国家科普知识重点图书

高新技术科普丛书

网络技术

宽带网·信息安全

侯自强 冯登国 编著

化学工业出版社

国家科普知识重点图书

高新技术科普丛书

网 络 技 术

宽带网·信息安全

侯自强　冯登国　编著

化 学 工 业 出 版 社
·北　京·

（京）新登字 039 号

图书在版编目（CIP）数据

网络技术/侯自强，冯登国编著 .—北京：化学工业出版社，2002.1
（高新技术科普丛书）
ISBN 7-5025-3552-7

Ⅰ.网… Ⅱ.①侯…②冯… Ⅲ.计算机网络-普及读物 Ⅳ.TP393-49

中国版本图书馆 CIP 数据核字（2001）第 087029 号

高新技术科普丛书
网 络 技 术
宽带网·信息安全
侯自强 冯登国 编著
总 策 划：陈逢阳 周伟斌
特邀策划：赵 萱
责任编辑：刘 哲 周国庆
责任校对：李 林
封面设计：田彦文
*
化学工业出版社出版发行
（北京市朝阳区惠新里 3 号 邮政编码 100029）
发行电话：（010）64918013
http://www.cip.com.cn
*
新华书店北京发行所经销
北京云浩印刷厂印刷
三河市东柳装订厂装订
开本 850×1168 毫米 1/32 印张 8 字数 208 千字
2002 年 1 月第 1 版 2002 年 1 月北京第 1 次印刷
ISBN 7-5025-3552-7/TP·302
定 价：18.00 元

《高新技术科普丛书》编委会

序

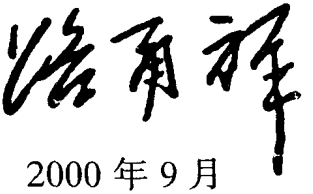
数万年来，人类一直在了解、开发、利用我们周围的自然界，同时不断地认识着自身，科学技术也从一开始就随着人类的生存需求而产生和发展着。人类发展史充分验证了邓小平“科学技术是第一生产力”的论断。科学技术的发展，促进了人类文明和社会的发展。

21世纪是信息时代，21世纪是生命科技的世纪，21世纪是新材料和先进制造技术迅速发展和广泛应用的时代，21世纪是高效、洁净和安全利用新能源的时代，21世纪是人类向空间、海洋、地球内部不断拓展的世纪，21世纪是自然科学发生重大变革、取得突破性进展的时代。科学技术的发展、新技术的不断涌现，必将引起新的产业革命，对我国这样的发展中国家来说，既是挑战，也是机遇，而能否抓住发展机遇，关键在于提高全民族的科学文化水平，造就一支具有科学精神、懂得科学方法、具有知识创新和技术创新能力的高素质劳动者队伍。所以，发展教育和普及科学知识、弘扬科学精神、提倡科学方法是我们应对世纪挑战的首要策略。为此，1999年8月，江总书记在视察中国科学院大连化学物理研究所时进一步强调了科普工作的重要性：“在加强科技进步和创新的同时，我们应该大力加强全社会的科学普及工作，努力提高全民族的科学文化素质。这项工作做好了，就可以为科技进步和创新提供广泛的群众基础。”

为了普及和推广高新技术，化学工业出版社组织几位两院院士和专家编写了《高新技术科普丛书》。本套丛书的特点是：介绍当今科学产业中的一些高新技术原理、特点、重要地位、应用及产业化的现状与发展前景；突出“新”，介绍的新技术、新理论和新方法不仅经实践证明是成熟、可靠的，而且是有应用前景的实用技

术；力求深入浅出，图文并茂，知识性、科学性与通俗性、可读性及趣味性的统一，并充分体现科学思想和科学精神对开拓创新的重要作用。

《高新技术科普丛书》涉及与我国经济和社会可持续发展密切相关的高新技术，第一批9个分册包括绿色化学与化工、基因工程技术、纳米技术、高效环境友好的发电方式——燃料电池、最新分离技术（如超临界流体萃取、吸附分离技术、膜技术）、化学激光、生物农药等。本套丛书以后还将陆续组织出版多种高新技术分册。相信该套科普丛书对宣传普及科技知识、科学方法和科学精神，正确地理解、掌握科学，提高全民族的素质将会起到积极的作用。



2000年9月

前　言

1994 年因特网开始商业化，把囚禁在潘朵拉盒子中的“小精灵”释放出来，迅速掀起了一场因特网风暴。因特网的快速普及，交互式媒体的出现，电子商务的兴起，正在改变着人们的生产、生活方式。网络经济的超常发展导致人们在谈论新经济，但是伴随网络经济发展出现了网络泡沫，随着网络泡沫的破裂，网络经济又陷入低谷，进入调整期。目前随着电子商务与传统产业的结合，宽带网络的发展以及信息网络安全技术的进展，网络经济正在逐步走上健康发展的轨道。今天回顾过去 7 年的发展历程，可以用一句话来概括——机遇和挑战并存。我国“十五”计划提出以信息化带动工业化，将使我国能够抓住机遇，迎接挑战，实现跨越式发展。

本书不打算全面讨论互联网技术和因特网及基于 Web 的新应用，因为已经有很多这方面的论述。本书重点讨论关系今后网络健康发展，为大家最关心的两个问题：宽带网络和信息网络安全技术。

第一部分是宽带网络。前 3 章介绍背景情况，第 4 章重点讨论构成宽带 IP 网的两项关键技术：高性能路由器和智能光网。第 5 章论述端到端的以太网将成为未来宽带 IP 网的主要结构。第 6 章讨论宽带 IP 接入网，指出五类线以太网符合我国国情，将得到迅速发展，为我国发展宽带接入网实现跨越式发展提供了历史机会。第 7 章宽带无线互联网，分析 3G 移动通信系统用做移动无线互联网的问题，提出新 3G 系统，指出这将有可能使我国在发展宽带无线互联网方面引领世界潮流。第 8 章讨论 QoS 协议和策略。第 4～8 章对宽带 IP 网的技术基础、结构和技术进展进行了较全面的介绍，第 9、10 两章则是介绍宽带 IP 网的应用。

第二部分讨论信息网络安全技术。第 11 章概述网络安全的重

要性和密码术的基本原理。第 12 章介绍对称密码术。第 13 章为非对称密码术。第 14 章介绍对于电子商务至关重要的数据完整性与数字签名。第 15 章为公开密钥基础设施技术。第 16 章介绍互联网网络层安全协议——IPSec 协议。第 17 章进一步介绍传输层安全协议——SSL 协议。第 18 章是应用层安全协议——S/MIME 和 SET 协议。

编著者

2001.10

内 容 提 要

本书是“高新技术科普丛书”之一。重点讨论关系今后网络健康发展的两问题：宽带网络和信息网络安全技术。

全书分为两大部分。第一部分宽带网络，讨论了高性能路由器和智能光网，端到端的以太网，宽带 IP 接入网，无线移动互联网，QoS 协议和策略等等。第二部分信息网络安全技术，介绍了对称密码术，非对称密码术，数据完整性和数字签名，公开密钥基础设施技术，以及 IPSec 协议、SSL 协议、S/MIME 和 SET 协议。

本书适合对网络技术感兴趣的读者。

目　　录

第1章 导 言

因特网的快速普及，交互式媒体的出现，电子商务的兴起正在改变着人们的生产、生活方式。

(1) 革命？演化？

因特网基于互联网即 IP 网技术，因特网的巨大成功对传统通信体制产生了强烈冲击，引发了一场通信体制革命。传统通信体制的特征是面向连接、时分复用、电路交换，IP 新体制是无连接、统计复用、分组交换。IP 网在网络层用 IP 协议互联，避免了异质网络在链路层互联的困难。IP 网的另一个最重要的特点是基础设施和应用是分离的，便于发展各种应用。随着因特网的快速普及，IP 数据流量开始超过话音，5 年前 IP 网开始取代 ATM，随后又取代 SDH 成为电信的基础网，进行了一场激烈的争斗。1998 年底国际电联咨询委员会 ITU-T 进行战略调整，将总体组 SG-13 组变成 IP 主导研究组，与 IETF 的标准研究机构合作制定标准，肯定了通信技术转向 IP 的发展趋势，进一步加速了电信业 IP 化的进程。目前太位路由器和密集波分复用技术结合可以提供太位 IP 骨干网。智能光网与万兆以太网 10GbE 结合，正在形成新一代的宽带 IP 骨干网和城域网。以太网正在成为新一代宽带接入网的标准。

传统电信运营商希望 IP 化是一个渐变的演化过程，而不是一场爆发式的革命，强调已经有的投资的保护和使用。新兴的竞争的运营商则认为这是一场改朝换代的技术体制革命，为革命者提供了机会。革命也好，演化也好，有一点是肯定的：不论是一个企业，还是一个国家，能否抓住这次机会，都是性命攸关的。为了应对面临的竞争局势，前不久中国电信决定在已有的 SDH 城域网之外，在裸光纤上另建宽带 IP 城域网，制定了雄心勃勃的发展以以太网接入网为主的宽带接入网计划。

（2）从封闭、垄断到竞争、开放

我国电信运营体制从封闭、垄断走向竞争所取得的成就如下，它使人们充分感受到互联网新技术和开放的新体制带来的影响。

① IP 电话打破了话音业务的垄断局面，使得长途电话价格大幅度下降。

② 中国网通等竞争的运营商采用 IP 新技术，发展 IP 新业务，进入电信领域，使得在电信骨干网的建设运营方面出现了竞争格局。2000 年网通建成 8000km40Gb/s 宽带 IP 骨干网。中国电信 CHINANET 结点连接速率提升到 2.5Gb/s，合计总带宽达 800Gb/s。

③ 国际物理出口权利被授给多家公司，竞争导致带宽迅速增加，成本大幅度下降。2000 年下半年从 1.23Gb/s 增加到 2.8Gb/s。

④ 带宽出租业务形成，用户可以租用裸光纤、波长、专线（622Gb/s、155Gb/s）以及 IP-VPN 等，价格成 10 倍下降。

⑤ 宽带 IP 城域网建设和运营出现竞争局面。

⑥ 宽带接入网建设和运营出现竞争局面，光缆到楼、五类线入户、以太网接入网正在成为主流。

⑦ 因特网数据中心 IDC 的建设和运营出现竞争局面。

⑧ 因特网业务价值链正在形成。

（3）机会均等？数字鸿沟？

因特网带来的最大变化，有人认为是改变了权利的分配方法。因特网提供了均等的机会，问题在于你是否能够抓住机会。对于任何能够把握住这一机会的人，互联网都会提供他强大的力量。互联网提供了无数个创业机会，为弱者——新兴小公司、发展中国家提供跨越式发展，迎头赶上的机会。人称 IP 是庶民的胜利。

问题是由于教育、社会和经济发展水平等原因的限制，落后地区、发展中国家往往不能抓住这一机会，其结果是先进的更先进，落后的更落后，这就导致出现“数字鸿沟”。

我国政府在制定“十五计划”时提出以信息化带动工业化，制定了雄心勃勃的发展计划，决心变“数字鸿沟”为“数字机遇”，

提出加强现代信息基础设施建设，抓紧发展和完善国家高速宽带传输网络，加快用户接入网建设，扩大利用互联网，促进电信、电视、计算机三网融合，健全国家公共信息网，加强信息化法制建设和综合管理，强化信息网络的安全保障体系。

（4）三网融合

宽带 IP 网将成为新一代信息基础设施的基础网，三网融合后产生的新一代信息网将是基于 IP 的多业务网。所谓融合包括电信网和数据网（包括传统数据网和因特网）的融合，有线固定网和无线移动网的融合，以及电信网、数据网和广播电视网的融合。新一代信息网将能够在统一的 IP 平台上提供各种已有业务和融合产生的新业务。这些业务可以分为两类：一类是 IP 网所固有的基于 Web 的、无连接的因特网开创和演化的新业务，从电子商务到宽带交互式新媒体；另一类是传统电信业务的延伸和演化。

IP 电话的存在价值和竞争优势在于将互联网基于 Web 的新业务和传统电话智能网业务的优势结合起来，提供创新的综合业务。新一代信息网是宽带交互式媒体。随着 10/100Mb/s 宽带接入网的普及，现在在频道上进行的音频、视频广播将转移到新一代信息网上进行，而且将发展成为具有交互能力的新媒体。这种新媒体的内容将既有因特网 Web 的交互能力，又有电视的动感和高质量的音像效果。

新一代信息网也是地面固定网和无线移动网融合的产物。这意味着在移动终端可以在任何时间、任何地点保持与统一的信息网的固定的宽带的连接。全世界每人一个号码，它将进一步改变人类生活、工作方式。

三网融合将改变现行的运行、管理体制和法律、法规。制定新的法律、法规，发展形成新的管理运行体制将是今后重要的任务。

（5）引起企业革命

因特网、WWW 的快速发展，电子商务的兴起，对企业商务运行产生巨大影响。.com 公司形成的网络泡沫的破灭消除了浮躁情绪，电子商务与传统产业结合正在推动企业革命。