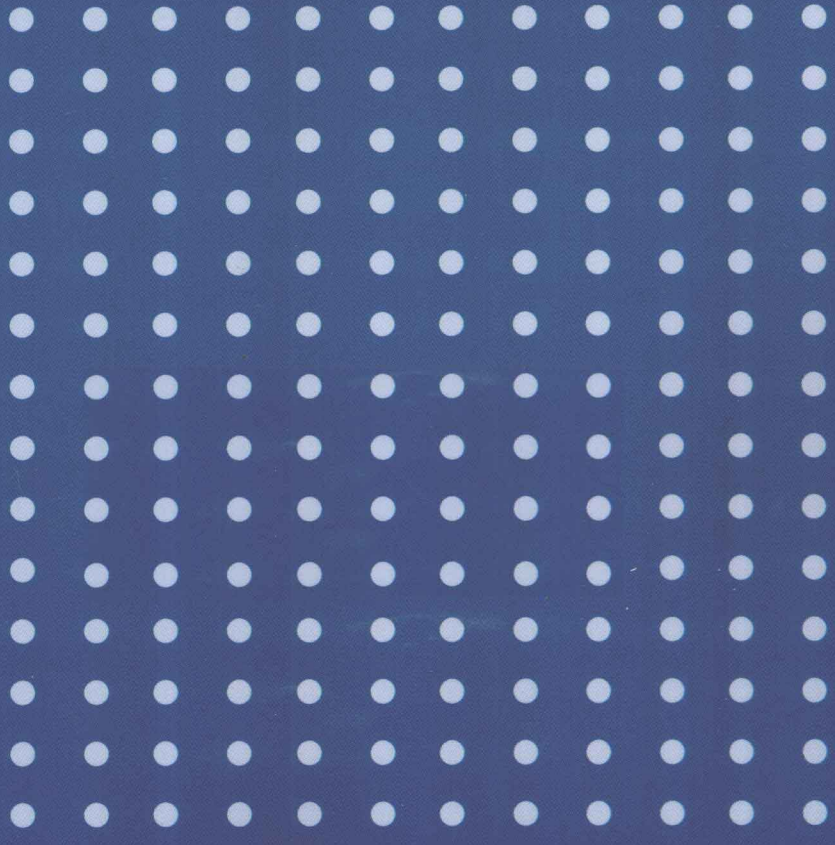
重点大学计算机专业系列教材

网络协议与网络安全
(第2版)

凌 力 编著

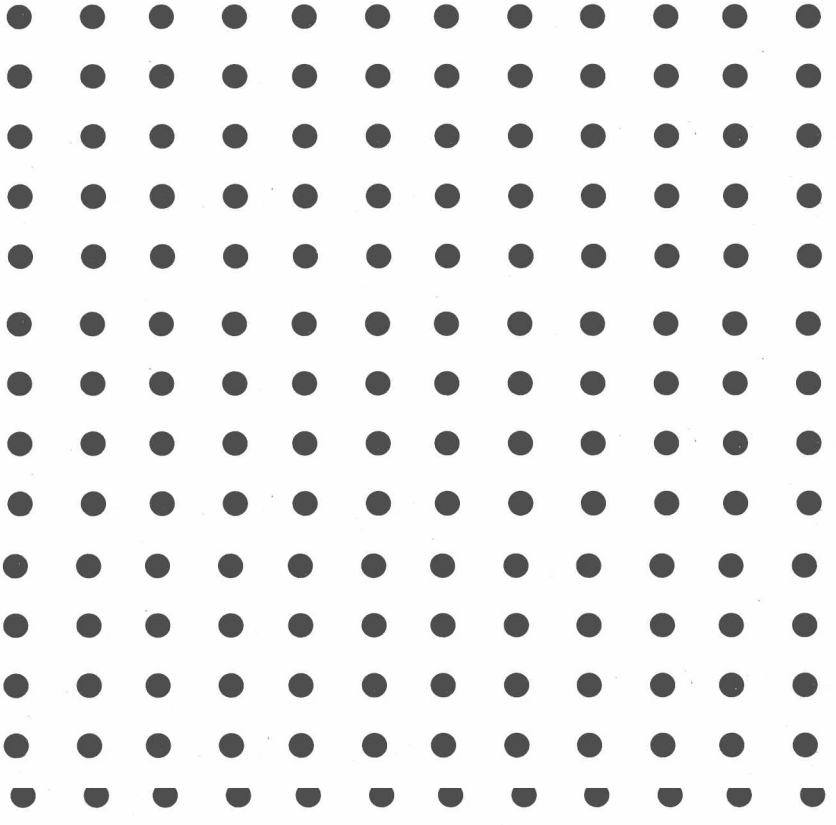


清华大学出版社

重点大学计算机专业系列教材

网络协议与网络安全
（第2版）

凌 力 编著



清华大学出版社
北京

内 容 简 介

本书由两个知识板块构成：网络协议原理和网络安全原理。两者有一定的相互独立性，可以分为两门课程讲授或学习，同时也存在较强的关联性，贯穿起来学习更有助于全面掌握网络技术，奠定扎实的理论基础。

网络协议原理部分的重点是 Internet 技术，其次包括 Ethernet、WLAN、自组网(Ad-hoc)、宽带网络和移动通信网络等重要的网络类型及其技术。从计算机网络 OSI 原理出发，具体剖析了各种网络协议、网络体系结构、路由算法和多媒体信息编码算法。此外，还分析了物联网、云计算、移动计算等新技术的基本概念、技术原理和发展趋势。

在网络安全原理部分，逐一详解了古典加密算法、对称密钥加密算法、非对称密钥加密算法和单向函数加密算法以及以密码学理论为基础形成的数字签名技术、网络安全协议和密钥管理方法，并通过对网络安全威胁技术的具体分析，详细讨论了网络安全防范的技术和体系。

本书作为适合高等院校计算机、网络、通信、信息等相关专业学科的研究生和本科生教材，也可作为其他专业学生的选修、自学的参考材料。

图书在版编目(CIP)数据

网络协议与网络安全/凌力编著. --2 版. --北京：清华大学出版社，2012.10
(重点大学计算机专业系列教材)
ISBN 978-7-302-28940-1

Ⅰ. ①网… Ⅱ. ①凌… Ⅲ. ①计算机网络－通信协议－高等学校－教材 ②计算机网络－安全技术－高等学校－教材 Ⅳ. ①TN915.04 ②TP393.08

中国版本图书馆 CIP 数据核字(2012)第 110894 号

责任编辑：魏江江　赵晓宁
封面设计：常雪影
责任校对：焦丽丽
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62795954
印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：18.5　　**字　　数**：452 千字
版　　次：2007 年 11 月第 1 版　2012 年 10 月第 2 版　　**印　　次**：2012 年 10 月第1 次印刷
印　　数：1～3000
定　　价：29.50 元

产品编号：036962-01

INTRODUCTION

出版说明

随着国家信息化步伐的加快和高等教育规模的扩大，社会对计算机专业人才的需求不仅体现在数量的增加上，而且体现在质量要求的提高上，培养具有研究和实践能力的高层次的计算机专业人才已成为许多重点大学计算机专业教育的主要目标。目前，我国共有16个国家重点学科、20个博士点一级学科、28个博士点二级学科集中在教育部部属重点大学，这些高校在计算机教学和科研方面具有一定优势，并且大多以国际著名大学计算机教育为参照系，具有系统完善的教学课程体系、教学实验体系、教学质量保证体系和人才培养评估体系等综合体系，形成了培养一流人才的教学和科研环境。

重点大学计算机学科的教学与科研氛围是培养一流计算机人才的基础，其中专业教材的使用和建设则是这种氛围的重要组成部分，一批具有学科方向特色优势的计算机专业教材作为各重点大学的重点建设项目成果得到肯定。为了展示和发扬各重点大学在计算机专业教育上的优势，特别是专业教材建设上的优势，同时配合各重点大学的计算机学科建设和专业课程教学需要，在教育部相关教学指导委员会专家的建议和各重点大学的大力支持下，清华大学出版社规划并出版本系列教材。本系列教材的建设旨在“汇聚学科精英、引领学科建设、培育专业英才”，同时以教材示范各重点大学的优秀教学理念、教学方法、教学手段和教学内容等。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 面向学科发展的前沿，适应当前社会对计算机专业高级人才的培养需求。教材内容以基本理论为基础，反映基本理论和原理的综合应用，重视实践和应用环节。

(2) 反映教学需要，促进教学发展。教材要能适应多样化的教学需要，正确把握教学内容和课程体系的改革方向。在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略，突出重点，保证质量。规划教材建设的重点依然是专业基础课和专业主干课；特别注意选择并安排了一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现重点大学

计算机专业教学内容和课程体系改革成果的教材。

(4) 主张一纲多本,合理配套。专业基础课和专业主干课教材要配套,同一门课程可以有多本具有不同内容特点的教材。处理好教材统一性与多样化的关系;基本教材与辅助教材以及教学参考书的关系;文字教材与软件教材的关系,实现教材系列资源配套。

(5) 依靠专家,择优落实。在制订教材规划时要依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后要认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

教材编委会

FOREWORD

第2版 前言

信安山有石室，王质入其室，见二童子对弈，看之。局未终，视其所执伐薪柯已烂朽，遂归，乡里已非矣。

——东晋穆帝永和年间(公元345年)虞喜作《志林》

从2007年本书的第1版到2012年的第2版，时间悄悄地过去了5年。5年不算久，弹指一挥间，够一名学子读完大学。但网络这个虚拟世界或许有自己的历法，颇有“洞中方七日，世上已千年”的“仙界”之风，只不过颠倒过来，日子过得飞快，现实世界的5年，互联网恰似飞越了50年，否则无法解释为何短时间内会冒出那么多新技术，产生那么巨大的变化。

比起那位在山中看仙童下棋的樵夫，我们不知道是幸或不幸。可怜的砍柴大哥仅仅偶发雅兴，旁观了一盘棋，结果连斧柄都朽烂了，自己的家和村子竟然物非人亦非。而我们5年前的PC和手机呢？朽烂倒未必，可是十有八九已被我们自己视为“破烂”，不少人的手机也许已经换了几部。

当然可以坚持不换老的PC，但用PC上网意味着必须端端正正地坐在桌子前，不像用平板计算机一样自由自在，不能走着看新闻，躺着看视频，或在地铁里悠闲地边听音乐边读书；用PC还意味着只能老老实实地用鼠标点击，而无法划拉、抓挠屏幕，与蔬菜、小鸟和怪兽作斗争。假如依依不舍，钟爱多年的老手机也不一定换。但如今，堂堂的嵌入式操作系统居然被打上了“非智能”的标签，成为“低能”一族，举目皆是多点触控的大屏智能机，桌面上各式各样的App(应用程序)浮动着，竞相争宠。你实现3G上网，我就有WiFi热点互联；你可以GPS(全球定位系统)导航，我就提供LBS(位置相关服务)业务。因此，PC和手机换与不换，这是一个问题。

这一切主要是拜乔布斯所赐。他的苹果既不是来自亚当和夏娃的伊甸园，也不是摘自牛顿头上的苹果树，而是被图林(计算机与人工智能之父)咬过的那一颗，半个多世纪后，完全退去了毒性，剩下的只有熠熠闪光的智慧、创新和维生素。刚刚过去的5年，打着苹果标志的平板计算机和手机覆盖了全球，更重要的是这些漂亮非凡、人见人爱的“尤物”改变了人们对计算机的认知、改变了一成不变的计算机操作习惯，让上网变成一种令人愉悦的旅程，

让获取信息像呼吸一样简单和自然,让地球上的任意两个人的沟通仿佛面对面。

所以,我们有理由相信,虚拟世界的时空超越了爱因斯坦的学说,时钟走得飞快,日子变得很短,距离趋近于零,而虚拟世界的演进速度则超过了达尔文的想象,甚至智能"生物"的诞生也并非痴人说梦,或许为期不远了。

5年来,山洞中的棋局大概还没走出一步,恰似IPv4协议依旧,Internet仍然不安全,国足还是没出线,但尘世间一直不可遏止地忙碌着,不论是现实世界还是虚拟世界,沧海总是或快或慢地往桑田方向变。想想云计算,想想物联网吧,早上晴空万里,下午就"云雾"缭绕了。闲不住的乔布斯驾鹤西去后肯定会带去人类的进取精神,这样仙童下棋的石桌就有机会支持滑屏了。

祝大家享受知识,也享受知识创造的成果。

编　者

2012年4月于复旦大学

FOREWORD

第1版 前言

■ 关于观点

我们不要惧怕亮出自己的观点——即使有失偏颇也可供大家评判、批评、争论、思考、品味。客观的数据是必要的，枯燥的理论是难免的，但最终还是要有观点和结论，这关系到立场问题。

在本书中可以找到许多观点，谦虚地说，它们不一定都是正确的。影响正确性判断的原因有三：一是认识有偏颇；二是事物在发展，丑小鸭长啊长，说不定是只白天鹅呢！三是有更多更好的事物在孕育中、诞生中。这正是计算机网络领域的特点：朝气蓬勃，欣欣向荣，这也是研究计算机网络的乐趣所在：推陈出新，创意无限，不过这也是置身计算机网络行业的辛苦所在：三日不见，形同陌路！

理解是观点的起步，观点是理解的体现。理解了，有观点了，往往就成功了一半。

■ 关于情感

为什么大数学家说在天书般的方程式堆中漫游是妙不可言、富有乐趣的？那就是情感。固然他们到达了某种常人无法企及的境界，但不可否认，任何事物都是可以有情感的，不管这种情感是其自身所具备的，还是感怀的人所赋予的。

所以我们可以大胆地说，技术文献是有情感的，论文讲义是有情感的，计算机网络也是有情感的。

计算机网络本来就是很拟人化的东西，人类逐渐在互联网上构筑起一个虚拟世界。这是一个多么富有想象力的全人类共同参与的大工程！所以，本书读者们在阅读到那些看上去和计算机网络术语、技术无关的文字时，请不要忽略，相信我，它们是属于计算机网络领域的。

■ 关于角度

但凡足球运动员用大家认为不可思议的角度射入一个球时，都会得到暴风雨般的喝彩，因为这个球与众不同，因为把自己从昏昏欲睡的比赛过程中

弄醒了。没有统计过,不知道有多少人在阅读技术文章时处于半清醒状态,我想应该不在少数,因为不客气地说,大部分的教科书都很教科书,有千篇一律的公式和行文,有从基础到深入的严密逻辑。

然而我不认为这有什么可取的,或者说不认为一定非得这样。花开两朵还各有不同呢!本书抓的一个个的点并不全落在"网"的"纲"上,但希望抓起这些点能有一些"目"能够张开,由点及面,窥一斑知全豹,也是一个了解"全网"的不容易睡着的方法。

本书的每一个章节都试图去了解一个或大或小的问题,并扩展到周围的问题。我们比较多地采用"比较性分析"的办法,通过对比来加深概念和技术方法的理解。不过是否能达到预期效果——还得靠读者自己琢磨!

■ 关于细节

有人说"细节决定成败",那大概是在说装配钟表吧。回想童年,你还记得多少细节?——无非是和谁闹别扭了,后来又要好了等等,至于为什么事情吵架多半已经不记得了。不要慌张,不是健忘,那是人脑的优秀性能之一:忘记不必要的东西。那样你才没有崩溃。

计算机网络中也有很多细节,它们是由许许多多数字、字母构成的,足够把人弄疯。所以,我们最好要学会什么时候要关注细节(当少尉排长),什么时候要看重全局(当五星将军)。

普天下阐述技术细节的书已经够多了,所以本书不打算凑这个热闹。而当我们把一些所谓的细节屏蔽掉之后,我们往往会发现技术的核心思想显露出来了。至于细节,很简单,我们可以检索有关资料来获取。

■ 关于本教材

- 本教材可作为本科生、研究生课程教学用书或参考书。
- 虽然涉及"网络协议",但并非以单纯的网络协议原理为首要内容,而是从较为宏观的网络与通信技术的角度来体现较为微观的协议技术,旨在从网络理解协议、从协议透视网络。
- 每章为一个大的知识点,阐述一个网络及其安全技术的"板块";每个板块由若干小的知识点构成。各板块间的内容略有交叉重叠,反映出网络通信领域各项关键技术的关联性,因此,既要对各个"分支"进行深入钻研,又要有全局的、整体的观念。
- 每章学习约需一两个"单元时间"(每单元时间为两三课时)。
- 由于涉及的概念、术语较多,这个"基础"打得不会很轻松,但会从知识面拓展上有所获益。
- 希望在学习过程中不要仅仅局限于书本内容,而应该主动去学习更多的相关知识,对感兴趣的问题予以纵深挖掘。这里包含两层意思:第一,鼓励借助计算机、互联网进行学习,而不要停留在书本涵盖的有限知识上;第二,把对理论的理性认识应用于实践中,获得感性认识,达到融会贯通的目的。
- 勤于思考,不迷信"权威"。对"可疑"观点应勇敢地提出质疑和自己的见解。同时也要善于发现问题、提出问题,并提高分析问题、解决问题的能力。
- 因为网络技术的发展速度很快,本教材也将不断更新,力争与本领域的新进展同步。

作　者

2007年6月于复旦大学

CONTENTS

目录

CHAPTER 1

第1章 计算机网络与协议

网络在自然界广泛存在，例如，由江河湖海构成的水系，蜘蛛辛勤编织的捕食网。网络在人类社会里更是无处不在，简单到渔家的渔网、猎人的捕兽网，复杂到遍布城市和乡村的道路网、输电网、输气网、自来水管网、下水道网，乃至错综复杂的人际关系网、国际关系网、疏而不漏的法网。网络无疑是人类赖以生存的重要手段之一。

网络体现了人类的大智慧。通过组网，可以建立相互间的联系，可以远程输送资源，可以实现 1+1>2 的集聚和放大效应。

网络的关键是通过经纬脉络组成某种结构，进而产生特定功效。因此，由空洞起作用的筛子不能算是网络，而同样被编织成网形的渔网则是一种网络。

英语中有许多词汇指代网络，除了 Network 和 Net，还有 Grid、Web、Matrix、Mesh 等，含义上有细微的差别，在网络技术术语中经常会出现。

网络造就了我们身处的信息时代，并被赋予了更为丰富的内涵。电话网、广播电视网、计算机网，满足了人们及时掌握信息、方便沟通交流、实现资源共享的需要，于是，越来越多的人不知不觉中对网络有了严重的、几乎不可逆转的依赖性，因为网络已经深入到了学习、工作和日常生活的方方面面。且不论这种依赖性本身孰是孰非，网络给人们带来的高效性、便捷化、无疆界是有目共睹的。仅凭这一点，网络无疑担当了这个时代当仁不让的主角。

人们平时说的“网络”，通常就是指计算机网络，甚至就是指 Internet。这个现象很令人深思，但并不费解。原因在于计算机和计算机网络引发了汹涌澎湃的数字化浪潮，不仅把传统的模拟网络逐一纳入怀中成为数字网络，而且通过替代或融合，把各种类型的计算机网络逐步统一为 Internet。或许有人会争论 Internet 一家独大的局面是否存在弊端的问题，但越来越多的人开始或已经习惯于上网搜信息、发言论、找朋友、买商品，谁会希望倒退到没有 Internet 的年代？计算机网络和 Internet 正是本书的重点。

1946 年，第一台计算机问世；1969 年，计算机网络诞生。计算机具备与生俱来的运算能力，可以让人摆脱烦琐的计算任务，让运算速度得到以数量