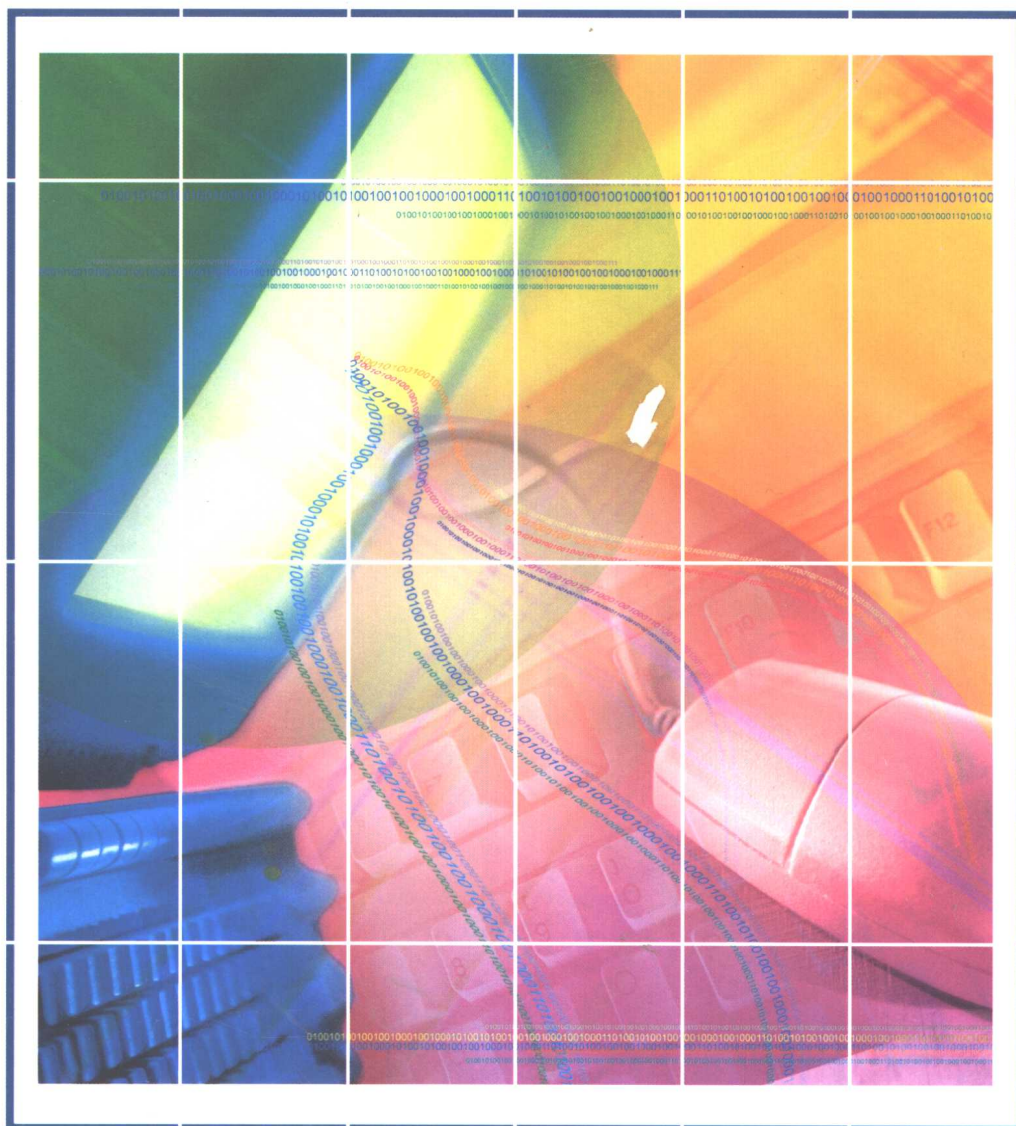


新世纪计算机类本科系列教材



操作系统实践教程

胡元义 徐甲同 编著



西安电子科技大学出版社

<http://www.xduph.com>

□新世纪计算机类本科系列教材

操作系统实践教程

胡元义 徐甲同 编著

西安电子科技大学出版社

2001

内 容 简 介

本书是作者在多年从事计算机操作系统课程的教学过程中积累起来的丰富的讲授和指导
学生上机实习的经验的基础上编写的, 书中的全部源代码都是作者亲手编写并上机通过的。

全书共七章。第一章为绪论; 第二章为单任务操作系统(STOS)的文件系统; 第三章为
STOS 的中断系统的内存管理; 第四章为 STOS 的实践; 第五章介绍多任务操作系统
(MTOS); 并给出了 MTOS 设计范例; 第六章介绍 UNIX 系统中的进程通信; 第七章介绍
Windows 编程。

本书可作为高等学校计算机有关专业的大专、本科操作系统课程实习指导书, 也可作
为科技、工程技术人员对操作系统进行学习、实践的参考书。

图书在版编目(CIP)数据

操作系统实践教程 / 胡元义, 徐甲同编著. —西安: 西安电子科技大学出版社, 2001.6

新世纪计算机类本科系列教材

ISBN 7-5606-1021-8

I. 操… II. ①胡… ②徐… III. 操作系统(软件)—高等学校—教材 IV. TP316

中国版本图书馆 CIP 数据核字 (2001) 第 21408 号

责任编辑 陈宇光 钟宏萍

出版发行 西安电子科技大学出版社 (西安市太白南路 2 号)

电 话 (029)8227828 邮 编 710071

<http://www.xduph.com>

E-mail: xdupfb@pub.xaonline.com

经 销 新华书店

印 刷 渭南邮电印刷厂

版 次 2001 年 6 月第 1 版 2001 年 6 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印张 11.25

字 数 265 千字

印 数 1~6 000 册

定 价 12.00 元

ISBN 7-5606-1021-8 / TP · 0504

*** 如有印装问题可调换 ***

本书封面贴有西安电子科技大学出版社的激光防伪标志, 无标志者不得销售。

前 言

从 1946 年第一台体积庞大且笨重的计算机发明至今, 仅仅半个多世纪, 计算机已经变得小巧玲珑、能力非凡, 它的应用已渗透到社会各个方面, 成为当今信息社会的最显著的特征。

操作系统是计算机系统中最核心和最底层的软件, 对操作系统的深入学习关系到对整个计算机系统运行机制的全面理解。因此, 对学习操作系统的学生来说, 首先是要有一本好的教科书, 其次还要有一本好的实践指导书。

操作系统的教材很多, 其中有不少的教材内容先进、结构清晰、体系合理、叙述严谨, 深受广大师生的好评。但是, 操作系统本身是一门实践性很强的课程, 虽然多数教材的作者尽力在自己的著作中强调其实践的重要性, 并用不少篇幅介绍了当时流行的各种操作系统的具体实例, 但由于读者缺乏具体的实践, 对操作系统的整体性和动态性仍不能透彻理解。基于这一想法, 我们编写了这本《操作系统实践教程》, 它作为操作系统课程的辅助教材, 供计算机专业的学生在操作系统课程实习时使用, 以期达到理论与实践相结合之目的。

本书共七章。第一章为绪论, 介绍了几种当前的主流操作系统, 强调了操作系统实践的重要性。第二、三、四章介绍单任务操作系统 STOS(Single Task Operating System), 它以 MS-DOS 为背景, 在第二章中介绍了文件系统, 在第三章中介绍了中断系统和内存管理, 在第四章中给出了八个 STOS 实践项目。第五章介绍了多任务操作系统 MTOS (Multiple Task Operating System), 给出了作者在 DOS 平台上开发的一个多任务操作系统范例。第六章为 UNIX 进程间通信的实践, 给出三个实践项目。第七章介绍了 Windows 编程的基础知识并给出了三个实践项目。

在本书的写作过程中, 为了尽量避免与操作系统教材的重复, 在各部分的叙述中只用较少的篇幅介绍基本概念, 随后给出相关的技术资料(这些资料在操作系统教材中往往找不到)以及大量例子, 最后给出了一些具有代表性的实践项目。其中每一个实践项目包括实践目的、实践内容、参考程序、实践要点和说明以及思考题, 使读者能举一反三, 触类旁通。

书中所有例题及实践中的源程序都是第一作者胡元义副教授亲手编写、上机调试所得的结果。

操作系统的核心部分通常采用汇编语言编写, 而系统的其余部分则采用 C 语言编写, 所以本书中的源代码均采用这两种语言。第七章的实践内容可在 C++ 或 VC 环境下运行, 对硬件则无过多要求, 目前常用的微机和计算机网络均能满足软件运行要求。

本书由胡元义副教授编写，由徐甲同教授对全书进行了修改、编排和审定。

在本书出版过程中，得到了西安电子科技大学出版社，尤其是陈宇光老师的热情帮助和大力支持，在此表示衷心的感谢。还要感谢西安理工大学的邓亚玲同志，她在本书初稿的录入中付出了辛勤的劳动。

编著《操作系统实践教程》对作者来说还是初次尝试。由于编著者水平有限，书中难免有不少错误和不妥之处，殷切希望广大读者批评指正。

编 著 者

2000年10月

目 录

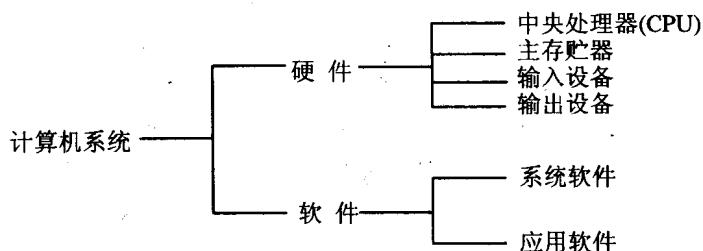
第一章 绪论	1	3.1.1 中断功能及特点	33
1.1 计算机与操作系统	1	3.1.2 中断程序设计	37
1.2 当前主流操作系统	2	3.1.3 中断程序实例	38
1.2.1 MS-DOS 操作系统	2	3.2 定时与时钟	42
1.2.2 UNIX 操作系统	2	3.2.1 日时钟运行原理	42
1.2.3 Windows 操作系统	3	3.2.2 中断 08H 时钟应用	43
1.3 操作系统的实践	3	3.2.3 INT 1AH 时钟应用	44
第二章 STOS 的文件系统	5	3.3 DOS 系统内存分配管理	46
2.1 STOS 系统的概述	5	3.3.1 DOS 系统内存映像	46
2.1.1 系统组成	5	3.3.2 内存控制块链	47
2.1.2 系统的引导	6	3.3.3 存储器的分段	52
2.1.3 DOS 文件管理特点	7	3.4 内存驻留	53
2.2 磁盘及其管理	8	3.4.1 TSR 程序结构	54
2.2.1 文件分配表结构	8	3.4.2 TSR 程序实例与编程要点	55
2.2.2 盘簇管理	10	第四章 STOS 的实践	60
2.3 DOS 目录管理	11	[实践一] 子目录管理	60
2.3.1 目录项结构	11	[实践二] 目录项结构——修改文件属性	62
2.3.2 子目录及其管理	13	[实践三] 文件分配表(FAT)作用——恢复 被删除文件	64
2.4 文件管理	15	[实践四] 创建文件	70
2.4.1 文件控制块 FCB	16	[实践五] 文件复制	72
2.4.2 FCB 文件管理方法	17	[实践六] 文件头结构——给 .EXE 文件 添加程序	77
2.4.3 文件句柄	19	[实践七] 程序加载方法——运行程序 中加载其他程序	82
2.4.4 文件句柄管理	20	[实践八] 内存驻留(TSR)方法——在屏幕 上弹出或隐去系统时间	86
2.5 可执行文件的加载执行	25	第五章 多任务操作系统(MTOS)	91
2.5.1 程序段前缀(PSP)	26	5.1 多任务操作系统概念	91
2.5.2 环境块(EVB)	27	5.2 MTOS 设计	92
2.5.3 映像加载 .COM 可执行文件	28	5.2.1 MTOS 总体方案	92
2.5.4 可重定位的 .EXE 文件	28		
2.5.5 EXEC 功能调用	31		
第三章 STOS 中断系统与内存管理	33		
3.1 中断系统开发技术	33		

5.2.2 MTOS 系统的数据结构	93	7.1.1 WinMain 函数	141
5.2.3 MTOS 系统中的进程状态变迁	95	7.1.2 窗口函数	145
5.2.4 MTOS 系统运行控制说明	95	7.2 Windows 实践	146
5.3 多任务操作系统程序示例	97	[实践一] Windows 窗口的创建	146
第六章 UNIX 进程间的通信实践	133	[实践二] 建立列表框	149
[实践一] 进程的创建	133	[实践三] 文件操作	153
[实践二] 生产者——消费者问题	134	附录 A DOS 系统功能调用	168
[实践三] 管道通信	137	附录 B BIOS 常用功能调用	170
第七章 Windows 操作系统的实践	141	附录 C ASCII 码表	172
7.1 Windows 编程基础知识	141	参考文献	174

第一章 绪 论

1.1 计算机与操作系统

一个完整的计算机系统包括硬件和软件两大部分，其组成如下：



硬件是指计算机的机器部分，即我们所见到的物理设备和器件的总称。软件通常指计算机系统中的程序和数据，并按功能分为系统软件和应用软件两类。系统软件是指为管理和使用计算机系统必须配置的那部分软件，如操作系统、汇编程序、编译程序等。应用软件是指针对某类专门应用需要而配置的软件，如计算机辅助教学 (CAI) 软件、财务管理软件以及飞机订票系统等。

仅有硬件的计算机系统称为裸机，直接使用裸机不仅不方便，而且严重降低了计算机的工作效率，特别是发展到今天的计算机，仅使用裸机已很难开展工作。为了对计算机所有软、硬件资源进行有效的控制和管理，在裸机的基础上形成了第一层软件，这就是操作系统。

操作系统是最基本的系统软件，是对硬件机器的首次扩充。其他软件都是建立在操作系统之上的，通过操作系统对硬件的功能进一步扩充，并在操作系统的统一管理和支持下运行。因此，操作系统在整个计算机系统中具有特殊的地位，它不仅是硬件与其他软件的接口，而且也是整个计算机系统的控制和管理中心，它为人们提供了与计算机进行交往的良好界面。有操作系统的计算机，其功能与裸机相比要大得多、完善得多，且使用起来也更加方便灵活。今天，操作系统已成为计算机必不可少的一部分，没有操作系统，计算机将无法运行。

1.2 当前主流操作系统

1.2.1 MS-DOS 操作系统

MS-DOS (Microsoft Disk Operating System) 是 Microsoft 公司的产品, 最初是为 IBM 的个人计算机配置的操作系统。MS-DOS 最早的设计目标是研制与 CP/M 兼容, 能在 16 位 INTEL 系列微处理器 (如 8086) 上运行的单用户、单任务操作系统。MS-DOS 自 1981 年问世以来, 一直是 PC 系列微型计算机及其兼容机上使用最广泛的操作系统。从 2.0 版开始, MS-DOS 在命令集上尽可能与 UNIX 兼容, 具有 I/O 重定向、管道等功能。随着硬件的飞速发展, MS-DOS 版本也不断升级: 2.0 版引入了层次树形结构的文件管理; 3.1 版增加了网络处理功能; 4.0 版提供了约束条件单用户、多任务的功能; 5.0 版支持多任务并可管理 16 MB 内存; 6.0 版在优化内存管理和压缩磁盘、高速缓存等方面提供了较多的功能。

MS-DOS 因为是单用户操作系统, 所以内存管理比较简单。早期的 8086/8088 只支持 1MB RAM 的地址空间, 且 PC 机在设计上只能直接寻址 640 KB 基本内存, MS-DOS 是以此为依据来设计内存管理部分的。因此, 尽管现在 IBM 微机寻址的空间已上百兆, 但考虑到兼容性, 一般软件仍只能在 640 KB 范围内运行, 若要用到 640 KB 以外的内存, 则必须有相应的软件支持。对于 I/O 管理, MS-DOS 实际上是由 ROM 和 MS-DOS BIOS 两部分组成的: 前者完成基本的 I/O 设备初始化工作, 后者处理逻辑设备到物理设备的映射。此外, MS-DOS 在管理 I/O 设备时还充分利用了系统调用方式为用户提供编程接口。MS-DOS 文件目录利用层次树形结构并通过路径名访问文件, 而 MS-DOS 文件的存贮结构则是通过文件分配表 (FAT) 索引链接进行的。

1.2.2 UNIX 操作系统

UNIX 操作系统是一个通用的、交互式的分时操作系统, 它是由美国 Bell 实验室的 K.Thompson 和 D.M.Ritchie 于 1969~1971 年设计实现的。UNIX 操作系统最初是用汇编语言编写的, 1973 年又用 C 语言改写了 UNIX。UNIX 已成为世界上一个著名的操作系统。

UNIX 本身是一个分时、多用户和多任务操作系统, 这是与 MS-DOS 的本质区别。UNIX 系统结构上分成两大部分: 内核部分和核外部分。内核部分就是 UNIX 操作系统本身, 它包括了进程管理、存贮管理、设备管理及文件管理。核外部分指从内核中分离出来以核外形式出现并在用户环境下运行的核外程序。内核向核外程序提供了强有力的支持; 核外程序则以内核为基础, 灵活地运用内核的支持。内核部分与核外部分两者结合成一个整体, 向用户提供了良好的服务。UNIX 向用户提供了两种界面: 一种是用户使用命令通过终端与系统进行交互作用的用户界面; 另一种是面向用户程序的系统调用界面。UNIX 具有一个树形结构的文件系统, 它由基本文件系统和若干个子文件组成, 且这个文件系统是可装卸的, 它不仅扩大了文件的存贮空间, 而且有利于安全和保密。在 UNIX 系统中, 文件和设备是统一处理的, 这样既简化了系统的设计又便于用户的使用。UNIX 系统还具有丰富的核外程

序, 它为用户提供了相当完备的程序设计环境。此外, UNIX 系统是用高级语言编写的, 可移植性好, 并且还具有易于理解、易于修改与扩充等特点。

1.2.3 Windows 操作系统

1985 年在 CPU 和图形显示技术发展的基础上, Microsoft 公司针对 MS-DOS 单任务处理方式和字符显示的不足, 推出了图形用户界面 (GUI) 的 Windows1.1 版操作系统。1990 年推出了走向成熟的图形窗口与“DOS”窗口并存的多任务系统 Windows3.x。从此, Windows 的操作方法和软件开发过程发生根本性变革, 即: 以“对话”、“图标”和“菜单”等图形画面和符号的全新操作方式替代了 DOS 环境下的命令行操作方式, 并由此引发了新的程序设计语言并大大简化了程序设计。

1995 年 8 月, Microsoft 公司再次适应 PC 机硬件的发展, 综合多年成就, 推出了全新意义的 Windows 95。Windows 95 摆脱了 Windows 对 MS-DOS 的依赖, 将 DOS 作为 Windows 的局部模块纳入系统, 全面实现了 32 位内存访问, 并将 Microsoft 网络并入到 Windows 系统中; 同时还更新了操作显示界面, 引入“即插即用”功能等许多先进技术。而随后推出的 Windows 98, 又将 Internet 的应用软件纳入系统, 使 Windows 向公用网络操作系统的方向迈进。

MS-DOS 作为单用户、单任务操作系统, 无论运行什么程序, 总是把系统资源全部分配给该程序, 这就造成了资源的极大浪费。Windows 是一种单用户、多任务操作系统, 它是在 DOS 基础上加入多任务功能形成的操作系统。Windows 实际上是在 MS-DOS 下接管内存及 I/O 管理并提供多任务机制的。对于每一个运行任务都有属于它自己的窗口和与之相联系的内存驻留程序, 不同的任务之间通过动态数据交换的通信机制来传送数据。Windows 维护一个全局的系统消息队列, 而对每一个窗口维护一个局部的消息队列; 只要消息队列不空, 任务(窗口)就继续运行。Windows 的内存管理比 MS-DOS 要复杂, MS-DOS 基本内存中的用户空间提供给 Windows 本身和应用程序使用。Windows 对存储器采用分段管理方法, 每段最大 64 KB; 段又分为固定段、可移动段和可删除段。固定段用于在 Windows 下运行 MS-DOS 程序; 可删除段是指在内存不够时, Windows 采用全局 LRU(最近最久不用)算法选择内存中某个可放弃的段予以删除; 可移动段是指可在内存中移动(需要重定位)但不能删除的段, 这样可以把内存中因分割而形成的碎片拼接成较大的连续空闲区。Windows 也支持段的共享。在 I/O 管理方面, Windows 除磁盘和打印机是由 ROM BIOS 完成之外, 其余均由 Windows 本身的设备管理程序完成。

1.3 操作系统的实践

操作系统是涉及概念多、理论性强且与实际联系紧密的一门计算机课程。但是, 由于操作系统自身的庞大与复杂, 加之操作系统教材普遍缺乏实践内容这一缺陷, 所以造成了许多学生在学过操作系统课程后, 总有一种“雾里看花”的感觉, 即只是支离破碎地了解了一些操作系统局部知识, 而很难将这些知识融会贯通, 形成一个对操作系统全面的、完整的理解和掌握; 对于灵活运用操作系统知识从事设计和应用, 则更是无从谈起。

本书主要涉及操作系统的实践，它作为操作系统课程的辅导教材，较好地解决了操作系统理论与实践的衔接，并给出了进行操作系统设计和应用的实例与方法。本书一方面考虑了微机的主流操作系统 MS-DOS，即单任务操作系统(STOS)的应用，因为它是微机应用和 Windows 操作系统的基础，也是微机操作系统的核心内容。另一方面，考虑到与操作系统进程等理论的衔接，即多任务操作系统 (MTOS) 的应用，本书给出了在 DOS 平台上开发一个多任务操作系统的实例。对目前影响广泛且流行的 UNIX 操作系统和 Windows 操作系统的应用也作了相应介绍。

操作系统的内核通常都采用汇编语言编写，而系统的其余部分则采用高级语言编写。由于 C 语言是目前从事系统程序开发的较好工具语言之一，所以，本书涉及的实践内容的编程均采用这两种语言之一编程，或用这两种语言混合编程。第七章的实践内容可在 C++ 或 VC 环境下运行。对于硬件，没有过多的要求，目前常用的微机和计算机网络均满足操作系统实践软件编程运行要求。

第二章 STOS 的文件系统

2.1 STOS 系统的概述

2.1.1 系统组成

MS-DOS 是具有代表性的 STOS (Single Task Operating System)。MS-DOS 由四部分组成, 即 DOS 引导记录 (BOOT)、基本输入输出系统 IO.SYS、DOS 内核 MS-DOS.SYS、命令处理程序 COMMAND.COM。含有上述四个部分的磁盘称之为 DOS 的系统盘。在引导记录的引导下, 将其余三个部分 (称之为 MS-DOS 的基本文件) 装入内存, MS-DOS 才成为一个可运行的操作系统。

MS-DOS 是个小巧精干的操作系统, 它采用模块化和层次化相结合的软件技术, 既把 MS-DOS 分成几个功能相对独立的模块, 又使这些模块之间呈现层次关系。MS-DOS 的系统层次结构如图 2-1 所示, 它有如下特点:

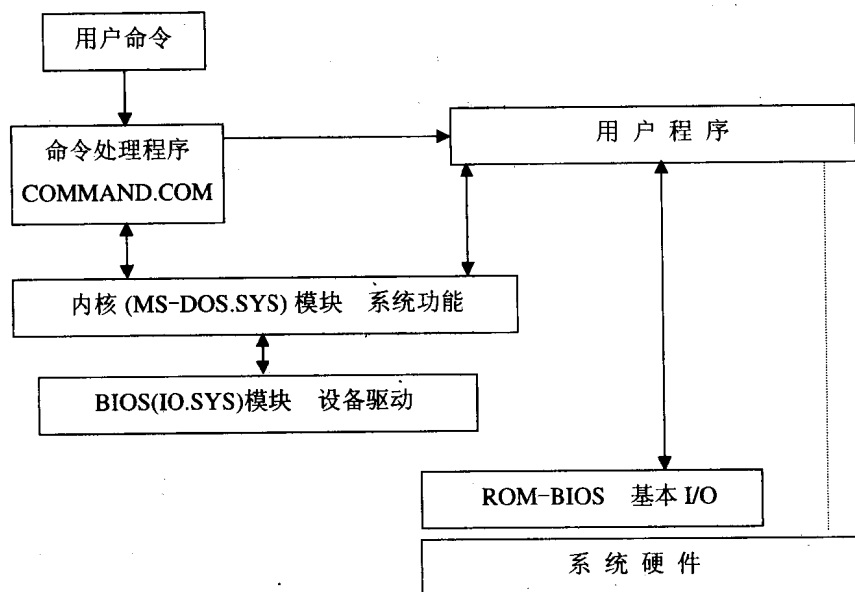


图 2-1 MS-DOS 系统层次结构

(1) 内核与硬件间两层隔离。在内核与硬件之间有 BIOS 和 ROM-BIOS 两层隔离,保证了 DOS 内核的独立性。IO.SYS 模块是 DOS 的基本输入输出系统 BIOS,它调用 ROM-BIOS 的设备的基本 I/O 功能的软中断,向内核提供设备驱动程序服务。这样, DOS 内核模块的代码中没有一条 I/O 指令,也没有这类软中断调用指令。

(2) COMMAND.COM 只是一个命令处理程序而不像 UNIX 的 shell 那样同时又是一种程序设计语言。用户程序一般不能出现 DOS 命令。

(3) 用户命令行和用户程序是不同的两个界面。用户命令行界面就是 COMMAND.COM,它接收用户键入的命令,并解释、执行予以响应。COMMAND.COM 层只调用 DOS 内核提供的系统功能服务,它绝不直接调用 BIOS 提供的设备驱动程序,更不去调用 ROM-BIOS 提供的设备 I/O 中断。

用户程序界面一般只调用 DOS 内核提供的系统功能(即系统调用)和 DOS 中断功能。但是,用户程序也可以绕过 DOS 内核,而直接调用 ROM-BIOS 的设备 I/O 中断,甚至可直接对设备硬件进行编程。

注意,使用 ROM-BIOS 中断编程易造成系统的不安全。例如,用户通过磁盘 I/O 中断——INT 13h 可在任何时间内对磁盘上的任何扇区进行无约束的访问,甚至可修改引导记录块、文件目录表(FDT)和文件分区表(FAT)等这些关键的系统数据区。MS-DOS 系统病毒之多正是由于 MS-DOS 对磁盘 I/O 缺乏全面的保护。

2.1.2 系统的引导

DOS 引导记录为一扇区 (512 B),位于逻辑 0 扇区处(软驱是 0 面 0 道 1 扇区,硬盘是 0 柱 0 面 1 扇区),由 FORMAT 程序形成,主要功能是完成 DOS 系统的引导(自举)。引导记录主要由两部分组成:一部分是磁盘 I/O 参数表(BPB),它记录了磁盘的重要信息,如每扇区的字节数、磁盘介质说明符等;另一部分就是 DOS 引导程序 boot 及其使用的数据。引导记录的最后两个字节内容为: 55h、AAh,这是有效的标志。引导记录的结构见表 2.1,而磁盘 I/O 参数表见表 2.2。

表 2.1 引导记录区结构

000h	转 移 指 令
003h	OEM 标志(厂家说明)
00Bh	磁盘 I/O 参数表 (BPB)
01Eh	其他参数及数据
036h	引导程序 boot
1FEh	55 AA

表 2.2 磁盘 I/O 参数表 BPB (以 360 KB 软盘、20 MB 硬盘为例)

偏 移	360 KB 软盘	20 MB 硬盘	说 明
BIOS 参数	0B 0C	00 02	每扇区字节数(0200h=512 B)
BIOS 参数	0D	02	每簇扇区数
	0E 0F	01 00	保留扇区数
	10	02	FAT 表个数
	11	70	根目录项数(软: 0070h=112 个)
	12	00	(硬: 0200h=512 个)
	13	D0	逻辑扇区数(软: 02D0h=720 个=360 KB)
	14	02	(硬: A370h=41840 个=20 MB)
	15	FD	磁盘介质说明符
补充信息	16	02	每个 FAT 占用扇区数(软: 2, 硬: 41)
	17	00	
	18	09	每道扇区数(软: 9, 硬: 17)
	19	00	
	1A	02	磁头数(软: 2, 硬: 4)
	1B	00	
	1C	00	隐藏扇区数(软: 0, 硬: 17)
	1D	00	

2.1.3 DOS 文件管理特点

自 DOS2.0 开始, DOS 借鉴了 UNIX 操作系统树形目录结构的优点, 将子目录也看作是一种文件类型进行统一管理, 这就取消了对文件个数的限制。DOS 文件系统的组织实际是一棵倒置的树: 最上层是根, 分支朝下; 从根目录出发的分支可以是树叶(即文件), 也可以是一个节点(子目录), 而每个节点又可以再分支出树叶或下一个节点, 从而形成了树形目录结构。在树形目录结构下, 不同的目录里可以出现相同的文件名。在树形目录结构中说明一个文件及其位置使用如下格式:

d:path filename.ext

其中, d: 是文件所在盘的驱动器符号, 缺省时指当前盘; path 是路径名, 它由一系列子目录名组成, 子目录名之间用"\ "符分隔, 路径名缺省时指文件在当前目录下, DOS 的每个盘卷(驱动器符)下都有自己的一个当前目录; filename 是文件名, 它最多由 8 个字符组成; ext 是文件扩展名, 最多由 3 个字符组成。

支持树形目录结构的关键是子目录。DOS 把子目录也看成是文件, 只不过这种文件是由一系列定长的目录项排列而成。DOS 把一盘卷上的全部文件和子目录文件都贮存在盘卷的文件区中, 文件存贮的分配单位是簇。DOS 规定一簇总是 2^n 个连续扇区, 即一簇可以是 1 扇、2 扇、4 扇、8 扇(每扇 512 B)等等; 具体某个盘卷采用的每簇扇区数, 取决于盘卷的类型和大小, 它们被记录在盘卷引导记录的 BPB 参数表中。一个文件的存贮空间由若干簇组成, 这些簇号可以不连续, 它们组成了文件的簇链。

无论是盘文件还是子目录文件，其簇链的组成情况都登记在盘卷的另一重要区域——FAT 区中。FAT 是文件分配表(File Allocation Table) 的简称，它的每个表项登记一个簇号。DOS 内核读取 FAT 表项内容，将簇号转换成逻辑扇区号，最后调用块设备驱动程序来完成扇区的读写操作。DOS 文件磁盘存贮状况全部登记在文件分配表 FAT 中。由于 FAT 如此重要，故有时也将 DOS 文件系统称为 FAT 系统。但遗憾的是，DOS 对 FAT 以及引导记录 boot 扇区基本上没有保护措施，这就给病毒程序造成了可乘之机。

DOS 盘卷的典型数据见表 2.3 所示。

表 2.3 DOS 盘卷典型数据

	保留扇数 (RS)	FAT 份数 (NF)	每个 FAT 扇区数 (FS)	根目录项数 (DS)	每簇扇数 (AU)
360 KB 软盘	1	2	2	112 项(7 扇)	2
1.2 MB 软盘	1	2	7	224 项(14 扇)	1
1.44 MB 软盘	1	2	9	224 项(14 扇)	1
10 MB 硬盘(单一分区)	1	2	8	512 项(32 扇)	8
42.5 MB 硬盘(单一分区)	1	02	81	512 项(32 扇)	4

DOS 盘卷中一些起始扇的逻辑扇号计算如下：

DOS 引导扇区扇号=0

FAT 表的始扇号=RS

备份 FAT 表的始扇号=RS+FS

根目录区始扇号=RS+NF×FS

文件始扇区号=RS+NF×FS+(32×DS/SS) SS: 每扇字节数

对盘卷文件区某簇第一扇的逻辑扇号计算如下：

逻辑扇号=文件区始扇区号+(簇号-2)×每簇扇数

注意：RS、NF、FS、DS 和 AU 均可以由磁盘 I/O 参数表 BPB 中获得。

2.2 磁盘及其管理

对于磁盘空间的管理，DOS 文件系统文件存贮采用了一个重要的数据结构——文件分配表 FAT。文件都存贮在 DOS 盘卷的文件区中，且是以簇为单位给文件分配存贮空间的：一个文件总是占有若干个整簇，首簇号登记在目录项中，其余的簇号则登记在 FAT 区中。DOS 盘卷通常有两个 FAT，即 FAT1 和 FAT2，它们是完全相同的。读出时只需从 FAT1 中即可读出，若不成功，再从 FAT2 读出，写入时却是同时写入。

2.2.1 文件分配表结构

文件分配表 FAT 有两种表结构：一种是每个表项为 1.5 B 的 12 位 FAT，另一种是每个表项为 2 B 的 16 位 FAT。目前，DOS 的各类软盘都使用 12 位 FAT；硬盘分区或逻辑盘是

采用 12 位 FAT 还是采用 16 位 FAT，由主分区表或逻辑分区表中的一个称为“系统标志”字节指出。表项为 2 B 的 FAT 表，每一项的内容是按低字节在前、高字节在后的规律存放的，而表项为 1.5 B 的 FAT 表则按“扣”状存放。两种存放形式如图 2-2 所示。

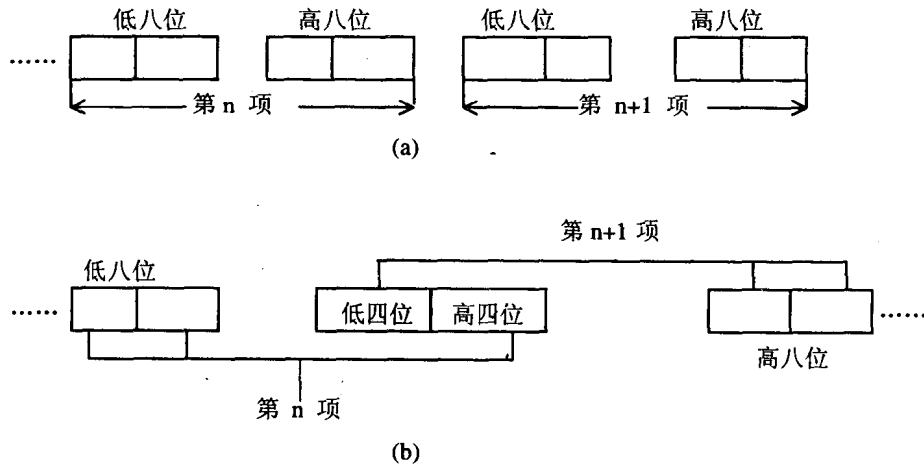


图 2-2 FAT 表表项的两种形式

(a) 2 B/项的 FAT 表表项形式；(b) 1.5 B/项的 FAT 表表项形式

在 FAT 表中，前两项(对应簇号 0 和簇号 1)被保留，用以说明磁盘性质和规格。以簇号 2 开始按逻辑区顺序方向编号(每簇扇区数由 BPB 指定)。每一个 FAT 表项在 FAT 表中的位置减去 1 为该项对应的簇号，而每一个 FAT 表项中的内容为文件下一簇的簇号(指一般情况)。FAT 表项内容见表 2.4。

表 2.4 FAT 表项说明

表 项 值	说 明
(0)00D	未占用
(F)FF0~(F)FF6	保留
(F)FF7	坏簇
(F)FF8~(F)FFF	最后一簇
(0)001~(0)002	不允许使用
其他	已占用，其值为下一簇的簇号

可见，FAT 表项的内容除少数用作特殊标志或保留外，大多数是表示下一簇的簇号。我们可以由目录项中偏移 1Ah 字域中给出的文件首簇号来查找 FAT 表，取此首簇号为序号对应的表项内容，从而得到顺序下一簇的簇号，再以它为 FAT 表项的序号取其表项内容得到第三簇的簇号……如此查找下去，直至所读出的表项内容大于或等于 (F) FF8 为止，从而找出了此文件顺序的全部簇号。DOS 的每个文件(包括子目录文件)就是由一系列簇号组成的一个簇链所构成的，除首簇号外，其余簇号全部登记在 FAT 表中并被衔接起来。图 2-3 给出了一个文件簇链的示意情况。

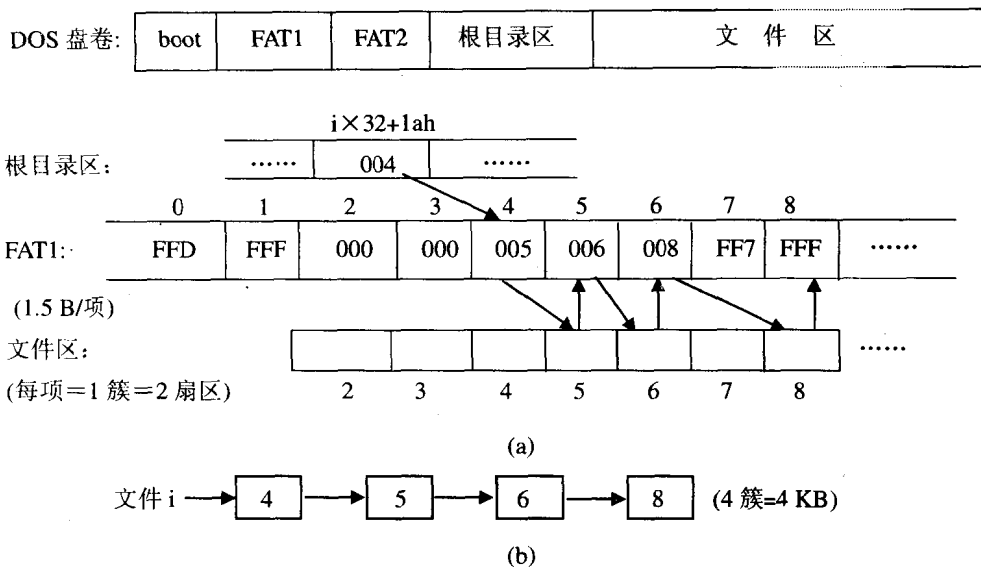


图 2-3 文件簇链组成情况(以 360 KB 软盘为例)

(a) 文件 i 簇链的形成; (b) 文件 i 簇链示意

注意: FAT 的头两个表项内容为 FFD 和 FFF, 其中 FD 是 360 KB 软盘的介质标记。任何一个 DOS 盘卷, 其 FAT 的第一个表项总保存有介质标记; 并且, FAT 的头两个表项总是保留不参加簇链的分配, 这就是文件区的簇号总是由 2 开始编号的原因。随着磁盘容量的不断扩大, 现在又出现了 32 位的 FAT。

2.2.2 盘簇管理

向一个文件(包括子目录文件)写入或追加新的内容, 就要进行簇的分配, 删除一个文件或一个子目录, 则要进行簇的释放, 这些都要涉及 FAT 的修改。

1. 簇的释放

当 DOS 响应“删除文件”系统调用时, 首先在目录项第一字节中写入 E5h, 置上删除标记; 然后沿文件首簇号搜索, 将 FAT1 中该文件占用的各簇号标记为 0, 变成可重新分配的未占用项。注意, FAT2 中该文件占用的各簇号并未标记为 0。

当 DOS 响应“删除子目录”系统调用时, 还要先做两件事: 一是先判断该子目录是否为当前目录, 若是则不准删除; 二是判断该子目录是否为“空”, 只有当子目录文件中只剩下“.”项和“..”项时, 该子目录才能被删除。两个判断都通过了, 删除子目录的操作与删除文件的操作就一样了。

这种删除操作表明, 只是文件分配表 FAT1 被修改, 一些簇号表项的内容变为(0)000h, 即可重新参与分配。但是, 被删除文件在文件区中所对应的各簇内的信息并没有被清除, 而且文件目录项也只是建立了删除标记(确切地说, 仅是将该文件名的头一个字符改为“?”), 文件的首簇号和文件长度信息以及目录项中的其他信息依然保存着。这时, 如果发现误删除了该文件, 并且在删除操作后还未执行像建立新文件或写文件以更新内容等导致 FAT 被修改操作的话, 那么利用 FAT2 完全能够恢复原文件。例如 PC-TOOL 工具软件中