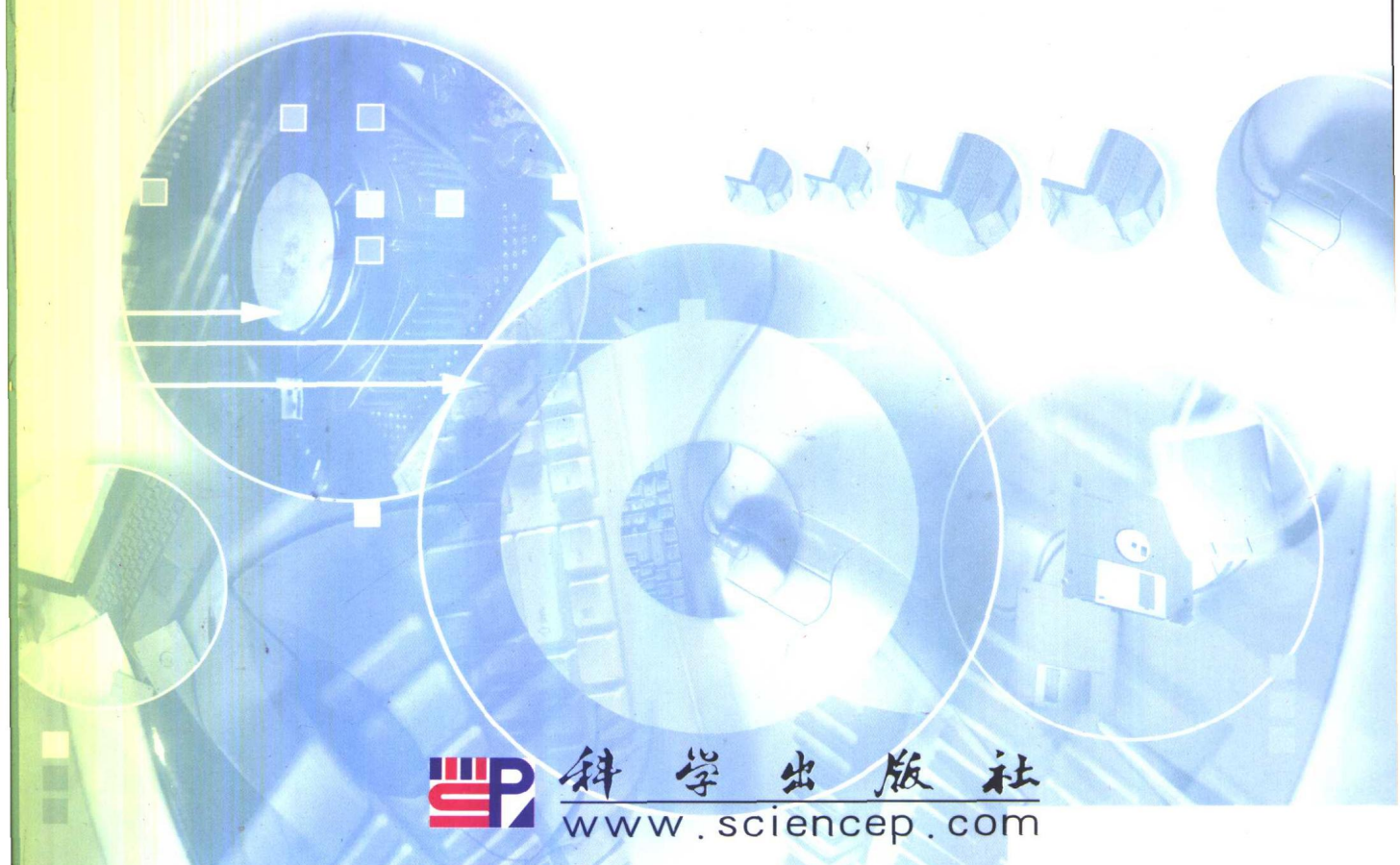
微软认证高级技术培训教材系列

实现Windows 2000网络基础结构

喻文芳　朱昀　罗靖 等　编著



科学出版社
www.sciencep.com

微软认证高级技术培训教材系列

实现Windows 2000网络基础结构

喻文芳　朱昀　罗靖 等　编著

科学出版社
www.sciencep.com

内 容 简 介

本书是微软认证高级技术培训教材系列之一。对应考试号：70-216，对应课程号：2153。

本书共有 11 章，包括了安装、配置、管理和支持采用 Windows 2000 Server 产品的网络基础结构。

每章均附有大量的微软认证全真习题，以及详细的分析和答案，凝聚了作者多年科研教学的经验教训。这些练习将极大的帮助读者理解和掌握所学的知识和参加微软认证考试。

本书适合作为微软认证高级技术培训班教材，也适合作为大中专院校计算机网络管理和开发人员的参考书、参加微软认证考试的自学辅导教材。需要本书或需要得到技术支持的读者，请与北京中关村 083 信箱北京希望电子出版社（邮编 100080）联系，电话：010-62630301，82675588(总机)，传真：010-62520573，E-mail: kobe@bhp.com.cn

图书在版编目（CIP）数据

实现 Windows 2000 网络基础结构 /喻文芳主编.—北京：科学出版社，2003.8

微软认证高级技术培训教材

ISBN 7-03-011872-3

Ⅰ.实… Ⅱ.喻… Ⅲ.窗口软件—网络服务器—技术培训—教材 Ⅳ.TP316.86

中国版本图书馆 CIP 数据核字（2003）第 065000 号

责任编辑：栾大成 /责任校对：吴胜

责任印刷：媛明 /封面设计：王翼

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京市媛明印刷厂印刷

科学出版社发行 各地新华书店经销

*

2003 年 8 月第 一 版 开本：787×1092 1/16

2003 年 8 月第 一次印刷 印张：32 3/4

印数：1—5 000 字数：776 500

定价：50.00 元

出版说明

为了配合微软高级技术培训的教学与考试，进一步推广微软认证系统工程师（MCSE）、微软认证数据库管理员（MCDBA）、微软认证系统管理员（MCSA）和微软认证产品专家（MCP）的培训和考试，特组织优秀的微软认证讲师（MCT）编写了本套微软认证高级技术培训教材。

全套教材共 7 本：

序号	书　名	对应考试号
1	Windows 2000 网络与操作系统基础	无
2	实现 MS Windows 2000 Professional 和 Server	70-210，70-215
3	实现 MS Windows 2000 网络基础结构	70-216
4	MS Windows 2000 目录服务基础结构设计和管理	70-217，70-219
5	MS SQL Server 2000 数据库管理	70-228
6	MS SQL Server 2000 数据库编程	70-229
7	管理 MS Windows 2000 环境	70-218

本套培训教材都由第一线的微软认证高级技术培训中心讲师（MCT）编写，凝聚了 MCT 们多年教学经验，符合中国人阅读习惯，教材的每章都有学习重点，在必要章节附有实验，供学员练习。本套教材还包括大量的模拟试题，所有模拟试题都加入了试题分析和知识点解析以适应不同考生考证使用。力求通过学习本套教材，即可通过 MCSE，MCDBA，MCSA 或 MCP 的考试。

学员通过学习课程 1，2，3，4，5，6，通过对应的考试，可以获得 MCSE 和 MCDBA 两种证书；通过学习课程 1，2，3 或 4，7，通过对应的考试，可获得 MCSA 证书；学习任何一门课程，通过对应的考试，均可获得 MCP 证书。

本套教材既可作为微软认证高级技术培训教材，微软高级技术认证的自学教材，也可供广大网络、数据库技术人员和爱好者学习、参考使用。

编　者

编 者 序

本书《实现 Microsoft Windows 2000 网络基础结构》可以作为“Microsoft 培训与认证”（Microsoft Training And Certification）系列教材之一。

本书包括了安装、配置、管理和支持采用 Microsoft® Windows® 2000 Server 产品的网络基础结构，为读者提供了必要的知识和技能。其中包括如下内容：保证 TCP/IP 网络互连的 Dynamic Host Configuration Protocol Server（DHCP-动态主机配置协议服务器）服务、Domain Name System Server（DNS-域名系统服务器）服务和 Windows Internet Name Service（WINS）的安装、配置、维护和管理；利用 Public Key Infrastructure（PKI-公共密钥基础结构）的证书服务、Internet Protocol Security （IPSec-Internet 协议安全性）配置网络安全性；配置远程访问网络的能力；配置 Web 服务器，如何利用 Internet Authentication Service（IAS-Internet 身份认证服务）集成扩展的远程访问能力；如何管理 Windows 2000 网络，如何利用 Windows 2000 的排故工具和实用程序识别和解决网络问题；如何在 NetWare、Macintosh 和 UNIX 网络之间启用网络连接性；最后介绍了如何利用 Remote Installation Services（RIS-远程安装服务）部署 Windows 2000 Professional。

本书有如下三大特点：

第一，图文并茂。在正文和实验中，大量的图解说明，便于读者对内容的理解。

第二，从第 2 单元开始包括课后实验。这些实验都是经过精心设计，为读者进一步了解本单元内容、Windows 2000 网络基础结构、和提高操作技巧和能力很有帮助。

第三，从第 2 单元开始包括模拟试题。该部分主要是为希望通过微软认证考试的读者设计的，概括了本单元的考点，非常经典，难度与考试相当，而且包括所有的考试题型。如果读者能够弄懂所有的题，通过本课程的认证应该没有问题。

由于时间仓促及编者水平有限，疏漏之处恳请读者批评指正。

第1章 绪 论

- 概述 Windows 2000 网络基础结构
- intranets
- 远程访问和远程办公
- 与 Internet 的连接
- Extranets

在本章中，将学习有关 Windows 2000 网络基础结构的基本要素。

如果你公司的规模比较大，为了保证公司内部有效的通信和资源共享，与外部的交流和合作，公司需要创建计算机网络，并需要专职人员（管理员）进行管理。Windows 2000 提供了一组网络服务组件，这些组件可以为你提供基于标准的网络协议和技术，用来建立可靠的、并且能够协同工作的网络基础结构。

学习目标

- **Windows 2000 网络基础结构** 简要说明典型 Windows 2000 网络基础结构中包含的五种元素：intranet、远程访问、远程办公室、Internet、Extranet。
- **intranets** intranet 作为企业内部网，可以实现公司内部用户共享信息和资源。Transmission Control Protocol/Internet Protocol（TCP/IP 协议）作为业界标准，为网络实现连接提供了基础。
- **远程访问和远程办公** Windows 2000 包括两种远程访问方法：拨号连接和 VPN（虚拟专用网络）。识别这两种类型的远程访问方法及各自的应用场合。在 Windows 2000 网络中，可以利用路由器将远程办公室连接到 intranet，从而实现资源的共享和远程办公。
- **与 Internet 的连接** 建立公司自己的 Web 站点，提供 VPN 远程访问功能，以及用户能够更好地展开研究工作和使用电子邮件通信，则需要与 Internet 互连。通常用来建立 Internet 访问的方法有两种：拨号连接和专用线路。
- **Extranets** 为了更好地宣传公司、增进与顾客的交流、与业务伙伴的合作，你可以配置一个 Extranet（企业外部网），为顾客、供货商和业务伙伴提供有限度的访问你的 intranet 的能力。

1.1 概述 Windows 2000 网络基础结构

利用 Windows 2000 提供的网络服务，你可以更容易地安装、配置、管理和支持网络基础结构。

Windows 2000 网络基础结构包含如下基本要素：

- ***intranet*** 企业内部网络。用于发布公司内部的信息，供公司员工查阅和交流。

intranet 也称为 LAN（local area network—局域网），它包括诸如文档分布、软件共享、数据库接入和员工培训等多种服务。除文件和打印机共享服务外，intranet 还包括一些与 Internet 相关的应用，如 Web 页、Web 浏览器、FTP（File Transfer Protocol）、网址、电子邮件、新闻组以及只供公司内部员工访问的邮政列表。

- **Remote Access and Remote Office（远程访问和远程办公室）** 为远程办公、移动工作者、以及监视和管理多个部门服务器的系统管理员提供远程网络技术。可供 LAN（Local Area Network — 局域网）连接的用户使用的服务，包括文件共享和打印机共享、访问 Web 服务器和消息发布，通常都可以通过远程访问连接使用。Remote Office 属于公司的组成部分，远程办公室通常在地理位置上处于独立区域。可以将远程办公室中的 LAN 连接到公司的总部，这样就创建了 WAN（wide area network—广域网）。WAN 连接就是到网络的共享远程访问连接。利用 WAN 连接，远程办公室中的所有用户可以在整个公司内部进行相互通信和资源共享。WAN 连接属于永久性链接，它们任何时候都可用。而典型的远程访问连接总是处于连接状态；在不使用时需要将其连接断开。
- **Internet** 这是一个全球范围内的网络和网关的集合。它利用 Transmission Control Protocol/Internet Protocol（TCP/IP）这一组协议进行相互之间的通信。Internet 的主要节点或主机之间用高速数据通信链路进行连接。这些主机包括成千上万的计算机系统，有商用的、政府的、教育部门的以及其他各式各样的计算机系统。主机用于发送数据和消息。
- **Extranet（企业外部网）** 是一种协作式网络，采用 Internet 技术，用于公司和它们的供应商、合作伙伴、顾客以及其他公司之间的通信联系。Extranet 可以是一家公司的 intranet 的组成部分，可以被其他公司访问；Extranet 也可以是一个共享网络，是多家公司进行相互协作的产物。其中的共享信息可以只供参与协作的各成员使用；某些情况下，也可能是完全向公众开放的信息。

为了建立网络基础结构，必须正确配置供网络基础结构中各个元素使用的所有必需的网络协议、设置值以及服务等。

1.2 intranets

利用 intranet，公司内部的用户就可以共享信息和资源了。TCP/IP 为计算机互连提供了基础，计算机通过互连就构成了 intranet。

intranet 属于公司内部专有网络，它将公司内的计算机链接在一起，彼此互通。这样，使得公司内部的用户可以实现信息和资源的共享。

TCP/IP 为网络连接提供了基础。TCP/IP 是一组网络协议，为业界所公认的一个工业标准。Windows 2000 中的大多数网络服务都建立在 TCP/IP 协议之上。TCP/IP 的可伸缩性使得它可以适应各种大小规模的网络。Windows 2000 实现的 TCP/IP（TCP/IP 是在 Windows 2000 安装过程中默认安装的网络协议）包括了所有标准的、针对 TCP/IP 主机和服务器的 Internet Engineering Task Force（IETF）需求条件。

TCP/IP 的正常工作依赖于所谓的名称解析功能。利用名称解析功能，用户可以采用他们容易记住的服务器名，而不要求记住与该服务器相对应的由一串数字构成的 IP 地址。在 TCP/IP 网络中，正是这种 IP 地址标识了服务器本身。

1.3　远程访问和远程办公

可以通过配置远程访问，为已授权的用户提供到公司网络的连接。这样，远程访问客户机可以从远程访问公司网络资源，就好像它们和网络之间存在直接的物理连接一样。

1.3.1　远程访问方法

Windows 2000 提供了两种的不同类型的远程访问连接方法：

- **Dial-up remote access（拨号远程访问）**　要实现拨号连接，首先需要远程访问客户机通过公共电话网络创建到远程访问服务器上的一个端口的物理连接，远程访问服务器驻留在专用网络上。然后远程客户机利用一个调制解调器或 ISDN（Integrated Services Digital Network—综合业务数字网）适配器，通过拨号就可以访问远程访问服务器了。
- **VPN—virtual private network（虚拟专用网络）**　可以通过 Internet 提供可靠的远程访问，而非通过直接拨号连接。通常，利用 VPN 远程访问技术时，你首先连接到 Internet 上，然后再在 VPN 客户机与驻留在专用网络上的 VPN 网关之间创建一个加密的、虚拟的点对点连接。

在决定远程访问解决方案时，你需要根据你的远程访问需求，选用一种远程访问方法，也可以部署两种方法。例如，某些机构采用 VPN 作为主要的远程访问连接技术，当 Internet 访问不可用时，则采用拨号连接技术。

拨号远程访问和 VPN 分别用于如下场合：

- 如果公司的远程用户较少，并且这些公司具有足够的模拟或者 ISDN 性能，或者它们的远程用户位于本地电话区号之内，拨号远程访问就可以满足这些公司的需求。
- VPN 远程访问办法可以降低公司的长途电话费用，并且可以利用现有的 Internet 网络基础结构，降低成本。如果远程用户数目和长途电话费用在快速增加，或者需要附加带宽支持时，则考虑采用 VPN 解决方案。

1.3.2　远程办公室

如果公司有自己的 intranet，同时也有分布在外地的办公室（如各地的销售点），就可以利用路由器将远程办公室连接到 intranet 上。其中路由器的作用是建立 LANs 之间的链路，使得它们彼此之间可以通信。

许多公司为了扩大规模，常常扩充一个或多个远程办公室，而与每个远程办公室之间用 LAN 进行连接。这样公司可以更加有效地运转。例如，远程办公室的雇员可以更容易地与公司总部的雇员共享信息和进行通信。另外，那些到其他办公室出差的雇员也可以从任何远程办公室访问需要的文件和资源。

你可以利用 IP 路由器将 TCP/IP 网络段连接在一起，因为 IP 路由器可以实现将数据包从一个网络段向另一个网络段进行转发。在基于 TCP/IP 的大型网络内，联合利用路由技术和其他的一些网络协议服务，可以为位于不同网络段上的主机提供转发功能。

1.4 与 Internet 的连接

很多公司要求具有访问 Internet 的能力，用以建立公司自己的 Web 站点，提供 VPN 远程访问功能，以及使用户能够更好地展开研究工作和使用电子邮件通信。

Windows 2000 提供了这种专门的服务，可以让公司连接到 Internet，而又不损失安全性、可靠性和性能。

访问 Internet，主要有两种方法：

- **拨号连接到 ISP** 这种方法主要用于小规模的公司和机构及家庭计算机用户。
- **专用线路** 例如连接到某个 LAN 的 T1 载波。这种方法供大型机构采用。这些机构在 Internet 上有他们自己的节点，或它们连接到某个 Internet 节点的 ISP。

1.5 Extranets

为了更好地宣传你的公司、增进与顾客的交流、与业务伙伴的合作，你可以配置一个 Extranet（企业外部网），为顾客、供货商和业务伙伴提供有限的访问你的 intranet 的能力。

利用 Extranet，公司可以将它的网络扩展到顾客、供货商和其他业务伙伴，以达到信息共享的目的。通过 Extranet，处于网络之外的用户可以有限的访问你的 intranet 上的信息。这种限度根据指定给他们的权限级别确定。

Windows 2000 提供了专门功能，用于简化配置 Extranet 的过程，以及保护 intranet 避免未经授权的访问。典型情况下，Extranet 通过可信赖的 VPN 连接提供。可以配置这样的 VPN 连接，使之满足特定需要。例如，业务伙伴可能需要访问 Extranet，一个部门可能需要访问另一个部门的 intranet，也可能想有选择地向公众开放你的 intranet。

1.6 小 结

本章概要说明了 Windows 2000 网络基础结构，初步介绍了 intranets、远程访问方法、远程办公室、访问 Internet、Extranets 等基本要素。

第 2 章　实现名称解析的 DNS 服务

- DNS 概述
- DNS 的工作过程
- 在网络中实现 DNS 服务
- 配置 Hosts File（主机文件）
- 配置 DNS 服务器
- 利用 DNS 实现负载均衡
- 实现区域动态更新
- 在企业内部配置 DNS 服务
- 维护 DNS 服务器

本章将学习如何在 Windows 2000 中安装、配置、管理、监视 DNS Server（域名系统服务器）服务，并排除其中的故障。

在一个基于 IP（Internet Protocol）的网络中，DNS（Domain Name System—域名系统）是通过客户机 / 服务器方式来实现通信的，它是一个分布式数据库。在 IP 网络中，DNS 将网络中计算机的名称解析为对应的 IP 地址，其中的计算机名称称为 FQDN（Full qualified domain name）。

在基于 Windows 2000 的网络中，主要利用 DNS 进行名称解析。基于 Windows 2000 的客户机利用 DNS Server（域名系统服务器）服务进行名称解析，以及查询提供用户身份认证的域控制器的位置。

学习目标

- **DNS 的工作过程**　描述在 DNS 中可以执行的两种类型的查询过程：递归查询和迭代查询，并描述可以针对 DNS 查询指定的两种 lookup（查找）类型：正向查找和逆向查找。
- **在网络中实现 DNS 服务**　安装 Windows 2000 域名系统服务器服务的 Windows 2000 Server 必须配置静态 IP 地址和必要的 TCP/IP 参数，利用“Windows 组件”的“网络服务”向导进行安装。如果某台计算机希望通过 DNS 服务器进行名称解析，则需要配置 DNS 参数选项。
- **配置 Hosts File（主机文件）**　主机文件是纯文本文件，它包含了网络中存在的主机的主机名与其 IP 地址的映射关系，这些映射关系需要用户手工写入。在 DNS 服务成为 Internet 上的名称解析服务标准之前，首先利用主机文件将计算机名解析为它所对应的 IP 地址的，Windows 2000 也可以利用本地的主机文件来进行名称解析。
- **配置 DNS 服务器**　针对 DNS 查询创建两种查找类型：正向查找和逆向查找区域。在一台 DNS 服务器上可以同时创建一个标准主区域（作为主服务器）和另一个区域的

标准辅助区域（作为辅助服务器）。而且可以在区域中添加主机或别名记录。可以在现有区域中创建子域。通过配置区域传输，如修改SOA资源记录、设置安全性和通知消息等，实现区域传输。利用Active Directory集成区域的优势，将区域配置为Active Directory集成的区域，而且可以将现有的区域转换为Active Directory集成的区域。同时，可以将给予BIND的DNS服务器迁移为Windows 2000 DNS服务器，并重新命名区域文件。

- **利用DNS实现负载均衡** 利用DNS服务所提供的round robin功能可以在同一网络中配置多台服务器提供相同服务，从而减轻一台服务器的负荷；还可以通过设置Enable netmask ordering启用子网优先来实现在不同子网中配置相同的服务器。
- **实现区域动态更新** 利用动态更新协议，客户计算机将能够自动更新它们在DNS服务器上的资源记录，而无需管理员手工输入或修改。默认情况下，所有基于Windows 2000的计算机被配置为支持动态更新。这将大大减轻管理员对DNS服务器的管理负担。运行早期版本的Windows客户机不支持动态更新的功能，为了实现这个功能，你必须配置DHCP服务器，和DHCP客户机，使他们都支持动态更新。你可以配置DNS服务器，使之可以针对Active Directory集成区域执行安全的动态更新。
- **在企业内部配置DNS服务** 当intranet没有连接到Internet，或者公司通过某个代理服务器连接到Internet上时，需要在intranet中的某个DNS服务器上配置一个根区域，以使名称解析开始于你的内部的根域，而非Internet的根域。
- **维护DNS服务器** DNS服务器对于网络来说非常关键，必须对它们进行日常维护和进行故障排除，以及优化DNS名称解析的性能。可以通过配置caching-only（高速缓存）服务器，用以降低与DNS有关的网络数据流量，从而改进DNS的性能。也可以通过维护资源记录信息，以确保DNS服务器上的各种记录信息是最新的。配置DNS服务器立即执行查询来测试监测“域名系统服务器”服务，利用事件日志则可以监测“域名系统服务器”服务。利用Nslookup实用程序确认资源记录已经被正确添加或修改。当网络中发生名称解析问题时，分别在客户机上排除名称解析问题、排除区域传输问题。

2.1 DNS概述

2.1.1 主机名称

主机名是一个用户友好的名称，它分配给用于标识TCP/IP主机的某台计算机的IP地址。主机机名可以长到255个字符，可以包含字母、数字、字符“.”以及字符“-”。对同一台主机可以指定多个主机名。对于基于Windows 2000的计算机来说，主机名不一定要与Windows 2000的计算机名相同。

Windows Winsock程序，如Internet Explorer和FTP实用程序，可以使用待连接目标的两个值中的一个：IP地址或主机名。指定IP地址时，不需要名称解析。指定主机名时，主机名必须首先解析为IP地址才能与所需资源进行基于IP的通信。

主机名可以采用不同形式，最通用的两种形式是昵称和域名。昵称是个人指派并使用

的 IP 地址的别名。如：计算机名为 rack；域名是 DNS 的分层结构名称空间中的结构化名称，如 www.BHP.com.cn。昵称通过 Hosts 文件中的记录来解析，Hosts 文件存储在 systemroot\System32\Drivers\Etc 文件夹中；域名是向所配置的 DNS 服务器发送 DNS 名称查询请求解析得到的名称。

2.1.2　DNS 的功能

在一个基于 TCP/IP 的网络中，IP 地址唯一标识一台计算机。如果某台计算机想访问网络中其它计算机，它就应该知道对方的 IP 地址。但在实际中，用户在访问网络中的资源时，一般并不使用对方的 IP 地址去访问对方，而是通过容易记忆的计算机名来访问。这就造成了一个矛盾，用户希望使用方便的、容易记忆的计算机名去访问网络中的资源，而计算机则必须要知道对方的 IP 地址才能访问对方。

如何来解决这个矛盾呢？Windows 2000 提供的 DNS 服务可以解决这个矛盾。DNS 的作用就是把用户习惯使用的计算机名翻译为计算机可以理解的 IP 地址，这个翻译的过程又称为解析。DNS 能够解析的名称为 FQDN（Full Qualified Domain Name）。

在 Windows 2000 中安装和配置域名系统服务器服务之前，我们首先回顾一下 DNS 的基本概念。

- DNS 是一个分布式的数据库系统，用于在基于 IP 的网络中进行名称解析。
- 域名空间的层次结构为：根域位于这个结构的顶层，用一个英文句号表示。在根域下方是顶级域，例如 com 代表商业，edu 代表教育等；另外还可以用地理位置来表示，例如 cn 代表 China（中国）。二级域通常由个人，公司或大的组织所注册，并且二级域下还可以有很多子域。
- FQDN（fully qualified domain name—完全符合标准的域名）。DNS 利用 FQDN 将主机名解析为它所对应的 IP 地址。
- 对位于某个 Zone（区域）的计算机来说，它们的名称与 IP 地址的对应关系存储在 DNS 服务器的区域数据库文件中。
- forward lookup（正向查找）的目的是将计算机的名称解析为它所对应 IP 地址。当客户机发出一个正向查找时，如果本地的 DNS 服务器不具备解析该域的名称的权限，它就向根区域的 DNS 服务器发送一个查询请求。

2.1.3　DNS 的 Name Space（名称空间）

DNS 的名称空间是一个分层次的树形结构。在这个树形结构的最顶层称为 Root 根，也称为根域，用“.”来表示。如图 2-1 示的实例。

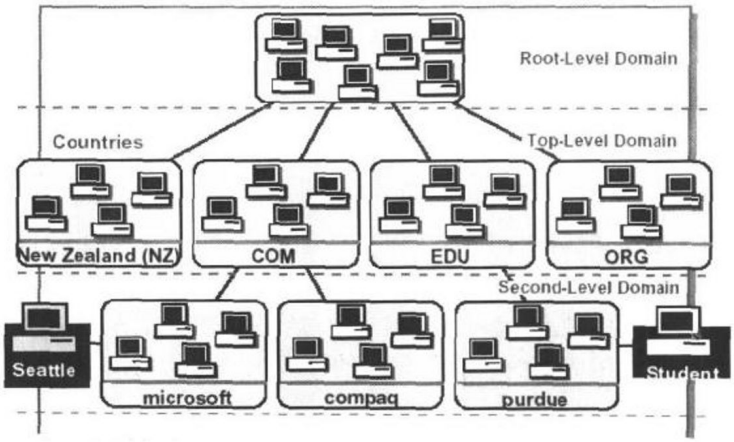


图 2-1 DNS名称空间的实例

在根域的下方是顶级域。顶级域根据其功能的不同分为七个域，如表 2-1 所示的前七个域名。另外每个国家有自己的一个顶级域名。在顶级域下面是二级域，二级域通常由某些大公司或组织注册。

表 2-1 各顶级域的简单介绍

级域	描述	域名举例
.com	代表商业性的公司或组织，例如微软公司	Microsoft.com
.edu	代表各种教育组织，大学等	Tinghua.edu
.gov	代表政府机构	whitehouse.gov
.int	代表国际性的组织，例如：北大西洋公约组织	Nato.int
.mil	代表军事组织	ddn.mil
.net	代表各种网络公司或组织，例如ISP（Internet 服务提供商）	263.net
.org	代表各种非营利性组织	Cnidr.org
.cn	每个国家有一个两位字符的顶级域名，例如cn代表中国	hopepress.cn

二级域以下的域统称为子域，在子域和二级域下都可以连有计算机。我们这里所说的连有计算机不是指网络上的物理连接，而是指在DNS中名称上的逻辑关系。

DNS服务器管理名称和IP地址的对应关系，不是以Domain（域）为单位进行的,而是以Zone（区域）为单位进行管理的。Zone是指DNS名称空间中一个连续的范围，如图 2-2 所示：

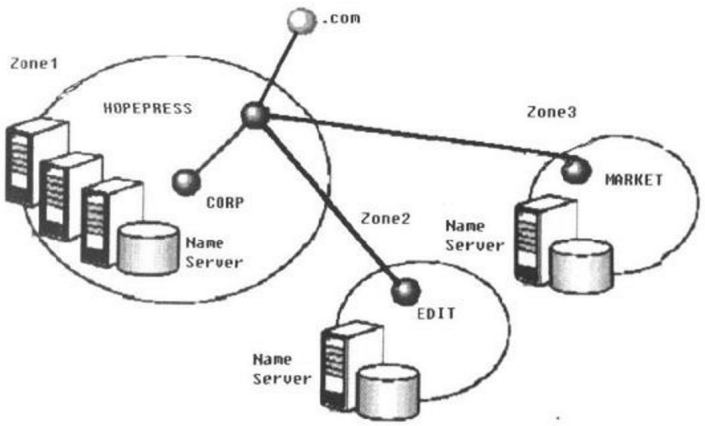


图 2-2　zone（区域）的实例

在图 2-2 中，由于 hopepress.com 域的数据库较大，因此为了管理方便可以把 hopepress.com 域划分为三个 Zone，hopepress.com Zone，edit.hopepress.com Zone，market.hopepress.com Zone。每个 Zone 必须有一台 DNS 服务器进行管理，一台 DNS 服务器可以管理多个 Zone。

2.2　DNS 的工作过程

DNS 是基于客户机 / 服务器模式运行的。在这种模型中，DNS 服务器上有一个数据库，其中保存着 DNS 名称空间中名称和 IP 地址的映射关系；而且 DNS 服务器利用这个数据库为客户端提供名称解析服务。这个数据库在 DNS 中被称为 Zone（区域）。DNS 客户机会向 DNS 服务器发出名称解析的查询请求，以获取有关 DNS 名称空间中 FQDN 名和 IP 地址的映射关系，如果这台 DNS 服务器的数据库不负责存储客户端所查询的名称和 IP 地址的映射关系，这台服务器会向其他的 DNS 服务器发出查询，直到获得客户端请求的名称和 IP 地址的映射关系为止。

2.2.1　DNS 组件

DNS 系统的实现依赖于如下一些 DNS 组件：

- **DNS 服务器**　运行 DNS 服务器端软件的计算机，负责存储有关 DNS 域树结构的 DNS 数据库，同时也负责响应客户机的查询。客户机查询时，DNS 服务器返回客户机所请求的映射信息；如果服务器不能解析客户机请求，则返回其他 DNS 服务器地址作为客户机继续查询的目标。
- **DNS Resolver（解析器）**　使用 DNS 查询信息向服务器请求名称解析的客户端程序。该程序既可与远程 DNS 服务器通信，也可与本机运行的 DNS 服务器通信。解析器可以在任何计算机上运行。
- **资源记录**　能够处理客户查询的 DNS 数据库信息。每个 DNS 服务器都包含若干资源记录，用以答复其负责的 DNS 空间的查询请求。
- **Zone（区域）**　服务器权限内的一部分 DNS 名称空间。一个服务器可以维护一个或

多个区域。

- **Zone file（区域文件）** 存储在区域中创建的资源记录。这些资源记录既可将主机名称解析为IP地址，也可将IP地址解析为主机名。

2.2.2 查询过程

在DNS中，查询请求有两种类型：递归查询和迭代查询。

- **Recursive（递归）查询** 服务器会解析客户端所查询的名称，如果解析成功，那么DNS服务器将把解析到的IP返回给客户端。如果解析不到，那么DNS服务器将向客户端返回一个错误信息，报告指定的名称不存在。并且该DNS服务器不会让客户端向其他的DNS服务器去查询。
- **Iterative（迭代）查询** 如果某台DNS服务器收到一个迭代查询，那么它会在自己的高速缓存或区数据库中查找客户端请求的记录。如果解析不到，它将向客户端返回另外一台DNS服务器的IP地址，客户端将向这台服务器发出查询请求，然后将重复这一过程，直到客户端找到了一台能够将它所请求的名称解析为IP的这样一台DNS服务器。

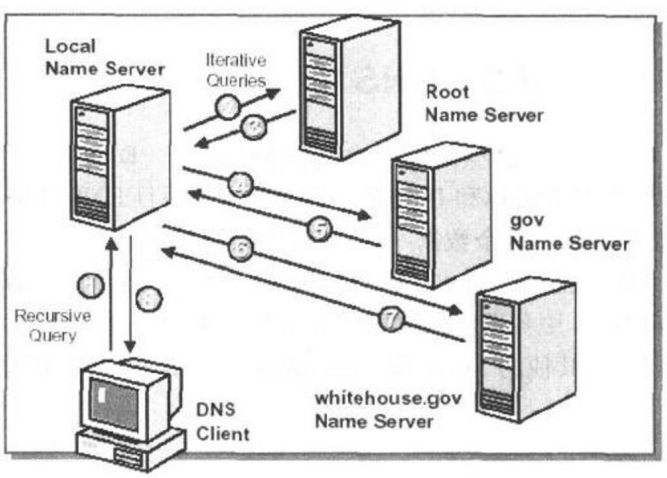


图2-3 DNS查询过程

下面举例说明DNS递归和迭代查询的过程，如图2-3所示，客户机需要访问名为www.whitehouse.gov的计算机，客户端需要知道这台计算机的IP地址。其查询过程如下：

1. 客户机向Local DNS Server（本地的DNS服务器）发送一个递归查询请求，要求得到www.whitehouse.gov所对应的IP地址。这个本地的DNS服务器是指在该客户端的TCP/IP属性中配置的DNS服务器的IP地址。
2. 这台本地的DNS服务器接收到查询请求后，检查自己的区域数据库，发现数据库中没有对应的记录。这时本地的DNS服务器向根域的DNS服务器发出一个迭代查询请求，要求解析www.whitehouse.gov所对应的IP地址。
3. 在根域的DNS服务器中记录着所有顶级域的DNS服务器的信息，根域的DNS服务器将带有.gov这一顶级域的DNS服务器的IP地址的响应返回给本地的DNS服务器。

4. 本地的 DNS 服务器接收到这个响应后，向.gov 域的 DNS 服务器发出迭代查询请求，要求解析 www.whitehouse.gov 所对应的 IP 地址。
5. .gov 域的 DNS 服务器中记录着 whitehouse.gov 域中的 DNS 服务器的信息，.gov 域的 DNS 服务器将 whitehouse.gov 域的 DNS 服务器的 IP 地址作为响应发送给本地的 DNS 服务器。
6. 本地 DNS 服务器接收到这个响应后，向 whitehouse.gov 域的 DNS 服务器发出迭代查询请求，要求解析 www.whitehouse.gov 所对应的 IP 地址。
7. 在 whitehouse.gov 域的 DNS 服务其中记录着 www.whitehouse.gov 这一 FQDN 名与其 IP 地址的对应关系，此时，它将 www.whitehouse.gov 所对应的 IP 地址作为响应发送给本地的 DNS 服务器。
8. 本地的 DNS 服务器将得到的 IP 地址响应给 DNS 客户端，客户端收到这个 IP 后，即可访问目的计算机。

综上所述，1，8 两个过程为递归查询；2~7 为迭代查询。

2.2.3　查找类型

DNS 服务器如果想为客户端提供名称解析的服务，那么在服务器上必须要创建 Zone，也就是保存名称和 IP 映射关系的数据库。

当在 DNS 服务器上创建 Zone 时，必须指定所建的 Zone 的类型。有两种查找类型：

- **Forward lookup（正向查找）**　这是最常用的查询类型，将客户端请求的名称解析为对应的 IP 地址。例如：某 DNS 客户机想知道域名为 robe.edit1.hopepress.cn 的 IP 地址，则发出一个类似 IP address for robe.edit1.hopepress.cn 的正向查找请求，DNS 服务器将返回 robe.edit1.hopepress.cn 的 IP 地址：192.168.0.9。
- **Reverse lookup（逆向查找）**　如果知道某台计算机的 IP 地址，但是还想知道该 IP 地址所对应的域名，那么就可以通过逆向查找来实现。例如，正在监测某个服务器的基于 IP 的连接，就可以利用逆向查找获得与该服务器连接的计算机的 IP 地址相关联的域名信息。例如：某 DNS 客户机想知道 IP 地址为 192.168.0.9 的主机名，则发出一个类似 Name for 192.168.0.9 的逆向查找请求，DNS 服务器将返回该 IP 地址对应的域名称：robe.edit1.hopepress.cn。

2.3　在网络中实现 DNS 服务

如果想在网络中利用 DNS 服务来实现名称解析的功能，那么我们必须在网络中安装 DNS 服务，并设置 DNS 客户端。而且，DNS 系统的实现依赖于一些 DNS 组件。

2.3.1　安装 DNS 服务

可以在一台运行 Windows 2000 Server 的计算机上安装 DNS Server 服务来创建一个 DNS 服务器。

配置TCP/IP

在默认情况下，每台运行Windows 2000的计算机都配置为从某台DHCP服务器接收TCP/IP协议的配置信息。为了配置TCP/IP，必须在安装DNS Server服务的计算机上，在Protocol（TCP/IP）Properties（Internet协议（TCP/IP）属性）对话框中指派一个静态的IP地址。

同时，Microsoft建议在安装DNS Server服务的计算机上首先配置域名称。

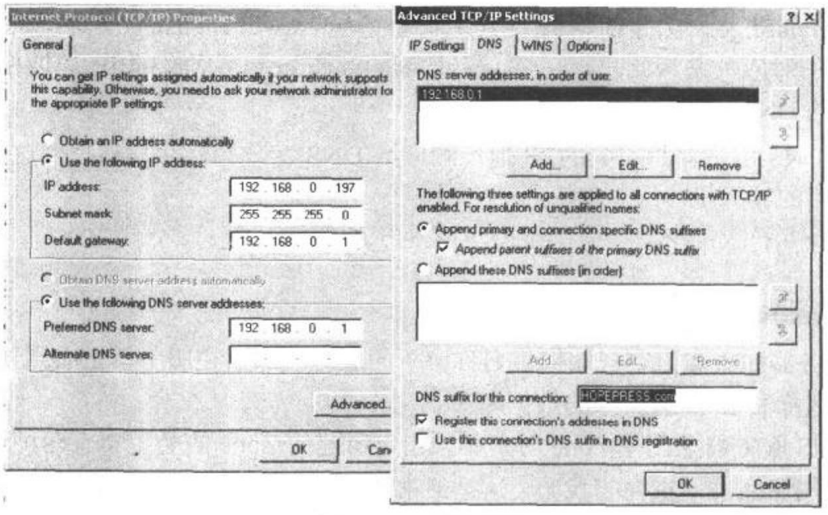


图2-4 配置域名称

配置域名称，按如下步骤操作：

1. 打开你正在配置的网络连接的Properties对话框。
2. 单击Internet Protocol（TCP/IP），然后单击Properties。
3. 在Internet Protocol（TCP/IP）Properties对话框中，如图2-4的左图所示，单击Advanced按钮。
4. 在Advanced TCP/IP Settings（高级TCP/IP设置）对话框中的DNS选项卡下，如图2-4的右图所示，确认DNS server addresses, in order of use（DNS 服务器地址使用顺序）框中的DNS地址是正确的。
5. 在DNS suffix for this connection（本连接的DNS后缀）框中键入该域的名称，然后单击OK按钮。

DNS（域名系统服务器）服务安装进程

安装DNS（域名系统服务器）服务，按如下步骤操作：

1. 在Control Panel上，单击Add/Remove Programs(添加/删除程序)，然后单击Add/Remove Windows Components（添加/删除Windows组件）。
2. 在Windows Components向导的Windows Components页上，单击Networking Services（网络服务），然后单击Details（详细资料），出现如图2-5所示的界面。
3. 选择Domain Name System（DNS）复选框，然后单击OK按钮。