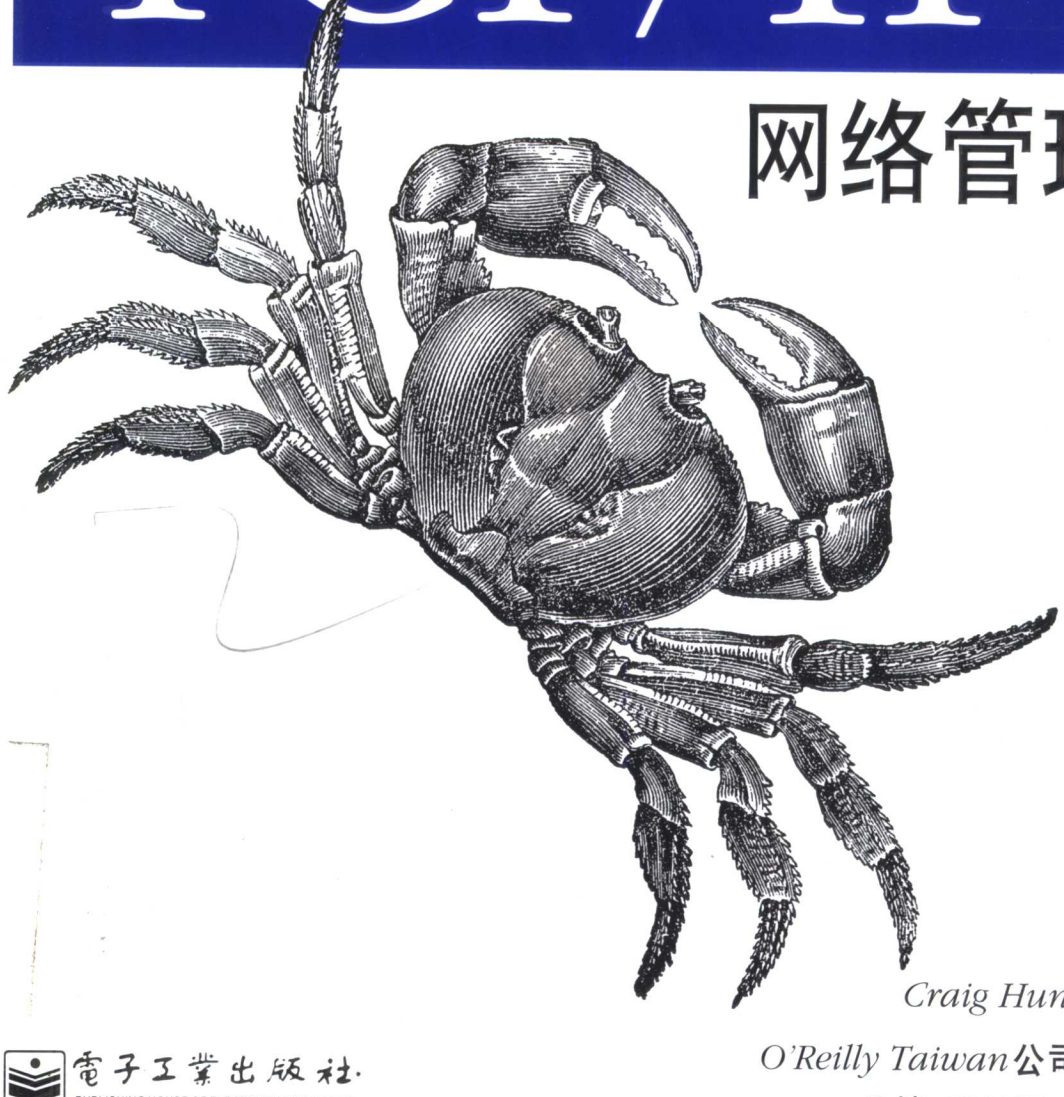
O'REILLY®

*TCP/IP Network Administration*

第三版

# TCP/IP

## 网络管理



*Craig Hunt* 著

*O'Reilly Taiwan* 公司 译

翁恺 周新运 审校

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

O'REILLY®

# TCP/IP 网络管理

## 第三版

*Craig Hunt* 著

*O'Reilly Taiwan* 公司 译

翁恺 周新运 审校

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

**图书在版编目（CIP）数据**

TCP/IP 网络管理（第三版）/（美）亨特（Hunt, C.）著；O'Reilly Taiwan 公司译．
北京：电子工业出版社，2006.3
书名原文：TCP/IP Network Administration, Third Edition
ISBN 7-121-01618-4

I. T... II. ①亨... ②O... III. 计算机网络－通信协议 IV. TN915.04
中国版本图书馆 CIP 数据核字（2005）第 087262 号

版权贸易合同登记号
图字：01-2004-1758



书　　名/ TCP/IP 网络管理（第三版）
书　　号/ ISBN 7-121-01618-4
责任编辑/ 顾慧芳，高洪霞
封面设计/ Edie Freedman，张健
出版发行/ 电子工业出版社（http://www.phei.com.cn）
地　　址/ 北京市海淀区万寿路 173 信箱（邮政编码 100036）
经　　销/ 各地新华书店
印　　刷/ 北京智力达印刷有限公司
开　　本/ 787 × 980　16 开本　49 印张　930 千字
印　　次/ 2006 年 3 月第 1 次印刷
印　　数/ 0001-4000 册
定　　价/ 79.00 元（册）

# O'Reilly Media, Inc. 介绍

为了满足读者对网络和软件技术知识的迫切需求，世界著名计算机图书出版机构O'Reilly Media, Inc. 授权电子工业出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc. 是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时是联机出版的先锋。

从最畅销的《The Whole Internet User's Guide & Catalog》（被纽约公共图书馆评为二十世纪最重要的50本书之一）到GNN（最早的Internet门户和商业网站），再到WebSite（第一个桌面PC的Web服务器软件），O'Reilly Media, Inc.一直处于Internet发展的最前沿。

许多书店的反馈表明，O'Reilly Media, Inc. 是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly Media, Inc. 具有深厚的计算机专业背景，这使得O'Reilly Media, Inc. 形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc. 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly Media, Inc. 还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly Media, Inc. 依靠他们及时地推出图书。因为O'Reilly Media, Inc. 紧密地与计算机业界联系着，所以O'Reilly Media, Inc. 知道市场上真正需要什么图书。

## 作者简介

**Craig Hunt** 在过去 25 年间都与计算机系统工作。他的第一份工作是在美国联邦政府任职程序设计师，然后担任系统程序设计师。后来在 TCP/IP 尚未问世时他辞去政府的工作跑去替 Honeywell 从事 WWMCCS 网络工作，当时的网络还是使用 NCP。离开 Honeywell 后，Craig 跑去替 National Institute of Standards and Technology (NIST) 工作，在那里他建立了该公司的第一个 TCP/IP 企业网络，并负责管理网络的中央服务器，之后又转入网络技术的研究。后来 Craig 离开 NIST 开始专心投入 Linux、Unix 与网络的写作与教学，除了本书《TCP/IP Network Administration》之外，他另外还有四本单独著作、两本合著 (co-authored)、五本参与编辑的书出版。他也在主要的会议（如 USENIX 与 LinuxWorld）中讲授 Linux、Unix 与网络。如果想要知道得更详细，可到作者的网站 *http://www.wrotethebook. com* 参观。

Craig 和他的太太及小孩住在马里兰州的盖兹堡。他很喜爱户外活动，最近他喜欢骑着山地车到处跑。

## 封面介绍

本书封面所采用的动物是陆蟹。在热带的美洲、西非和印度与太平洋间的地区都可以发现它的踪迹。它们的居所是在原野间的地洞、沼泽和红树林；但偶而也可以在离开海边 8 公里的内陆看到它们，然后千辛万苦地爬回海里产卵。陆蟹隶属 4500 种甲壳类中的一种。与虾类、龙虾类和淡水螯虾类同属，但与它们不同的是尾部的结构。螃蟹的尾部是卷曲在它们的胸甲里，因此，它们的甲壳大得有些夸张。美国的陆蟹通常不会生长超过 18 盎司重、4 或 5 英寸大，一般的螃蟹大小不会小于一公分，但确有很大的螃蟹，例如，日本的蜘蛛蟹，它的螯爪伸展开来可以到 12 尺长。

# 目录

# 前言

第一版的《TCP/IP网络管理》是在1992年写成的，至今已经十年了，有许多事情已经改变了，但仍有些事情维持原貌。要想连接分散于各地的计算机，TCP/IP依然是首选的通信协议，而且至今依然是数据交换与全球计算机网络的基础。最基层的IP（Internet Protocol）、TCP（Transmission Control Protocol）与UDP（User Datagram Protocol）完全没有改变，但是TCP/IP本身的用法与管理方式，却有新的诠释。

这种改变的明显现象之一，莫过于我岳母也会在自己家里使用TCP/IP网络，与她的“老”朋友互发电子邮件、压缩图文件与HTML文件。在她看来，这就是所谓的“上网”，但事实上，她并不知道她的小系统里包含了一套TCP/IP协议堆栈，此堆栈能管理一个自动配置得到的IP地址，并处理十几年前并不存在的数据类型。

在1991年，网络管理员只需管理少数几台机器，因为当时的TCP/IP网络规模不大，而且所有用户清一色全是“高手”，具有程度相当高的技术知识水准。时至21世纪的今天，网络的使用人数远超过以往的规模，而且大多数用户普遍缺乏处理技术问题的能力，在这种情况下，需要训练更多的技术人员来管理网络。本书的宗旨就是要提供足够的信息，让你成为一位高效率的TCP/IP网络管理员。

《TCP/IP网络管理》是第一本专为TCP/IP网络管理人员所写的实践书籍，而且我可以颇为自豪地说，它仍是目前最好的一本。在本书第一版问世之后，关于TCP/IP与Internet的书籍如雨后春笋般地大量涌现，然而，只有少数几本书具体谈到系统管理员在面对TCP/IP网络时所必须知道的背景知识，以及相关的实践技巧。大部分网络书籍普遍倾向于学院派，纯粹从协议设计者的角度来写作，学术理论多于实践操作；而强调“实践”的网络书籍普遍偏向于如何使用TCP/IP的应用（E-mail，WWW，...），很少提到UNIX系统管理员必须知道的网管实践。因此，本书仍然将焦点摆在TCP/IP与UNIX，并尝试在理论与实践之间取得适当的平衡。

写作并非易事，改版也一样。一本书能够持续改版，表示该书持续得到读者肯定。包括这次在内，《TCP/IP网络管理》已经历经两次改版，这是第三版。我将继续秉承前两次改版的精神，在尝试任何改进时尽可能地维护本书的基本特质。

本版的新增主题包括用来动态分配IP地址的DHCP（Dynamic Host Configuration Protocol），以及用来架设HTTP网站的Apache web server。原本关于Domain Name System（DNS）的主题，则更新到BIND 8与最新的BIND 9；关于电子邮件系统部分，则按照目前的sendmail v8全面改写；示范平台则改用Solaris 8/9与Linux。在路由协议方面，我更新了关于RIPv2（Routing Information Protocol version 2），OSPF（Open Shortest Path First）与BGP（Border Gateway Protocol）的内容。此外，我还特地为xinetd另辟一章新篇幅，并解释如何使用iptables来架设防火墙。尽管新增了这些额外主题，本书的篇幅仍保持在合理范围内。

TCP/IP是一组通信协议，它定义了如何使得不同类型的计算机互相交谈。《TCP/IP网络管理》是一本关于如何架设TCP/IP网络的书，它同时包含TCP/IP网络功能的“为何”（why）与“如何”（how）方面，也提供了特定网络服务程序的参考资料。

# 读者

本书的读者对象是所有有一台连到TCP/IP网络的UNIX机器的读者。很明显，这包括了负责架设计算机与网络的系统管理员和网络管理员。不过，有兴趣知道自己的计算机如何与其他系统进行沟通的所有人也都适合阅读本书。事实上，“系统管理员”与“一般用户”的界限已经越来越模糊了，你或许自认为只是一般用户，但桌上摆了一台UNIX工作站，也就难免会涉及一些系统管理工作。

近几年来，有些摆明了专为“dummies”和“idiots”而写的书籍大行其道。如果你自认在UNIX方面的确是“idiot”，那么本书将不适合你。反过来说，如果你自认为是网络技术的“天才”，本书恐怕也不适合你。然而，如果你处于这两种极端之间，那么本书对你的帮助应该不小。

我们假设读者熟知计算机的基本架构，并具备了相当高的程度的操作经验，而且熟悉一般的UNIX系统管理事务。如果还不太熟悉这方面的技巧，建议你参考O'Reilly出版的《UNIX系统管理》或《Linux技术手册》来补充相关的基础技能。

# 内容编排

在概念上，本书内容分成三大篇：基础概念、教材与参考资料。第一篇包含前三章，重点在于探讨TCP/IP协议与服务的基本概念，这些都是理解本书其余主题所需的基础。本书第二篇主要提供“如何办到...”的指导教材：第四章到第七章讨论如何设计、安装网络，配置网络使之能进行的必需的软件。第八章到第十一章讨论如何架设各种重要的网络服务；在最后的第十二章与第十三章，则探讨如何维持网络的可靠性，包括安全防护与故障排除。本书第三篇是一系列附录，收录了各种重要命令与程序的技术参考资料。

本书实际的章节编排如下：

第一章“TCP/IP概论”。谈论TCP/IP的发展史，说明协议的组织架构，以及各协议的用途与原理。

第二章“数据传输”。说明寻址法则，以及数据如何通过网络抵达正确的目的地。

第三章“网络服务”。讨论客户端与服务器系统之间的关系，以及各种关于internet核心功能的服务。

第四章“开始行动”。开始讨论网络的基本配置，包括在开始着手设定网络上的主机系统之前应该事先规划好的相关事项。

第五章“基本配置”。说明如何配置UNIX内核的TCP/IP功能，以及如何配置系统使其启动网络服务。

第六章“网络接口配置”。告诉你如何让网络软件识别网络接口，本章分别以Ethernet和PPP为例，示范如何配置不同种类的网络接口。

第七章“路由配置”。说明路由（routing）的原理与概念，解释计算机系统是如何与其他网络上的主机顺利通信的。其中包括静态路由表、常用的路由协议，以及一套实现了多种路由协议的软件包——`gated`。

第八章“配置DNS服务器”。说明如何架设、管理名称服务器软件，将网络名称顺利转换为IP地址。

第九章“局域网服务”。讨论如何规划多种常用的网络服务，包括DHCP服务器、LPD打印服务器、POP与IMAP邮件服务、网络文件系统（NFS）、网络信息系统（NIS），以及Samba文件/打印服务器。

第十章“sendmail”。介绍如何配置全球使用率最高的电子邮件传送系统：sendmail。

第十一章“配置 Apache 服务器”。说明如何配置 Apache 网页服务器软件。

第十二章“网络安全”。讨论如何在危机四伏的Internet上求生存，本章说明网络可能带来怎样的安全风险，以及防范这些威胁的防护措施。

第十三章“TCP/IP 故障排除”。告诉你当网络出问题时可以采取哪些措施来排除故障，以及日常的维护工作。本章会介绍一些能用来解决、测试 TCP/IP 问题的工具程序与技术，并示范几种实际问题的解决办法。

附录一“PPP工具”。说明一些常用来为TCP/IP配置串行端口的工具软件，包括dip，pppd与chat。

附录二“gated 参考资料”。提供 gated 配置语言的参考资料。

附录三“named 参考资料”。BIND 名称服务器软件的参考信息。

附录四“dhcpd 参考资料”。dhcpd 的参考信息。

附录五“sendmail 参考资料”。详细说明 sendmail 的语法、选项与标记。

附录六“Solaris httpd.conf 文件”。列出第十一章讨论的 Apache 配置文件的详细内容。

附录七“RFC 节选”。直接从 RFCs 节选出来的协议的细节资料，供排除故障时参考。本附录还提供了获取 RFC 文档的方法。

# 软件版本

本书大多数范例以 Red Hat Linux 7.x/8.0（多数人用的是 Linux 发行包）与 Solaris 8/9（以 System V Unix 为基础的 Sun 操作系统）为示范平台。幸运的是，在各种不同的系统之间，TCP/IP软件被刻意标准化了，如此一致的结果，使得本书的范例也可以用于任何公司发行的Linux包（例如SuSE，Debian，Slackware，...），System V或BSD-based UNIX 系统。当然，某些命令的输出格式与命令行选项会略有区别，但是这些区别应该不至于造成太大的问题，毕竟万变不离其宗，基本的概念都是一样的。

某些经常伴随UNIX系统出现的网络软件，它们自己有一套独立于UNIX系统之外的版本号，我们也会论及这些软件，并注明本书信息所适用的版本。最重要的几个软件包如下：

*BIND*

我们对BIND软件的讨论主要是依据Solaris 8系统随附的BIND 8。我们选择此版本是因为BIND 8支持所有标准的资源记录（resource records），而且在基本配置方面，BIND 8与较新版本的BIND 9只有非常小的管理性差异。

*sendmail*

我们对sendmail的讨论是以8.11.3版为主。该版本与sendmail v8的其他版本应该是兼容的。

# 排版约定

本书用各种印刷效果来强调不同的内容：

斜体字（*Italic*）

用于重要的文件名、目录名、主机名称、域名。当首次引入新名词时，用斜体字予以强调。

等宽字体（Constant Width）

用于表现文件内容或命令的输出。在正文中，这种字体也用来表示命令、选项、关键字。

等宽黑体（**Constant Width Bold**）

在范例中，用于凸显手工键入的部分，以便和计算机的输出部分区别开来。

等宽斜体（*Constant Width Italic*）

在范例和内文中，用于表示应该代换为实际值的变量。例如：

```
ls filename
```

这表示你应该将 filename 换成实际存在的文件名称（如 *readme.txt*）。

%、#

每当我们示范交互式命令时，我们通常使用C shell的默认提示符（%），对于必须以root身份才能执行的命令，则将提示符改成#。此外，某些范例可能涉及网络上的多个系统，在提示符之前，可能会有一个系统名称，那表示我们是在该系统发出的命令。

[ 选项 ]

在表示命令的语法时，放在方括号之间的部分，是可有可无的“选项”。例如：ls [ -l ]表示你可以加上 -l 选项，也可以不加。

# 建议与评论

我们已经尽可能地测试和完善本书给读者提供的信息和技术了，但是我们不能保证书中提供的功能完全没发生什么变化（甚至是书中出现错误！）。如果有热心的读者阅读了本书，并且发现什么可以改进的功能，请将这些信息反馈给我们。如果有任何的错误、缺陷，或者是误导读者的地方，以及不清楚的地方，甚至是印刷上的问题，请批评指正，我们不胜感激。

如果读者还希望本书为您提供哪方面的信息，也请联系我们。我们会很重视任何读者的意见和建议，并且在以后的版本中尽量纠正错误，并且提供更丰富的信息来满足读者的要求。我们的地址和联系电话是：

美国：

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472

中国：

100080 北京市海淀区知春路 49 号希格玛公寓 B 座 809 室
奥莱理软件（北京）有限公司

要获取有关本书的实例、勘误表，以及其他一些内容，请访问以下网页：

*http://www.oreilly.com/catalog/tcp3*

要询问技术问题或对本书提出建议，请发送电子邮件至：

*info@mail.oreilly.com.cn*
*bookquestions@oreilly.com*

如果有什么技术上的问题或者注释不明白，可以发送电子邮件到：

*bookquestions@oreilly.com*

如果想了解与本书相关的其他信息，可以访问 O'Reilly 的网站：

*http://www.oreilly.com*
*http://www.oreilly.com.cn*

要获取作者有关信息，请访问他的网站：

*http://wrotethebook.com*

# 致谢

我要感谢所有协助我准备本书的人，尤其是曾经在第一版与第二版就做出贡献的人们，因为他们的努力成果仍然留在此版本里。对于第一版，他们是John Wack，Matt Bishop，Wietse Venema，Eric Allman，Jeff Honig，Scott Brim 与 John Dorgan；对于第二版，他们是 Eric Allman，Bryan Costales，Cricket Liu，Paul Albitz，Ted Lemon，Elizabeth Zwicky，Brent Chapman，Simson Garfinkel，Jeff Sedayao 与 Æleen Frisch。

第三版也是众人努力的结果，其中有不少是独当一面的作家。他们给了我有条理的技术细节，并帮助我改进了我的表达文笔。我尤其要特别感谢其中三位作家。Cricket Liu —— DNS权威书的作者之一 —— 为我的DNS章节提供了许多建议。David Collier-Brown —— "Using Samba"的作者之一 —— 很详细地审校了我的Samba文章。Charles Aulds —— 关于 Apache 管理的畅销书作者 —— 提供了 Apache 配置文件的全新观点。在这些高手的帮助之下，我才有信心第三版会比前两版更好！感谢他们！

在O'Reilly & Associates的人们更是对我助益良多。我尤其应该特别感谢我的编辑，Deb Cameron。当我那美丽的新生女儿Bethany Rose让我忙得不可开交时，Deb保持一切进度照常进行。Emily Quill是本书的制作编辑与策划管理人；Jeff Holcomb 与 Jane Ellin 负责品质控制与检查；Leanne Soylemez 提供制作协助；Tom Dinse 编写索引；Edie Freedman 设计封面；Melanie Wang 设计内文排版格式；Neil Walls 将我的文章从 Microsoft Word 改成 Framemaker 格式；Chris Reilley 与 Robert Romano 绘制前版的插图，而 Robert Romano 与 Jessamyn Read 更新了这些插图。

最后，我要感谢我的家人 —— Kathy，Sara，David 与 Rebecca。当我面临交稿期限的压力时，他们鼓励我脚踏实地，使一切走上正轨。他们是最优秀的！