



下一代网络 移动IPv6技术

蒋亮 郭健 等编著



NGN
Mobile IPv6



机械工业出版社
CHINA MACHINE PRESS



下一代网络移动 IPv6 技术

蒋 亮 郭 健 等编著



机械工业出版社

2004年6月, IETF正式发布了移动IPv6的国际标准RFC3775《Mobility Support in IPv6》。本书以RFC3775为基础, 首先介绍下一代网络和IPv6协议的基本内容, 作为移动IPv6整体介绍的基础; 然后, 介绍移动IPv6的基本内容, 包括与移动IPv4的比较、对IPv6协议的修改和扩展、消息类型、节点要求与操作等; 随后, 进一步探讨了移动IPv6的相关问题, 如快速切换、分级移动IPv6、网络管理问题、防火墙问题等。

本书内容详实准确而新颖, 既可以作为高校电子信息、通信工程、计算机网络相关课程的参考用书, 也可以作为网络设备研制人员、网络管理人员、网络设计与开发人员、网络应用研发人员、运营商和服务提供商等相关人员的移动IPv6学习与培训用书, 同时对于关心网络技术发展的热心读者也会有所助益。

图书在版编目(CIP)数据

下一代网络移动IPv6技术/蒋亮, 郭健等编著. —北京: 机械工业出版社, 2005.6

ISBN 7-111-17165-9

I. 下... II. ①蒋...②郭... III. 计算机网络-传输控制协议 IV. TN915.04

中国版本图书馆CIP数据核字(2005)第090187号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)

责任编辑: 张俊红 版式设计: 张世琴 责任校对: 吴美英

封面设计: 陈 沛 责任印制: 石 冉

三河市宏达印刷有限公司印刷·新华书店北京发行所发行

2005年8月第1版·第1次印刷

787mm×1092mm 1/16·17.5印张·429千字

0001—4000册

定价: 29.00元

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

本社购书热线电话(010) 68326294

封面无防伪标均为盗版

前 言

移动 IP 技术,是指移动用户在跨网络随意移动和漫游中,使用基于 TCP/IP 的网络时,不需要修改计算机原有的 IP 地址,仍能继续享有原网络中一切权限和服务的技术。其主要目标是无论连接在本地链路还是移动到外地网络,移动节点总是通过本地地址寻址。移动 IP 在网络层加入了新的特性,在改变网络连接点时,运行在节点上的应用程序不用修改或重新配置仍然可用。这些特性使得移动节点总是通过本地地址进行通信。这种机制对于 IP 层以上的协议层是完全透明的。同时,移动 IP 技术既适用于跨越同类媒体的移动,也适用于跨越不同种类媒体的移动。

目前移动 IP 技术分为移动 IPv4 和移动 IPv6。作为 IPv6 内在组成部分的移动 IPv6 技术,对于下一代网络,尤其对于下一代移动通信网络,有着极其重要的影响。

下一代网络(NGN)是目前网络发展的趋势,是今后通信业务和互联网业务的核心,其核心承载网将使用 IPv6 技术。而作为下一代网络的重要组成部分之一,下一代移动通信网络将会在传统的语音业务的基础上,给用户带来更加丰富的移动数据业务应用。

移动数据业务是在移动通信平台上开展的多种数据业务,如视频点播、移动定位、远程监控、企业网络访问、多媒体短信、互联网访问、WAP 和电子商务等。移动数据业务是移动通信和数据通信相结合的产物,具有业务个性化和多样化特色,其作为移动业务收入的重要增长点之一,正在成为移动运营商和各类增值业务提供商的关注焦点。移动数据业务的发展有许多内在的要求,例如对移动网络接入速度和移动互联网安全性等方面的要求,目前 3G、802.11、802.20、WiMax、WAPI、WAP 2.0、WTLS 等技术的研究和发展正是为了解决这些要求。而对于移动数据业务来说,其最重要的要求就是对移动性的支持。

然而,目前的移动数据业务并不支持 IP 的移动性。同时,由于目前移动网络与固定网络的分割,实际应用中也尚未提供真正的移动应用。实际用户在网络中变更位置时需要不断自动或被动地更改地址,并相应地不断重新进行连接。此外,由于 IPv4 地址的匮乏,目前移动网络运营商一般都使用私有地址与 NAT-PT 技术相结合的地址解决方案,人为地在网络中引入大量的 NAT-PT 设

备,这使得大量的互联网业务,尤其是端到端业务的开展变得非常困难。这一系列难题,都需要移动 IPv6 来解决。

首先,以 IPv6 大量的地址资源和其他先进的性能做基础,使得现网上的端到 NAT 的通信模式向 P2P 模式转变, P2P 最终将成为基本的通信模式。其次,用户可以通过全球范围的下一代移动网络和有限范围的 WLAN、蓝牙等来接入下一代网络,通过移动 IPv6 技术,用户从某种接入技术覆盖的区域移动到另一种接入技术覆盖的区域时仍然能够保持不间断的连接,从而实现真正意义上的全 IP 网络。通过移动 IPv6,可以将各种接入方式,将宽带、移动互联网和现有的无线系统等都无缝地集成到 IP 层中,通过一种网络基础设施提供所有通信和信息服务,既是下一代网络发展的方向,也是移动 IPv6 的核心优势。

为此,笔者结合科研与实践的经验,根据目前下一代网络、IPv6 技术(尤其是移动 IPv6 技术)的最新成果和发展趋势,编写了本书。本书内容主要分为 3 部分。第 1 部分为第 1 章和第 2 章,主要介绍了下一代网络的基本情况、下一代网络与 IPv6 和移动 IPv6 的关系,以及 IPv6 的基础知识;第 2 部分为第 3 章~第 10 章,其中比较了移动 IPv4 和移动 IPv6,并就移动 IPv6 协议的相关内容作了详细的介绍和说明,包括移动 IPv6 的消息/选项格式、移动 IPv6 对 IPv6 邻居发现机制的修改、移动 IPv6 对各类网络节点的要求及移动 IPv6 中对端节点、家乡代理和移动节点各自所进行的操作,并介绍了移动 IPv6 中的相关安全问题等;第 3 部分为第 11 章~第 15 章,主要介绍了与移动 IPv6 相关的其他问题,包括快速切换、分级移动 IPv6、移动 IPv6 网络管理、移动 IPv6 与防火墙,以及移动 IPv6 访问控制等问题。

本书主要由蒋亮和郭健编写。同时,参与本书编写工作的人员还有丘子隽、陈志强、郑涛、陈铮、蒋建新等,在此向他们表示感谢。

希望通过本书的介绍,读者能够对移动 IPv6 有一个全面且比较深入的了解。同时,由于笔者能力和知识范围有限,且 IPv6 和移动 IPv6 的发展非常迅速,书中疏漏之处在所难免,欢迎广大读者和同行批评指正。

作者
2005 年 4 月

目 录

前言

第1章 下一代网络与移动 IPv6 1

1.1 下一代网络..... 1

1.1.1 当今网络面临的问题 1

1.1.2 下一代网络概述 2

1.1.3 下一代网络研究进展情况 3

1.1.4 下一代网络特征 5

1.1.5 下一代网络构成 7

1.1.6 下一代网络关键技术 9

1.1.7 下一代网络相关协议 10

1.1.8 下一代网络业务 22

1.2 下一代网络与 IPv6 24

1.2.1 下一代网络业务承载网 24

1.2.2 在下一代网络中引入 IPv6 25

1.3 移动 IPv6 在下一代网络中的应用..... 25

第2章 IPv6 协议结构、编址与其他相关内容..... 28

2.1 IPv6 发展现状 28

- 2.1.1 IPv6 的历史 28

2.1.2 IPv6 发展现状 29

2.1.3 IPv6 标准化现状 30

2.2 IPv6 特点 31

2.2.1 新的协议报头格式 32

2.2.2 改进的扩展和选项支持 32

2.2.3 巨大的地址空间 32

2.2.4 全新的地址管理方案 32

2.2.5 有效的、分级的寻址和路由结构 32

2.2.6 内置的安全特性 33

2.2.7 即插即用功能 33

2.2.8 对移动性的支持 33

2.2.9 对 QoS 的更好支持 33

2.2.10 新的邻接点交互处理协议 34

2.3 IPv6 基本报头 34

2.3.1 IPv4 报头格式 34

2.3.2 IPv6 报头格式 35

2.3.3 IPv6 和 IPv4 报头格式比较 38

2.4 IPv6 扩展报头 39

2.4.1 扩展报头的顺序 40

2.4.2 逐跳选项报头 41

2.4.3 目的地选项报头 42

2.4.4 路由报头 42

2.4.5 片段报头 43

2.5 编址方案 43

2.5.1 IPv4 编址 43

2.5.2 IPv6 编址 44

2.6 IPv4 向 IPv6 过渡技术 48

2.6.1 双协议栈技术 48

2.6.2 隧道技术 49

2.6.3 NAT-PT 51

2.7 IPv6 路由协议 52

2.7.1 RIPng 53

2.7.2 OSPFv3 54

2.7.3 BGP-4+ 54

2.7.4 IS-ISv6 55

第3章 移动 IPv4 与移动 IPv6 56

3.1 移动 IP 技术产生的背景 56

3.2 移动 IPv4 概述 57

3.2.1 移动 IPv4 的 4 种实体 57

3.2.2 移动节点的两种地址 57

3.2.3 移动节点的 3 种功能 58

3.3 移动 IPv6 概述 59

3.3.1 移动 IPv6 组成	59	5.1.1 概述	84
3.3.2 移动 IPv6 基本操作	60	5.1.2 邻居发现选项	85
3.3.3 新的 IPv6 协议	61	5.1.3 邻居发现报文	88
3.3.4 新的 IPv6 目的地的选项	62	5.1.4 邻居发现基本过程	92
3.3.5 新的 IPv6 ICMP 消息	62	5.2 移动 IPv6 对 IPv6 邻居发现机制	
3.3.6 总体数据结构	62	的修改	94
3.3.7 站点本地编址	62	5.2.1 更改路由器通告报文格式	94
3.4 移动 IPv4 与移动 IPv6 比较	62	5.2.2 更改前缀信息选项格式	94
第 4 章 移动 IPv6 消息/选项格式	64	5.2.3 新的通告时间间隔选项	95
4.1 移动报头	64	5.2.4 新的家乡代理信息选项	96
4.1.1 格式	64	5.2.5 对发送路由器通告的更改	96
4.1.2 绑定更新请求消息	65	第 6 章 移动 IPv6 节点类型的要求	98
4.1.3 家乡测试初始消息	66	6.1 所有 IPv6 节点	98
4.1.4 转交测试初始消息	66	6.2 支持路由优化的 IPv6 节点	98
4.1.5 家乡测试消息	67	6.3 所有 IPv6 路由器	99
4.1.6 转交测试消息	67	6.4 IPv6 家乡代理	99
4.1.7 绑定更新消息	68	6.5 IPv6 移动节点	100
4.1.8 绑定确认消息	69	第 7 章 移动 IPv6 对端节点操作	101
4.1.9 绑定错误消息	70	7.1 总体数据结构	101
4.2 移动选项	71	7.2 移动报头处理	101
4.2.1 格式	71	7.3 数据包处理	102
4.2.2 Pad1	72	7.3.1 接收具有家乡地址选项的	
4.2.3 PadN	72	数据包	102
4.2.4 绑定更新建议选项	72	7.3.2 发送数据包至移动节点	102
4.2.5 备用转交地址选项	73	7.3.3 发送绑定错误消息	103
4.2.6 随机数索引选项	73	7.3.4 接收 ICMP 错误消息	103
4.2.7 绑定授权数据	73	7.4 返回路由可达过程	104
4.3 家乡地址选项	74	7.4.1 接收家乡测试初始消息	105
4.4 第 2 类路由报头	75	7.4.2 接收转交测试初始消息	105
4.5 新的 ICMPv6 消息	76	7.4.3 发送家乡测试消息	105
4.5.1 ICMPv6 概述	76	7.4.4 发送转交测试消息	105
4.5.2 ICMP 家乡代理地址发现请求		7.5 绑定维护	106
消息	81	7.5.1 对端节点和移动节点之间绑定	
4.5.3 ICMP 家乡代理地址发现应答		维护消息交互	106
消息	81	7.5.2 对端节点绑定维护操作	107
4.5.4 ICMP 移动前缀请求消息格式	82	7.6 缓存替换策略	110
4.5.5 ICMP 移动前缀通告消息格式	82	第 8 章 移动 IPv6 家乡代理操作	111
第 5 章 对 IPv6 邻居发现机制的		8.1 总体数据结构	111
修改	84		
5.1 移动 IPv6 邻居发现机制	84		

8.2 处理移动报头	111	9.7.1 发送绑定更新至家乡代理	150
8.3 绑定维护	112	9.7.2 对端注册	151
8.3.1 家乡代理和移动节点之间绑定 维护消息交互	112	9.7.3 接收绑定确认	153
8.3.2 家乡代理绑定维护操作	113	9.7.4 接收绑定刷新请求	154
8.4 数据包处理	116	9.8 重传和速率限制	154
8.4.1 截取至移动节点的数据包	116	第 10 章 移动 IPv6 的安全性	155
8.4.2 处理截取的数据包	117	10.1 移动 IPv6 安全概述	155
8.4.3 组播成员控制	118	10.1.1 对于家乡代理的绑定更新	155
8.4.4 有状态地址自动配置	118	10.1.2 对于对端节点的绑定更新	156
8.4.5 处理反向隧道数据包	119	10.1.3 动态家乡代理地址发现	161
8.4.6 保护返回路由可达过程	119	10.1.4 移动前缀发现	161
8.5 动态家乡代理地址发现	119	10.1.5 净荷数据包	161
8.6 发送前缀信息至移动节点	121	10.2 移动 IPv6 安全考虑	161
8.6.1 家乡网络前缀列表	121	10.2.1 移动 IPv6 面临的安全威胁	161
8.6.2 安排前缀分发	121	10.2.2 移动 IPv6 安全特性	163
8.6.3 发送通告	122	10.2.3 至家乡代理的绑定更新	163
8.6.4 更改的前缀的生存周期	123	10.2.4 至对端节点的绑定更新	165
第 9 章 移动 IPv6 移动节点操作	124	10.2.5 动态家乡代理地址发现	168
9.1 总体数据结构	124	10.2.6 移动前缀发现	168
9.2 处理移动包头	125	10.2.7 经由家乡代理的隧道	168
9.3 数据包处理	125	10.2.8 家乡地址选项	169
9.3.1 离开家乡时发送数据包	125	10.2.9 第 2 类路由报头	169
9.3.2 与外向 IPSec 处理互操作	130	10.3 IPSec 概述	169
9.3.3 离开家乡时接收数据包	131	10.3.1 IPSec 体系结构	170
9.3.4 路由组播数据包	132	10.3.2 安全联盟	171
9.3.5 接收 ICMP 错误消息	133	10.3.3 IPSec 实现模式	171
9.3.6 接收绑定错误消息	133	10.3.4 IPSec 的安全协议	172
9.4 家乡代理和前缀管理	134	10.3.5 IPSec 实施	174
9.4.1 动态家乡代理地址发现	134	10.3.6 IPSec 协议处理	175
9.4.2 移动前缀发现	136	第 11 章 移动 IPv6 快速切换	177
9.5 移动	138	11.1 简介	177
9.5.1 移动检测	138	11.2 协议概述	179
9.5.2 从家乡链路移动至外地链路	140	11.2.1 切换时延分析	179
9.5.3 移动至新的外地链路	145	11.2.2 移动 IPv6 快速切换操作	180
9.5.4 返回家乡	147	11.2.3 网络发起切换操作	181
9.6 返回路由可达过程	148	11.3 协议细节	182
9.6.1 发送测试初始消息	148	11.4 其他相关问题	184
9.6.2 接收测试消息	149	11.4.1 切换能力交换	184
9.6.3 保护返回路由可达数据包	149	11.4.2 确定新转交地址	185
9.7 处理绑定	150	11.4.3 数据包丢失	185

11.4.4 重复地址检测处理	185	12.6 移动节点选择移动锚点时的 注意事项	216
11.4.5 快速或错误移动	186	12.6.1 在分布式移动锚点环境中的移动 锚点选择	216
11.5 消息格式	186	12.6.2 扁平移动管理架构中的 MAP 选择	217
11.5.1 新的邻居发现消息	187	12.7 移动锚点失败检测及恢复	217
11.5.2 内部接入路由器消息	190	12.8 分级移动 IPv6 安全考虑	218
11.5.3 新的移动报头消息	192	12.9 区域移动 IPv6	218
11.5.4 新的选项	195	12.10 小结	219
11.6 相关安全问题	197	第 13 章 移动 IPv6 网络管理	220
11.6.1 场景一: 不安全的快速绑定 更新	198	13.1 网络管理概述	220
11.6.2 场景二: 安全快速绑定更新, 恶意或疏忽地重定向	198	13.1.1 网络管理的功能	220
11.6.3 场景三: 从新接入路由器链路 发送快速绑定更新	198	13.1.2 简单网络管理协议(SNMP)	220
11.7 802.11 网络中的移动 IPv6 快速切换	198	13.2 SNMP 的管理信息库 (MIB)	223
11.7.1 简介	198	13.3 IPv6 网络管理技术	224
11.7.2 802.11 协议概述	199	13.3.1 IPv6 网络管理技术概述	224
11.7.3 移动 IPv6 在 802.11 网络上的 部署	201	13.3.2 IPv6 相关 MIB	225
11.7.4 802.11 网络中的移动 IPv6 快速 切换的实现	202	13.4 移动 IPv6 网络管理技术	228
11.7.5 信号扫描和新接入 路由器发现	204	13.4.1 概述	228
11.7.6 相关应用场景	205	13.4.2 移动 IPv6 监测和控制要求	228
11.7.7 其他相关问题	205	13.4.3 移动 IPv6 MIB 设计	229
第 12 章 分级移动 IPv6	207	13.4.4 移动 IPv6 MIB	229
12.1 简介	207	13.4.5 安全考虑	236
12.2 对标准移动 IPv6 的扩展	210	第 14 章 移动 IPv6 与防火墙问题	237
12.3 协议操作	211	14.1 概述	237
12.3.1 移动节点操作	211	14.2 背景信息	237
12.3.2 移动锚点操作	212	14.2.1 有状态检查数据包过滤器 概述	237
12.3.3 家乡代理操作	213	14.2.2 与 3G 网络数据包过滤相关的 移动 IPv6 问题	238
12.3.4 对端节点操作	213	14.3 场景分析	238
12.3.5 移动锚点域中的本地移动管理 优化	213	14.3.1 外部节点为移动节点时的 场景	238
12.3.6 位置保密	213	14.3.2 内部节点为移动节点时的 场景	240
12.4 移动锚点发现	214	14.3.3 返回路由可达测试	241
12.4.1 动态移动锚点发现	214	14.3.4 更改转交地址相关的问题	242
12.4.2 移动节点操作	215		
12.5 更新先前的移动锚点	215		

14.3.5 更改防火墙	242	15.3.3 访问令牌生成的流程	252
14.4 小结	242	15.3.4 标记数据报的流程	253
第 15 章 移动 IPv6 访问控制问题	243	15.4 DHCPv6 协议	253
15.1 概述	243	15.4.1 DHCPv6 协议的概述	253
15.1.1 对移动节点实现访问控制的 目标	243	15.4.2 DHCPv6 消息类型	254
15.1.2 实现对移动节点的访问控制 所面临的一些问题	243	15.4.3 DHCPv6 消息格式	255
15.1.3 移动 IPv6 对访问控制系统的 要求	244	15.4.4 DHCPv6 的选项	256
15.2 移动 IPv6 的访问控制体系 结构	244	15.4.5 DHCPv6 消息的合法性	257
15.2.1 移动节点的自动配置	247	15.4.6 DHCPv6 服务器查找	259
15.2.2 初始会话	247	15.4.7 DHCPv6 客户端发起的配置信息 交换	259
15.2.3 访问令牌的生成	248	附录	260
15.2.4 标记数据报	248	附录 A IPv6 RFC 索引	260
15.2.5 数据报过滤	248	附录 B 移动 IPv6 相关草案	264
15.2.6 对于切换的支持	249	附录 C 移动 IPv6 协议常量和协议 配置变量	265
15.3 访问控制的操作流程	250	附录 D IPv6/移动 IPv6 相关 网址	265
15.3.1 初始会话的流程	250	参考文献	268
15.3.2 数据报过滤的流程	252		

第 1 章 下一代网络与移动 IPv6

1.1 下一代网络

1.1.1 当今网络面临的问题

当前, Internet 的发展趋势已经向我们预示, 21 世纪人们将在网上开创新的工作方式、管理方式、商贸方式、金融方式、思想交流方式、文化教育方式、医疗保健方式以及消费与生活方式, 人们将通过网络获得各种各样的、满足社会各界的应用, 以满足生产和生活等多方面的需求。

与此同时, 随着网络的发展, 其革命性的变革可能不仅仅在于我们目前所熟悉的电脑和移动电话, 而在于使得其他各种设备, 从汽车的仪表盘、建筑物的空调系统到信息家电, 从音响设备、电冰箱到调光开关和电咖啡壶, 诸如此类, 即日常生产生活中遇到的所有设备都真正具有通信能力, 并使其真正成为网络组成的一部分。各种设备之间的信息交互与控制、设备与人之间的信息交互与控制将带来革命性的网络新应用。配合网格技术, 诸如生物信息传递、异地备份、Web 缓存、多播馈送、新闻馈送、信息批处理、数据库同步、多媒体电子信箱、数据库挖掘等应用都将获得长足的发展, 并且将在生命科学、工程设计、生产制造和金融服务等方面都将发挥前所未有的作用。

但是, 当前网络越来越不能满足网络技术与应用发展的需求!

首先, 当前网络依然存在带宽瓶颈。为了支持更多更有价值的宽带服务与应用, 需要消除带宽瓶颈, 使网络的每一个环节都不会产生堵塞。然而, 随着越来越多的设备接入网络, 越来越多的信息将通过网络来传输, 尤其是机器设备与机器设备之间的信息交互, 将成为未来网络流量的重要组成部分。这一切对于网络带宽提出了更高的要求, 使得网络带宽成为目前阻碍网络发展的重要因素之一。

其次, 当前网络面临地址瓶颈。正如我们上面所提到的, 将来网上更多的用户是机器设备, 而不是人。因此, 网络的发展就必须消灭地址壁垒, 让数十上百亿的人和设备能够连接网络, 同时恢复因地址有限而失去的端到端连接功能。惟有这样, 将来才能开展普遍的机对机应用, 并且把服务方式由提取 (Pull) 演进为推送 (Push)。但是, 目前主要使用的 IPv4 技术在很大程度上难以满足网络发展的需求。尽管 IPv4 有 32 位地址空间, 可以容纳 4294967296 个地址, 但是 IP 地址分配原则造成 IP 地址的大量浪费, 这使得 IPv4 技术面临着地址枯竭的困境。因此, 目前在网络上不得不引入大量的 NAT (Network Address Translation, 网络地址转换) 设备和技术, 进行网络地址的转换。但是 NAT 不仅造成网络性能上的瓶颈, 而且有些应用是无法穿透 NAT 的, 例如经过加密的数据包以及一些不使用 UDP 和 TCP 协议头的数据包等, 这严重制约了网络的进一步发展。

再次, 当前网络不能完全满足网络应用对服务质量 (QoS) 的要求。QoS 是指用来表示

电信服务性能之属性的任何组合,其决定用户对业务满意程度的业务性能的综合效果。为了使其具有价值,这些属性必须是可提供的、可管理的、可验证和计费的。QoS 包括两层含义:业务性能和业务差别。体现业务性能的关键参数有带宽、时延、抖动和丢包率,对业务性能的保证应该是端到端的、连续的、可预测的、大于或等于预定值的。业务差别意味着为不同的业务应用提供不同的性能保证,对于一些紧急的或关键性业务,即使在高负载的情况下,也要保证其 QoS 不受影响,尤其是对于语音业务,IP 网络要能够提供与传统的 PSTN 相当的电信级 QoS。然而,目前互联网尽力而为(Best Effort)的服务并不能提供服务质量保证,这导致了运营商 IP 业务与流量一直在高速增长,但其收入却增长缓慢。因此,QoS 对各种网络应用的真正商用有着极其重要的影响,进而对网络盈利和运营商的生存与发展十分关键。只有使网络应用的服务质量得到保证,令用户满意,服务提供商和网络运营商才能进行收费或推出相应的盈利模式,才能为网络发展提供推动力。

最后,应用的发展对网络安全性提出了越来越高的要求。网络安全与信息安全是休戚相关的,网络不安全,就谈不上信息安全。在新的经济体系下,网络安全和信息安全保障能力将是国家的综合国力、经济竞争实力和生存能力的重要组成部分。为了适应国家安全、经济建设、科研生产和保护公众利益的需要,必须不断提高网络的安全性。

1.1.2 下一代网络概述

针对当今网络所面临的各种问题,同时为了满足数据业务急剧增长、用户对多媒体业务和移动性的强烈需求,1996 年,美国政府与相关大学分别牵头提出了下一代 Internet 行动计划(NGI)和 Internet2。与此同时,各国政府部门、行业团体、标准化组织等机构发起组织了多个下一代网络(NGN)行动计划,如 IETF 的下一代 IP、3GPP 与 UMTS 论坛的下一代移动通信、加拿大的 CANET3、欧盟的 NGN 行动计划等。1997 年,朗讯公司的 BELL 实验室提出了软交换的概念,声称吸收了现有 PSTN 和 Internet 的优点,是一个相对完美的网络。从此,各个主流的设备厂商纷纷推出自己的 NGN 解决方案,如朗讯的 7RE、西门子的 Surpass、阿尔卡特的 2IP、华为的 iNET 等等。

自 1999 年起,NGN 成为与“3G”和“宽带”齐名的通信行业关注焦点,成为大家讨论最多的一个话题。NGN 是“下一代网络(Next Generation Network)”或“新一代网络(New Generation Network)”的英文缩写,它包含了非常广泛的内容:

- 1) 从计算机网络看,NGN 是以高带宽和 IPv6 为基础的 NGI(下一代互联网)。
- 2) 从传输网络看,NGN 是以 ASON(自动交换光网络)和 GFP(通用帧协议)为基础的新一代传输网络。

- 3) 从移动通信网络看,NGN 是以 WCDMA 和 cdma2000 为代表的 3G。

- 4) 从电话网看,NGN 是指以分组交换和软交换为基础的电话网络。

一些行业组织和标准化机构也启动了本领域的 NGN 技术研究,如 IETF 的下一代 IP 网,ITU、3GPP 与 3GPP2 的下一代移动通信网,ITU 的 NGN Project 2004。因此,对于 NGN,业界也一直存在诸多不同的解释。在 2004 年年初国际电联 NGN 会议上,经过激烈的辩论,NGN 的定义终于有了定论:NGN 是一个分组网络,它提供包括电信业务在内的多种业务,能够利用多种带宽和具有 QoS 能力的传送技术,实现业务功能与底层传送技术的分离;它为用户提供了对不同业务提供商网络的自由接入,并支持通用移动性,实现用户对

业务使用的一致性和统一性。

NGN 是电信史上的一个里程碑, 标志着新一代电信网络时代的到来。下一代网络是一个建立在 IP 技术基础上的新型公共电信网络, 能够容纳各种形式的信息, 在统一的管理平台下, 实现音频、视频、数据信号的传输和管理, 提供各种宽带应用和传统电信业务, 是一个真正实现宽带窄带一体化、有线无线一体化、有源无源一体化、传输接入一体化的综合业务网络。Internet 是下一代网络的主体, IP 技术是实现计算机互联网、传统的公共服务电话网 (PSTN) 和有线电视网三网融合的关键技术。随着 Internet 技术的发展, 最终将实现计算机互联网、电话网和有线电视网实现三网融合。下一代网络除了能向用户提供语音、高速数据、视频信息业务外, 还能向用户方便地提供视频会议、电话会议功能, 而且能像广播网一样, 向有特定要求的用户提供统一的消息、时事新闻等。

1.1.3 下一代网络研究进展情况

NGN 的研究在世界各国非常活跃, NGN 的主要研究领域包括 NGN 的通用框架模型、NGN 的功能体系结构模型、端到端业务质量、业务平台 (APIs)、网络管理与安全、通用移动性、网络控制体系及协议、业务能力和业务体系结构、NGN 中业务和网间的互操作性和编号、命名及编址等。

截至 2004 年 7 月的 SG13 末期会议, ITU SG13 专题组已经完成的课题包括: NGN 概述、NGN 总体原则和通用参考模型、NGN 总体要求、NGN 功能要求及其体系架构、NGN 融合技术方案、NGN 移动性管理要求及其体系架构、NGN 用户可管理的 IP 网络、NGN 的网络融合、PSTN 向 NGN 的演进、NGN QoS 总体要求和网络性能要求、NGN 端到端要求及其体系架构、集中控制资源的端到端 QoS 架构、基于以太网接入的 QoS 架构、基于 IP 接入网的 QoS 架构、异构网络的网络性能, 其形成的 ITU 标准草案 (Draft) 如表 1-1 所示。

表 1-1 ITU SG13 NGN 标准草案

草 案 名 称	草 案 内 容
Y. NGN-Overview	NGN 功能和特性概述
Y. GRM-NGN	NGN 通用参考模型
Y. NGN-FRM	NGN 功能要求及体系架构
Y. NGN-SRQ	NGN 业务要求
Y. NGN-MOB	NGN 移动性管理要求与架构
Y. NGN-MAN	可管理的 IP 网络架构
Y. NGN-MIG	NGN 演进
Y. NGN-CON	NGN 融合
Y. e2eqos	演进至 NGN 的 IP 网络端到端 QoS 架构
Y. 123.qos	基于以太网的 IP 接入网络 QoS 架构
Y. NGN-TERM	NGN 术语

其中, Y. NGN-Overview 是一个描述 NGN 功能和特点的综述性新建议草案。草案给出了 NGN 的定义和基本特点, 描述了 NGN 的功能和预计达到的目标, 并重点描述了 NGN 的研究领域。草案主要对 NGN 的形态和特征进行了描述。NGN 的基本特征包括: 基于分组

技术传输；在承载层面、会话/呼叫、应用/业务之间实现控制功能的分离；业务提供和传送层面分离，基于开放接口提供业务；支持多种类型的业务（实时、流媒体、非实时、多媒体等）；宽带能力，具有端到端的服务质量；通过开放接口实现和传统网络的互通；具有移动性；用户可以无限制地接入不同的业务提供商；多样化的标识机制；对于用户来说，同样的业务具有统一的业务特征；在固网与移动网络之间实现融合；上层业务功能与低层传输技术独立；支持多种接入技术；适应各种调整要求，例如紧急通信、安全与隐私保护等。

Y.GRM-NGN 建议草案在 Y.100、Y.110 和 X.200 等建议的基础上提出了 NGN 的基本原则和参考模型，它将 NGN 垂直划分为业务层和传输层。业务层包括各种会话型和非会话型业务，如语音、数据、视频等多媒体业务；传输层用于通信实体间的信息传输，实现对 NGN 业务的支持。同时，该建议草案又将业务层和传输层水平划分为用户平面、控制平面和管理平面。在 NGN 的参考模型中还提出了广播与电信的融合、多媒体业务支持、用户和终端的标识与定位、应急通信、与非 NGN 互通、安全以及 QoS 方面的基本要求。

Y.NGN-FRM 建议草案提出了 NGN 的功能框架模型，内容涉及 NGN 的参考模型、功能实体定义和功能参考点定义等多个方面。该建议草案以 Y.GRM-NGN 提出的参考模型为基础，细化定义了 NGN 业务层和传送层的一些功能实体，并将这些功能实体与用户平面、控制平面和管理平面相对应，如业务层的控制平面中有接入控制、定位、与分组互通、与 PSTN/ISDN 互通和媒体资源控制等功能实体；业务层管理平面中有代理、网络及网元管理、业务管理等功能实体；传送层的管理平面中有代理、网络及网元管理等功能实体。该建议草案还对业务体系提出了总体要求。

Y.NGN-SRQ 建议草案提出了 NGN 的业务总体技术要求和网络要求的框架，内容涉及 NGN 的通用要求、NGN 的业务要求（包括对数据平面、VPN、控制平面和管理平面的要求）和 NGN 的网络要求（包括对数据平面、操作维护、QoS、流量管理、安全和认证、移动性、互通、计费、网络演进、控制平面等的要求）。

Y.NGN-MOB 建议草案描述了 NGN 中的移动性管理要求及其体系结构，将 NGN 的移动性分为网间移动、网内移动和接入网内移动 3 种情况，并从通用、用户和网络 3 个方面提出了对移动性管理的要求，提出了 NGN 移动性管理的功能体系结构。

Y.NGN-MAN 主要关注从用户角度出发的可管理 IP 网的业务定义、业务需求、参考模型和功能要求。可管理 IP 网的业务是向用户提供网络资源控制和管理。可管理 IP 网应具有用户分组及业务分集、信息接入控制和安全、移动控制和管理、带宽分配和 SLA（Service Level Agreement，服务水平协议）、端到端 QoS 配置和优先权配置等多种能力。

Y.NGN-CON 建议草案初步分析了 NGN 和 Pre-NGN 的网络，计划分析多种融合示例，如接入部分融合、核心部分融合、终端部分融合、移动性部分融合、业务部分融合和内容部分融合；并对应 NGN 的业务和传输分离的特点，将其分为业务和网络两个管理域。

为了顺应电信网络的发展趋势，在分组化的 IP 平台上提供丰富的、多样化的业务，满足市场对全球性 NGN 标准的迫切需求，ITU 及时整合了各方面资源，并在 2004 年 6 月的 13 组会议上组建了新的 NGN 专题组（FGNGN）。FGNGN 主要是在 SG13 体系结构和业务需求等工作的基础上，重点对 NGN 领域的关键技术进行研究和标准制定，在体系结构方面、需求和移动方面、服务质量和性能方面、演进和互通方面、多业务提供商针对 NGN 业务的接口方面继续完善和深入。FGNGN 的主要研究领域包括业务需求、功能体系架构和移

动性、IPQoS、控制和信令能力、网络安全、网络演进以及 IP 承载能力要求。

1.1.4 下一代网络特征

下一代网络是三网融合的产物，是一个高度融合的网络，主要体现在技术融合、网络融合、业务融合、产业融合 4 个方面。从技术融合来讲，在下一代网络中，电信技术、数据通信技术、移动通信技术、有线电视技术及计算机技术相互融合，出现了大量的混合各种技术的产品，如路由器支持语音、交换机提供分组接口等。从网络融合来讲，在下一代网络中，原本相互独立的固定网络与移动网络、语音网络和数据网络开始融合，逐步形成一个统一的网络。从业务融合来讲，未来的电信经营格局绝对不是数据和语音的地位之争，而更多的是数据、语音两种业务的融合和促进，同时，图像业务也会成为未来电信业务的有机组成部分，从而形成语音、数据、图像 3 种在传统意义上完全不同的业务模式的全面融合；大量语音、数据、图像融合的业务，如 VOD、VoIP、IP 智能网、Web 呼叫中心等不断广泛应用，网络融合使得网络业务表现更为丰富。从产业融合来讲，下一代网络中的网络融合和业务融合必然导致传统的电信业、移动通信业、有线电视业、数据通信业和信息服务业的融合，电信业运营商、设备制造厂商、服务和应用提供商、数据通信厂商、计算机厂商以及传统的属于广电领域的电影电视部门等，都将开始相互收购与融合。

因此，下一代网络具有如下基本特征：

- 1) 分组传送；
- 2) 控制功能从承载、呼叫/会话、应用/业务中分离；
- 3) 业务提供与网络分离，提供开放接口；
- 4) 利用各基本的业务组成模块，提供广泛的业务和应用（包括实时、流媒体、非实时和多媒体业务）；
- 5) 具有端到端 QoS 和透明的传输能力；
- 6) 通过开放接口与传统网络互通；
- 7) 具有通用移动性；
- 8) 允许用户自由地接入不同业务提供商；
- 9) 支持多样标识体系，并能将其解析为 IP 地址以用于 IP 网络路由；
- 10) 同一业务具有统一的业务特性；
- 11) 融合固定与移动业务；
- 12) 业务功能独立于底层传送技术；
- 13) 适应所有管理要求，如应急通信、安全性和私密性等要求。

下一代网络是基于统一协议的、基于分组的网络，采用开放的网络构架体系。传统的有线和移动电话有各自独立的交换和传输网络，而移动电话的接入网络更是复杂，它们有着不同的空中传输标准，这不仅增加了成本，也给使用者、管理者带来不便。在 NGN 中将实现固定网和移动网的融合，固网通信和移动通信仅仅是接入方法不同。IP 网采用开放的体系结构、统一的标准协议，任何接入网络只要是采用 IP 都可以和它互通互连。接入网可以是固定电话网、移动电话网、有线电视网、ADSL、LAN 接入等。统一的 IP 核心网用一套统一的设备代替了原来各系统的独立设备，可以大大降低开发和运营成本。

下一代网络将传统交换机的功能模块分离成为独立的网络部件，各个部件可以按相应的

功能划分,各自独立发展;部件间的协议接口基于相应的标准;部件化使得原有的封闭的电信网络逐步走向开放,运营商可以根据业务的需要自由组合各部分的功能产品来组建网络。部件间协议接口的标准化可以实现各种异构网的互通。

下一代网络的核心承载网采用高速包交换网络,可实现电信网、计算机网和有线电视网三网融合,同时支持语音、数据、视频等业务。同时,下一代网络具有独立的网络控制层。网络控制层即软交换,采用独立开放的计算机平台,将呼叫控制从媒体网关中分离出来,通过软件实现基本呼叫控制功能,包括呼叫选路、管理控制和信令互通,使业务提供者可自由结合承载业务与控制协议,提供开放的业务应用编程接口,从而可使第三方快速、灵活、有效地实现业务提供。通过采用软交换技术,下一代网络将传统交换机的功能模块分离为独立网络部件,各部件按相应功能进行划分,独立发展。采用业务与呼叫控制分离、呼叫控制与承载分离技术,实现开放分布式网络结构,使业务独立于网络。通过开放式协议和接口,可灵活、快速地提供业务,个人用户可自己定义业务特征,而不必关心承载业务的网络形式和终端类型。从现有网络到 NGN 是一个渐进演化的过程,为了充分利用现有设备,以软交换为核心的重叠网策略是一种可行的过渡策略。

此外,下一代网络还实现了网络互通、网络设备网关化以及多样化接入方式。通过接入媒体网关、中继媒体网关和信令网关等网关,下一代网络可实现与 PSTN、PLMN、IN、Internet 等网络的互通,有效地继承原有网络的业务。同时,普通用户可通过智能分组语音终端、多媒体终端接入,通过接入媒体网关、综合接入设备(IAD)满足用户的语音、数据和视频业务的共存需求。

下一代网络是业务驱动的网络,其业务与呼叫控制分离、呼叫与承载分离。分离的目的是使业务真正独立于网络,灵活有效地实现业务的提供。用户可以自行配置和定义自己的业务特征,不必关心承载业务的网络形式以及终端类型,使得业务和应用的提供有较大的灵活性。

此外,下一代网络还具有开放、高效、多用户、多媒体、资源共享、低成本等特点。NGN 可以根据所处网络的不同及所提供功能的不同划分为几个模块,每个模块能独立发展,互不干涉,又能有机组合成一个整体。同时,这种开放性也表现为各运营商可根据自己的需求来选择市场上的优势产品,而不必担心不同设备间的互连互通。因为 NGN 能实现业务与呼叫控制的分离,为业务真正的从网络中独立出来,有效的缩短新业务的开发周期提供了良好的条件。而且,随着多网互通的实现,许多新兴业务也应运而生。NGN 综合了固定电话网、移动电话网和 IP 网络的优势,使得模拟用户、数字用户、移动用户、ADSL 用户、ISDN 用户、IP 窄带网络用户、IP 宽带网络用户,甚至是通过卫星接入的用户都能作为下一代网络中的一员相互通信。而语音、视频以及其他多媒体流在下一代网络中的实时传输成为了 NGN 的又一亮点。国际互联网为电信运营商的各种应用与服务提供了丰富的信息资源,由于采用了 IP 技术,NGN 的出现使得在呼叫过程中获取国际互联网的资源变得不再是难事。与此同时,采用了相对廉价的 IP 等网络作为中间传输的载体,因而 NGN 的通信费用将大大降低,这种优势尤其体现在长途和越洋电话上。

NGN 具有开发、布署和管理各种业务的能力。在 NGN 中,业务和网络的分离,这使得网络和业务可以独立发展与演进。与此同时,NGN 中的各功能实体分布在现有或新网络之中,从而使得 NGN 具有与现有网络互通的能力,这大大提高了网络演进的速度,并降低

了建设和推广成本。在 NGN 中, 将新增多种终端, 同时 NGN 也提供了对现有终端的完全支持。在 NGN 的初期阶段, 语音业务仍将是重要组成部分, 在全部信息流量和业务收入中占有举足轻重的作用。因此, NGN 提供对现有语音业务向 NGN 的过渡中关键技术的支持。在业务领域, NGN 支持通用移动性, 具有用户接入的无关性和业务使用的一致性特点。

总之, NGN 是一个高速宽带的网络, 是能综合实时业务、非实时业务、宽带业务、窄带业务的网络, 特别是能满足即将崛起的多媒体业务的发展需求。而下一代网络业务和终端趋于 IP 化。在下一代网络中, 将采用单一业务承载网和多个业务网与承载网相分离的体系结构, 多业务网能够共享一个业务承载网, 其中业务网采用业务与呼叫控制分离、呼叫控制与承载分离的体系结构。在网络安全方面, NGN 是安全和可信任的, 运营者保证网络是足够安全的, 用户可以放心地、可信任地使用网络资源。在服务质量方面, 下一代网络能保证提供电信级的服务质量, 保证现有的电信业务和今后可能产生的电信业务获得与传统电信业务相同的服务质量。此外, 下一代网络成功的尤为重要的一点就是必须具有良好的生态模型和价值链, 能使该价值链上的所有商家赢利。

1.1.5 下一代网络构成

传统网络通常都是分层描述的。在互联网上通常可以采用 5 层参考模型, 即互联网层、传输层、网络层、数据链路层和物理层。ISO 有 OSI 7 层参考模型, 即应用层、表示层、会话层、传输层、网络层、数据链路层和物理层。同理, 传输网络、电话网络都是分层描述和实现的。NGN 同样也需要分层描述和实现。

与传统网络不同的是, NGN 以在统一的网络架构上解决各种综合业务的灵活提供能力为出发点, 提供诸如业务逻辑、业务的接入与传送手段、业务的资源提供能力和业务的认管理等服务等。为此, 在 NGN 中, 以执行各种业务逻辑的软交换 (Softswitch) 设备为核心进行网络的构架建设。除此之外, 业务逻辑可在应用服务器上统一完成, 并可向用户提供开放的业务应用编程接口 (API)。因此, 在 NGN 中, 业务层面和业务控制层面从传统的网络中分离出来, 并已成为重要的一部分。而对于媒体流的传送和接入层面, NGN 将通过各种接入手段将接入的业务流集中到统一的分组网络平台上传送。另外重要的一点就是, NGN 强调网络的开放性。分组化的、开放的、分层的网络架构体系是下一代网络的显著特征。

因此, NGN 是一个综合性的大网, 其采用统一的 IP 核心网结构, 结合了现有的各种网络环境和周边的接入设备以及终端产品, 从功能的角度自上到下可以分为网络服务层 (Network Service Layer)、控制层 (Control Layer)、媒体传送层 (Media and Transport Layer) 和接入层 (Access Layer), 如图 1-1 所示。各层之间通过标准的开放接口互连。

其中, 网络服务层是一个开放的、综合的业务接入平台。在电信网络环境中, 它智能地接入各种业务, 提供各种增值服务; 而在多媒体网络环境中, 也需要相应的业务生成和维护环境。在 NGN 中, 业务层由一系列的业务应用服务器组成, 提供各种各样的业务控制逻辑, 完成增值业务处理; 同时提供开放的第三方接口, 易于引入新型业务。控制层主要指网络为完成端到端的数据传输进行的路由判决和数据转发的功能, 它是网络的交换核心, 决定用户收到的业务, 并能控制低层网络元素对业务流的处理, 目的是在传输层基础上构建端到端的通信过程。软交换 (Softswitch) 将是下一代网络的核心, 体现了 NGN 的网络融合思想。媒体传送层将信息格式转换成为能够在网络上传递的信息格式, 例如将语音信号分割成