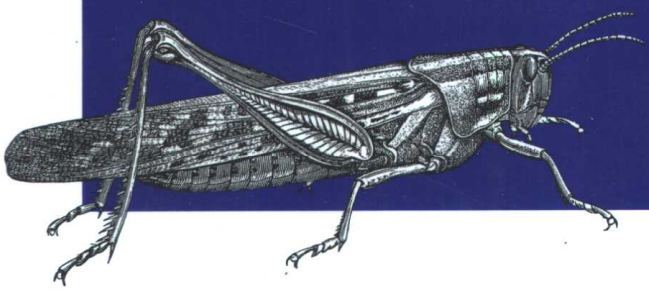
DNS and BIND

第三版
内含 BIND 8

DNS与BIND



O'REILLY®
中国电力出版社

Paul Albitz & Cricket Liu 著
雷迎春 陈世林 杨传军 译

DNS与BIND

第三版

Paul Albitz & Cricket Liu 著

雷迎春 陈世林 杨传军 译

O'REILLY®

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

中国电力出版社

图书在版编目（CIP）数据

DNS与BIND/（美）阿尔比兹（Albitz, P.）、刘（Liu, C.）著；雷迎春等译. -北京：中国电力出版社，2001.1

书名原文：DNS and BIND

ISBN 7-5083-0231-1

Ⅰ.D… Ⅱ.①阿… ②刘… ③雷… Ⅲ.网络服务器 Ⅳ.TP393.09

中国版本图书馆CIP数据核字（2000）第76726号

北京市版权局著作权合同登记

图字：01-1999-3743号

书　　名/ DNS与BIND

书　　号/ ISBN 7-5083-0231-1

责任编辑/ 刘江

技术审校/ 孙国念

封面设计/ Ellie Volckhausen，Hanna Dyer，张健

出版发行/ 中国电力出版社

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　35.75印张　580千字

版　　次/ 2001年1月第一版　2001年1月第一次印刷

印　　数/ 0001-5000册

定　　价/ 59.00元（册）

DNS与BIND

目录

前言

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

作为人，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）来称呼彼此。在互联网络上，这样的地址是一个32位的数字，或者说是介于0到大约40亿之间的一个数字（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。真的不好记吗？现在请翻开一本电话簿，任意将一些区号和电话号码连起来。记住它们，就和记住十个任意的互联网络地址差不多难。

这就是我们需要DNS的部分原因。DNS是用于处理方便我们人类使用的主机名字和由计算机来处理的互联网络地址之间的映射。实际上，DNS是Internet上一个标准机制，用来发布和访问有关主机的各种信息，而不只是地址。而且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：　而对于IP version 6而言，它很快就会是128位长了，或者说是介于0到一个39位的十进制数字之间。

DNS另一个重要特性就是它使得从Internet上任何地方都能获得主机的信息。将主机信息按照某种格式存成文件，放在某台计算机上，只能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。

还不止这些，DNS使你能对许多场所和机构中的主机信息进行分布式管理。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，只保证名字服务器（name server）上称为区（zone）的部分是最新的就行。你的名字服务器会使网络上其他的名字服务器都能访问你区中的数据。

因为数据库是分布式的，所以系统还需要能够通过搜索一定的位置来确定要查找的数据在哪里。域名系统使得名字服务器能够很聪明地在数据库之中查找，找到任何区中的数据。

当然，DNS也有它的问题。例如，为了冗余，系统允许不止一个名字服务器存储一个区的同样的数据。但是这就会导致这些区数据之间的一致性问题。

不过，关于DNS最糟糕的问题是，尽管它在Internet上广泛使用，但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厂家认为应该提供的资料，再就是从有关这个问题的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，对这种非常重要的互联网络服务 —— 今天Internet的关键之一 —— 的理解要么是从一个管理员传授给另一个管理员，就像一个保守严密的家族秘方；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。新的系统管理员重犯着无数人犯过的错误。

我们写这本书的目的就是为了帮助解决这一状况。我们意识到你们当中并非所有人都想成为DNS的专家。毕竟，你们中的大多数除了管理一个域（domain）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是完全不可想像的。我们会试着给你足够的信息，让你无论是运行一个小的域还是管理一个跨国的大家伙，无论是负责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。现在你想知道多少，就读多少，如果你想知道更多，可以返回来继续读。

DNS是个很大的话题——至少大到需要两个作者——但是我们将试着尽可能讲得通俗易懂。头两章是从理论上概述，并且让你了解一些实用的信息，余下来的章节讲的都是核心细节。我们在开始的时候提供了一个路线指南，它根据你的工作或兴趣向你建议适合的阅读路线。

当我们谈到实际的DNS软件时，我们主要讲的是BIND，即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）。我们力图在本书中精心提炼我们在用BIND管理和维护域当中的经验——顺便说一句，这个域可能是Internet上最大的一个（不是吹牛，我们有这样的把握）。只要有可能，我们就会给出在管理中实际用到的程序，为了速度和效率，其中许多都用Perl进行了重写。

如果你还是个生手的话，我们希望这本书能帮助你熟悉DNS与BIND，如果你已经熟悉了DNS，我们希望它能增进你的理解。即使你对DNS已经了如指掌，我们还是希望能提供一些有价值的理解和经验。

版本

这本书主要是讲新的8.1.2版的BIND，同时也涉及了早一点的4.9版。虽然8.1.2是我们撰写这本书时最新的BIND版本，但许多供应商的UNIX版本中还不包括它，部分是由于8.1.2只是最近才刚刚发布，同时许多供应商对于使用这么新的软件还很谨慎。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较老版本的BIND的。要是一个特性只适用于4.8.3、4.9或者8.1.2版，或者在不同版本的使用情况有所不同的话，我们将会指出不同版本的不同使用情况。

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*的版本是随同BIND 8.1.2代码一起提供的。较早版本的*nslookup*也提供了8.1.2中*nslookup*大部分的功能，不过并非全部。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，我们会注明的。

组织

本书或多或少是按照域和域管理员的发展历程来组织的。第一、二章讨论了域名系统理论。第三章到第六章帮助你决定是否建立你自己的域，还讲述了如果你选择建立自己的域，又该如何来做。中间的几章，第七章到第十章讲的是如何维护你的域，如何配置主机以使用你的名字服务器，如何规划你的域扩展，以及如何创建子域。最后几章，第十一章到第十五章，讲述一些排错工具和常见问题，以及使用解析器库例程编程的技术和技巧。

下面是每一章更详细一些的介绍:

- 第一章“背景”，提供了一些历史资料，讨论了导致DNS发展的问题，然后还概述了DNS理论。
- 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、域和名字服务器。我们还介绍了一些很重要的概念，像名字解析（name resolution）和缓存（caching）。
- 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，以及一旦你得到了又该怎么办：如何确定你的域名是什么，以及如何同域的授权组织联系。
- 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，它允许管理员指定别的主机来处理发往给定目的主机的邮件。这一章涉及了对各种网络和主机的邮件路由策略，包括有安全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（resolver）。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和NT的解析器。
- 第七章“维护BIND”，讲述了为保证一个域的平稳运行管理员所需要做的定期维护的工作，如检查名字服务器是否正常，以及它的授权情况。

- 第八章“扩展你的域”，涉及的是如何规划扩大和发展你的域，包括如何扩大和如何为移动和出错做准备。
- 第九章“担当父域”，探索了成为父域的乐趣。我们解释了何时成为一个父域（创建子域），如何命名你的子域，如何创建它们，以及如何监视它们。
- 第十章“高级特性和安全性问题”，讲述了一些较少用到的名字服务器配置选项，它们能帮助你优化你的名字服务器的操作，使你的名字服务器更安全，还能使你的管理更轻松。
- 第十一章“nslookup”，详细介绍了最常用的调试DNS的工具，包括挖掘远程名字服务器给出的模糊信息技术。
- 第十二章“理解BIND调试的输出”，这些输出开始时就像是罗赛塔石碑上的文字（译注1）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你的名字服务器。
- 第十三章“DNS和BIND疑难排错”，涉及了许多常见的DNS和BIND问题及其解决方法，然后还讲述了一些不太常见、较难诊断的情况。
- 第十四章“用解析器和名字服务器库例程编程”，演示了如何在一个C程序中使用BIND的解析器例程，来查询名字服务器并从中检索数据。我们还包括了一个有用的程序（希望如此!），它可以用来检查你的名字服务器正常与否以及授权情况。
- 第十五章“其他问题”，将所有松散的头绪连在一起。我们讲到了DNS通配符、通过防火墙连接到Internet网络的特殊配置、通过拨号断断续续地连接到Internet的主机和网络、网络名字编码，还有新的试验性的记录类型。
- 附录一“DNS消息格式和资源记录”，包括一个字节一个字节地分解了DNS查询和响应中使用的格式，另外还有当前定义的资源记录类型的综合列表。
- 附录二“在Sun主机上编译和安装BIND”，包含了关于如何在Solaris 2.X上编译和安装8.1.2版BIND的一步一步的指令。

译注1：罗赛塔碑是1798～1799年拿破仑远征埃及期间，法军发现的埃及古碑。由于碑文同时刻有古埃及象形文字、通俗体文字和希腊文，它成为法国古文字学家商博良破译古埃及象形文字的关键线索。

- 附录三“顶级域”，列出了目前Internet域名空间中的顶级域名。
- 附录四“域注册表”，是目前申请建立一个由InterNIC运行的子域的表格。
- 附录五“in-addr.arpa注册表”，是American Registry for Internet Numbers目前申请建立一个*in-addr.arpa*域的子域的表格。
- 附录六“BIND名字服务器和解析器语句”，总结了用来配置名字服务器和解析器的每一个参数的语法和语义。

读者

本书主要是为管理一个域和一个或多个名字服务器的系统管理员而写的，但是它也适合于网络工程师、邮件管理员以及其他一些人。不过，不同的读者对各个章节的兴趣大小并不一样，你不一定要读完所有的十五章才找到与你工作相关的信息。我们希望下面的阅读指南能帮助你找到自己的阅读路线。

第一次建立自己域的系统管理员要了解DNS的理论，应该读第一、二章；要了解开始和选择一个好域名，应该读第三章；要学习第一次如何建立域，应该读第四章和第五章。第六章解释了如何配置主机来使用新的名字服务器。接下来他们就该读第七章了，这一章介绍了如何通过建立其他的名字服务器和添加附加数据，使他们的域“有血有肉”。然后是第十一、十二和十三章，讲述了排错工具和技术。

有经验的管理员读读第六章，能够学习如何在不同的主机上配置DNS解析器，读第七章能学习维护域方面的知识。第八章包含有如何为域的扩大和发展做准备，这对于大域的管理员更有价值。第九章解释了成为父域——创建子域——这对考虑要进行大的移动的管理员来说是很应该看一看的。第十章涉及了新的BIND 8.1.2名字服务器的安全特性，其中许多对有经验的管理员来是也是很有用的。第十一到十三章描述了排错的工具和技术，即使是对高级管理员来说也是值得一读的。

没有完全连接到Internet的网络的系统管理员应该读一读第五章，学习一下如何在这类网络上配置邮件，还应该读一读第十五章，学习一下如何建立一个独立的DNS基础设施。

程序员应该读一下第一、二章，了解一下DNS，然后是第十四章，其中详细介绍了如何使用BIND解析器库例程编程。

不直接负责域的网络管理员还是应该读一下第一、二章，了解一下DNS理论，然后是第十一章，学习如何使用nslookup，及第十三章，学习排错技巧。

邮件管理员应该读第一、二章，了解一下DNS理论，还有第五章，学习DNS和电子邮件是如何共存的。第十一章描述了*nslookup*，这将有助于邮件管理员从域名空间中挖掘出邮件路由信息。

感兴趣的读者可以读一读第一、二章，学习DNS理论，除此之外，想读什么就读什么吧!

注意，我们假设你很熟悉基本的UNIX系统管理以及TCP/IP网络工作原理，并能够使用简单的Shell脚本和Perl来编程。除此之外，我们不要求您有任何其他专业的知识。当我们提到一个新的术语或概念的时候，我们会尽力定义或解释的。只要可能，我们将与UNIX（以及现实世界）相比较，来帮助你理解。

获取示例程序

本书中的示例程序可以通过*ftp*从下面的网址获得:

ftp://ftp.uu.net/published/oreilly/nutshell/dnsbind/dns.tar.Z
ftp://ftp.ora.com/published/oreilly/nutshell/dnsbind/dns.tar.Z

无论你从何处下载，都要输入以下命令来解开压缩文件:

```
% zcat dns.tar.Z | tar xf -
```

系统V中则要求输入下面的tar命令:

```
% zcat dns.tar.Z | tar xof -
```

如果你的系统上没有*zcat*，可以分别使用*uncompress*和*tar*命令。

如果你不能直接通过Internet得到这些例子，但可以收发邮件，你可以用*ftpmail*来获取它们。要想了解如何使用*ftpmail*，发送电子邮件到*ftpmail@online.oreilly.com*，不用写主题，只用在正文中写一个单词“help”。

本书中所使用的约定

我们用下面所示的字体和格式惯例来表示UNIX命令、工具和系统调用：

- 脚本或配置文件的摘录以固定宽度的字体来显示：

```
if test -x /etc/named -a -f /etc/named.conf
then
    /etc/named
fi
```

- 简单的交互式会话的例子，命令行输入和相应的输出，是以固定宽度的字体来显示的，其中需要用户输入的用黑体显示：

```
% cat /etc/named.pid
78
```

- 如果命令必须由超级用户输入，那么我们在前面使用#符号：

```
# /etc/named
```

- 当命令行正好作为用户输入出现时，如果在段落中就用斜体表示。例如：运行*ls*来列出一个目录中的文件。
- 当域名在段落中出现时也用斜体表示。
- 在一段文字中出现的UNIX命令（只是随便提到，而不是作为命令行的一部分时）和UNIX联机手册，也用斜体表示。例如：想找到关于*named*的更多信息，用户可以求助于*named*（1m）的联机手册。
- 文件名用斜体印刷；例如：BIND名字服务器的配置文件通常是*/etc/named.conf*。