从零开始当网管

网络服务与网络安全管理教程

郝文化 主 编
周 明 谢荣清 等编 著

本书读者对象：

- 各大中专院校的教材用书
- 广大网络爱好者的自学用书
- 各网络服务与网络安全管理的从业者日常工作中的参考用书

机械工业出版社
China Machine Press

从零开始当网管

网络服务与网络安全管理教程

郝文化　主编
周　明　谢荣清　等编著

机 械 工 业 出 版 社

本书以了解现代主流操作系统，掌握 Windows 和 UNIX 的基本应用，熟悉并掌握网络安全知识为目标，分章介绍了 Windows 2003 Server 和 UNIX 在网络应用及安全方面的知识。全书从最基础的层次开始，全面介绍了基于 Windows 2003 Server 的各种应用，包括创建 DHCP、FTP、Web 等常用的服务器设置，基于 UNIX 的 FTP、新闻组服务等应用，网络安全方面的各种主流技术，Windows 2003 Server 下的安全问题及防范方法，UNIX 下的安全问题及防护等知识。

本书内容丰富，图片资料详细，语言通俗易懂。可作为各大、中专院校在校学生学习网络服务与网络安全管理技术的教材用书；也可作为广大网络爱好者学习网络服务与网络安全管理技术的自学用书；还可作为各网络服务与网络安全管理的从业人员在日常工作中的参考用书。

图书在版编目（CIP）数据

网络服务与网络安全管理教程/郝文化主编.
-北京：机械工业出版社，2004.11
（从零开始当网管）

ISBN 7-111-15536-X

Ⅰ.网… Ⅱ.郝… Ⅲ.①计算机网络-服务-教材
②计算机网络-安全技术-教材 Ⅳ.TP393

中国版本图书馆 CIP 数据核字（2004）第 112259 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：夏孟瑾 责任编辑：王金航 版式设计：侯哲芬
北京蓝海印刷有限公司印刷·新华书店北京发行所发行
2005 年 1 月第 1 版第 1 次印刷
787mm×1092mm 1/16·14.25 印张·341 千字
0001-5000 册
定价：19.00 元

前　言

面对众多的网络服务和网络安全管理的书籍，读者怎样选择一本适合自己在短时间内学习的书籍呢？编者放心地告诉读者朋友，请您选择本书吧！这是因为，在当今众多的网络服务和网络安全管理的书籍中，很多书籍缺少实用性、针对性和通俗易懂性。本书由知名计算机教师主编，他们结合多年的计算机教学经验，源于计算机教学特点和工作实际，在写作过程中，以初学者的身份和心理量身编写和安排了本书内容，同时列举了大量的具体实例。

现在世界上使用最广泛的两种操作系统是 Windows 操作系统和 UNIX 操作系统。它们占据了目前操作系统市场的 80%左右，其中 Windows 操作系统的市场份额约为 45%，UNIX 操作系统及其变体的市场份额约占 35%。UNIX 操作系统由于其具有高度的可靠性、稳定性及安全性而多应用于大型机构的服务器上。Windows 系列操作系统以其所具有的易操作性、方便性赢得了大多数个人消费者及中小型公司机构的青睐。

Windows 和 UNIX 系统为用户提供了很多非常有用的服务，如 FTP 服务、电子邮件服务、新闻组服务、媒体服务和 Web 服务等。种种有价值的服务体系为广大使用者提供了极大的方便，而且这些服务的实现和维护也相对比较容易，特别是 Windows 系列更是这样，它以图形化的界面直观快捷地替代了以前命令行式的操作方式，这使用户学习和掌握操作系统变得更加容易。

在 Internet 深入千家万户，并将以前单独的计算机连接起来的同时，它也打开了一个潘多拉魔盒。无数的隐患和危险随着盒子的开启纷纷冒出来，这些在 Windows 系统上得到了体现。如今受攻击最多的系统就是 Windows 系统，这除了与它使用最广泛而容易引人注意之外，也与它本身固有的缺陷有关。当然，现在 UNIX 系统也出现了不少安全隐患，但大多数的问题还是集中在 Windows 系统身上。

本书首先给读者介绍基于 UNIX 和 Windows 系统的各种服务，如何配置和管理这些服务。然后再为读者讲述关于安全知识的基本理论，最后介绍 UNIX 和 Windows 操作系统下的安全措施。使大家在整体上对操作系统的应用及安全有一个整体的认识。

主要内容

本书的具体章节安排如下：

第 1 章主要介绍 Windows 系统下各种服务的具体实现方法，通过图示和说明让读者在较短的时间内快速掌握 Windows 下的主要的几种应用服务。

第 2 章主要介绍 UNIX 系统下各种服务的实现方法。由于 UNIX 系统下主要是使用命令行的方式来配置各种服务，因此较为枯燥。书中尽量以简单的语句为读者阐述如何安装和配置这些服务。

第 3 章主要介绍安全知识的内容。关于安全问题的研究已经开始了很多年，其中的知识的确是太复杂繁琐了，而且涉及面极广。因而以较短的篇幅来讲述这么多的内容是不大

可能的。本章中主要以现在最热门和比较基础的知识为主向朋友们介绍它们的基本常识。

第 4 章主要介绍了 Windows 系统下实现安全的新技术 IPSec 和 SSL，以及虚拟网。现在的数字签名逐渐流行起来，网上涉及到安全性比较高的，如银行金融系统都需要数字签名，以增强安全性。虚拟网和 IPSec 的结合更是增加了网络的安全性。

第 5 章主要介绍了 UNIX 系统的一些基本的安全知识，UNIX 系统相对来说还是比较安全的，但是它同样存在一些安全漏洞，UNIX 系统同样处在一个不断完善的阶段。用户最好定时下载最新的源码。

第 6 章主要介绍 Windows 和 UNIX 操作系统的互联。

适用对象

本书内容丰富，图片资料详细，语言通俗易懂。可作为各大、中专院校在校学生学习网络服务与网络安全管理技术的教材，也可作为广大网络爱好者学习网络服务与网络安全管理技术的自学用书，还可作为各网络服务与网络安全管理的从业人员在日常工作中的参考用书。

编写分工

本书由郝文化主编，由周明、谢荣清担任主要的编写工作。同时，参与本书编写的人员还有王安贵、陈郭宜、程小英、谭小丽、卢丽娟、刘育志、吴淬砺、赵明星、贺洪俊、李小平、史利、张燕秋、周林英、黄茂英、李力、李小琼、李修华、田茂敏、苏萍、巫文斌、邹勤、粟德容、童芳、李中全、蒋敏、刘华菊、袁媛、李建康等。

由于编写时间仓促，书中疏漏之处在所难免，欢迎广大读者和同行批评指正。

其他服务：如果读者愿意参加“网络服务与网络安全管理技术”的学习培训，或是在学习过程中发现问题，或有更好的建议，欢迎提出来。同时，我们也非常愿意同网络服务与网络安全管理技术高手经常保持联系，E-mail：bojia@bojia.net，网址：http://www.bojia.net，我们将认真、负责地对待每位读者的来信。

编者

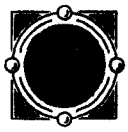
目　　录

前言

第 1 章　Windows 2003 Server 下的网络服务 1
1.1　DNS 服务 1
1.1.1　DNS 概述 1
1.1.2　安装和配置 DNS 服务器 2
1.1.3　管理服务器 3
1.1.4　优化和监视服务器 5
1.2　DHCP（动态主机配置协议）服务 6
1.2.1　DHCP 概述 6
1.2.2　安装和配置 DHCP 服务器 6
1.2.3　监视和管理服务器 9
1.3　Windows Internet 名称服务（WINS） 10
1.3.1　WINS 概述 10
1.3.2　安装和配置 WINS 服务器 11
1.3.3　管理 WINS 服务器 14
1.4　Internet 验证服务（IAS） 15
1.4.1　IAS 概述 15
1.4.2　安装和配置 IAS 服务器 16
1.4.3　为用户身份验证和记账配置日志 17
1.5　IIS（互联网信息服务服务） 18
1.5.1　IIS 概述 18
1.5.2　使用 IIS 所提供的服务 19
1.6　配置 SMTP（简单邮件传输协议）服务器 20
1.6.1　SMTP 服务介绍 20
1.6.2　安装和配置 SMTP 服务器 20
1.6.3　维护 SMTP 服务器 23
1.7　Web 服务 24
1.7.1　Web 服务介绍 24
1.7.2　安装和配置 Web 服务器 25
1.7.3　管理 Web 服务器 26
1.8　FTP 服务 27
1.8.1　FTP 服务介绍 27

1.8.2 使用 IIS 配置 FTP 服务器 27
1.8.3 管理 FTP 服务器 29
1.8.4 使用 Server-U 配置 FTP 服务器 30
1.9 简单网络管理协议（SNMP） 31
1.9.1 简单网络管理协议概述 31
1.9.2 安装和配置 SNMP 服务 32
1.9.3 管理 SNMP 服务 34
1.9.4 配置捕获编译器的事件 35
1.10 远程和路由访问（RRAS） 36
1.10.1 远程和路由访问概述 36
1.10.2 启用路由和远程访问服务 37
1.10.3 配置和管理路由和远程服务 39
1.11 网络视频电话会议 40
1.11.1 Net meeting 和网络视频电话会议 40
1.11.2 使用 Net meeting 进行网络视频电话会议 42
1.11.3 使用 Net meeting 远程共享桌面 42
1.12 Windows 媒体服务 43
1.12.1 流媒体服务概述 43
1.12.2 安装和配置 Windows 媒体服务器 45
1.12.3 管理 Windows 媒体服务器 47
1.13 本章小结 47
1.14 本章习题 48

第 2 章 UNIX 下的网络服务 49
2.1 电子邮件服务 49
2.1.1 概述 49
2.1.2 电子邮件系统的构成 49
2.1.3 电子邮件程序 Mailx 50
2.1.4 电子邮件程序 Sendmail 52
2.2 FTP 服务 55
2.2.1 概述 55
2.2.2 建立 UNIX 下的 FTP 服务器 56
2.3 新闻组服务 70
2.3.1 概述 70
2.3.2 新闻阅读器 rn 72
2.3.3 新闻阅读器 trn 74
2.3.4 新闻阅读器 tin 76
2.3.5 新闻阅读器 nn 80



2.4 Internet 服务 83
2.4.1 概述 83
2.4.2 Telnet 83
2.4.3 Archie 和 WAIS 服务 84
2.4.4 WAIS 服务器 90
2.4.5 Gopher 服务 94
2.4.6 WWW 服务 96
2.5 远程访问 97
2.5.1 概述 97
2.5.2 TCP/IP 远程访问操作 99
2.5.3 UUCP 103
2.6 本章小结 106
2.7 本章习题 107

第 3 章 网络安全知识 108
3.1 网络安全的重要性和网络安全策略 108
3.2 关于 TCP/IP 协议 114
3.2.1 OSI 和 TCP/IP 协议层 114
3.2.2 TCP/IP 的不同协议层 116
3.3 密码技术 119
3.3.1 密码技术概述 119
3.3.2 对称和非对称密码技术 121
3.3.3 数字签名 122
3.4 黑客和病毒 123
3.4.1 黑客攻击原理 123
3.4.2 特洛伊木马 125
3.4.3 黑客防范法 126
3.4.4 病毒原理 128
3.4.5 病毒检测和防范方法 133
3.4.6 防火墙工作原理 140
3.4.7 防火墙安全设计策略 142
3.4.8 防火墙发展的新方向 147
3.5 入侵检测技术 148
3.5.1 入侵检测系统（IDS）概述 148
3.5.2 入侵检测系统的结构 151
3.5.3 入侵检测系统应用的新技术 151
3.6 本章小结 154
3.7 本章习题 155

第 4 章 Windows 2003 Server 下的网络安全 156
4.1 网际协议安全（IPSec） 156
4.1.1 网际协议安全概述 156
4.1.2 定义和指派 IPSec 策略 157
4.2 数字证书服务和 SSL 157
4.2.1 数字证书服务概述 157
4.2.2 构建数字证书服务 158
4.2.3 向 CA 申请数字证书 158
4.2.4 数字证书的安装 159
4.2.5 SSL（Secure Socket Layer）介绍 160
4.2.6 SSL 原理 161
4.2.7 在 Web 服务器上配置 SSL 164
4.3 虚拟专用网络（VPN） 166
4.3.1 虚拟专用网络概述 166
4.3.2 建立虚拟专用网络 167
4.4 本章小结 170
4.5 本章习题 170

第 5 章 UNIX 的网络安全 171
5.1 安全问题概述 171
5.1.1 选择安全策略 172
5.1.2 安全网络对策 186
5.1.3 口令安全 187
5.1.4 UNIX 下的入侵分析 189
5.2 构建防火墙 191
5.2.1 防火墙网关 191
5.2.2 建立应用级网关 193
5.2.3 使用鉴别的方法 194
5.2.4 使用网关工具 194
5.3 本章小结 196
5.4 本章习题 196

第 6 章 Windows 与 UNIX 的互联 197
6.1 UNIX 和 Windows 概述 197
6.1.1 UNIX 概述 197
6.1.2 Windows 概述 201
6.1.3 Samba 概述 202
6.2 安装和配置 Samba 203

6.2.1 安装 Samba 203
6.2.2 配置 Samba 204
6.3 应用互联服务 211
6.3.1 域名服务 211
6.3.2 文件共享 212
6.3.3 打印共享 213
6.4 本章小结 216
6.5 本章习题 216

第 1 章　Windows 2003 Server 下的网络服务

知识点：

- 组建和管理 DNS 服务器
- 组建和管理 DHCP 服务器
- 组建和管理 WINS 服务器
- 组建和管理 IAS 服务器
- 使用 IIS 控制台
- 组建和管理 SMTP 服务器
- 介绍 Web 服务，组建和管理 Web 服务器
- 组建和管理 FTP 服务器
- 介绍和使用路由和远程服务
- 配置 SNMP 服务
- 使用 Net meeting 进行网络视频电话会议
- 组建和管理 Windows 媒体服务器

本章概述：

Microsoft 已经推出了 Windows 2000 的升级产品——Windows 2003 Server 系列，Windows 2003 号称“do more with less”，意思就是“用更少的资源做更多的工作”。实际上正是这样，Windows 2003 在资源使用、网络应用及安全性方面有了较大改善，集成了 Microsoft.NET 技术，使用 XML Web 服务和.NET 框架，提供了通过 XML Web 服务迅速、可靠地构建安全的联网解决方案。使用 Windows 2003 系列在操作方面更简便，网络支持功能更强大，数据更安全。应用 Windows 2003 Server 可以组建用户需要的所有网络服务。本章主要介绍如何在 Windows 2003 Server 下创建和管理各种网络服务器。

1.1　DNS 服务

1.1.1　DNS 概述

Windows 为用户提供了多种多样的服务，本节介绍的 DNS 服务就是其中一种，DNS（Domain Name System）是域名系统的英文缩写。域名简单说来就是指平时上网时输入的网址，比如 www.yahoo.com、www.163.net 等。域名是具有层次结构的，它的一般表示方法是：域名机器.n 级域名……二级域名.顶级域名。顶级域名可分为一般域名和国家域名。一

般域名指的是 com、net、edu、mil、gov 等。这里详细介绍一般域名的含义。com：适用于工、商、金融等企业；net：适用于互联网络、接入网络的信息中心（NIC）和运行中心（NOC）；org：适用于各种非盈利性的组织；edu：适用于教育机构。由于历史原因，下列域名限美国专用。gov：适用于美国政府部门，国内机构不能注册；mil：适用于美国的军事机构，国内的机构不能注册。国家域名指的是国家的缩写，如中国是 cn，日本是 jp 等。前面所说的 www.yahoo.com 中，yahoo 就是域名机器名，而 com 就是它的顶级域名。

实际上计算机是通过一组八位二进制数来与远程服务器联系的。这组数字就是 IP 地址。理论上，输入 IP 地址比输入上面的域名连接速度更迅速，但这些枯燥的数字不易记。而域名相对来说更便于记忆，但是要怎样将域名转换成计算机认识的 IP 地址呢？这就是 DNS 的作用了。DNS 提供了域名和 IP 地址的映射和转换，当用户的服务器在 DNS 上注册了域名时，要远程访问用户的服务器，就可以直接输入这个域名以访问用户的服务器。比如新浪的服务器 IP 是 66.77.9.79，域名是 www.sina.com。当用户在 URL 中输入域名时 DNS 就会将 www.sina.com 转换为 66.77.9.79。然后通过这个 IP 访问新浪的服务器。这个将域名映射为 IP 地址的过程就叫域名解析。现在中国互联网络信息中心（CNNIC）也提供一种叫做中文域名解析的 URL 输入方式，就是在 URL 中直接输入中文域名，这样更适合中国人的习惯，以自己耳熟能详的中文网站名称输入，提供了很大方便。其实也是使用了这种方法。

1.1.2 安装和配置 DNS 服务器

要配置 DNS 服务器，请先确认 Windows 2003 Server 上已经安装了 DNS，在控制面板选择“添加/删除程序”中选取“添加/删除 Windows 组件”。在组件列表中选择“联网服务”，如图 1-1 所示。如果已经选中“域名系统（DNS）”则已安装，如没有则选中安装。完成以后就可以进行 DNS 的配置。

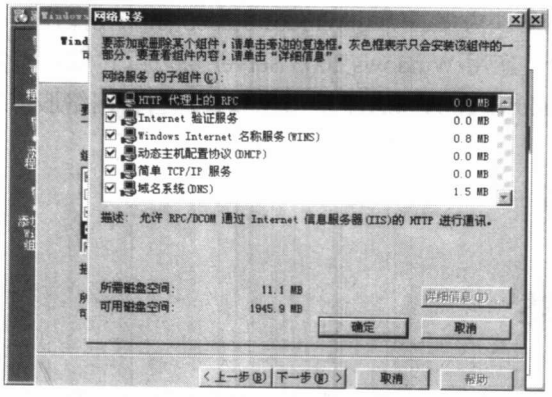
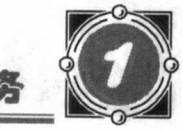


图 1-1 DNS 主界面

要配置 DNS 服务，请在控制面板中选择管理工具，然后选择 DNS，右击服务器名称，其中服务器名称为该服务器的名称，选择“配置 DNS 服务器”。“配置 DNS 服务器向导”



就会启动，如图 1-2 所示。

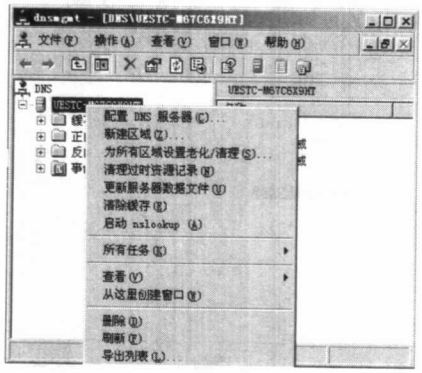


图 1-2　配置 DNS 服务器

在配置 DNS 服务器前，请先阅读 DNS 清单，选择“下一步”。根据 DNS 服务器的角色来选择用户需要的 DNS 服务器类型。例如：创建正向搜索区域（推荐用于小型网络）。对于使用 Active Directory 或者使用 Internet 服务提供商（ISP）解析 DNS 名称查询的小型网络，请使用此选项。通过使用此选项，用户可以为用户的网络使用的 Active Directory 域所对应的 DNS 域创建 DNS 区域。为位于用户的 ISP 的 DNS 服务器所承载的 DNS 区域创建第二个区域。创建正向和反向搜索区域（推荐用于大型网络）。如果用户要给已具有 DNS 结构的大型网络添加 DNS 服务器，请使用此选项。通过使用此选项，用户可以创建正向和反向搜索区域，以解析对用户的 DNS 名称空间的 DNS 域中资源的查询。指定将 DNS 服务器用作转发器，此 DNS 服务器无法回答的名称查询将会在此被发送。为用户要创建的区域指定复制范围（如果此 DNS 正在 Active Directory 域控制器上运行）。指定将 DNS 服务器用作转发器，此 DNS 服务器无法回答的名称查询将在此被发送。为用户要创建的区域配置动态更新。只配置根提示（只推荐高级用户进行此工作）。如果用户要创建纯正向 DNS 服务器，或者，要给当前配置了区域和转发器的 DNS 服务器添加根提示，请使用此选项。请按照该向导其余各页上的说明来配置用户的 DNS 服务器。

1.1.3　管理服务器

默认情况下，DNS 服务可以响应服务器绑定的所有 IP 地址。本来每个 DNS 分配一个 IP 地址就可以了。但由于成本或其他因素只能使用一台服务器时，就需要给一台 DNS 服务器分配两个或更多 IP 地址，给该服务器指定两条 DNS 主机名字记录，并且使用它们的主机名字和响应的 IP 地址注册到域中。可以用鼠标右键单击 DNS 控制台，选择属性中的接口选项，为服务器配置进行响应的 IP 地址。如果想用绑定在服务器上的所有 IP 地址就选择“所有 IP 地址”选项。如果需要限制服务器响应时使用的列在相关联的框中的 IP 地址范围，选择“只在以下 IP 地址”选项，并将需要的 IP 地址添加到列表中即可，如图 1-3 所示。

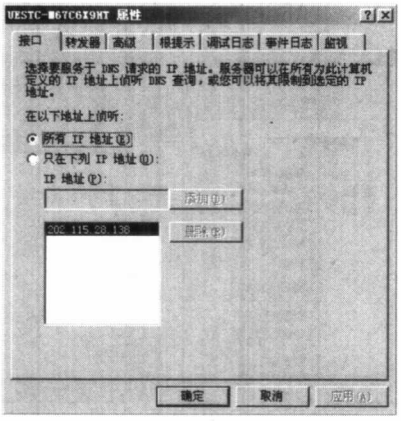


图 1-3　设置 DNS 绑定 IP 地址

在“转发器”选项卡中可以设置转发器的属性。转发器是网络上的 DNS 服务器，用来将外部 DNS 名称的 DNS 查询转发给该网络外的 DNS 服务器。也可使用“条件转发器”按照特定域名转发查询。通过让网络中的其他 DNS 服务器将它们在本地无法解析的查询转发给网络上的 DNS 服务器，该 DNS 服务器即被指定为转发器。使用转发器可管理网络外的名称的域名解析，并改进网络中的计算机的域名解析效率。在这个选项卡中可以设置转发器所属的 DNS 域和转发器的 IP 地址。

“高级”选项卡中可以设置服务器的选项，包括：

- 禁用递归（也禁用转发器）：该选项防止服务器执行递归查询。选择该项后，服务器以引用而不是递归的方法来答复，直到一个解决方法出现。
- BIND 辅助区域：为优化性能，如果服务器不在早期的系统上执行区域传送，请不要选择此项。因为这会使 DNS 服务器的执行速度变慢。如果区域数据不正确，加载会失败。默认情况下，Windows 2003 的 DNS 服务器在加载区域时遇到错误并不会使该操作失败而是将错误信息记录进日志中。选择该项后，DNS 遇到错误将停止加载区域数据。
- 启用循环：循环复用是 DNS 服务器用于共享和分配网络资源负载的本地平衡机制。如果找到多个 RR（资源记录），则可使用循环法交替使用查询应答中包含的所有 RR 类型。默认情况下，DNS 使用循环法来交替查询应答中返回的 RR 数据的顺序，在这些应答中，对于查询的 DNS 域名来说，存在相同类型的多个 RR。该功能提供了一种非常简便的方法，用于对客户端使用 Web 服务器和其他频繁查询的多计算机的负载平衡。如果 DNS 服务器禁用循环复用，那么这些查询的响应顺序以应答列表中在 RR 区域（或者是它的区域文件，或者是 Active Directory）中存储时的静态排序为基础。
- 启用网络掩码排序：DNS 服务器可以根据主机记录的地址检查客户端的 IP 地址，如果该记录在客户端所在的子网内，DNS 会将该主机记录放进响应列表中，这将使客户机与被请求的主机是距离最近的并且访问速度最快。默认情况下该选项是

选定的，取消它可以防止 DNS 对基于子网的响应顺序重排。

- 保护缓存防止污染：DNS 服务器使用一个缓存来在本地暂时保存上个请求的应答。这被用来避免总是花费时间来向上级 DNS 服务器进行查询。也可以加快响应请求的时间。默认情况下该选项是被选中的，可以避免与缓存无关的应答。

默认情况下，DNS 不会大规模地记录日志，这是因为如果有大量的客户端进行查询，将会产生数量巨大的记录，对于服务器来说开销太大。如果用户要检查日志文件，可以在“事件日志”选项卡中选择如何记录日志，在“调试日志”选项卡中可以具体地配置日志以及日志文件的路径，默认是%systemroot%\winnt\system32\Dns\DNS.log。

1.1.4 优化和监视服务器

对服务器的监视可以使用服务器属性中的监视选项卡。在这里可以针对本地服务器进行测试，也可以对其他名字的服务器进行递归查询。这可以帮助测试服务器顺利通信的能力。这里的递归查询是指客户端可使用从先前的查询获得的缓存信息就地应答查询。DNS 服务器可使用其自身的资源记录信息缓存来应答查询。DNS 服务器也可代表请求客户端查询或联系其他 DNS 服务器，以便完全解析该名称，并随后将应答返回至客户端，这个过程就叫做递归。“监视”选项卡如图 1-4 所示。

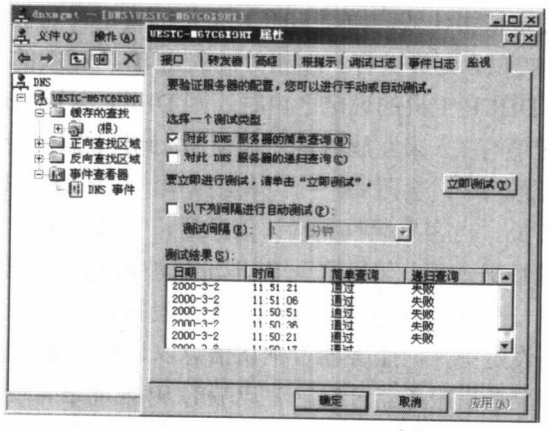


图 1-4　对 DNS 服务器的查询

“监视”选项卡中包含以下信息：

- 对此 DNS 服务器的简单查询：表示执行对本地服务器的重复查询。
- 对此 DNS 服务器的递归查询：表示执行对本地服务器的递归查询。
- 以下列间隔进行自动测试：表示以设定时间进行定时、自动的查询。
- 测试结果：显示了测试的结果，包括测试时间、查询方式和查询效果。

1.2 DHCP（动态主机配置协议）服务

1.2.1 DHCP 概述

在使用 TCP/IP 协议的网络中，每一台计算机都具有至少一个 IP 地址，才能与其他计算机进行通信。在一个小型的局域网中这样还可以，但是在大的局域网中，比如校园网或者大公司的内部网中就比较麻烦。手动一个一个设置每台机器的IP地址将非常繁琐而无聊。为了统一规划和管理网络中的 IP 地址，DHCP 就应运而生了。它能有效地管理起局域网中的 IP 地址。DHCP 指的是由服务器控制一段 IP 地址范围，客户机登录服务器时就可以自动获得服务器分配的 IP 地址和子网掩码。首先，DHCP 服务器必须是一台安装有 Windows 2000 或者 Windows 2003 Server/Advanced Server 系统的计算机；其次，担任 DHCP 服务器的计算机需要安装 TCP/IP 协议，并为其设置静态 IP 地址、子网掩码、默认网关等内容。

DHCP 的工作过程是：每当 DHCP 客户端在开机或是重新激活网卡时，它会向网络中所有计算机发出 DHCP client 请求。而网络中非 DHCP 服务器的计算机在收到这个数据包后会丢弃它。当 DHCP 服务器收到这个包以后，DHCP 主机首先会针对该次请求的信息所携带的目的计算机的网卡 MAC（用户计算机的网卡中的硬件地址，该地址是惟一的）地址与 DHCP 主机本身的设定值去比较，如果 DHCP 主机的设定针对该 MAC 作静态 IP（每次都给予一个固定的 IP）提供，则提供客户端相关的固定 IP 与相关的网络参数；而如果该信息的 MAC 地址并不在 DHCP 主机的设定之内时，则 DHCP 主机会选取目前网域内没有使用的 IP（这个 IP 与设定值有关）来发放给客户端使用。此外，需要特别留意的是，在 DHCP 主机发放给客户端的信息当中，会附带一个“租约期限”的信息，以告诉客户端用户这个 IP 可以使用的期限有多长。当客户端收到确认信息后，它又会向网络中所有计算机发出广播，以确认是否该 IP 地址被占用，如果这个 IP 地址已被其他计算机占用，它就再向 DHCP 服务器发请求重新分配一个 IP 地址。如果该 IP 地址没被占用，它会将服务器返回的网络参数加入到自己的网络设定中并向服务器发确认信息以告知服务器这次的需求已经确认。

DHCP 中的租约期限是指服务器分配给客户端的 IP 地址是有使用期限的，这可以在服务器中设置期限的长短。当租约期限到期后，服务器会收回该 IP 地址。如果还需要使用，客户端应该再次向服务器发 DHCP client 请求。

1.2.2 安装和配置 DHCP 服务器

安装 DHCP 服务器可以在控制面板中通过“选择添加/删除程序”完成。在“添加/删除 Windows 组件”中打开“网络服务”，在其中选择“DHCP”就可以安装了。安装好后在管理工具中就可以直接选取 DHCP 进行配置，如图 1-5 所示。

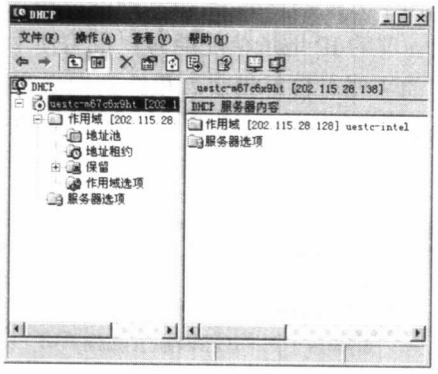


图 1-5　DHCP 控制台主界面

Windows 2003 提供了一个 MMC（微软管理控制台）控制台来对本地和远程的 DHCP 服务器进行管理。默认情况下，它连接的是本地的 DHCP 服务器，如要添加新的服务器可以在树型目录顶部的 DHCP 处右击选择“新建 DHCP 服务器”，输入新服务器的名称或 IP 地址并确定，新的 DHCP 服务器就添加到服务器列表中。

DHCP 作用域是一个属性集合，包括定义一个 IP 地址的范围以及相关设置，如 DNS 服务器、默认网关和客户需要从 DHCP 服务器取得的其他信息。在开始使用 DHCP 服务器前，必须要创建至少一个作用域。创建它可以通过向导来完成，如图 1-6 所示。

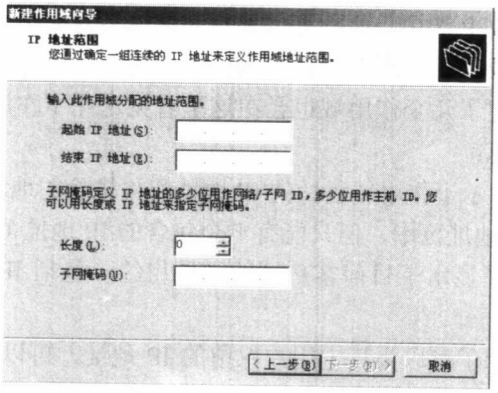


图 1-6　DHCP 新建作用域向导

新建作用域向导包括以下信息：

- 作用域名：这个作用域的名称及描述。
- IP 地址范围：在这里用户可以限定用户的 DHCP 服务器管理的 IP 地址范围。通过设置子网掩码和 IP 地址的长度可以设置多少位用作子网 ID，多少位用作主机 ID。这里的位数指的是 IP 地址换算成二进制后的位数。关于子网、超网与子网掩码的关系这里不再详细解释。
- 添加排除：指的是 DHCP 服务器不包括的 IP 地址范围。因为在网络中有些设备需要使用静止 IP 地址，比如路由器、交换机和服务器等。必须把它们使用的 IP 地