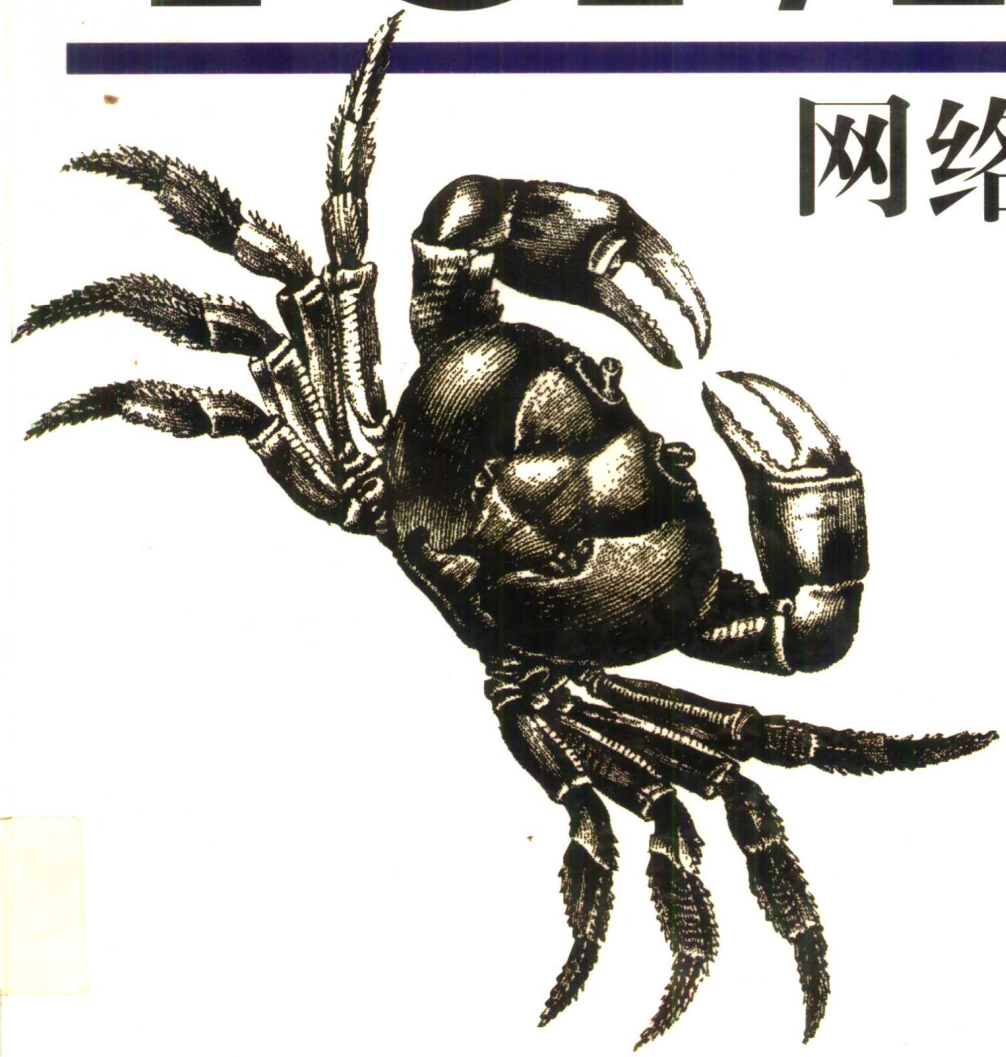
TCP/IP Network Administration

TCP/IP

网络管理



[美] *Craig Hunt* 著

翟 炯 石祥生 石秋云 译

O'REILLY™

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

内 容 简 介

本书全面、系统地阐述了TCP/IP协议。随着Internet的飞速发展，越来越多的人想了解、熟悉和掌握Internet的基本原理和精髓。作为Internet的核心技术之一的TCP/IP协议就成为广大Internet用户追求的对象。

本书共13章。前三章讨论TCP/IP协议的基础，为全书提供必要的背景知识；第4章到第7章讨论了如何配置使网络运行所必需的基本软件；第8章到第10章论述了如何设置各种重要的网络服务，大多数是自动实现的；第11章到第13章介绍一些事务性的工作，如故障检修、安全性、提供最新网络信息等。

原 书 名: TCP/IP Network Administration
书　　名: TCP/IP 网络管理
著　　者: 〔美〕Craig Hunt
译　　者: 翟 炯　石祥生　石秋云
责任编辑: 陆伯雄
特约编辑: 黄宪东
印 刷 者: 北京市顺义县天竺颖华印刷厂印刷
出版发行: 电子工业出版社出版，发行
北京市海淀区万寿路173信箱　邮编：100036　发行部电话 (010) 68214070
URL: http://www.phei.co.cn
经　　销: 各地新华书店经销
开　　本: 787 × 1092 1/16　印张: 21.75　字数: 500 千字
版　　次: 1997 年 8 月第 1 版　1997 年 8 月第 1 次印刷
印　　数: 5500 册
书　　号: ISBN 7-5053-4139-1
TP · 1828
定　　价: 35.00 元
著作权合同登记号　图字: 01-97-0499

前言

Internet（互联网）是全世界最大的网络，在1986年，联网的计算机还不到6, 000台，但在短短的五年时间内，却猛增到60万台，这种爆炸式的增长说明了人们对网络服务的迫切要求。遗憾的是伴随着这种增长，却缺乏实用的网络管理信息，大多数网络管理员只能无可奈何地满足于操作手册或哪些从协议设计者的观点编写的协议资料和学术著作。我们中的大多数人都已感觉到了那些已经联网的朋友们发出的、迫切需要实用信息的建议。本书就是在这一基础上问世的，它为UNIX系统管理员提供了大量实用而详细的网络信息，从而解决了缺乏信息的问题。

适用的读者

本书面向已经具有一台连接TCP/IP网络的UNIX计算机的任何人，显然，包括了负责设置和运行计算机及网络的网络管理员和系统管理员，以及那些希望了解他的计算机如何与其它系统通信的任何用户。“系统管理员”和“最终用户”之间的差别已日益模糊，你可以将自己看成是最终用户，但如果你有一台UNIX工作站，那么就可能要完成某些系统管理员的任务。

我们假定你对计算机及其操作已相当了解，而且已一般性地熟悉UNIX系统管理。否则，请阅读AEleen Frisch著的“*Essential System Administration*（系统管理基础）”一书。

内容编排

从概念上可以将本书分成四部分。前三章属于对TCP/IP协议的基础讨论，这种讨论为理解本书其它部分提供了必要的背景知识；第4到第7章讨论了如何配置使网络运行所必需的基本软件；第8到第10章论述了如何设置各种重要的网络服务，大多数服务是自动实现的，但有些服务则需要专门进行配置；第11到第13章，介绍一些事务性的任务，如故障检修、安全性、提供最新网络信息等。

本书包含如下章节：

第一章，TCP/IP概述。提供TCP/IP的历史，说明该协议的体系结构，从根本上解释具有这一体系结构的各个协议是如何工作的。

第二章，数据传输。说明寻址过程和数据如何在网络上传送到合适的目的地。

第三章，名服务概念。讨论标识计算机系统的地址和名字之间的关系，介绍将数字地址转换成名字的各种表和程序。

第四章，入门知识。开始讨论网络的设置和配置，在该章中讨论了在网络中配置系统前需要的原始配置规划，还解释了网络可能需要的各种正式的书面材料。

第五章，基本配置。介绍如何在UNIX内核中配置TCP/IP，以及如何配置网间守护程序（daemon），它可以启动大多数网络服务。

第六章，接口配置。介绍如何标识连接网络软件的网络接口，还提供了一些以太网（Ethernet）、SLIP、PPP等接口的配置实例。

第七章，路由选择配置。阐述如何设置路由选择，使得网络中的系统能正确地与其它网络通信；介绍静态路由选择表、RIP和EGP路由选择协议和网关守护程序（一个提供几种最新版本路由选择的软件包）。

第八章，DNS名服务的配置。阐述如何管理将系统名变换成Internet地址的名服务器程序。

第九章，网络应用程序。说明如何配置那些需要专门配置的公用网络服务，介绍UNIX的r例程（**rlogin**等）、网络文件系统（UNIX）、网络信息系统（NIS）等。

第十章，sendmail。讨论如何配置**sendmail**（负责传送电子邮件的守护程序）。

第十一章，TCP/IP故障检修。告诉你出现某些问题时如何去做，介绍检修各种TCP/IP故障所使用的各种技术和工具，列举了一些具体的故障及其解决方法。

第十二章，网络安全性。讨论如何才可以不冒太大的风险在网络上运行，介绍由网络引起的某些安全威胁及遇到这些威胁时应该如何打算和作哪些准备。

第十三章，Internet信息资源。介绍在Internet上可以使用的信息资源，以及如何利用它们。讨论如何设置你自己的匿名**ftp**服务器程序。

附录A，网络提供者名单。列出了美国和其它国家的各种网络服务提供者的名单。

附录B，表格。包含向网络信息中心（NIC）注册你的网络所需的各种表格。

附录C，网关守护程序gated参考资料。这是有关**gated**路由选择软件包的配置语言的完整参考指南。

附录D，名服务器守护程序named参考资料。这是有关“Berkeley Internet名域（BIND）”的名服务器程序的参考指南。

附录E，sendmail.cf范例文件。该附录包含一个**sendmail**范例配置文件，是第十章中各个例子的发展。

附录F，TCP/IP报头实例。该附录包含直接取自RFC的各种详细的协议参考资料，它们支持第十一章中的协议故障检测例子。

附录G，passwd+参考资料。该附录是有关配置**passwd+**（一个增强口令安全性的软件包）的参考指南。

附录H，软件来源。该附录包含一张表格，列出本书所用的全部免费软件。还列出了每个软件包及如何获取的说明。

UNIX版本

本书中大多数例子都使用SunOS 4.1.1，这是一个基于Berkeley的操作系统。一些System V的例子则使用基于System V 3.2版的SCO UNIX。幸运的是TCP/IP软件对不同的系统都是很标准的，由于它是如此的统一，因而这些例子将适用于任何System V系统或基于BSD

的UNIX系统。在命令输出或命令行选项方面可能存在一些细小的差异，但这种差异不会引起任何问题。

某些辅助网络软件单独地标识了需要特殊版本的UNIX操作系统，本书中将讨论这类软件包，在合适的场合还标注上版本号。其中最重要的软件包有：

gated 我们是以2.0.1.14版为基础讨论**gated**软件包的。请注意，该版本与以前的版本之间存在着重大的差别。

BIND 我们是以4.8.1版为基础讨论BIND软件的，这是在SunOS 4.1.1中使用的版本，其当前版本是4.8.3，但在这两种版本之间几乎没有什么差别。

Sendmail 我们是以5.65版为基础讨论**sendmail**软件的，这一版本已经使用了多年。

约定

在本书中使用下列印刷上的约定：

斜体 用于文件名、目录、主机名、域名等；当一些新的术语首次出现时，利用斜体（字母、数字）或楷体（汉字）着重说明。

黑体 用于命令名。

%, # 当提示你在交互方式提供的命令时，通常使用提示符%。如果该命令必须作为根执行，就使用提示符#。由于有些例子可能在一个网络中包含多个系统，在提示符之前可能冠以提供该命令的系统名。

[*option*] 在说明命令语法时，我们将该命令的可选择部分放在括号内，例如，**ls[-1]**意味着**-1**选项并不是必须的。

目 录

第一章　TCP/IP概述

就像价廉而功能很强的UNIX桌上计算系统问世时，要求我们中的很多人（工程师、教师、科学家和商人等）成为UNIX系统管理员一样，将这类计算机联网则要求我们能胜任网络管理员的新任务。

网络管理和系统管理是两件不同的工作。系统管理任务（如增加用户和做备份工作）仅限于一个单独的计算机系统，而网络管理却不然。一旦将计算机连接到网络上，它就要与很多其它的系统交互。执行网络管理任务的好坏不仅会影响你的系统，还会影响网络中的其它系统。因此，充分地了解基本的网络管理对每个人都有好处。

本书是有关在UNIX计算机系统中配置和管理TCP/IP网络软件的实用而渐进的指南。TCP/IP是当前控制UNIX数据通信的众多软件包中的一个，作为一个领先的UNIX局域网通信软件，它起着特别重要的作用。

TCP/IP是指一整套数据通信协议，其名字是由这些协议中的两个协议组成的，即传输控制协议（Transmission Control Protocol——TCP）和网间协议（Internet Protocol——IP）。虽然还有很多其它协议，但是TCP和IP显然是两个最重要的协议。

本书的第一部分将讨论TCP/IP的基础知识以及它是如何在网络上传输数据的，第二部分将解释如何在UNIX中配置和运行TCP/IP。首先让我们简要地回顾一下它的历史。

TCP/IP和Internet

在1969年，美国国防部高级研究计划管理署（DARPA）给一个研究和开发项目投资，以创建一个实验性的分组交换网络。该网络的名称是*ARPANET*，其目的是研究各种能提供强壮、可靠、独立于厂家的数据通信技术，现代很多数据通信技术都是在该网络中开发的。

这一实验性的ARPANET非常成功，以致与它联网的很多单位都用它进行日常的数据通信。1975年，ARPANET从一个实验性网络变成一个可运行网络，管理该网络的责任落到了国防部通信局（DCA，现已改名为国防部信息系统局DISA）的肩上。然而，ARPANET的开发工作并没有停止，因为它正被用作一个可运行网络。基本的TCP/IP协议是在ARPANET可供使用后开发的。

1983年，TCP/IP协议被用作军用标准（MIL STD），并要求所有与该网络连接的主机都采用这一新协议。为了便于这种转换，DARPA投资给Bolt、Beranek和Newman（BBN），要求在Berkeley（BSD）UNIX中实现TCP/IP，这就开始了UNIX和TCP/IP的结合。

大约在TCP/IP被作为一种标准时，Internet这一术语开始得到较普遍的使用。1983年，老的ARPANET分成MILNET（国防数据网（DDN）的无分级部分）和一个新的较小的ARPANET，术语*Internet*是指整个网络：MILNET加上ARPANET。1990年，ARPANET在形式上已不复存在，不过目前的*Internet*要比以前大得多，包括在世界各地的很多网络。

Internet已发展得大大地超过了它原来的规模。DDN是该网络的一个重要部分，像DISA这一类代理在整个网络中仍然起着重要的作用，而且一些新的网络（如NSFNET）和各种各样的地区性网络，在Internet的形成过程中起着越来越重要的作用。Internet的发展壮大吸引了很多新的组织加入到该网络中。

名词“*internet*”，最初只是用作基于网间协议构建的网络的名字；现在“*internet*”已成为用来泛指整个一类网络的代名词。“*internet*”（*i*是小写）是一些单独的物理网络通过一个公共协议互联在一起构成的一个逻辑网络的总称；“*Internet*”（*I*是大写）是世界范围内被互联在一起的所有网络的总称，它是从最初的ARPANET发展而来的，利用网间协议（*IP*）将各个物理网络连接成一个单一的逻辑网络。在本书中，无论是“internet”还是“Internet”都是指通过TCP/IP互联在一起的网络。

由于进行Internet连接需要TCP/IP，因而最近大量连接Internet的各种各样的组织已对TCP/IP感兴趣。由于越来越多的组织熟悉TCP/IP，他们认为该协议可以适用于其它的网络应用。在UNIX领域，网间协议通常用于局域网，这些局域网甚至可以不连接到大型Internet上。一般情况下，在本地以太网中采用TCP/IP通信，而与远程计算机站通信时使用UUCP。

TCP/IP的特点

TCP/IP协议在Internet上的普及速度不是很快，这是因为该协议本身就存在于Internet中，此外，一些军事单位控制着它的使用。TCP/IP协议有一些重要的特点，以确保在特定的时刻能满足一种重要的需求，即世界范围的数据通信。其特点包括：

- 开放式协议标准。可免费使用，且与具体的计算机硬件或操作系统无关。由于它受到如此广泛的支持，因而即使不通过Internet通信，利用TCP/IP来统一不同的硬件和软件也是很理想的。
- 与物理网络硬件无关。这就允许TCP/IP可以将很多不同类型的网络集成在一起，它可以适用于以太网、令牌环网、拨号线、X.25网络以及任何其它类型的物理传输介质。
- 通用的寻址方案。该方案允许任何TCP/IP设备唯一地寻址整个网络中的任何其它设备，该网络甚至可以像全球Internet那样大。
- 各种标准化的高级协议。可广泛而持续地提供多种用户服务。

协议标准

协议就是正式的行为法规。在国际关系中，当各国在一起合作时，协议可以最大限度地减少由于文化差别而引起的问题。通过签订一组公共法规，使得任何国家的客户都了解它，但又独立于任何一个国家。外交协议可以最大限度地减少误解，每个人都知道如何行动，也知道如何解释别人的行动。计算机通信亦是如此，很有必要定义一组法规去管理计算机之间的通信。

在数据通信中，这类法规也称为“协议”。在同机种网络中，单一的计算机厂家规定了一组通信规则，其目的是充分利用该厂家的操作系统和硬件体系结构的能力。但同机种网络类似单一国家的文化，只有本国公民才真正理解它。TCP/IP试图用开放式协议去构建

一个异机种网络，这种协议与操作系统和体系结构的差别无关。TCP/IP协议可供每个人使用，根据一致的意见进行开发和修改，而不是按一个厂家的命令办事。每个人都可以自由地开发符合这些开放式协议规范的产品。

TCP/IP协议的开放性质要求公开提供其标准文档，TCP/IP协议组中的所有协议已在三个Internet标准出版物中定义。若干协议已用作*军用标准（Military Standards——MIL STD）*，其它的协议则发表在*"Internet Engineering Notes（IEN）"*中。目前，IEN形式的出版物已被取消，有关TCP/IP协议的大多数信息是以*"Requests for Comments（RFC）"*的形式公开的，在RFC内包含了所有标准TCP/IP协议的最新版本规范*。顾名思义，"RFC文档"的形式和内容是不固定的，这与大多数的标准文档不一样，它包含着范围很广的各种有趣而有用的信息，并不局限于数据通信协议的法定规范。

毫无疑问，作为网络系统管理员必须亲自阅读很多RFC资料。其中有些是具体的建议和指导，很容易理解；而有些则是用数据通信专用的技术术语定义的实施规范。

数据通信模型

为了讨论计算机网络，必须使用一些在数据通信中具有特定含意的术语。由于即使是计算机专业人员也未必能熟悉全部网络术语，因为通常情况下，英语和计算机用语并不是完全等同（或完全兼容）的语言。虽然在讲述和例子中应该使得网络术语的意义较明确，但有时这些术语却是模棱两可的。因此，为了理解数据通信术语，必须建立一个共同的参考框架。

国际标准化组织（ISO）开发的一个体系结构模型被经常用来描述数据通信协议的结构和功能，该体系结构模型称为*"开放系统互连（OSI）参考模型"*，它为讨论数据通信提供了一个公用的基准。该模型所定义的各个术语很容易理解，被广泛用于数据通信领域。事实上，它使用得如此广泛，以致于离开了OSI术语就很难讨论数据通信问题。

开放系统互连参考模型包括七层，用来定义数据通信协议的多种功能。每一层表示数据在网络上传送时两个协作的应用程序间执行的一种功能。图1.1用其名字来标识每一层，并提供一个简单的说明。从图中可以看出，协议就像堆叠在一起的一堆积木块，因此，这种结构往往称为*"栈"*或*"协议栈"*。

一层并不是定义一个单独的协议，而是定义一种可以由任何数量的协议执行的数据通信功能。因此，每一层可以包含多个协议，每个协议提供一个适用于该层功能的服务。例如，一个文件传输协议和一个电子邮件协议都能提供用户服务，它们都是"应用层"的一部分。

每个协议均与其对等者（peer）通信，所谓"对等者"就是远程系统中对等层内的相同协议。例如，本地文件传输协议就是远程文件传输协议的对等者。为了成功地进行通信，必须标准化对等级别的通信，简而言之，每个协议只考虑与它的对等者通信，并不考虑高于或低于它的其它层。

然而，由于每一层都涉及将数据从本地应用程序发送到等价的远程应用程序，因此在

---

* 如果你对如何形成Internet标准感兴趣，请参考RFC 1310"Internet 标准制定程序"。

图1.1 开放系统互连（OSI）参改模型

单独一台计算机的各层之间如何传送数据必须有一个相同的约定。数据在网络上传输时，上层依赖于下层，数据沿着栈一层一层地向下传输，直到按照物理层协议在网络上传完数据为止。在远端，数据沿着栈向上一层一层传送到接收应用程序。每一层不必知道其它层是如何工作的，只需知道如何将数据发送给它们。将各种网络通信功能隔离在不同的层中，可以最大限度地减少整个协议组修改时的影响，不必修改物理网络就可增加新的应用程序，安装新的网络硬件时也不必改写应用软件。

虽然OSI模型非常有用，但TCP/IP协议并不完全与它的结构相匹配。因此，在讨论TCP/IP时，我们按下列方法使用该模型中的各层：

应用层 应用层是网络中与用户访问有关的协议层。本书中所说的TCP/IP应用程序是在传输层以上发生的任何网络进程，这包括与用户直接交互的所有进程，以及在这一层中用户不必知道的其它进程。

表示层 对于交换数据的协作应用程序来说，它们必须商定数据的表示形式。在OSI中，这一层可提供标准的数据表示例程，而在TCP/IP中，这种功能是在应用层内处理的。

会话层 与表示层一样，会话层不能看作是TCP/IP协议层次中的单独一层。OSI的会话层管理协作应用程序间的会话（连接）。在TCP/IP中，这一功能基本上是在传输层中实现的，并不使用“会话（session）”这一术语。对于TCP/IP而言，使用“软插口（socket）”和“端口（port）”来说明协作应用程序间通信的路径。

传输层 在讨论TCP/IP时，大部分内容都涉及传输层中的协议。在OSI参考模型

中，传输层可以确保接收方正确地接收到所发出的数据。在TCP/IP中，这一功能是由*传输控制协议（TCP）*完成的。然而，TCP/IP还提供了第二种传输层服务，即“*用户数据报协议（UDP）*”，它并不执行端对端的可靠性检查。

网络层 网络层管理网络上的连接，并将上层协议与底层网络的细节隔离开。网间协议（IP）通常可看作是TCP/IP的网络层，它可以将上层与基本网络隔离开，并处理寻址和数据传输功能。

数据链路层 在基本物理网络上可靠地传输数据是由数据链路层完成的。TCP/IP很少创建数据链路层中的协议，与数据链路层有关的大多数RFC只讨论IP如何使用现有的数据链路协议。

物理层 物理层定义传送数据传输信号所需的硬件特性，如电平、接口的针头和位置等都是在该层定义的。物理层中的标准有关于接口连接器的（如RS-232C和V.35）和关于局域网布线的（如IEEE 802.3）等。TCP／IP并不定义各种物理标准，它只使用现有的标准。

OSI参考模型的术语有助于描述TCP／IP，但为了能完全理解TCP／IP，我们必须采用一个能完全符合TCP／IP结构的层次模型。下一节将介绍这一协议模型。

TCP／IP协议结构

虽然没有统一规定如何用一个层次模型去描述TCP／IP，但通常将其看成是少于OSI七层模型的层次结构。在描述TCP／IP时，一般只定义该协议层次结构中的3到5个功能层。图1.2展示的4层模型是以“*DDN协议手册第一卷（DDN Protocol Handbook-Volume 1）*”中的DOD三层（应用层、主机对主机层和网络访问层）协议模型为基础的，并增加了一个单独的网间层。该模型提供了一种TCP／IP层次结构的相当形像化的层次表示方法。

图1.2 TCP／IP协议结构中的各层