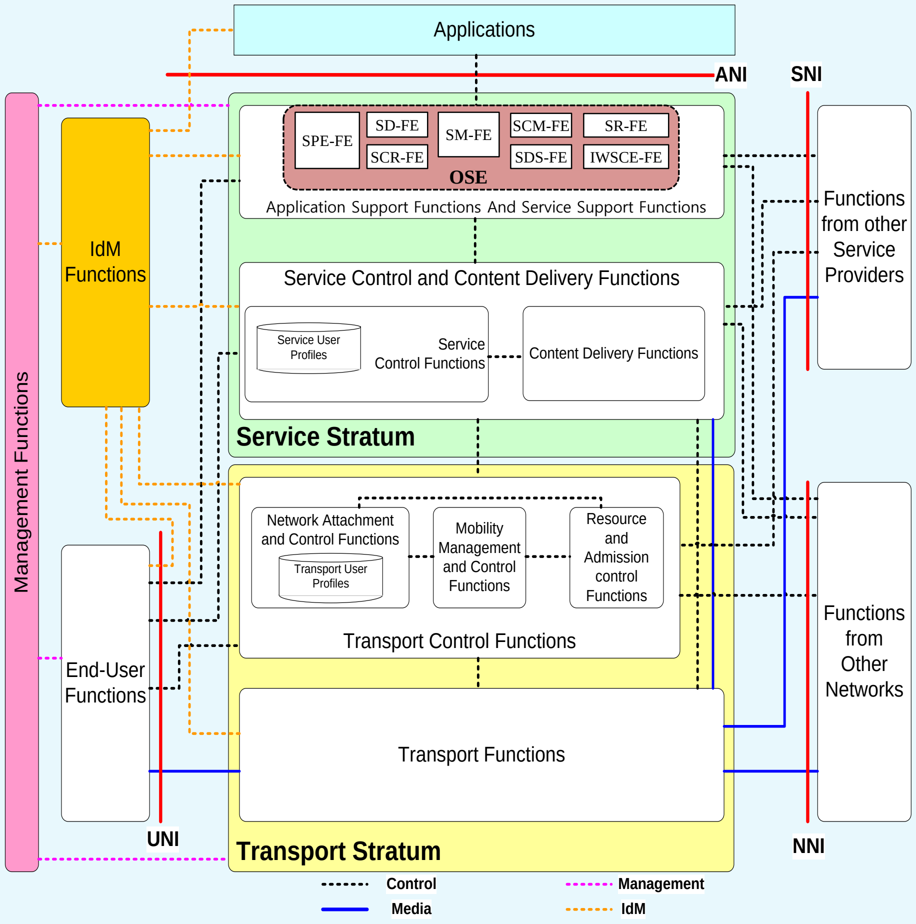
- Support the following three classes of service creation environments

The NGN policy enforcement functions are required to:

- Provide a description language to express various kinds of policy rules such as those related to authorization, charging, service level agreement and logging. This language is recommended to support policy re-use;
- Provide a policy execution framework to interpret and execute the policies;
- Protect services from unauthorized users' requests and manage requests based on the policy rules;
- Support the selection of appropriate services for service composition to respond to the needs and preferences of a user or a group of users.

Figure 2-2 shows the extended NGN architecture overview [ITU-T Y.2012] in order to illustrate the positioning of the OSE functional group.

Figure 2-11: OSE positioning in the NGN architecture


Applications
ANI
SNI
SPE-FE
SD-FE
SCR-FE
SM-FE
SCM-FE
SDS-FE
SR-FE
IWSCE-FE
OSE
Application Support Functions And Service Support Functions
Functions from other Service Providers
Management Functions
IdM Functions
Service Control and Content Delivery Functions
Service User Profiles
Service Control Functions
Content Delivery Functions
Service Stratum
Network Attachment and Control Functions
Transport User Profiles
Mobility Management and Control Functions
Resource and Admission control Functions
Transport Control Functions
End-User Functions
Functions from Other Networks
Transport Functions
UNI
NNI
Transport Stratum
Control
Media
Management
IdM

3 Next Generation Ubiquitous Networking (NGUN)

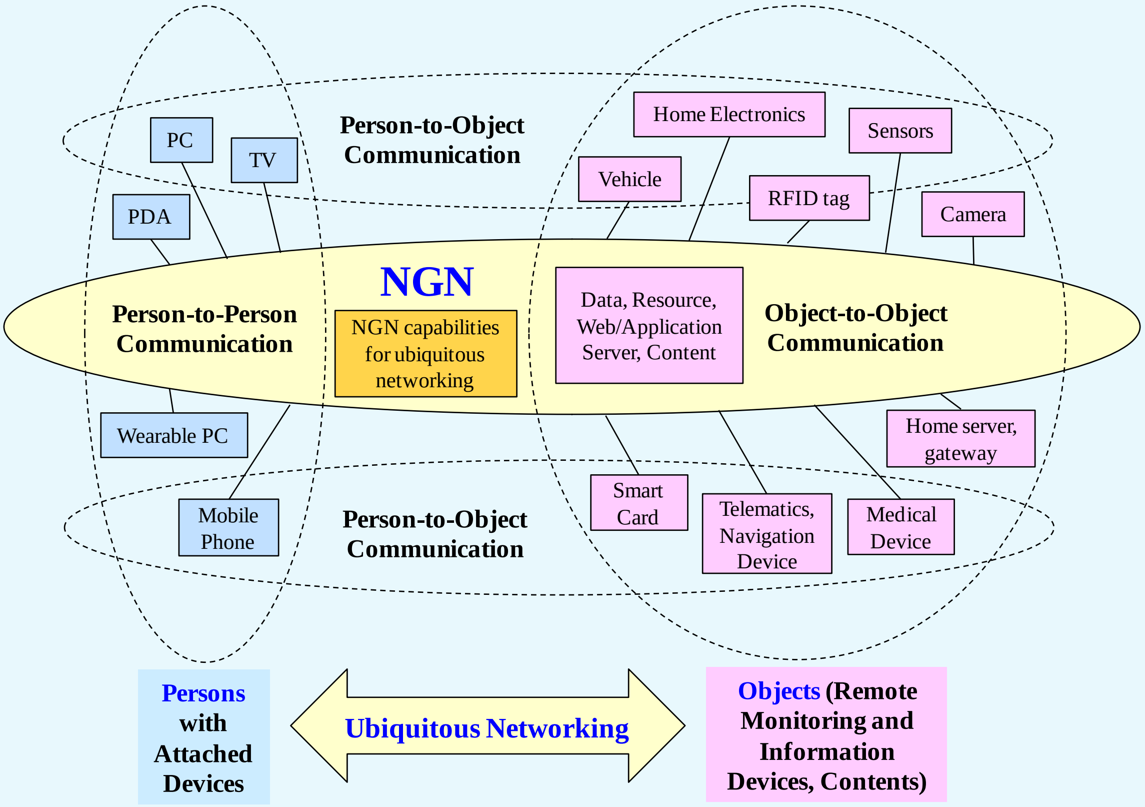
To realize the vision of "Connect to Anything" or in other words IoT “Internet of Things”, networks should have capabilities of Ubiquitous Networking. It is not easy to define of “Ubiquitous Networking” because of the conceptual features of “Ubiquitous” or “Ubiquity”. ITU-T developed a recommendation to specify the “Ubiquitous” features as a networking capability of NGN. The ITU-T Recommendation Y.2002 (10/2009) specifies “Next Generation Ubiquitous Networking” as a part of NGN recommendations.

In this recommendation, “Ubiquitous Networking” identifies as “The ability for persons and/or devices to access services and communicate while minimizing technical restrictions regarding where, when and how these services are accessed, in the context of the service(s) subscribed to”. Based on this definition, this recommendation identifies fundamental characteristics of ubiquitous networking as followings:

- IP connectivity: IP connectivity will allow objects involved in ubiquitous networking to communicate with each other within a network and/or when objects have to be reachable from outside their network. Particularly, as many new types of objects will be connected to networks, IPv6 will play a key role in object-to-object communications
- Personalization: Personalization will allow to meet the user’s needs and to improve the user’s service experience since delivering appropriate contents and services to the user. User satisfaction is motivated by the recognition that a user has needs, and meeting them successfully is likely to lead to a satisfying client-customer relationship and re-use of the services offered
- Intelligence: Intelligence which enables network capabilities to provide user-centric and context-aware service is essential to meet numerous network requirements in terms of data handing and processing capabilities. Introduction of artificial intelligence techniques in networks will help to accelerate the synergies and ultimately the “fusion” between the involved industries
- Tagging objects: Tag-based solutions on ubiquitous environment will allow to get and retrieve information of objects from anywhere through the network. Radio frequency identifier (RFID) is one of tag-based solutions for enabling real-time identification and tracking of objects. As active tags have networking capabilities, a large number of tags will need network addresses for communications. As IP technology will be used for ubiquitous networking, it is essential to develop mapping solutions between tag-based objects (e.g. RFIDs) and IP addresses
- Smart devices: Smart devices attached to networks can support multiple functions including camera, video recorder, phone, TV, music player. Sensor devices which enable detection of environmental status and sensory information can utilize networking functionalities to enable interconnection between very small devices, so-called ‘smart dusts’. Specific environments such as homes, vehicles, buildings will also require adaptive smart devices

Figure 3-1 illustrates the different types of communications for ubiquitous networking.

Figure 3-1: Ubiquitous networking communication types


Person-to-Object Communication
PC
TV
PDA
Home Electronics
Sensors
Vehicle
RFID tag
Camera
NGN
Person-to-Person Communication
NGN capabilities for ubiquitous networking
Data, Resource, Web/Application Server, Content
Object-to-Object Communication
Wearable PC
Home server, gateway
Smart Card
Telematics, Navigation Device
Medical Device
Mobile Phone
Person-to-Object Communication
Persons with Attached Devices
Ubiquitous Networking
Objects (Remote Monitoring and Information Devices, Contents)

Note: objects include all of things which are attached in the network. Some objects can be attached with persons and others can be located remotely with persons. "person-to-person" communication relies on a "object-to-object" communication.

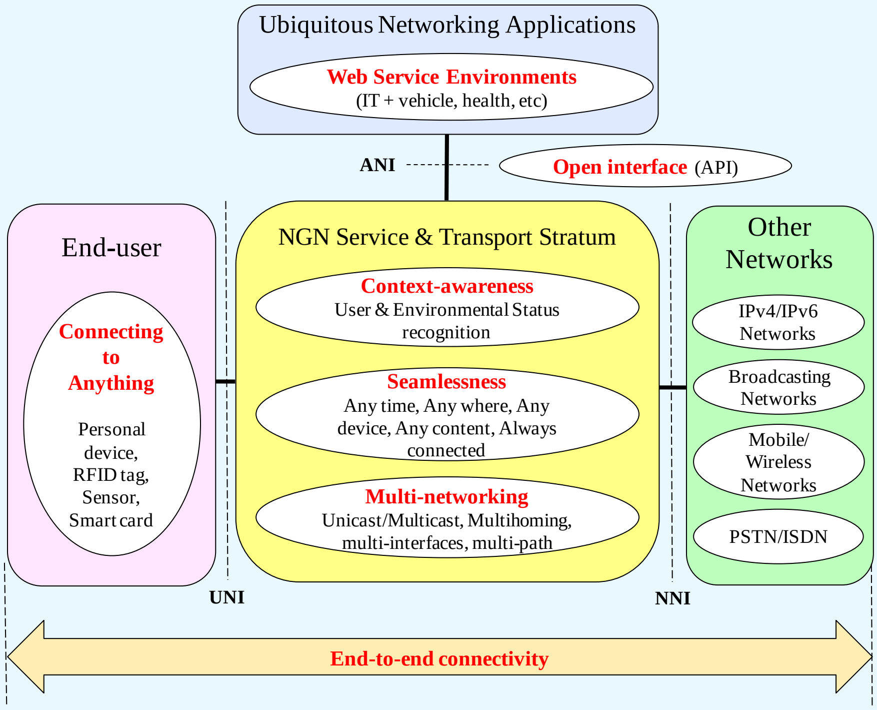
Figure 3-1 makes a distinction between the following users of ubiquitous networking: persons (using attached devices such as PC, PDA, mobile phones) and objects (such as remote monitoring and information devices, contents) and shows three different types of communications:

- Person-to-Person Communication: persons communicate with each other using attached devices (e.g. mobile phone, PC);
- Person-to-Object Communication: persons communicate with a device in order to get specific information (e.g., IPTV content, file transfer);
- Object-to-Object Communication: an object delivers information (e.g. sensor related information) to another object with or without involvement of persons.

Ubiquitous networking aims to provide seamless communications between persons, between objects as well as between persons and objects while they move from one location to another.

Figure 3-2 shows the high-level architectural model for ubiquitous networking in NGN. This model is based upon the NGN overall architecture as described in [ITU-T Y.2012] showing the necessary capabilities to support of ubiquitous networking.

Figure 3-2: High-level architectural model for ubiquitous networking in NGN


Ubiquitous Networking Applications
Web Service Environments
(IT + vehicle, health, etc)
ANI
Open interface (API)
End-user
Connecting to Anything
Personal device, RFID tag, Sensor, Smart card
NGN Service & Transport Stratum
Context-awareness
User & Environmental Status recognition
Seamlessness
Any time, Any where, Any device, Any content, Always connected
Multi-networking
Unicast/Multicast, Multihoming, multi-interfaces, multi-path
Other Networks
IPv4/IPv6 Networks
Broadcasting Networks
Mobile/ Wireless Networks
PSTN/ISDN
UNI
NNI
End-to-end connectivity

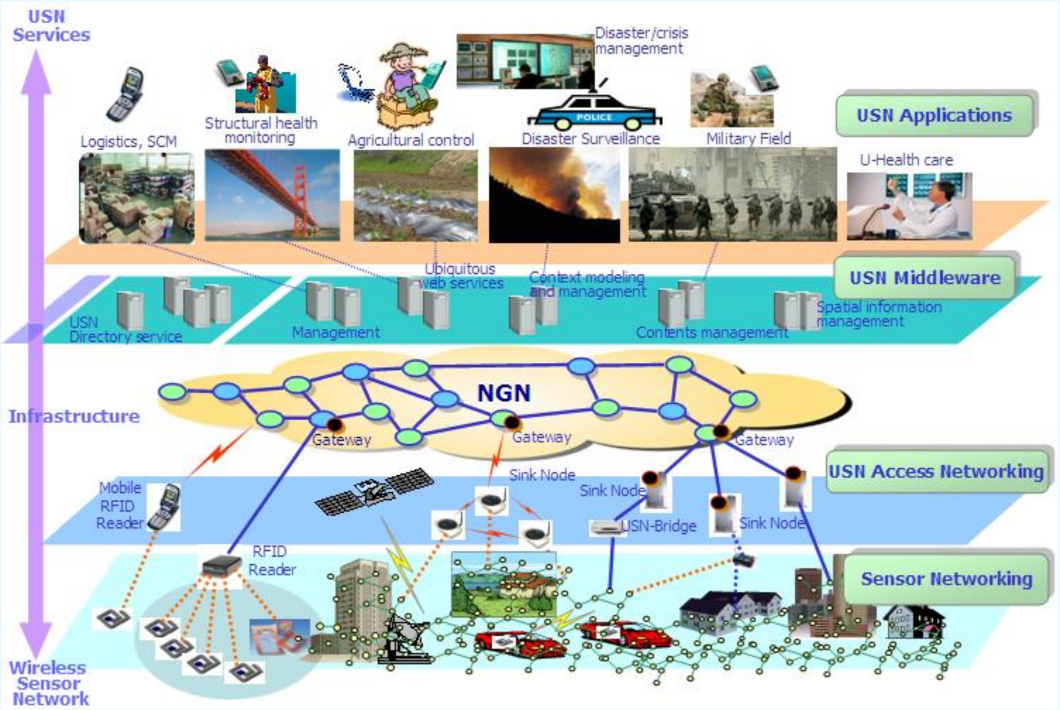
4 Ubiquitous Sensor Networks (USN)

The technology using sensors has huge potential as it could generate applications in a wide range of fields, including ensuring safety and security, environmental monitoring, promoting personal productivity and enhancing national competitiveness. The term of "Ubiquitous Sensor Networks" (USN) is used to describe a network which is configured with sensors that could provide ubiquitous connectivity.

ITU-T Recommendation Y.2221 provides a description and general characteristics of USN and their applications and services. This recommendation also analyzes service requirements of USN applications and services, and specifies extended or new NGN capability requirements based on the service requirements. The main components of a USN, as described in Figure 4-1 are:

- Sensor Networking: Comprising sensors which are used for collecting and transmitting information about their surrounding environment and an independent power source (e.g., battery, solar power);
- USN Access Networking: Intermediary collection of information from a group of sensors through "sink nodes" and facilitating communication with a control centre or with external entities;
- Network Infrastructure: Next Generation Network (NGN);
- USN Middleware: Software for the collection and processing of large volumes of data;
- USN Applications Platform: A technology platform to enable the effective use of a USN in a particular industrial sector or application.

Figure 4-1: Schematic Layers of a Ubiquitous Sensor Network



Sensor is a device that captures a physical stimulus such as temperature, sound, light, pressure, heat, vibration, or magnetism. Sensor data has to be transmitted to users for data processing and corresponding reactions.

Sensor networks can be established by wire-line or wireless. Typical wire-line networking techniques are RS-232, RS-422, RS-485, Power Line Communication, etc. A variety of wireless networking techniques has been used. But nowadays standardized ways have emerged as hot topics and a new term, WSN (Wireless Sensor Network), was made for technology and business marketing. Typical wireless PHY/MAC networking solutions are IEEE 802.15.4, IEEE 802.15.3, Bluetooth, etc. Multi-hop networking solutions over these wireless networks are ZigBee, 6LoWPAN, etc.

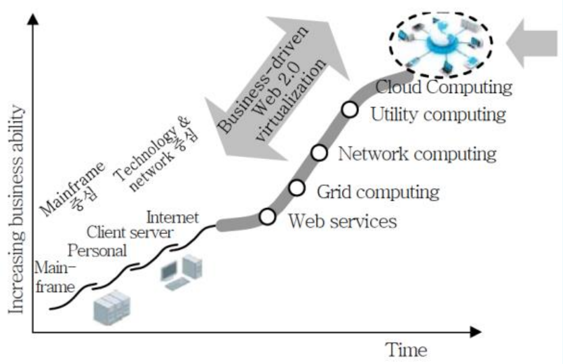
5 Cloud Computing

5.1 Background and definition of Cloud Computing

The background history about the cloud computing may back to the dates when mainframe became available in academia and corporations, accessible via dumb terminals which were used for communications but had no internal computational capacities. Thus it had been required to share main-frame with multiple users by multiple terminals in terms of physical access to the computer as well as to share the CPU time such as time-sharing. In the 1990s, telecommunications with offering virtual private network (VPN) services with comparable quality of service, but at a lower cost, it began to use the cloud symbol to denote the demarcation point between providers including users. Cloud computing extends this boundary to cover servers as well as the network infrastructure. Following Figure 5-1 shows brief summary of such history about cloud computing developments.

According to the developments of computing capabilities, users such as scientists and technologists explored ways to make large-scale computing power available to more users over time sharing, optimal use of the infrastructure, platform and prioritized access to the CPU. In addition, the ubiquitous availability of networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, autonomic, and utility computing have led to growth of cloud computing.

Figure 5-1: History of computing



Cloud computing is defined as a model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or resource pooling provider interaction. Cloud computing enables cloud services which identified as a service that is delivered and consumed on demand at any time, through any access network, using any connected devices using cloud computing technologies. It is considered from a telecommunication perspective that users are not buying resources but cloud services that are enabled by cloud computing environments.

The cloud computing model promotes availability and is composed of six essential characteristics, five cloud service categories and four deployment models as followings:

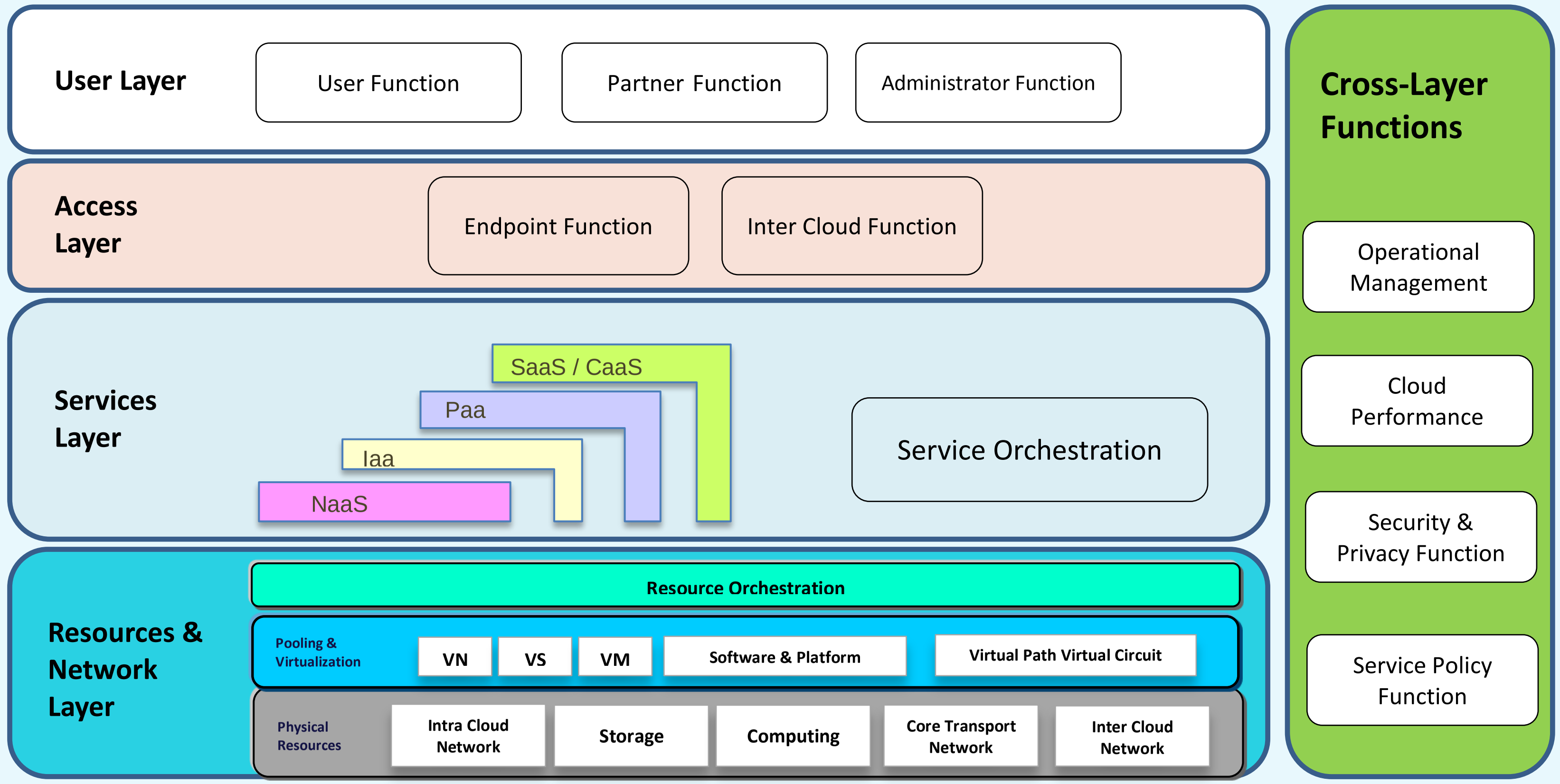
- On-demand self-service: A cloud service user can unilaterally provision computing capabilities, such as server time, network storage and communication and collaboration services, as needed automatically without requiring human interaction with each service's cloud service provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- Resource pooling: The cloud service provider's computing resources are pooled to serve multiple users or organisations using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction (e.g., country, state, data center). Examples of resources include storage (typically on hard or optical disc drives), processing, memory (typically on DRAM), network bandwidth, and virtual machines.

- Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the cloud service user, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured Service: Cloud systems automatically control and optimize resource use (e.g., storage, processing and bandwidth) by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., the number of active user accounts). Resource usage can be monitored, controlled, and reported. It provides transparency for both cloud service provider and cloud service users.
- Multi-tenancy: A characteristic of cloud in which resources are shared amongst multiple cloud tenants. Tenant is intended here as any Cloud Service User (CSU) workload that has unique requirements and/or a unique operating agreement with the Cloud Service Provider (CSP). There is an expectation on the part of the cloud tenant that its use of the cloud is isolated from other tenants' use in the same share resource pool; that tenants in the cloud are restricted from accessing or affecting another tenant's assets; that the cloud tenant has the perception of exclusive use of, and access to, any provisioned resource. The means by which such isolation is achieved vary in accordance with the nature of the shared resource, and can affect security, privacy and performance.

5.2 Architecture model

Figure 5-1 shows a functional architecture model of cloud computing. These functional layers in the architecture are derived by grouping cloud related functions.

Figure 5-1: Functional Architecture Model of Cloud Computing



- User Layer: performs interaction between the cloud service user and the underlying cloud architecture layers. The User Layer is used to setup secure mechanism with cloud computing, send cloud service requests to cloud and receive cloud services from cloud, perform cloud service access, administrate and monitor cloud services;
- Access Layer: provides a common interface for both manual and automated cloud service capabilities and service consumption;
- Services Layer: the cloud service provider orchestrates and exposes services of the five cloud service categories. The Cloud Services Layer manages the cloud components required for providing the services, runs the software that implements the services and arranges to offer the cloud services to the cloud service user;
- Resources & Network Layer: The Resources and Network layer is where the physical resources reside including equipment typically used in a data centre such as servers, networking switches and routers, storage, etc, and the corresponding non-cloud-specific software that runs on the servers and other computers such as host operating systems, hyper-visors, device drivers, generic systems management software, etc;
- Cross-Layer Functions: perform overall system management (i.e., operations, administration, maintenance and provisioning (OAM&P)) and monitoring, and provide secure mechanisms.

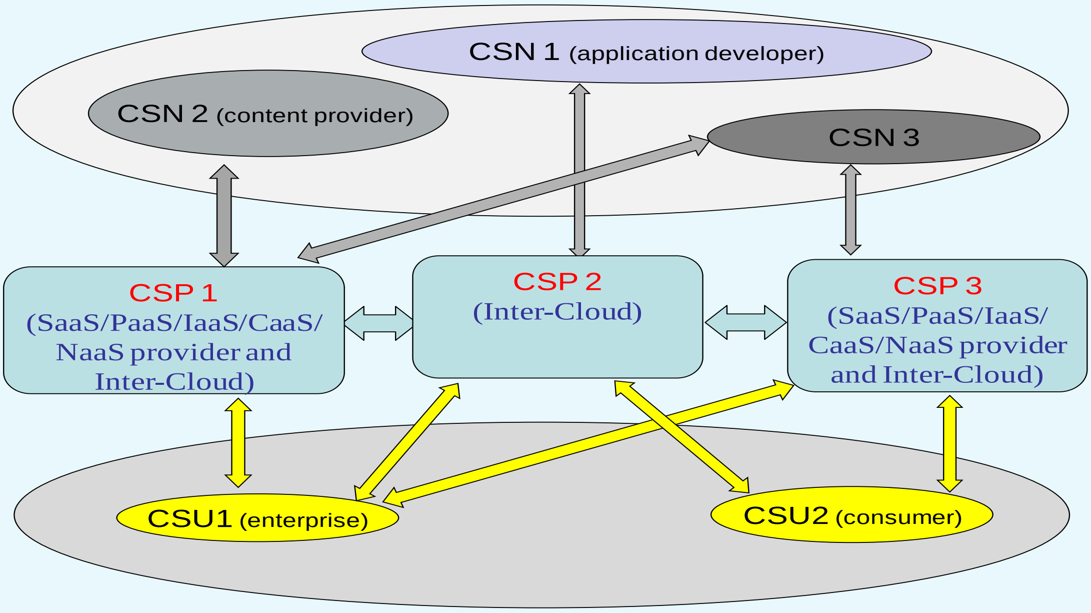
5.3 Cloud Computing Eco-systems

A cloud computing business ecosystem (cloud ecosystem) is a business ecosystem of interacting organizations and individuals - the actors of the cloud ecosystem - providing and consuming cloud services. The following actors are identified in a cloud ecosystem:

- Cloud service users (CSU): A person or organization that consumes delivered cloud services;
- Cloud service providers (CSP): An organization that provides and maintains cloud services to be delivered and consumed;
- Cloud service partners (CSN): A person or organization that provides support to the building of the service offer of a cloud service provider (e.g. service integration).

Figure 5-2 depicts the actors with some of their possible roles in a cloud ecosystem.

Figure 5-2: Actors with possible roles in a cloud ecosystem



5.4 Cloud Service categories

One of the key features of the cloud computing is “Anything as a Service” so called “XaaS”. There are plenty of candidate issues to be part of “as a Service”, but at this stage, ITU-T, especially SG13 is being discussed about following five services as key service categories.

- Cloud Software as a Service (SaaS): A category of cloud services where the capability provided to the cloud service user is to use the cloud service provider’s applications running on a cloud resources;

- Communications as a Service (CaaS): A category of cloud services where the capability provided to the cloud service user is to use real time communication and collaboration services. NOTE - Communication and collaboration services include voice over IP, instant messaging, video conferencing, for different user devices;

- Cloud Platform as a Service (PaaS): A category of cloud services where the capability provided to the cloud service user is to deploy user-created or acquired applications onto the cloud resources using platform tools supported by the cloud service provider;

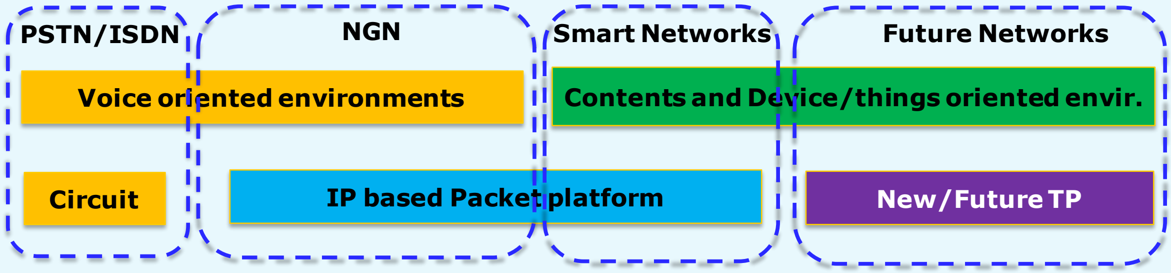
- Cloud Infrastructure as a Service (IaaS): A category of cloud services where the capability provided by the cloud service provider to the cloud service user is to provision processing, storage, intra-cloud network connectivity services (e.g. VLAN, firewall, load balancer, application acceleration), and other fundamental computing resources of the cloud resources where the cloud service user is able to deploy and run arbitrary application;

- Network as a Service (NaaS): A category of cloud services where the capability provided to the cloud service user is to use transport connectivity services and/or inter-cloud network connectivity services.

6 Future study direction of NGN

Considering this, ITU-T based on the NGN-GSI is continuing of their developments for the NGN will play a crucial role in a future environment as well. For this, as shown in Figure 6-1, ITU-T NGN GSI will continue their study covering various technical subjects. Recently one of the important subjects is providing smart and intelligent capabilities into the NGN as well as its beyond. This issue has been raised mainly from network providers considering the difficulties to provide better services to meet end user's requirements taking into account the status of network resources. Under this subject, NGN-GSI is now develop various solutions and mechanisms to resolve "smart usage of network resources" and "being pipeline of networks" This study will contribute in the development of called "Future Networks" which is being developed as a new paradigm of networks (for example, could be not use of IP).

Figure 6-1: Future study direction of NGN



Annex 9: ITU NGN standards

Internet Protocol Aspects

1 General aspect of IP based networks

Y.1001: IP framework – A framework for convergence of telecommunications network and IP network technologies

2 Architecture, access, network capabilities and resource management

Y.1221: Traffic control and congestion control in IP-based networks

Y.1222: Traffic control and congestion control in Ethernet-based networks

Y.1223: Interworking guidelines for transporting assured IP flows

Y.1231: IP Access Network Architecture

Y.1241: Support of IP-based services using IP transfer capabilities

Y.1242/G.769: Circuit multiplication equipment optimized for IP-based networks

Y.1251: General architectural model for interworking

Y.1261: Service requirements and architecture for voice services over Multi-Protocol Label Switching

Y.1271: Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks

Y.1281: Mobile IP services over MPLS

Y.1291: An architectural framework for support of Quality of Service in packet networks

Y.1292: Customizable IP networks (CIP): Framework for the requirements and capabilities related to the customization of IP service networks by customers

3 Transport

Y.1310: Transport of IP over ATM in public networks

Y.1311: Network-based VPNs – Generic architecture and service requirements

Y.1311.1: Network-based IP VPN over MPLS architecture

Y.1321/X.85: IP over SDH using LAPS

Y.1370/G.8110: MPLS layer network architecture

Y.1370.1/G.8110.1: Architecture of Transport MPLS (T-MPLS) layer network

Y.1371/G.8112: Interfaces for the Transport MPLS (T-MPLS) hierarchy

Y.1374/G.8151: Management aspects of the T-MPLS network element

Y.1381/G.8121: Characteristics of Transport MPLS equipment functional blocks

Y.1382/G.8131: Linear protection switching for transport MPLS (T-MPLS) networks

4 Interworking

Y.1401: Principles of interworking

Y.1402/X.371: General arrangements for interworking between Public Data Networks and the Internet

Y.1411: ATM-MPLS network interworking – Cell mode user plane interworking

Y.1412: ATM-MPLS network interworking – Frame mode user plane interworking

Y.1413: TDM-MPLS network interworking – User plane interworking

Y.1414: Voice services – MPLS network interworking

Y.1452: Voice trunking over IP networks

Y.1453: TDM-IP interworking – User plane interworking

Y.1454: Tandem free operation (TFO) – IP network interworking – User plane interworking

5 QoS and Network Performance

Y.1501/G.820/I.351: Relationships among ISDN, IP-based network and physical layer performance Recommendations

Y.1530: Call processing performance for voice service in hybrid IP networks

Y.1531: SIP-based call processing performance

Y.1540: Internet protocol data communication service – IP packet transfer and availability performance parameters

Y.1541: Network performance objectives for IP-based services

Y.1542: Framework for achieving end-to-end IP performance objectives

Y.1543: Measurements in IP networks for inter-domain performance assessment

Y.1544: Multicast IP performance parameters

Y.1560: Parameters for TCP connection performance in the presence of middleboxes

Y.1561: Performance and availability parameters for MPLS networks

6 Operation, administration and maintenance

Y.1704/G.7713: Distributed call and connection management (DCM)

Y.1704.1/G.7713.1: Distributed Call and Connection Management (DCM) based on PNNI

Y.1704.2/G.7713.2: Distributed Call and Connection Management: Signalling mechanism using GMPLS RSVP-TE

Y.1704.3/G.7713.3: Distributed Call and Connection Management: Signalling mechanism using GMPLS CR-LDP

Y.1710: Requirements for Operation & Maintenance functionality in MPLS networks

Y.1711: Operation & Maintenance mechanism for MPLS networks

Y.1712: OAM functionality for ATM-MPLS interworking

Y.1713: Misbranching detection for MPLS networks

Y.1714: MPLS management and OAM framework

Y.1720: Protection switching for MPLS networks

7 IPTV

Y.1901: Requirements for the support of IPTV services

Y.1902: Framework for multicast-based IPTV content delivery

Y.1910: IPTV functional architecture

Y.1911: IPTV services and nomadism: Scenarios and functional architecture for unicast delivery

Y.1991: Terms and definitions for IPTV

Next Generation Networks

1 Frameworks and functional architecture models

Y.2001: General overview of NGN

Y.2002: Overview of ubiquitous networking and of its support in NGN

Y.2006: Description of capability set 1 of NGN release 1

Y.2007: NGN capability set 2

Y.2011: General principles and general reference model for Next Generation Networks

Y.2012: Functional requirements and architecture of next generation networks

Y.2013: Converged services framework functional requirements and architecture

Y.2014: Network attachment control functions in next generation networks

Y.2015: General requirements for ID/locator separation in NGN

Y.2016: Functional requirements and architecture of the NGN for applications and services using tag-based identification

Y.2017: Multicast functions in next generation networks

Y.2018: Mobility management and control framework and architecture within the NGN transport stratum

Y.2019: Content delivery functional architecture in NGN

Y.2020: Open service environment functional architecture for next generation networks

Y.2021: IMS for Next Generation Networks

Y.2022: Functional architecture for the support of host-based ID/locator separation in NGN

Y.2023: Functional requirements and architecture for the NGN for multimedia communication centre serviceY.2031: PSTN/ISDN emulation architecture

Y.2051: General overview of IPv6-based NGN

Y.2052: Framework of multi-homing in IPv6-based NGN

Y.2053: Functional requirements for IPv6 migration in NGN

Y.2054: Framework to support signalling for IPv6-based NGN

Y.2055: Framework of object mapping using IPv6 in next generation networks

Y.2056: Framework of vertical multi-homing in IPv6-based NGN

Y.2057: Framework of node identifier and routing locator separation in IPv6-based next generation networks

Y.2058: Roadmap for IPv6 migration from the perspective of the operators of next generation networks

Y.2062: Framework of object-to-object communication for ubiquitous networking in NGN

Y.2091: Terms and definitions for next generation networks

2 Quality of Service and performance

Y.2111: Resource and admission control functions in next generation networks

Y.2112: A QoS control architecture for Ethernet-based IP access networks

Y.2113: Ethernet QoS control for next generation networks

Y.2121: Requirements for the support of flow-state-aware transport technology in NGN

Y.2122: Flow aggregate information exchange functions in NGN

Y.2171: Admission control priority levels in Next Generation Networks

Y.2172: Service restoration priority levels in Next Generation Networks

Y.2173: Management of performance measurement for NGN

Y.2174: Distributed RACF architecture for MPLS networks

Y.2175: Centralized RACF architecture for MPLS core networks

3 Service aspects

Y.2201: Requirements and capabilities for ITU-T NGN

Y.2205: Next Generation Networks – Emergency telecommunications – Technical considerations

Y.2206: Requirements for distributed service networking capabilities

Y.2211: IMS-based real-time conversational multimedia services over NGN

Y.2212: Requirements of managed delivery services

Y.2213: NGN service requirements and capabilities for network aspects of applications and services using tag-based identification

Y.2214: Service requirements and functional models for customized multimedia ring services

Y.2215: Requirements and framework for the support of VPN services in NGN, including the mobile environment

Y.2216: NGN capability requirements to support the multimedia communication centre service

Y.2221: Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment

Y.2232: NGN convergence service model and scenario using web services

Y.2233: Requirements and framework allowing accounting and charging capabilities in NGN

Y.2234: Open service environment capabilities for NGN

Y.2235: Converged web-browsing service scenarios in NGN

Y.2236: Framework for NGN support of multicast-based services

Y.2237: Functional model and service scenarios for QoS-enabled mobile VoIP service

Y.2240: Requirements and capabilities for next generation network service integration and delivery environment

Y.2251: Multi-connection requirements

Y.2261: PSTN/ISDN evolution to NGN

Y.2262: PSTN/ISDN emulation and simulation

Y.2271: Call server-based PSTN/ISDN emulation

Y.2281: Framework of networked vehicle services and applications using NGN

Y.2291: Architectural overview of next generation home networks

4 Network Management

Y.2401/M.3060: Principles for the Management of Next Generation Networks

5 Security

Y.2701: Security requirements for NGN release 1

Y.2702: Authentication and authorization requirements for NGN release 1

Y.2703: The application of AAA service in NGN

Y.2704: Security mechanisms and procedures for NGN

Y.2705: Minimum Security Requirements for Interconnection of Emergency Telecommunication Services (ETS)

Y.2720: NGN identity management framework

Y.2721: NGN identity management requirements and use cases

Y.2722: NGN identity management mechanisms

Y.2740: Security requirements for mobile remote financial transactions in next generation networks

Y.2741: Architecture of secure mobile financial transactions in next generation networks

Y.2760: Mobility security framework in NGN

Y.2770: Requirements for Deep Packet Inspection in Next Generation Networks

6 Generalized Mobility

Y.2801/Q.1706: Mobility management requirements for NGN

Y.2802/Q.1762: Fixed-mobile convergence general requirements

Y.2803/Q.1763: FMC service using legacy PSTN or ISDN as the fixed access network for mobile network users

Y.2804/Q.1707: Generic framework of mobility management for next generation networks

Y.2805/Q.1708: Framework of location management for NGN

Y.2806/Q.1709: Framework of handover control for NGN

Y.2807: MPLS-based mobility capabilities in NGN

Y.2808: Fixed mobile convergence with a common IMS session control domain

Y.2809: Framework of mobility management in the service stratum for next generation networks

Y.2810: Mobility management framework for IP multicast communications in NGN

7 Supplements and Handbooks on NGN (use cases)

Y Suppl. 1: ITU-T Y.2000 series – Supplement on NGN release 1 scope

Y Suppl. 2: ITU-T Y.2012 – Supplement on session/border control (S/BC) functions

Y Suppl. 3: ITU-T Y.2000 series – Supplement on service scenarios for convergence services in a multiple network and application service provider environment

Y Suppl. 4: ITU-T Y.1300 series – Supplement on transport requirements for T-MPLS OAM and considerations for the application of IETF MPLS technology

Y Suppl. 5: ITU-T Y.1900-series – Supplement on IPTV service use cases

Y Suppl.6: ITU-T Y.2000-series – Supplement on the use of DSL-based systems in next generation networks

Y Suppl.7: ITU-T Y.2000-series – Supplement on NGN release 2 scope

Y Suppl. 8: ITU-T Y.2000-series – Supplement on a survey of global ICT forums and consortia

Y Suppl. 9: ITU-T Y.2000-series – Supplement on multi-connection scenarios

Y Suppl. 10: ITU-T Y.2000-series – Supplement on distributed service network (DSN) use cases

Y Suppl. 12: ITU-T Y.2720 – Supplement on NGN identity management mechanisms

Y Suppl. 13: ITU-T Y.2000-series - Scenarios for the evolution of NGN network capabilities to include information storage, processing and delivery

Y Suppl. 14: ITU-T Y.2000-series – Supplementary service scenarios for fixed-mobile convergence

Y Suppl. 15: ITU-T Y.2000-series – Profile-based application adaptation service using NGN

Y Suppl. 16: ITU-T Y.1900-series – Guidelines on deployment of IP multicast for IPTV content deliveryHandbook: Converging networks (2010)

NGN Related ITU-T SG11 Approved Q-Series Supplements

1 Network signalling and control functional architecture

Q.3030: Signalling architecture for the NGN service control plane

Q.3040: Signalling architecture for IPTV control plane

2 Bearer Control Signalling

Q.3150/Y.1416: Use of virtual trunks for ATM/MPLS client/server control plane interworking

Q.3151/Y.1417: ATM and frame relay/MPLS control plane interworking: Client-server

3 Signalling and control requirements and protocols to support attachment in NGN environments

Q.3201: EAP-based security signalling protocol architecture for network attachment

Q.3202.1: Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN

Q.3203: Signalling requirements and architecture of network attachment control functions to support IP mobility

Q.3220: Architectural framework for NACF signalling interface Recommendations

Q.3221: Requirements and protocol at the interface between the service control entity and the transport location management physical entity (S-TC1 interface)

Q.3222: Requirements and protocol at the interface between transport location management physical entities (Ng interface)

Q.3223: Requirements and protocol for the interface between a transport location management physical entity and a policy decision physical entity (Ru Interface)

4 Resource control protocols

Q.3300: Architectural framework for the Q.33xx series of Recommendations

Q.3301.1: Resource control protocol No. 1, version 2 – Protocol at the Rs interface between service control entities and the policy decision physical entity

Q.3302.1: Resource control protocol No. 2 (rcp2) – Protocol at the Rp interface between transport resource control physical entities

Q.3303.0: Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Overview

Q.3303.1: Resource control protocol No. 3 – Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and a Policy Enforcement Physical Entity (PE-PE): COPS alternative

Q.3303.2: Resource control protocol No. 3 – Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and a Policy Enforcement Physical Entity (PE-PE) (Rw interface): H.248 alternative

Q.3303.3: Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Diameter

Q.3304.1: Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity (TRC-PE) and a transport physical entity (T-PE): COPS alternative

Q.3304.2: Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity (TRC-PE) and a transport physical entity (T-PE): SNMP alternative

Q.3305.1: Resource control protocol No. 5 (rcp5) – Protocol at the interface between transport resource control physical entity and policy decision physical entity (Rt interface): Diameter-based

Q.3306.1: Resource control protocol No. 6 (rcp6) - Protocol at the interface between intra-domain policy decision physical entities (PD-PE) (Rd interface)

Q.3307.1: Resource control protocol No.7 - Protocol at the interface between inter-domain policy decision physical entities (Ri interface)

Q.3308.1: Resource control protocol 8 (rcp8) Protocol at the interface between Resource Admission Control Physical Entity (RAC-PE) and CPN Gateway Policy Enforcement Physical Entities (CGPE-PE) (Rh interface): COPS alternative

Q.3309: QoS coordination protocol

Q.3311: Enhancement of resource and admission control protocols to use pre-congestion notification

Q.3312: Use of the access node control protocol on the Rp interface

Q.3313: Signalling protocols and procedures relating to flow state aware QoS control in a bounded subnetwork of a next generation network

5 Service and session control protocols

Q.3401: NGN NNI signalling profile (protocol set 1)

Q.3402: NGN UNI signalling profile (Protocol set 1)

6 Service and session control protocols – supplementary services

Q.3610: Signalling requirements and protocol profiles for customized ring-back tone service

Q.3611: Signalling requirements and protocol profiles for NGN customized ringing tone service

Q.3612: Signalling requirements and protocol profiles for IP Centrex service

7 Testing for NGN networks

Q.3900: Methods of testing and model network architecture for NGN technical means testing as applied to public telecommunication networks

Q.3901: Testing topology for networks and services based on NGN technical means

Q.3902: Operational parameters to be monitored when implementing NGN technical means in public telecommunication networks

Q.3903: Formalized presentation of testing results

Q.3904: Testing principles for IMS model networks, and identification of relevant conformance, interoperability and functionality tests

Q.3906.1: Test scenarios and catalogue for testing fixed-broadband access networks using a model network - Part I

Q.3909: The framework and overview of NGN conformance and interoperability testing

Q.3910: Parameters for monitoring NGN protocols

Q.3911: Parameters for monitoring voice services in NGN

Q.3925: The types of traffic flows which should be generated for voice, data and video on the Model network for testing QoS parameters

Q.3931.1: Performance benchmark for the PSTN/ISDN emulation subsystem of an IP multimedia system - Part 1: Core concepts

Q.3931.2: Performance benchmark for the PSTN/ISDN emulation subsystem of an IP multimedia system - Part 2: Subsystem configurations and benchmarks

Q.3941.1: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 1: Test suite structure and test purposes for SIP-ISDN

Q.3941.2: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 2: Abstract test suite and partial protocol implementation extra information for testing proforma specification for SIP-ISDN

Q.3941.3: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 3: Test suite structure and test purposes for SIP-SIP

Q.3941.4: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 4: Abstract test suite and partial protocol implementation extra information for testing proforma specification for SIP-SIP

Q.3945: Test specifications for next generation network services on model networks - Test set 1

Q.3948: Service testing framework for VoIP at the user-to-network interface of next generation networks

Q.3950: Testing and model network architecture for tag-based identification systems and functions

8 Supplements and Handbooks

Q Suppl. 51: Signalling requirements for IP-QoS

Q Suppl. 52: NNI mobility management requirements for systems beyond IMT-2000

Q Suppl. 53: Signalling requirements to support the International Emergency Preference Scheme (IEPS)

Q Suppl. 54: Signalling requirements at the interface between SUP-FE and I/S-CSC-FE

Q Suppl. 55: Signalling requirements at the interface between AS-FE and S-CSC-FE

Q Suppl. 56: Organization of NGN service user data

Q Suppl. 57: Signalling requirements to support the emergency telecommunications service (ETS) in IP networks

Q Suppl. 58: Organization of NGN transport user data

Q Suppl. 59: Signalling flows and parameter mapping for resource control

Q Suppl. 60: Supplement to Recommendations ITU-T Q.3610 and ITU-T Q.3611 - Service flows for customized multimedia ring-back tone (CRBT) and customized multimedia ringing tone (CRT) services

Q Suppl. 61: Evaluation of signalling protocols to support ITU-T Y.2171 admission control priority levels

Q Suppl. 62: Overview of the work of standards development organizations and other organizations on emergency telecommunications service

Handbook on deployment of packet based networks (2009)

Handbook on Testing (2011)

IMT related Recommendations

Q.1711: Network functional model for IMT

Q.1721: Information flows for IMT capability set 1

Q.1731: Radio-technology independent requirements for IMT layer 2 radio interface

Q.1741.1: IMT references to release 1999 of GSM evolved UMTS core network with UTRAN access network

Q.1741.2: IMT references to release 4 of GSM evolved UMTS core network with UTRAN access network

Q.1741.3: IMT references to release 5 of GSM evolved UMTS core network

Q.1741.4: IMT references to release 6 of GSM evolved UMTS core network

Q.1741.5: IMT references to Release 7 of GSM-evolved UMTS core network

Q.1741.6: IMT references to Release 8 of GSM-evolved UMTS core network

Q.1741.7: IMT references to Release 9 of GSM-evolved UMTS core network

Q.1742.1: IMT references to ANSI-41 evolved core network with cdma2000 access network

Q.1742.2: IMT references (approved as of 11 July 2002) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.3: IMT references (approved as of 30 June 2003) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.4: IMT references (approved as of 30 June 2004) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.5: IMT references (approved as of 31 December 2005) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.6: IMT references (approved as of 31 December 2006) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.7: IMT references (approved as of 30 June 2008) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.8: IMT references (approved as of 31 January 2010) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.9: IMT references (approved as of 31 December 2010) to ANSI-41 evolved core network with cdma2000 access network

Q.1751: Internetwork signalling requirements for IMT capability set 1

Q.1761: Principles and requirements for convergence of fixed and existing IMT systems

Operation & Tariff related Recommendations

D.271: Charging and accounting principles for NGN

E.370: Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks

E.4110: Framework for operations requirements of next generation networks and services

NGN Management related Recommendations

M.3210.1: TMN management services for IMT-2000 security management

M.3340: Framework for NGN service fulfilment and assurance management across the business to business and customer to business interfaces

M.3341: Requirements for QoS/SLA management over the TMN X-interface for IP-based services

M.3342: Guidelines for the definition of SLA representation templates

M.3343: Requirements and analysis for NGN trouble administration across B2B and C2B interfaces

M.3344: Requirements and analysis for NGN appointment management across the business-to-business and customer-to-business interfaces

M.3345: Principles for self-service management

M.3347: Requirements for the NGN service activation of NMS-EMS interface

M.3348: Requirements of the NMS-EMS management interface for NGN service platforms

M.3350: TMN service management requirements for information interchange across the TMN X-interface to support provisioning of Emergency Telecommunication Service (ETS)

M.3361: Requirements for business-to-government management interfaces - B2G interfaces – Introduction

M.3400: TMN management functions

M.3410: Guidelines and requirements for security management systems to support telecommunications management

NGN Related ITU-R Recommendations

Recommendation S.1806: Availability objectives for hypothetical reference digital paths in the fixed-satellite service operating below 15 GHz

Report ITU-R M.2176-1: Vision and requirements for the satellite radio interface(s) of IMT-Advanced

Preliminary draft new Recommendation ITU-R S.1897: Cross-layer based QoS provisioning in IP-based hybrid satellite-terrestrial networks

Recommendation F.1094-2: Maximum allowable error performance and availability degradations to digital fixed wireless systems arising from radio interference from emissions and radiations from other sources

Recommendation F.1704: Characteristics of multipoint-to-multipoint fixed wireless systems with mesh network topology operating in frequency bands above about 17 GHz

Recommendation F.1763: Radio interface standards for broadband wireless access systems in the fixed service operating below 66 GHz

Recommendation M.819: International Mobile Telecommunications-2000 (IMT-2000) for developing countries

Recommendation M.1457: Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2000 (IMT-2000)

Recommendation M.2012: Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications Advanced (IMT-Advanced)

国际电信联盟（ITU）
电信发展局（BDT）
主任办公室
Place des Nations
CH-1211 Geneva 20 – Switzerland
电子邮件： bdtdirector@itu.int
电话： +41 22 730 5035/5435
传真： +41 22 730 5484

副主任
兼行政和运营协调部负责人（DDR）
电子邮件： bdtdeputydir@itu.int
电话： +41 22 730 5784
传真： +41 22 730 5484

基础设施、环境建设和
电子应用部（IEE）
电子邮件： bdtiee@itu.int
电话： +41 22 730 5421
传真： +41 22 730 5484

创新和
合作伙伴部（IP）
电子邮件： bdtip@itu.int
电话： +41 22 730 5900
传真： +41 22 730 5484

项目支持和
知识管理部（PKM）
电子邮件： bdtpkm@itu.int
电话： +41 22 730 5447
传真： +41 22 730 5484

非洲

埃塞俄比亚

国际电联
区域代表处
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

电子邮件： itu-addis@itu.int
电话： +251 11 551 4977
电话： +251 11 551 4855
电话： +251 11 551 8328
传真： +251 11 551 7299

喀麦隆

国际电联
地区办事处
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroon

电子邮件： itu-yaounde@itu.int
电话： + 237 22 22 9292
电话： + 237 22 22 9291
传真： + 237 22 22 9297

塞内加尔

国际电联
地区办事处
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

电子邮件： itu-dakar@itu.int
电话： +221 33 849 7720
传真： +221 33 822 8013

津巴布韦

国际电联
地区办事处
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

电子邮件： itu-harare@itu.int
电话： +263 4 77 5939
电话： +263 4 77 5941
传真： +263 4 77 1257

美洲

巴西

国际电联
区域代表处
SAUS Quadra 06, Bloco “E”
11° andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

电子邮件： itubrasilia@itu.int
电话： +55 61 2312 2730-1
电话： +55 61 2312 2733-5
传真： +55 61 2312 2738

巴巴多斯

国际电联
地区办事处
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

电子邮件： itubridgetown@itu.int
电话： +1 246 431 0343/4
传真： +1 246 437 7403

智利

国际电联
地区办事处
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

电子邮件： itusantiago@itu.int
电话： +56 2 632 6134/6147
传真： +56 2 632 6154

洪都拉斯

国际电联
地区办事处
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

电子邮件： itutegucigalpa@itu.int
电话： +504 22 201 074
传真： +504 22 201 075

阿拉伯国家

埃及

国际电联
区域代表处
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

电子邮件： itucairo@itu.int
电话： +202 3537 1777
传真： +202 3537 1888

亚太

泰国

国际电联
区域代表处
Thailand Post Training Center, 5th
floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

邮寄地址：
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

电子邮件： itubangkok@itu.int
电话： +66 2 575 0055
传真： +66 2 575 3507

印度尼西亚

国际电联
地区办事处
Sapta Pesona Building, 13th floor
JI. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

邮寄地址：
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

电子邮件： itujakarta@itu.int
电话： +62 21 381 3572
电话： +62 21 380 2322
电话： +62 21 380 2324
传真： +62 21 389 05521

独联体国家

俄罗斯联邦

国际电联
地区办事处
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

邮寄地址：
P.O. Box 25 – Moscow 105120
Russian Federation

电子邮件： itumoskow@itu.int
电话： +7 495 926 6070
传真： +7 495 926 6073

欧洲

瑞士

国际电联
电信发展局（BDT）欧洲处（EUR）
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
电子邮件： eurregion@itu.int
电话： +41 22 730 5111

国际电信联盟
电信发展局
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

瑞士印刷
2014年，日内瓦

01/2014