网络与计算机安全丛书

可信的移动IPv6网络及协议

张玉军 著

科学出版社
www.sciencep.com

网络与计算机安全丛书

可信的移动 IPv6 网络及协议

张玉军 著

科学出版社

北京

内 容 简 介

移动 IPv6 协议是为下一代互联网提供的网络层宏移动解决方案，本书系统地论述了构建移动 IPv6 网络的各种关键技术，目的是为构建移动 IPv6 网络提供可信保障的基础理论和指导。本书的主要内容包括移动 IPv6 协议本身的安全技术、切换过程中的服务质量保障技术、切换过程中的安全保障技术、跨域移动的信任控制技术、协议的形式描述和验证技术、网络设备的可靠性测试技术、移动代理的容错和负载均衡技术等方面。全书图文并茂，在全面分析现有研究成果的基础上，阐述了作者自主创新的研究成果和结论。

本书可作为从事网络与通信专业研究的高等院校教师、研究生和高年级本科生的教学用书，也可作为从事移动 IPv6 网络建设、配置和管理工作的技术人员的参考书。

图书在版编目(CIP)数据

可信的移动 IPv6 网络及协议/张玉军著. —北京:科学出版社,2008
(网络与计算机安全丛书)
ISBN 978-7-03-020428-8

Ⅰ. 可… Ⅱ. 张… 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(2008)第 031304 号

责任编辑:任 静 王志欣/责任校对:邹慧卿
责任印制:刘士平/封面设计:耕者工作室

科学出版社出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

源海印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销

*

2008 年 3 月第 一 版 开本: B5 (720×1000)
2008 年 3 月第一次印刷 印张: 17 1/2
印数: 1—3 000 字数: 336 000

定价: 48.00 元

(如有印装质量问题，我社负责调换〈新欣〉)

序

随着互联网、电信网和广播电视网的不断融合，IP 将成为下一代网络的核心承载协议。未来的网络将会是有线网络和无线网络、固定网络和移动网络最终融合的全 IP 网络，能够提供语音、数据、视频等融合的高品质、多样化的服务。伴随着网络逐步呈现出的移动宽带化和宽带移动化的趋势，用户将可以享受到端到端的实时通信、全球范围的移动互联和超高速的宽带接入。

移动 IP 技术是 IP 网络中支持移动的核心技术，正受到越来越多的关注，将使得人们一直梦想的无处不在的移动互联成为可能。移动 IPv6 是为下一代网络设计的网络层宏移动解决方案，定义了节点移动过程中保持可寻址性的机制，在网络层解决与节点移动相关的移动检测、位置管理以及安全防护等诸多问题。未来网络上的许多新颖而精彩的服务将基于移动 IPv6 得以实现。

下一代网络将成为未来信息社会的重要基础设施，如何基于移动 IPv6 实现可信任的移动互联面临许多迫切需要解决的问题。例如，如何有效缩短切换延时，为用户提供有质量保证的实时服务；当用户在不同的管理域之间移动时，如何对移动用户进行有效的身份认证和接入控制；如何建立跨域移动过程中的服务质量保障和安全保障体系；如何提高移动互联网基础设施的可靠性等。这些问题都属于可信保障的范畴，也是本书关注的重点。

本书聚焦于构建可信移动 IPv6 网络的关键技术，突出特色在于学术性和前瞻性。作者多年来从事 IPv6 和移动 IPv6 相关技术的研究，在移动 IPv6 的可信与安全技术方面，先后承担了包括国家自然科学基金、国家 863 计划等多项研究课题，取得了一系列的研究成果，本书正是这些研究成果的系统总结。

与其他移动 IPv6 相关书籍显著不同的是，本书没有花费很大的篇幅介绍移动 IPv6 的基本原理和运行过程，而是集中论述了作者在移动 IPv6 切换过程中的服务质量保障技术、切换过程中的安全保障技术、跨域移动的信任控制技术、协议的形式描述和验证技术、网络设备的可靠性测试技术、移动代理的容错技术等方面的创新研究成果，包含了作者对移动 IPv6 的基本原理、运行机制和安全机制的全新看法和理解。因此，本书的出版有助于丰富这一领域的学术研究，进而对下一代网络的发展起到积极的促进作用。全书图文并茂，有一定的理论深度和实际应用价值，相信本书对从事 IP 网络工作的科研人员和工程技术人员具有较大的学术参考价值和指导作用。

中国工程院院士
中国科学院计算技术研究所所长
李国杰

前　言

对移动性的支持是未来网络的发展方向之一。IPv6（IP version 6）是下一代互联网协议，是构建下一代互联网的基础，协议中明确提出了对移动性的支持，移动 IPv6 协议是为下一代互联网提供的网络层移动解决方案。以移动 IPv6 技术为基础的移动互联网将为用户提供一个开放的网络环境，能够满足用户随时、随地接入网络的需求。移动 IPv6 协议提供了网络层的宏移动解决方案，适应大范围移动性的要求，能够解决全 IP 环境下全球范围的各种网络和接入技术之间的移动问题。

对于移动 IPv6 网络的实用化来说，切换过程中的服务质量保障和安全保障以及基础设施的可靠性等是必须要解决的问题，这些都属于可信网络的范畴。可信网络的概念已经出现多年，大体包括安全性、可生存性、可服务性、可控性、可管理性等基本特性，但目前还没有形成严格的定义，目前有许多人在从事可信网络方面的研究。作者无意在书中对可信网络的概念进行界定，之所以为本书如此命名，是因为书中涵盖的切换质量保障、切换安全保障、跨域信任控制、协议验证和测试、移动代理容错等各项技术都是构建可信移动 IPv6 网络的基础。

本书直接来源于相关协议标准的内容较少，多数内容来源于作者在移动 IPv6 网络可信技术方面的研究成果，目的是为构建移动 IPv6 网络提供可信保障的基础理论和技术。书中的部分研究成果已经通过相关学术刊物和会议正式发表，有些还在进一步的整理过程中。全书图文并茂，特别关注研究成果对网络实践的指导意义，基于研究成果的结论给出了许多关于网络建设、网络配置、网络管理的指导，如网络参数的配置、网络结构的设计、网络设备的部署等。

在本书付梓之际，特别感谢我的导师——中国科学院计算技术研究所的李忠诚研究员，书中包含的研究成果是作者在攻读硕士、博士学位期间，在他的指导、关心以及科研项目的支持下取得的。除作者本人之外，还有多人参与了本书相关内容的研究，他们的研究成果分别被选入了本书的各个章节中，分别是赵庆林（第 5 章）、田野（第 6 章）、肖文曙（第 5、7、10 章）、张瀚文（第 7、10 章）、张娇（第 7 章）等。除上述人员之外，胡琪、许智君、王淼、马超等人也参与了本书的讨论和编写工作，在此向他们表示衷心的感谢。

移动 IPv6 技术是目前的研究热点，国内外每年发表的关于这方面的学术论文达数百篇，在本书的撰写过程中参考了大量的学术论文，直接引用和标注的有

150 多篇，在此向相关作者表示感谢，同时向未被明确标注的论文作者表示歉意。

由于作者水平有限，书中难免存在不妥之处，恳请广大读者和同行批评指正。

目　录

第 1 章　下一代互联网协议 IPv6

IPv6 是下一代互联网协议，是构建下一代网络的基础。本章在分析 IPv4 协议地址危机的基础上介绍了 IPv6 协议的产生和发展历程，详细分析了 IPv6 的技术特征并与 IPv4 进行了比较，给出了 IPv4 向 IPv6 的演进技术。

第 1 节，介绍了 IP 协议的发展历程；第 2 节，分析了现行的 IPv4 协议面临的地址危机；第 3 节，给出了 IPv6 协议的产生和发展过程；第 4 节，从多个方面阐述了 IPv6 协议的技术特点；第 5 节，分析了 IPv4 向 IPv6 的演进技术；第 6 节，分析了推动 IPv6 网络实用化应该重点关注的几种技术。

1.1　IP 协议的发展历程

IP 协议是 TCP/IP 体系结构的最重要组成部分，在成为真正的标准之前，已经经历了将近 12 年的实际测试。早在 20 世纪 60 年代初期，科技工作者就考虑搭建计算机网络，实现科研组织之间的资源共享与协作。最早的计算机网络是 ARPAnet，它是美国国防部高级研究计划署（Advanced Research Projects Agency，ARPA）于 20 世纪 60 年代末期开始建设的，其目的是为了保障计算机系统在战争时也能够持续工作。在 ARPAnet 出现将近十年之后才出现了 ISO/OSI 参考模型，但 ARPAnet 中使用了与 OSI 模型的传输层和网络层相近的 TCP/IP 协议，TCP/IP 为今天互联网的发展和普及奠定了基础。

互联网的发展使得计算机系统和信息资源不仅能够服务于科学家等高层专业技术人员，同时也能为大众所用，进入商业运营领域。这一切正是因为互联网采取统一的 TCP/IP 协议作为共同的通信协议，将不同地域范围内的许多计算机连接在一起，使互联网具备良好的可扩展性。TCP/IP 采取分组交换的方式，向应用程序屏蔽了网络的硬件细节，同时避免了应用级主机互联的缺陷，使得主机互联和应用都得到了解脱。

TCP/IP 协议的核心是 IP 协议，IP 协议具有两个非常重要的特点：一是提供无连接、非可靠的数据传输机制；二是支持基于目的地址的路由机制。可以说 IP 协议的主要功能就是数据传输和路由选择，运行 IP 协议的网络层允许数据丢失或损坏，网络层可以丢弃数据并可随意选择传输路径，这使得网络层能够以极大的自由提供数据传输的能力。TCP/IP 所确立的层次思想为互联网的发展奠定了基础，可以说互联网的成功就是 TCP/IP 协议的成功。

1.2 IPv4 的危机

目前获得广泛应用的网络层协议是 Internet Protocol Version 4（IPv4）。在实际应用中，IPv4 获得了巨大的成功，但随着网络规模的扩大和网络用户的增加，IPv4 显现出一定程度的不足。

1.2.1 地址分配方式的缺陷

IPv4 的地址空间为 32 位，理论上能够支持 40 亿台终端设备的互联，表面上看不会存在地址不够用的问题。在 IPv4 的地址分配方面，32 位的地址被分为网络号（network number）和主机号（host number）两部分，网络号由专门的分配机构 IANA（Internet Assigned Numbers Authority）分配给申请单位，主机号由申请单位自主在单位内部进行分配。

IPv4 可分配的网络号根据其长度可分为不同的类型，包括 A、B、C 等类别，每个类型的主机号长度都是固定的，可以容纳固定数量的主机数。A 类地址共有 126 个，每个网络可容纳 1600 万台主机；B 类地址共有 16000 个，每个网络可容纳 65000 台主机；C 类地址共有 200 万个左右，每个网络可容纳 254 台主机。

按照这种分配方式，每个单位都将按照其最大可能的主机数申请地址类型，现有的 A、B、C 等类型划分过于粗糙，不可避免地浪费掉大量地址。A、B、C 等地址类型的划分以及许多其他的特殊规定和用途，使得实际可利用的 IPv4 地址数量大大降低，一般来说，整个 IPv4 地址空间的利用率只能达到 10%多一点。IPv4 的另一个设计缺陷是路由表中只能存储 A、B、C 等类型的网络号，每一个网络号都必须作为一条路由条目在路由表中单独存在，不能实现路由聚合，使得路由表随着网络规模的扩大而急剧膨胀，严重影响了路由效率。

地址空间的耗尽和路由表的急剧膨胀是 IPv4 的两个致命弱点，由此导致了无类别域间路由技术和网络地址翻译技术的提出和广泛应用，但这两种技术只能延缓问题的恶化进程，不能从根本上解决问题。

1.2.2 无类别域间路由技术

无类别域间路由技术（classless inter domain routing，CIDR）的基本原理是可以为拥有数千台主机的单位分配多个连续的 C 类地址，而不是分配一个 B 类地址，而且多个连续的 C 类地址可以重新聚合成一个网络号长度小于 C 类地址网络号长度、但大于 B 类地址网络号长度的路由条目。CIDR 技术通过连续 C 类地址的分配可以降低分配 B 类地址造成的浪费，通过路由聚合可以降低路由