GOTOP

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。适于网络管理人士学习，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

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　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社总机：010-62770175　　**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的角度，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。

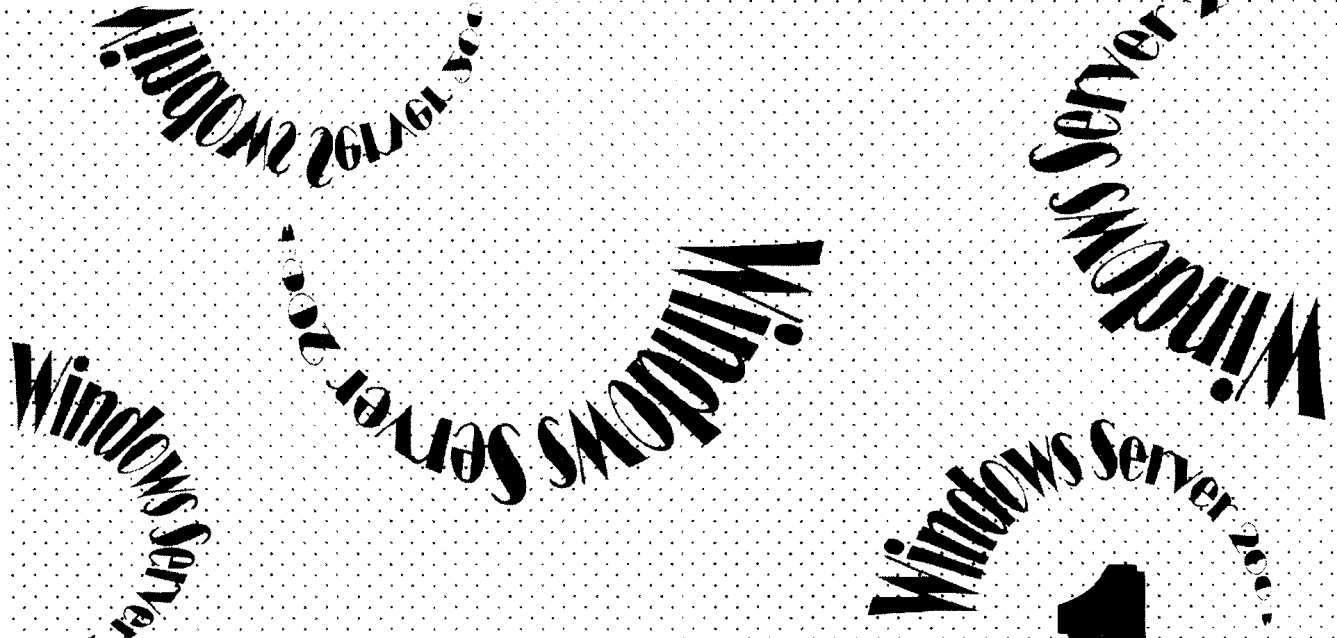
本套丛书包括《Windows Server 2003 用户管理指南》、《Windows Server 2003 网络专业指南》、《Windows Server 2003 Active Directory 配置指南》3 本，内容丰富详实，相信这几本书，仍然会不辜负您的期望，在您学习 Windows Server 2003 时，将给予您最大的帮助。

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

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。

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)×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)×256×256 = 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，不可拿来做其他用途。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。

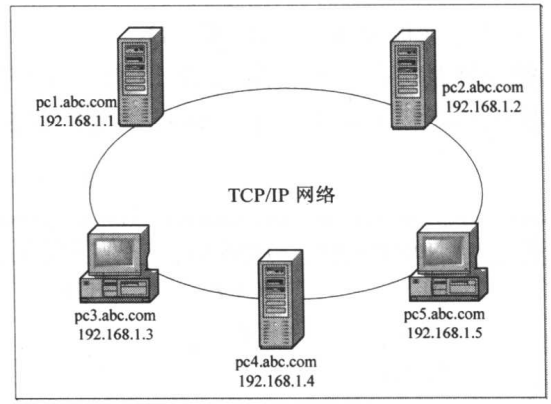


图 1.1

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，它有两大功能：

- 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。

说明

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