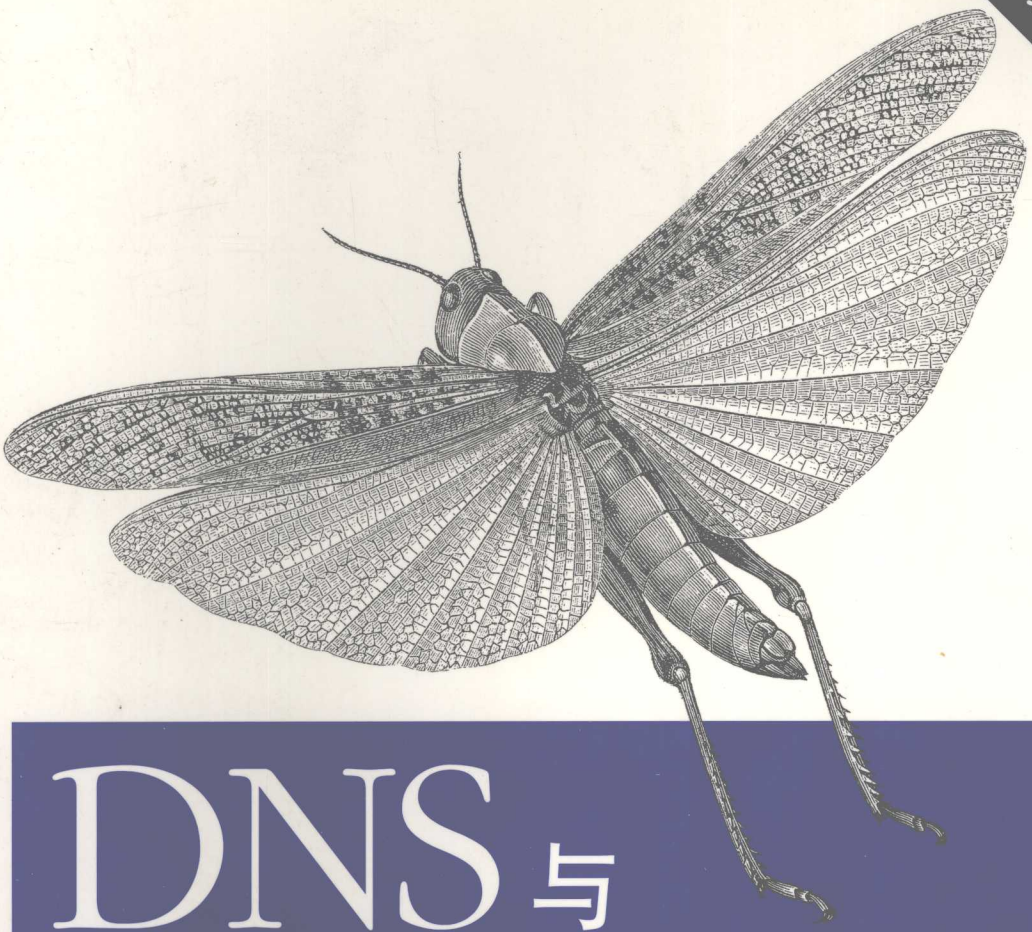
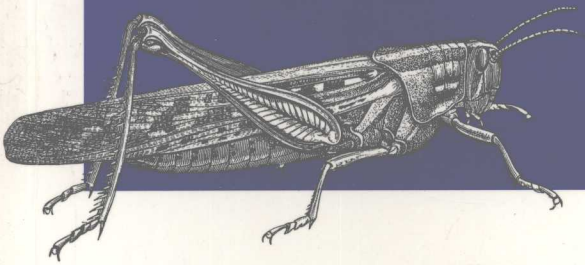
DNS and BIND

第四版
涵盖 BIND 9



DNS与BIND



O'REILLY®
中国电力出版社

Paul Albitz & Cricket Liu 著
雷迎春 龚奕利 译

DNS与BIND

第四版

Paul Albitz & Cricket Liu 著

雷迎春 龚奕利 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

O'Reilly & Associates, Inc. 授权中国电力出版社出版

中国电力出版社

图书在版编目（CIP）数据

DNS与BIND（第四版）/（美）阿尔比兹（Albitz, P.），刘（Liu, C.）著；雷迎春，龚奕利译．-北京：中国电力出版社，2002.8

书名原文：DNS and BIND, Fourth Edition

ISBN 7-5083-0980-4

I. D... II. ①阿... ②刘... ③雷... ④龚... III. 网络服务器 IV. TP368.5

中国版本图书馆CIP数据核字（2002）第053051号

北京市版权局著作权合同登记

图字：01-2002-2274号

书　　名/ DNS与BIND（第四版）

书　　号/ ISBN 7-5083-0980-4

责任编辑/ 程璐

封面设计/ Edie Freedman，张健

出版发行/ 中国电力出版社（www.infopower.com.cn）

地　　址/ 北京三里河路6号（邮政编码100044）

经　　销/ 全国新华书店

印　　刷/ 北京市地矿印刷厂

开　　本/ 787毫米×1092毫米　16开本　42印张　633千字

版　　次/ 2002年8月第一版　2002年8月第一次印刷

印　　数/ 0001-5000册

定　　价/ 69.00元（册）

O'Reilly & Associates 公司介绍

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 & Associates公司授权中国电力出版社，翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly & Associates 公司是世界上在 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 & Associates 一直处于Internet 发展的最前沿。

许多书店的反馈表明，O'Reilly & Associates 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 & Associates 公司具有深厚的计算机专业背景，这使得O'Reilly & Associates形成了一个非常不同于其他出版商的出版方针。O'Reilly & Associates 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 & Associates 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 & Associates 依靠他们及时地推出图书。因为O'Reilly & Associates 紧密地与计算机业界联系着，所以O'Reilly & Associates 知道市场上真正需要什么图书。

作者简介

Paul Albitz 现为惠普公司的软件工程师。他获得了威斯康星大学理学学士学位和普渡大学的理学硕士学位。

Paul从事与HP-UX 7.0和8.0有关的BIND工作。工作期间，Paul开发了用于管理hp.com域的工具。此后，Paul就一直做着惠普DesignJet绘图仪互联和惠普的OfficeJet多功能传真子系统的工作。加盟惠普之前，Paul在普渡大学计算机系担任系统管理员。作为系统管理员，Paul使用了比与4.3 BSD一起发行的BIND更早版本的BIND。现在，Paul与他的妻子Katherine住在加州圣迭戈。

Cricket Liu 就读于加州伯克利分校，那里是自由演讲的阵营，有不受限制的Unix和便宜的比萨饼。他毕业后开始为惠普公司工作，一口气干了九年。

Cricket在Loma Prieta地震后开始管理*hp.com*域。地震使得域的管理不得不从惠普的实验室搬到公司的办公室。他担任*hostmaster@hp.com*三年多，然后加入惠普的专业服务组织，创建了惠普的Internet咨询流程。

1997年，Cricket离开惠普，并和他的朋友（现在的合著者）Matt Larson组建了Acme Byte & Wire，一个DNS咨询和培训公司。Network Solutions在2000年6月收购了Acme，并在同一天与VeriSign合并。Cricket现在是VeriSign全球注册服务的DNS产品管理主任。

Cricket和他的妻子Paige、儿子Walt以及两只爱犬Annie和Dakota住在科罗拉多州。在暖暖的周末下午，你也许能够看到他们正在荡秋千。

封面介绍

本书封面上的昆虫是蝗虫，它们遍及世界的每个角落。在北美5000多种昆虫中，蝗虫有100多种。蝗虫呈褐绿色，体长从0.5英寸到4英寸不等，翼展可达6英寸。它们的身体分为三部分：头、胸和腹部。

雄性蝗虫用后腿和前翅发出一种“唧唧”的声音。它们的后腿上有一排小的突起，摩擦前翅上硬化的血管，产生的震动听起来就像拉动弓弦的声音。

蝗虫是主要的田间害虫，特别是当它们成群结队的时候。一只蝗虫每天消耗30毫克的食物。如果蝗虫的密度为每平方码50只及以上时（爆发蝗灾时通常能达到这个密度），每英亩蝗虫的消耗同一头牛的消耗相当。除了侵食叶子外，蝗虫还袭击植物柔弱的部位，导致茎干折断，破坏植物的生长。

目录

前言

到目前为止，你可能仍然对DNS（Domain Name System，域名系统）所知甚少，但是无论你何时使用Internet，都会用到DNS。每次发送电子邮件或是在网上冲浪，你都必须依赖DNS。

作为普通人，我们都宁愿记计算机的名字，而计算机却喜欢用数字（即，主机IP地址）来彼此称呼。在互联网络上，这样的地址是一个32位的数字，或者说是一个介于0到大约40亿之间的数字（注1）。对于计算机来说这是很容易记住的，因为计算机的内存很适合存储数字，而对于我们人来说这就不那么好记了。从电话簿中随机挑出10个电话号码，试试记住它们。不容易吧？然后在每个电话号码前加上随机的区号，这就和记住10个任意的互联网络地址差不多难了。

这就是我们需要DNS的部分原因。DNS负责主机名字之间和互联网络地址之间的映射，前者我们人类会觉得很方便，而后者是由计算机来处理的。实际上，DNS是Internet上的一个标准机制，用来发布和访问关于主机的各种信息，而不只是地址。实际上几乎所有的网间互联软件都在使用DNS，包括电子邮件、远程终端程序（如，Telnet）、文件传输程序（如，FTP）以及Web浏览器（如，网景的Navigator和微软的Internet Explorer）。

注1：对于IPv6而言，它很快就是128位长的了，也就是介于0到一个39位的十进制数之间。

DNS的另一个重要特性就是它使主机信息在Internet上随处可得。将主机信息按照某种格式存为文件，放在某台计算机上，并只对那台计算机的用户有用。DNS则提供了一种远程检索信息的方式，你能从网络上任何一个地方查找信息。

除此之外，DNS还能将主机信息的管理分布到许多地点和组织。你不需要将数据提交给某个中心，或定期地检索中心的数据库，你只要保证你的名字服务器（name server）上称为区（zone）的那一部分是最新的即可。你的名字服务器会使网络上其他的名字服务器都能访问到你区中的数据。

因为数据库是分布式的，所以系统还需要能够通过搜索一些可能的位置来确定你要查找的数据在哪里。DNS使得名字服务器能够很聪明地在数据库之中查找，并找到任何区中的数据。

当然，DNS也有一些问题。例如，出于冗余考虑，系统允许多个名字服务器存储一个区的同样数据，这就会引发这些服务器上区数据之间的一致性问题。

不过关于DNS最糟糕的问题则是尽管它在Internet上广泛使用，却很少有关于如何管理和维护DNS方面的资料。Internet上大多数管理员使用的是商家认为应该提供的资料，再就是从相关领域的Internet邮件列表和Usenet新闻组中搜集到的一些信息。

缺乏资料就意味着，对这种当今Internet上最关键的服务的理解要么是从一个管理员传授给另一个管理员，就像祖传秘方；要么是从一个个互不相识的程序员和工程师那里重复搜集取得，并且新的系统管理员犯着无数人犯过的错。

我们写这本书的目的就是为了帮助解决这一问题。我们意识到你们当中并非所有人都想成为DNS专家。毕竟，大多数人除了管理一个区或名字服务器之外还有许多其他事情要做：系统管理、网络工程或软件开发。要一个人只负责DNS是不可想像的。我们会试着给你足够的信息，让你无论是运行一个小的区还是管理一个跨国的庞然大物，无论是照顾一个名字服务器还是管理上百个名字服务器，都只做需要做的事。你可以现在需要知道多少就读多少，等需要知道更多的时候，再回来接着读。

DNS是个很大的话题——至少大到需要两个作者，不过我们会尽力使它易于理解。本书的前两章是理论上的概述以及一些实际信息，余下来的章节讲的都是些核心细节。我们首先提供了一个路线指南，有了它，你可以根据自己的工作或兴趣选择合适的学习路线。

谈到实际的DNS软件时，我们主要讲的是BIND（Berkeley Internet Name Domain）软件，它是DNS规范的一种最为常见的实现（也是我们所知道的最好的）。我们尽力将自己使用BIND管理和维护区的经验浓缩在本书当中。（我们所管理的一个区曾经是Internet上最大的区，不过那已经是很久以前的事了。）只要有可能，我们就会给出在管理中实际用到的程序，为了提高速度和效率，其中许多都用Perl重写了。

如果你还是个新手的话，我们希望本书能帮助你熟悉DNS和BIND；如果你已经对DNS有所了解，我们希望能增进你的理解。即使你对DNS已经了如指掌，我们还是希望能给你一些有价值的见解和经验。

版本

本书的第四版主要是讲新的9.1.0和8.2.3版的BIND，同时也涉及较早的4.9版。虽然9.1.0和8.2.3是我们撰写本书时最新的BIND版本，但是许多供应商的Unix版本中还不包括它们，部分原因是由于这两个版本最近才刚刚发布，同时也因为许多供应商对于使用这些新软件还是抱着小心谨慎的态度。我们也会偶尔提到其他版本的BIND，特别是4.8.3版，因为许多供应商的Unix产品中包括的代码还是基于这个老版本的BIND。如果某个特性只适用于4.9、8.2.3或9.1.0版，或者在不同版本中使用情况有所不同的话，我们将会分别讨论各种版本。

我们在例子中大量使用了*nslookup*这种名字服务器实用程序。我们所使用的*nslookup*是同BIND 8.2.3代码封装在一起的那个版本。较早版本的*nslookup*也提供了8.2.3中*nslookup*大部分的功能，不过并非全部（注2）。在例子中，我们尽量使用对大多数*nslookup*都通用的命令，如果无法做到这一点，会特别注明的。

第四版新增加的内容

除了更新内容以涵盖最新的BIND版本之外，在第四版中我们还增加了相当多的新东西：

注2：在BIND 9中封装的*nslookup*版本也是如此。详情请见第十二章。

- 更多的动态更新和NOTIFY内容，包括带签名的动态更新和BIND 9当中新的更新策略（update-policy）机制，参见第十章。
- 增量区传送（incremental zone transfer），参见第十章。
- 支持条件转发的转发（forward）区，参见第十章。
- 使用新的A6和DNAME记录以及位串标号的IPv6正向和反向地址映射，参见第十章的最后部分。
- 一种新的事务认证机制——事务签名（transaction signature），又称为TSIG，参见第十一章。
- 扩展了保护名字服务器安全的部分，参见第十一章。
- 扩展了有关Internet防火墙的部分，参见第十一章。
- 包括了一种新的对区数据进行数字签名的机制——DNS安全性扩展（DNS Security Extension），简称DNSSEC，参见第十一章。
- 专门有一节讲述Windows 2000客户机、服务器和域控制器（Domain Controller）与BIND的兼容问题，参见第十六章。

组织

本书的内容或多或少是按照区及其管理员的不断发展过程来组织的。第一、二章讨论了关于DNS的理论。第三章到第六章帮助你决定是否要建立你自己的区，还讲述了如果选择建立了自己的区，又该如何来做。中间的几章，第七章到第十一章讲的是如何维护区、如何配置主机使之使用指定的名字服务器、如何规划区的发展、如何创建子域，以及如何保护名字服务器。最后几章，第十二章到第十六章，讲的是一些有关排错工具、常见问题，以及使用解析器库例程编程的技术和技巧。

下面是关于每一章更详细的介绍：

- 第一章“背景”，提供了一些历史资料，讨论促使DNS发展的问题，然后是DNS理论的概述。
- 第二章“DNS是如何工作的？”，更详细地回顾了DNS理论，包括DNS名字

空间、域、区和名字服务器的组织。另外还介绍了一些很重要的概念，比如名字解析和缓存。

- 第三章“我该从哪里开始？”，谈到了如果你还没有DNS软件的话，该如何获取BIND，以及得到之后又该怎么办：如何确定你的域名是什么，以及如何同区的授权组织联系。
- 第四章“建立BIND”，详细介绍了如何建立你的头两个BIND名字服务器，包括创建你的名字服务器数据库、启动你的名字服务器和检查它们的操作。
- 第五章“DNS和电子邮件”，讲的是DNS的MX记录，它允许管理员指定其他主机来处理发往给定目的主机的邮件。这一章涉及对各种网络和主机的邮件路由策略，包括有Internet防火墙的网络和没有直接连到Internet的主机。
- 第六章“配置主机”，解释了如何配置一个BIND解析器。我们还将注明许多常见Unix厂商的解析器实现的特性，同时还会谈到Windows 95、NT和2000的解析器。
- 第七章“维护BIND”，讲述了为保证区的平稳运行，管理员所需要做的定期维护工作，比如说检查名字服务器是否正常以及它的授权状况。
- 第八章“扩展你的域”，涉及了如何规划和发展你的区，包括如何扩大、如何为移动用户和故障做准备。
- 第九章“担当父域”，探讨了成为父区的快乐。我们解释了何时成为一个父区（创建子域）、如何命名你的孩子以及如何创建（!）和监控它们。
- 第十章“高级特性”，讲述了一些不太常用的名字服务器配置选项，它们能帮助你优化名字服务器的操作，使管理更轻松。
- 第十一章“安全”，讲述了如何保护名字服务器，以及如何配置名字服务器同Internet防火墙一起工作，此外还讲述了DNS的两个新增的安全性功能：DNS安全性扩展和事务签名。
- 第十二章“nslookup和dig”，详细介绍了最常用的调试DNS的工具，包括从远程名字服务器挖掘模糊信息的技术。
- 第十三章“阅读BIND的调试输出”，这些输出开始时就像是罗赛塔石碑上的文字那样神秘。这一章将会有助于你理解那些BIND显示的神秘信息的意义，从而使你能更好地了解名字服务器。