DNS on Windows NT

DNS

—*Windows NT*版

Paul Albitz, Matt Larson & Cricket Liu 著

雷迎春 译

O'REILLY®

中国电力出版社

DNS —Windows NT版

Paul Albitz, Matt Larson & Cricket Liu 著

雷迎春 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 — Windows NT 版 /（美）阿尔比兹（Albitz, P.）、拉尔森（Larson, M.）著；雷迎春译 . - 北京：中国电力出版社，2001. 1

书名原文：DNS on Windows NT

ISBN 7-5083-0455-1

Ⅰ .D … Ⅱ . ①阿 … ②拉 … ③雷 … Ⅲ . 服务器 - 操作系统，Windows NT DNS Server Ⅳ .TP316.7

中国版本图书馆 CIP 数据核字（2000）第 56110 号

北京市版权局著作权合同登记

图字：01-2000-3336 号

书　　名 / DNS — Windows NT 版
书　　号 / ISBN 7-5083-0455-1
责任编辑 / 刘江
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　24.25 印张　365 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 / 39.00 元（册）

DNS —Windows NT版

作者简介

Paul Albitz 是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度大学的理学硕士学位。

Paul 从事与 HP-UX7.0 和 8.0 有关的 BIND 方面的研究。在这一时期，Paul 开发了用于运行 hp.com 域的工具。从那时起，Paul 就一直从事惠普 DesignJet 绘图仪联网和 OfficeJet 多功能传真子系统。加盟惠普之前，Paul 在普度大学计算机系担任系统管理员。作为系统管理员，Paul 在 BIND 最初与 4.3BSD 同时发布之前就开始用 BIND 了。现在 Paul 与他的妻子 Katherine 住在加州圣地亚哥。

Matt Larson 与 Criket Liu 于 1997 年 1 月创建了 Acme Byte & Wire，一个专业的 DNS 咨询培训公司。此前，他供职于惠普公司，先是作为 Criket 的继任者，负责 hp.com 域，然后在惠普的专业服务组中任咨询专家。

Matt 于 1992 年毕业于西北大学，获得了计算机和音乐两个学士学位。他与妻子 Sonja Kahler，以及两条哈巴狗，住在马里兰州的 Bethesda 市。业余时间他喜欢在家里演奏 10 阶管风琴，或者驾驶轻型飞机。

Cricket Liu 就读于加州大学伯克利分校，那里是自由演讲的阵地，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，一直干了九年。

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。他担任主机管理员(hostmaster@hp.com)三年多，然后加入惠普的专业服务组织，他创建了惠普的 Internet 咨询项目。

Cricket 目前还和他的朋友兼合著者 Matt Larson 一起经营着自己的 Internet 咨询和培训公司——Acme Byte & Wire。

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。

译者简介

雷迎春 1995年毕业于武汉大学计算机科学系计算机软件专业，获学士学位。1998年毕业于武汉大学计算机科学系计算机体系结构专业，获硕士学位。1998年9月至今，在中国科学院计算技术研究所攻读博士学位。他曾经就DNS发表过多篇论文。

过去的研究方向为QoS、网络流量分析、网络工程、网络安全。曾参加北京市北辰高速宽带多媒体综合信息网的Internet平台和网络平台的建设。目前研究兴趣为ScalaServer、分布式Web处理、操作系统等。

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Microsoft DNS Server，它是DNS规范说明的一种比较常见的实现，包括在Windows NT Server 4.0及其以后的版本。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NT上的DNS，如果你已经熟悉了DNS，我们希望它能增进你的理解，而即使你对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

本书讲的是运行在Windows NT Server版本4.0上的DNS服务器，特别是Microsoft DNS Server。由于这个版本的Microsoft DNS Server是封装在NT Server 4.0中的，里面有一些bug，所以我们主要讲的是微软在Service Pack 3作为热修补之后发布的版本（注2）。我们偶尔还会提到运行在NT上的其它DNS服务器，特别是BIND的移植，BIND也是DNS规格说明的一个很常见的实现。不过，如果你需要一本专门讲BIND的书，我们会推荐本书的姐妹篇，《DNS and BIND》（译注1）。本书实际上就是《DNS and BIND》的Windows NT版本。

我们在例子中大量使用了*nslookup*这种名字服务器的实用程序。我们所使用的*nslookup*的版本是同Windows NT Server 4.0封装在一起的那个版本。其它版本的*nslookup*也提供了同NT中*nslookup*相似的功能。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。

注2：关于如何获取刻该服务器软件，见第三章“我该从哪里开始？”

译注1：该书第三版的中文简体版《DNS与BIND》已由中国电力出版社于2000年11月出版。

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，以及如何创建子域。最后几章，第十一章到第十三章，是关于一些常见的问题和排错的工具。

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，讨论了引起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，该如何选择和获得它，以及一旦你得到了又该怎么办：如何确定你的域名，以及如何同域的授权组织联系。
- 第四章“建立Microsoft DNS Server”，详细介绍了如何建立你的头两个名字服务器，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Windows解析器。
- 第七章“维护Microsoft DNS Server”，讲述了为保证一个域的平稳运行，管理员应该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“DNS疑难排错”，涉及了许多常见的DNS问题以及它们的解决方法，然后还讲述了一些不太常见、较难分析的情况。
- 第十三章“其它问题”，将一些松散的头绪连在一起。我们讲到了DNS通配符、提供防火墙连接到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“从光盘安装DNS Server”，描述了如何从Windows NT的光盘加载Microsoft DNS Server。
- 附录三“从BIND转换到Microsoft DNS Server”，涉及的是从现有的BIND 4转换到Microsoft DNS Server。
- 附录四“顶级域”，列出了目前Internet域名空间中的顶级域名。
- 附录五“域注册表”，是目前申请建立一个由InterNIC运行的子域的表格。
- 附录六“in-addr.arpa注册表”，是American Registry for Internet Numbers的目前申请建立一个in-addr.arpa域的子域的表格。
- 附录七“Microsoft DNS Server注册表设置”，描述了如何使用Windows NT注册表来自定义DNS Server的操作。

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Windows NT系统管理员而写的，但是它也适合于网络工程师、邮件管理员以及其它一些人。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十三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”。然后是第十一和十二章，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。第九章解释了如何来成为父域 —— 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Microsoft DNS Server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。第十一和十二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，还应该读一读第十三章，学习一下如何建立一个独立的DNS基础设施。

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，及第十二章，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!