

Windows Server 2003

网络专业指南

- DHCP服务器、WINS服务器、DNS服务器
- PKI、电子邮件的加密与验证、IPSec
- 远程访问、虚拟专用网(VPN)、RADIUS、路由器、桥接器
- NAT、基本防火墙、终端服务器、远程管理
- IIS网站、SSL安全连接
- FTP服务器、电子邮件服务器、NNTP服务器
- 远程安装(RIS)、网络监视器

戴有炜 编著



清华大学出版社

Windows Server 2003

网络专业指南

戴有炜 编著

清华大学出版社
北 京

内 容 提 要

这是台湾操作系统资深人士戴有炜先生针对 Windows Server 2003 推出的又一力作,旨在引导读者轻松搭建自己的网络服务,并根据实际需求完成必要的配置和管理。

书中秉承作者务实的写作风格,并融合其多年的教学经验,按照 MCSA/MCSE 认证考试的要求,循序渐进组材。全书共 17 章,内容包括:Windows Server 2003 的网络功能,利用 DHCP 自动分配 IP 地址,解析 NETBIOS 名称,PKI、IPSec 与网络安全,远程访问与 VPN, RADIUS 与 IAS 服务器, Windows Server 2003 路由器, NAT 与基本防火墙, SSL 网络安全连接, 终端服务器、IIS 网站、FTP 站点、电子邮件服务器、NNTP 服务器的安装与设置, 远程安装服务等。

本书突出实用性和可操作性,语言精炼,通俗易懂,配有大量演示性图例。适于网络管理人员学习,并可作为 MCSA/MCSE 认证考试的教学参考书,还可供高校相关专业和各类培训班用作教材。

版 权 声 明

本书为经台湾基崙资讯股份有限公司独家授权发行的中文简体字版本。本书中文简体字版在中国大陆之专有出版权属清华大学出版社所有。在没有得到本书原版出版者和本书出版者书面许可时,任何单位和个人不得擅自摘抄、复制本书的一部分或全部以任何方式进行传播。本书原版版权属基崙资讯有限公司。版权所有,侵权必究。

北京市版权局著作权合同登记号 图字: 01-2004-1118

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

Windows Server 2003 网络专业指南/戴有炜编著.

—北京:清华大学出版社,2004.4

ISBN 7-302-08508-0

I. W… II. 戴… III. 服务器—操作系统(软件), Windows Server 2003 IV. TP316.86

中国版本图书馆 CIP 数据核字(2004)第 035510 号

出 版 者: 清华大学出版社

<http://www.tup.com.cn>

社总机: 010-62770175

地 址: 北京清华大学学研大厦

邮 编: 100084

客户服务: 010-62776969

组稿编辑: 科海

文稿编辑: 徐建军

封面设计: 杨月静

版式设计: 佩芸

印 刷 者: 北京科普瑞印刷有限责任公司

发 行 者: 新华书店总店北京发行所

开 本: 787×1092 1/16 印张: 35.375 字数: 860 千字

版 次: 2004 年 6 月第 1 版 2004 年 6 月第 1 次印刷

书 号: ISBN 7-302-08508-0/TP·6111

印 数: 1~5000

定 价: 53.00 元

(如有印装质量问题,我社负责调换)

出版说明

《Windows Server 2003 用户管理指南》、《Windows Server 2003 网络专业指南》和《Windows Server 2003 Active Directory 配置指南》是我国台湾地区的资深 Windows 培训专家和咨询顾问戴有炜先生的最新力作。

戴有炜先生历任微软认证讲师、微软认证系统工程师、微软资深顾问、综合生活股份有限公司技术支援部技术总监和教育训练中心讲师,拥有十几年使用、咨询和讲授 Windows 操作系统的成功经验,并于 1997 年编撰出版了《Windows NT Server 4.0 专业指南》和《Windows NT Server 4.0 实用指南》,于 2000 年推出了升级版《Windows 2000 网络实用指南》和《Windows 2000 网络专业指南》,这 4 种图书的简体中文版销售累计超过 30 万册,被誉为 Windows NT 4.0 和 Windows 2000 Server 的一般用户和管理员的福音书。

本次推出的 Windows Server 2003 三卷本,秉承了作者一贯的写作风格和体例,凭借丰富的教学与咨询经验,完全从读者使用和学习角度,以详实的步骤与精到的说明教读者迅速掌握 Windows Server 2003,充分考虑读者操作时可能发生的问题,并提供解决方案,还适应 MCSA/MCSE 认证考试的需求,无疑是最佳实践参考书籍。

- ▶ 《Windows Server 2003 用户管理指南》的主要内容是: Windows Server 2003 基本概念、安装 Windows Server 2003、熟悉 Windows Server 2003 环境、创建 Windows Server 2003 域、用户账户的管理、组账户的管理、NTFS 的数据管理功能、访问网络上的文件、分布式文件系统、打印机的设置、设置用户的工作环境、安全设置与审核资源的使用、监控资源的访问行为、注册表编辑器、磁盘系统的管理、自动安装与磁盘复制、系统启动的疑难排除。
- ▶ 《Windows Server 2003 网络专业指南》的主要内容是: Windows Server 2003 的网络功能,利用 DHCP 自动分配 IP 地址,解析 NETBIOS 名称,PKI、IPSec 与网络安全,远程访问与 VPN, RADIUS 与 IAS 服务器, Windows Server 2003 路由器, NAT 与基本防火墙, SSL 网络安全连接,终端服务器、IIS 网站、FTP 站点、电子邮件服务器、NNTP 服务器的安装与设置,远程安装服务等。
- ▶ 《Windows Server 2003 Active Directory 配置指南》的主要内容是: Active Directory 概论、建立 Windows Server 2003 域、域用户与组账户的管理、组策略、利用组策略部署软件、软件限制策略、建立域树与林、域信任关系、Active Directory 的复制、操作主机的管理、Active Directory 数据库的维护、将资源公布到 Active Directory、自动信任根 CA、Active Directory 与防火墙、自定义 MMC 等。

Windows NT Server 系列和 Windows 2000 系列出版以来,一直受到广大读者的好评和厚爱,希望本次推出的 Windows Server 2003 系列也能对用户有所帮助,继续得到读者朋友的支持。

序

首先要感谢读者长期以来的支持与爱护！本书仍然采用我一贯的写作风格，也就是完全站在读者的角度考虑问题，并且以实用的观点来编写这三本 Windows Server 2003 的书籍。我花费相当多的时间不断测试与验证书中所叙述的内容，并融合多年的教学经验，然后以最容易让您理解的方式将其写到书内。书中完整和清晰的操作步骤，让您能够轻松地安装与使用 Windows Server 2003。

长期以来，对需要参加 MCSA/MCSE 认证考试的读者来说，研读官方的原文教材是一件苦差事，读起来似懂非懂又不知如何操作，而其他引进的英文书籍也一样难以消化，中文翻译书又大都翻译的很“英式中文”，还不如看原版书。现在这些读者有福了，本书特别考虑到 MCSA/MCSE 认证考试的需求，是非常适合这些读者阅读的中文参考书籍，尤其是在实践方面。

本套丛书包括《Windows Server 2003 用户管理指南》、《Windows Server 2003 网络专业指南》、《Windows Server 2003 Active Directory 配置指南》3 本，内容丰富详实，相信这几本书，仍然会不辜负您的期望，在您学习 Windows Server 2003 时，将给予您最大的帮助。

感谢所有让这本书能够顺利出版的朋友们，特别是花费很多精力帮我校稿的李尚白先生，还有“综合生活股份有限公司”，这家专门承接微软技术支持项目的公司，为我提供了各种最新、最快的资源与各种测试设备。

戴有炜
2004 年 1 月

目 录

第 1 章 Windows Server 2003 的网络功能..... 1

- 1.1 Windows Server 2003 所提供的网络功能..... 2
- 1.2 TCP/IP 通信协议..... 2
 - 1.2.1 IP 地址 (IP Address) 2
 - 1.2.2 IP 地址的类别 3
 - 1.2.3 子网掩码 (subnet mask) 4
 - 1.2.4 利用子网掩码来划分子网..... 5
 - 1.2.5 默认网关 (default gateway) 7
 - 1.2.6 私有 IP (Private IP) 的使用 8

第 2 章 利用 DHCP 自动分配 IP 地址..... 9

- 2.1 IP 地址的配置..... 10
- 2.2 DHCP 的运行原理..... 11
 - 2.2.1 从 DHCP 服务器获取 IP 地址..... 11
 - 2.2.2 更新 IP 地址的租约 13
 - 2.2.3 自动分配私有 IP 地址 14
- 2.3 安装 DHCP 服务器..... 14
- 2.4 DHCP 服务器的授权..... 16
 - 2.4.1 DHCP 授权的原理与注意事项 16
 - 2.4.2 执行 DHCP 授权的工作 17
- 2.5 IP 作用域的建立与管理..... 18
 - 2.5.1 建立 IP 作用域..... 18
 - 2.5.2 租期该设置多久..... 21
 - 2.5.3 建立多个 IP 作用域 22
 - 2.5.4 保留特定 IP 地址给客户端 23
 - 2.5.5 作用域的协调..... 25
 - 2.5.6 安装多台 DHCP 服务器 25
- 2.6 DHCP 客户端的配置..... 26
- 2.7 配置选项..... 28
 - 2.7.1 DHCP 配置选项的等级 28

- 2.7.2 DHCP 的类别选项 31
- 2.8 DHCP 中继代理..... 35
 - 2.8.1 配置 DHCP 中继代理 37
- 2.9 超级作用域与多播作用域..... 42
 - 2.9.1 超级作用域..... 42
 - 2.9.2 多播作用域..... 44
- 2.10 DHCP 数据库的维护..... 46
 - 2.10.1 数据库的备份 46
 - 2.10.2 数据库的还原..... 47
 - 2.10.3 数据库的重整..... 47
 - 2.10.4 将 DHCP 数据库转移到其他的服务器..... 48

第 3 章 解析 NetBIOS 名称..... 49

- 3.1 利用 NetBIOS 名称与其他计算机通信 50
 - 3.1.1 何谓 NetBIOS 名称..... 50
 - 3.1.2 通过 NetBIOS 名称来解析 IP 地址..... 51
 - 3.1.3 NetBIOS 节点类型 52
- 3.2 使用 LMHOSTS 文件..... 53
 - 3.2.1 LMHOSTS 文件的内容 54
 - 3.2.2 了解 LMHOSTS 的运行 55
 - 3.2.3 集中管理 LMHOSTS 文件 55
 - 3.2.4 启动 LMHOSTS 文件 56
- 3.3 WINS 的操作原理 57
 - 3.3.1 名称注册..... 57
 - 3.3.2 更新注册的名称..... 58
 - 3.3.3 名称查询..... 58
 - 3.3.4 名称释放..... 58
- 3.4 WINS 服务器的安装与客户端的配置... 59
 - 3.4.1 WINS 服务器的安装..... 59
 - 3.4.2 WINS 客户端的配置..... 60



3.4.3 DHCP 客户端的 WINS 配置	61	4.3 区域的建立	89
3.4.4 检查 WINS 服务器的数据库	61	4.3.1 区域的类型	89
3.4.5 删除 WINS 服务器内的记录	64	4.3.2 建立主要区域	90
3.5 对非 WINS 客户端的支持	65	4.3.3 在主要区域内新建资源记录	92
3.5.1 静态映射	66	4.3.4 建立辅助区域	97
3.5.2 WINS Proxy 的配置	67	4.3.5 建立反向区域与新建反向记录	100
3.6 WINS 数据库的复制	68	4.3.6 子域与委派域	104
3.6.1 复制伙伴 (replication partner)	68	4.3.7 建立存根区域	106
3.6.2 设置复制伙伴	69	4.4 域的设置	110
3.6.3 自动复制的设置	70	4.4.1 更改区域类型与区域文件名称	110
3.6.4 手动立刻复制	71	4.4.2 SOA 与区域复制	111
3.7 修改 WINS 服务器设置值	72	4.4.3 名称服务器的设置	112
3.7.1 常规设置	72	4.4.4 选择与通知区域复制服务器	113
3.7.2 间隔	73	4.4.5 与 WINS 服务器的整合	113
3.7.3 数据库验证	74	4.5 动态更新	115
3.7.4 高级	75	4.5.1 启动 DNS 服务器的动态更新 功能	115
3.8 WINS 服务器数据库的维护	76	4.5.2 DNS 客户端的设置	115
3.8.1 清除数据库	77	4.5.3 DHCP 服务器的动态更新设置	117
3.8.2 验证数据库的一致性和版本的 一致性	77	4.5.4 DnsUpdateProxy 群组	119
3.8.3 备份 WINS 数据库	78	4.6 求助于其他 DNS 服务器	121
3.8.4 还原 WINS 数据库	78	4.6.1 指定 root 服务器	121
3.8.5 数据库的整理	78	4.6.2 转发器的设置	122
第 4 章 解析 DNS 主机名称	79	4.7 检测 DNS 服务器	123
4.1 DNS 概述	80	4.7.1 监视 DNS 设置是否正常	123
4.1.1 DNS 域名空间	80	4.7.2 利用 nslookup 来检查记录	124
4.1.2 区域	81	4.7.3 缓存的清除	126
4.1.3 DNS 服务器	83	第 5 章 PKI 与网络安全	127
4.1.4 Caching-Only Server	84	5.1 PKI 概述	128
4.1.5 查找的模式	84	5.1.1 公开密钥加密法 (Public Key Encryption)	128
4.1.6 反向查找	85	5.1.2 公开密钥验证法 (Public Key Authentication)	129
4.1.7 动态更新	85	5.1.3 证书认证机构 (Certification Authority, CA)	130
4.1.8 缓存文件	85	5.1.4 CA 的信任	131
4.1.9 启动文件	86	5.1.5 CA 的架构	131
4.2 DNS 服务器的安装与客户端的设置	86	5.1.6 CA 的种类	132
4.2.1 DNS 服务器的安装	86		
4.2.2 DNS 客户端的设置	87		
4.2.3 使用 HOSTS 文件	88		

5.2 企业 CA 的安装与证书申请	6.3 彻底了解 IPSec 策略	177
实例演示	6.3.1 因特网密钥交换 (Internet Key	177
6.3.1 安装证书服务并架设企业根	Exchange, IKE)	177
CA	6.3.2 IPSec 策略	180
133		
5.2.2 域用户如何向企业 CA 申请	第 7 章 远程访问与 VPN	187
证书	7.1 连接远程访问服务器的方式	188
136	7.1.1 通过 PSTN 连接	188
5.2.3 利用证书来发送经过签名与	7.1.2 通过 ISDN 连接	188
加密的电子邮件	7.1.3 通过 X.25 连接	189
141	7.1.4 直接连接	189
5.2.4 企业从属 CA 的安装	7.1.5 通过虚拟专用网 (VPN) 连接	190
147	7.2 数据传输通信协议	190
5.3 独立根 CA 的安装与证书申请	7.2.1 远程访问通信协议	190
实例演示	7.2.2 局域网通信协议	190
148	7.2.3 IP 路由器	191
5.3.1 安装证书服务并架设独立根	7.2.4 IPX 路由器	191
CA	7.2.5 NetBIOS 网关	192
149	7.3 拨号连接到远程访问服务器	192
5.3.2 用户如何向独立根 CA 申请	7.3.1 架设远程访问服务器	192
证书	7.3.2 给予用户远程访问的权限	196
149	7.3.3 客户端的设置	197
5.3.3 如何信任独立根 CA	7.4 虚拟专用网 (VPN)	200
153	7.4.1 VPN 原理	201
5.4 独立从属 CA 的安装	7.4.2 PPTP VPN 实例演示	202
154	7.4.3 L2TP VPN 实例演示 1——使用	
5.4.1 安装证书服务并架设独立从属	IPSec 证书	211
CA	7.4.4 L2TP VPN 实例演示 2——使用	
154	“预共享密钥”	218
5.4.2 将独立从属 CA 的申请文件	7.5 直接连接	220
传给父 CA	7.5.1 安装两台计算机之间的通讯	
156	电缆	220
5.4.3 安装下载的 CA 证书	7.5.2 服务器端的设置	221
159	7.5.3 客户端的设置	222
5.5 证书的管理	7.6 多重链接与带宽分配协议 (BAP)	224
160	7.6.1 服务器端的多重链接设置	225
5.5.1 CA 的备份与还原	7.6.2 客户端的多重链接设置	225
160	7.7 验证通信协议	227
5.5.2 增加证书模板	7.8 远程访问策略	229
161		
5.5.3 自动或手工发放证书		
162		
5.5.4 吊销证书与证书吊销列表		
(CRL)		
163		
5.5.5 导出与导入用户的证书		
167		
5.5.6 申请一个可以导出私有密钥的		
证书		
169		
5.5.7 更新证书		
170		
第 6 章 IPSec 与网络安全		
173		
6.1 IPSec 概述		
174		
6.2 启动 IPSec		
174		
6.2.1 默认的 IPSec 策略		
174		
6.2.2 启动 IPSec 策略		
176		
6.2.3 IPSec 测试		
176		



7.8.1 新建远程访问策略.....	230	9.5.1 RIP 路由器概述.....	284
7.8.2 是否接受连接的详细流程.....	234	9.5.2 启动 RIP 路由器.....	285
第 8 章 RADIUS 与 IAS 服务器	237	9.5.3 RIP 路由接口的设置.....	287
8.1 RADIUS 与 IAS 的运作流程.....	238	9.5.4 RIP 路由筛选	289
8.1.1 IAS RADIUS 服务器	238	9.5.5 与相邻路由器的互动设置	290
8.1.2 IAS RADIUS 代理服务器	239	9.6 网桥	291
8.2 安装与注册 IAS 服务器.....	241	第 10 章 NAT 与基本防火墙	293
8.2.1 安装 IAS 服务器	241	10.1 NAT 的特色与原理	294
8.2.2 让 IAS 服务器读取 Active Directory 内的用户账户	242	10.1.1 NAT 的网络结构图实例.....	294
8.3 RADIUS 服务器与 RADIUS 客户端的设置	243	10.1.2 NAT 的 IP 地址	296
8.3.1 指定 RADIUS 客户端.....	243	10.1.3 NAT 的工作原理.....	297
8.3.2 设置让远程访问服务器或 VPN 服务器来使用 RADIUS	245	10.2 NAT 架设实例演示	299
8.4 RADIUS 代理服务器的设置.....	247	10.2.1 固定 ADSL 的 NAT 设置	299
8.4.1 连接请求策略.....	247	10.2.2 非固定 ADSL 的 NAT 设置	302
8.4.2 建立远程 RADIUS 服务器组	249	10.2.3 局域网内客户端的设置	309
8.4.3 修改 RADIUS 服务器组的设置	250	10.3 DHCP 分配器与 DNS 代理.....	310
第 9 章 Windows Server 2003 路由器.....	253	10.3.1 DHCP 分配器	310
9.1 路由器的原理	254	10.3.2 DNS 代理.....	311
9.1.1 一般主机的路由表.....	254	10.4 内部网络的开放与防火墙.....	312
9.1.2 路由器的路由表.....	258	10.4.1 NAT 网络接口与防火墙.....	312
9.2 Windows Server 2003 路由器的设置	260	10.4.2 端口映射.....	313
9.2.1 启动 Windows Server 2003 路由器.....	260	10.4.3 地址映射.....	316
9.2.2 检查路由表	262	10.5 Internet 连接共享 (ICS)	317
9.2.3 添加静态路由.....	263	10.6 IPSec 跨越 NAT 的问题	319
9.3 筛选进出路由器的数据包	264	第 11 章 终端服务器的安装与设置	321
9.3.1 入站筛选器的设置.....	265	11.1 终端服务器概述	322
9.3.2 出站筛选器的设置.....	266	11.1.1 终端服务器的功能.....	322
9.3.3 通信协议号与连接端口号	267	11.1.2 客户端的需求.....	322
9.4 请求拨号连接	271	11.2 终端服务器的架设与连接设置.....	323
9.4.1 双向请求拨号连接的设置.....	271	11.2.1 架设终端服务器.....	323
9.4.2 单向请求拨号连接的设置.....	281	11.2.2 客户端安装所需软件.....	324
9.5 动态路由 RIP	283	11.2.3 赋予用户通过终端服务登录的权限	325
		11.2.4 利用“远程桌面连接”来连接终端服务器	327
		11.2.5 注销或中断连接.....	329

11.2.6 远程桌面连接的高级设置	330	12.6.3 远程管理 (HTML)	383
11.3 终端服务的设置	333	12.7 通过 WebDAV 来管理网站上的 资源	385
11.3.1 登录设置	333	12.7.1 启动网站上的 WebDAV 功能	386
11.3.2 远程控制的设置	334	12.7.2 建立 WebDAV 虚拟目录	386
11.3.3 客户端设置	335	12.7.3 WebDAV 的安全措施	387
11.3.4 用户工作环境的设置	336	12.7.4 WebDAV 客户端	389
11.4 远程控制实例练习	337	12.7.5 WebDAV Redirector	392
11.5 在终端服务器上安装应用程序	339	第 13 章 SSL 网站安全连接	393
11.5.1 安装应用程序的方法	339	13.1 SSL 概述	394
11.5.2 应用程序兼容性脚本文件	340	13.1.1 SSL 的功能	394
第 12 章 IIS 网站的架设	341	13.1.2 SSL 的工作原理	394
12.1 安装与测试 IIS	342	13.2 网站的 SSL 实例演示	395
12.1.1 环境设置	342	13.2.1 在网站上建立证书申请文件	396
12.1.2 安装 IIS	343	13.2.2 将申请文件传送到企业 CA 并下载证书文件	399
12.1.3 测试 IIS 是否安装成功	344	13.2.3 将申请文件传送到独立 CA 并下载证书文件	402
12.2 网站的基本设置	346	13.2.4 安装证书与启用 SSL	407
12.2.1 主目录与默认文件	346	13.2.5 建立与网站之间的 SSL 连接	409
12.2.2 添加 default.htm 文件	349	13.3 将网站的证书存盘	411
12.2.3 文档页脚	349	13.3.1 将网站的证书导出存盘	411
12.3 实际目录与虚拟目录	351	13.3.2 将证书导入到网站	412
12.3.1 实际目录实例演示	351	第 14 章 FTP 站点的架设	415
12.3.2 虚拟目录实例演示	353	14.1 安装与测试 FTP 站点	416
12.4 建立新网站	356	14.1.1 架设 FTP 站点	416
12.4.1 利用主机头名称来建立多个 网站	356	14.1.2 测试 FTP 站点是否架设成功	417
12.4.2 利用多个 IP 地址建立多个 网站	361	14.2 FTP 站点的基本设置	419
12.4.3 利用 TCP 连接端口建立多个 网站	367	14.2.1 主目录与目录列表样式	419
12.5 网站的安全性	373	14.2.2 FTP 站点标识、连接限制、 日志记录	422
12.5.1 启动与停用动态属性	373	14.2.3 FTP 站点的消息设置	423
12.5.2 验证用户的身份	374	14.2.4 验证用户的身份	424
12.5.3 通过 IP 地址来限制连接	380	14.2.5 检查目前连接的用户	426
12.5.4 通过 NTFS 权限设置来增加 网页的安全性	382	14.2.6 通过 IP 地址来限制连接	426
12.6 远程管理网站	382	14.3 实际目录与虚拟目录	427
12.6.1 IIS 管理器	382	14.3.1 实际目录实例演示	427
12.6.2 终端服务器	383		



14.3.2 虚拟目录实例演示.....	427	15.7 消息传递设置.....	469
14.4 创建将用户隔离的 FTP 站点.....	430	15.7.1 重传与间隔时间设置.....	470
14.4.1 创建“隔离用户”的 FTP		15.7.2 消息跳跃计数设置.....	470
站点.....	431	15.7.3 伪装域设置.....	470
14.4.2 创建“用 Active Directory 隔离		15.7.4 完全规范域名 (FQDN) 设置 ...	471
用户”的 FTP 站点.....	436	15.7.5 中继主机设置.....	472
14.4.3 创建不隔离用户的 FTP 站点.....	443	15.7.6 反向 DNS 查询设置.....	473
第 15 章 电子邮件服务器的架设.....	445	15.8 邮件的管理.....	473
15.1 电子邮件服务器简介.....	446	15.9 建立 SMTP 域.....	475
15.2 POP3 服务验证身份的方法.....	447	15.9.1 添加 SMTP 域.....	476
15.2.1 本地 Windows 账户验证.....	447	15.9.2 为远程域启用 ATRN 功能.....	477
15.2.2 Active Directory 集成验证.....	448	第 16 章 NNTP 服务器的架设.....	479
15.2.3 加密的密码文件验证.....	448	16.1 架设 NNTP 服务器.....	480
15.3 架设电子邮件服务器.....	449	16.1.1 安装 NNTP Service.....	480
15.3.1 安装电子邮件服务.....	449	16.1.2 默认的新闻组.....	481
15.3.2 POP3 服务器的设置.....	450	16.1.3 在用户端建立新闻组账户.....	482
15.3.3 在客户端建立电子邮件账户.....	452	16.1.4 隐藏 Control 新闻组.....	484
15.3.4 架设一个功能完整的电子邮件		16.2 改变 NNTP 的设置.....	485
服务器.....	455	16.2.1 一般设置.....	486
15.4 SMTP 服务器的基本管理工作.....	457	16.2.2 访问设置.....	487
15.4.1 IP 地址与 TCP 端口号的设置....	457	16.2.3 文章限制、控制消息与审查	
15.4.2 启动、停止、暂停 SMTP		设置.....	487
服务器.....	457	16.2.4 指定 NNTP 服务器操作员.....	489
15.4.3 启动、停止、暂停 SMTP 服务....	458	16.3 添加新闻组.....	490
15.4.4 连接设置.....	459	16.3.1 添加新闻组的步骤.....	491
15.4.5 添加 SMTP 虚拟服务器.....	461	16.3.2 限制新闻组枚举.....	492
15.4.6 启用日志记录.....	461	16.4 添加虚拟服务器与虚拟目录.....	493
15.5 SMTP 的安全性.....	461	16.4.1 添加 NNTP 虚拟服务器.....	493
15.5.1 指定 SMTP 服务器的操作员.....	461	16.4.2 添加虚拟目录.....	493
15.5.2 连入连接的验证设置.....	461	16.5 过期策略设置.....	497
15.5.3 出站连接的验证设置.....	462	第 17 章 远程安装服务.....	499
15.5.4 利用 IP 地址来限制连接.....	463	17.1 远程安装概述.....	500
15.5.5 设置或删除转发限制.....	464	17.2 架设 RIS 服务器.....	503
15.5.6 TLS 安全连接设置.....	464	17.2.1 安装远程安装服务.....	503
15.6 SMTP 服务器的运作流程.....	467	17.2.2 设置与激活 RIS 服务器.....	503
15.6.1 SMTP 域.....	467	17.2.3 给予用户建立计算机账户的	
15.6.2 SMTP 服务器的文件夹结构		权限.....	507
与发送流程.....	468		

17.3 管理 RIS 服务器.....	508	17.7.1 RIPrep 映像的制作流程.....	527
17.3.1 客户端计算机名称与计算机 账户的设置.....	509	17.7.2 复制系统管理员的本地用户 配置文件.....	528
17.3.2 预先设置客户端计算机.....	510	17.7.3 执行远程安装准备向导.....	529
17.3.3 响应客户端的请求.....	512	17.7.4 使用 RIPrep 的注意事项.....	533
17.4 RIS 客户端开始远程安装.....	513	17.8 映像权限、安装选项与多国语言.....	534
17.4.1 制作远程启动磁盘.....	513	附录 A 网络监视器的使用.....	539
17.4.2 开始远程安装 Windows 操作 系统.....	514	A.1 数据包的结构.....	540
17.5 新建各种操作系统的映像.....	516	A.2 安装与执行网络监视器.....	542
17.6 利用应答文件来新建映像.....	521	A.2.1 安装网络监视器.....	542
17.6.1 建立应答文件.....	521	A.2.2 执行网络监视器.....	543
17.6.2 将应答文件关联到现有的 映像.....	523	A.3 捕获与检查数据包.....	544
17.7 制作 RIPrep 映像.....	527	A.4 捕获筛选器的设置.....	547
		A.5 捕获触发器的设置.....	550

第 1 章

Windows Server 2003 的网络功能

Windows Server 2003 的网络功能，提供了各种不同的网络解决方案，让您可以利用它来创建各种不同的网络环境。另外我们还要介绍 Windows Server 2003 网络主要依赖的通信协议 TCP/IP。

本章要介绍的主题有：

- Windows Server 2003 所提供的网络功能
- TCP/IP 通信协议



1.1 Windows Server 2003 所提供的网络功能

Windows Server 2003 提供了许多网络技术与服务, 让您在配置各种不同结构的网络时更为容易, 例如您可以通过它们来配置以下网络:

- ▶ **Intranet** 也就是一般公司内部的局域网(Local Area Network, LAN)。通过 Intranet, 用户可以将文件、打印机等资源共享出来, 供网络中的其他用户来访问。随着 Internet 的蓬勃发展, 目前一般 Intranet 内会配置各种与 Internet 技术有关的应用程序与服务, 例如通过浏览器来访问资源、通过电子邮件来传递信息、通过新闻群组来讨论议题等。
- ▶ **Internet** 通过 Internet, 让您的网络与全世界提供 Internet 服务的网络连接在一起。用户可以通过浏览器来访问 Internet 的资源, 通过电子邮件来传递信息, 通过新闻群组来讨论议题, 为公司提供一个电子商务活动的网络环境。
- ▶ **Extranet** 您可以将公司的局域网与客户、供货商、合作伙伴的网络通过 Internet 的技术连接在一起, 组成一个所谓的 Extranet, 以便相互分享资源。
- ▶ **远程访问** 它让用户、系统管理员等可以通过远程访问的技术, 来连接、访问、监控和管理公司内部的 Intranet。公司内两个位于不同地点的局域网, 也可以通过 Windows Server 2003 的网络功能连接在一起, 组成一个广域网(WAN), 以便能够相互分享资源。

Windows Server 2003 提供了各种不同的技术和服务, 让您来创建以上所叙述的网络环境。

1.2 TCP/IP 通信协议

TCP/IP 通信协议是目前最完整、最被广泛支持的通信协议, 它可以让不同网络结构、不同操作系统的计算机相互通信, 例如 Windows Server 2003、Windows 2000 计算机、UNIX 主机、大型计算机(mainframe)、NetWare 客户端等。它也是因特网(Internet)的标准通信协议, 更是 Windows Server 2003 Active Directory 网络所必须采用的通信协议。

在 TCP/IP 的网络上, 每一台连接到网络上的计算机(与部分设备)被称为是一台“主机(host)”, 而主机与主机之间的通信, 主要是通过以下 3 个主要部件:

- ▶ IP 地址(IP address)
- ▶ 子网掩码(Subnet mask)
- ▶ IP 路由器(IP router)

1.2.1 IP 地址(IP Address)

在以 TCP/IP 为通信协议的网络上, 每一台主机都有一个惟一的 IP 地址(它的功能就好像是您家的门牌号码), 而且不可以跟其他的主机相同。IP 地址不但可以用来辨识每一

台主机，而且其内也隐含着如何在网络间传送信息的路由信息（Routing Information）。

IP 地址一共占用 32 位（bit），一般是以 4 个十进制数来表示，每一个数字称为一个 Octet（八位组）。Octet 与 Octet 之间以点（dot）隔开，例如：

192.168.1.31

这个 32 位的 IP 地址内包含了 Network ID 与 Host ID 两部分信息：

- Network ID 网络识别码。每一个网络都有一个惟一的网络识别码。
- Host ID 主机识别码。同一个网络内的每一台主机都必须有一个惟一的主机识别码。



说明 此处所介绍的 IP 地址为目前最被广泛使用的 IPv4，它共占用 32 位。Windows Server 2003 也支持新版的 IPv6（IP version 6），它是利用 128 位来代表 IP 地址，因此可以提供更多的 IP 地址。

如果您的网络要与外界通信，则您必须为您的网络申请一个 Network ID，整个网络内的所有主机都使用一个相同的 Network ID，然后再赋予网络内每一台主机一个惟一的 host ID，因此网络上每一台主机都会有一个惟一的 IP 地址（Network ID 与 Host ID 的组合）。您可以直接向 ISP 申请 Network ID。

当然，如果您的网络并未与外界的 Internet 连接在一起，那么您可以自行选用任何一个可用的 Network ID，不用申请，不过同一个网络内，各主机的 IP 地址不可相同。

1.2.2 IP 地址的类别

IP 地址被分为 A、B、C、D、E 五大类型（见表 1.1），其中的 A 类地址、B 类地址、C 类地址是可供主机使用的 IP 地址，每种类型所支持的 IP 数量都不相同，以便满足各种不同大小规模的网络需求。而 D 类地址和 E 类地址则是特殊用途的 IP 地址。

表 1.1 IP 地址分类

类别	Network ID	Host ID	W 值可为	所支持的网络数目	每个网络可支持的主机数目
A	W	X.Y.Z	1~126	126	16 777 214
B	W.X	Y.Z	128~191	16 384	65 534
C	W.X.Y	Z	192~223	2 097 152	254
D			224~239		
E			240~254		

IP 地址一共占用 4 个字节（byte），表中我们将 IP 地址的各字节以 W.X.Y.Z 的形式来加以说明。

- A 类地址 A 类 IP 地址适合于超大型的网络，其 Network ID 占用一个字节（byte），即 W。W 值的可用范围是 1~126，因此可提供 126 个 A 类的 Network ID。
Host ID 共占用 X、Y、Z 3 个字节（1 byte = 8 bits），因此 24 位可支持 $(2^{24}) - 2 = 16\,777\,216 - 2 = 16\,777\,214$ 台主机（减 2 的原因我们将在后面讨论）。



- B类地址 B类IP地址适合于中、大型网络，其 Network ID 占用 2 字节（W、X），W 值的可用范围是 128~191，因此可提供 $(191 - 128 + 1) \times 256 = 16\,384$ 个 B 类的网络。Host ID 共占用 Y、Z 2 个字节，因此每一个网络可支持 $(2^{16}) - 2 = 65\,536 - 2 = 65\,534$ 台主机（减 2 的原因我们将在后面讨论）。
- C类地址 C类IP地址适合于小型网络，其 Network ID 占用 3 字节（W、X、Y），W 值的可用范围是 192~223，它可提供 $(223 - 192 + 1) \times 256 \times 256 = 2\,097\,152$ 个 C 类的网络。Host ID 只占用一个字节（Z），因此每一个网络可支持 $(2^8) - 2 = 254$ 台主机（减 2 的原因我们将在后面讨论）。
- D类地址 这个 Network ID 具有特殊的用途，它是一个“多点传播（multicast）”所使用的群组 ID（group ID），这个群组内包含多台主机。其 W 值的范围为 224~239。
- E类地址 这是一个专供实验用的 Network ID，其 W 值的范围为 240~254。

这 5 个等级中只有 A 类地址、B 类地址和 C 类地址是可以供一般主机使用的，但是在使用时，需注意以下事项：

- Network ID 不可以是 127。127 是用来执行回送测试（loopback test）的，不可拿来作其他用途。您可以利用 ping 127.0.0.1 命令执行回送测试，以便检查网卡与驱动程序是否正常运行。
- 每一个网络的第 1 个 IP 地址是代表网络本身，最后一个 IP 地址代表广播地址，因此实际可分配给主机的 IP 地址将少 2 个。

如果你所申请到的 Network ID 为 203.3.6，则共有 203.3.6.0 到 203.3.6.255 的 256 个 IP 地址，但 203.3.6.0 是用来代表这个网络（因此我们一般会说此网络的 Network ID 为 4 个字节的 203.3.6.0，而不是 3 个字节的 203.3.6）；而 203.3.6.255 是保留给广播用途的（255 代表广播），例如若发送信息到 203.3.6.255 这个地址，表示将信息广播给 Network ID 为 203.3.6.0 网络内的所有主机。

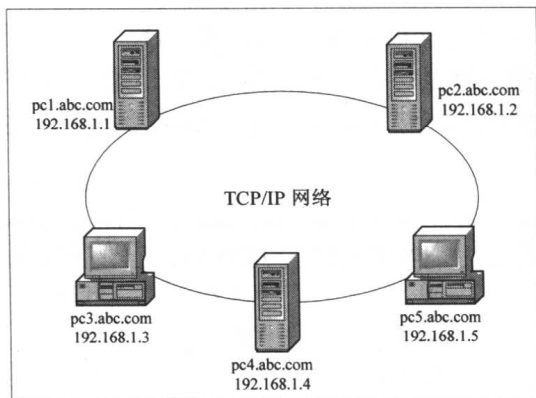


图 1.1

图 1.1 为 C 类网络范例，其 Network ID 为 192.168.1.0，网络内 5 台主机的 Host ID 分别为 1、2、3、4、5。

1.2.3 子网掩码（subnet mask）

子网掩码也是占用 32 位，它有两项功能：

- 用来区分 IP 地址中的 Network ID 与 Host ID。
- 用来将网络切割为数个子网（sub-network）。

当 IP 网络内的主机在相互通信时,它们利用子网掩码(见表 1.2)来得知双方的 Network ID,进而得知彼此是否在同一个网段内。

表 1.2

类别	默认的子网掩码 (二进制)	默认的子网掩码 (十进制)
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

表 1.2 中为各类子网默认的掩码设置值,表中为 1 的位用来指定 Network ID,为 0 的位用来指定 Host ID。例如,若某台主机的 IP 地址为 192.168.1.3,其二进制值为 11000000.10101000.00000001.00000011;而子网掩码为 255.255.255.0,其二进制值为 11111111.11111111.11111111.00000000。则计算其 Network ID 的原则是:

- 将 IP 地址与子网掩码两个值中相对应的位做 AND 逻辑运算(参见表 1.3)。
- 将 AND 逻辑运算后的结果与子网掩码中的各字节互相对应,只要在子网掩码中值为 1 的,其所对应到的位,就是其 Network ID,表 1.3 中上箭头符号所指的位就是其 Network ID。在 IP 地址中扣除 Network ID 后,其余的部分就是 Host ID。

因此,IP 地址 192.168.1.3 的 Network ID 是 192.168.1(上箭头符号所指的部分),也就是 192.168.1.0,而 Host ID 就是 3。

表 1.3

192.168.1.3	→	11000000	10101000	00000001	00000011
255.255.255.0	→	11111111	11111111	11111111	00000000
AND 后的结果	→	11000000	10101000	00000001	00000000
		(192)	(168)	(1)	
		↑↑↑↑↑↑↑↑	↑↑↑↑↑↑↑↑	↑↑↑↑↑↑↑↑	

若 A 主机的 IP 地址为 192.168.1.3,子网掩码为 255.255.255.0,B 主机的 IP 地址为 192.168.1.5,子网掩码为 255.255.255.0。当 A 主机要和 B 主机通信时,A 主机会将 A 主机的 IP 地址与子网掩码做 AND 运算,以便得知其 Network ID 为 192.168.1.0,然后再利用类似的方法(详情参阅第 9 章),得知 B 主机的 Network ID 为 192.168.1.0。由于两台主机的 Network ID 都是 192.168.1.0,故表示它们都是在同一个网段内,因此它们可以直接通信。

 若两台主机的 Network ID 不同,则表示它们是分别位于两个不同的网络内,因此它们无法直接通信,必须通过路由器(router)来路由。

1.2.4 利用子网掩码来划分子网

为了方便管理与提高网络运行的效率,有时可能需要将一个较大的网络,划分为数个以 IP 路由器连接的子网;或将数个分布于各地的子网以 IP 路由器连接在一起。每一个子