Windows 2000 Professional 网络应用教程

计 算 机 教 程

青苹果电子图书系列

Windows 2000 Professional
网络应用教程

前　言

正如 Windows 95 标志着图形化界面操作系统的崛起一样，Windows 2000 的发布标志着计算机操作系统在网络化（包括 Internet 和 Intranet 支持）和智能化方面迈进了一大步。

Windows 2000 采用 NT 的内核，并在此基础上加入了 Windows 98 的易用性特征，这就是崭新的 Windows 2000 家族，事实上，甚至在 β 3 测试版之前，Windows 2000 的产品名称还是 Windows NT5.0，这也就是我们看到一些 NT5.0 的软件和书籍的原因。

以前版本的 Windows NT 分为 Workstation（工作站）和 Server（服务器）两个版本，正如它们的名字所示，它们分别在网络中担任不同的角色；而 Windows 2000 则分了 4 个不同的版本。

关于 Windows 2000 的 4 个版本

Windows 2000 Professional，也就是本书着重介绍的版本，从 Windows NT4.0 Workstation 发展而来，适用于家庭用户、一般商业平台和网络工作站，是 Windows 2000 家族中的工作站/客户机版本。它的安全性、稳定性是以应付一般商业计算的需要，它的灵活性、易用性又使它能够被家庭用户所接受。

Windows 2000 Server，这个版本是在 Windows NT4.0 Server 的基础上发展而来的，是 Windows 2000 家族中的服务器版本，可以作为部门级或小型公司的服务器平台，能提供应用程序文件、打印、Web、通迅等多种服务。Windows 2000 Server 最重要的改进就是活动目录（Active Directory）技术，这是一种强大、透明与系统密切集成的目录服务系统。

Windows 2000 Advanced Server，除了 Windows 2000 Server 的功能之外，Advanced Server 还提供了一些新的特性，例如对集群（一种热备份容错技术），SMP（对称式多处理器）技术等。

Windows 2000 Datacenter Server，这是一个全新的 Windows 版本，是一个 64 位的强大的服务器操作系统，支持多达 16 个 CPU 和最多 64G 的内存。此外，Windows 2000 Datacenter Server 还针对数据仓库、电子商务、科学计算、工程分析等方面进行了优化，力图成为高性能服务器操作系统中的极品，以改变以往此类领域中 UNIX 一统天下的局面。

关于本书

本书共分 21 章，全面深入地介绍了 Windows 2000 Professional 在网络应用方面的强大功能，本书包括的具体内容有：

第 1 章　简单介绍了 Windows 2000 家族以及 Windows 2000 的新特性。阅读本章，可以初步了解 Windows 2000 产品的情况。

第 2 章　介绍如何安装 Windows 2000 Professional。为读者开始学习 Windows 2000 Professional 做好准备。

第 3 章　引导读者认识 Windows 2000 Professional 的新外观。

第 4 章　讲解系统账号管理。Windows 2000 建议为每个用户设立单独的账户而不是多人共同享有一个账户，这样发现问题时比较容易确定责任人，用户也可以有更强的责任心保护自己的账户。学习本章，对于读者管理和使用好自己的账号很有帮助。

第 5 章　文件及系统权限的管理。本章对于用户组织和管理好自己的文件十分重要。

第 6 章　共享资源及权限设置。介绍如何对系统资源进行共享以及相应的权限设置。

第 7 章　Windows NT Server 采用了域（domain）的网络管理手段。域中包括了众多的工作站和一定数目的服务器，并且使用仅有的一个安全数据库，处理多服务器间共享安全机制的问题。了解域的概念对于读者使用 Windows 2000 很有必要。

第 8 章　介绍 Windows 2000 的安全性问题以及策略。

第 9 章　介绍 Windows 2000 的注册表管理的基础知识和基本操作。

第 10 章　磁盘管理。管理磁盘上的信息资源仍然是计算机的主要任务，网络服务器更是如此。Windows 2000

不但继承了这些优点，而且还从 Windows NT 处学到了强大的安全管理功能。

第 11 章　用户环境管理及组策略。用户的工作环境管理可以通过包括用户配置文件（User Profile）、系统规则(System Policy)、登录脚本(Logon Script)，以及环境变量(Environment Variables)的手段进行管理。本章将讲述这些内容。

第 12 章　管理控制台。Windows 2000 的最大特色无疑应该是崭新的管理控制台，作为一个全面的控制台，它添加了许多方便快捷的手段，帮助管理员顺利地完成任务。

第 13 章　备份。Windows 2000 提供了非常方便、实用的备份工具，这是一个可以很容易地备份和恢复数据的工具，用户可以使用备份工具手工进行备份或按照计划定期进行备份作业。

第 14 章　性能监视。介绍如何对系统的性能进行监视，对于维护和保护系统十分重要。

第 15 章　IIS 介绍。IIS（Internet Information Server，因特网信息服务器）可以与 Windows NT、Windows 2000 很好地结合，这样就可以把 NT 设置成为一个 Internet Server，因此它是微软的一个重要产品。

第 16 章　审核。审核是系统安全的重要保障，就像公司或者企业需要查账以确认收支平衡一样，Windows 2000 操作系统也需要审核来帮助检查是否存在安全或者性能等其他方面的问题。本章的内容对于系统管理员尤其重要。

第 17 章　应用程序的支持及管理。本章描述的是 Windows 2000 对应用程序的兼容性问题。

第 18 章　Windows 2000 的维护。本章介绍如何对系统进行维护。

第 19 章　网络基础。介绍网络的基础知识，方便读者对后两章进行学习。

第 20 章　连接到 Internet。介绍如何设置好硬件和软件，使系统接入到 Internet 中。

第 21 章　动用 Internet。讲述如何进行网上浏览、收发电子邮件等内容。

本书由柳敦、薛业涛、陈宇华、许超共同编写。在编写过程中，得到了张鹏、张守连等同志的帮助，在此表示感谢。还要特别感谢中科院高能所的迟少鹏同志为编写本书提供了大量资料。

内 容 提 要

从 Windows 2000 开始，微软公司将 Windows 95/98 和 Windows NT 4.0 合二为一，本书所介绍的 Windows 2000 Professional 是 Windows 2000 家族中的工作站/客户机版本，适用于家庭用户、一般商业平台和网络工作站。

本书全面深入地介绍了 Windows 2000 Professional 在网络方面的应用技术，适合有 Windows NT 背景的用户阅读。全书共分 21 章，包括：Windows 2000 新特性、Windows 2000 安装、Windows 2000 初步认识、系统账户管理、文件及系统权限管理、共享资源及权限设置、域、安全性介绍、注册表管理、磁盘管理、用户环境管理及组策略、管理控制台、备份、性能监视、IIS 介绍、审核、应用程序的支持及管理、Windows 2000 的维护、网络基础、连接到 Internet、运用 Internet 等。

目　录

第 1 章　Windows 2000 新特性

1999 年 12 月 19 日，一推再推的 Windows 2000 终于正式宣布交付 OEM 厂商，无数企业和个人用户为之一振；新千年伊始，微软为之耗费了无数心血的崭新的操作系统就将与广大用户见面了。

无需多言操作系统对于计算机的重要性。随着计算机应用日益广泛，人们对操作系统的性能、稳定性以及易用性也有越来越高的要求。长期以来，尽管微软 Windows 系列的技术水平受到质疑，却仍然是操作系统中无可争辩的龙头，而 Windows 2000 的发布，无疑为这个地位的巩固加上了一个极具分量的砝码。

本章内容包括：

- Windows 2000 简介
- Windows 2000 的新特性

1.1　Windows 2000 简介

微软即将推出的 Windows 2000 将有多个版本，囊括了从低端到高端的所有应用。具体地说，包括专业版（Professional），服务器版（Server），高级服务器版（Advanced Server）以及数据中心版（Data Center）。

为了让大家对其有一个整体的了解，我们简单地介绍各个版本的不同点和硬件需求。

专业版是用来替换 Windows NT 4.0 工作站和 Windows 98 的(但是,由于发现用 Windows 2000 代替 Windows 98 有许多技术上的困难，所以微软继续开发了 Windows 98 的后继版本，名字叫“千禧年”)，被设计为个人电脑或网络客户端的操作系统。专业版的最小硬件要求是 166MHz Pentium；32MB RAM（推荐 64MB）；2GB 硬盘驱动器和至少 650MB 的自由磁盘空间。我们这里介绍的主要是这个版本。

服务器拥有所有的专业版的特点，支持双 CPU，还加入了活动目录控制器（Active Directory）和 Microsoft 的 IIS 5.0 完全版本。服务器版本需要至少 166MHz Pentium 或更高频率的 CPU，至少 64MB 的内存(推荐 128MB)，2GB 硬盘驱动器和至少 850MB 的自由磁盘空间。

高级服务器版能支持 4 个 CPU，并且至少需要 32GB 的内存。

数据中心版与高级服务器不同的是能同时支持 16 个 CPU，最小内存需求是 64GB。

1.2　Windows 2000 的新特性

1.2.1　Windows 2000 的登录

和所有需要极高安全性的操作系统一样，Windows 2000 也必须输入账号和密码，经系统确认无误后才能进入。用过 Windows 95 和 Windows 98 的朋友千万不要认为仍旧可以按 Esc 键进入系统。如果对 Windows 2000 账号和密码漫不经心，就可能导致遗忘密码以致无法登录，甚至密码被人窃取从而失去对系统的控制权。

建议：如果计算机用在重要场所，为了确保计算机的安全，密码不要短于 6 位，而且不应设为生日、单词、姓名，应该字母和数字混用，而且最好每月更改一次。

1.2.2　支持更多的文件系统

众所周知，DOS 和 Windows 95 使用的都是传统的 FAT 文件系统，而在 Windows 98 中使用了增强的 FAT32 系统。

与上述操作系统不同，Windows 2000 沿用了 Windows NT 特有的文件系统，微软称之为 NTFS，这种文件系统在 Windows NT 中开始使用，在 Windows 2000 中又有所改进。同时 Windows 2000 也可以使用 FAT 及 FAT32 分区。

与使用 FAT 及 FAT32 相比，使用 NTFS 的最大优越处在于 NTFS 允许系统为文件及目录设置访问权限，这样一来，Windows 2000 的系统管理员可以很容易地将系统保护起来。NTFS 还支持磁盘压缩，这样可以通过压缩不常用的文件来提高磁盘利用率，这是 Windows 98 的磁盘压缩所做不到的。NTFS 磁盘利用率更高还在于它的簇比 FAT 和 FAT32 小。

NTFS 也有一些缺点。例如，在 Windows 98 和 DOS 下都无法访问 NTFS 分区，这会造成一定的不便，如果要安装多操作系统，就无法兼顾系统安全和数据共享。此外，当 NTFS 下的 Windows 2000 发生故障时，修复和备份数据都比较困难。

提示：由于 NTFS 是一个未公开的文件格式，所以相关工具较少，要访问、删除一个 NTFS 分区或将 NTFS 分区转化为 FAT、是比较困难的。新发布的 Partition Magic5.0 是一个好用的工具，提供了删除 NTFS 和将 NTFS 转化为 FAT 的功能，其功能比较强大。

1.2.3 硬件抽象层 HAL

HAL 的全称是 Hardware Abstraction Layer。使用硬件抽象层可以管理片外高速缓存、定时器、I/O 总线、设备寄存器、中断控制器等硬件设备，并把平台特定的细节对系统其余部分隐藏起来，从而消除了对不同系统厂商对不同版本操作系统的要求。

1.2.4 抢占式多任务方案

与 Windows 95 的协作式多任务方案相比，Windows 2000 的抢占式多任务方案使得操作系统可以控制各个程序得到的 CPU 时间，甚至可以控制各个程序的优先级，因此执行效率更高，并且有助于减少崩溃和延迟，使系统更稳定。

1.2.5 支持即插即用

即插即用在 Windows 95 中已受到了广泛的关注和好评，然而在 Windows NT 4.0 并不支持这个功能，尽管 NT4.0 更先进也更强大。作为 NT 的新生代产品，即插即用理所当然地被微软纳入了 Windows 2000 旗下，喜欢 NT 的朋友可以放心了。

提示：为什么 NT4.0 不支持这一好用的功能呢？答案是硬件抽象层在挡路。要使即插即用正常工作，操作系统需要通过 BIOS（该软件被固化在计算机主板中）在最底层与硬件和软件进行通讯。而在 Windows 95 中，即插即用代理软件，通过 BIOS 判断有哪些存在的硬件以及它们所需的中断号，然后返回来与操作系统通讯协商，确保硬件和软件能够协调地工作。

1.2.6 更强大的管理功能

Windows 2000 推出的崭新的管理工具是激动人心的，包括 Internet 服务管理器、个人 Web 管理器、事件查看器、性能、数据源（ODBC）、服务器扩展管理器、组件服务以及计算机管理 7 大部分。如图 1-1 所示就是计算机管理控制台，它采用树状节点，清晰明了，而且功能完善，显著地加强了可管理性，这些内容在管理控制台一章中将有详细的介绍。

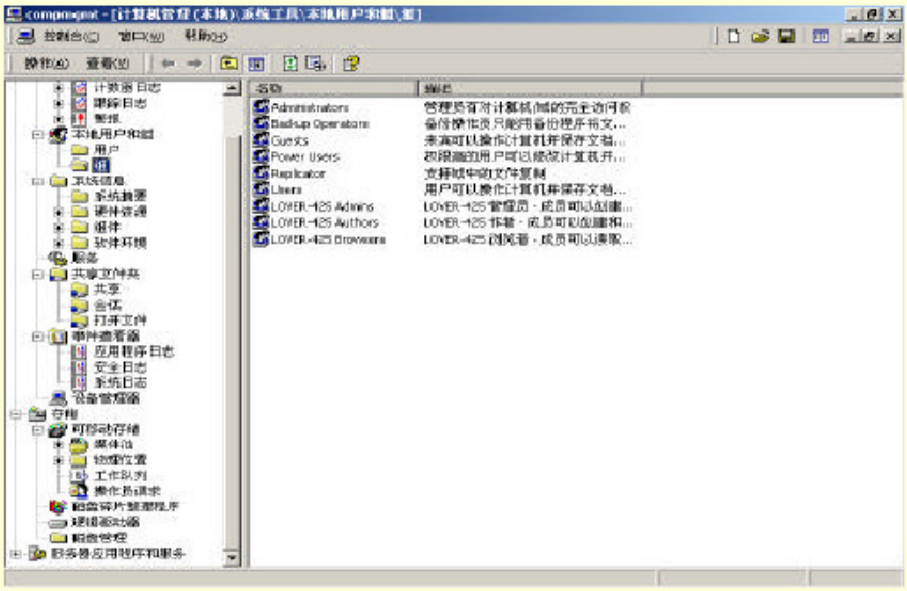


图 1-1　全新的计算机管理控制台

1.2.7　多语言平台

Windows 2000 **采用** UNICODE **双字节编码技术，可以容纳大字符集，并支持多语种。用户不必再为乱码导致的系统崩溃而发愁了。**

第 2 章　Windows 2000 安装

对一个电脑用户来说，最高兴的事莫过于升级自己的系统了。升级系统后所带来的先进功能和强大性能确实是一件让人兴奋的事情，而 Windows 2000 就是一个能带来这一切的操作系统。下面我们将一步步地走入 Windows 2000 的世界，去体会它的强大功能。

本章内容包括：

- 安装方式介绍
- 安装 Windows 2000
- 卸载 Windows 2000

2.1　安装方式介绍

（1）升级安装

如果系统中已经安装有 Windows 95 或者 Windows 98，并且已经安装了一些软件，可以执行升级安装。升级安装将 Windows 2000 安装到 Windows 95/98 的系统磁盘中，一般是 C 盘，安装程序将替换现有的 Windows 系统文件，保留现有的设置和应用程序。

注意：某些应用程序可能与 Windows 2000 不兼容，升级之后在 Windows 2000 中将无法正常运行。

（2）全新安装

全新安装就是在一个没有 Windows 的磁盘中安装 Windows 2000。这种安装比较简单，直接运行光盘中的安装程序就可以开始了。另外，如果在 DOS 或 Windows 3.1 下安装 Windows 2000，安装方法也和全新安装相类似。

（3）双重启动安装

如果系统中已经安装了 Windows 95/98 或者 Windows NT，并且有足够的剩余磁盘空间，那么可以选择这种双重启动的安装方式。

采用这种方式安装，当电脑启动时，Windows 2000 会出现一个启动菜单，以供选择是使用原来的操作系统启动，还是使用 Windows 2000 来启动。这种安装方式有很大的灵活性，但是也有相当的不安全性。

对于家庭用户来讲，由于硬件和软件的兼容性问题，Windows 95/98 还将长期存在，Windows 2000 在短期内还不能完全取代它们，所以采取双重启动的安装方式是一个明智的解决方案。一方面，可以使用 Windows 2000 的全部先进性能；另一方面，可以在某些情况下使用 Windows 98 来完成在 Windows 2000 下不能完成的工作，比如一些较老的游戏和应用程序。

建议：由 Windows NT 的知识我们知道，Windows NT/2000 既可以安装在基本分区上，亦可安装在逻辑分区上。由于 Windows 2000 同时支持了 FAT16/FAT32/NTFS 4/NTFS 5 文件系统，所以它没有基本分区必须是 FAT16 或 NTFS 的限制，没有全新安装必须是在 FAT16 下的限制，也没有 Windows NT 4.0 安装在大于 8.4GB 容量硬盘上的种种麻烦，但我们仍然建议单独划分一个 2GB 以上的独立硬盘空间来安装 Windows 2000。还有就是由于单个物理硬盘最多 4 个基本分区的限制仍未打破，所以仍需把 Windows 2000 安装在前 4 个分区中，否则 Windows 2000 将无法引导。

2.2　安装 Windows 2000

2.2.1　在 DOS 下安装

在 DOS 提示符下安装 Windows 2000 的方法虽然复杂一些，但是成功的几率更大。下面是安装的具体步骤：

（1）进入 DOS 状态

用 Windows 95/98 的启动软盘启动计算机，进入 DOS 状态。也可以从 Windows 95/98 中退出到 DOS 状态，或者从光盘启动进入 DOS 状态。

（2）运行 smartdrv.exe

在 DOS 的 C：\>提示符下，键入 cd windows，进入 windows 目录，然后键入 smartdrv 并执行，这样可以加快安装速度。

加载 Smartdrv.exe 是非常必要的，除非使用高速 IDE/SCSI 硬盘，否则会发现在不加载 Smartdrv 的情况下，在安装过程中系统复制安装文件的时间足够睡个午觉了（当然这个情况在安装 Windows NT 4.0 时也是存在的，不知大家是否注意到了）。不过易于安装一向是微软产品的优良传统，用户只需按着提示进行就可以了，唯一需要注意的是如果使用的是采用 Highpoint 芯片的 DMA66 卡或者其他“另类”SCSI 卡的话，必须先准备好它们的 Windows 2000 驱动软盘，不然很可能设备无法正常运行；如果使用的是 Promise 的 DMA66 卡，则没有上述问题，从 Windows 2000 Build 2183 起已经内置了该卡的驱动程序。

（3）放入光盘

在光盘中放入 Windows 2000 的安装光盘，键入 F：并回车，进入光驱的盘符（这里假设光驱是 F：）。

也可以将安装文件拷贝到硬盘上，然后从硬盘安装，这样可以快一点，还可以防止安装过程中拷贝文件出错。

（4）运行 winnt.exe

键入 cd　i386，进入安装程序所在目录。键入 winnt，开始安装。

下面介绍一下 WINNT 命令的各种参数：

WINNT [/s[:sourcepath]] [/t[:tempdrive]]

[/u[:answer file]] [/udf:id[,UDF_file]]

[/r:folder] [/r[x]:folder] [/e:command] [/a]

/s[:sourcepath]

指定 Windows2000 安装源文件的位置，必须是一个完整的路径，比如 f：\i386\，或者网络路径 \servershare[path]。

/t[:tempdrive]

为安装程序放置临时文件指定驱动器，并把 Windows2000 安装在这个驱动器上。如果没有指定，安装程序

将尝试自动定位在一个驱动器上。

/u[:answer file]

执行一个无人干预的应答文件，使安装程序在无人干预的情况下进行安装。

/udf:id[,UDF_file]

包括了一个唯一性数据库文件的 ID，用于指定安装程序通过哪个唯一性数据库文件来改动无人干预的情况下进行安装所使用的自动应答文件。这个参数将改动自动应答文件的值，并且决定这个唯一性数据库文件中哪个值将被使用。如果没有指定，安装程序将提示你插入一张包含*.udb 文件的磁盘。

在需要同时在多台计算机中安装 Windows 2000 时，往往使用无人干预应答文件（Answer File）和唯一性数据库文件（UDF File）来共同完成自动安装。

/r[:folder]

指定一个将被安装的可选文件夹，这个文件夹在安装结束后将被保留。

/rx[:folder]

指定一个将被拷贝的可选文件夹，这个文件夹在安装结束后将被删除。

/e

指定一个命令，这个命令将在图形安装的最后被执行。

/a

开启辅助功能选项。

Winnt.exe 是在 DOS 下安装 Windows 2000 的程序，在这个目录中还有一个 Winnt32.exe 程序文件，用来升级 Windows NT3.51-4.0、Windows 98，或 Windows 95 的早期版本，并从以前的安装中获取用户的所有设置。

（5）开始安装

Windows 2000 的安装程序提示输入安装文件所在目录，默认是在 i386。按回车键将继续。

（6）复制安装文件

Windows 2000 将一些必要的安装文件拷贝到磁盘中，在以后安装的时候就直接从磁盘中读取，安装程序将自动安排拷贝文件的空间。

（7）重新启动系统

在这之前，安装程序将提示从软驱中取走软盘，从光驱中取走光盘，然后，按回车键重新启动系统。

（8）启动选项

系统重新启动后，提示将安装 Windows 2000，提示时间很短，在这个时间内，你可以选择进入不同的操作系统。

（9）装载设备驱动文件

安装程序装载必需的驱动程序，用来使用计算机中的设备。

（10）选择安装项目

在这一步，直接按回车将开始安装 Windows 2000。此外，按 R 键，可以修复以前的 Windows 2000；按 F3 键，可以退出安装程序。

（11）许可证协议书

按 Page Down 键可以查阅许可证协议书，按 F8 键表示同意。

完成之后，安装程序将检测计算机中的 Windows 版本，如果检测到磁盘上已经安装了一个 Windows 2000，它将提示你是否要再次安装 Windows 2000。

（12）选择磁盘分区、删除和建立分区

安装程序列出了磁盘中的所有分区，可以使用上下箭头选择将 Windows 2000 安装到哪一个分区中。

如果要建立 Windows 2000 双启动系统，一定要选择非系统分区（C 盘），如 D 盘分区、E 盘分区等，不过安装 Windows 2000 的分区必须有大于 800MB 的剩余空间。

在这一步中，我们还可以进行一些分区操作，比如可以将 E 分区删除，然后将这部分空间创建为两个新的分区，在其中一个分区空间安装 Windows 2000，另外一个备用。

如果要删除分区，用光标键选择要删除的分区，按 D 键，然后按照提示操作。可以利用这个办法删除 NTFS 分区。

如果要建立新的分区，用光标键选择未使用的分区项，按 C 键，程序给出创建分区窗口，在“创建磁盘分区大小（单位 MB）”栏中输入新建分区的大小，然后按回车键，程序返回上一界面。

如果选择的磁盘分区包含有一个操作系统，下一步安装程序会提示你是否继续安装程序（按 C 键）或者是选择另外一个分区（按 Esc 键）

（13）选择分区格式

选择 Windows 2000 的安装分区后，程序显示该分区的数据，并列出几个选项：

·用 NTFS 文件系统格式化磁盘

·用 FAT 文件系统格式化磁盘

·保持现有文件系统

如果安装 Windows 2000 这个分区还有其他需要使用的文件，则必须使用“保持现有文件系统”的选项。

如果安装 Windows 2000 这个分区是一个专门指定的分区，没有其他文件还要使用，就可以选择前面的两个选项之一，即选择某种文件系统进行格式化。

最好使用一个指定的分区来安装 Windows 2000，并将该分区格式化成 NTFS 文件系统，虽然这个分区不能被 Windows 95/98 系统识别，但 NTFS 文件系统比较安全，磁盘空间的使用效率也比较高。

（14）格式化分区

假设我们选择上一步的第一项，也就是“用 NTFS 文件系统格式化磁盘”，则就要等待系统完成这一工作，如果选择“保持现有文件系统”就没有这一步。

格式化时按 F 键就开始格式化。安装程序将显示格式化进度条。

（15）复制文件

安装程序开始检测磁盘，为开始复制文件作准备，检测通过后，安装程序将开始实行把 Windows 2000 的操作系统文件复制到磁盘上。

（16）重新启动

文件复制完成后，进行一些初始化工作，将系统的一些初始配置值设定完成，然后重新启动。

第一次启动 Windows 2000 的步骤：

第一步：加载 Windows 2000

系统的这一次启动，就将以 Windows 2000 的内核来启动，启动后再继续以后安装。首先出现对话框，提示安装开始，点击下一步。

当长时间不点击下一步，安装程序将自动继续。

第二步：检测设备

这一步检测系统的设备，检测的时间可能比较长。Windows 2000 将查一下你的硬件是否已被包含在支持硬件列表里了

第三步：区域和键盘设置

这一步设置你所在的区域和使用的键盘布局，一般我们选择默认的设置就可以了，如果你要修改某一项，可以单击相应的自定义按钮，然后进行修改。单击下一步继续。

第四步：输入姓名和单位名称

这一步要求输入名称和单位名称。这个姓名可以作为 Windows 2000 中的一个登录名称，这还要看以后的设置。

第五步：输入产品序列号

这一步输入 Windows 2000 的安装密码，这个密码是印刷在 Windows 2000 的安装光盘的包装外壳的背面。

第六步：输入系统名称和登录密码

首先，安装程序提示它为这一台计算机提供了一个名称，这个名称就是计算机的标识，主要用于计算机网络的识别。你完全可以不理会安装程序给你指定的这个名称，而使用一个你认为比较有意义的名称。

在 Windows 2000 中，可以设置多个用户，而且用户的级别不同，对操作系统的操作权限也不同，不同的用户都要用自己的名称，即账户，进行登录。Windows 2000 中设置了一个有最高权限的登录账户，administrator，在安装的时候，要为该登录账户设置一个密码。

第七步：设置日期和时间

这一步，设置系统的时区、日期和时间，一般情况下，我们都可以按照默认的设置继续以后的安装。

第八步：安装网络组件

开始安装网络组件，并弹出选择窗口，选择是典型还是自定义安装。对于一个高级的操作系统，选择自定义安装更好。

自定义安装的项目是一些局域网络设置，这些设置在安装成功后也可以进行。

第九步：选择网络类型

选择典型安装后，还需要简单选择以下你的网络类型，对绝大多数家庭用户来说，一般选择第一项：“ 此计算机不在网络上 ”。

第十步：开始安装网络组件

这一步将安装所选择的网络组件。

第十一步：安装系统的一些组件

在 Windows 2000 中，安装组件（比如附件程序等）是自动进行的，不像 Windows 95/98 需要自己选择。安装组件的过程比较长，分为安装组件、注册组件、保存设置、删除用过的临时文件 4 个部分。

第十二步：完成

完成后，系统将又一次重新启动。

第十三步：设置网络标志

重新启动后，还有一些网络设置过程，安装程序提示将进行网络设置，点击下一步，出现网络标识设置，点击下一步，出现网络标识设置画面，选择 “ 要使用本机，用户必须输入用户名和密码 ”，这样当第一次启动的时候系统就只有两个账户：administrator 和 guest，其中 guest 是系统默认不能使用的账户。如果选择 “ Windows 假设下列用户已经登录到本机上 ”，然后在下面的栏中输入一个账户名称和密码，系统开机时将以该用户自动登录。重新启动后，安装彻底完成。

2.2.2 其他的安装方式

以上介绍的是比较典型的安装方式。但是随着系统和选择的不同，安装的步骤也有很大的不同，可能会多几个必须的步骤。

下面再简单介绍一下如何在 Windows 95/98 下进行 Window2000 的安装，其实步骤和在 DOS 下安装程序差不多，只不过是界面形式和顺序变了一些，许多收集信息的工作是在开始安装以后，通过 Windows 的对话窗口来完成的，后面的步骤和形式就和在 DOS 下差不多了，可以参考前面。

（1）首先放入 Windows 2000 的安装光盘，如果设置了光盘自动运行，将弹出提示升级窗口，如图 2-1 所示。选择 “ 是 ”，将进入 Windows 2000 安装向导，如图 2-2 所示。

图 2-1 提示升级

图 2-2　安装向导

（2）然后，选择“升级到 Windows 2000 ”(如果语言版本不同，则这个选项是灰色，不可选)，单击“下一步”，安装程序开始检测你现有的系统，如果一切正常，则会弹出选择安装程序窗口，选择“全新安装”即可实现双重启动。单击“下一步”按钮将出现许可证协议书。如图 2-3 所示。

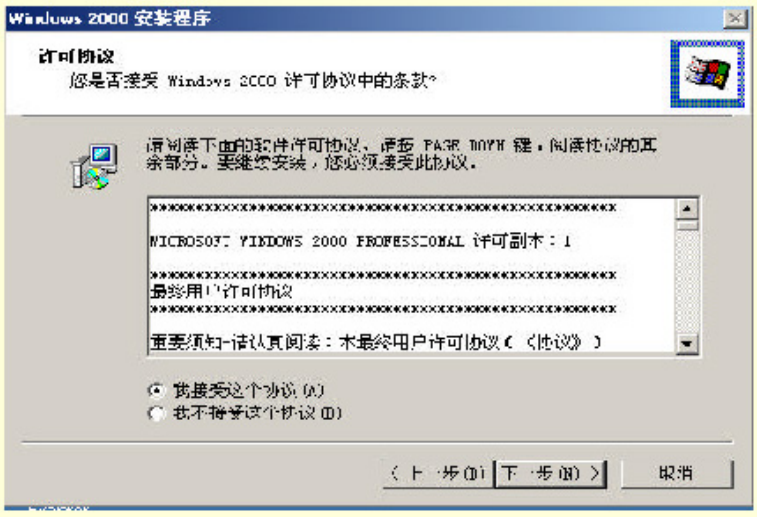


图 2-3　许可证协议书

（4）选择“我接受这个协议”，单击“下一步”按钮，出现安装程序选择项目。如图 2-4、图 2-5、图 2-6 所示。

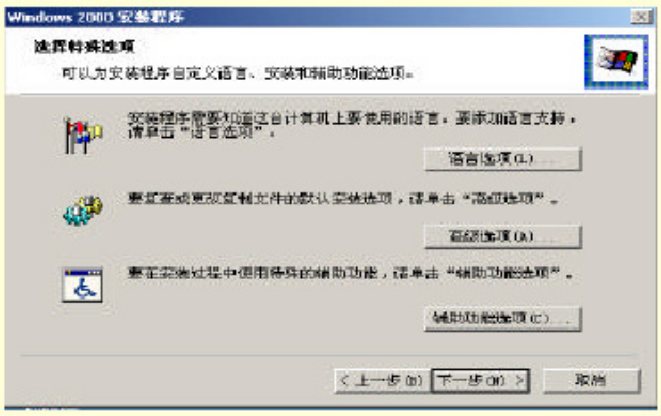


图 2-4　安装程序选项

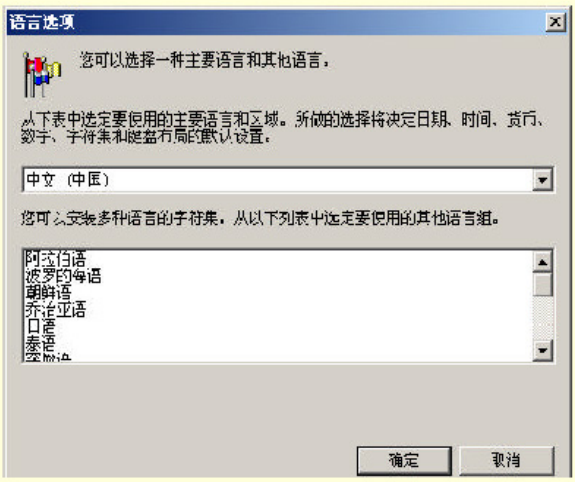


图 2-5　语言选项

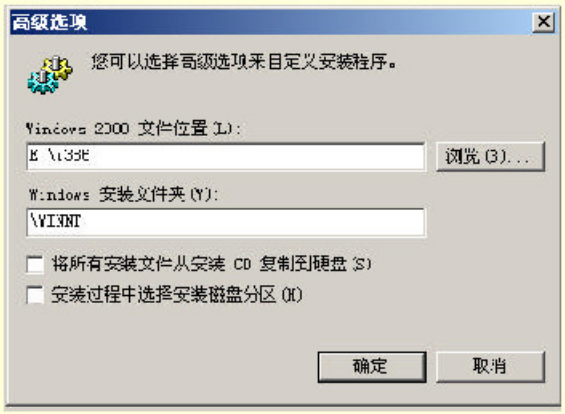


图 2-6　安装路径选择

（5）正确选择安装选项之后，安装程序将出现监测系统信息窗口，如图 2-7 所示。

（6）下面的安装步骤就是从安装光盘上复制所需要的文件到硬盘上。屏幕将出现安装进度条，如图 2-8 所示。

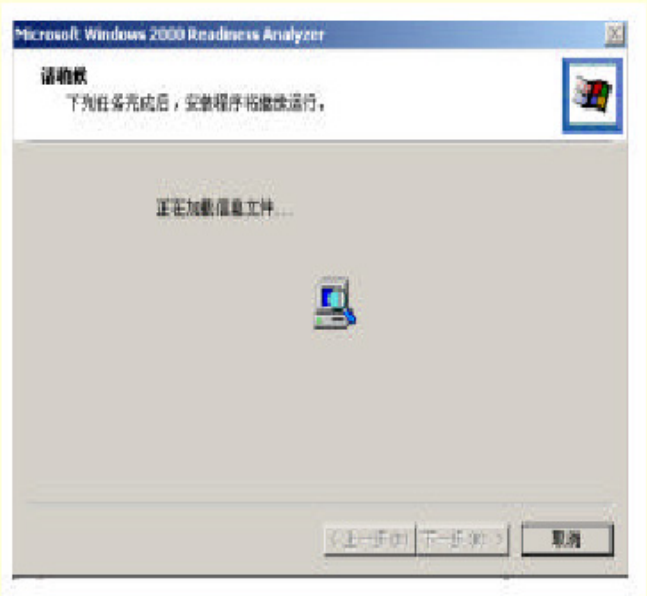


图 2-7　监测系统信息

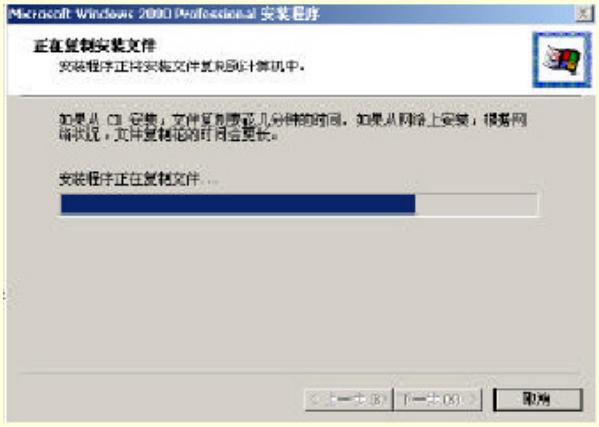


图 2-8　复制文件到磁盘

（7）安装程序复制完文件后，将重新启动系统，进入系统的设置阶段。

2.3　卸载 Windows 2000

卸载 Windows 2000 比卸载 Windows 95/98 要麻烦一些，我们下面分 FAT、FAT32 和 NTFS 来说明。

FAT 和 FAT32 下的卸载相对而言比较简单，这种卸载又可以分为多重启动和非多重启动两种：

（1）如果不是多重启动，可以用 Windows 95/98 的启动盘启动计算机，直接将 Windows 2000 系统文件所在分区进行格式化，然后安装其他操作系统，或者重新安装 Windows 2000 。

（2）如果是多重启动，用 Windows 95/98 启动计算机，进入 Windows 95/98 后，删除 Windows 2000 的文件，就完成卸载了。这样一来，原来 Windows 2000 下的软件就不能用了。

NTFS 下的卸载就稍微麻烦一些，这种卸载也可以分为多重启动和非多重启动两种：

（1）如果不是多重启动，可以用 Windows 95/98 的启动盘启动计算机，用 FDISK 程序直接将 Windows 2000 系统文件所在分区进行删除操作，再在这部分空间上建立一个分区，对它进行格式化，然后安装其他操作系统，或者重新安装 Windows 2000 。

（2）如果是多重启动，用 Windows 95/98 启动计算机，运行 FDISK 删除 Windows 2000 的 NTFS 分区，然后在上面建立新的分区，重新启动，对新分区进行格式化，重新启动计算机，即可进入 Windows 95/98，完成卸载。

建议：使用这种方法不能去除 Windows2000 的多重启动菜单，如果想去除 Windows2000 的多重启动菜单，可以使用这个方法。卸载 Windows2000 之后，用 Windows95/98 的启动软盘启动计算机，放入 Windows95/98（你所安装的操作系统）的光盘，运行 Setup.exe，进行安装，安装过程中选择不保留原系统文件，执行安装直至开始复制文件，然后退出，这时重新启动系统，可以看到 Windows2000 的启动菜单已经不见了。

第 3 章　Windows 2000 初步认识

为了增加对 Windows 2000 的感性认识，在开始学习使用 Windows 2000 之前，我们首先简单介绍一下 Windows 2000 的总体情况。

本章内容包括：

- Windows 2000 的新外观
- 控制面板介绍

3.1　Windows 2000 的新外观

3.1.1　动态桌面

Windows 2000 有一个比过去更简洁的桌面，使用户视觉更加舒适；另外微软引入了活动桌面（Active Desk）的概念，可以把一个 Web 页作为桌面，如果熟悉 VBScript 或 JavaScript 脚本语言，还可以编程添进动态内容使桌面“动”起来。

要选择 web 页作桌面，只需在桌面上单击右键，从上下文菜单中选择“动态桌面”中的“显示 web 内容”即可，如图 3-1 所示。

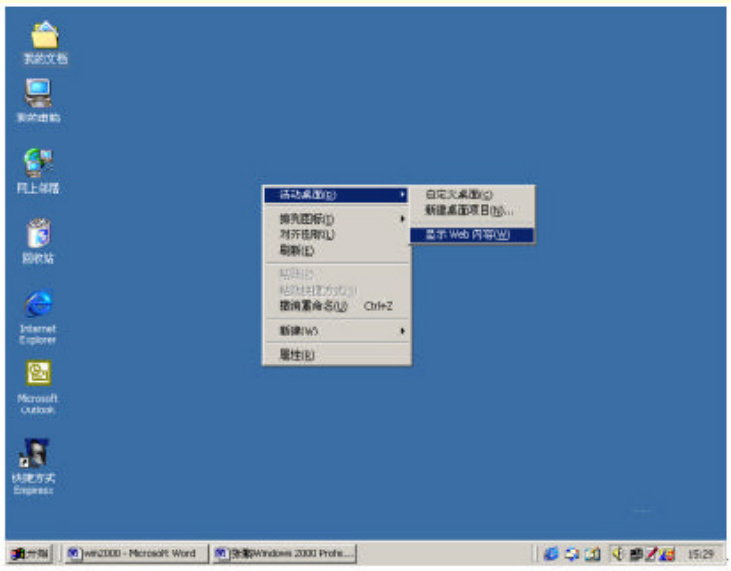


图 3-1　显示动态桌面

用自己的 Web 页面作为桌面后，也许你不愿再显示“我的电脑”，“回收站”等图标，这时候只需在桌面上单击右键，从“活动桌面”下拉菜单中选择“隐藏桌面图标”即可。当然你还可以自定义自己的桌面。

提示：也可以从控制面板中的“文件夹选项”里设置 Active Desktop 或允许显示 Web 内容。

3.1.2　新的工具栏

活动桌面只是微软“个性化桌面”的一部分，细心的用户会注意到，工具栏也有了新的变化。在工具栏单击鼠标右键，从快捷菜单中选择“工具栏”命令，如图 3-2 所示，可以添加地址、链接、桌面等工具栏。默认的工具栏是快速启动，微软在里面添加了 IE 浏览器和 OUTLOOK，与活动桌面一样，这样做都是为了使

INTERNET，特别是 IE 浏览器与 Windows 2000 更好地集成。

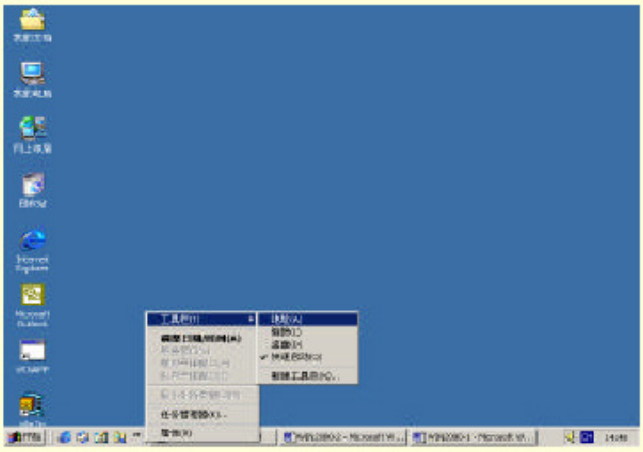


图 3-2　个性化的工具栏

此外，也可以自定义工具栏，把常用的文件夹添加入内，从而避免在资源管理器中一层层地展开。在图 3-2 中所示的快捷菜单中，选择“新建工具栏”命令，出现如图 3-3 所示的新建工具栏对话框，这时候可以选择文件夹、网上邻居、Internet 地址、回收站等项目并添加到自己的工具栏上作为快捷方式。

图 3-3　自定义工具栏

3.1.3　简化的开始菜单

Windows 2000 中还有一个显著的变化，当单击“开始”菜单，选择“程序”后，新的发现是菜单变得十分的简洁，不再像 Windows 95 或者 Windows NT 4.0 那样臃肿了。只有常用的程序才显示，不常用的则被隐藏起来。如果需要使用一个平时不太常用的程序也不难，只需把鼠标稍微停留一会儿，它就会出现，如图 3-4 所示。

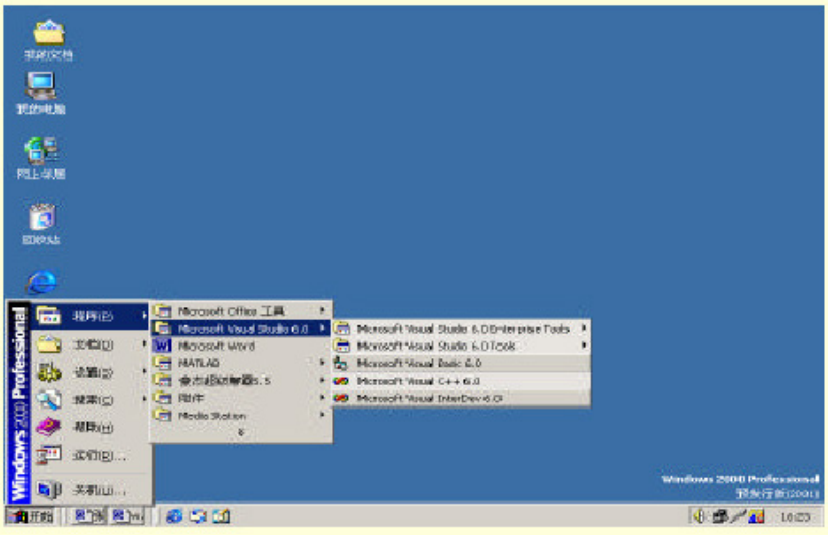


图 3-4　简化的“开始”菜单

Windows 2000 根据用户使用的情况，可以自动调节程序显式出现还是隐藏。一旦某个程序被调用，它就会在下次打开“开始”菜单时出现；如果它很长时间没再被使用，就会被系统隐藏起来。

3.1.4 更方便的资源管理器

除此之外，Windows 2000 的整体风格得到了进一步的统一，我们所熟悉的 Internet Explorer 与资源管理器已经体现了从外观到精神上的统一。如图 3-5 所示，资源管理器中融入了 IE 的搜索工具和“历史”查看栏，不但可以整理自己的收藏夹，还可以方便地链接到微软的网站上去，相应地，也可以随意地通过 IE 浏览本地资源或在网上冲浪。此外，全新推出的计算机管理工具（Computer Management）在界面上也与资源管理器十分相似。统一的风格意味着界面的友好性，用户在不同程序间的切换不会带来视觉的陌生。可以预见的趋势是：微软致力于将自己的 Windows 系列产品发展成为具有相似的界面，统一的风格以及一致的功能的操作系统，在未来的桌面网络操作系统中，用户操作本地资源与访问远程资源将不会感觉到有什么不同。

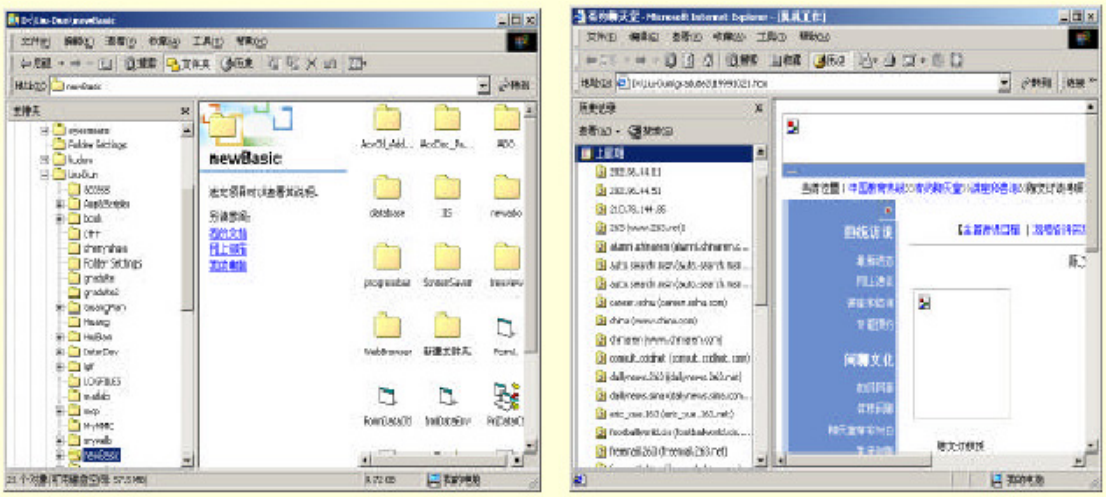


图 3-5 统一的资源管理器与 IE 界面

3.2 控制面板

控制面板和资源管理器都是最常用的管理工具之一（也许读者已经注意到，控制面板的界面也已经和资源管理器相统一了），可以使用控制面板来配置自己的计算机。

简单的如鼠标快慢、日期时间、区域、桌面和屏幕保护程序；高级的如用户及密码管理、数据源（ODBC）、Web 管理都可以在这里设置。控制面板还可以管理计算机外设，比如打印机、扫描仪、照相机；可以通过硬件向导添加和管理硬件；通过程序向导合理干净地添加或删除程序，还能通过设置任务计划让计算机自动执行任务。控制面板如图 3-6 所示。

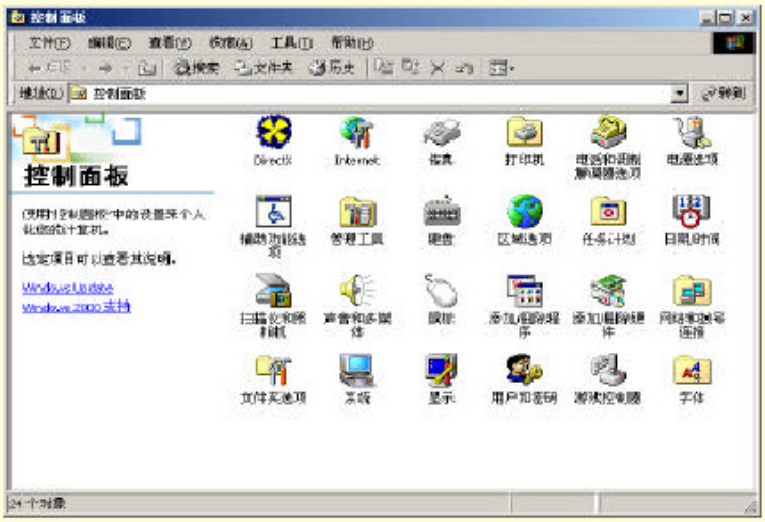


图 3-6 控制面板

控制面板各类功能简单介绍如下：

3.2.1　个人配置

区域设置、声音和多媒体、字体、显示、日期时间、文件夹选项同属此类。通过适当的设置，可以使计算机更符合用户的个人习惯。

提示：出于安全的考虑，Windows 2000 自动隐藏了一些操作系统文件，如 C 盘下的 Bootsect、Config.sys 等，微软认为编辑或修改它们会给计算机造成危险。要想查看这些它们，从控制面板中的“文件夹选项”里选择“查看”选项卡，清除选项“隐藏受保护的操作系统文件”即可。

3.2.2　外设管理

外设管理包括键盘、鼠标、打印机、传真、扫描仪和照相机。用户还可以通过“添加/删除硬件”里的硬件向导方便地管理计算机中的各种硬件设备，比如 DMA 控制器等。

3.2.3　网络连接

Internet、网络和拨号连接、电话和调制解调器选项，帮助用户方便、安全地与外部世界通讯或是进行本地连接。在进行本地连接中，需要设置相应的协议，如 TCP/IP 通信协议、NWLink 通信协议、NetBEUI 通信协议以及相应的客户服务，如 CSNW 服务等。这些内容在后面的网络基础部分将有详细介绍。

3.2.4　强大的向导

控制面板还拥有强大的向导管理功能：配置硬件有硬件向导；上网有连网向导；添加/删除程序也有向导，它们都能帮新手一步步到位。

提示：机器使用时间长了以后，会发现启动越来越慢，一个原因是一些程序没有干净地删除，遗留了少部分垃圾文件。通过添加/删除程序向导的帮忙，有助于减少垃圾文件。

3.2.5　内部管理与性能优化

Windows NT 素以强大的功能与可靠的安全性著称。Windows 2000 继承和壮大了这一特性。

“用户和密码”帮助系统管理员更可靠地管理系统，防止外来入侵；“管理工具”是 Windows 2000 的最大特色之一，通过对事件查看器、性能查看器和组件服务等工具的集成，大大加强了管理；进行数据库工作，需要使用数据源（ODBC）管理器设置数据源；控制面板里的“系统”选项也是十分重要的工具，除了帮助管理虚拟内存以优化系统性能外，还可以设置系统的启动和故障恢复选项。

注意：只有系统管理员或者特权用户（Power Users）才有权利通过管理工具和用户密码管理系统里的用户及权限，普通用户没有这个权力。

第 4 章　系统账户管理

在个人电脑领域，Windows 95 和 Windows 98 无疑是操作系统中的佼佼者。然而作为网络操作系统，Windows NT 在 1993 年 Microsoft 初次推出时与 UNIX、NetWare 相比，并不占优势。1996 年，随着 NT 4.0 Workstation 与 Server 的推出，情况发生了变化。Windows NT 已经逐渐发展为功能强大、先进的操作系统，应用范围从企业级的数据库和文件服务器，部门级的 CPU 服务器，到个人 PC 操作系统，以至商业用的掌上机，得到了广泛的承认。

Windows NT 4.0 的成功也许借助了它与 Windows 95 的相似界面，但是作为先进的网络操作系统，它的稳定性，及安全性都是 Windows 95 和 Windows 98 所无法比拟的。Windows 2000 原称 NT 5.0，其构造基于 NT 内核，理所当然继承了 NT 的许多优点。下面我们就来看一些 NT 在保护安全性方面的例子。

实例一

一个 3 口之家，父亲是部门经理，电脑里有许多重要资料，但妻子和孩子也要使用计算机。这时，可以在机器里装 Windows 2000，父亲做管理员（Administrator），将妻子和孩子设为普通用户（Users），这样一来就可以控制他们的权限，防止他们访问敏感资料及不小心导致的破坏。如图 4-1 所示。

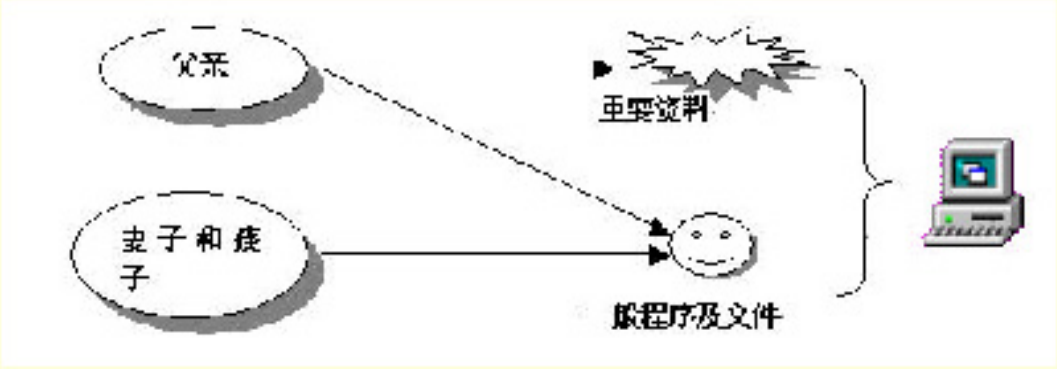


图 4-1　实例一图示

实例二

在一个大的公司里，不同部门里的不同等级人员都要使用电脑，而且总裁，部门经理和普通工作人员的权力和职责都不一样。好的办法是：通过不同的域和工作组，将用户合理地组织起来，并给他们不同的权限。这样，下层人员将无法获得上层机密（例如公司利润，职员薪水数据库等）。实施一定的安全规则，采用登录口令、限制登录时间、进行安全审核等计划可以最大限度地保障系统安全。为了工作效率考虑，共享网络资源是必不可少的，而如果共享目录位于 NTFS 文件系统分区中，还可以针对共享目录里的个别目录和文件设置使用权限。这些要求都是 Windows 95 和 Windows 98 所无法满足的。

所有这些安全性的设置都必须从账户的设置开始，就像我们每个人在银行都有自己的账户一样，Windows 2000 建议为每个用户设立单独的账户而不是多人共同享有一个账户，这样发现问题时比较容易确定责任人，用户也可以有更强的责任心保护自己的账户。

本章内容包括：

- 内置的用户账户
- 添加用户账户
- 用户管理
- 账户策略
- 组管理方案

4.1　内置的用户账户

系统安装完毕后，自动产生两个内置的账户，分别是：

■ Administrator （管理员）

系统管理员具有系统中最高的权力，可以增加、删除或者是禁用各个账户，可以为不同用户设置不同的权限以及通过系统工具深入优化系统性能。不能删除内置的 Administrator 账户。但是如果觉得 Administrator 太长不容易输入，或者处于安全的考虑，可以为这个账户改名，例如改为 Admin。

系统安装时会要求输入 Administrator 账户的密码，请牢记这个密码。

■ Guest（来宾）

Guest 是供来宾临时访问计算机设置的账户，只有有限的权限，不能安装程序和进行对系统设置可能有破坏性的改动。缺省时，Guest 账户被禁用。

如果安装的是 Windows 2000 Server，或者在 Windows 2000 Professional 中安装了 Internet Information Server（IIS），则会另外添加两个用户账户 IUSR_ComputerName 和 IWAM_ComuterName。顾名思义，IUSR_ComputerName 是 Internet 来宾账户，同 Guest 账户相似，可以匿名访问 Internet 信息服务；IWAM_ComuterName 账户则可用于启动进程之外的应用程序的 Internet 信息服务。

建议：系统管理员应该为自己设两个帐号：管理员帐号和普通用户帐号。平时用普通用户帐号登录，当需要做一些系统的高级管理和内部性能优化工作时，再用管理员帐号登录，这样有利于系统的安全。

4.2　添加用户账户

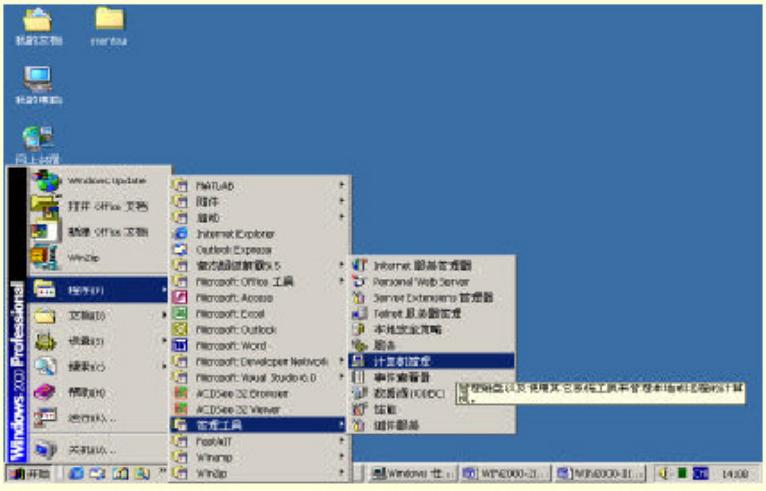
添加用户账户是最基本的账户管理手段之一，通过全新的 MMC（Microsoft Management Console）控制台，可以非常方便地做到这一点。

注意：必须是系统管理员或者是特权用户（Power Users），才有这个权力。普通用户不能使用管理工具添加用户帐号。

步骤如下：

（1）启动开始菜单，选择程序组。

（2）从程序组中选择“管理工具”→“计算机管理”，如图 4-2 所示。



（3）从计算机管理单元中选择“本地用户和组”，在“本地用户和组”下的“用户”文件夹上单击右键，选择“创建用户”命令，如图 4-3 所示。

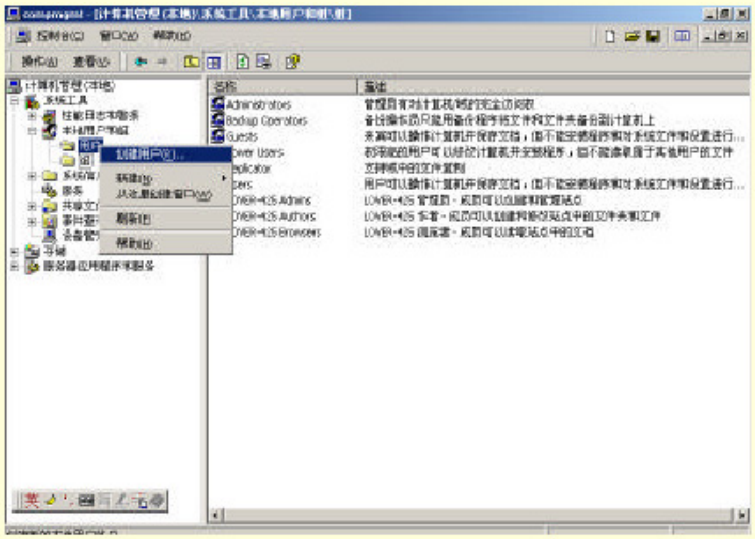


图 4-3 计算机管理控制台

（4）在图 4-4 所示的“创建用户”对话框中，“用户名”和“密码”必须输入，并要求确认密码。而“全称”和“描述”是可以省略的，只是为了更方便地区分用户。

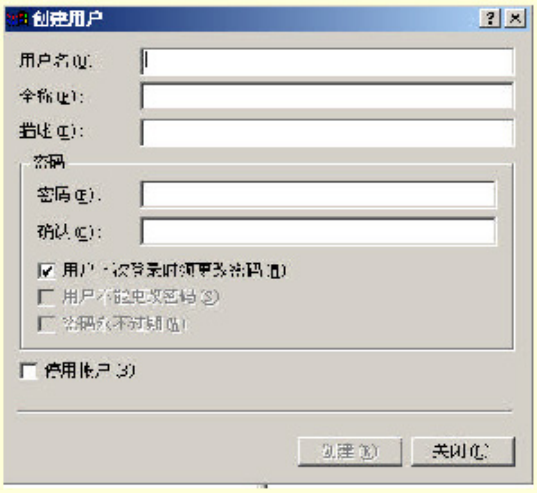


图 4-4 “创建用户”对话框

管理员对新用户的密码设置可以有不同方案：

■ 用户下次登录时需更改密码：缺省设置。由于新用户的密码是管理员代设的，所以一般选中此项，用户设置自己易记的密码。

■ 用户不得更改密码：如果此账户是多人共享的，应该禁止私自更改密码。

■ 密码永不过期。

■ 停用账户：确知此用户暂不使用时，禁用这个账户,以防止他人窃用。

提示：新建的用户默认为是普通（低级）用户，要想设为高级用户，可以通过加入组来实现。

在 Server 版本中，还需要设置用户的可登录时间、允许登录的工作站、账户有效日期等信息。

4.3　用户管理

通过 MMC 中的本地用户和组管理工具，可以十分方便地管理用户，如果要一次管理多个用户，只要按住 Ctrl 键，就能同时选择多个用户。

4.3.1　用户属性

用户的管理可以通过用户属性来进行。用户属性包括用户名、密码、隶属的组，以及配置文件、登录脚本等信息，如图 4-5 所示。

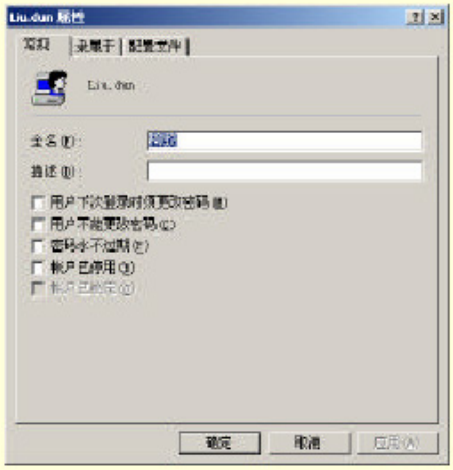


图 4-5　用户属性

用户环境的设置包括用户配置文件（User Profile）、登录脚本（Logon Script）及主目录（Home Directory），这部分的设置在用户高级环境管理一章中有详细讲述。此外，可以通过 Windows 2000 中的组策略对用户环境管理进行强化，Windows 2000 内设了许多组，后面将有详细讲述，并可以很方便地将用户添加到组中进行管理，而不用一项项地添加权限。

4.3.2　用户任务

Windows 2000 对本地用户管理的一大改进是可以为用户设置任务。一般的任务如设置密码；而高级任务主要为工作站或服务器编写应用程序的人员使用。

4.3.3　重命名账户

选择需要重命名的用户账户，单击右键，选择“重命名”，然后输入新用户名即可。

对内置账户重命名是保护系统安全的一种手段，例如为 Administrator 账户重命名，可以有效地阻止别人窃取密码。

4.3.4　删除及禁用账户

为防止用户登录，可以用两种办法：删除或禁用账户。被禁用的用户账户依然存在，只是暂时无法用它登录。例如当某位工作人员出差时，可以在其出差期间禁用此账户，当他回来时再恢复此账户的使用。注意：Administrator 内置账户是无法禁用的，试图禁用它时，将出现错误提示，如图 4-6 所示。

图 4-6　不能禁用 Administrator 内置账户

要禁用某一账户，打开如图 4-5 所示的用户属性对话框，选择“账户已停用”复选框即可。禁用账户仍存在用户列表中，但有红色标志，如图 4-7 所示。

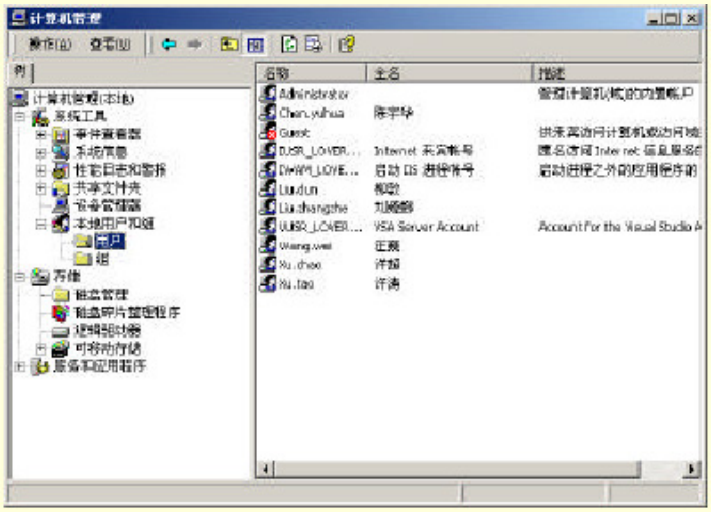


图 4-7 禁用的账户

常常通过禁用账户的办法保护系统的安全，如果发现某个账户存在安全问题，可以禁用这个账户，例如禁用 Guest 账户可以禁止系统外部人员匿名登录。

删除账户则要严厉的多。账户的删除是永久性的，无法恢复，也不再出现在用户列表中。初次接触这种安全机制的管理员可能会犯这个错误：以为删除的账户可以简单地通过建立同名的账户恢复，但事实上，即使名字相同，建立的也将是一个全新的账户。这意味着新账户的属性、权力、权限等配置都和过去不一样，需要重新设置。所以删除账户时必须十分小心，对个人和小的用户群，也许只是小小的麻烦，但对大的公司来说，这个疏忽意味着成倍的时间和金钱。系统将在删除账户时提出警告，如图 4-8 所示。

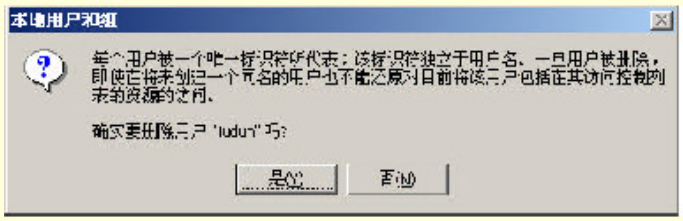


图 4-8 删除用户时的警告

比较合理的办法是：管理员先停用账户，然后周期性地做删除工作。

提示：由前面允许对帐户重命名也可以看出来，系统内部不是根据用户名存储用户权限信息的。事实上，这里起作用的是 SID（Security Identification），每次添加新的帐户，系统会给他一个安全标志符，也就是 SID，用来设置用户权限。

4.4 账户策略

一个系统规模越大，用户越多，从安全性的角度来考虑就越容易受到攻击。外部攻击往往通过窃取、猜测口令从而试图进入系统，制定一定的措施可以最大限度地保障安全。

首先，让我们站在入侵者的立场上看看我们可能做点什么。假设我们的朋友恰巧不在身边，而我们又很想用用它的机器（当然，我们只是想玩玩游戏消磨时光，并没有恶意），那么我们一定会想尽办法输入一些有意义的符号，比如他的生日、姓名、喜欢的东西等等，看看有没有可能恰好就是他的密码。现在你应该明白密码也

有不可靠的地方，虽然每个人都不会忘记自己的生日，但别人也能记在心上，因此不要使用生日等有意义的数字或者字母组合作为账户密码。强化的密码要求包含大小写字母，阿拉伯数字甚至一些古怪的字符，应该是别人，包括最亲近的朋友也觉得匪夷所思的组合。虽然这比较麻烦，但如果用户做的是重要工作并需要绝对的安全，这点代价是完全值得的。

Windows 2000 始终关注系统的安全性，可以十分方便地利用微软的设计，实施安全可靠的账户密码措施。Windows 2000 为系统配置了安全模板（Security Templates），针对不同的版本，提出了不同强度的保障措施。这些措施可以分为 5 个级别，以适应不同程度的要求：

- 基本（Basic）
- 兼容（Compatible）
- 安全（Secure）
- 高度安全（Highly Secure）
- 专为域控制器设置（Dedicated Domain Controller）

这些模板文件 Workstation、Server、Domain Controller 的不同版本和用途之分，地位越高，对安全的要求也越高。

模板文件都以纯文本格式存储，缺省保存在\%systemroot%\security\templates 路径下，后缀名为.inf。这里\%systemroot%指系统路径，一般为 C:\winnt。读者可以从资源管理器中打开他们浏览。用户也可以对安全策略进行浏览、调整，并应用到本地计算机或者导入到组策略对象中。

管理员可以在管理控制台中打开“本地计算机策略”中的“计算机配置”做进一步的管理。“本地计算机策略”是一个为安全模板文件提供编辑功能的独立的 MMC 管理控制单元，如果您的控制树里还没有这个单元，应该首先把它添加入内，步骤为：

（1）从控制台主菜单中选择“添加/删除管理单元”，如图 4-9 所示。

（2）在对话框中单击添加按钮，新的管理控制单元可以添加到控制台根节点，也可以加到某个子节点，视用户方便而定。

（3）从管理单元列表中选择“组策略”，如图 4-10 所示，单击“确定”按钮即可。在本地计算机中，组策略将变为“本地计算机策略”。

现在，本地计算机策略出现在控制台根节点下。

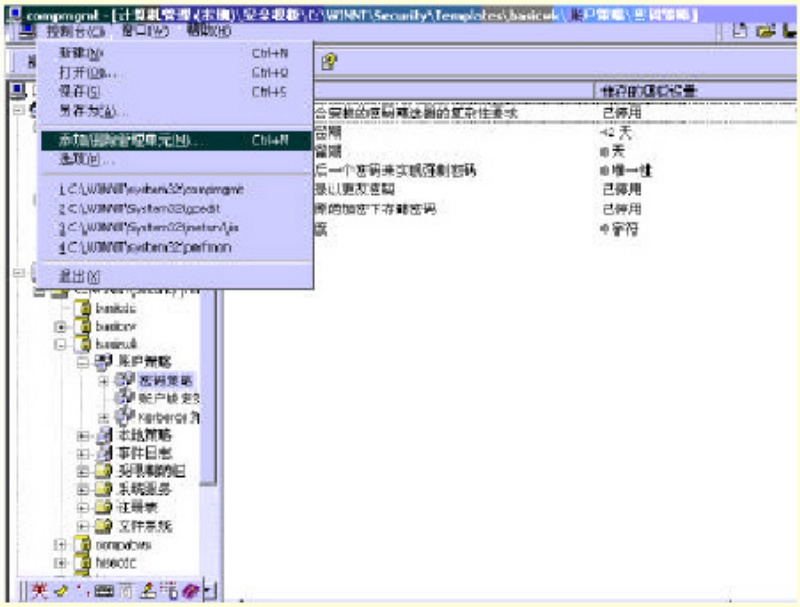


图 4-9　添加/删除管理单元

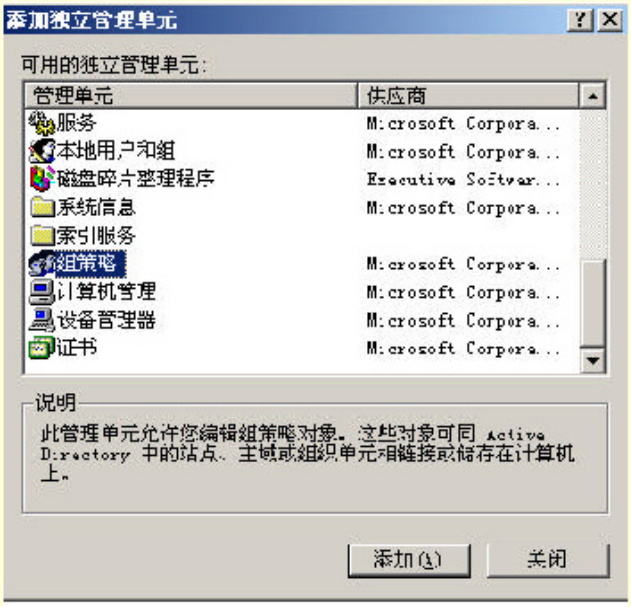


图 4-10 添加“组策略”

将本地计算机策略添加入到管理台后，下一步的工作就是进行具体的密码及账户锁定策略的安排。步骤如下：

(1) 从“本地计算机策略”中选择“Windows 设置”。

(2) 继续从子节点中选择“安全设置”。

(3) 继续从子节点中选择“账户策略”。

(4) 继续从子节点中选择“密码策略”并打开。此时的显示如图 4-11 所示。

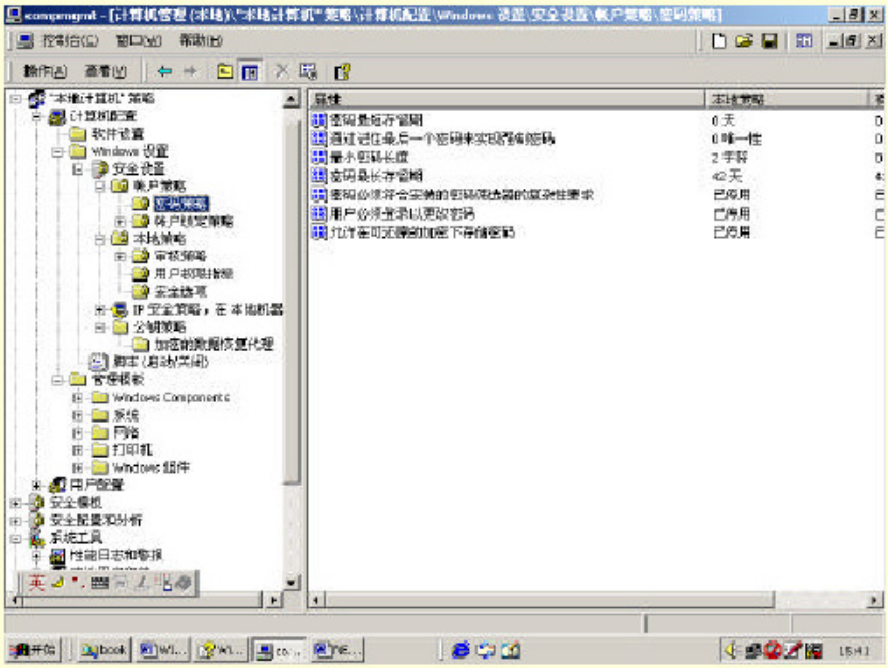


图 4-11 层层打开的“密码策略”

这里只介绍账户及密码策略，其余安全性问题部分后面会继续讨论。

微软提出的账户策略包括密码策略和账户锁定策略，其中大多数策略我们在 Windows NT 4.0 中都已有所了解了。

4.4.1　密码策略

表 4-1　密码策略设置

密码策略	设置
密码必须符合安装的密码筛选性的复杂性要求	停用/启用
密码最长存留期	天数
密码最短存留期	天数
通过记住最后一个密码来实现强制密码	唯一性个数
用户必须登录以更改密码	停用/启用
允许在可还原的加密下存储密码	停用/启用
最小密码长度	位数

密码策略设置如表 4-1 所示。各个设置选项说明如下：

■　密码必须符合安装的密码筛选性的复杂性要求

也就是说，强化的口令要求包含大小写字母、阿拉伯数字甚至一些特殊的字符（比如！@ # $ % ^ & * 等）。

■　密码最长存留期

用户使用密码的最长期限，到时系统会要求用户重新设置密码。

■　密码最短存留期

用户使用密码的最短期限，此期限未到时用户不得更改密码。最短期限可以设为 0 天，这对应于过去 NT 中的允许立即更改选项。

■　通过记住最后一个密码来实现强制密码

此处设置旧的密码是否可以重复使用。如果设为 0，则表示不保存密码历史记录。管理员也可以要求保存密码记录，例如设为 3，则新设的密码不能与最近 3 次所设的密码相同。经常变化的密码不利于黑客的破坏。

■　用户必须登录才能更改密码

此选项防止用户在密码过期后自行更改密码，此时只有管理员才能更改密码。

■　最小密码长度

建议最小设为 6～8 位，使口令不容易被猜出。

具体管理时，打开模板文件的“密码策略”，在要修改的策略上单击右键，选择“安全性”，如图 4-12 所示。

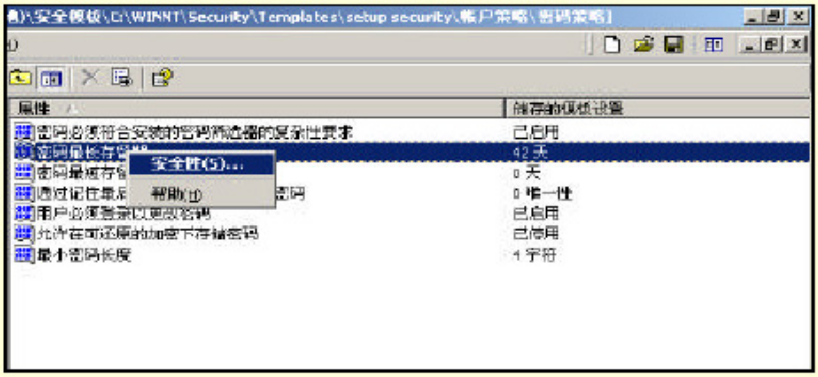


图 4-12　选择安全性

然后可以进行具体的策略修改，修改密码的最小长度如图 4-13 所示。

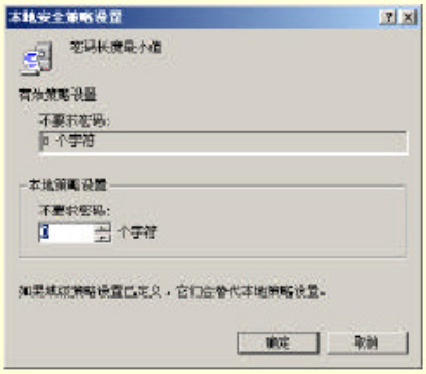


图 4-13 密码策略安排

例如，设置密码最小长度为 6 位的策略后，再设置某用户密码只有 5 位或更少，则会出现如图 4-14 的错误信息：

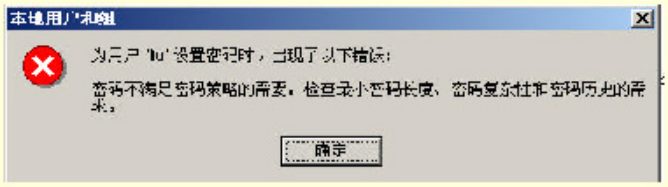


图 4-14 不满足密码策略要求时出错

4.4.2 账户锁定策略

账户锁定是通过锁定特定账户，以防止外人试图通过猜测本账户密码以登录的策略。

账户锁定策略有如下三项：

■ 账户锁定时间

账户锁定时间是指锁定账户后，系统自动解除锁定的时间。

■ 账户锁定计数

设定为某一账户无效登录达到一定次数后，系统将自动锁定账户。

也可设为不锁定，但将是极不安全的。

■ 之后复位账户锁定计数

管理账户锁定策略与管理密码策略大同小异，在具体的策略上单击右键，选择“安全性”,可以做具体的策略修改，如图 4-15 所示。

图 4 -15 账户锁定策略管理

4.5　组管理方案

前面我们已经多次提到了用户的权限（Permissions）和权力（Rights），这是 NTFS 文件系统较之 FAT 在安全性的优越之处：可以通过为用户分配权限和权力，限制他们使用的能力，从而保障系统的安全。

具体地说，权力（Rights）允许用户在计算机上执行一定的操作，例如备份文件和文件夹、关闭系统、安装程序等；而权限是指和对象有关的规则，Windows 2000 中对象的范围很广，凡是可以操作的目标都可以称为对象，比如文件、文件夹、打印机都可以称为对象。权限规定了一个用户能访问对象的方式，比如读取、修改、完全控制等。

做这样的设想：一个有数十至数百雇员的中等公司，为每个人建立一个账户，再为每个账户设置权力和权限，这样的内部管理的工作量是相当可观的。事实上，许多雇员应该被分配相同的权限，这相当于把同样的工作重复了许多遍。

幸运的是，Windows NT 和 Windows 2000 提供了组的管理手段，这种思维也是符合客观情况的。组的概念指的是一些具有相同属性的用户的集合。利用组的管理，可以为管理员省去许多重复繁琐的工作。只要为组设置了一定的权限，组中的用户就会具有这个权限。如果将新用户加入已设好的组中，那么新用户就立即能获得与组中其他成员相同的权限和平等的权力。可见，用组来管理用户有许多优越之处，除非必要，建议不要单独为某个用户设置权限，这样既浪费时间，又不利于日后的管理。

4.5.1　内置的组

安装 Windows 2000 Professional 后，系统将自动生成一些内置的组，观察这些内置的组（Built-In Groups）的划分有助于迅速了解组的概念和管理的手段。

■ 管理员组（Administrators）

管理员组的成员拥有对系统完全控制的最高权力，Administrator 就是管理员组的初始成员，Administrator 可以将别的用户加入管理员组，这样这个用户也拥有和 Administrator 同样高的权力。

Administrators 本地组是唯一的被自动授予所有内置权力和能力的组。

■ 备份操作员组（Backup Operators）

备份操作员组的成员可以备份和恢复计算机上的文件，而不受保护文件权限的限制，成员还可以登录到计算机上关闭系统。但是备份操作员组的成员不能改变系统的安全设置。

■ 高级用户（Power Users）

高级用户可以添加新的用户账户，但只能管理（修改和删除）自己设置的账户，对别的账户无能为力。

高级用户能够创建本地组，以及从自己创建的本地组中删除用户，或者从高级用户组、用户组、来宾组中删除用户。

■ 普通用户组（Users）

Users 组的成员能执行大多数的普通任务，例如执行应用程序、使用本地和网络上的打印机、关闭系统或者是锁定工作站。本组成员可以创建本地组，但同样只能修改自己创建的本地组。成员不能共享目录或者添加本地打印机。

■ 来宾组（Guests）

来宾组是为偶尔或是一次性访问的用户准备的，用户可以通过这个账户登录工作站。本组成员只有十分有限的权力，但也可以关闭系统。

■ 复制员组(Replicators)

复制员组支持目录复制功能。复制员组的唯一成员应该是登录到域控制器服务的域用户账户，不要将实际用户的账户加入到本组中。

除此之外，还有一些缺省的特殊组，如表 4-2 所示：

表 4-2 缺省的特殊组

组名	描述
EVERYONE	任何使用计算机的人员，包括本地用户和远程用户。EVERYONE 组包括了 INTERACTIVE 组和 NETWORK 组
INTERACTIVE	EVERYONE 组的子集，包括任何在本机登录的用户
NETWORK	也是 EVERYONE 组的子集，包括任何通过网络登录的用户
CREATOR OWNER	任一系统资源（包括文件，文件夹，打印机等）的建立者，或者是所有者

这些组一般并不出现在组列表中，但在查阅文件或文件夹属性时，在拥有权力的组与用户列表中，可以看见它们的名字。以上是一些本地用户组的实例。如果计算机加入了一个域，那么还会碰到其他的一些全局组，比如内置的 Domain Admins 组、Domain Guests 组、Domain Users 组以及管理员建立的其他一些全局组。

提示：全局组包括从域中其他部分访问你的计算机的用户，只能在一个运行 Windows 2000 Server 或者是 Windows NT Server 4.0 的系统上建立。

4.5.2 创建组

创建新的组同创建新用户大同小异。展开本地用户和组并选择“组”，单击右键，选择“新建”中的“组”，如图 4-16 所示。接下来，在图 4-17 所示的创建组对话框中，输入新组的信息即可。

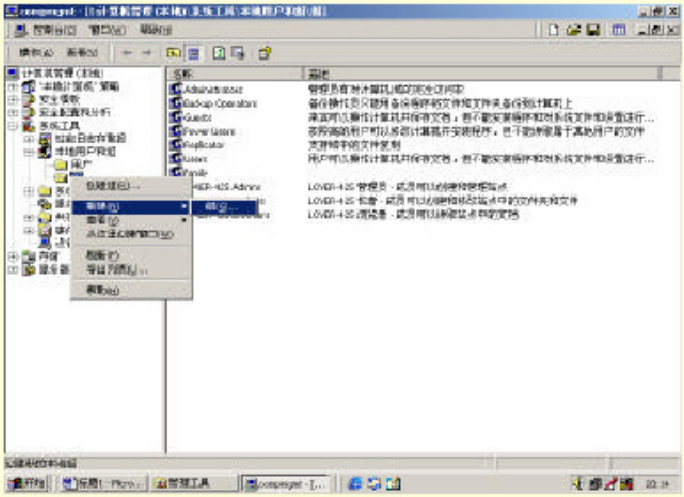


图 4-16 创建新组

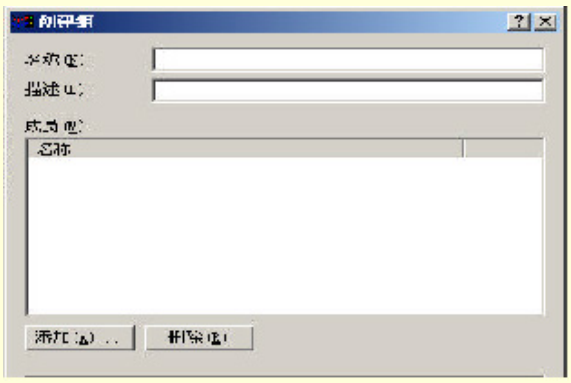


图 4-17 创建新组对话框

例如，要创建一个名为“ family ”的组，只需往“ 名称 ”栏里输入“ family ”，“ 描述 ”栏是可省的。

注意：组名和用户名都不能包括以下字符：” / \ [ ] : ; | = + ? < >

如图 4-18 所示，新加入的 family 组出现在组列表中。

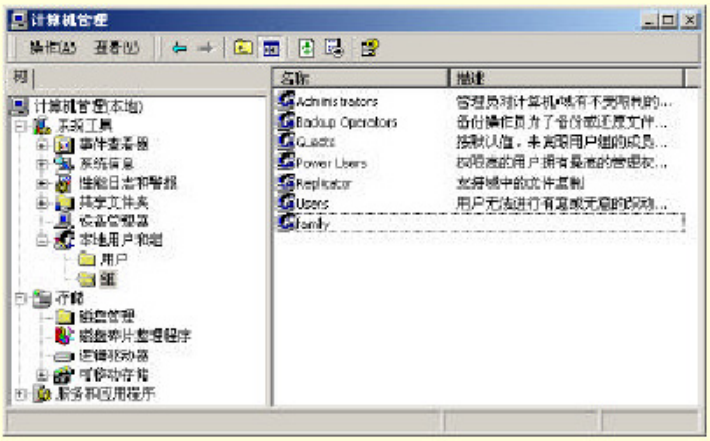


图 4-18　新创建的 family 组

然而，过多的组也容易产生干扰和混淆，由于系统已经建立了一些内置的组，建议尽可能地利用已有的组。

4.5.3　在组中添加成员

如果是新创建的组，则可直接在图 4-17 所示的创建新组对话框中，单击“ 添加 ”，就可以从用户列表中选择用户加入自己新建的组中。

如果是已建的组，也可以右击选中的组，从上下文菜单中选择“ 添加到组 ”，如图 4-19 所示，剩下步骤同上。

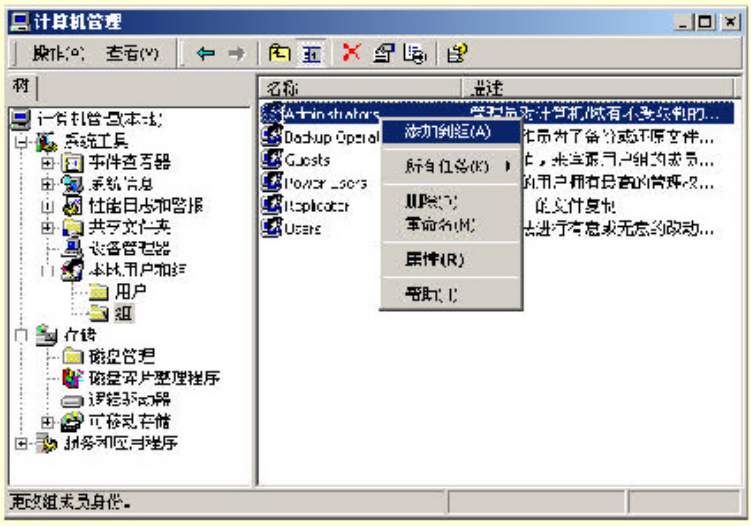


图 4-19　成员添加到组

再来看看前面的例子。假设 Richard 曾是市场部的主管，并有自己的账户，现在 Richard 离职了，那么当然要禁用他的账户，但对于 Richard 的接替者，管理员还得依样画葫芦地为他重新设置权力和权限，这是相当不便的。组的管理提供了更好的办法：建立一个叫 Marketing Supervisors 的组，为它分配合适的权力和权限，那么管理员所要做的工作只要把 Richard 的接替者放入 Marketing Supervisors 组就行了。

管理员和普通用户都可以管理组，但管理的范围有很大区别。很显然，管理员对系统有完全控制权，因此管理员可以将任意用户添加到任意组中，比如说，将普通用户 Jack 添加到 Power User 组中甚至是 Administrators 组中，这样 Jack 就将具有高级用户或是管理员的权力。事实上，这种管理方法方便快捷，也是常用的方法。

普通用户就不同了，仅可以管理自己创建的组，也就是说只能把别的用户加入到自己创建的组中去，而对别人创建的组和内置的组就无能为力了。这个道理十分明显，如果普通用户就可以把自己加入到管理员组中，那后果将是无法想象的。

不知读者有没有想过这个问题：如果普通用户将 Administrator 加入到自己创建的受限制的组中，Administrator 的权力是否会降低呢？答案是不会。同一用户可以隶属于多个组，这时候这个用户拥有所有这些组中最高级的权力。例如某一用户既是 Backup Operators 组又是 Power Users 组的成员，那么他同时拥有这两个组的所有权力。所以，即使加入了普通用户组，也不影响 Administrator 的权力。

4.5.4 从组中删除成员

从组中删除成员有两种方法：从用户角度删除其隶属的组，或者从组的角度删除其内部成员。打开“本地用户和组”并展开用户列表，选择某一具体用户后，单击右键，选择属性对话框中的“成员身份”选项卡，从所属组的列表中选择希望不隶属的组，单击“删除”即可，如图 4-20 所示。

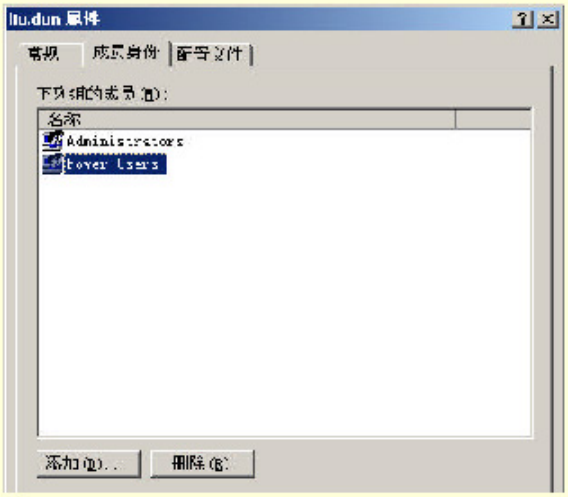


图 4-20 删除组的成员

从组的角度删除成员的思维是一样的。首先打开“本地用户和组”并展开组列表，右键选定的组，打开属性对话框，从组成员列表中选择要删除的成员，单击“删除”即可。

4.5.5 组的删除

组的删除与用户的删除基本一样。需要注意的是：每一个组都有自己的 SID 号，删除掉的组将无法恢复，即使重新建立了一个同名的组，也必须重新设立权限。

内置的组，如 Administrators 组，Users 组是不能删除的。

删除组并不会删除组内成员的账户，只有当删除用户账户时才会把具体的成员删除。

第 5 章　文件及系统权限管理

对系统内部文件及文件夹的权限管理完全是出于安全的考虑。本书反复提到了“安全”这一字眼，后面还有专门的一章讲述系统安全性的问题。提到安全，总有人感到不方便，一些对安全性要求很低甚至从不考虑安全问题的个人用户也会有受限制的感觉。但事实上，随着网络在全球的普及，因特网、广域网、局域网与计算机用户已经密不可分，我们完全可以足不出户地了解世界动态，参加各种有趣的活动，或是方便快捷地获取急需的资料并且要求与别人共享有用的资源，但由此而来的一个重要问题就是如何保护自己系统的安全。

我们前面已经讲过建立和组织用户及其账号的问题，如果将系统比喻成一个大家庭，那么管理员和普通用户的关系就好比是家长和孩子的关系。家长、孩子和客人的角色已经确立，但是电脑并没有学过家庭伦理学，因此还得完成剩下的工作：为他们分配权力和权限。

家长当然应该对家庭享有完全控制的权力；孩子们就必须受点限制了，他们可以读书、看电视，但不应该能做到更改家里的下一项支出计划，而且保险柜也应该对他们拒绝访问。至于一般的客人，他们能对家庭的影响就更有限了。当然，他们可以共享女主人精心准备的一桌可口饭菜！

这个例子也许不十分恰当，但大致表达了权力和权限的意义。Windows 2000 的文件系统的一大特色就是可以实施文件级的权限安全。

本章内容包括：

- FAT 和 NTFS 安全性比较
- 单独的权限
- 标准目录和文件权限
- 权限管理
- 审核规则

5.1　FAT 和 NTFS 安全性比较

文件包含的范围很广，比如各种源程序和目标程序、设备表、报表、目录、系统程序等等，只要是一个数据的集合，经过命名后都可以称之为文件。系统内部有数量庞大的文件，而文件系统就是负责存取和管理这些文件信息的组织。

一个良好的文件系统应当具备的功能有：用户能方便地建立、修改和删除文件；能在文件间进行数据传输；用户之间能共享彼此之间的成果；并提供可靠的保护和保密措施。总之，文件系统既要提供用户的私人信息访问，也要负责为用户提供以有控制的方式访问共享的信息。

在 Windows 2000 和 Windows NT 4.0 中，支持的文件系统主要有 FAT 和 NTFS，以及 CDFS（Windows 2000 还支持 FAT32）。过去在 Windows NT 3.5X 中，磁盘文件系统可以选择 OS/2 的 HPFS（High Performance File System），但它已不再被 NT4.0 支持。下面将主要针对 FAT 和 NTFS 两种系统的安全性进行比较。FAT32 可以认为是 FAT 的升级版，它用更小的簇来存储文件，但从安全性的角度来说，二者没有什么区别；而 CDFS 是光盘存储文件的文件系统，这里不予以讨论。

FAT（File Allocation Table，文件分配表）是旧式的文件系统，被 MS-DOS、Windows 3.x、Windows 95/98、Windows NT 以及 OS/2、Macintosh 等多种操作系统所支持。Windows 2000 也支持 FAT 文件系统。

NTFS（New Technology File System）的使用范围则相对要有限得多，只有 NT 支持这种格式的文件。Windows 2000 已对 NTFS 的性能做了更大的改善。

提示：Windows 2000 是基于 NT 的内核构造的，其最初的名称是 Windows NT 5.0，因此完全有理由认为 Windows 2000 是 NT 的新生代产品而不是 Windows 9X 系列产品的后续。本书将 NT 与其他产品作整体比较时，包括 Windows 2000。

不错，NTFS 的兼容性不如 FAT，但不要因此认为 FAT 比 NTFS 更先进，二者后面还要做更具体的比较，这里我们先讨论它们在文件共享和权限设置上的表现。

5.1.1 FAT 的不足

FAT 分区可以设置为资源共享，从安全性考虑，可以通过设置组策略来保护内部文件，但这种策略是十分粗糙的，由于不能设置文件级的权限，共享权限是唯一可以限制用户访问该目录和它里面文件的方法。也就是说，对整个目录，FAT 或者拒绝所有访问，或者干脆完全敞开大门。这种策略是不能令人满意的。

同时还要注意：在 FAT 卷上，共享权限只能对通过网络访问文件的用户起限制作用，对本地用户就无能为力了。

由此可见，FAT 文件系统有许多不足之处。

5.1.2 NTFS 的安全性

NTFS 的高可靠性使其成为要求高度安全的系统的最佳选择。

NTFS 首先要求用户验证，并在访问文件前得到指定的具体访问权限。NTFS 存储了 NTFS 分区上的各个文件信息并管理一个访问控制列表（ACL，Access Control List），将这些权限信息与存储在本地计算机或者是域中的账户数据库上的账户信息相联系，从而有效地维护文件的安全。

在具体权限的安排上，NTFS 也显得功能强大而灵活多样。在 NTFS 卷上，不但可以对文件夹设置目录权限，与 FAT 相比，一个明显的优势还在于它能够设置文件级的权限。比如给 Everyone 某个目录完全控制权限，再建立另外一个组，对目录下的具体文件为部分用户分配不同的权限。NTFS 能给目录和文件安排相当精细的权限，而不像 FAT 只有简单地共享与不共享。由于权限和账户有着紧密的联系，因此可以把权限赋予单个用户或者是用户组，FAT 在这点上也是无能为力的。

NTFS 卷在安全性上的特殊之处还在于它可以进行文件级的加密，这在 FAT 卷上也无法做到。

提示：如果选择了对敏感文件进行加密，那么你不能对它进行压缩；此外，系统文件不能被加密。

NTFS 的权限设置不单对网络用户有效，同样也对本地用户实施管理，即使外人在计算机前，也做不了一些不被授权的事。

由于 NT 的不兼容性，NTFS 对非法物理访问的抵抗能力也更强。用户不能从 MS-DOS 上启动而访问 NTFS 磁盘，因为 NTFS 文件系统驱动程序只允许 NT 访问 NTFS 磁盘。正是由于以上的种种原因，NTFS 在安全性能上全面超越了 FAT，因此 NT 组网的安全性超过了其他 Microsoft 网络操作系统。

下面对用户权限的设置进行详细介绍。

5.2 单独的权限

在 Windows NT 4.0 中，NTFS 文件系统支持 6 种单独的权限，分别是读取、写入、运行、删除、更改权限和取得所有权。Windows 2000 大大扩充了这些单独的权限（也可以称为专门权限，即 Special Permissions），使得权限的分配更加细致合理。单独的权限即可以用于目录下，也可以用于文件下；即可以单独使用，也可以将它们组合起来使用。下面是对单独权限的具体说明。

■ 遍历文件夹/执行文件 （Traverse Folder/ Execute File）

遍历文件夹适用于文件夹的权限，允许用户移动到另一个文件夹中，并查看里面的文件，即使用户并没有目标文件夹的权限。只有当用户或组在组策略管理单元中没被授予 Bypass traverse checking 时，遍历文件夹才有意义。Everyone 组缺省有 Bypass traverse checking 权力。

需要注意：将用户对某个文件夹的权限设为遍历文件夹，该文件夹下的文件并不会自动成为可执行的。

■ 列出文件夹/读取数据 （List Folder/ Read Data）

列出文件夹只适用于文件夹权限，允许用户浏览文件夹下的文件名和子文件夹。
读取数据只适用于文件权限，允许用户查看文件数据。

■ 读属性（Read Attributes）

本权限允许读文件夹或是文件的属性，比如只读或隐藏的属性。属性是在 NTFS 里定义的。

■ 读扩展属性（Read Extended Attributes）

本权限允许读文件夹或是文件的扩展属性，扩展属性是被程序定义的，并有可能随程序而变动。

■ 创建文件/写入（Create Files/Write Data）

创建文件适用于文件夹，允许在该文件夹内创建文件。
写入适用于文件，允许更改文件并且覆盖现有文件。

■ 创建子文件夹/添加（Create Folders/Append Data）

创建子文件适用于文件夹，允许在该文件夹内创建子文件夹。
添加适用于文件权限，允许在文件末尾写入新的数据，但不能更改，删除或者是覆盖现有数据。

■ 写属性（Write Attributes）

写属性允许更改文件或者文件夹的属性，比如只读，隐藏等属性。

■ 写扩展属性（Write Extended Attributes）

写扩展属性允许更改文件或者文件夹的扩展属性。

■ 删除子文件夹和文件（Delete Subfolders and Files）

删除子文件夹和文件权限允许用户删除子文件夹和文件，即使该用户在此子文件夹和文件上并没有删除的权限。

■ 删除（Delete）

允许用户删除文件夹或者文件。

注意：如果用户并没有本权限，但在该文件夹或文件的上级文件夹拥有删除子文件夹和文件的权限，那么此用户同样有删除的权力。

■ 读权限（Read Permissions）

读权限允许用户读取文件或者文件夹的权限设置，比如完全控制、读取、写入等。

■ 更改权限（Change Permissions）

更改权限允许用户更改文件或者文件夹的权限设置，比如完全控制、读取、写入等。

■ 取得所有权（Take Ownership）

取得所有权允许用户取得文件夹或者文件的所有权。

所有权在 NTFS 的权限中是一个很重要的概念，取得所有权意味着可以对这个文件夹或者文件进行完全的控制，并更改其权限，而无视现存的对这个文件夹或者文件进行保护的权限。

■ 同步（Synchronize）

本权限只适用于多线程和多处理器的任务，允许不同的线程等待句柄并与之通信的线程保持同步。
当标准的目录权限和文件权限尚不满足工作需要时，可以单独分配这些特殊权限。

5.3　标准目录和文件权限

一般地说，系统已预先分配好了两组分别针对目录和文件的权限，管理员可以参照这些设置为不同用户分配权限。

5.3.1　标准文件权限

标准文件权限包括完全控制（Full Control）、修改（Modify）、读取和执行（Read&Execute），读取（Read）、和写入（Write）。每个权限都由一组特殊的权限组成，表 5-1 是具体的权限与相关联的特殊权限关系列表。

表 5-1 标准文件权限说明

特殊的权限	完全控制	修改	读取和执行	读取	写入
执行文件	X	X	X		
读取数据	X	X	X	X	
读属性	X	X	X	X	
读扩展属性	X	X	X	X	
写入	X	X			X
添加	X	X			X
写属性	X	X			X
写扩展属性	X	X			X
删除子文件夹和文件	X				
删除	X	X			
读权限	X	X	X	X	X
更改权限	X				
取得所有权	X				
同步	X	X	X	X	X

表注：X 表示该选项具有该权限。

读者可以发现，读取和写入所包含的权限都相当有限，仅能读取数据或者是添加数据，读取和执行比读取稍好一点，多了执行的权限（如果该文件是可执行文件的话），但仍然无法删除。修改相对来说权力就很大了，既能读数据又能往里写入，还有删除文件的权力。完全控制是最强有力的权限，除了具有修改权限所有的一切权限外，完全控制还包括更改现有的权限，以及取得所有权。

更改权限意味着可以管理不同用户对文件的权限，放宽对用户的限制，或者收回部分甚至全部权限以限制用户对文件的访问。系统管理员如果被某个文件拒绝访问（注意：管理员并非自动地获得所有资源的访问权），可以通过取得所有权实现对该文件的完全控制。管理员和创建者（Create Owner）可以享有完全控制的权限。

提示：如果对该文件所在的文件夹拥有完全控制的权限，那么对这个文件夹下的所有文件（当然包括此文件），即使访问权限是有限的，例如只有读取和写入的权限，仍可以删除它。

5.3.2 标准文件夹权限

标准文件夹权限包括完全控制（Full Control）、修改（Modify）、列出文件夹目录（List Folder Contents）、读取和执行（Read&Execute）、读取（Read）和写入（Write）。每个权限都由一组特殊的权限组成，表 5-2 列出了具体的权限与相关联的特殊权限关系。

表 5-2 标准文件夹权限说明

特殊的权限	完全控制	修改	读取和执行	列出文件夹目录	读取	写入
遍历文件夹/执行文件	X	X	X	X		
列出文件夹	X	X	X	X	X	
读属性	X	X	X	X	X	
读扩展属性	X	X	X	X	X	

创建文件	X	X				X
添加	X	X				X
写属性	X	X				X
写扩展属性	X	X				X
删除子文件夹和文件	X					
删除	X	X				
读权限	X	X	X	X	X	X
更改权限	X					
取得所有权	X					
同步	X	X	X	X	X	X

读者可以发现，与文件标准权限相类似，读取和写入所包含的权限都相当有限，仅能列出文件夹，读属性（相当是读取数据）或者是创建文件，写属性（相当于添加数据）；读取和执行比读取稍好一点，多了遍历文件夹的权限，但仍然无法删除。

读者或许已经发现，读取和执行与列出文件夹目录所包含的特殊权限是一致的，但它们继承的是不同的权限。列出文件夹目录适用于文件夹，只有在查看文件夹属性时才会出现；读取和执行则继承了文件和文件夹两种权限，适用于文件夹和文件的属性。如果将用户对某一文件夹设为享有读取和执行与列出文件夹目录权限，那么对此文件夹下的文件，缺省有读取和执行的权限；对此文件夹下的子文件夹，缺省有读取、执行和列出文件夹目录的权限。但如果对此文件夹只有列出文件夹目录权限而没有读取和执行的权限，那么对此文件夹下的文件，缺省也没有读取和执行的权限。

修改的权力就很大了，既能读数据又能往里写入，还有删除文件的权力。完全控制是最强有力的权限，除了具有修改权限所有的一切权限外，完全控制还包括更改现有的权限，以及取得所有权。

需要注意的是：这两套文件和目录权限并不是相互独立的，从前面的例子就可以看出，它们之间有一定的联系。由于文件总是组织在文件夹中的，因此弄清楚它们之间的关系非常重要，下面就来了解一些权限设置的常识。

5.3.3　所有权概念

所有权是一个十分重要的权限概念，用 CREATE OWNER 代表资源的所有者。这里说的资源包含的范围很广，文件夹和文件都是资源的一部分。一般说来，所有者就是资源对象的建立者，所有者对资源对象有完全控制的权力。

资源的所有者完全可以通过配置自己的私人目录，严格控制其他用户对本资源的访问，甚至对管理员也可以拒绝访问，这意味着管理员并不能自动地获得所有资源的完全控制权。

此外，所有者可以给其他用户分配权限，甚至使其他用户享有取得所有权（TAKE OWNERSHIP）的权限。被授予这个权限的用户也随时可以取得所有权，接管资源。

5.3.4　管理员对策

虽然资源的所有者可以设置对管理员拒绝访问，但管理员却有通向“后门”的钥匙。由于统管理员拥有对系统的完全控制的能力，因此管理员总可以设法获得文件夹或者文件的所有权。这点对系统的管理是十分重要的。比如某个用户离开了原来的系统，而在此之前他的个人信息拒绝他人访问，这时候管理员可以通过取得所有权来重新管理资源对象，并分配给别人使用。

管理员不应该滥用这个特权，任意地取得所有权给普通用户以“侵吞”的不安全之感，更重要的是，取得所有权后无法交还给原来的所有者，也无法将所有权转移给其他用户。因此除非在十分必要的情况下，不要轻易地“取得所有权”。此外，如果用户发现丢失了所有权，可以通过查看权限了解谁接管了所有权。

建议：我们已经发现管理员身份享有太多的特权，但这也许不完全是一件好事。如果系统管理员也经常需要使用机器，应该为自己设立另外一个普通用户的账号，在平时用普通用户的账号登录，只有当需要进行系统管理时，才以管理员身份登录。这样在普通登录时，可以避免一些不小心犯下的错误，也可以提高自己管理员的责任心。特别是初学者，要小心自己的鼠标和键盘。

5.3.5 权限的累加及拒绝

用户权限是可以累加的。由于通常采用组的管理手段，当某一用户分属不同的组，而这些组又被赋予了不同的权限时，这个用户的权限将被累加，也就是说，用户的权力将得到增加，但拒绝访问除外。

前面说过的权限有大有小，但毕竟用户都还可以一定程度地访问文件或者是文件夹。如果没有对某个用户设置访问权限，他可能无法访问文件或者文件夹（这取决与该用户是否在其他组获得权限），要注意不给用户分配权限与设置拒绝访问是不一样的。

如果特意要拒绝用户的某种访问，请注意拒绝权限可以覆盖其他权限，这是因为拒绝比允许的优先级更高，这也是权限累加的一个特例。也就是说：如果用户或者是用户所属的组有某项权限被拒绝，那么即使另外的组赋予了该用户这个权限，他也不能获得访问权。拒绝访问比同时赋予的完全控制还要强大。

注意：况并没有完全堵死，用户有可能通过别的组或者是父系等别的途径不给用户设置某个权限和拒绝用户某个权限是不一样的。前者的情获得权限；但是在后者的情况下，用户被明确拒绝了这个权限，别的途径都失去了意义。

5.4 权限的设置

5.4.1 标准权限设置

现在开始具体的权限设置。针对某个文件或文件夹设置权限的步骤是：

（1）打开资源管理器或者“我的电脑”。

（2）找到相关的设置对象，在对象上单击鼠标右键，选择弹出菜单中的“属性”命令。

（3）选择“安全”选项卡，这时可以看见被分配的用户权限列表，如图 5-1 所示。

图 5-1 用户权限列表

（4）图 5-1 列出的是文件夹的标准权限，如果要改变现有用户或组的权限，只需要直接在权限列表复选框上选择即可。注意图中“ 允许 ”一栏的复选框是灰色的，表示这个文件夹的权限是从其父系继承过来的，不能直接改动。此时可以回到父文件夹中变动；或者不允许继承父系权限（将“ 允许将来自父系的可继承权限传播给该对象 ”复选框清除），关于父系权　　限的继承后面有具体分析。

（5）如果要增添对对象拥有访问权的用户，单击“ 添加 ”按钮，出现如图 5-2 所示的选择用户、计算机或组对话框。

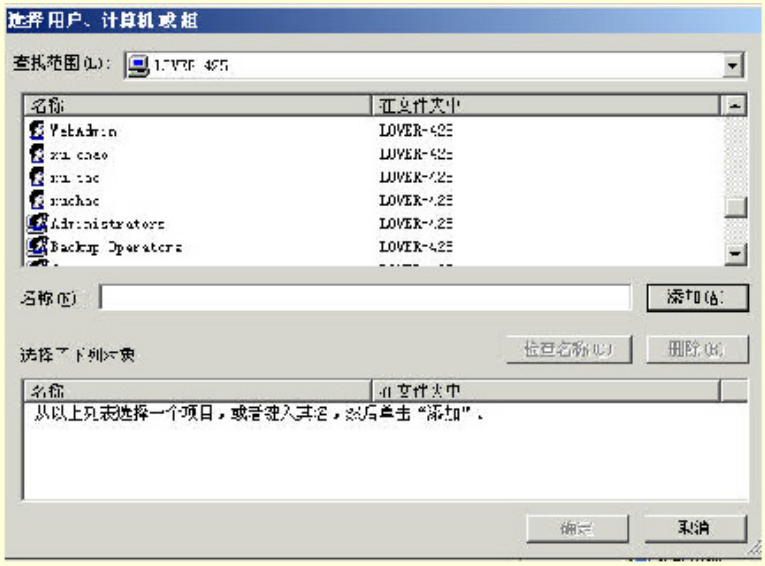


图 5-2　选择新用户、计算机或组

例如选择了一个新组 Group1，此时组 Group1 就出现在用户列表中，缺省为组 Group1 分配的权限有“ 读取及运行 ”、“ 列出文件夹目录 ”和“ 读取 ”，即用户有读取和运行此目录下文件的权限，如图 5-3 所示。与前面稍有不同的是，这里 Group1 的权限列表不是灰色的，可以直接做改动，这是因为 Group1 在这个文件夹的权限不是通过父系继承而来的。

图 5-3　添加的“ Group1 ”

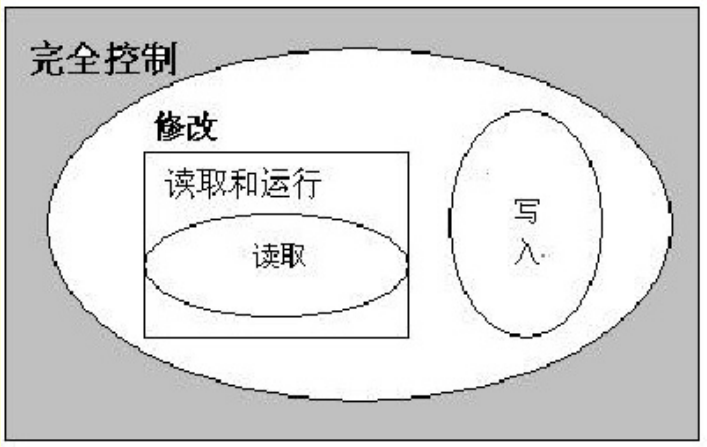
（6）如果要去掉某个用户或者组的权限，在用户列表中选定此用户或组，单击“ 删除 ”按钮即可。

注意：这里删除按钮不是指删除用户的某些权限，而是删除用户，删除之后此用户就没有被指定权限。删除时没有警告信息，所以要小心。

另外，只有这个文件夹/文件的所有者，或者被所有者分配了足够的权限（“ 更改权限 ”或是“ 取得所有权 ”），才能更改其他用户的权限。如果这两个条件都不具备，就无法更改其他用户的权限。

上面说的是文件夹的权限设置，文件的权限设置与此类似。首先从资源管理器或“我的电脑”中定位文件，然后单击鼠标右键并选择“属性”中的“安全性”，就可以对用户权限进行设置。

关于标准权限用户需要注意：它们之间不是互相独立的，从第三节所列的关系列表中可以得出结论：它们之间有包容的关系，大致关系示意图如下：



因此，假如用户被分配了读取和写入的权限，那么该用户自动拥有了读取的权限；如果分配了修改的权限，那么自动拥有读取和运行、读取以及写入的权限；如果分配了完全控制的权限，那么在图 5-3 中，从修改到写入的复选框会自动全部作上标志，表示用户拥有所有的这些权限。

同样的道理，如果现在要拒绝用户的访问并且选中了“拒绝”一栏的“完全控制”时，底下从修改到写入的复选框也会自动全部作上标志，表示此用户被拒绝了所有权限。

5.4.2 单独权限设置

在 5.3 节中已经提过：权限包括标准权限和特殊权限。上面介绍的标准权限是系统预定义的一组权限，包括读取、写入、修改、完全控制等，而每一种标准权限都是由更细的几条特殊权限组成的。例如读取，就是由列出文件夹/读取数据、读属性、读扩展属性、读权限这几条特殊权限组成的，所以特殊权限是最小的权限组成单位，也可以称之为单独权限。

前面所讲的权限设置指的都是一般的标准权限设置，标准权限设置出现在权限列表中。如果这些标准权限设置不能满足要求时，就需要进一步设置单独权限。

设置单独权限时，在图 5-3 中，单击“高级”按钮，出现如图 5-4 所示的访问设置控制台。

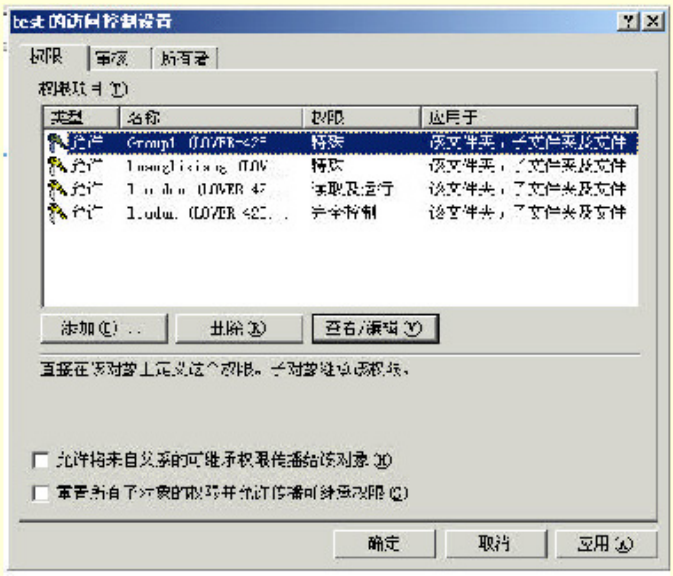


图 5-4 访问设置控制台

在此访问控制台中，“添加”和“删除”两个按钮的作用与前面是一样的，仍然可以通过单击它们来增加

或者删除具有权限的用户。

单击“查看/编辑”按钮，将出现如图 5-5 所示的权限项目框。图中列出了详细的单独权限情况，可以更加具体地设置允许或者拒绝的单独权限。

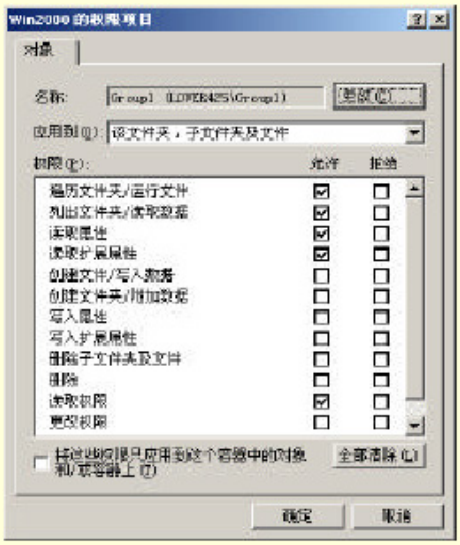


图 5-5　权限项目框

例如，想给某一用户读取和写入的权限，可以在图 5-1 所示的用户权限列表中给该用户分配读取的标准权限，然后单击“高级”按钮，再单击“查看/编辑”，在如图 5-5 的权限项目框中，给用户分配创建文件/写入数据、创建文件夹/附加数据、写入属性、写入扩展属性 4 种权限，这样用户就将拥有读取和写入的双重权限。

另外一种方法是：给用户分配修改的标准权限，修改权限既包括了读取也包括了写入的标准权限，但修改权限还包括了删除的单独权限，这是不希望出现的。可以在权限项目中单独拒绝用户删除的权限。

单击对象一行末尾的“更改 …”按钮，出现类似图 5-2 所示的添加新用户或组对话框，可以选择新的用户或组，来更改拥有修改后权限的用户对象。

在图 5-5 所示的单独权限列表中做了具体设置后，下次查看该文件或文件夹的安全性时，将出现提示信息，提示有额外的单独权限存在，由于属性框中只列出了标准的权限，因此必须按“高级 …”按钮，才能查看到详细的权限信息。

按“高级”按钮，可以看到在访问控制设置台中，用户的权限用“特殊”来概括，而不是用标准权限来描述了，这表明此用户拥有的是经特殊组合而成的权限，如图 5-6 所示。

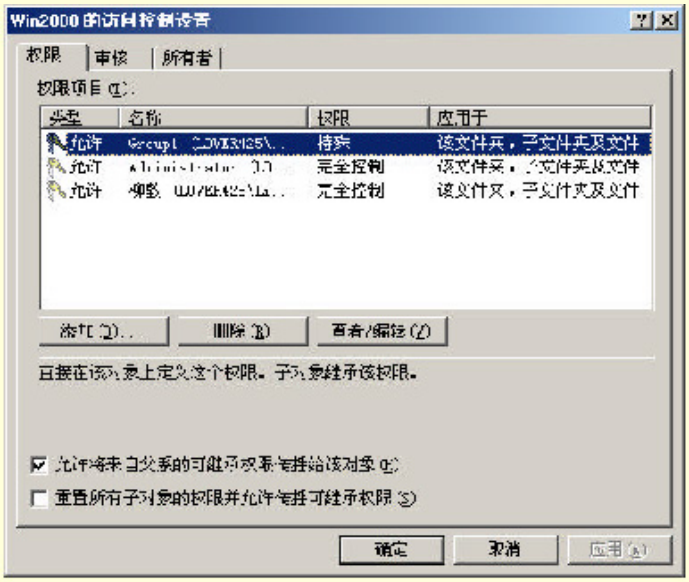


图 5-6　显示用户有特殊组合而成的权限

5.4.3 通过组分配权限

用组来组织用户几乎总是比单独地管理用户来得更简洁也更清楚，权限设置时也不例外，仍然推荐读者采用组的手段去分配权限。

一个用户可能存在不同的组中，如果给这些不同的组分配了不同的权限，那么这个用户的实际权限将得到累加。假如用户 Mike 被分配了删除的权限，Mike 属于服务部，而服务部被分配了写入的权限，与此同时，Everyone 组有读取的权限，由于 Mike 也是 Everyone 组的，所以 Mike 实际拥有的权限相当于删除+读取+写入，也就相当于拥有修改的权限。这是符合逻辑的，一个人同时属于不同的组，说明他能扮演不同的角色，起多方面的作用，那么他相应地也就应该有更多的权限。

5.4.4 小心使用拒绝

权限的累加只适用于“允许访问”的权限。要注意的是：权限设置里还有专门的“拒绝”一栏。任何时候都要牢记：拒绝的优先级比允许的优先级更高，这就像四则运算中，乘除的优先级比加减的优先级高一样。如果 Mike 被分配了删除的权限，Mike 属于服务部，而服务部被拒绝了删除的权限；或者 Mike 被拒绝了删除的权限，而服务部享有删除的权限，结果对 Mike 是一样的，他被拒绝了删除的权限。

一般说来，可以采取折衷的办法，当不能确定是否要给某个用户一个权限时，可以在允许和拒绝两栏中都不做标志，这样用户如果在别的组中被分配有这个权限，或者是在父系中拥有可以覆盖的权限，那么此用户实际上拥有这个权限。

前面介绍了通过组获得新的权限的例子。另外一种情况是：用户在名为 TEST 的文件夹有读取和执行、读取和写入的权限；在 TEST 根目录下有一个记事本文件，用户有读取的权限而没有写入的权限，但此用户并没有被明确拒绝写入，此时由于用户对目录 TEST 有写入的权限，所以他照旧可以打开这个记事本文件并往里添加内容。这就是一个通过父系“曲线”获得权限的例子。

提示：通过父系获得权限有一个前提，那就是要求允许将父系的权限继承给底下的子对象。在这个例子中，记事本文件应该能继承 TEST 目录的权限。

但是，如果在拒绝一栏里明确注明了拒绝用户某种权限，那么无论通过组还是通过父系，都再没有办法获得这个权限。如果你不怀疑某个用户的动机，请慎用拒绝。

如果设置的拒绝权限与允许权限出现了矛盾，系统会发出警告信息。如图 5-7 所示。

图 5-7 设置拒绝的警告信息

5.4.5 继承权限

正如孩子可以继承父辈的财产，权限也是可以从上层继承的。

例如在 TEST 目录中，用户甲有读取、读取及运行和列出文件夹目录的权限，用户乙有完全控制的权限，用户丙有用户甲的全部权限，还有删除的单独权限。在 TEST 下新建一个 TEST1 子目录和一个记事本文件，并且都允许继承 TEST 的权限。此时在 TEST1 子目录中，甲、乙、丙仍有与 TEST 下相同的权限。在记事本文件中，甲的权限为读取和读取及运行；乙可以完全控制；丙有读取和读取及运行的标准权限，还有删除的单独权限。这时无论是 TEST1 子目录，或是记事本文件，权限列表中的复选框都是灰色的，表示这些权限是从 TEST 父目录下继承而来的，无法在子目录或者根目录下文件中直接删除。

用户从父文件夹继承的权限无法删除，这就好比不能剥夺孩子从父母继承的财产，除非能够证明这笔财产首先不应该属于孩子的父母。也就是说，修改应该从父文件夹开始，如果这个父文件夹的权限还是继承而来的，只能回到更上一层。此外，也不能删除用户列表中的用户，尽管删除按钮没有变灰，但系统会给出错误信息，如图 5-8 所示。

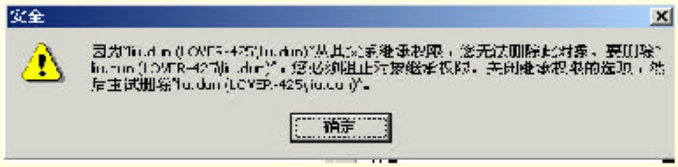


图 5-8　无法删除继承父系权限的用户

但是可以增加享有权限的用户（按“ 添加 …”按钮，仿前面的操作），如果现有用户没达到完全控制的权限，也可以增加他们的权限，包括标准权限和单独权限。对象权限中如果既有从父系继承过来的权限，又有自己明确定义的权限，那么在高级访问控制设置台中，这两种权限会分别列开，它们的标志是不一样的：前者用一个灰色的钥匙表示权限是继承而来的，后者的钥匙标志则没有灰色。同一用户可能被两次列出，因为他既有继承而来的权限，又有被明确定义的权限。

继承权限的优点是创建者和管理员都可以比较方便地组织和管理资源。新建的文件夹和文件都默认是继承父系权限的。如果要设置某些资源从其父系中继承权限，那么用前面的方法找到此文件或文件夹的“ 属性 ”中的“ 安全 ”，选中底部的“ 允许将来自父系的可继承权限传播给该对象 ”复选框即可，如图 5-9 所示。

图 5-9　继承父系权限

一般说来，子对象总是继承父系的权限。有时如果觉得用户的某项权限不妥，但这项权限是从父系继承过来的，你无法直接改动，因此只有回到上一级去做修改。这时你有几种办法可以选择。

第一种情况，由于需要，你在父系文件夹中，为某个用户或组增加了特殊权限（单独权限），但如果只希望在子对象中用户继承父系设置的标准权限，这时候应该阻止用户继承额外设置的特殊权限，也就是说：特殊权限应该只适用于父系文件夹。任何时候都应该保持清醒的头脑，正确地分析问题有助于迅速地找到对策。现在首先打开特殊权限的设置台。

（1）在父系对象上单击右键，选择“ 属性 ”，“ 安全性 ”标签。

（2）在用户权限列表中，设置好用户的标准权限，这是在子对象中可以继承的。

（3）选择要添加特殊权限的用户，单击“ 高级 …”，出现如图 5-6 所示的访问控制设置，单击“ 查看/编辑 ”。

（4）在图 5-10 所示的特殊权限列表中，为用户添加特殊权限，比如“ 取得所有权 ”。

（5）单击“ 应用到 ”下拉列表（缺省是“ 应用到该文件夹，子文件夹及文件 ”），选择“ 只有该文件夹 ”，单击“ 确定 ”。

这样一来，用户在子对象中继承的就只有标准权限，不能继承“ 取得所有权 ”的特殊权限。

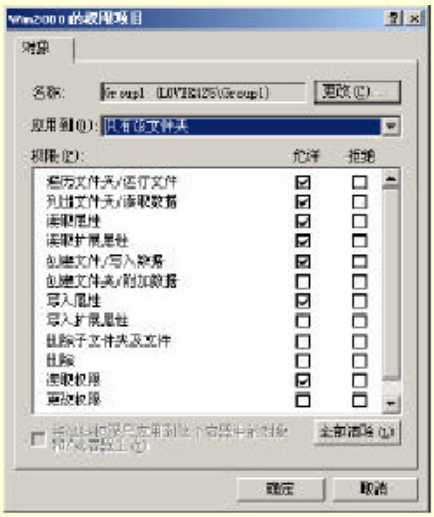


图 5-10 将特殊权限只应用到当前的父文件夹

第二种情况，假如不希望改变父系的权限设置，又希望重新定义用户在子对象中某几个特殊文件或者文件夹的权限。这时候怎么办呢？因为继承权限并非总是完美的，也许你应该考虑禁止用户从父系继承权限。

阻止用户从父系继承权限的办法很简单：只需要从文件或文件夹属性的安全性框的底部清除“允许将来自父系的可继承权限传播给该对象”复选框即可。这时会出现一个提示框，征求你的意见，如图 5-11 所示。这时可以有下面不同的对策。

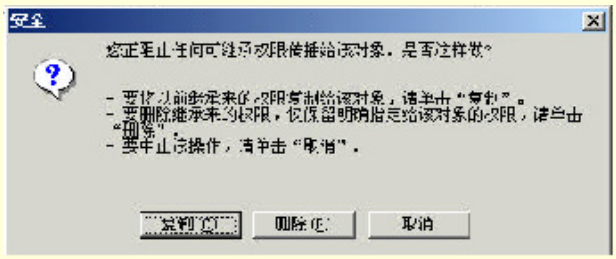


图 5-11 阻止继承父系权限

（1）如果你觉得麻烦而且危险，还拿不定主意，请单击“取消”按钮，谨慎总是更有利于系统的稳定。

（2）要将以前继承来的权限复制给该对象，请单击“复制”按钮。还拿不定主意时，也可以用这个办法。复制后，用户的权限与过去完全一样，但是现在的权限列表框中不再是灰色的，也就是说现在可以把用户的部分权限去掉，或者将这个用户删除。此后，这个对象不再从父系继承权限，父文件夹做的任何变动都不再影响这个子对象。

（3）要删除继承来的权限，仅保留明确指定给该对象的权限，请单击“删除”按钮，之后，凡是继承过来的权限都将被删除，也就是灰色框里的权限都将被删除。只有那些额外添加的权限和用户才会保留。注意：如果没有任何额外添加的权限和用户，那么删除后将没有用户在对此对象中享有权限，这时系统会出现警告信息，如图 5-12 所示。这时所有者应该重新为用户（也许包括自己）分配权限。

图 5-12 删除后可能出现无人能访问的情况

还有一种比较极端的选择：通过分配相反的允许/拒绝权限来覆盖继承而来的权限。

与此正好相反的情况是：如果觉得当前对象的子对象权限定义没有条理，可能会要求子对象继承当前对象

的权限。这时要做的是：

（1）选择好当前对象（应该是文件夹），在对象上单击鼠标右键，选择弹出菜单中的“属性”命令，然后选择“安全”选项卡。

（2）在被分配的用户权限列表中单击“高级...”按钮，出现如图 5-13 所示的高级访问控制设置。在此设置台底部，选中“重置所有子对象的权限并允许传播可继承权限”，然后单击“确定”按钮。

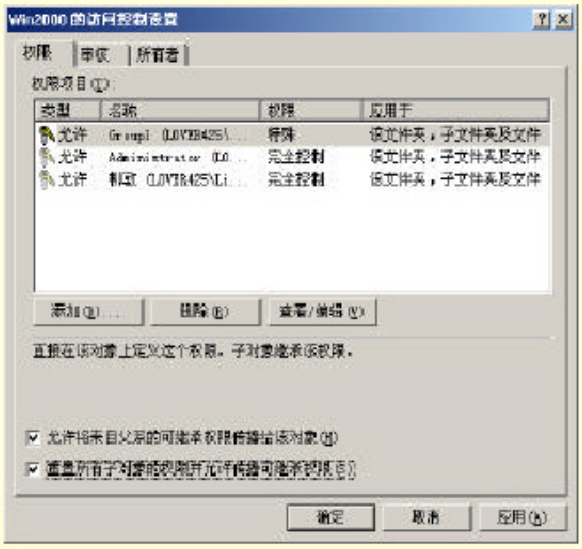


图 5-13　传播可继承权限

与阻止用户继承父系权限时的情形正好相反，“重置所有子对象的权限并允许传播可继承权限”意味着子对象中明确定义的权限将被删除，而当前（父系）文件夹中定义的权限将会被全部继承。图 5-14 所示的警告框正是这个意思。

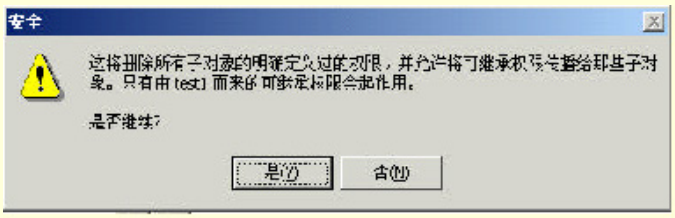


图 5-14　“重置子对象的权限并允许传播可继承权限”将删除子对象中原先设置的权限

另外，由于只有文件夹才包含子对象，因此只有在文件夹的权限设置中才能完成这项工作。

5.4.6　选择权限应用到的范围

前面已经提及特殊权限的应用范围，这些范围设置包括“只有该文件夹”、“该文件夹、子文件夹及文件”、“该文件夹和子文件夹”、“该文件夹和文件”、“只有子文件夹和文件”、“只有子文件夹”和“只有文件”。它们的具体意义与特殊权限设置里底部的权限应用复选框有关，如图 5-15 所示。选中或者清除此复选框表示是否将设置的特殊权限只应用到这个容器中的对象和/或容器上。缺省状态下，这个复选框是清除的。

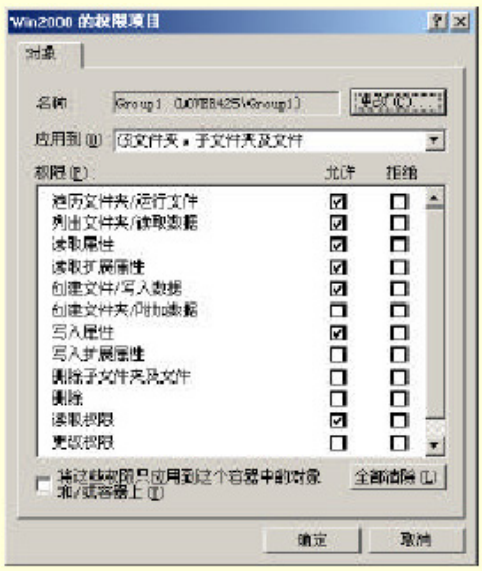


图 5-15 权限应用到容器

5.4.7 所有权

在 NTFS 文件系统中，每一个文件夹和文件都有自己的 Owner，也就是所有者。缺省情况下，文件夹或者文件的建立者就是它们的所有者。所有者是权限最高的用户，可以为所有用户（当然也包括自己）分配资源权限，或者剥夺用户的权限。所有者利用这个特权可以保护自己的资源不被他人访问（包括管理员），并依此配置自己的私有目录，建立严格的控制保护措施。

可以查看资源的所有者。仍在资源对象上单击右键，选择“属性”、“安全性”，单击“高级...”按钮，并选择“所有者”选项卡，如图 5-16 所示。

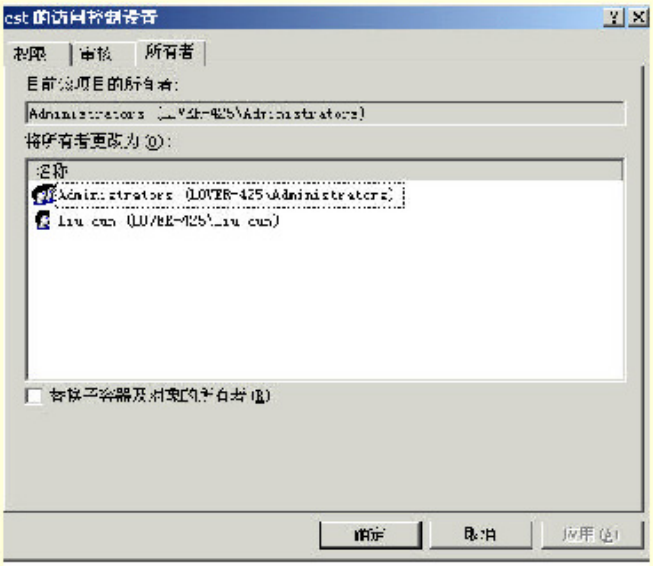


图 5-16 显示所有者

对象的所有者不能转移对象的所有权，这个设置看起来似乎不合情理，但这种强制措施可以防止不负责任的转移所有权，毕竟所有者的权力太大了。如果所有者想把所有权转移给其他用户或者组，可以为他们分配“取得所有权”的权限。这样被分配了这个权限的用户或组可以随时取得所有权。

取得所有权十分简单。在如图 5-16 所示中，只要从“将所有者更改为”列表框中选出自己的用户名，单击“确定”即可。顺便还可以成为子对象（子容器）的所有者，只要选中如图 5-16 所示中的“替换子容器及对象的所有者”复选框即可。

有两种人可以取得所有权，除了被分配了这个权限的用户或组外，管理员或管理员组的成员总可以取得所

有权，这样可以确保管理员在必要的时候接管系统资源。

5.4.8　移动和拷贝对权限的影响

作为设置权限的最后一小节，这里介绍一下移动和拷贝文件对其权限的影响。这种影响与采用的操作有关，也与前后路径有关。

■　复制文件

复制（拷贝）文件相当于产生一个新的文件，这时无论目标路径与原路径是否在同一分区，新文件的权限总是与目标路径（新的路径）下的权限设置一致。

例如，用户原来对文件 File1 有读取的权限，现在将其复制至 MyFolder 目录下，而此用户对 MyFolder 目录有完全控制的权限，那么现在用户对文件 File1 的复制品有完全控制的权限。

■　移动文件

移动文件对权限可能会产生影响，这要视前后路径而定。

- 如果文件是移动到同一分区的不同目录，则权限设置不受影响。
- 如果移动文件到新的分区中，将应用目标目录的权限。例如将 D 盘下自己目录的一个文件移动到 C 盘中，此文件将继承 C 盘设置的文件权限。这是由于此时移动文件的内部操作是：文件先被拷贝到目标路径下，此时拷贝文件继承目标路径权限，然后再删除原来的文件。

值得注意的是：以上的讨论都是在 NTFS 卷下的前提下做的。如果文件从 NTFS 卷拷贝或移动到 FAT 卷中，所有的权限设置都不再保留，因为 FAT 卷根本就不支持安全设置。

5.5　审核规则

权限管理明确了每个用户的权限大小及其可以进行的操作，从理论上说已经可以保障系统安全运转。问题是总有用户试图越过权限，这其中有无意识的错误，也有不良的企图。与此同时，一些权限比较大的高级用户（包括管理员及管理员组的成员）进行的系统操作及特权使用也应该有所记录，更值得注意的是一些连续多次失败的不成功登录，这些操作都潜在有影响安全的危险因素。安全审核在这时候发挥作用。

安全审核是权限管理必不可少的补充，二者是相辅相成的。可以利用审核追踪访问文件、文件夹或其他资源的用户账号，以及登录企图、系统的关闭或者重启、取得所有权等等事件，可以选择审核成功或是失败操作，或者两者都予以审核。通过将这些操作“记录在案”，管理员可以更方便地监督系统的运转。比如，当你发现某个账号被多次试图非法登录，这时就应该提醒账号的主人加强密码安全并采用账号锁定策略；而当有人试图窥视某个机密文件，可以考虑将文件加密等等。

注意：只有系统管理员或者是管理员组的成员，才能进行安全审核。

一旦成功地设置了审核规则，就可以选择审核的对象（文件，文件夹，打印机等）、被审核的用户，以及这个用户的哪一类操作。审核帮助管理员查看用户执行了什么操作，或者用户试图执行的超过其权限的操作。但是在启动安全审核之前，必须要做的工作是启动组策略的审核策略，否则设置审核规则时，会出现错误信息，而且不会完成任何审核工作。此外，正确配置后，你需要用事件查看器（Event Viewer）里的安全日志（Security Log）来查看审核信息。

5.5.1　启动本地计算机策略

组策略中的“本地计算机策略”属于独立的管理单元，首先应将其加入控制管理单元，再利用其中的计算机配置设置审核。由于前面已经介绍过用本地计算机策略设置账号策略和密码策略，如果这个单元加入了控制台，那么 1~4 步都可以省去。另外，管理控制台在后面第 12 章还有专门介绍。

（1）从控制面板中，启动管理工具中的“计算机管理”，并打开主控制台。如果是从命令行启动，则键入 mmc。二者的区别是从命令行启动时产生一个新的控制文件，但是由于在 Windows 2000 关于管理的新观念中，各个管理单元都是独立而且是可插入任意节点的，所以不会有什么本质区别。

（2）在控制台主菜单中，打开“控制台”→“添加/删除管理单元…”菜单。此时出现“添加/删除管理单

元”窗口，如图 5-17 所示。

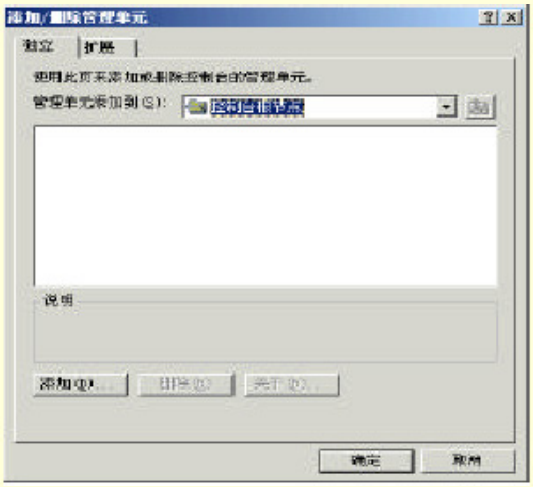


图 5-17 “添加/删除管理单元”

（3）将新的单元添加到控制台根节点中，如果根节点下已经有了其他管理单元，也可以选择将新单元添加到其他节点下，这不会影响实际操作，一切视个人喜好而定。之后单击“添加”按钮，出现添加独立管理单元列表，选择“组策略”，然后单击“添加”按钮，如图 5-18 所示。

出现安装提示框时，将会要求选择组策略对象，如果你的计算机是本地计算机，那么只有“本地计算机”可选，单击“完成”结束安装。本地计算机策略将出现在你的控制台根节点或自设的其他节点中。

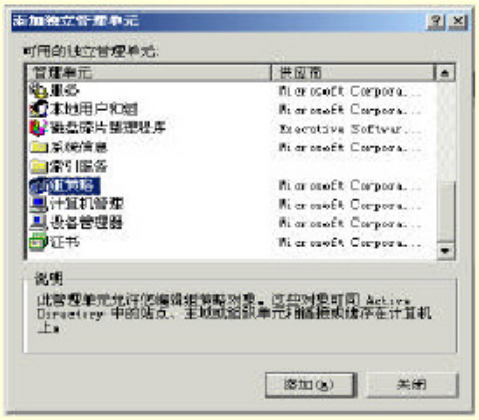


图 5-18 添加独立管理单元

（4）审核策略隐藏在很深的角落，让我们来找到它。打开“本地计算机策略”，依次展开“计算机设置”、“Windows 配置”、“安全设置”、“本地策略”，就可以找到“审核策略”，如图 5-19 所示。

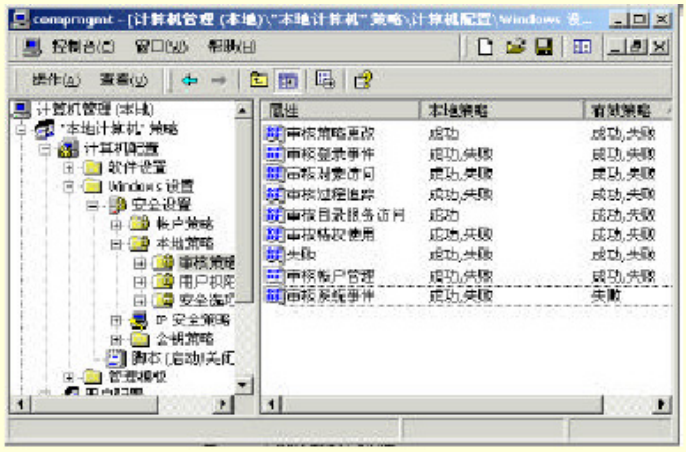


图 5-19 审核策略

如图，审核策略包括“审核登录事件”、“审核对象访问”、“审核特权使用”、“审核账户登录事件”、“审核账户管理”、“审核系统事件”、“审核策略更改”、“审核过程追踪”和“审核目录服务访问”。各个设置简略说明如下：

■ 登录事件：

指系统及账户登录的事件，有成功登录也有失败登录。

■ 对象访问：

指用户对资源对象（包括文件，文件夹等）的访问，注意如果选择审核对象访问还必须在资源管理器中对相应的文件或者文件夹设置审核规则。

■ 特权使用：

高级用户使用特权的事件，比如系统管理员查看安全日志，设置用户密码，改变系统策略等等。

■ 系统事件：

指关机、系统重启、清空安全日志等影响系统的事件。系统事件的用户为系统（System），而其他事件的用户为具体用户。

■ 账户管理：

建立/删除账户、启用/停用、修改密码等涉及账户的事件。

■ 策略更改：

安全策略、账户策略、密码策略等策略的更改。

■ 过程追踪：建立新的过程，退出过程等。

缺省时，这些策略都是不审核的，可以启动本地策略，设置审核成功或失败的事件，也可以设成同时审核成功和失败的事件。方法是：在具体策略上单击右键，在快捷菜单上选择“安全性…”，然后在弹出的审核策略更改对话框上进行具体更改，如图 5-20 所示。

图 5-20　审核策略更改对话框

5.5.2　事件查看器

前面设置的是启动审核，审核的结果记录在安全日志上，因此要完成审核还必须得借助安全日志。安全日志保存在另一个管理单元——事件查看器中，事件查看器与“本地用户和组”、“共享文件夹”、“系统信息”、“性能日志和警报”、“设备管理器”等管理单元同属于系统工具。它的启动同上面本地计算机策略一样，这里就不赘述了。

事件查看器中由 3 部分组成：应用程序日志、安全日志和系统日志。我们这里着重谈的是安全日志。与其他两种日志不一样的是：应用程序日志和系统日志可以被任何用户查看，而安全日志只对管理员开放。安全日志中记载了诸如合法与不合法的登录以及创建、打开、删除文件之类的资源使用。缺省情况下，安全日志是关闭的，管理员可以启动安全日志以及增添或减少安全日志记载的具体项目，这由前面安全审核的设置决定。

第一次查看安全日志时，也许会被庞大的表格（如图 5-21 所示）所迷惑，但熟练使用后，就会发现它们的确可以提供许多关于对象访问以及特权使用的信息。

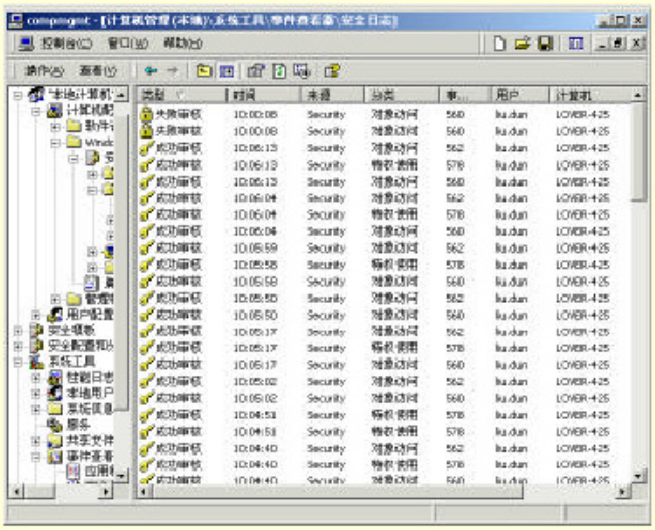


图 5-21 安全日志

前面已经提及，要让安全审核和安全日志记录对文件、文件夹这类的访问，首先必须设置让它们接受审核。这是因为：如果系统自动地记录所有文件和文件夹的安全信息，那将在性能上付出十分可观的代价，而为绝大部分无关紧要的资源对象浪费性能也是得不偿失的，所以应该只对重要的文件或文件夹设置审核。现在再回到它们的属性上去。

5.5.3 设置文件审核

设置文件审核的操作与前面设置安全性大同小异。选择“属性”→“安全性”，然后单击“高级...”，并选择“审核”选项卡，如图 5-22 所示。权限、审核、所有者共同构成了安全设置的三大部分，所有者体现了资源的主人，权限负责具体的使用规范，而审核则在幕后监督使用的事件。

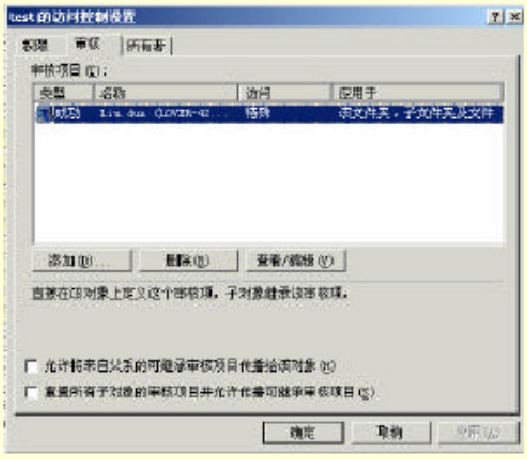


图 5-22 审核控制设置

在图 5-22 中可以发现，设置审核的操作与设置高级权限的界面十分相似。管理员可以添加被审核的用户或组（按“添加...”按钮）；也可以删除被审核的用户或组（选中用户，按“删除”按钮）；对审核的具体内容的查看或编辑，则通过按“查看/编辑”按钮进入审核项目对话框进行操作。

当新增审核的用户时，也会自动调用审核项目对话框。这个对话框与特殊权限设置的对话框界面是统一的，可以很方便地使用。具体审核的项目与特殊权限的条目，从“遍历文件夹/执行文件”到“取得所有权”一一对应，可以审核成功或失败的事件，也可以全部审核。设置后的结果表现在图 5-22 中。

其他的一些设置，包括如图 5-22 中的“允许将来自父系的可继承审核项目传播给该对象”、“重置所有子对象的审核项目并允许传播可继承审核项目”以及在审核项目对话框中的审核应用范围（该容器或包括其子对象）的设置都与权限里的设置一样。如果不明白，可以参阅前面第 5.4 节内容。

设置好审核项目后，我们来看看安全日志里记载的内容。

打开安全日志，在任一条记录中，单击右键，从快捷菜单中选择“ 属性 ”，然后选择“ 事件详细信息 ”选项卡，就可以查看详细信息。我们来看看图 5-23 和图 5-24 记载的两条信息：

图 5-23　成功取得所有权的审核信息

图 5-24　访问失败的审核信息

如图 5-23 所示的例子中，“ 描述 ”框里的 SeTakeOwnerShip 的意思就是该用户成功取得所有权，类别是特权使用；如图 5-24 所示的例子表现了用户由于权限不足而访问资源失败，类别是对象访问，“ 描述 ”框里的“ 主要用户名 ”和“ 对象名称 ”指明了访问失败的用户名及其企图访问的资源路径。这些信息对管理员的安全管理会有帮助。关于事件查看器的内容在第 8 章中还有介绍。

第 6 章　共享资源及权限设置

上一章讨论了如何管理本地资源的问题，实际生活中，还有另一件重要的事，就是和别人进行资源共享。如果没有共享，工作也许将是孤立而枯燥的，而且由于成果无法得到及时的交流和共享，工作的效率也不可能提高。

本章内容包括：

- 特殊的系统共享
- 建立共享
- 共享权限设置
- 使用共享文件夹管理工具
- 使用脱机资源
- 同步

6.1　特殊的系统共享

与内建的账号和组相似，Windows 2000 也会自动地创建一些系统共享（一个或多个，根据你的计算机配置而定），供管理员和系统使用。

这些特殊的共享目录是无法从我的电脑或者资源管理器中直接浏览到的，但它们确实存在，从管理工具中的共享文件夹管理单元中就可以发现它们。一般说来，这些特殊的共享是无法删除或者被修改的，就如同内建账号无法被删除一样。下面我们就来了解它们：

■ drive letter$（盘符）

比如 A$、B$、C$、D$等等，C$就是 C：驱动器的系统管理共享。这种共享允许管理员或管理员组的成员从网络上连接驱动器的根目录。 对于安装 Windows 2000 Professional 的系统，只有管理员组（Administrators ）或者备份操作组（ Backup Operators group）的成员才能连接到这个共享目录；对于安装 Windows 2000 Server 的系统，服务器操作组（Server Operators group）的成员也能访问。

■ ADMIN$

远程管理计算机系统所使用的共享资源，其路径是 Windows 2000 的根路径，一般说来，就是 C：/WINNT。

■ IPC$

系统管理共享支持命名管道机制，对程序间通讯是必不可少的。用于计算机的远程管理以及查看计算机的共享资源。

■ PRINT$

用于远程管理打印机的资源。

■ REPL$

这个共享只有在安装了 Windows 2000 Server 并配置成复制服务器才提供，并用于支持目录输出。Windows 2000 Professional 中不提供这个共享。

■ NETLOGON

这个共享也只有在 Windows2000 Server 才提供，这个共享目录被 Net Logon 服务用于处理域登录请求。

■ FAX$

发送传真时用于暂时缓存数据。

上面的许多共享只适用于 Server，对 Professional 版本只有前面 3 种共享。不知读者是否已经发现，上面的共享绝大多数后面的都有$标志。任何一个以$符号结尾的共享都有一个特点：不出现在诸如“我的电脑”，“资源管理器”，“网上邻居”等浏览列表中，属于被隐藏的共享。隐藏的共享可以屏蔽一些没有必要被其他用户使用的资源。需要提醒的是：对于这些特殊的系统共享，即使普通用户知道它们的存在，依旧无法访问他平时无法访问的区域。比如驱动器根目录的系统管理共享，只有 Administrators 组和 Backup Operators group 组的成员

法访问的区域。比如驱动器根目录的系统管理共享，只有 Administrators 组和 Backup Operators group 组的成员才有权限访问。尽管如此，你可以利用这个特点，创建你自己的共享，并在共享名后加上一个$，以便隐藏自己的共享目录。

6.2　建立共享

6.2.1　基本属性设置

建立一个共享目录的步骤是：

（1）打开资源管理器或者我的电脑，展开目录树，找到要建立共享的目录。

（2）单击右键，在弹出的快捷菜单上，选择“共享…”命令，或者选择“属性”命令后单击“共享”选项卡，将出现共享对话框，如图 6-1 所示。

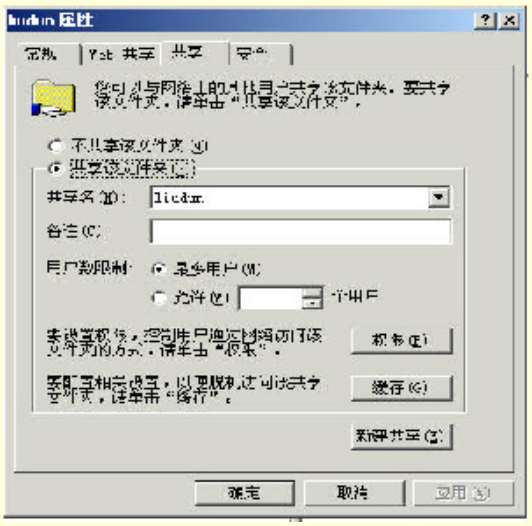


图 6-1　“共享”对话框

下面我们来设置共享属性。缺省情况下，对话框里的选择是“不共享该文件夹”，现在选择“共享该文件夹”，激活下面的共享设置。

在“共享名”文本框中，输入设置的文件夹共享名（网络上出现的将是这个名字），缺省情况下，这个名字就是文件夹原来的名字。可以在共享名后面加上一个$符号，这样可以隐藏该文件夹。

在“备注”文本框里，输入适当的描述性信息，帮助其他用户迅速理解共享的内容。

用户数限制中，缺省情况是最多用户，也即没有限制。选择“允许多个用户”，指定最多连接的用户。

缺省情况下，Everyone 组对共享目录有完全控制的权限，单击“权限”可以做进一步的具体设置，我们下面再详细讨论。

希望用户能够离线使用，请单击“缓存”。

如果想以原有文件夹建立新的共享，单击“新建共享”。此时弹出新建共享对话框，可以设置其他共享名，最多允许的用户数以及设置不同的用户权限。

提示：对于 Professional 版本，实际可以共享你的文件夹的最大用户数是 10，如果设置了超过 10 的用户数，比如 11，系统会自动重新修改为 10。

注意：尽管你可以在共享名后加$用以在网络上隐藏共享，但如果有其他用户知道这个共享并且知道你的路径，仍然可以映射到你的共享文件夹上去。

建立共享后，文件夹的图标下会出现一只手托着的图案，表示这是一个共享的文件夹。还有一点需要说明的是：如果网络有 MS-DOS 或者 Windows 3.x 的用户，并且希望这些用户也能使用共享文件夹，共享名必须遵守 DOS 时代“臭名昭著”的 8.3 命名规则，不能使用长文件名。而 Windows 95、Windows 98 和 Windows NT 的用户可以使用长文件名。我们知道：MS-DOS 访问网络上的文件时，长文件名会自动按一定的规则转换为 8.3 的短格式，然而对长共享名就没有办法了。

6.2.2 连接共享

由于资源管理器、我的电脑、网上邻居等都已经完全统一，用户完全可以打开任意一个工具，找到希望使用的文件夹，然后双击打开就行了。要查看更多的计算机，可以打开整个网络。

对于 Windows 3.x，Windows NT 3.x 的用户，可以使用旧式的文件管理器查看网络资源。

对于 MS-DOS 的用户，则只能使用非图形界面的手段了。提供的查看网络共享资源的命令是 net view \\computername 命令。当然，Windows 95、Windows 98 、Windows NT 和 Windows 2000 的用户也可以用 DOS 的命令，可以使用外挂的 16 位 DOS 程序，也可以使用开始菜单中的“运行 …”命令，为了看清楚执行结果，应该用外挂的 DOS 程序（在开始菜单，程序，附件中），“运行 …”命令的执行结果总是一闪而过，根本无法看清。图 6-2 展示了使用 net view \\computername 命令的运行结果。

如图所示，当 net view 命令参数正确时，将显示名为 computername 的计算机上的共享资源（包括文件和打印机）。如果运行失败并出现错误信息：系统发生 53 号错误，请确认输入的计算机名正确无误，并且在你的计算机和对方计算机上的网关和路由是良好运转的。

使用 net view \\computername 命令看到的共享与在图形界面中看到的一样，对于被隐藏的共享都觉察不到。

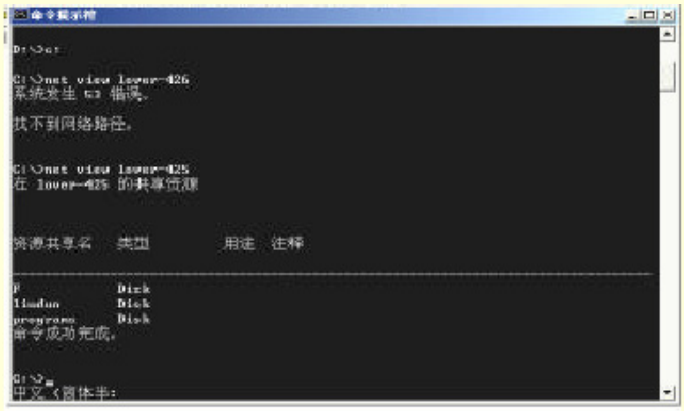


图 6-2 使用 DOS 的 net view \\computername 命令

提示：net view 的命令格式如下：

net view [*computername* | /domain[:*domainname*]]

net view /network:nw [*computername*]

参数说明：

1．无参数：

单独的 net view 命令列出当前域的计算机名。

2．加\\computername 参数

列出此计算机上的共享资源

3．domain[:*domainname*]

列出域中想查看的可用计算机,如果域名(domainname)省略，将列出网络中所有的域。

4．network:nw [*computername*]

列出 NetWare 网络上以 computername 命名的计算机上的共享资源，如果省去计算机名，则列出 NetWare 网络上所有可用的服务器。

6.2.3　映射网络驱动器

为了更方便地使用网络上的共享资源，通常使用的方法是将共享文件夹映射成为本地硬盘上的一个驱动器（就好比自己机器上的 C 盘，D 盘），为这个新的“驱动器”加一个没用过的盘符，比如 G 盘之类。这样打开 G 盘实质上就是打开远程计算机上的共享文件夹，但感觉上和打开自己本地的 D 盘毫无区别。将共享文件夹映射为本地文件夹的方法是：在网上邻居找到共享的文件夹，单击右键，并选择“映射网络驱动器...”命令，如图 6-3 所示：

图 6-3　映射网络驱动器

在如图 6-3 中，执行以下操作：

（1）从驱动器下拉框中选择一个未使用的驱动器盘符。

（2）当每次登录都要连接该共享文件夹时，选中“登录时重新连接”复选框。

（3）单击其他用户名，选择你打算用以连接身份的账号和密码，如图 6-4 所示。默认应是你登录本地工作站的账号，但如果当前登录的账号权限不足时，就要输入有足够权限的账号，这时你必须知道其他账号的密码。

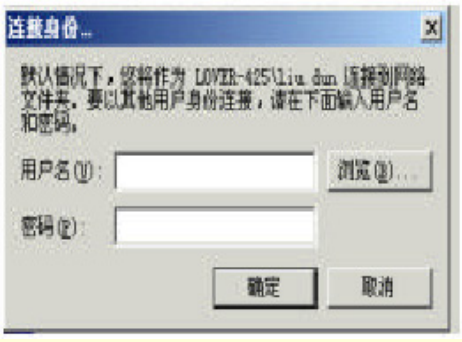


图 6-4　选择连接身份

（4）单击“完成”结束。

此外，也可以在资源管理器中，打开“工具”→“映射网络驱动器...”菜单，映射操作同上。

如果知道一些隐藏的共享，可以在映射网络驱动器时手工输入路径，就可以访问其中的资源了。当然前提是有一定的权限，比如像前面提过的 C$之类的共享，如果没有管理员或备份操作员的权限，即使知道有这样的共享，仍然无法访问。

完成映射工作后，就可以像使用本地资源一样使用共享资源了，如图 6-5 所示的 G 盘，就是映射网络上的共享文件夹。另外，文件夹下有只手托着的图标表示这个文件夹是本地设立的共享文件夹。

如果用外挂的 DOS 程序，在提示符下键入 G：就可以进入“G 盘”了。

图 6-5 资源管理器中的映射目录和共享目录

对于 MS-DOS 的用户，可以用 net use 命令映射共享文件夹，net use 命令有丰富的功能，一些基本的语法及例子如下：

■ **net use** [devicename]: [\\computername\sharename]：建立连接

如用驱动器 M：连接\\lover\app 的命令是：net use m: \\lover\app

又如用 LPT1 连接 Accounting 服务器上的打印机 Laser1 的命令是：

net use LPT1: \\Accounting\Laser1

如果共享名中有空格，需要用引号括起来，如 net use m: “\\lover\program files”

■ net use [*devicename*]:/delete：断开连接

如断开驱动器 M：的连接，用 net use m: /delete 命令。

■ net use [devicename | *] [\\computername\sharename[\volume]] [password | *]] [/**user:**[domainname\]username]：选择用户连接。如 net use m: \\lover\app /user:jack 等。

可以有两种方法设置共享：或者将文件夹直接设为共享，或者将其父文件夹设为共享，这样子文件夹事实上也被共享。要注意的是：如果父文件夹的共享名为 ShareName1，与此同时，子文件夹也设为一个独立的共享且共享名为 ShareName2，这时两个共享在网络上是并列的关系。比如用 net use 命令映射 ShareName2，其命令是：

net use m: *computername*\ShareName2 而不是：

net use m: *computername*\ShareName1\ ShareName2。

6.2.4 停止共享

要停止共享，只需在如图 6-1 所示的“共享”对话框中，选择“不共享该文件夹”即可。

一般说来，不应去终止系统自动创建的共享目录（管理员才有权力终止它们），如果强行终止，下次系统重新启动时也会再次建立。终止共享目录后，就不能再通过网络使用它们。如果此时有用户正在连接，则会被强制断开。

要断开网络驱动器，在资源管理器选择“工具”→“断开网络驱动器 …”菜单，将出现断开网络驱动器的对话框。但是如果有以打开而尚未关闭的文件，强行断开连接有可能造成数据丢失，系统会弹出警告框，如图 6-6 所示。

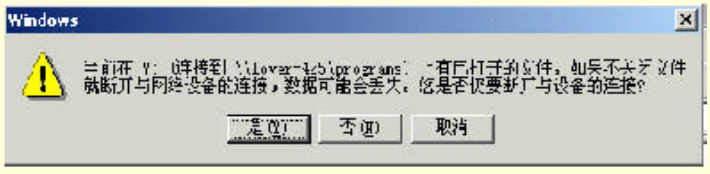


图 6-6 是否断开连接？

6.3　共享权限设置

在第 5 章里我们已经花了相当大的篇幅来讲 NTFS 的本地权限管理，同样，也可以为用户分配网络的共享权限。在如图 6-1 所示的共享对话框中单击“权限”按钮，弹出权限对话框。

缺省情况下，Everyone 组对共享目录有完全控制权限，也可以设置更严格的权限。共享权限的设置对话框如图 6-7 所示。

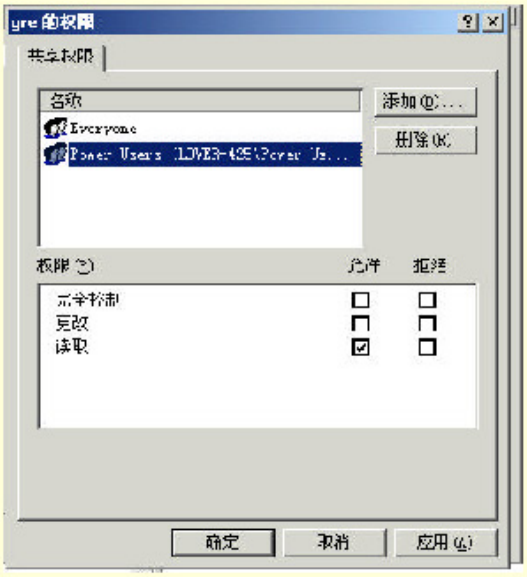


图 6-7　共享权限设置

读者可以发现，共享权限设置与本地权限设置非常地相似。缺省时，只有 Everyone 组对共享目录有权限，而且是完全控制权限，和前面一样，单击“添加 ...”按钮可以增添拥有共享权限的用户或组；单击“删除”按钮可以减少拥有权限的用户。新添加的用户缺省时拥有的权限是读取。相比之下，共享权限只有 3 种：完全控制、更改和读取，比本地权限的设置要简单得多。表 6-1 具体给出了每种权限赋予用户的权限。

表 6-1　权限赋予的内容

允许的操作	完全控制	更改	读取
查看文件名和子文件夹	X	X	X
遍历子文件夹	X	X	X
查看文件数据和执行程序	X	X	X
在共享文件夹上添加文件和子文件夹	X	X	
修改文件	X	X	
删除文件和子文件夹	X	X	
更改权限（只适用于 NTFS）	X		
取得所有权（只适用于 NTFS）	X		

用户的共享权限也是可以累加的。同样，由于拒绝比允许优先，如果该用户被拒绝访问，那么他将不会有任何操作的能力。另外，共享权限只能在共享目录的根目录设置，子目录会全部继承根目录的共享权限。有时候，为了削减用户在子目录的共享权限，可以对子目录另外设立一个共享，并重新分配较低的权限。

共享权限与另外设置的本地权限是否可以叠加呢？答案是不会。与此相反，用户通过网络访问资源时，对某个共享的实际权限是取共享权限与本地权限两者中的较严者。前面提过，缺省情况下，对某个共享文件夹，Everyone 组具有完全控制的权限，由于 Everyone 组包含所有从网络或本地登录的用户，这时候应该首先设好用

户的本地权限，再设置共享文件夹的权限，否则用户可能登录后对资源进行破坏。

值得强调的是：共享权限只对通过网络访问资源的用户有效，当用户从本地登录时，共享权限没有约束作用，为了防止破坏，应该设置严格的本地权限。在 NTFS 卷中，NTFS 文件系统强有力地支持权限设置，在本地设置权限的具体措施参见第 4 章的内容。

对于 FAT 卷上的文件，就没有这么幸运了。首先我们知道，FAT 文件系统不支持在本地实施权限管理，因此如果用户从本地登录，将可以完全自由地访问所有资源。

如果共享目录位于 FAT 卷上，那么共享权限是唯一可以限制用户访问资源的手段。一旦 FAT 卷上的某个目录被设置成可以共享，用户就可以从网络上自由地访问它下面的所有文件和文件夹。NTFS 的共享权限虽然比本地权限略有简单，但比起 FAT 卷来仍然要安全得多。

综上所述，对于 FAT 卷，限制用户从网络访问的唯一方法，是使用 Share 权限；限制用户从本地访问资源的唯一方法，是不允许其从本机登录。

建议：如果设立 Programs Files 共享目录，里面存放着公用的各个程序，由于程序已不需要修改，可以只给用户分配读取的共享权限。然后为 Create Owner 分配完全控制权限，用户对自己的临时文件夹可以完全控制，可以添加、删除文件，添加文件夹等等。

6.4 使用共享文件夹管理工具

Windows 2000 提供了共享文件夹这个独立的管理单元以管理共享，这个工具只有管理员有权使用。共享文件夹同事件查看器、本地用户和组一样，都位于系统工具之下，管理员可以在管理控制台下的系统工具内找到它。共享文件夹是 Windows 2000 新提供的工具，利用这个工具，可以非常方便地查看和管理共享的资源以及当前的连接和会话（Session），具体如下：

- 管理共享文件夹，包括添加新的共享文件夹，如果需要可以停止一个或多个共享。
- 管理共享权限，包括查看、设置、删除用户或组对共享文件夹的权限。
- 管理当前的会话，包括查看连接的用户信息，如果需要可以断开与他们的连接。
- 查看当前被使用的共享文件夹或文件，如果需要可以关闭一个或多个文件。

对于 Windows 2000 Server，还可以为 Macintosh 计算机配置服务，使 Macintosh 的用户也可以共享资源。

Windows 2000 Professional 里只有管理员组和高级用户组（Power Users Group）的成员可以使用共享文件夹工具，在 Windows 2000 Server 中，Server Operators Group 组的成员也可以使用这个工具。

下面我们就来看看这个共享文件夹的工具，打开控制台根目录后，展开“系统工具”下的“共享文件夹”，可以看到下面包括 3 个部分：“共享”、“会话”和“打开文件”，如图 6-8 所示。

6.4.1 共享

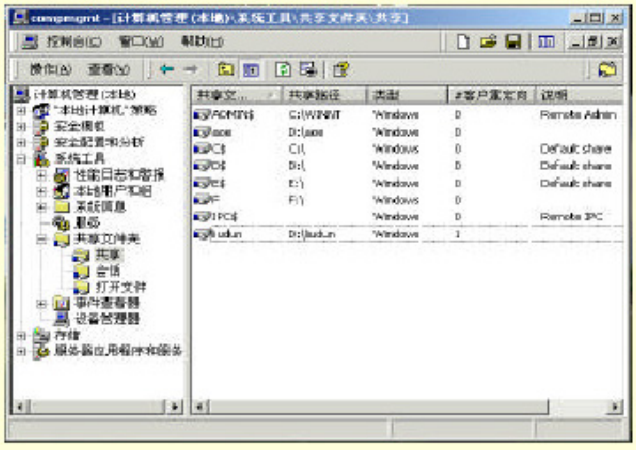


图 6-8 共享文件夹

在图 6-8 中，列出了当前设置的所有共享，包括隐藏的（共享名后有$符号），公开的以及所有系统内置的共享。每一列的意思是：

■ 共享文件夹：当前计算机上所有可以使用的共享资源，包括共享目录、共享打印机以及命名管道。

> 提示：命名管道是一个进程用以传送信息给另一个进程的一部分内存，这两个进程可以是本地的，也可以是远程的。

■ 共享路径：共享资源在本地的路径。

■ 类型：网络连接的类型，包括 Windows、NetWare、Macintosh 等等。

■ 客户重定向：当前连接该共享资源的用户数。

■ 说明：对共享资源的描述。

可以在这里很方便地管理共享文件夹。

6.4.1.1　添加新的共享

在“共享”上单击右键，在弹出的快捷菜单上，选择“新文件共享”。此时将出现添加新共享向导对话框，要求选择新共享的文件夹，如图 6-9 所示。单击“下一步”，出现如图 6-10 所示的权限设置对话框。

图 6-9　创造新共享文件向导

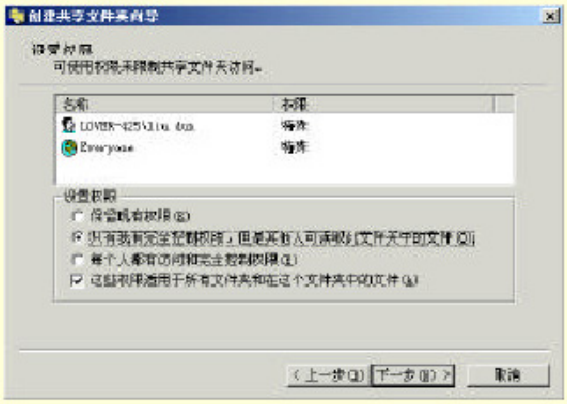


图 6-10　设置权限

这时有 3 种选择：缺省情况是“保留现有权限”，也就是前面所说的给 Everyone 组分配完全控制的权限，这时底下的“这些权限适用于所有文件夹和在这个文件夹中的文件”复选框是灰色无效的，因为在这种缺省情况下，Everyone 组对下层资源自动有完全控制的权限。第二种选择是给设置共享的用户分配完全控制权限，给 Everyone 组分配特殊读取权限，第三种选择是给 Everyone 组访问和完全控制权限的特殊权限，作这两种选择时，可以再选择是否将权限传递给子文件夹和文件。

单击“下一步”，输入共享名，描述以及可以访问的计算机系统（Microsoft Windows、Novell NetWare、Apple Macintosh），完成设置。

6.4.1.2 停止共享

在如图 6-8 所示中，选定文件夹，单击右键，在弹出的快捷菜单上，选择“停止会话”或“所有任务”→“停止共享”。

在连接的另一端，如果停止共享使您的机器断开了连接，会有一个汽球状的提示从状态栏中升起，提示连接已经断开，但还可以脱机使用。后面第五节会详细介绍脱机使用。

6.4.1.3 查看属性

选定共享文件夹并单击右键，在弹出的快捷菜单上，选择“属性”，查看其共享权限设置和安全设置，也可以在这里修改权限。

此外，也可以在图 6-1 所示中直接按“权限”按钮，在建立共享时设置权限。

对于系统内建的特殊共享，由于是为管理用途共享的，不能为其设置共享权限，属性框里没有“共享”这一选项卡，IPC$共享还不能进行安全设置。

此外也不应该停止特殊共享，如果强行停止，服务器重新启动或者计算机重新启动时也会重新建立这些共享。如图 6-11 所示是试图关闭这些共享时的提示。

图 6-11 试图停止系统共享时的警告

此外，还可以通过信使服务给远程计算机发送消息。

在“共享”文件夹上单击右键，从快捷菜单中，选择“所有任务”→“发送控制台消息”命令，将出现如图 6-12 所示的消息框，可以在里面输入文字，把一些重要信息传送给网络上的其他计算机，这样也方便了网络间的通讯。

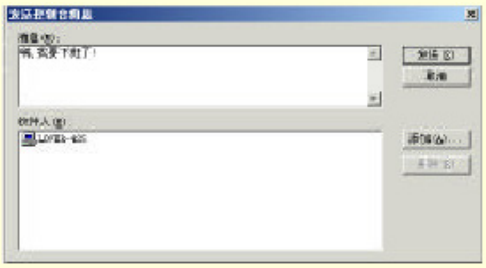


图 6-12 发送控制台消息

6.4.2 会话

会话可以理解为用户从网络上登录后，与本地计算机建立的连接。

会话项是共享文件夹管理工具的一部分，列出了当前所有与本计算机相连的网络用户信息。如图 6-13 所示是省去了控制树的会话查看信息，容易发现，该信息也是由几列组成的。

- 用户：连接到本地计算机上的网络用户。
- 计算机：用户所在的计算机，一般不是当前用于查看的计算机。
- 类型：网络连接的类型，可以是 Windows、 NetWare 或者 Macintosh。
- 打开文件：该用户打开的本地计算机上的资源数目。
- 连接时间：会话建立后持续的时间。

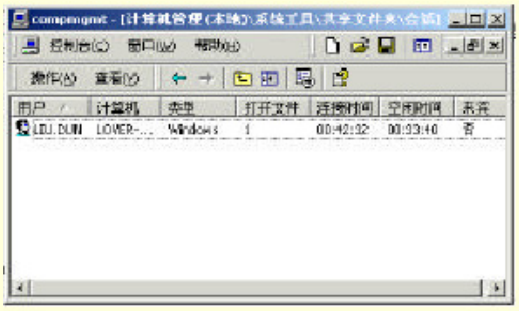


图 6-13　会话信息

■ 空闲时间：用户最后一次动作后持续的时间。

■ 来宾：确定该用户是否以来宾身份登录。

选定用户后，单击右键，在弹出的快捷菜单上选择“关闭会话”命令，可以断开与此用户的对话。如果有多个用户对话，还可以同时断开所有对话，方法是在会话项上单击右键，在弹出的快捷菜单上选择“中断全部的会话连接命令”。

如果是管理员远程登录管理本地计算机，则这个连接不会被中断。

6.4.3　打开文件

打开文件提供了当前打开的共享文件的信息，图 6-14 是省去了控制树的打开文件查看信息，其各字段含义如下：

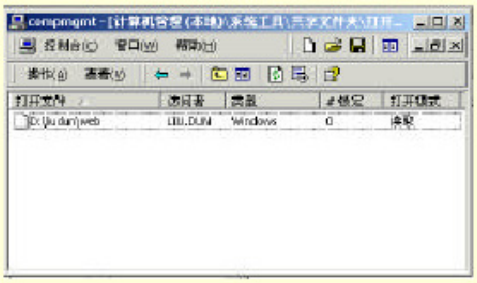


图 6-14　打开的共享文件

■ 打开文件：列出了当前打开的资源文件，这些资源可能包括数据文件、命名管道以及打印作业等。

■ 访问者：打开文件的用户。

■ 类型：与会话中的类型一样，指网络连接的类型，可以是 Windows、NetWare 或者 Macintosh。

■ 锁定：资源锁定的个数。

■ 打开模式：打开资源所用的权限。

可以很方便地在控制台中将打开的文件关闭：选定要关闭的文件，单击右键，从快捷菜单中，选择“将打开的文件关闭”，或“所有任务”→“将打开的文件关闭”，如图 6-15 所示。

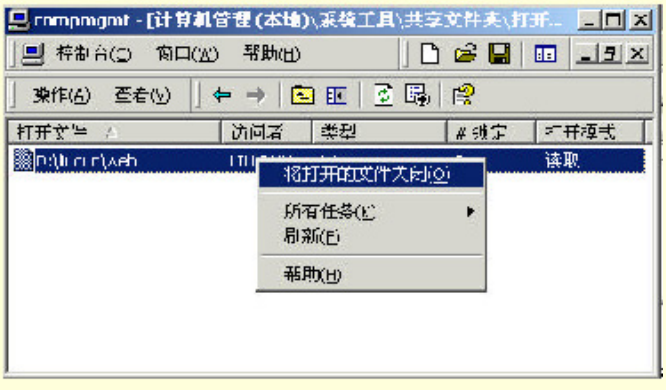


图 6-15　关闭打开的文件

6.5 使用脱机资源

虽然可以通过映射网络驱动器模拟本地硬盘资源，但事实上使用网络上的共享资源总是没有本地来得稳定，总会有这样那样的原因使得网络断开，比如网络故障、关机，或者使用的便携式电脑需要离开网络等等，这时的对策是离线使用。

可以设置选项，使状态条在用户的电脑将要与网络断开时发生变化，并发出通知。机器与网络断开后，用户仍旧可以继续工作，像正常状态一样使用共享的文档和程序，甚至访问权限也与正常连接时一样。重新与网络连接后，离线使用的变动可以反映到网络上，对原有资源进行更新。

要使用离线文件，必须首先对计算机进行设置。步骤如下：

（1）打开“资源管理器”，打开“工具”→“文件夹选项…”菜单，或者在控制面板中打开“文件夹选项”，选择“脱机文件”选项卡，如图 6-16 所示。

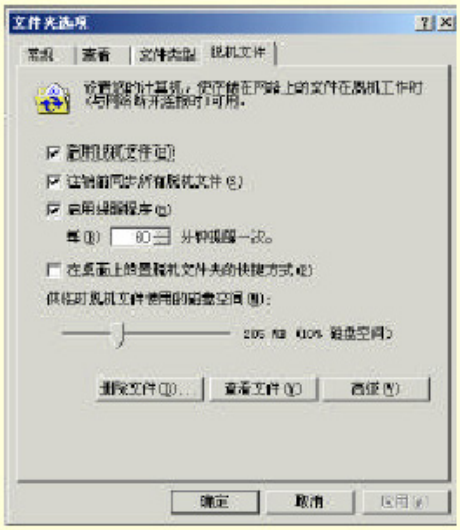


图 6-16 启用脱机文件

（2）选中“启用脱机文件”复选框。

（3）选择或清除“注销前同步所有脱机文件”。选中时启用的是完全同步，清除时启用的是快速同步。

提示：正如很难把事情做得又快又好一样，完全同步和快速同步的区别是：完全同步保证每个离线文件有最新的版本，而快速同步的工作则要迅速得多，并保证每个离线文件有完整的版本，以使用户能照旧正常工作，但这可能不是最新的版本。

（4）决定是否启用提醒程序和在桌面上放置脱机文件夹快捷方式。如果启用了提醒程序（缺省），当网络中断时，状态栏会升起一个消息汽球，提醒用户网络连接已发生了变化并开始使用脱机文件，消息汽球还可以提供更多提示。

（5）用滑动条决定给脱机文件预备的硬盘空间，缺省是 10%的硬盘空间。如果觉得脱机文件会很大，可以预留更多的空间。

提示：如果一个文件的快捷方式被设为离线使用，这个文件可以被离线使用，但如果一个文件夹的快捷方式被设为离线使用，这个文件夹底下的内容不能被离线使用。

（6）单击“查看文件”，查看同步文件。

（7）单击“删除文件”，在“确认文件删除”对话框中，删除脱机文件（不会删除网络上的文件），可以选择只删除临时脱机文件或者同时删除临时脱机文件以及始终可以脱机使用的版本。

需要提醒的是：即使已经通过“文件夹选项”设置了使用脱机文件，用户还必须选择具体的共享文件和文件夹，并将之设为允许脱机使用。在网络的另一端，管理员也可以将设为共享的文件夹继续设为允许脱机使用，这时文件夹下的每个文件会自动允许被脱机使用，这样用户就不用自行配置了。管理员设置方法为：在设置共享文件夹，如图 6-1 所示的对话框中，单击“缓存”按钮，出现如图 6-17 所示的缓存设置对话框，并确保“允许在这个文件夹中缓存文件”复选框被选中。

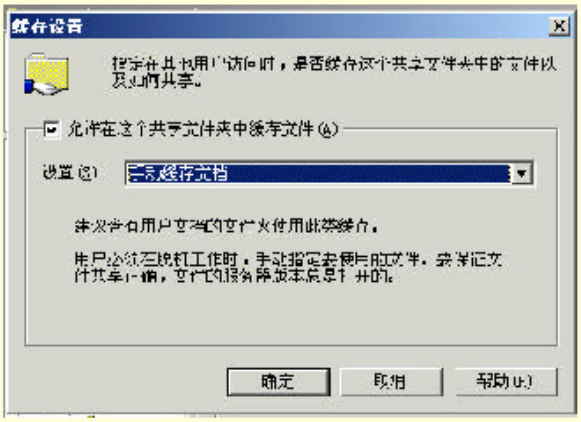


图 6-17　允许缓存文件

脱机工作时，离线文件储存了网络上共享文件的一个版本，并将其存放在用户预留的本地磁盘当中，这部分磁盘空间缺省是用户可用磁盘空间的 10%。这样一来用户可以自由地在缓存上启用脱机文件，而不用顾及网络是否仍然相连。

如图 6-17 所示，管理员可以为共享用户设置 3 种缓存选择：

■ 手动缓存文档

只有共享用户明确（手动）设置要求脱机使用的文档才可以被离线使用，这种选择适用于有多个用户有权访问和更改含有用户文档的共享文件夹。要保证共享正确，文件的服务器版本总是被打开的。这也是设置共享文件夹时的缺省配置。

■ 自动缓存文档

自动缓存文档保证用户从共享文件夹打开的每个文档可以脱机使用，但是不会使共享文件夹中的所有文件自动可以脱机使用，未被打开的文档将不能脱机使用。

使用自动缓存文档，用户打开的每个文档会自动下载，同时原有的旧的文档将会被删除，为新打开的文档腾出空间。要保证共享正确，也要求文件的服务器版本总是打开的。

■ 自动缓存程序

当共享文件夹里存放的是不会被改动的文件，比如含有只读数据和从网络运行的应用程序的共享文件夹应该考虑使用自动缓存设置。管理员往往会建立一个 program files 的共享文件夹，在里面存放一些公用的程序，这种情况就可以使用自动缓存程序配置。离线使用的文件可以被读取或运行，但不应该被更改，所以要严格设置权限，保证共享文件是具有只读访问权限的。同样，用户打开的每个文件会自动下载，同时原有的旧的副本将会被删除，为新打开的文件腾出空间。

使用自动缓存程序的优点是：由于用户总是直接打开离线文件，而不用访问网络的版本，因此可以减少网络堵塞。

如果启用了提醒信息，初始断开网络时，可以根据信息汽球提示，选择查看脱机文件状态，如图 6-18 所示。

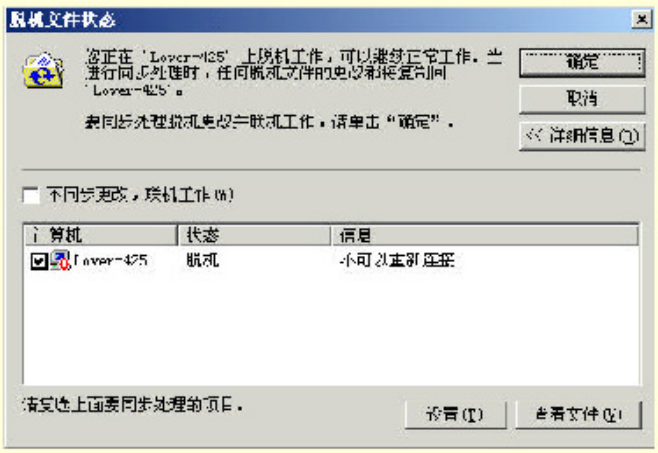


图 6-18 脱机文件状态

当重新连接后，选中“不同步更改，联机工作”复选框后，可以重新联机工作。

6.6 同步

重新连接到网络上去后，可能要刷新缓存中的离线文件，取得最新的版本，或者需要将自己的离线工作改动到网络版本上去，这就叫做同步（Synchronization）。同步包括在本地网中更新文件和程序，也包括在因特网上更新网页。离线浏览过 Internet 的读者一定不会对同步陌生。Windows 2000 提供了同步管理器负责同步的管理。

在“资源管理器”中，打开“工具”→“同步”菜单，选择要同步的项目，单击“同步”即可。

利用同步管理器，可以作进一步的同步设置：

（1）在“资源管理器”中，打开“工具”→“同步”菜单。

（2）单击“设置...”按钮，进入如图 6-19 所示的同步设置对话框。

（3）在“在使用这个网络连接时”下拉框中，选择网络连接类型，可以是本地局域网，modem 连接等等。可以为不同网络连接类型选定不同的同步项目。在“同步以下选定项目”框中，选择要同步的项目。更好的措施是采用自动同步，可以选择登录计算机时同步，也可以选择注销时同步，或者在登录、注销时都同步。采用自动同步可以确保新的变化及时得到反映。

（4）选择“空闲状态”选项卡，选择在计算机空闲时同步的项目（计算机不懂得偷懒！）。单击“高级...”按钮，如图 6-20 所示，进一步告诉计算机同步的频率和空闲多长时间后开始同步。

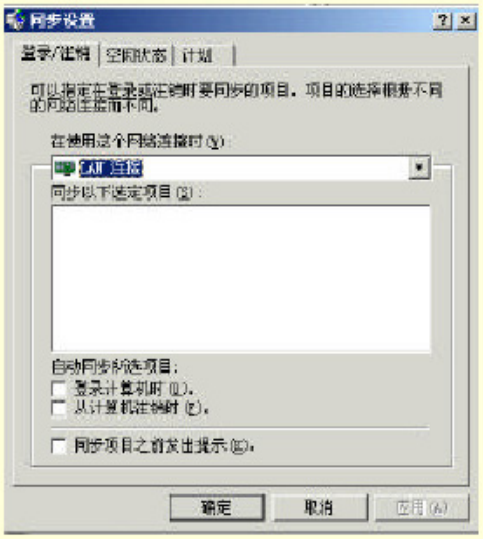


图 6-19 同步设置

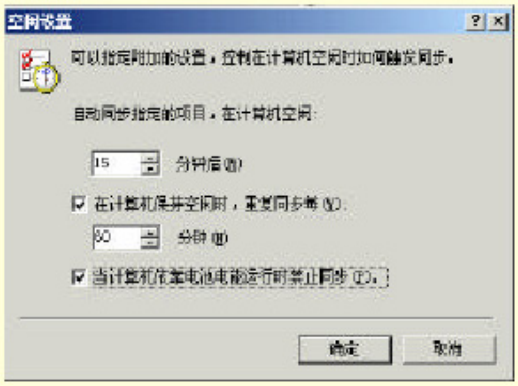


图 6-20　空闲设置

同步文件时，在离线期间打开和更改过的文件会和网络上的版本进行比较，如果在该用户脱机期间，这个文件没有被其他用户更改，那么此用户的改动将覆盖旧版本，成为新的网络上的版本。但是情况并不总是如此顺利，总会难以避免地出现数据冲突。

如果不巧有别的用户已对这个文件做了修改，那么用户可以选择保留自己的版本、保留网络上的版本，或者两者都保留，如果保留两者的话，就要给自己的版本起个新名，二者都会保存在同一路径。

如果用户在离线工作时，删除了自己计算机上的网络文件版本，但在这期间，别的用户对这个文件做了改动，那么这个文件从你的计算机上删除了，但不会从网络上删除。

如果用户在离线工作时，对网络文件做了更改，而在这期间，别的用户在网上删除了这个文件，这时可以选择将自己的改动文件版本保存在网络上或者将之从本地计算机上删除。

最后，如果用户在离线工作时，有新的文件添加到设为可以离线使用的共享文件夹上去，那么当该用户重新连接网络并同步后，该文件也会添加到你的计算机上。

第 7 章　域

在前面几章讲述账号和权限时，已经不断提到了网络和域。随着计算机的越来越普及，联网已蔚然成风：大学校园里，年轻学子利用自己组建的局域网通宵达旦地联机游戏，而在世界各地，愈演愈烈的国际互联网浪潮冲击着全球的网民。各种网络中，数据以从数十造千至数吉的信息速率“呼啸”而过，安坐桌前，就可以和对门邻室、楼上楼下乃至千里之外的人们交流，因此毫不夸张地说，网络改变了我们的生活和工作方式，个人计算机的联网也成为必然趋势。

可是问题并不是“联网去”那么简单，如果鼠标轻轻一点，就可以自由自在地享受高速的信息交流，而且不用担心安全的问题，那么网络工程师和电信运营商就只能失业了。我们这里不打算介绍复杂艰深的网络专业知识，但是为了更好地理解 NT 及其新生代产品 Windows 2000，虽然本书以讲述 Professional 版本为主，而且 Server 版本更高深一些，但二者一脉相承，适当了解微软的网络解决方案，对 Professional 版本的配置及理解都会更上一层。

本章内容包括：

- 网络管理模型
- 域的组成
- 域的创建和管理
- 多域结构

7.1　网络管理模型

长期以来，网络开发人员对网络管理方案倾注了很高的热情，如何更方便、更有效地组织和管理网络资源，一直是人们关注的焦点。随着网络规模越来越庞大，在管理上下的工夫就得越来越大。我们现在就来看看当今的一些网络管理是如何进行的。

7.1.1　工作组模型

局域网中的一种模型是工作组模型。这种管理方案十分简单，就是用网络把许多计算机相连接在一起工作就行了（当然，我们这里考虑的是宏观的相连，具体联网时还要考虑网卡，网线、协议等设置）。最原始的联网，比如两台计算机的相连应该就是从这种工作组的形式开始的。

在这种工作模式下，所有计算机是平等的，所以用对等工作组来描述可能会更容易让人理解。回忆以下我们在 Windows 95 中大量地通过“网上邻居”使用其他计算机上的应用程序，就更能体会对等的含义。对等意味着每台计算机既可以为网络上其他计算机提供资源，也可以使用其他计算机的资源，只要有足够的权限就可以了。

初看起来，这没有什么不好，只要允许，就可以方便地使用资源，也可以十分慷慨地把自己的资源供给共享。而且这种连接简单易行，基本无需管理。但是当网络规模增大时，将会出现许多难以解决的问题。

首先，随着计算机的增多，有用的资源也随之增多，这时查找资源的工作将变得越来越困难，缺乏条理的组织使得工作很没有效率。

其次，由于每台计算机上都要保存可以访问自己资源的用户信息，包括用户名，密码以及访问权限等，也就是要有自己的账号数据库，这将是资源的巨大浪费。更麻烦的还不在此，用户将很快被淹没在膨胀的网络中，让我们来举个简单的例子：假设有一个用户需要使用其他机器上的资源，包括 A 计算机上的应用程序，B 计算机上的共享文件夹，以及 C 处的打印机，那么他就必须同时记住登录 A，B，C 的密码，时间在不停的登录、注销、再登录、再注销中流逝。此外，当密码过期后，需要设置新的密码，不同计算机上的新旧密码很快就会使人晕头转向。这还只是 3 台计算机，设想一下一个公司里的计算机的数目，恐怕没有人不会焦头烂额。

用户的管理也是一件十分头疼的事，每增加一个用户，各台计算机就应该开始为设置他的权限而忙碌；而

新增用户也不轻松，需要记住众多的密码，这些都很容易让人失去享受资源共享的乐趣。如果要把用户组织起来分配权限，那么建组的依据是什么呢？这也十分棘手。

还有其它许多问题，比如共享数据丢失和移动的问题、文件备份的问题、安全性的问题等等都不好解决。关键就在于：对等工作组中，每个人既要管理别人，又同时接受别人的管理，整个网络将十分混乱无序。因此，对等工作组只适用于小型的，没有大量数据流动而且没有重要资料的环境，在一个大的公司里采用对等工作组管理网络简直就是一场灾难。

7.1.2　客户——服务器模型

当完全的自由主义行不通时，就需要加强管理的力度。为工作组设立一个服务器是一个好办法，这时候原来的工作组里的计算机就成为客户计算机。

客户－－服务器模型是一种有效的工作模式。服务器上存放了所有用户的账号信息，服务器上提供共享资源，包括共享文档、打印服务、大型数据库管理等等服务，这时用户只要登录到服务器上，就可以向服务器发出资源请求，服务器负责响应客户的请求。

使用单一服务器的优点首先是资源易于管理，用户需要使用某种资源时，无需像在对等工作组一样遍历整个网络去寻找资源，只要登录到服务器上去就可以了。此外，可以在这台单一的服务器上建立一个账号数据库，更改密码可以在这个数据库上得到统一、及时的更新，这样一来对用户账号也可以很方便地统一管理密码和权限信息。

虽然还比较简单，但毕竟一定程度上有效的管理已经可以实现了。这时可以设立管理员，负责管理用户账号，实施统一的账号策略，监督网络的运行，优化系统性能，并对重要数据进行备份等管理工作，使系统能够稳定、有序地运转。

用户享受管理的好处之一是上面所说的可以方便地查询资源，还有很重要的一点是只需要一个用户账号和密码就可以登录，无需牢记不同的密码，也不用忍受无休止的登录、注销的等待。这样客户工作站完全省去了管理的职能，只需要安心工作就可以了，所有的管理交给服务器去完成。而且统一的账号管理也大大提高了网络的安全性。

但是，这种单一服务器的工作模式也有相当大的局限。由于需要管理所有的用户账号信息，以及支持所有网络共享资源，这就给服务器带来了相当大压力，对服务器的性能也提出了相当高的要求。万一服务器出了故障而无法登录，整个网络将陷于瘫痪。另外，当用户和工作站数目增加时，需要不断提高服务器的性能；这个数目继续增长时，一对多的局面将很难维持下去，就会迫使第二台服务器的加入来改变这种局面。事实上，在比较大的网络里，处理电子邮件服务和大型 SQL、Oracle 数据库需要消耗大量的系统资源，用单独的一台服务器进行资源管理是比较可行的办法。

这时问题就逐步暴露出来了，用户需要在不同服务器上登录，以使用不同服务器上的资源，这样用户就必须清楚资源的分布，另外用户必须有不同服务器上的账户名和密码。和对等工作组类似，要保持不同服务器上密码的一致是非常困难的事情。现在情况已经有点像对等工作组的情形了。而且，管理多台服务器也是相当繁重的任务。那么，能不能既用多台服务器来容纳众多的共享资源，又只用一个账户呢？答案是肯定的。我们来看看更合情理的管理方案。

7.1.3　域

Windows NT Server 采用了域（Domain）的网络管理手段。域中包括了众多的工作站和一定数目的服务器，并且使用仅有的一个安全数据库，处理多服务器间共享安全机制的问题。

域的最显著特点是用户密码的唯一性。用户使用一个域账号，只需要一次登录验证，就可以登录到域中，进行网络浏览并使用权限保障的共享资源。由于大型网络上可供共享的资源很多，而且出于更可靠的考虑，域中采用多台服务器来管理资源，这有点像对等工作组中资源分散的情形；域仍采用服务器的管理模式，这又是单一服务器模式的强化。域兼有对等工作组和单一服务器的特点。

域具有比以上二者都更强的可管理性。服务器在域中扮演重要角色，这是对等工作组混乱无序的状态所无法比拟的，另一方面，域又不像单一服务器那样大权独揽，集中控制。域采用多台服务器共同管理网络资源，并有更强的可扩充性。

需要注意的是：域并非如想象的那样松散，只是把原来单一服务器的功能分散给多台服务器如此简单。域中的不同服务器并不是没有区别的。在这些服务器中，有主域控制器（PDC），备份域控制器（BDC）以及独立的服务器（或叫成员服务器）。虽然都可以管理共享资源，但作为最重要的安全信息，只有主域控制器可以掌握。主域控制器中组织了所有用户、组账号以及安全设置等数据，集中存放在 PDC 的计算机目录数据库（Directory Database）中，这样虽然资源分布在多台服务器中，但用户确实只需要一个用户账号就可以登录访问所有服务器上的资源了。

尽管有多台服务器，但域中只能有也必须有一台主域控制器，以避免安全信息的混乱。同时，作为主域控制器的强有力的支援，备份域控制器也在管理中发挥相当大的作用。首先，备份域控制器分担了相当规模的网络资源共享管理工作，防止了所有用户都到主域控制器申请资源而造成的网络堵塞；其次，备份域控制器提供了主域控制器中安全数据库的备份，防止了最重要信息的丢失，由于存放有账号信息，用户也可以在备份域控制器中登录，这也给主域控制器减轻了相当大的负担。正因为备份域控制器的重要性，虽然域中可以不必设立备份域控制器，但稍具规模的网络中，备份域控制器都是必不可少的，而且往往不止一台。

域中还有相当数量的独立服务器，可以提供文档、打印、应用程序等不同方面的服务，这使得网络的工作更有效率，并且很容易得到扩展。

由于管理方案的层次化，使得整个网络更有条理，可以分配不同级别的有管理功能的用户，并增加磁盘备份，UPS 等工具，这样也减轻了管理员的负担。

从上面可以看出，域是一种比较成熟的网络管理方案，整个网络是在有组织的控制管理之下运行的，管理不仅在单个服务器上进行，而且是在整个网络上都可以有效的管理，管理员和用户都可以十分方便地工作。

域的一个不足之处是：和对等工作组一样，资源的定位不很方便。由于采用简单的网络浏览方法，而多个服务器上都有共享资源，这增加了资源查找的难度。用户仍然需要记住不同服务器上有什么不同的资源。但是，域的管理手段已经在 Windows NT Server 4.0 中给人留下了深刻的印象。

7.1.4 目录服务

在域中，登录后可以访问所有服务器的资源，但域没有提供帮助用户定位网络资源的办法，用户如果不熟悉网络资源，很容易迷失在浩瀚的信息当中。目录服务是一种寻找资源的全新机制。设想打开一本书，我们最常做的事首先应当是浏览一下目录，看看这本书有些什么内容，然后根据目录打开我们想要理解的章节。目录服务与此类似。当“打开”一个网络目录，你可以方便快捷地找到需要的资源，而不必关心资源位于哪台服务器上。

可以想象，目录服务将大大简化网络，特别是大型网络中的资源利用。在 Microsoft 的 Windows NT 4.0 及以前的版本中，没有提供目录服务，而作为网络操作系统的另一杰出代表，Novell 的 NetWare 4.0 服务器提供了 Novell 的目录服务 DNS（Novell Directory Services）,实现了包容网络上所有资源的分布式数据库并提供访问资源的途径。在新的 Windows 2000 Server 中推出了崭新的活动目录服务（Active Directory），这是一个运行在 Microsoft 域结构上的目录服务，包含了所有网络对象。用户只要一次登录，就可以访问许可的资源，并且可以简单地在目录将导航和选择。由于提供了直观的资源对象体系，对用户的使用和管理员的管理都提供了方便。

为了设置一个目录，至少需要一个 Windows 2000 Server 作为域控制器，通过服务管理器创建和管理这个目录。

7.2 域的组成

作为 Windows NT 网络操作系统的重要概念，我们有必要了解域的工作模式，为此首先了解一下域的组成。

7.2.1 主域控制器

如前所述，域控制器就是一台运行 Windows 2000 Server 的计算机，通过它管理域用户对网络资源的访问。而主域控制器（Primary Domain Controller，PDC）就是域控制器中最重要的角色。

域的最基本需求是主域控制器。实际上，创建主域控制器的过程就是创建域的过程，主域控制器建立后，一个新的域就建立起来了，从这个角度说，一个 PDC 就代表了一个域。主域控制器的重要性源于它控制和管理

着所有可被域识别的用户和组账号及权限信息，这些信息组织在一个称为 SAM（Security Access Manager）的安全数据库中。用户登录时，就必须在 SAM 数据库中验证用户名和密码。

只有在主域控制器中可以修改 SAM 数据库的安全信息，包括建立、修改、删除用户账号，建立、修改、删除域中的全局组和属于自身的本地组，修改用户和组的权限，以及修改账号规则和密码规则。

7.2.2　备份域控制器

如果网络发生灾难，最严重的，比如主域控制器瘫痪并导致 SAM 数据库的损坏，这时如果没有安全信息的备份，那么域也就无法工作了。幸亏域中还有其他域控制器，那就是备份域控制器（Backup Domain Controller，BDC）。

网络中往往有不止一台的备份域控制器，用来存放主域控制器中安全信息的备份，实际工作中，主域控制器采取同步的手段，不断给每个备份域控制器一份 SAN 数据库的备份，这样一来 SAM 数据库就有多个备份了。

备份域控制器除了为主域控制器提供账号数据库的备份，还可以帮助主域控制器进行用户登录身份验证。设想一下每天早晨上班的情形，公司职员纷纷打开电脑，登录到域中并开始新的一天工作，要处理如此密集的登录请求，如果只有主域控制器负责身份验证，其高峰期的繁忙程度是可想而知的。备份域控制器由于存放有 SAM 数据库的备份，可以在这时候助主域控制器一臂之力，也不至于白白浪费资源。此外，当主域控制器由于故障不能启动时，用户照样可以通过备份域控制器登录。

尽管如此，备份域控制器还是不能取代主域控制器的地位。虽然 BDC 中有用户账号信息，但只有在主域控制器中才能管理这些信息，比如添加、修改和删除用户和组等等，再把修改后的信息备份到备份域控制器中去。不能在备份域控制器中进行以上操作。

备份域控制器的另外一个重要用途是：当主域控制器无法工作时，备份域控制器可以升级为主域控制器。必须牢记：尽管可以有多个备份域控制器，但主域控制器永远只有一部。

7.2.3　独立服务器

在域中，并不是所有的服务器（Server）都要配置成域控制器，也存在有运行 NT Server 或者 2000 Server 的独立服务器。

独立的服务器（Stand-alone Server）也可以称为成员服务器(Member Server)，与域控制器不同的是，它不存放域的账号数据库，当然也不负责域成员的登录审核。这时如果独立服务器不加入域中，那么它就只有自己的用户账号数据库，无法使用任何域内的用户账号；如果加入了某一个域，那么可以使用所属域内的用户账号。

独立的服务器照样可以提供共享资源，可以把它当作是提供应用程序、文档或者打印服务的服务器。那么为什么要设立独立的服务器呢？可能有这样一些理由：

（1）这是专用的大型服务器，提供数据库服务，电子邮件服务等大型工作，这时不希望把资源浪费在审核用户登录上。

（2）独立的服务器由于不存放域的 SAM 数据库，可以非常方便地离开一个域，转到另一个域中。而域控制器就没有这个优势，要改变它的域，必须重新安装 Windows 2000 Server.

除了服务器，域中可以支持多种客户工作站，比如 Windows 2000 Professional、Windows NT Workstation、Windows95、 Windows98、Windows 3.x，MS-DOS 等客户软件。

7.3　域的创建和管理

7.3.1　域的创建

7.3.1.1　主域控制器

如果选择安装主域控制器，需要为新域制定一个域名。域名必须唯一，安装程序会查找是否有相同的域名，这需要一段时间。如果域名合乎要求，系统将创建一个域管理员 Administrator 账号，并要求输入账号密码。尽管空的密码可以接受，但出于安全性考虑，强烈建议明确指定一个密码。同时请小心，在没有添加管理员组其他成员时，千万不要忘记 Administrator 账号的密码，否则将无法对域进行管理，此时只能重新安装 Server。

7.3.1.2 备份域控制器

安装备份域控制器必须以域管理员身份登录，安装程序会要求输入此 BDC 要加入的域名，并要求输入域系统管理员账号名与密码。

需要注意的是：域控制器建立后，主域控制器可以与备份域控制器互换角色（主域控制器可以降级为备份域控制器，反之亦然），但它们不能再变成独立的服务器。

7.3.1.3 其他成员

如果是 Windows 2000 的计算机，可以以工作站（Professional）或者服务器(Server)的身份加入到域中。在安装 Windows 2000 时，输入所要加入的域名，并在域中建立一个计算机账号就可以了。

如果是 Windows95、 Windows98、Windows 3.x、MS-DOS 等作为工作站成员，则不需要加入域，但要配置适当的通信协议，以便能访问 NT 网络的资源。

7.3.2 域的管理

7.3.2.1 同步

如前所述，SAM 数据库首先是在主域控制器中进行改动，再备份到备份域控制器当中，这个过程叫做同步。同步是域能稳定工作的有力保障。

通常系统每隔 5 分钟（这个值由注册表决定，可以调整）会要求所有备份域控制器进行同步操作。如果备份域控制器不在网上，就有可能丢失部分信息。另外，主域控制器对 SAM 数据库的修改会记录在修改日志中，修改日志的存储空间是有限的，缺省时大约可以记录 2000 个操作，当操作超过 2000 时，旧的修改信息会被删除而为新的信息腾出空间。如果同步操作相隔的时间适当，比如通常 5 分钟不会有超过 2000 个修改操作，这时备份域控制器可以完全同步。但如果这个间隔设置不妥，备份域控制器也会丢失信息。

当有修改信息丢失时，备份域控制器会被要求进行完全同步操作。完全同步会造成一定的延时，这在通常具有 10Mbit/s 以上的高带宽（高带宽比低带宽在同样时间内能传送更多的信息）的局域网中也许问题不大，但对相对带宽较低的广域网（WAN）中，可能会造成网络堵塞的现象，所以应该避免频繁的完全同步操作。为此，可以采取增加修改日志大小或者缩短同步间隔时间的方法。

7.3.2.2 域控制器角色互换

由于主域控制器在域中的重要作用，当主域控制器由于性能无法满足要求，或者有故障而较长时间内无法连接到网络上，或者干脆毁坏时，应当把备份域控制器升级为主域控制器。

备份域控制器的升级有两种情况：主域控制器在网上正常工作以及不在网上的情形。这两种情况有些区别。当前一种情况，主域控制器在网上时，选择某一备份域控制器升级为主域控制器后，由于域中不能同时存在两台主域控制器，此时原有的主域控制器将自动降级为备份域控制器，同时最新的账号信息及安全设置将复制到新的主域控制器中。需要注意，升级过程中，系统会自动关闭用户与域控制器的连接，因此最好先要求已登录的用户注销。

后一种情况，当主域控制器不在网上时，仍可以将备份域控制器升级为主域控制器，但此时如果安全信息尚未完全同步，由于原主域控制器处于脱机状态，无法复制，此时尚未更新的数据将丢失。如果升级完成后，原主域控制器重新连接，由于域中不能同时存在两台主域控制器，此时可能造成一定的混乱。原主域控制器无法连入域中，而且显示为断线状态，要使其继续工作，必须降级为备份域控制器。

7.3.2.3 安全标识符

日常生活中，我们往往是通过名字来识别所认识的人，但如果有朋友改了名，我们不会因此不认识这个人，从另一个角度看，如果有两个人有相同的名字，我们也不会将二者混为一谈。这是因为名字仅仅是一个符号，而我们是从外表、性格等更深层的特征来理解别人的。同样的道理，域名和计算机名帮助用户和管理员方便地识别域和计算机对象，但这并不是它们的本质特征，系统也不理解这些名字。在系统内部，用一个安全标识符还认识和区别每一个不同的对象，这些对象包括域、计算机、用户以及组。在第 4 章中谈到建立和删除用户和组时也提过安全标识符（SID），它实际上是一个很长的数字，当新的对象建立时由系统创建以加以识别，不可能有两个不同的对象共享一个相同的 SID 号。

创建主域控制器的同时也就创建了一个新的域，系统为这个域设立一个 SID 号，在向域添加备份域控制器时，会用域的 SID 号与备份域控制器的 SID 号共同表明其身份。

假如域中的主域控制器不能使用，正确的应对措施是把备份域控制器升级为主域控制器，但如果采取这样的做法：使用一台新的 Server 作为主域控制器，并为其设置相同的域名和主域控制器名，将是错误的。尽管名字都一样，但新的“主域控制器”并不认识域中其它备份域控制器和工作站，同样，原有的备份域控制器和工作站也不认识新的主域控制器。原因就是系统为新建的域分配了不同的 SID 号，而原域中的计算机还遵循着旧域的 SID 号。

7.3.2.4　更改域名

更改域名是允许的，因为虽然有了不同的名字，但使用相同的 SID 号，因此不会造成混淆。要更改域名，只要在“控制面板，系统，网络标识”中更改就可以了。

但这时更改域名并不像更改用户名或更改组名那么简单，重命名域，需要逐个地对域中的计算机进行重命名。首先是主域控制器，然后是备份域控制器，再到其他服务器和工作站。这是因为，用户和组都是相对独立的，改变名字后就整个改了过来。但域的情况不一样，主域控制器改名后，可以理解为建立了一个新的域，但此时旧的域仍然存在，系统无法确定备份域控制器需要作的是升级为主域控制器以维持旧的域，还是跟随原主域控制器转到新的域。所以这时要手工改变备份域控制器的域名。此后工作站和其他服务器也依此作域名转换。

此外，如果是多域结构，且原域与其他域有信任关系，那么这些信任关系也要重新确立，可见，域的更名不是一件简单的事。

7.3.2.5　域的容量

域的容量并不是无穷大的。如果有不同的部门加入，大批的用户和组使管理者感到力不从心，就可以考虑增添新的域。

从理论角度上说，域的容量与 SAM 数据库大小有关。所有管理对象的信息都存放在 SAM 数据库中，而且不同类别的对象在数据库中所占的空间不同，比如每个用户账号占用 1K 空间，每个客户计算机账号占用 0.5K 空间，每个组账号占用 4K 空间。由于每次登录时，整个 SAM 数据库要被调入域控制器的内存当中，因此 SAM 数据库的容量越大，对域控制器的硬件，特别是内存的要求就越高。

微软经过测试后，认为一个 SAM 数据库的容量不应超过 40MB 大小，40MB 的数据库相当于将要处理 26，000 个用户，26，000 台客户机以及 250 个组。（26000×1+26000×0.5+250×4=40，000）。可以看出，这是一个相当大的规模。在实际工作中，微软的推荐是域控制器支持的用户数量不应超过 5000。考虑到网络高峰期（比如每天早晨上班时登录）的网络堵塞，这个数目或许应该更小。

7.3.2.6　工作站加入域

许多用户使用的是 Windows 2000 Professional，这个版本相当于 Windows NT Workstation 4，要与域通信时，应当作为域的工作站加入域。

可以用以下方法加入或者改变工作站所属的域：

① 打开开始菜单，选择设置，控制面板。

② 打开系统程序，并选择网络标识选项卡，将显示计算机名和网络标识，如图 7-1 所示。

图 7-1　网络标识

③ 单击更改按钮，将出现网络标识向导对话框，按照提示，如果您想连接到域中，应该选择本机是商业网络的一部分，用它连接到其他工作着的计算机，以及公司使用带有域的网络。此时向导会提示您收集域和账号信息，包括用户名、密码、计算机名、用户账号域以及计算机的域。之后出现如图 7-2 所示的对话框。系统将查找指定的域，并要求加入域的系统管理员账号和密码。正确输入后，重新启动登录时，输入域名和用户信息即可。

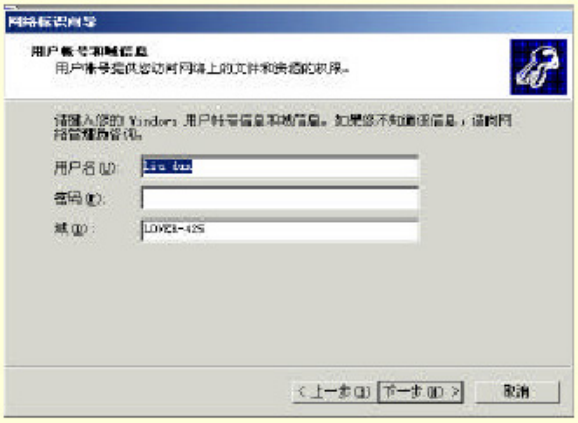


图 7-2 输入账号信息和域信息

此外，也可以在图 7-1 的网络标识选项卡中，直接单击高级按钮，在如图 7-3 的标识更改对话框里输入计算机隶属的域。

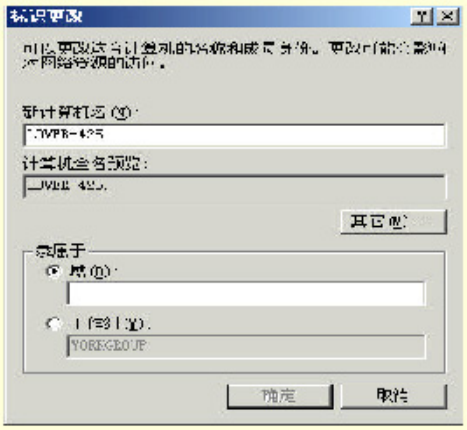


图 7-3 标识更改以加入域

如果要求域管理员预先将计算机加入域中，要确保添加的计算机名和实际计算机名吻合。

7.4 多域结构

上面所说的是单域结构。由于一个域可以支持上千的用户，对大多数的组织已经足够了。但当有某些部门需要与其他部门共同工作，而又希望保持自己相对的独立性时，多域方案可能是解决的办法。微软的 Windows 网络提供了灵活多变的组网方案，它们是：

- 单域方案
- 单主域方案
- 多主域方案
- 完全信任域方案

其中单域方案是最基本的组网方式。其他都属于多域的范畴。

7.4.1　信任关系

多域之间通过一定的关系相合作，这种关系叫做信任关系。我们首先来举个信任关系的例子。A 和 B 是公司里的两个不同的部门，职员甲属于部门 A。现在甲受命到部门 B 查阅存放在那里的一些工作资料，虽然是不同的部门，但在同一公司中，这些资料对 A 部门的工作是有益的。此时，B 的检查机构就会询问甲的身份。甲回答是 A 部门的，或者出示 A 提供的证明。这样，部门 B 给 A 打电话查询或查看甲出示的证明，如果确定甲是属于部门 A 的，就会允许甲查阅资料。

为什么甲不属于部门 B，而仍能查阅 B 的资料呢？原因是 B 信任 A 的职员，或者更大胆地说，B 信任 A。这就可以理解为一种信任关系。

现在假设部门 A 中建立了自己的域 A，部门 B 也建立了自己的域 B，那么现在的情形就是域 B 信任域 A，这样域 A 的用户甲即使在域 B 中没有账号，但仍可以在域 B 中登录，访问共享资源。此时，A 叫做被信任域（Trusted Domain）,B 叫做信任域(Trusting Domain)。建立了信任关系后，被信任域的用户账号就可以在信任域中使用，或者说被信任域允许信任域共享它的安全数据库（SAM 数据库）。信任域只要给被信任域上的用户和组分配合适的资源访问权限，这些用户和组就可以在信任域上登录，并使用共享资源，就像上面例子中的职员甲一样。

7.4.1.1　单向信任关系

信任关系可以是单向的，也可以是双向的。在单向信任关系中，Trusting 域信任 Trusted 域，反之不成立，也即 Trusted 域不信任 Trusting 域。这种关系可以用下页的框图来表示。

假设用户甲已经登录到 Trusted 域上，甲此时希望使用 Trusting 域的资源。由于 Trusting 域信任 Trusted 域，可以使用 Trusted 域的安全信息，这样 Trusting 域就可以审阅甲是否通过了 Trusted 域的认证，同时还可以获知甲的账号标识和组成员身份。另一方面，由于在单向信任关系中，Trusted 域不信任 Trusting 域，所以 Trusting 域的用户无法使用 Trusted 域的资源。

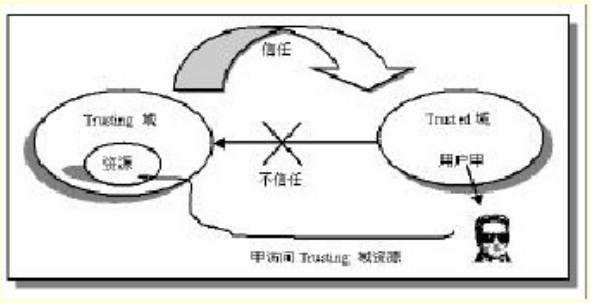


图 7-4　单向信任关系

7.4.1.2　双向信任关系

双向的信任关系给予双方更大的透明度,这时两个域之间相互信任,双方都同时既是 Trusted 域又是 Trusting 域。两个域的系统管理员都可以为对方的用户分配本域的资源访问权限。

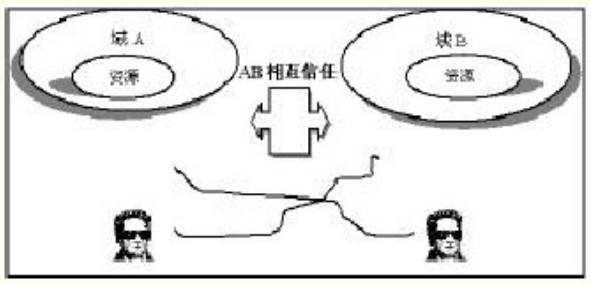


图 7-5　双向信任关系

7.4.1.3 信任关系不能传递

有必要提醒读者的是：信任关系不能传递。

在如图 7-6 中，域 A 信任域 B，域 B 信任域 C，但不能由此推断出域 A 信任域 C。如果域 C 需要得到域 A 的信任，必须明确指定二者间的信任关系。

7.4.1.4 信任关系的建立和终止

建立信任关系并不难，但请注意设置的先后顺序：

（1）被信任域（Trusted Domain）允许信任域(Trusting Domain)信任它。

（2）信任域信任被信任域。

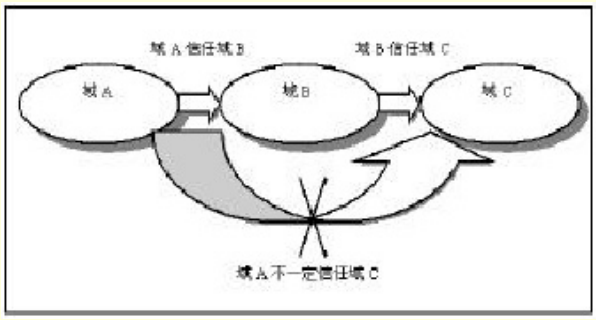


图 7-6 信任关系不能传递

当要终止信任关系时，应当先使正在使用共享资源工作的用户退出，并且在信任和被信任的双方都要实行删除工作。

信任关系为多域之间的配合工作搭起了坚固的桥梁，如果没有信任关系的存在，那么各个域之间是孤立隔绝的，这也不符合实际工作的情况。

7.4.2 全局和本地

全局和本地是多域模型中的重要观念。大多数第一眼看到这两个词的朋友都不会感到费解，尤其在有了多域的概念后。

正如想象中的那样，全局对象具有全局的作用范围，这也就是说，全局对象可以在所有域中使用，而不仅仅适用于创建其的域。与之相对应的，本地对象只具有本地作用范围，仅适用于创建它的域。

在信任关系中，我们已经看到，被信任域（Trusted Domain）的用户可以在信任域（Trusting Domain）中登录。这些被信任域中的用户就可以理解为在被信任域中创建的全局用户。如果计算机不是域中的一部分，那么创建的用户将是本地用户。

在域中缺省建立的用户账号是全局用户账号，这样，如果该域被其他域所信任， 那么，这些全局用户就可以被信任域引用。事实上，这也是多域模型中常使用的思维。

在用户和组一章中已经讲过，可以采取为单独的用户账号分配权限的办法，但更值得推荐的是使用组将用户组织起来统一分配权限。现在我们来看看全局组和本地组。它们的理解需要用心体会，我们先来帮助建立一个感性的认识。

仍然考虑信任域 A 和被信任域 B 的模型。为了方便管理，需要建立一个组，将被信任域 B 中需要使用信任域 A 资源的全局用户组成一个全局组。当然，域 A 的管理员可以为域 B 中全局组分配权限，但这样做需要在两个域中分别维护账号和密码。

实际上常采用这样的办法：在信任域 A 中建立一个本地组，然后包含被信任域 B 中的全局组，或者说，引入域 B 中的全局组。下面我们用框图说明。

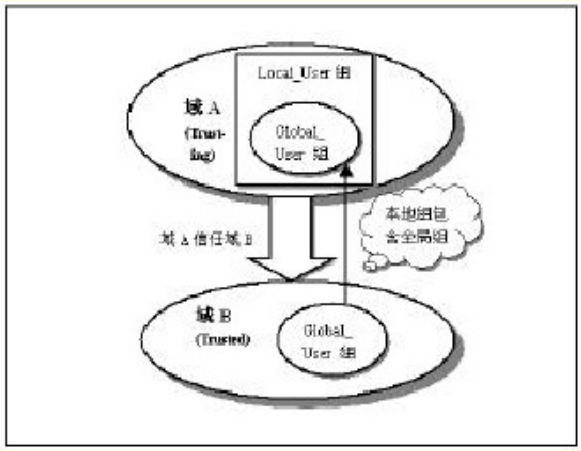


图 7-7　全局组和本地组的关系

图 7-7 中，Local_User 组是信任域 A 中的本地组，只能在创建它的域 A 中使用；Global_User 组是被信任域 B 中创建的全局组，可以在其他域中使用。为了使 Global_User 组在域 A 中能合理地使用共享资源，在域 A 中创建一个本地组 Local_User 组，并将 Global_User 组“输入”到 Local_User 组中（或者说在 Local_User 组包含 Global_User 组），然后为 Local_User 组分配权限，这同时就相当于为 Global_User 组分配了权限。这样一来，被信任域 B 中属于全局组 Global_User 组的用户就具有了信任域 B 分配给其本地组 Local_User 组的权限了。

由此可以看出，本地组可以包含全局组，但反过来就不行了，也就是说，全局组不能包含本地组。从逻辑上分析，因为全局组的创建是使其适用于其他的域，因此包含到本地组中就可以享有本地组的域权限；而本地组的适用范围是创建它的域，如果它能被其他的全局组所包含，则意味着它可以在其他的域中使用，这是不合逻辑的。

在 Windows 2000 Professional 中不能创建和维护全局组。但如果 Windows 2000 Professional 加入了 某个域，那么可以允许域中的全局组加入其中的本地组，并给全局组分配权限。

具体地说，全局组是在一个域中的域控制器中建立的，全局组

- 只可以包含所属域内的用户
- 不能包含其他域中的用户，也不能包含其它的本地组和全局组。

而本地组：

- 可以包含本计算机中的账号
- 可以包含本域中的用户账号和全局组账号
- 可以包含其他被信任域中的用户账号和全局组账号
- 不可以包含其他的本地组

域控制器给每个域中的本地组分配权限，当有其他域的全局组加入到此本地组中，将有此本地组的权限。

7.4.3　单主域结构

现在我们开始了解多域模型。

在多域协同工作时，容易想到的是建立一个域，用以处理所有的用户的身份验证。这个域就叫做主域（Master Domain）。其他的域则用来进行提供共享资源及其他内部的工作，这些域可以叫做资源域。主域专管处理登录，其他资源域则负责各自相对独立的工作，这样它们就不用分神处理登录，从而提高了工作效率。同时为了使在主域登录的用户能够访问资源域，所有资源域必须信任主域。

这种工作模式可以用下面的框图表示：

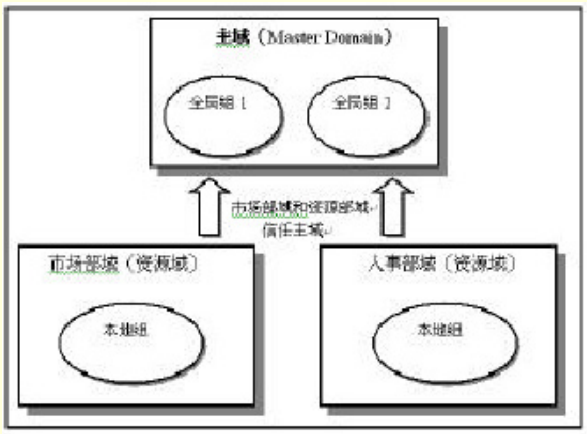


图 7-8 单主域模型

由于各个资源域信任主域，可以在主域中创建全局组，并引入到资源域的本地组中。甚至在资源域中都不用设立本地管理员进行本地管理，只要在主域中建立 Domain Admins 全局组，并用各资源域的 Administrators 本地组包含 Domain Admins 全局组，这样 Domain Admins 全局组的成员就可以对各资源域进行管理了。还可以将主域中的 Domain Users 全局组包含到各资源域的 Users 本地组，道理同上。

在各个部门希望独立管理本部门的系统情况下，仍然可以在自己的资源域中设立本地的 Administrators 组，并且不包含主域中的 Domain Users 全局组，这时候系统管理员就需要在各自的域进行登录。或者采取另一种办法，将主域中特定的一些用户账号添加到资源域中的本地组当中，而不是将 Domain Users 全局组添加到本地组中。这样，仍旧只需要在主域登录就可以了。

另外，在各个部门的域当中，仍可以建立一定的信任关系，以便部门之间的协同工作。

单主域模型的优点是：

（1）账号集中管理维护。

（2）各部门分散独立管理。

（3）部门域可以很方便地为主域全局组分配权限。

（4）可以方便地扩展，当增加部门时，只需简单地将新域设置为信任主域，并设置相应的用户权限即可。

7.4.4 多主域模型

当公司里组建的是真正的大型网络时，并有庞大的用户群时，只有一个负责登录的主域也许会不堪重负。这时候需要增加主域，以分担处理登录带来的压力，这就是多主域结构。

多主域结构是单主域结构的扩展。

这时候仍然需要的是各个资源域必须信任每一个主域，这将使每个主域都能进行登录的身份验证。同时主域之间也应当相互信任，这时多主域模型中兼有单向信任关系和双向信任关系。下面我们仍是来看模式框图。

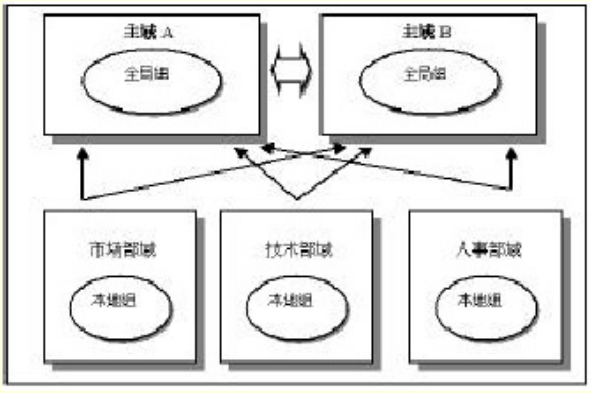


图 7-9 多主域模型

图中各箭头仍表示信任关系。

与图 7-8 的情形相比，信任关系明显增多了。首先各个资源域必须信任每一个主域，其次各主域之间也应当相互信任。假设原有 m 个主域，n 个资源域，那么新增一个主域，则新增的信任关系是：$m+n$。

为了能够对各域进行管理，各域全局组和本地组的设立如下：主域 A 和主域 B 的 Domain Admins 全局组分别是各自 Administrators 本地组的成员；此外这两个主域的全局组又应该都是各资源域的 Administrators 本地组的成员。

在多主域模型中，每个用户仍只需要一个账号。由于所有用户账号是在主域中保存的，这时候有不止一个的安全信息数据库（SAM 数据库）。

多域模型已经可以解决真正大型网络的问题。

7.4.5　完全信任域模型

微软还曾经提出过完全信任的域模型。这种模型最重要特点是：各个域相互之间有信任关系。与主域模型的区别在于：由于此时域之间都是平等的，事实上不存在主域，没有专门的域负责登录身份验证。

在完全信任域模型中，可以将各个域理解为不同的部门，它们有相对的独立性，但又希望协同工作，共享资源，并在任意两个域中建立信任关系，并且在它们当中没有统一的网络集中管理机构。这种域的模型可以用下图描述：

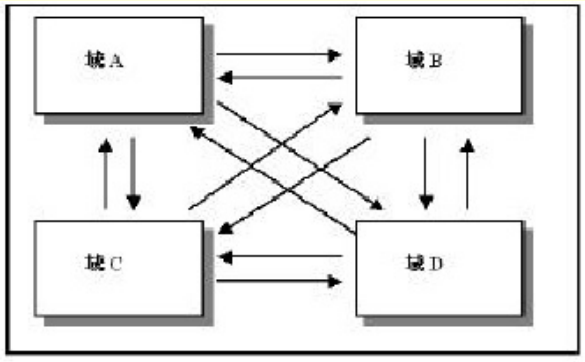


图 7-10　完全信任域模型

这个结构模型很容易让我们回想起工作组的网络管理模型。的确，由于缺乏统一的管理机制，整个域组织给人一种松松散散的感觉。主域不仅仅是统一负责登录，还可以进行账号规则、密码措施等的统一规划、以及系统维护、重要资料备份等工作。而在完全信任域模型当中，我们找不到这样的管理。系统的安全规划只能由各个域自行管理，而不同域间几乎是不可能完全一致的。总之，这不像是一个有机的公司下的各个部门在合力工作。由此导致的网络安全问题几乎是不可避免的。

另外一个缺点是太多的信任关系。我们再来做一个数学运算。假设有 n 个域，由于每两个域间都要建立一对（两个）信任关系，那么一共需要的信任关系是：$2\times[1+2+\ldots+(n-1)]=n\times(n-1)$个。假如有 4 个域，那么需要 12 个信任关系；如果再增加一个（5 个），那么就需要 20 个信任关系。而如果采用两个主域，3 个资源域，那么只需要 8 个信任关系（见图 7-9），再加上众多全局组和本地组的设立，实在是一件费力的事。

第 8 章　安全性介绍

网络的蓬勃发展也许是本世纪末最激动人心的革命。个人电脑虽然也在飞速发展，但无论 CPU、内存、硬盘还是显示器的性能有多么出色，在网络的威力面前都将黯然失色。今天，从学生寝室到规模庞大的公司企业，局域网正为人们创造着高速的数据传输。另一方面，Internet 的迅猛膨胀正在使我们的地球变得越来越像一个地球村，报告显示：每一分钟都有局域网或者主机（连网的计算机）与 Internet 相连。

比尔　盖茨不会忽视这个巨大的市场。正是这个原因，微软的操作系统，无论是 Windows 9X 还是 Windows NT，还是全新推出的 Windows 2000，都必须具有方便的联网功能。Windows 2000 支持各种流行的网络协议，只要装配有网卡，就可以很方便地实现计算机互联；如果再配置了调制解调器，找到合适的 ISP，就可以上网冲浪了（后面将有详细的联网介绍）。

但是在享受网络乐趣的同时，有一点是需要铭记在心的，那就是安全性问题。

本章主要内容有：

- 安全性概述
- Windows 2000 的C2 级安全性
- 登陆策略
- 账户策略
- 密码策略
- 注册表的安全性
- 其他
- 文件加密
- 安全模板及安全配置和分析工具
- 证书管理

8.1　安全性概述

事实上每个人即使没有联网，也需要维护自己的程序、文档、表格和设备免遭他人在非法情况下访问和使用，从而导致破坏，这就是安全性的问题。只是当用户的计算机联网时，这个问题尤其显得尖锐。作为一个公司或者企业的网络管理者，更有责任维护整个系统的数据安全，使其免遭损坏、盗窃或者误用。

首先要弄清楚：谁是需要注意的防范对象？在互联网中，有许多人经常攻击各种站点，他们以“黑客”的称谓为无尚的光荣。这些人中有些怀着各种政治或商业的目的，还有许多纯粹以进行破坏为乐趣。用户上网的时间越长，受到攻击的可能性就越大。如果是公司的网站，就更需要高度的警惕。

与外部攻击同时存在的是来自内部的威胁。说不清哪位雇员会心怀怨恨而试图获取公司的绝密数据，而那些天生有着强烈冒险精神和好奇心的人更应该被严格限制，无意识的破坏同样会带来严重的后果。

内部网络的安全性管理在有些企业没有得到应有的重视，这或许是因为细致的管理需要太多的精力和高昂的费用，或者是因为严格的管理对普通的职员带来这样那样的限制招致抱怨。然而当数据破坏或网络瘫痪的情况出现时，后悔就来不及了。作为网络的管理员，有责任提醒负责人安全的重要性，无论如何不能容忍管理松懈的网络存在。

与此同时，另一方面需要注意，矛盾的存在总是绝对的。过于严厉的管理有可能为绝大多数的用户带来工作的不便，从而导致效率的低下。现代的网络管理给管理员提出了很高的要求，必须经过周密的思考才能进行完备的计划。

Windows 2000 是一种先进的网络操作系统，它可以帮助系统管理员快速有效地控制、管理和监督网络的运行。

8.2　Windows 2000 的 C2 级安全性

有识之士在普通用户之前很早就表现了他们对计算机安全性的担忧。美国计算机安全中心（NCSC）提出了自己的安全性标准，对操作系统、网络构件及安全子系统进行了产品安全的等级评价，这就是所谓“桔皮书”。桔皮书的分类级别分为 A、B、C、D 级，Windows 2000 满足其 C2 级安全要求，下表对分类有进一步的说明。

表 8-1　安全性级别说明

级 别	说 明
D	最小安全要求
C1	慎重安全
C2	控制访问
B1	标记安全
B2	结构化保护
B3	安全域
A1	验证保护

在这个分类级别中，D 级是级别最低的，A 类是安全性最强的，而 B，C 级还有更细致的区分，其中 C2 的级别比 C1 要高，相应地在 B 类中，B1、B2、B3 的安全级别也不断提高。1995 年，微软的 NT 3.51 就通过了 NCSC 的 C2 级安全性审核，又比如 Oracle 公司的 Oracle7 也被评估为 C2 级的可信程序。

NCSC 的 C1 级别要求设置某些形式的控制，使用户能保护用户的私人信息，这一级别系统要求用户能够标志自己的身份（采用用户名以及密码），并由系统进行身份验证。系统需要维持用户以及密码数据的完整性，防止未授权用户的访问。系统还要求保证用户在自己职权范围内行事，不应该允许用户使用某种程序以避开安全机制。

C2 级安全性除了要求 C1 级别的所有安全机制外，还要求针对每一个用户准许或者限制他们对数据文件的访问，要求只能由授权的用户为当前没有访问权限的用户分配权限。C2 级别的安全性的另外一项要求是对象或者文件被删除后，任一部分不应该能被恢复。此外还要求提供完备的审核记录，以监督用户的各种行动。

C2 级安全性提出的要求以及 Windows 2000 的表现如下：

- **慎重控制**

  通过访问控制列表（Access Control List，ACL），实现针对具体用户的对象访问控制权限。对象包括文件、文件夹、进程、打印机等等。

- **对象再生**

  不能再生或恢复已经删除的对象。例如，任何 NTFS 分区的文件被删除后，都不能再恢复数据。

- **用户标识与身份验证**

  用户必须提供用户名和密码才能获准登录，系统将进行身份验证以判断用户是否是合法的。此外，登录时提供的用户信息将用于跟踪用户的活动，比如进行审核等。

- **审核**

  能够审核系统内所有的对象访问及有关安全的行动，而且只有具有一定权限的用户（比如系统管理员）能够查看审核信息。

读者可以发现，Windows 2000 对这些要求都作了相当严密的布置，上面提到的安全性都在 Windows 2000 的用户、账号等方面的管理中都受到了相当程度的重视

事实上，B、A 的安全级别比 C 级提出了更高的要求。读者也许会问：为什么 Windows 2000 不遵循更高的安全性要求呢？回答是：对大多数商业应用来说，C2 级的安全级别就是最好的了，别忘了对安全的要求越高，往往也就意味着工作效率的降低。除非要同政府机密打交道，否则不需要提出那些不近人情的要求。

8.3 登录策略

首先从登录机制来看看 Windows 2000 的安全性。

8.3.1 Ctrl+Alt+Del 登录

Windows 2000 同 Windows NT 一样，需要用户按“Ctrl+Alt+Del”键，才能打开登录窗口，输入登录所需的用户名和密码信息。

有一种叫做特洛伊木马（Trojan Horse）的程序，会通过仿造登录窗口的方法骗取用户输入登录信息，以此获得用户的用户名和密码，之后进入系统进行破坏。

也许许多人仍然记得在 MS-DOS 和 Windows 3.x/95 的时代，人们通过按“Ctrl+Alt+Del”键重新启动系统或者关闭某个程序，然而在 Windows NT 和 Windows 2000 中，通过采取“Ctrl+Alt+Del”键登录的方式，可以阻止模仿登录屏幕的程序。这种登录机制相当有效，因为捕获密码的特洛伊木马程序，几乎不可能写成同时按“Ctrl+Alt+Del”键。

也可以将系统设置成不需要按“Ctrl+Alt+Del”键才能输入用户名和密码，但考虑到系统的安全性，这点是必不可少的。

要设置用户必须按 Ctrl+Alt+Del 键以登录，管理员采用以下操作：

（1）双击打开“控制面板”中的“用户和密码”。

（2）选择“高级”选项卡。

（3）选中底部的要求用户在登录之前按“Ctrl+Alt+Del”键，如图 8-1 所示。

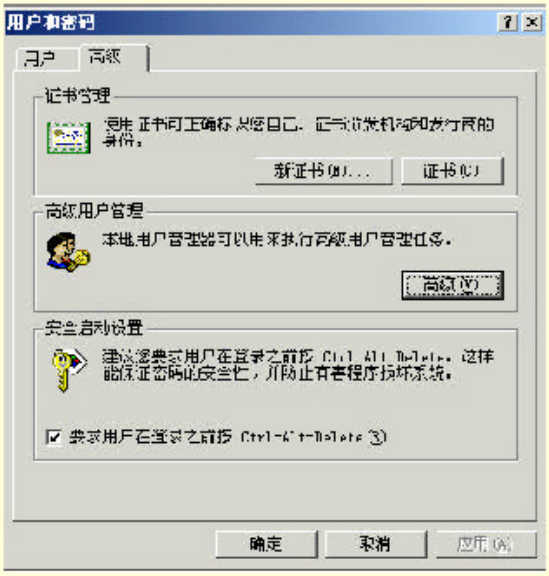


图 8-1 要求按 Ctrl+Alt+Del 键登录

8.3.2 DES 和 RSA 加密技术

用户的密码保存在 SAM 数据库中，并采取了先进的加密手段。

DES 加密的密码长 16 个字节，其前 8 个字节由密码的前 7 个字节计算产生，后 8 个字节由密码的后 7 个字节计算产生。

SAM 数据库中还存有第二个密码，与前者不同，这个密码使用 Unicode 字符集，区分大小写。这个密码采用 RSA 公共密钥密码的加密方法，这种加密方法是 70 年代末开发出来的，它也用来生成数字签名。

8.3.3 显示警告

有些人只是处于好奇心而猜测密码以图进入系统，如果在他打坏主意时，显示一个警告框是一个好办法，

可以通过修改注册表以达到在显示登录对话框时出现警告。方法是：

（1）在“运行”对话框中，输入“regedt32”运行注册表。

（2）选择以下键值：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon，如图 8-2 所示。

找到 LegalNoticeCaption 和 LegalNoticeText 两个键，分别为它们输入文本字符串（缺省情况下它们是空的）。LegalNoticeCaption 显示的是提示框的标题，而 LegalNoticeText 显示的是提示框的正文。

提示：缺省时，注册表是处于只读的状态，要修改注册表，请先清除它的只读状态。这需要管理员的权限。

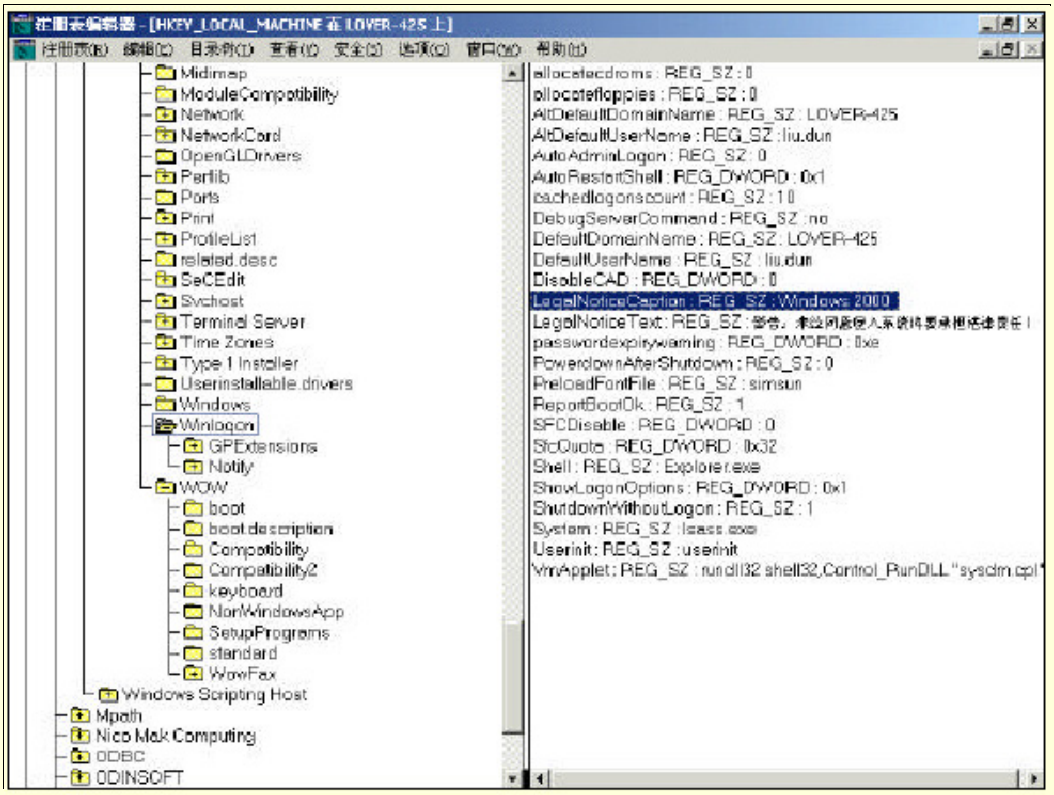


图 8-2　修改注册表中的键值

注意：你已经在修改注册表了！不要以为这是一件有趣的事情，注册表是系统得以正常工作的重要保证。错误的改动有可能使系统崩溃。

输入警告字符串类似图 8-3 所示。

图 8-3　输入警告字符串

8.3.4　不显示上一登录的用户名

用户或许已经习惯了登录对话框中显示上一登录的用户名，如果用户是再次登录，这样的确可以省去许多

不必要的麻烦，至少用户不必一遍又一遍地重复输入工作。

但是考虑到安全性的问题，这种设置并不可取。试想一下，当有陌生人来到机器前，按下 Ctrl+Alt+Del 键，在他面前出现上一登录的用户名，那么这个陌生人就可能根据用户名提供的信息（如果他认识那个用户的话），猜测这个账号的密码。因此，严密的安全设施应该禁止上一登录的用户名。

这一设置可以在管理控制台中执行。方法是：

（1）打开管理控制台。

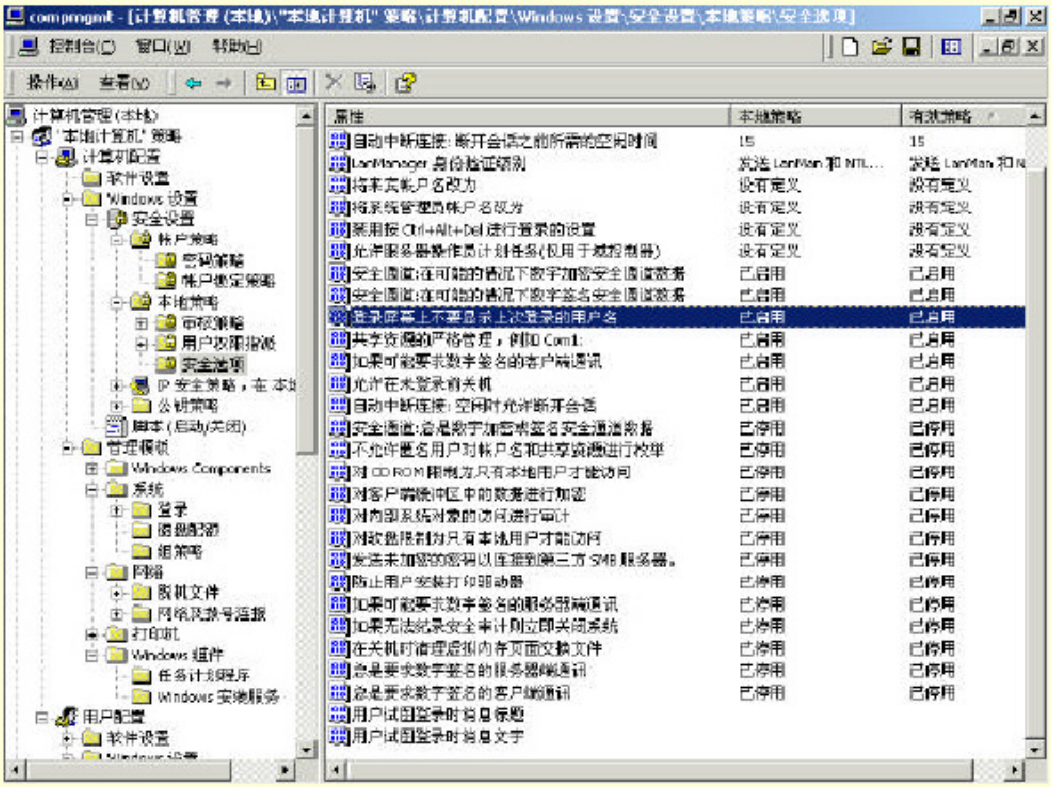


图 8-4 设置登录屏幕上不显示上次登录的用户名

（2）打开组策略，如果是本地计算机，启动的将是“本地计算机策略”。

（3）依次打开“Windows 设置”→“安全设置”→“本地策略”→“安全选项”。

（4）在如图 8-4 所示的大屏幕中，找到“登录屏幕上不要显示上次登录的用户名”这一设置，缺省时，这一策略没有启用。

（5）单击右键，选择“安全性”，在如图 8-5 中，选择“启用”单选按钮，启用不显示上登录用户名策略。

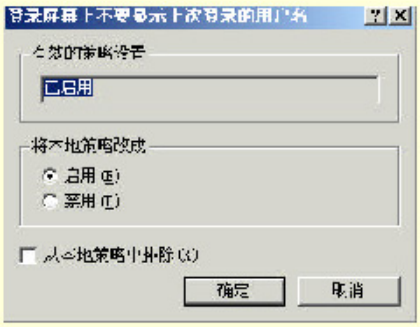


图 8-5 启用策略

这一设置也许将招致用户的抱怨，用户开始会认为不断重复输入用户名令人生厌，但为了安全，这点工作量是值得的，而且用户也会很快习惯。

8.3.5　登录验证机制

用户输入的用户名和密码将与账户数据库进行对照以验证身份，如果正确无误的话，系统将为这次会话创建一个安全访问令牌，令牌中包含了用户的安全身份信息，如果用户属于某个组的话，令牌中还会包括用户所属组的安全身份信息。

由于系统中每个对象（文件、文件夹或者打印机等等）都包含一个访问许可权限列表，这些列表中含有用户账户的安全信息、组的安全信息以及他们的权限，如果用户对这些对象进行访问，对象就会检查访问许可权限列表，将列表中的信息与用户的安全访问令牌信息进行对照，之后允许用户以合法的权限进行访问。

如果用户希望从工作站中登录到域中去，那么输入的登录信息就要由本地的安全控制转移到域控制器中，由域控制器（主域控制器或者备份域控制器）进行登录验证。

需要注意的是，用户可能在本地工作站和域中有相同的用户名，但这两个用户账号并不是同一码事，它们包含了不同的权限信息，因为由管理员分配的访问权可能是不一样的，如果用户发现登录后能执行的操作发生了变化，需要检查一下是否进行了正确的登录。

8.3.6　限制用户在工作站登录

在域管理器中，可以限制用户在某个工作站登录。对于一些作风不严谨的用户，可以限制其在存有重要资料的工作站登录。

8.3.7　设置用户登录的时间

这项工作也将在域控制器中完成，可以设置用户只能在上班时间登录，而晚上就不能登录，这也可以保证系统的安全。

另一方面，比较大的公司或者企业，往往也需要选择夜里做备份工作，这时候允许用户登录也是不适合的。

8.4　账户策略

Windows 2000 有安全的登录机制，然而要保障系统安全，管理员需要花费更多的精力，进行更精密周全的规划。

账户管理是规划的重要部分。Windows 2000 和 Windows NT 都使用账户来识别有权访问本地资源和网络资源的用户，因此必须验证为本地或者域的有效用户（通过按“ Ctrl+Alt+Del ”输入账户和密码登录），才能获得资源对象的访问权，使用账户管理有力地维护了系统的安全。

8.4.1　安全标识

系统使用安全标识（SID）对每个系统对象进行区别，包括用户、组、域中的计算机账号，都有一个独一无二的安全标识号。

对象创建时，下列 3 个条件决定了 SID 号码的产生：

（1）计算机名称

（2）当前计算机的系统时间

（3）当前线程的用户型执行时间

系统根据这 3 个 32 位数字，利用散列算法创建出一个独一无二的 SID 号码，从概率和统计学角度来说，任何两个 SID 号码应该是不会相同的。

可以打开注册表查看 SID 号码。

（1）在“ 运行 ”对话框中，输入“ regedt32 ”运行注册表。

（2）选择以下键值：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList，如图 8-6 中，标出了系统的各个 SID 号码。

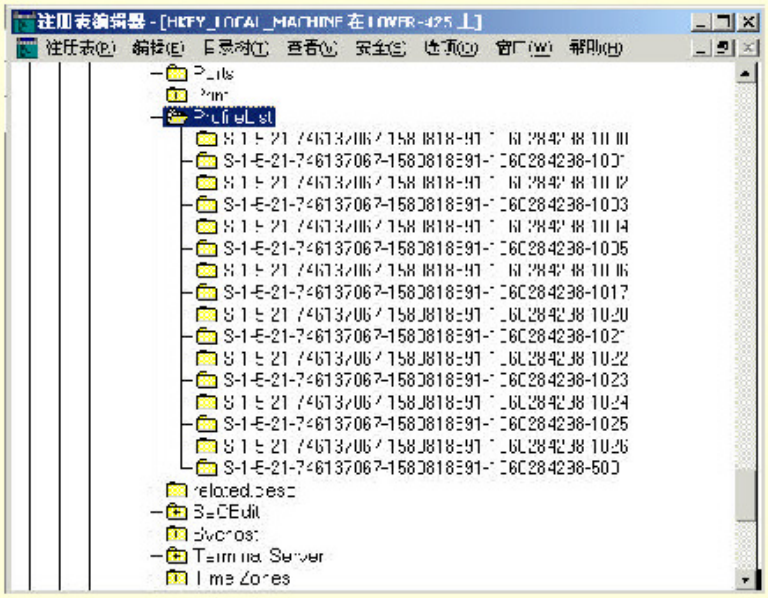


图 8-6 SID 号码

现在可以说明为什么删除了一个用户或者组账号后，即使用完全一样的账户名和密码重新命名一个新账号，也无法恢复相同的权限信息。由于两个创建的时间不一样，因此它们的 SID 号码不一样，这实际上就是两个不同的账号。

8.4.2 管理管理员账户

由于系统管理员拥有系统的完全控制权，从而往往成为攻击的首要对象。窥视系统的破坏分子总是试图窃得管理员的密码，以获取各种资料。因此，管理员必须得时时小心，管理员的密码必须设置得十分复杂以保证安全。

安装 Windows 2000 时，会自动创建管理员的 Administrator 账号，为安全起见，可以把这个账号重新命名，新的名字可以让破坏分子难以猜到。相应地，限制 Administrator 账号的权力，这样即使黑客破获了 Administrator 账号的密码，他也将发现其权力相当有限，无法对系统造成破坏。

另外一点需要注意的是，一定要慎用管理员账户。用管理员账户运行 Windows 2000 可能会使系统变得十分脆弱，比如访问一个 Internet 站点这样一件简单的事都可能产生严重的安全问题，在一个陌生的 Internet 站点中，可能会有特洛伊木马等程序下载到系统中并执行，从而导致删除重要的系统文件、格式化硬盘，甚至创建一个新账号等重要破坏。

管理员如果也需要经常使用程序、文件等数据，应该为自己添加一个普通的用户（User）账号，在平时使用这个账号登录，和其他普通用户一样操作，仅当需要做管理工作时，才用管理员账号登录，而且应当在执行完任务后马上注销。

8.4.3 停用 Guest 账户

一般说来，系统允许通过客户（Guest）账户进行匿名登录，为了运行 FTP 服务，提供客户账号有时是十分必要的。

客户账号的权限相当有限，不能执行特权操作，也有许多对象拒绝客户访问，管理员可以对客户加强控制。但是，客户允许查看注册表和系统这样重要的设施，虽然不能做改动，但客户可以查看系统的设施，了解配置情况，这也是不安全的。为了更加有效的保障，可以停用 Guest 账户。

过去的 NT 中，Domain Guests 组是 Domain Users 组的成员，现在的 Windows 2000 已经改变了这一点，Domain Guests 全局组不再是 Domain Users 全局组的成员，这样也就不是本地 Users 组的成员，从而不能访问系统资源。

8.4.4　使用组的管理

众所周知，采用组管理用户，大大简化了系统管理员的管理工作。采用组管理用户的另一个优点是，能够更明确地分配权限，从而减少了权限漏洞出现的可能性，客观上加强了系统的安全性。

8.4.5　采用域的管理手段

在第 7 章中已经介绍了域，域的出现的确为大规模网络管理提供了强有力的工具。如果采用对等工作组的方式，由于缺乏统一的账户管理，各个单元的控制松紧程度不一，十分容易产生安全漏洞。域的概念引出了主域控制器和备份域控制器，进行域的账户管理，这样一来用户必须通过域的登录验证，从而大大加强了安全性。

当网络的规模继续扩大时，又提出了多域，并采取主域进行登录验证，仍旧是强调账户的管理。主域和资源域通过信任的关系对账户统一管理。需要注意的是，有人也许会有误解，认为建立了信任关系后，可以移交一定级别的管理权限。事实上，用户的权限仍然需要由本域的系统管理员统一规划管理。

8.4.6　停用账户

当某个用户离开公司出差时，如果他有一段时间不在公司里工作，就应该停用这个账号，以防别人盗用。

停用某个账户的方法是：启动管理工具中的计算机管理，选择“本地用户和组”，在用户列表中，选定用户，接着单击右键，从快捷菜单中，选择“属性”命令。如图 8-7 所示，从属性列表中，选择“账户已停用”复选框。

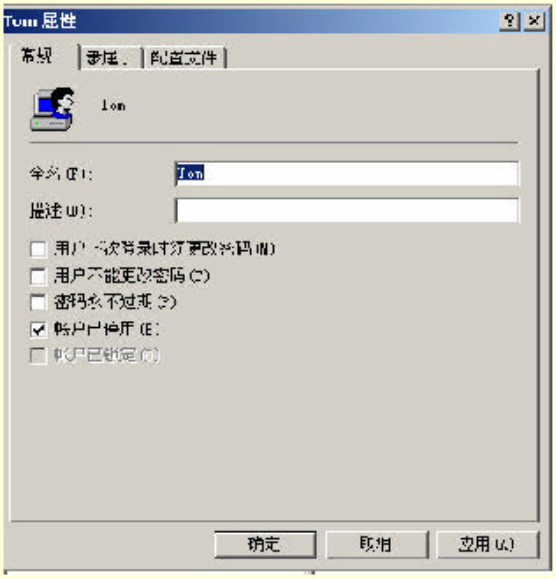


图 8-7　停用账户

同理，如果需要恢复账号的使用，只要清除这个账号即可。

另一种情况是：当公司里的某个职员离开公司后，管理员需要做的头一件事就是将这个职员的用户账户停用。最安全而又合乎人情的或许是人事管理层提前通知系统管理员，在发出解雇的同时，停用这个用户账号。尤其当这个职员是重要人物时更要小心，因为他可能有各种原因带走或者破坏机密的数据。如果职员在离开公司一段时间后，发现仍能通过过去的用户账户登录进入系统，那么管理员就是不称职的。

注意：在无法确认用户是否会重新回到原来的部门时，选择账户停用比删除账户更合适。因为重新启用某个账号比起重新建立一个用户账号要简单得多。

8.5　密码策略

用户密码也许是系统最为机密的数据，尽管它不是保护的最终目的，但掌握了密码就意味着掌握了管理数据的权力。一个安全的系统应该尽可能地加强密码管理。

8.5.1 系统对密码的处理

Windows 2000 对用户密码采取单向加密的办法（参见 8.3.2 小节），并保存在注册表中。但是任何人都不能查看这些密码，包括管理员都没有办法。这是由于密码的加密是一个单向的过程，不能反向解密。所以万一遗忘了密码，只能由系统管理员重新设置。

8.5.2 明确设置密码

有的系统账号不设置密码，这几乎是不能容忍的，尤其是管理员这样一个敏感的账号，尽管系统创建时允许不为管理员指定密码，但永远不要有空的密码。

8.5.3 保护密码

一定要小心地保护密码，下面是一些推荐的保护措施和注意事项：

（1）不要把密码写下来，特别是把它记在靠近电脑的附近。

（2）不要为了方便而与他人共享同一个密码。

（3）对管理员来说，用于进行普通登录的密码不应该同管理员账号的密码一样。

（4）每隔一定的时间更改密码，比如 60～90 天。

（5）如果觉得有危险，或发现有人试图用你的账户名登录，马上修改密码。

有的人有把密码写下来或者告诉别人的坏习惯，他们提出的理由是会遗忘密码，这说明他们内心对密码的重视程度不够，不然不会对这么重要的信息都记不住。

一些密码破解程序采用各种方法破解密码，智能猜测、词典轮询以及自动查询等等。这些方法猜测各种字符组合的可能性，只要有足够的时间，几乎所有的密码都可以被破解，而且这种破解程序仍在不断发展。因此千万不要不以为然。

对于需要高度安全的系统，对付密码破解程序的办法就是设置强化的密码。一个强化的密码提出了以下几项要求：

（1）至少需要 7 个字符的长度。

（2）包含各种大小写字母，比如 A、B、C、a、b、c 等。Windows 2000 对密码是有大小区分的。

（3）包含阿拉伯数字。

（4）包含一些其他字符，比如#、￥、%、$、&、*、~、”、^等等。

（5）决不能包含你的名字或者用户名。

（6）不能是一个普通的词汇。

8.5.4 设置密码规则

管理并制定统一合理的密码规则是系统管理员的重要任务。

8.5.4.1 密码最长存留期

通过设置密码最长存留期，保证用户一定时间后更改密码。前面说过，只要有足够的时间，密码破解程序几乎可以破解任何密码。但加强后的密码有可能需要几个月的时间才能破解，这也就失去了实时性。

设置密码最长存留期，强制用户到时后更改密码，是对付密码破解程序的一个办法。

8.5.4.2 密码最短存留期

微软认为，过于频繁地更改密码会使用户遗忘。因此设置密码最短存留期，防止用户频繁更改密码。

8.5.4.3 密码唯一性

如果允许用户设置同样的密码，那么每次系统要求更改密码时，用户为了方便起见，都会原封不动地启用上次的密码。这样一来，密码最长存留期的设置实际上就失去了意义。合理的密码策略应该设置为系统记住用户设置的前几个密码（比如 3~5 个），这样用户就必须修改密码。

密码策略的设置在第 4 章已经作了详细介绍，这里就不再赘述了。

8.6　注册表的安全性

如果账号权限的分配不合适，可能会有人因为不小心删除而导致文件丢失或者其他一些安全性问题，但还有其他一些刻意要攻击系统的人，对他们来说注册表往往是攻击的重点对象，因为注册表中保存着 Windows 2000 系统中几乎所有重要的控制参数。

8.6.1　注册表中的重要信息

一般说来，有权进入系统的用户几乎都有访问注册表的权利。虽然大多数情况下，用户没有必要亲自修改注册表，但并不能阻止它们访问注册表以查看系统配置等各种重要信息。

例如，任何用户都可以查看的有：注册表中 HKEY_LOCAL_MACHINE\HARDWARE 键、HKEY_LOCAL_MACHINE\SOFTWARE 键、HKEY_LOCAL_MACHINE\SYSTEM 键等等。这些键都包括了系统的敏感性信息，HKEY_LOCAL_MACHINE\HARDWARE 键包含了硬件信息：中央处理器的数量和类型、RAM 的大小、使用什么适配器以及显示卡等等；HKEY_LOCAL_MACHINE\SOFTWARE 键包含系统安装的各种软件、网络的配置；HKEY_LOCAL_MACHINE\SYSTEM 键包含系统启动信息等。这些都可能被黑客用以寻找系统的安全缺陷，从而成为突破口。

8.6.2　保护注册表

保护注册表的重要方法是限制用户对注册表的访问权。但是有一个必须考虑的问题是：许多软件程序及服务程序需要访问注册表的项值，如果采用简单粗暴的方法：阻止用户读注册表，那么许多程序将无法安装或者无法运行，这个后果是无法估量的，因此这种办法并不值得提倡。就像本章开头提到过的安全性和使用的方便性几乎永远是一对矛盾体，如何有效地将二者结合，是一个既包含了科学性和包含了艺术性的问题。

Windows 2000 提供两种注册表编辑工具：Regedt32 和 Regedit，Regedit 有熟悉的资源管理器式的树形界面，很容易被 Windows 95 、Windows 98 的用户接受，它的另一个优点是非常容易查找和查看；但 Regedt32 却能够支持访问权限的设置等更强的功能，所以要限制用户对注册表的访问，唯一的工具是 Regedt32。

利用 Regedt32，可以禁止用户修改注册表，从而相当程度上保护了注册表的安全。进一步，管理员还可以设置对注册表访问的审核。关于这些问题，在注册表管理一章中都有详细介绍，请读者参看。

8.7　其他

8.7.1　隐藏的安全性问题

通过隐藏对象来防止敌人攻击，从而实现安全性是古老的方法，从古到今有众多的寻宝故事就是例子。往往有这种认识：如果其他人不知道重要资源存放在哪儿，他们就没有办法进行破坏。

比如有这样一种情况，有些人害怕因忘记密码而无法登录，他们会要求管理员建立一个文件以存放这些密码，并且将它隐藏起来。另外，共享目录可以设置以$为后缀的共享名，这样就可以将共享目录在网络上隐藏起来，不知道共享目录的人无法在浏览时查看到这个资源。

但是必须意识到：依靠隐藏来实现的安全是非常脆弱的，如果因此以为别人不知道某些事情，而自信系统的安全没有问题，这种“指望”别人的态度是十分武断的。时间一长，泄密的可能性会越来越大。而系统管理员完全有更多的方法进行安全性的设置，而不是采用简单的隐藏办法，Windows 2000 提供了 NTFS 的文件系统，可以保证更有效的安全性，即使别人知道资源的位置，他们也没有办法进行攻击。

8.7.2　锁定计算机

有的工作人员喜欢忙里偷闲，比如喝杯咖啡什么的。为了方便，他们不会把计算机关闭。的确，频繁的开机关机会严重影响工作效率。但是，让计算机处于工作状态是不安全的，任何人都可能趁没人的机会使用计算机，这种感觉就好像把自己的家门开着然后去购物，或者不锁车门一样让人不放心。

Windows 2000 提供了锁定计算机的功能，可以在工作的暂时离开期间把自己的计算机锁定，就好象锁上家门再出去购物一样是可以放心的。要锁定计算机，可以采取如下步骤：

（1）按“ Ctrl+Alt+Del ”键。

（2）在出现的对话框中，选择“ 锁定计算机 ”。

（3）这时候原来屏幕的工作信息将全部隐藏，取而代之的是显示锁定的对话框。只有本人或者管理员才能解除锁定。

当工作人员重新回到计算机前时，可以解除锁定，回到原来的工作环境。用户只要按 Ctrl+Alt+Del 键，输入有效的密码即可。

8.7.3 设置加密的屏幕保护程序

也有这样一种情况：当用户离开计算机时，并不知道自己将耽误多少时间，或者由于急事干脆忘了锁定计算机。这时的唯一解救办法是事先设置的屏幕保护程序。

屏幕保护程序是长时间不操作时，用来保护计算机显示器不受过长时间射线损坏的。可以利用它来实现锁定计算机的功能。

（1）打开控制面板中的“ 显示 ”。

（2）选择“ 屏幕保护程序 ”选项卡，如图 8-8 所示。

（3）设置等待的时间，这样系统在闲置一定时间后，将会启动屏幕保护程序。

（4）在对话框下方，选中“ 密码保护 ”复选框。

这样一来，当设置的时间到了以后，在屏幕保护程序的同时，将使计算机处于锁定状态，用户需要重新工作时，必须输入有效的密码。

由于有一定时间的等待，使用屏幕保护程序来锁定计算机没有直接锁定计算机来得更安全。

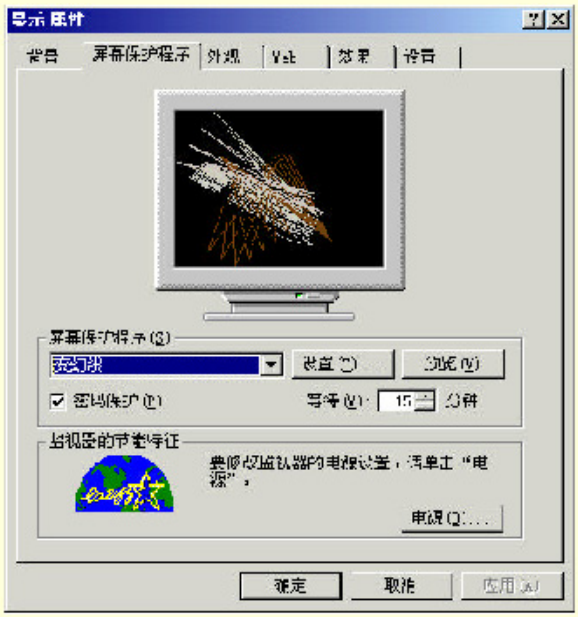


图 8-8 为屏幕保护程序设置密码保护

8.8 文件加密

使用加密是 Windows 2000 比较 Windows NT 4.0 新增的一个新功能。和所有其他支持安全功能（如设置用户权限，设置资源对象所有者）一样，对文件和文件夹的加密只能在 NTFS 卷下进行。

在 Windows 2000 中，对文件和文件夹的加密使用的是称为“ 加密文件系统 ”（EFS，Encrypting File System）的核心文件加密技术，这种技术是 Windows 2000 的 NTFS 文件系统的重要新特色。幸运的是：使用这种加密技

术对文件或者文件夹加密后，可以像使用其他文件和文件夹一样使用它们。对加密该文件的用户，加密是透明的，这表明不必在使用前解密已加密的文件。可以像平时那样打开和更改文件。但是，试图访问已加密文件或文件夹的入侵者将被禁止这些操作。如果入侵者试图打开、复制、移动或重新命名已加密文件或文件夹，将收到拒绝访问的消息。

8.8.1　通过属性加密

对文件或者文件夹加密的方法是：

（1）从资源管理器或者我的电脑中选择要加密的文件或者文件夹。

（2）单击鼠标右键，从快捷菜单中选择“属性”命令。

（3）从属性对话框中，按“高级”按钮，如图 8-9 所示，出现高级属性对话框。

（4）选择“加密内容以便保护数据”。

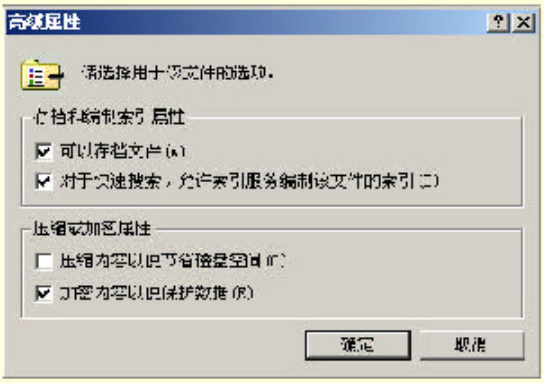


图 8-9　高级属性

可以看见，正如设置其他任何属性（如只读、压缩或隐藏）一样，通过为文件夹和文件设置加密属性，可以对文件夹或文件进行加密。

在图 8-9 中，提供了两个选择：压缩以节省磁盘空间或者加密数据，这两个选择是互相排斥的。如果选择了压缩就不能加密，反之亦然。如果想对压缩的文件或者文件加密，必须首先将它们进行解压缩。

建议：由于加密的文件不能被其他用户打开，所以系统文件不能被加密。

加密对象有两种：文件或者文件夹。由此系统会有不同的提示：

如果对文件夹加密，在如图 8-9 中，单击“确定”按钮后，出现如图 8-10 的提示。

在如图 8-10 中，选择仅对该文件夹加密或者对该文件夹、子文件夹和文件加密。如果选择的是后者，那么文件夹中当前的和将来要添加的所有文件或子文件夹都将被加密。如果选择仅加密文件夹，则文件夹中当前所有文件和子文件夹将不加密。然而，任何将来被加入文件夹的文件和子文件夹在加入时均被加密。

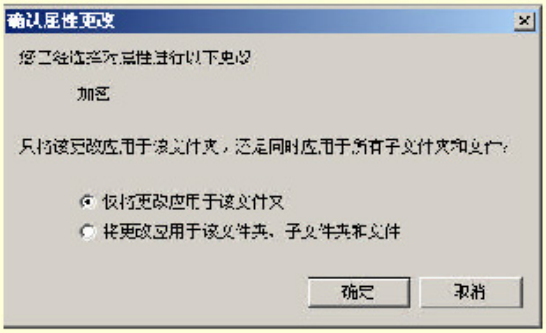


图 8-10　加密文件夹

如果对文件加密，在如图 8-9 中，单击“确定”按钮后，出现如图 8-11 的提示。

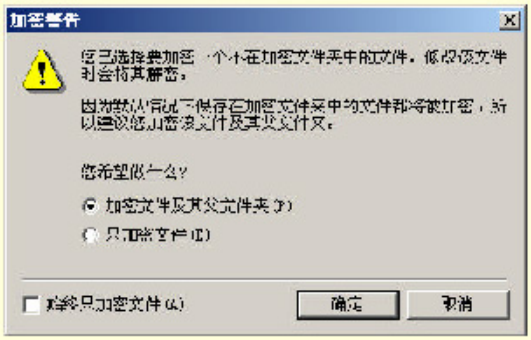


图 8-11 文件加密

在为单个文件加密时，如果选择了加密文件及其父文件夹，那么以后添加到这个文件夹的文件都会被自动加密。

以下是一些 EFS 的推荐加密方法：

- 如果将大多数文件保存在我的文档中，则对我的文档文件夹进行加密，这样可以确保个人文档的保密。
- 加密 temp 文件夹，使程序创建的临时文件加密。
- 加密文件夹而不是文件，这样可以使临时文件得到加密。

如果需要对已经加密的文件复制或者移动到其他地方，需要注意：如果复制或者移动到非 NTFS 的卷中，这些加密的文件将被自动解密，因为只有 NTFS 文件系统才支持对文件进行加密。

另外一点需要小心：在将加密文件和文件夹移动或者复制到不同的计算机上时，必须能够在这些计算机上使用加密证书和私钥。否则，将无法打开或者解密所要移动或者复制的文件或者文件夹。

可以从微软管理控制台（MMC）的证书管理，使用导出命令，在软盘上制作文件加密证书和私钥的备份副本，将软盘保留在安全位置。这样即使丢失了文件加密证书（由于磁盘故障或任何其他原因），仍然可以从 MMC 的证书中使用导入命令从软盘还原证书和相关的私钥，并打开加密的文件。

提示：加密的文件不能防止被删除，任何拥有删除权限的用户都可以将加密的文件或者文件夹删除。

8.8.2 使用命令行 cipher 加密

cipher 是命令行提示符下的加密命令，其命令参数和语法如下：

cipher [/e| /d] [/s:*dir*] [/a][/i] [/f] [/q] [/h] [*pathname* [...]]

如果使用不带参数的命令，则显示当前文件夹和所包含的文件的加密状态。以下是一些主要参数的说明：

/e：加密指定的文件夹。文件夹将被标记，以后添加到此文件夹中的文件将被加密。

/d：将指定的文件夹解密。文件夹将被标记，以后添加到此文件夹的文件将不会被加密。

/s:dir：对在给定目录及全部子目录中的文件执行指定操作。

/a：对带指定名称的文件执行所选操作。如果没有匹配的文件，该参数将被忽略。

pathname：指定样式、文件或文件夹。

要注意每个参数之间至少有一个空格分隔，如果需要查阅详细信息，可以在命令行下输入 cipher /?。

例如：要确定 father 文件夹下的 son 子文件夹是否加密，可以输入命令：

cipher father\son

要确定子文件夹中哪些文件处于加密状态，可以输入命令：

cipher father\son *

要加密文件夹 *father* 中的子文件夹 son，可以键入下列命令：

cipher /e father \ son

如果只想加密 *son* 子文件夹中的 book.doc 文件，可以键入下列命令：

cipher /e /a father\ son \ book.doc

8.8.3　解密文件或者文件夹

可以非常简单地对已经加密的文件或者文件夹进行解密，采用相反的手段，从如图 8-9 的高级属性对话框中，清除加密选项即可。

在对文件夹解密时，系统将询问是否要同时将文件夹内的所有文件和子文件夹解密。如图 8-12 所示。如果选择仅解密文件夹，则在解密文件夹中的加密文件和文件夹仍保持加密。但是，在已解密文件夹内创立的新文件和文件夹将不会被自动加密。

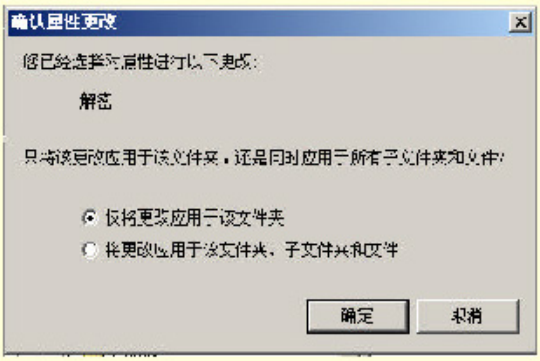


图 8-12　解密

提示：如果希望文件或者文件夹与别人共享，那么首先需要对文件或者文件夹进行解密。

8.9　安全模板及安全配置和分析工具

Windows 2000 提供了安全模板管理单元，通过查看和调整系统安全性，对安全性进行集中式管理。应该认识到，安全模板并没有存放新的安全信息，只是简单地将所有现有的安全属性组织到一个位置，从而实现了安全性管理的简化。当对安全配置和分析管理单元使用时，安全模板也可以用做安全分析的基本配置。

安全模板存放的信息包括：

- 安全策略，包括密码策略（管理密码、账户锁定和 Kerberos 策略的安全性）和本地策略（用户权利和记录安全事件）信息
- 本地组成员的管理信息
- 本地注册表项的安全性信息
- 本地服务的安全性和启动模式信息
- 本地文件系统的安全性信息

事实上，除了 IP 安全性和公用密钥策略之外，安全模板中几乎包含了所有的安全属性。

8.9.1　安全模板文件

安全模板是以 inf 为后缀名的文件，用记事本就可以把安全模板文件打开，如图 8-13 所示。

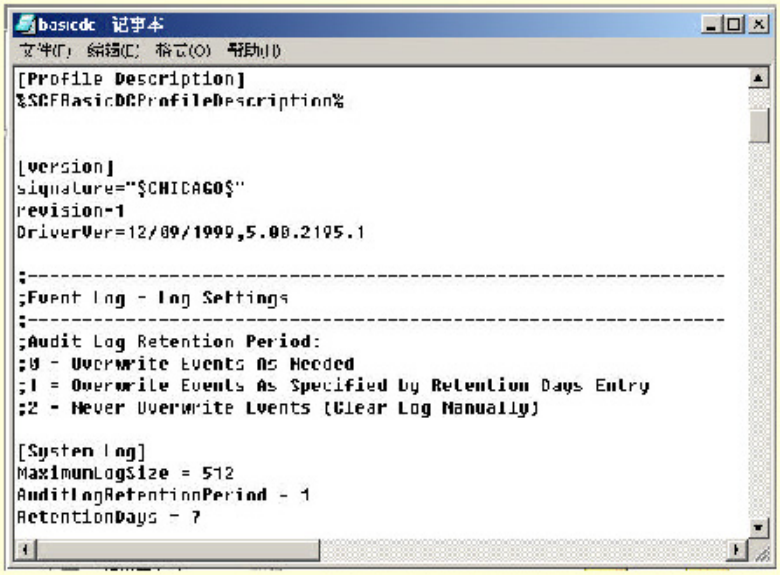


图 8-13 安全模板文件

既然安全模板文件是基于文本格式的，就可以很方便地通过复制、粘贴等方式导入或导出模板属性语句，仿照格式，制作自己的安全模板。

计算机上的初始模板被称为本地计算机策略，可以将本地计算机策略导出到安全模板文件，以保存初始的系统安全设置，这样一来，就可以利用保存好的导出的模板文件恢复初始的安全模板（通过相反的手段：导入）。并启发我们，可以将本地计算机策略进行配置修改后，通过导出保存模板文件，不必手工地在记事本上制作自己的安全模板了。这种导出模板的方法更简单易行。如图 8-14 所示是导出模板文件的对话框。

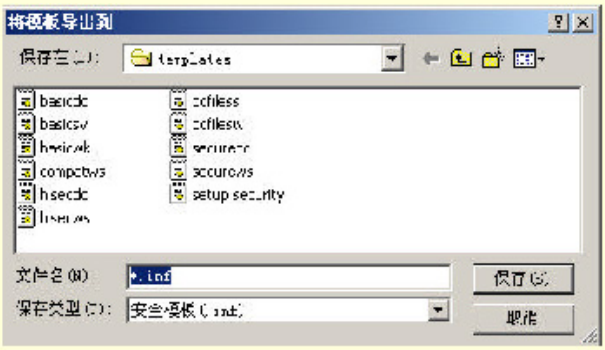


图 8-14 导出模板

如果将安全模板应用到本地计算机或导入到组策略对象中，就可以通过立即配置计算机的安全性，从而大大简化了安全性的管理工作。

配置安全模板还可以采用 secedit 命令。这个命令的语法是：

secedit /configure [/DB *filename*] [/CFG *filename*]

语法中包含了部分参数：其中/DB *filename* 参数提供了到包含应该使用的安全模板数据库的路径；/CFG *filename* 参数是到安全模板的路径，如果这个参数没有指定，将应用已存储在数据库中的模板。

同样地，导出安全模板也可以用 secedit 命令。此时的语法是：

secedit /export [/mergedPolicy] [/DB *filename*] [/CFG *filename*]

各参数意义是：/mergedPolicy 参数指明合并并导出域和本地策略安全设置；/DB *filename* 参数提供了到包含应该使用的安全模板数据库的路径，如果没有指定，将使用系统策略数据库；/CFG *filename* 参数也同上，是保存模板的文件的路径和名称。

Windows 2000 中预定义了一些模板文件，用以满足不同的安全性需求，保存在 C:\Winnt\Security\templates 文件夹中，它们分别是：

■ 默认工作站（basicwk.inf）

- 默认服务器（basicsv.inf）
- 兼容工作站或服务器（compatws.inf）
- 安全工作站或服务器（securews.inf）
- 高度安全工作站或服务器（hisecws.inf）
- 专用域控制器（dedicadc.inf）
- 安全域控制器（securedc.inf）
- 高度安全域控制器（hisecdc.inf）

8.9.2　安全配置和分析管理单元

安全配置和分析管理单元是 Windows 2000 提供的一个对安全性配置进行分析的工具。在现实当中，有时候出于解决某种问题的需要，可能要求对系统进行安全性方面的改动，改动后的系统或许就不再在满足安全性的要求了。这时候可以利用安全配置和分析管理单元工具帮助管理员进行分析。

8.9.2.1　分析安全配置

安全配置和分析单元可以将存档的安全性数据库和安全模板与当前系统的配置进行分析，分析的结果将提供关于系统有关安全方面的信息。安全级别调整后，经过检测，可以发现系统出现的安全故障，进而对计算机重新配置。

进行安全配置和分析的步骤是：

① 单击安全配置和分析根节点右键，选择“打开数据库”命令，打开一个相关的数据库，如果这不是当前配置使用的数据库，系统将提示选择加载到数据库的安全模板；如果还没有这个数据库，系统会提示并帮助创建一个新的数据库。

② 打开数据库后，就可以对当前系统的安全设置进行分析了。单击安全配置和分析根节点右键，选择“立即分析计算机”命令。

③ 输入日志的文件名和有效路径，或者使用默认的日志。

分析的时间可能会稍长，因为将分为几个部分进行分析，它们是：账户策略、本地策略、事件日志、受限制的组、系统服务、注册表和文件系统。检查完毕后，将不同的安全区域进行显示，如图 8-15 所示，此时可以检查日志文件或复查结果。

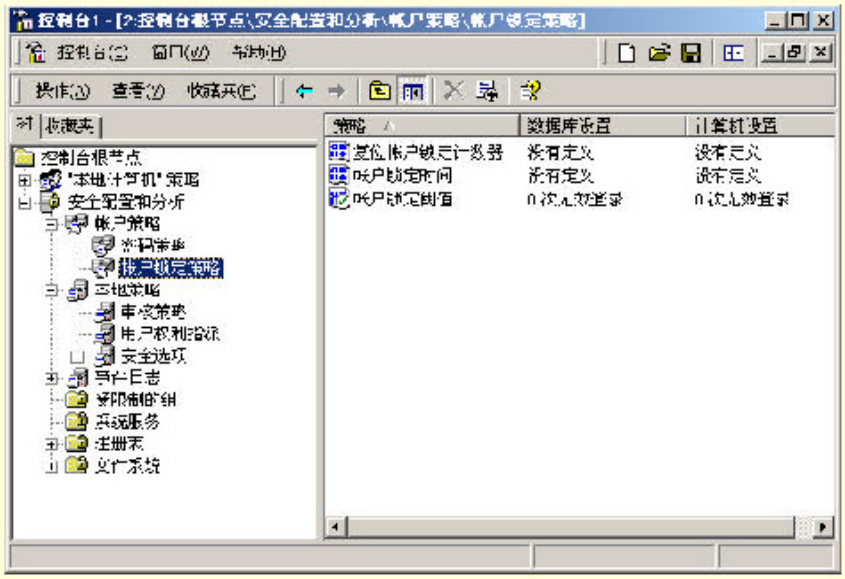


图 8-15　分析结果

从详细信息面板中检查结果，其中数据库设置一栏给出的是模板中的安全值；计算机设置一栏表明系统中的当前安全设置。仔细查看，可以发现各项前的标志有所不同，其中有绿色的复选标记的项表明当前计算机的设置与安全模板数据库的配置一致；没有图标的表明模板中不包含本项安全属性，无法进行分析；而如果前面图标是一个红色的“×”就要小心了，因为它表明当前计算机的设置与安全模板数据库的配置有差异。

8.9.2.2 对计算机进行配置

如果发现当前的安全配置有问题，可以利用这个工具，马上对计算机进行安全配置。右键单击安全配置和分析，然后选择“立即配置计算机”命令。

同样，配置注册表和文件系统会导致花费比较长的时间，配置过程如图 8-16 所示。

图 8-16 配置计算机

配置完成后，可以查看配置过程的日志文件，单击右键“安全配置和分析”，然后选择“查看安全日志”命令，如图 8-17 所示。由图中的日志文件，可以了解配置的过程，这个过程基本上是按照用户权限（包括受限组）、注册表、文件系统、系统服务、安全策略进行的。过程中的问题都以日志的形式提出。

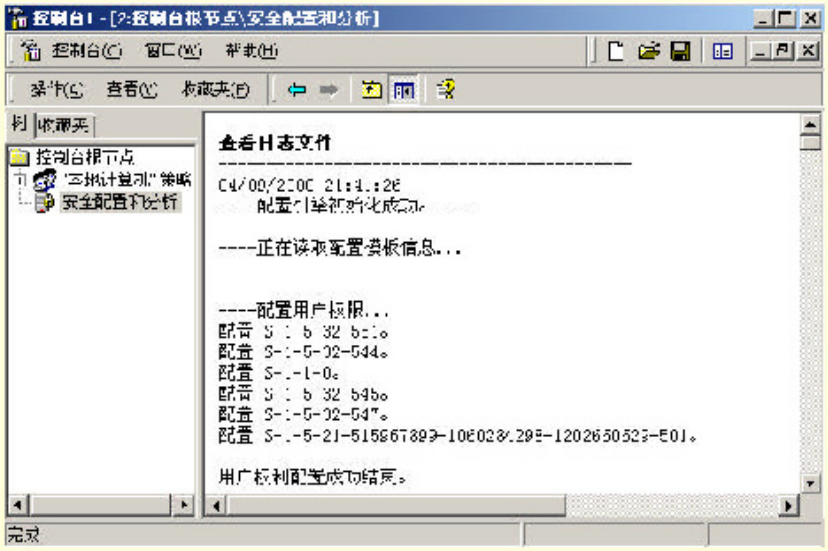


图 8-17 查看日志文件

配置过程中，如果确定本地系统的安全级别有效，则接受或更改已标记或不包含在配置中的值。当选择“立即配置系统”时，将更新基本配置中的这些属性值，并将它们应用到系统。

8.9.2.3 导出模板

可以通过将多个模板导入到数据库中创建复合安全模板，如果要将复合模板另存为单独的文件，单击右键安全配置和分析，然后选择“导出模板”命令。

此复合模板以后可用于系统分析和配置。只有选择覆盖时，才不会将它们合并为复合模板（存储的配置）。

8.10 证书管理

作为本章的最后一节，我们将看到在日益发展的通讯时代，是如何对通信内容进行保密的。众所周知，过去人们上网主要是浏览各种静态的 HTML 页，但随着各种动态网页技术以及带宽的发展，人们已经不再满足于用 WWW 下载没有变化的 Web 页了，交互正在 Internet 上越来越频繁地进行，电子商务就是最好的例子。

今天，各种敏感而重要的数据在 Internet 传送，许许多多的用户需要提交他们的用户名和密码以得到身份

验证，电子商务的进行需要信用卡号码等等。这些数据在网上来回传送，没有强大的保密措施是难以想象的，数据加密技术在其中扮演重要的角色。

8.10.1　加密方案

古老的加密方法有许多种，最简单的比如对字母采用 ASCII 编码等等。采用编码加密的方式：对各个字母，根据一定的编码原则将其与另外一些字符相对应，从而进行加密。从字面看来，它们似乎十分费解，但是事实上这种加密是十分小儿科的，完全可以从某些数字或者字符重复出现的频率进行相关的猜测。早就有人统计过英语字母出现的频率，比如 e 是出现最多的字母，根据这个规律，花上不太长的时间就可以推测出各个字符代表的原始意义。在计算机大量引入的今天，这种计算量并非不可想象。

幸运的是，有许多更加优秀的加密方案。

数据加密标准（DES）是由 IBM 公司开发出来的产品，1977 年被美国政府采纳。这种方法采用 64 位加密单元对数据加密，但在这 64 位中，有 8 位属于奇偶校验码，所以实际上起作用的是 56 位。DES 在国际上有很广泛的影响力，还曾经被 ISO 采用为加密标准。

DES 加密标准是一种对称的加密方法，所谓对称，指的是采用同一个密钥对数据进行加密和解密，所以解密者必须知道用以加密的密钥，换句话说，这个密钥是双方共享的。DES 保密性只取决于密钥的保密，它的算法是公开的。

DES 加密方法已经经受了多年的考验，但它也有许多不足之处：一个显著的问题是：如果接收方不知道密钥，就无法破解。如果依靠信使来传送密钥，在技术飞速发展的今天显然是无法接受的，而依靠网络传送则本身又带来了新的保密问题。这样一来，就必须在任何两个相互通信的人之间事先进行密钥约定。那么如果许多人之间需要两两之间通信（这是十分常见的），数量庞大的密钥保存对每个人都是困难重重的。

应运而生的是非对称的加密方法，即所谓的公用密钥加密方法。与 DES 不同，这种技术采用两个不同的密钥：公用密钥与私有密钥。前者是公开的，大家都可以自由使用，后者则是有私人用户所私有的。使用时，用一个密钥加密，另一个密钥解密。

公用密钥加密方法中，公用与私有密钥是可以双向使用的。可以使用公用密钥进行加密而后用私人密钥解密，反之，使用私有密钥进行加密而后用公用密钥解密也完全可以行得通。这样以来，就不必再花费过多的精力来互相约定密钥和保存密钥了，可以采用公用密钥进行加密，接收端用个人的私有密钥解密就可以了。

另一方面，公用密钥加密方法解决对称加密方法所无法解决的又一个难题：身份验证。如果 A 采用 A 的私有密钥进行报文加密后传给 B，B 可以用公用密钥进行解密，同时也就可以验证 A 的身份，因为只有 A 知道自己的私有密钥。

公用密钥加密方法中最著名的体制是３位美国科学家 Rivest、Shamir 和 Adleman７０年代末提出来的，也称为 RSA 算法。

公用密钥加密方法比起对称加密方法的缺点是它的转换比较慢，但它是一种更加有效的办法。

8.10.2　理解证书

为了确保执行任务的公用密钥不被盗用，使用了证书的认证方法。简单地说，证书是由颁发证书的机构采用数字签名证明有效性的文档资料，而颁发证书的机构（颁证机构）作为一个管理组织，用于证明公用密钥持有者的身份，并且为证书签名分配密钥。用户可以拥有一份签名证书的“复印件”，用于在需要的时候证明自己的身份。

目前最常用的证书形式是基于 X.509 标准的，Windows 2000 公钥使用的基本技术就是 X.509 标准。

一份完整的证书应该包括：主题公用密钥、证书版本、颁发者标识符信息、有效期、主题名、主体公钥和主体标识信息之间绑定关系的有效性等信息。需要注意的是：证书使用的期限不是无限的，也就是说，证书有一定的有效期。每个证书都包含起始日期和终止日期，一旦超过了证书的有效期，就必须申请新的证书。

另一方面，证书的颁发者和签署者称为证书颁发机构（CA）。证书也可以由一个机构颁发给另一个机构，从而建立证书等级。颁发机构的任务除了颁发带有数字签名的证书外，证书还必须处于有效期，负责发布无效的证书列表 CRL（注意：列表中不包括过期的证书，而是被吊销的证书）并确认证书不在被吊销的证书之列等等。

8.10.3 证书管理单元

Windows 2000 有证书管理单元，用户和管理员可以使用证书管理单元向证书颁发机构申请新的证书，或者在证书存储区内查找、查看、导入和导出证书。这样证书的发布、更新和撤消就不用依赖于外部的认证机构。

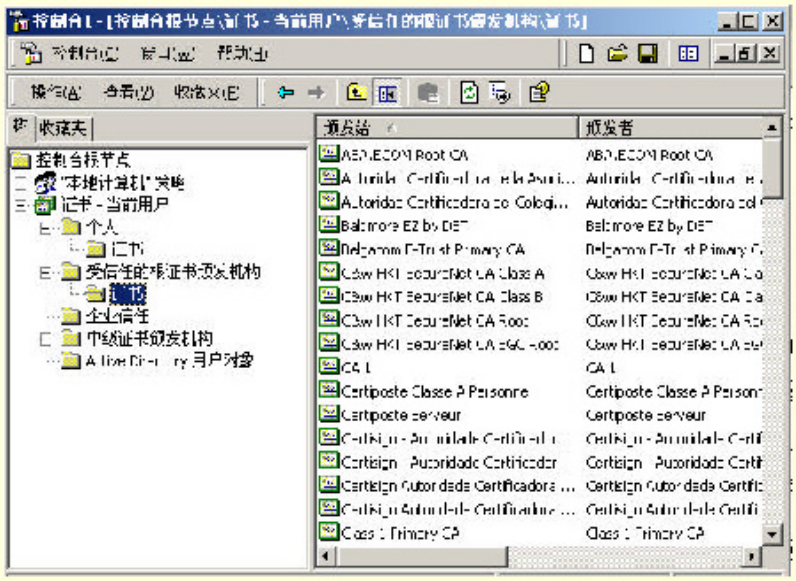


图 8-18 证书管理

8.10.3.1 查找证书

图 8-18 可以看为一个证书存储区，包括个人、受信任的根证书颁发机构、中级证书颁发机构等。在证书存储区中可以有许多操作，首先是查找证书。

单击右键，选择“查找证书”命令，如图 8-19 所示。可以在对话框下拉列表中选择查找范围和字符域。

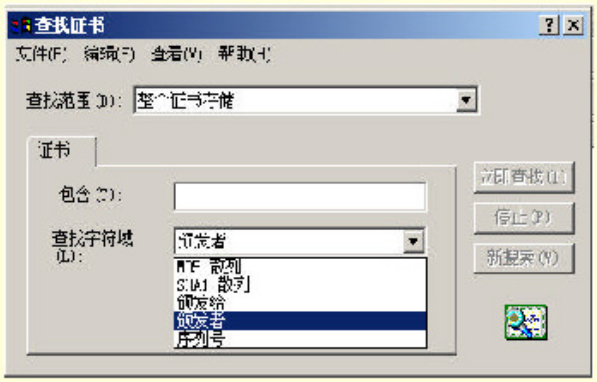


图 8-19 查找证书

8.10.3.2 查看证书

在证书存储区中，选择要查看的证书，单击右键，从快捷菜单中，选择打开命令，或者直接双击要查看的证书，则可以查看这个证书的详细信息。在如图 8-20 中的常规选项卡中，可以查看证书的目的、持有者、颁发者和有效期。选择详细信息选项卡，可以查看这个证书详细包含的信息。

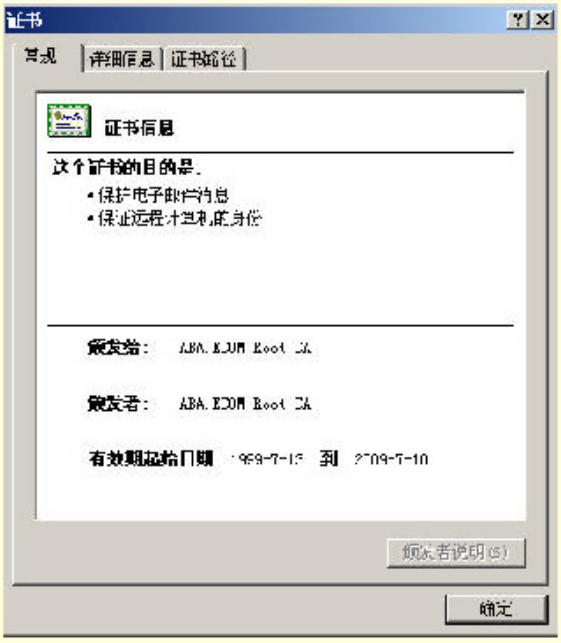


图 8-20　查看证书

8.10.3.3　导出证书

使用导出证书的目的是保存可信证书的副本，导出证书的过程包括复制证书、证书信任列表和证书吊销列表到磁盘上，导出的证书用在需要证明自己的身份场合，比如要将某个文件解密。

选定某个证书后，从快捷菜单中选择“所有任务”→“导出”命令，证书管理器使用向导帮助用户导出证书。向导首先要求选用导出格式，包括 DER 编码二进制、Base64 编码和加密消息语法标准，接着指定导出文件的路径和文件名。如图 8-21 所示，之后将完成导出任务。

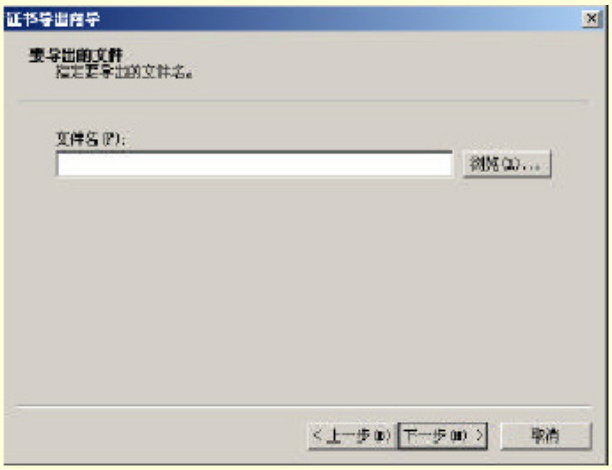


图 8-21　导出证书

8.10.3.4　导入证书

与导出证书相反的过程是导入证书，导入的过程包括将复制证书、证书信任列表和证书吊销列表从磁盘复制到证书存储区中。相应的也有导入证书的向导。操作同证书的导出是基本相似的，包括选择需要导入的证书以及导入的证书区。根据向导提示操作完成后，如图 8-22 所示。

图 8-22 导入证书

数据加密是一门相当艰深而又很有意思的学问，涉及到密码学的方方面面，有兴趣的读者还可以参考其他书籍。

Windows 2000 的安全性保护一章到此结束，作为安全保护另外一个重要手段，审核和时间查看器扮演着重要的角色，我们将另设一章介绍。作为新世纪的产品，Windows 2000 继承了前辈 Windows NT 的许多优点，并有了更强的改进，这些都是因为时代的前进，网络和计算机的安全性越来越受到人们的重视。

第 9 章　注册表管理

毫无疑问，注册表数据库是 Windows 2000 中最重要的组成部分。千万不要造成误解：以为注册表是类似用来注册 Windows 2000 操作系统的程序（从来就没有这样的程序），可以把注册表当作一个中心仓库，它储存了系统所有的重要配置参数以及绝大多数 32 位 Windows 应用程序的配置参数，包括所有的用户和计算机账号、它们的密码和权限设置等安全信息、用户的配置文件及脚本信息、各种硬件配置（如中断、I/O 端口、DMA 通道），各种软件信息，性能数据等等。

在本章开始就要提醒读者：正因为注册表的重要性，必须对它建立高度的责任心，不能有丝毫的疏忽。一些文件或者程序可以被误删，这种破坏只是局部性质的，但如果注册表被破坏，Windows 2000 可能无法正常工作，甚至将无法启动，这时的损失可是无法估量的。

如果用户对古老的 Windows 3.x 还有印象的话，可能会记得.INI 文件，当时的大多数 16 位程序都用.INI 文件作为它们的初始化文件（也就是配置文件），而系统则用 AUTOEXEC.BAT、CONFIG.SYS、WIN.INI、SYSTEM.INI、REG.DAT 等文件保存系统配置。但是较新的 Windows 95、Windows NT 4.0、Windows 98 以及 Windows 2000 都采用了注册表的配置数据库，取代了过去的.INI 文件。注册表比.INI 文件功能更强，管理更方便，也更安全，更不易受到破坏。为了兼容 Windows 3.x 而写的 16 位程序，.INI 文件仍会被支持，但是它们将逐渐从 Microsoft 的舞台中消失。

注册表数据库是一个相当庞大的组织，用包罗万象来形容并不过分，因此查找的工作也许会比较困难，而且保存也很费事，尽管如此，注册表的优点要远胜于这些弊端。

本章内容包括：

不同的注册表工具
注册表概览
注册表中的各键及其子键
间接改动注册表
使用注册表编辑器
保护注册表
注册表的保存
远程编辑注册表

9.1　不同的注册表工具

Windows 2000 有两种不同版本的注册表编辑工具：regedt32.exe 和 regedit.exe，在 Windows 2000 中，它们都是 32 位的编辑工具。

regedt32.exe 是比较老的编辑版本，继承了在 Windows 3.x 中的版本风格，并在 Windows NT 4 中继续应用，是一个多文档界面的工具，如图 9-1 所示。另外一个比较新的版本是 regedit.exe，它的界面是单文档型的，采用了 Windows 95 的风格，如图 9-2 所示。

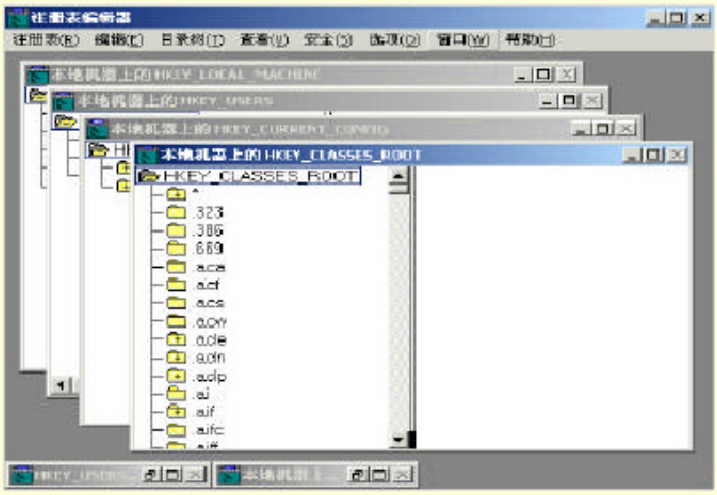


图 9-1 regedt32.exe 界面

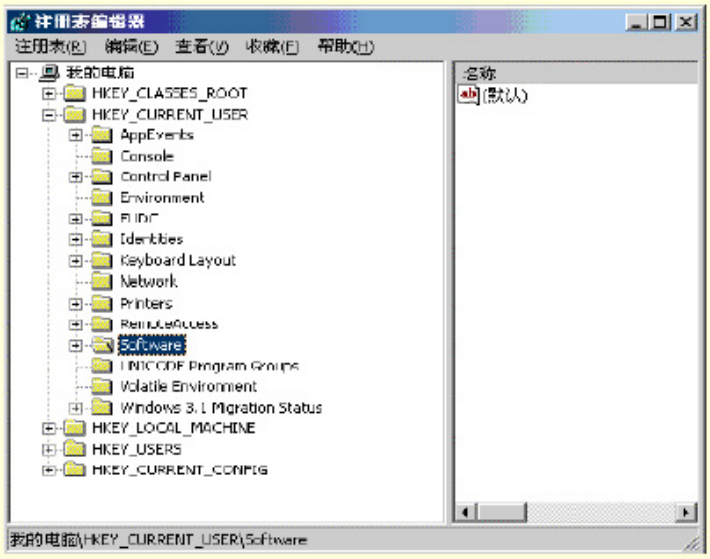


图 9-2 regedit.exe 界面

很显然，由于采取了 Windows 95 的树型结构，regedit.exe 的界面更容易让人接受。但是需要注意的是，regedit.exe 失去了旧版本的 regedt32.exe 的一些功能。在 regedt32.exe 中，可以设置用户的权限和审核规则，管理更为方便。而 regedit.exe 的优点除了界面比较漂亮外，查找也比 regedt32.exe 来得方便。习惯了 Windows 95 的用户可能会选择 regedit.exe，但是从管理员的角度来看，还是老版本的 regedit.exe 更好用。

提示：微软在 Windows 95 和 Windows NT 4.0 中都采用了注册表管理，二者的概念一样，管理的信息也是一致的，但它们的内部结构却存在对硬件控制的差异，具体地说，Windows 95 使用即插即用的环境控制信息，而 Windows NT 4.0 使用的是 HAL 的硬件抽象层。因此微软在推出 Windows NT 4.0 后，人们发现无法从 Windows 95 升级到 Windows NT 4.0。这导致了许多额外的工作，比如应用程序运行不正常而要求重新安装，重建图标等。

9.2　注册表概览

9.2.1　注册表组成

由图 9-2 所示的 regedit.exe 界面可以看得很清楚，注册表中包含 5 个根键，即 HKEY_LOCAL_MACHINE、HKEY_CURRENT_USER、HKEY_CLASSES_ROOT、HKEY_CURRENT_CONFIG、HKEY_USERS。每个根键的所包含的内容大致如下：

■ HKEY_LOCAL_MACHINE

其下又包括了 SAM、Security、Software、System、Hardware5 个子键，包含了计算机硬件和软件的各种配置信息，以及本机的安全信息。

■ HKEY_CURRENT_USER

当前登录用户的配置文件数据。

■ HKEY_CLASSES_ROOT

包含对象链接与嵌入（OLE）以及 Activex 信息和文件关联数据。

■ HKEY_CURRENT_CONFIG

包含用来启动系统的硬件配置信息。

■ HKEY_USERS

缺省用户（Default Users）的配置文件信息。

提示：在前面讲述用户管理的时候，已经对 C 盘下用户配置文件夹和 Default Users 配置文件夹有了一定程度的介绍。这两种配置文件基本上就对应于注册表中的 HKEY_CURRENT_USER 键和 HKEY_USERS 键。

5 大根键（Root Key）下都包含了数目众多的子键，子键下还有许多的子键。用户如果打开 regedit.exe 并逐层展开，就可以发现其中嵌套的层次关系十分深。本章后面对这 5 个键将有更详细的介绍。

9.2.2　注册表的数据结构

值得注意的是，无论打开新版本的 regedit.exe 还是老版本的 regedit32.exe，都可以发现，注册表的数据库结构是层次型而不是关系型的数据库。这种层次型的关系与资源管理器中的文件夹、文件的组成关系十分相似。最底层的子键包含着系统信息，可以认为是一个包含着数据的文件。

9.2.3　键的组成

前面已经介绍过，各个子键分别记载了系统的不同配置信息。组成各个键的有 3 个组成部分：

（1）键名：用于标识各个键的名字。

（2）数据类型：使用过编程语言的用户可以跟容易地理解数据类型，正好比 C 语言或者 BASIC 语言的整型、字符型、浮点型等等，指的是数据的格式。

（3）键值

键的数据类型又包括以下几种：

■ REG_BINARY：

普通二进制数据。

■ REG_DWORD：

四字节二进制数据，在注册表编辑器中，以二进制，十进制，或者十六进制数据表示。

■ REG_EXPAND_SZ：

扩展的字符串，以扩展符%开始和结尾。REG_EXPAND_SZ 的扩展符将扩展成一个代表环境变量的实际值，比如%SystemRoot%将被扩展成为 C:\WINNT\

■ REG_MULTI_SZ：

由多个值表示的数据。

■ REG_SZ：

常规的可读文本字符串数据。

键的数据由其数据类型所决定，可能是一个数字或者是字符串，对于一些二进制数据，无法从注册表编辑器的显示读到有用的信息，但可以利用更有效的管理工具，比如 Windows 2000 提供的“系统”管理单元插件来查看。

9.3 注册表中的各键及其子键

5 大键中，HKEY_CURRENT_USER 和 HKEY_USERS 基本代表了 C:\Documents and Settings 下的用户配置文件夹和 Default Users 文件夹中的内容，其他大部分信息则贮藏在 C:\Winnt\System32\Config 中，用户可以在资源管理器中打开这个文件夹，查看其中的文件信息。

如图 9-3 所示正是 Config 文件夹中的各种系统文件，其中灰色的是被隐藏的文件，缺省情况时是看不见的。要显示所有文件，请在资源管理器中，打开“工具”→“文件夹选项”菜单，选择“显示”选项卡，选择“显示所有文件和文件夹”。

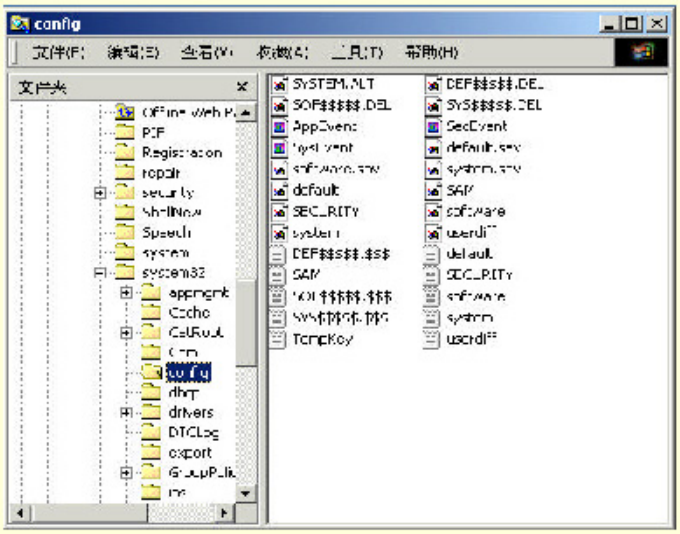


图 9-3 注册表文件信息

在图 9-3 中显示的文件可以用表 9-1 说明：

表 9-1 注册表项和相关文件

注册表项	相关文件
软件（Software）	software, software.log, software.sav
系统 (System)	system, system.log, system.alt, system.sav
SAM	SAM
安全 (Security)	SECURITY
缺省	Default, default.sav

其中，不带后缀名的文件是当前版本的配置信息，其他则是一些附属文件，并有不同的后缀名。它们的含义是：

.log：日志文件。

.Event：事件查看器文件，可以在事件查看器中打开它们进行检查。

.sav：作为上次的正确系统配置（Last Known Good）引导进程的一部分保存下来的文件。

.alt：保存 HKEY_LOCAL_MACHINE_\System 键的备份副本。

9.3.1　HKEY_LOCAL_MACHINE

前面已经提过，HKEY_LOCAL_MACHINE 键包括系统的许多软件和硬件信息以及配置细节，包括整个系统所使用的所有文件名，文件位置以及设置信息和与系统连接的所有设备名，因此是十分重要的。

HKEY_LOCAL_MACHINE 键下有如下几个重要的子键：

（1）HKEY_LOCAL_MACHINE\SAM

SAM 代表的含义是安全账号管理器（Security Account Manager），包含着所有用户和组的信息，如果计算机在域中，则还包括域的安全信息。为了向活动目录过渡，现在也可以用目录服务数据库来称呼它。

HKEY_LOCAL_MACHINE\SAM 键也是 HKEY_LOCAL_MACHINE\Security\SAM 键下的内容，对任一者所作的改动也会影响另外一者。

系统管理员可以通过用户管理器（本地用户和组或者域用户管理，参见第四章）管理账户来影响 SAM 键。

（2）HKEY_LOCAL_MACHINE\Security

注册着用户和组的安全信息，以及所有的权限和优先级别。Security 键又包括 Cache、Policy、RXACT 和 SAM4 个子键。

需要注意的是，SAM 和 Security 这两个子键都受到了系统的严格保护，不能用注册表编辑器对它们进行改动，但可以在用户管理器，资源管理器中进行管理。如图 9-4 所示，这两个键是灰色的。

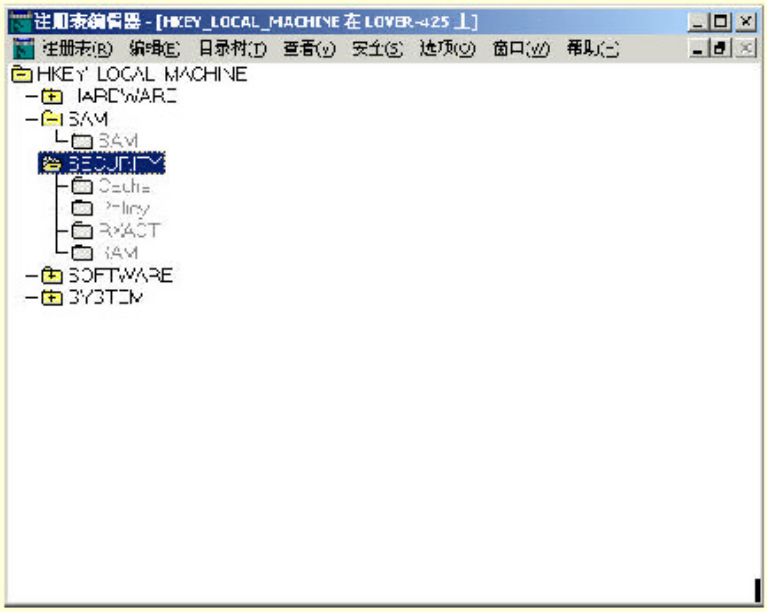


图 9-4　无法查看 SAM 和 Security 子键

（3）HKEY_LOCAL_MACHINE\Software

包含着用户安装的所有 32 位程序信息，如图 9-5 所示。

图 9-5 Software 子键

图 9-5 所示的是作者计算机上的键值，读者的界面可能会有所不同，这取决于每个用户具体安装的软件程序，安装不同的程序，会对这个键添加不同的子键。

此外，一些共同的子键列举如下：

■ Classes：这其实与 HKEY_CLASSES_ROOT 根键完全相同，后面会有详细讨论。

■ Microsoft：微软公司的产品当然要有它们的软件信息。这个键记载了微软的许多产品信息，令人目不暇接。一般用户都会安装许多微软的软件，比如 Word、Visual Basic，\isual C++、FrontPage 等等，此外还有许多连同 Windows 2000 安装的产品信息。

例如打开 Windows NT 子键，如图 9-6 所示，将可以看到如下信息：

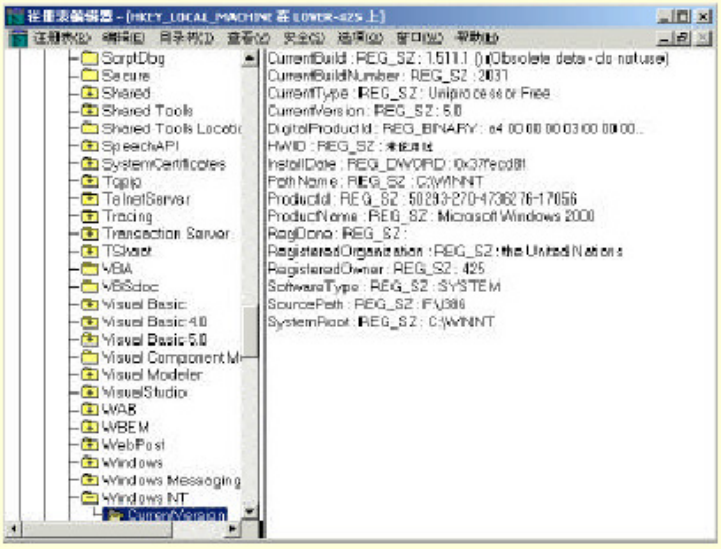


图 9-6 Windows NT 版本信息

比如当前产品号（CurrentBuildNumber）是 2031，当前版本(CurrentVersion)是 5.0，源路径(SourcePath)是 F:\I386，系统路径(SystemRoot)是 C:\WINNT，产品名称(ProduntName)是 Windows 2000 等等。

■ Program Groups：包括通用程序组的信息。

■ Secure：保存具有较高安全性的键的地点。

（4）HKEY_LOCAL_MACHINE\System

这个键下有控制集，所谓控制集是指系统启动所需要的所有信息，包括出现故障时恢复所需的信息。所以 System 键就包含了系统启动、驱动程序以及所加载服务的信息，系统在 System 键中保存所有必要的同启动相关的数据。

System 键下的控制集(ControlSet)包括 ControlSet001、ControlSet002、CurrentControlSet 等。

各个 ControlSet 键中包含有 Control 键、Services 键、Enum 键和 Hardware Profiles 键，Control 键的一些内容说明如表 9-2 所示。

表 9-2　Control 键的一些内容

ComputerName	计算机名称
KeyboardLayout	键盘布局
Print	定义打印和打印机系统环境
PriorityControl	优先级别
TimeZoneInformation	时区设置
VirtualDeviceDrivers	虚拟设备驱动器
Windows	窗口模式
WOW	16 位应用程序信息

其他键的含义简述如下：

Hardware Profiles 键：利用硬件配置文件选择启动以后激活的硬件，通常用于笔记本或其他便携式系统。

Services 键：Windows 2000 自带的所有标准服务。

Enum 键：总线的枚举器信息。

System 键下还包括了 Select 子键、CurrentControlSet 子键、Setup 子键。

Select 子键指当前所使用的控制集，如图 9-7 所示。其中 Current 代表当前启动所用的控制集号（0X1 即表示 ControlSet001），Default 代表缺省使用的控制集号，Failed 代表启动失败所使用的控制集号，LastKnownGood 代表上次成功启动所使用的控制集号。

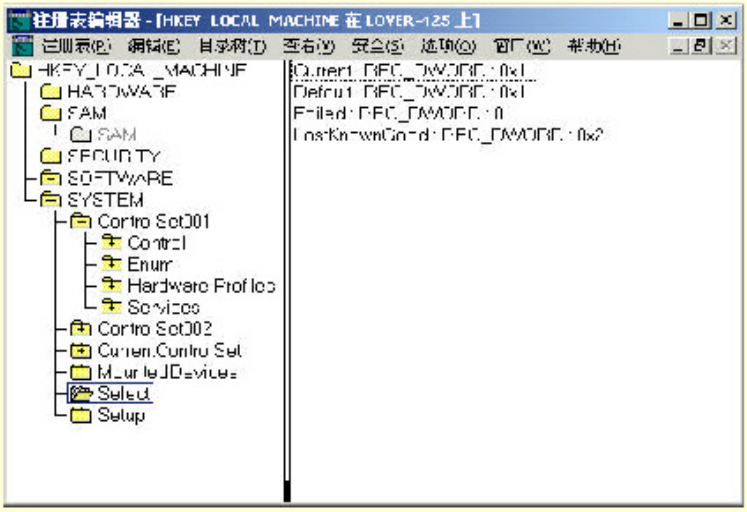


图 9-7　Select 子键的内容

提示：有时当改动注册表后系统无法正常启动，这时候的一种修复办法就是选择上次的正确配置启动（LastKnownGood），方法是在启动选择配置时直接按空格键，选择 LastKnownGood 菜单。

CurrentControlSet 子键是启动时指定使用的控制集的映射，与其他某个控制集相连接。

Setup 子键指向系统文件位置，如系统分区，设置状态以及与系统设置有关的其他信息。

有时 System 键下面还有一个 Clone 子键，它是由 RDISK.EXE 程序所保存的上次正确系统配置（LastKnownGood）启动，指向&SystemRoot&\Repair(缺省为 C:\WINNT\repair)，帮助完成系统正常的备份维护工作，该键可以用来建立 LastKnownGood 值，当正确启动时，Clone 子键就被复制到 LastKnownGood 当中。

（5）HKEY_LOCAL_MACHINE\Hardware

包括对所有硬件设备进行控制的项和子项。Windows 2000 不允许应用程序对硬件设备进行直接控制。Hardware 下的子键说明如下：

■ DESCRIPTION

包括硬件信息的描述，如中央处理器（CentralProcessor）、浮点处理器/数学协处理器（FolatingPointProcessor）、多功能适配器（MultifunctionAdapter）的描述。

■ DEVICEMAP

包括键盘、并行端口、串行端口、显示器、SCSI 适配器等设备的存放位置。

■ RESOURCEMAP

每种资源在注册表中存放的位置。

9.3.2 HKEY_CLASSES_ROOT

本键包括如下系统：

■ 所有的文件扩展名，例如.BMP，.TXT 等。

■ 所有的应用程序和文档间的关联。

■ 所有的驱动程序名。

■ 所有的 DDE、OLE、ActiveX 的信息。

■ 所有的应用程序和文档资料所使用的图标。

HKEY_CLASSES_ROOT 键用于控制应用程序和操作系统，如果用户展开这个键，会发现它庞大的规模。正是由于组织庞大，所以像 SYSTEM.INI 和 WIN.INI 这样的文件已经无法适应这种复杂的管理。

需要注意的是：这个根键其实与 HKEY_LOCAL_MACHINE\Software\Classes 键完全相同，打开 REGEDT32.EXE，并分别展开 HKEY_LOCAL_MACHINE\Software\Classes 和 HKEY_CLASSES_ROOT 键，经过对照就可以发现这点，如图 9-8 所示。

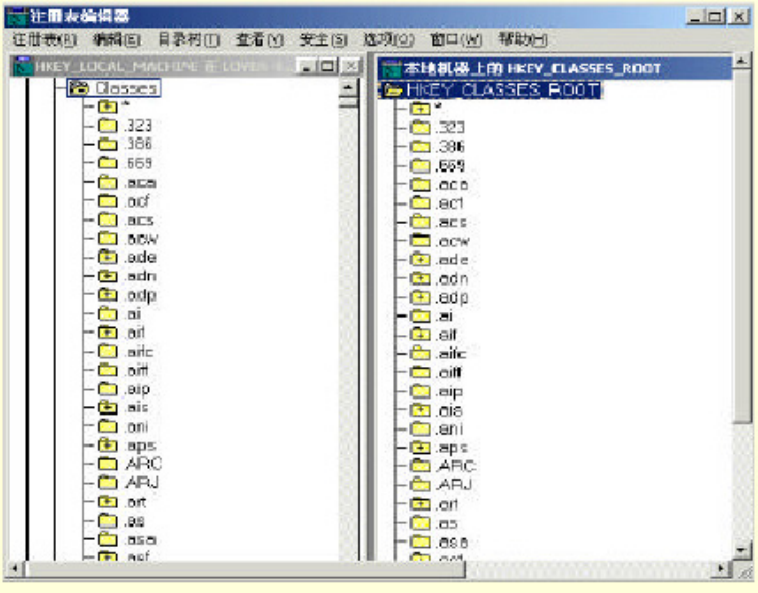


图 9-8 HKEY_LOCAL_MACHINE\Software\Classes 和 HKEY_CLASSES_ROOT 键

由于这两个键完全相同，它们的变动是同步进行的，对其中一个做改动，另一个也会相应地变动。之所以做这样的设置，也许是为了方便程序员安装过程中发送必要的注册表信息。

9.3.3　HKEY_CURRENT_CONFIG

这个键代表启动时选择使用的当前硬件配置文件。使用硬件配置文件是为了用户能方便迅速地变换硬件配置，比如笔记本电脑的用户就可能会有两种不同的硬件配置文件。

HKEY_CURRENT_CONFIG 键下包括 Software 和 System 两个子键，对 Software 键，如果不同的硬件配置文件间不存在软件的差异，这个键就不会有内容，只有包含硬件专用的软件，Software 键才会有具体内容。

HKEY_CURRENT_CONFIG 键其实也是多余的，细心的用户可能会发现它的内容其实与 HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Hardware Profiles\Current 键完全相同。当配置文件被载入系统时，就会自动加载到这两个键中。

9.3.4　HKEY_USER

本键包含着活动的用户文件，每个文件在一个子键下。子键带有用户的安全 ID 字符串，如图 9-9 所示。此外还有一个 Default 子键，代表着缺省用户的配置文件。

图 9-9　HKEY_USER 键的内容

因为两者都代表了用户的配置信息，因此它们有相似的结构。下面是一些它们相同的子键例子：

（1）Control Panel

代表在控制面板设置的信息，比如附件、颜色、Internet、鼠标、桌面、屏幕保护、声音等设置。

（2）Environment

存放着由控制面板中存放着的系统信息。

（3）KeyboardLayout

存放着用户定义的键盘布局。

需要注意的是：虽然有相同的子键，它们的键值是不一样的，因为带有用户的安全 ID 字符串的子键包含的是当前用户的配置信息，而 Default 子键包含的是缺省用户的配置信息。

9.3.5　HKEY_CURRENT_USER

HKEY_CURRENT_USER 键同样是当前用户的配置信息。读者可以猜想到，这个根键其实与上面的 HKEY_USER 键下带有用户的安全 ID 字符串的子键所包含的内容是一模一样的。

当用户注册登录时，配置文件从 HKEY_USER 键下拷贝到 HKEY_CURRENT_USER 键中，如果 HKEY_USER 键中没有这个用户的安全 ID 字符串的子键，就用缺省的配置文件，即 Default 子键来初始化

HKEY_CURRENT_USER 键，这正是在用户配置文件一章中所讲述的内容。

9.4 间接改动注册表

正如本章开始所说的，注册表是系统得以正常运转的重要保证。即使是很小的改动，也可能导致非常严重的后果。因此一定要慎用注册表编辑器。

其实，有许多工具可以帮助用户调整系统的性能，以及其他配置，用户完全可以自由方便地使用这些系统提供的工具，而不用冒着风险深入注册表中修修补补。控制面板就是常用的工具，表 9-3 是对它底下所属的一些设置与其相对应的注册表键列表说明：

表 9-3 控制面板中一些设置及其相对应的注册表键

辅助选项	HKEY_Current_User\Control Panel\Accessibility
日期/时间	HKEY_Local_Machine\System\CurrentControlSet\Control\TimeZoneInformation
显示（系统设置）	HKEY_Local_Machine\Hardware\Resourcemap\Video
显示（用户设置）	HKEY_Current_User\ Control Panel\Desktop
字体	HKEY_Local_Machine\Software\Microsoft\windowsNT\CurrentVersi-on\Fonts
Internet	HKEY_Local_Machine\Software\Microsoft\windows\CurrentVersion\ Internet Setiings
键盘	HKEY_Current_User\ Control Panel\Desktop
调制解调器	HKEY_Local_Machine\Software\Microsoft\windows\CurrentVersion\UNIMODEM
鼠标	HKEY_Current_User\ Control Panel\Mouse
打印机	HKEY_Current_User\Printers
区域选项	HKEY_Current_User\ Control Panel\International

Windows 2000 提供的另外一个查看系统的配置信息的工具是“系统”信息管理单元，在管理控制台中，打开这个单元，如图 9-10 所示。

可以利用这个管理单元查看系统的硬件注册表登记。图 9-10 中展示了计算机的系统摘要，如操作系统名称、版本、计算机名、处理器类型、物理内存总量、虚拟内存总和、可用虚拟内存、页文件空间、时区、BIOS 版本等重要信息。

系统信息管理单元包括的内容远不止以上内容，它分为 3 个部分：硬件资源，包括冲突\共享、IRQ、 DMA、I/O、内存；组件部分包括多媒体、显示卡、输入、网络端口、USB、有问题的设备；软件环境部分包括驱动程序、环境变量、加载的模块、服务、程序组、启动程序和 OLE 注册。管理的范围是相当广的。如果用户对某种配置心存疑问，不需要检查注册表，可以打开系统信息管理单元。这是一个相当快捷的手段，比起在浩瀚如海的注册表中大海捞针要方便许多。

图 9-10 系统信息管理单元

其实在 Windows NT 4.0 中也有类似的工具，在 Windows NT 4.0 中叫做 Windows NT 诊断程序（Windows NT Diagnostics）。NT 诊断程序包括九个选项卡：版本、系统、显示、驱动器、内存、服务、资源、环境和网络，基本上与 Windows 2000 的系统信息管理单元功能相当。

在 Windows NT 4.0 中运行 NT 诊断程序的方法是：启动开始菜单，在“运行”对话框中输入 winmsd，相应地在 Windows 2000 中也可以输入 winmsd 来快速启动管理工具。此时的界面如图 9-11 所示，图中显示了系统的 IRQ 资源。

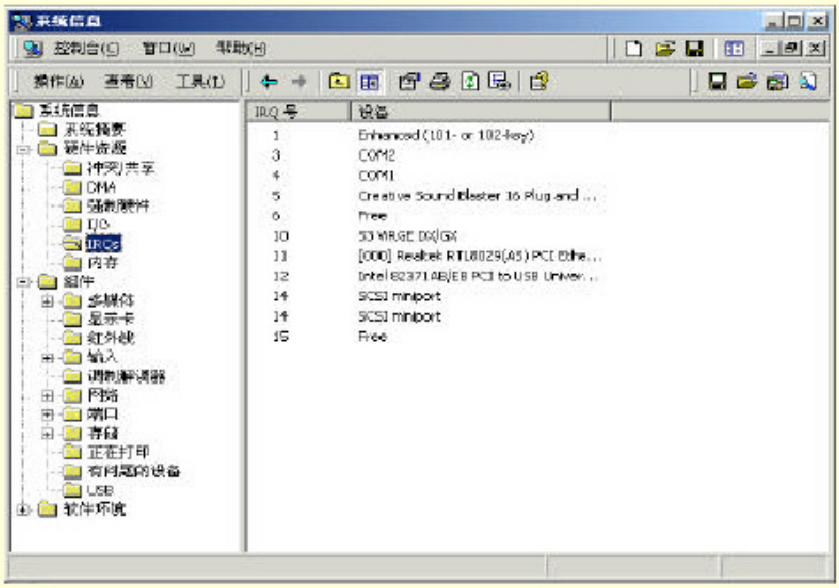


图 9-11　系统 IRQ 资源

为了方便查看，还可以把信息转存为文本文件，并打印出来。

除了控制面板和系统信息管理单元外，还可以通过本地用户和组、事件查看器、磁盘管理器等工具代替注册表进行系统管理，总之，有更直观、更方便也更安全的工具时（Windows 2000 提供了相当多的管理工具），就不要随便使用注册表编辑器。

9.5　使用注册表编辑器

非常遗憾，有时候除了直接对注册表进行编辑改动之外，别无其他办法。一定要小心！修改注册表就好像对病人转动手术刀一样需要十足的把握。新手总会感到战战兢兢，但是如果真的没有其他办法，那么就请拿出勇气，并做好相应的备份工作。俗话说：艺高人胆大，只要熟练，也会发现修改注册表并不是一件神秘的事。

9.5.1　查看注册表

Windows 2000 中有两个版本的注册表编辑器。要运行注册表编辑器，首先打开开始菜单，选择“运行”命令。在文本框中，输入 regedt32，就可以打开 regedt32 的注册表编辑器版本。

图 9-12　输入 regedt32

同样地，输入 regedit，可以打开 regedit 版本的注册表编辑器。

提示：也可以在资源管理器中找到这两个应用程序，其中 regedit 在%SystemRoot%(C:\WINNT)中，而 regedt32 在 C:\WINNT\System32 中。

建议：为了安全起见，可以设置注册表为只读模式，这样一来可以确保不会因为不小心改动而引起对注册表的破坏。设置注册表为只读模式的方法在 9.5.5 中介绍。

读者也许会问：为什么要用两种注册表呢？二者的内容是完全一致的，也许微软是为了使 Windows 95/98 和 Windows NT 的用户都能习惯原先的版本。接下来可以看到： regedit 有比 regedt32 更漂亮的界面，也更容易查找，但除此之外，就看不出它有什么更先进之处。下面是二者的简单比较：

9.5.1.1 regedit 的功能

可以编辑 Windows 95 的注册表；
支持鼠标右键，可以在弹出的快捷菜单方便地改动；
可以搜索特定的值或者数据串；
方便地导入导出注册表文件。

9.5.1.2 regedt32 的功能

相比之下， regedt32 的功能更强大，它的功能有：
支持更改字体；
支持设置只读模式，防止误删等操作；
支持设置用户对注册表的使用权限，稳妥保护注册表的安全；
支持设置审核规则，系统管理员可以审核不利于注册表安全的动作；
支持远程修改注册表等。正因为 regedt32 的强大功能，更多用户喜欢使用 regedt32。

提示：微软并不鼓励用户使用注册表编辑器，所以这两个注册表编辑器都没有显式地列出来，即没有在开始菜单中出现，也没有在管理工具中提供，用户也许只有在运行命令中输入程序名才能打开注册表编辑器。

在 regedt32 的注册表版本中，用户可以选择查看目录树或者数据，或者同时查看二者。一般都会愿意同时查看数据和目录树，就像在资源管理器中同时查看文件夹和文件一样，可以非常清楚地浏览。

9.5.2 查找注册表

用户可以层层展开注册表树，搜索一个项，值或者数据，但如果对要搜索的东西比较陌生的话，这项工作的困难远远将超出想象，因为注册表的组织实在是太纷繁复杂了。幸好有查找工具可以提供服务。

毫无疑问，在查找这方面 32 位版本的 regedit 比起 regedt32 有强大得多的优越性。

在 regedit 中，打开“编辑”→“查找”菜单，出现如图 9-13 所示的查找对话框。可以发现，在 regedit 中，可以根据项、值或者数据查找，非常方便。

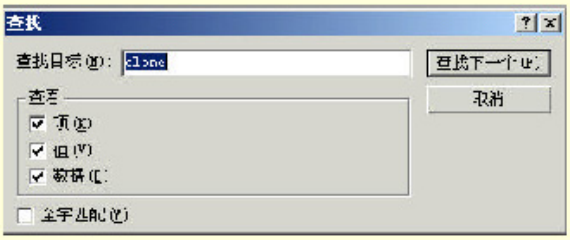


图 9-13　在 regedit 中查找

如果把“全字匹配”选项选中，将使查询结果仅限于包含整个的查找目标。但如果不能确认名称的话，推荐不要选中这个复选框，因为许多项或者数值的名字都是组合名，比如涉及登录的就有许多项，logon 也许只是长名中的一部分。

而在老版本的 regedt32 中，就没有如此幸运了。

在 regedt32 中，打开“查看”→“搜索项”菜单，如图 9-14 所示，用户将发现，在查找对话框，只能查找项，而无法像 regedit 那样，可以根据值或者数据查找，而且查找方向只能向上或者向下，如果不巧需要查找的项在相反方向的话，必须查找两次。

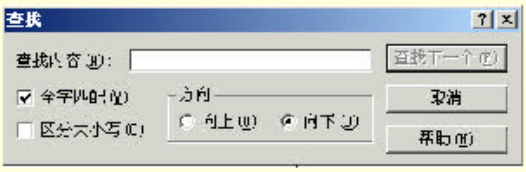


图 9-14　在 regedt32 中查找

9.5.3　添加新项或者值

regedt32 和 regedit 中添加的功能差不多。添加又可以分为添加新值或新项，而添加新值又可以分为添加新的不同数据类型的值。

在 regedt32 中，选择“编辑”→“添加项”或者“编辑”→“添加值”命令，与添加新项不同之处在于，添加新值时还需要选择数据类型，可以选择 REG_SZ、REG_EXPAND_SZ、REG_DWORD、REG_MULT_SZ 等，如图 9-15 所示。

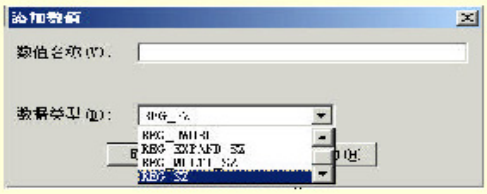


图 9-15　添加新值

在 regedit 中，相应地可以通过打开“编辑”→“新建”菜单，创建新的项或值，方法同上类似，这里就不赘述了。

需要注意的是，如果使用的是 regedt32 版本，而且当前激活的根键是 HKEY_USERS 或者 HKEY_LOCAL_MACHINE，那么“添加键”命令不能在根键下使用，如果需要添加注册表键，只能用“注册表”→“加载配置单元”命令，如图 9-16 所示。

在 regedit 版本中，也不能在 HKEY_USERS 或者 HKEY_LOCAL_MACHINE 根键下添加新项，用了这个命令后，系统会出现出错框，提示无法创建项，写入注册表时出错。

加载配置单元后，新加载的文件将成为当前项的子项。加载单元后，如果觉得不满意，可以在原菜单中，选择“卸载配置单元”命令，将加载单元卸载。

图 9-16 加载配置单元

加载配置单元和卸载配置单元命令只有 regedt2 的注册表版本中才提供，在 regedit 中没有这个命令。

提示：必须作为管理员或者管理员组成员登录，才能加载配置单元和卸载配置单元。如果是通过网络登录，还需要得到系统策略的允许。

9.5.4 添加入收藏夹

在 regedit 中，可以将键添加入收藏夹。方法是：

（1）打开“收藏”菜单，选择添加到收藏夹命令，如图 9-17 所示。

图 9-17 添加到收藏夹

（2）在如图 9-18 所示的对话框中，输入新收藏夹名。

通过收藏夹，用户可以方便地组织最近需要频繁访问的注册表键。

当不需要访问后，可以在如图 9-17 所示中的编辑器界面中，选择“收藏”→“删除收藏夹”命令，删除添加的收藏夹。

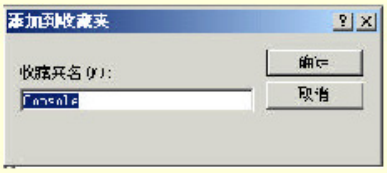


图 9-18　输入收藏夹名

9.5.5　修改注册表

现在可以真正修改注册表了。但还有一件事情：如果用户是新手，请在第一次查看注册表各项设置前首先将注册表设为只读模式，方法是 4：

（1）打开 regedt32 的注册表版本。

（2）选择“选项”菜单的“只读模式”命令，确认该选项前有选中标志，如图 9-19 所示。

图 9-19　设置注册表为只读模式

将注册表设为只读模式后，另一选项“确认删除操作”将变为灰色，表明它已经失效。这样一来即使用户不小心做了改动，系统也不会保存改动，不会有任何危险。

需要说明的是，只能在 regedt32 的版本中才能设置只读模式，在 regedit 中并没有这个选项。

再提醒一次：许多情况没有必要直接修改注册表。在 9.4 节中，介绍了许多利用其他工具的办法，它们不但界面友好，而且更加安全。只有一些实在没有良策的情况时，才应该考虑修改注册表。

在安全性设置一章中，我们已经看到了修改注册表以不显示上次登录用户名的例子，现在再来看看其他一些具体修改注册表的实例。

9.5.5.1　设置自动登录

设置自动登录将使系统自动填写登录用户的密码，以实现登录的完全自动化。可以添加一个注册表数值以实现这个功能。需要注意的是：这个设置需要允许自动登录，同时修改默认的用户名，否则系统填写的用户名和密码不匹配，将无法登录。

方法如下：

（1）启动 regedt32 注册表版本。

（2）选择 HKEY_LOCAL_MACHINE 窗口。

（3）依次展开以下键：　HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon。如图 9-20 所示是 Winlogon 子键下的数据。

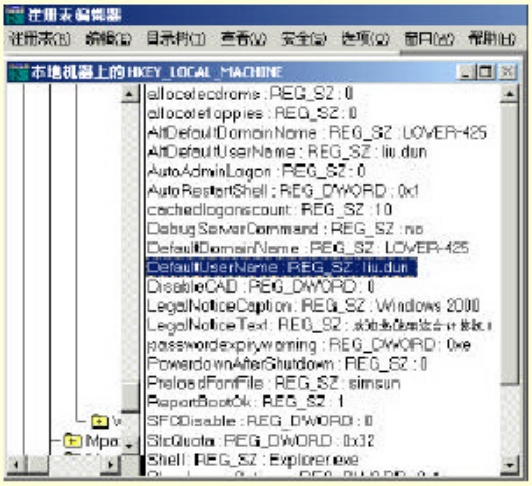


图 9-20 Winlogon 下的数据

（4）依照前面所述，首先检查 DefaultUserName（默认的用户名）数据是否合适，如果不合适，双击数据，在字符串编辑框中修改为自己的用户名。

注意：此时如果提示注册表处于只读状态，参照设置只读状态的方法，在如图 9-19 所示中，取消只读状态。

（5）将 AutoAdminLogom 值设为 1。这个值缺省为 0，即用户必须经过登录对话框登录。

（6）选择“编辑”→“添加数值”菜单命令，打开添加数值对话框，如图 9-21 所示。在“数值名称”文本框中，输入 DefaultPassword（不含空格），并从“数据类型”下拉列表框中，选择 REG_SZ。

图 9-21 添加 DefaultPassword 值

（7）单击“确定”按钮。此时出现字符串编辑器对话框，如图 9-22 所示，在文本框中，输入与默认的用户相匹配的密码。

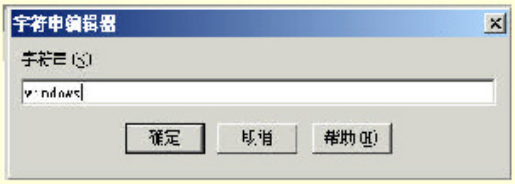


图 9-22 输入密码

单击“确定”按钮后，系统将保存新的注册表值。设置完成后，系统下次启动时，将实现自动登录功能。

注意：上面所举的例子仅仅是为了介绍注册表的使用。设置自动登录是非常不安全的，因为用户缺省都有查看注册表的权限，这样一来任何登录的人都可以获得用户名和密码，因此几乎在任何时候也不要将注册表设置改动为注册表。除非是用于非联网或者不存放敏感数据的计算机。

提示：如果是在域中登录，还需要设置登录的域名（DefaultDomainName）。

当需要去除这个功能时，将 AutoAdminLogon 值重新设置为 0 即可。另外，如果启动时临时改为需要输入用户名和密码，则在登录前一直按住 Shift 键不放，就会出现登录对话框，要求输入用户名和密码。

9.5.5.2　更改登录的背景

可以选择登录时的背景图案，也即要求按“ Ctrl+Alt+Del ”登录时的背景图案，方法如下：

（1）运行 regedt32。

（2）选择 HKEY_USER 窗口。

（3）选择 HKEY_USER\DEFAULT\ControlPanel\Desktop 键。

（4）找到 Wallpaper 数值，缺省时这个数值名为空，双击打开字符串编辑器。如图 9-23 所示，输入代表背景图案文件的路径名，比如以 bmp 为后缀名的文件。

图 9-23　输入背景图案的路径

同上面一样，必须注销后重新登录测试。

9.5.5.3　设置最大支持的处理器数目

如果计算机中安装了多处理器内核，可以设置系统最大支持的处理器数目。方法是：

（1）在 regedt32 版本中，选择 HKEY_LOCAL_MACHINE 窗口。

（2）选择区性择该窗口下的\SYSTEM \CurrentControlSet \Control \SessionManager \RegisterProccessor 键，缺省时支持的处理器数目是 2。双击该值进行改动，如图 9-24 所示。

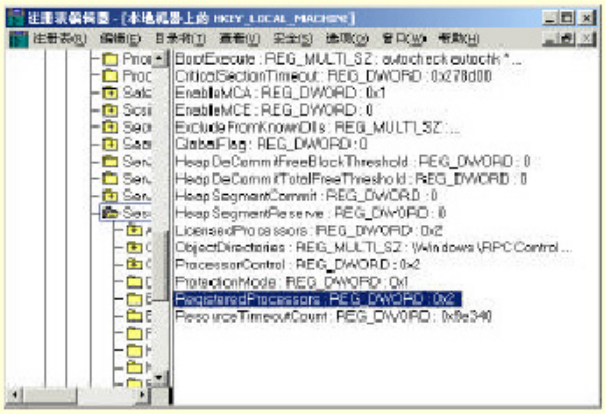


图 9-24　最大支持的处理器数目

9.6　保护注册表

Windows 2000 可以对注册表进行周密的保护，防止用户滥改注册表，或者窥视系统秘密的可能。前面已经介绍了 Windows 2000 提供的利用只读模式保护注册表的安全的方法，但这种方法对象是没有恶意的用户，如果有人存心要进行破坏，就根本不会理睬这个模式。所以系统管理员应该更加严格地设置访问权，从根本上限

制用户使用注册表的权限。

Windows 2000 支持对注册表的权限设置，正如同可以设置对文件、文件夹、打印机等系统资源对象的访问权限一样。不过，只有在 regedi32 的版本中，才能进行权限的设置，而 regedit 中没有这个能力，这又一次体现了 regedi32 较之 regedit 的优越性。

9.6.1 设置权限

首先选定设置的键，接着在 regedi32 中，打开“安全”菜单的“权限”命令，如图 9-25 所示。

如图 9-25 所示的界面中显示了选择的注册表项及其所有者，在名称列表中，列出了拥有权限的用户名单以及他们的权限。

读者应该已经熟悉了在资源管理器中设置文件夹或者文件的访问权限，设置注册表权限的方法同设置文件权限基本上是一样的。

对于每个用户或组，基本权限可以是读取或者完全控制，显然只有读取权限的用户所能做的操作是相当有限的，他们不能修改注册表；而享有完全控制的用户则被允许访问或者修改注册表。

如果需要作更细致的分配工作，则从访问类型下列框中，选择“选择性访问”命令。如图 9-26 所示，弹出选择性访问对话框。如果使用过 Windows NT 4.0，就不会对选择性访问感到陌生，另一方面，它和权限管理一章中介绍过的特殊权限设置（special permissions）也很相像，可以利用这个对话框分配更加具体的权限。

图 9-25 设置注册表的访问权限

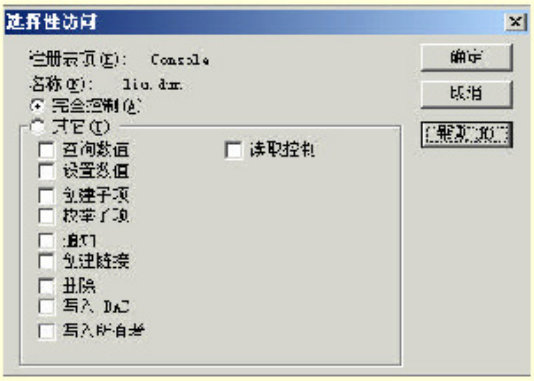


图 9-26 选择性访问

在“其他”框中，列出了具体的选择性访问权限设置。表 9-4 对这些权限设置说明如下：

表 9-4 选择性访问

查询数据	从注册表中查询并读取数据
设置数值	设置注册表键的值
创建子项	为选定的注册表项创建子项

枚举子项	标识项的子项和值的入口
通知	从注册表中审核通知事件
创建链接	为所选的想创建符号链接
删除	删除选定的项
写入 DAC	允许更改项或值的访问权限
写入所有者	有权获得所有权
读取控制	允许读取设置的权限

如果需要添加设置权限的用户或者组，在如图 9-25 中，单击“添加”按钮，出现如图 9-27 所示的对话框。图中列出了计算机中的组，如果没有列出具体的用户，则单击“显示用户”按钮，就会出现用户列表。

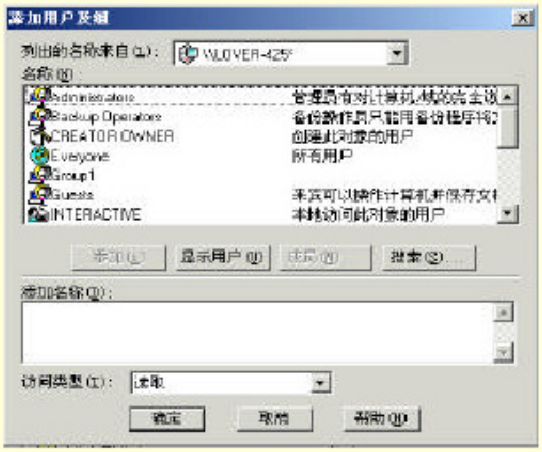


图 9-27　添加用户或者组

选择需要添加的用户或者组，单击“添加”，选择新加用户或组的访问类型：读取或者完全控制，然后按“确定”。要细分权限，在如图 9-25 所示中，使用选择性访问命令。

需要删除拥有权限的用户，选定它后，在如图 9-25 所示中，单击“删除”即可。

也许希望像在资源管理器中设置文件夹权限时同时设置子对象的权限那样，这也可以做到。在如图 9-25 所示中，设定用户对某个键权限后，选中“替换已有子项的权限”，就可以同时设置当前项及其所有子项的权限。

注意：并非对注册表的访问权限设置得越严格越好，过于苛刻可能适得其反，导致系统不能访问和修改注册表，严重时甚至无法引导。所以应该只对那些必须限制访问的区域设置访问许可，而且在设置权限前，一定要对注册表做备份工作。

9.6.2　设置审核

设置审核是保护注册表安全的重要组成部分，系统管理员可以通过审核及时发现存在的对注册表安全不利的动作，比如对敏感项的访问，企图修改键值，或者发现是谁对注册表作了改动。只有系统管理员或者在组策略中被赋予权限的用户才能审核注册表。

设置审核时，首先需要选定设置的键，在 regedi32 中，打开“安全”菜单的“审核”命令，如图 9-28 所示。

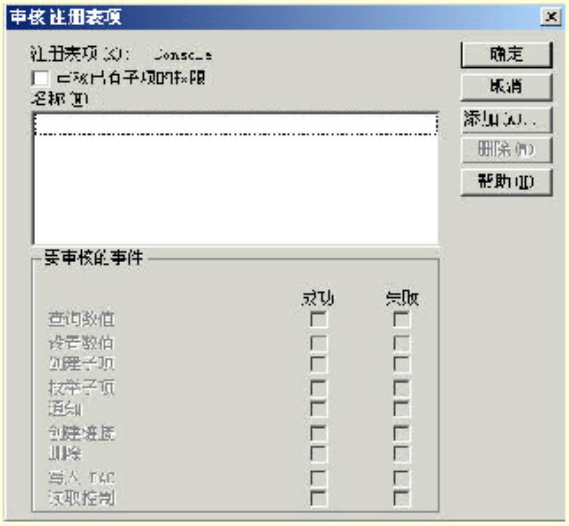


图 9-28 审核注册表项

在如图 9-28 中，要审核的事件一栏各选项都是灰色的，表明无法设置审核。这是因为还没有添加用户。要添加审核对象，按“添加”按钮，出现的选择用户或者组对话框与图 9-27 中添加用户和组完全一样，添加的道理也是一样的。可以从列表中选择要审核动作的用户或者组，这里就不赘述了。

添加用户以后，要审核的事件一栏各选项就是可选的。仔细观察后可以发现供审核的各个事件如图 9-26 所示的选择性访问权限各项也完全一样，同样有查询数据、设置数值、创建子项、枚举子项、通知、创建链接、删除、写入 DAC、写入所有者和读取控制各中选择。管理员可以对这些事件进行审核，并选择审核成功、失败的操作或者二者同时审核。一般尽量少用成功审核，因为这种事件实在是太多了，用户对桌面的更改，对应用程序的设置修改等等都会被记录，审核中将充满着这些无意义的事件，反而不利于管理员的检查。

审核的设置也可以传递给当前选定的项的子项，只要在如图 9-28 所示中的对话框选中“审核已有子项的权限”复选框即可。

9.6.3 管理所有权

注册表键的所有者可以允许其他用户取得这个键的所有权，此外系统管理员可以取得某个键的所有权，也可以为用户分配取得所有权的权力。

在 regedi32 中，打开“安全”菜单的“所有权”命令，如图 9-29 所示，可以查看当前键的所有者。

图 9-29 取得所有权

要取得所有权，单击“取得所有权”按钮即可。

9.7 注册表的保存

备份注册表是一个相当重要的工作，特别是在出于需要对注册表改动之前，更要做好备份工作。

9.7.1 在 regedt32.exe 中保存

在 regedt32 的版本中，可以将某个特定的键保存备份，方法是：

（1）选定要保存的键。

（2）打开“注册表”→“保存项”菜单命令，如图 9-30 所示。

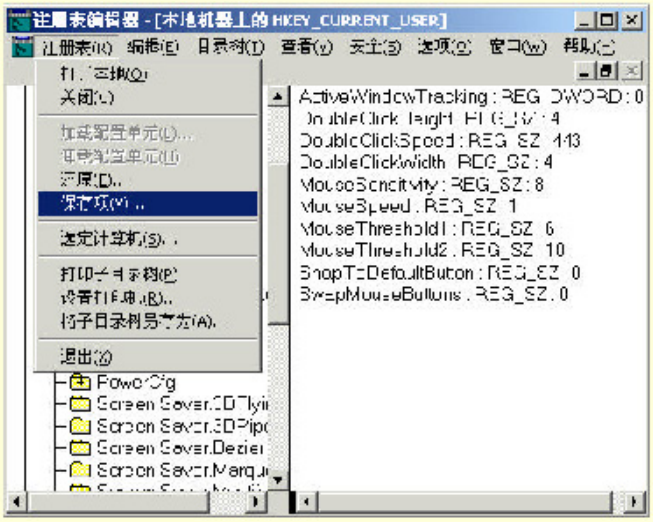


图 9-30　在 regedt32 中保存键

（3）输入保存的文件名，并选择保存的路径。可以将数据保存到磁盘、磁带或者网络上。

从注册表菜单中选择“还原”命令，可以选择备份数据来恢复注册表。

更周全的备份计划可以将子目录树另存为其他文件，在图 9-30 所示的编辑器中选择“注册表”→“将子目录树另存为”命令，按提示做下面操作。

9.7.2　在 regedit 中保存

regedit 的版本也可以方便地备份注册表，方法如下：

（1）选定要保存的键。

（2）打开“注册表”→“导出注册表文件”菜单命令，如图 9-31 所示。

图 9-31　在 regedt32 中备份

（3）在对话框中，输入保存路径和保存的名，如图 9-32 所示。选择导出的范围，可以是选定的注册表分支，也可以选择导出整个注册表。

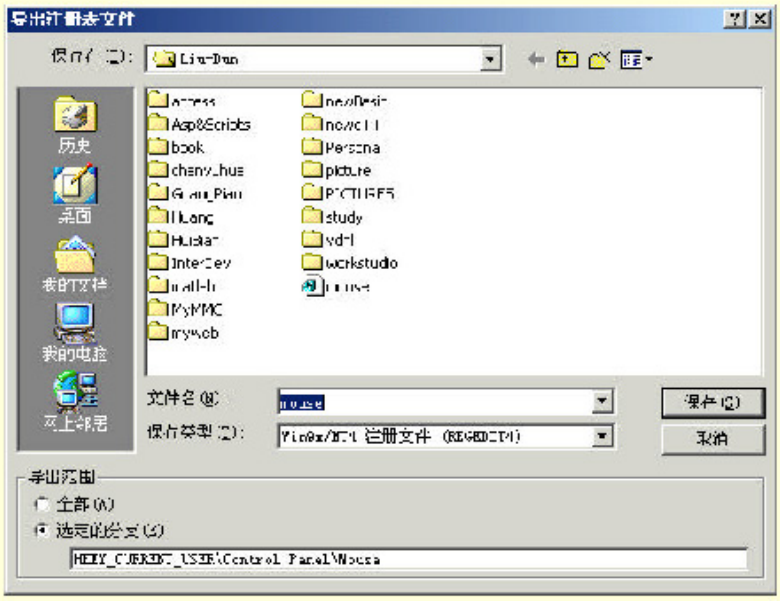


图 9-32 选择导出文件

导出文件以 reg 做后缀名，以纯文本格式存储。可以利用这个文件导入注册表，恢复原来的注册表结构。

在如图 9-31 中，选择“注册表”→“导入注册表文件”菜单命令。保存的注册表文件信息就可以成功地输入注册表。

另一方式，也可以在资源管理器中找到保存的注册表文件，双击执行，系统将自动将文件输入到注册表中。

由于导出文件以纯文本格式存储，可以在记事本中打开文件查看。仍旧在资源管理器中找到保存的注册表文件，并单击右键，在弹出的快捷菜单中，选择“编辑”命令，即可在记事本中打开，如图 9-33 所示，图中保存的是 HKEY_CURRENT_USER\Control Panel\Mouse 键的各项值。

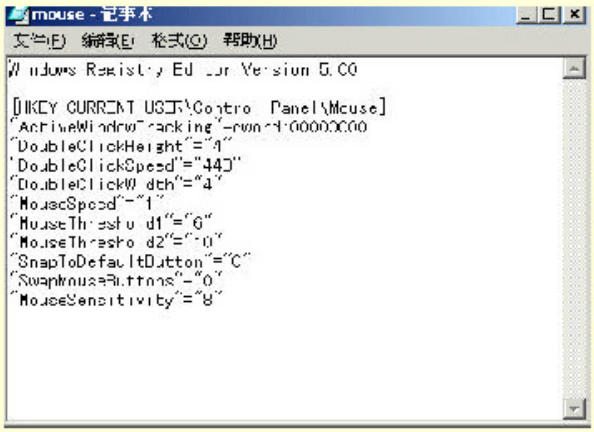


图 9-33 打开注册表文件

9.8 远程编辑注册表

作为网络管理员，可能时常会被要求解决各种客户端计算机的问题，如果必须在各地奔波，那么管理员的工作量将是难以承受的。这时候，联网提供了强有力的帮助。

许多时候，系统故障必须通过修改注册表来解决，或者至少需要查看注册表来了解发生了什么问题，有时候即使管理员知道毛病所在，但是普通用户根本无法修改注册表，因为他们没有这个权限。当然，不可能为了这一点而冒赋予用户权限的风险。这时候，远程编辑用户计算机的注册表使管理员可以免受长途跋涉之苦。

用 Windows 2000 编辑远程注册表，需要首先选定远程计算机。方法如下：

（1）启动 regedt32 注册表版本。

（2）选择“注册表”→“选定计算机“菜单，如图 9-34 所示。

图 9-34　选择远程计算机

（3）从列表中选择远程计算机或者直接输入远程计算机名，单击“确定”按钮后即可编辑远程注册表。

注意：修改远程注册表时，所做的改动会立即生效，因此可能影响到正在工作的用户，可以选择空闲的时间来进行这项工作。

需要注意：打开远程注册表时，只能看到两个根键：HKEY_LOCAL_MACHINE 和 HKEY_USERS。但正如前面所说的，读者应该已经注意到：注册表的 5 大根键其实只有这两个键是独立的，其他 3 个键在 HKEY_LOCAL_MACHINE 和 HKEY_USERS 下都有映像，另一方面，这两个根键也是最常用的注册表键。

注册表一章的介绍到此可以告一段落了。可以看到，注册表中有成千上万的配置单元、项和数据，是个名副其实的庞然大物，注册表也非常关键，请不要因此对它产生畏惧心，因其实它并不难掌握，但是有一条是必须小心的：那就是一定要做好备份工作，必须不断更新配置，并且注意每一个细节。

第 10 章　磁盘管理

早期的操作系统，如 DOS，它的主要功能就是对存储在磁盘上的信息进行管理（其实 DOS 就是 Disk Operating System 的简称，即磁盘操作系统）。发展到后来，出现了 Windows 3.x 操作系统，它们为用户提供了方便的可视的浏览及磁盘资源的功能，这主要是指其中的文件管理器（File Manager），但它还不够完善，以至于在后期的 Windows 95、Windows 98 出现了功能更强大的资源管理器。Microsoft 所做的这一切无非是想提供给用户一个方便的磁盘资源管理工具。同时也可以看出，虽然现在的微型计算机能做的事情很多，如多媒体、网络访问、游戏等等，但管理磁盘上的信息资源仍然是计算机的主要任务，网络服务器更是如此。Windows 2000 不但继承了这些优点，而且还从 Windows NT 处学到了强大的安全管理功能。Windows 2000 下的文件系统功能会令使用者赏心悦目，而且在设置磁盘分区和存储盘卷上给用户提供更大的自由度。它不再限制用户在每个硬盘上只能有一个单独的主分区。Windows 2000 允许用户在一个物理硬盘上创建多个主分区，一个磁盘卷还可以扩展到多个硬盘上，且其容量可以扩展到非常大。Windows 2000 采用的文件系统 —NTFS 比 FAT 有着更强大的纠错功能。NTFS 还支持文件级的压缩，这些都是以前的操作系统无法比拟的。另外，Windows 2000 对磁盘有了一项新的管理功能 —磁盘配额管理，我们将在以后的小节中详细讲解。总之，Windows 2000 与以前的操作系统相比，既有相同的地方又有本质上的区别，这些也正是 Windows 2000 的优点所在。

本章内容包括：

- 理解硬盘、分区和磁盘卷
- 文件系统
- 使用磁盘管理
- 管理磁盘分区
- 使用基本卷
- 使用动态卷
- 使用跨区卷（卷集）
- 使用带区卷
- 使用镜像卷
- 使用 RAID-5 卷
- 使用磁盘碎片整理
- 使用磁盘配额

10.1　理解硬盘、分区和磁盘卷

Windows 2000 下物理硬盘和驱动器盘符的关系并不是很明确的对应关系。它分为两种情况：一种是一个物理硬盘对应多个磁盘卷，一个磁盘卷对应一个明确的驱动器盘符。另一种情况是，一个指定的磁盘卷对应多个硬盘或多个硬盘的一部分。也就是说，可以用一个驱动器盘符来访问多个硬盘的一部分。要想充分利用以上这些功能，需要了解一些关于 Windows 2000 设置硬盘、分区、驱动器和磁盘卷的原理。

10.1.1　硬盘

Windows 2000 能够支持各种各样的存储设备，如硬盘、软盘、只读光驱、读/写光驱、磁带机等等。但我们平常使用最多的仍然是硬盘，因为它具有存储速度高、存储容量大、安全性高、低能耗等特点。

衡量硬盘的性能需要看几个指标，它们是：硬盘的容量、速度和接口类型。应该说硬盘的容量越大越好，毕竟我们现在要装的东西越来越多，尤其是网上有许多吸引人的文件，稍不留神就下载了不少，硬盘容量大就不用太在意这个问题了。现在硬盘的技术越来越先进，单片的容量越来越大，导致每兆字节的价格降低。现在市场上的硬盘容量最大的有 73GB 的，转速为 10000r/min，但不建议用这么大的硬盘，毕竟它太贵，除非是用

在服务器上。对于一般用户 20GB 就差不多了。

硬盘的速度是系统的瓶颈之一，它会拖慢整个系统的速度。影响速度的因素很多，如转速、磁头形式、寻道时间、缓冲区容量等。其中转速是一个关键的问题。目前硬盘的转速有 3600r/min、4500r/min、5400r/min、7200r/min 甚至于 10000r/min。理论上讲，转速越快越好。因为较高的转速可以缩短硬盘的平均寻道时间和实际读写时间。可是转速越高发热量越大，不利于散热。现在主流硬盘的转速一般在 7200rpm 以上。

接口界面标准也是影响硬盘速度的一个因素，硬盘的接口分为 EIDE（Enhanced Intelegrated Device Electronics）和 SCSI（Small Computer System Interface，小型计算机系统界面）两种。对比这两种硬盘，EIDE 的价格便宜，性能好，容易安装，能增加的外设较少，CPU 占用率从 30%到 50%以上；SCSI 的性能则更好，速度更快，能增加的外设更多，CPU 的占用率为 4%到 6%，能更好利用 CPU 资源，但其安装较复杂，需要购买一块 SCSI 卡，价格昂贵。

10.1.2　分区

一个操作系统在安装到硬盘上以前，要对硬盘进行分区处理，这样才能在硬盘上存储文件。一个分区就是硬盘上的一个逻辑划分，一个分区上可以包括若干个格式化的存贮卷。分区分为两类，即主分区和扩展分区。

Windows 2000 允许将一个硬盘最多分为 4 个分区，它们或者由 4 个主分区构成，或者最多由一个扩展分区及 3 个主分区构成。也就是说如果需要 4 个以上的逻辑驱动器号（字母）或分区，就必须在一个扩展分区里创建逻辑驱动器。考虑到这方面的原因，事先安排好物理驱动器的布局是相当重要的。在一个扩展分区里，倘若使用的是标准的 BackOffice 应用程序，就可以创建任意数量的逻辑驱动器。但是同时存在一个不可避免的物理限制，那就是可用的驱动器字母数量。在 Windows 2000 中，最多可以分配 26 个驱动器字母，也就是说可以一个扩展分区里存在 26 个逻辑驱动器。

主分区是用未分配的磁盘空间创建的一个卷，它可以被设置为引导 windows 2000 或者其他操作系统的分区。MS-DOS/Windows 95 和 Windows 98 系统在一个给定的硬盘上只能识别出一个主分区，即用来引导该系统的分区。而 Windows 2000 和 Windows NT 在一个硬盘上最多可以创建 4 个主分区，并且主分区只能创建在物理硬盘上。

扩展分区顾名思义就是可以用来扩展出更多的子分区的磁盘空间。它能够将一个硬盘分为若干个存储卷。比如说，Windows 2000 最多支持 26 个存储卷。如果不将扩展分区设置为包括了一个或多个逻辑盘，它将不能用于存储文件。在 Windows 2000 和 Windows NT 系统中，扩展分区用于当有必要在一个硬盘中分配多于 4 个驱动器盘的情况。扩展分区可以占据创建主分区之后所剩的所有空间。用户无法从一个扩展分区引导，而且每个硬盘只能有一个扩展分区。

提示：给磁盘分区的原因

可能因为以下几个原因要对磁盘分区：

（1）你需要 NTFS 的安全性，但有时你必须使用 MS-DOS 运行老的应用程序，而它需要 FAT 文件系统。

（2）你发现把某些类型的文件放在不同的卷上可以更容易组织、管理和备份文件。

10.1.3　磁盘卷和驱动器

在分区被创建之后，它们必须被格式化以建立可用于文件存储的磁盘卷，这些磁盘卷对应着我们熟悉的驱动器盘符：C、D、E、F 等。因此，具有一个硬盘的系统在 Windows 2000 Explorer 中也可以显示出多个本地硬盘，它们是以卷的面貌出现的。扩展分区中的每一个磁盘卷都可以独立地按照 NTFS 或 FAT 文件系统进行格式化，这样它们就可以被视为一个物理上独立的磁盘驱动器。以上讲的都是基本存储方式，还有一种存储方式，叫做动态存储。它包括简单磁盘卷（Simple Volume）、跨接磁盘卷（Spanned Volume）、镜像磁盘卷（Mirrored Volume）、带区磁盘卷（Striped Volume），以及廉价多余磁盘阵列（RAID）-5 磁盘卷。动态磁盘是通过升级基本磁盘来创建的。关于动态磁盘的知识，将在以后的小节中详细讲述。

提示：在安装 Windows 2000 过程中，可以将 Windows 2000 设置成从主分区启动，但从扩展分区中的一个逻辑驱动器运行。

10.2 文件系统

文件系统是指在一个操作系统中，文件被命名、存储和组织的全面结构。一个物理硬盘上的分区或卷只有在被格式化成某一个特定的文件系统后，才能用来存储文件和对文件进行管理。文件系统可以分为以下 3 种：FAT（File Allocation Table 文件分配表）、FAT32 和 NTFS（Windows NT 文件系统）。Windows 2000 支持这 3 种文件系统。现在讨论一下这 3 者各自的特点。

10.1.3.1 NTFS 提供了以下功能：

（1）文件夹和文件级别的安全性

NTFS 为在它卷上的每个文件或文件夹存有一个用户访问权限列表，它被称为访问控制列表（ACL，Access Control List）。当用户试图访问一个文件或文件夹时，Windows 2000 就去检查 ACL，并根据 ACL 中的用户的许可入口授予访问权。

（2）磁盘管理功能

·压缩：NTFS 支持文件级别的压缩，以便在一个分区中存放更多数据。

·磁盘配额：NTFS 按照针对用户的原则来控制硬盘，以限制每个用户所能使用的最大的磁盘空间（关于“磁盘配额”的具体内容，将在本章的后几节中详细讨论）。

·加密：NTFS 支持文件级别的数据压缩，用以防止未经授权的访问。

（3）大文件和大分区尺寸

NTFS 典型的硬件的最大可用分区是 2048GB，这由工业标准和硬件在磁盘扇区的最大数目和尺寸上的限制来决定的。

（4）增强的容错功能

Windows 2000 将磁盘的读写动作记录在事务日志上，从而在错误发生或是硬件故障中断了磁盘的写操作时回退到初始状态或是再进行一次。事务日志可以保护整个文件系统不至于像采用 FAT 或 FAT32 文件系统时出现系统崩溃事件。

（5）NTFS 支持热修复（Hot-Fixing）

当文件出问题的时候，NTFS 不是显示 FAT 中常见的 Abort（退出）、Retry（重试）、Fail（失败）信息，而是试图以一种对用户透明的方式将坏簇（Cluster）中的数据移到一个新的地方，然后将坏簇标志为“不可用”。不过，由于存在数据恶化的可能，因此移动后的数据也有可能是不可用的，但如果采用了容错技术，则从未损坏的簇中复制的数据仍是可用的。

（6）支持长文件名

NTFS 不再将文件名的长度限制在 MS-DOS 所要求的 8+3 文件名命名规则下。它最多可以支持总长达 255 个字符的文件名，但由命令行创建的文件名最长达 253 个。

10.1.3.2 FAT 和 FAT32 支持以下的功能

（1）FAT 是一个受到广泛支持的文件系统，但它较老而且效率不高。它所支持的单个分区最大可以到 2GB。它还支持采用其他操作系统的双引导机制，例如，Windows 95、Windows 98 和 MS-DOS。

（2）FAT32 是 FAT 的增强版本。对于 Windows 2000 而言，FAT32 所支持的分区最大可以到 32GB。在大容量硬盘上，它所支持的簇的尺寸也比 FAT 要小。所以 FAT32 可以比 FAT 有更高的空间利用率。FAT32 也支持采用其他操作系统的双引导机制。

（3）要改善存储效率，通常对 FAT 卷进行压缩。压缩实用程序一般包括在 MS-DOS 的后期版本、Windows 95 和 Windows 98 中，也可以从第三方软件厂家中得到。

提示：如果在安装 Windows 2000 的时候，你选择将引导分区格式化为 NTFS 文件系统，那么 ACL 会自动对系统进行设置，并对 Windows 2000 系统文件进行保护。

下面对 NTFS 和 FAT、FAT32 进行总结性的比较：

表 10-1　NTFS 和 FAT、FAT32 的比较

NTFS	FAT 和 FAT32
支持文件或文件夹级别的安全性	根本不支持文件的安全性保护
支持文件或文件夹的压缩	不支持文件的压缩
支持文件或文件夹的加密保护	不支持文件加密
可以对磁盘进行磁盘配额管理	不可以进行磁盘配额管
支持大文件及大分区	对于 FAT32，分区最大为 32GB
提供强大的磁盘容错功能，出错后可以自动标识坏区	出错后只能由用户参与处理

10.3　使用磁盘管理

在 Windows NT 4.0 中，“ 磁盘管理器 ”被单独提出来并放置在“ 程序 ”菜单的“ 管理工具 ”下面。在 Windows 2000 中“ 磁盘管理器 ” 被重新命名为 “ 磁盘管理 ”，而且它被放置在 “ 计算机管理 ” 模块中。磁盘管理是一个图形化的磁盘管理工具，它支持对卷、分区、逻辑驱动器、新的动态存储和远程磁盘管理功能。

10.3.1　启动磁盘管理

由于 Windows 2000 的 “ 磁盘管理 ” 与以前的 “ 磁盘管理器 ” 的位置不一样，所以先介绍一下如何启动磁盘管理。启动磁盘管理的方法是：

（1）打开任务栏上的 “ 开始 ” 菜单。

（2）选中 “ 设置 ” →“ 控制面板 ”。

（3）“ 控制面板 ” 打开后，选择其中的 “ 管理工具 ” 并打开它；

（4）“ 管理工具 ” 中有一项是 “ 计算机管理 ”，选择并打开它；

（5）从左边的树状的控制列表选择并打开其中的 “ 存储 ” 文件夹；

（6）其中的一个文件夹叫做 “ 磁盘管理 ”，打开它就可以看到磁盘管理的界面了。

打开的 “ 磁盘管理 ” 如图 10-1 所示。

注意：如果用户不是以管理员或管理员组中的成员登陆 Windows 2000 时，计算机管理会提示出错信息，将不能使用计算机管理中的任何管理功能。

从图 10-1 中可以看到，磁盘管理功能是计算机管理中的一个功能模块，它不再以以前的 Windows NT 中的单独模块出现，这也是 Windows 2000 计算机集成管理的一个体现。从右边磁盘管理区的最下边可以看到有 3 个注释，不同的颜色代表不同的分区。以上图为例，“ 本地磁盘（C:）” 和 “ 本地磁盘（E:）” 是建立在主磁盘分区上的，而 “ 本地磁盘（D:）” 是建立在扩展磁盘分区上的。如果想要观察的舒服一些，可以将左边的控制台树关掉。具体做法是点击工具栏上的第 4 个按钮，令它呈现浮起状态即可。

另外，可以看出它有两层菜单，第一层是 “ 计算机管理 ” 的菜单，第二层才是 “ 磁盘管理 ” 的菜单。只有

对第二层菜单操作，才能进行相应的磁盘管理。

图 10-1　磁盘管理界面

10.3.2　设置显示形式

磁盘管理中的工具都是非常好用的，它易于阅读，而且显示磁盘大小的方式也非常形象。但如果不习惯相对大小和默认的颜色，可以通过磁盘管理提供的工具来改变设置。

改变磁盘区域的相对大小：

（1）选择“查看”菜单项下的“设置”。

（2）选择比例选项卡，如图 10-2 所示。

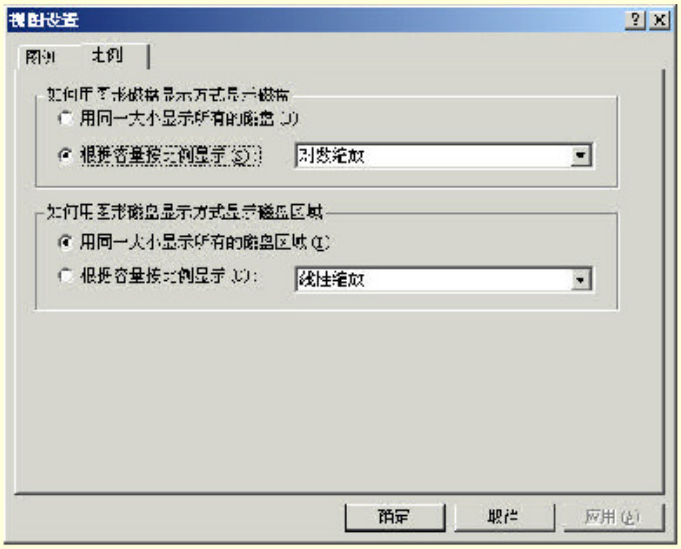


图 10-2　视图设置

（3）选择“如何用图形磁盘显示方式显示磁盘区域”框架中的“用同一大小显示所有的磁盘区域”的选项。

（4）单击“确定”按钮，如图 10-3 所示。

图 10-3　改变后的磁盘区域图形显示方式（这里去掉了左边的控制台树）

改变磁盘区域的显示颜色：

（1）选择“查看”菜单项下的“设置”。

（2）在“项目”一栏中有若干项目可以选择，选择其中的一个项目，改变相应的颜色、图案下拉式列表的选项。

（3）单击“确定”按钮。

同样可以通过查看菜单改变诸如顶端、底端所显示的内容，改变工具栏按钮等设置。它们都是很简单的操作，这里就不再赘述了。

10.3.3　关闭磁盘管理

由于磁盘管理不是一个单独的模块，所以不能将磁盘管理独自关闭，而只能关闭整个的“计算机管理”。具体的实现方法有如下几种：

（1）执行“控制台”菜单下的“退出”命令。

（2）单击屏幕右上角的“关闭”按钮。

（3）按下“Alt+F4”键。

10.4　管理磁盘分区

创建一个磁盘分区相当于在一块物理磁盘上划分一个区域用于以后存储文件。只有在一个分区上才能创建一个或多个逻辑驱动器，每个逻辑驱动器都必须在使用之前被格式化，以用来管理磁盘。删除已有分区意味着清除这一块磁盘区域上的一切东西，包括数据（文件）、文件系统等等。

10.4.1　创建一个分区或逻辑驱动器

按照 10.3.1 中介绍的方法打开“磁盘管理”，如果要创建一个分区，则选择一个基本磁盘上的未分配区域，单击鼠标右键，然后选择“创建分区”命令。按照“创建分区向导”的提示，单击“下一步”，选择是创建主分区还是创建扩展分区，然后再按照提示一步步做下去即可。

如果要创建逻辑驱动器，则选择扩展分区上的可用空间，单击鼠标右键，选择“创建逻辑驱动器”命令，并按照“创建分区向导”的提示去做即可。

10.4.2　格式化一个新的分区或逻辑驱动器

在用户使用一个新的主分区和一个扩展分区中的逻辑驱动器之前，必须把它格式化，还要给它起一个卷名，

这就等于创建了一个卷。

要格式化一个新的分区或扩展分区中的一个逻辑驱动器，具体方法如下：

（1）在“磁盘管理”窗口中，选择新创建的分区或逻辑驱动器。

（2）单击鼠标右键，选择“格式化”命令。

（3）系统会弹出“格式化”窗口，可以选择文件系统格式、分配单位大小和卷标，以及选择是否启动文件和文件夹压缩。

（4）做完上述设置后，单击“确定”按钮开始格式化，如图 10-4 所示。

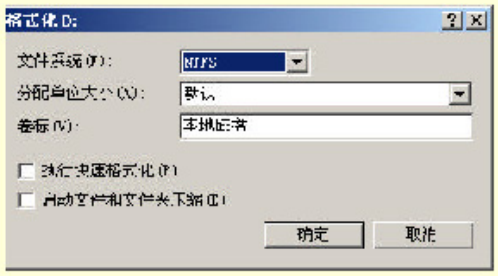


图 10-4 格式化设置

10.4.3 删除一个分区或逻辑驱动器

在做这个操作以前，必须明确的一点就是：确定这个分区或逻辑驱动器中的所有数据都是无用的或者都已经备份，只有在这两种情况下才可以做这个“危险”的动作，因为它可以令存储在这个分区或逻辑驱动器中的所有数据丢失，造成无法挽回的后果。

在基于 x86 的系统上，Windows 2000 不允许用户删除处于下列状态下的分区：

- 启动硬盘上的活动分区（比如图 10-1 所示的磁盘 C：，因为它被标为（启动））
- 存在逻辑驱动器的扩展分区；（要想删除它，需要先删除这些逻辑驱动器）
- 包含有 Windows 2000 系统文件的分区（用户可以将系统文件放在另一个分区而不是用于启动的主分区）

删除一个分区或逻辑驱动器的具体实现方法：

（1）选择要删除的分区（单击图形视图中相应的分区），注意不能选择上述 3 种状态下的分区，否则系统会提示出错，如图 10-5 所示。

图 10-5 警告信息

（2）选择“操作”菜单下的“所有任务”→“删除磁盘分区”命令，或者在其上单击鼠标右键两种情况分别示于如图 10-6 和图 10-7 所示。

（3）这时系统会提示是否真的想删除这个分区，单击“是”，这样就完成了删除分区的操作。

提示：如果想删除扩展分区，Windows 2000 要求先将扩展分区中的所有逻辑驱动器或其他卷删除，然后才能删除此扩展分区。

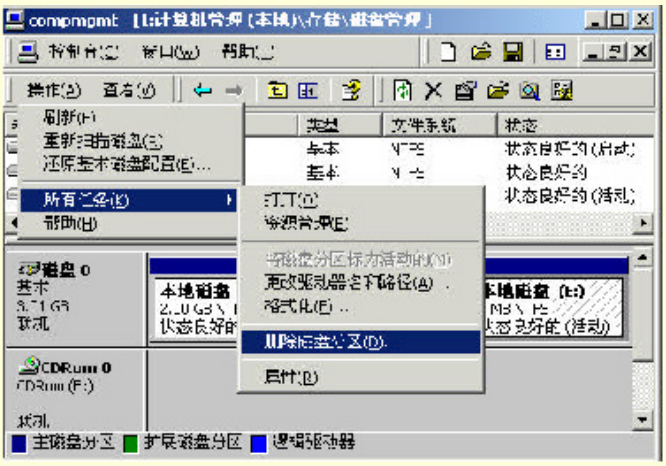


图 10-6　执行删除命令

10.4.4　标记活动分区

一个硬盘上的活动分区是一个基于 x86 的计算机的引导分区。在这些机器上，一个主分区必须被标记为活动的，这样计算机才能启动它自己和一个操作系统。活动分区必须永远在连接到系统的第一块硬盘（Disk 0）上。

要将一个分区标记为一个活动分区，要做的事情如下：

（1）在“磁盘管理”窗口中，选择要标记为活动的那个分区。

（2）单击鼠标右键，选择“将分区标记为活动”命令。

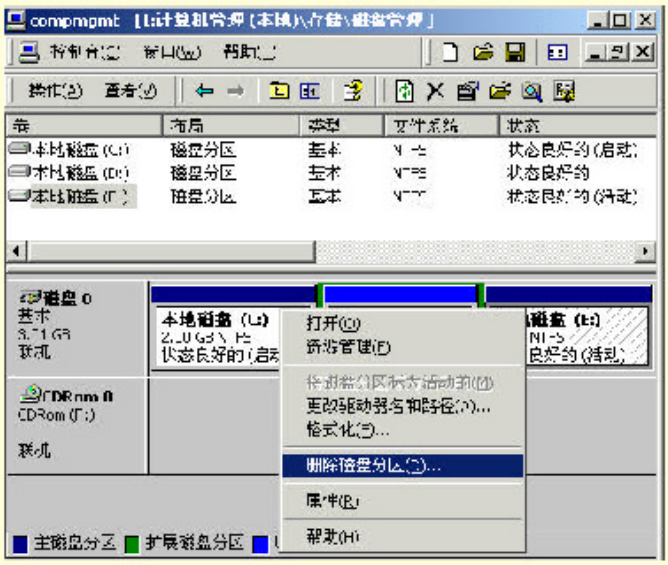


图 10-7　执行删除命令

10.5　使用基本卷

基本卷包括分区和逻辑驱动器，它是一个硬盘上被格式化成某一个文件系统的空间。

10.5.1　格式化基本卷

格式化一个基本卷，会删除此卷上的所有内容，所以执行此操作时一定要小心。在完全确定要删除时，才能做以下操作：

（1）在“磁盘管理”中选择要格式化的卷。

（2）打开“操作”菜单，并选择“所有任务”→“格式化”。

（3）系统会弹出如图 10-5 所示的格式化设置窗口，设置完成后单击“确定”。

提示：如果在设置窗口中选择了“执行快速格式化”选项，那么快速格式化将删除磁盘上的文件，但不扫描磁盘以确定是否有坏扇区。

10.5.2 更改驱动器名和路径

磁盘管理可以使用户很方便地管理磁盘上的任何一方面的内容。有时用户会新添加一个基本磁盘并创建新的卷，一般都需要对驱动器名进行重新整理，也就是更改相应的驱动器名和路径。

Windows 2000 根据几个简单的规则在启动时对驱动器分配字母：

（1）操作系统将字母 C 分配给第一块硬盘的第一个主分区，它是启动硬盘上的启动分区。

（2）字母 D 分配给第二块硬盘的第一个主分区，E 分配给第三块硬盘的第一个主分区。 （3）将剩下的字母依次分配给第一块硬盘的其他分区，然后是第二块硬盘的其它分区。

（4）Windows 2000 将字母分配给所有分区后，给 CD-ROM 和其他可拆卸盒式磁带机分配字母。

（5）Windows 2000 可以给驱动器分配 24 个字母，其中字母 A 和 B 保留下来给软盘驱动器使用。

要把一个字母分配给一个基本卷，则需要按照如下方法去做：

（1）在磁盘管理中选择要分配驱动器字母的卷。

（2）打开“操作”菜单，选择“所有任务”→“更改驱动器名和路径”。

（3）此时系统会给出“更改本地磁盘（D：）的驱动器号和路径”窗口，如图 10-8 所示。

图 10-8 更改驱动器号和路径

（4）如果要对新创建的卷分配驱动器字母，那么单击“添加”按钮，系统会给出“新加的驱动器号和路径”窗口，选择一个字母，然后单击“确定”按钮。

（5）如果要改变原有的驱动器名，那么单击“编辑”按钮，弹出“编辑驱动器号和路径”窗口，在“指派驱动器号”的下拉列表框中选择一个字母，然后单击“确定”按钮。

（6）如果要删除现有的驱动器号，则单击“删除”按钮即可。

10.5.3 删除逻辑驱动器

删除逻辑驱动器会删除此驱动器中所有的数据，这是一个非常危险的操作，执行此操作前一定要想清楚，否则会丢失大量的数据。

删除逻辑驱动器的具体方法是：

（1）在“磁盘管理”中选择要删除的驱动器。

（2）单击操作菜单下的所有任务，选择删除逻辑驱动器。

（3）系统会弹出警告信息窗口，如果真的要删除则单击“是”按钮，否则单击“否”按钮。

10.6　使用动态卷

动态卷是 Windows 2000 的新特性，只能在动态磁盘上创建。使用动态磁盘，系统就不再限制每个磁盘使用 4 个主分区或 3 个主分区和一个扩展分区了。

10.6.1　概述

动态磁盘是 Windows 2000 所特有的，只有在运行 Windows 2000 的计算机上才能访问动态磁盘上的动态卷。动态卷有 5 种类型，分别是：简单卷、跨区卷、镜像卷、带区卷和 RAID-5 卷。

注意：在便携计算机上是不支持动态卷的，并且只有在运行 Windows 2000 Server 的计算机上才能使用镜像卷和 RAID-5 卷。

10.6.2　将基本磁盘升级为动态磁盘

既然只有在动态磁盘才能创建动态卷，那么现在就介绍一下如何将基本磁盘升级为动态磁盘。要将基本磁盘升级为动态磁盘，需要做的事情如下：

（1）选择要升级的基本磁盘（比如磁盘 0）。

（2）单击“操作”→“所有任务”→“升级到动态磁盘”菜单。

（3）系统弹出“升级到动态磁盘”窗口，单击“确定”按钮，如图 10-9 所示。

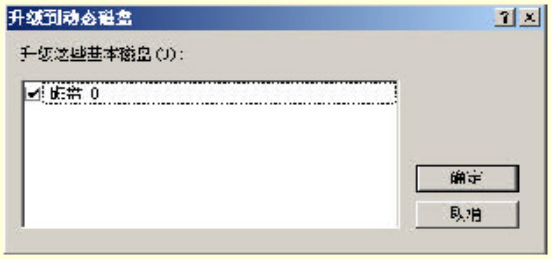


图 10-9　升级到动态磁盘

10.6.3　格式化动态卷

基本磁盘被升级到动态磁盘后，可以对其上的卷进行诸如格式化、分配驱动器名和路径、删除等操作。要格式化一个动态卷，需要做如下的事情：

（1）在“磁盘管理”中选择要格式化的动态卷。

（2）单击“操作”菜单下的“所有任务”→“格式化”。

（3）系统会弹出如图 10-4 所示的格式化设置窗口，设置其中的选项后，单击“确定”按钮。

10.6.4　更改或删除驱动器号

要更改或删除由动态卷创建的驱动器号，需要做的工作和更改或删除基本卷上创建的驱动器号相同，且分配字母的方法也相同。具体方法如下：

（1）在磁盘管理中选择要分配驱动器字母的卷。

（2）打开“操作”菜单，然后选择“所有任务”→“更改本地磁盘（D：）的驱动器名和路径”。

（3）此时系统会给出“更改本地磁盘（D：）的驱动器号和路径”窗口，如图 10-8 所示。

（4）如果要对新创建的卷分配驱动器字母，那么单击“添加”按钮，系统会给出“新加的驱动器号和路径”窗口，选择一个字母，然后单击“确定”按钮。

（5）如果要改变原有的驱动器名，那么单击“编辑”按钮，弹出“编辑驱动器号和路径”窗口，在“指

派驱动器号”的下拉列表框中选择一个字母，然后单击“确定”按钮。

（6）如果要删除现有的驱动器号，则单击“删除”按钮即可。

10.6.5 删除动态卷

和删除基本卷相同，这会删除此卷上的所有数据，执行时一定要小心。

删除的具体做法是：

（1）在“磁盘管理”中选择要删除的驱动器。

（2）单击操作菜单下的所有任务，选择删除逻辑驱动器。

（3）系统会弹出警告信息窗口，如果真的要删除则单击“是”，否则单击“否”。

10.7 使用跨区卷（卷集）

从前面可以看到 Windows 2000 可以使用多于一个的物理硬盘和磁盘分区，这就为由多个硬盘上的多个互相不连续的、大小不一的空间组成一个卷创造了条件。这些空间可以来自最多 32 个硬盘上的空闲空间，它们被组织在一起，并为其赋予一个驱动器字母。这样一个磁盘空间的集合就叫做跨区卷。在 Windows NT 4.0 和以前的操作系统版本中，跨区卷被称为卷集。

创建卷集有许多好处，比如说，它不用重新对磁盘进行分区就可以把几个较小的区域结合成一个大的逻辑区域；它减少了使用的驱动器字母，这是因为一个驱动器字母就可以引用一个或多个硬盘上的多个存储空间。

但是卷集有一个致命的缺点，那就是当组成卷集的一个硬盘上的一块存储空间发生问题，比如硬盘的物理破损导致这一存储空间不能访问，那么这个卷集中的其他硬盘上的其它空间也不能被访问，使整个的卷集崩溃，并造成数据丢失。

如图 10-10 所示，表明一个跨区卷形成的过程。跨区卷所拥有的空间可以是所有未分配空间的总和，也可以是它们中的一部分。

图 10-10 跨区卷形成示意图

10.7.1 创建一个跨区卷

这里首先要说明的一点是，Windows 2000 的“磁盘管理”对基本磁盘上的卷集提供有限支持。可以删除卷集，但是不能在基本磁盘上创建新的卷集或扩展卷集。而只能在动态磁盘上新建跨区卷。如果要在动态磁盘上创建一个跨区卷，就必须有一个或多个硬盘，并且每一块硬盘上至少有一个未分配空间。在安装 Windows 2000 时，一般会将所有的硬盘空间都分配出去，如果想要创建一个跨区卷，可通过删除已有分区或逻辑驱动器来创建空闲空间。

在上述条件满足时，可以通过以下方法创建一个跨区集：

（1）打开“磁盘管理”工具；

（2）单击右键要创建跨区卷的动态磁盘中的未分配空间，然后单击“创建卷”；

（3）或者按住 Ctrl 键，鼠标左键单击跨区卷要包含的多个硬盘上的多个未分配空间，然后单击鼠标右键，选择“创建卷”；

（4）在创建卷向导中，单击“下一步”，再单击“跨区卷”，然后按照屏幕上的指令操作即可。

提示：“磁盘管理”工具只有在动态磁盘上才能创建跨区卷，所以所有用来创建跨区卷的硬盘一定要先升级为动态磁盘。跨区卷最多可以扩展到 32 个动态磁盘，而且跨区卷不具备容错能力。

10.7.2　扩展一个跨区卷

在已有一个跨区卷时，如果系统新添加了一个硬盘，而且存在未分配空间，此时就可以将这个空间扩展到那个已有的跨区卷上。

要实现以上的目的，可以通过以下操作完成：

（1）打开“磁盘管理”工具。

（2）单击右键要扩展的跨区卷，单击“扩展卷”，然后按屏幕上的指令操作即可。

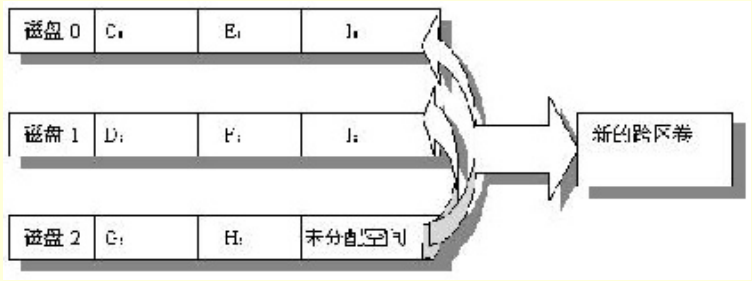


图 10-11　扩展跨区卷

图 10-11 表明了一个跨区卷的扩展。

10.7.3　删除一个跨区卷

虽然“磁盘管理”工具不能在基本磁盘上创建跨区卷，但是它能够删除基本磁盘上的原有跨区卷。

要删除基本磁盘上的跨区卷或是动态磁盘上的跨区卷，只要按照如下方法去做：

（1）打开“磁盘管理”工具；

（2）右键单击要删除的跨区卷，然后单击“删除卷”。

注意：删除一个跨区卷的操作是非常危险的。它会删除跨区卷所包含的所有空间中的内容，会造成大量的数据丢失。

10.8　使用带区卷

带区卷能够在两个或更多物理磁盘的带区上存储数据。并且交替而均匀地（以带区方式）将带区卷中的数据分配到带区卷的磁盘中。带区卷可以充分提高访问硬盘的速度。在 Windows NT 4.0 和更早的版本中，带区卷称为带区集。

和对跨区卷的管理一样，“磁盘管理”对基本磁盘上的带区卷提供有限支持。可以删除带区卷，但是不能在基本磁盘上创建新的带区卷，而只能在动态磁盘上创建新的带区卷。和跨区卷一样，带区卷也不具备容错功能。所谓的容错功能是指当硬件出现故障时，计算机或操作系统保证数据完整性的能力。如果组成带区卷的一个硬盘出现故障，那么此带区卷就不能被访问从而丢失带区卷上的所有数据。

10.8.1　创建一个带区卷

同样创建一个带区卷至少需要两个动态磁盘才可以。带区卷最多可以创建在 32 个物理磁盘上。

要创建一个带区卷，只要按照下面的方法去做即可：

（1）打开“磁盘管理”工具。

（2）单击右键需要创建带区卷的动态磁盘上的未分配空间，然后单击“创建卷”。

（3）在创建卷向导中，单击“下一步”，单击“带区卷”，然后按照屏幕上的指令操作。

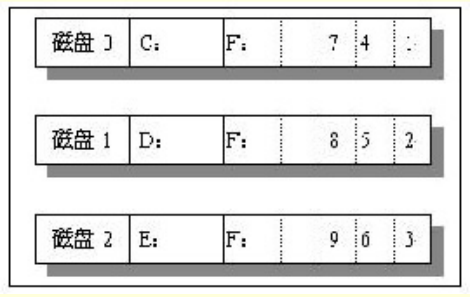


图 10-12 带区卷示意图

如图 10-12 所示，带区卷把每一个硬盘上的空间均匀地分成若干份，在存储时信息就按照数字的顺序保存。由于它均匀地把每一个硬盘上的空间分开，所以它能够提高操作系统对硬盘的访问速度。

从前面可以看到，跨区卷和带区卷有类似的地方，这里有必要详细地比较一下它们的异同。

带区卷因为是把数据在硬盘均匀分层，所以包含大小大致相同的分区。在向带区卷中存储数据时，系统先将一个硬盘上的一小块空间存储满，然后再向另一块硬盘上的一块空间上存储数据，直到存完为止；而跨区卷由于没有对空闲空间均匀分层，所以只能在存储完一个硬盘上空间后，才能在另一块硬盘上存储数据。由于操作系统对多块硬盘的访问能力大于对单个硬盘的访问，所以对带区卷上的数据的访问速度大于访问跨区卷上的数据。

同时也可看到它们有相同的地方：

- 它们都是创建在多个硬盘上的数据存储空间。
- 它们都可以通过一个驱动器字母来访问。
- 如果组成它们中的一个硬盘出现故障，那么整个卷将不能访问。
- 它们对 Windows 98 和 MS-DOS 都是不可见的。

10.8.2 删除一个带区卷

与分区、跨区卷和逻辑驱动器的情况一样，删除一个带区卷也意味着丢失存储在它上面的信息，所以要在执行这个操作之前备份要保留的所有数据。虽然“磁盘管理”工具不能在基本磁盘上创建跨区卷，但是它能够删除基本磁盘上原有的带区卷。

要删除一个带区卷，需要做如下工作：

（1）打开“磁盘管理”工具。

（2）右键单击要删除的带区卷，然后单击“删除卷”。

10.9 使用镜像卷

镜像卷是在两个物理硬盘上复制数据的容错卷。通过使用卷的副本（也就是镜像）复制包含卷中的信息来提供数据冗余。镜像位于不同的磁盘上。如果其中一个物理磁盘失败，则该磁盘上的数据将无法使用，但系统可以使用未受影响的磁盘继续操作，这是镜像卷的优势所在。在 Windows NT 4.0 或更早的版本中，镜像卷称为镜像集。

注意：镜像卷只能在运行 Windows 2000 Server 的计算机上使用。

镜像卷就像是对磁盘进行备份一样，如果镜像卷被损坏，则镜像卷将不能使用，但系统可以使用未受影响的磁盘继续操作，这使系统的稳定性提高，所以建议在服务器上使用镜像卷。

10.9.1　创建一个镜像卷

“磁盘管理”工具对基本磁盘上的镜像卷只提供有限的支持。可以修复、重新同步、分割和删除现有镜像卷，但是不能在基本磁盘上创建新的镜像卷，只能在动态磁盘上创建新的镜像卷。

要创建一个镜像卷，需要做如下的工作：

（1）打开“磁盘管理”工具；

（2）右键单击要创建镜像卷的动态磁盘上的未分配空间，然后单击“创建卷”；

（3）在创建卷向导中，单击“下一步”，然后再单击“镜像卷”，并按屏幕上的指令操作即可。

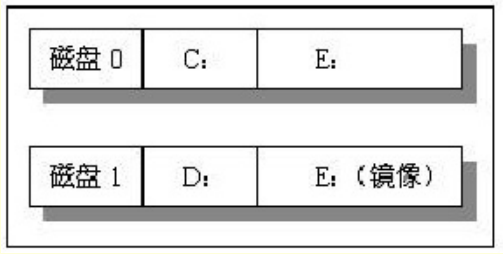


图 10-13　镜像卷

图 10-13 所示是镜像卷的示意图，从中可以看到镜像卷的两个备份使用同一个驱动器号。从镜像卷的定义中，可以知道镜像卷的两个备份中存储的是相同的内容。所以当一个备份损坏时，还可以应用另一个。

10.9.2　将镜像添加到现有简单卷

要添加镜像到现有简单卷，必须保证简单卷具有足够的未分配空间（至少要具有与要镜像的简单卷相同的存储空间）。如果空间不够大，则无法将镜像添加到此简单卷上。当添加操作完成后，则原有的简单卷被分配与镜像的卷相同的启动器字母，并且上面保存相同的数据。

添加镜像到现有简单卷，需要完成的操作如下：

（1）打开“磁盘管理”工具。

（2）单击右键要做镜像的简单卷，单击“添加镜像”。

（3）选择未分配空间，然后按照屏幕上的指示操作即可。

10.9.3　将镜像卷分成两个卷

镜像卷存在一个缺点，就是它非常浪费磁盘空间，因为存储的数据将被备份到另一个空间中，所以它利用的空间是在简单卷中存储相同大小数据的两倍。如果不再需要镜像卷，可以将镜像卷重新分成两个卷。

要将镜像卷重新分成两个卷，只要进行如下操作即可：

（1）打开“磁盘管理”工具。

（2）单击右键要分开的镜像卷中的卷，然后单击“分割镜像”。

在分割后，组成镜像卷的两个卷副本就会成为两个单独的简单卷，而且这些卷不再具备容错能力。它们的驱动器号也不再相同，但这两个卷上的数据还会被保留。

10.9.4　重新同步镜像卷

如果由于某种原因断开镜像卷中某个硬盘的连接，则系统就不会把数据同时写到两个磁盘上，这就造成了两个卷上的数据不一样的情况。如果重新连接该磁盘，则该磁盘上的数据已经陈旧。要使该镜像卷重新具有容错能力，必须重新同步镜像卷才能更新重新连接磁盘上的信息。

要重新同步镜像卷，操作非常简单：

（1）打开“磁盘管理”工具。

（2）单击右键要重新同步的镜像卷，然后单击“重新同步镜像”。

10.9.5 从镜像卷中删除镜像

由于镜像卷需要两倍的存储空间，所以当存储的数据要求的安全性不高时，是没有必要使用镜像卷的。

删除镜像卷中的镜像，需要做如下操作：

（1）打开“磁盘管理”工具。

（2）单击右键要删除的镜像，单击“删除镜像”，然后按屏幕上的指令操作即可。

一旦从镜像卷中删除镜像，被删除的镜像就变成未分配的空间，而且剩余镜像变成不再具备容错能力的简单卷，并且已删除镜像中的所有数据都将被删除。

提示：删除镜像卷将删除该卷包含的所有数据以及组成该卷的分区，并且只能删除整个镜像卷。

10.10 使用 RAID-5 卷

RAID-5 卷是包含数据和奇偶校验、间歇跨 3 个或更多物理磁盘的划分带区的容错卷。如果物理磁盘的一部分发生故障，可以从剩余数据和奇偶校验重新创建发生故障部分的数据。对于多数活动由读取数据构成的计算机环境中的数据冗余来说，RAID-5 卷是一种很好的解决方案。

注意：只能在运行 Windows 2000 Server 的计算机上使用 RAID-5 卷。

10.10.1 创建 RAID-5 卷

要创建 RAID-5 卷，至少需要 3 个动态磁盘。RAID-5 卷最多可以跨接 32 个物理硬盘。

要创建一个 RAID-5 卷，需要做如下操作：

（1）打开“磁盘管理”工具。

（2）右键单击要创建 RAID-5 卷的动态磁盘上的未分配空间，然后单击“创建卷”。

（3）在创建卷向导中，单击“下一步”，单击“RAID-5 卷”，然后按屏幕上的指令操作即可。

10.10.2 修复 RAID-5 卷

虽然在“磁盘管理”中不能创建 RAID-5 卷，但是它可以修复基本磁盘的 RAID-5 卷。在“磁盘管理”中会显示 RAID-5 卷的状态，如果包含部分 RAID-5 卷的基本磁盘断开连接或出现故障，则 RAID-5 卷的状态将变为冗余失败，则该卷将不再具有容错能力。要避免数据丢失，应尽快修复该卷。

要修复 RAID-5 卷，只要按如下操作即可：

（1）打开“磁盘管理”工具。

（2）单击右键要修复的 RAID-5 卷，然后单击“修复卷”。

在基本磁盘上修复 RAID-5 卷需要一个对部分 RAID-5 卷有足够可用空间的其他基本磁盘。如果没有这样的磁盘，则不能使用“修复卷”选项，并且不能修复该卷。在修复过程中，RAID-5 卷的状态应该是“重新生成”，修复完成后，RAID-5 卷将转换到“完好”状态。修复基本磁盘上的 RAID-5 卷之后，“磁盘管理”将把部分 RAID-5 卷重新安置在一个完好的磁盘上，并重新生成奇偶校验。

提示：必须使用基本磁盘修复基本 RAID-5 卷（带奇偶校验的带区集）。不能使用动态磁盘。

10.10.3 删除 RAID-5 卷

要删除 RAID-5 卷，需要按照如下方法操作：

（1）打开“磁盘管理”工具。

（2）右键单击要删除的 RAID-5 卷，然后单击“删除卷”。

删除 RAID-5 卷，将删除该卷中存储的所有数据以及组成该 RAID-5 卷的所有分区，并且只可以删除整个 RAID-5 卷。所以删除以前要对重要的数据进行备份。

10.11　使用磁盘碎片整理

在使用 Windows 2000 的时候，可以看到它提供了许多简单、方便、而且有效的附带程序，比如说：CD 唱机、记事本、计算器、通讯薄、Internet Explorer 等等。磁盘碎片整理程序也是它提供给我们的一个非常有用的工具。

由于我们在对文件进行操作时，免不了要删除、移动某些文件，这样就在磁盘空间上留下了许多空白区域，导致以后存储文件时，一个文件被分成好多部分以弥补以前的空白，从而产生了零碎的文件。磁盘上包含大量的这种文件，Windows 2000 访问它们的时间会加长，同样其他的文件操作也会延长。“磁盘碎片整理”能够确定本地卷上的这种零碎的文件或文件夹的位置，并将每个文件或文件夹的各部分移动到卷上的同一个位置，以便每个文件或文件夹占据卷上的单独的、邻近的空间。这样 Windows 2000 就可以有效地、快速地进行文件操作。也可以合并出大块的空间，以减小新文件出现碎片的可能。

查找和合并文件或文件夹碎片需要用到“磁盘碎片整理程序”，打开它有两种方法，一种是如图 10-1 所示，单击左边控制树“存储”根目录下的“磁盘碎片整理程序”即可。另一种方法是：单击“开始”→“程序”→“附件”→“系统工具”→“磁盘碎片整理程序”，这样就可以打开它了。打开后的磁盘碎片整理程序如图 10-14 所示。

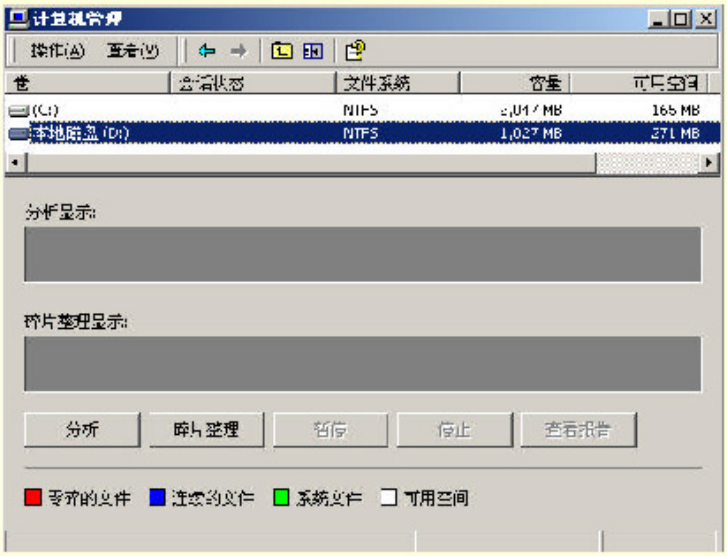


图 10-14　打开后的磁盘碎片整理程序

这时看到的磁盘碎片整理程序还没有对某一个卷进行任何的处理，要想让它对某一个卷进行文件或文件夹碎片的分析，先要选中一个卷，然后单击“分析”按钮，就可以在分析显示条形框中看到各种文件在磁盘上的物理位置的情况。以本地磁盘（D：）为例，进行碎片分析。分析完毕后，系统会建议你进行磁盘碎片整理，如图 10-15 所示。

图 10-15　分析完毕

如果此时想进行磁盘碎片整理，就单击“碎片整理”按钮；如想查看详细的碎片资料，那么就单击“查看报告”按钮，系统会显示“分析报告”窗口，列出详细的碎片信息。此窗口还能列出该卷的使用情况以及最零碎的文件，如图 10-16 所示。

单击关闭按钮后，可以看到分析后图形显示的结果，如图 10-17 所示。在分析显示条形框中，不同的颜色分别代表：

- 红色：零碎的文件。
- 蓝色：连续的文件。
- 绿色：系统文件。
- 白色：可用空间。

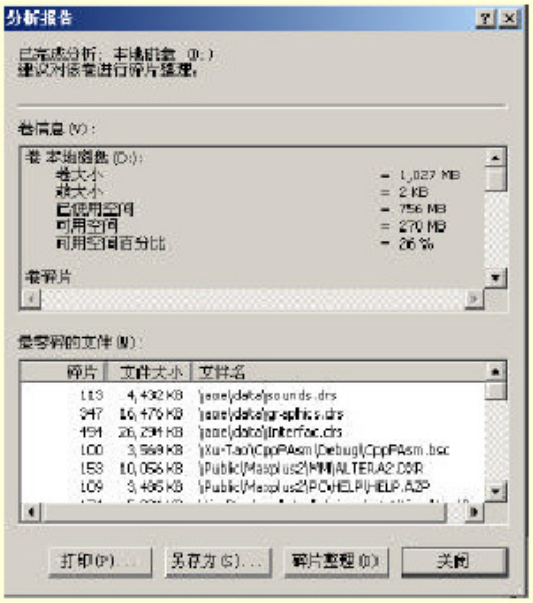


图 10-16　分析报告窗口

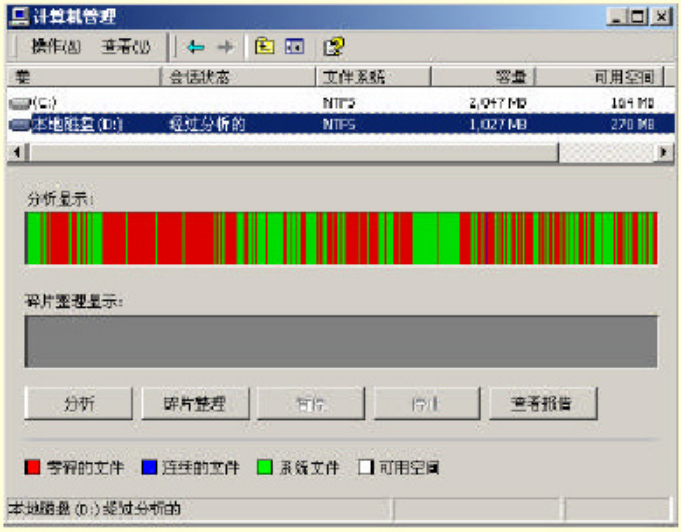


图 10-17　碎片分析后

从中可以分析出此卷上文件零碎的程度。从图 10-17 中可以看到此卷上连续的文件很少，零碎的文件很多。此卷非常需要进行磁盘碎片整理。单击此时的碎片整理按钮，就可以进行碎片整理了。

提示：进行磁盘碎片整理时，可能需要一定的剩余空间，如果该卷的剩余空间不够，磁盘碎片整理程序将不能进行碎片整理。

磁盘碎片整理程序可能需要几分钟的时间，分析完成后可以从碎片整理显示条形框中看到零碎的文件已经减少，连续的文件增多，如图 10-18 所示。

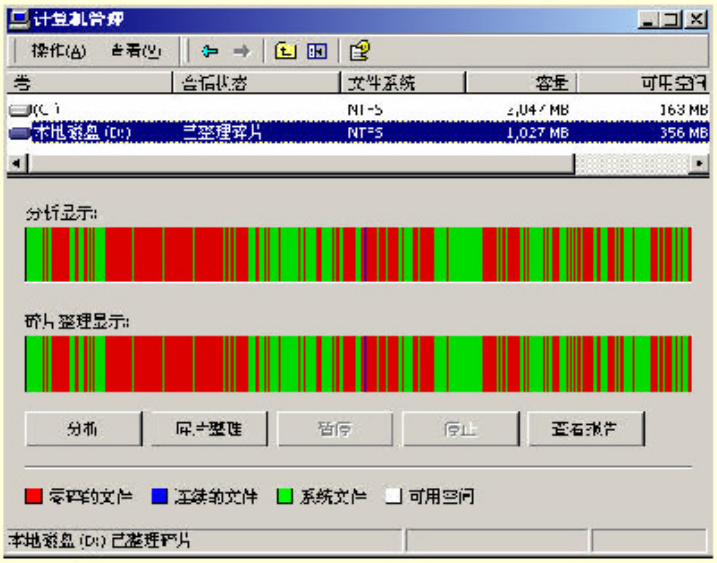


图 10-18　磁盘碎片整理后的情况

10.12　使用磁盘配额

前面我们曾经讲到过 NTFS 文件系统支持对磁盘的配额管理。磁盘配额允许你根据用户拥有的文件和文件夹为用户分配磁盘空间。磁盘配额管理允许进行以下操作：为所有用户设置磁盘配额、为具体的某一个用户设置磁盘配额、设置磁盘配额警告级别和限度级别。你还可以监视用户使用的磁盘空间以及相对磁盘限额所剩余的磁盘空间。这些限制指定了允许用户使用的磁盘空间容量。磁盘限度级别限制了用户可以使用的最大的磁盘空间，磁盘警告级别则规定了用户接近其配额限度的值。如果用户使用的磁盘空间超过了这一限度，系统则把磁盘配额系统记录为系统事件。

10.12.1　磁盘配额概述

Windows 2000 磁盘配额根据每个用户和每个磁盘来跟踪和控制磁盘的使用。系统管理员可以将 Windows 2000 设置为 4 种磁盘配额管理模式：

- 启用或禁用卷上的配额。
- 拒绝为超出配额限制的用户分配磁盘空间。
- 当用户超过指定的磁盘空间警告级别时记录事件。
- 当用户超过所指定的磁盘空间限额时，系统阻止你进一步使用磁盘空间和记录事件。

磁盘配额只适用于卷，而且不受卷的文件夹结构及物理磁盘上的布局的限制。如果该卷拥有若干个文件夹，则分配给该卷的配额将整个应用于所有的文件夹。

由于磁盘配额监视单个用户的卷使用情况，因此每个用户对磁盘空间的利用都不会影响同一卷上的其他用户的磁盘配额。也就是说，如果某一用户在此卷上的使用空间已经超过磁盘限额，那么他必须删除或移动此卷上的一些文件，才能把其他数据写到这个卷上。而其他户在此卷上仍可继续存储到磁盘限额所限制的大小的空间。磁盘配额是以文件所有权为基础的，并且不受卷中用户文件的文件夹位置的限制。

10.12.2　启用磁盘配额

由于磁盘配额只适用于某一个卷，所以启用磁盘配额要对单个的卷进行操作。启用磁盘配额的具体办法是：

（1）在 Windows 2000 的桌面上选择“我的电脑”，并双击它；

（2）在要启用磁盘配额的磁盘卷上单击鼠标右键。
（3）选择并单击“属性”，打开“属性”对话框。
（4）选择并单击“配额”选项卡，如图 10-19 所示。
（5）在“配额”属性页上，单击“启用磁盘配额”复选框，然后单击“确定”按钮。

注意：如果卷不是用 NTFS 文件系统格式化的，或者你不是 Administrators 组的成员，那么你将无法看到“属性”对话框中的“配额”选项卡。

图 10-19 配额选项对话框

这时可以看到如图 10-19 所示最上一行标明“状态：磁盘配额已被启动”。它对应着左边“交通灯”中的一种颜色。

表 2 磁盘配额状态

“交通灯”颜色	所代表的意义
红灯	没有启动磁盘配额
黄灯	Windows 2000 正在重新创建磁盘配额信息
绿灯	表示磁盘配额系统处于活动状态

单击“启用磁盘配额”复选框后，会看到下面有许多复选框或文本框被激活，在这里就可以对磁盘使用空间限制或警告等级进行设置，如图 10-20 所示。

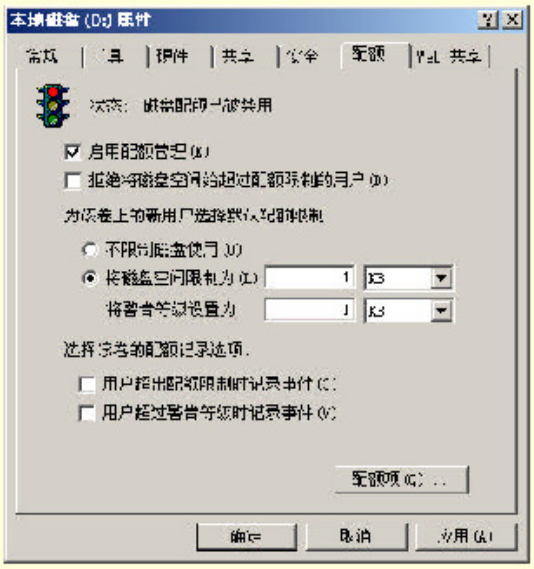


图 10-20　激活“启用配额管理”后的“属性”对话框

10.12.3　磁盘配额限度设置

在图 10-20 中可以看到有一个复选框为“拒绝将磁盘空间给超过配额限制的用户”，选择它，则用户在使用空间超过磁盘配额限度时，Windows 将提示用户“磁盘空间不足”的错误，而且如果不从此卷中删除或移动一些现有文件，那么就不能再把其他数据写到此卷上。如果不想拒绝用户在该卷上再存储文件，而又想跟踪每个用户对磁盘空间的使用情况，则选择“启用磁盘配额”而不选择“拒绝将磁盘空间给超过配额限制的用户”的复选框即可。

另外还可以对新加入的用户设置默认磁盘配额限制。这有两种选择方式，它们是：“不限制磁盘使用”和“限制磁盘使用”。在“不限制磁盘使用”情况下，系统不限制新用户对磁盘空间的使用，但会对新用户的使用情况进行监视。如果要限制新用户使用磁盘的空间，那么就选择“限制磁盘使用”方式。这里不但可以限制新用户可以使用的磁盘空间的大小，还可以设置警告等级。具体的方法是：

（1）选中“为该卷上的新用户选择默认配额限制”下的“将磁盘空间限制为：”前的单选框，这时其后面的文本框被击活。

（2）在“将磁盘空间限制为：”后的文本框中添入限制新用户使用磁盘空间大小，在其后的下拉式列表中选择空间大小的单位，如 KB、MB、GB 等，如图 10-21 所示。

图 10-21　设置新用户磁盘配额

（3）同样的道理，可以设置警告等级。

如图 10-21 所示是一种典型的新用户磁盘配额设置形式，将警告级别设置为小于空间限制是必要的，这样系统就会在用户使用的磁盘空间接近空间限制的情况下警告此用户。

在如图 10-21 所示的“属性”对话框中，我们还可以做两件事情，它们给系统管理员提供了一个监视用户磁盘使用情况的机会。具体做法是：选择如图 10-21 所示中最下面的两个复选框，如果选择了“用户超出配额限制时记录事件”复选框，那么系统会检查用户磁盘空间使用情况，以便在用户使用了超出限额的磁盘空间（即图 10-21 中“将磁盘空间限制为：”后的文本框中所规定的）时，生成一个事件日志项；如果选择了“用户超过警告等级时记录事件” 复选框，则系统在用户使用的磁盘空间超过警告等级（即图 10-21 中“将警告等级设置为”后的文本框中所规定的）时，以便生成一个事件日志项。

在做完上述想设置的所有选项后，单击“确定”按钮后，系统会提示确定信息，如图 10-22 所示。单击“确定”按钮后，就可以启动磁盘配额管理了，这会需要几分钟的时间。

图 10-22　磁盘配额提示信息

启动后的磁盘配额管理属性对话框如图 10-23 所示，这里需要重新打开“磁盘配额属性”对话框。可以看到图 10-23 中标明“状态：重建磁盘配额信息”，且左边的“信号灯”显示为黄色。这时单击“确定”按钮，然后再重新打开“磁盘配额属性”对话框，如图 10-24 所示。这时磁盘配额管理才真正被启动，而且标明的状态为：“磁盘配额系统正在使用中”，左边的“信号灯”显示为绿色。

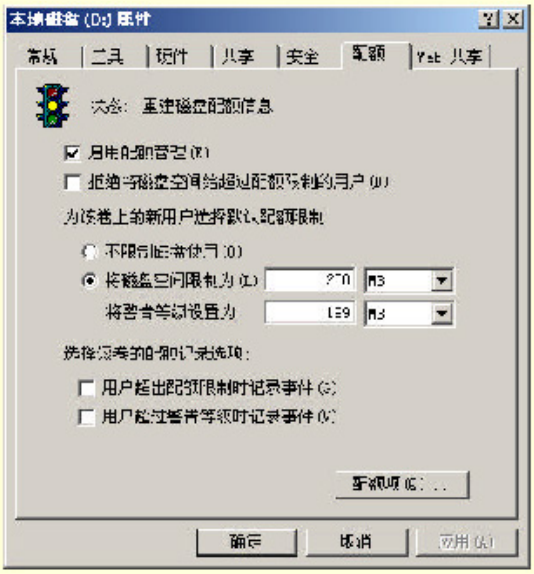


图 10-23　重建磁盘配额

10.12.4　管理磁盘配额项目

磁盘配额限制是针对每个用户在一个卷上的空间使用情况而言的，所以真正的设置是针对每个用户的，每个用户在这个卷上的文件操作都将导致文件占用的磁盘空间受用户配额限度的控制。两种典型的受限制的操作是：

- 用户将新的文件复制或保存到启用磁盘配额后的卷上。
- 用户获得一些原先不具有所有权的文件的所有权。

所以用户在进行上述两种操作时，一定要注意。

图 10-24　启动后的磁盘配额管理

前面介绍的是针对所有用户进行的磁盘配额管理，现在重点讲述针对个人的磁盘配额管理。

10.12.4.1　查看此卷所有用户的磁盘配额信息

按照 10.6.2 介绍的方法打开磁盘配额属性对话框，然后单击“配额项目”按钮，会看到出现配额项目窗口，其中每一行都将包含此卷的一个用户信息，如图 10-25 所示。

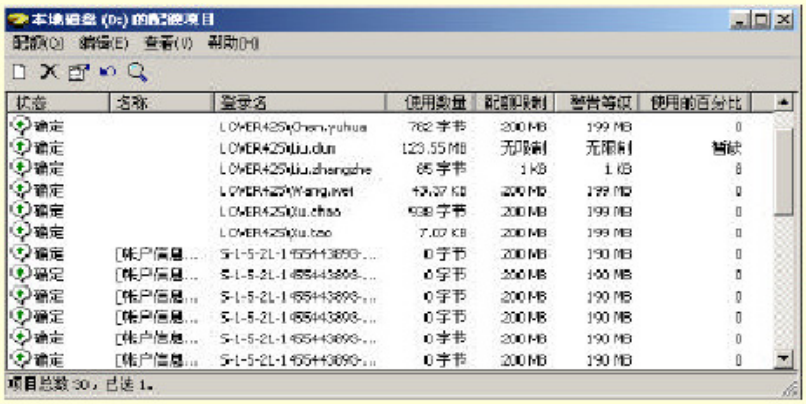


图 10-25　配额项目

从图 10-25 中可以看到窗口中列出了所有用户的“状态”、“名称”、“登录名”、“配额限制”等项目。要想查找某个用户的信息，只要在“编辑”菜单中单击“查找”就可以了，如图 10-26 所示。

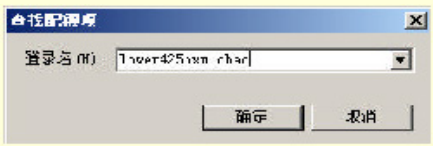


图 10-26　查找配额项

在登录名后添入要查找的登录名，单击“确定”按钮，就会在图 10-25 中将光条定位在该用户上。

2．设置用户配额

查找到某一个用户之后，要想对其磁盘配额进行设置，只要单击要修改选项的用户项目，并单击“配额”菜单下的“属性”，就会出现“配额设置”对话框，并显示出该用户在此卷上的详细配额信息，如图 10-27 所示。

图 10-27 用户的详细配额信息

在“配额设置”对话框中，修改需要更改的下列选项，然后单击“确定”按钮。

·不限制磁盘使用：单击在“不限制磁盘使用”前的单选按钮，以便将无限制的磁盘配额指派给该用户，该用户的使用空间将不受限制；

·将磁盘空间限制为：单击在“将磁盘空间限制为”前的单选按钮，以便将配额警告等级和配额限制值指派给该用户，在文本域中键入数值，并从下拉列表中选择磁盘空间限额单位，则该用户在该卷上的使用空间会受到其数值的限制。

10.12.4.3 添加新配额项目

对于新加入的用户，如果不想对其使用默认磁盘空间限度和警告级别，则添加新配额项目是非常必要的。通常，对于新用户，默认磁盘空间限度及警告级别值足够了。

添加新的配额项目方法如下：

（1）在图 10-25 中，单击“配额”菜单上的“新配额项目”；

（2）在“选择用户”对话框的“搜索范围”列表框中，选择要从中选择用户名的域或工作组的名称，如图 10-28 所示；

（3）找到要添加的用户名，单击它；

（4）单击“添加”按钮，如图 10-29 所示。

（5）单击“确定”按钮。

（6）系统会弹出如图 10-27 所示的对话框，以便对新用户设置配额。

（7）设置后单击“确定”按钮，添加用户完毕。

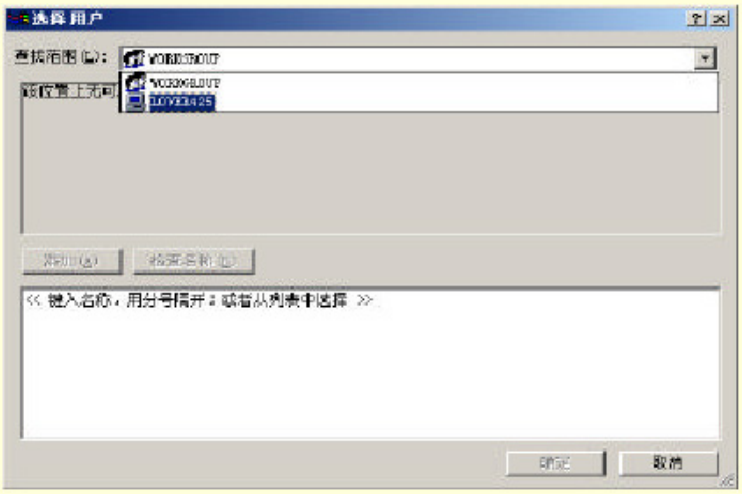


图 10-28 选择域或工作组

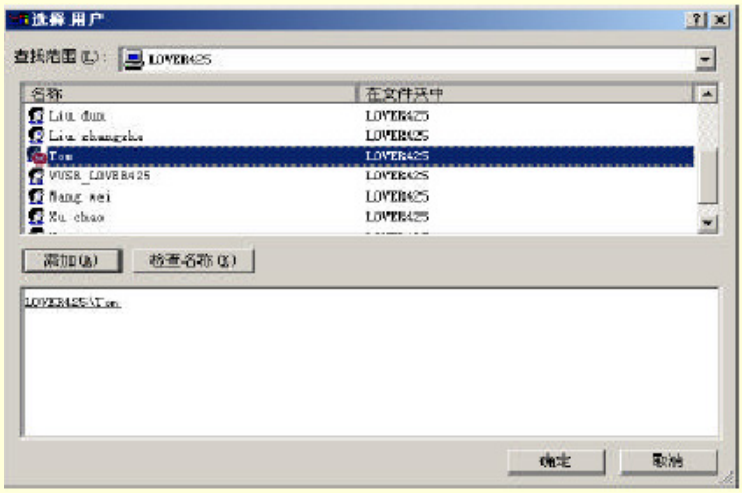


图 10-29　添加配额项

10.12.4.4　删除配额项目

当用户不再需要使用启用配额的卷时，可以通过从“配额项目”窗口中删除用户项目，除去用户警告级别和配额限度。

具体的删除配额方法如下：

（1）在图 10-25 所示的配额项目列表中单击要删除的用户；

（2）单击“配额”菜单下的“删除配额项”，如图 10-30 所示；

（3）系统会提示是否真的要删除此配额项；

（4）单击“确定”按钮，这样就删除了此配额项。

图 10-30　删除配额项

提示：只有当该用户所拥有此卷上的全部文件从该卷中删除或者将文件的所有权转给其他用户之后，才可以删除此配额项。

10.12.4.5　创建配额报告

有时需要将磁盘配额项目的详细信息打印出来，以便管理员更容易管理，这时就需要创建配额报告。

创建配额报告，需要一些应用软件，比如 Microsoft Excel 电子表格。

创建配额报告具体方法如下：

（1）在如图 10-25 所示的配额项目列表中，选择将要列入配额报告的用户（选择多个用户时，可以按住 Ctrl 键，再单击列表中的用户）。

（2）打开上述的应用程序，如 Microsoft Excel 电子表格。

（3）用鼠标将选中的列表拖至 Microsoft Excel 电子表格中，如图 10-31 所示。

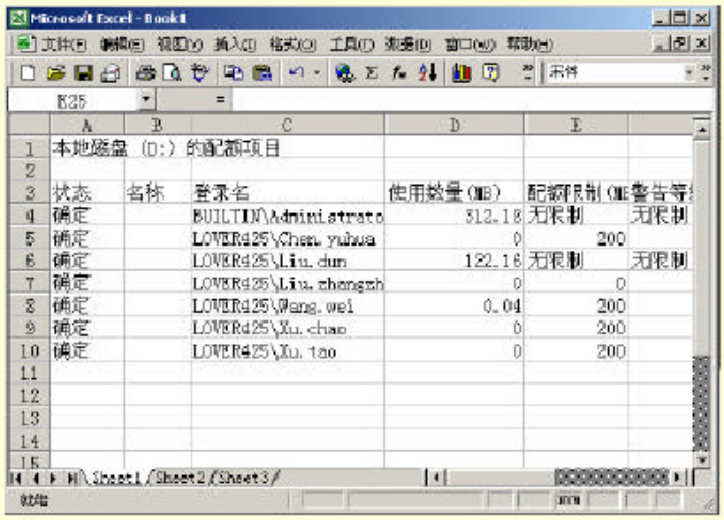


图 10-31 配额报表

（4）在 Microsoft Excel 电子表格中保存此文件即可。

10.12.4.6 配额设置到其他卷

有时可以将一个或多个用户在磁盘上的配额信息导出到其他卷上。如果目标卷上已经存在这些用户的配额信息，那么导出到该卷时，是对这些用户在该卷上的配额信息进行重新设置；如果目标卷上没有这些用户的配额信息，那么导出到该卷时，是创建这些用户的配额项目，用户的磁盘空间限额和配额警告级别值与源卷上的相同。

导出配额设置的具体方法是：

（1）在“配额项目”窗口中单击要导出的用户配额记录；

（2）单击“配额”菜单下的“导出”命令或单击鼠标右键，选择“导出”命令；

（3）在弹出的“导出配额设置”对话框中添入文件名并选择文件路径，如图 10-32 所示；

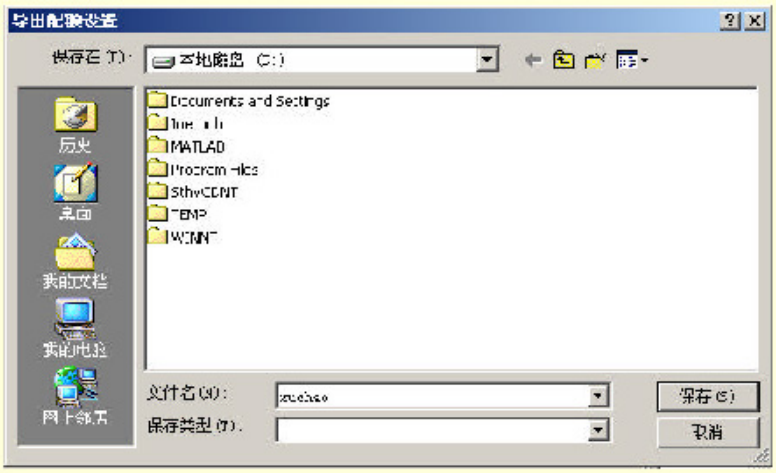


图 10-32 导出配额设置

（4）单击“保存”按钮。

提示：此种导出方法是将配额保存成文件的形式，并放入统一的文件夹中，以便以后在其他卷上导入或恢复用户的配额信息。

10.12.4.7 从其它卷上导入磁盘配额

为了应用其他卷上的用户的配额信息到另一个卷上，需要从其他卷上将一个或多个用户的配额设置导入到

此卷上。如果此卷上没有这些用户的配额信息，则导入命令将在此卷上创建这些用户的配额信息；如果此卷上已经存在这些用户的配额信息，则导入命令将重新设置这些用户的配额信息。

从其他卷上导入磁盘配额的具体方法是：

（1）在“配额项目”窗口中单击“配额”菜单下的“导入”；

（2）在“导入配额设置”对话框中的文件列表中选出要导入的文件（导出时所创建的文件），如图 10-33 所示；

（3）单击“打开”按钮。

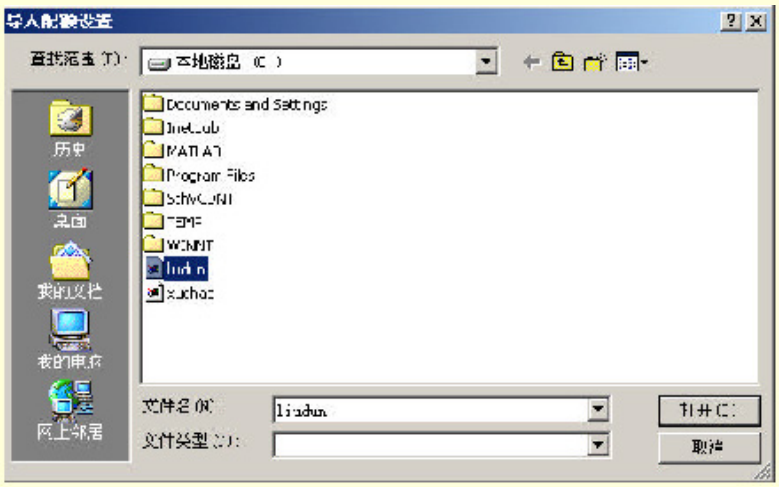


图 10-33　导入配额设置

还有一种直接导入、导出的方法，那就是打开两个“配额项目”窗口：一个用于要导入配额记录的卷，另一个用于配额记录要导入到的卷。然后，可把配额记录从源卷的“配额项目”窗口拖到目标卷的“配额项目”窗口。

第 11 章　用户环境管理及组策略

每个人都习惯在熟悉的工作环境工作，无论是在自己的工作台，还是在计算机前。用户环境管理可以帮助我们置身于熟悉的环境之中，得心应手地完成各种不同类型的任务。环境的管理，不但适用于未联网的单机，还可以通过网络为用户进行配置，从而简化了管理员的管理工作。

总的来说，用户的工作环境管理可以通过包括用户配置文件（User Profile）、系统规则（System Policy）、登录脚本（Login Script）以及环境变量（Environment Variables ）的手段进行管理。

本章内容包括：

- 用户配置文件
- Windows 2000 的组策略
- 安全设置
- 管理模板
- 脚本管理
- 主目录管理

11.1　配置文件

简单地说，用户配置文件是当用户登录时系统自动加载的信息，包括用户对 Windows 2000 环境的设置，如屏幕颜色、网络连接、打印机的连接、鼠标设置、窗口的大小和位置。

用户在退出到下一次登录过程中，系统会保留上次的一些配置。这样一来，用户重新登录后，将回到自己熟悉的工作环境，比如漂亮的桌面背景，桌面上自设的应用程序的快捷方式，开始菜单的个人程序组，显示器的设置，网络和打印机的连接等都会和退出时一样，就像在工作台中，书籍的摆设、文具的摆放，以及椅子的高低等都按自己喜欢的位置摆放。这些信息就存放在用户配置文件中，帮助你迅速进入工作状态。

下面是用户配置文件应用的一些例子：

- 在资源管理器中对查看工具栏、状态栏、浏览栏、大图标、小图标等的设置；
- 在桌面上添加的应用程序快捷方式及其图标；
- 屏幕保护及背景图案；
- 查阅帮助里添加的书签；
- 对应用程序组的设置等。

提示：用户配置文件只适合于 Windows 2000 或者 Windows NT 计算机的用户，DOS 和 Windows3.x 的用户无法使用用户配置文件。

用户配置文件包括以下 3 种类型：本地配置文件（Local User Profile），漫游配置文件（Roaming User Profile）和强制配置文件（Mandatory User Profile）。

■ 本地配置文件

用户在运行 Windows 2000 或 Windows NT 的机器上第一次登录时，计算机自动在本地创建的配置文件。

■ 漫游配置文件

与本地配置文件不同的是，漫游配置文件是建立并保存在服务器中的。当用户登录时，漫游配置文件从服务器上下载到用户的本地计算机中；用户注销后，所做的配置改动将对服务器上和本地的配置文件都进行更新。

■ 强制配置文件

与漫游配置文件一样，强制配置文件也存在网络的服务器中。但二者也有区别：用户所做的配置改动无法更新强制配置文件。

在后面对这 3 种配置文件还将有更详细的介绍。

11.1.1　配置文件的结构组成

保存在用户配置文件中的设置可以用表 11-1 说明。

表 11-1　配置文件设置

来源	保存的配置参数
控制面板	用户定义的设置值
附件	对计算器、时钟、记事本等附件项目的具体设置
资源管理器	所有在资源管理器中设置的自定义项
任务栏	个人程序组、程序项及其属性
Windows 应用程序	用户对应用程序的设置
帮助文件	在帮助系统中添加的书签
打印设置	网络打印机的连接

用户配置文件并不是一个特定的文件，它实际上由三部分组成，它们是用户配置文件夹、All Users 配置文件夹以及注册表中的 HKEY_CURRENT_USER 的内容。

11.1.1.1　用户配置文件夹（User Profile）

每个用户的用户配置文件夹与用户名相同，而且每个用户都会有其自己的用户配置文件夹，这些文件夹存放在 C:/Documents and Settings/路径下。从资源管理器中打开后，可以看见这一目录，如图 11-1 所示。

提示：在 Windows NT 4.0 中，用户配置文件夹存放在%SystemRoot%\Profile 路径中（默认的是 C:/Winnt/Profile），与 Windows 2000 略有不同。

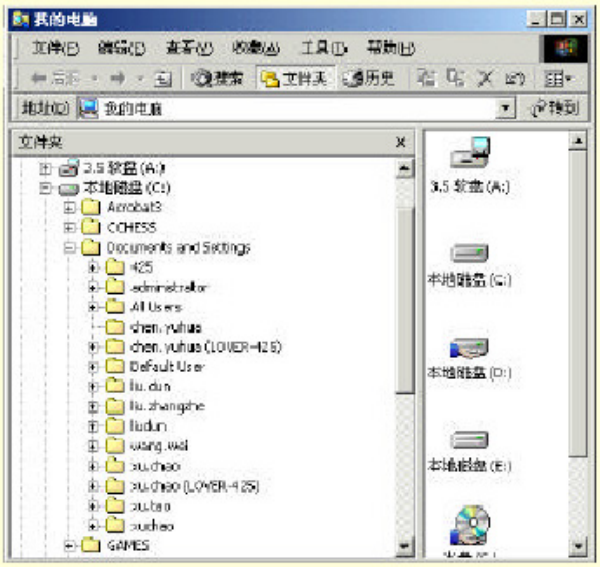


图 11-1　用户配置文件夹

打开每个用户的用户名配置文件夹，可以看到开始菜单、桌面、Favorites、My Documents 和 Cookies5 个文件夹。但实际上为了安全起见，系统还自动隐藏了一些文件夹和文件。要想显示隐藏文件，请按以下步骤操作：

（1）在资源管理器中，打开“工具”→“文件夹选项”菜单，或者在控制面板中，双击选择文件夹选项。

（2）选择查看选项卡，此时的对话框如图 11-2 所示。

（3）在如图 11-2 的对话框中，选择“显示所有文件和文件夹”（缺省为“不显示隐藏的文件和文件夹”）。

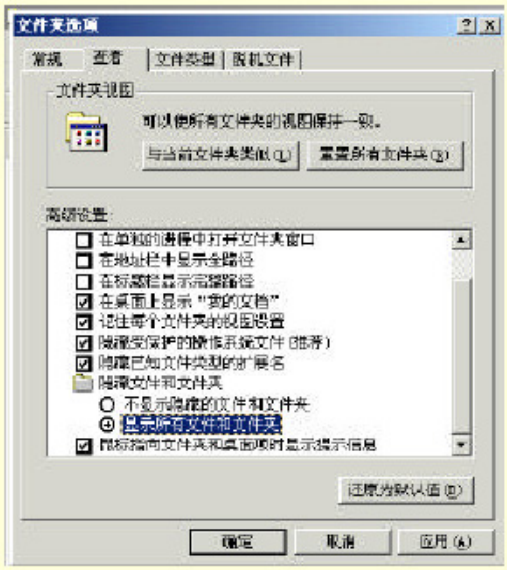


图 11-2　选择显示文件和文件夹

此时将有可能出现警告提示，按“确定”按钮即可。

回到资源管理器中再次查看用户配置文件夹，将出现更多的文件夹和文件，现在对每个文件夹所存放内容阐述如表 11-2 所示。

表 11-2　用户配置文件内容

用户配置文件夹	内容
“开始”菜单	用户开始菜单中的个人部分程序项
Application Data	客户的应用程序数据
Cookies	
Favorites	包括媒体，链接两个文件夹，提供了微软在互联网上网页的快捷方式
Local Settings	包括一些最近访问过的网页以及临时文件
My Documents	存放着我的文档，包括传真、图片、网页等一些文档数据
NetHood	网上邻居中定义的快捷方式
PrintHood	打印机文件夹定义的快捷方式
Recent	被一些应用程序最近使用的文档，比如 Word 文档
SendTo	在文件或者文件夹上单击右键出现的快捷菜单中，“发送到”菜单项出现的目标地
Templates	指向模板项目的快捷方式
桌面	用户桌面上非系统设置的快捷方式图标

读者可以发现，在 Documents and Settings 中，除了用户配置文件夹外，还有两个特定的文件夹，那就是 All Users 和 Default Users 文件夹。一般说来，当某个用户第一次登录时，由于不具备自己的用户配置文件，这时系统就会从 Default Users 文件夹中指定一个默认的配置文件，并初始化这个用户的工作环境。当用户注销后，对设置的改动会保存到该用户的个人配置文件夹中。我们再来看看 All Users 文件夹。

11.1.1.2　All Users 文件夹

与于个人设置相对应的是一些公用的、适用于所有用户的工作环境配置，这些信息就存放在 All Users 文件

夹，与用户的个人配置文件夹共同构成了用户的工作环境。

在 Windows 2000 以前的 Windows 95 或者 Windows NT 中，开始菜单尚未得到简化（开始菜单的简化详见第 3 章），用户想必会注意到程序下级联菜单中的分隔线，分隔线下方的就是系统定义的公用程序组。在 Windows 2000 中，简化开始菜单后，虽然分隔线没再出现，但 All Users 文件夹仍然存在。

公用程序组及其他公用的配置定义在 All Users 文件夹中，包括桌面及开始菜单的设置，与其他用户配置文件夹不同的是，All Users 文件夹中只有“开始”菜单、Application Data、Documents、Favorites、Templates 及桌面 6 个文件夹。

需要提醒的是：添加应用程序时，安装程序（Setup.exe 或者 Install.exe）会把应用程序快捷方式的图标放在开始菜单下级联的程序菜单中，但具体存放在个人用户配置文件夹中还是公用的 All Users 文件夹中，则不是确定的。可以在程序安装完成后，再在资源管理器中具体查看。

11.1.1.3　Ntuser.dat 文件

用户工作环境的配置还有第 3 个重要组成部分是 Ntuser.dat 文件。当在“资源管理器”中查看用户配置文件，并已经选择了查看所有文件和文件夹而不是隐藏受保护的文件后，就可以看见 Ntuser.dat 文件，如图 11-3 所示。

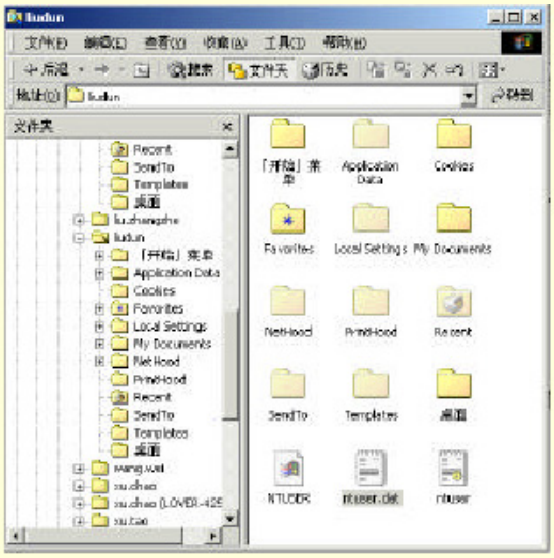


图 11-3　不被隐藏的 Ntuser.dat 文件

Ntuser.dat 数据文件是与注册表的 HKEY_CURRENT_USER 根键相关联的这个文件保存了用户配置文件中除去各文件夹中的其他内容，如图 11-4 所示。

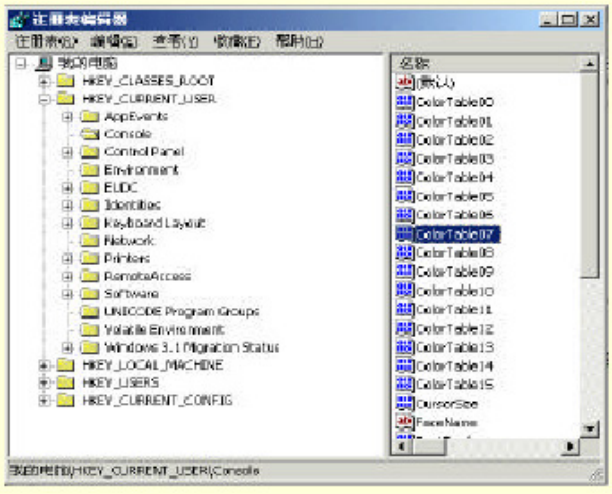


图 11-4　注册表的 HKEY_CURRENT_USER 根键

提示：要运行注册表以查看或者编辑，请在“开始”菜单中打开“运行”对话框，在“打开”文本框中输入 regedit。

在如图 11-4 所示的注册表编辑器中，可以看到 HKEY_CURRENT_USER 根键下所包含的内容，很容易想到，此根键保存的是当前用户（CURRENT USER）的配置信息，包括用户对控制面板（Control Panel）、键盘布局（Keyboard Layout）、已安装的软件（Software）、网络连接（Network）等的设置。用户对控制面板等的设置项存放在系统注册表中，对这些信息的处理有别于其他的用户配置文件，这时候引用了 Ntuser.dat 文件。

警告：注册表中包含了许多重要的系统配置信息，微软并不支持用户修改注册表，因此没有把注册表编辑器放在开始菜单中。不要随便改动，否则可能导致系统崩溃！

此外还有一个名为 Ntuser.dat.LOG 的日志文件。用户对配置的更改会保存在该日志文件中，当用户注销时，更改的数据会再复制到 Ntuser.dat 文件中去。

HKEY_CURRENT_USER 根键下的内容视当前用户而有区别，而且 Ntuser.dat 文件与 HKEY_CURRENT_USER 根键是双向联系的。当某个用户登录时，其用户配置文件夹下的 Ntuser.dat 文件会对 HKEY_CURRENT_USER 根键的内容初始化；而当用户注销时，HKEY_CURRENT_USER 根键将再对 Ntuser.dat 文件进行更新。

由此可以看出，用户配置文件夹和注册表中 HKEY_CURRENT_USER 的内容组成了用户的个人配置，而 All Users 文件夹则是公用的配置信息。

下面我们来看看用户配置文件的工作。

11.1.2 配置文件的分类

11.1.2 1 本地配置文件

如前所述，当用户登录时，用户配置文件夹下的各子文件夹和 Ntuser.dat 文件会初始化用户的个人配置，它们和 All Users 文件夹共同构成了用户的工作环境。

如果用户是第一次登录，那么系统会把 Default Users 文件夹和 All Users 文件夹一同供用户使用，配置用户的工作环境。此后将会在 Documents and Settings 文件夹中建立一个以用户名命名的本地配置文件夹（实际上是把 Default Users 文件夹复制到此新建的用户配置文件夹中），当用户注销后，所做的改动就会保存在此用户配置文件夹中，供用户下次登录时使用。而 Default Users 文件夹的内容不变。

有时读者可能会看到这样的情况：假设用户名为 wang，此时在 Documents and Settings 文件夹中出现了两个配置文件夹，一个名为 wang，而另一个名为 wang.000，这是怎么回事呢？当然，该用户在本地计算机上有用户名为 wang 的账号，如果此用户在域上还有一个账号，就会出现这样的情况。用户在本地计算机和域中分别建立账号后，系统会给两者不同的 SID 号，实际上将两者区别对待。这样用户以不同身份登录，就会有不同的用户配置文件。当两个账号有相同的用户名时，为了区分不同的用户配置文件，就在一者后面加上.000 以示区分。用户以不同身份登录，系统启用的是不同的用户配置文件；同样的道理，用户注销时，改动也会保存到不同的用户配置文件中。

11.1.2.2 漫游配置文件

与本地配置文件不同，漫游配置文件不是保存在用户登录的本地计算机中，而是保存在网络上的服务器计算机中。

漫游配置文件的建立是出于这样的考虑：在网络中，如果用户需要在不同的计算机上登录，而又希望总能

在熟悉的工作环境中工作，这时候就应当建立一个保存在服务器中的配置文件，当用户“漫游”在网络中时，他可以打开这个配置文件来初始化自己的工作环境。当用户注销时，所做的改动会保存在服务器上的漫游配置文件中。

与本地配置文件不同，不会有一个 Default Users 文件夹存放在服务器中，自动为用户建立漫游配置，需要管理员亲自设置。

为用户设立一个漫游配置文件的方法是：

（1）以系统管理员身份登录，打开用户管理器。

（2）找到需要设立漫游配置文件的用户。

（3）在用户名上单击右键，在弹出的快捷菜单中，选择“属性”命令。

（4）在属性对话框中，选择配置文件选项卡。如图 11-5 所示。

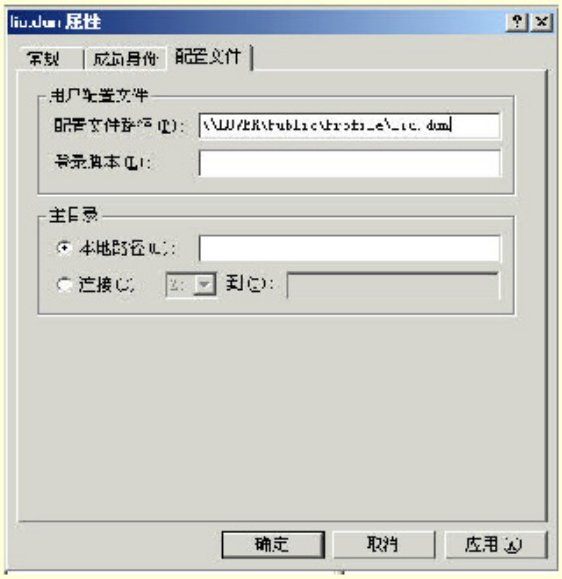


图 11-5　设立漫游配置文件

（5）在“配置文件路径”文本框中，输入为用户设置的漫游配置文件的路径与名称，其中路径名称包括服务器以及下属的文件夹名。

在图 11-5 所示的文本框中，输入的是 UNC 名（Universal Naming Convention）。UNC 名是在 Windows 域中，指明网络资源的统一命名约定，采用两个反斜线开始一个计算机名，一个反斜线开始该计算机中的共享文件名，之后是底下的子目录，其格式为\\server name\profiles folder name\user profile name。

用户不需要输入后缀名（.usr 或.man），如果输入的路径文件夹不存在，用户第一次登录时系统会自动创建。

当输入此配置文件名称后，用户下次登录时，就会在设定的路径下建立一个新的漫游配置文件，并用来在注销时保存用户对环境的更改。此后，这个配置文件就成为用户在网络上的漫游配置文件。

如果用户习惯了本地的设置，想把他在本地存在的现有配置文件作为漫游配置文件，方法是：

（1）打开控制面板中的系统命令，或者在“资源管理器上”“我的电脑”中，单击右键，在弹出的快捷菜单中选择“属性”命令。

（2）在系统特性对话框中，选择“用户配置文件”选项卡，如图 11-6 所示。

（3）在图 11-6 中，可以查看到存放在计算机上的现有配置文件，选择准备选用的用户配置文件。

（4）单击“复制到”按钮，输入目标路径的 UNC 名。

（5）单击“更改”按钮，更改应用此配置文件的用户。

此外值得注意的是：设置漫游配置文件，管理员除了要将配置文件路径添加到用户账号上外，还需要在服务器中创建共享的配置文件夹，并为用户配权限。这个任务并不繁重，而为了工作的方便，设置漫游配置文件总是很必要的。

最后需要保证网络的服务器必须是启用的，否则用户就不可能使用漫游配置文件。

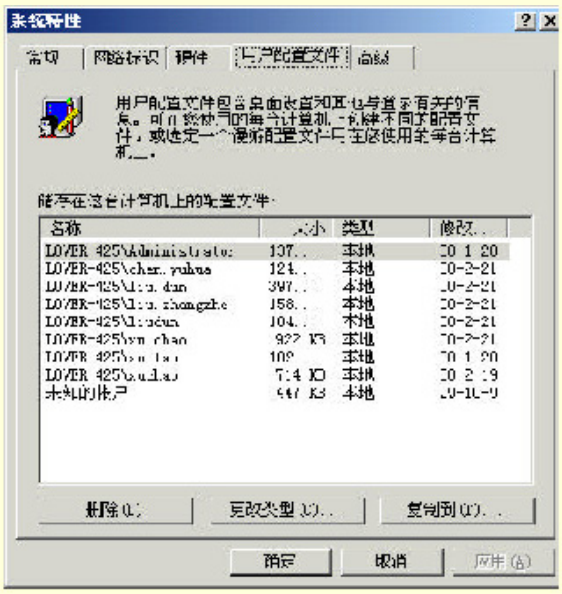


图 11-6 查看用户配置文件

11.1.2.3 各个配置文件关系

使用漫游配置文件的首要条件是服务器必须是启动的并能访问，如果服务器停用，为了能够正常工作，用户仍然需要本地配置文件的帮忙。

实际上，即使为用户配置了漫游配置文件，在登录的计算机上仍有本地配置文件。两者是这样配合工作的：

当用户第一次利用漫游配置文件登录时，这个漫游配置文件会自动复制到本地的配置文件中，如果此时服务器尚未启用，则用本地 Default Users 文件夹的内容进行本地配置文件的初始化。

用户注销时，设置的改动将同时对网络配置文件和本地配置文件更新，但如果服务器无法访问，那么无法回存到服务器上，就只能保存在本地配置文件中。

这时候会有一个问题：用户下次登录时，选用网络配置文件还是本地配置文件呢？一般情况下，服务器处于启用状态时，网络配置文件和本地配置文件能够同时更新，这时两个 Ntuser.dat 文件标志的修改时间相同，所以选用哪个配置文件的效果一样，不存在这个问题。（为了提高效率，可以直接使用本地配置文件）。但如果像上一段所说的，因故无法保存网络配置文件时，那么登录时系统在比较漫游配置文件与本地配置文件中就会发现本地配置文件比较新，这时将采用本地配置文件；如果是另外一种情况，用户在一台不经常使用的计算机上登录，系统发现网络上的配置文件版本更新，这时候就采用漫游配置文件，并把漫游配置文件复制到较旧的本地配置文件中以更新。

11.1.2.4. 强制配置文件

如果服务器上存放的配置文件是为多个用户准备的，那么就要设置共享配置文件，但事实上把漫游配置文件设为共享有许多麻烦：单个用户对配置的改动会影响到其他用户；用户注销时，由于其他用户仍在使用而无法保存配置文件等等。这时候更好的办法是将配置文件设为强制配置文件。

用户使用配置文件时，登录后可以修改自己的工作环境，但注销时无法存放在服务器中，这样一来就保证了用户使用相同的配置文件，而且不会被改动。需要注意：用户的修改虽然不能改变网络上的强制配置文件，但当其注销时，仍可以保存在本地配置文件中，以供无法使用网络配置文件时使用本地配置文件。

建立强制配置文件的方法是：将服务器上的漫游配置文件夹中的 Ntuser.dat 文件的后缀名改为 man，即将此文件更名为 Ntuser.man 即可。

同样可以采用上面配置漫游配置文件的方法，在用户属性对话栏配置文件选项卡中输入强制配置文件的网络路径，设置用户使用强制配置文件。

11.1.3　使用和管理配置文件

11.1.3.1 慢速连接

漫游配置文件和强制配置文件同属于网络配置文件，当用户通过较慢的广域网（WAN）或者出差在外通过笔记本电脑使用拨号连接的方式慢速连接网络时，从服务器中下载网络配置文件将需要相当长的时间，此外也占据了本来就不富裕的带宽资源，因此网络配置文件在慢速连接中是不受欢迎的。

如果连接时间过长从而导致超时，系统会提示继续下载网络配置文件还是使用本地配置文件，这时候可以选用效率较高的本地配置文件，并在网络通畅或者返回工作时重新连接网络以更新网络配置文件。

此外，可以指定用户使用强制配置文件，这将会防止用户从慢速网络中对网络配置文件更新所造成的麻烦和性能的损失。

11.1.3.2. 复制配置文件

双击打开控制面板中的“系统”命令，选择“用户配置文件”选项卡，将会看到本计算机上存储的配置文件。

提示：普通用户在其中只能看到自己的配置文件，而系统管理员可以存放在本计算机上的所有配置文件。

前面已经讲过复制配置文件的方法，打开“用户配置文件”选项卡后（如图 11-6 所示），在“存储在这台计算机上的配置文件”列表中，选择一个配置文件，单击“复制到”，如图 11-7 所示。

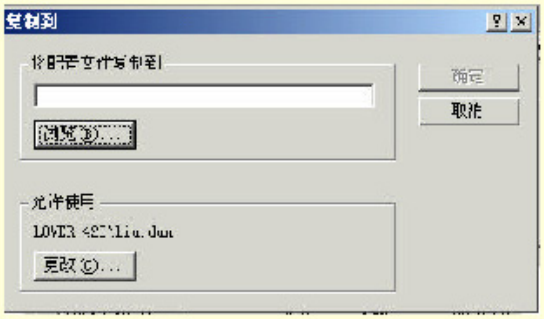


图 11-7　复制配置文件

在“将配置文件复制到”文本框中，输入复制路径，或者单击“浏览”，查找目标路径。

缺省情况下，复制的配置文件允许使用的用户就是原配置文件的用户，如果希望别的用户也使用这个配置文件，单击“更改”，在如图 11-8 所示的选择用户对话框中，选择使用此配置文件的用户或者组，单击“添加”，则此用户或组出现在“添加名称”框里。

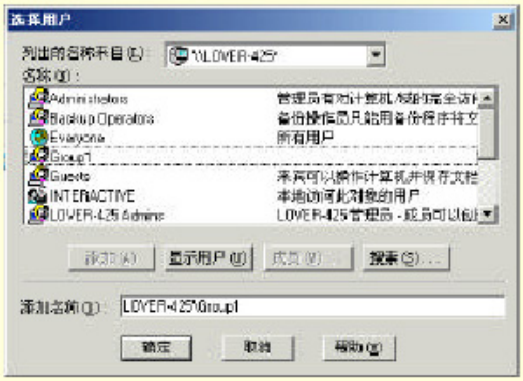


图 11-8　选择使用复制配置文件的用户

注意，必须是系统管理员才能复制配置文件。

11.1.3.3 删除配置文件

删除配置文件的方法与复制配置文件类似，在如图 11-6 中，选定要删除的配置文件，单击“删除”即可。

注意：当前使用的用户配置文件（也就是以当前用户命名的配置文件）不能删除，此外同样必须是系统管理员才能删除配置文件。

11.1.3.4 更改配置文件类型

用户可以选择更改当前使用配置文件的类型，在漫游配置文件和本地配置文件中两者间切换。在如图 11-6 中，选定要更改类型的配置文件，单击“更改类型”，如图 11-9 所示。

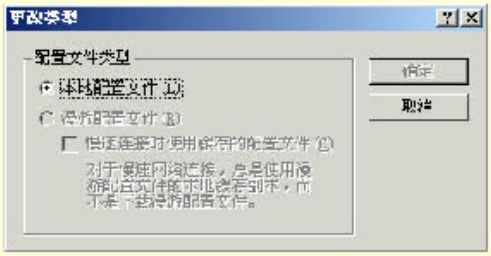


图 11-9 更改配置文件

当遇到前面所说的慢速连接的问题时，就可以将使用漫游配置文件更改为本地配置文件以节省带宽。如果选择漫游配置文件，并希望避免从慢速连接中下载的耗时，可以选中“慢速连接时使用缓存的配置文件”复选框。

11.2 Windows 2000 的组策略

除了使用配置文件外，还可以对用户的工作环境进行更强化的控制管理，限制用户的一些操作。

11.2.1 组策略介绍

在 Windows NT 4.0 中，提供了“系统策略编辑器”（System Policy Editor）进行用户工作环境的强化工作，管理员可以通过这个工具对存储在注册表数据库中的用户配置和计算机设置信息进行配置和修改，此外还可以创建系统策略以控制用户工作环境以及操作，并加强所有运行 Windows NT 的计算机的设置管理。系统策略可以针对用户、组或者计算机，提供全面的强化管理。

在 Windows 2000 中，系统策略编辑器被全新的组策略（Group Policy）所取代。组策略是在系统策略编辑器的基础上建立起来的，并提供了对用户配置和计算机设置的更方便强大的管理。在前面建立密码策略和账户锁定策略，以及审核策略时都已经用过了组策略这个管理工具，相信读者对它的强大功能已有深刻的印象。

系统管理员可以利用组策略设置管理用户桌面环境，包括用户可用的程序、用户桌面上出现的程序以及开始菜单选项。使用组策略管理单元，还可以为特定用户组创建特定的桌面配置。

微软提出了组策略对象（Group Policy Objects，或 GPOS）的概念。策略设置存放在组策略对象中，作为微软控制台的一个插件（独立的管理单元），组策略可以看作是一个文档类型是组策略对象的系统级应用程序。组策略对象和所选择的站点（sites）、域（domains）或组织单元（Organization Units）的 Active Directory 对象相关联。具体地说，组策略对象包括本地组策略对象、站点组策略对象、域组策略对象和组织单元组策略对象。

表 11-3 对本地组策略对象和非本地组策略对象进行比较。

表 11-3 本地组策略对象和非本地组策略对象

本地组策略对象	每台 Windows 2000 计算机中只有一个本地组策略对象（Local group policy object， LGPO），本地组策略对象设置可能会被与之发生冲突的非本地策略对象覆盖，如果没有冲突，那么两者都有效力
非本地组策略对象	存放在域控制器中（Domain Controller），只在活动目录（Active Directory）环境中存在。它们只适用于与此对象相关联的 Site 域，OU 单元中的用户和计算机

由表 11-3 可以看出，本地组策略对象相对是活动目录中级别最低的组策略对象，因为它可以被级别较高的站点、域和组织单元中的组策略对象所覆盖。除非运行的 Windows 2000 没有连接到网络上，或者网络中没有域控制器，则它不会被覆盖。

11.2.2　组策略单元的继承性

组策略是对活动目录中的阶层组织设置的，同权限的设置一样，存在子对象对父对象的继承问题。以下是一些继承规则。

■ 继承的方向

继承的方向总是从上到下，在子单元设置的策略不会被父单元所继承。

■ 关于未配置的策略

未明确设置的策略不会被继承。

■ 禁止设置的继承

父单元中对某些设置的禁止会被子单元继承。

■ 配置设置的继承

如果父单元中配置了某项设置，而子单元中没有设置，那么子单元将继承父单元的策略设置。

■ 可以兼容的设置继承

如果父单元中配置的某项设置可以与子单元兼容，那么子单元可以继承此策略。比如设置一个文件夹的快捷方式在桌面中，那么子单元中这个文件夹的快捷方式同样会出现在桌面中。

■ 不兼容的策略不被继承

如果父单元中配置的某项设置不能与子单元兼容，此时子单元不从父单元中继承此策略。在子单元中设置的策略在这里应用。

11.2.3　启动组策略单元

以下着重介绍本地组策略单元的使用。启动本地组策略单元的方法是：单击开始菜单中的“运行”，并键入 gpedit.msc。也可以通过“添加/删除管理单元”命令选择组策略来使用组策略单元，这时候还能够通过扩展选项卡扩展组策略单元（如图 11-10）。如图 11-11 所示是启动的组策略单元（本地计算机策略）。

图 11-10　扩展组策略单元

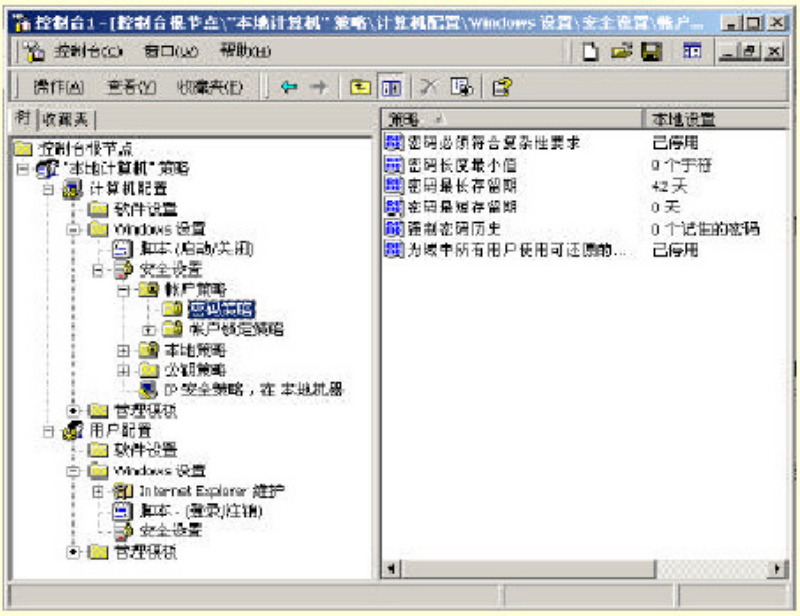


图 11-11 本地组策略单元

11.2.4 用户配置和计算机配置

由图 11-11 所示可以看出，组策略包括两个部分：针对用户的“用户配置”，以及针对计算机的“计算机配置”。二者小有区别，用户配置设置适用于用户的策略，不管用户登录哪一台计算机；相反地，计算机配置设置针对的是计算机，无论什么用户登录到此计算机上，管理员所作的计算机配置都有效。

尽管如此，如果安装的是 Windows 2000 Professional 版本而且没有连接到网络上时，这两个设置是大体上相同的。用户配置和计算机配置两个单元通常包含“软件设置”、“Windows 设置”和“管理模板”3 个子节点，但正如在管理控制台一章所述，由于组策略可向它添加或删除管理单元扩展组件，因此子节点的确切数目可能不同。

可以设置禁用用户配置或者计算机配置，在组策略根节点上单击右键，选择“属性”命令，如图 11-12 所示，在下方选择“禁用用户配置设置”或者“禁用计算机配置设置”，这样可以提高性能。

图 11-12 组策略属性

11.2.5　使用组策略单元

前面已经介绍过，组策略设置可以帮助系统管理员对需要管理的用户桌面环境的多种组件进行配置，例如用户可用的程序、用户桌面上出现的快捷方式、开始菜单选项等等，通过使用组策略管理单元，可以大大减少为特定用户组创建特定的桌面配置所花费的时间。

组策略单元具有的功能包括：

■ 通过管理模板管理基于注册表的策略。组策略的介入使基于注册表编辑器的注册表修改大为简化，同时很大程度上避免了直接修改注册表冒的风险。组策略所作的注册表设置被写入到注册表数据库的相应部分。例如，登录到工作站或服务器的用户，这些用户配置文件写在注册表 HKEY_CURRENT_USER 下，而计算机的特定设置写在 HKEY_LOCAL_MACHINE 下。

■ 分配脚本。脚本是指登录和注销时需要执行的批处理文件或者映射到网络驱动器等命令。可以利用组策略设置脚本。

■ 重定向文件夹。从本地计算机上的 Documents and Settings 文件夹重定向到网络位置。

■ 管理应用程序。管理应用程序的分配、发布、更新、修复等工作。

■ 进行安全管理。集中使用的组策略更方便地完成系统安全保护设置。

下面将对组策略的一些子单元进行详细介绍。

11.3　安全设置

其实组策略单元的使用一直贯穿在我们介绍过的 Windows 2000 管理之中，比如密码策略、账号锁定策略、审核策略等，只是没有集中讨论过罢了。组策略的管理范围远远超过上面几点，是非常强大的管理单元，这里限于篇幅，只能着重介绍其中几条。首先是位于“计算机配置”、“Windows 设置”下的“安全设置”子单元。

11.3.1　用户权利指派

用户权利指派位于安全设置的本地策略下，逐层展开后可以发现这个节点，如图 11-13 所示。

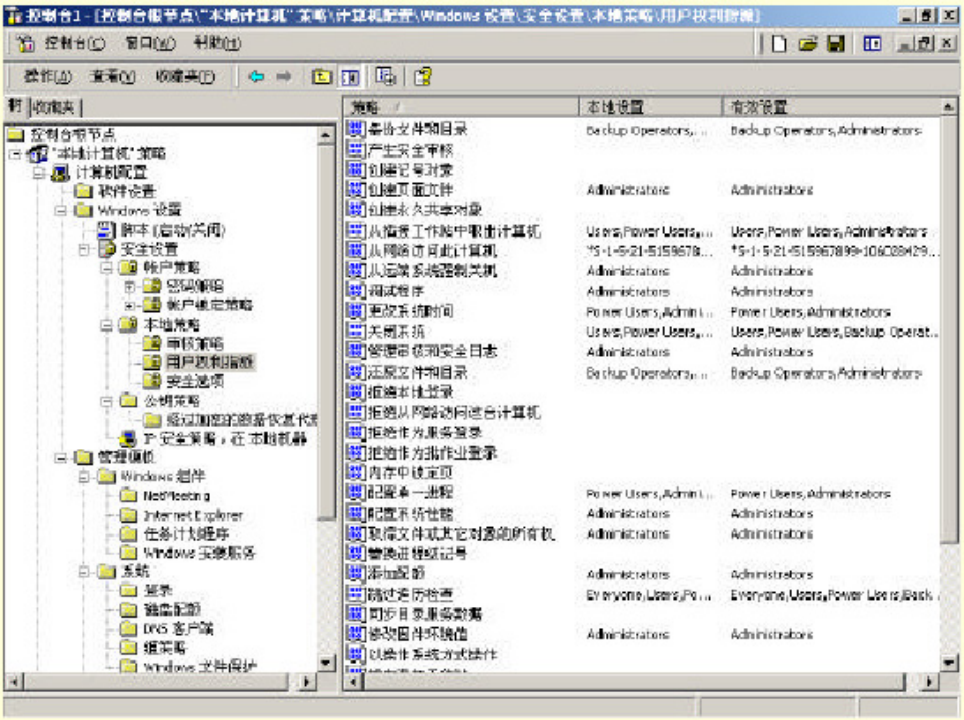


图 11-13　用户权利指派

由于 Windows 2000 中有内建的组，比如 Administrators、Power Users、Backup Operators、Users 等，对这

些组系统默认地为它们分配了权利（rights），以下是部分默认的用户权利分配：

- 备份文件和目录： Backup Operators、Administrators
- 创建页面文件：Administrators
- 远端系统强制关机：Administrators
- 更改系统时间：Administrators、Power Users
- 关闭系统：Administrators、Power Users、Backup Operators、Users
- 管理审核和安全日志：Administrators
- 还原文件和目录：Backup Operators、Administrators
- 配置系统性能：Administrators
- 取得文件和其它对象的所有权：Administrators
- 添加配额 ：Administrators
- 在本地登录：Administrators、Power Users、Backup Operators、Users 以及本机的 Guests、IUSR_computername
- 添加和卸载设备驱动程序：Administrators

在这个单元中，可以改变系统默认的这些权利指派，方法是双击某项权利，如图 11-14 所示，显示的是 Administrators、Power Users 有更改系统时间的权利，单击“添加”按钮，可以添加拥有这项权利的用户，也可以选择用户后，单击“删除”按钮，禁止其拥有更改系统时间的权利，其他各项的设置与此类同。

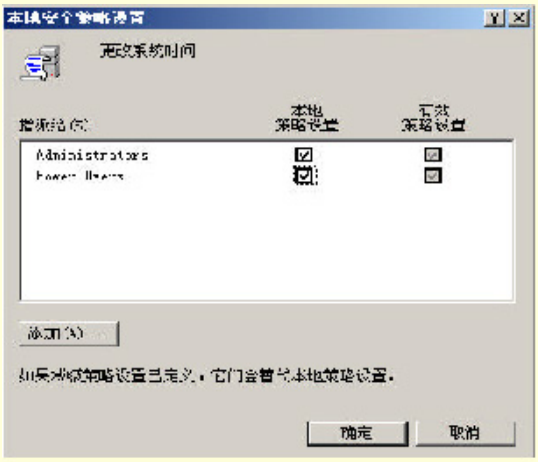


图 11-14 添加或者删除组的权利

11.3.2 安全选项设置

安全选项与用户权利指派一样，位于安全设置的本地策略下，这个设置用于通讯及其他方面安全的保障措施，如图 11-15 所示。

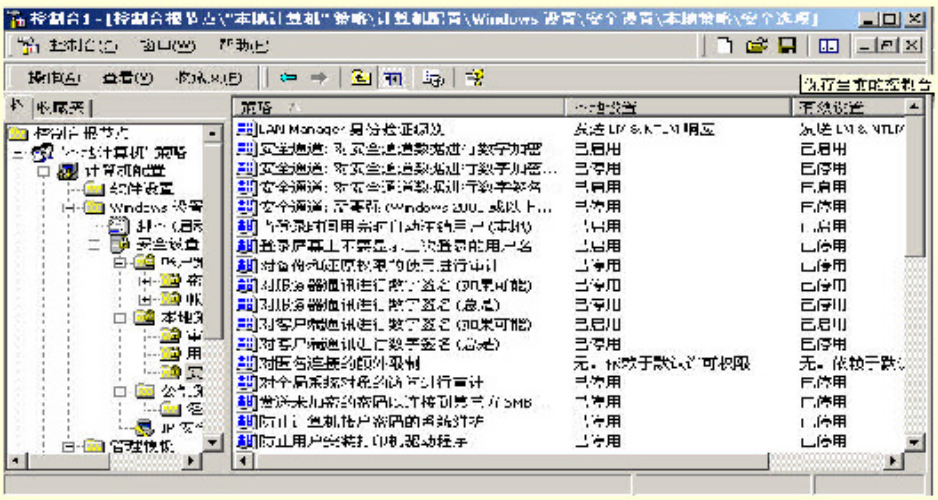


图 11-15 安全选项

可以在这里设置的安全选项有匿名连接的额外限制、登录消息标题文字、允许不登录关机、本地登录的用户才能访问 CD-ROM 和软盘、重命名管理员账户和 Guest 账户等。其中许多选项在安全性设置中都已经有过介绍。

图 11-16 显示的是设置不显示上次登录用户名，同样只要在该选项上双击就可以进行设置。各项设置的对话框会有所不同。

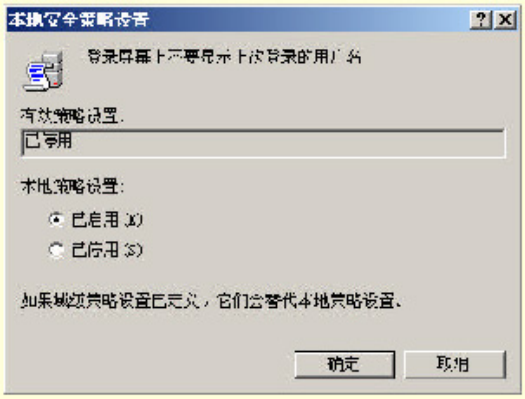


图 11-16　设置不显示上次登录用户名

在注册表一章中也谈过如何设置不显示上次登录用户名，相对而言，显然通过组策略的设置方法界面更友好，更令人放心。

11.3.3　导入策略

安全设置节点允许管理员为本地计算机策略配置安全等级，方法是将安全模板导入组策略对象中，这样当账户在组策略设置刷新时，将自动接收该模板的安全设置。在系统启动或组策略设置指示时，将应用安全设置。

导入策略的方法是：在安全设置节点上单击右键，从快捷菜单中选择“导入策略”命令，出现如图 11-17 所示的对话框。

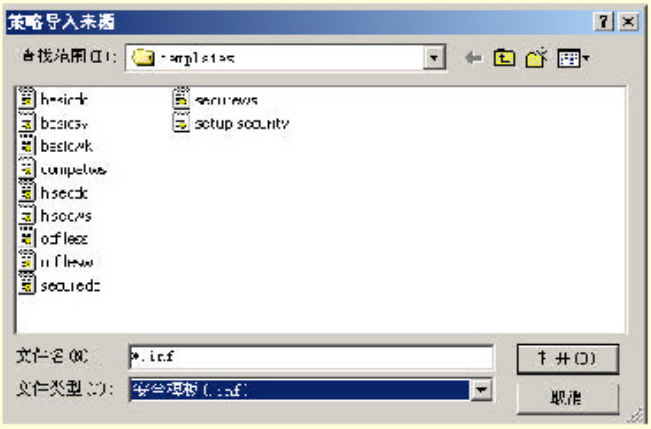


图 11-17　导入策略到组策略中

导入的策略来源于保存在 C:\Winnt\Security\templates 中的一些安全模板文件，Windows 2000 根据不同的安全性要求，制定了不同的安全模板。当计算机启动或“组策略”设置指定时，将应用安全模板中的设置，通过立即配置计算机的安全性来简化管理员的管理任务。

关于安全模板文件在安全性一章里还有介绍。

11.4　管理模板

前面已经介绍过，组策略的重要功能是通过管理模板管理基于注册表的策略，在 Windows NT 4.0 的系统策

略中，也使用管理模板进行管理工作。

在 Windows 的早期版本中，管理模板是 ANSI 编码的文本文件，在 Windows NT 4.0 中，管理模板的介入使得对注册表的编辑变得方便易行。同 NT 4.0 一样，Windows 2000 中管理模板的扩展名也为 .adm，此外，Windows 2000 还支持基于 Unicode 的 .adm 文件。两种模板文件的功能基本相同，但是在 Windows 2000 中引入 Windows NT 4.0 的系统策略可能导致一些不可预计的问题。由于管理模板只公开 .adm 文件中明确提到的注册表项，从而提供了一种比注册表编辑器（regedit.exe） 更友好的用户界面，增加了安全性，因此使用管理模板是管理用户环境的好主意。

管理策略中有两个模板节点，位置分别在：“本地计算机策略”\“计算机配置”\“管理模板”与“本地计算机策略”\“用户配置”\“管理模板”下。其中，“计算机配置”中保存有 HKEY_LOCAL_MACHINE 的设置；而“用户配置”保存有 HKEY_CURRENT_USER 的设置。二者管理的配置项目有区别，但也有相同的项目，如果在相同的项目中发生了冲突，Windows 2000 的处理与 Windows NT 4.0 系统策略中的处理一样，即计算机策略拥有更高的优先级。下面首先根据上面所说的位置，打开管理模板节点，如图 11-18 所示。

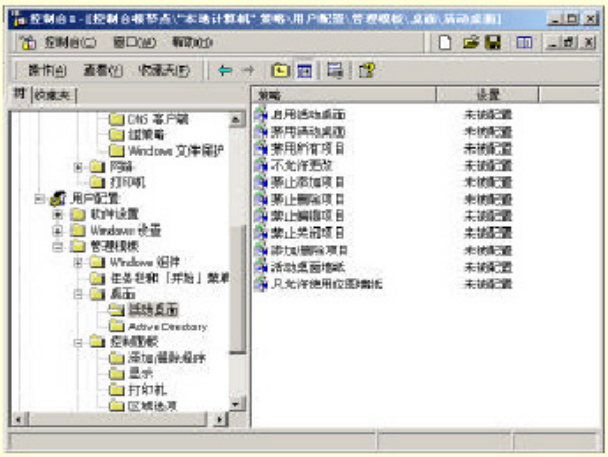


图 11-18 管理模板

管理模板的视图如上图 11-18 所示，各条策略共同组成了管理模板文件，如果已经熟悉了管理控制台，可以很方便地使用模板中的策略。图 11-18 中显示的是用户配置中关于桌面的配置管理模板策略，通过配置这些策略可以了解管理模板的使用。

如果管理员希望对用户的活动桌面进行限制，可以直接利用这些编制好的策略。在图 11-18 中双击某条策略，就可以从如图 11-19 所示的对话框中进行设置。

图 11-19 活动桌面属性管理

另外，还可以在各条策略上单击右键，从快捷菜单上选择“ 属性 ”命令，同样可以打开图 11-19 所示的属性对话框。有 3 种配置按钮可供选择：

■ 未配置：本策略未在系统中配置。

■ 启用：在系统中启用了这条策略。

■ 禁用：在系统中禁用这条策略。

管理员可以在这些选择中进行切换，然后选择“ 确定 ”或者“ 应用 ”即可。如果要对上一策略或者下一条策略进行配置，可以单击下面对应的按钮。启用或者禁用策略的选择都将保存到注册表中。

如果对某条策略不了解，可以在如图 11-20 所示对话框中选择“ 说明 ”选项卡，通过查看说明帮助了解本条策略。

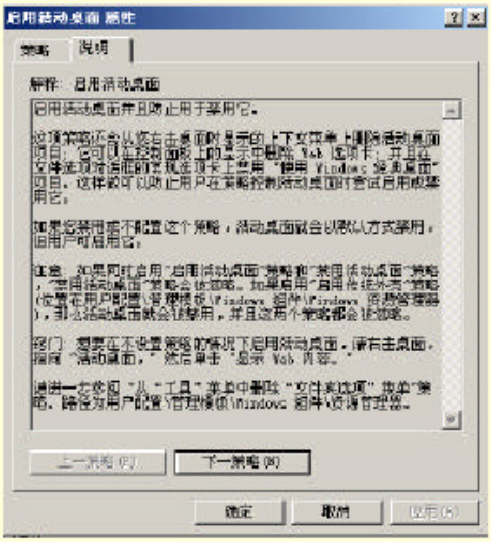


图 11-20　策略说明

了解了活动桌面的策略管理，对其他策略的使用就很容易理解了，它们实质上是相同的模板文件。管理模板提供的其他管理还有许多，这里着重介绍比较常用的一些设置。首先是用户的开始菜单和任务栏。这个管理节点位于用户配置的管理模板下。

如图 11-21 所示对开始菜单中是否删除运行菜单策略进行配置，如果删除了“ 运行 ”菜单，用户将无法进行一些通过命令行启动的命令。

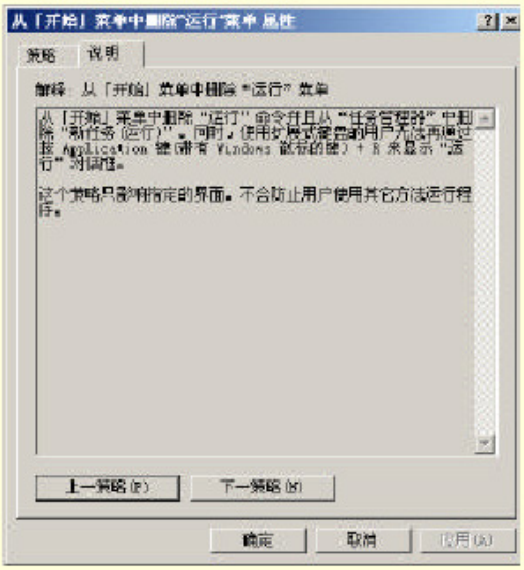


图 11-21　从开始菜单中删除“ 运行 ”菜单

这个节点还可以进行如下一些配置：从开始菜单删除公用程序组、删除文档菜单、删除帮助命令、删除搜

索菜单、添加注销命令、不保留最近打开的文档记录、禁用任务栏的上下文菜单等等。

下面是关于用户登录/注销的策略，这个节点位于用户配置\管理模板\系统\登录/注销下，包括禁用任务管理器、禁止锁定计算机、禁止注销、同步运行登录脚本、限制配置文件大小、禁止改变密码等，如图 11-22 所示。

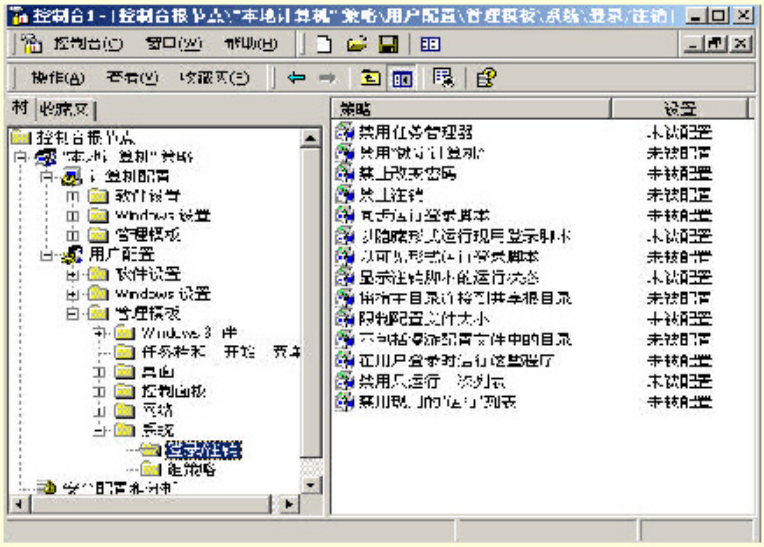


图 11-22 登录/注销策略

计算机配置节点中也有相应的登录/注销策略，如果计算机配置和用户配置发生矛盾时，计算机配置的优先级别更高。

再举一个例子：如果希望禁止用户更改墙纸，可以在“用户配置”\“管理模板”\“控制面板”\“显示”中进行配置，禁止更改墙纸可以统一桌面。

与此类似的例子可以举出很多，管理模板中涉及到用户管理的许多方面，每条策略的配置都基本相似，这里有许多各种常用的设置，充分利用可以省去修改注册表的繁琐与危险。

11.5 脚本管理

所谓脚本是指一个程序文件，比如带扩展名.BAT，.CMD，或者.EXE 的文件，这些程序文件伴随着系统或者用户的动作执行。环境管理包括设置用户登录与注销的脚本程序，或者计算机启动与关机的脚本，当登录、注销或是启动、关机时程序将自动执行。

在用户管理一章中，读者可能已经注意到管理用户属性时就包括了分配脚本，可以在用户属性对话框里直接输入脚本文件。从本地用户和组中选择用户，单击右键并选择“属性”命令，选择配置文件选项卡，出现如图 11-23 所示的用户配置对话框。

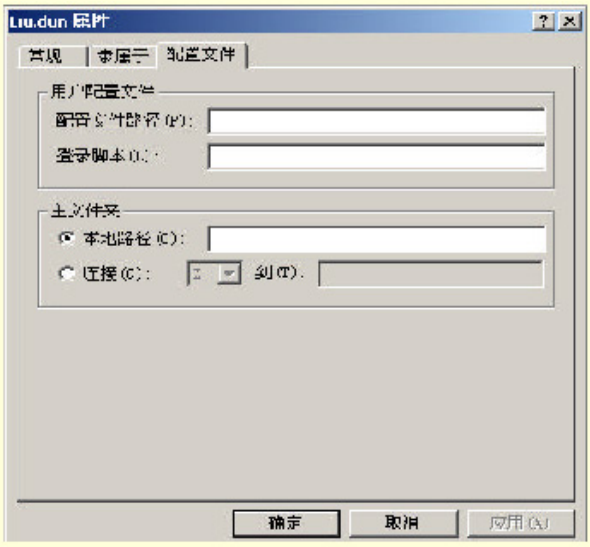


图 11-23 在用户配置文件中指定脚本

计算机关闭、启动的脚本默认存放在系统路径（%Systemroot%）下的 System32\Grouppolicy\Machine\Scripts 下的 Shutdown 和 Startup 目录中，相应地，用户登录、注销使用的脚本默认存放在%Systemroot%\System32Grouppolicy\User\Scripts 下的 Logon 和 Logoff 目录中，一般来说，系统路径%Systemroot%就是 C:\Winnt。需要注意，Windows 2000 中的脚本路径与 Windows NT 4.0 的 C:\Winnt\System32\repl\import\repl\import\scripts 不同。可以把脚本放在这个路径中，然后在图 11-23 中指定脚本文件名。

脚本的设置还可以在组策略管理单元中完成。

启动组策略单元（本地计算机策略）后，可以发现有两个脚本控制节点，位置分别是“计算机配置”\“Windows 设置”\“脚本”以及“用户配置”\“Windows 设置”\“脚本”。

两个脚本节点的名称并不一样：在计算机配置节点中是“脚本（启动/关闭）”，而在用户配置节点中是“脚本（登录/注销）”，也即脚本是分别针对计算机和用户的。

双击某个脚本节点（启动/关闭，或是登录/注销），出现如图 11-24 所示的脚本对话框。

单击“添加”按钮，可以指定脚本文件。在已经存在的脚本文件中，单击“编辑”按钮，可以配置脚本文件的命令参数，单击“删除”，则删除已有的脚本文件。

可以指定多个脚本文件，这时候需要安排多个脚本文件的执行顺序，单击“上移”或者“下移”，可以调整各个脚本文件的执行顺序，如图 11-24 所示。

另一方面，Windows 2000 包括 Windows 脚本宿主（Windows Scripts Host），这是一种用于 32 位 Window 平台，并且不受脚本语言约束的支持组件，包括 VBScript 和 JScript 脚本引擎。可以使用 Windows 脚本宿主直接在桌面或者命令控制台上运行 .vbs 和.js 脚本，而不必将这些脚本插入到 HTML 文档中，因此这种脚本也可以用于计算机启动、关机或是用户登录、注销的脚本程序。

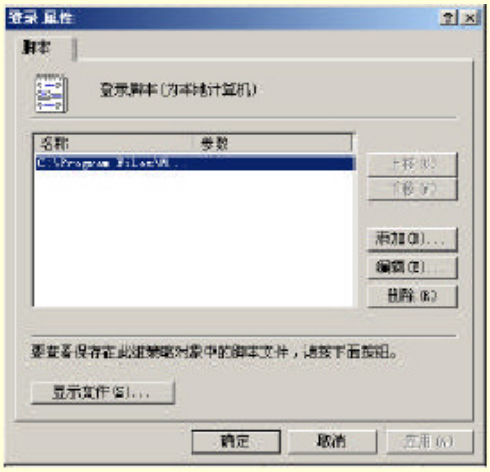


图 11-24　配置脚本文件

11.6　主目录管理

在本地用户和组中，管理用户配置的方法还包括为用户指定主目录。一般说来，Windows2000 为用户指定了“我的文档”文件夹，用于集中保存用户的个人文档，当用户保存或打开文件时，对话框往往最先调出“我的文档”。除了“我的文档”之外，系统还允许管理员为用户创建另外一个保存文档的文件夹，这个文件夹叫做“主目录”。

主目录的指定在“本地用户和组”管理单元中完成。办法很简单，选择某个需要配置的用户，单击右键后，选择“属性”命令的“配置文件”选项卡，如图 11-25 所示。

图 11-25 主目录

指定了主目录后，一些程序将把文档保存到用户的主目录中。此时主目录和“我的文档”文件夹之间的关系是：这些程序先在主目录中查找是否有与要打开或保存的文件类型匹配的文件，例如，*.doc 或 *.txt。如果有，程序将打开主目录而忽略“我的文档”。如果没有找到该类型的文件，程序再打开“我的文档”。但是主目录并不能取代我的文档，因为还有一些程序不理会主目录而只打开”我的文档”，比如写字板程序。

主目录可以位于用户的本地路径，也可以在网络的服务器中。要配置服务器中的主目录，在图 11-25 中选择“连接”，选择驱动器号，然后输入连接的路径名。可以用 %username%代替路径中最后的子目录，例如：\\server_name \Users\%username%。当然，这时候首先要在网络服务器上创建和共享这个用来储存主目录的文件夹，并分配合理的权限。注意：主目录不是漫游用户配置文件的一部分，它的大小不会影响登录的传输速度。

第 12 章　管理控制台

Windows 2000 的最大特色无疑应该是崭新的管理控制台。管理控制台在 Windows NT 4.0 中和 IIS 一块推出，并在 Windows 2000 中得到了更好的改善，实现了紧密的结合。前面介绍的用户管理、计算机管理、性能监视、共享管理、系统策略、事件查看等等工作都可以在管理控制台中执行，这意味着管理员完全可以在同一处对整个系统进行全面的管理工作，而再也不用像在 Windows NT 4.0 那样打开管理工具，在各个工具中频繁切换进行不同的工作了。同时请注意：管理控制台并非是各个工具的简单集成，作为一个全面的控制台，它添加了许多方便快捷的手段，帮助管理员顺利地完成任务。管理控制台大大提高了工作的效率，使管理不再困难而变得有趣。

本章内容包括：

- 初识管理控制台
- 使用控制台
- 添加插件单元
- 创建任务板

12.1　初识管理控制台

认识新事物的最好办法就是使用它，可以通过在开始菜单中的“运行”命令键入 mmc 运行管理控制台。

初次打开管理控制台的界面如图 12-1 所示。这是一个空白的面板，看起来平无奇，但千万不要小看它，因为这张白纸完全可以做成一幅最美丽的图画。

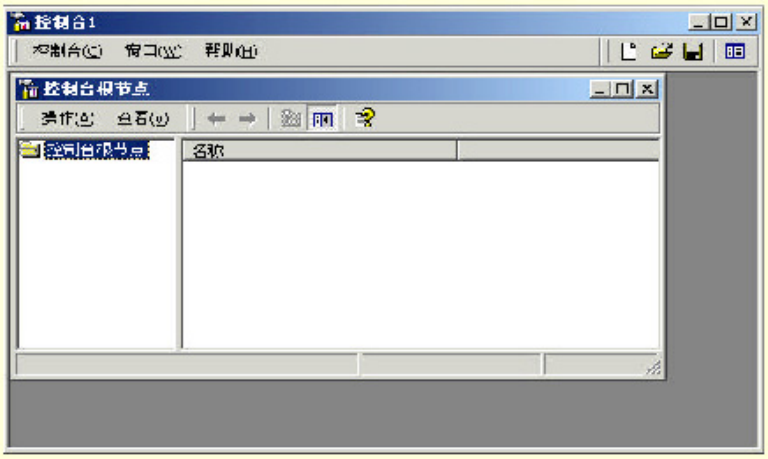


图 12-1　空白的管理控制台

简单地说，可以把管理控制台（Microsoft Management Console ，MMC）理解成为一个用于创建、保存和打开管理工具集合的控制台。控制台中包括插件单元、扩展插件单元、监视控制、任务向导以及各种文档，在管理控制台上可以完成 Windows 2000 系统中的各种硬件、软件以及网络组成等资源的管理工作。

提示：插件单元是 Windows 2000 重要概念，它实际上同 NT 4.0 的管理工具是等同的，比如目录服务管理器（Directory Service Manager）或者设备管理器(Device Manager)等。不过在 Windows 2000 中，插件可以在控制台中控制树上添加或者删除，这就使得它变得更加灵活。插件单元可以分为两种：独立的插件单元和扩展的插件单元。前者可以直接添加，而后者不能独立添加，只能添加到其它的插件单元中。

常用的插件单元有：安全模板、安全配置和分析、本地用户和组、性能日志和警报、系统信息、服务、共享文件夹、事件查看器、设备管理器、可移动存储、磁盘碎片整理程序、索引服务、FrontPage 服务扩展、IP 安全策略管理、磁盘管理、逻辑驱动器、Web 地址连接、Internet 信息服务、证书等。

现在可以理解为什么说如图 12-1 所示的空白的管理控制台可以画出“最美的图画”了，答案是往控制台上添加各种插件单元（这个工作十分简单），在很短的时间里，控制台将变得十分的强大，可以完成各种管理工作。如图 12-2 所示就是一个功能强大的管理控制台。

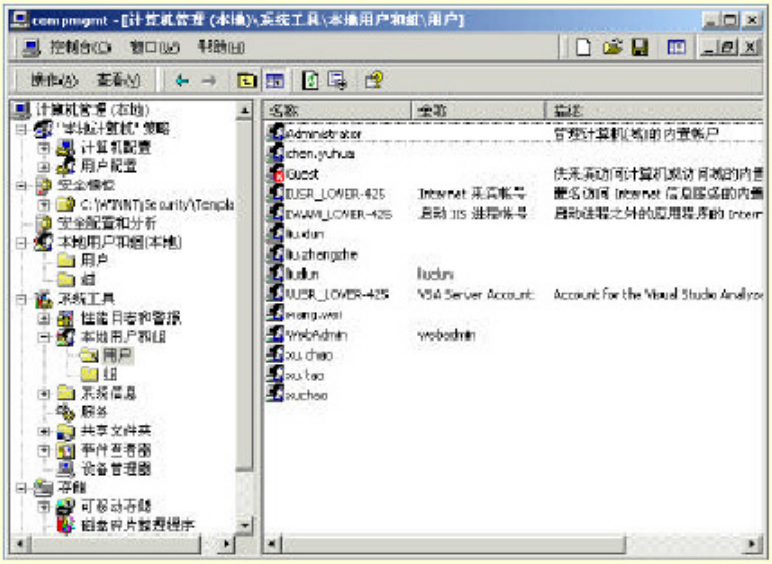


图 12-2　添加了插件的管理控制台

从图 12-2 中也可以看出，管理控制台的界面非常友好，它的组织同资源管理器十分相似，左边采用树状结构，右边是具体内容的面板，因此并不难理解，这在很大程度上降低了人们对管理工作的畏惧感。

必须明白：管理控制台不是僵化不变的，可以自由伸缩变化，进行细节上具体的配置，这通过创建、修改和保存自己的控制树完成。

12.2　使用控制台

12.2.1　作者模式和用户模式

有两种使用管理控制台的模式：作者模式和用户模式，而用户模式还有 3 种等级，因此访问共有 4 种模式。

- 作者模式（Author Mode）：处于作者模式下可以对管理控制台有完全控制权，包括添加或者删除插件单元，创建新的窗口，创建任务板和任务以及查看控制树的所有部分。
- 用户模式—全面访问（User Mode—full access）：用户可以访问 MMC 的所有管理窗口功能，还能对管理树做全面访问。但不允许用户添加或者删除插件单元和更改控制台文件选项。菜单上没有保存命令，但是不影响管理单元关系的更改会自动保存。
- 用户模式—受限访问，多窗口（User Mode—limited access, multiple window）：用户无法打开新窗口，而且无权访问在保存控制台文件时不可见的控制台树区域。在全面访问用户模式中实行的所有限制同样适用。允许多个窗口，但用户无法关闭这些窗口。
- 用户模式—受限访问，单窗口（User mode —limited access, single window）：对于多窗口有限访问拥护模式实行的所有限制也在此适用，唯一不同的是只有一个子窗口，因此没有多窗口所用的限制。

改变访问模式的方法是：在管理控制台中选择“控制台”→“选项”命令，如图 12-3 所示，从“控制台模式”下拉列表框中，选择使用的模式。

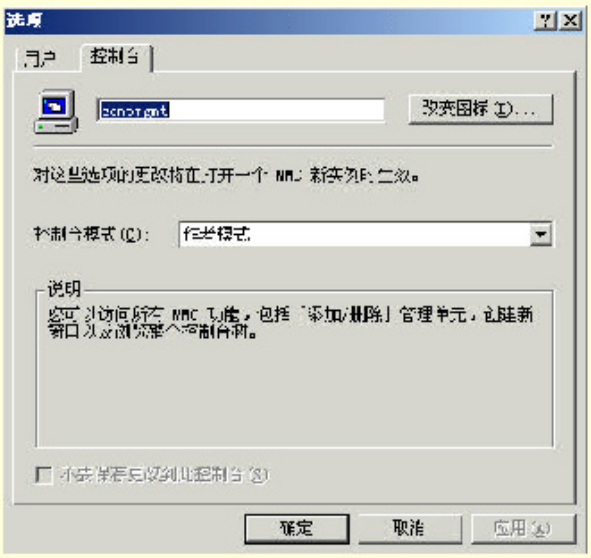


图 12-3　改变访问模式

对那些不需要创建或者修改控制台的普通用户，作者模式是不必要的，管理员应该限制他们的操作，可以通过访问模式的控制做到这点。

当然，使用作者模式可以使管理员最大限度地自由管理控制台，管理员通过将控制树组织到自己喜欢的节点上，并且添加管理单元，或者建立新的窗口从而方便自己的工作。

使用作者模式打开管理控制台的方法是：在开始菜单中的“运行”命令键入 mmc/a。如果缺省的已经是作者模式，则打开任何管理窗口时都已经处于作者模式。另一方面，在管理控制台中选择“控制台”→“选项”命令，如图 12-4 所示，选择“用户”选项卡，并且选中“总是以作者模式打开控制台文件”复选框。

图 12-4　总是以作者模式打开控制台文件

提示：用户只有处于作者模式或者用户模式—全面访问时才能使用用户选项卡，而只有处于作者模式才能使用控制台选项卡。

12.2.2　使用命令行打开管理控制台

前面已经介绍过通过在开始菜单中的“运行”命令键入 mmc 或者 mmc/a 命令以打开管理控制台，这条命令的完整格式是：mmc path\filename.msc [/a /s]。各参数的解析如下：

path\filename.msc：

由于可以将控制台存成文件（后面将有介绍），因此可以通过打开打开控制台文件来打开管理控制台，就好象打开一个 Word 文档也就打开了 Word 应用程序一样。path\filename.msc 参数给出了控制台文件的路径和文件名。

例如：mmc c:\winnt\system32\console_name.msc。如果控制台文件存在系统目录下，可以通过键入 %systemroot%以代替系统根路径。这时候只需键入：

mmc %systemroot%\system32\console_name.msc

/a：

使用/a 命令，以作者模式打开保存的控制台文件，这时可以修改文件或者创建新的控制台。如果管理控制台是以这种方法打开的，则所有控制台文件都处于作者模式，而无论原先文件的缺省模式是否是用户模式。但是/a 命令并不改变文件的缺省模式，下次不用/a 命令打开它时，仍然按照缺省的模式打开。

/s：

使用/s 命令，则打开控制台时不会出现提示屏幕。

12.2.3 打开控制台文件

在控制台中，打开“控制台”→“打开”菜单命令，出现如图 12-5 所示的对话框，选择保存的控制台文件（后缀名为 msc）并打开即可。

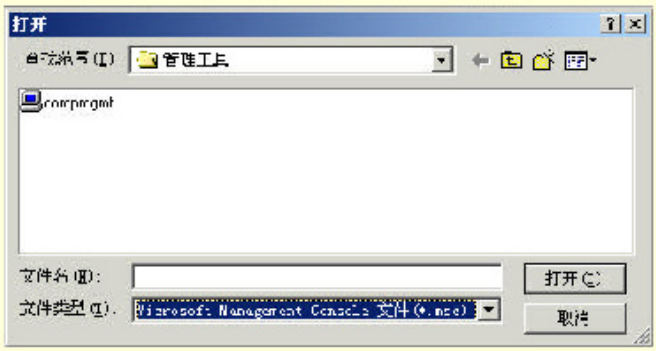


图 12-5 打开管理文件

12.2.4 保存控制台文件

在打开的控制台中，打开“控制台”→“另存为”菜单命令，如图 12-6 所示。

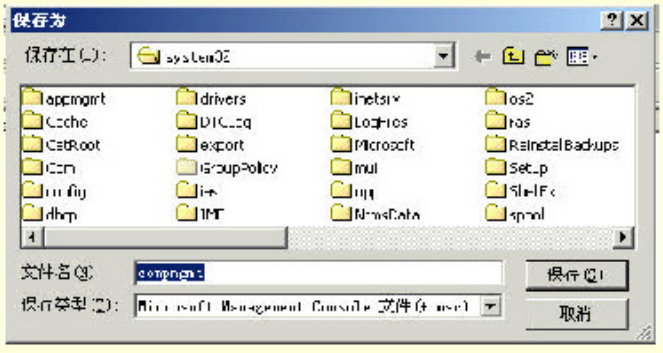


图 12-6 保存控制台文件

这时可以保存为 msc 控制台文件。

保存文件时，同时也就保存了控制台中的插件单元、控制窗口中的内容及其组织，以及模式和访问的等级。下次打开这个文件时，这些信息也被同时恢复。

在 Windows 2000 Professional 中，缺省时在开始菜单的程序组中，并没有管理工具这一项，这同 Windows NT 4.0 是不一样的。但是如果将一个控制台文件存放在\\systemroot\Documents and Settings\user\开始菜单\程序\管理

工具中，这时候在开始菜单中就会出现管理工具了。

12.3　添加插件单元

前面的介绍已经表明：管理控制台 MMC 并不能完成具体的管理工作，它只是相当于一个各种管理工具的宿主（Host）。

管理控制台下容纳了众多的管理工具，这些工具实现的才是具体的管理工作，而管理控制台作为一个平台，提供了统一的界面，比起过去各个零乱、分散的管理工作，管理控制台的出现可以帮助管理员更好地完成管理工作。

全新的管理控制台的一大特色是可以添加管理单元。管理单元被看成为一个 Snap-In，亦即插件，它是管理控制台中可以添加的最重要，最常用的管理工具。插件单元还包括独立的插件和扩展的插件。其他可以在控制台中添加的工具包括 ActiveX 控制（ActiveX Controls）、Web 页的连接（Links to Web pages）、文件夹（Folders）、任务板（Console Taskpads）等。

尽管可以作这样的分类，但他们其实完成的都是管理工作，只是形式上有区别而已。要在管理控制台中完成管理工作，就必须在控制台上添加这些工具：或者在本地添加或者给其他计算机添加。

12.3.1　添加本地管理单元

在本地添加插件单元的方法是：

（1）打开管理控制台中的“控制台”→“添加/删除管理单元”命令，如图 12-7 所示。此时，还可以选择管理单元添加到哪一个节点上，可以是控制台根节点，也可以是其他的节点。选择不同的节点是为了单元组织得更加合理，或者更符合管理员的习惯。

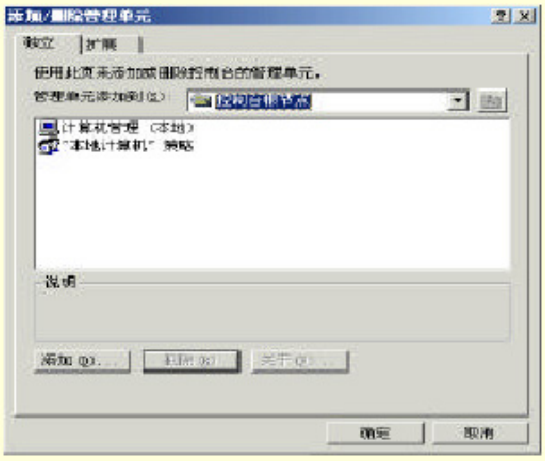


图 12-7　添加/删除管理单元

（2）单击“添加”按钮，出现如图 12-8 所示的独立管理单元列表。

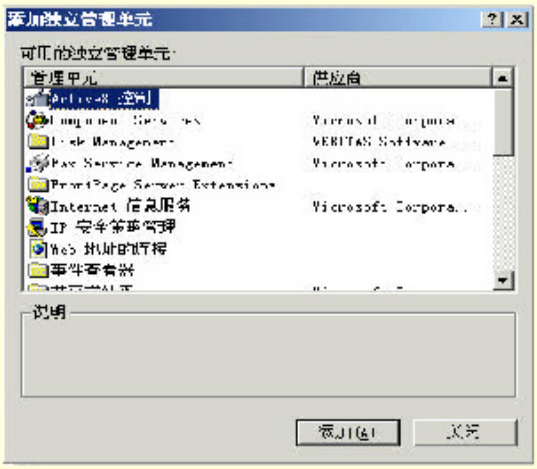


图 12-8　添加独立管理单元

（3）在可用的独立管理单元列表中，滚动选择管理单元完成添加。具体的管理单元可能取决于用户的 Windows 2000 的版本是 Professional 还是 Server 版本。此外，有些管理单元只需要直接按“添加”即可完成添加，有些则可能会出现向导帮助完成添加。

下面以从 Internet 服务管理器（IIS）中添加“Web 地址的连接”管理单元为例，介绍添加的过程。

（1）打开 Internet 服务管理器管理控制台。

（2）按前面的方法，逐步选择添加/删除管理单元，并从如图 12-8 所示的对话框中选择“Web 地址的连接”管理单元。

（3）单击“添加”按钮，此时出现如图 12-9 所示的向导，在“目标 URL”文本框中，输入网址。如图中 12-9 所示输入的是 www.microsoft.com。

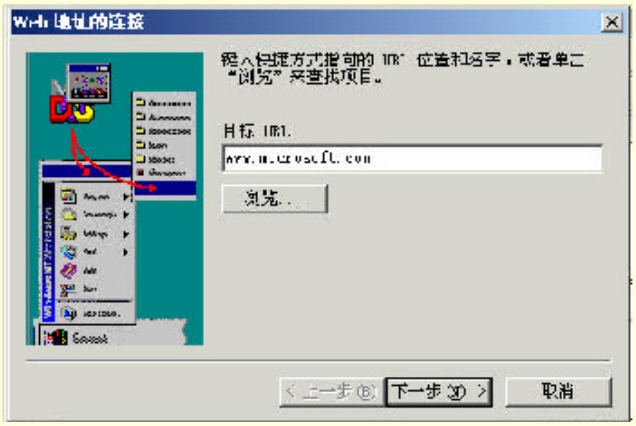


图 12-9 Web 地址的连接添加向导

（4）单击“下一步”按钮，如图 12-10 所示，这时候向导提示输入目标 URL 的参照名。键入一个友好的名字以方便记忆。本例输入的是 microsoft。

（5）如图 12-10 所示，单击“完成”按钮，完成添加。

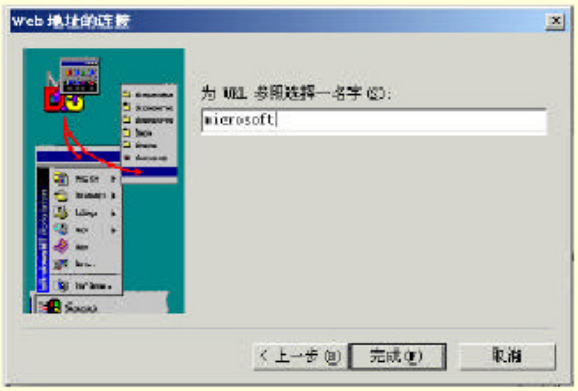


图 12-10 输入目标 URL 的参照名

完成之后，在 IIS 管理控制台就会出现名为 microsoft 的 web 地址连接，在接入 Internet 的条件下，单击 microsoft 即可连接微软的网址。

提示：如果某一个你想添加的插件单元没有出现在单元列表中，则可能是相应的服务或者软件没有在你的计算机上安装，这时候应该首先安装软件。

12.3.2　为远程计算机添加管理单元

除了在本地计算机中安装管理单元外，还可以选择给远程计算机控制台安装。

远程安装的前面两个步骤同本地安装一样，首先从菜单命令中选择添加/删除管理单元，单击添加后，在如图 12-8 的可用管理单元列表中，选择要添加的管理单元，并在其上双击。如果是可以为远程计算机添加的管理单元，将出现如图 12-11 的“选择计算机”对话框。

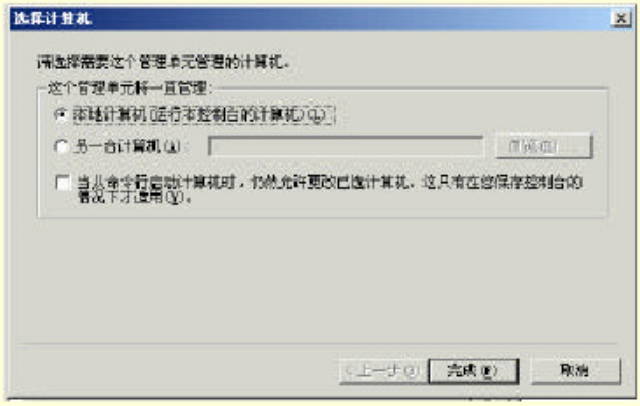


图 12-11　选择远程计算机

选择了远程计算机后，单击“完成”按钮即可按照提示进行添加。

如果此时没有出现如图 12-11 所示的对话框，而是直接出现添加向导，那么这个管理单元只能在本地计算机上添加。

12.3.3　添加扩展管理单元

插件单元可以分为独立的单元和扩展的单元。与独立的管理单元不同，扩展的管理单元不能直接添加到节点中，它们只能添加到独立的管理单元中，帮助扩展管理单元的管理。

在如图 12-7 所示对话框中，单击“扩展”选项卡，如图 12-12 所示。

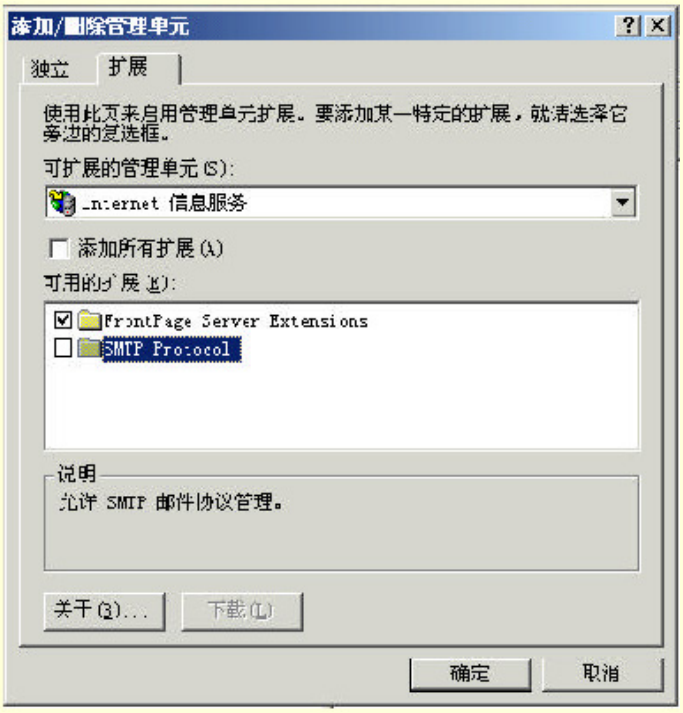


图 12-12　扩展的管理单元

在此页面中启用管理单元扩展。要添加某一种扩展，先选择可扩展的管理单元，然后选择特定的扩展单元，

选中复选框即可。如果对某个单元不了解，单击“关于”按钮，将出现这个单元的版本号。

如果选中“添加所有扩展”，则不需要为每个扩展作标记，这时候所有扩展自动添加。

12.3.4 建立新窗口

如果觉得控制树过于“根枝繁茂”而不利于观察的话，可以为某一个管理单元建立新的窗口。方法是：选中插件单元后，单击右键，从快捷菜单中，选择“从这里创建窗口”命令，如图 12-13 所示。

图 12-13 从这里创建新窗口

创建新窗口后，管理窗口将变得简洁，并且可以在不同的窗口间切换。

12.4 创建任务板

管理控制台的又一大特色是可以在控制台中创建任务板，从而使控制台的任务执行起来更加简便。

任务板是一个可以自定义的窗口，同时可以认为任务板是一个 HTML 页面，在其中创建一个加标注的大图标，以代替标准的快捷菜单和 MS-DOS 命令。利用任务板中的快捷方式，管理员或者用户可以方便地启动向导，打开属性页、执行命令行命令或者打开 Web 页等等。总之，用户完全可以配置自己的任务板以容纳所有需要执行的任务。

微软认为，任务板可以帮助 Windows 2000 的新手更容易地执行任务，他们可以在熟悉新的管理控制台之前使用自己的任务板，当然，需要把可执行的任务集成到任务板中去。但是这样一来用户同样需用面临着熟悉新的任务板的过程。所以，笔者认为任务板的优点反倒应当是帮助那些熟悉控制台的管理员执行比较复杂的任务，比如，如果他们经常使用一组插件，可以把那些需要的对话框、属性页、命令行和脚本放在一起。

创建任务板的方法是：

（1）在需要创建任务板的插件单元上，单击右键，选择创建任务板命令（注意：不是每个单元都有这个命令），如图 12-14 所示。

（2）单击“下一步”按钮，如图 12-15 所示，可以创建单一项目的，这时显示详细信息。也可以创建独立的类型，这时只显示任务。

（3）单击“下一步”按钮，可以为控制台树的任何项目创建任务板，选中具体的项目。如图 12-16 所示。

（4）单击“下一步”按钮，选择水平列边或者垂直列表作为自己的列表样式。以下各步不再附图说明。

（5）单击“下一步”按钮，选择是否需要添加一个更改按钮。若创建一个更改按钮，任务板一次只能用于一个项目，但可以通过选择更改按钮，使任务板用于其他项目。

（6）单击“下一步”按钮，选择使用的标题类型，可以是路径类型，也可以自己添加命名，或者干脆不使用命令。

（7）单击“下一步”按钮，输入任务板的描述性信息。

（8）单击“下一步”按钮，并单击“完成”按钮，完成任务板的创建。

图 12-14　任务板向导

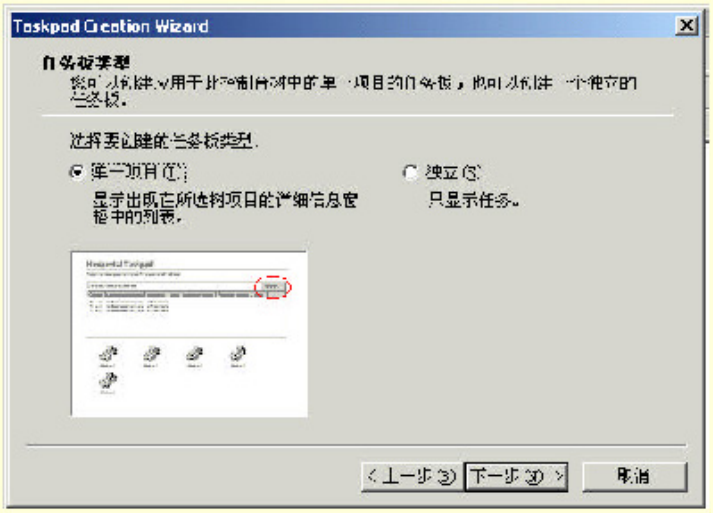


图 12-15　选择创建的任务板类型

图 12-16　选择创建任务板的项目

图 12-17 所示是在 IIS 控制台中为默认 Web 站点项目创建的任务板。

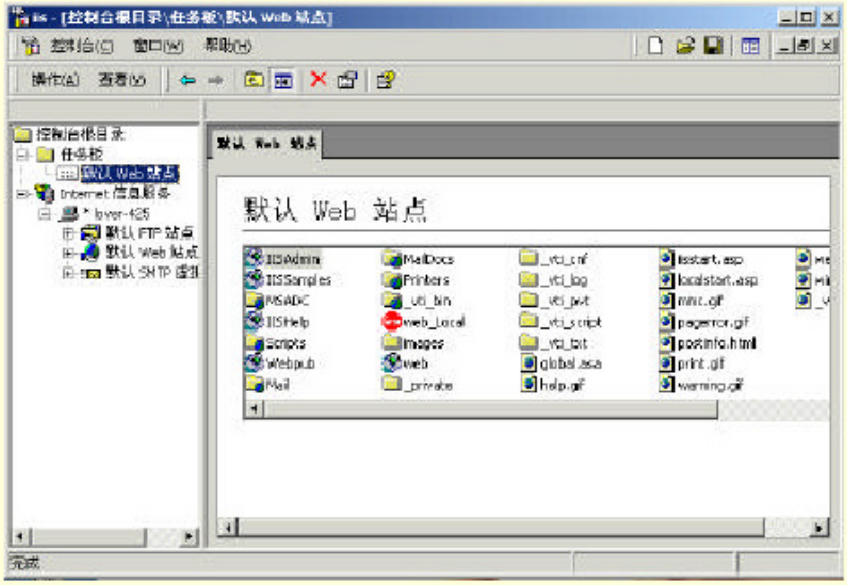


图 12-17 任务板

以上各项设置都可以在任务板创建完成后，再进行配置改动。方法是在如图 12-17 所示的任务板名称（图中是默认 Web 站点）上单击鼠标右键，此时将出现“编辑任务板”快捷命令。选择这个命令后，就可以从如图 12-18 中的“常规”选项卡中修改前面的设置。

任务板中可以添加各种常用任务的快捷图标。当任务板创建完成后，向导会自动出现创建新任务的新向导，可以立即创建任务，也可以过后再创建任务。这时仍然在任务板名称上单击鼠标右键，选择“编辑任务板”快捷命令，然后选择任务选项卡，如图 12-18 所示。

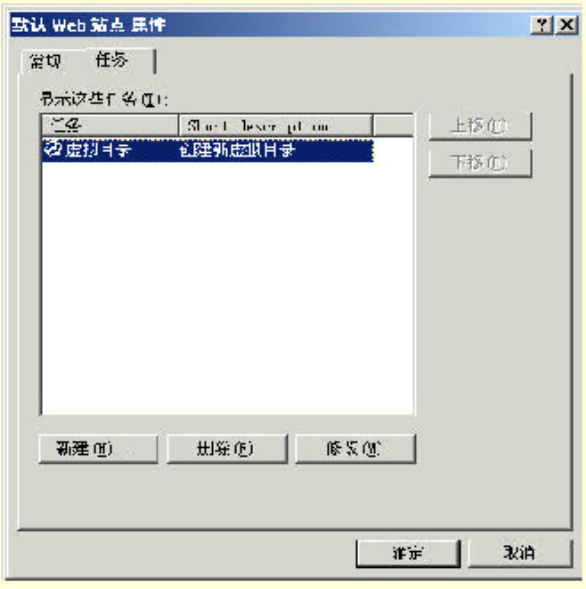


图 12-18 编辑任务板

单击“新建”按钮，此时出现类似图 12-14 所示的向导。依照向导的提示，单击“下一步”按钮，选择启动一个菜单命令，或者运行一个 MS-DOS 命令。

选择菜单命令，出现如图 12-19 所示的对话框。

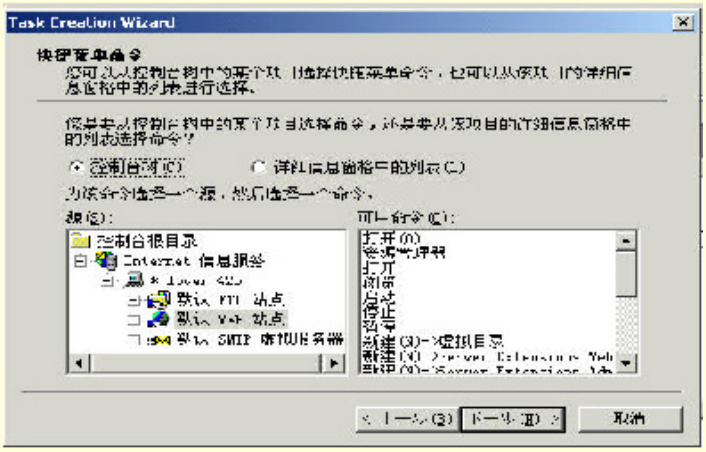


图 12-19　选择快捷菜单命令

用户可以从控制台树中的某个项目选择命令，或者从该项目的详细信息窗口中的列表选择命令。这取决于对某个命令的使用频繁程度。所有的命令都在如图 12-19 中显示，比如打开、浏览、启动、停止、新建虚拟目录等等。

如果选择的是运行一个 MS-DOS 命令，则出现如图 12-20 所示的对话框，提示输入命令的路径和命令参数。

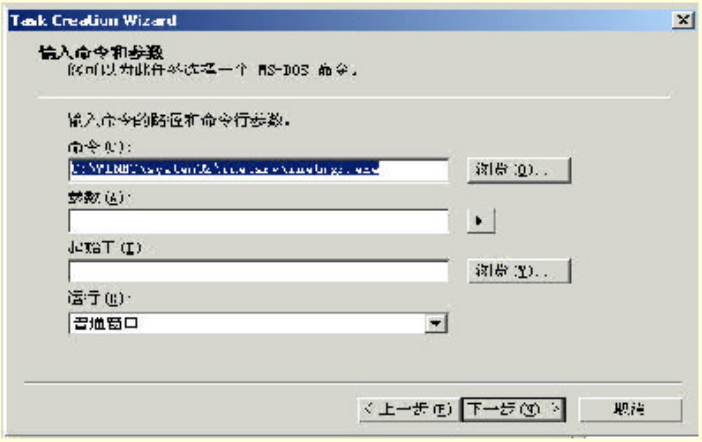


图 12-20　输入 MS-DOS 命令的路径和参数

无论是选择快捷菜单命令还是运行 MS-DOS 命令作为任务，都会为该任务输入描述性信息以及分配一个引人注目的大图标。系统将提供一个选择图标的对话框，选定图标后的控制台如图 12-21 所示。

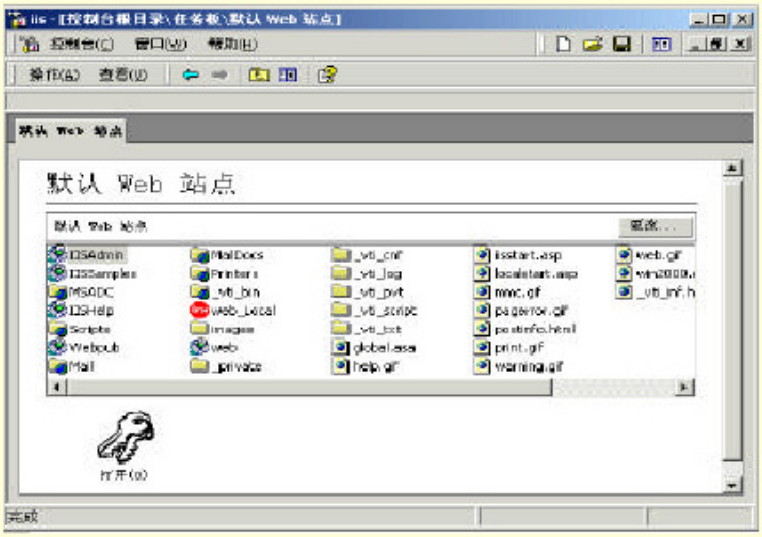


图 12-21　带大图标的管理控制台任务板

选中某个图标之后，在任务板上就可以直接单击图标执行对应的命令。老实说，这个图标虽然很可爱（也许微软觉得大图标更有意思），却并非十分协调。但是无论如何，对需要经常执行某项任务的管理员来说，命令图标使得他们只需要点击图标，就可以直接进入操作，不再需要繁琐地展开各层控制台树。

不止是在 IIS 管理控制台，许多其他单元也可以创建任务板和任务，这个特性大大方便了管理员的操作。

本章详细介绍了管理控制台的基本操作，但需要注意：管理控制台本身不能完成任何的管理工作。要更好地管理 Windows 2000，需要对各个管理工具非常熟悉。本书其他章节有对各种管理单元的详细介绍。前面已经讲过用户和组的管理、权限管理、磁盘管理、用户高级配置和组策略、注册表配置等问题，后面还将对性能监视、Internet 信息服务器（IIS）、证书管理、审核工具等做进一步的介绍。

第 13 章　备 份

当长时间不用计算机时，非常可能发生数据丢失的现象，给用户带来很大的烦恼。备份作业的目的就是有效地恢复丢失的数据。备份作业就是备份数据的简单过程。通常情况下在客户机和服务器上备份数据可以防止磁盘驱动器出现故障、电源断电、感染病毒和其他发生事故时丢失数据。如果发生了数据丢失，但是你已经在仔细计划的基础上进行了定期的备份作业，那么就可以恢复数据，恢复整个硬盘或恢复单个文件。

Windows 2000 提供了非常方便、实用的备份工具，这是一个可以很容易地备份和恢复数据的工具。用户可以使用备份工具手工进行备份或按照计划定期进行备份作业。用户还可以把数据备份到一个文件或备份到磁带上。文件可以存储在硬盘上和可移动磁盘上，还可以存储在可刻录光盘和光学驱动器上。

本章内容包括：

- 备份概述
- 备份和用户权限
- 启动 Windows 2000 备份
- 备份文件和文件夹
- 备份计划
- 还原文件和文件夹
- 备份选项设置
- 系统修复

13.1　备份概述

用户可以利用备份工具完成以下工作：

■ 备份硬盘上选定的文件或文件夹；

■ 将备份的文件和文件夹还原到硬盘或可以访问的任何其他磁盘上；

■ 复制计算机的系统状态，包括注册表、系统文件和启动文件；

■ 制作紧急修复盘，在系统文件被意外删除或被破坏时，它可以快速修复这些文件；

■ 计划定期的备份使备份的数据保持最新。

备份程序支持 5 种备份类型，它们是：

■ 普通备份：复制所有选中的文件，并标志每个备份后的文件为已备份。使用普通备份，只需要最近备份的文件或磁带的副本来还原所有文件。第一次创建备份集时，通常执行普通备份；

■ 每日备份：复制进行备份中的当天修改的所有的被选中的文件，并且已备份的文件不再重新做标记；它可以保存一天的工作而不会影响正常的日常备份工作；

■ 增量备份：只复制被选定的自最近一次正常或增量备份后创建或改变的文件，并且备份后对已备份的文件进行标记。因此，一次普通备份之后的第一次增量备份将复制自普通备份以来改变过的所有文件，第二次增量备份则只复制第一次增量备份以来改变过的所有文件，依此类推；

■ 副本备份：复制所有选中的文件，但不将这些文件标记为已经备份；

■ 差异备份：指上次正常或增量备份后，创建或修改的差异备份副本文件。备份后的文件不标志为已备份文件。

选择一个备份类型一方面要涉及到安全性，另一方面要涉及到时间及介质空间的折中。如果安全性占主要地位，那么可以每小时备份一次，但这会花费大量的时间及备份空间。如果关心的是时间及介质空间的利用，

那么可以一个月或更长的时间备份一次重要文件。

一个比较好的方案是把普通备份和差异备份结合起来使用，具体方法是：

■ 以一个固定的间隔进行普通备份；

■ 在两个普通备份之间以固定的间隔进行一次差异备份。

这种结合的备份方案有一个优点是，容易还原数据，因为备份集通常只存储在少量磁盘和磁带上。但是它又有一个缺点是，备份数据更加耗时，尤其当数据经常更改时。

另一个组合的备份方案是使用普通备份和增量备份来备份数据。因为增量备份只复制被选定的自最近一次正常或增量备份后创建或改变的文件，所以这种备份组合只需要很少的存储空间，并且它的备份方法。但它也有一个缺点就是，这种备份是非常耗时和困难的，因为备份的数据可能存储在多个磁盘或磁带上。

13.2 备份和用户权限

一定要具有特定的权限才能备份特定的文件或文件夹。Windows 2000 提供了一个特殊的成员组，叫做备份操作员组（Backup Operators）。备份操作员是专门进行备份工作的人员。他们可以为了备份或还原文件而替代文件的安全限制。如果使用者是本地组中的管理员或备份操作员，则可以备份本地计算机上本地组适用的所有文件和文件夹。同样地，用户是某个域的管理员或备份操作员，那么可以备份此域中的所有文件。如果是普通用户想要备份文件，那么他必须是这些文件的所有者或者至少应该具有这些文件的如下权限：读取、读取和执行、修改，或完全控制。

另一种备份的限制存在于磁盘配额的选项中。要想备份某一个磁盘上的数据，那么用户在这个磁盘上应该不受磁盘配额的限制否则将无法备份数据。

注意：任何一个用户只能备份本地计算机上的系统状态数据。即使是管理员或远程计算机上的备份操作员，也不能备份远程计算机上的系统状态数据。

13.3 启动 Windows 2000 备份

在运行 Windows 2000 Backup 之前，必须拥有一盒磁带和磁带驱动器，或者至少有一个软盘驱动器和一张软盘，然后就可以打开备份程序了。

具体方法如下：

（1）单击任务栏上的“开始”按钮；

（2）鼠标依次指向下列命令：“程序”→“附件”→“系统工具”→“备份”；

（3）单击“备份”按钮。

此时会打开备份窗口，如图 13-1 所示。

提示：另一种打开备份程序的方法是，在“我的电脑”中选中要求备份的磁盘，单击鼠标右键，打开属性窗口，选择工具选项卡，单击开始备份按钮，同样会打开如图 11-1 所示的备份窗口。

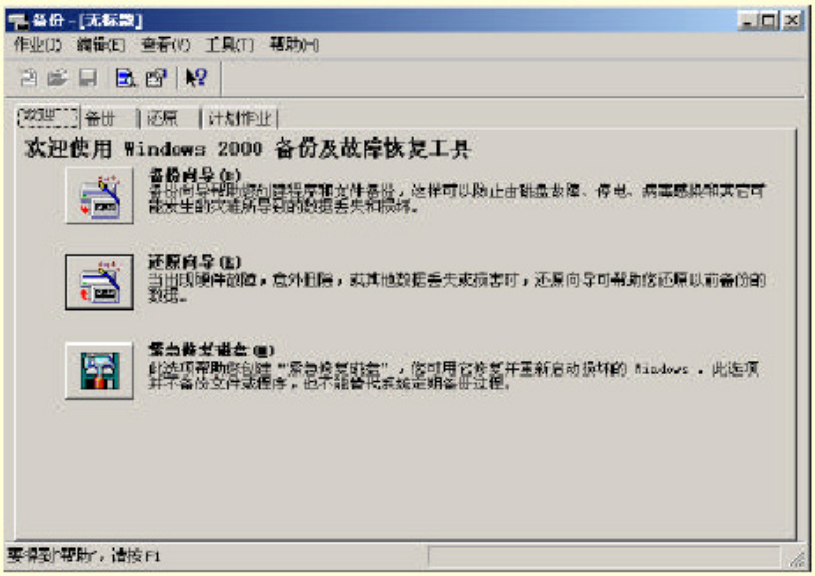


图 13-1　备份窗口

13.4　备份文件和文件夹

“备份”允许将数据备份到文件或磁带上。将数据备份到文件上时，必须指定文件要保存的名称和位置。备份文件的扩展名通常被默认为 .bkf，但是用户仍可以将扩展名更改为本人喜欢的扩展名。备份文件可以保存到硬盘、软盘或任何其他可以保存文件的可移动或不可移动媒体上。

将数据备份到磁带时，计算机必须接有磁带或可移动存储设备。尽管“备份”与“可移动存储”一同工作，但可能须使用“可移动存储”来执行某些维护任务，例如准备和弹出磁带。在备份时，必须指定文件要保存的名称和存储设备的位置。

13.4.1　选择要备份的文件、文件夹和驱动器

在图 13-1 中单击备份选项卡，出现如图 13-2 所示窗口。

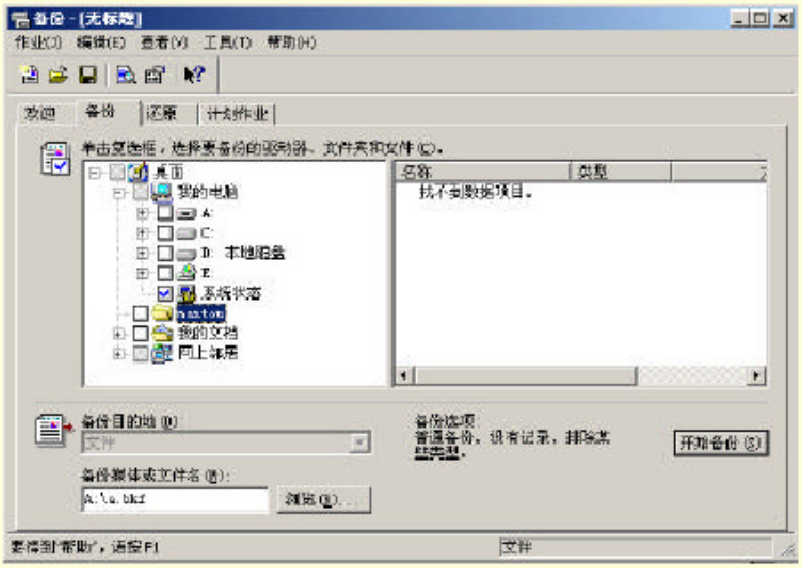


图 13-2　备份选项

此窗口提供了计算机中驱动器、文件和文件夹的目录树视图，可以使用该视图来选择要备份的文件和文件夹。这和使用 Windows 2000 的资源管理器相类似，用呈“　”状的鼠标在要备份的文件或文件夹前的复选框中

单击鼠标左键，这样就选中了这个文件或文件夹。图 13-3 是一个典型的例子。

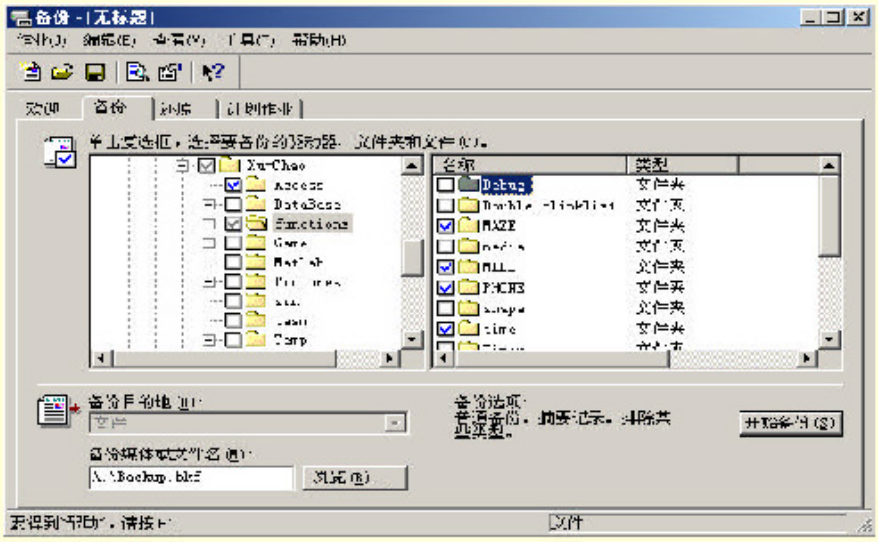


图 13-3 选择文件或文件夹

可以看到被选中的文件夹前的复选框中的“ ”呈蓝色，而灰色的“ ”复选标记意味着只是该文件夹的一部分被选中，如果单击这样的复选框使“ ”标记消失，则此文件夹中原先被选中的部分将不再被选中。

13.4.2 选择文件位置和存储媒体

Windows 2000 提供了两种备份选项。一种可以将数据备份到存储设备上的一个文件中。存储此文件的存储媒体可以是硬盘、软盘、光盘等任何可以保存文件的可移动或不可移动的存储设备。这种选项是始终可以使用的。

另一种选择可以将数据备份到磁带设备上。此选项只有在计算机安装了磁带设备时才能使用。

在图 13-3 中的“备份目的地”下的下拉列表中可以选择备份的目的地为“文件”或“可移动存储”。由于现在没有磁带设备，所以只显示出“文件”选项，而且字体呈灰色的不可选状态。在“备份媒体或文件名”下的文本框中添入备份的文件名和路径。也可以通过“浏览”按钮来选择文件保存路径。如果没有磁带设备，建议使用软盘来备份比较小的文件。因为如果备份在本地硬盘上，而硬盘又发生了故障，导致备份的文件丢失，那么以后就无法还原文件了。

13.4.3 设置备份选项

在做完上述的工作后，就可以单击“开始备份”按钮，启动备份程序。但这时的备份选项是备份程序默认的值。如果想更改这些值，则要重新设置备份选项。

打开选项对话框的具体方法是：单击“工具”菜单下的“选项”命令，弹出选项对话框，如图 13-4 所示。

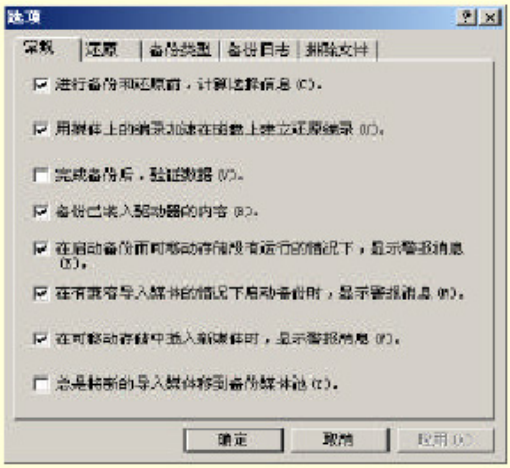


图 13-4 选项对话框

在常规选项卡中，用户可以进行一些设置，比如“完成备份后，验证数据”等。

选择“备份类型”选项卡时，可以选择 5 种备份类型中的任意一种，如图 13-5 所示。

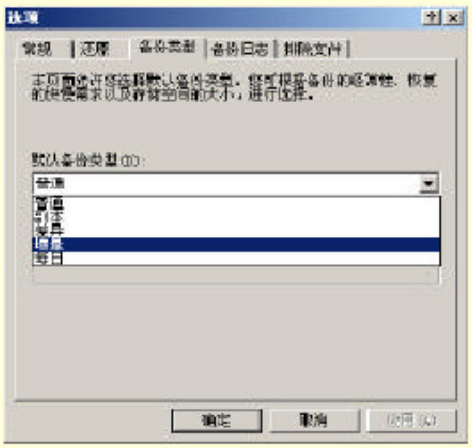


图 13-5　选择备份类型

选择“备份日志”选项卡时，有 3 种选择，选择其中一种，如图 13-6 所示。然后单击“确定”按钮。

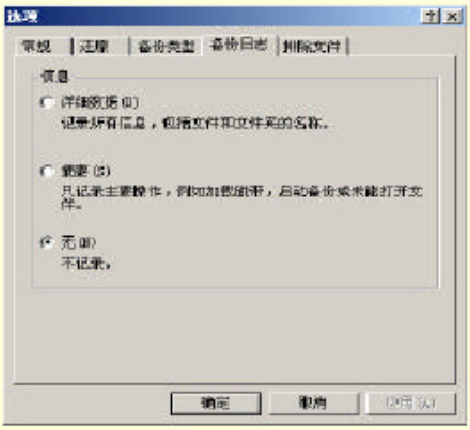


图 13-6　选择备份日志信息

在以后的小节中将详细地介绍各种备份选项的含义，这里我们使用默认的备份设置，以使初学者更容易掌握。

13.4.4　开始备份

做完上述工作后就可以开始备份了。单击备份窗口中的“开始备份”按钮，备份程序开始工作，并弹出“备份作业信息”对话框，如图 13-7 所示。其中用户可以在“如果媒体已经包含备份”下的两个只选框选择是直接将备份附加在媒体上还是覆盖已有的备份。如果选择“用备份替换媒体上的数据”选项，则处在对话框底部的选项被激活，选择它使备份的数据只有所有者和管理员才能访问。

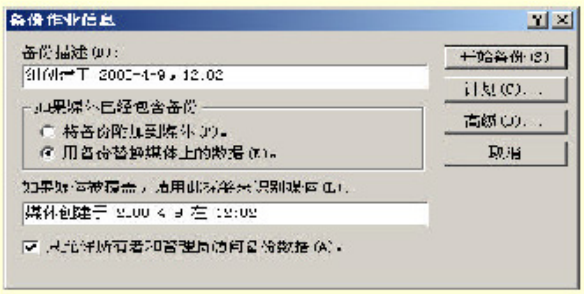


图 13-7　备份作业信息

如果用户在前面没有进行备份选项设置，那也不必着急，此时备份程序允许用户再重新设置这些属性。单击右边一列按钮中的“高级（D）…”，弹出高级备份选项窗口，其中可以进行一些基本的选项设置（如图 13-8 所示）。设置完后单击“确定”按钮。

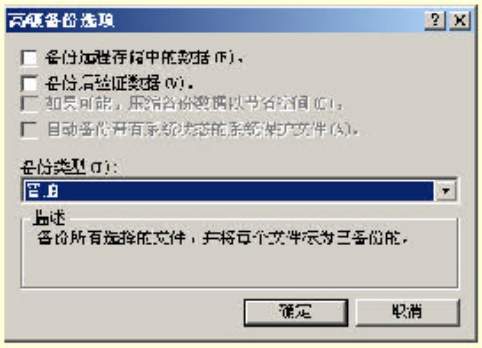


图 13-8　高级备份选项

这时可以单击图 13-7 中的“开始备份”按钮。从开始备份到备份结束，“备份进度”窗口会一直提示用户备份进行的情况。从中用户可以了解到诸如媒体名、备份状态、备份时间等信息，如图 13-9 所示。

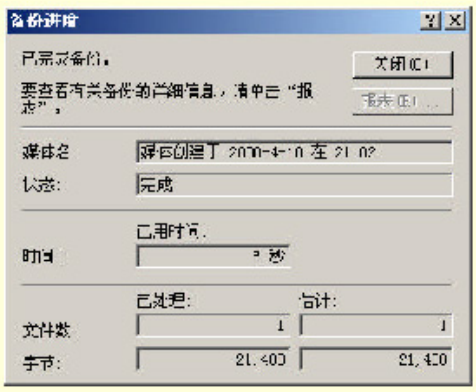


图 13-9　备份进度

单击“关闭”按钮，完成备份操作。这时从“资源管理器”中可以看到备份在软盘上的备份文件。它显示在其中的图标与其他文件的不同。

如果备份的是非常重要的数据，建议将备份后的软盘或磁带贴好标签并放在一个防磁、防潮的安全的地方，这对保护数据是非常有利的。

13.4.5　备份系统状态数据

对于 Windows 2000 Professional，系统状态数据只包括注册表、COM+类注册数据库和引导文件。对于 Windows 2000 Server 操作系统，系统状态数据包括注册表、COM+类注册数据库、系统引导文件和证书服务数据库。如果服务器是域控制器，Active Directory 和 SYSVOL 目录也包含在系统状态数据中。如果服务器运行群集服务，那么系统状态数据也将包括所有资源注册表检查点和仲裁资源恢复日志，该日志含有最新的群集数据库信息。

要备份系统状态数据，只要用“　”标记在如图 13-2 中“系统状态”前的复选框中即可。可以看到系统状态这一项是不可再分的，也就是说如果要备份系统状态数据，就必须将上面讲到的各种类型的系统数据全部备份，而不能选择备份或还原系统状态数据的单独组件。这是由于系统状态组件间的依存关系决定的。选定“系统状态”后，单击“开始备份”按钮，按照前面讲的方法一步步进行下去即可。

13.5　备份计划

备份程序还为用户提供了创建将来的、每日的、每天的、启动时的等情况下的备份计划的可能。这大大地方便了用户，使用户不必费心地时刻想着去备份重要数据，而由操作系统自动完成。

计划备份的具体方法是：

（1）在图 13-1 中选择“计划作业”选项卡，如图 13-10 所示。

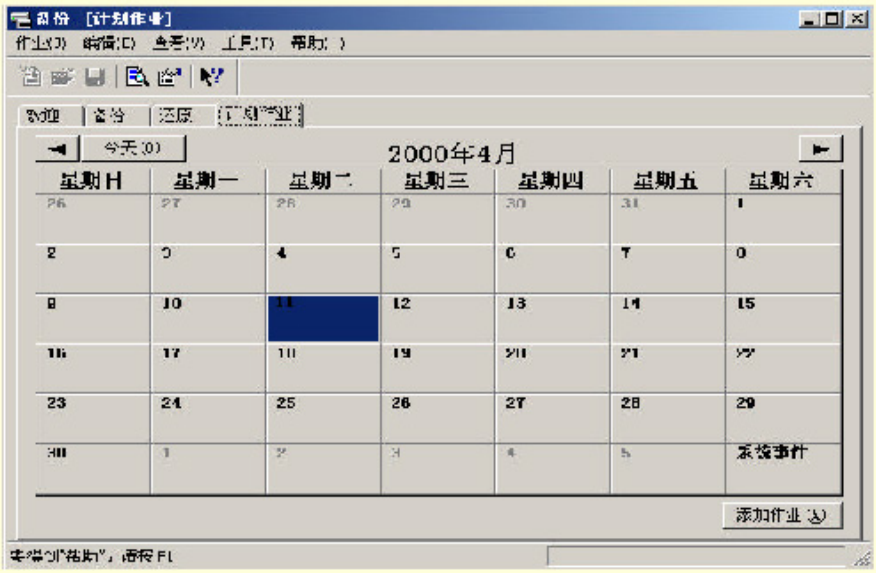


图 13-10　添加作业

（2）选择要执行备份的日期，单击“添加作业”按钮。

（3）这时启动了“备份向导”，按照每步的提示选择设置选项（这些和以前提到过的是一样的），单击“下一步”按钮。

（4）在出现如图 13-11 所示的窗口时，单击“设定备份计划”按钮，出现如图 13-12 所示的窗口。

（5）按窗口中的各项提示选择备份计划方式，其中可以设置备份周期、备份开始时间、备份持续时间等，单击“确定”按钮。

（6）在“设置账户信息”对话框中，输入要在其下运行的计划备份的用户名和密码。

（7）依次单击“确定”→“下一步”→“完成”按钮。

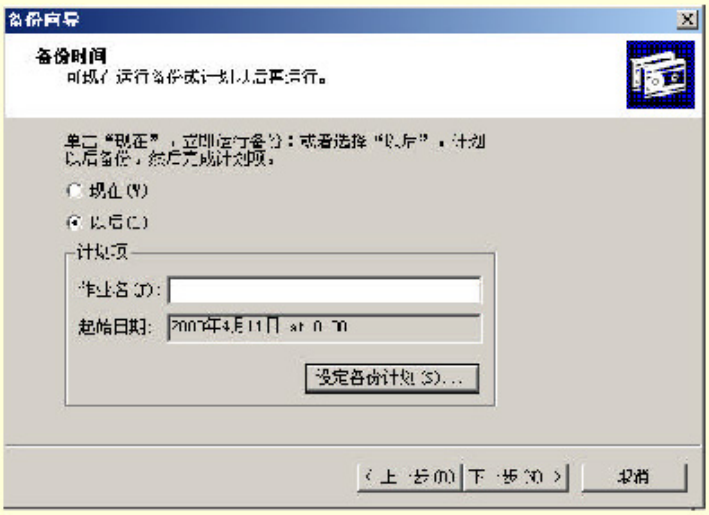


图 13-11　备份向导

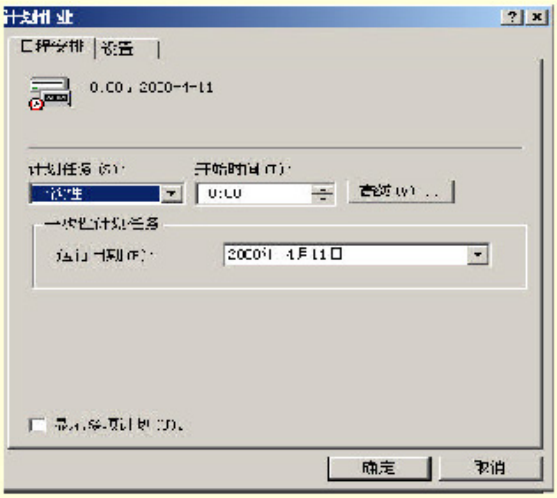


图 13-12 计划作业

13.6 还原文件和文件夹

一旦有重要的数据丢失或被破坏，但如果它们被做了备份，那就需要将备份还原成原来的文件或文件夹。

13.6.1 选择要还原的文件和文件夹

在图 13-1 中选择“还原”选项卡，出现如图 13-13 所示的窗口。备份为用户提供了已备份文件或文件夹的树状视图，通过展开左边的文件目录树，可以选择还原的文件或文件夹；或双击左边的备份项目，也可以选择要还原的文件或文件夹，如图 13-13 所示。这和选择备份的文件或文件夹的方法是类似的。

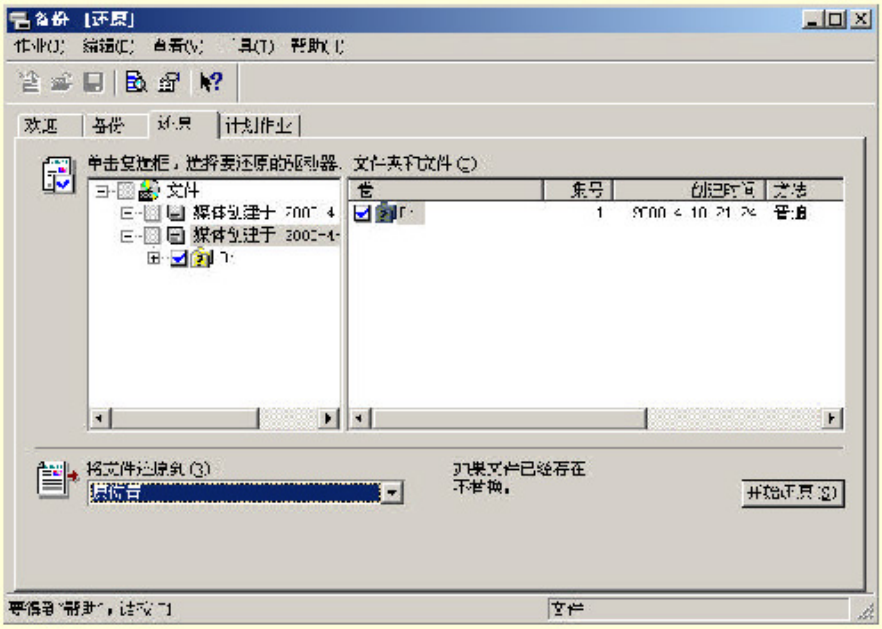


图 13-13 还原窗口

13.6.2 选择备份文件或文件夹要还原的位置

备份允许被还原的文件或文件夹，选择 3 种目的地中的一个，它们是：

■ 将备份的数据还原到原来的文件或文件夹的位置，此种方法适用于此文件或文件夹丢失的情况。

■ 将备份的数据还原到替换此文件或文件夹的位置上。备份后的文件或文件夹被存在用户给定的备份文件夹中，并且备份的文件或文件夹的结构将保留在此文件夹中。也就是说原来的文件或文件夹的完整路径会被保存在此备份目录中。此种方法适用于用户需要使用一些旧文件而又不想用它们替换现有文件的情况。

■ 将备份的数据还原到单个文件中。备份后的文件或文件夹被存在用户给定的备份 文件夹中，但备份的文件或文件夹的结构将不被保留在此文件夹中，而只保留这一文件或文件夹，它以上的目录级别将不被保留。

图 13-13 所示左下方向的下拉列表框中的原位置、替换位置、单个文件夹依次对应上面的 3 种情况。用户可以根据实际情况选择 3 种中的一种。如果选择了替换位置和单个文件夹，则需要在“备用位置”下键入文件夹的路径，或者单击“浏览”按钮寻找文件夹。

13.6.3　设置还原选项

备份程序提供了还原选项设置。单击“工具”菜单下的“选项”命令，系统会弹出“还原选项”对话框，如图 13-14 所示。

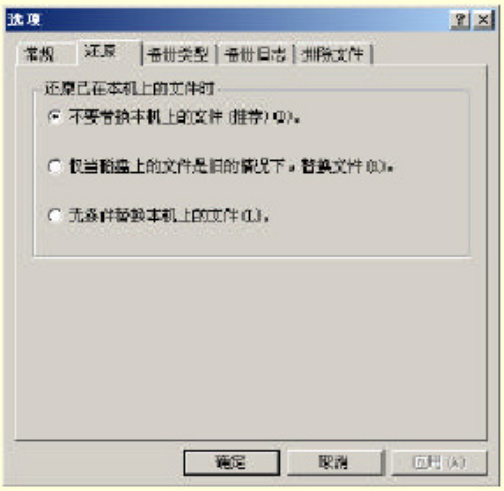


图 13-14　还原选项

在此处可以选择文件和文件夹的还原方式。必须在 3 个选项中选择一个：

■ 不要替换本机上的文件：此种方法不允许还原的文件替换硬盘上的现有文件。这是最安全的还原方法；

■ 仅当磁盘上的文件是旧的情况下，替换文件：此种方法可以保证还原的文件是最新的，所做的任何修改都不会丢失；

■ 无条件替换本机上的文件：此种方法将备份集中的所有文件替换硬盘上相应的文件，如果自从上次备份数据以来做了任何更改，该选项将删除这些更改。

Windows 2000 建议用户使用第一种方法，因为它是最安全的，虽然这会多使用一些磁盘空间。

注意：如果正在操作的文件包含在备份中，选择无条件替换本机上的文件可能导致数据丢失。

13.6.4　开始还原

设置完还原选项后，就可以单击“开始还原”按钮并启动还原程序。在还原过程中，“还原进度”窗口始终出现，并时刻显示还原的状态。还原结束后，“还原进度”窗口如图 13-15 所示。如果需要查看详细的还原信息，单击“报表”按钮，系统会列出详细的资料。

提示：如果选择了替换位置或单个文件夹作为被还原文件或文件夹的位置，则还原后的文件或文件夹仍然具有原来的安全属性。只有具有一定权限的用户才能访问。

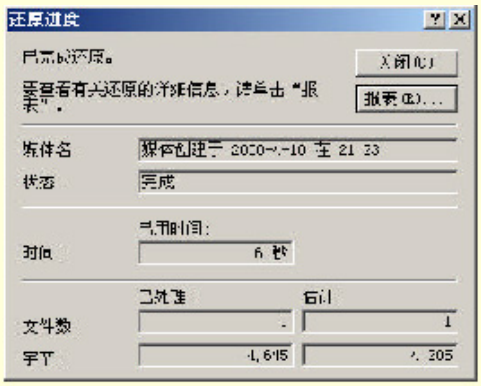


图 13-15 还原进度

单击“关闭”按钮，以完成还原操作。

提示：如果选择了替换位置或单个文件夹作为被还原文件或文件夹的位置，则还原后的文件或文件夹仍然具有原来的安全属性。只有具有一定权限的用户才能访问。

13.6.5 还原系统状态数据

如果在还原以前备份了系统状态数据，则在图 13-13 中会列出“系统状态”这一项，用“ ”标记单击“系统状态”旁的复选框，这将还原系统状态数据和当前还原操作选定的其他数据。类似于前面还原文件或文件夹的方法，选定备用位置，设置还原选项，然后单击“开始还原”按钮。

如果还原系统状态数据前，有为还原数据指定备用位置，备份将清除当前计算机上的系统状态数据并用还原的数据替换它。如果指定了系统状态数据的备用位置，那么只有注册表文件、SYSVOL 目录文件、群集数据库信息文件和系统引导文件被还原到备用位置。而不还原 Active Directory 目录服务数据库、证书服务数据库和 COM+类注册数据库。

13.7 备份选项设置

由于备份选项设置的选项比较复杂，所以这里单列出一个小节进行详细讲解。

13.7.1 常规选项

如图 13-4 打开选项对话框，在“常规”选项卡中看到有许多复选项，它们的含义如下：

■ “进行备份和还原前，计算选择信息”：在备份和还原前，系统自动计算将要备份和还原的文件或文件夹的文件数和字节数。

■ “用媒体上的编录加速在磁盘上建立还原编录”：备份将会扫描整个备份集（或用户的全部数据），然后创建磁盘上目录。

■ “完成备份后，验证数据”：在备份完成后，系统自动检查硬盘上的源数据和备份的数据是否相同。如果不同，则说明备份的媒体有问题，应该重新进行备份。

■ “备份已装入驱动器的内容”：备份已装入驱动器上的数据。如果选择该选项而备份已装入驱动器，则将备份该驱动器上的数据。如果不选择该选项而备份已装入驱动器，则将只备份该驱动器的路径信息。

■ “在启动备份而可移动存储没有运行的情况下，显示警报消息”：在备份前检查可移动存储器的情况，如果设备没有就绪，则系统会弹出警告对话框。此选项非常适合于使用磁带或其它可移动存储设备作为存储媒体的情况。

■ “在有兼容导入媒体的情况下启动备份时，显示警报消息”：在启动备份时，如果发现另外有兼容的媒体在媒体池中，系统将给出提示信息，要求用户选择其中的备份媒体。

■ “在可移动存储中插入新媒体时，显示警报消息”：有时用户会插入新的存储媒体，当运行备份时，备份程序检测到这个新的媒体，并显示一个对话框，要求用户选择其中的备份媒体。

■ “总是将新的导入媒体移到备份媒体池”：选择此选项，可以自动将新的媒体移动到媒体池中，以便对所有媒体进行统一管理。

13.7.2　为用户排除备份文件类型

在图 13-4 中单击“排除文件”选项卡，可以为所有用户排除备份文件类型，也可以为单个用户排除备份文件类型，如图 13-16 所示。

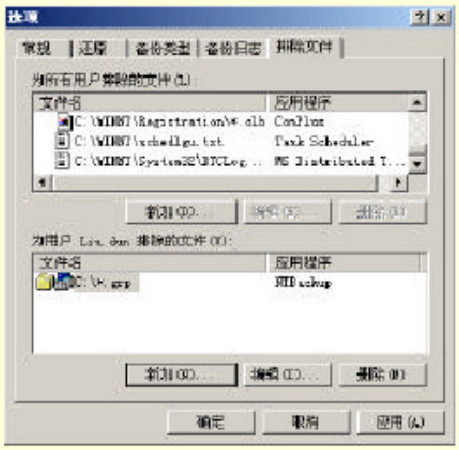


图 13-16　排除文件选项

指定了排除的文件限制在指定路径（文件夹）后，则该路径下的所有子文件夹中的文件都将受到限制，除非用户清除了“应用于所有子文件夹”复选框。

如果想要为所有用户排除备份文件类型，则在“为所有用户排除的文件”列表下单击“添加”按钮。系统会弹出“添加排除的文件”窗口（如图 13-17 所示），在“已注册的文件类型”列表下单击要排除的文件类型，然后在“应用于路径”下的文本框中添入路径；如果想要排除自定义的文件类型，则需要在“自定义文件掩码”中添入如下形式的扩展名：输入小数点，然后加上一个有两个或 3 个字母的文件扩展名。如果要将排除文件类型应用于“应用路径”下的所有子文件夹，则选择最下面“应用于所有子文件夹”前面的复选框。单击确定，完成排除文件类型的任务。这时可以看到在“为所有用户排除的文件”列表中添加了新的文件类型。如果要修改已选的文件类型，需要在列表下选定要修改的类型，然后单击编辑按钮，在“添加排除的文件”窗口重新选定类型即可。

如果要为单个用户选定排除的类型，需要以此用户的身份登陆 Windows 2000，然后按照为所有用户选择排除文件类型的方法操作即可。

图 13-17　添加排除的文件

13.8 系统修复

Windows 2000 有几种实用的方法用于修复不能启动或不能加载 Windows 2000 的系统。如果某些系统文件崩溃或者意外删除，或者如果安装了导致系统不能正常工作的软件或者设备驱动程序，那么可以使用这些修复方法。

13.8.1 概述

主要有 3 种方法来修复系统：安全模式、系统故障恢复控制台、紧急修复。其中安全模式允许用最少的驱动程序和服务来启动系统，从而可以删除那些影响系统启动的应用程序，达到修复系统的目的。故障恢复控制台向用户提供命令行接口，该接口允许用有限的命令行命令集修复系统。它可以通过软盘或 Windows 2000 CD-ROM 复制一个文件到硬盘来修复系统，或者对一个阻止计算机正常启动的服务进行重新配置，以达到修复系统的目的。对于一般的故障修复，紧急修复是一个比较好的方法。

13.8.2 创建紧急修复盘

紧急修复盘（ERD）能够帮助用户解决系统的文件问题、启动环境问题，和在引导卷上的分区引导扇区问题。在使用“紧急修复盘”特性之前，必须创建紧急修复磁盘。可以用“备份”实用程序创建紧急修复磁盘。具体方法是：

（1）单击任务栏上的“开始”按钮；
（2）鼠标依次指向下列命令：“程序”→“附件”→“系统工具”→“备份”；
（3）单击“备份”，打开如图 13-1 所示的“备份”窗口；
（4）单击“工具”菜单下的“创建一张紧急修复软盘”命令。

此时系统会弹出一个提示窗口，如图 13-18 所示。按提示在软盘驱动器中插入一张软盘，如果要将注册表也备份到修复目录中，则选择窗口中的唯一复选框。

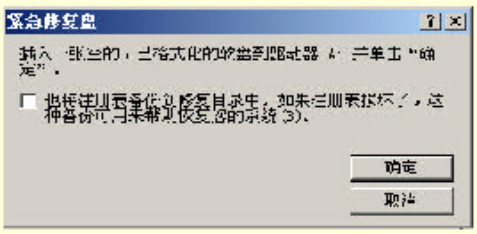


图 13-18 创建紧急修复盘提示

单击“确定”按钮，系统开始创建紧急修复盘。创建紧急修复盘的过程取决于 winnt\repair 目录下的文件，所以此目录一定要仔细保管，不要随意修改。备份到软盘上的文件包括：autoexec.nt、setup、config.nt3 个文件。

13.8.3 使用紧急修复

要修复系统，需要有一张 Windows 2000 的安装 CD 和一张紧急修复盘。修复过程如下：

（1）从 Windows 2000 安装 CD 启动计算机；
（2）在安装过程中，按照提示选择修复选项；
（3）选择修复类型；
（4）开始修复操作，此时需要紧急修复盘。

在本章的最后，还需要提到的一点就是，前面所讲的备份和还原的方法是基于手工操作的，即每一个操作执行都要由用户自己去做。另一个比较好的方法是利用备份工具提供的备份、还原、备份计划向导。只要启动向导，用户唯一要做的就是选择各种各样的属性设置，而工作步骤则完全由系统完成。这为用户省下了大量的时间，是值得推荐的方法。但是它和前面讲到的方法的原理是一样的，所以这里就不再赘述了，希望读者能够举一反三，这样才能够取得更大的进步。

第 14 章　性能监视

性能几乎是每一个计算机用户最关心的问题之一。除非有足够的资金，总可以保证有最快的芯，最快的内存，以及最大的硬盘，但并不是所有的人都有这样好的运气，对于大多数普通用户，希望自己有限的配置能有最好的性能；对于公司、企业的网络管理员，这也是一个相当有挑战性的问题。

那么，怎样了解计算机的性能呢？许多人凭直觉推测。当应用程序执行太慢，游戏画面出现停顿，或者硬盘总像老牛拉破车似的怪叫，人们就会说：哦，又该换新产品了。直觉的确是很好的老师，但其实还有一样更专业、更科学的工具，那就是微软提供的性能监视器。许多人知道有这个东西，但是往往被复杂的图表弄得眼花缭乱。也许它的确没有 Word 或者 Excel 那么简单明了，但如果读者已经熟悉了权限管理，对注册表也有相当程度的认识，就完全没有必要对性能监视器有敬畏之心。另一方面，它丰富漂亮的界面常常引人入胜，还是个相当好玩的东西呢！下面我们就来了解一下有关性能监视的一些知识。

14.1　了解性能监视器

14.1.1　新的性能监视器版本

性能监视器并不是一个新东西，在 Windows NT 4.0 中，微软就在管理工具里添加了 Performance Monitor(性能监视器)这个工具。许多人认为它的界面不够友好。Windows 2000 中使用的是功能有所增强的版本：性能监视器和性能日志和警报两个相互关联的工具，但是在其 Beta 版本仍保留了旧的 Performance Monitor。

在 Windows 2000 的 Beta 版本之中用户在管理工具已经找不到旧的版本，但仍然可以在开始菜单的“运行”命令中启动它。

在运行命令的“打开”提示符下，输入 Perfmon 并回车，将出现如图 14-1 所示的提示对话框。毫无疑问，微软希望人们更多地使用他们的新版本的性能监视器。

图 14-1　Perfmon 说明

不妨按“取消”键，看看旧的性能监视器版本，如图 14-2 所示。

的确，这不是一个很友好的界面，初次接触它的用户可能会被一片空白所镇住，不知道他们可以做点什么，底下一排排的新名词也十分费解。总之，它不容易上手。

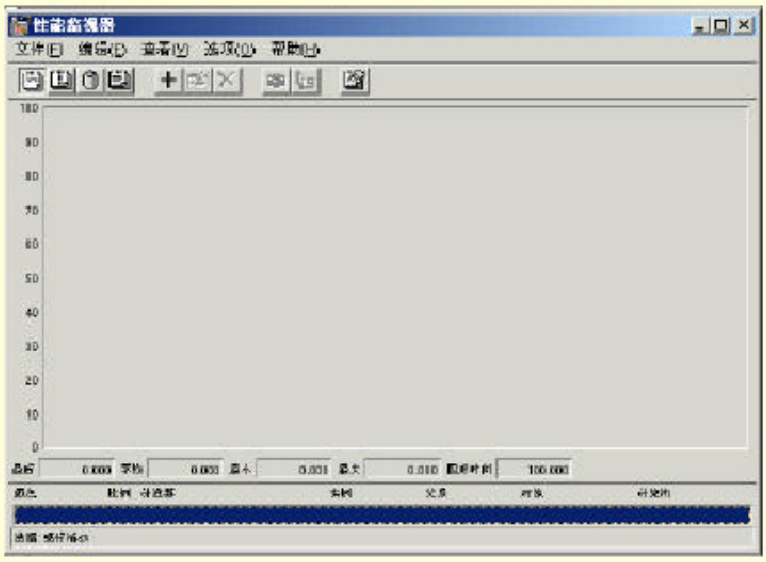


图 14-2 旧的性能监视器

注意：正式发布的 Windows 2000 中已经不再包括旧的版本，新的性能监视器可以在控制面板下管理工具中找到，它的新名叫做性能。此外，如果用的仍然是 Windows 2000 的 Beta 版本，并且已经熟悉了在 NT 4.0 中按 perfmon 键打开性能监视器的用户也可以在如图 14-1 的提示说明框中，选择“确定”，就可以打开新的版本。如图 14-3 所示。

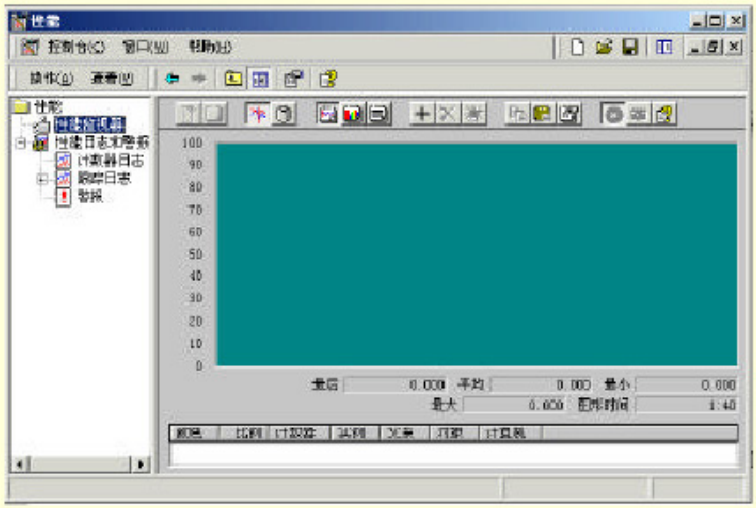


图 14-3 新的性能监视器版本

读者以为如何呢？的确，新的版本要比原来的要更“色彩斑斓”，显得更漂亮些，但总的说来，它也并非能够一目了然，而且原来版本的一些功能被移植到了性能日志和警报下面去。老用户可能会发现在新的“性能监视器”中无论如何找不到警报视图，或者即使在性能日志和警报单元下发现了，也不知如何使用。因此，老的用户必须得重新认识性能监视器的使用，一旦熟悉后，也许他们会马上喜欢新的版本，毕竟它的界面更漂亮；而新的用户也会发现这是个相当有用的工具。

14.1.2 了解监视术语

可以这样理解：性能监视器使用计数器来描绘系统中各个对象的行为状态，从而了解系统的性能。这里有 3 个术语需要用户了解，那就是对象（Objects）、计数器（Counters）和实例（Instances）。

前面已经多次提到资源对象，那里的对象指的是文件、文件夹、打印机等系统资源，这里的对象有所不同，它包括处理器（Processor）、内存(Memory)、磁盘(Disk)、系统(System)、服务器(Server)、高速缓存(Cache)等等，它们系统地体现了计算机的性能情况。

提示：不同的计算机上的对象可能会略有差别，这要取决于系统安装的情况，比如和网络有关的对象就有 IIS 服务器、FTP 服务器、NWLink IPX、Browser 等等，如果发现有的对象没有，可能需要重新安装。

如果使用过面向对象的遍程语言，比如 C++等，就很容易理解对象的属性是怎么一回事。计数器的作用是从对象的不同属性来描述对象，因此当一个对象有多个属性时，它就会有许多个计数器。打个比方，对于人这样一个对象，就可以从身高，体重，年龄，性别等不同的角度来描述，相应地就有不同的计数器；而汽车是不同于人的对象，描述它的计数器也就和人的计数器不一样。

了解了对象，就很容易理解实例。一个对象可能有多个实例，这就好像汽车还有许多辆一样，每一辆就是汽车这个对象的一个实例。实例可以用编号来区别，比如 0 号、1 号等等，也可以给它们起名。尽管有区别，但它们却可以用相同的参数来描述和比较使用情况，因此不同实例用同一套计数器来观察。比如计算机中可能会有多处理器，这时候每个处理器是处理器对象的一个实例。

14.2　性能监视器的视图

在旧的监视器版本中，有 4 种视图，它们分别是：图表、日志（Log）、报告（Report）、和警告（Alert）。可以在工具栏中非常方便地进行切换。而在新版本的性能监视器中，把图表分为图表（线型）和直方图两类，此外还有报告视图，而把警告和计数器日志、追踪日志放在了一起，归于性能日志和警告统一管理。

使用多种视图，使用户能够从不同角度查看系统性能，同时有利于及时发现系统瓶颈，从而使监视更加有效。下面就分别来说明这几种界面。

14.2.1　图表

图表是打开性能监视器后缺省的视图，这种视图是线型图的表示方法，如图 14-4 所示。

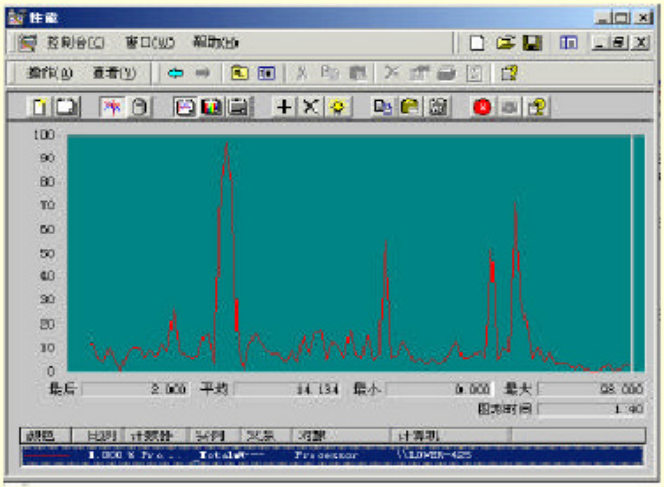


图 14-4　线型图表

14.2.2　直方图

直方图如下图 14-5 所示。

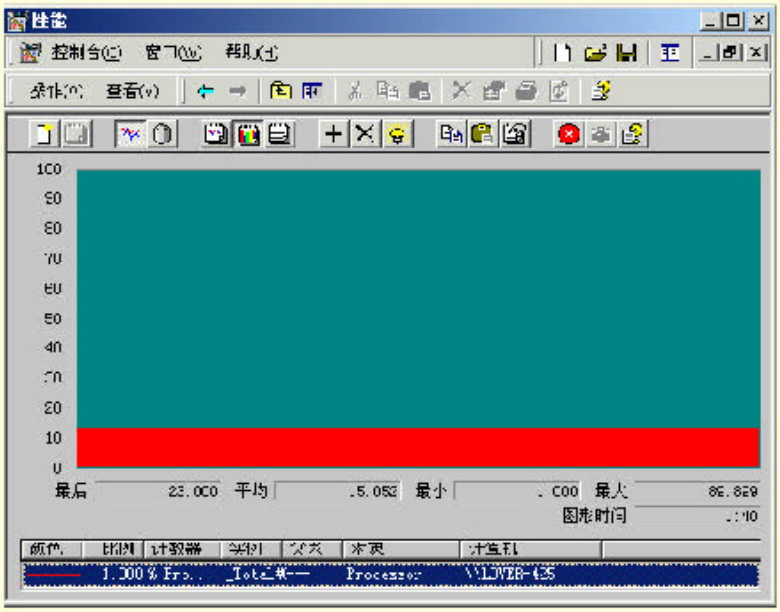


图 14-5 条形图表

这两个图表都屏蔽了控制台树，这样读者可以专心查看图表。其实这两种视图在旧的版本中同属于图表范围内，而在新的版本中，将它们区分开来。在如图 14-4 或者图 14-5 中，上方有一个工具栏，可以在线型图和条形图间来回切换。其中，图表（线型）的图标上有曲线，而直方图的图标上是柱形的，很容易区别。

显然前者线型图更有利于一段时间内显示性能数据，而条形图有利于显示性能的峰值，当峰值到来时，一片鲜红十分的触目惊心。但是条形图不利于观察数据的连续变化，这在相当程度上损失了图表视图的优越性，因此一般来说，人们会更喜欢用线型图。

可以更改图表或者直方图的显示属性（二者的更改方法是一样的），比如颜色、字体、坐标轴等，以更方便地查看数据。在图表区中，单击鼠标右键，在弹出的快捷菜单中，选择“ 属性 ”命令，出现系统监视器属性对话框，如图 14-6 所示。

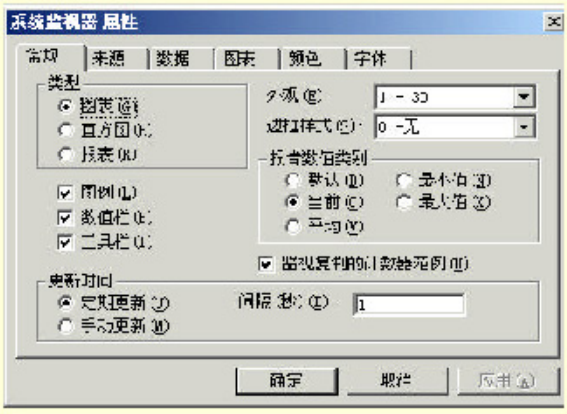


图 14-6 系统监视器属性

可以作的设置如下：

·常规选项卡：选择查看的类型，更新时间和类型（定期更新或者手动更新），外观（3D 或者平面），以及边框样式等。

·来源选形卡：选择查看当前选定的活动或者日志文件。

·数据选项卡：可以在里添加计数器（后面还将详述），选择曲线的颜色（我选择的是红色），线宽，线型（实线、虚线、点划线等）以及显示的比例。如果曲线显示与区域不成比例，比如太过压缩在底部或者许多超出了边界，就可以调整显示的比例。

·图表选项卡：在这里给图和 Y 轴添加标签，为图增加横线与纵线网格以增强图的可读性，以及显示的最大值和最小值（缺省是从 0～100）。

·颜色选项卡：调整背景和系统颜色。

·字体选项卡：选择显示的字体。

如图 14-7 中，给图表加了横纵网格，同时调整了背景颜色，并且将显示值的范围缩减为 0～50，使图表尽可能地充满整个界面，从而更加清晰明了。读者也可以自由地调整显示的界面，以求最佳的组合。

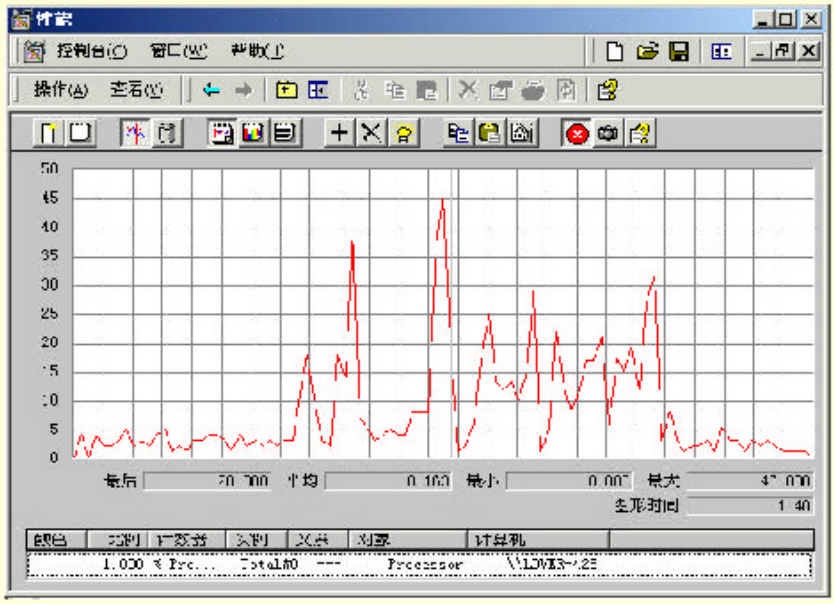


图 14-7　调整后的图表显示

图表和直方图是使用的最多的视图，大多数人都喜欢这种生动的观察方式，因此性能监视器在工具栏里还提供了许多工具帮助人们更好地使用图表。

如图 14-8 所示是上方的工具栏。从左到右依此是：

图 14-8　工具栏

·新计数器集：选择新的计数器集。

·清除显示：清除当前所有显示，重新记录数据。

·显示当前活动：使选中的计数器活动。

·查看日志文件数据：选择存放在磁盘的日志文件导出到性能监视器中。

·表格显示：选择图表视图。

·直方图显示：选择直方图视图。

·报表显示：选择报表视图。

·添加：添加新的计数器。

·删除：如果显示有多个计数器，则删除当前的计数器。当前计数器可以由底部状态栏加亮的一栏看出来。

·加亮：加亮当前计数器的图表曲线。注意加亮只对图表的视图有效，对于直方图视图无效。

·属性：显示如图 14-6 所示的属性对话框，可以改变计数器的属性设置，详见前面的设置。

·冻结显示：冻结当前的观测。再次按下这个按钮，将恢复显示新的数据。

·更新数据：如果选择的是手动更新，则平时图表相当于冻结状态。只有按下它才能更新显示；如果选择的是定期更新，则这个按钮是灰色的。

14.2.3　报表

用户也可以选择通过报表显示的格式查看数据。

在工具栏中，报表的图标与图表、直方图的图标紧挨在一起。报表的缺点是只能显示计数器最近的值（并

不断变化），而不能显示一段时间的数据。从图形界面来说，报表显然没有图表更直观，也更能显示变化趋势和总体情况。那么为什么还要用报表来查看数据呢？请读者先来看看如图 14-9 所示的图表曲线。图中同时有多个计数器在工作，所以各条曲线互相交错，界面显得十分复杂，数据的追踪有一定困难。

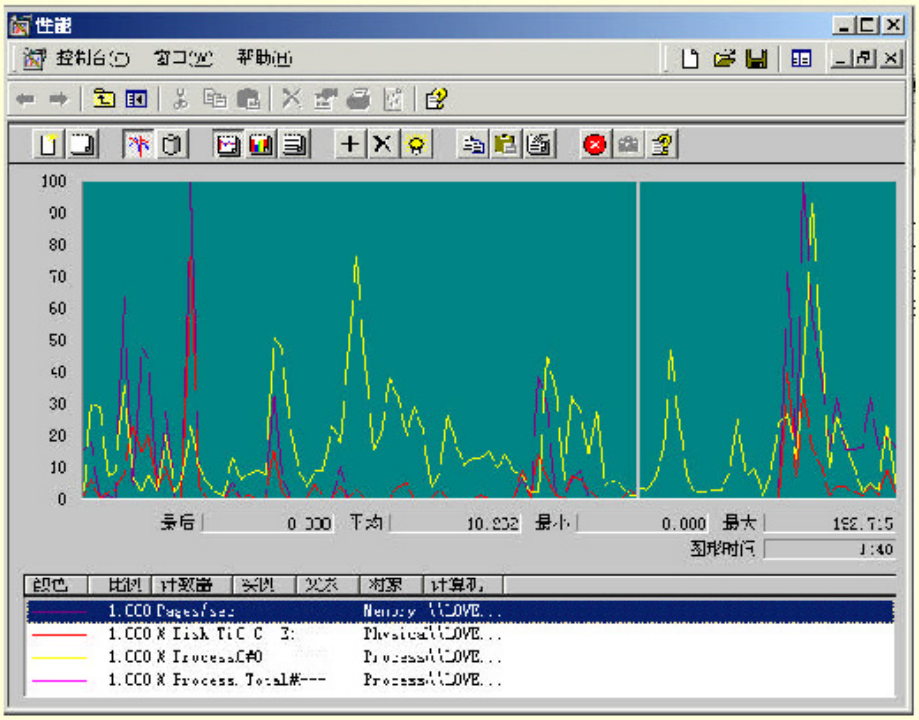


图 14-9　多条曲线

这时采用报表视图是个好主意，如图 14-10 所示，在多个计数器同时工作时，报表有它自己的优点，它的视图显得干净简洁，易于观察，在另一个角度揭示了性能。当然，如果只有一个计数器，那么查看报表显然是不理想的，只有一个孤零零的数据，很没有说服力。但在很多情况下，可能需要同时观察几个计数器，以图比较或者发现性能瓶颈，这时正如图 14-9 所示，图表视图中将充满了各种颜色的曲线。报表提供了另一种视图，用户可以结合进行比较。

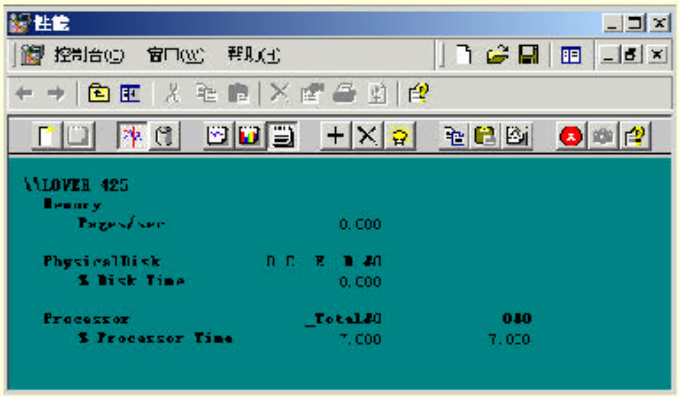


图 14-10　报表形式

14.2.4　日志和警告视图

同 Windows NT 4.0 不同，警告视图的按钮不再和图表、报表的按钮在同一个工具栏中出现，需要查看和设置日志或者警报，打开性能监视器下的性能监视和警报管理单元，将看到有计数器日志、跟踪日志和警报 3 个工具。

使用计数器日志，可以记录硬件的使用情况以及本地或者远程系统服务的活动情况。可以人工地进行日志，也可以由用户自定义任务列表，由系统自动记录，此外还可以设置日志文件的大小以限制日志的膨胀。日志记

载的数据可以使用性能监视器来观察演示，或者由别的程序或者数据库执行分析和打印报表。

跟踪日志可以追踪特定的活动，比如磁盘 I/O 或者是页面错误，当这些事件发生时，数据将被传送到日志服务中进行记载。

使用过 Windows NT 4.0 的用户不会对警告陌生，在 Windows NT 4.0 中，可以为计数器设置警告，当计数器记录的数据超过、等于或者小于预设的值，出现警告。警告的形式可以有多种，可以选择将值记录到应用程序事件日志、发送网络消息或者执行某个应用程序，如图 14-11 所示是日志和警报视图。

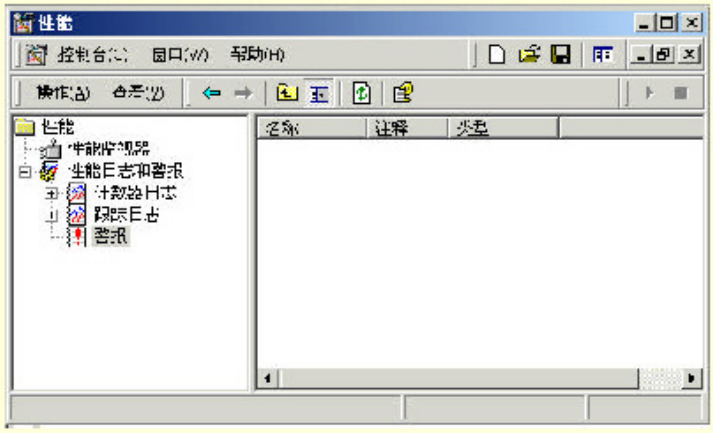


图 14-11　日志和警报视图

14.3　监视器中的计数器

14.3.1　添加计数器

缺省打开性能监视器时是一片空白的，为了使性能监视器工作，首要条件是为监视器添加计数器。计数器的概念前面已经讲述过了，具体为性能监视器添加计数器的方法是：

（1）启动性能监视器，在如图 14-3 中，单击有一个加号的按钮，出现如图 14-12 的对话框。

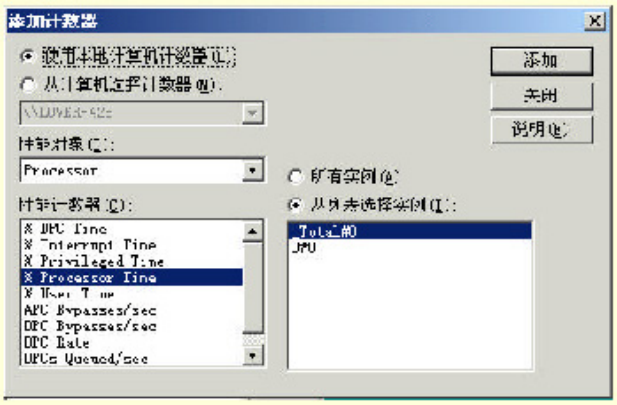


图 14-12　添加计数器

（2）选择使用本地计算机或者从网络中选定计算机。

（3）选择查看的性能对象。单击“性能对象”列表，出现可供选择的所有对象。正如前面所说，每个对象都有自己的性能计数器。

（4）选择对象的性能计数器。如果对对象和计数器代表的意义不清楚，可以单击“说明”按钮，这时候系统会出现介绍说明。

（5）选择计数器的实例。

（6）重复 1～5 各步骤工作，使监视器同时监测多个计数器。如果不再添加，单击“完成”按钮，开始监

测。需要注意的是：过多的性能曲线可能适得其反，使用户无法准确及时地获取信息。

14.3.2 Processor 对象

初次使用性能监视器时，最感到头疼的莫过于一长串的对象和计数器，大多数人可能会对着纷繁的曲线不知所措。的确，必须经过认真的学习和使用，才能真正了解这些看似明白，却往往一知半解的名词。而在学习和使用的过程中，同时会对自己计算机的性能有更全面的了解，这是一个既有趣又有挑战性的工作。下面我们首先来看看 Processor 对象。

对于单处理器系统，处理器的状态大致上反映了系统的运行情况，几乎所有的活动都会影响处理器，因此 Processor 对象是我们了解系统性能的一面镜子。如果系统中有多处理器，则选择 Processor 对象时，每个处理器就是一个实例；一般说来，要为每个处理器添加一条不同颜色的线，以便于观察。

建议：对于多处理器系统，一个处理器的活动通常并不能反映出准确的系统运行情况，这时候还应当用系统对象进行观察。

当添加计数器时，默认添加的是 Processor 对象的%Processor Time 计数器，Processor 对象下还有别的许多计数器，下面是一些可能常用到的计数器的说明：

（1）%Processor Time 计数器

% Processor Time 指处理器执行非闲置线程时间的百分比。这个计数器设计成用来作为处理器活动的主要指示器。它通过在每个范例间隔中衡量处理器用于执行闲置处理线程的时间，并且用 100% 减去该值得出。可将其视为范例间隔用于做有用工作的百分比。这个计数器显示在范例间隔时所看到的忙时平均值。这个值是用 100% 减去该服务不活动的时间计算出来的。 例如如果显示的数据是 25%，那么处理器有 75%的时间在执行闲置线程，这 75%的时间是闲置时间。

提示：所谓闲置时间(Idle Time)是一个需要解释的概念，操作系统不会允许处理器“游手好闲”，因此处理器永远不可能像人一样空闲休息。Windows 2000 在启动时，会为处理器分配一个闲置线程，该线程在没有其它线程可以运行时消耗周期，因此系统在没有实际工作执行时，处理器就转去执行闲置线程。

有人选择长时间（比如一天）地统计处理器时间百分比的平均值，这种统计也许不能准确地反映处理器的性能状态。比如在域一章里所讲的，当每天早上各位人员登录注册时，用于处理身份验证的域控制器就会处于高峰时间，而当这段时间过后，处理器就可能没什么事情可做了。这时候真正有意义的数据应当是处理身份验证时的处理器性能数据，如果用一天的时间进行平均，就有可能无法体会到处理器的压力。

此外，需要注意的是：处理器时间计数器的曲线变化比较快，即使当负担很轻时，在短暂的时间内也可能猛增到 80%甚至 90%，而在工作繁忙时，也可能偶尔处于闲置状态。这点同磁盘的计数器不一样。

建议：使用这个计数器需要小心的是：不要指定太短的更新时间，否则系统会频繁采样数据，这会导致处理器时间百分比持续过高，从而造成系统负担过重，处理器性能偏低的假象，因为以过高的频率采样本身会大量消耗处理器资源，而实际上并没有必要工作给处理器带来压力。合理的选择是为处理器安排一个适当的采样间隔。

（2）%Interrupt Time 计数器

% Interrupt Time 指处理器在范例间隔期间用于接收和为硬件间隔提供服务的时间的百分比。该值间接地显示了产生间隔的设备(如系统时钟、鼠标、磁盘驱动程序、数据通讯线、网络界面卡和其它附属设备)的活动。这些设备通常在完成一项任务或需要引起注意的情况下中断处理器。正常的线程执行在间隔时暂停。大多系统时钟每隔 10 毫秒中断处理器一次，成为中断活动不重要的部分。

（3）%Privileged Time 计数器

指非闲置处理器时间用于特权模式的百分比(特权模式是为操作系统组件和操纵硬件驱动程序而设计的一种处理模式，它允许直接访问硬件和所有内存。另一种模式为用户模式，它是一种为应用程序、环境分系统和整数分系统设计的一种有限处理模式。操作系统将应用程序线程转换成特权模式以访问操作系统服务)，特权时间的 % 包括为间断和 DPC 提供服务的时间。这个计数器将平均忙时作为样本时间的一部分显示。

特权时间比率高可能是由于失败设备产生的大数量的间隔而引起的，而且如果系统花太多的时间用于执行系统服务，而不是执行应用程序。

（4）% User Time 计数器

指用于用户模式的非闲置处理器时间的百分比(用户模式是为应用程序、环境分系统和整数分系统设计的有限处理模式。另一个模式为特权模式，它是为操作系统组件设计的并且允许直接访问硬件和所有内存。操作系统将应用程序线程转换成特权模式以访问操作系统服务。)。这个计数值将平均忙时作为实例时间的一部分显示。

（5）Interrupts/sec 计数器

指处理器每秒钟接收并维护的硬件中断的平均值。它不包括 DPC，DPC 将单独计算。这个值是产生中断的设备(如：系统时钟、鼠标、磁盘驱动器、数据交流线路、网络街面卡和其它附件设备)的活动的间接指示器，这些设备通常在完成了一项任务或需要注意时中断处理器。正常的线程操作在中断时悬停。大多数的系统时钟每隔 10 毫秒中断处理器一次，形成了间隔活动的后台。这个计数值显示用上两个实例中观察到的值之间的差除于实例间隔的持续时间所得的值。

14.3.3　Memory 对象

除了处理器对象外，内存对象也是影响系统性能的重要部分。特别是 Windows NT 和 Windows 2000，更是消耗内存的好手。许多时候，增加内存甚至比对处理器升级更能解决性能问题。

与处理器对象不同，Memory 对象的统计数据通常能够准确反映当前系统内存的状态。如果发现内存使用出现高峰，可能是由于内存不够，这时候系统的运转就会变慢。

（1）Commit Limit 计数器

Commit Limit 是指在不用扩展分页文件的情况下可以使用的虚拟内存的数量。这是用字节来计算的(确认的内存是指保留在磁盘分页文件上的物理内存。在每个逻辑磁盘上可以有一个分页内存)。如果扩展分页文件，这个限量将相应增加。这个计数器只显示上一回观察到的值；而不是一个平均值。

关于虚拟内存、物理内存及分页文件的概念，下一章将有详细叙述。

（2）Committed Byte 计数器

Committed Byte 是指以字节表示的确认虚拟内存，也就是已经提交给应用程序请求的内存总量。它由分页文件的大小而决定的。如果扩大了分页文件，该比例就会减小。这个计数器同样只显示上一回观察到的值；它不是一个平均值。

（3）% Committed Bytes In Use 计数器

% Committed Bytes In Use 是前面 Committed Bytes 与 Commit Limit 两个计数器之间的比值。这个计数器只显示当前百分比；它不是一个平均值。

如图 14-13 所示是 Commit Limit、Committed Byte 和% Committed Bytes In Use 的报表显示。表明可用的虚拟内存是 154MB，而当前使用的是 81MB，百分比是 52%。

（4）Pages Input/sec 计数器

Pages Input/sec 指为解决页错误从磁盘上读取的页数。所谓页错误是指当处理过程需要不在其工作集或物理内存的任何地方的代码或数据，而需要从磁盘上检索时出现的错误。Pages Input/sec 计数器是显示这种导致系

统范围延缓错误的主要显示器。

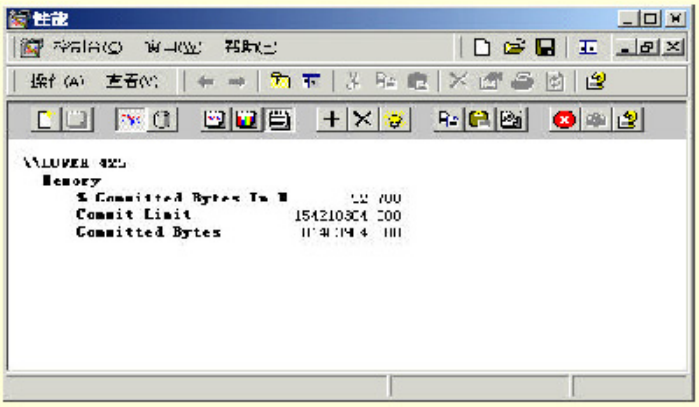


图 14-13 Commit Limit、Committed Byte 和% Committed Bytes In Use 的报表显示

5．Pages Output/sec 计数器

Pages Output/sec 是指为了释放物理内存空间而写入磁盘的页数，而只有在物理内存中更改时页才会写回到磁盘上。注意：高速的页输出可能表示内存不足，因为当物理内存不足时，Windows 2000 会将页写回到磁盘以便释放空间。

6．Pages/sec 计数器

Pages/sec 是前面 Pages Input/sec 和 Pages Output/sec 两个计数器的总和，是用页数计算的，以便在不用做转换的情况下就可以同其它页计数器做比较。如果超出 10，说明系统交换太过频繁，扩大内存可能可以提高性能。

14.3.4 PhysicalDisk 对象

PhysicalDisk 对象设计磁盘的性能。注意它不代表逻辑驱动器，物理盘中可能会有多个逻辑盘。为了提高磁盘的访问速度，可以对硬盘进行升级，提高硬盘转速，或者增大高速缓存空间，这样也可以减少来自磁盘的请求数量。

（1）%Disk Read Time 计数器

%Disk Read Time 指所选磁盘驱动器忙于读操作所用的时间的百分比。

（2）%Disk Write Time 计数器

%Disk Write Time 指所选磁盘驱动器忙于写操作所用的时间的百分比。

（3）%Free Space 计数器

%Free Space 指在逻辑磁盘单位上的可用空间与所有逻辑磁盘驱动器提供的可用总磁盘的比率。

（4）%Idle Time 计数器

%Idle Time 汇报磁盘闲置时间的百分比。

（5）Current Disk Queue Length 计数器

Current Disk Queue Length 指在收集操作数据时在磁盘上未完成的请求的数目。它包括在快照内存时正在为其提供服务中的请求。这是一个即时长度而非一定间隔时间的平均值。这个计数器可能会反映一个暂时的高或低的列队长度，但是如果在磁盘驱动器存在持续负载，可能值会总是很高。请求等待时间与这个列队的长度减去磁盘上的主轴成正比。这个差值应小于 2 才能保持良好的性能。

（6）Avg. Disk sec/Read 计数器

Avg. Disk sec/Read 指从磁盘读一次数据所需的平均时间。相应地，Avg. Disk sec/Write 指从磁盘写一次数据所需的平均时间。

（7）Disk Reads/sec 计数器

Disk Reads/sec 指在此盘上读取操作的速率。相应地，Disk Writes/sec 指在此盘上写入操作的速率。

（8）Split IO/Sec 计数器

Split IO/Sec 汇报磁盘上的输入输出（I/O）分割成多个 I/O 的速率。一个分割的 I/O 可能是由于请求的数据太大不能放进一个单一的 I/O 中或者磁盘碎片化而引起的。

14.3.5　System 对象

如果系统中安装了多个处理器，则可能需要使用 System 对象来考察系统性能。与 Processor 对象不同，System 对象将所有处理器作为整体以考察系统性能。

（1）%Total Processor Time 计数器

系统上所有处理器忙于执行非空闲的线程所花费的时间的平均比例。

（2）%Total Interrupt Time 计数器

该值是所有处理器的%Total Interrupt Time 计数器的值的和除以该系统中处理器的个数。

（3）% Total Privileged Time 计数器

所有处理器以特权模式运行所花时间的平均百分比。相应地有% Total User Time 计数器是所有处理器以用户模式运行所花时间的平均百分比。

上面所列的单子已经足够长了，但性能监视器中还有许许多多的对象，包括 Browser、Cache、IP、Network Interface、Redirector、Server 等等。这里不可能逐个地详细介绍，但经过对 Processor、Memory、PhysicalDisk、System 对象的介绍，读者应该已经有了一个整体的概念，更深入地学习需要大家的努力，请记住：这些工具对监视系统以及网络性能有着相当有效的作用，对监视器的了解越深入，解决性能优化问题就越强。

14.4　数据观察

除了可以在性能监视器中直接观察数据，还可以用其他工具以获取和查看。比如许多公司使用 SNMJP（简单网络管理协议，Simple Network Management Protocol）进行监视。但由于价格昂贵，只有部分网络管理员才可能使用。幸好还有一些简单易行的方法可以将数据导出。

新版本的性能监视器支持在微软的 Internet Explorer，这也是他们的拿手好戏。可以非常容易地将性能图表存成.htm 文件，然后在 IE 浏览器中打开查看。只需在图表区域中单击右键，在弹出的快捷菜单中，选择“另存为”命令，如图 14-14 所示，选择后缀名为.htm，并输入合适的路径名和文件名。

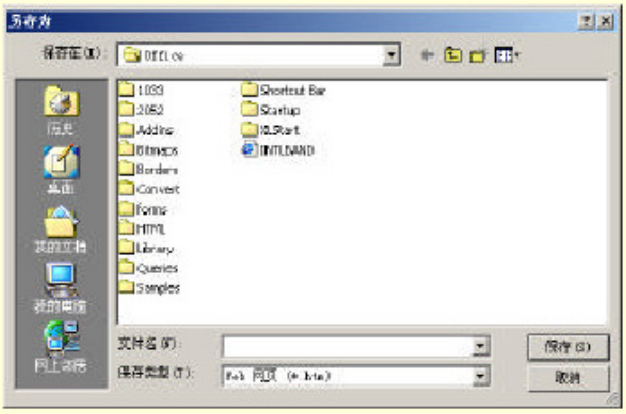


图 14-14　将图表保存为 htm 网页或者 tsv 报表文件

转存为.htm 文件后，就可以在 IE 浏览器中下载查看，如图 14-15 所示。这样就可以做成很有说服力的网页。

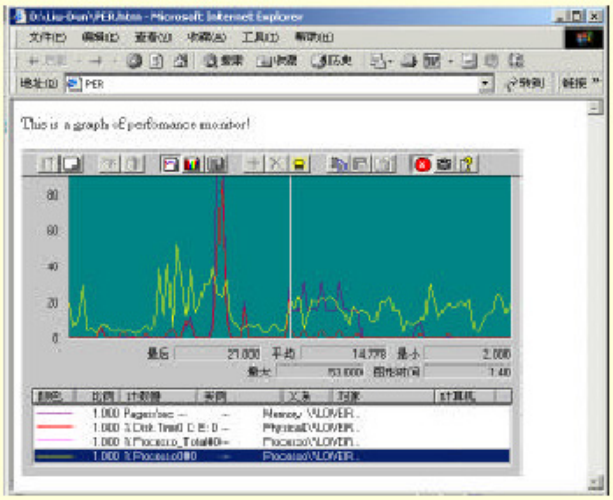


图 14-15 在 IE 浏览器中查看数据

性能图表还可以使用电子表格 Excel 等程序进行数据观测，整理成柱形图、饼图、曲线图等进行进一步的数据分析。在图 14-14 中，从保存类型下拉框中，选择 Report(*.tsv)，就可以保存为报表文件。

14.5 使用警告

日志和警告是 Windows NT 4.0 和 Windows 2000 版本的性能监视器差别最大的地方。Windows 2000 增强了这两方面的功能，并将它们集成为一个新的控制树。

打开性能监视器，并展开性能监视和日志，并选择“警报”子树。第一次打开时，还没有警报项目的设置，这时候右边面板是空白的。在上面单击右键，从弹出的快捷菜单中，选择“新建”→“创建新的警报设置”命令，如图 14-16 所示。

也可以选择“创建警报设置”自命令，这时候从“打开”对话框中选择保存的 HTML 文件，用以创建警报。

图 14-16 创建新的警报设置

选择了创建新的警报设置后，将出现如图 14-17 所示的对话框，要求输入新警报的名称。在文本框中，输入所设置的警报名，比如 alert。

图 14-17 添加名称

单击“确定”后，出现如图 14-18 所示的对话框，初次建立警报时需要添加新的计数器。单击“添加”按钮，在与图 14-12 类似的框图中，选择对象、计数器和实例。

图 14-18　为警告添加计数器

选定计数器后，就可以设置告警的门限，以及数据采集的间隔。可以选择超过或者是低于某个数值，并选择合适的间隔。如图 14-19 所示。注意间隔不要设得太短，否则过于密集的采集数据有可能降低系统性能，系统会缺省地设置为 5 秒，这是一个不错的选择。

不要为太多的计数器设置警报，因为这样可能会适得其反。如果人们对警告习以为常，就会失去警惕性，当真正严重的问题出现时，反倒会不当一回事。

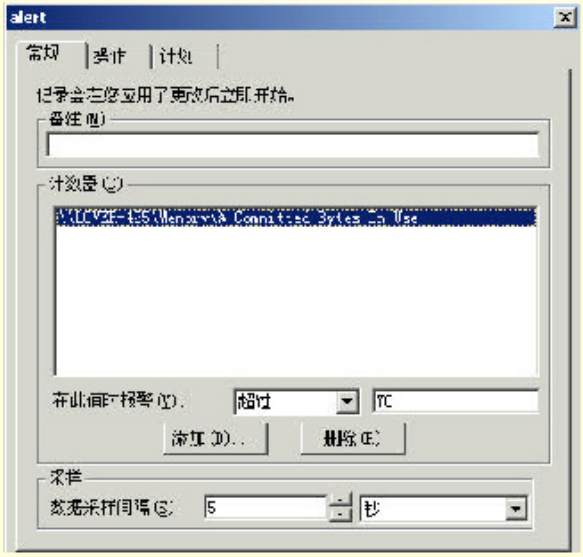


图 14-19　设置告警门限和采样间隔

警报的设置包括操作和计划两个选项卡。可以在添加新的警报时配置，也可以之后配置。计划指的是警报日志的开始和停止时间，可以通过快捷菜单手动设置，也可以预先指定开始和停止的日期，如图 14-19 所示。

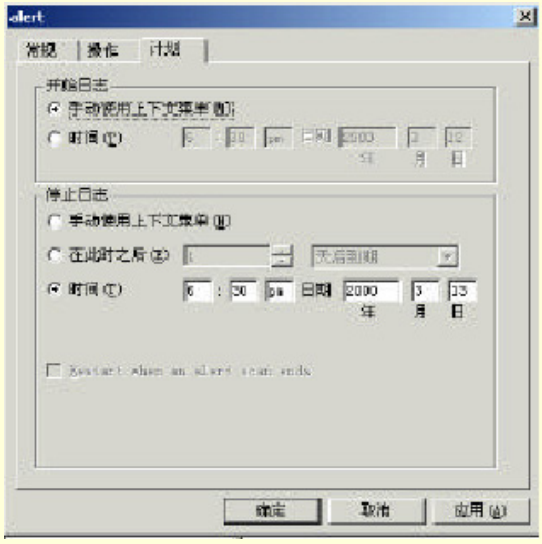


图 14-20　设置警报计划

警报的操作选项卡帮助用户设置发生警报时的其他动作，如图 14-21 所示。

·将项记入应用程序事件日志：选中这个复选框，使日志服务创建一个可以在时间查看器中查看的条目。

·发送网络信息到：该选项使日志服务触发消息发送服务，将消息发送给网络用户。

·执行命令文件：当警报发生时，同时执行的命令文件。可以通过单击“浏览”按钮，选择可执行的命令文件名及其路径。在命令行参数中，选择参数列表，底部有采样参数列表的示例。

·启动性能数据日志：如果希望警告发生时，运行一个计数器日志，就选中此复选框，并从右边的下拉菜单中选择合适的计数器日志。

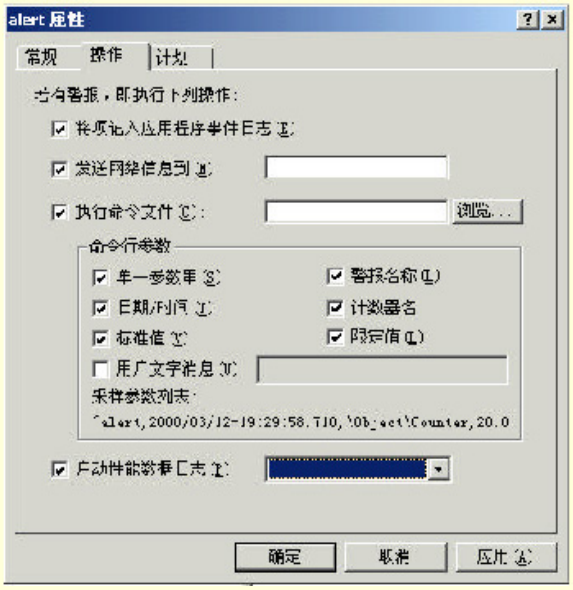


图 14-21　设置发出警报的同时操作

当设置完成后，在如图 14-16 所示的日志和警报视图中，就可以看到警报条目，前面的图标如果是红色的，表示这个警报尚未启动。单击鼠标右键，从快捷菜单中选择开始命令，就可以启动警报，这时候图标变成绿色。

在旧版本的性能监视器中，也可以设置警告，方法与前类似。如图 14-22 所示是对 Memory 对象的 Pages/Sec 计数器设置警告后的视图。

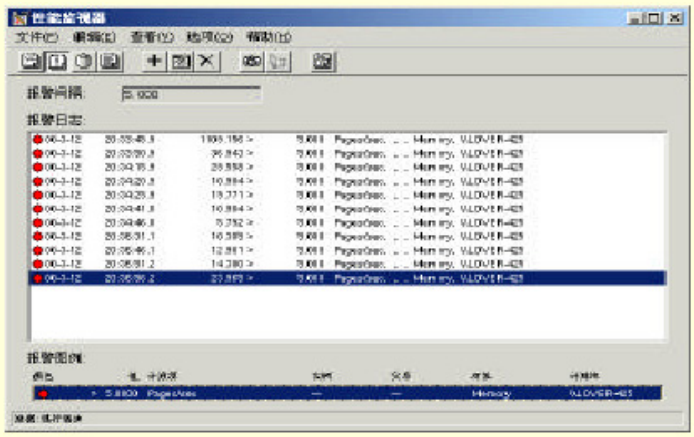


图 14-22　页面交换超过警告线

以下是一些常用的警报：

・逻辑磁盘对象的%Free Space 计数器：指定磁盘最低空闲百分比。可以将这个值设为 10 或者更大。

・内存对象的 Pages/Sec 计数器：设置门限为 5，用它来标识系统交换太过频繁。

14.6　使用日志

使用日志是性能监视器的另外一个重要组成部分。日志和警报一样，帮助用户从本地计算机或者远程计算机中自动收集性能数据。记载的计数器日志数据可以通过性能监视器查看，也可以输出到其他程序或者数据库中进行分析，并生成数据报表，从而更好地检查系统的性能。

在 Windows 2000 中，日志的功能和使用比起 Windows NT 4.0 已经得到了很大的加强。包括以下几个方面：

・可以使用逗号分隔或者制表分隔的格式，从而更方便地将数据导入到其他程序中。此外，也可以使用二进制的格式循环采集数据。

・从性能日志或者警报中采集的计数器数据，可以在采集过程中查看，也可以在采集停止后查看。

・日志以服务方式运行，因此无论任何用户在此计算机中登录，数据采集工作都会进行。

・可以更加灵活地配置长期记载的日志。用户可以定义开始和中止日志的时间、文件名、文件的大小以及其他自动日志需要的参数。

・可以在一个单独的管理控制窗口管理多个日志会话。

14.6.1　计数器日志

日志包括两个部分：计数器日志和追踪日志，它们都在同一个位置：性能日志和警报文件夹下。计数器日志与性能监视器一样，日志的使用是从对象、计数器和对象实例着手的，用以监察硬件资源和系统服务。所有日志都需要设置记载的对象，对象下的计数器，以及实例。

打开性能日志和警报，选择计数器日志。缺省情况下的计数器日志文件是 System Overview，此日志提供了系统性能概述，如图 14-23 所示。

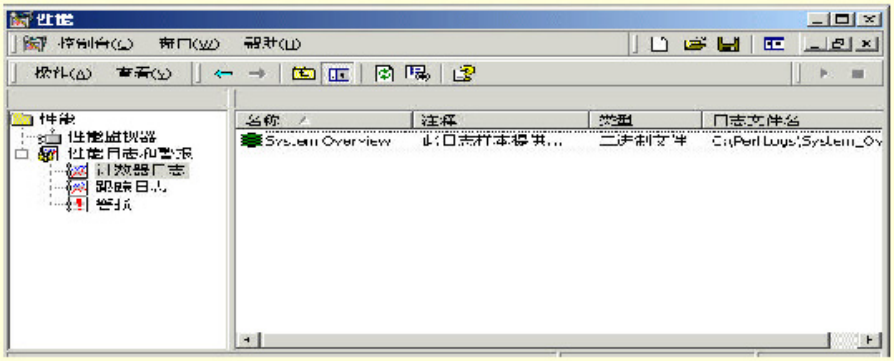


图 14-23　计数器日志

如图计数器日志中有四个栏目：名称、注释、类型和日志文件名。名称和注释帮助用户了解日志的功能。日志文件有多种类型，如 System Overview 是二进制文件；而日志文件名提供了日志文件的路径和名称。

可以添加自己的日志。同警报中的操作一样，在右边面板栏中单击右键，从弹出的快捷菜单中，选择“新建”→“建立新日志设置”命令，并输入新日志名称。接下来的操作如下：

（1）在如图 14-24 中，单击“添加”按钮，为新日志添加计数器。

（2）添加计数器后，选择采样数据间隔，缺省时间是 15 秒。

（3）点击“文件”选项卡（在添加新计数器之前，无法选择“文件”或者“计划”选项卡），如图 14-25 所示。可以为日志文件输入注释，并选择日志文件类型。缺省是二进制文件，即后缀名为 blg 的文件，还有文本文件，二进制循环文件等类型。

Windows 2000 为日志文件提供的新功能是限制文件大小，可以允许日志文件增长到最大值，或者将日志文件限制在一定的大小范围内。

缺省时日志文件存放在 C:\Perflogs 下，可以单击“浏览”按钮，选择日志文件存放的路径，以及文件名。在日志文件名文本框中，输入的名字是在性能日志和警报视图中看到的日志名，可以将它理解为一个友好的名字，实际存放的文件名在底部显示。

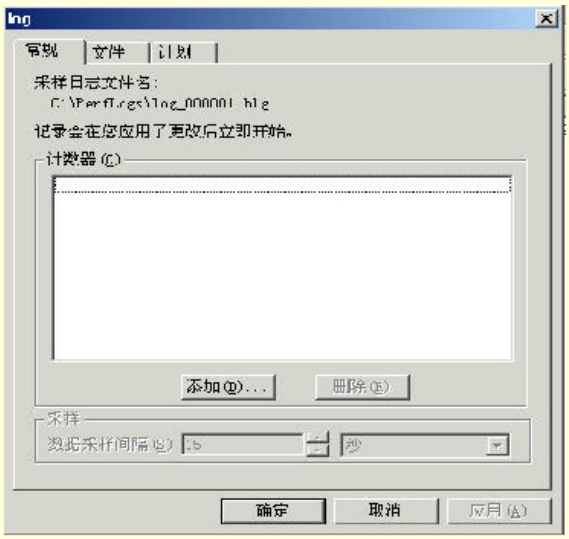


图 14-24 在日志中添加计数器

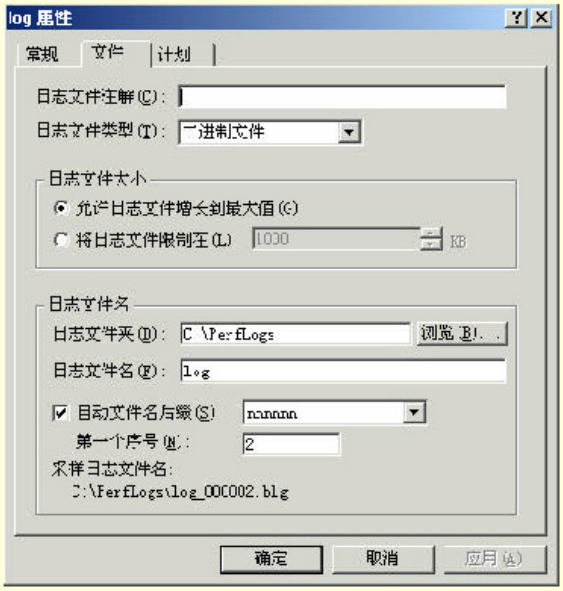


图 14-25 文件选项卡

（4）单击“计划”选项卡，如图 14-26 所示。

可以手动或者定义某个时间以开始和停止日志，比如可以将日志停止的时间设为下午 11:59，而一个新的记录在上午 12:00 开始。如图 14-27 所示，定义具体时间或者相对时间都可以，非常方便。如果选择了限制日志文件大小，还可以选择日志满后停止日志。此外，还可以定义一个日志停止时执行的程序。

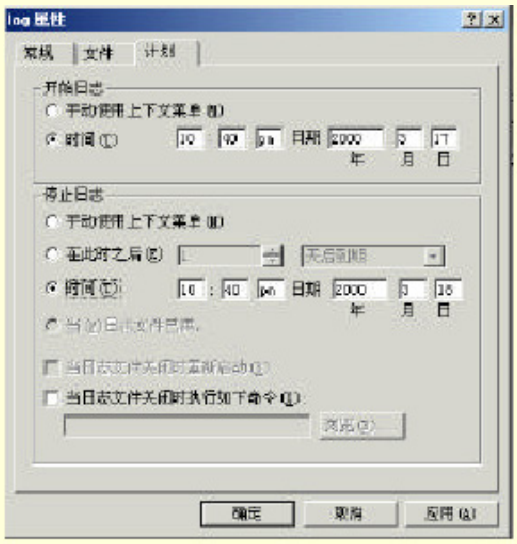


图 14-26　设置日志开始和停止时间

前面讲过将性能曲线存为 htm 文件，理所当然地，可以将 htm 文件导出设置为日志。同样单击鼠标右键，从快捷菜单中选择“新建”→“建立日志设置”自命令，之后在打开对话框中选中 htm 文件，如果这个 htm 文件是在性能图表中存入的，则会自动地将图表中有的计数器列出，否则还需要自己添加计数器。

14.6.2　跟踪日志

跟踪日志是新增添的日志种类。可以用来追踪系统性能数据。缺省时没有设置追踪日志，用户必须建立自己的追踪。

建立一个新的追踪日志与前面所说的建立计数器日志或者警报方法完全一样。在右边面板栏中单击鼠标右键，从弹出的快捷菜单中，选择“新建”→“建立新日志设置”命令，并输入新日志名称，如图 14-27 所示。

图 14-27　设置追踪

单击“显示活动的提供者”，将出现已经安装的提供者以及它们的状态（启用或是停用），只有 Windows 的核心追踪提供者是启用的。

图 14-28 显示活动的提供者

有两种方案可供选择：单击“系统”单选钮，缺省的提供者（provider）是 Windows 的核心追踪提供者，它负责监视进程，线程以及其他一些活动。单击右边的“显示详细信息”按钮，可以查看监控大有关事件，如图 14-27 所示，这时候磁盘 I/0 和网络 TCP/IP 也在监控之内，而页错误与文件 I/O 没被选中。用户可以在里做自己的选择，添加或者去掉一些有关的事件。

提示：页错误与文件 I/0 的追踪日志可以产生数量惊人的数据，因此微软并没有将这它们列为缺省的事件。如果需要监视它们的活动，推荐使用时间限制，比如两个小时。

如果单击“常规”单选钮，则可以通过单击“添加”或者“删除”按钮使用自己的数据提供者。每次只有一个追踪提供者的实例可以使用。

与在计数器日志中一样，单击文件选项卡，在对话框中配置日志文件的大小（用 KB 为单位），存放的路径以及文件类型。需要注意：与计数器日志不一样，追踪日志有两种类型，系列追踪文件和循环追踪文件，它们都是后缀名为 etl 的文件。系列追踪文件顺序记载数据，直到用户设置的限制条件满足后停止，并等待重新开始时间。而循环追踪文件采用循环追踪，持续写入至同一个文件中，并用新的数据覆盖前面的记录。这两种文件类型都是追踪日志中特有的。

单击计划选项卡，配置追踪日志的开始和停止时间。

与计数器日志不一样的是追踪日志还有缓冲器这个选项卡，用以设置追踪日志的缓冲大小。包括缓冲器大小、最小缓冲区和最大缓冲区，如图 14-29 所示。

用户还可以设置启用定期缓冲刷新，这样每到刷新间隔，就会自动刷新跟踪日志的数据。

计数器日志和跟踪日志二者是有区别的。在跟踪日志中，选定的事件发生后，提供者会将数据传送给日志服务，这点和计数器日志不同。当计数器日志启用时，日志服务每次刷新间隔到了后会从系统中取得数据，而不是等待一个确切的事件发生。

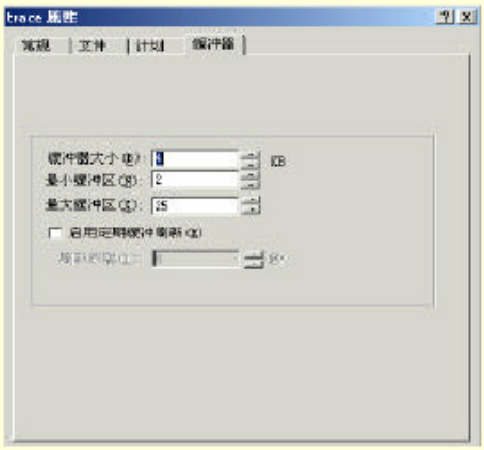


图 14-29 设置缓冲区

14.6.3　查看日志数据

初次使用日志的用户可能会不习惯日志的查看，因为添加和配置日志与查看日志并不在同一个视图中。添加一个新的日志在性能日志和警报中，如果希望查看进行检查，却出现了无论如何找不到数据的尴尬。答案是必须在性能监视器视图中完成这个工作。所以说，微软的这个工具界面并不十分友好，至少他们应该在性能日志和警报中提供单击右键，从快捷菜单中选择命令的手段。

要查看日志数据，请依旧回到性能监视器视图，在图表上单击鼠标右键，从快捷菜单中选择属性命令，之后选择来源选项卡，并选中日志文件选项卡，如图 14-30 所示。

图 14-30　选择查看日志数据

单击“浏览”按钮，如图 14-31 所示。缺省情况下，系统都将日志文件存放在 C:\Perflogs 目录中（除非用户在前面所说的文件属性的文件选项卡中改动了文件路径）。

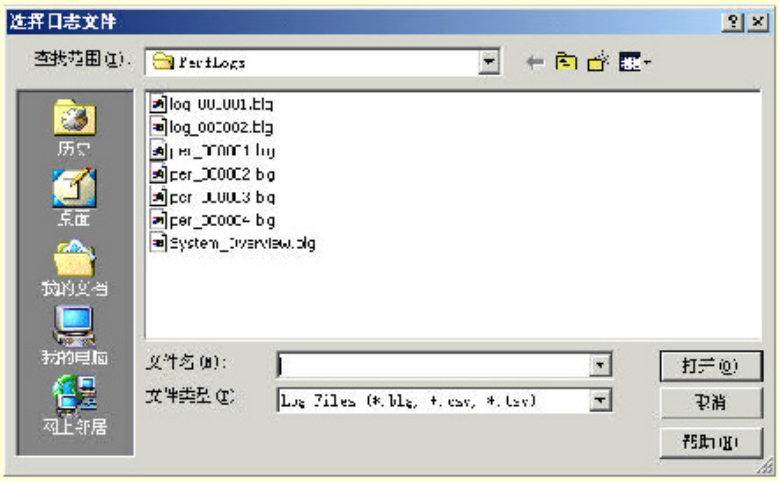


图 14-31　选择日志文件

细心的读者会发现，可以选用的类型有.blg、csv 和 tsv 文件，这些都是计数器日志中的日志文件而没有跟踪日志的类型。如果在图 14-31 所示的文件类型中选择所有文件，也会在 C:\Perflogs 目录中找到跟踪日志文件，但选择打开后，将出现提示，说明指定的日志文件可能不正确或找不到。

事实上只有计数器日志数据才能在性能监视器中查看，而跟踪日志的数据输出需要通过特定的解析工具帮助“翻译”，开发者可以使用提供的 API 函数制作这种工具。

在图 14-31 所示中会发现同一个设置的日志文件名有好几个后缀，比如 per_0000001 、per_0000002、per_0000003。这是由于每个文件停止后有被重新启动，因此用后缀名来区分每一个日志文件。后缀名在如图 14-25 所示中设置，由自动后缀和第一个序号决定。缺省时提供的自动后缀是 nnnnnn 其他的后缀名有：mmddhh、mmddhhmm、yyddd、yymm、yymmdd、yymmddhh，它们的含义都很明显。

选定日志文件后，就可以在性能监视器中查看数据了，如图 14-32 所示。

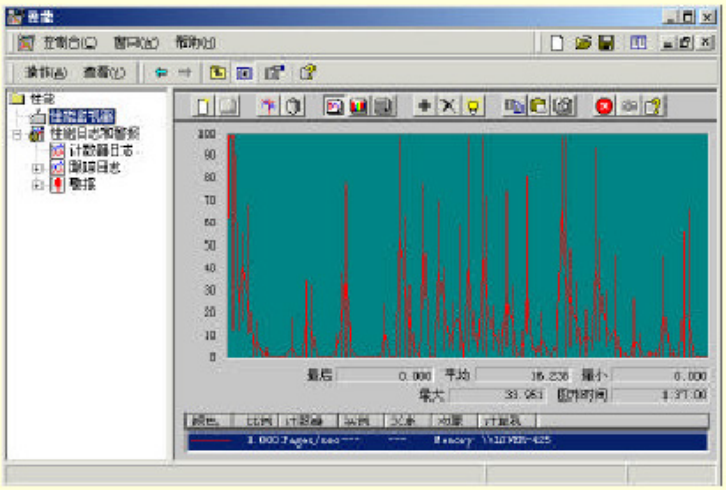


图 14-32 查看日志文件数据

Windows 2000 中的性能监视工具的确是一个面目全新的东西，尽管在界面上仍然显得专业化而且不好理解，但并不妨碍它执行强有力的监视工作。特别在查找系统性能瓶颈时，性能监视器几乎是最为常用的工具，我们将在后面继续介绍。

另一方面，作为 Windows 2000 中的管理单元，它还有一个新的特性：通过创建任务板简化任务工作。我们将在下一章中全面介绍管理控制台的使用，其中自然也包括创建任务板，因此这一功能这里就不赘述了。

第 15 章　IIS 介绍

Internet 的冲击给全球带来了深远的影响，因为它有可能是世界上最方便、最普及的信息交流方式，从长远来说，Internet 的前途是无可估量的。关于 Internet，在本书的其他章节有详细介绍，这里就不打算赘述了。需要注意的是：虽然现在的 Internet 已经非几年前可以相提并论，但是它还在不断地成长，并且不单是计算机公司在注意，许多通信巨头也在开发自己的“无线 Internet”计划，未来的 Internet 会是什么样，是几乎所有的因特网用户都在时刻关心的问题。像微软这样的大公司更不会坐视这么大的市场份额而不顾。但是在几年前，即使是比尔· 盖茨，也曾经忽视过 Internet 的威力，当时大部分的浏览器是网景公司的 Netscape，当微软发现自己的失误时，采取了捆绑 Internet Explorer 的手段，才使 IE 压倒了盛极一时的 Netscape。

有了这个经验教训，如何更好地与 Internet 结合，开发什么样的 Internet 软件以使得其既方便好用又能满足市场和用户的要求，已经成为微软软件开发的重要课题：浏览器有最新的 IE5 的版本；开发应用程序的王牌产品 Visual C++和 Visual Basic 的新版本也不断集成了先进的 Internet 特性；开发 VBScript 与 JavaScript 进行脚本市场的竞争，以及 ADO、ActiveX、ASP 等新产品的不断涌现都是这个市场策略的重要代表。在赖以生存的操作系统方面，IIS（Internet Information Server，因特网信息服务器）可以与 Windows NT、Windows 2000 很好地结合，这样就可以把 NT 设置成为一个 Internet Server，因此它是微软的一个重要产品。

本章内容包括：

- IIS 简介
- IIS 的安装
- 客户/服务器模型
- 用 IIS 配置 WWW 服务
- 建立新的 Web 站点
- 用 IIS 配置 SMTP 服务
- 用 IIS 配置 FTP 服务

15.1　IIS 简介

IIS 是一个很棒的产品，它与 Windows 2000 能够很好地集成，利用它，可以十分方便地创建一个 Web 服务器。很短的时间内，IIS 已经有好几个版本。在 Windows NT 4.0 中包含有 IIS 的 2.0 版本，比较新的版本则是 4.0，为了配合 Windows 2000，微软推出了 IIS 的 5.0“完全版本”，IIS5.0 比 IIS2.0 更加强大和全面。

15.1.1　IIS 组件

微软为了扩充 Windows NT 4.0 的功能，开发并提供了著名的 BackOffice 服务器应用程序系列。BackOffice 是一个很大的软件包，包括有：Microsoft SQL Server，用于客户机-服务器数据库系统管理；Microsoft Exchange Server，用于客户机-服务器邮件系统管理；Microsoft Proxy Server；Microsoft SNA Server，用于管理 IBM 网络大型机和小型机的数据访问；Microsoft Systems Management Server ，用于对负责的分布式系统的集中管理；Microsoft Commercial Internet Server 等等。IIS 为 BackOffice 提供了附加的 Internet 技术和增强的内容。

IIS4.0 最早是作为微软发布的 Windows NT 4.0 的补丁 Option Pack 中的核心产品。在当时的 Option Pack 中，还有 Microsoft Certificate Server、Data Access Components、Microsoft Index Server、Microsoft Management Console、Microsoft Transaction Server、Microsoft Site Server 等系列产品。Certificate Server（证书管理器）和 Microsoft Management Console（管理控制台）也是 IIS 的核心组件，构成了 IIS 平台。如今在 Windows 2000 中的 IIS5.0 有所不同，证书管理器已经从 IIS 中独立出来（后面将有介绍），管理控制台也已经成为了微软所有管理工具的共有平台，然而 IIS 的基本功能没有变化。

15.1.2 IIS 功能

IIS 是一个功能丰富的软件包，它支持最新的 HTTP 1.1 标准，HTTP（Hypertext Transfer Protocol，超文本传输协议）是 Internet 最重要的协议之一。HTTP 1.1 改进了传输速度，从而提高了 Web 的整体性能。

IIS 之所以能够成为 Web 服务器，是因为它包含了各种最流行的 Internet 服务，以下是一些主要的服务：

15.1.2.1 WWW 服务

World Wide Web 服务是 Internet 上最流行的服务，它包含各种丰富的功能。Web 页的可浏览性正变得越来越强，随着带宽的改善，图形、动画、音乐甚至电影都能在网上浏览，CGI 和 ASP 也提供了强大的交互功能。

作为 Web 服务器，IIS 必须能够把 Web 页文档传送给其他计算机上的浏览器(Internet Explorer 或者 Netscape)，这些文档一般是 HTML 格式的，其中可以包括文本、图形、动画、视频文件或者用于交互的表单。

15.1.2.2 FTP 服务

文件传输协议（FTP）是基于 TCP/IP 网络和 Internet 的计算机之间传送文件所用的工业标准协议。FTP 甚至比 WWW 服务提出的时间更早。

15.1.2.3 SMTP 服务

SMTP 服务（Simple Mail Transfer Protocol，简单邮件传输协议）是安全且可扩展的邮件服务器。它支持 POP3 版本的分布式邮件服务，允许在多个服务器间进行收件箱分区，比如可以把服务器分为成百上千的用户收件箱，为公司职员服务。

15.1.2.4 NNTP 服务

NNTP 服务（Network News Transfer Protocol，网间新闻传送协议）是商业用的服务器。它可以创建公用或者私有的讨论组，向用户提供对远程讨论组的访问，包括受到广泛欢迎的 Usenet 新闻组。为了保证安全，还提供 SSL（Secure Sockets Layers，安全套接层）的加密明文认证。

15.1.2.5 Gopher 服务

Gopher 服务提供了在 Internet 上查询有用信息的服务。

15.1.2.6 Telnet 服务

Telnet 服务可以为远程用户提供注册的服务功能。

15.2 IIS 的安装

Windows 2000 包括最新的 IIS5.0 版本，在微软的网站 www.microsoft.com 上也可以得到 IIS4.0 的免费版本。

15.2.1 硬件和软件需求

IIS 可以在基于 Intel x86 或者 Alpha 的计算机上安装。在上一小节中列出了 IIS 的大部分重要的服务功能，但不是必须要将它们全部安装，用户完全可以根据自己的需求选择安装的组件，例如如果不需要创建动态的 Web 内容，就不需要安装活动服务器页面（Active Sever Pages）。表 15-1 是微软推荐的在 Intel x86 平台上的硬件需求，如果在 Alpha 平台上，则需要更高的硬件资源。

表 15-1 Intel x86 平台需求

组件	最小需求	推荐需求
CPU	50MHI 486	90MHz Pentium
RAM	16MB	32MB~64MB
空闲空间	50MB	200MB
显示器	VGA	Super VGA

如果需要安装 SMTP 服务或者 NNTP 服务，则需要更高的硬件资源。

软件上，IIS 需要 Microsoft Internet Explorer 4 或者更高的 IE 版本作为浏览器。

如果在 Windows 95 或者 Windows 98 上安装 IIS，由于缺少了一些 Windows 2000 和 Windows NT 的功能，此时 IIS 将变成为 PWS（Personal Web Server）。Windows 95 上的 PWS 缺少 NT 特有的安全机制，所实现的功能也相应地减少了许多，比如不能实现多 Web 站点主机，ODBC 日志等。

15.2.2　安装过程

将 Windows 2000 光盘放入光驱中，此时如图 15-1 所示，选择“安装附加组件”。

图 15-1　安装附加组件

如图 15-2 所示是可供安装的附加组件，包括 Internet 信息服务（IIS）、管理和监视工具、脚本调试器、索引服务、消息队列服务、网络服务、其他网络和文件打印服务等选项。

图 15-2　选择附加组件

下面是除 IIS 之外的组件的简单介绍：

- 脚本调试器（Microsoft Script Debugger）：提供全面的脚本调试环境，用以发现客户机和服务器的 VBScript 和 JavaScript 脚本中的错误并进行调试。
- 索引服务（Index Server）：创建站点索引，帮助搜索多种格式的文本。
- 网络服务：包含专门的、网络相关的服务和协议，如 RTP 侦听器，简单 TCP/IP 协议等。
- 管理和监视工具：包含简单网络管理协议（SNMJP），用以监视网络设备的活动并且向控制台汇报。
- 消息队列服务：提供可靠的网络通讯服务。

安装选项中提供了各个组件所需的磁盘空间，选择要安装的组件，如果组件下还有各个部分，可以单击“详细信息”按钮，作进一步查看，同时选择需要安装的子组件。

前面说过，不需要安装所有的 IIS 组件，但是一般说来，WWW 服务、FTP 服务、ADO 数据对象（ActiveX Data Objects）都是需要安装的。选择组件列表中的第一项 Internet 信息服务（IIS），单击“详细信息”按钮，如图 15-3 所示。

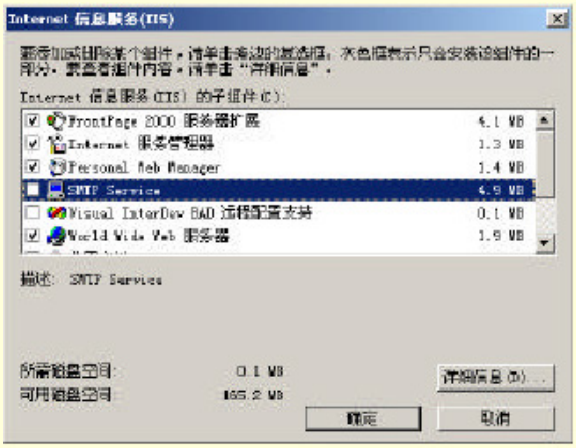


图 15-3 IIS 的组件内容

在 IIS 组件中，还包括如下一些选项：

■ FrontPage 2000 服务器扩展（FrontPage Extensions）：使用 FrontPage 扩展，可以帮助使用 Microsoft FrontPage 和 Visual Interdev 创建 Web 站点。

■ World Wide Web 管理器（WWW 管理器）：用以实现管理和对 Web 站点的访问。安装 FrontPage 2000 服务器扩展时需要安装 WWW 管理器的进行支持。

■ 文件传输协议管理器（FTP 管理器）：允许建立 FTP 站点，用以上传和下载文件。

■ Internet 服务管理器：IIS 的管理界面，在管理控制台（MMC）中以管理单元显示。FrontPage 2000 服务器扩展、World Wide Web 管理器、文件传输协议管理器都需要 Internet 服务管理器的支撑。

■ SMTP 服务：简单网络传送协议。

此外，还包括一些文档和帮助示例文件。此时实际上相当于进行自定义安装，给用户提供了较大自由度的安装选择。用户完全可以选择部分组件安装，然后再次运行安装程序安装其它的一些组件。

安装完成后，会为 Windows 2000 提供两个新的账号：LUSR-ComputerName 和 IWAN-ComputerName，其中 ComputerName 是安装了 IIS 的计算机名称。LUSR-ComputerName 用于许可那些不能通过用户名和密码登录的用户进行匿名登录；而 IWAN-ComputerName 用于提供 Web 应用程序管理员的许可权限。

15.3 客户/服务器模型

Microsoft Internet Information Server（IIS）起到了网络服务器的作用，它响应网络客户端上所运行的 IE、Netscape 等网络浏览器发出的请求。

客户/服务器的模型在计算机网络中非常普遍。客户端发出对系统资源的请求，而服务器作为模型中的另外一个实体，对资源请求进行响应。系统资源由服务器直接管理，并且只有在接受到客户请求时才能触发服务器。

大家相当熟悉的一种客户/服务器的模型是数据库服务器，当客户端向服务器发送一个包含 SQL 查询的请求时，服务器接受这个查询，查询自己管理的数据库并找到符合要求的记录，然后将查询结果回送给客户端。除了数据库服务器外，任何这种请求/服务的操作都属于客户端/服务器模型。

IIS 是一个可以良好运转的网络服务器软件。它可以对客户请求实现多种响应。

15.3.1 静态文件

过去在 Internet 上，大多数网页都是静态文件，当有客户端对进行 Web 请求时，IIS 在硬盘上读取静态文件，

加上适当的 HTTP 标题后，传送回客户端。

15.3.2　CGI 程序

CGI 应用程序是可执行文件，当客户端请求一个应用程序时，服务器将启动这个可执行文件。一般说来，这种应用程序生成一个 HTML 页面并将之传送给 IIS，IIS 再将这个 HTML 页回送给客户端。

15.3.3　ASP 程序

ASP（活动服务器页面）程序大大丰富了网络的功能，通过 ASP 和各种脚本程序的结合，可以非常方便地实现很多过去必须用繁琐的 CGI 才能编写的功能程序。

15.4　用 IIS 配置 WWW 服务

安装 IIS 完成后，就可以在管理工具栏上启动 IIS，或者叫 Internet 服务管理器。可以通过开始菜单或者是从控制面板中找到管理工具，再从管理工具下启动 IIS，如图 15-4 所示。

从图 15-4 中可以看出，正如前节所言，IIS 支持各种 Internet 上的标准服务，比如 WWW 服务，FTP 服务，SMTP 服务等。如何利用这些服务功能，是理解和使用 IIS 的关键所在。本节首先介绍用 IIS 实现 Internet 上最普遍的 WWW 服务。

许多人对 Internet 的认识是从 WWW（World Wide Web）开始的。尽管曾经对 WWW 有过许多批评，比如因为网页传送过慢，有人把 WWW 戏称为“World Wide Wait”。但是有更多的人还是热衷于在网上冲浪，他们足不出户就可以了解世界各个角落的最新消息，而且往往比传统的报纸和电视传媒来得更快。

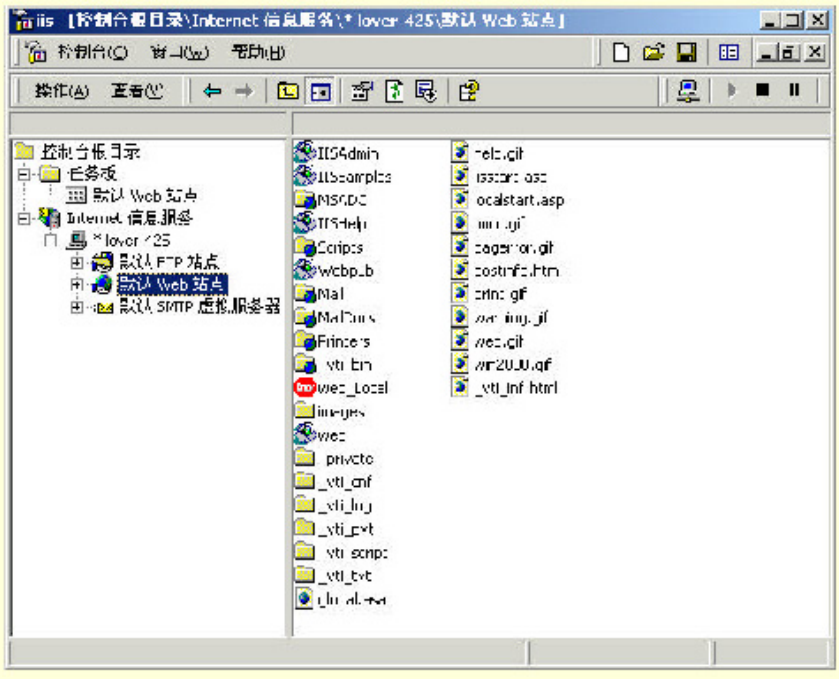


图 15-4　IIS 管理控制台

15.4.1　HTTP 协议

万维网（WWW）使用超文本传输协议 HTTP，这是一个可以为 Web 站点提供图形用户界面的协议。位于 Internet 协议栈的上层。其它上层协议包括 FTP 协议和 Gopher 协议。大家都知道 Internet 是基于 TCP/IP 协议的，这些协议间的关系可以用框图 15-5 表示。

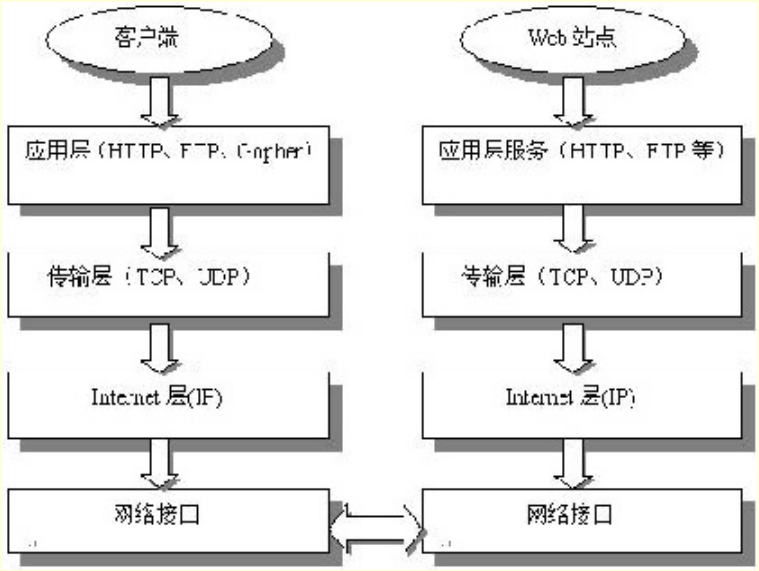


图 15-5 TCP/IP 协议栈

15.4.2 虚拟服务器

虚拟服务器可以使单台计算机实现容纳多个服务器的功能，这个功能通过在单个 IP 地址上虚拟多个服务器来实现。在安装了 IIS 后，计算机可以容纳多个域名，只要为不同的域名赋予不同的 IP 地址，就可以将它们配置成为 IIS 上的虚拟服务器主机，可以用框图 15-6 表示：

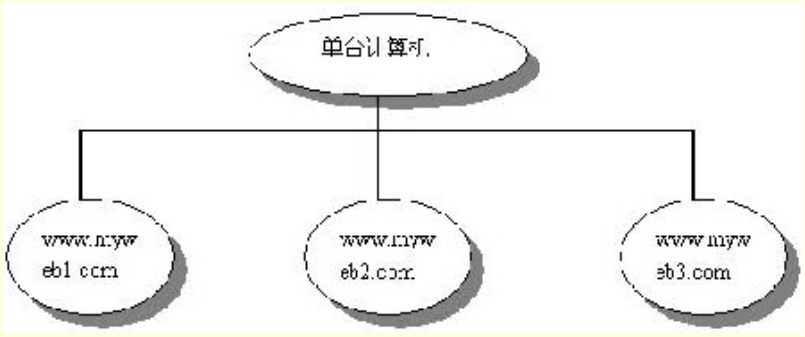


图 15-6 虚拟服务器

虚拟服务器的功能可以使一台计算机上容纳多个 WWW 服务器和多个 FTP 服务器，这样就可以不用为每个站点分配计算机和相应的软件，从这点来说，虚拟服务器相当程度上节省了资源。但是在 Windows 2000 Professional 中不支持这个功能。

但是并非一味地增加虚拟站点就是好事，使用虚拟服务器是以降低性能为代价的。必须考虑计算机上的硬件配置，不要让它承受太重的负担。

15.4.3 虚拟目录

虚拟目录是一个存放 Web 站点的主文件夹，一般说来是 Wwwroot 文件夹。另一方面，可以把虚拟目录存放在计算机的其他目录中，甚至是域中的其他计算机上，可以为虚拟目录赋予一个别名。

IIS 上的 WWW 服务器和 FTP 服务器都应该创建分别的虚拟目录。

15.4.4 配置 WWW 服务

WWW 服务有许多属性以供管理员进行具体配置。

启动 IIS 后，如图 15-4 所示，依此展开 Internet 信息服务、计算机名和默认 Web 站点。在“默认 Web 站点”节点上单击右键，然后选择“属性”，出现如图 15-7 的窗口。

这个窗口一共有 9 个选项卡，我们将依次进行介绍。

15.4.4.1　Web 站点选项卡

最先出现的是“Web 站点”选项卡，如图 15-7 所示。在本选项卡中，配置 Web 站点的标识、TCP 端口、连接限制以及是否启动安全日志。

“Web 站点标识”中，给出了 Web 站点的描述性说明，IP 地址以及 TCP 端口。

IP 地址填入的数值必须是在控制面板中定义过使用的地址。

TCP 端口确定了每个服务的运行端口，缺省值是 80，可以改动这个值，但是必须事先通知客户，否则将无法正常连接。例如，如果将 TCP 端口改为 100，那么请求将要改动为：http://WebSite_name:100/default.htm。改动端口值通常是为了不让公司外部的人员进入，从而把站点的使用限制在一个特定的用户群体中。

如果要把多个地址和端口和同一个站点相关联，单击“高级”按钮，将弹出如图 15-8 所示的高级 Web 站点配置的对话框。

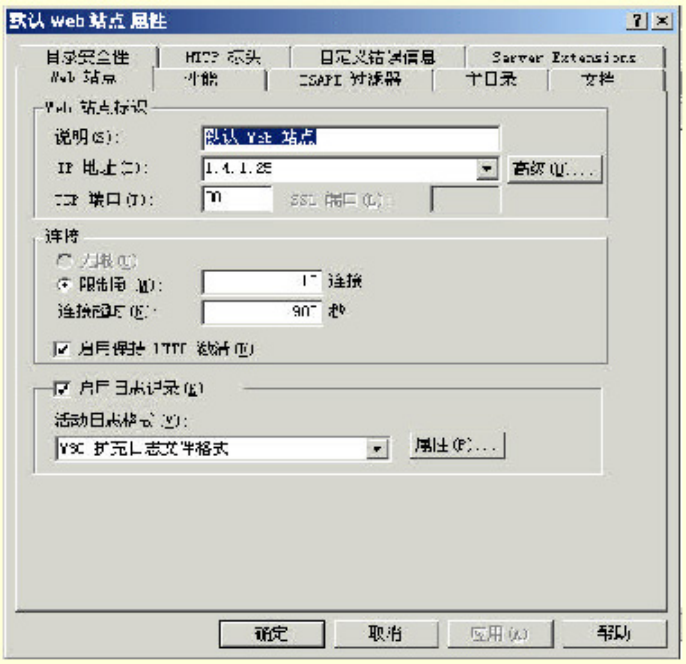


图 15-7　默认 Web 站点属性

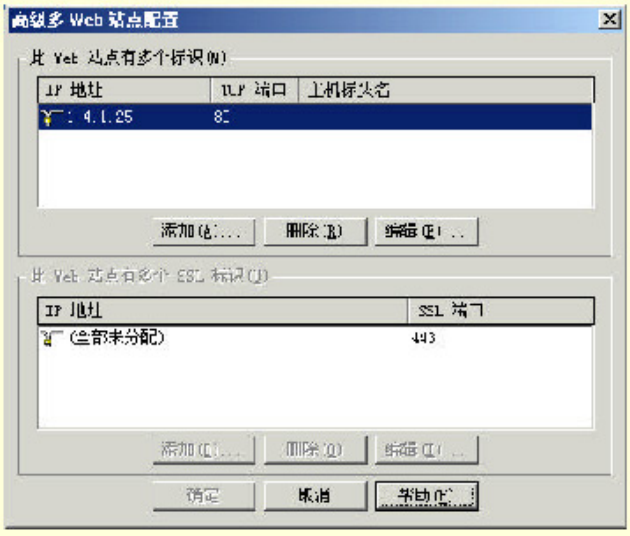


图 15-8　高级多 Web 站点配置

在 DNS 服务器中增加条目或者编辑 TCP/IP HOSTS 文件后，可以给同一个 IP 地址赋予不同的计算机名，从而区分不同的站点。例如如果有两个不同的主机：computer1.domain.com 和 computer1.domain.com，它们经过

解析后对应着相同的 IP 地址，此时浏览器必须在 IP 地址前附加主机名（比如可能是 host1:computer1.domain.com），才能得到正确的信息。这种技术叫做主机前缀名技术，与 HTTP1.1 版本兼容的客户端浏览器，比如 IE4.0 和 IE5.0，都支持这种技术，但也还有一些低版本的浏览器不支持。

由于可以虚拟多个 WWW 服务器，因此可以添加多个 Web 站点。在如图 15-8 所示中，单击“添加”按钮，出现如图 15-9 所示的对话框。

图 15-9 添加 Web 站点

根据提示输入新 Web 站点的 IP 地址、TCP 端口以及主机标头名。仍旧需要注意：IP 地址填入的数值必须是在控制面板中定义过使用的地址；TCP 端口的改动必须事先通知客户。如果作为服务器的计算机需要一个域名作为主机标头名，必须首先在域名系统中（Domain Name System，DSN）注册，然后域名服务器将注册的域名和 IP 地址进行映射，从而使要求连接域名的用户能够正确连接到这台计算机上。

可以为一个 IP 地址指定多个域名（或者说主机标头名），如果客户端浏览器能够支持主机标头名的使用，服务器可以正确地将客户路由到 Web 站点上。但如果不支持，服务器将传送一个默认的 Web 站点，一般说来，Internet 服务提供商会将自己的主页设为默认的 Web 站点，但如果没有默认的 Web 站点，客户端将出现错误消息。

SSL 端口决定了安全套接层（Secure Sockets Layer ，SSL）加密服务的端口，默认的端口是 443。同样地，这个端口值可以改动，但必须事先通知客户，否则请求将会出错。

提示：除非安装了服务的证书，否则将不会提供 SSL 加密服务。

再回到如图 15-7 所示的选项卡中，“连接”框设置了最大连接数以及连接不成功的超时时间。

选择启用日志可以启动 Web 站点的日志功能。这样可以记录用户活动的细节，同时可以选择各种不同的日志格式。日志格式包括：W3C 日志文件格式、NCSA 公共日志文件格式、Microsoft IIS 日志文件格式。

单击旁边的“属性”按钮，出现如图 15-10 所示的日志记录属性对话框，在这个对话框中设置新日志的时间间隔、日志文件目录和日志文件名，这里就不赘述了。

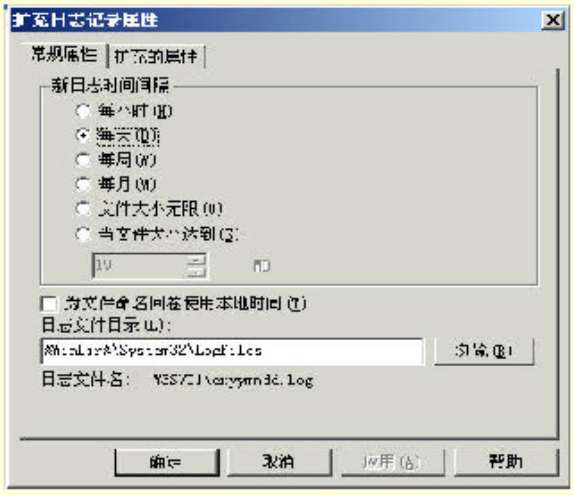


图 15-10 日志记录属性

15.4.4.2　性能选项卡

性能选项卡实现服务器对 Web 站点的性能调整。管理员应该首先估计每天连接 Web 站点的连接数量，并根据这个数值调整服务器的内存。如果估计太低，则预置的内存数不足，用户的连接可能会变得很慢；而如果估计值过高，则会造成内存闲置。

在本选项卡调整的还有启用带宽节流。

15.4.4.3　ISAPI 过滤器选项卡

ISAPI 过滤器是在 HTTP 请求事件进行时触发的 DLL 程序。对映射到一个过滤器的 URL 的请求可以激活这些程序，在选项卡中列出了每个 ISAPI 过滤器的状态（装入、未装入或者未启用）、名称和优先等级。

15.4.4.4　主目录选项卡

主目录可以理解为 Web 站点的文件所在的中心位置，缺省在安装 WWW 服务时，会将主目录安装在 \Wwwroot 路径中，这是最简单的情况。在本选项卡中可以将主目录重新设置为其它路径。可以设为本地计算机目录、网络上的其他计算机共享目录或者重定向到一个 URL 中，如图 15-11 所示。

■ 本地计算机目录：在本地路径文本框中输入详细的路径名称。

■ 另一计算机上的共享位置：输入网络中其他服务器的名称和共享名。在这种情况下，IIS 为网络中的其他计算机上的数据服务，这些计算机上就不必安装 IIS 了。在连接到远程计算机时，为了防止安全问题，可以使 IIS 要求输入用户名和密码。单击“连接到”按钮，出现要求输入身份验证的对话框，如图 15-12 所示。

■ 重定向到一个 URL：输入详细的 URL 名称。

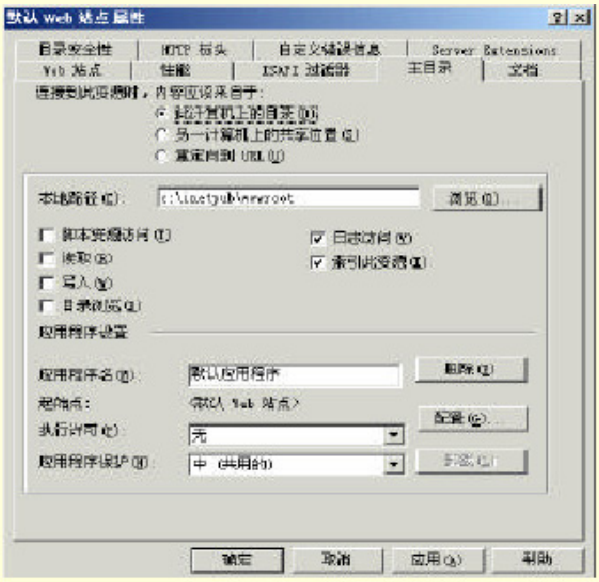


图 15-11　主目录选项卡

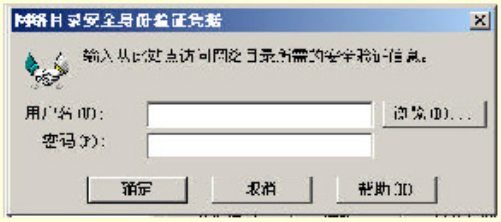


图 15-12　输入身份验证

除非选择重定向到一个 URL，都需要输入详细的路径名。

选择本地计算机目录和另一计算机上的共享位置都涉及到访问权限的问题，由图 15-11 可以看到，有如下一些复选框：选中“读取”复选框，允许 Web 客户的用户读取保存在主目录中的文件；选中“写入”复选框，允许 Web 客户的用户将文件上传到服务器中；选中“目录浏览”复选框，允许用户可以查看该目录中的文件和

子目录结构；选中“日志访问”复选框，允许在一个日志文件中记录对该目录的访问；选中“索引此资源”复选框，用户可以使用 Microsoft Index Server 快速搜索 Web 站点文档。

应用程序设置包括应用程序名、起始名、执行许可和应用程序保护（包括低、中和高）。执行许可的各个级别如下：

■ 无：任何程序或者脚本都无法在该目录下运行。

■ 纯脚本：启用一个脚本在目录下运行。

■ 脚本和应用程序：允许任何应用程序，包括脚本、.exe 和.dll 文件。

单击右边的“配置”按钮，进一步设置应用程序，包括应用 ASP 脚本在客户端和服务器端调试，传送错误消息等。

15.4.4.5 目录安全性选项卡

本选项卡用于为 Web 站点设置匿名访问和认证控制、安全通信和 IP 地址和域名验证。

匿名访问和认证控制用以启用匿名访问和编辑认证控制的方法。单击右边的“编辑”按钮所示，如图 15-13 所示。

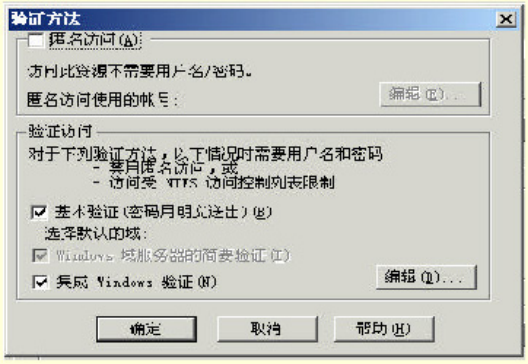


图 15-13 控制匿名访问

如果没有选中“匿名访问”复选框，将不能实现对 Web 站点的匿名访问；反之，如果选中了“匿名访问”复选框，将可以进行匿名访问。缺省时，在安装 IIS 中，会提供 IUSR_computername 账号以供匿名访问。管理员可以进行账号配置，单击右边的“编辑”按钮，如图 15-14 所示。

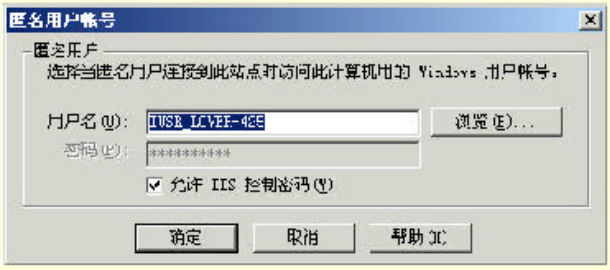


图 15-14 设置匿名用户账号

管理员可以重新设置匿名访问的账号，单击“浏览”按钮，选择现有的用户账号作为匿名用户名。匿名用户的密码可以由 IIS 控制，也可以由管理员自己设定。为了避免密码混乱，可以告诉 IIS 在这两个存储地点同步的密码变化。

如果不允许匿名访问，或者访问受到 NTFS 访问控制列表的限制，此时与 Web 站点的连接就需要输入用户名和密码。

客户端浏览器素提供的用户名和密码经过服务器认证，支持认证过程的方案有两种：

■ 基本验证（Basic Authentication）：基本认证使用一种称为 Base 64 的基于 64 进制的加密方法。这种加密方法使用 64 位进制对所有的字符进行编码，然后用纯文本的格式（明文）传送。需要注意的是：基本验证的方法并不安全，密码在网络上传输时，黑客可以使用协议分析器在验证过程中检查用户密码，因此是不安全的。系统将出现如图 15-15 所示的警告。

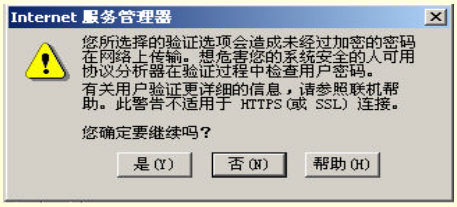


图 15-15　对基本验证的警告

■ 集成 Windows 验证：一种更为安全的验证方式。

安全通信选项使用密钥管理器来创建一个证书请求，关于密钥在后面还将继续介绍。

15.4.4.6　文档选项卡

本选项卡用于配置 Web 站点的缺省文档和文档页脚配置。

如果一个对 Web 站点的客户请求没有明确指定所需要的 Web 页，则服务器将自动把缺省文档传送给客户。一般系统会设置 Default.htm 或者 Default.asp 页为默认文档，如图 15-16 所示。

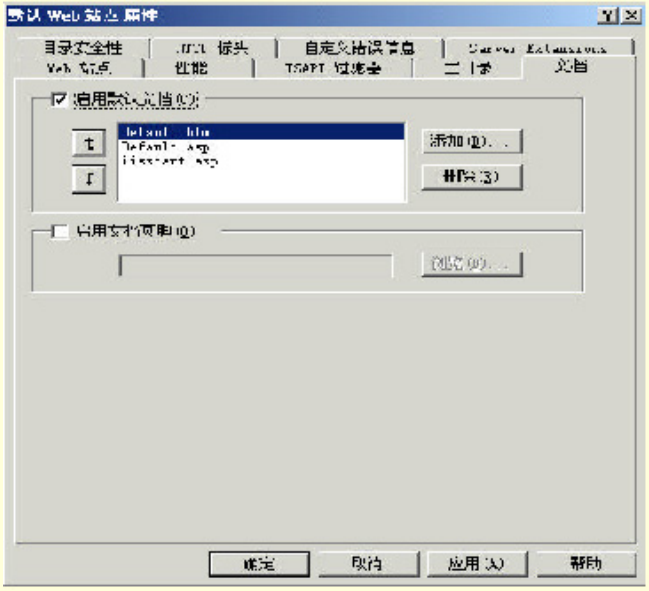


图 15-16　默认文档

在默认文档列表中，可以调整它们的先后次序，系统将依照优先次序查找这些文档。单击“添加”按钮，可以添加默认文档。

15.4.4.7　HTTP 标头选项卡

使用本选项卡启动内容失效，以及失效的时间。管理员还可以单击“添加”按钮，定制给客户端发送的 HTTP 标头，同时在标头中输入关于等级的描述信息。如图 15-1 所示是关于分级的启用信息。

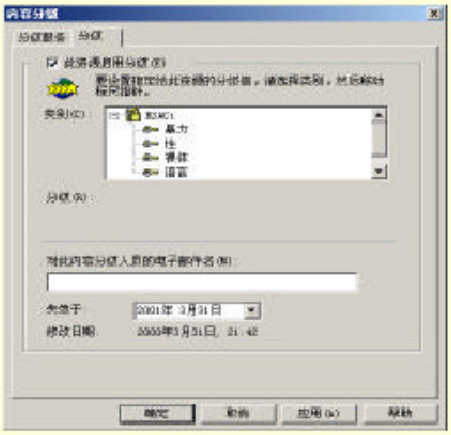


图 15-17　内容分级

IE3.0 或者更高版本的浏览器可以支持检查内容标签，这样就可以帮助用户识别目标网站内容的等级和种类。

还可以在本选项卡中自定义 HTTP 头信息：在自定义 HTTP 头框旁单击“添加”按钮，如图 15-18 所示，可以添加或者编辑 HTTP 头信息，这样服务器将可以向客户端传送这些附加信息。相反，如果要删除某一个 HTTP 头信息，可以在本选项卡中单击“删除”。

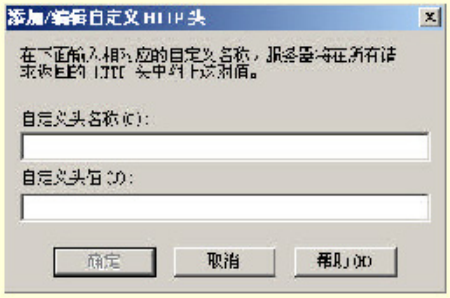


图 15-18 添加自定义 HTTP 头

15.4.4.8 自定义错误信息选项卡

IIS 在报告错误方面有很强的灵活性，如图 15-19 所示是自定义错误信息选项卡。

当错误发生时，IIS 服务器向客户端传送错误信息，这些信息以 HTTP 状态码形式传送，可能还会包括一些消息文本，这样一来用户可以检查错误的根源。

在如图 15-19 所示的选项卡中，可以配置与错误相关联的信息文本，包括类型代码、错误类型和关联的文件位置。

可以配置自己的错误信息，方法是：选中某一个 HTTP 错误代码，单击下方的“编辑属性”按钮，如图 15-20 所示。在消息类型下拉表中，选择文件默认值或者 URL，如果选择了文件，可以单击“浏览”按钮，选择相应的 htm 文件。

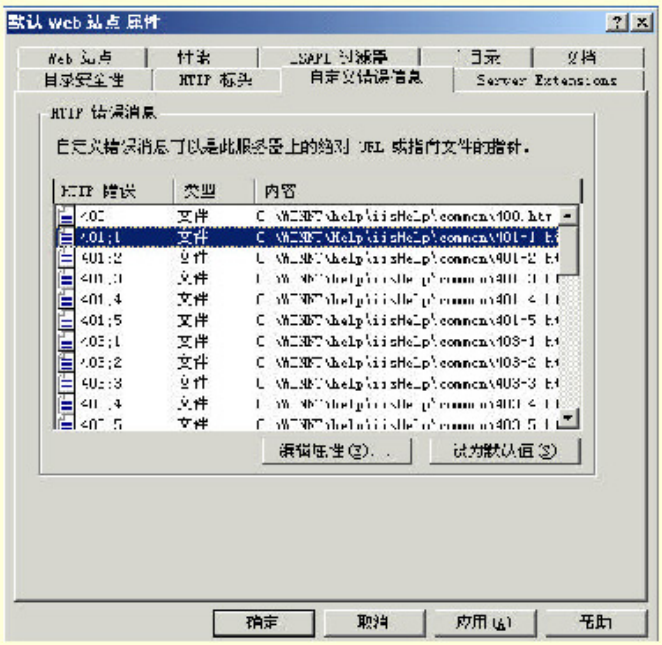


图 15-19 自定义错误信息

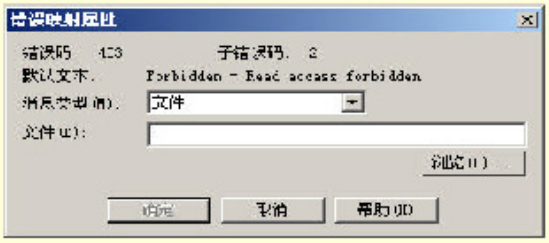


图 15-20　自定义错误信息

15.5　建立新 Web 站点

在 IIS 中，很容易就可以建立一个新的 Web 站点。可以在默认 Web 站点或者根站点下的某个子站点下建立新的站点。

选中某个站点（将成为父站点），单击鼠标右键，从快捷菜单中选择“新建”→“服务器扩展站点”命令，如图 15-21 所示。

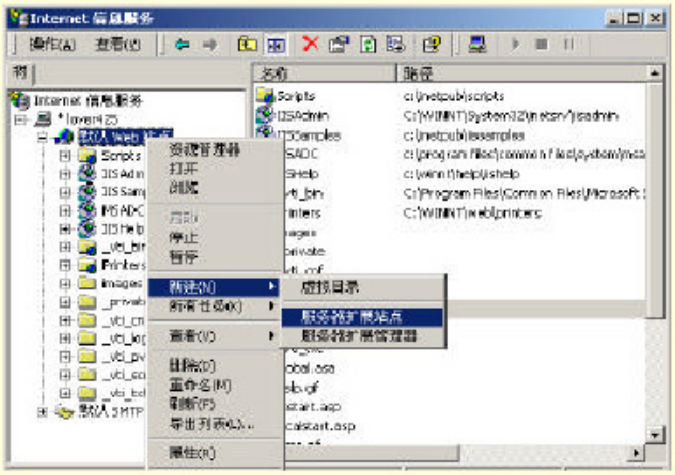


图 15-21　建立新 Web 站点

系统将调出建立新站点向导，根据向导要求，输入新站点的目录（目录不能重复）和标题。向导的第二步要求选择新站点的管理员，默认是采用其父站点的管理员，这时候子站点继承父站点的安全设置。

也可以选用其他用户成为其管理员，此时要求输入严格的 Windows 账号。Windows2000 提示建立 3 个基本命令组：*websitename* Admins、*websitename* Authors、*websitename* Browsers 并用新命名的目录名（*websitename* ）作为基本名。向导运行完毕后，可以利用本地用户和组将拥有权限的用户添加到这些组中。

如图 15-22 所示是向导完成后的新站点创建介绍。

图 15-22　完成新建子站点向导

单击“完成”后，新站点建立完毕，可以在 FrontPage 服务器扩展中看到这个新站点。Microsoft 提供了 FrontPage 和 Visual Interdev 两个工具开发完整的 Web 站点，FrontPage 具有强大的 WYSIWYG（What You See Is What You Get）功能，也就是所见即所得的功能，即使是不熟悉 HTML 语言的人也可以利用这个工具开发出漂亮的站点。而 Visual Interdev 具有更强的专业功能，可以使用 VBScript 和 JavaScript 等脚本编程，同时附加有强大的 ActiveX 和服务器组件，并且利用 ASP 快速编制灵活的交互性页面。Visual Interdev 也是 Visual Studio 的最新组件。

15.6 用 IIS 配置 SMTP 服务

电子邮件可以说是 Internet 最早的用途之一，它比 WWW 出现的更早。直到今天，它仍然是 Internet 中使用最为广泛的用途之一，有许多人认为电子邮件是上网最实用，最有效的工作。过去，由于没有今天这样多的电子邮件程序提供丰富的图形界面，人们使用命令行来发送电子邮件，比如 UNIX 环境下的一些程序。今天，像 Outlook 这样的程序已经极大地改善了这种情况。然而大多数电子邮件的发送仍是基于简单邮件传送协议（SMTP）的，本节介绍 IIS 中的 SMTP 服务功能。

15.6.1 邮件传送机理

首先，用户从一个 Outlook 或者其他的客户程序端发送电子邮件，它们的第一个目的地是本地的 SMTP 服务器。之所以说第一个的原因是：每一个 SMTP 服务器都有自己的“管辖”域，如果该电子邮件要传送到的地址在本管辖域中，服务器只需要将它存放在特定的目录中，并发送到客户用户的邮箱中即可；如果地址不在本 SMTP 服务器的管辖域中，它就必须执行 DNS 查找对应的 SMTP 服务器，并且建立二者之间的网络连接，然后通过 SMTP 协议发送这个电子邮件。

需要注意的是：客户端只认识本地的 SMTP 服务器，如果是跨域传送，也必须借助本地服务建立连接，而无法直接发送。客户端将邮件传到本地 SMTP 服务器后，就不用再操心了。

另一方面，用户需要借助 POP3 服务器来收取自己的电子邮件，POP3 协议用于将邮件从 SMTP 服务器中传送到客户端的计算机当中，但是它与 SMTP 服务并没有联系，也就是说，SMTP 服务器负责发送邮件，而 POP3 服务器负责接受邮件。用户在试图进入自己的邮箱接收邮件时，必须向 POP3 服务器提供自己的用户名和密码，经过验证后方能查看邮箱并提取自己的邮件。

15.6.2 SMTP 服务组成

安装 SMTP 时，系统默认的路径是 c:\Inerpub\Mailroot，之后在此目录下再建立以下目录，完成各自的功能：

- Badmail 目录：用以存放发生特殊情况无法传送的电子邮件。
- Drop 目录：存放所有输入的邮件报文文件。
- Pick 目录：SMTP 服务器将存放在本目录的邮件立即传送出去，或者传到 Drop 目录（本地）中，或者传到其它域的 SMTP 服务器中，这样一来就可以简化外部邮件服务。
- Queue 目录：如果出现了网络故障或是其它一些原因，使得无法正常发送邮件，SMTP 服务就会把邮件存放在这个目录中，一段时间后再尝试传送。
- Route、SortTemp 以及 Mailbox 目录：将邮件进行排序和整理，以提高效率。

15.6.3 配置 SMTP 服务

SMTP 服务与 WWW 服务同处在 IIS 的管理界面中，它们的管理树都十分相似，如图 15-23 所示。缺省时，当系统启动后，SMTP 服务自动启动，也可以手动停止或者重新启动服务。如图，在默认 SMTP 虚拟服务器中，单击鼠标右键，从快捷菜单中，选择停止或者暂停命令即可，此外工具栏上也有相应的工具按钮（方形黑按钮）。

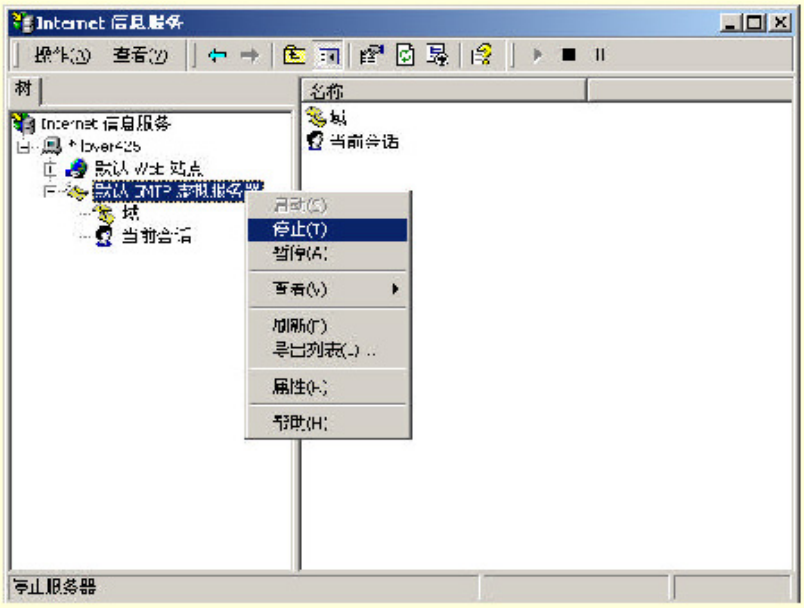


图 15-23　SMTP 服务及其停止

前面已经提及，域是 SMTP 服务组织的单位。SMTP 虚拟服务器至少有一个域：本地（默认）域。可以添加其他域并将其配置为本地域或远程域。可以删除所创建的任何域，但不能删除默认域。如果计算机没有加入一个域名系统，则使用默认域。此时此计算机名默认就是用于电子邮件的 SMTP 服务域名。

如图 15-23 所示，在默认 SMTP 虚拟服务器中，从快捷菜单选择“属性”命令，则出现类似 WWW 服务的属性表单，进行默认域 SMTP 服务的配置。

将图 15-24 与图 15-7（默认 Web 站点属性）进行比较，可以看出它们十分相似，在这里进行一些基本的设置，包括默认 SMTP 服务的名称，IP 地址以及是否启用日志记录。这些设置大多与 WWW 服务中的配置相似。首先是常规选项卡。

15.6.3.1　常规选项卡

如图 15-24 所示，单击右边的“高级”按钮，可以为计算机配置多个 IP 地址，默认情况下，SMTP 服务会对所有计算机中配置的所有 IP 地址的连接请求响应。单击“连接”按钮，可以设置待发和待收连接的控制，如图 15-25 所示。

图 15-24　常规选项卡

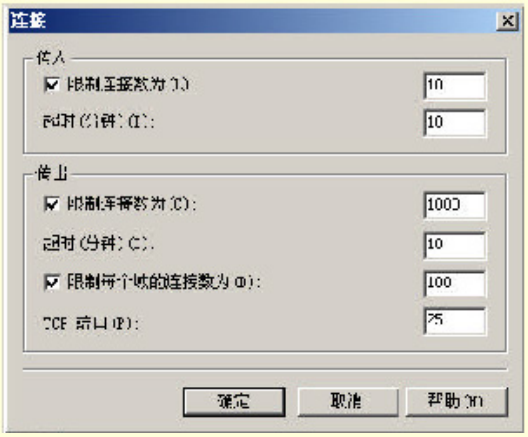


图 15-25 连接属性

在如图 15-25 中，设置最大传入数、最大传出数以及它们的超时时间，根据网络的流通理论，最大传入数不应该超过最大传出数，否则可能造成这个节点的堵塞崩溃。

SMTP 服务器的默认 TCP 端口地址是 25，和 WWW 服务中的情况类似，不要随便改动这个数值，除非事先通知客户。

SMTP 服务中也有日志格式的选择，在图 15-24 中，选中“启动日志记录”复选框，这样就可以通过记录跟踪 SMTP 虚拟服务器从网络接收 SMTP 客户端的命令，可以有 3 种日志格式，分别是：

■ W3C 扩充日志文件格式（默认选项）：采用 ASCII 格式并且可以自定义设置需要跟踪的项目（单击“属性”按钮）。

■ Microsoft IIS 日志文件格式：固定的 ASCII 文件格式。

■ ODBC 日志格式：采用符合 ODBC 规范的数据库，存储日志记录。

单击属性按钮，可以进一步配置各日志文件的记录方案，包括记录间隔日志文件大小以及存放的路径等。

15.6.3.2 访问选项卡

访问选项卡如图 15-26 所示，用以配置对 SMTP 虚拟服务器的客户机访问以及建立传输安全性。

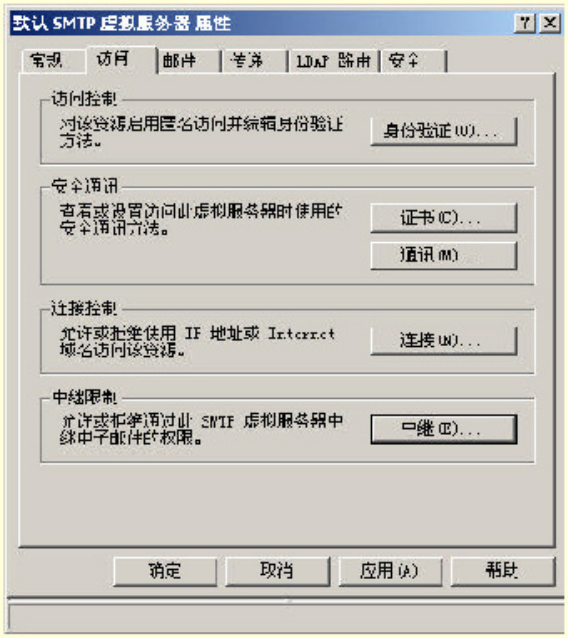


图 15-26 访问选项卡

使用“访问控制”，可以配置 SMTP 服务以允许匿名访问或提示用户输入用户名和密码。单击“身份验证”按钮，可以选择一个或多个身份验证方法。

■ 匿名访问：可以使用匿名访问目录内容的所有客户机，如果再清除其余选项，就可以使 SMTP 服务不进行身份验证。

■ 基本（明文）验证：要求输入用户名、密码以及所属 Windows 2000 域信息，但这时用户名和密码都以明文传送，这是很不安全的。为此可以选用“需要 TLS 加密”复选框，建立网络传输层的加密。

■ Windows 安全程序包：启动 Windows2000 提供的标准“安全程序包”安全机制，使用加密技术验证用户身份，不需要用户传送实际密码。

一旦授予访问权限，就能用“安全通讯”为虚拟服务器设置安全性。单击“证书”按钮可以启动向导帮助创建一个新的证书或者导入一个证书。

单击“通讯”按钮，可以进行邮件传送方面的通讯安全保护，如图 15-27 所示。

选择“需要安全通道”，要求服务器之间启用“传输层加密”（TLS）以确保接收数据被加密。如果使用 TLS 加密，则必须创建密钥对并配置密钥证书，这时的传送过程是这样的：客户端将邮件进行加密并提交给 SMTP 服务器，SMTP 服务器在接收端进行解密。

密钥对由表明密钥安全级别的许多位组成，默认的级别是 40 位。位数越高，该密钥解码的难度越大，而且试图保护访问的用户必须使用设置相同的加密级别。如图 24 所示中有启用 128 位密码的选项，但是由于技术出口限制，128 位密码仅限于美国和加拿大。

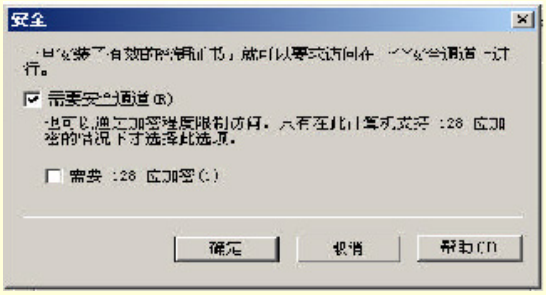


图 15-27　启用安全通道

“连接控制”允许通过客户机的 IP 地址或域名来限制对 SMTP 虚拟服务器的访问。可以将访问权限授予所有计算机，然后再作为特殊情况拒绝某些特定计算机的访问权限。同样，如果拒绝了所有计算机的访问权限，仍然可以再将访问权限授予某些特定的计算机。

另一方面，如果需要防止处理不必要的邮件，可以用“中继限制”阻止对虚拟服务器的中继访问。但是如果 SMTP 虚拟服务器连在 Internet 上，则建议不要使用中继，否则虚拟服务器可能会中断传送强行送交的推销邮件。

15.6.3.3　邮件选项卡

邮件选项卡用以邮件大小、会话大小、最大连接数、每个邮件最多接收人数等设置，如图 15-28 所示。请注意会话大小应该超过邮件大小的设置。当发送邮件字节数超过了限制，将收到错误信息。默认的邮件大小是 2048KB，默认的会话大小是 10240KB。

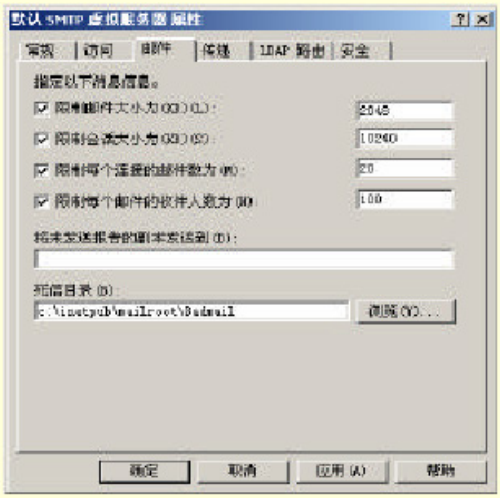


图 15-28　邮件选项卡

在下方有两个文本框：副本目录和死信目录。前面说过，当网络发生故障或其他原因造成邮件无法及时传送时，SMTP 服务器将这些邮件送回到发件人的信箱中，并且回送一个 NDR 报告，邮件的副本保存在副本目录中，并稍后再发。

如果一封邮件重发的次数超过了限制，将视为死信，存放到死信目录中。存放到死信目录中的邮件既无法发送也无法回送，是名副其实的“死信”。死信增多后会降低服务器的性能，因此应该定期检查并清除。在默认情况下，副本目录没有指定，而死信目录是 c:\inetpub \mailroot\Badmail，可以改变这个目录。

15.6.3.4 传递选项卡

传递选项卡设置所有的发送选项，包括设置发送邮件的重试间隔、延期通知和过期超时限制等，如图 15-29 所示。

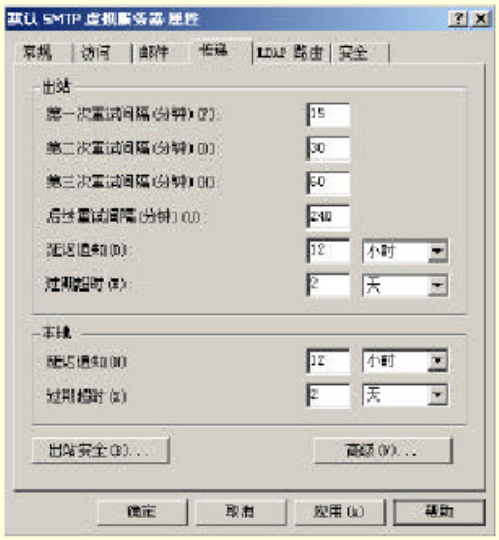


图 15-29 传递选项卡

单击“高级”按钮，设置邮件发送的路由选项。例如限制发送时到服务器的跳跃总数，确定用来在“从”栏中代替发件人原始域名的虚拟域名等，如图 15-30 所示。

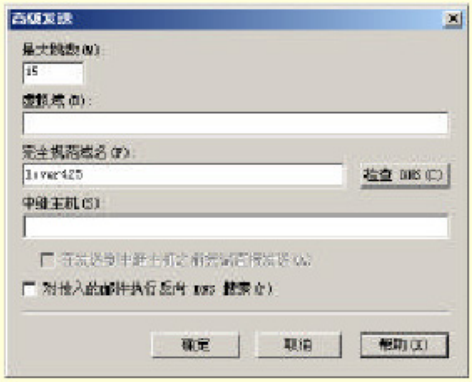


图 15-30 高级发送

如前所述，非传送给本地域目标的邮件可能会经过许多不同的域才能到达目标地，由于每经过一个服务器，都会在邮件头部进行处理并添加自己的信息，因此查看邮件头部的接收字段就能够确认它的跳转数，默认的最大跳转次数是 15 次。当跳转数超过了设置值时，邮件将被传回给发件人，并附加一个未发送报告 NDR。

在电子邮件中，存在邮件欺骗，即伪装发件人的行为。可以在 SMTP 服务器中指定反向查找头部信息是否匹配来制止这种行为。但是这种功能需要以降低服务器的性能为代价，对一个繁忙的 SMTP 服务器这项设置未必可取。

这些设置都可以在单击“高级”按钮后的对话框中进行设置。

15.6.3.5　LDAP 路由选项

使用本选项卡来指定用于该 SMTP 虚拟服务器的目录服务服务器的标识和属性。该目录服务将存储有关邮件客户及其信箱的信息。SMTP 虚拟服务器使用“轻便目录存取协议”(LDAP) 来与该目录服务进行通讯。

若要激活 LDAP 路由，请选择“启用 LDAP 路由”复选框。然后可以配置下列选项：服务器、架构、绑定、域、用户名、密码、库。

15.6.3.6　安全选项卡

使用“安全”选项卡可将 Windows 2000 中的账户和组添加到 SMTP 虚拟服务器操作员列表。默认的操作员是系统管理员 Administrator，如图 15-31 所示。

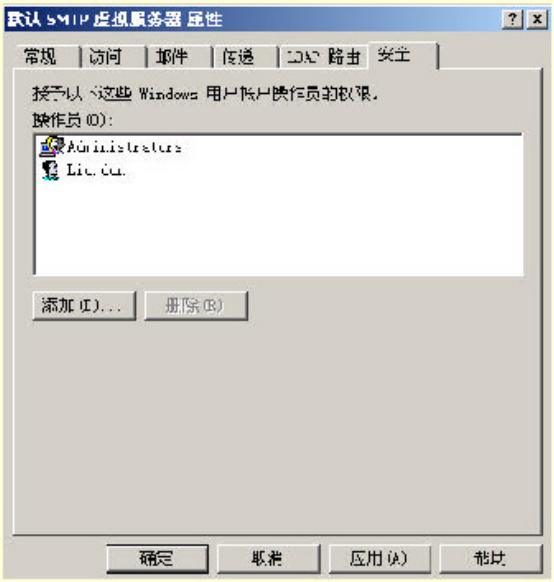


图 15-31　安全选项卡

15.6.4　新建域

可以非常方便地利用向导创建本地域的别名或者远程域。这只需要在域节点上单击右键，从快捷菜单中选择“新建”→“域”命令，就可以启动向导，如图 15-32 所示是选择域名。

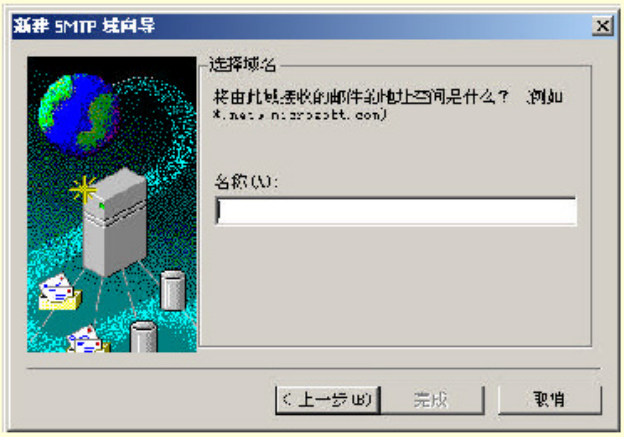


图 15-32　选择域名

每台计算机上只能有一个默认本地域，因此所创建的本地域都将成为默认本地域的别名。如果使用的是伪装域，别名可以起到重要的作用。

15.7 用 IIS 配置 FTP 服务

网络的重要功能之一在于它方便的文件共享能力。在文件共享一章里已经提过，在 Windows 中，可以通过网上邻居、映射网络驱动器等方法方便地实现资源共享。但是还是应该看到，不同操作系统之间存在平台共享的兼容性问题，比如像 UNIX、Macintosh 客户机就没有办法像 Windows 操作系统那样简单地实现网络驱动器的映射。

这种情况使人们重新想起了文件传输协议（FTP，File Transfer Protocol）。FTP 在传输层使用 TCP 协议，这是一个面向连接的协议，可以保证数据传输的可靠性。毫无疑问，FTP 在 TCP/IP 和 Internet 上使用的最古老的协议之一，尽管如此，它仍是在计算机之间实现传输程序和数据的更有效的办法。正因为 FTP 的使用的方便性，许多大型站点都设有自己 FTP 站点，比如 ftp.microsoft.com 等。许多用户通过登录公用的 FTP 站点，以获取最新的软件版本、程序范例、教学文档等资料。

今天 WWW 服务已经取代了 FTP 的许多功能，但是 FTP 仍然用于在客户/服务器间拷贝文件，此时一台计算机充当 FTP 客户机，而另外一台计算机充当 FTP 服务器，尽管往往是远程传输数据，但看起来数据却好像储存在本地一样。IIS 可以管理 FTP 服务器，而 FTP 客户端软件也很容易获得。

下面就来看看如何管理 FTP 站点。

15.7.1 默认 FTP 站点属性

15.7.1.1 FTP 站点选项卡

默认 FTP 站点的管理也是通过属性表单进行的。如图 15-33 所示是 FTP 站点选项卡。它与 WWW 站点、SMTP 站点十分相似，比如对于显示在 IP 地址框中的地址，同样必须先在“控制面板”中定义为可使用。稍有区别的是 FTP 站点的默认 TCP 端口是 21。其他如说明、连接限制、超时、日志格式等配置都与前面相近，很容易理解。

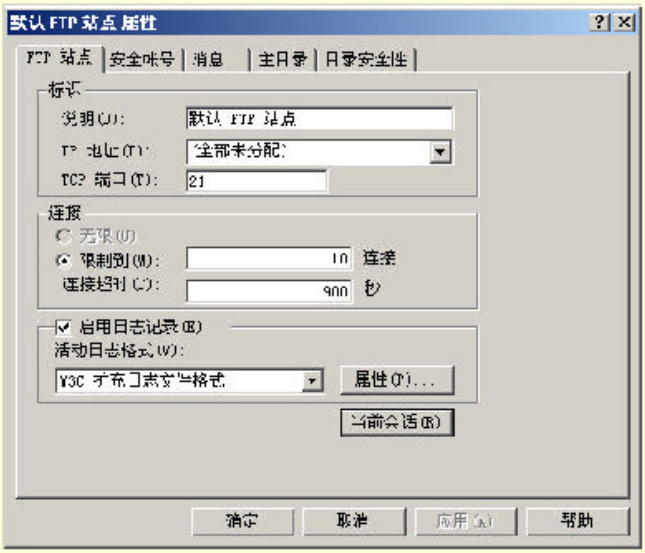


图 15-33 FTP 站点选项卡

在这个选项卡中可以显示所有的会话信息，单击当前会话按钮，就可以显示当前登录的用户列表，对匿名登录的用户一般通过电子邮件地址予以区别。也可以切断当前部分或者所有会话。

15.7.1.2 安全账号选项卡

如图 15-34 所示是安全账号选项卡，在这里设置是否允许匿名访问、FTP 站点操作员等安全控制。这些与 WWW 站点中的设置也基本相同。一般都会设为允许匿名连接，以防止用户名和密码在网络传输中被截获。

图 15-34　安全账号选项卡

15.7.1.3　消息选项卡

消息选项卡中包含了进入和退出 FTP 站点，以及由于达到最大连接数的标题消息。可以在这里输入一些警告性的标题，比如管理员对站点内容不负责等信息。

15.7.1.4　主目录选项卡

在“主目录”选项卡中，对 FTP 站点的主目录进行配置。默认情况下，FTP 站点的本地路径是 C:\inetpub\ftproot，如图 15-35 所示。可以改变为计算机上的其他目录，也可以设置为另一计算机上的共享目录。

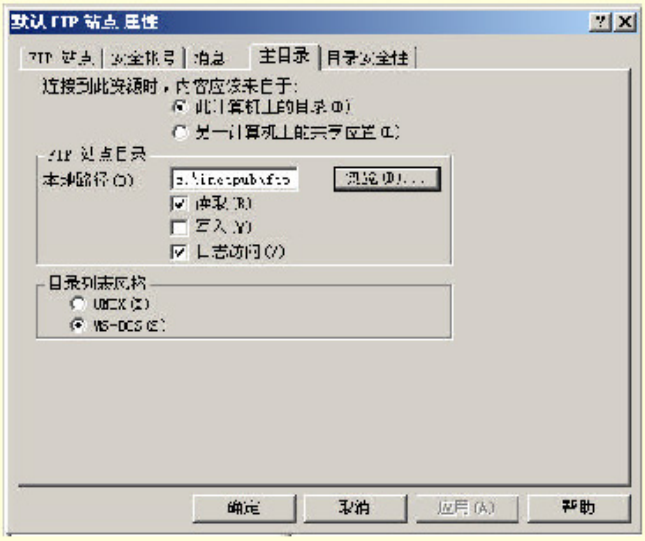


图 15-35　主目录选项卡

权限设置包括读取、写入、日志访问，读取权限允许客户机下载文档，写入权限允许客户机上传文档，这些都是 FTP 站点的重要功能。

15.7.1.5　安全目录选项卡

利用本选项卡配置访问限制，来阻止某些个人或群组访问 FTP 服务器。

15.7.2　添加虚拟目录

用户可以不用局限于仅通过缺省的 FTP 根目录访问文件，通过添加虚拟目录可以为用户设置其他可以使用的目录。IIS 向导可以非常方便地帮助添加虚拟目录。在默认 FTP 站点上单击右键，选择“新建”→“虚拟目录”命令，就可以启动向导。

向导将要求输入新虚拟目录的别名及物理路径，以及允许的权限（读取或者写入）等。设置完成后，用户

将可以连接这个目录进行访问。

15.7.3 连接 FTP 站点

可以在浏览器中直接连接 FTP 站点，这只需要在地址栏中，键入要连接的 FTP 站点的 Internet 地址，例如 ftp://ftp.microsoft.com/ 即可。

在许多 FTP 站点上，都可以自动匿名登录，从而查看或下载文件。但是如果需要上载、重命名或删除文件，有可能需要使用其他用户名和密码登录。同时，相同站点的不同区域也可能需要进行不同的登录。以其他用户身份登录到此 FTP 站点的方法：选择“文件”→“登录”菜单命令，如图 15-36 所示。

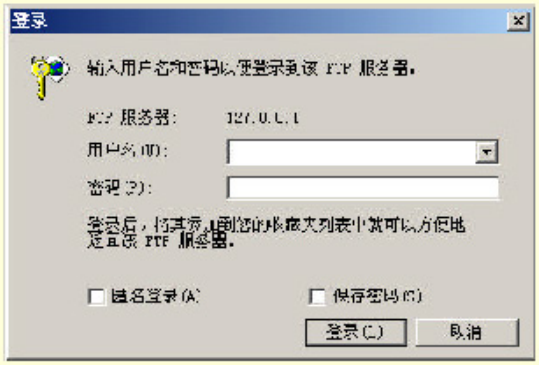


图 15-36 以其他用户身份登录

也可以通过命令行，只需要在提示符下输入 ftp，就可以打开一个 FTP 会话。ftp 命令类似于 DOS 命令，也有 cd、dir、delete 等命令，熟悉 DOS 的用户可以很方便地使用 FTP 会话，此外可以通过帮助查阅 ftp 命令，比如可以使用 put 命令上载文件，用 get 命令下载文件等。

第 16 章　审核

审核是系统安全的重要保障，就像公司或者企业需要查账以确认收支平衡一样，Windows 2000 操作系统也需要审核来帮助检查是否存在安全或者性能等其他方面的问题。对于一个规模较大的组织，Windows 2000 可以帮助管理员制定完善的安全保护体系，但是由于各种可能性，时间一长，仍然会存在这样那样的漏洞。这时候，可以通过审核及时发现问题并把漏洞补上。

管理员的一个重要任务是设计一个合理的审核计划，必须清楚哪些事件需要审核？哪些资源需要特别的保护？或者，哪些人是不被信任的，需要对他们的行动时刻保持警惕。Windows 2000 有完备的审核功能，并能产生数量惊人的审核记录，管理员应该做到心中有数，这样才能从众多的数据中筛选出有用的东西。如果不分青红皂白，事无巨细地要求系统审核，不但严重影响系统的性能，使之无法正常工作，管理员也很难找到真正值得注意的问题。因此，制定一个合理的审核计划是相当必要的。此外，如果这个公司对安全性有相当高的要求，就应该考虑加强审核的力度，否则就没有必要给系统添加太重的负担。

下面是一些管理员可能需要注意的事件：服务启动失败、磁盘满、用户注册和注销、不成功的登录、重要策略的改变、特殊权限的使用、程序非正常运行等等。管理员应该对这些事件予以足够的重视，同时还有其他许多重要的信息和警告，管理员应该在审核时捕捉这些信息并给出相应的对策。

本章内容包括：

- 事件查看器
- 查看和管理日志审核
- 安全日志满时暂停计算机

16.1　事件查看器

Windows 2000 使用事件查看器帮助审核，事件查看器与本地用户和组、共享文件夹、系统信息、性能日志和警报、设备管理器等管理单元同属于管理工具下的计算机管理中的系统工具节点，展开这个节点，就可以发现事件查看器工具。

在事件查看器中使用的是事件日志，通过日志收集和记载有关硬件、软件及系统问题方面的信息，并监视 Windows 2000 安全事件，这样管理员就可以通过查看日志仔细检查审核的项目。因此，为了顺利完成审核并取得预期的成果，管理员应该首先熟悉事件查看器的使用。

组成事件查看器的 3 种日志是：应用程序日志、系统日志和安全日志，分别对应于事件查看器下的 3 个节点，可以在 3 种视图中进行切换，以选择不同的日志。它们的功能分别是：

■ 应用程序日志：应用程序日志包含由应用程序或一般程序记录的事件。例如，数据库程序可以用这个日志来记录文件错误。

■ 系统日志：系统日志包含由 Windows 2000 系统组件记录的事件。例如，在系统日志中记录启动期间要加载的驱动程序或其他系统组件的故障。

■ 安全日志：使用安全日志记载系统的各种安全事件和资源使用的情况。

在文件权限管理一章中，已经着重谈过了使用安全日志记载诸如有效和无效的登录尝试、成功或者失败地访问资源对象、取得对象所有权、特权使用等安全事件。值得特别注意的是：安全日志只有管理员可以查看，而任何用户都可以查看应用程序日志和系统日志。而且缺省情况下，安全日志是关闭的，管理员必须启动安全日志并且通过对组策略中安全审核的设置来决定安全日志记载的具体项目。有关安全日志的使用问题，可以参见文件权限与管理一章。

系统日志与应用程序日志的使用与安全日志很相似，它们的界面也基本一样，如图 16-1 中显示的是系统日志。

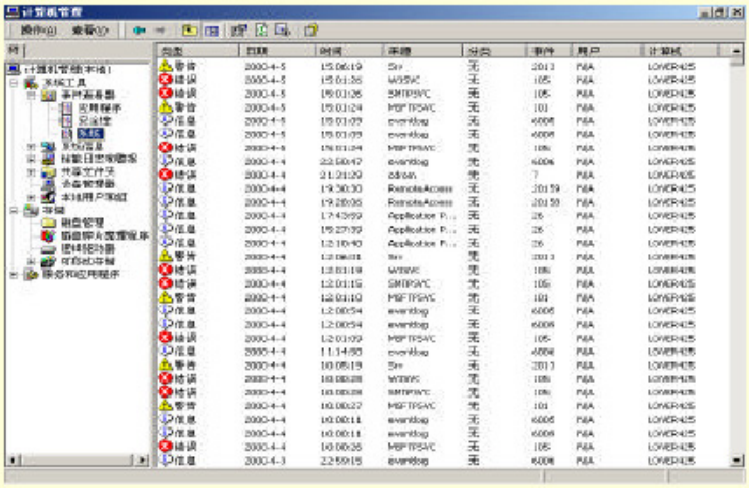


图 16-1 系统日志

16.1.1 了解事件查看器界面

虽然如图 16-1 显示的是系统日志界面，但应用程序日志和安全日志的界面也是统一的。从图中可以看到，日志中记载着许多条记录，组成这些记录的字段是：类型、日期、时间、来源、分类、事件、用户和计算机。

类型又可以分为 5 种，在系统日志和应用程序日志中的类型是错误、信息和警告，而安全日志使用的类型是成功审核和失败审核。

- 当数据丢失或功能丧失等重要的问题产生，例如启动服务失败，则会产生一个错误事件。
- 警告事件当不是非常重要但将来可能出现的问题出现时产生，常见的警告事件比如有磁盘空间不足。
- 信息事件用来描述应用程序、驱动程序或服务的成功操作的事件。例如，成功地加载一个驱动程序。

相应地，成功审核和失败审核用来审核安全尝试是否成功，二者在文件权限管理一章中已有详细介绍。

从图 16-1 中可以看出，这些类型使用的是不同的标志，错误是一个红色的叉号，警告是一个黄色的惊叹号，成功审核的标志是一把钥匙，而失败审核使用一把锁表示。

在图 16-1 中还可以通过日期、时间、来源、分类、事件 ID、用户和计算机等字段帮助了解信息，例如如果同时管理多台计算机，则计算机名称这个字段就很有用。

默认情况下，事件查看器中各条记录的排列是依照时间顺序排列的，可以改变为按照其他字段进行排序，这时的操作类似于资源管理器中的操作。单击某个字段，就可以依照这个字段排序，再次单击，则反序排列。可以用这个方法更快地找到所需的信息。

16.1.2 选择查看字段

如图 16-1 所示的众多字段中，并不是每个都是必要的，有时候去掉几列，反倒可能更有利于集中精力，发现重要信息。选择查看字段的方法是：从管理控制台中选择某一个日志节点，单击右键，从快捷菜单中选择“查看”→“选择列”命令，如图 16-2 所示。

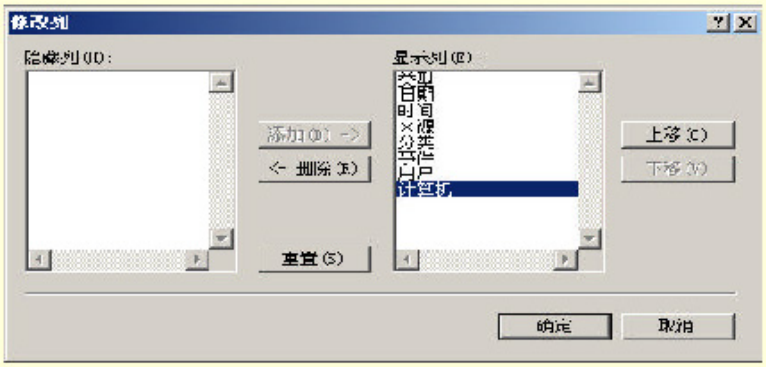


图 16-2 选择列查看

如图 16-2 中，选定某个字段后，单击“ 删除 ”按钮，这个字段就出现在隐藏列中，这样在事件查看器中就实现了隐藏。同时通过“ 上移 ”和“ 下移 ”还可以调整各列的顺序。

16.1.3　查看事件详细信息

在图 16-1 所示的列表中，只能查看到各种事件的大致信息。一般管理员可以在列表中粗略地浏览，如果某条消息引起了注意，可以双击这条消息，或者单击鼠标右键，选择“ 属性 ”命令，以查看详细信息，如图 16-3 所示。

在图 16-3 中，给出了事件的详细描述（磁盘几乎满载），可以帮助了解详细信息，单击向上或者向下箭头，可以查看上一条或者下一条信息。

详细信息中还提供了二进制数据的查看方式，要查看作为字符的二进制数据，单击数据框中的“ 字节 ”单选钮。要查看作为 字的二进制数据，单击“ 字 ”单选钮。但是，不是所有事件都产生二进制数据，而且二进制数据往往晦涩难懂，一般只有经验丰富的技术支持人员才能解释。

另外，打开日志时，事件查看器显示的是日志的当前信息，如果这时候出现了新的日志事件，视图不会更新，必须使用“ 刷新 ”命令（在日志条目的快捷菜单中）才能看到最新的信息。但是，如果切换到另一个日志然后返回到原先的日志，此时第一个日志将自动更新。

图 16-3　查看事件详细信息

16.2　查看和管理日志审核

上一节初步介绍了事件查看器的使用，但如何管理事件查看器并更合理地使用日志仍然需要进一步讨论。由于系统几乎可以为事件查看器提供所有的数据，如何从这些数据中提取有用的信息具有一定的困难，也需要管理员具备丰富的经验。

16.2.1　筛选事件

筛选事件查看器的审核是有效地寻找信息的重要手段，通过日志的筛选器（filter），可以筛选事件类型、事件来源、类别、事件 ID、用户以及计算机，从而使事件查看器只审核需要注意的信息。

使用筛选器的方法是：选中某种日志并单击鼠标右键，从快捷菜单中选择“ 查看 ”→“ 筛选 ”命令，则调出属性对话框的“ 筛选器 ”选项卡，如图 16-4 所示。

如图 16-4 所示，筛选审核的事件类型，可以从信息、警告、错误、成功审核、失败审核 5 种类型中选择，此外还提供了事件来源和类别两个下拉框（默认都是全部），管理员可以从中作细致的挑选。

其他的筛选选项包括审核的事件 ID、用户、计算机以及事件发生的时间范围，这些都是如图 16-1 所示的字段。

需要注意，这些选项都是针对特定的日志的，也就是说，只对选中的日志有效，如果希望其他的日志也进行同样的筛选，必须对各个日志条目逐个地设置。

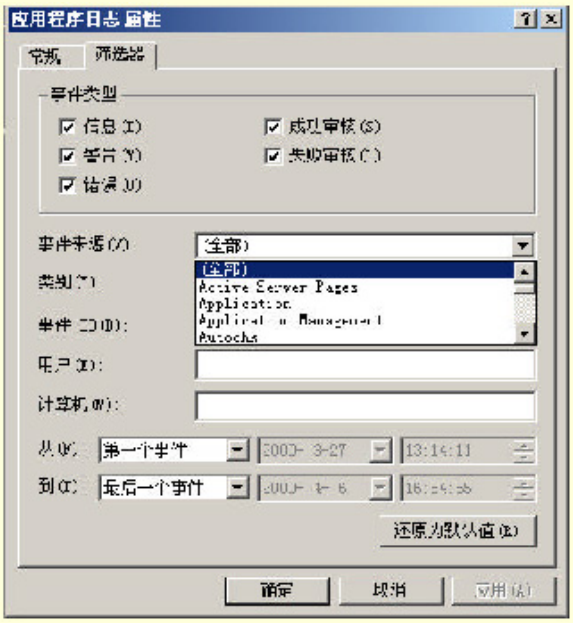


图 16-4 筛选

16.2.2 使用查找工具

如果您是第一次打开日志界面，几乎肯定会被纷繁的日志记录弄得头昏眼花，即使是很有经验的管理员，也难保不会漏掉敏感的信息。但如果是怀疑某一方面出了问题，主动寻找问题则要好办得多，因为微软提供了强大的查询工具。例如，如果对某个用户产生了不信任，可以查找他的审核记录，这是很容易办到的。

调出查找工具的方法是：选中某种日志并单击鼠标右键，从快捷菜单中选择“查看”→“查找”命令，则调出查找对话框，如图 16-5 所示。

图 16-5 查找记录

显然，图 16-5 与图 16-4 的筛选对话框界面非常相似，所做的操作也是大同小异的。例如，在如图 16-5 所示中输入查找的用户名，单击“查找下一个”，就可以非常迅速地找到该用户的相关记录。

同样需要注意，查找只针对当前的日志的，如果要查看其他日志中的情况，还需要在其他日志中进行查找。

16.2.3　控制日志大小

合理地控制日志文件大小非常重要，由于系统的审核范围相当广泛，每天都会产生许多的事件审核记录，如果不善于管理，日志文件就会不断膨胀，过大的日志文件将会导致系统性能的降低。

通过以下几种方法避免日志文件不断膨胀：

- 设置最大的日志文件大小。默认是 512KB。
- 按需要改写日志。
- 清除一定天数以前的事件日志，默认是 7 天。
- 不改写日志，而是手动清除日志。

选择某个日志条目后，单击右键并从快捷菜单中选择属性命令，或者从操作台菜单中选择“操作”→“属性”命令，此时如图 16-6 所示，在属性对话框中控制设置改写日志事件的方案。

需要注意：后三种选择是互相排斥的，只能选择一种方案。如果对所设置的方案不满意，单击图 16-6 所示的“还原为默认值”按钮，则可重设为原来的方案。

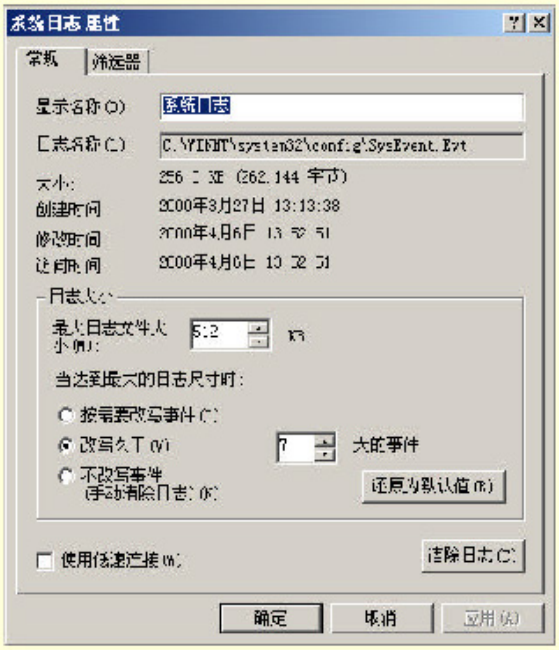


图 16-6　设置日志文件大小

当日志文件已满时会停止记录新的事件，这时清除日志后才能开始记录新的事件。另一方面，只有管理员才可以清除日志。

图中的“使用低速连接”选项是为管理远程计算机的事件查看器而设置的。

16.2.4　保存日志

如图 16-6 所示，单击“清除日志”，可以更干脆地为更新的日志腾出空间，这时会出现对话框，提示是否需要保存日志文件。由于清除日志以后，只能显示新的日志，为了日后处理的方便，可以将一些日志文件存档，而且最好将各个日志文件集中存放，这样管理比较有利。

还可以从操作台菜单中选择“操作”→“另存日志文件”命令，如图 16-7 所示，将日志文件归档保存。

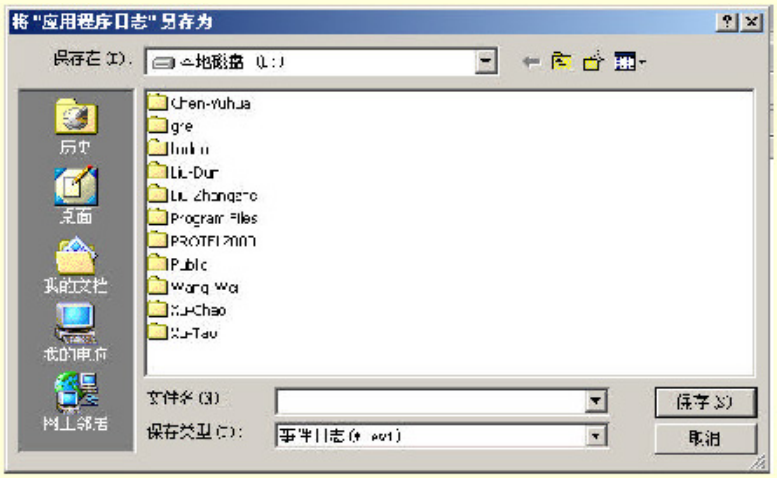


图 16-7 另存日志文件

提示：保存日志时，不管筛选选项如何，整个日志都被保存，这时候也不保留排序顺序。

默认情况下，日志文件以.evt 的后缀名保存，提供的另外两种保存格式是文本（制表符分隔）的 txt 文件和.csv 文件（以逗号分隔）。

这几种保存格式的区别是打开的方式不同，如果用默认的保存方式，即保存为 evt 文件，则只能在事件查看器里打开，而且无法从资源管理器中通过双击文件的方式直接打开，必须首先启动事件查看器，然后从操作台菜单中选择“操作”→“打开日志文件”命令。而文本文件用记事本程序就可以打开了，csv 文件可以通过电子表格程序 Excel 打开，既然如此，如果日志文件涉及敏感信息，就必须实行一定的文件权限保护措施，这可以通过 NTFS 文件的属性设置。如图 16-8 和图 16-9 所示分别是使用记事本和电子表格打开的日志文件。

图 16-8 以文本方式打开的日志文件

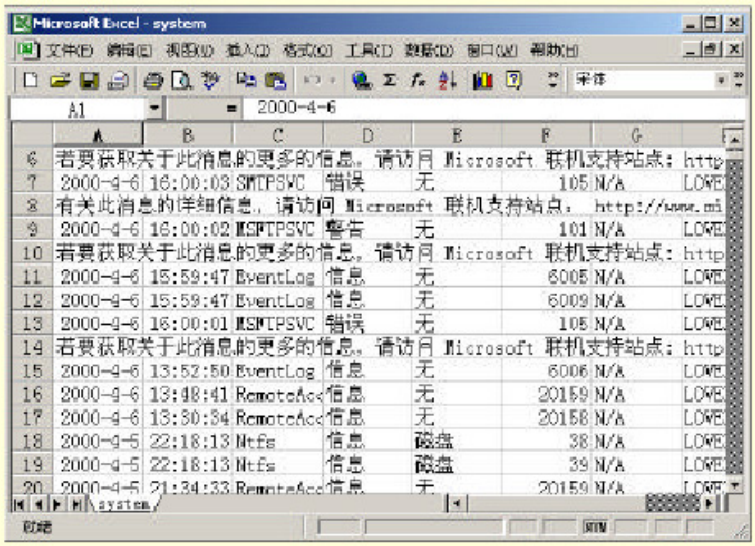


图 16-9　以 csv 格式打开的日志文件

16.2.5　查看远程计算机的事件查看器

除了可以查看本地计算机的事件查看器之外，Windows 2000 还提供了管理远程计算机的方法。

从管理控制台中添加管理单元时（添加的方法见管理控制台一章），选择事件查看器管理单元后，将出现如图 16-10 所示的选择计算机对话框，可以从中选择远程计算机。

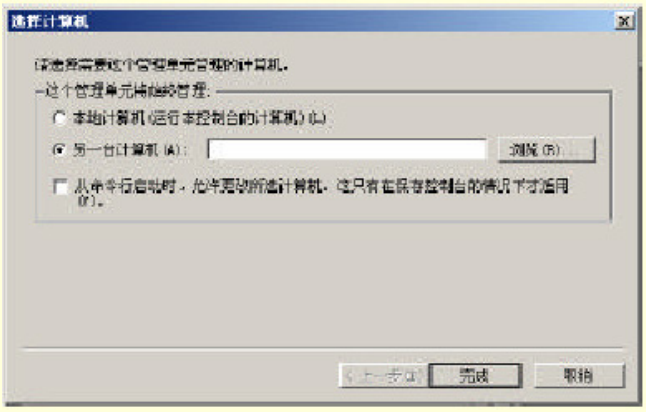


图 16-10　选择远程计算机

其他远程计算机可以是运行 Windows 2000 Professional 或者 Windows NT Workstation 的工作站，也可以是运行 Windows 2000 Server 或者 Windows NT Server 的服务器或域控制器，甚至是微软过去的 LAN Manager 2.x 服务器。

16.3　安全日志满时暂停计算机

在文件权限管理一章中已经详细地介绍过使用安全日志审核系统的安全性事件，比如策略更改、特权使用、对象访问、账户管理、登录事件等等，需要记住的要点是必须启动组策略中的审核策略才能完成安全日志设置，如果要审核文件或者文件夹的成功以及失败访问，还必须从该文件或者文件夹的属性中设置为允许审核。有关安全日志的使用详见文件权限管理一章。

安全日志具有其他两种日志所不同的一些特性，比如默认时，它是不会启动的，只有执行了上面所说的设置，安全日志才会为管理员服务；此外，默认时，安全日志只有管理员或者管理员组成员才能查看，而普通用户只有查看其他两种日志的权限。

毫无疑问，对于要求安全性比较高的系统，安全日志是相当重要的，管理员应该经常查看安全日志，以发现可能存在的安全性问题。

如图 16-6 所示的日志文件大小同样适用于安全日志，但有一点很重要：如果注册表中 HKEY_LOCAL_MACHINE\SYSTEM 配置单元，\CurrentControlSet\Control\Lsa 下的项：CrashOnAuditFail 设为 1，安全日志满后系统将会停机，

显然，这种设置对许多用户十分的不近情理，一旦安全日志已满，系统不会通知用户让他们做好准备而直接停机并显示审核失败的消息。但另一方面，如果安全性的要求相当高，也许必须要求任何的安全事件都逃不过审核的记录。

系统停止后，若要进行恢复，必须首先将日志文件存档，然后清除安全日志。接着从注册表中依旧找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 路径，并使用数据类型 REG_DWORD 和数值 1，删除并替换 CrashOnAuditFail 值。注意：必须作为管理员或管理组成员登录才能完成该过程，另一方面，对注册表的改动需要非常小心谨慎，关于修改注册表，详见注册表一章。

第 17 章　应用程序的支持及管理

毫无疑问，操作系统是计算机上最重要的软件系统，负责管理和调度计算机的系统资源，任何应用程序都必须在操作系统的支撑下才能良好地运转，如果没有得到主流操作系统的支持，即使编写得再好的程序也是没有商业生命力的，软件业中这样的例子屡见不鲜。但是另一方面，一种操作系统要想得到承认，本身也必须对各种程序能够实现合理的支持，具有良好的兼容性。Windows 2000 延续了 Windows 系列的功能，能支撑众多的应用程序，这一点对许多老程序的使用者是一个好消息。

本章内容包括：

- 应用程序体系结构
- 对 32 位应用程序的支持
- 对 DOS 程序的支持
- 对 Win16 位应用程序的支持
- 对 OS/2 和 POSIX 的支持
- 任务管理器的使用
- 调整应用程序优先级别

17.1　应用程序体系结构

多年来，计算机技术发展经历了各种不同应用程序的使用时代。早先的程序基本上都是 DOS 时代的产物；随着 Windows 的出现，诞生了 Windows16 位应用程序；而今天，绝大多数应用程序是基于 Windows32 位的，此外还流行过有非 Windows 的 OS/2、POSIX 应用程序，尽管它们当中许多程序已经过时了，但 Windows 2000 仍然为它们留有一席之地，这也是 Windows 2000 的设计目标之一。

Windows 2000 对各种不同体系程序的支持是通过环境子系统（Environment Subsystem）和虚拟机实现的，这些子系统或者虚拟机为应用程序提供了能被识别的编程接口，使这些程序能够感觉上是运行在原先的操作系统当中。各种应用程序的环境子系统构建于 Windows 2000 的用户模态（User Mode）之上，处在系统的最高层，而用户模态下层是系统的核心态（Kernel Mode），所有的基本操作系统功能都是在核心态中的执行体完成的，这些管理功能包括 I/0 管理、进程管理、本地过程调用、虚拟内存管理、图形设备接口等。值得注意的是：用户态和核心态有严格的分隔，应用程序不能直接访问执行体服务，从而保证了系统的稳定性。

Windows 2000 通过 NTVDM、WOW、OS/2、POSIX 等子系统实现对各种程序的支持。但是这些子系统并不是自动启动的，为了节省内存和其他资源，只有应用程序需要时这些子系统才会被载入，从而避免了整个系统过于庞大而效率低下。另外，Win32 应用程序、Win16 应用程序以及 DOS 虚拟机下的 DOS 应用程序被映射成 Win32 子系统，OS/2 和 POSIX 则有自己的子系统。各个子系统被物理隔离，运行在自己的内存空间中，即使有某一个子系统崩溃也不会影响其他子系统。

注意：只有 Intel X86 系列才全部支持这几种子系统，RISC 平台并不支持 OS/2 子系统，只能运行 OS/2 的绑定（bound）程序，并通过 Forcedos 命令在 NTVDM 下运行。

17.2　对 32 位应用程序的支持

伴随着指令执行时间的大大缩短，32 位应用程序已经成为今天的主流，大多数在 Windows 2000 中执行的应用程序是 32 位的。Windows 2000 中的 Win32 子系统支持这些 32 位应用程序，同时还对其他环境子系统提供

支持。

与过去的 16 位应用程序相比，32 位应用程序有非常明显的优越性，这体现在如下几点：

- 各应用程序拥有独自的 2GB 地址空间，可靠性更强。
- 支持多线程应用程序（Multithreaded Application）。
- 能发挥抢占式多任务（Preemptive Multitasking）的优越性。
- 发挥多处理器系统（Multiprocessor System）的优越性。

由于 32 位应用程序具有各自独立的 2GB 地址空间，防止了拙劣的程序覆盖另外一个应用程序地址空间的可能，因此当一个程序崩溃时，只要关闭这个程序就可以了，并不会影响其它程序的运行，这一点可以极大地保证系统的稳定性。

应一个与 16 位应用程序相比的重要优点是 32 位应用程序的多线程特性。可以把线程理解为程序作业的子单元，或者是一个程序任务的子任务。正如一个大任务是由许多小的子任务组成一样，一个多线程应用程序是由许多线程组成的。线程是 Windows 2000 完成调度的基本实体，因此完成一个程序实际上是在执行许多的子单元线程。

提示：线程的好处是系统开销更少，而且线程可以更方便有效地实现并行性。每个程序进程创建时只有一个主线程，由这个主线程再创建其他子线程。

多线程特性的 32 位应用程序可以实现抢占性多任务的功能。多任务的概念由来已久，无疑地，在电子技术飞速发展的今天，把大量的资源花费在单任务上是很不划算的。而多任务又有协同式多任务和抢先式多任务之分。

在 Windows16 位实行的协同式多任务程序中，一个程序对资源的使用依赖于其他程序是否“愿意”释放它所占有的资源，如果程序编写得不好，例如陷入死循环或者总是霸占着资源而不肯释放，其他程序将无法获得需要的资源，这对多任务的执行是很不利的。但是抢先式多任务则不同，操作系统直接介入到资源的分配工作当中，各个线程对资源的使用有优先权之分，而且每个线程按照时间片来分配，操作系统会根据充分考虑到低级别的线程并保证它们能得到时间片以运行。这样一来，程序就不会一味地消极等待其他程序释放资源。

由于实行了多线程，各个线程成为任务调度的基本单位，从而充分发挥了抢先式多任务的优点。

多线程也可以发挥系统的多处理器优势，这时候每个线程可以安排在不同的处理器中执行。

17.3 对 DOS 程序的支持

Windows 2000 对 DOS 程序的支持是通过一个叫做 NTVDM（NT virtual Dos Manager）的虚拟 DOS 机完成的。NTVDM 是一个特殊的 32 位应用程序，Windows 2000 用它来实现虚拟一个 DOS 环境，每次调用 DOS 程序就会启动 NTVDM，使 DOS 程序在其中执行，也就是说，所有 DOS 程序都以一个 NTVDM 的进程显示。由于 NTVDM 本身是一个 32 位程序，拥有自己的执行线程，因此也有自己独立的地址空间，这就使得 DOS 程序也可以实现多任务，而且单个 DOS 程序的崩溃不会影响其他 DOS 程序。

需要注意的是，DOS 程序不能直接访问硬件设备，NTVDM 会截获这些对硬件设备的访问，并传送到 Windows 2000 的 32 位设备驱动程序，由虚拟设备驱动程序进行调用，如果没有相应的设备驱动程序，DOS 将无法运行，这也是许多 DOS 程序不能运行的原因。

对 DOS 程序进行任务信息配置是 DOS 程序的重要工作，这些工作通过配置程序的 PIF（Program Information File）完成。DOS 程序的 PIF 信息可以在它们的属性对话框中找到。

17.3.1 配置程序 PIF 属性

从资源管理器中 DOS 程序，单击右键并选择“属性”命令，可以发现 DOS 程序的属性框比普通文件对话的属性对话框多了许多选项卡，除了基本的常规、安全、摘要外，还包括程序、字体、屏幕、内存和其他选项。

如图 17-1 所示是 DOS 程序的程序选项卡。

图 17-1　MS-DOS 程序的属性框

其中的各个选项卡意义是：

- 命令行：指定了 MS-DOS 程序运行的路径。
- 工作目录：指定存储应用程序数据文件的目录。
- 批处理文件：指定程序运行之前执行的批处理文件。
- 快捷键：指定启动运行程序的快捷键组合。
- 运行方式：指定运行程序时的窗口选项，包括常规窗口、最大化或者最小化。

Windows 2000 对每个 MS-DOS 程序指向不同的 Autoexec 文件和 Config 文件。DOS 程序运行之前，系统会首先分析它们的运行环境，默认情况下，这两个文件分别是%Systemroot%\system32 目录下的 Autoexec.nt 文件和 Config.nt 文件。

如果希望重新设置这两个文件，单击如图 17-1 所示的对话框中的“高级”按钮，接着在如图 17-2 的对话框中配置 MS-DOS 程序的系统初始化信息。

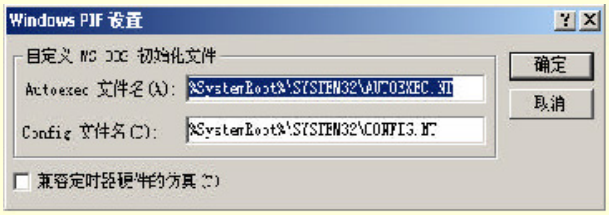


图 17-2　MS-DOS 初始化文件设置

17.3.2　配置 DOS 程序的内存选项

每个 DOS 程序都运行在 NTVDM 设立的 1MB 虚拟机器上，除了常规的内存分配值外，还可以在需要时提供扩充和扩展内存，这些内存类型包括 XMS、EMS、DPMI 内存等。缺省情况下，系统自动进行配置。从 DOS 程序属性框中选择“内存”选项卡，可以进行配置。如图 17-3 所示。

图 17-3 配置 DOS 程序的内存选项

一般的 DOS 程序都不需要修改这些自动参数，只有需要手工限制 DOS 程序的最大内存时，可能会需要修改。

17.4 对 Win16 程序的支持

Windows 2000 中也支持 Win16 位应用程序，这时使用的子系统是“WOW”，或者叫“Win16 On Win32”。在系统的%Systemroot%\system32 目录下就有 wowexec.exe 执行文件，Win16 位应用程序在这个环境下执行。

要注意 WOW 环境是运行在 NTVDM 虚拟机下的，如果启动任务管理器并选择“进程”选项卡，就可以看见 wowexec.exe 线程运行在 NTVDM 中，如图 17-4 所示。

图 17-4 NTVDM 下的多个 Win16 线程

17.4.1 在相同内存空间运行 Win16 程序

与 DOS 程序不同，默认情况下所有的 Win16 位应用程序运行在同一个 NTVDM 虚拟机下，它们共享同一片地址空间，这由图 17-4 也可以看出，在 NTVDM 进程下有两个并列的“下级”Win16 线程，它们在 NTVDM 下是缩进的形式。DOS 程序则相反，每一个 DOS 程序执行时都会有不同的 NTVDM 进程启动。

在同一个 NTVDM 下运行多个 Win16 应用程序意味着这些程序之间共有同一片地址空间，而且它们之间是非强占式多任务的，当有一个 Win16 程序失效时将会影响到其他的 Win16 程序。

17.4.2　在单独的内存空间运行 Win16 程序

为了防止上面所说的一个失效程序影响其他程序的情况出现，也可以为 Win16 位程序配置单独的内存空间，这样就允许多个 Win16 位程序同时运行，并且能够得到更好的运行性能，更安全的内存隔离和更有效的应用程序保护。对那些容易崩溃的程序或者需要稳定性很高的程序来说，将它们配置为在单独的内存空间运行可以大大降低它们出错的可能性。

也可以在命令提示符窗口下使用 start /separate appname 的格式启动 16 位程序，使其在单独内存空间下运行。命令开关 separate 表示将该程序设置为在单独内存空间下运行。

相反的例子是 start /shared appname 命令。读者一定可以猜到，命令开关 shared 表示将该程序设置为在同一片内存空间下运行。

另一个将某一个 Win16 位程序设为在单独内存空间下运行的方法是 :为该 Win16 位程序创建一个快捷方式，并在资源管理器中用右键单击这个快捷方式，从快捷菜单中选择属性命令的快捷方式选项卡，如图 17-5 所示，选中在“ 单独的内存空间中运行 ”复选框。

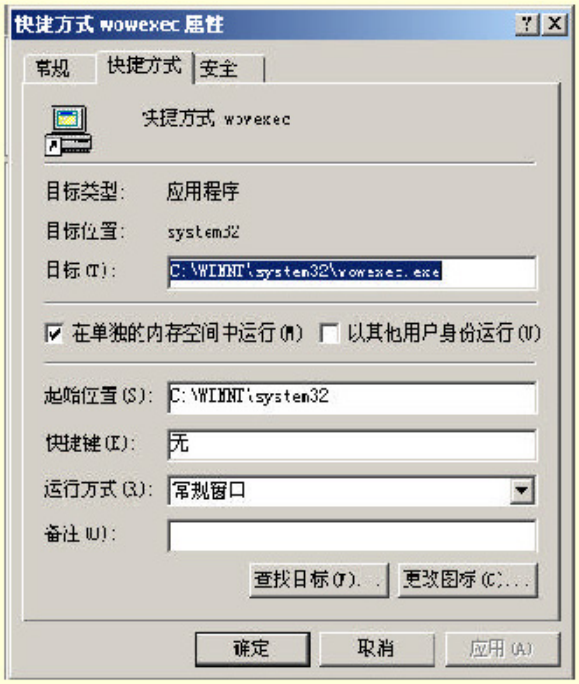


图 17-5　设置在单独内存空间下运行

通过上面介绍的设置，可以使某个 Win16 位程序在单独内存空间下运行，但如果希望使所有 Win16 位程序都在单独内存空间下运行，逐个地设置显然是相当繁琐的，这时候需要借助对注册表的修改。

使用注册表编辑器 regedt32.exe 找到下面的条目：

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ WOW

该条目下有一个 REG_SZ 类型的 DefaultSerparateVDM 值，默认是 no，即缺省情况下所有的 Win16 位应用程序运行在同一个 NTVDM 虚拟机下，把这个值改为 yes 后，每个 Win16 应用程序就可以运行在不同的 NTVDM 虚拟机、不同的 WOWEXEC 实例下了，如图 17-6 所示。

关于 WOW 的注册表下还有其他一些键值，如 wowsize、cmdline、wowcmdline 等，分别表示环境尺寸、命令行参数等意义。关于注册表的修改及其相关注意问题请参考注册表一章，不要随便修改注册表。

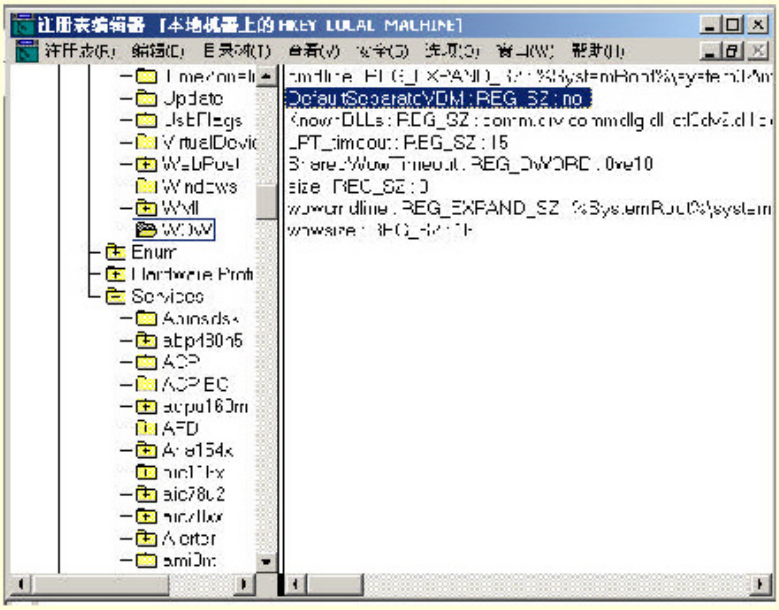


图 17-6 修改注册表使所有 Win16 位程序都在单独内存空间下运行

17.5 对 OS/2 和 POSIX 的支持

可以在注册表的以下键值中找到 Windows 2000 对 OS/2 和 POSIX 程序的支持文件：

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ Session Manager \ Subsystems

打开注册表编辑器并找到这个位置，可以发现 OS/2 和 POSIX 两个键值。如果打开资源管理器，也可以在 %Systemroot%\system32 目录下 os2ss.exe 和 psxss.exe 两个系统文件。

OS/2 和 POSIX 程序今天已经很少使用了。和 DOS 以及 Win16 程序不同，尽管也需要额外的子系统支持，但显然这些程序仍然经常需要使用（至少在安装 Windows 2000 就少不了 DOS 的介入），没有人会禁止系统对 NTVDM 的支持。然而，OS/2 和 POSIX 程序却没有那么流行，另一方面，OS/2 和 POSIX 子系统也不符合 C2 安全标准。

由于实用性不强，完全可以删除这两个子系统以节省系统资源，这只需要在资源管理器中删除 os2ss.exe 和 psxss.exe 这两个系统文件就可以了。

17.6 任务管理器的使用

使用任务管理器可以更全面地查看和管理当前运行的应用程序，包括所有的 DOS、16 位和 32 位程序，这些程序当前的运行状态，占有的系统资源在任务管理器都非常清楚地得到展现。如果某些程序运行不正常或者已经崩溃，可以使用任务管理器对它们进行关闭。

启动任务管理器的方法有 3 种：

- 按“ Ctrl+Alt+Del ”键，然后单击“ 任务管理器 ”按钮。
- 在任务栏窗口单击鼠标右键，然后从弹出菜单中选择任务管理器。
- 在开始菜单的“ 运行 ”对话框中，输入 taskmgr。
- 直接按“ Ctrl+Shift+Esc ”键。

17.6.1 应用程序选项卡

任务管理器有 3 个选项卡，分别是“ 应用程序 ”、“ 进程 ”和“ 性能 ”。启动任务管理器后首先出现的是“ 应用程序 ”选项卡，如图 17-7 所示。

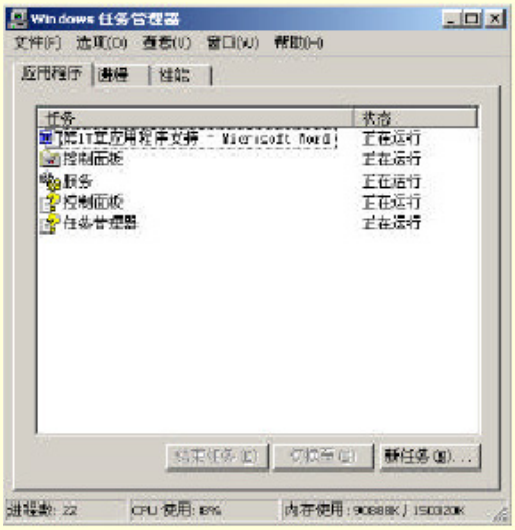


图 17-7　任务管理器中的应用程序列表

应用程序列表中列出了当前运行的所有应用程序以及当前的运行状态。状态一般有两种：正在运行或者是未响应。对未响应程序，可以直接结束任务以释放系统资源，如图 17-8 所示。

需要注意：非正常地结束应用程序可能会导致数据丢失，这时候系统会出现警告，并提示是否保存数据。但是，对未响应的程序却无法保存数据。

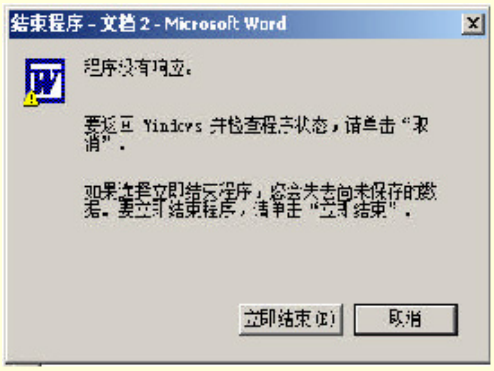


图 17-8　非正常地结束程序可能会导致数据丢失

如前所述，默认情况下，DOS 程序和 32 位程序在自己单独的内存空间运行，结束任务对其它程序没有影响；而 16 位程序共有一片内存空间，结束任务则可能影响其他程序对系统资源的使用。

还可以在这里启动新任务，方法是从文件菜单中选择“新任务（运行）”命令，或者直接按对话框中的“新任务”按钮，这将启动运行对话框。启动新任务相当于开始菜单中的运行命令。

17.6.2　进程选项卡

系统当前运行的进程数要比程序多得多，打开进程选项卡可以看到当前正在运行的进程。这中间包括运行的应用程序进程，后台运行的服务进程，以及一些系统固有的进程，比如总会有的空闲进程（Idle Process）。在任务管理器中，单击“进程”选项卡，如图 17-9 所示。

图 17-9 进程选项卡

此时出现的各列有映像名称、PID、CPU、CPU 时间、内存使用。各项的含义是：

■ 映像名称：显示当前运行进程的名称。

■ PID：是该进程的标志，这个标志是唯一的。

■ CPU：表示 CPU 使用情况，即当前分配给该进程的 CPU 使用百分比。从上图 17-9 中可以看到，当前分配给 Idle Process（空闲进程）的百分比高达 98%，可见系统比较空闲。

■ CPU 时间：该进程已经使用的 CPU 总时间。

■ 内存使用：系统分配给该进程的内存数量。

单击各栏，可以按照升序或者降序的顺序查看各个进程间的信息。例如有些后台服务可能占去相当多的内存资源。

除了这几栏外，可以查看到更多的信息，从查看菜单中选择“选择列”命令，如图 17-10 所示。可供选择的列还有页面错误、虚拟内存大小、基本优先级别、线程记数等。尝试假如更多的列，并仔细对比，可以对各个进程有更深的了解。

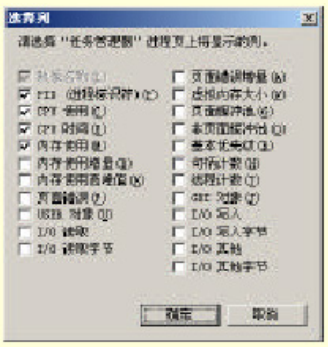


图 17-10 选择查看列

在如图 17-9 所示的“进程”选项卡里可以关闭当前运行的一些进程：选择某个进程，然后单击“结束进程”。此时会出现警告，提示可能会出现数据丢失或者导致系统不稳定，如果确信不会有问题，确认即可。如果不小心结束了某个不应该结束的进程，可以从文件菜单中选择新任务重新启动这个进程。

不过需要注意：有些进程属于“关键系统进程”，是无法关闭的，比如 services.exe、winlogon.exe 和 System Idle Process，如果试图强行关闭，将出现如图 17-11 的提示框。

图 17-11　无法中止关键进程

在任务管理器中不能关闭的进程大多属于系统服务，这些服务有些归于 services.exe 之下，另外一些服务则拥有自己的进程，比如打印池服务 SPOOLSV.EXE。要关闭某个服务，更好的办法是通过管理工具中的服务工具。单击开始菜单，从程序组里选择“管理工具”→“服务”，如图 17-12 所示。

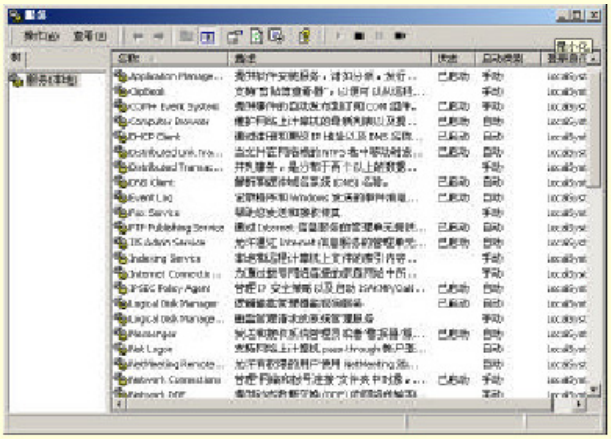


图 17-12　服务列表

如图 17-12 显示了系统中的服务以及它们的状态（是否已经启动），启动类别（手动、自动或是禁止），窗口中还给出了各个服务的详细描述信息。菜单栏中有类似于录音机播放、暂停、停止的按钮，可以用来启动或者停止某项服务。这时候要小心，因为有些服务是互相关联的，不能独立地启动或者停止，关闭某个服务可能会相应地关闭与之关联的其他一些服务。因此在停止某项服务之前最好查看这项服务的依存信息。

选择想停止的服务后，单击右键并选择“属性”命令，接着选择依存关系选项卡，如图 17-13 所示。从中可以查看这个服务依赖的服务以及依赖本服务的其他服务。

图 17-13　服务的依存关系

17.6.3　性能选项卡

任务管理器的最后一个选项卡用来检测系统性能，包括 CPU 使用记录和内存使用记录图表，计算机上正在

运行的句柄、线程和进程的总数以及物理内存使用情况，如图 17-14 所示。

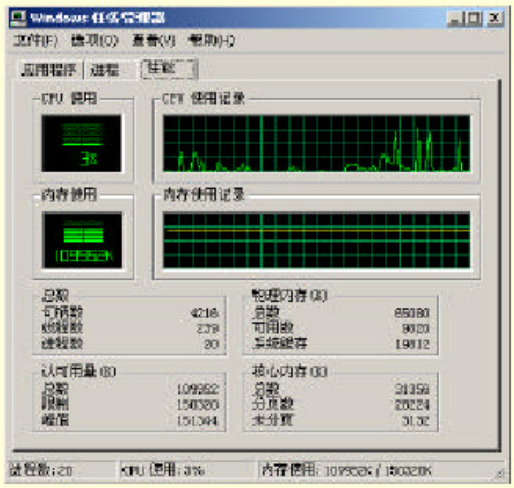


图 17-14 性能选项卡

图表中显示了最近一段时间的 CPU 和内存使用情况，刷新时间间隔由查看菜单中的刷新速度决定，可以更改刷新频率的选项。另外，如果选择了查看菜单中的“显示内核时间”选项，则会有一条红线显示系统内核的 CPU 使用时间。

需要监测系统性能，使用管理工具中的性能工具是更好的办法（见性能监视一章），那里的对象和计数器更全面，资料更详细，而且可以记录和打印性能信息，这些功能任务管理器都不支持，但是使用任务管理器可以更方便一些。

17.7 调整应用程序优先级别

前面已经介绍过，32 位应用程序实行的是抢占式多任务，这时候系统根据各个程序的优先级别为它们分配时间片，优先级别高的程序比优先级别低的程序有更多的时间访问处理器。另一方面，操作系统可以根据一定的算法调整运行中应用程序的优先级，比如等待的时间、作业的类型（比如输入输出的优先级别比较高）等。

Windows 2000 同 Windows NT 一样，调度的单位是线程而不是进程，各个线程的优先级别又与进程的优先级别有关。虽然操作系统会根据一定的依据调整优先级别，但各个进程都有一个初始就设立好的基本优先级别，它们在进程创建时已经设立好了，基本优先级别往往是决定性的。

Windows 2000 把优先级别分为 32 级，其中有四类基本优先级别：低（Low）、标准（Normal）、高（High）和实时（Real-time），各个级别的基本优先安排是：低：4；标准：8；高：13；实时：24。一般来说，许多程序初始是以标准（Normal）执行的。可以在任务管理器中查看各个进程的基本优先级别，在如图 17-11 所示的选择列对话框中选择基本优先级别，就可以在进程选项卡中看到各个进程的基本优先级。例如，任务管理器的基本优先级别是高（High），比普通程序的标准（Normal）基本优先级别更高，除非最小化运行，否则任务管理器总是处于前台。

另一方面，可以在程序执行时动态地更改进程的优先级。这也可以在任务管理器中的进程选项卡中完成。如图 17-15 所示，在某个进程中单击右键，选择“设置优先级”命令。

图 17-15　设置优先级

需要注意的是：升高或者降低优先级，可以使其运行更快或更慢，但也可能对其他进程的性能有相反的影响。例如不应该把普通进程设为实时优先级别，其他程序将无法访问处理器进行 I/O 操作，从而导致性能降低。

提示：只有管理员组的成员才能将进程设置为实时优先级别。

此外，还可以使用 start 命令设置程序初始时的优先级别。命令的语法是：

start [/low | /normal | /high | /real-time | /belownormal | /abovenormal] [command/program]。

Windows 2000 中除了调整各应用程序执行的优先级别外，还能调整后台运行程序的性能。在控制面板中双击“系统”图标，打开系统属性对话框，并选择“高级”选项卡，单击“性能选项”按钮，如图 17-16 所示。

图 17-16　优化后台服务

默认情况下，前台程序比后台程序的优先级别更高，即在应用程序响应中选中的是“应用程序”，如果选择“后台服务”，将对所有程序都分配相同数量的处理器资源，后台程序和前台程序是平等对待的。如果需要后台任务（如备份工具）运行更快，就应该考虑优化后台程序性能。

第 18 章　Windows 2000 的维护

虽然 Windows 2000 具有很好的稳定性和安全性，但是仍然有损坏的可能。如果 Windows 2000 损坏了，如何恢复 Windows 2000 的数据将是一件很重要的工作，这时事先做好应对的准备会使这一工作容易很多。

本章的内容包括：

- 创建 Windows 2000 的启动盘
- 备份重要的磁盘信息
- 修复损坏的磁盘结构

18.1　创建 Windows 2000 的启动盘

尽管紧急修复盘在 Windows 2000 遭到破坏时，确实能起到救生员一样的作用，但它并不能帮助引导 Windows 2000，因为它不是一张启动盘，因此，创建一张专门的引导 Windows 2000 启动盘作为恢复数据的一个补充手段，不失为一个好主意。在 Windows 2000 引导失败的情况下，可以用这张盘来引导系统硬盘中的 Windows 2000，然后访问硬盘中的资源，即使硬盘是 NTFS 格式的！这种磁盘在下面任何一种情况下，特别有用：

引导驱动器的主引导记录（MBR，Master Boot Recordor）损坏。

■ 引导驱动器的分区引导扇区（PBS，Partition Boot Sector）损坏。

■ MBR 或 PBS 感染病毒。

■ MTLDR 或 MTDETECT.COM 丢失或损坏。

■ 错误的 NTBOOTDD.SYS（对于带有 SCSI 卡、并使用 SCSI 设备驱动程序而非系统 BIOS 来启动的 RISC 系统或 INTEL 系统而言）。

■ 主驱动器损坏，需要从位于镜像／双工的 RAID 1 卷中的镜像驱动器启动（然而，要使这种方式工作，需要对软盘中的 BOOT.INI 文件进行修改）。、

如何创建 Windows 2000 启动盘取决于 Windows 2000 所使用的硬件平台。在下面的部分中，我们将介绍如何在基于 INTEL X86 的系统和基于 RISC 的系统上创建这张磁盘。

（1）在任何情况下，启动到 Windows 2000 中，使用 Windows 2000 的格式化命令格式化一张磁盘。这是必要的，因为 Windows 2000 会将它自己的分区引导扇区放到磁盘上，这是作为 Windows 2000 引导盘必须的。

（2）拷贝必需的文件到这张刚刚被格式化的磁盘中，这些文件的属性缺省的被设置为只读、隐藏、系统类型。因此，在能够显示并将这些文件拷贝到启动盘中之前，需要进行一些准备步骤，按如下的步骤进行，可以使这些文件可见，然后可以拷贝它们。

（3）使用我的电脑或 Windows 2000 的资源管理器，打开包含有 Windows 2000 启动文件的驱动器根目录（在 RISC 系统中，应打开包含有 OSLOADER．EXE 和 HAL．DLL 文件的目录，如＼OS＼WINDOWS）。

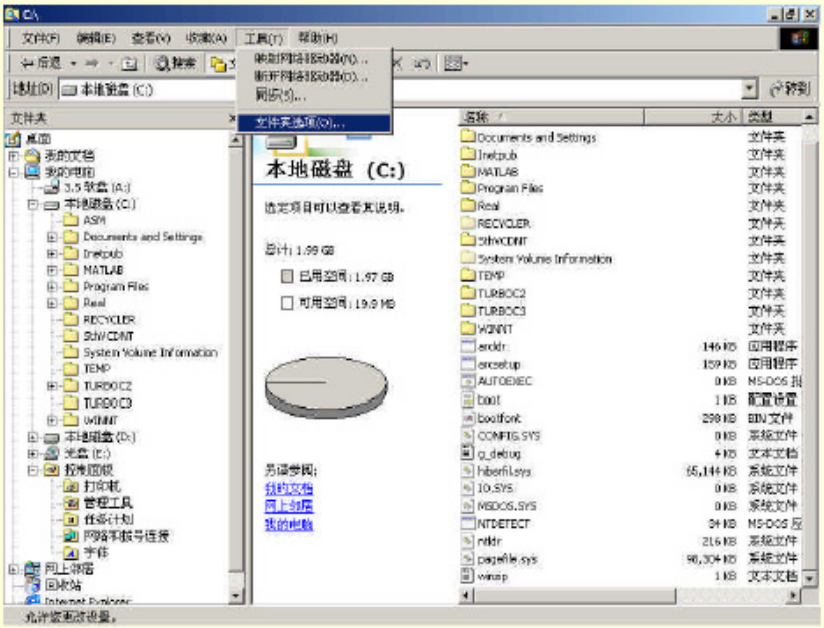


图 18-1　选择“文件夹选项”

（4）在“我的电脑”或 Windows 2000 的“资源管理器”的菜单中，选择“工具”，然后选择“文件夹选项”，选择“查看”标签页，选择在“隐藏的文件和文件夹”下的“显示所有文件和文件夹”单选按钮，并去掉“隐藏受保护的操作系统文件（推荐）”前的选中对勾，然后单击“确定”按钮。

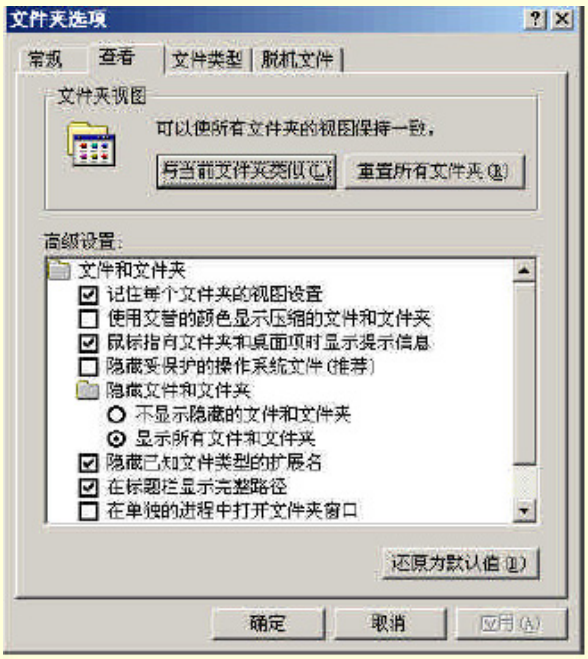


图 18-2　文件夹选项对话框

（5）这样所要拷贝的文件就可以看到了，然后就可以拷贝文件了。

在基于 X86 的系统中要拷贝的文件：

■ NTLDR，Windows 2000 的引导装载模块。

■ BOOT.INI，描述系统中多个引导分区位置的文件，分区是用 ARC（高级精简指令芯片计算，Advanced RISC Computing）路径指明。

■ NTDETECT.COM，Windows 2000 中用来进行自动硬件检测的文件。

■ BOOTSECT.DOS，该文件包含在一个可进行多重启动的系统上，Windows 2000 以外的其他操作系统的引导扇区。

与 INTEL 基于 X86 的系统使用 BOOT．INI 文件来定义主分区（包含有操作系统的）的位置不同，RISC 系统使用固件配置工具来维护这个列表，配置在系统启动时自动得到验证，并且该工具可以在配置丢失的情况下，用来快速重建内容。对于使用 BOOT．INI 的基于 X86 的系统（特别是在 NTFS 分区上的），解决 BOOT．INI 文件的丢失问题会相当困难。

在基于 RISC 的系统中要拷贝到启动盘中的文件。

创建一张基于 RISC 系统的 Windows 2000 启动盘，需要将这些文件拷贝到磁盘中：

■ OSLOADER.EXE 该文件在功能上与基于 X86 的 NTLDR、NTDETECT 和 BOOTSECT.DOS 的总和相等。

■ HAL.DLL Windows 2000 的硬件抽象层（HAL，Hardware Abstraction Layer）。

*.PAL 所有后缀为 PAL 的文件（仅适用于 DEC Alpha 基于 AXP 的系统）。

这些文件应当保存在与它们在系统引导驱动器中时的文件夹路径相同的路径中。例如，如果启动文件在 RISC 系统中是保存在硬盘目录 C：\OS\WINDOWS 中，则它们应当拷贝到软盘中的 A：\OS\WINDOWS 目录中，否则，会使启动盘无法启动系统。

一旦文件被成功地拷贝到磁盘中，就可以用该磁盘从 A：盘启动系统，以测试新的引导盘。对于基于 INTEL X86 的系统，请确认系统的 BIOS 设置为首先从 A：启动，而不是从 C：。对于基于 RISC 的系统，也有将第一引导设备设置为软盘驱动器的选项，但不是用 A：/C：的命名方法，因为这不是 ARC 兼容名称。

18.2 备份重要的磁盘信息

最后但并非最不重要的，这是一个在所有重要的 Windows 2000 系统上都应当采取的预防措施，就是对两个在系统正常运作中有至关重要作用的特殊磁盘结构进行备份，它们是主引导记录（MBR）和 Windows 2000 所在分区（也称为 Windows 2000 的系统分区）的分区引导扇区（PBS）。这些文件有可能由于多种原因而遭到破坏，包括病毒、驱动程序或操作系统中的错误、电源中的故障、硬件或硬件配置错误或者磁头损坏。由于这一类错误通常是 Windows 2000 无法控制的，因此保护它们的唯一办法就是拥有它们的最新备份。

主引导记录（MBR）是磁盘中的一个特殊记录，它包含磁盘中分区的信息。基于 INTEL X86 的计算机中的 BIOS 通过该记录读取磁盘分区表并找出 Windows 2000 系统分区（可引导分区）的分区引导扇区，这个扇区也包含分区表。如果 MBR 由于某种原因损坏了，计算机就无法定位系统分区来引导 Windows 2000。另一点，分区引导扇区是位于每个磁盘分区中的特殊的扇区。它指导计算机加载操作系统核心程序和引导程序（例如 Windows 2000 系统启动时出现的引导程序）。与 MBR 一样，分区引导扇区的损坏也会影响系统的正常启动。

应当非常仔细地确认所要恢复的扇区与系统的磁盘子系统当前的配置情况相一致，如果不小心恢复了错误的或过期的记录，最终会使问题更糟。为了避免这种情况的发生，在每次作出了影响主引导记录和分区引导扇区的改动之后，应立即对它们进行保存。当改变了系统中的磁盘分区后（如添加、删除或修改分区，或者设置了不同的活动引导分区）应更新备份主引导记录。而当执行了如格式化卷、安装 Windows 2000 到一个卷上或将一个卷由 FAT 文件系统转换到 NTFS 文件系统这样的操作后，应备份分区的引导扇区。

此外，如果系统中有多个硬盘驱动器，或每个磁盘有多个分区，则应备份每个磁盘上的主引导记录和每个分区的分区引导扇区。其中，启动盘上的主引导记录和 Windows 2000 系统分区上的分区引导扇区是最重要的。位于其他驱动器或分区上的 MBR 和 PBS 对引导过程并不重要，但如果他们出现了错误或者损坏，那么这些驱动器中的文件将无法访问。

可以使用 Windows 2000 资源套件中的两个实用程序中的任何一个来备份这些特殊的磁盘扇区：基于 Windows 2000 的程序 DISKPROBE 或者基于 MSDOS 的程序 DISKSAVE。这些工具包含在 Windows 2000 资源套件的 CDROM 中。

18.2.1 使用 DISKSAVE 备份 MBR 和 PBS

DISKSAVE 是一个 MSDOS 实用工具，可以将主引导记录和分区引导扇区备份成文件。要使用 DISKSAVE，必须用 MSDOS 引导盘启动系统，如果没有一张 DOS 启动盘而且系统不能运行 MSDOS，则只能使用基于 Windows 2000 的 DISKPROBE 工具来代替了。

必须将系统启动到 MSDOS 下才能使用 DISKSAVE，DISKSAVE 不能从 Windows 2000 的命令提示符下运

行。

用 DISKSAVE 创建的文件应保存到 Windows 2000 的启动盘或 DOS 引导盘中。如果日后由于 MBR 或 PBS 损坏而导致计算机出现了引导问题，可以用这些软盘中的一个来恢复它们，以便尝试并恢复系统。DISKSAVE 工具的另一个强大功能是它可以允许关掉 Windows 2000 系统分区的系统 ID 字段中的容错控制位。当主驱动器失败时，这对镜像的（RAID 1）或者双工的磁盘卷很有帮助。在这种情况下，如果 Windows 2000 在主驱动器失败后无法启动，可以用 DISKSAVE 工具关闭镜像磁盘中系统分区的容错控制位。

DISKSAVE 程序的文件名为 DISKSAVE.EXE 它位于 Windows 2000 资源套件的主安装目录中。将该工具拷贝到软盘中是个好主意，因为当它所在的驱动器失败时，会无法访问它。要运行该程序，首先用 MSDOS 启动盘启动系统，然后在 MSDOS 提示符进入 DISKSAVE 所在的目录，然后键入 DISKSAVE，如果 DISKSAVE 所在的卷不是 FAT 卷，就需要将 DISKSAVE 程序拷贝到软盘中以便运行它。

DISKSAVE 的主菜单选项有：

F2：备份主引导记录。该功能会将启动盘上第 0 柱面，第 0 磁头，第 1 扇区存储到指定的文件中。当创建或删除了一个分区，或者改变了分区中所用的文件系统的时候，需要新建一个该记录的拷贝。

F3：恢复主引导记录。该功能会将指定的文件拷贝到启动盘上第 0 柱面、0 柱面，第 0 磁头，第 1 扇区上。恢复该扇区的同时也更换分区表。恢复过程中程序不会检查该文件是不是正确的主引导记录。

F4：备份分区引导扇区。该功能将磁盘 0 上系统分区的第一个扇区保存到指定的文件中。

F5：恢复分区引导扇区。该功能用指定文件中的内容替换系统分区的第一扇区。恢复过程中程序不会检查该文件是不是正确的分区引导扇区记录。

F6：关闭启动盘上的容错。这个功能在当 Windows 2000 无法从一个系统分区的镜像集中启动时非常有用。该功能寻找系统分区，然后检查系统 ID 字节高位是否设置，如果该分区是容错卷的成员，Windows 2000 会设置高位，关闭该位与打开镜像等效。一旦关闭了该位，DISKSAVE 将无法重新设置该位。

当用 DISKSAVE 备份 MBR（F2 菜单选项）或 PBS（F4 菜单选项）时，会提示输入备份目标文件的全名，包括路径，该名字可以是任何喜欢的符合 8.3 的 MS-DOS 文件名规范的名字。

DISKSAVE 只保存磁盘 0 上的主引导记录和磁盘 0 上系统分区的分区引导记录。

18.2.2　使用 DISKPROBE 备份 MBR 和 PBS

尽管基于 Windows 2000 的 DISKPROBE 实用工具可以完成所有与基于 MS-DOS 的 DISKSAVE 相同的功能，但 DISKPROBE 比 DISKSAVE 的功能更完善。实际上，DISKPROBE 工具（包含在 Windows 2000 资源套件的 CDROM 中），完全是一个低级磁盘编辑器，并且与其他的商业程序相类似，如 Symantec 的 Norton DiskEdit。与大多数其他低级磁盘编辑工具一样，DISKPROBE 允许保存、恢复、定位、显示和修改磁盘中的数据。实际上，DISKPROBE 可以让管理员对驱动器上的每一个字节的数据进行访问，而不注重安全性。

由于 DISKPROBE 潜在的危险性，在使用 DISKPROBE 对磁盘进行任何改动之前，拥有一个当前系统的完全备份，包括注册表，是非常重要的。

尽管 DISKPROBE 为管理员提供了非常强大的故障处理和诊断能力的功能，但是在这里，我们将讨论的范围仅限制在它的备份 MBR/PBS 功能上。

依照下列步骤使用 DISKPROBE 工具备份主引导记录：

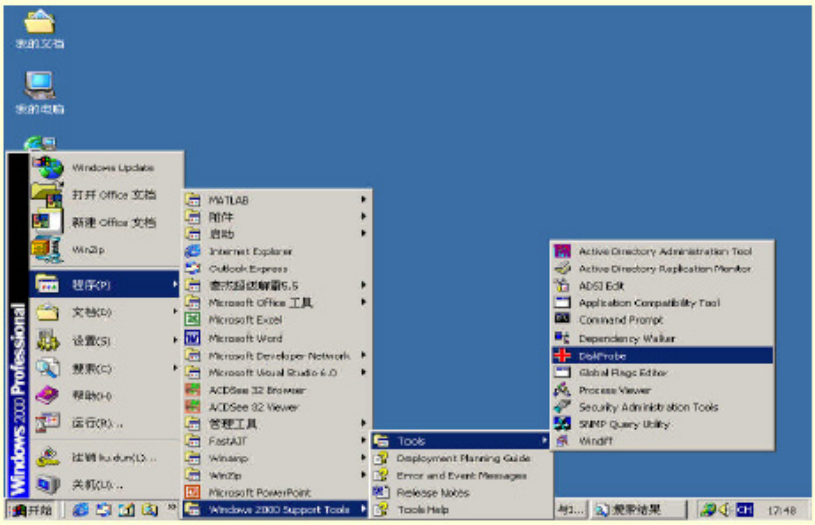


图 18-1 打开 DISKPROBE

（1）通过选择 DISKPROBE 工具的快捷方式启动它，它的快捷方式通常位于 StartMenu“开始”→“程序”→“Windows 2000 Support Tools”→Disk Tools（磁盘工具）菜单中，将会显示如图 18-2 所示的 DISKPROBE 主窗口。

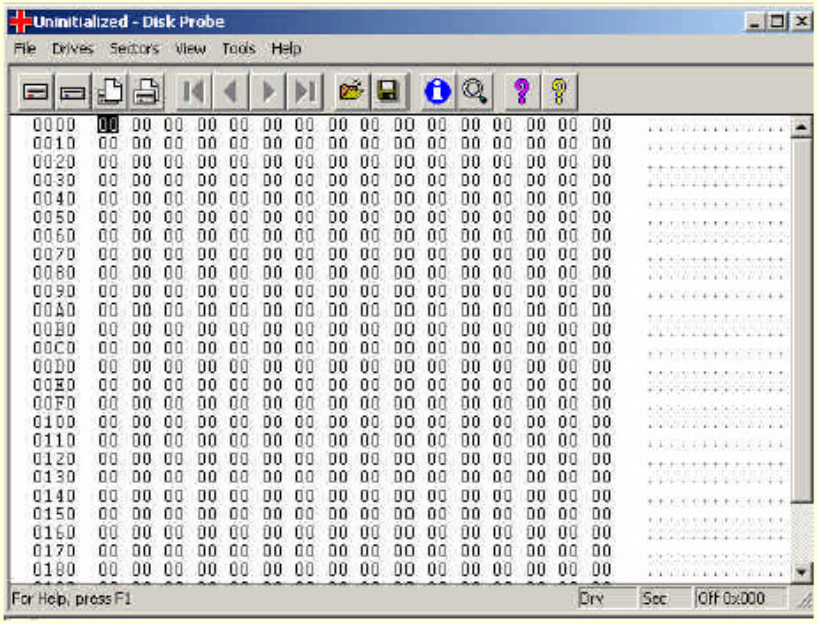


图 18-2 DISKPROBE 的窗口

（2）从菜单中选择 Driver（驱动器）→Physical Drive（物理驱动器），将会看到如图 18-3 所示的打开物理驱动器的对话框。系统中的每个物理驱动器都以 PhysicalDriveN 为名列出，其中 n=0 是第一个硬盘驱动器，n=2 是第二个，依次类推。双击包含要保存的主引导记录（由于包含系统分区的物理驱动器上的 MBR 最重要，因此第一个要保存的 MBR 就是它）的驱动器。在基于 INTEL X86 的系统中，这个驱动器总是 PhysicalDrive0，而在基于 RISC 的系统中，它可能会是其他驱动器。

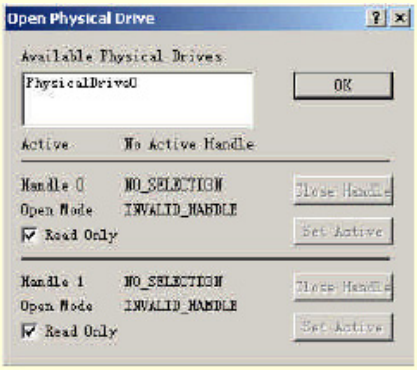


图 18-3　物理驱动器对话框

（3）在 Handle0 组群框中，选择“ Set Active（设为活动）”按钮并单击“ Close（关闭）”。

（4）接着，选择菜单中的“ Sectors（扇区）→Read（读取）”，这将打开 Sector Range（扇区选择）对话框。在对话框中，设置 Starting Sector 文本框为 0，Number of Sector 文本框为 1，然后单击 Read，这时应显示该驱动器的主引导记录。

（5）从菜单中选择“ File（文件）”→“ Save As（另存为）”。

（6）接着输入备份 MBR 的文件名。建议将这个文件保存到紧急恢复盘、Windows 2000 启动盘或 MS-DOS 引导软盘中。如果除正在备份的主引导记录所在的硬盘以外，还有其他硬盘，也可以将不同驱动器的多个 MBR 保存到软盘上。

使用 DISKPROBE 工具同样也可以备份驱动器分区中的分区引导扇区。实际上有两种不同的方法可以满足需要：一个是使用物理驱动器，一个是使用逻辑驱动器。此外，使用不同的方法取决于所涉及的分区是主分区还是扩展区。

主分区是唯一能包含操作系统的类型，可以给每个主分区分配一个驱动器盘符，如 C：或 D：，并且每个物理驱动器最多可以有 4 个主分区。扩展分区是除主分区外的另一种类型的磁盘驱动器分区，它可以被分为一个或多个逻辑驱动器。

使用 DISKPROBE 通过物理驱动器方式备份任何类型的分区引导扇区，需要使用和每次查看驱动器分区表相同的步骤，就是前面介绍的查看驱动器主引导记录的继续。按照备份主引导记录的过程中的（1）～（4）步进行，然后按下述步骤查看分区表。

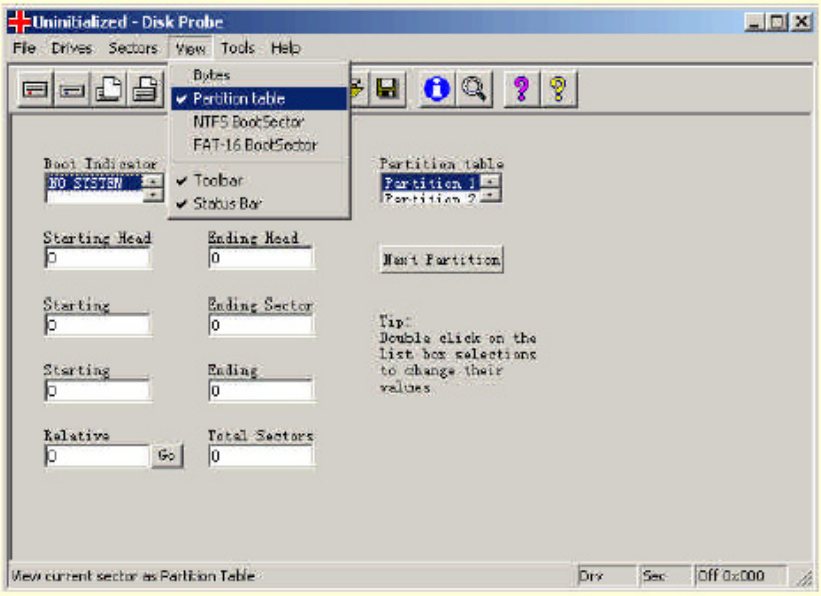


图 18-4　查看分区表

（1）在菜单中选择“ View（查看）”→Partition Table（分区表），会看到分区表显示在一个对话框中。

（2）在“ Partition Table Index（分区表索引）”框中，双击包含所要查看的分区的驱动器号。如果需要，可

以单击 Next Partition（下一个分区）按钮来查看下一个分区第一个扇区中的信息。当查看主分区时，单击“ Next Partition ”按钮可以读出下一个分区的分区引导扇区，当下一个分区是一个扩展分去时，单击“ Next Partition ”按钮可以读出扩展分区中的第一个逻辑驱动器的分区表扇区。

（3）对于主分区，单击 GO 按钮，可读出当前分区的分区引导扇区，而当 System ID 为 EXTENDED（扩展）时，单击 GO 按钮，可读出扩展分区中的下一个逻辑驱动器的分区表扇区，当查看主引导记录分区表区域内的扩展分区的信息时，Total Sectors（扇区总数）显示的是扩展分区的总尺寸。

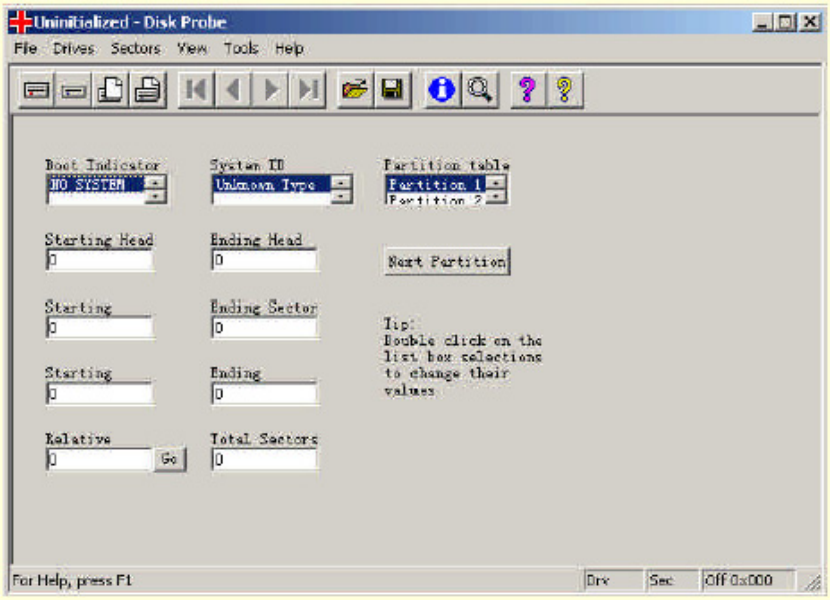


图 18-5 查看扩展分区

如果对分区表作了任何改动，必须通过选择菜单中的 Sector（扇区）→Write（写）命令将扇区写回磁盘，这只有在驱动器不是只读的情况下才起作用。

用物理驱动器方式备份分区的分区引导扇区，步骤如下：

（1）用前面介绍的步骤读出和查看分区表。

（2）在分区表索引列表矿中，双击要保存的分区引导扇区的分区号。例如，要保存系统分去的分区引导扇区，则双击 Boot Indicator（引导指示灯）为 SYSTEM 的分区号。

（3）要读出分区引导扇区，单击 Relative Sector（有关字段）字段旁的 GO 按钮。在 View 菜单中，单击 NTFS BootSector 或 FAT BootSector，来以合适的方式显示扇区中的信息，以便确认所读的扇区是分区引导扇区。

（4）从菜单中选择 File（文件）→Save As（另存为）。

（5）然后，输入备份分区引导扇区的目标文件名。建议在保存分区引导扇区时，使用的文件名用包括所备份分区引导扇区的相对磁盘和扇区号的方式来命名，格式为 PBSXXXXXXDISKN.DISK 其中 XXXXXX 是分区引导扇区的相对扇区，N 是磁盘号。这样做可以较容易地将备份的拷贝与原来的分区联系起来，同时还建议将这个备份保存到紧急恢复盘、Windows 2000 启动软盘或 MS-DOS 引导盘中。

通过使用逻辑卷方式备份分区引导扇区，步骤如下：

（1）通过选择 DISKPROBE 工具的快捷方式启动它，它的快捷方式通常位于（开始菜单）→（程序）→ Resource Kit（资源套件）→Disk Tools（磁盘工具）菜单中。

（2）从菜单中选择 Drives（驱动器）→Logical Volume（逻辑卷），在逻辑卷列表框中，双击要备份的分区引导扇区所在分区的驱动器盘符。

（3）在 Handle 0 组群框中，选择 Set Active（设为活动）按钮并单击 Close（关闭）。

（4）选择此菜单中的 Sector（扇区）→Read（读取），这将显示该驱动器的分区引导扇区。

（5）从菜单中选择 File（文件）→Save As（另存为）。

（6）接着输入目标备份文件名。建议在保存分区引导扇区时，使用的文件名用包括所备份分区引导扇区的相对磁盘和扇区号的方式来命名，格式为 PBSdDISKn.DISK 其中 d 是逻辑驱动器的盘符，n 是磁盘号。这样

做可以较容易地将备份的拷贝与原来的分区联系起来，同时还建议将这个备份保存到紧急恢复盘、Windows 2000 启动软盘或 MS-DOS 引导盘中。

要备份扩展分区中的分区引导扇区应使用物理驱动器方式，步骤如下：

（1）用前面介绍的步骤读出和查看分区表。

（2）在分区表索引列表矿中，双击要保存的扩展分区的分区号，然后单击“GO”按钮。这样会读出扩展分区中的第一个分区表记录。

（3）该对话框允许浏览扩展分区来找出要备份的分区引导扇区所在的逻辑驱动器。

（4）要读出分区引导扇区，单击 Relative Sector（有关字段）字段旁的“GO”按钮。在 View 菜单中，单击 NTFS BootSector 或 FAT BootSector，来以合适的方式显示扇区中的信息，以便确认所读的扇区是分区引导扇区。

（5）从菜单中选择 File（文件）→Save As（另存为）。

（6）接着输入目标备份文件名。建议在保存分区引导扇区时，使用的文件名用包括所备份分区引导扇区的相对磁盘和扇区号的方式来命名，格式为 PBSdDISKn.DISK 其中 d 是逻辑驱动器的盘符，n 是磁盘号。这样做可以较容易地将备份的拷贝与原来的分区联系起来，同时还建议将这个备份保存到紧急恢复盘、Windows 2000 启动软盘或 MS-DOS 引导盘中。

拥有所有驱动器和分区的 MBR 和 PBS 的拷贝，当这些磁盘的结构受到损伤或被破坏时，会使系统的恢复工作变得容易些。将这些信息与系统和注册表的完全备份结合使用，将会使数据得到很好的保护。

18.3　修复损坏的磁盘结构

不论是 MBR 还是 PBS 受到任何严重的损坏都将导致引导失败。

例如，MBR 丢失或损坏会在引导过程中产生下列信息：

Missing Operating System

Invalid Partition Table

而下列信息则表示分区引导扇区有问题：

Couldn't find NTLDR

A kernel file is missing from the disk

还有其他出错信息。如果是在出现 Windows 2000 引导程序菜单之前遇到引导错误，可以怀疑是 MBR 或 PBS 受损，可以用以下方法修复受损的结构。

使用 DISKSAVE 恢复 MBR 或 PBS

如果有一张可用的 MS-DOS 引导盘，最简单的恢复受损 MBR 或 PBS 的方法，就是使用 DISKSAVE 工具。

使用 DISKSAVE 工具恢复 MBR 或 PBS 的步骤如下：

（1）准备一张 MS-DOS 引导盘和一张含有 DISKSAVE.EXE 的磁盘。

（2）启动计算机并运行 DISKSAVE 程序，DISKSAVE 提供了一个选择菜单。F3 和 F5 两个选项用来恢复 MBR 和 PBS，F3 替换 MBR，F5 替换 PBS。

（3）提示输入保存的 MBR 和 PBS 的文件名，输入全路径名并回车。

使用 DISKSAVE 恢复了 MBR 或 PBS 之后，应当立即退出应用程序并重新启动计算机。如果问题就是出在 MBR 或 PBS 上，则现在系统可以正常启动了。

维护计算机的知识还有很多，如果全写出来将是一本巨著，而且这门学问还在不断的增加新的内容，所以只靠一时半会儿是难以掌握的，需要在长期实践中积累。这里只介绍了几种基本的方法，为以后的学习打下基础。

第 19 章　网络基础

在前面的各章里，讨论了 Windows 2000 的单机特性，现在开始进一步介绍 Windows 2000 对网络的支持。作为 Microsoft 公司在新世纪推出的操作系统，Windows 2000 能以更好的兼容性来融合了网络，但在这一章中只是对网络的基本知识进行讨论，以达到抛砖引玉的作用。如果能对网络的基础知识有较好的认识，可以跳过这一章，继续下面的学习。

计算机网络涉及到通信与计算机两个领域。计算机与通信日益紧密的结合，已对人类社会的进步做出了极大的奉献。计算机与通信的相互结合主要有两个方面。一方面，通信网络为计算机之间的数据传输和交换提供了必要的手段；另一方面，数字计算技术的发展渗透到通信技术中，又提高了通信网络的各种性能。

本章的详细内容包括有：

- 网络的体系结构
- 网络协议内容
- TCP/IP 协议结构与内容
- Internet 的基本知识
- Internet 的应用工具

19.1　网络体系结构

网络的一个重要特性就是计算机可以互相通信，需要近距离的，也需要远距离的，这就要求设置一套标准做法，否则每个人都只是简单地去做自己的操作系统、软件应用程序、网卡等等，而不去考虑与另外组件的通信，这样就会遇到兼容的问题。在这一点上，国际标准化组织（ISO）已经意识到迫切地需要一个具体的网络模型，用于网络设备生产厂商生产相互间融合的网络设备。于是在 80 年代初期，国际标准化组织就开发了一套网络设备生产厂商都要遵循的标准模型。

实在由于计算机网络是个非常复杂的系统。相互通信的两个计算机系统必须高度协调工作才行。而这种协调是相当复杂的。为了设计这样复杂的计算机网络，早在最初的网络设计时就提出了分层的方法。分层可以将庞大而复杂的问题，转化为若干较小的局部问题，而这些较小的局部问题就比较易于研究和处理。这样一来就提出了计算机网络体系结构的概念。

19.1.1　OSI 参考模型

OSI（开放系统互连，Open Systems Interconnection）模型是一个 7 层的参考模型，如图 19-1 所示，将两台计算机之间通过网络媒体传递信息的问题分成 7 个更小和更易于管理的子问题，其中每个子问题都具有自包含性，解决这些子问题基本上不需要过多的外部信息。OSI 自身的协议也正在不断的发展，现在 OSI 参考模型被作为工业上参考结构的模型。

应用层(Application)
表示层(Presentation)
会话层(Session)
传输层(Transport)
网络层(Network)
数据链路层(Data Link)
物理层(Physical)

图 19-1 OSI 参考模型

19.1.1.1　应用层

使用应用层时，通过该层和操作系统通信，这样就避免应用程序来关心资源是从计算机来或是从网络来的。它与其他层的区别在于它不需要为其他任何一层提供服务，也可以说是位于 OSI 参考模型范围之外的一些应用程序，一般经常使用的应用程序包括有：电子表格程序、文字处理程序、航空订票程序等。

19.1.1.2　表示层

表示层与通信应用中使用的数据句法结构差异有关，可以从应用层获得信息，并且转换成可识别的方式把信息提供给操作系统和网络。很少有仅提供表示层功能的协议，该功能经常并入会话层或者应用层。

19.1.1.3　会话层

会话层负责提供在两个通信应用之间建立、维护和结束会话连接的功能，也负责提供错误恢复功能。会话包括两个或多个表示实体之间的对话。会话层使表示层实体之间的会话同步，并管理它们的数据变换，除了基本的会话规则之外，会话层还为数据的传递、服务的分类、以及会话层、表示层和应用层出现错误的报告等提供了规则。

19.1.1.4　传输层

传输层目的在于定义如何维护数据的完整性，它保证了系统之间有秩序、可靠地传输数据，也提供了多方面的机制，用于建立、维护以及有序的终止虚拟电路，检测和恢复传输错误，以及控制信息的流量。

19.1.1.5　网络层

网络层负责给信息加装地址、保证信息传到正确的目的地，同时也提供了路由。路由协议在一系列子网中寻找最佳的路径，传统的网络层可能会沿最佳路径传输数据。

19.1.1.6　数据链路层

数据链路层定义了数据分组的创建、传输及接收方法。这一层的分组称为帧。帧（Frame）按照不同网络体系结构创建（如 Ethernet、ARCNET、Token Ring）。每种网络结构有其独特的帧类型。帧寻址用介质访问控制（MAC）地址定义。MAC 地址一般由制造商编程到网络接口设备中，用户不能更改。而且数据链路层可以看作由网络协议和网卡驱动程序组成，提供了可靠的数据传输，它通常与物理地址、网络拓扑、布线方法、错误提示、帧的有序发送以及流量控制紧密相关。

提示：帧是数据链路层协议通信使用的信息单位，有源地址及目的地址。帧类型识别符是从高层传输来的含有信息的数据段。同一网络上的网络设备必须用相同类型的帧进行通信。

19.1.1.7　物理层

物理层是 OSI 参考模型中的最底层，它提供了物理传输服务，定义了硬件的物理特性。它连续地从数据链路层接收数据，然后再传输到物理媒介上。在这个层上，定义了机械的（连接器的类型），电气的（电压电平），功能的（脉冲信号设定）和规程的（信息交换）特性。物理层标准的例子有 IEEE 802 系列和 EIA-232D（RS-232 的扩展，如调制解调器等等）。

提示：电子与电气工程协会（IEEE）为通信及联网制订标准。IEEE 标准的 802 系列为 Token Ring（802.5）和 Ethernet（802.3）等底层网络结构定义规范。

19.1.2 计算机间的通信

来看一个 OSI 参考模型通信的实例，如图 19-2 所示，假定图中的计算机 A 需要向计算机 B 发送信息，首先计算机 A 的应用程序与第 7 层（最顶层）联络，第七层与第 6 层联络，

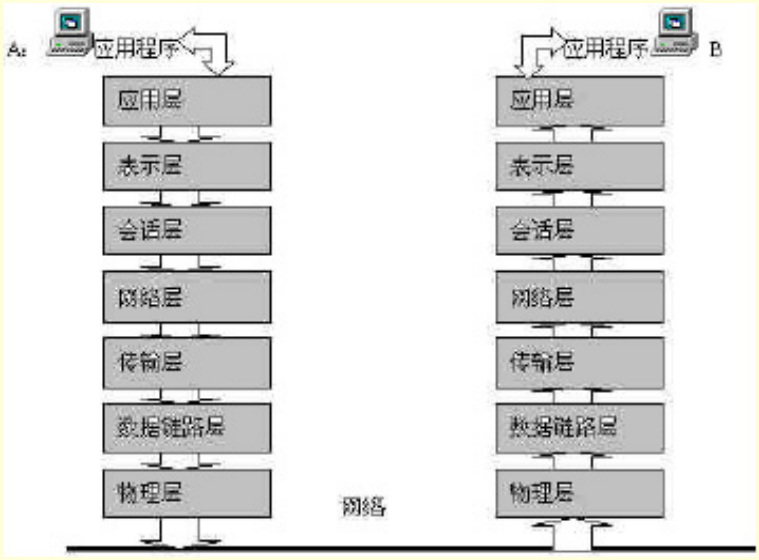


图 19-2 计算机 A、B 之间的通信

第 6 层再与第 5 层联络，以此类推直到信息传递到计算机 A 的第一层为止，第 1 层在将信息直接传递到物理网络媒体上。在信息横向穿过物理网络被计算机 B 吸收之后，信息通过计算机 B 的网络的 7 层以相反的方向向上传递（首先是第 1 层，然后是第 2 层，依此类推），直到信息最终到达计算机 B 的应用程序为止。

虽然计算机 A 中的每一层都与本系统内的相邻层联络，但是它的主要目的是与计算机 B 中的同名层联络。也就是说，计算机 A 中的第 1 层主要目的是与计算机 B 中的第 1 层联络，计算机 A 的第 2 层是与计算机 B 的第 2 层联络，其余各层也都如此。

19.2 网络协议

协议（Protocol）在词典中会查到的解释决不会包含任何与计算机有关的内容，但从计算机的术语来说，Protocol 就是指网络上计算机交换信息的标准方式，主要用于保证所有涉及的计算机都能识别信息。相当于人的社会来说，Protocol 就是人类的语言。

在 Windows 2000 中，有很多的协议都可以安装，主要的网络协议有：

- Microsoft NetBEUI.
- Microsoft IPX/SPX.
- Microsoft TCP/IP.

为了在网络上通信，一个网络计算机至少应安装一种协议，但两个计算机中的通信必须有相同的协议支持。例如，在如图 19-3 所示，如果计算机 A 安装了 NetBEUI 和 IPX/SPX，它可同只安装了 NetBEUI 的计算机 B 和只安装了 IPX/SPX 的计算机 C 通信，计算机 B 和 C 之间却不可通信，因为它们没有安装共同的协议。

下面部分将讨论不同的协议和怎样确定安装什么协议。

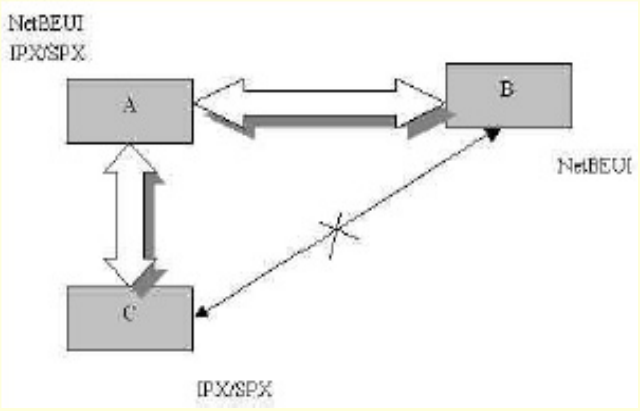


图 19-3　协议的互通

19.2.1　NetBEUI (NetBIOS Enhanced User Interface)

NetBEUI 实际上是一个字首组合词，它表示 NetBIOS 增强型扩展用户接口。IBM 在 1985 年将它引入网络世界。最初是 Microsoft 为 LAN Manager 网络操作系统开发的，之后 Microsoft 又将它纳入了 Windows for Workgroups、Widows95 和 WindowsNT 中。

注意：NetBEUI 是协议，而 NetBIOS 是编程接口。NetBIOS（网络基本输入/输出系统，Network Basic Input/Output System）。

NetBEUI 是默认的 Windows 协议，在中小规模（20～200 台计算机）而且位置比较集中的网络中工作得相当出色。该协议配置简单而且性能不错，NetBEUI 具有自调节功能，提供很好的错误保护，占用的内存也很少。但是 NetBEUI 不像 TCP/IP 和 IPX 那样可路由，它只提供令牌环式的路由。

NetBEUI 协议有如下的优点：

■ 处理客户请求时动态的分配内存，这意味这它仅在需要时才使用内存。

■ 支持拨号通信，这意味着用户可以在家里或者路上以拨号的形式连接到服务器，然后访问网络资源。

■ 同时提供面向连接和无连接的数据传输服务。

■ 可以与实现了如下服务的程序一块工作：NetBEUI、Network DDE（动态数据交换，Dynamic Data Exchange），NetBIOS 之上的 RPC（远过程的调用，Remote Procedure Call）等等。

19.2.2　IPX/SPX

该协议是 Novell 公司在 NetWare 局域网上实现的面向数据报的协议 IPX 和面向会话的协议 SPX。现在，Novell 公司和 Microsoft 公司都为 Windows 系统发行了 32 位的驱动程序。

・IPX (Internetwork Packet Exchange)，是 NetWare 的文件重定向模块的基础协议，仅仅支持没有连接关系的数据报信息。IPX 与 OSI 参考模型中的网络层相对应，其功能与 IP 协议类似，它提供了地址、路由和将信息报文传送到其目的地的服务。

・SPX (Sequenced Packet Exchange) 是一个会话层的面向连接的协议。在 SPX 报发送或接收之前，欲交换信息的双方必须建立连接。一旦建立了连接，会话内部信息报文将可以被发送往任一方向，它们发送的信息报文被保证传送。如果多个信息报同时被发送 SPX 还要监查信息报是否以正确的次序到达目的地。SPX 存在于 OSI 参考模型的网络层，也有部分特性属于会话层。

如图 19-4 所示的表示了 IPX/SPX 与 OSI 参考模型的对应关系。

应用层 表示层 会话层	上层的网络协议： NetWare 核心协议（NCP） 服务通告协议（SAP）等
传输层	SPX
网络层	IPX
数据链路层 物理层	网络体系结构 如以太网、令牌环网等

图 19-4 IPX/SPX 与 OSI 参考模型的对应关系

19.2.3 TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP，传输控制协议/网际协议)，随着 Internet（国际互联网）的火热而出名的，但该协议不只是用于 Internet 的。首先，不像 NetBEUI 和 IPX/SPX 这些单一的协议，TCP/IP 是一套协议和实用程序，它是目前应用最广泛的协议，也是一种工业标准的协议。主要的优点在于：

■ TCP/IP 提供了强有力的 WAN 连接。TCP/IP 的协议组是适应 WAN 的需要而发展的。因此，TCP/IP 是众多 WAN 有效的方法之一，可以用来连接地理上分散的机构，而且主张与 Internet 连接的企业具有利用 Internet 网络连接分支机构到总部的选择权。

■ TCP/IP 是一个开放的系统，允许将不同的操作系统互相连接，而不必担心兼容性的问题。

■ TCP/IP 对 Internet 广泛的支持。允许访问到任何可以找到的、遍及世界的成千上万网站的丰富资源。

理解了 TCP/IP 协议的优点后，开始学习 TCP/IP 协议组的主要内容。

19.3 TCP/IP 基础

正如前面指出的，通信网络是众多的物理网络相互连接成的。而所有的通信协议组的最重要特性就是其使用了一套已经定义的信号发送方法，处理传输的错误、管理路由和数据交付以及控制实际传输的能力。TCP/IP 就是提供以上服务的一个协议组。

19.3.1 TCP/IP 的发展历史

在 70 年代初期，美国国防部开始投资研究阿帕网—ARPANET (Advanced Research Projects Agency Network)，目标是建立一个实用的通信网络，为全国许多实验室和教育机构的大量数据中心连接起来，赋予它们交换数据的能力。在 ARPANET 的研究过程中，为寻求一个能够适应规定要求的解法，TCP/IP 就作为一网络互连的分组交换研究项目。到 1979 年，TCP/IP 的研究工作进展顺利，很多人参加了这项工作，这也促使了美国国防研究计划署成立了一个非正式的委员会来协调和指导通信协议的结构的设计开发工作。这个委员会被称为网际控制和配置委员会。

到 1983 年，TCP/IP 被正式作为军用标准之后，所有连接到 ARPANET 的网络都必须依照新的标准。在此期间，Internet 是最早建立的包括 ARPANET 的网络，后来 ARPANET 被分为 MILNET 和新的较小规模的 ARPANET 网络。MILNET 是用于军事的目的，ARPANET 是用于研究和开发工作。多少年后，ARPANET 的成功大大超出了当初的构想。计算机设施密集的北美、欧洲、日本和世界其他地方都通过各自的子网连接到 Internet，构成了世界上最大的网络。1990 年 ARPANET 被撤销，Internet 被宣布成为正式的全球性网络。

19.3.2 TCP/IP 的 4 层模型

前面提到了 OSI 参考模型的 7 层结构，但 TCP/IP 协议组作为一种分层式的通信协议将不同的功能组合到预定好的网络层里。于是该协议分成了 4 个概念层，分为网络接口层（Network Interface layer）、因特网层（Internet layer）、传输层（Transport layer）以及应用层（Application layer）等层次，如图 19-5 所示。这些层次的每一个都对应于 OSI 参考模型的一个或更多个层次，例如，网络接口层对应于 OSI 参考模型的物理层和数据链路层，互联网层对应于 OSI 参考模型的网络层，传输层对应于 OSI 参考模型的传输层，而应用层对应于 OSI 参考模型

的会话层、表示层和会话层。而且在每一层中，都包含着 TCP/IP 组中的几个最重要协议。

图 19-5　OSI 层与 TCP/IP 层的对应关系

19.3.2.1　网络接口层（Network Interface layer）

此层负责与物理网络进行通信的协议。首先必须了解网络所用的结构，例如令牌环或以太网结构等，并提供了一个允许互联网层与其通信的接口。TCP/IP 并没有提供了专门的网络接口协议，而是旨在提供了灵活性，以适应于各种的网络协议。

19.3.2.2　因特网层（Internet layer）

因特网层提供消息的寻址和把逻辑地址和名称转换成物理地址的功能，而且传输层的所有协议都必须通过使用 IP 来发送数据。因特网层协议含有对报文如何编址和引导、对报文进行分段和重新装配、提供安全信息以及区分所用的服务类型等规则。因特网层中已存在的协议有 IP (因特网协议，Internet Protocol)、ICMP (网间控制报文协议，Internet Control Messaging Protocol)，IGMP (网际分组管理协议，Internet Group Management Protocol) 和 ARP (地址解析协议，Address Resolution Protocol)。

19.3.2.3　传输层（Transport layer）

传输层负责主机与主机之间的端对端的通信。这种通信可以是基于连接的，也可以基于非连接的。该层也包含了两种协议：TCP (传输控制协议，Transmission Control Protocol)和 UDP (用户数据报协议，User Datagram Protocol)。

19.3.2.4　应用层（Application layer）

应用层是在 TCP/IP 模型中的最高层，是负责发生在 OSI 参考模型的会话层、表示层和应用层的所有活动。这一层有很多的协议被开发出来，例如，FTP (文件传输协议，File Transfer Protocol)、Telnet (远程登录)、DNS (域名服务，Domain Name Service)和 SNMP (简单网络管理协议，Simple Network Management Protocol)。

应用层中也包括了使非网络应用程序能够与网络通信的应用程序编程接口（Application Programming Interfaces ），例如 Windows Sockets 和 NetBIOS。

这些层两两之间的接口能够担负起它们彼此相互传递信息的任务。

19.3.3　TCP/IP 协议和技术

事实上，前面提到的 4 层模型只能提供一些指南，实际的工作是由包含在它们的协议完成的。本节将 TCP/IP 协议作为一套协议进行了讨论，而不是只是对它们的两个（TCP 协议和 IP 协议）进行说明。其中有 6 个主要的协议与 TCP/IP 紧密相关：

- 传输控制协议（TCP）
- 用户数据报协议（UDP）

- 因特网协议（IP）
- 网间控制报文协议（ICMP）
- 网间分组管理协议（IGMP）
- 地址解析协议（ARP）

19.3.3.1 传输控制协议（TCP）

该协议是基于连接的协议，提供了可靠的数据传输，它要求数据在两台计算机之间进行传输之前必须建立一个会话进程。会话将在主机之间建立一个正式的会话，使错误修复得以实现。TCP 协议是寄存在传输层的，位于应用层和因特网层之间，能够为数据的顺利发送往目的地提供了一种可靠的、有保证的机制。

TCP 把数据分为字节流，而不是单个帧。较大的消息被分成了小段，然后分段传输。TCP 的数据报被发送到套接字（或软接口，Socket）或端口，然后它能校验并保证一台计算机所发出的所有数据报在另一端被接收到。而且它会通过跟踪通信过程中单个数据报的发送和接收，基于连接地保证了它们的正确发送。当一个数据报被发出时，会话能够通过监视数据报的发出时间、发出顺序并通知发送者它的发送时间，以便它能够继续被发送，达到跟踪单个数据报进程的目标。如果因为某种原因丢失了一些数据报，可使发送端的机器进行重发。

另外，TCP 机制还提供了流量控制和数据包的排序。当然，由于要建立一个会话并保证数据报的发送，在使用 TCP 进行数据报传输的时候会有一些额外的开销。

初始化一个 TCP 会话的过程常被称为 3 次握手（Three-Way Handshake）。在此过程中间，两台计算机要对它们每一次所发数据量的跟踪方法，收到数据时的应答代号，以及何时不再需要连接等达成共识。只有在这个会话被建立起来之后，数据传输才能开始。为提供可靠的发布，TCP 协议将数据报按一定的顺序进行安排，并要求它们到达其目的地发回应答信号，以便它继续发送新的数据。所以在传输大宗数据的情况下，或应用程序需要在数据被接收之后得到应答信号时，一般常使用 TCP 协议。

会话完成之后，关闭会话的正式过程确保了通信中止之前所有的数据都被传输和确认。

19.3.3.2 用户数据报协议（UDP）

该协议是一种基于非连接的协议，它并不需要两台计算机在传输数据之前建立一个会话，这与 TCP 协议正相反。但是因为 UDP 协议没有在计算机之间建立会话，因此它不能提供数据报的顺序发布，而且也不能在数据报被丢失之后保证重发。

但对于一个应用程序来说并不需要时时保持一个连接，而且事实上也没有必要，因为这样将增加了通信量。这样一来，对于流量很大的音频和视频传输中，不加保障的数据报发送不仅能够传输大量的数据（因为广播需要极少甚至不需要额外的开销），而且在这种情况下重发是没有必要的。

19.3.3.3 因特网协议（IP）

因特网协议是 TCP/IP 的最重要的组成部分，因为这个协议集是以 IP 作为基础的地址和传输的设备。如果不通过因特网层的 IP 协议进行通信，那么传输层的通信就根本无从谈起。IP 协议里面包括了地址分配、广播、对数据进行划分和重组的功能。

IP 协议的最基本的要素是它使用的地址空间。在网络上，每一台计算机都被分配了一个 32 位的地址，也即平常所说的互联网地址或 IP 地址。互联网标准定义了五种类型的 IP 地址，当前有 A、B、C、D、E 共五级的地址。一个计算机特有的互联网地址是由 A、B 和 C 类的地址派生而来的，D 类的地址是用来将计算机连接成为一个功能组，E 类的地址现在只是在实验的阶段，并不能使用。

如果计算机连到因特网上的时候，它必须要有一个网络地址，而且只能由 InterNIC 分配。InterNIC 管理网络地址的分配，以保证每一个计算机得到的网络 ID 号是在互联网上是独一无二的。这样一来 IP 协议就能对这个特定的地址进行维护、使用和调整，以便两台计算机之间的通信。而且如果 IP 从网络层收到不属于本身地址的数据的时候，也判断出不是网络广播的时候，它将放弃当前的数据报而不对它进行进一步的处理。

尽管 IP 协议能够将报文直接发送到特定的计算机，但是它却宁愿将报文发往一段物理网络连接的所有机器上，这就是 IP 协议的广播功能。如果计算机从网络接口层得到一个广播的数据报，它必须对此报文进行接收并进行处理，好像这个报文就是发给它的一样。

另外，IP 协议的任务之一就是将过长的数据报文分解成适应预先规定的数据报的尺寸进行分段传输，然后到达目的计算机的时候将几个数据报再进行重组还原成原来的数据。这个功能使网络的流量得到充分的利用，

以便数据量很大的数据也能利用基础网络进行传输。IP 通过划分将数据分成了一些能够控制的帧，并为没一个数据报加上一定的控制代号，以便在数据序列中标识它们，从而使每个数据报可以在目的计算机里得到重组。

还有一个方面，IP 定义了存活时间的概念，TTL（Time to Live）规范被设置为 128 的缺省值，它表示 128 个波跳（Hop）或 128 毫秒。路由器每处理一次数据报，它就将 TTL 减少一个单位，如果数据报在超过 1 秒的时间中还没有被路由器传输出去，路由器可以将 TTL 减少不止一个单位。假如数据报到达目的计算机的时候 TTL 已经超时，那么它就不得不被网络丢弃。这样的好处就避免了数据报在网络中无限的循环从而耗费大量的带宽和数据同步开销并最终带来灾难性的后果。

19.3.3.4　网间控制报文协议（ICMP）

假定一个数据报文被抛弃的原因是 TTL 区域达到了 0，或者一个大的报文中有一两个数据报在传输的过程中被丢弃了，那么发送端如何知道有出错的信息返回呢？这就是网间控制报文协议的任务，它负责报告与 IP 数据报发布有关的错误和消息。此外，它还能发出数据源结束以及其他的自调节信令，这些信令能够自动调整和优化数据的传输过程。

通常验证网络上的一个 IP 地址是否确实存在的最常用的工具是个人互联网探索器（Ping）。它使用了网间控制报文协议（ICMP）的反馈请求和应答机制。反馈请求是一种简单的有向数据报，它用来请求网上某一特定 IP 地址的应答消息。如果具有该地址的计算机存在并接收到上述请求，那么就按规定发出一个反馈应答报文，该报文表明向源计算机通知它的存在。Ping 工具程序的最常用的两种用途：确认主机间端到端的连接和测量往返延迟时间。

19.3.3.5　网间分组管理协议（IGMP）

网间分组管理协议是一套规范，它允许按前面所述的 D 类地址向 IP 地址组添加和删除计算机。IP 负责将 D 类地址分配到各计算机组，以使它们能够作为一个功能单元接收广播数据。它也提供了带有多播组标识的路由器，它们能够在其连接的网络里是活动的。这个消息在传播到其他的路由器上，致使整个网络都支持多播。

19.3.3.6　地址解析协议（ARP）

在局域网或广域网上从一台计算机向另外一台计算机发送数据报，如果目的计算机的物理地址是未知的，就需要一些方法来解决 IP 地址与物理地址相对应的关系，除非 IP 协议打算在网络上进行全程广播。为得到这个信息，就依赖地址解析协议，它负责将网络上的 IP 地址映射到存储器中的物理地址。另外也有一个协议叫做逆向地址解析协议（RARP），它能逆向映射，将一个物理地址转换成 IP 地址。

提供 IP 地址到物理地址的解析的很有效的方法是对每一台计算机建立一个转换表。当一个应用程序发送数据到另一台计算机时，软件能够检查转换表寻找相应的物理地址。如果它的内存里缺少某一映射，它就必须到网络上寻找一个。

通常 ARP 是通过本地广播的方法来寻找计算机的物理地址，只要目标地址是本地的，ARP 所作的不过是对计算机进行一次本地广播，并向 IP 返回相应的物理地址。IP 协议知道目标地址是本地的情况下，只需将数据报附上目标计算机物理地址之上的 IP 地址即可。

但是实际上，目标地址经常在远程网络上，这时路径往往包括了沿途的好几个路由器。为达到其他的网络，需要路由器监听该报文并把它向前传递。然而，使它监听报文的唯一途径要么进行一次广播，要么将该报文发往路由器的物理地址。IP 可以非常敏锐的认识到 IP 地址在哪个远程网络里，而且数据报必须被发往路由器进行处理，但它不知道相关路由器的物理地址，为此它必须求助于 ARP 并由它寻找。

19.3.4　TCP/IP 里著名的服务和高层协议

在 TCP 和 UDP 处理数据报后将之提交给高层的协议 TCP/IP 协议组中的高级协议中常包括了 OSI 参考模型中会话层、表示层、应用层的功能。这些协议提供了如文件传输、电子邮件终端等功能。本节就讨论 Internet 会遇到的常用应用及协议。

19.3.4.1　域名服务（Domain Name System，DNS）

DNS 是一种服务，把 IP 地址翻译成易于记忆的名字的机制。在 TCP/IP 的早期，主机设备是通过它们的 IP 地址进行通信，或者通过每台主机上所安装的名为 HOSTS 的文件标识。HOSTS 文件中包含了 Internet 上所有

计算机的 IP 地址与主机名称的映射。但随着 Internet 的日益壮大，主机数目突飞猛进，维护和管理 HOSTS 文件副本的工作变得难于管理。另外，定期下载更新的 HOSTS 文件也占用了大量的通信线路。很明显，这就需要一个中心数据库，执行注册和主机名称与 IP 地址的注册和转换等功能。

名字解析有多种实现的方法，其中主机表方案最简单。主机表是一个文本文件，它存有 IP 地址和对应的主机名。程序中使用主机名时，该应用在主机表中查找是否有该主机名。若找到了，则将信息送给该主机。这样每次传输文件时可用主机名，不用 IP 地址。

主机表很容易实现，但也不能太大。而且在动态网络环境下需要不断修改主机名，因此它只能适应与极小的网络。而 DNS 创建了一个大型的、分布式、层次型的数据库，从而克服了主机表的限制。在整个数据库（名字空间）中被分为若干各自维护的单位（域），每个域中含其子域的地址信息。

InterNIC (互联网信息中心，Internet Network Information Center)负责高级域名的管理。这些高级域名有.com (表示商业组织)，.edu (表示教育机构，如大学等)，.gov (表示政府机构)，以及.org (表示非赢利的组织)，此外还有表示国家的域名。表 19-1 对常见的一些互联网域名作了一些总结。

表 19-1 组织域名类型

DNS 域名	组织的类型
.com	Commercial：分配给商业组织。如 microsoft.com
.edu	Educational：分配给教育机构。
.gov	Government：分配给政府机构。如 whitehouse.gov
.mil	Military：分配给美国政府军事机构。
.org	非赢利的组织。
.net	Networking organization：分配给网络组织。

由于顶级的域名实在太少，所以 Internet Ad Hoc Committee (IAHC)又创建了以下新的顶级域，从 1997 年起开始使用：

.store——货物交易

.webWeb——事务组

.arts——文化艺术团体

.rec——娱乐休闲资源

.info——信息服务

.nom—个人

另外，随着 Internet 的国际化发展，就有必要引进地理域（ geographical domains）标识每个国家。Internet 采用 ISO 3166 建立的两字符国家代码，例如，www.bplus.au 站点位于澳大利亚。

19.3.4.2 文件传输协议（File Transmission Protocol, FTP）

文件传输协议（FTP）是一种高层的客户/服务器协议，用于向远端主机传送文本和二进制文件和从远端主机取得文本和二进制文件。

FTP 服务器在 TCP 端口 21 上倾听到来的 FTP 请求。请求到达后，服务器会提示用户输入有效的用户名和口令，然后才能访问 FTP 服务器，用该用户名的有限的权限上装和下载文件。但大多数的服务器有一特殊的用户名 Anonymous (匿名)，口令可以输入电子邮件的地址，这样就可以让未注册的用户可访问共用的文件。

除了 Web 服务器能访问 FTP 之外，一个好的客户端软件是最有用的工具。当要传送大量的文件的时候，一个专用的客户端软件会更快地完成任务也更方便。两种最著名的 FTP 客户端软件是 WS—FTP 和 CuteFTP。如表 19-2 所示就显示了 FTP 最常用的命令：

因为各 FTP 服务器支持的命令不尽相同，只能在登录 FTP 服务器后输入：

help command

来得到关于该命令的详细信息。

表 19-2　FTP 常用的命令字

命 令	用 法
ascii	设置文件的传输类型为 ASCII（用于传输 ASCII 文件）
bin OR binary	设置文件的传输类型为二进制（用于传输二进制文件）
Cd directory	改换当前目录
close	关闭到当前的连接
Dir	列当前的目录文件内容
Get filename	下载该文件
hash	在传输的每 1724，2048 和 4096 字节打印一个#号
Help	显示可用命令的清单
Lcd directory	进入本地系统的目录（非 FTP 服务器的）
Ls	列出当前目录中的文件
Mget operator	下载匹配操作符的所有文件
Mput operator	上载匹配操作符的所有文件
Open hostname	在该主机的 FTP 服务器上打开一个新的 FTP 会话
Put filename	上载一个文件
Pwd	列出当前工作的目录
Rmdir directory	删除该目录

19.3.4.3　简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）

SMTP 与 FTP 一样，是用于主机间传输数据的高层客户/服务器的协议。SMTP 的作用是提供可靠的信息发送机制，为达到这个目的，SMTP 是使用了 TCP 而非 UDP。但不完全由它来确认信息已传输给指定收信人，因为任何的 Internet 的使用者自己也可以查看。

STMP 是基于一种存储–转发（Store-and-forward ）的模式，在这种模式下，所有的邮件信息作为一个整体从发送主机传输到目标主机，中途可以经过多个主机的存储和转发。当信件到达目的主机后经过重组，转到一个存储地点——通常叫信箱——等待用户来检索。

19.3.4.4　终端登录（Telnet）

Telnet 是位于上层的终端模拟协议，它可以使一台主机上的用户可以登录到另一台远程主机上，并在上面建立一个终端对话的过程。就用户和远程主机而言，似乎是用户就坐在远程主机的前面。

19.3.4.5　超文本传输协议(HTTP)

HTTP 是和 WWW 关系最密切的协议。在 Internet 上，使用 Web 浏览器时，HTTP 协议负责传输 Web 页面。HTTP 定义了 Web 浏览器与服务器之间的通信。典型的 HTTP 服务中，Web 浏览器初始化与服务器间的连接，并请求某文档或服务。服务器处理请求并往所要求的 Web 浏览器传回文档。

Web 浏览器用统一资源定位器（URL）请求资源。URL 用于标识协议、网络主机名、文件路径和文件名。Web 浏览器用此公共标识来请求文档。

Web 文档用 HTML 语言来描述，而 HTML 语言不依赖任何一种平台，用简单的记事本程序都可以编写出来，它定义了超文本文档的外观。

19.4 什么是 Internet

简单的定义，计算机的网络就是通过电缆，电话线或其他的通信线路和设备将两台或两台以上的物理位置相同的或不同的计算机连接起来。而 Internet 就是全球最大的、开放的、有众多网络互连而成的计算机互联网。

但是这样描述上面的 Internet 又过于空乏，计算机网络仅仅是传输信息的媒介，而 Internet 的美妙与实用在于信息的本身。当计算机连入计算机网络的时候，就可以与其他人共享在网络上的资源，如文件、程序、打印机等等。从网络通信的角度来看，Internet 是一个以 TCP/IP 网络协议连接各个国家、各个地区、各个机构的计算机网络的数据计算机网。从信息资源的角度来看，Internet 是一个集各个部门、各个领域的各种信息资源为一体，供网上用户共享的信息资源网。

所以当了解到 Internet 所提供的服务及各种各样实用而有趣的巨大的信息资源时，一定会觉得 Internet 是一个庞大的数据资源网，它把全世界内各部门，各领域的信息资源都连为一体。只要计算机连上 Internet 后，不但可以与网上的任意用户交换信件，也可以跨越地区和国界使用远程计算机的资源，查询网上的各种各样的数据并获取你所需要的信息与数据。

Internet 可堪称人类历史上最伟大的成就之一，它的出现可以说是世界经济由工业化走向信息化的里程碑。它第一次使如此众多的人们感受到地球村的概念，而且 Internet 打破了传统的国界界限。在这里，你会发现人们能够自然地沟通和互相帮助，你会看到 Internet 对人类的文明，社会发展与进步所做出的贡献。

19.5 Internet 的地址

在网络通信的最底层，所有的网络设备都必须使用物理地址进行通信。需要与网络的所有其他设备进行通信的任何设备，都必须最终确定目标设备的物理地址，或者路由器的物理地址，(如果远程设备是位于不同的子网上，路由器就是用来与该远程设备进行通信的)。

19.5.1 IP 地址的编制

但是由于网络设备的物理地址比较长，而且比较隐晦，对用户也不够友好，就必须用 IP 地址来标识网络设备的位置。IP 地址约定，从一个范围比较广的标识一个独一无二的网络开始，然后缩小范围，直到标识出该网络上的单机为止。一旦确定了这种的编址方法，那么任何主机都能够与该网络上的或通过 Internet 连入的其他网络上的主机进行通信。

一个 IP 地址是由 4 字节 32 位数值组成，习惯上用点将 4 字节的十进制分隔开来，这种格式叫做 dotted decimal notation（点分十进制格式），例如 202.112.104.13。其实 IP 地址的每一个八位组（Octet）是一个八位二进制数(称做 byte)，用 0～255 之间的十进制数表示。以上一个例子作解释：

二进制格式是：11001010　01110000　01101000　00001101

点分十进制格式是：202.112.104.13

19.5.2 IP 地址的种类

Internet 标准定义了 5 种类型的 IP 地址。3 种基本的 IP 地址是 A 类、B 类和 C 类，还有 D 类地址是用来多目的传输，E 类地址是用来将来的扩展使用的。网络的种类决定了 TCP/IP 地址的哪一部分用于表示该网络，以及哪一部分是标识网络上的主机。

19.5.2.1 A 类地址

Internet 的 A 类地址只用第一个字节来表明网络地址，其他的 3 个字节都可以用来给网络中的主机分配地址。所以只有很少的 A 类网络地址，确切的说只有 126 个。但是 A 类地址有 2 个字节用于主机地址，所以每个网络地址可以包括 2^{24}，即 16，774，214 台主机地址。但是可以用计算器来计算 2^{24}，得到的却是 16，774，216，而不是 16，774，214，其中是因为所有位都是 0 或 1 的 IP 地址被保留下来用于特殊的用途。

使用 A 类地址可以分配的网络地址是：

1.x.y.z126.x.y.z。

因为 A 类地址确实比较少，只能为最大的组织机构或政府实体所保留。只有象 IBM 或者 Microsoft 那样的大公司才能申请取得 A 类地址。

> 提示：在一个单独的网络里分配 16 000 000 台主机，是一个很大的数目。分配 A 类地址的单位会将进一步划分主机 ID，以创建多个不同的内部子网。这种做法就是划分子网。可以在一个大型的网络里，分配其宝贵的 IP 地址。

19.5.2.2　B 类地址

因为 A 类地址不多，所以一个相当大的公司也只能申请到 B 类地址，而且随着 Internet 的日益壮大，甚至连 B 类地址也难以取得。

Internet 的 B 类地址用两个字节来表明网络地址，但总是将前两位设置为 10，因为这表明了互联网中所有的 IP 地址均是这样划分，前两个八位组（16 位）是指定的网络地址，而后两个八位组（16 位）指定了主机地址。因此总共有 2^{14}，即 16，384 个 B 类网络地址。B 类地址可以有两个字节用于主机地址，因此也有 2^{16}，即 65，534 个主机。

而使用 B 类地址可以分配的网络地址是：

128.0.y.z——191.255.y.z。

19.5.2.3　C 类地址

C 类地址是为较小的局域网而准备的，由于 A 类和 B 类的地址的缺乏，已经迫使许多的大型局域网也使用 C 类地址。C 类地址用前 3 个字节来表明网络地址，但总是将前 3 位设置为 110，因为这表明了互联网中所有的 IP 地址均是这样划分，前 3 个 8 位组（24 位）是指定的网络地址，而后一个 8 位组（8 位）指定了主机地址。那么有 2^{22}，约有 2，097，152 个 C 类网络地址，每一位均是 0 或 1 的地址被保留，故要比 2^{22} 少 2。C 类地址中只有一个字节用于主机地址，所以每一 C 类地址可容纳 2^{8}，即 254 台主机。

使用 C 类地址可以分配的网络地址是：

192.0.0.z——223.255.255.z。

> 提示：C 类地址把单个网络上的主机数限定在 254 个之内，一般需要较多主机地址的机构乐意申请多个 C 类地址。

19.5.2.4　D 类地址和 E 类地址

即使全面描述了 Internet 的 D 类地址和 E 类地址，也不可能碰到它们。D 类地址是用来多播（Multicasting）而用的，多播就是同时将消息发送给一组主机。D 类地址的范围从 244.0.0.0 到 239.255.255.254。而 E 类地址是为了将来的扩张而用的，同样也用于实验目的。范围从 240.0.0.0～255.255.255.255。

19.5.3　主机地址系统

向 InterNIC 申请到一批地址时，所获得的只是网络地址部分，还要用户来为每一台计算机分配具体的地址。例如，如果申请了而且被批准了一个 C 类地址，下面来看一看如何给计算机分配主机地址，并且如何管理新的 C 类地址。

Internet 中已经定义了分配主机地址的约定，如果不遵循这些约定的话，在不同制造商的设备中就会引起兼容性的问题。首先，因为主机地址是用来标识网络上的特定的接口的，所以每一主机接口都必须有一个独一无二的主机地址。其次，分配给主机的地址，不能全为 0 或者全为 1。另外，分配给主机的地址必须在其子网的 IP 地址范围内。

假如 InterNIC 批准的 IP 地址是 202.112.104.0。因为所有的主机必须赋予一个非零的主机号，所以可以分配给计算机的最低地址是 202.112.104.1，最高的是 202.112.104.254，而 255 号地址是因为所有位均为 1 而保留给

多播使用。这表明可以有 254 个地址用于给网络上的计算机来分配。

可以用两种方法之一来分配 IP 地址：

■ 静态 IP 地址分配

这需要为手工为每一台设备设置特定的 IP 地址，而这个地址一旦设定就不再改变。怎样设置 IP 地址对不同的设备是各不相同的，对一些计算机的系统来说需要编辑配置文件。

■ 动态 IP 地址分配

它表明要建立一个 IP 地址集，可以根据需要给设备分配 IP 地址。通过动态主机配置协议（DHCP）就能实现动态 IP 地址分配。

但是一旦设备的数目增加，几乎就不可能用手工进行配置。而且随着移动通信设备的出现，对计算机随处上网的需求不断增加都要求动态的 IP 地址分配，今天大多数的网络管理员都喜欢用 DHCP 来从 IP 地址集为需要的设备分配动态的 IP 地址。

19.5.4 子网

出于管理、性能和安全的考虑，可以将单一的网络划分成多个物理网络，并使用路由器把它们联结起来。子网划分技术就是能够使单个网络地址横跨几个物理网络。

随着 Internet 的兴旺，原来以为用之不完的网络地址变得越来越奇缺。在以前，如果告诉 InterNIC 说有 3 个不同的办公地点，那 InterNIC 会自然的分配 3 个不同的网络地址。即使每个地方都有 10 台的计算机连在一起，那也将另外的 244 个地址浪费掉了。但是那时候也不会觉得有什么大不了的，因为它们觉得有太多的 IP 地址可用却太少的需求。如今就抢着要一个 C 类地址。这样就迫使划分已分配的地址空间，在每个区使用可用地址的一部分。

当网络划分为更易于管理的多个部分时，每一个任务就变得更小和更易于控制。子网使得指定单独的管理员负责管理每个子网的本地用户、计算机以及其他的网络资源更为容易。

随着网络的增长，容纳了更多的主机，因而也使网络通信变得更为繁忙，这样会导致冲突、丢失数据包以及重传，降低了主机间的通信效率。子网划分通过使用路由器指导通信，所以也能够减少了网络的阻塞。

另外，路由器就像一堵墙把各个子网隔离开，这样本地的通就不会转发到其他的子网。同一子网的主机之间的广播和通信就只能在它们所属的子网中进行。对于需要互相通信的不同子网的主机，可以配置路由器筛选通信，使需要传送到其他子网上的信息可以被转发。

出于安全的考虑，单位也可以创建隔离网络的子网。一个部门也许会把信息放在有敏感信息的网络服务器上，可以配置子网将来自 Internet 的攻击阻止在外。

19.5.5 子网屏蔽

子网屏蔽是一个 32 位的数字，它告诉主机 IP 地址的哪些位对应于网络地址，哪些位对应于主机地址。TCP/IP 协议使用子网屏蔽判断目标主机地址是位于本地地址，还是位于远程子网。

屏蔽网络地址即可以实现以上的判断，屏蔽只是简单的指定网络的 ID 和主机 ID 的分界点。子网屏蔽中对应于网络地址的所有位都被设为 1，而对应于主机地址的所有位都被设为 0。

19.6 Internet 的应用工具

Internet 丰富的资源涉及到人们所从事的各个领域，行业以及社会公共服务的方面，包括了自然科学，社会科学，技术科学，农业，气象，邮电，医学，军事，机械等。Internet 的信息资源是分布在整个网络中的没有统一的组织和管理，也没有统一的目录。以下是对于用户来说，Internet 提供的一些基本的信息服务：

■ 通信：如电子邮件（E-mail），电子新闻（Usenet News），对话（Talk）等。

■ 获取信息：如匿名文件传送（Anonymous FTP），索引检索数据库（Archie），分布式文本检索（Gopher），万维网（WWW）等。

■ 共享计算机资源：如远程登录 Telnet、客户机/服务器系统等。

第 20 章　连接到 INTERNET

与 Internet 的连接主要包括硬件的连接和软件的配置。硬件的连接主要是通过本地局域网（LAN）、调制解调器和电话线以及其他的线路进行。软件的安装包括安装网络适配卡的驱动程序、TCP/IP 协议、调制解调器驱动程序及其配置，拨号网络适配器的安装、连接的建立等等。

如果用户所在的公司、学校、单位中已经建立 LAN 网，并已经与 Internet 相连，那么选择加入当地的局域网是较为适宜的方法。利用现有的电话线，既降低了联网的成本，又使得上网的费用对绝大多数的家庭来说可以接受。如何将自己的计算机通过现有的电话线与某一个 Internet 上的主机连接，也就是拨号上网的话题也就成为了热点。

本章的主要内容包括有：

- 硬件的安装，例如安装网络适配卡，调制解调器等
- 软件的安装，例如上网必需拨号程序等

20.1　安装硬件

20.1.1　安装和配置网络适配卡(Web Adapter)

对于要加入 LAN 的用户来说，网络适配卡往往成为必须的硬件设备。网络适配卡通常具有较高的传输速度，而且不占用 COM 通信端口,而受到广泛的应用。

将一块网络适配卡正确安装到计算机后，就可以开始网络适配卡驱动程序的安装。因为 Windows 2000 像 Windows 98 和 Windows 95 一样支持即插即用 P&P（Plug & Play）的功能，这样对于安装网络适配卡来说就方便多了。在正确安装了网络适配卡后的第一次开机时，Windows 2000 会自动对硬件进行检测，如果发现新的硬件，会提示用户选择驱动程序。一般用户应选择硬件厂商提供的驱动程序，安装网络适配卡随带的驱动程序。如果没有硬件厂商提供的驱动程序或者该程序因为种种原因丢失或损坏，用户也可以选择 Windows 默认的驱动程序来安装 Windows 自带的驱动程序。一般较为常见的网络适配卡都会在 Windows 2000 中具有相应的驱动程序。

即插即用的另一好处就是其占用的计算机资源（端口、中断和 IO 地址）一般都不用自己动手配置，即使需要也可以通过软件的方法设定，而不必在网络适配卡上跳线，而这些配置一般是最棘手的问题，所以用户可以尽可能的选择带有即插即用功能的网络适配卡，这样可以省去很多麻烦。

如果手中的网络适配卡不支持即插即用功能也不必担心，一般配置网络适配卡也非常的方便，执行以下的步骤安装网络适配卡（假如网络适配卡是以太网络适配卡）：

（1）在“开始”菜单中的“设置”选择“控制面板”，如图 20-1 所示，双击“添加/删除硬件”图标，就会出现欢迎窗口提示用户进入新的安装硬件向导，如图 20-2 所示。

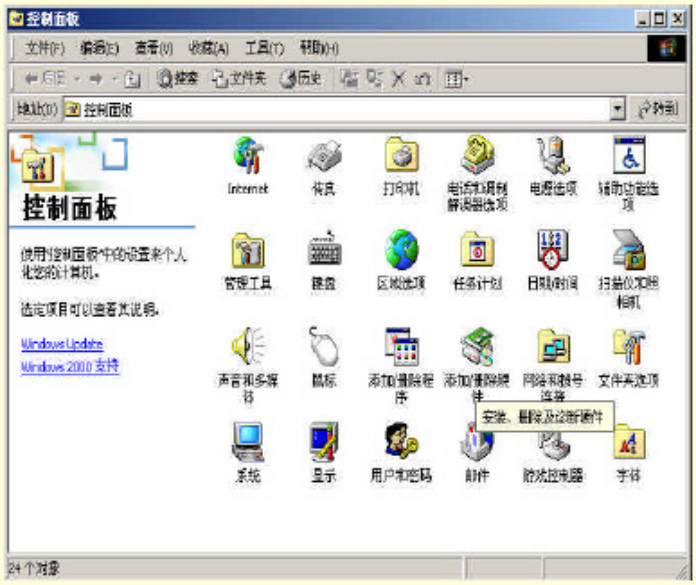


图 20-1 “ 控制面板 ” 窗口

图 20-2 添加/删除硬件向导

（2）单击 “ 下一步 ” 按钮，提示将要进行的对硬件进行的任务，选择 “ 添加/排除设备故障 ”，如图 20-3 **所示。**

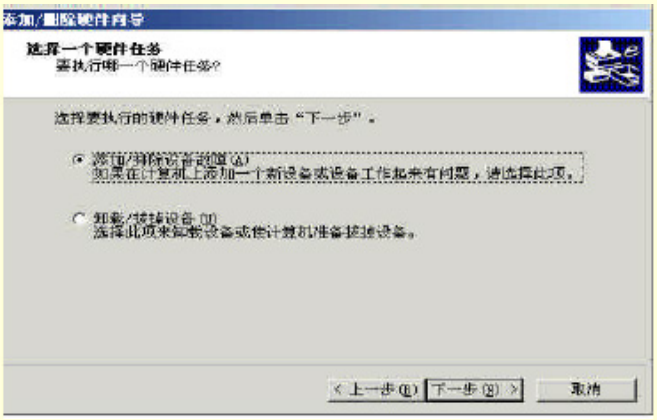


图 20-3 选择 “ 添加/排除设备故障 ”

（3）单击 “ 下一步 ” 按钮，Windows 2000 **会对硬件设备进行搜索，以找出新的硬件，如图** 20-4 **所示。单**

击“下一步”按钮，会完成对以太网络适配卡的安装，如图 20-5 所示。

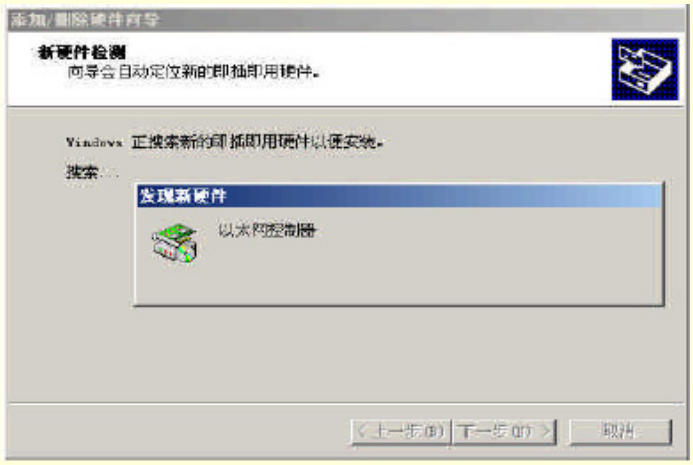


图 20-4　找到新的硬件“以太网控制器”

图 20-5　成功安装网络适配卡

（4）如果还没有找到新的硬件的话，会弹出一个询问框，如图 20-6 所示。用户可以在询问框中选择“添加新硬件”。

（5）单击“下一步按钮”，Windows 2000 会提示用户，可以对硬件重新搜索，也可以在列表中查找，如图 20-7 所示。

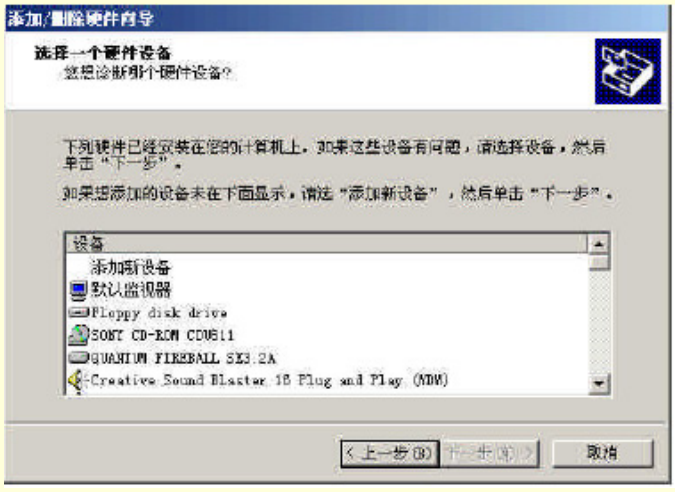


图 20-6　询问框中选择“添加新设备”

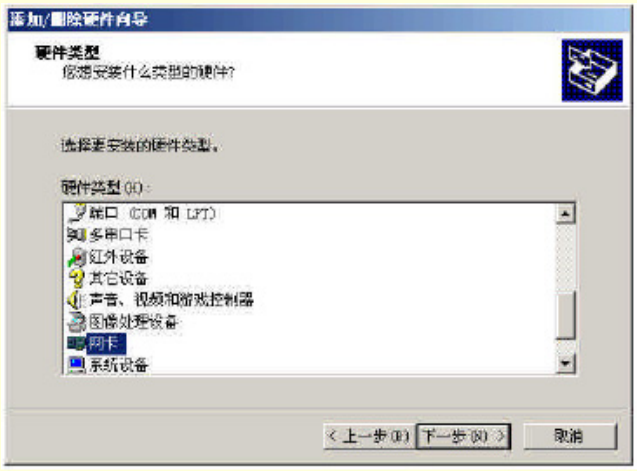


图 20-7　列表中选择“网卡”

提示：在这一个状态下，还可以对硬件进行诊断，更改硬件的资源或者进行配置。

（6）可以在列表中选择 Windows 2000 提供的驱动程序,选择“制造商”里的厂商，而后选择“网卡”里的网络适配卡类型。或者选择“从磁盘安装”，如图 20-8 所示。

提示：如果用户有随网络适配卡附带的驱动程序，最好还是安装该驱动程序，因为随制造商提供的驱动程序能更好的与网络适配卡配合，最大发挥该网卡的功能。

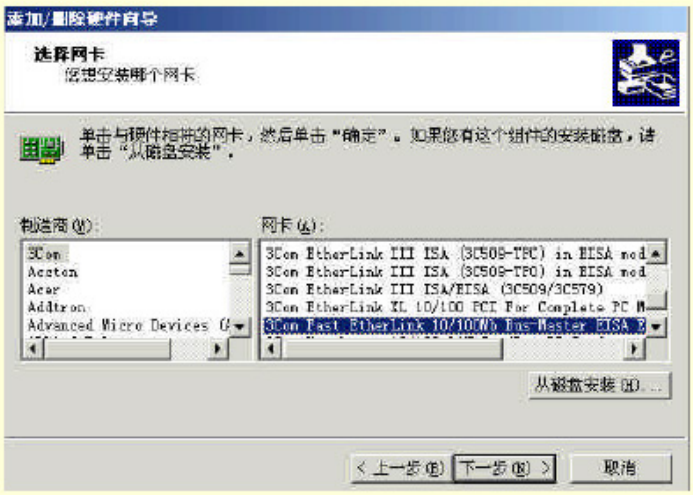


图 20-8　在列表中查找相应的网络适配器或者选择“从磁盘安装”

（7）插入制造商提供的软盘，找到相应的驱动程序，安装即可，如图 20-9 所示。之后可能会提示重新启动计算机。

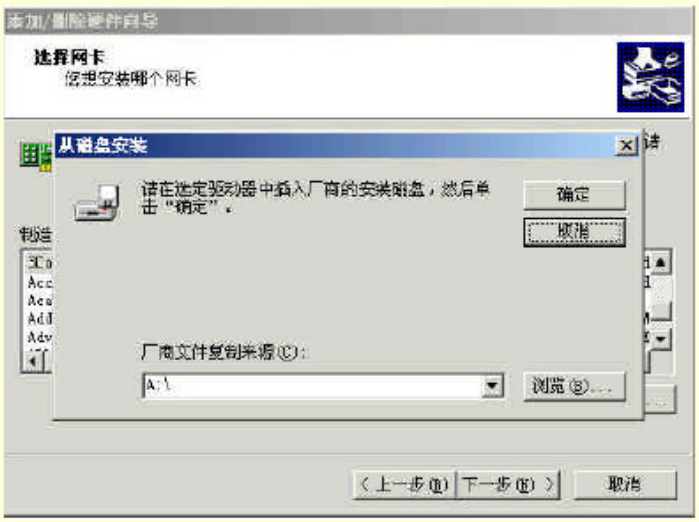


图 20-9　在厂商提供的软盘中选择驱动程序

一般这样安装网络适配卡，Windows 2000 会自动的将计算机的资源配置正确，所以用户不用管其他的资源配置。可以打开“控制面板”中的“管理工具”，在“设备管理器”中找到刚安装上的以太网络适配卡，如图 20-10 所示。

双击刚安装上的以太网络适配卡，可以看到它的属性，如图 20-11 所示，也可以更改它的属性。在“常规”选项卡中可以看到该网络适配卡的“设备类型”、“制造商”和“位置”，另外还特别强调设备运行的状态。在底部还可以选择对该设备的应用，例如：“使用这个设备（启用）”或者“不要使用这个设备（停用）”。

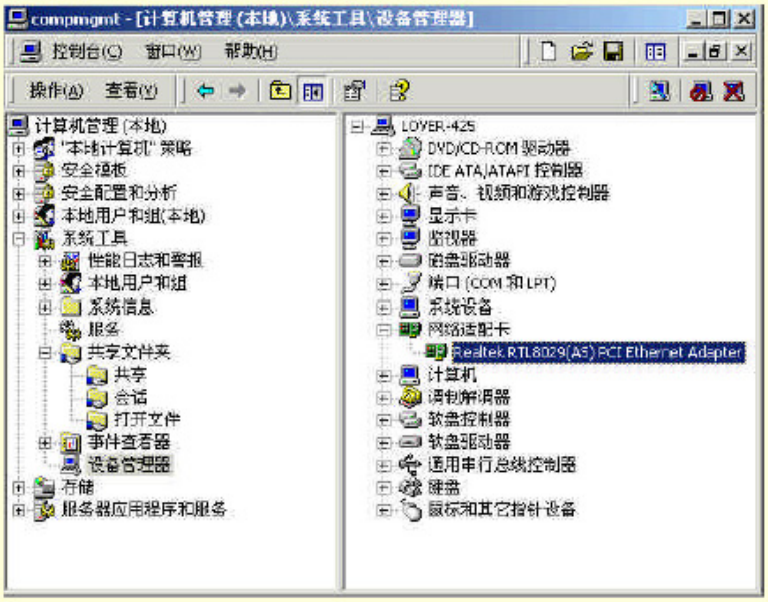


图 20-10　设备管理器中的网络适配卡

提示：如果对这设备不了解，或者这设备有问题可以单击疑难解答，用来启动 Windows 帮助。

图 20-11 “网络适配器”的属性

在“高级”选项卡中，用户可以对网络适配卡的线路速度进行配置，如图 20-12 所示。其中左边是该网络适配卡列出的“属性”，在右边是该属性的“值”。

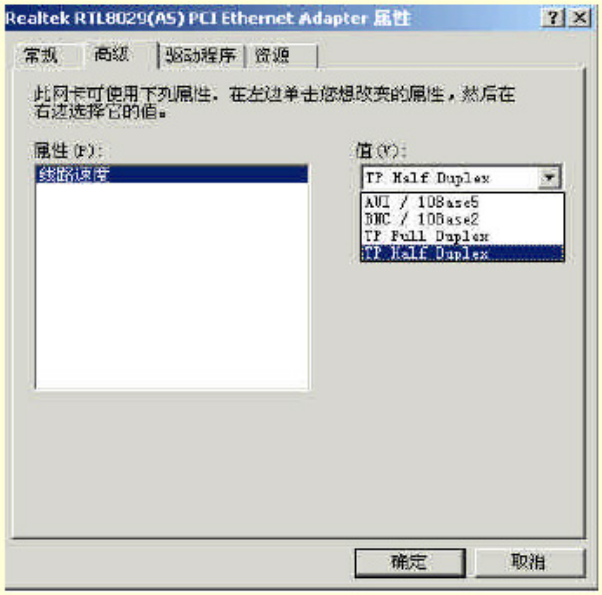


图 20-12 “高级”选项卡

- AUI：Attachment Unit Interface，连接单元接口。
- BNC：同轴电缆接插件。
- TP FULL DUPLEX：全双工的方式。
- TP HALF DUPLEX：半双工的方式。

半双工的方式：通道两端都具有接收和发送功能，但是不能在同一时刻内接收和发送。
全双工的方式：可以在同一时刻内接收与发送。

在“驱动程序”选项卡中，可以了解到驱动程序的提供商、驱动程序的日期和版本，还有数字签名程序。在下面还有 3 个按钮：“驱动程序详细信息”、“卸载”和“更新驱动程序”。

- 驱动程序详细信息：提供了驱动程序文件的地址、提供商、版本号和版权。

■ 卸载：提供卸载的途径。

■ 更新驱动程序：可以弹出一个更新的欢迎向导，帮助更新该设备。

在“资源”选项卡中，可以对“资源的设置”进行更改，如图 20-13 所示。其中“资源类型”包括了“输入/输出范围”和“中断请求”。另外，也可以设置当前的设置是基于何种配置，是否“使用自动设置”，是否要“更改设置”，还可以提供“冲突设备列表”。

至此，完成了对网络适配卡的配置工作,下面来谈一谈调制解调器的性能与安装。

图 20-13　“资源”选项卡

20.1.2　调制解调器

对于绝大多数的家庭来说，通过调制解调器和电话线与 Internet 相连是一种花费廉价而实用的方法。

利用调制解调器可以在个人计算机和网络间建立一个连接，因为计算机只认识 0、1 的二进制数字信号，而调制解调器和电话线中只能传输连续的模拟信号（Analog）。因此在利用电话线传递信号之前，从计算机里出来的像 0、1 这样的数字信号必须转变成模拟信号才能在电话线中传输。调制解调器就起着这样的作用，即调制。不仅如此，它还能将电话线中传来的模拟信号转变成为数字信号，即解调作用。因此安装了调制解调器，计算机才能将数据发送到电话线中传输或者接收电话线的数据。

20.1.2.1　认识调制解调器

为了让 PC 机连上 Internet ，一台调制解调器是必不可少的。但如何选购一个性能良好的调制解调器呢？这可能是用户最关心的话题了。

在市场上，可以见到各种各样品牌、型号的调制解调器，用户在选择的时候不仅要关心调制解调器的价格外，还要注意以下的 3 个因素：

■ 速度

速度是调制解调器的主要技术指标，它影响了用户时的速度。调制解调器的速度一般以每一秒钟内通过调制解调器可以传输的最大数据位数，也就是 bit/s(位每秒)。市场上经常可以见到的调制解调器的速度一般有 9600bit/s、14.4Kbit/s、28.8Kbit/s、33.6Kbit/s 和 56Kbit/s。

影响传输速度的原因有很多，其中调制解调器提供的只是一个最高的速度。如果网络服务提供商（ISP）设在本地，而且安装了 33.6Kbit/s 的调制解调器，那么确实可以得到最高 33.6Kbit/s 的传输率，否则就可能降到 31.2Kbit/s，甚至发现跟 28.8Kbit/s 的连接没有什么区别。另外，上网速度又取决于双方的调制解调器的速度，如果 ISP 不提供 56Kbit/s 的接入服务，那就可以说白买了 56Kbit/s 的调制解调器，最高也只是得到 ISP 方的最高接入速度。

■ 传输率

传输率也随访问对象的不同而有不同。本地的电子公告系统（BBS）总是最快的，或者某些在线服务，由

于 ISP 不断升级他们的调制解调器，因此速度也不会太慢。但在 Internet 上，网络的服务有可能就拖了后腿，一些 Web 网页会由于在网络中兜圈子而迟迟发不过来，或者在同一时间中有太多的请求，致使大家不得不陷入等待。

■ 价格

现在由于调制解调器的价格趋于廉价，33.6Kbit/s 的，或者 56Kbit/s 的调制解调器都可以令用户接受。最好不要再购买 28.8Kbit/s 或者以下的调制解调器，因为低速的网络速度往往不能让人忍受。

20.1.2.2 内置式调制解调器

内置式的调制解调器又称做调制解调卡，工作时不需要单独供电，也不需要占用单独的串口。正因为其绕过了串口，所以速度一般也比外置式的调制解调器更快一些。但其安装时需要打开机箱，也需要占用一个扩展槽，而且没有指示灯显示呼叫及传输过程。在调制解调卡的后部一般有两个接口，标有“ LINE ”的接口与电话线相连，标有“ PHONE ”的接口与电话相连。带有语音功能的调制解调卡一般还多出两个插口，标有“ MIC ”的可以与麦克风相连，标有“ SPEAKER ”的与外置音箱相连。连接了这样两个设备后，就可以替代电话的功能了。

20.1.2.3 外置式调制解调器

外置式调制解调器是一个完全独立于计算机的硬件设备，所以拆卸十分方便。外置式调制解调器的后部除了电源接口和开关之外，还有一些数据线接口，其中“ RS232 ”接口需要通过专用的电缆与计算机串口（COM）相连。还有标有“ LINE ”的接口与电话线相连，标有“ PHONE ”的接口与电话相连。在前部一般有指示灯显示呼叫及传输过程，还有“ MIC ”和“ SPEAKER ”插口。

20.1.2.4 调制解调器的安装

买了调制解调器后，一般会发现制造商附带两根数据线。电话线的一端插头插入调制解调器的背后标有 LINE 的插口，然后用一根数据线分别接到调制解调器上标有“ PHONE ”的端口和电话，这样就可以在不用调制解调器的时候可以正常打电话。

将连接电缆一端插入调制解调器，另一端插入电脑的 9 针的或者 25 针的串口上，插好调制解调器的电源，然后拿起话筒，试试看能否打电话（调制解调器的电源不用打开），如果可以通话就表明安装没有问题。

上述工作完成后，就需要在 Windows 2000 下安装和配置调制解调器。下面就以调制解调器为例说明一下如何安装：

（1）在“ 开始 ”菜单中的“ 设置 ”选择“ 控制面板 ”，双击“ 电话和调制解调器选项 ”图标，如图 20-14 所示，会弹出“ 电话和调制解调器选项 ”的对话框。另外这一步也可以通过双击“ 添加/删除硬件 ”图标来完成添加新的调制解调器。

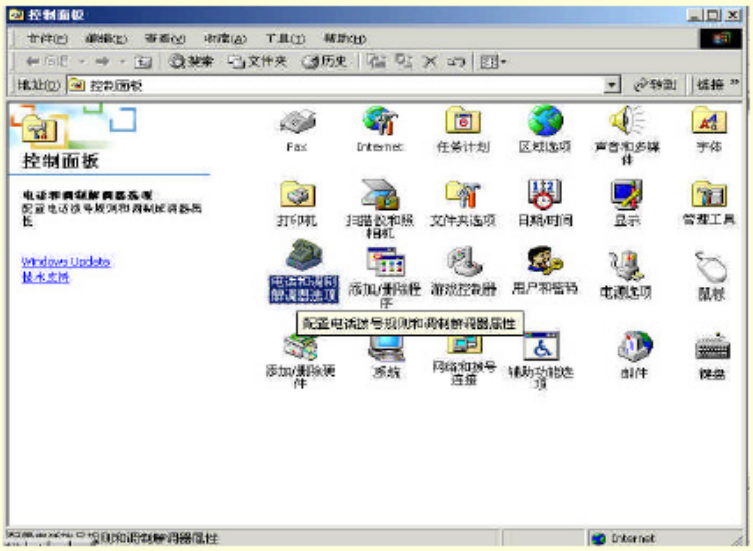


图 20-14 “ 控制面板 ”中“ 电话和调制解调器选项 ”

（2）“ 电话和调制解调器选项 ” 中有 “ 拨号规则 ”、“ 调制解调器 ” 和 “ 高级 ” 3 个选项卡，如图 20-15 所示。

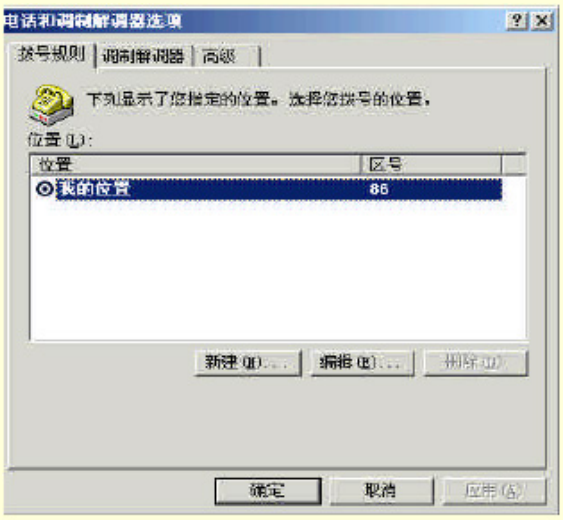


图 20-15　“ 电话和调制解调器 ” 选项

其中 “ 拨号规则 ” 选项卡显示了指定的调制解调器的 “ 位置 ”，有 “ 新建 ”、“ 编辑 ” 和 “ 删除 ” 3 个选项可以对这个位置进行修改。

在 “ 调制解调器 ” 选项卡中，有一个显示框显示出所使用的调制解调器，在下部有 3 个按钮可以让用户进行 “ 添加 ”、“ 删除 ” 和修改 “ 属性 ”。

而在 “ 高级 ” 选项卡中，显示的是计算机中所安装的电话服务驱动程序，用户也可以 “ 添加 ” 新的电话服务驱动程序，或者 “ 删除 ”，或者进行属性 “ 配置 ”。

在 “ 调制解调器 ” 选项卡里，选择 “ 添加 ”，会弹出安装新的调制解调器的欢迎窗口，如图 20-16 所示，指引用户一步一步的安装调制解调器。

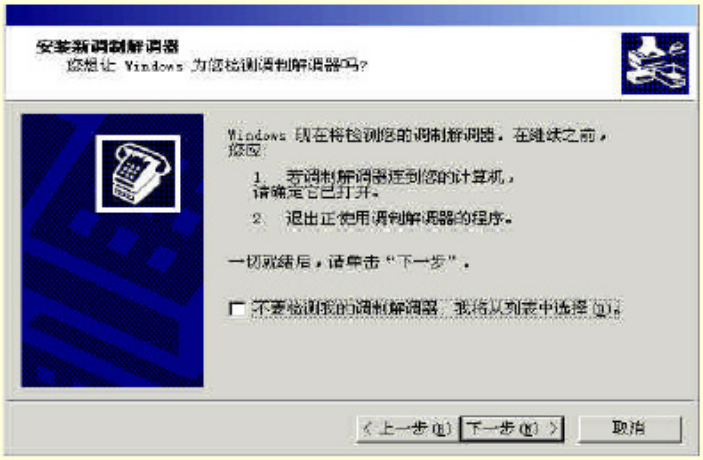


图 20-16　“ 安装新调制解调器 ” 的欢迎窗口

（3）在此欢迎窗口上，可以让计算机自动检测新的调制解调器，也可以选上 “ 不要检测我的调制解调器，我将从列表中选择 ” 的复选框，自己进行选择调制解调器。如果要求计算机帮助检测，单击 “ 下一步 ” 按钮。这样计算机就从串口上寻找新的硬件，如图 20-17 所示。

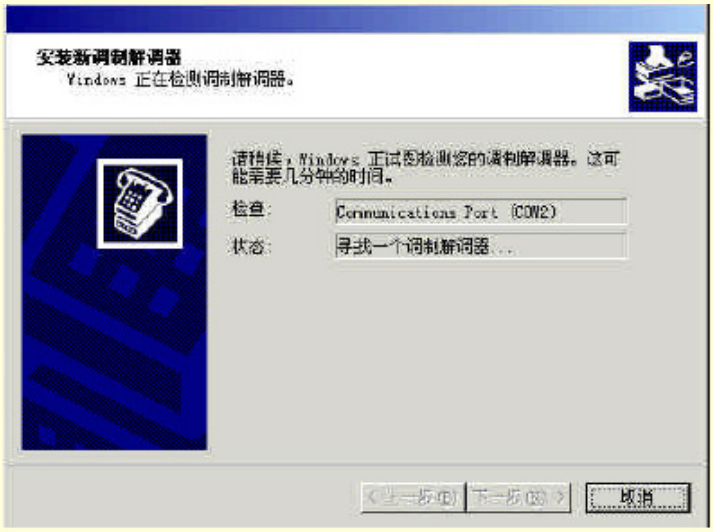


图 20-17　计算机寻找调制解调器

图 20-18　安装调制解调器

（4）计算机会很快地找到连到串口上的调制解调器，并且会自动的安装调制解调器，如图 20-18 所示，使得安装完全变得很简单。这时候可以单击“ 完成 ”按钮，如图 20-19 所示。

图 20-19　安装完毕

（5）那么在图 20-20 中可以找到刚装上的调制解调器。

图 20-20　在“调制解调器”选项卡中可以发现新的调制解调器

一般建议用户这样来安装调制解调器，不过有可能因为调制解调器的品牌过于老，计算机没有检测出来，于是只能采用手工安装。可以在图 20-16 中把“不要检测我的调制解调器，我将从列表中选择”的复选框选中，然后单击“下一步”按钮。这时会弹出一个供用户选择的窗口，如图 20-21 所示，左边是“制造商”，右边是“型号”。用户可以选择计算机里自带的调制解调器驱动程序，如果在列表中找不到自己调制解调器型号也可以选择“从磁盘安装”，如图 20-22 所示。

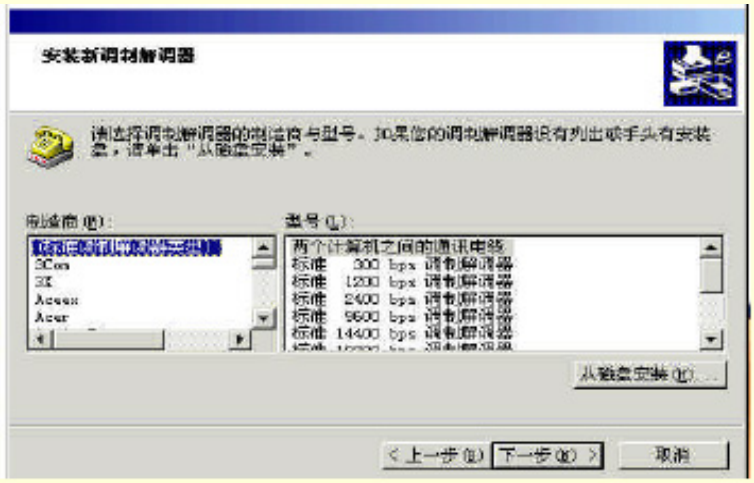


图 20-21　选择调制解调器的型号

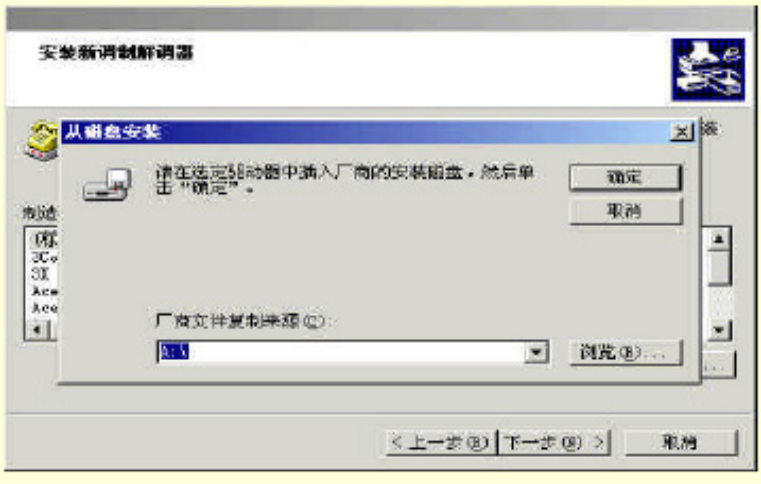


图 20-22　从磁盘安装

插入制造商提供的软盘，然后单击“确定”按钮，选择符合型号的调制解调器，单击“下一步”即可，如图 20-23 所示。

同样在图 20-20 中的“电话和调制解调器选项”可以看到刚安装上的调制解调器。

20.1.2.5 配置调制解调器的属性

调制解调器的属性一般包括占用的端口号、扬声器的音量、传输速度和传输数据格式及呼叫的设置。在电话和调制解调器的选项对话框中，选择已经安装的调制解调器，然后单击“属性”，就会出现所选的调制解调器的属性，如图 20-24 所示。

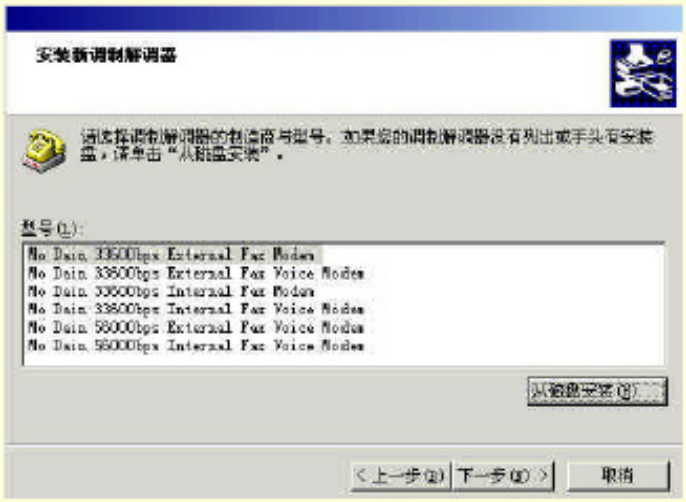


图 20-23 选择调制解调器的型号

图 20-24 调制解调器的属性

可以看到有 3 项选项卡：常规、诊断与高级。

■ 在“常规”选项卡中，有调制解调器所用的“端口号”，一般在计算机中，因为 COM1 已经被鼠标占用，所以调制解调器多使用的是 COM2。另外也可以调节“扬声器的音量”。在“最大的端口速度”里可以选择调制解调器的最大压缩速度，这个速度可以根据调制解调器来进行调节。在“拨号控制”里，可以选择是否在“拨号前等待拨号音”。

注意：这个速度并不代表着调制解调器的传输速度，而只是调制解调器端口的压缩数据的速度。

■ 在“诊断”选项卡中，如图 20-25 所示，有“调制解调器的信息”，里面包括了调制解调器的硬件的 ID。单击“查询调制解调器”，可以看到计算机对调制解调器所用的命令和调制解调器对计算机的响应。在选择“附加到日志”的复选框后，单击“查询日志”，就可以看到详细的命令和响应了，如图 20-26 所示。这作为一个文本文件存在，文件名可以是“ModemLog_Rockwell DPF External PnP”。

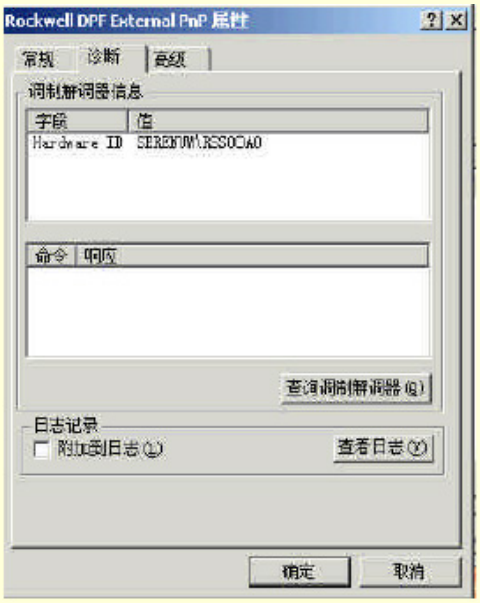


图 20-25　诊断选项

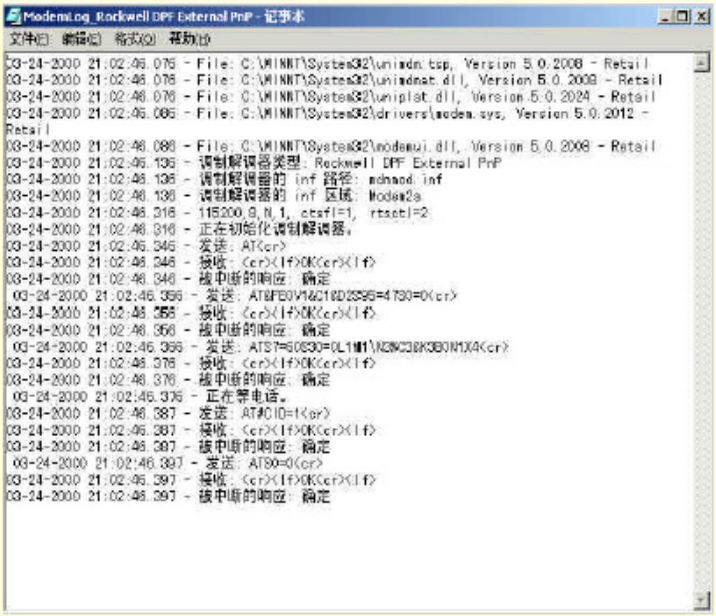


图 20-26　计算机的命令和调制解调器的响应

■ 在“高级”选项卡里，如图 20-27 所示，用户可以额外设置调制解调器的初始命令。另外在“更改默认首选项”里也可以更改调制解调器的初始选项。里面还有“常规”与“高级”的选项卡，如图 20-28 所示。

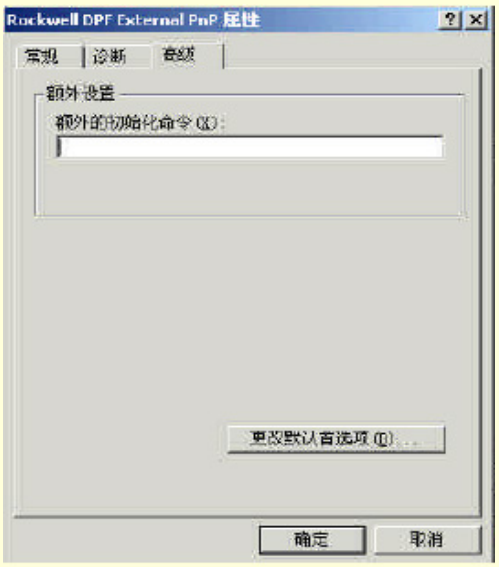


图 20-27 “高级”选项卡

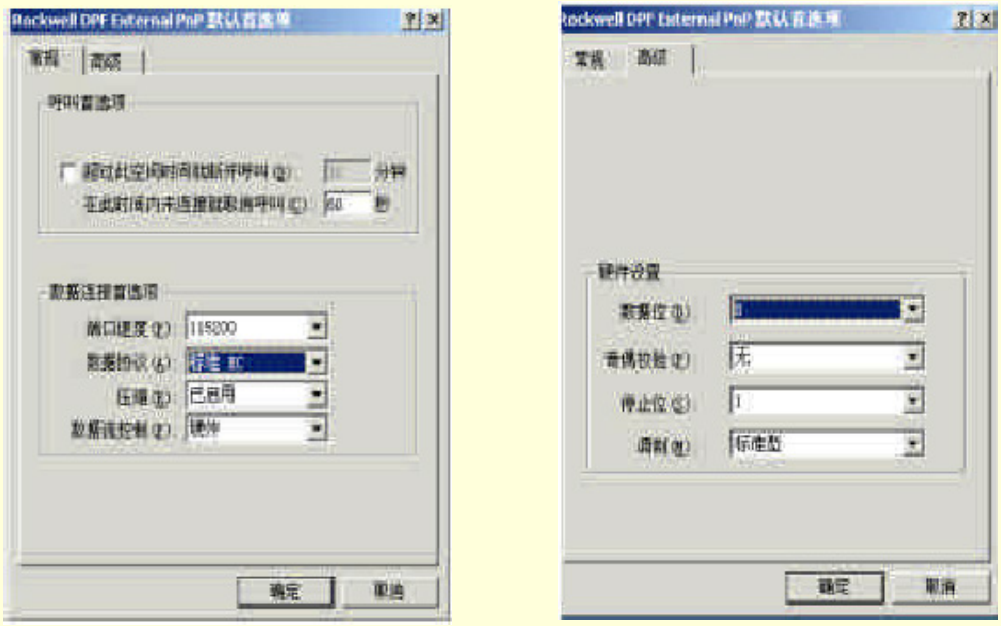


图 20-28 “默认首选项”里内容

看一看“常规”选项卡里，“呼叫首选项”里的“超过此空闲时间就断开呼叫”，可以让用户在空闲计算机的时候或者在用户离开了计算机而忘了关掉网络连接的时候，断开连接，而节省用户的上网费用。“在此时间内未连接就取消连接”令用户在网络忙时可以避免连续的呼叫而花费不必要的时间，两个选项均可让用户更改时间。

“数据连接首选项”里包括有“端口速度”、“数据协议”、“压缩及数据流控制”。“端口速度”可以让用户设定调制解调器的压缩速度，里面有 300～115200bit/s。“数据协议”里有“标准 EC”、“已停用”、和“强制的 EC”。一般在台式机中选择“标准 EC”。“压缩”里可以选择“已启用”和“已停用”，让调制解调器工作在压缩状态，可以提高调制解调器的传输速度。“数据流控制”里有“Xon/Xoff”、“硬件”和“无”选项。如果调制解调器不支持硬件的数据流控制，那么就应该启用 Xon/Xoff 的软件数据流控制。

在“高级”的选项卡中，说明了“硬件设置”。可以采用计算机的默认设置，“数据位”一般选择 8 位，“奇偶校验”里选择无，“停止位”选择 1，“调制”里选择标准型。

20.2　安装软件

所有的硬件安装完毕后，那么离连入 Internet 就只差最后的一步了，还要安装上网的一些拨号设置。其实 Windows2000 已经将以前的拨号网络集成到一个应用组上,这个组叫做“网络与拨号连接”。只要简单的步骤就可以轻松的实现通过调制解调器将计算机连到 Internet 上。

20.2.1　建立新的连接

20.2.1.1　利用 Windows2000 自带的工具

建立一个到其他计算机的连接，可利用的硬件就是调制解调器或者 Cable。而通过修改设置可以更改网络或拨号连接。每个连接都定义了它的拨号设置（例如连接的电话号码，重拨次数等等）。这些连接前和连接后的设置不会修改或影响其他连接的设置。例如，可能有一个拨号连接要重拨 10 次一台经常很忙的服务器。而可能还有一个拨号连接，它对于另一台更容易连接的服务器要重拨 3 次。第一个连接的重拨设置绝不会导致第二个连接的重拨次数超过其自身规定的 3 次。在拨号连接设置之外不需要更改任何设置。

具体的步骤如下：

（1）在“开始”菜单中选择“设置”，再选择“网络与拨号连接”，里面包含了“新建连接”和“本地连接”。其中“新建连接”就是针对用调制解调器连接其他计算机的，而“本地连接”就是对局域网的连接的。而这一步也可以打开控制面板，双击“网络与拨号连接”即可。然后双击“新建连接”，可以弹出“网络连接向导”，如图 20-29 所示，此向导会一步一步的引导用户快速建立 Internet 的连接。

图 20-29　“网络连接向导”欢迎窗口

（2）单击“下一步”按钮后，就可以选定网络连接的类型，如图 20-30 所示。其中有“拨号到专用网络”、“拨号到 Internet”、“通过 Internet 连接到专用网络”、“接受传入的连接及直接连接到另一台计算机”。因为要连接到 Internet 中去，选择第二个选项。

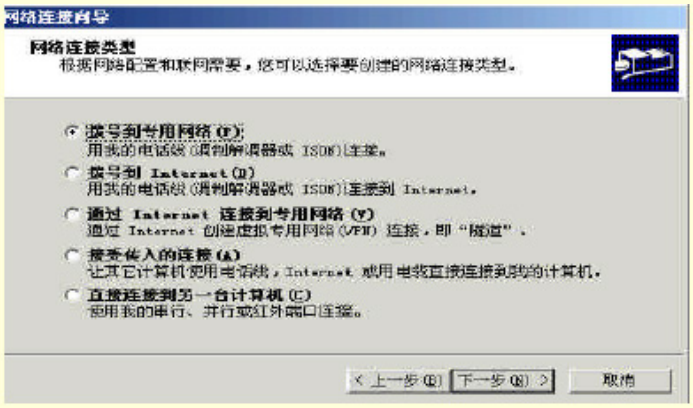


图 20-30　选择网络连接的类型

（3）单击“下一步”按钮后，网络连接向导会提问建立 Internet 应该通过哪种方法，如图 20-31 所示。一般的用户通过调制解调器来上网就应该选择通过电话线连接，但在科研单位或者学校里，由于可以通过局域网来上网的，也可以选择通过局域网（LAN）来连接。

（4）单击“下一步”按钮后，网络连接向导会询问是否建立新的拨号连接，还是使用现有的拨号连接，如图 20-32 所示，可以选择“新建拨号连接”。

图 20-31　建立 Internet 连接

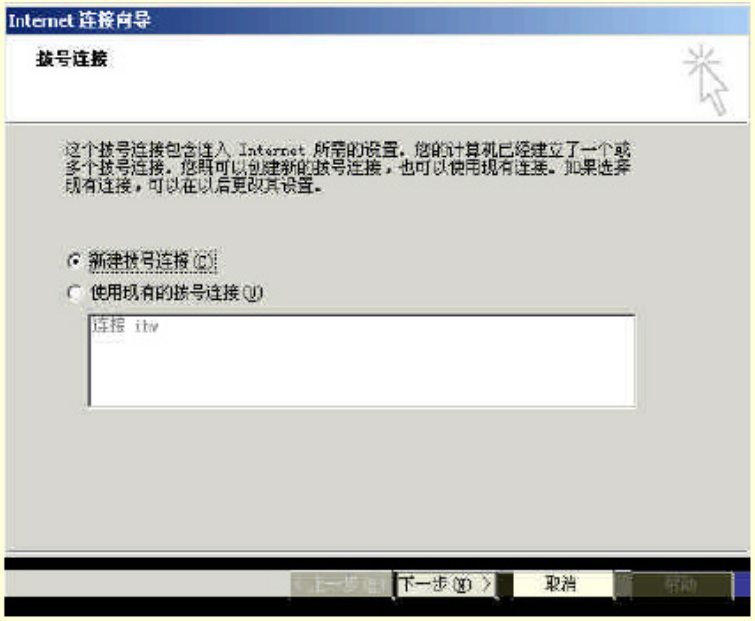


图 20-32　拨号连接

（5）单击“下一步”按钮后，这样就进入了 Internet 账号拨号连接信息，如图 20-33 所示，这个步骤共有 3 步。步骤 1 是设置“Internet 账号连接信息”，就是填入 ISP 的电话号码，因为处在中国，所以区号、国家（地区）名称和代码都可以使用默认值。也可以用使用“高级”来配置 ISP 的设置，如图 20-34 所示。

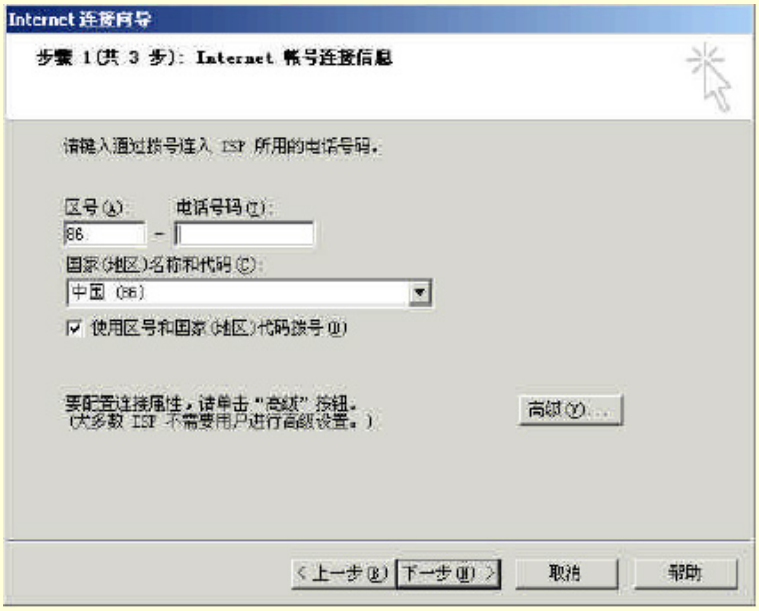


图 20-33　步骤 1——Internet 账号连接信息

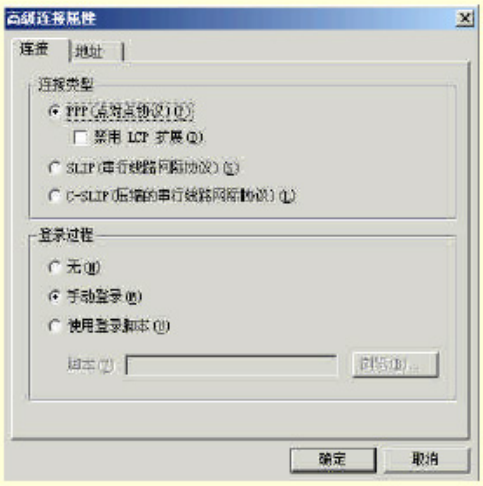


图 20-34　“ 高级连接属性 ” 的连接

“ 高级连接属性 ” 里面包括了 “ 连接 ” 与 “ 地址 ” 两个选项卡。

“ 连接 ” 有 “ 连接类型 ” 和 “ 登录过程 ”，“ 连接类型 ” 里规定了登录 Internet 所使用的协议，包括有 “ PPP（点对点协议）”、“ SLIP（串行线路网际协议）” 和 “ C-SLIP（压缩的串行线路网际协议）”。使用电话线来登录网络一般选用的是 PPP，这样确保可以登录上 Internet。“ 登录过程 ” 里有 “ 无 ”、“ 手动登录 ” 及 “ 使用登录脚本 ” 的 3 个单选按钮。如果选择 “ 无 ”，那么在登录网络的时候就会自动检测是否使用自动连接；如果选择 “ 手动登录 ”，那么在登录网络的时候就会那么有可能会弹出终端窗口让用户填入用户名和密码；而且在 Windows 2000 里面还可以有登录脚本，使用登录脚本可以让用户更方便地使用登录过程。

而 “ 地址 ” 选项卡里，如图 20-35 所示，里面是 TCP/IP 的一些参数设置，例如 “ IP 地址 ” 是否由 Internet 服务提供商自动分配或者使用固定的 IP 地址，由 ISP 自动分配 IP 地址可以避免设定的 IP 地址在 Internet 内重复使用。不过如果是分配了固定的 IP 地址那么使用固定的 IP 地址会更让别的用户方便的找到自己。“ DNS 服务器地址 ” 也可以由 ISP 自动分配一个域名服务器（DNS）地址，不过也可以使用已知的 DNS 地址，因为 DNS 服务器的地址都差不多是统一的。用户可以填入主 DNS 服务器和备用 DNS 服务器的地址。

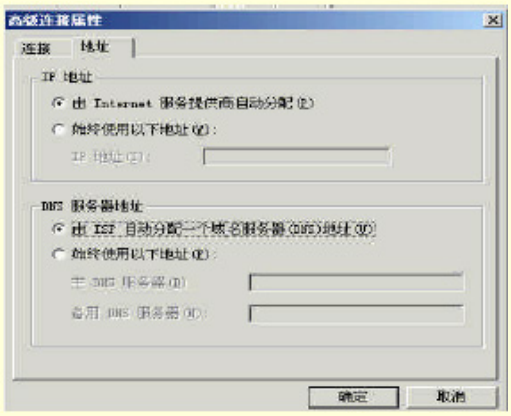


图 20-35　高级连接属性的“地址”

（6）单击“下一步”按钮后，进入了拨号连接的步骤 2，“Internet 账号登录信息”，里面包含了要登录上 Internet 的“用户名”和“密码”。如图 20-36 所示。

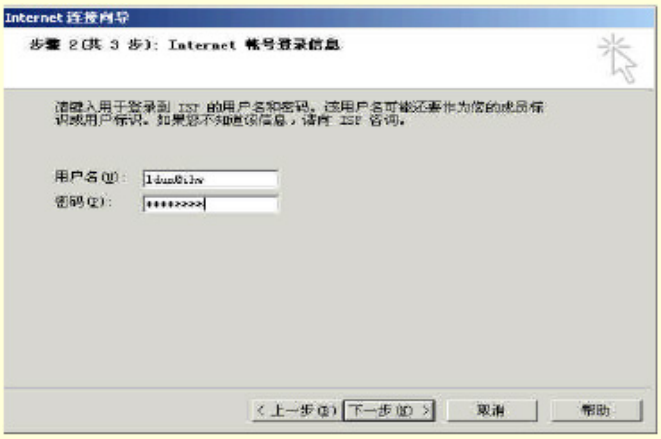


图 20-36　步骤 2——Internet 账号登录信息

注意：如果在上一步选用了无的登录过程，那么就是自动登录上 Internet，所以在这一步中就不能填错，否则如何也不能连上 Internet，因为用户名和密码都是错的。

（7）单击“下一步”按钮后，进入了拨号连接的步骤 3，“配置您的计算机”。因为有关 Internet 账号的信息是按照拨号连接分组存放的，用户可以选用自己喜欢的名称来标记此 Internet 账号。要进行连接时，就可以区分使用不同的拨号连接，如图 20-37 所示。

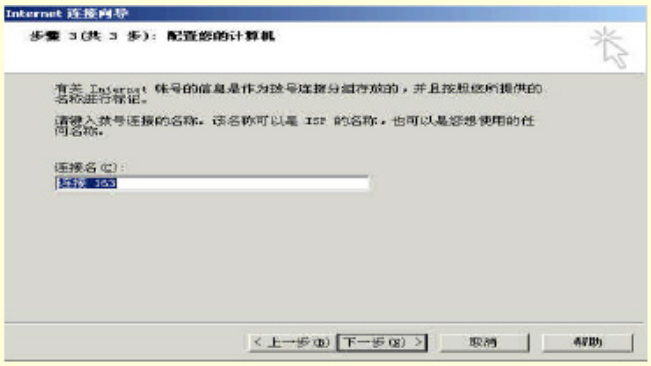


图 20-37　步骤 3—配置您的计算机

（8）单击“下一步”按钮后，很高兴的祝贺您，已经将拨号设置成功地配置完成，如图 20-38 所示。单击“完成”就可以使用这个连接登录到 Internet 中了。如果发现前几步有错，也可以单击“上一步”来进行修改。

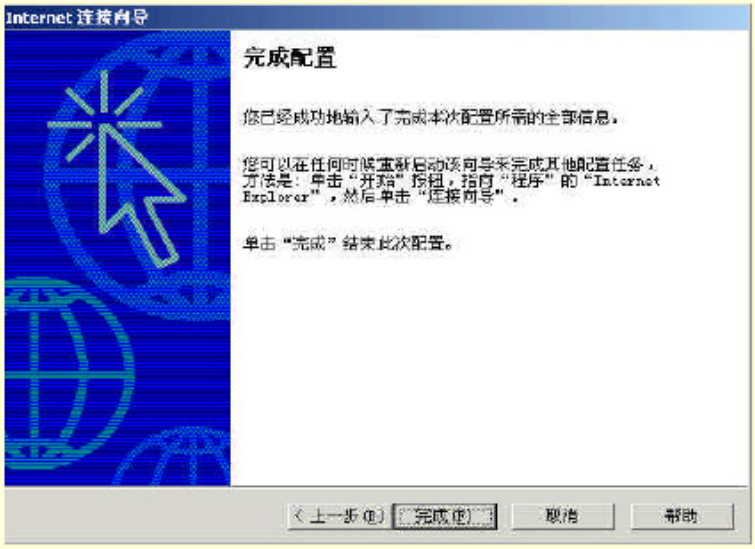


图 20-38　祝贺您完成配置

20.2.1.2　利用 Internet Explorer5.0 携带的工具

除了 Windows2000 自带的拨号工具之外，其实也可以使用“Internet 连接向导”，它是 IE5.0 提供给用户快速建立 Internet 连接账号的工具，通过这个连接向导，可以快速的设置各项上网的数据，轻松地上网。

建立新的连接的步骤如下：

（1）在安装了 Windows2000 后，因为系统已经捆绑了 IE5.0，其中也包括了“Internet 连接向导”。如果没有设置任何的连接数据，则在第一次打开 IE 浏览器或者 IE Outlook Express 时，便会自动打开“Internet 连接向导”。也可以在“开始”菜单中单击“程序”，单击里面的“附件”→“通讯”→“Internet 连接向导”，这样特也会弹出“Internet 连接向导”的欢迎窗口，如图 20-39 所示。可以选择“注册新的 Internet 账号（电话线已经与调制解调器相连）”、“使用已有的 Internet 账号（电话线已经与调制解调器相连）”，此时要确保电话线已经与调制解调器相连，但这样经常找不到本地的 ISP，所以一般的用户也很少选择这两项。如果已经有了曾经建立的拨号连接的话，可以选择“手动设置 Internet 连接或通过局域网（LAN）连接”。选择“手动设置 Internet 连接，或者通过局域网（LAN）连接”的复选框。

（2）单击“下一步”按钮后，可以设置 Internet 的连接方法，有“通过电话线和调制解调器进行连接”和“通过局域网连接”。因为家庭用户一般使用电话线上网，选择“通过电话线和调制解调器进行连接”复选框，如图 20-40 所示。

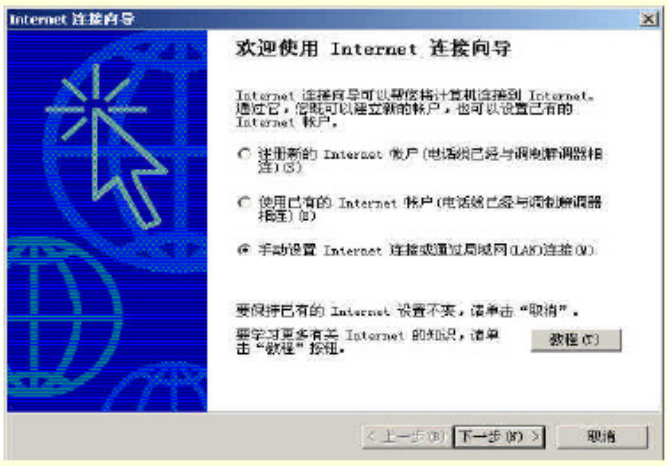


图 20-39　“Internet 连接向导”的欢迎窗口

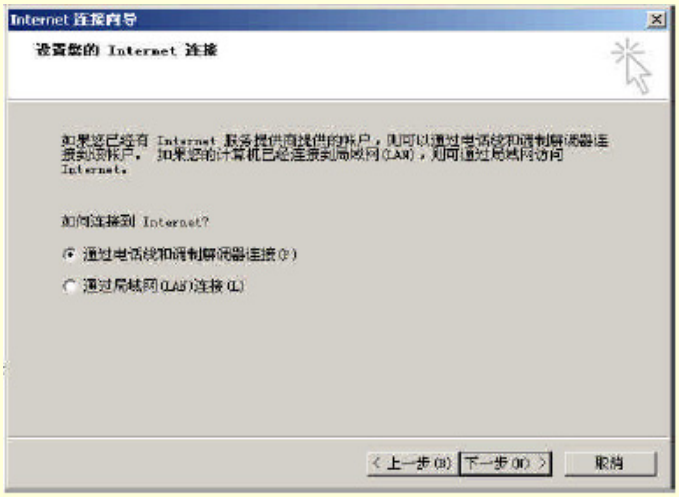


图 20-40　设置您的 Internet 连接

（3）单击“下一步”按钮后，这一步就是前面讲过的 Internet 的连接向导的３个步骤，那么以下就可以参看如图 20-33～图 20-37 所示的进行配置。

注意：如果不知道 ISP 的接入电话，可以打电话咨询自己的 ISP，确保要有固定的帐号。

（4）在图 20-41 中单击“下一步”按钮后，欢迎窗口会询问是否设置 Internet 电子邮件账号，选择“否”。

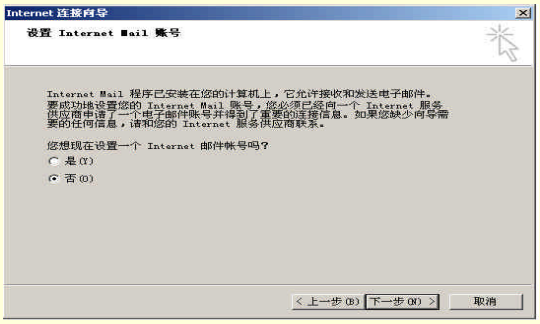


图 20-41　设置 Internet Mail 账号

（5）单击“下一步”按钮后，祝贺您，Internet 连接向导已经设置完毕。

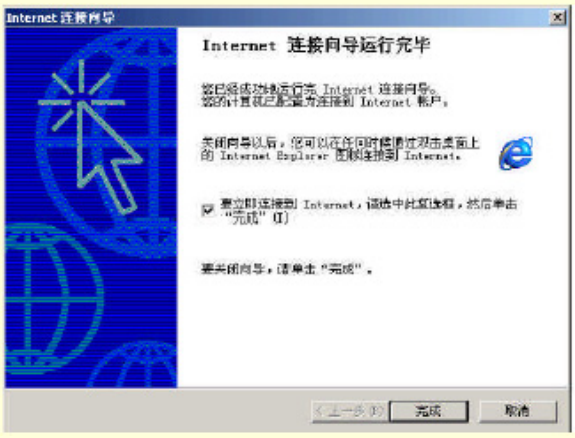


图 20-42　完成窗口

使用 Internet 连接向导，设置 Internet 就会变得非常的方便。如图 20-43 所示就是 IE5.0 自带的拨号连接对话框。

图 20-43　IE 的拨号连接

20.2.2　使用拨号连接连上 Internet

安装好连上 Internet 的硬件和软件后，就可以尝试一下登录 Internet，去感受丰富的 Internet 世界。可以按照以下步骤进行连接：

（1）在“开始”菜单中选择“设置”，可以打开“控制面板”也可以单击“网络与拨号连接”，打开“网络与拨号连接”，如图 20-44 所示。

（2）双击刚刚建立的“连接到 163”，就弹出拨号属性的欢迎窗口，提示用户进行拨号或者属性修改，如图 20-45 所示。

图 20-44　网络与拨号连接

图 20-45　“连接到 163”的拨号属性

（3）单击“拨号”后，拨号属性就会打开通信端口，进行拨号，如图 20-46 所示。

图 20-46　正在拨号

（4）如果选择是非自动的连接入 Internet，经过一会儿的等待后就可以出现“终端窗口”，如图 20-47 所示，提示用户键入登录 Internet 的用户名和密码。键入“回车键”后，单击“完成”，那么就会显示登录 Internet 的状态。

（5）好了，现在计算机已经和 Internet 连接上了。在窗口的状态栏上就可以看见小小的两台计算机在互相通信呢。双击这个小状态图标，可以看到此时调制解调器的详细资料，如图 20-48 和图 20-49 所示。

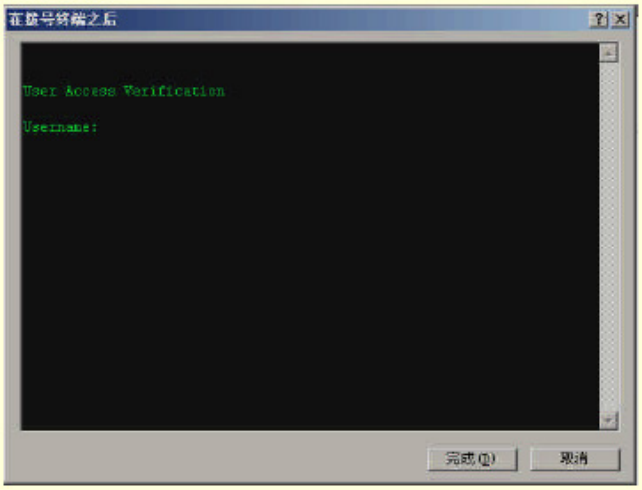


图 20-47　拨号后的终端窗口

图 20-48　连接的状态之一　　图 20-49　连接状态之二

连上 Internet 有很多种的方法，从计算机的硬件和软件都要着手配置。本章就通过局域网和调制解调器上网的基本配置进行介绍，只有将硬件部分配置好了那么上网就少了一分忧虑，多了一分乐趣。下面请一起来翱翔那精彩的 Internet 世界吧！

第 21 章　运用 Internet

Internet 是一个世界范围内互相互连的网络，它可以把世界各地的计算机连接在一起，进行数据传输。Internet 无论是在科学研究、教育、商业还是军事等领域的影响都越来越大。现在越来越多的人也开始学习 Internet，而且利用 Windows 2000 内置的 Internet 浏览器，可以在 Internet 中自由的翱翔，如图 21-1 所示就是 WWW 页面。

在这一章中的详细内容有：

- Windows 2000 自带的 IE 浏览器
- Outlook Express 5.0 的使用
- NetMeeting 的使用

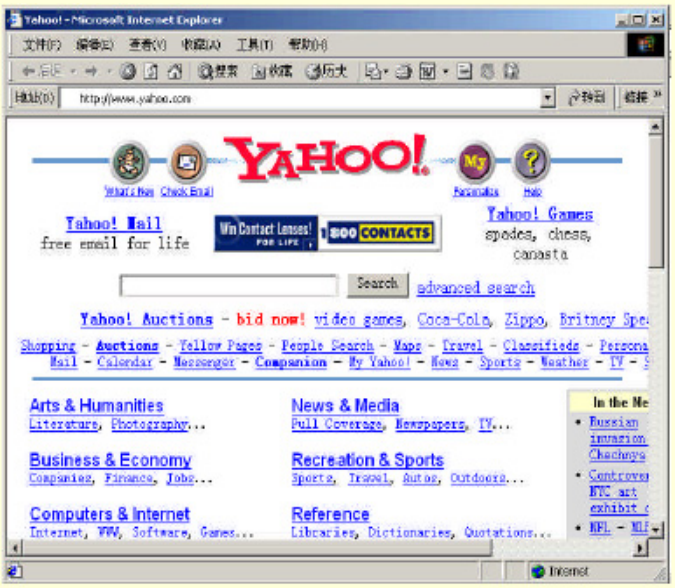


图 21-1　Yahoo 的网页

21.1　Windows 2000 与 Internet 的紧密结合

Windows 2000 将 IE5 集成起来，这种集成不仅仅是使用了 IE 的软件包，而且让用户意识到 Internet 是计算机不可缺少的一部分。Windows 2000 已经和 Windows 98 一样将 Internet 网页应用在桌面上，所有的资源窗口，包括“我的电脑”、“网上邻居”以及“控制面板”等，都变成了类似 Internet 浏览器的图标，如图 21-2 所示。而且在 Windows 资源管理器中既可以访问本机上的资源，例如“桌面”、“磁盘”、“控制面板”、“网上邻居”和“打印机”等，又可以直接输入 WWW 地址登录上 Internet。Windows 2000 使得本地计算机与 Internet 天衣无缝的融合起来。

图 21-2　活动桌面

21.1.1　活动桌面

活动桌面将 Internet 集成在计算机系统中，只需要掌握一些技巧就可以导航 Internet，也可以导航自己的计算机系统。活动桌面的外观和行为都和 Internet 浏览器非常相似，例如可以把文件名变成超连接的方式，只需要单击一次就打开文件或者执行程序。系统上每一个文件夹都变成了 Web 页，能够显出许多类型的精彩内容。

将常规的桌面切换到活动桌面的方法，其实很简单。在桌面上右击鼠标，从弹出的菜单中选择“活动桌面”，里面就有多项的选择，如图 21-3 所示。

图 21-3　活动桌面的选项

■ “自定义桌面”将“显示属性”弹出来，如图 21-4 所示，可以自定义自己喜爱的桌面或者定制“背景”、“屏幕保护程序”、“外观”、“Web”、“效果”和“设置”。

图 21-4　显示属性中 WEB 的定制

在“ Web ”的选项卡里选择“ 在活动桌面上显示 Web 内容 ”，就可以选择不同的主页作为桌面。这样就可以把普通桌面设置为活动桌面，如图 21-2 所示。当然也可以自己将喜爱的主页面设置为活动桌面，单击“ 新建 ”，弹出“ 新建 Active Desktop 项 ”，如图 21-5 所示。而访问“ 画廊 ”，可以连接 Microsoft 的 Web 站点的活动桌面画廊。如果想添加已知的 Web 页，可以选择“ 浏览 ”，挑选自己喜爱的 HTML 页。

图 21-5　新建 Active Desktop 项

■ “ 新建桌面项目 ”也会弹出图 21-5 的“ 新建 Active Desktop 项 ”，让用户重新建立新的桌面项目。

■ “ 显示 Web 内容 ”是将选定的活动桌面显示出来。

然后在显示活动桌面后单击鼠标右键，会增加几个选项：“ 显示桌面图标 ”，“ 锁定桌面项目 ”、“ 同步 ”和“ 当前主页 ”的选择。

21.1.2　文件夹的 Internet 应用

打开资源管理器，看到的就是普通的 Windows 传统的窗口，但是在 Windows 2000 中就可以将文件夹设置为自己喜欢的 Web 风格。

步骤是：

单击资源管理器菜单上的“ 工具 ”里的“ 文件夹选项 ”，弹出“ 文件夹选项 ”。里面包括有“ 常规 ”、“ 查看 ”、

“文件类型”和“脱机文件”4 个选项卡。

在“常规”选项卡中就可以设置“Active Desktop”、“Web 视图”、“浏览文件夹”和“打开项目的方式”。

■ “Active Desktop”选项可以选择“允许桌面上使用 Web 内容”、“使用 Windows 传统风格的桌面”。

■ “Web 视图”选项中可以选择“允许文件夹中使用 Web 内容”和“使用 Windows 传统风格的文件夹”。那么在文件夹中就可以浏览文件的属性，帮助用户是否选择打开文件，这对于 HTML 页面或者一些文档很方便。而 Windows 传统风格的文件夹则不能浏览文件的大概。

■ “打开项目的方式”可以让用户更加的觉得与 Internet 的紧密结合。选择“通过单击打开项目”就像点击 Internet 的超级连接一样，文件在单击后就会打开。而“通过双击打开项目”就像传统的 Windows 文件夹一样需要双击。

图 21-6 文件夹选项

21.2 Internet Explorer 5.0 导航

21.2.1 Internet Explorer 特点

IE5.0 是 Windows 2000 的捆绑的 Web 浏览器，使用它能够帮助用户顺利地进入 Internet 大世界。主要的特点有：

■ 快速、便利

IE5.0 能够将 Web 以各种方式与 Windows 的界面结合起来，操作更加方便。并且 IE5.0 包括一系列的能够帮助用户顺利进行网络通信的工具。

- Outlook Express：阅读电子邮件以及新闻组的工具。
- NetMeeting：Internet 电视会议软件。
- Web Publish：在 Internet 中发布自己的主页工具。

■ 浏览用不同的语言编写的 Web 页

在 Internet 上进行环球漫游时，使用 Web 浏览器浏览会遇到用不同的语言编写的 HTML 页面，但只需要安装不同的语言的字符集就可以正确的显示出网页内容。

■ 脱机浏览

可以一次性下载喜欢的 Web 站点内容，并在空闲的时候浏览。这样可以节约阅读的时间和费用。

■ 安全浏览

使用安全区域用户可以为 Web 的不同的区域设置不同的安全级，以保护计算机的安全。而且可以启动分级

审查功能，可以删除、禁止查看令人不愉快的或者不健康的内容。

21.2.2　Internet Explorer 的界面与应用

Internet Explorer 的窗口界面，如图 21-7 所示。

图 21-7　Internet Explorer 界面一览

21.2.2.1　标题栏

位于窗口的上部，它显示了当前正在访问的 Web 页面的名称，同时还有最大、最小和关闭按钮。这个与标准的 Windows 窗口非常的相想像。

21.2.2.2　菜单栏

菜单栏中包括了执行全部功能的命令，IE 的控制就全在菜单的某一个选项中。其中包括有“ 文件 ”、“ 编辑 ”、“ 查看 ”、“ 收藏 ” 和 “ 帮助 ”。这里会将一些比较常用的和与 IE4.0 有区别的选项进行介绍。

“ 文件 ” 中包括了传统的 “ 新建 ”、“ 打开 ”、“ 保存 ”、“ 另存为 ”、“ 页面设置 ”、“ 打印 ”、“ 发送 ”、“ 属性 ”、“ 脱机浏览 ” 和 “ 关闭 ”。另外还有一些新加的选项。

“ 新建 ”中不但可以打开一个新的页面“ 窗口 ”,而且还可以打开“ 邮件 ”、“ 发布信息 ”、“ 联系人 ”和“ Internet 呼叫 ”。这正是 IE5.0 一系列产品的融合的结果。

“ 使用 Microsoft Word for Windows 编辑 ” 是新加的一个选项，可以实时地将所见的网页用 Microsoft Word 进行编辑，体现了所见即所得的好处。

“ 编辑 ” 中含有的是常见的 “ 剪切 ”、“ 复制 ”、“ 粘贴 ”、“ 全选 ” 和 “ 查找 ”（在当前页）。

“ 查看 ”中包括的菜单有较大的变化。除了原有的“ 工具栏 ”、“ 状态栏 ”、“ 浏览栏 ”、“ 转到 ”、“ 停止 ”、“ 刷新 ”、“ 文字大小 ”、“ 源文件 ” 和 “ 全屏 ” 外，在工具栏增加了 “ 电台 ” 的选项，可以在 IE 的浏览器里打开电台栏。而在 “ 编码 ” 中增加了多种文字支持的功能，可以在浏览器中显示出简体中文、繁体中文和其他的文字。

“ 收藏 ” 是 IE5.0 的一大明显的特色。“ 添加收藏夹 ” 和 “ 整理收藏夹 ” 都显示出 IE5.0 对用户的照顾。

“ 工具 ” 中 “ 邮件和新闻 ” 可以将当前的网页发送给自己的朋友。“ 同步 ” 可以使在脱机浏览时有最新的数据，让脱机文件保持着最新的状态。“ Windows Update ” 可以将用户引到 Microsoft 公司的 Windows Update 页面，让用户了解当前的 Windows 最新的状况。“ Internet 选项 ” 会弹出配置 Internet 的各项选项。

21.2.2.3　工具栏

工具栏中的标准按钮包括了最常用的快捷命令，帮助用户能够快速的执行所需要的命令。

21.2.2.4　地址栏

可以让用户敲进 Web 页面的地址，IE 浏览器会把网页显示出来，并将页面在工作区内显示出来。

21.2.2.5　链接栏

单击链接栏上的各种不同的链接，可以快速的切换到指定的页面上去。

21.2.2.6 工作区

显示了用户正在访问的 Web 页面内容。

21.2.2.7 状态栏

显示了当前访问页面的状态。

21.2.3 使用 IE5.0 浏览 Internet

IE5.0 浏览器最重要的、最基本的功能就是可以在 Internet 中多个网页之间浏览。这种浏览可以借助于超级链接来实现，超级链连接将相关的主页连接起来，顺着超级链接可以一直的链下去，直到找到自己所需的内容为止。

21.2.3.1 输入地址

在“地址栏”中输入地址就可以打开网页，如图 21-8 所示，在地址栏中输入http://www.sina.com.cn，按“回车键”后，就可以连接到著名的网络公司“新浪网”上。并且开始在“地址栏”中输入经常使用的 Web 地址时，下面会出现一个相似地址的列表供用户选择。而且如果 Web 页的地址有误，Internet Explorer 会自动进行近似搜索，找出匹配的地址。

在网页中单击其中的超级链接就可以跳转到其它的网页去。将鼠标指在超级链接就可以发现鼠标变成了一个小手（脱机浏览时小手旁边有一个小圈，禁止往下链接）。

图 21-8 浏览 Internet

21.2.3.2 使用浏览器工具栏

使用浏览器工具栏可以提高浏览网页的速度，如图 21-9 所示，这些快捷键可以让用户提高浏览的效率。

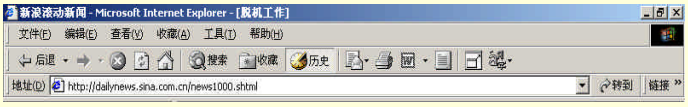


图 21-9 浏览器工具栏

“后退”按钮，可以移到刚才看过的 Web 页。如果是刚刚启动了 IE，除了默认的主页外还没有做过任何的访问，那么该工具是显示灰色的，暂时还不能用。

“前进”按钮，如果在访问的时候按过“后退”按扭，那么按下“前进”按扭后，会重新回到这一页。如果还没有按过“后退”按扭，那么这个按扭仍是显示灰色的，暂时还不能用。

“停止”按钮，如果觉得当前的网页下载的速度非常慢，而且里面的内容也不合心意的话，可以按下“停止”按扭，会停止下载这一页。

“刷新”按钮，更新当前的网页，它会自动的下载当前显示的页面。在按下了“停止”按扭后，觉得还想把刚才的网页看全了，就可以按下此按扭。

“主页”按钮，转到设置的主页去，实现快速的跳转。这个主页地址可以让用户自定义。

“搜索”按钮，按下此按扭后，工作区分为两部分，左边就会显示带有搜索引擎的 Web 页，搜索按扭可以方便的搜索 Web 信息。

“收藏”按钮，按下此按扭后，工作区也分为两部分，左边就会显示“收藏夹”，单击收藏夹栏中的连接，可以快速的访问到喜欢的站点，如图 21-10 所示。

图 21-10　收藏夹栏中的连接

“历史”按钮，按下此按扭后，工作区也分为两部分，左边就会显示“历史记录”栏，这个“历史记录”栏忠实的记录了最近访问的全部站点，如图 21-11 所示。

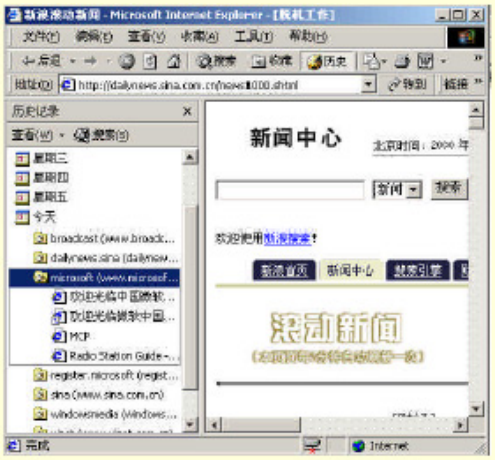


图 21-11　历史栏里的连接

“邮件”按钮，可以让用户选择“阅读邮件”、“新建邮件”、“发送连接”、“发送网页”和“阅读新闻”。这样用户就可以在浏览的同时，选择邮件和新闻组的工作，也可以将自己觉得喜爱的网页发送非自己的朋友。

“打印”按钮，按下此按扭后，将当前的 Web 页打印到默认的打印机上，以便做书面的保存。

“编辑”按钮，按下此按扭后，将会把当前的网页用 Microsoft Word 打开，这样就可以自己编辑所见到的网页，把所见即所得的优点发挥的淋漓尽致。

“讨论”按钮，按下此按扭后，将会连接到指定的服务器上，与大家对同一个喜爱的话题进行讨论，增加了 Internet 的实时性。

“全屏”按钮，按下此按扭后，可以将工作区扩展到整个屏幕区，增加了观看网页的可视性。

“编码”按钮，按下此按扭后，会弹出选择多种语言支持的选项。如果观看来自宝岛——台湾的网页的时候（因为台湾的网页是用 BIG5 码编辑的，用简体中文的浏览器就不能正常地观看），那么就可以用来切换到繁

体中文。

21.2.3.3 使用快捷键浏览网站

除了使菜单外和工具栏外，还可以使用快捷键选择命令和查看文档。IE 的快捷键见表 21-1。

表 21-1 浏览 IE 的快捷键

按 键	目 的
F1	显示 Internet Explorer 帮助，或显示对话框中某个项目的相关帮助信息
F11	在全屏幕和常规浏览器窗口之间进行切换
TAB	在 Web 页、地址栏和链接栏中向前移动到下一个项目
SHIFT+TAB	在 Web 页、地址栏和链接栏中向后返回到上一个项目
ALT+HOME	进入您的主页
ALT+向右箭头	转到下一页
ALT+向左箭头或 BACKSPACE	返回前一页
SHIFT+F10	显示某个链接的快捷菜单
CTRL+TAB 或 F6	在不同框架之间向前移动
SHIFT+CTRL+TAB	在不同框架之间向后移动
向上箭头	向文档起始处滚动
向下箭头	向文档结尾处滚动
PAGE UP	向文档起始处翻页
PAGE DOWN	向文档结尾处翻页
HOME	移动到文档的开头
END	移动到文档的结尾
CTRL+F	在 Web 页中查找
F5 或 CTRL+R	仅当 Web 上的页面与本机存储的 Web 页时间戳不同时，才刷新当前 Web 页
CTRL+F5	即使 Web 上的页面与本机存储的 Web 页时间戳相同，仍然刷新当前 Web 页
ESC	停止下载 Web 页
CTRL+O 或 CTRL+L	转到新位置
CTRL+N	打开新窗口
CTRL+W	关闭当前窗口
CTRL+S	保存当前页
CTRL+P	打印当前页或当前框架
ENTER	激活选定的链接
CTRL+E	在浏览栏中打开搜索页
CTRL+I	在浏览栏中打开收藏夹
CTRL+H	在浏览栏中打开历史记录
CTRL+单击	在历史记录或收藏栏上，打开多个文件夹

21.2.4　使用 IE5.0 进行网页搜索

Internet 的内容日益增加，用户不可能知道那么多的 Internet 站点，也不可能知道那么多的站点中哪一个提供了自己想要知道的内容，那么 Internet 搜索就应运而生。

21.2.4.1　搜索 Internet 站点

如果查找某种信息却不知道由哪些站点提供，可以求助于专用的搜索工具，其实这些搜索工具也是 WWW 站点，这些站点一般向用户提供了免费的搜索服务。它们的数据库里拥有了成千上万的站点信息，收集了全世界的上亿的 Web 页的内容简介。

搜索可以直接从“地址栏”开始，只需键入一些普通的名称或单词，Internet Explorer 就能自动领到与要搜索的内容最匹配的站点，并列出其他类似内容的站点。只需使用“显示相关站点”功能，甚至不需要进行搜索，就能进入需要查看的页面近似的其他 Web 页。

另外在工具栏中单击“搜索”按扭，在工作区可以分为左右两边，如图 21-12 所示，在搜索区中可以看到在 Internet 上搜索时，可以选择使用哪些搜索类别，以及可在哪些搜索提供商中进行搜索。

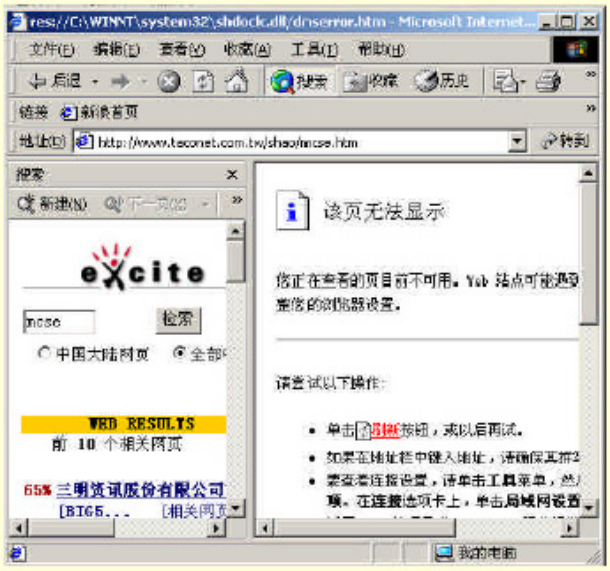


图 21-12　搜索区中进行搜索

21.2.4.2　搜索 Web 页面的文本

这就像传统的 Word 之类的搜索，如图 21-13 所示。步骤如下：

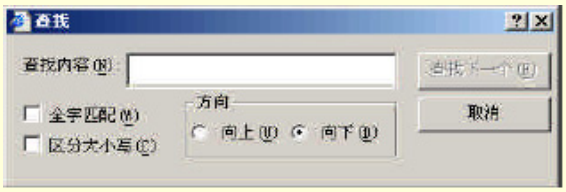


图 21-13　搜索当前页的匹配内容

（1）在“编辑”里选择“查找”，就可以弹出“查找”的对话框。输入要查找的内容，单击“查找下一个”即可。

（2）根据需要调整设置。可以“全字匹配”、“区分大小写”、“方向”可以“向上”或者“向下”。

21.2.5　使用 IE5.0 进行网页管理

21.2.5.1　将 Web 页添加到链接栏

“链接栏”位于“地址栏”旁边，用于添加一些指向频繁访问的部分 Web 页的链接，非常方便。只需单击

“链接”即可显示站点，将 Web 页添加到“链接栏”的方法有很多：

- 将 Web 页的图标从“地址栏”拖到“链接栏”。
- 将链接从 Web 页拖到“链接栏”。
- 在收藏夹列表中将链接拖到“链接”文件夹中。

21.2.5.2 使用收藏夹

在用户浏览网页的时候，不免会遇到自己喜爱的页面和站点。为了以后可以再次访问这些网址，可以利用 IE5.0 提供的“收藏夹”，将自己喜爱的网页添加到收藏夹中。

必要的时候打开“收藏夹”，在其中选择自己要访问的网址，便可以迅速连接到该站点。使用“收藏夹”的步骤有：

（1）在当前的网页存在时候，单击“收藏”菜单，在其下拉菜单中选择“添加到收藏夹”命令，那么“添加到收藏夹”的对话框就会弹出，如图 21-14 所示。

“名称”可以使用网页的标题，也可以自己加上喜爱的标题。另外还可以设置是否令它可以“脱机使用”。在“自定义”中还可以设置脱机收藏夹的内容，如图 21-15 所示。可以将该页中包含的其他连接也下载下来，以便可以脱机浏览。

> 注意：如果没有选择允许脱机使用，那么就只会保存连接到该网页的地址，而并不将页面保存下来。但是如果选择了太多的连接页面层数，会导致了浏览速度变慢，而且会大量的充斥硬盘空间。

（2）创建到某一个文件夹，可以便于用户管理已经下载下来的页面。例如，可以创建音乐类、足球类等等。

另外用户还可以根据自己的喜好来整理收藏夹，如图 21-16 所示。

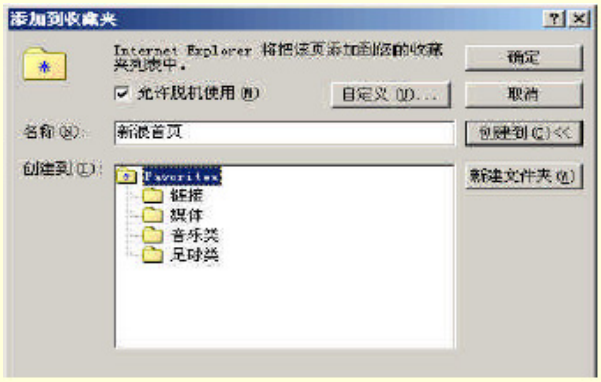


图 21-14 添加到收藏夹对话框

图 21-15 脱机收藏夹向导

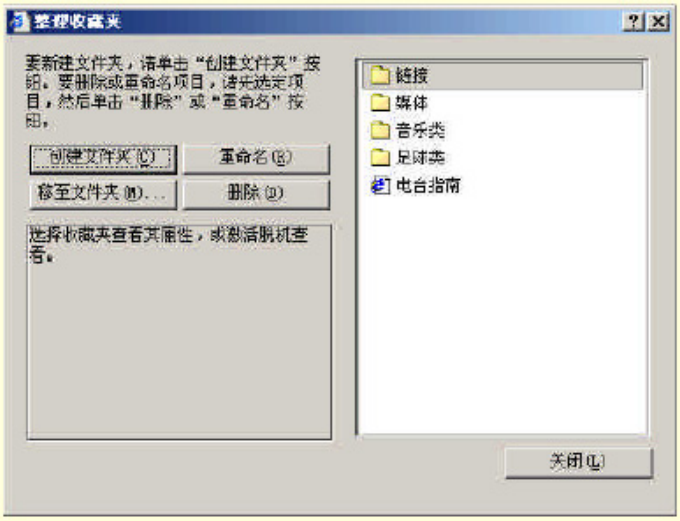


图 21-16　整理收藏夹

如果在几台计算机上使用 Internet Explorer，通过导入收藏的项目可以很容易实现共享。而且，如果您同时使用 Internet Explorer 和 Navigator，则通过在程序之间进行导入可使收藏和书签相互更新。

21.2.6　利用 IE5.0 收听广播

IE5.0 有一个很有趣的功能——电台。确保用户已经安装了 Windows Media Player，那么就可以使用增加的“电台”来收听电台广播。一旦电台打开后，用户即可以从“电台指南”中选择一个电台收听，并且可以从 IE5.0 的界面上调整音量的大小。

使用电台的方法：

（1）在浏览器的“查看”菜单中选择“工具栏”，选择“电台”选项，如图 21-17 所示。

（2）此时会出现“电台”的工具栏。单击“电台”的下拉菜单可以选择自己喜爱的电台来进行收听。

图 21-17　收听电台广播

21.2.7　安全性的 Internet Explorer

当用户从 Internet 下载或运行程序时，用户一定想知道程序是否来自可靠而且已知的地方。这就是当用户选择从 Internet 将程序下载到用户的计算机时，Internet Explorer 为什么要用 Microsoft Authenticode 技术核实该程序身份。Authenticode 技术可检查程序是否拥有有效的证书，软件发行商的身份是否与证书相符，以及证书是否仍然有效。

注意：这样并不能阻止某些蓄意破坏的程序下载到用户的计算机上并在本地运行，但这样可减少某些人通过伪造的程序蓄意破坏的机会。

21.2.7.1 安全区域

用户可以针对 Internet Explorer 处理下载程序和文件的方式指定不同的设置，这取决于下载发生于哪个区域。例如，用户可能相信在用户的企业 Intranet 中下载的所有内容都是安全的。所以，可将“本地 Intranet 区域”的安全设置调整到较低的级别，以便下载时尽量少出或不出提示。如果下载源的位置属于“Internet 区域”或“受限站点区域”，可将安全级设置为“中”或“高”。这样，在程序下载之前，系统会提示用户提供有关程序证书的信息，否则用户将无法下载全部程序。

那么什么是安全的区域呢？Internet Explorer 将 Internet 世界按区域划分，以便用户将 Web 站点分配到具有适当安全级的区域。

Internet Explorer 状态栏的右侧显示当前 Web 页处于哪个区域。无论何时打开或下载 Web 上的内容，Internet Explorer 都将检查该 Web 站点所在区域的安全设置。

目前有 4 种区域：

■ Internet 区域：默认情况下，该区域包含了不在用户的计算机和 Intranet 上以及未分配到其他任何区域的所有站点。Internet 区域的默认安全级为“中”。

■ 本地 Intranet 区域：该区域通常包含按照系统管理员的定义不需要代理服务器的所有地址。包括在“连接”选项卡中指定的站点、网络路径（如 \\server\share）和本地 Intranet 站点（地址一般不包括句点，例如 http://internal），也可以将站点添加到该区域。本地 Intranet 区域的默认安全级为“中低”。

■ 可信站点区域：该区域包含用户信任的站点——用户相信可以直接从这里下载或运行文件，而不用担心会危害用户的计算机或数据，可将站点分配到该区域。可信站点区域的默认安全级为“低”。

■ 受限站点区域：该区域包含用户不信任的站点——不能肯定是否可以从这里下载或运行文件而不损害用户的计算机或数据，可将站点分配到该区域。受限站点区域的默认安全级为“高”。

此外，已经存放在本地计算机上的任何文件都被认为是最安全的，所以它们被设置为最低的安全级。无法将本地计算机上的文件夹或驱动器分配到任何安全区域。

21.2.7.2 设置安全级

为了对付来自网络中病毒或者恶意的攻击一定要设置安全级来进行防护。设置安全级的步骤有：

（1）单击“工具”菜单，选中“Internet 选项”，就会弹出“Internet 选项”对话框，如图 21-18 所示。

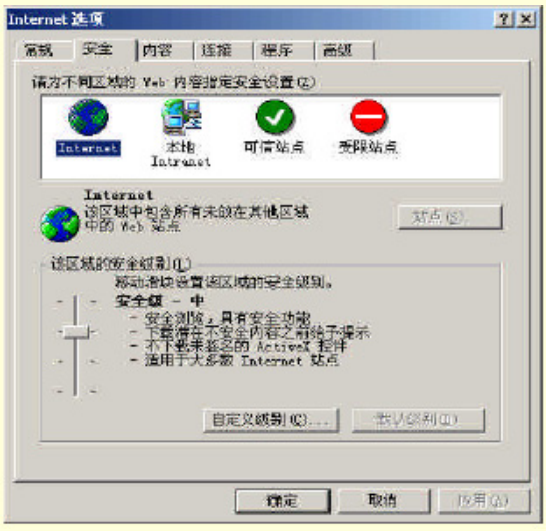


图 21-18 安全级的设置

（2）单击“安全”选项卡，就可以设置安全级。另外，还可以“自定义级别”，如图 21-19 所示，用户可以设定自己认为的安全级。

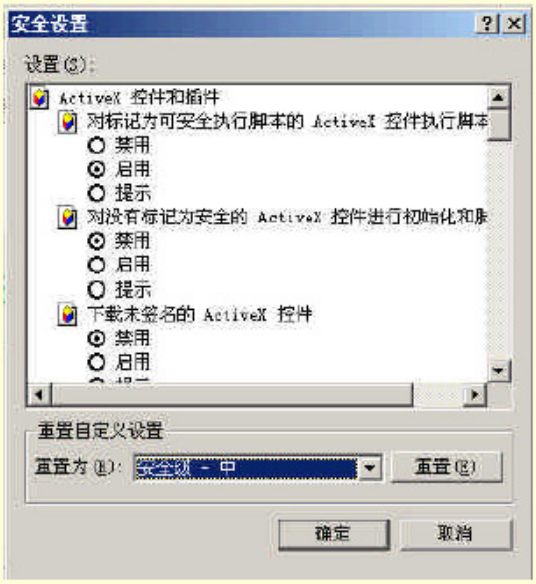


图 21-19　安全设置

21.2.7.3　设置分级审查

Internet 的资源浩如烟海、无穷无尽。但是，并非所有信息都是好的、健康的。例如，用户可能要防止小孩看到有关暴力或性等方面的内容，这些内容对孩子的毒害是非常的严重。

Internet Explorer 使用分级审查控制用户的计算机在 Internet 上可以访问的内容类型。当用户打开分级审查时，只能显示满足或超过标准的分级内容，用户可以调整这些设置。

（1）打开“Internet 选项”，选择“内容”选项卡，如图 21-20 所示。

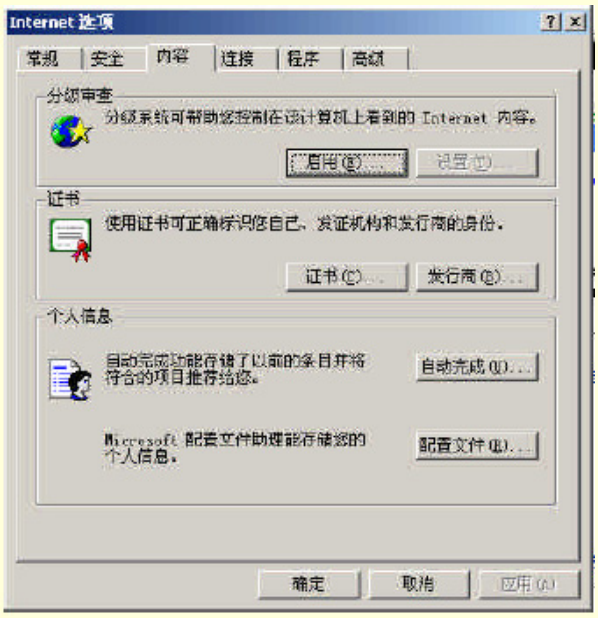


图 21-20　“内容”选项卡中的“分级审查”

（2）单击“启用”按钮，会弹出设置监护人密码的窗口，如图 21-21 所示，系统将提示用户创建监护人密码。

（3）按照所需要的安全级别设置，如图 21-22 所示。

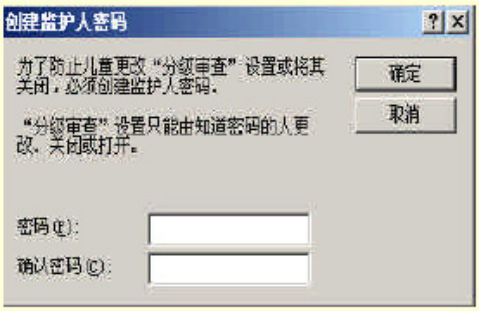


图 21-21 创建监护人密码

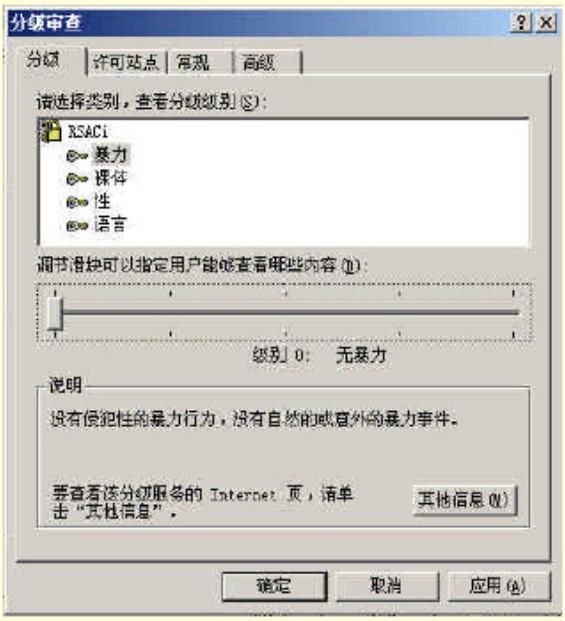


图 21-22 分级审查

（4）如果用户已经启用“分级审查”，可以单击“常规”选项卡，在“监护人密码”中单击“更改密码”，然后就可以修改监护人密码。

提示：用户可能需要将监护人的密码记下来，以后无论何时更改“分级审查”设置都需要键入该密码。

21.2.8 定制个性化的浏览器

Web 页面一般按照设置的大小、字体和颜色显示文本。不过，也可以按照自己的喜爱来定做原有的设置。这些改动可能影响了页面的布局，但却是页面更个性化或者更加易于阅读。在 Internet 选项中有各种的设置可以让用户修改，如图 21-23 所示。

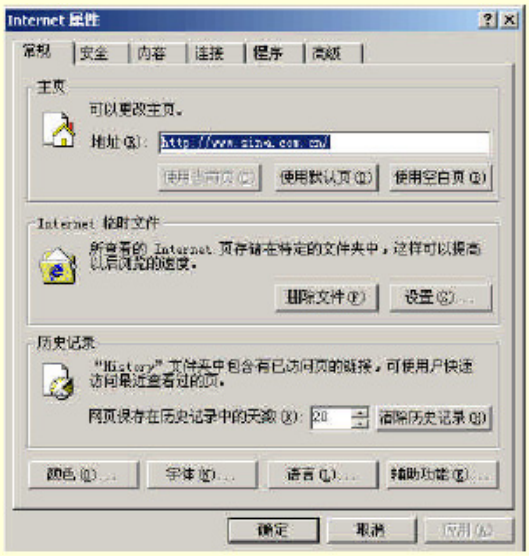


图 21-23　Internet 选项中的常规选项卡

21.2.8.1　更改主页

主页是在第一次启动 Internet Explorer 时显示的页面。一般默认的主页是 http://www.microsoft.com/windows/ie_intl/cn/start/，但这往往并不时用户想要浏览的网页，并且为了连接到它还浪费了上网时间。那么可以在更改主页中单击“使用当前页”，就可以输入要连接的主页地址了。

21.2.8.2　Internet 临时文件和历史记录

IE5.0 能够将以前用户访问过的文件保存下来，在 Windows 2000 中这些文件就保存在 c:\Documents and settings\的每一个用户的 Temporary Internet Files 文件夹中。以便当用户要进行脱机工作时的需要，其实可以对 Internet 临时文件进行设置，如图 21-24 所示。

图 21-24　Internet 临时文件的设置

其中用户可以将文件夹移动到另外的自己设定的地方去，以便更好地保存所浏览的网页和资料。用户也可以指定存放文件的磁盘空间。

注意：因为存放文件需要占用了一定的磁盘空间，如果设置了大量的磁盘空间来存放 Internet 文件，那么用户的硬盘也会因此而变小。

在历史记录区域中，用户可以指定网页在历史记录保存的天数，也可以单击“删除记录”来释放大量的已经占用的磁盘空间。

21.2.8.3 定制浏览器风格

如果对传统的 IE 有厌倦的想法，可以自己来定制浏览器的各种色彩与文字，使得浏览器符合个人的喜好要求。在图 21-22 所示中，可以看到有“颜色”、“字体”、“语言”和“辅助功能”的选择。如图 21-25 所示是对“颜色”的设置。

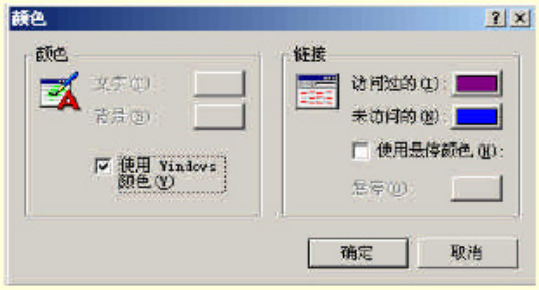


图 21-25 对浏览器“颜色”的设置

图 21-26 所示是对“字体”的设置。

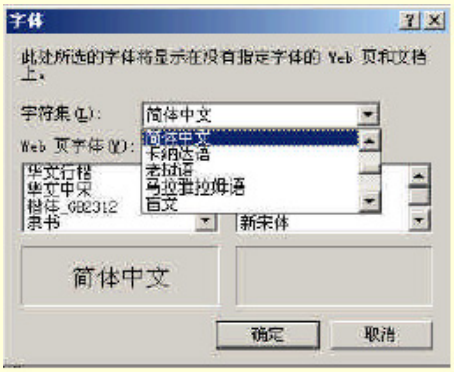


图 21-26 对浏览器“字体”的设置

而且还是可以添加对各种语言的支持，如图 21-27 所示。

图 21-27 语言的添加

如果用户视力不好、需要更大的字体或高对比度颜色，“辅助功能”对用户非常有用。可以设置 Internet Explorer 使用指定的颜色和字体、默认的 Windows 颜色和字体或者使用样式表中指定的设置，如图 21-28 所示。

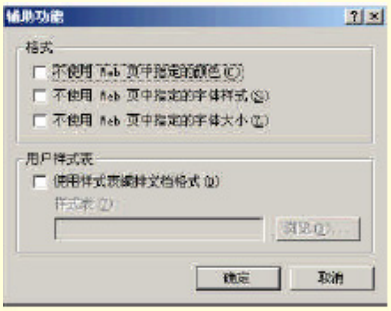


图 21-28　“辅助功能”选项

21.2.2.4　自动完成功能

其实在 IE5.0 中已经具有了智能化的导航，“自动完成”功能就是一个很好的例子。有了它在浏览的时候就可以不用记住以前填过的 Web 地址、表单、密码等。当然也可以将保存在内存里的内容清除，如图 21-29 所示。

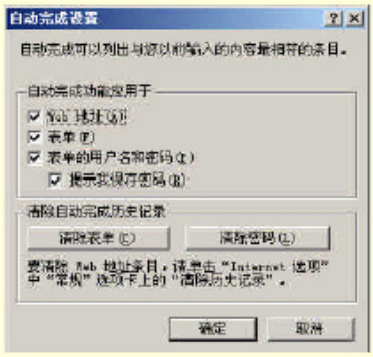


图 21-29　自动完成的设置

21.2.8.5 使用另外的通信程序

虽然 IE5.0 是 Windows 2000 内置的通信程序，但也可以在 IE 中使用别的程序来代替其他的程序，如图 21-30 所示。

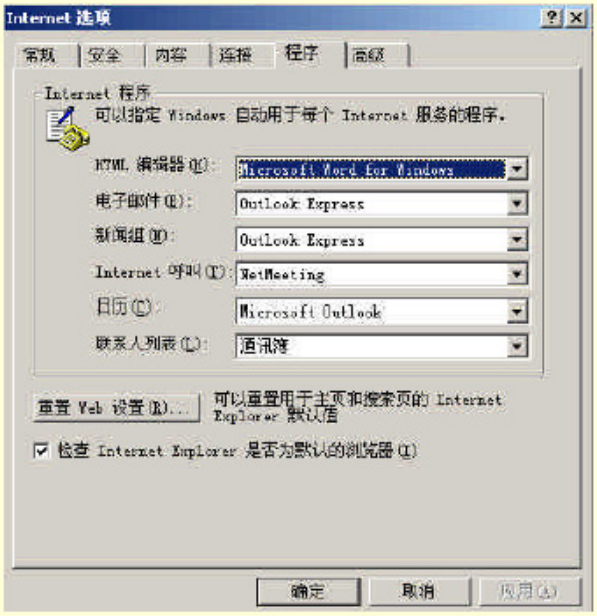


图 21-30　选择不同的程序用于 Internet

21.3 Outlook Express 5.0 联系你与我

Outlook Express 5.0 是一个用于电子邮件和新闻组的客户软件，利用它可以在全球的范围内与其他的用户进行联机通信。当利用 Internet 与朋友交换电子邮件的时候，或者是加入新闻组进行信息，交流的时候，Outlook Express 5.0 可能是最得力的助手。如图 21-31 所示为 Outlook Express 的用户界面。

通过计算机网络收发信息的服务，也是 Internet 提供的使用最广泛的信息服务。电子邮件有如下的特点：

■ 方便性

可以像使用留言电话那样在自己方便的时候处理记录下的请求，与联络的人知道在下一次打开电子邮箱的时候一定能够看到他们留给自己信件。另外你不但可以通过电子邮件来传送文本信息，也可以在适当的电子邮件软件的支持下传送图像文件、声音文件、报表或计算机的程序等。

■ 广域性

电子邮件系统具有开放性，使得许多非 Internet 网上的用户可以通过一些作为网关(Gateway)的计算机与 Internet 网上的用户交换电子邮件。目前， Internet 的电子邮件的服务区域远远超过了正式加入 Internet 的国家和地区。

■ 廉价与快捷性

如果使用常规的信函通过邮局来给同一国家或者外国的朋友传递信件，有可能会花费掉几天甚至十几天的时间，而使用电子邮件可能只需几分钟或者几个小时的时间。如果使用电话来与另一城市或另一国家的朋友来通话，就要求支付昂贵的电话费，而使用电子邮件则非常经济，甚至是免费的。

在 Windows 2000 中捆绑的 Outlook Express 5.0 有其独特的特点：

- 能够快速地发送，收取信件；
- 支持多用户，多账户。

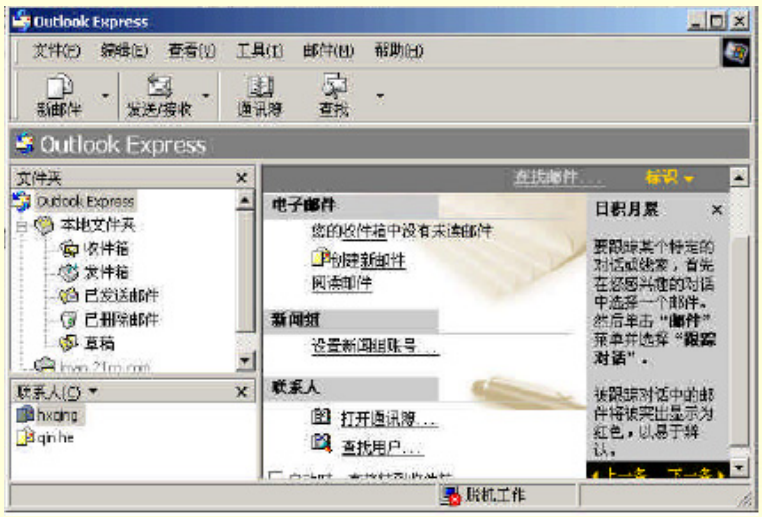


图 21-31 Outlook Express 的用户界面

- 账户访问口令控制。
- 信件浏览窗口，方便快速地阅读信件。
- 内置拨号网络管理，自动拨号上网和挂断。
- 方便地附加任意大小的文件到邮件中发送出去。
- 使用通信簿存储和检索电子邮件地址。
- 下载新闻组以便脱机阅读。

21.3.1　添加邮件账号和新闻服务器

如果从 ISP 或者其他途径中得到了自己邮件账号，那么就可以使用 Outlook Express 进行收发邮件。按照以下的步骤来设置 Outlook Express 新账号：

> **提示：要确保得到了电子邮件的帐号名、密码以及发送和接收邮件服务器的名称。另外如果要阅读新闻组，还需要所要连接的新闻服务器的名称。如果必要，还需要帐号名和密码。**

（1）在“工具”菜单中，单击“账号”，如图 21-32 所示。

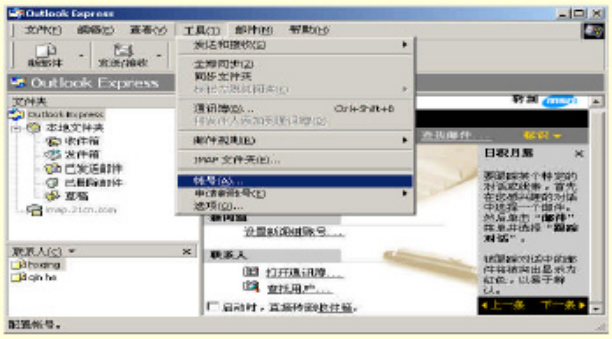


图 21-32　设置 Outlook Express 的邮件账号

（2）弹出“Internet 账号”对话框，如图 21-33 所示，然后单击“添加”按钮。

（3）选择“邮件”或“新闻”以打开“Internet 连接向导”如图 21-34 所示，以便建立与邮件或新闻服务器的连接，首先要求输入用户的姓名。

（4）单击“下一步”按钮后，要求输入用户已经拥有的电子邮件地址，如图 21-35 所示。这时候用户如果还没有指定的电子邮件地址，可以免费申请一个新的账号，这是 HOTMAIL 中的免费邮件账号。

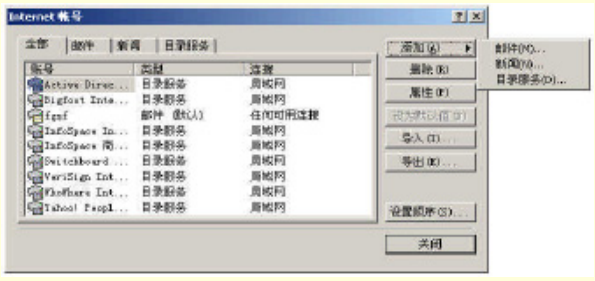


图 21-33　Internet 账号对话框

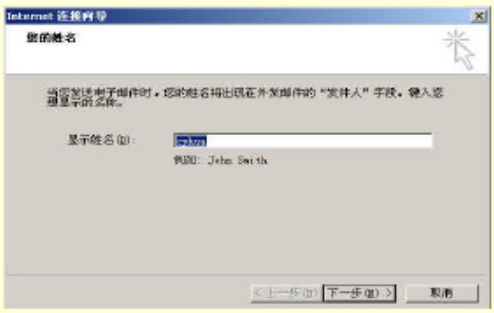


图 21-34　Internet 连接向导之——输入名称

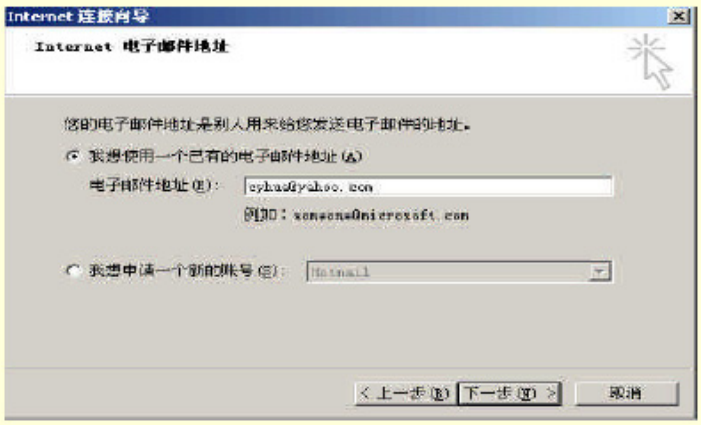


图 21-35 Internet 连接向导之二——输入邮件地址

（5）单击“下一步”按钮后，如图 21-36 所示，要求输入邮件服务器的类型（POP3、IMAP 或 HTTP），以及接收邮件服务器的名称、POP3 和 IMAP 所用的发送邮件服务器的名称。

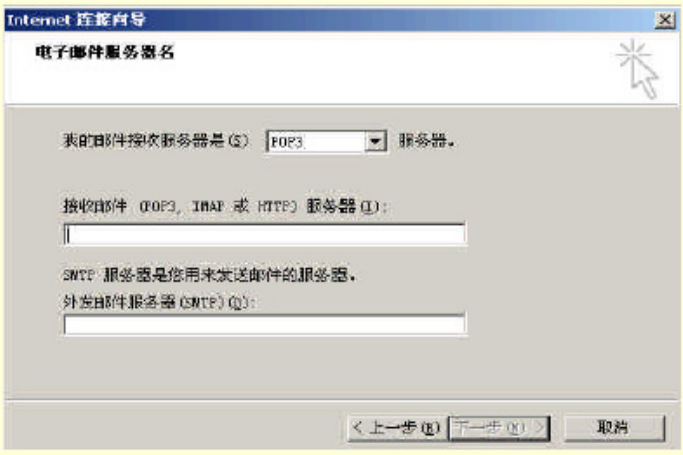


图 21-36 Internet 连接向导之三——输入邮件服务器的信息

（6）当正确输入了服务器的地址后，可以单击“下一步”按钮，此时要求输入账号名和密码如图 21-37 所示。

（7）单击“下一步”按钮后，就完成了 Internet Mail 的设置，如图 21-38 所示。

请注意新闻组的设置与电子邮件的设置是有一点区别，在上面的步骤 4 开始，要求输入新闻组服务器的地址，图 21-39 所示，单击“下一步”后就可以完成了设置，没有设置邮件的另外几个步骤。

如果用户还有其他的电子邮件的地址，还可以按照前面的步骤来继续添加。

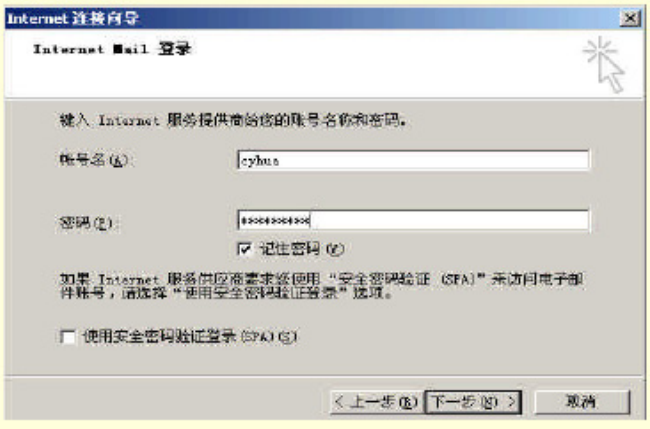


图 21-37 Internet 连接向导之四——输入账号名与密码

图 21-38　完成 Internet Mail 的设置

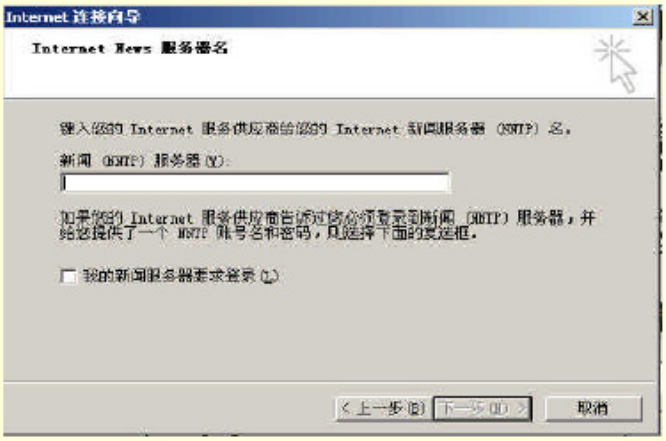


图 21-39　新闻组服务器地址的设置

21.3.2　接收和发送电子邮件

单击“工具栏”上的“发送/接收”按钮，就会弹出图 21-40 **所示的下载窗口。**Outlook Express **会自动地到用户电子邮件信箱去接收存放在邮局的邮件。另外还会将要发送的邮件发送到指定的** SMTP **服务器上，以便等待发送给收信人。如果选择了“完成后自动挂断”的复选框，那么** Outlook Express **还会在完成了所有的任务之后将网络挂断连接。**

图 21-40　接收和发送邮件

21.3.3 阅读邮件

将邮件接收回到收件箱后，就可以在 Outlook 单独的窗口或预览窗格中阅读邮件。

（1）单击文件夹列表中的“收件箱”图标，如图 21-41 所示。

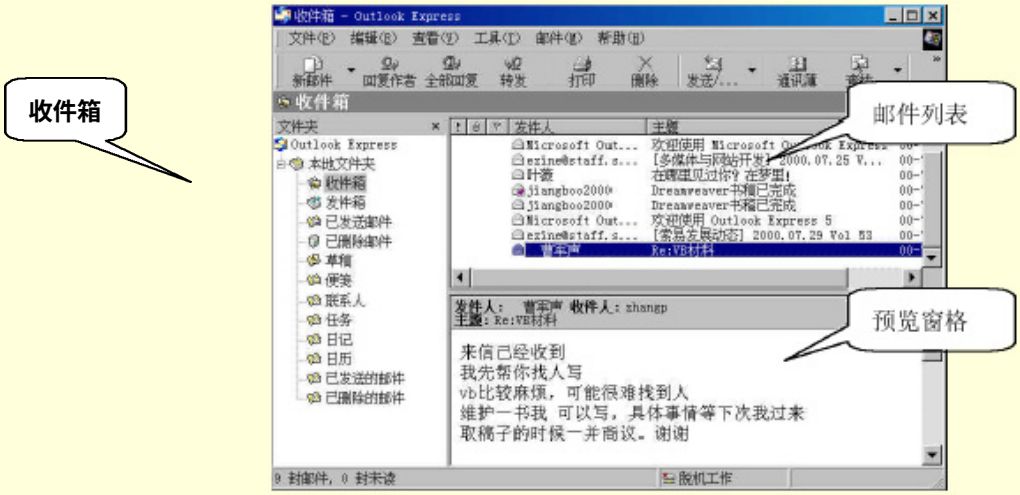


图 21-41 收件箱中阅读邮件

（2）若要在预览窗格中查看邮件，在邮件列表中单击该邮件。

（3）若要在单独的窗口中查看邮件，在邮件列表中双击该邮件。

（4）另外如果要查看有关邮件的所有信息（如发送邮件的时间），请单击“文件”菜单，然后单击“属性”。

（5）如果邮件中携带了附件，还可以双击预览窗格中的回形针，那么就会要求用户是否打开附件或者“保存附件”。

21.3.4 发送邮件

在“工具栏”上单击“新邮件”，就会弹出写邮件的模板，如果要选择信纸，还可以在新邮件的下拉菜单中挑选，如图 21-42 所示。

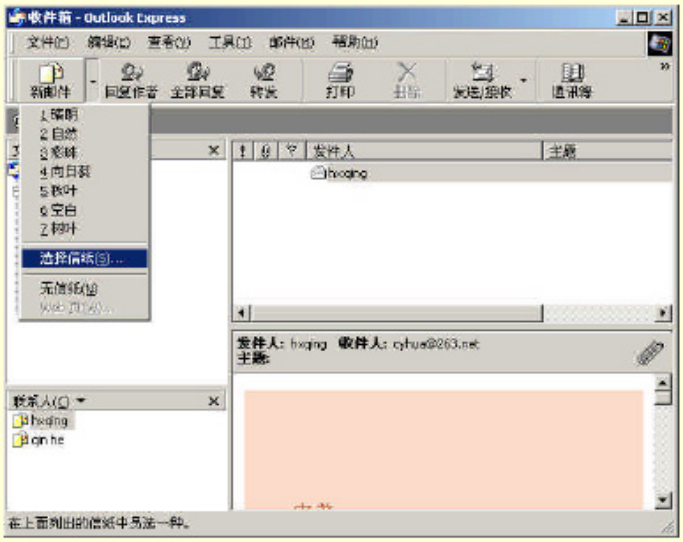


图 21-42 选择信纸

当将邮件的内容写好后，填上收件人的邮件地址和主题，就可以按工具栏上的“发送”，可以将邮件顺利地发送出去，如图 21-43 所示。

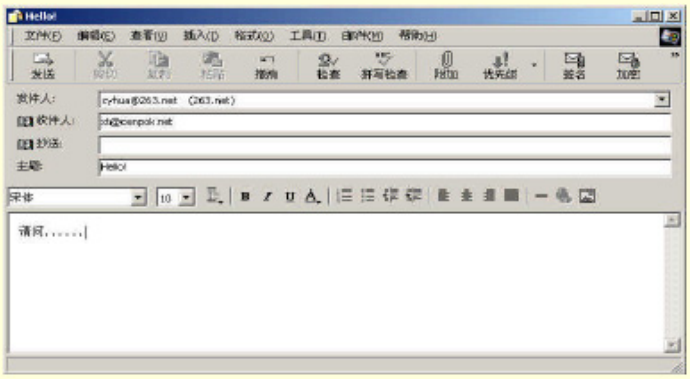


图 21-43　写新邮件

如果想要加上“附件”，可以单击工具栏上的回形针图标，选择在磁盘上的文件。

用户还可以设置“优先级”，使邮件的状态处于高级、普通或者低的优先级。“高优先级”的邮件带有一个感叹号标志，使收件人决定是立即阅读（高优先级），而“低优先级”邮件以一个向下的箭头表示，另收件人有空时再看（低优先级）。

用户可以选择“签名”，那么在发送邮件的时候就可以加上自己的数字签名，为邮件加密发送。

当然用户还可以将自己的邮件设置为“加密”的邮件。因为越来越多的人通过电子邮件发送机密信息，因此确保电子邮件中发送的文档不是伪造的，同时保证所发送的邮件不被除收件人以外的其他人截取和偷阅也同样重要。那么发送加密邮件就是最好的防护办法。

21.3.5　管理邮件

利用“邮件规则”，可以将所接受的满足某项条件的邮件发送到所需的文件夹中。当用户接收到大量邮件时，Outlook Express 可以帮助用户更有效地处理邮件。例如，用户可以将接收到的邮件自动分类并放入不同的文件夹中、以彩色突出显示特定的邮件、自动回复或转发特定的邮件，等等。

设置步骤如下：

（1）在 Outlook Express 的“工具”菜单下，选择“邮件规则”，如图 21-44 所示。如果从没有设置过邮件规则、新闻组规则，那么会弹出“新建规则”的窗口，如图 21-45 所示。

（2）输入接收邮件需要满足的条件，那么当邮件接收回来后，会自动的检查是否满足邮件规则符合的条件，然后要它执行规则规定的动作。

（3）接受邮件的时候，可能会有一些来自不清楚的邮件发送给用户，长年累月地将用户的邮箱挤得满满的。此时可以运用“阻止发件人规则”，如图 21-46 所示。从该发件人或域发来的电子邮件或新闻邮件将不会进入用户的收件箱或所阅读的新闻邮件。被阻止的发件人所发的电子邮件将直接进入“已删除邮件”的文件夹，而被阻止的发件人所发的新闻组邮件将不会显示，这样用户就不会看到那些讨厌的垃圾邮件。

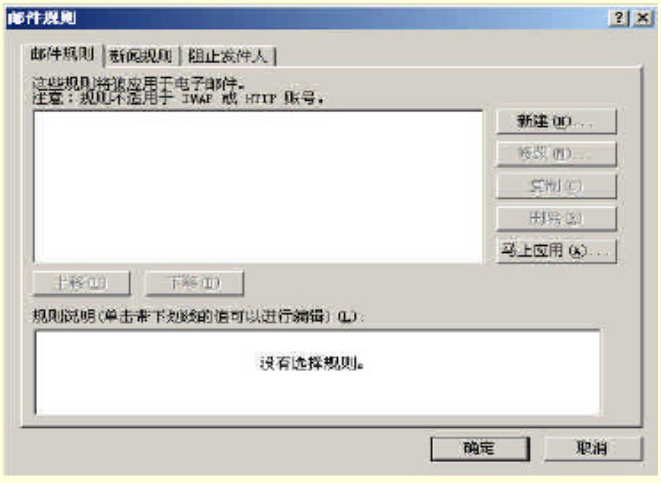


图 21-44　设置邮件规则

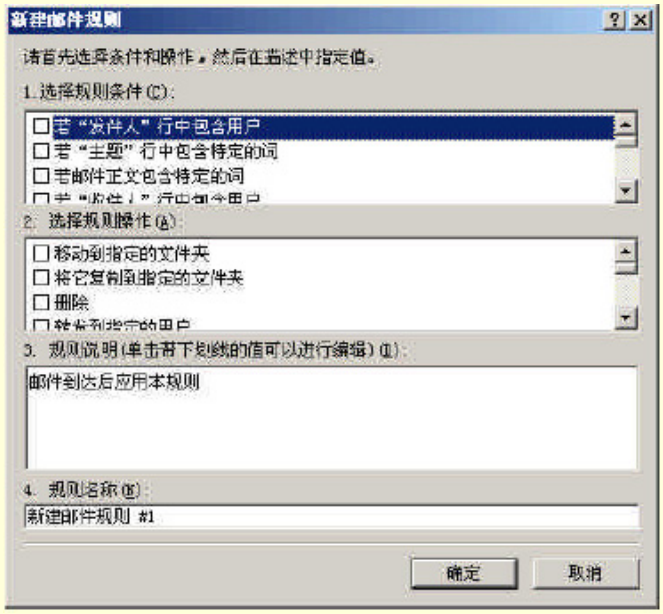


图 21-45　新建的邮件规则

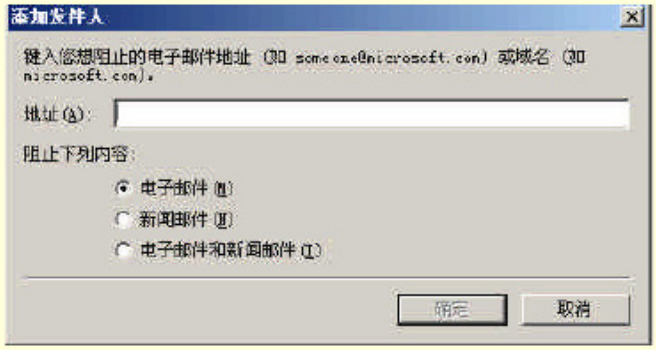


图 21-46　阻止发件人

21.3.6　阅读新闻

新闻组是个人向新闻服务器所张贴邮件的集合，一台计算机上可建立数千个新闻组，一般有公司、群组或个人负责管理和维护。用户几乎可以找到任何主题的新闻组。但是有些新闻组受到监控的，需要用户提供账号名与密码。

新闻组里包含成千上万的邮件，这使得邮件的分拣工作变得相当费时，而 Outlook Express **具有的多种功能可帮助用户快速地找到所需的新闻组信息。**

21.3.6.1　查找新闻组

要查找感兴趣的新闻组，可以通过新闻组服务器搜索新闻组名称中的特定单词。按照下列的步骤进行：

（1）在文件夹列表上，选择新闻组服务器名。

（2）单击“工具栏”上的“新闻组”按钮。

（3）在“显示包含以下内容的新闻组”中输入要搜索的内容，如图 21-47 **所示。**

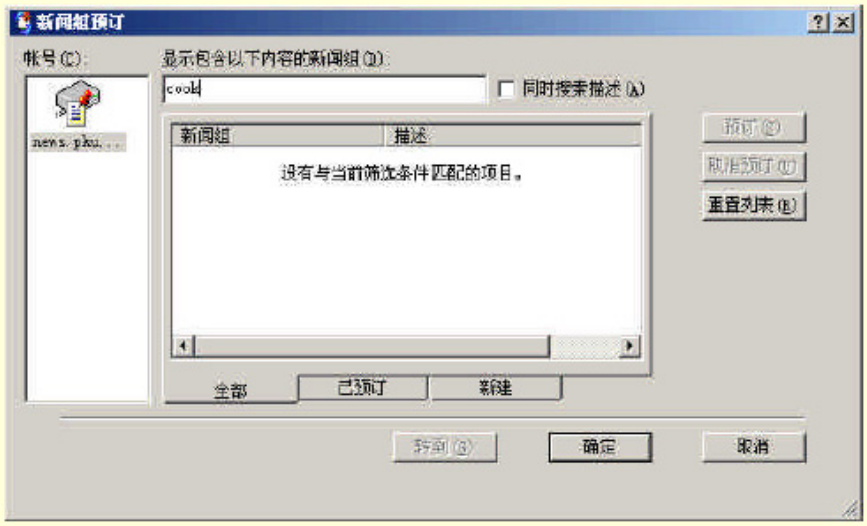


图 21-47　搜索感兴趣的新闻组

提示：如果在列表中没有找到特定的新闻组，这可能是因为在新闻服务器上没有这个新闻组。

21.3.6.2　预定新闻组

预订的好处在于，预订后的新闻组将包含在文件夹列表中，访问起来很方便。用户可以采取以下方式预订新闻组：

（1）单击文件夹列表中的新闻服务器名，然后单击“新闻组”按钮。选择要预定的新闻组，然后单击“预订”按钮。当然用户也可以在这里取消预订，如图 21-48 所示。

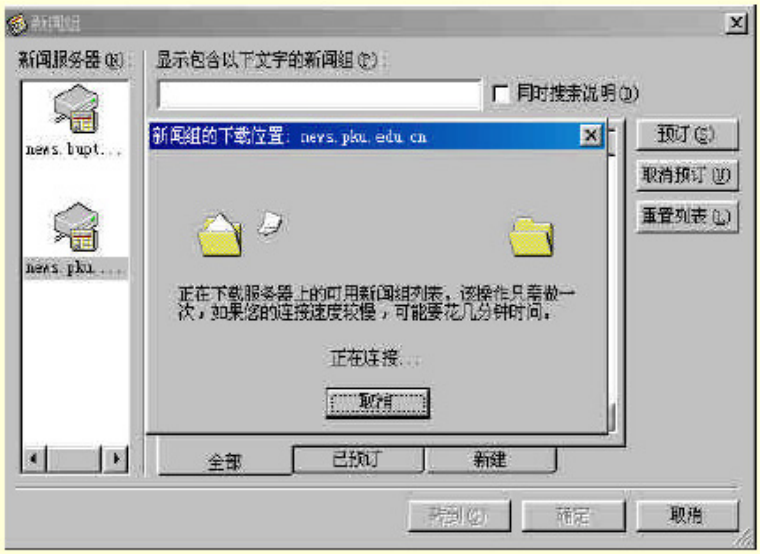


图 21-48　下载预定的新闻组

（2）在 Outlook Express 的左面的新闻组服务器上就会显示出所预订的新闻组，如图 21-49 所示。

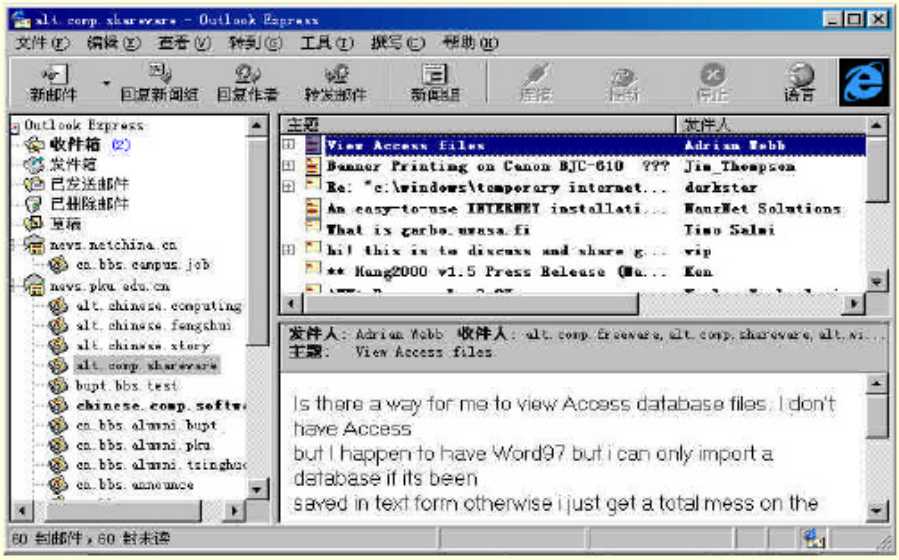


图 21-49 列出预订的新闻组

21.3.6.3 阅读新闻组

进入新闻组，从邮件列表中查找要阅读的邮件，然后双击邮件即可，如图 21-50 所示。

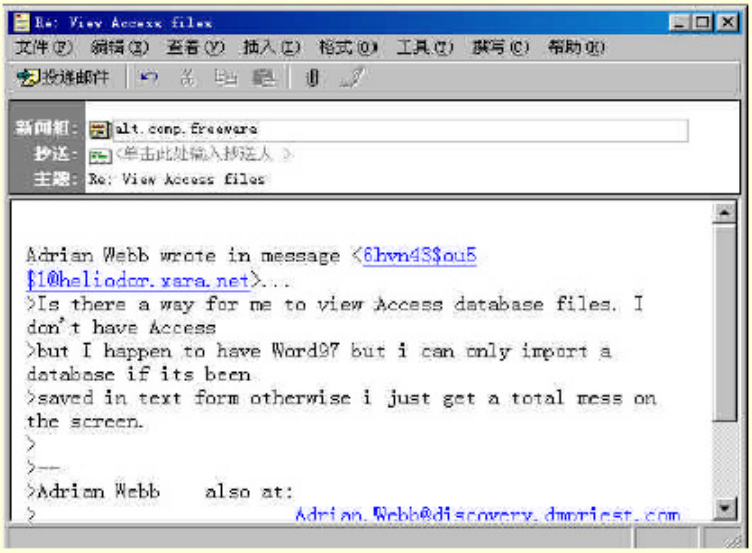


图 21-50 阅读新闻组中的邮件

21.3.6.4 投送邮件到新闻组

如果要回复新闻组里的内容，可以单击“回复作者”，然后写下自己要发表的内容，就可以将自己的邮件投送到新闻组中。

另外，还可以选中要投送的新闻组，单击“新投递”按钮。然后键入邮件的“主题”，注意 Outlook Express 无法张贴没有主题的邮件。

写好邮件后，可以单击“发送”按钮发送邮件。

提示：用户可以将一封特定邮件同时发送到多个新闻组中，但前提是所有这些新闻组必须在同一台新闻服务器上。若要将邮件发送到其他新闻服务器的新闻组中，请为每一台新闻服务器创建单独的邮件。

21.4　利用 NetMeeting 搭通天地线

Microsoft NetMeeting 为全球的用户提供了一种通过 Internet 进行交谈、召开会议及共享程序的全新的方式。随着 Internet 在世界上的广泛使用，网上交谈、网上会议是既实用又流行的交流方法。Windows 2000 中自带的 Microsoft NetMeeting 3.0 可以帮助用户方便地与世界各地的朋友及亲属进行面对面的交流！

NetMeeting 3.0 提供的功能包括有以下的几项：

- Internet 视频会议。
- Internet 电话及音频会议。
- 应用程序共享和文件传输功能。
- 白板程序，会议双方可以通过画图来交换信息。
- 聊天程序，会议双方可以通过输入文字来交换信息。
- 远程桌面共享，允许用户从另一位置的计算机访问某处的计算机桌面和文件。

21.4.1　硬件的需求

如果使用 NetMeeting 3.0 的音频功能，应该在启动 NetMeeting 的时候检查计算机中的声卡、话筒等是否工作正常；如果要在使用视频功能，还要检查摄像头是否安装好，NetMeeting 3.0 可以使用任何的支持 Windows 的视频捕捉卡或摄像机；另外还要保证已经连接上 Internet。

21.4.2　启动 NetMeeting

用户如果是第一次使用 NetMeeting，可以按照以下的步骤来进行：

（1）单击“开始”菜单，在“程序”中选择“附件”→“通讯”，就可以看到 NetMeeting 的选项，如图 21-51 所示。

（2）因为第一次使用 NetMeeting，会自动的弹出设置向导，其中包括了个人信息的设置，视频和音频的设置等。

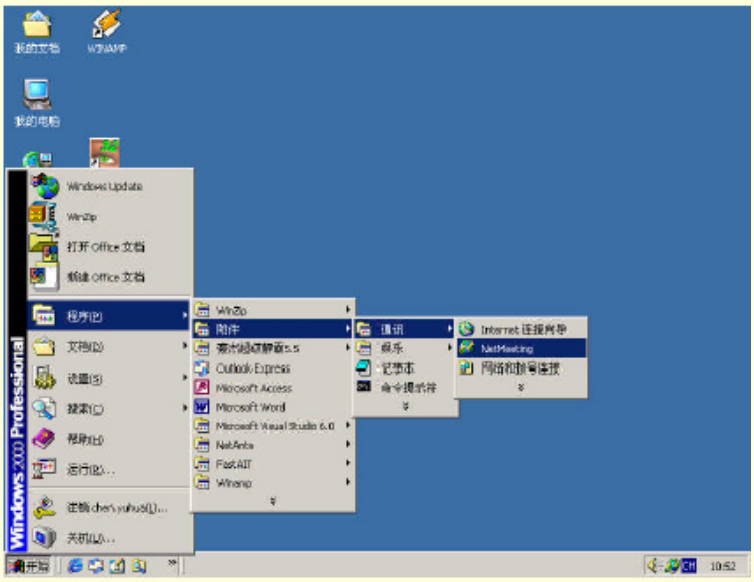


图 21-51　打开 NetMeeting

（3）如图 21-52 所示，说明了使用 NetMeeting 的各种功能。其中的功能包括了：与其他人谈话；通过视频看到别人或让别人看到自己；与其他人共享应用程序或文档；在共享的应用程序中与其他人进行协作；将文件发给其他人；在共享的白板中与其他人通过画图来进行交谈；将消息发送给聊天的其他人。

（4）单击“下一步”按钮后，弹出了要求输入个人信息的窗口，如图 21-53 所示，个人信息是在网络中标识用户的基本信息，可以要求 NetMeeting 服务器不要将这些信息显示出来，不过如果要结交朋友可以将个人

的信息填得真实一些，那么在网络中看到用户信息的朋友也会找到您，从而更好地和您聊天。

图 21-52　使用 NetMeeting 的各种功能

（5）单击“下一步”按钮后，要求选择“目录服务器”，如图 21-54 所示。“目录服务器”记录了目前登录到该服务器的人，一旦用户登录上该服务器后，其他的用户就可以看到您的名字，并且可以呼叫您。这时，用户为了保护自己，也可以选中“不要在目录中列出我的名字”复选框，这样其他的用户就不能在目录中发现您的名字，也就不能呼叫您了。

图 21-53　输入个人信息

图 21-54　选择目录服务器

图 21-55　网络的设置

（6）单击“下一步”按钮后，弹出的是网络的设置，如图 21-55 所示，可以设置为“14400bps 的调制解调器”、“28800bps 或更快的调制解调器”，或者是否使用“电缆、xDSL 或 ISDN”，又或者是否使用的是“局域网”。

（7）单击“下一步”按钮后，询问用户是否“请在桌面上创建 NetMeeting 的快捷方式”，是否“请在快速启动栏上创建 NetMeeting 的快捷方式”的选择，如图 21-56 所示。

图 21-56　桌面设置

图 21-57　调节音频效果

（8）然后会自动地弹出了音频调节向导，如图 21-57 所示。这时候确保扬声器和耳机已经连接好。可以测试采样的声音，是否过大或者过小，并且可以调整。

（9）接着下来是测试麦克风的效果，确保录音音量合适，如图 21-58 所示。

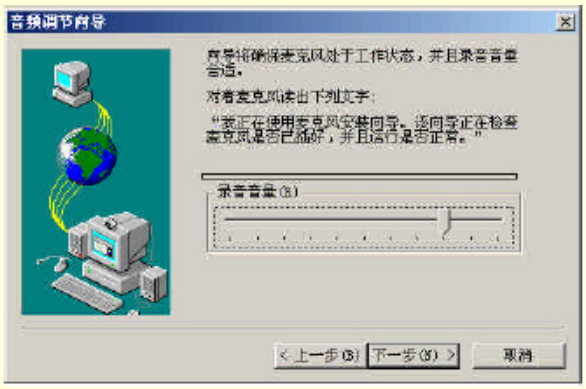


图 21-58　调节麦克风的工作状态

（10）当话筒没有安装完好的时候，会弹出如图 21-59 所示的警告窗口，这时候要返回上一步来进行重新的调整麦克风。

图 21-59　音频调节向导无法录音

（11）接下来祝贺您，已经将设置配置完好，如图 21-60 所示。

图 21-60　完成配置

21.4.3　如何用 NetMeeting 与别人连通

NetMeeting 提供了多种链接方式，可以根据具体的情况选择最适合的一种方法。

21.4.3.1　发出呼叫

用户可以将 NetMeeting 呼叫发送给多个用户。这时候 NetMeeting 需要直接连接到 Internet 目录服务器或其他计算机。要发送呼叫，既可以选择登录到服务器上的某人，也可以通过键入计算机名或地址来呼叫另一台计

算机。

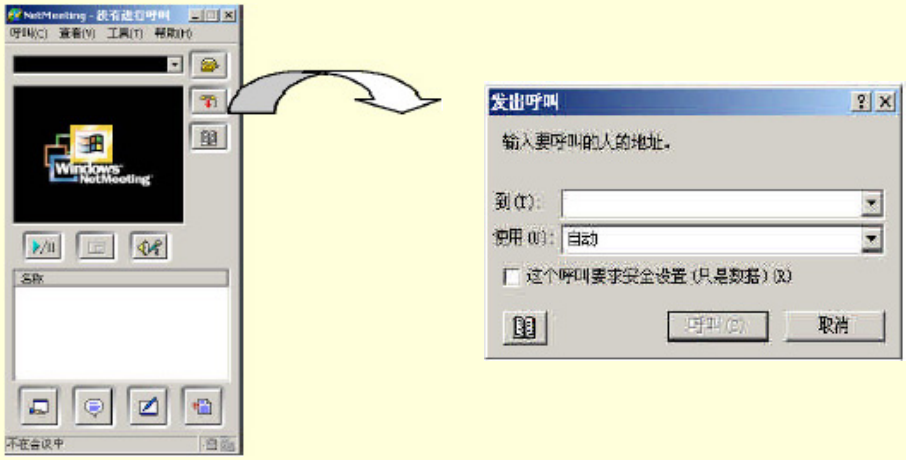


图 21-61　NetMeeting 的主界面

可以使用 Microsoft 维护的 Microsoft Internet Directory 查找其他 NetMeeting 用户。要查看 Microsoft Internet Directory，单击“呼叫”菜单中的“目录”，或者单击“在目录中找到某人”的图标，就会弹出如图 21-62 所示的“找到某人”的窗口。然后在“选择一个目录”中的单击“Microsoft Internet 目录”。

图 21-62　利用 Microsoft Internet 目录寻找某人

如图 21-60 所示，发出呼叫的步骤有：

（1）在“地址栏”上键入电子邮件地址、计算机名、电话号码和 IP 地址。也可以在“Microsoft Internet 目录”中寻找要寻找的用户，将他加入“地址栏”中去。

（2）单击“进行呼叫”按钮。

当有别的用户呼叫时，将显示“拨入的呼叫”对话框。请单击“接受”或“忽略”按扭。

21.4.3.2　音频会议功能

NetMeeting 允许用户与朋友或同事之间交换信息、进行项目协作、授课和进行展示。会议期间，无须在每台计算机上安装软件，即可共同地创建文档、电子表格或其他文件。此外，还可以向一个或全部会议参加者发送文件。

可以从用户的计算机或称为会议服务器的计算机上主持会议。主持会议时，可以选择会议名、密码、安全性以及谁能够被邀请参加会议。从会议服务器主持会议时，可以访问服务器并从列表中选择会议。如果会议未命名，用户可以使用默认名“Personal Conference”，或提供用户自己的名称。

一旦呼叫成功，便可以在 Internet 或 Intranet 上进行实时、点对点的音频会议。NetMeeting 音频会议提供了

多项的功能，包括了实时会议的半双工和全双工支持，自动设置麦克风的敏感度以及话筒的静噪特性，以确保声音的清晰。

如图 21-63 所示，主持会议的步骤有：

（1）在“呼叫”菜单中，单击“主持会议”。

（2）在“会议名称”中键入“会议名称”或保留个人首选项。

（3）在“密码”对话框中，要求输入“会议密码”，然后单击“确认”来启动会议。

（4）要创建安全会议，单击“要求安全性会议”复选框。安全会议是仅数据的呼叫。

（5）要监视谁加入了会议，单击“只有您可以接收拨入呼叫”复选框。

（6）要禁止与会者邀请其他人，单击“只有您可以发出拨出呼叫”复选框。

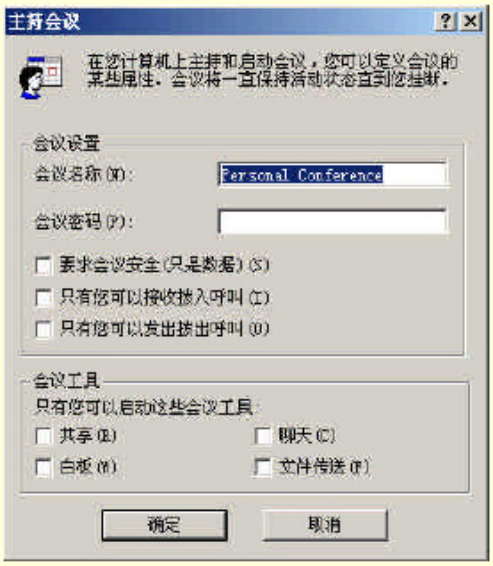


图 21-63　主持会议的设置

（7）要限制在会议中使用的工具，请选择“会议工具”下的某个选项，例如“共享”、“聊天”、“白板”和“文件传输”。如果用户正在主持安全会议，用户将无法使用音频和视频功能。

但如果不是用户自己主持的会议，加入会议就是呼叫会议主持人或任何会议参加者。但是如果用户呼叫某个非主持人与会者，呼叫可能会失败。如果这样，请呼叫会议主持人以加入会议。另外当用户要呼叫参加者时，只要与呼叫的人保持连接，用户就可以一直处于连接状态。当这个人从会议上离开或断开连接时，用户也将断开连接。

另外如果会议主持人要从会议中删除某人，用右击会议参加者，然后单击“从会议中删除”选项。

21.4.3.3　使用视频会议功能

可以使用 NetMeeting 为其他会议参加者发送自己的或所讨论项目的视频图像。但是要发送视频图像，需要有视频捕获卡和照相机，或者支持 Windows 视频的照相机。如果不需要发送自己的视频图像，仍然可以接收由其他的用户发送的图像。

如果要调整视频的效果，可以单击“工具”菜单，选择“选项”，弹出如图 21-64 所示的窗口。单击“视频”选项卡，然后拖动“视频质量”滑块，用户可以在速度与质量之间进行选择。用户也可以在这里设置“发送图像的大小”，例如小、中和大。

图 21-64　视频功能的设置

21.4.3.4　使用聊天和白板程序

使用“聊天”，会议参加者可以同时进行相互交谈，如图 21-65 所示。由于只有两个人能进行音频或视频连接，所以聊天在分组会议中很有用，这样一来每个人都能加入。

而使用“白板”，如图 21-66 所示，允许会议中的每个人同时绘制图形并键入文本。用户可以添加白板页、画图形、键入文本以及使用荧光笔或远程指示器强调某个项目。

图 21-65　聊天程序

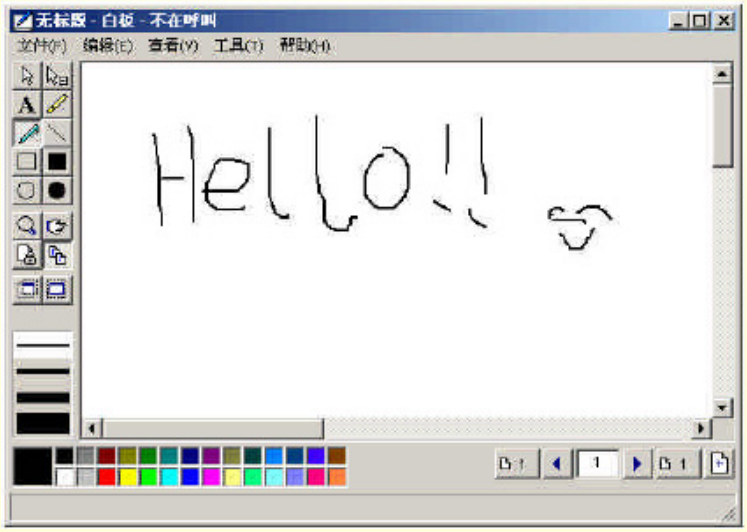


图 21-66 白板程序

21.4.3.5 在会议中共享程序

如图 21-67 所示，共享程序允许会议参加者同时查看和使用文件。例如，用户可能有个需要多人处理的 Microsoft Word 文档。用户可以在计算机上打开文档，将它共享，然后每个人都可以直接在该文档上添加他们的注释。只有打开文件的人需要在其计算机上安装程序。其他参加者可以在没有程序的情况下处理文档。

在同一时刻只能有一人控制共享程序。如果“可控制的”显示在共享程序窗口的标题栏内，说明共享该程序的人拥有控制权并允许其他人在该程序中工作。如果鼠标指针有一个带大写字母的对话框，则说明另一个会议参加者控制着该程序。

所有会议参加者都可以在开会期间共享程序。每个参加者的共享程序显示在其他参加者桌面的一个独立共享程序窗口内。

图 21-67 共享程序

共享程序的步骤有：

(1) 单击“共享程序”按钮。

(2) 在“共享”对话框中，单击要共享的程序名称。

(3) 单击“共享”。

注意：如果共享了“Windows 资源管理器”窗口，如“我的电脑”、“控制面板”或计算机上的文件夹，那么所有打开的“资源管理器”窗口都将被共享。另外，一旦共享了这样的窗口，则用户在会议期间启动的每个程序都将自动共享给其他与会者。

用户还可以允许别的用户控制共享程序，达到与其它的用户一起协作工作。操作步骤如下：

（1）单击“共享”对话框上的“允许共享”。

（2）在 NetMeeting 主窗口中，右击想让他人使用程序的相应人名，然后单击“授予控制权”。

（3）如果“允许控制”复选框灰显，说明尚未共享程序。必须先共享程序或桌面，然后才能允许控制。这一步操作在图 21-66 所示中体现，选中“允许控制”。

（4）当参加者请求获得控制权时，NetMeeting 将显示消息请求用户的准许。如果要自动授予许可，在图 21-66 中选中“自动为控制接受请求”复选框。

（5）如果除了当前有控制权的人外，用户不要任何人获得控制权，选中“现在不要为控制请求打扰”复选框。

（6）如果要停止对其他用户共享程序，可以单击“不共享”可以停止共享一个程序，单击“全部不共享”，可以停止共享全部程序。

21.4.3.6　使用发送文件与其他与会者交流

通过文件传送的功能，可以在后台将一个或多个文件发送给当前会议中的某一个人或所有的人。当然对方既可以接受文件也可以拒绝接受，如图 21-68 所示。

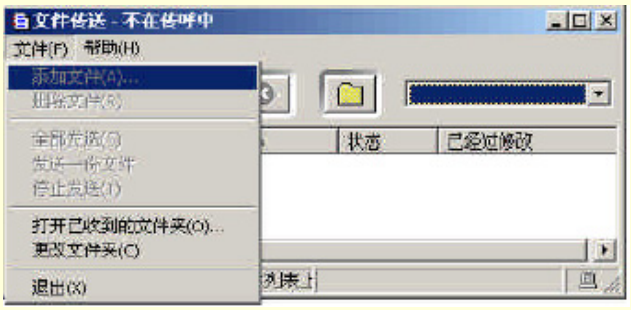


图 21-68　发送文件程序

具体步骤是：

（1）单击“传送文件”按钮。

（2）在“文件传送”对话框中，单击“添加文件”按钮，选择要发送的文件。

（3）单击想向其发送文件的人的姓名，或单击“全部”将文件发送给会议中的每个人。

（4）单击“全部发送”按钮。

（5）单击“接受”可以接收文件并关闭对话框。

提示：NetMeeting 将文件存放在您硬盘的 NetMeeting\Received Files 文件夹中。