Windows 技术丛书

Windows

2000

(美) Roger Abell Andrew Daniels
Herman Knief Jeffrey Graham 著
陈海涛 岳 虹 田艳芳 等译

Windows 2000 DNS 技术指南

Windows 2000 DNS 技术指南

机械工业出版社
China Machine Press
New Riders

本书全面讲述了Windows 2000 DNS系统的设计和配置，讨论的主题主要包括：设计和确保DNS服务、计划互操作性、DNS系统与DNS系统的集成、安装和使用DHCP和WINS服务以及Windows 2000活动目录等。

本书是Windows用户、系统管理员和网络设计师必读的关于域名系统的参考书。UNIX系统管理员也可从中获取足够信息，以使UNIX的DNS服务器可以与Windows的DNS系统协同工作。

本书版权登记号：图字：01-2000-1568

图书在版编目（CIP）数据

Windows 2000 DNS技术指南 /（美）阿贝尔（Abell, R.）等编著；陈海涛等译．－北京：机械工业出版社，2000.11

（Windows 技术丛书）

书名原文：Windows 2000 DNS

ISBN 7-111-07571-4

I. W… II. ①阿… ②陈… III. 服务器－操作系统（软件），Windows 2000 IV.TP316.86

中国版本图书馆CIP数据核字（2000）第47465号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：陈 谊

北京昌平第二印刷厂印刷 · 新华书店北京发行所发行

2000年11月第1版第1次印刷

787mm × 1092mm 1/16 · 19.25印张

印数：0 001- 5 000册

定价：32.00元

译 者 序

网络管理员必须正确地配置域名系统（DNS），只有这样网络用户才能顺利地访问Internet。在一个大型组织的内部网中，DNS服务也是必不可少的。尤其在Windows 2000操作系统中，将DNS的重要性提到了前所未有的高度。但是讨论DNS的书籍实在是太少了。

本书是一本专为Windows 2000 系统管理员和网络设计师撰写的使用手册，专门讨论了DNS系统的设计和配置。作者依据多年的实际工作经验，为网络管理员提供了许多第一手的资料，用来设计、安装和配置可靠和安全的Windows 2000 域名系统。

在Windows环境下，除了DNS系统以外，还存在另外一个传统的名字系统——WINS，可以用来查找和解析Windows计算机。本书对WINS系统也做了比较详细的讨论。此外，还讨论了DNS系统和WINS系统的集成，从而使网络管理员不仅能正确地使用DNS系统，也能充分利用WINS系统。

本书还介绍了Windows 2000 引进的活动目录的概念，重点介绍了DNS与活动目录的集成、它们的相互影响以及带来的一些新问题。在讨论中作者给出了许多好的建议和立即可用的解决方案。

UNIX系统管理员也能从本书中得到足够的信息，以使UNIX的DNS服务器可以和Windows 2000 的DNS系统协同工作。

本书是Windows 2000 网络管理员和设计师必读的关于域名系统的参考书，并可以作为有关培训班的教材，也是其他网络管理员和希望深入了解Windows 2000 系统管理的计算机爱好者难得的参考书。

参加本书翻译工作的还有曲向丽、鲁云、蒋瑜、晏小波、余海洲、岳霞、刘海波等，在此表示感谢。由于译者水平有限，书中难免有疏漏之处，尽请批评指正。

译 者

前　言

多年以来，DNS系统像胶水一样将全世界的网络粘成一个有凝聚力的通信网格。DNS并非停步不前，而是不断地修改以满足新的需求和迎接挑战，这些需求和挑战来自于Internet的飞速增长和Internet的许多新的以及正在出现的用途。

从根本上来说，DNS是一个允许通过友好的名字连接世界上任一台计算机的巨大的索引。域名系统在Internet中的作用就像电话号码簿在电话系统中的作用一样重要，但DNS是一个分布式系统，好像电话号簿的A部分在菲尼克斯、B部分在伦敦、C部分在东京等。

从90年代中期以来，DNS在某些方面已有所加强。增加了更有效的分布数据的方法，还定义了自动登录和数据更新的方法。对网络系统使用的增加，尤其是敏感应用已引出了可靠的访问DNS数据和控制数据内容安全的新方法。Internet的许多新应用导致了新的资源数据记录的定义，所以DNS服务现在可用于新的网络资源类型。

本书讲述了DNS的设计以及如何使它与世界范围内的其它数千台DNS服务器交互操作。本书还详细介绍了在设计DNS服务背后存在的问题以及有助于运行DNS的工具。

本书也讲述了Windows 2000中DNS的使用以及Windows 2000提供的DNS服务器。该Windows的最新版本将DNS置于其核心结构中非常重要的位置。Windows 2000 对DNS的依赖和使用的程度在商业操作系统中是前所未有的。Windows 2000中提供的DNS服务器与Windows NT提供的相比有较大的不同和提高。它支持DNS的绝大多数最新特性。Windows 2000中的活动目录和网络服务的互操做能力都对DNS的使用做了深层次的考虑。本书所提供的内容试图成为帮助你找到所有这些方法的指南，并提供一个关于维护网络服务健康的参考。

本书的读者对象

刚进入需要运行DNS环境的用户将在本书中找到对域名系统的完整介绍。本书详细解释和完整描述了客户端对DNS的使用、不同的DNS服务器、内部服务器的操作以及DNS所控制的信息。

那些有在UNIX或NT上运行DNS经验的用户将找到把他们的经验扩展到Windows 2000 平台上的DNS的信息。本书阐述了Windows 2000 DNS服务器如何顺应时代的潮流（带有DNS的许多新特性），哪些特性还太生涩，以及这些新特性与最新的BIND相比又是如何。这些信息将有助于互操作性设计。

那些需要评估和设计DNS使用以支持Windows 2000和其活动目录的人将找到有关Windows 2000第1版的信息。本书详细介绍了存在的内容及它们的含义，并预测了新的发展。与大多数关于DNS的信息不同，这里的注意力放在确保读者完全地获得信息上，而让读者自己得出结论。

管理Windows域网络环境和支持Windows客户端的用户将在这里找到“整幅画卷”。Windows使用包括DNS在内的几种技术来进行名字服务，这些技术的互操作有时会引起混淆。本书通过介绍DNS，同时也涉及到WINS和DHCP服务以及它们与DNS的接口，给出了这些管

理所需要的信息。

本书的组织结构

本书分三个部分讨论了这些主题。本书的第一部分设定了框架，主要侧重于介绍在所有服务器中都能找到的符合工业标准的DNS。中间部分讨论了管理员在设计和确保DNS服务、计划互操作、理解需求和Windows 2000 与其它DNS服务器（如BIND）相比专有的特征时将面临的问题。中间章节详细介绍了Windows 2000 DNS服务器，它的安装和配置，运行DNS常见的任务（一般的任务和Windows 2000特有的）。最后一部分集中于客户端的问题以及Windows 2000与DNS相关的服务。这些章节涉及了Windows客户端的配置，如何理解这些配置对NetBIOS和DNS使用的影响，以及DHCP和WINS服务的安装和使用。

英文原书书号：ISBN 0-7357-0973-4

目　录

第四部分 附 录

第一部分 理解域名系统

第1章 域名系统简介

本章包括以下各节:

- 域名注册、解析和分布。域名系统（DNS）是已注册的计算机名和可以被迅速定位的IP地址的目录。该节将概述 DNS中的一个重要部分——名字服务，以及它是如何注册、解析和传送计算机名的。DNS服务器可以用来定位它们所授权的域内的服务。如果该服务定位功能被实现，便可以发出不是寻找某台计算机而是寻找域内某种服务的请求，并且可以得到一个作为回答的IP地址。注意: Windows 2000 要求使用服务记录（SRV记录将在以后提到）。
- 主机名的特征。不论是准备给一台计算机命名还是计划为上千台计算机命名， DNS计算机命名规则都是十分重要的。该节将介绍一些必要的命名规则并提供一些如何为计算机命名的建议。
- 全域名。Internet上的计算机都是某个域的成员。该节将叙述域名、全域名以及它们是如何形成的。

本书是一本讲述域名系统的书，既适合新手又适合熟练的DNS管理员阅读。本书也讲述了新的Windows 2000 DNS服务器以及在Windows中如何使用DNS。阅读本书不要求读者有DNS的预备知识，但是有一定背景知识的读者很可能会发现一些新知识。这并不意味着书中提供的信息质量有问题，也不意味着读者的背景知识有缺陷。

Windows 2000操作系统使用DNS的方式不同于微软以前的操作系统——事实上，也不同于以前的任何操作系统。尽管本书开始是从世界通用标准的角度剖析和解释DNS的，但它以对Windows 2000特征的完整回顾而结束。本书的中间部分讨论了Windows 2000中对BIND 的使用，在非Windows环境下使用Windows 2000 DNS ，新的DNS特征和关注点以及在新界面下对DNS操作的实践。

在Windows 2000对活动目录域环境的支持中，DNS处于一个中心并且大量使用的位置。当询问100个Windows 2000 配置专家哪些是你能正确工作的10件最重要的事情时，在所提到的1000件事中几乎有100件是DNS。从活动目录的设计阶段到使用者的日常行为，Windows 2000系统的重要特征都与DNS相关。

本书的介绍将从DNS本身开始，看一下它是什么、它的定义、它是如何工作的以及各类操作系统（与时间有关的BIND版本或是Windows 2000）是如何使用它的。最后将介绍新版本DNS的一些特征，以及在Windows 环境下使用时应注意的事项和它的使用方法。

本章在介绍域名系统时不要求读者有很多的预备知识，只要知道计算机是如何工作以及如何和Internet交互的就可以了。凡是需要了解DNS和DNS服务器的人都可以通过阅读本书以获得必要的知识。在本章可以从概念上，也可以在一定程度的细节上学到什么是域名系统以

及DNS服务器是怎样满足成千上万的本地和世界各地计算机用户的需要的。

1.1　域名注册、解析和分布

Internet上计算机之间的TCP/IP通信是通过IP地址来进行的。因此，Internet上的计算机都应有一个IP地址作为他们的唯一标识。域名系统是用于注册计算机名及其IP地址的。DNS是在Internet环境下研制和开发的，目的是使任何地方的主机都可以通过比较友好的计算机名字而不是它的IP地址来找到另一台计算机。DNS是一种不断向前发展的服务，该服务通过Internet工程任务组（IFTF）的草案和一种称为RFC（Request For Comment）文件的建议不断升级的。在本书的后续章节将介绍这些草案和RFC文件的存放地点。

不要混淆域名系统服务器和域名系统。域名系统服务器只是域名系统中的工具，通过它们不停的工作来实现域名系统的功能。本章将介绍域名系统和域名系统服务器，请随时注意两者的差别。

DNS服务器为客户机提供一种方法来存储和搜索其他主机的主机名和IP地址，这里所说的客户机可以是单独的计算机用户、应用服务器，甚至是其他 DNS服务器。主机是计算机的另一种名称，主机名就是计算机在域名系统中使用的名字。域名空间是指Internet上所有主机的唯一的和比较友好的主机名所组成的空间，它是一个重要的概念。

每一个主机名及其 IP地址存储在一台或多台DNS服务器中，以便Internet中的其他用户可以通过计算机名来搜索相应主机的IP地址。为此，DNS服务器之间必须能进行可靠的通信，以便将Internet域名树的每一个分支捆绑在一起以形成一个综合系统。域名树是域名空间的骨架，DNS服务器工作时可在其上下左右移动。第2章中将详细介绍DNS是如何工作的并讨论域名空间是什么。

域名服务中有两个最基本的概念：域名注册和解析。这两个概念对于理解 DNS名字和DNS服务器都非常重要。但是，让我们首先简单地介绍一下注册和解析的对象：主机名和IP地址。

1.1.1　主机名和IP地址

DNS的数据文件中存储着主机名和与之相匹配的IP地址。从某种意义上说，域名系统类似于存储着用户名以及与此相匹配的电话号码的电话号码服务系统。

虽然 DNS记录中除了主机名和IP地址外还有一些其他的信息，DNS系统本身也有一些较复杂的问题要讨论，但 DNS最主要的用途和对用户来说最重要的价值是，通过它可以从主机名找到与之匹配的IP地址，并且在需要时输出相应的信息。

1.1.2　主机名的注册

主机名和 IP地址必须注册。注册就是将主机名和 IP地址记录在一个列表或者目录中。注册的方法可以是人工的或者自动的、静态的或者动态的。过去的DNS服务器都是通过人工的方法来得到原始的主机注册，也就是说，主机在DNS列表中的注册是要由人工从键盘输入的。最近的趋势是动态的主机注册。更新是用DHCP服务器触发完成的，或者直接由具有动态DNS更新能力的主机完成。DHCP是Dynamic Host Configuration Protocol的缩写，即动态主机配置协议。

除非使用动态DNS，DNS注册通常是人工的和静态的。Windows 2000中就提供了动态DNS的功能。当主机的信息有所变化时，主机记录的更新通常由人工来完成。图1-1表示了若干主机在 DNS服务器中的注册。在 DNS服务器中，最主要的信息只是主机名和IP地址（某些重要的例外见第4章）。

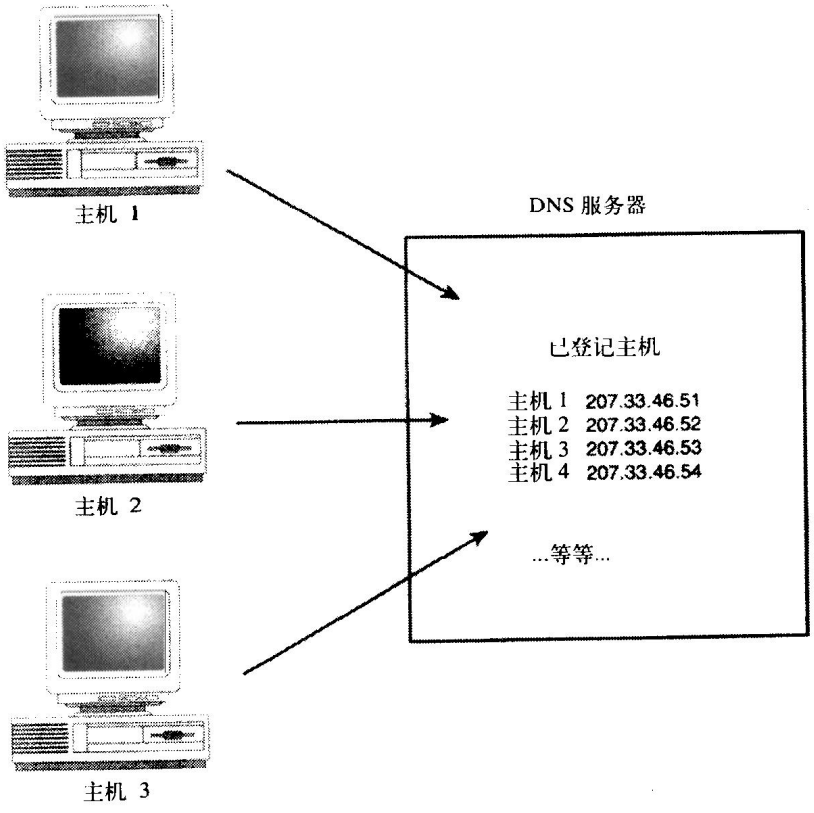

图1-1 主机在DNS服务器中的注册

图1-1并没有表示出主机名是如何注册的，因为注册的方法并不是只有一种。当然人工注册是最常见的，但也有若干自动注册的方法。自动注册的方法之一就是让DNS服务器去查阅WINS服务器。本书中将不断提到DNS和WINS的交互。通过WINS服务器的自动注册方法将在第16章中介绍。

另一种自动注册的方法是通过 DHCP服务器向具有动态DNS能力的DNS服务器注册名字。也就是 DHCP服务器在客户机上网时自动给它分配一个IP地址。 因为该方法经过完整的测试并受到广泛的支持，所以它是使用各种DNS服务器最容易的方法。该方法几乎在任何情况下都能正常工作。当注册完成以后（尤其是当已被提醒成功时），所有的DNS服务器都收到了主机的注册信息。

大多数的计算机由人工向一台DNS服务器进行注册，这台服务器一般是和这些计算机在同一个大楼或者同一个校园，或者至少在同一个企业内。一般来说，中型或大型企业都有自己的DNS服务器。这时编辑和修改服务器的主机列表将比求别人——如Internet服务供应商——注册主机的变化既迅速又容易。当使用UNIX 或Windows 2000时，如果有一个内部环境，就很有可能需要自己在内部运行DNS。

主机名必须在DNS服务器中注册，这台服务器称为主服务器。辅DNS服务器自动地从主DNS服务器获得所有的数据。管理员对这种备份很感兴趣，因为这可以让他们在几个不同的地方安置具有相同数据库的服务器。例如，中心办公室可以有一台主DNS服务器，而远地的机构可以有本地的辅服务器，以便加速地址的查找，也可防止因网络失效而找不到DNS服务器。主、辅DNS服务器的搭配使得所有的服务器都能找到已注册的主机，客户机能从离它最近的服务器获得回答。如果本地网络中的DNS服务器失效，无论安装的是Windows 2000还是其他操作系统，对主机的可用性都是一场灾难。而且如果一些主机通过辅服务器解析域名，还可以获得一定的负载平衡。

1.1.3　主机地址的资源记录

无论主机注册是如何完成的，这种注册的主要目的是在某个列表中记录下其他计算机在需要时可以被查到的主机名及其源地址，这种记录称为资源记录。资源记录可以有多种格式，第4章中将做详细介绍。

图1-2显示了在 Windows 2000 DNS管理器上显示的几个计算机的主机记录。

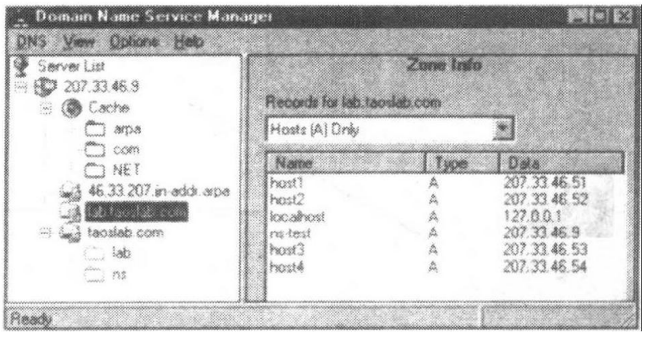

图1-2　查看主机地址记录

如果使用的是 UNIX DNS服务器和文本方式的配置文件，其条目就很像主机在这些记录中的注册(IN代表Internet，A代表 地址Address)：如果使用的是Windows 2000 DNS，则可以将记录信息记录在同样的文件中，但也可以不必这样做。第一列为主机名（如host1），第二列为记录的类型（本例中为Internet），第三列为资源记录的类型（A代表地址），第四列为IP地址。

```
host1    IN    A    207.33.46.51
host2    IN    A    207.33.46.52
host3    IN    A    207.33.46.53
host4    IN    A    207.33.46.54
```

1.1.4　主机名的解析

只要进行了注册，主机名就可以被解析。解析是一个客户端过程，目的是查找已注册的主机名或者服务器名以便得到相应的IP地址。客户端得到了目标主机的IP地址后，就可以直接在本地网上通信，或者通过一个或几个路由器在远程网上通信。

显然，一个DNS服务器可以有许多已注册的主机。解析注册在同一台DNS服务器上的其

他主机名应该是比较快的。一个具有上千主机的企业只需要少数几台DNS服务器。

图1-3显示了DNS客户机如何解析另一个在同一台DNS服务器注册的主机名。

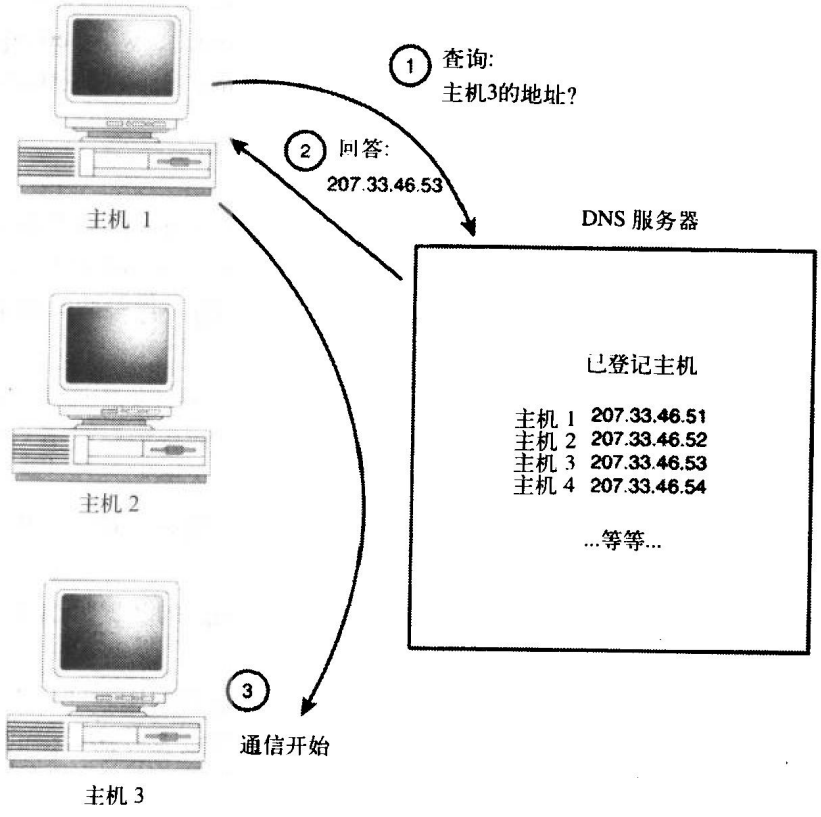

图1-3 一个DNS客户机查询DNS服务器以解析另一个主机名

1. 解析器

本章对主机名查询的解释似乎意味着DNS服务器担当了所有的主机名解析工作。对此，必须有所澄清。实际上，主要的角色是一种称为解析器的程序，解析器运行在所有使用TCP/IP协议的有DNS能力的计算机上。解析器将包含网络主机域名的路径描述转换为查询请求。解析器甚至还可以缓存已定位的主机，以加速接通的过程。

解析器几乎无所不在，可以是本地的或者远程的，可以在客户机上也可以在DNS服务器上。DNS服务器可以在需要时通过解析器查询另一台DNS服务器，这种情况是经常发生的。当一台DNS客户机作为客户机时，它的解析器就处于工作态，当一台DNS服务器作为客户机时，它的解析器也处于工作态。当一台DNS服务器作为服务器使用时，它的作用就是响应客户机的解析器的查询，而这台客户机也可能是另一台DNS服务器。

RFC文件 国际标准化机构和志愿管理机构共同管理Internet。这些管理机构通过工作委员会使用RFC文件来评估一些有可能成为标准的新思想。RFC文件可以由个人提出，也可以是出于某种商业利益的考虑。有不少RFC文件变成了正式的标准。要查阅RFC文件，可以通过http://www.dns.net/dnsrd/ 访问其中的域名服务资源目录，即dnsrd目录(Domain Name Services Resource Dictionary)。对DNS、Internet协议以

及Internet本身的标准制定有影响的机构有：

- Internet体系结构组（IAB, Internet Architecture Board）。
- Internet授权地址分配组（IANA, Internet Assigned Number Authority），www.iana.org。
- Internet工程指导组（IESG, Internet Engineering Steering Group），www.ietf.org/iesg.html。
- Internet工程任务组（IETF, Internet Engineering Task Force），www.ietf.org。
- Internet 协会（ISOC, Internet Society），www.isoc.org。
- Internet网络信息中心（InterNIC），www.internic.net。

RFC 1034“域名：概念和设备”中指出，解析器至少要访问一台域名服务器来直接得到所需信息，或通过其他的域名服务器来继续跟踪查询。在RFC 1034的第5、6页中说：“从解析器的角度来说，域名系统是由数目不详的域名服务器组成的，每台域名服务器具有整个域名树中的一个或几个分支的数据。”

经过查询后，返回给解析器的结果可能是下列结果中的一种（见RFC 1034第29页）：

- 给出所需数据的一个或几个资源记录。在这种情况下，解析器将以适当的格式返回得到的回答。
- 主机名错误。当所查询的名字不存在时给出这种错误。例如，可能是用户在键入主机名时出错。
- 数据未找到错误。当存在所查询的主机名，但找不到相应的数据时出现这种错误。

2. 逆向查找

到目前为止，我们的讨论都是围绕着 DNS如何从主机名查到IP地址。但也可以由IP地址来查找主机名，因为， DNS服务器中的数据文件是自动排序或者自动索引的，以便快速由名字查找，从IP地址出发的逆向查找还需要数据库按IP地址进行排序或索引。逆向查找也称为反向查询。

DNS服务器用来进行逆向查找的数据库称为 in-addr. arpa区或者称为ARPA域中的Internet地址区。如果仔细观察图1-2，可以看到属于207.33.46.9域名服务器的46.33.207. in-addr.arpa区。这个 in-addr区包含一个从IP地址到主机名的数据库，以便服务器执行从IP地址出发而不是从主机名出发的查找。第4章在讲述反向地址记录（PTR）时将讨论这种反向映射是如何建立的。

逆向查找的使用并不像正向查找那样普遍，但也不时有所使用。大多数的逆向查找是在用户（如系统管理员）已经知道本地主机的 IP地址，但需要查找它的主机名时进行的。逆向查找的一种实际用途是查找一个已知IP地址的主机的全域名。FTP服务器有时也通过逆向查找来证实所连接的主机是否为它所宣布的主机。另外，一些工具如nslookup也使用逆向查找的特性（见第12章）。这种技术提供了另一种验证所连接的主机是否为假冒的方法，这可以减少但不能消除攻击。

3. DNS服务器的搜索顺序

可以设置 DNS客户机为解析主机名搜索 DNS服务器的顺序。图1-4显示了Windows 95客户机搜索 DNS服务器的顺序。列表中的第一个 DNS服务器地址为192.168.1.24，这台客户机就是在这台服务器中注册，并成为example.net域的一个成员。如果客户机通过查询第一台服务器不能得到答案，它将继续查询第二台、第三台服务器。Windows 2000 客户端的设置允许列表中有更多的服务器。第14章将详细介绍不同版本客户端的配置。

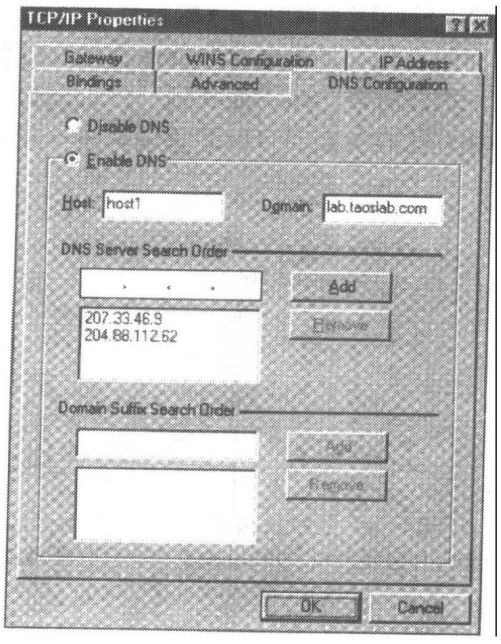

图1-4 DNS服务器搜索顺序是可选的

客户机所注册的DNS服务器应该是所属域的主服务器，大多数管理员也将这台服务器设置为客户机的首选搜索服务器。但并没有理由一定要求首选搜索服务器必须是主服务器或注册服务器。事实上客户机使用辅服务器作为首选搜索服务器是很普遍的。当使用动态DNS注册时，如果客户机试图在辅DNS服务器注册，辅DNS服务器将把请求提交给主DNS服务器，也就是说不会造成真正的错误。后续部分将介绍许多关于对不同类型的需求使用不同类型的服务器的策略。

搜索服务器的顺序完全是可选的。为了解析域名，首先查询的 DNS服务器并不一定是机器所注册的服务器。第二台和第三台搜索服务器也可以是任何你觉得合适的服务器，如可以是在其他域中的服务器、ISP的域名服务器或者其他可以快速响应查询的服务器。只要列表中有一台服务器响应了客户机，搜索就立即终止。

1.1.5 主机名的分布

并不是一台单独的 DNS服务器就包含了全世界的主机名，这是不可能的。如果存在这样的主 DNS服务器的话，客户机和这台服务器的距离就太遥远了。也很难想象这样一台为整个Internet服务的 DNS服务器需要多大能力和带宽。除此以外，如果这台主DNS服务器停机的话，遍布全球的Internet将陷入瘫痪！与这种设想相反，主机名分布于许多DNS服务器之中。

主机名的分布解决了不是只用一台DNS服务器的问题，但这对客户机又出现了另一个问题：客户机如何得知向哪一台DNS服务器查询？域名系统通过使用自顶向下的域名树来解决这个问题，每一台主机是树中某一个分支的叶子，而每个分支具有一个域名。重要的是，你所拥有的每一台主机都和一个域相关联。

那究竟总共需要多少DNS服务器呢？尽管实际的数字是不可知的，并且依实际原因而变化，但从理论上来说，域名树的每一个分支需要一台DNS服务器。