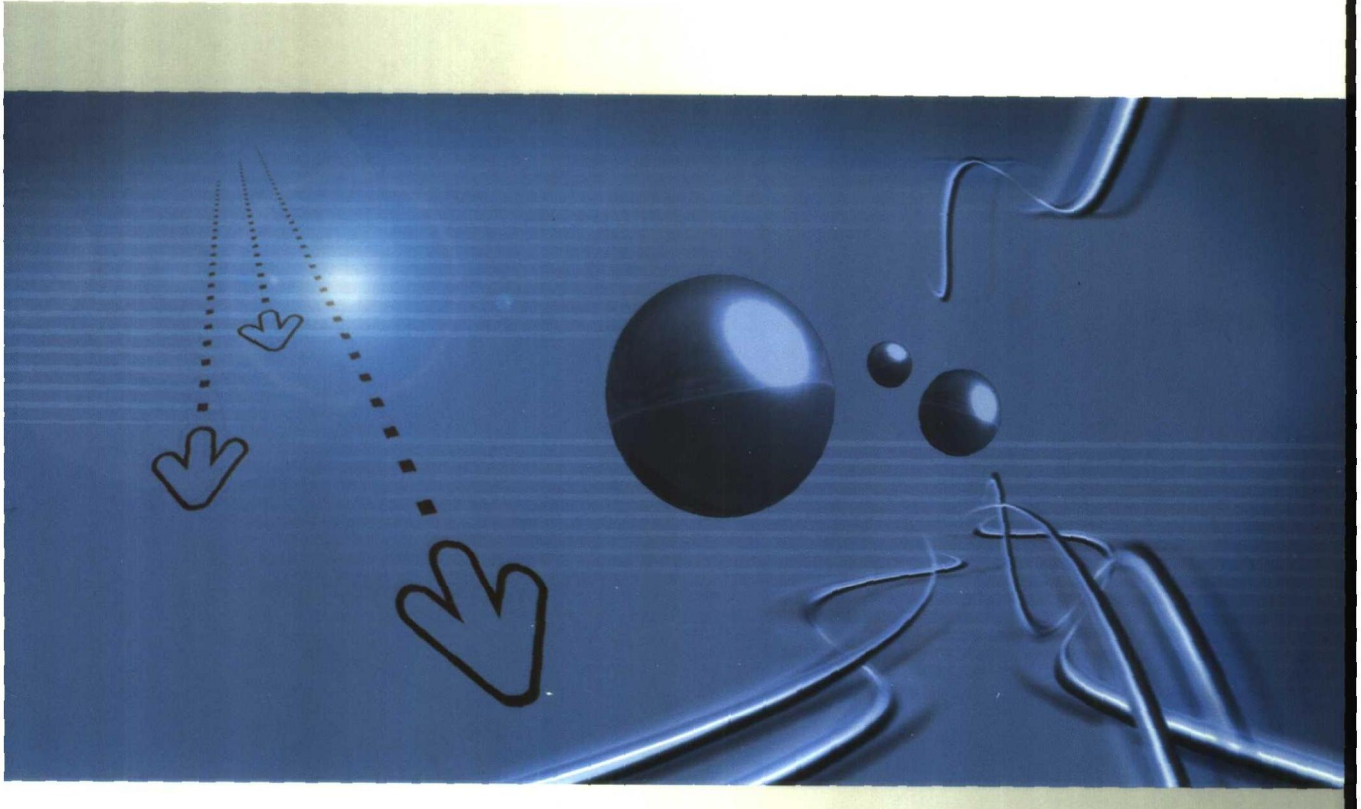
实用组网、用网与管网技术

Windows
网络安全配置、管理和应用实例



王　群　主编
王　磊　编著

清华大学出版社

Windows 网络安全配置、管理和应用实例

王 群 主编
王 磊 编著

清华大学出版社
北 京

内 容 简 介

本书详细讨论了在 Windows NT/2000 网络环境中通过系统配置提高网络安全性的具体方法，同时介绍了各种部署场景下的服务器安全配置技术和步骤，并引导读者利用微软公司提供的系统工具分析与加固基于 Windows NT/2000 的服务器和客户端系统。此外，本书还详细介绍了使用微软公司的防火墙软件 Internet Security & Acceleration Server（ISA）在用户和服务器之间建立安全屏障的具体实施办法。

本书适用于需要设计、规划、实现和支持 Windows 网络环境中安全性的 IT 专业人员阅读，对于网络公司的系统设计人员、高校学生和各行业的网络从业人员也具有较强的指导性。另外，本书还适合网络初学者学习、使用。

图书在版编目(CIP)数据

Windows 网络安全配置、管理和应用实例/王群主编；王磊编著. —北京：清华大学出版社，2004.4
ISBN 7-302-08238-3

I. W… II. ①王… ②王… III. ①窗口软件，Windows NT/2000 ②计算机网络—安全技术
IV. TP316.7 ②TP393.08

中国版本图书馆 CIP 数据核字（2004）第 017372 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：丁　岭
文稿编辑：许振伍
印 装 者：北京鑫海金澳胶印有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：16　**字数**：397 千字
版　　次：2004 年 4 月第 1 版　2004 年 4 月第 1 次印刷
书　　号：ISBN 7-302-08238-3/TP・5945
印　　数：1~4000
定　　价：24.00 元

前　言

随着IT系统平台的发展及应用的不断拓展，其所面临的安全风险也日益增加。如果希望有效地保护本单位的环境免受攻击，管理员就必须全面彻底地了解可能遭遇的各种危险。目前，绝大部分单位的网络环境是基于Window NT或Windows 2000平台的，为此本书以Window NT或Windows 2000网络环境为基础，较系统地介绍其安全配置、管理和使用方法。

在识别网络面临的安全威胁时，管理员应该考虑两上主要因素：

- 可能面临的攻击类型。
- 这些攻击会从什么地方发起。

许多管理员往往疏忽了第二个因素，以为危险攻击只来自外界（一般通过他们的Internet 连接）。然而调查研究发现，31%的被调查者证明他们的内部系统也经常被攻击。许多公司可能对正在发生的内部攻击毫不知情，主要是因为他们没有监视这类内部行为。万无一失的IT环境根本就不存在，但这并不代表管理员应该放弃防守。相反，应该更加深入地了解IT系统，根本环境的变化及应用的需求保持网络的安全防御措施经常更新。

本书共分11章和两个附录。其中：

第1章　介绍在Windows NT/2000系统中，使用NTFS分区的磁盘提供最安全服务，从而保护用户存储在磁盘中数据的安全性。

第2章　介绍使用Active Directory组策略对Window 2000系统进行安全配置和管理。

第3章　介绍运用Windows 2000组策略对网络进行安全配置和管理的方法。

第4章　针对企业中的所有成员服务器和域控制器定义的基准策略，介绍了通过对特定功能的锁定来提高网络性能的具体方法。

第5章　介绍通过微软公司提供的系统工具对网络进行安全配置和管理的方法。

第6章　介绍Software Update Services（SUS）服务器的设计方法，以及通过SUS提高系统可靠性和安全性的具体步骤。

第7章　介绍Windows NT/2000网络中审核与入侵检测的配置和应用。

第8章　系统介绍了微软公司的拳头安全产品Internet Security and Acceleration（ISA）的安装和配置。

第9章　专门介绍了在ISA Server中通过使用访问规则来提高网络安全性的方法。

第10章　介绍通过配置容错、负载平衡和分布式缓存的ISA Server计算机来提高系统安全性的具体方法。

第11章　介绍通过配置ISA服务器的缓存优化网络性能的具体方法。

附录A和附录B分别列出了Windows 2000的基准策略访问控制列表和Windows 2000所提供的各种服务功能。

序

计算机技术与通信技术相结合产生了计算机网络，同时随着计算机技术和通信技术的飞速发展，网络技术也出现了空前的繁荣景象。从应用来看，大到跨国公司、小到家庭，网络都在发挥着重要的作用；从技术来看，从早期的 10Mb/s 共享到目前的 10000Mb/s 交换，其技术更新使人眼花缭乱；从用户的需求来看，大家已不再满足于原来的文件和设备共享，而是在享受着今天互动式的多宽带媒体应用。所以说，今天的网络已非昨天的网络，今天的网络无论在组建方式、使用方式和管理方式上都存在着很大的不同。本系列书的出版正是为了满足目前网络用户的具体需求，从网络的组建入手，到网络的具体应用，再到网络的管理，较为系统、全面地介绍中小型网络的组建、应用和管理方法。

本系列书主要围绕网络组建、应用和管理三个方面，其中：

网络组建 网络组建一般分为硬件系统集成和软件系统集成两部分。其中：硬件部分主要以目前广泛使用的以太网技术为主，较为完整地介绍网络的规划、设计和具体组建过程与方法。在这部分内容中，强调了网络组建中要视具体的应用需求来确定硬件设备和集成方式，严格按照网络的分层（接入层→汇聚层→核心层）原则来规划网络；考虑到目前中小型网络用户的具体需要，软件部分主要以微软的 Windows NT/2000/2003 Server 为主进行介绍，同时兼顾部分用户的需要，还介绍了 NetWare5.x/6.x 及 Red Linus 8.x/9.x 网络的组建方法以及 Windows、NetWare 与 Linux 操作系统之间的集成方法。另外，针对一些小型公司、办公室、网吧及家庭用户，还介绍了 Windows 对等网络的组建过程。

网络应用 建网的目的是为了应用，许多单位投入了大量的资金组建了网络，但是由于种种原因根本没有发挥网络的应用价值，致使现有的网络资源被白白浪费。针对目前国内许多中小型网络存在的这种情况，本系列书较为全面地介绍了各种网络应用方案，除包括常见的 WWW、FTP、Mail 等服务器的构建外，还广泛介绍了各种行业软件和流行软件的使用方法。通过对这些软件的安装、调试及使用方法的系统介绍，使读者感觉到一个网络用户到底需要哪些方法的应用，另外也告诉大学目前的网络可以提供哪些服务。

网络管理 对于大部分网络用户来说，网络管理是一项技术难度较大且较为烦琐的工作，因为一个网络管理人员不但要熟悉网络的规划和组建这些基础过程，而且还要从更高的层次和不同的角度来研究所使用的网络，通过收集和分析相关的信息或观察网络的运行状况，发现网络存在或可能存在的问题，进而采取相应的措施，保障网络的正常运行。在本系列书中，将较全面地介绍网络管理的基本概念、技术和相关软件的使用方法，并通过大量管理实例的介绍，使读者掌握不同规模、不同环境和不同架构的网络的管理方法。

网络技术的发展日新月异，具体的网络应用之间也存在着差异，同时针对不同网络或同一网络所采取的管理方法也不尽相同。所以，为了保证本系列书的权威性、全面性和实用性，我们特约了国内网络界一些知名专家和工程技术人员负责本书的编写和校审工作。

目　录

第 1 章　使用 NTFS 保护文件

在 Windows 2000 系统中，使用 NTFS 分区的磁盘能够提供最安全的服务，保护用户存储在磁盘中数据的安全。在 NTFS 分区中，通过复杂的访问权限管理来帮助管理员实现不同场合中的应用，同时还提供了压缩、配额、加密等其他有助于提高文件存储安全性的功能。

1.1　磁盘分区比较

如果读者刚开始接触 Windows 2000，可能对 NTFS 文件系统的复杂结构还不甚了解，只是耳闻，FAT 文件系统与 NTFS 文件系统分别适用于不同的应用环境。本节将介绍这两种文件系统的不同，并说明如何发挥它们各自的优势。

1.1.1　何谓 FAT

FAT 是文件分配表 File Allocation Table 的缩写，用于一些操作系统磁盘维护的表格或列表，用来跟踪存储在磁盘中各种文件的位置、大小等信息。

自 1981 年首次问世以来，FAT 已经成为一个常用的计算机术语。随着时间推移，包括 Windows NT、Windows 98、Mac OS 以及多种 UNIX 版本在内的大多数操作系统均支持 FAT 文件系统。

FAT 文件系统限制使用 8.3 格式的文件命名规范。也就是说，在一个文件名中句点之前部分的最大长度为 8 个字符，句点之后部分的最大长度为 3 个字符，文件名必须以字母或数字开头，并且不得包含空格。此外，FAT 文件名中的字母不区分大小写。

例如，abc123.txt 就是一个符合 8.3 标准的文件名。在句点之前有 3 个字母和 3 个数字的组合，加起来少于 8 个，在句点之后有 3 个字符。

FAT 又名为 FAT16，它使用 16 位文件分配表跟踪分配给每个文件的磁盘空间。由于只有 65 536（64 KB）个不同的 16 位数字，因此使用 FAT16 格式化的分区至多有 64 KB 个分配单元，它们被称作簇。每个簇最大为 32 KB。用 32 KB 乘以 64 KB 个簇，FAT16 分区最大不超过 2 GB。因此如果使用 FAT16，任何绝对空间超过 2 GB 的驱动器都必须分为多个分区。

1.1.2　何谓 VFAT

作为 FAT 文件系统的一种扩展，VFAT 在 Windows 95 操作系统发行时被首次引入。VFAT 在保持针对 FAT 向后兼容能力的同时，大大放宽了各项规范。例如，VFAT 文件名

中最多可以包含 255 个字符，并且允许使用空格或多个句点。尽管 VFAT 能够保持文件名的大小写状态，但同样无法对其加以区分。换句话说，虽然用户可以从磁盘管理工具中看到一个文件名为 AbC.txt 的文件，但是当用户在此目录下创建一个文件名为 aBc.txt 的文件时，操作系统将提示有重名的文件存在。

当用户通过 VFAT 创建一个长文件名（长度超过 8.3）时，文件系统实际上同时创建了两个文件名。其中一个为实际输入的长文件名，这个文件名对于 Windows 95、Windows 98 和 Windows NT（4.0 及更高版本）是可见的；另一个文件名为 DOS 下所使用的别名，该文件名为长文件名的缩写。这个 DOS 别名由长文件名中的前 6 个字符（不包含空格）、代字符（～）以及数字后缀所组成。

例如，一个长文件名 abc 123 def 456.txt 文件，在 DOS 别名中表示为 abc123～1.txt。

VFAT 文件系统存储长文件名的方式产生一个有趣的副作用。当用户在 VFAT 文件系统中创建一个长文件名时，VFAT 将为 DOS 别名分配一个目录项，为长文件名中的每 13 个字符分配一个目录项。从理论上讲，一个长文件名最多可以占用 21 个目录项。一般情况下根目录中最多可以包含 512 个文件，然而如果在根目录中使用最大长度的文件名，那么上述限制条件将缩小为最多包含 24 个文件。由此可见，应当尽可能避免在根目录中使用长文件名。除根目录外，其他目录均不受这一限制。

需要注意的是，当用户在 Windows 2000 环境下，在磁盘管理工具中使用 FAT 对某一分区进行格式化时，该分区实际将被格式化为 VFAT。在 Windows 2000 系统环境下，用户惟一可能接触真正 FAT 分区的方式便是使用由其他操作系统（如 MS-DOS）完成格式化的分区。

1.1.3 何谓 FAT32

Windows 95 OSR2 和 Windows 98 开始支持 FAT32 文件系统，它是对早期 DOS 的 FAT16 文件系统的增强。由于文件系统的核心——文件分配表 FAT 由 16 位扩充为 32 位，所以称为 FAT32 文件系统。在硬盘的分区超过 512 MB 时使用这种格式，会更高效地存储数据，减少硬盘空间的浪费，一般还会使程序运行加快、使用的计算机系统资源更少，因此是使用大容量硬盘存储文件的极有效的系统。

1.1.4 何谓 NTFS

为了弥补 FAT16/32 功能上的缺陷，Microsoft 创建了一种称作 NTFS 的新型文件系统技术。NTFS 提供的新增特性包括容错性和增强安全性等。下面将从不同角度对以上所介绍的这些文件进行性能对比。

1．兼容性

在确定某一分区所需使用的文件系统类型前，必须首先考虑兼容性。如果多种操作系统都将对该分区进行访问，那么用户必须使用一种所有操作系统均可读取的文件系统。通常，具备普遍兼容性的 FAT 文件系统可以胜任这种要求。相比之下，只有 Windows NT/2000

能够支持 NTFS 分区。

需要说明的是，这种限制条件仅适用于本地计算机。例如，如果一台计算机上同时安装了 Windows 2000 与 Windows 98 两种操作系统，并且这两种操作系统都要对同一分区进行访问，那么用户必须通过 FAT 方式对该分区进行格式化。与此相反，如果这台计算机上只安装了 Windows 2000 一种操作系统，那么用户可以将该分区格式化为 NTFS。此时运行其他操作系统的计算机，例如 Windows 98，仍可通过网络方式对该分区进行访问。

2．分区物理容量

另一项决定因素为分区物理容量。FAT16 最大支持 2 GB 分区容量。如果用户想要分区容量超过 2 GB，必须通过 NTFS 方式对其格式化，或者将其拆分为多个容量较小的分区。需要注意的是，NTFS 本身需耗费的资源多于 FAT。如果用户所使用的分区容量小于 200 MB，则应选择 FAT 文件系统，以避免 NTFS 文件系统自身占用过多磁盘空间。NTFS 分区的最大容量为 16 EB。

3．容错性

在妥善考虑分区容量与兼容性之后，还需要考虑容错性。Windows 2000 能够通过软件对几种用以提高访问速度或实现容错性的交替磁盘访问方式提供支持。其中包括普通 RAID-0 卷（带区卷）及 RAID-5 卷。这类访问方式通常需要 NTFS 文件系统为其提供支持。如果用户计划使用基于硬件实现方式的带区卷，则可以随意选择文件系统类型。

Windows 2000 软件创建的带区卷是通过将 2～32 个磁盘上的可用空间区域合并到一个卷上而创建的。数据被分块并以固定的顺序分布在该卷中的所有磁盘中。例如，用户有 5 个容量为 18 GB 的磁盘，则可以创建一个容量为 90 GB 的卷。

通过使用带区卷，Windows 2000 将数据写入多个磁盘，如图 1.1 所示。带区跨越所有磁盘写入文件，以便将数据以相同速率添加到所有磁盘中。带区卷中的数据被交替地均匀分布在这些磁盘的带区中。

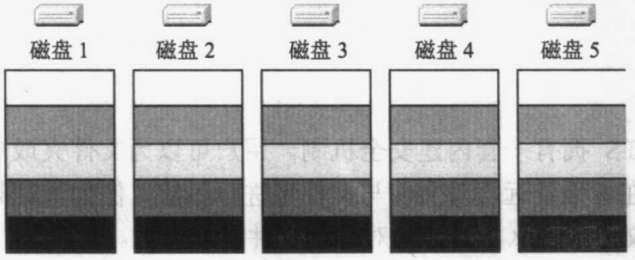


图 1.1　带区卷原理

在 Windows 2000 的所有磁盘类型中，带区卷提供了最佳的磁盘操作性能。但是如果带区卷中的某一个磁盘发生故障，就会使整个卷中的数据丢失。

RAID-5 是一种容错卷。所谓容错就是当部分磁盘出现故障之后，其余磁盘还能继续为用户提供数据存储服务的功能。在 Windows 2000 中使用软件创建 RAID-5 卷，最少需要 3 个磁盘驱动器，最多可达 32 个磁盘驱动器。计算机中的数据和奇偶校验值在 3 个或更多

的物理磁盘上成间歇的带区分布，如图 1.2 所示。

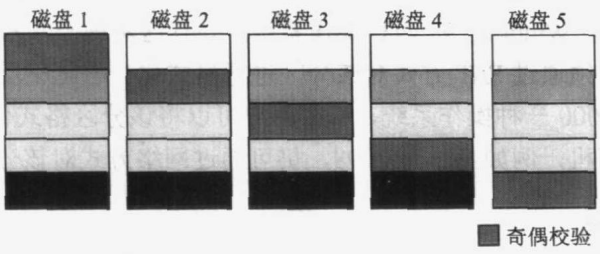


图 1.2 RAID-5 卷工作原理

奇偶校验是一种数学方法，用于确定一个数字或一系列数字中奇数位和偶数位的个数。当一个数字或一系列数字丢失后，可以利用奇偶校验重新构造数据。

在一个 RAID-5 卷中，Windows 2000 通过在该卷的各个磁盘分区中添加奇偶校验信息来实现容错功能。如果单个磁盘出现了故障，Windows 2000 可以利用剩余磁盘中的数据和奇偶校验信息重新构造失败磁盘上的数据。例如用户使用了 5 个磁盘创建了一个 RAID-5 卷，其中一个磁盘出现了故障，从系统中卸载掉，用户仍然可以正常访问 RAID-5 卷中的数据，虽然现在只有 4 个磁盘。

即便不考虑这些高级容错选项，NTFS 自身仍旧包含了远远优于 FAT 的内建容错功能。例如，当 NTFS 将更改内容写入磁盘时，它将自动在相应日志文件中对更改内容加以记录。当出现电源故障或磁盘错误之后，在恢复系统时，Windows NT 可以使用这些日志文件对磁盘中的数据进行修复。

NTFS 还可以在不显示错误消息的情况下自动修复硬盘错误。当 Windows NT 向 NTFS 分区写入文件时，它将在内存中为该文件保留一个备份。完成写入操作后，Windows NT 将再次读取该文件，以验证其是否与内存中所存储的备份相匹配。如果两份副本内容不一致，Windows NT 将把硬盘上的相应区域标记为受损并不再使用这一区域。此后，它将使用存储在内存中的文件副本在硬盘的其他位置上重新写入文件。FAT 文件系统未提供任何安全保护特性。

4. 安全性

如前所述，NTFS 拥有一套内建安全机制。用户可以为文件夹或单个文件设置不同权限。这些权限可以在本地及远程对文件与文件夹进行保护。例如，若某人坐到您的计算机前并尝试使用受限文件，那么 NTFS 将对这些文件予以保护。

5. 文件压缩

NTFS 的另一优势在于针对文件压缩功能的内建支持能力。这项功能使用户能够对选定文件或文件夹进行压缩。由于此项功能以文件为单位进行压缩，因此局部硬盘故障，例如磁盘坏道，不会破坏整个压缩方案并导致磁盘中的数据丢失。此外，对单独文件或文件夹执行压缩时还允许用户只对不经常使用的文件进行压缩。通过这种方式，用户可以在不降低操作系统运行速度的情况下在每次执行文件访问操作时对其进行解压。

1.1.5　在 FAT16、FAT32、NTFS 之间做出选择

用户计划在计算机上安装微软公司的操作系统时需要在 FAT16、FAT32、NTFS 磁盘系统之间做出选择。究竟使用哪种文件系统，用户要根据自己将要安装的系统不同来做出不同的选择。表 1.1 列出了不同操作系统所支持的文件系统。

表 1.1　对比 FAT 16、FAT 32 与 NTFS

	FAT 16	FAT 32	NTFS
最小分区容量	无	512 MB	20 MB
最大分区容量	2 GB	2 TB	推荐最大 2 TB
操作系统	MS-DOS Windows 3.1 Windows 95 Windows 98 Windows NT 3.1 Windows NT 3.51 Windows NT 4.0 Windows 2000 Windows 2003	Windows 98 Windows 95 OSR2	Windows NT 4.0 Windows 2000 Windows 2003

如果用户计划在计算机中只安装 Windows 2000 这一操作系统，建议用户只采用 NTFS 文件系统就可以了。但是如果用户计划在计算机中同时安装多个操作系统，实现多引导，就需要考虑磁盘中的文件系统，使不同的文件系统都可以访问到相同的磁盘分区。

但是，如果用户从网络中访问计算机存储在本地磁盘中的文件，就不存在使用什么操作系统来访问什么文件系统的问题了。

但是出于安全的考虑，建议用户不要在同一台计算机中同时安装多个操作系统，并且所有的磁盘分区都应该是 NTFS 文件系统。

1.2　转化分区

用户在安装 Windows 2000 时，在 DOS 窗口中会询问对安装 Windows 2000 的磁盘是使用 NTFS 文件系统格式化磁盘分区还是使用 FAT 文件系统格式化，如图 1.3 所示。

用户也可以在完成 Windows 2000 安装后方便地转换磁盘分区。如果不需要保留以前磁盘分区中的文件，并且这个磁盘分区不是存放 Windows 2000 系统文件的分区，则用户可以利用 Windows 2000 的磁盘管理工具快速将这个磁盘分区重新格式化为 NTFS 文件系统。

如果这个分区中保存有文件并且还想保留它，或者是计划转换的分区中保存有 Windows 2000 的系统文件，那么用户可以使用 Convert 命令，在不损坏磁盘分区中文件的情况下将分区从 FAT16 或 FAT32 转换到 NTFS 文件系统中。建议用户在使用 Convert 命令转换磁盘分区

前，先对操作系统做一次全面的备份。对于磁盘中保存有重要文件的分区，建议用户先将所有文件复制到其他安全的地方，然后将磁盘重新格式化，这将更加稳妥。具体操作如下。

（1）在 Windows 2000 系统中，执行【开始】|【运行】命令，在随后出现的对话框中输入 cmd，然后单击【确定】按钮。

（2）在出现的命令行窗口中，输入 help convert 命令，然后回车。将出现图 1.4 所示的画面，显示 Convert 命令的所有参数的使用方法。

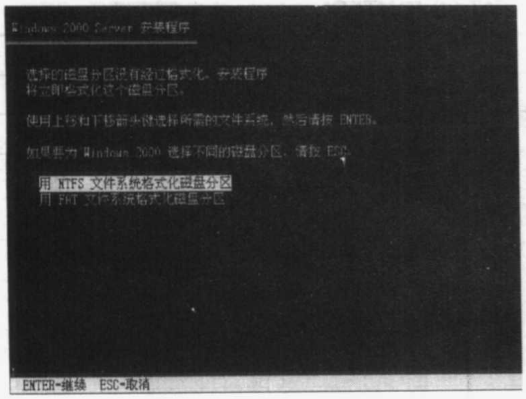


图 1.3 选择文件系统格式化磁盘分区

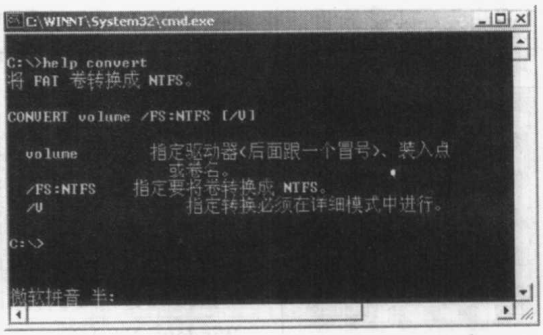


图 1.4 Convert 命令参数

（3）假设用户计划将磁盘分区 E 转换为 NTFS 文件系统，则可以输入 convert e: /fs:ntfs 命令，然后回车。

需要注意的是，Windows 2000 提供的 Convert 命令行工具只能将 FAT16 或 FAT32 文件系统转换到 NTFS 文件系统并保留所有文件，而没有工具可以将一个使用 NTFS 的文件系统的磁盘分区转换到使用 FAT16 或 FAT32 文件系统。

1.3 NTFS 权限

在 Windows 2000 操作系统中，利用 NTFS 文件系统在磁盘分区中存储数据是极有效的。利用 NTFS 可以为文件夹和文件授权，用以控制用户对资源的访问。NTFS 权限只适于 NTFS 磁盘分区，不能用于由 FAT 或 FAT32 文件系统格式化的磁盘分区。

Windows 2000 只为使用 NTFS 进行格式化的磁盘分区提供 NTFS 权限。为了保护 NTFS 磁盘分区上的文件夹和文件，管理员需要为访问该资源的每个用户账户授予 NTFS 权限。用户必须获得明确的授权才能访问资源。用户账户如果没有被组织授予权限，他就不能访问相应的文件或文件夹。不管用户是访问文件夹还是文件，也不管这些文件夹或文件是存储在计算机上还是共享在网络中，NTFS 的安全功能都会有效。

1.3.1 访问控制列表

对于 NTFS 磁盘分区上存储的每一个文件夹和文件，NTFS 都存储一个远程访问控制