

DOS

系统调用详解

北京天方图书创作室

李振格等 编著

北 京
航空航天大学
出 版 社

DOS 系统调用详解

天方图书创作室

李振格 等编著

北京航空航天大学出版社

(京)新登字 166 号

内容简介

本书详细讨论了 DOS 2.0,3.0,3.1,3.2,3.3,4.00,4.01 各版本的系统调用、调用汇编宏、调用实例等。介绍了所有 DOS 的数据结构,如 PSP,FCB,EXE 和 COM 头结构;环境块,DTA;中断矢量表;日期和时间表等,以及 BIOS 扩充和扩展内存调用方法,并说明了 IOCTL 的用法。

本书是在 DOS 环境下进行开发的必备工具,不仅提供了完整的 DOS 技术信息,还有助于提高程序的通用性和兼容性。

- 书 名: DOS 系统调用详解
DOS XITONG DIAOYONG XIANGJIE
- 编 著 者: 天方图书创作室 李振格 等编著
- 责任编辑: 杨昌竹
- 出 版 者: 北京航空航天大学出版社
- 地 址: 北京市海淀区学院路 37 号 100083
- 印 刷 者: 朝阳科普印刷厂印刷
- 发 行: 新华书店总店科技发行所
- 经 售: 北京航空航天大学出版社发行科
全国各地新华书店
- 开 本: 787×1092 1/16
- 印 张: 30
- 字 数: 774 千字
- 印 数: 8000 册
- 版 次: 1994 年 8 月第 1 版
- 印 次: 1994 年 9 月第 1 次印刷
- 书 号: ISBN 7-81012-481-1/TP·115
- 定 价: 30 元

前 言

DOS BIOS 系统调用是 IBM 个人计算机的核心,因为 PC 的操作系统就是由 ROM-BIOS、IBMBIO(对 MS-DOS 而言是 IO.SYS)、IBMDOS(对 MS-DOS 而言是 MSDOS)和命令解释程序 COMMAND 组成,而 DOS BIOS 系统调用(即服务子程序)是构成上述各部分的基本元素。

BIOS 调用管理了 PC 机的硬件特性,把与硬件相关的繁琐的管理与控制以子程序的方式提供;DOS 调用在 BIOS 调用的基础上,把 BIOS 子程序进一步“累积”,变成用户使用更为方便的子程序。BIOS 对 PC 机的控制最为全面,而 DOS 则次之,但 BIOS 的编程比 DOS 编程繁琐、难度大。

BIOS 不仅提供所有标准设备驱动程序,而且支持装载和初始化系统,DOS 提供应用编程接口(API)层,这包括设备支持(键盘、显示器、打印机和通讯口)以及文件支持,大多数功能可以通过 INT 21H 应用编程接口(Application Programming Interface 简写 API)访问,21H 中断提供很多不同的子功能,其他功能可通过 INT 25H,INT 26H,INT 2FH API 访问。

DOS 也包括文件分配表(FAT)文件系统。一个文件系统是一组子程序,也就是所说的存取方法,即在支持的介质上,把应用程序对数据的引用转换成物理的地址。FAT 术语的意思是文件分配表,正是具有像 FAT 的文件系统,才使得应用程序不需了解数据如何物理地存储在介质上,不需处理设备参数,如磁柱、磁头和扇区,取而代之的是应用程序只处理称之为文件的有名字的数据集。文件存储在称为目录的文件组里。由于具有像 FAT 的文件系统,允许 DOS 支持对已存在的应用程序不起或极少起作用的更新、更大的介质。例如 DOS 4.0 引进了大于 32MB 介质的支持。除了一少部分工作在介质物理级的磁盘实用程序外,现存的应用程序可以在没有任何改变的情况下存取这些大磁盘。

应用程序是建立在 PC 操作系统之上的,系统调用是应用程序完成所需功能的工具。本书讨论了 DOS 2.0, 3.0, 3.1, 3.2, 3.3, 4.0, 4.01 各系统调用,调用汇编宏,调用实例。介绍了几乎所有 DOS 的数据结构如 PSP FCB EXE COM 头结构、环境块、DTA、中断矢量表、日期和时间格式等。还介绍了 BIOS 扩充和扩展内存调用的方法,专论了 IOCTL 的用法。

本书在编译时得到了占卫兵的热忱帮助,在此表示感谢。

编 者

1991 年 1 月

目 录

第一部分 DOS 2.0,3.0,3.1,3.2,3.3 系统调用

第一章 MS-DOS 系统调用的用法

1.1 何谓系统调用(功能调用)	2
1.2 系统调用的种类	4
1.3 用 COM 模式开发程序	6
1.3.1 COM 模式的程序格式	6
1.3.2 宏定义与头文件	7
1.3.3 COM 模式的编译/连接的批处理	8
1.4 本书使用的头文件	8
1.4.1 STDIO.H(标准 I/O 头文件)	8
1.4.2 FILE.H(FCB 文件头)	12
1.4.3 FILEH.H(文件句柄头)	14
1.4.4 MEMORY.H(内存头)	15

第二章 MS-DOS 上的重要概念

2.1 PSP(Program Segment Prefix)	17
2.1.1 PSP 的结构	17
2.1.2 命令行的参数	18
2.2 使用 FCB 的文件处理	19
2.2.1 FCB 与 DTA	19
2.2.2 顺序文件与随机文件	20
2.2.3 文件属性	21
2.2.4 日期/时间的格式	22
2.3 使用文件句柄的文件处理	22
2.3.1 文件句柄	22
2.3.2 标准文件句柄	23
2.4 磁盘的结构	23
2.4.1 磁盘的分配	23
2.4.2 目录	24
2.5 内存管理	24

2.5.1 段与偏移量.....	24
2.5.2 内存分配.....	25
2.6 进程.....	26

第三章 MS-DOS 的隐含中断

中断类型 20H	29
中断类型 21H	30
中断类型 22H	30
中断类型 23H	32
中断类型 24H	34
中断类型 25H,26H	38
中断类型 27H	40

第四章 系统调用的详细说明

4.1 标准输入输出.....	42
4.2 文件管理(利用文件句柄).....	43
4.3 目录管理.....	43
4.4 磁盘管理.....	44
4.5 进程管理.....	44
4.6 内存管理.....	45
4.7 设备管理/MS-Networks 管理	45
4.8 其他.....	45
4.9 版本 2.0 以前的系统调用.....	46
功能 00H	46
功能 01H	47
功能 02H	48
功能 03H	49
功能 04H	52
功能 05H	52
功能 06H	54
功能 07H	56
功能 08H	57
功能 09H	59
功能 0AH	60
功能 0BH	62
功能 0CH	63
功能 0DH	64
功能 0EH	65
功能 0FH	66

功能 10H	68
功能 11H	70
功能 12H	71
功能 13H	73
功能 14H	74
功能 15H	76
功能 16H	77
功能 17H	79
功能 19H	81
功能 1AH	82
功能 1BH	83
功能 1CH	85
功能 21H	87
功能 22H	89
功能 23H	93
功能 24H	93
功能 25H	95
功能 26H	97
功能 27H	98
功能 28H	100
功能 29H	102
功能 2AH	105
功能 2BH	106
功能 2CH	107
功能 2DH	108
功能 2EH	109
功能 2FH	110
功能 30H	112
功能 31H	113
功能 33H	114
功能 35H	116
功能 36H	117
功能 38H	118
功能 39H	121
功能 3AH	124
功能 3BH	125
功能 3CH	127
功能 3DH	129
功能 3EH	131

功能 3FH	133
功能 40H	135
功能 41H	137
功能 42H	138
功能 43H	141
功能 44H, 高功能 00H, 01H	143
功能 44H, 副功能 02H~05H	145
功能 44H, 副功能 06H, 07H	147
功能 44H, 副功能 08H	148
功能 44H, 副功能 09H, 0AH	150
功能 44H, 副功能 0BH	151
功能 45H	152
功能 46H	153
功能 47H	155
功能 48H	157
功能 49H	159
功能 4AH	162
功能 4BH, 子功能 00H	164
功能 4CH, 子功能 03H	167
功能 4CH	170
功能 4DH	171
功能 4EH	173
功能 4FH	175
功能 54H	177
功能 56H	178
功能 57H	180
功能 58H	181
功能 59H	183
功能 5AH	186
功能 5BH	188
功能 5CH	190
功能 5EH, 子功能 00H	194
功能 5EH, 子功能 02H	195
功能 5FH, 子功能 02H	195
功能 5FH, 子功能 03H	196
功能 5FH, 子功能 04H	197
功能 62H	198

第二部分 DOS 4.00,4.01 系统调用

第六章 DOS4.0 和 DOS4.01 功能调用

6.1	DOS INT 21H 功能总结	261
6.2	DOS INT 21H 扩展错误代码一览	265
6.3	DOS INT 21H 扩展错误类型一览	268
6.4	DOS INT 21H 扩展错误处理一览	268
6.5	DOS INT 21H 扩展错误位置一览	268
6.6	常用功能使用建议	269
00H	——程序终止	269
01H	——带回显的控制台输入	269
02H	——显示输出	270
03H	——辅助输入	270
06H	——直接控制台 I/O	270
07H	——无回显,直接控制台输入	270
08H	——无回显、控制台输入	271
09H	——显示字符串	271
0AH	——缓冲键盘输入	271
0BH	——检查标准输入状态	272
0CH	——清键盘缓冲区、调用键盘功能	272
0DH	——磁盘复位	272
0EH	——选择磁盘	273
0FH	——FCB 打开文件	273
10H	——FCB 关闭文件	274
11H	——FCB 查找第一目录项	274
12H	——FCB 查找下一项	276
13H	——FCB 删除文件	276
14H	——FCB 顺序读	276
15H	——FCB 顺序写	277
16H	——FCB 创建文件	278
17H	——FCB 重命名文件	279
19H	——当前磁盘	279
1AH	——置磁盘传送地址	280
1BH	——分配表信息	280
1CH	——给定设备的分配表信息	280
1FH	——取缺省设备参数块	281
21H	——FCB 随机读	282
22H	——FCB 随机写	282

23H —— FCB 文件尺寸	283
24H —— 设置相对记录域	284
25H —— 置中断向量	284
26H —— 创建新程序段前缀	285
27H —— FCB 随机块读	285
28H —— FCB 随机块写	286
29H —— 分析文件名	287
2AH —— 取日期	287
2BH —— 置日期	287
2CH —— 取时间	288
2DH —— 置时间	288
2E00H —— 复位确认状态	288
2E01H —— 置确认状态	289
2FH —— 取盘传送区地址	289
30H —— 取 DOS 版本号	289
31H —— 结束并驻留	290
32H —— 取设备参数块	290
3300H —— 取 Break 状态	290
3301H —— 置 Break 状态	291
3305H —— 取引导驱动器	291
34H —— 取 DOS 内部标志地址	291
35H —— 取中断向量	292
36H —— 取磁盘自由空间	292
3700H —— 取开关字符	292
3701H —— 设置开关字符	292
38H —— 取/置国家信息	293
39H —— 创建子目录	294
3AH —— 删除子目录	294
3BH —— 改变目录	294
3CH —— 创建一个文件	295
3DH —— 打开文件	295
3EH —— 关闭文件句柄	297
3FH —— 读文件或设备	297
40H —— 写文件或设备	297
41H —— 删除一个文件	298
42H —— 移动文件读/写指针	298
4300H —— 取文件属性	298
4301H —— 置文件属性	299
4400H(IOCTL) —— 取设备状态	299

4401H(IOCTL)——置设备状态	300
4402H/4403H (IOCTL)——读/写字符设备	301
4404H/4405H(IOCTL)——读/写块设备	302
4406H/4407H(IOCTL)——取 I/O 状态	302
4408H(IOCTL)——测试块设备是否可移动	302
4409H ——测试逻辑设备是本/远地	303
440AH(IOCTL)——测试句柄为本/远地	303
440BH(IOCTL)——设置共享重入重试计数	303
440CH/440DH(IOCTL)——句柄/块设备通用 IOCTL 请求	304
440EH/440FH(IOCTL)——取/置逻辑驱动器	304
45H ——复制文件句柄.....	305
46H ——强迫复制文件句柄.....	305
47H ——取当前目录.....	305
48H ——分配内存块.....	306
49H ——释放内存块.....	306
4AH ——修改分配的内存块	307
4B00H ——执行程序(EXEC)	307
4B01H ——装入程序	308
4B03H ——装入覆盖	308
4CH ——终止进程(Exit).....	309
4DH ——取子进程的返回码	309
4EH ——查找第一个匹配文件	309
4FH ——查找下一个匹配文件	310
50H ——设置活动进程数据块.....	311
51H ——取活动进程数据块.....	311
52H ——取 DOS 内部值	311
54H ——取验证状态.....	312
55H ——复制 PDB	312
56H ——重命名/移动文件(重命名目录)	313
5700H ——取文件日期和时间.....	313
5800H ——取分配策略.....	314
5801H ——设置分配策略.....	314
59H ——取扩展错误信息.....	315
5AH ——以唯一名创建文件	315
5BH ——创建新文件	316
5C00H ——锁定文件存取	316
5C01H ——打开文件锁定	317
5D00H ——DOS 调用服务器	317
5D01H ——提交所有文件	318

5D02H ——以名字关闭文件	318
5D03H ——关闭特定计算机的所有文件	318
5D04H ——关闭特定进程的所有文件	319
5D05H ——取打开文件列表项	319
5D06H 和 5D0BH ——取 DOS 数据区地址	319
5D07H ——取打印流状态	320
5D08H ——设置打印流状态	321
5D09H ——截断打印流	321
5D0AH ——设置扩展错误信息	321
5E00H ——取机器名字	321
5E01H ——设置机器名	322
5E02H ——置打印机设置(Set up)	322
5E03H ——取打印机设置	323
5E04H ——设置打印机模式	323
5E05H ——取打印机模式	323
5F00H ——取重定向模式	324
5F01H ——置重定向模式	324
5F02H ——取重定向列表项	325
5F03H ——重定向设备	325
5F04H ——取消重定向	326
5F05H ——取扩展的重定向列表项	326
60H ——翻译文件规范	327
62H ——取 PSP 地址	327
6300H ——取 DBCS 前导字节表	328
6301H ——置/复位 Hangeul 模式	328
6302H ——取 Hangeul 模式	328
6501H ——取扩展国家信息	329
6502H/6504H ——取文本/文件大写(UpperCase)表地址	330
6506H ——取对照表地址	330
6507H ——取 DBCS 向量	331
6520H/6521H/6522H ——大写映射功能	331
6523H ——YES/NO 检查	332
6600H ——取全局(Global)代码页	332
6601H ——设置全局代码页	332
67H ——设置句柄计数	333
68H ——提交文件	333
6900H ——取介质 1D	333
6901H ——置介质 1D	334
6CH ——扩展打开/创建文件	334

第七章 DOS 4.00 功能调用实例

00H —— 程序终止	336
01H —— 带响应的控制台输入	336
02H —— 显示输出	337
03H —— 辅助设备输入	337
04H —— 辅助设备输出	337
05H —— 打印输出	338
06H —— 直接控制台 I/O	338
07H —— 无响应的直接控制台输入	339
08H —— 无响应的控制能输入	339
09H —— 显示字符串	340
0AH —— 带缓冲的键盘输入	340
0BH —— 检测标准输入状态	341
0CH —— 清除键盘缓冲区并调用键盘功能	341
0DH —— 磁盘复位	341
0EH —— 选择磁盘	341
0FH —— 打开文件	342
10H —— 关闭文件	342
11H —— 搜索第一个目录项	343
12H —— 搜索下一个目录项	344
13H —— 删除文件	345
14H —— 顺序读	345
15H —— 顺序写	346
16H —— 建立文件	346
17H —— 文件换名	347
19H —— 当前磁盘	348
1AH —— 设置磁盘传输地址	348
1BH —— 分配表信息	348
1CH —— 指定设备的分配表信息	349
21H —— 随机读	349
22H —— 随机写	350
23H —— 文件大小	351
24H —— 设置相对记录字段	351
25H —— 设置中断向量	352
26H —— 建立新程序段	352
27H —— 随机块读	352
28H —— 随机块写	353
29H —— 解析文件名	354

2AH ——取日期	355
2BH ——设置日期	355
2CH ——取时间	356
2DH ——设置时间	356
2EH ——设置/复位 Verify 开关	357
2FH ——取磁盘传输地址(DTA)	357
30H ——取 DOS 版本号	358
31H ——终止进程并保持常	358
33H ——读取/设置系统值	359
35H ——取中断向量	359
36H ——取磁盘自由空间	360
38H ——读取/设置国别信息	361
39H ——建立子目录(MKDIR)	362
3AH ——取消子目录(RMDIR)	363
3BH ——改变当前目录(CHDIR)	363
3CH ——建立文件(CREAT)	364
3DH ——打开文件	364
3EH ——关闭文件句柄	368
3FH ——从文件或设备读入	368
40H ——写到文件或设备	369
41H ——从指定目录删除文件(UNLINK)	370
42H ——移动文件读/写指针(LSEEK)	370
43H ——改变文件模式	371
44H ——设备输入/输出控制	371
45H ——复制文件句柄(DUP)	372
46H ——强行复制文件句柄(FORCDUP)	373
47H ——取当前目录	373
48H ——分配内存	374
49H ——释放已分配的内存	374
4AH ——修改已分配的内存块(SETBLOCK)	374
4BH ——装入或执行程序(EXEC)	375
4CH ——终止进程(EXIT)	377
4DH ——取子进程的返回代码(WAIT)	377
4EH ——查找第一个相符的文件(FIND FIRST)	378
4FH ——查找下一个相符的文件(FIND NEXT)	379
54H ——取检验开关设定值	379
56H ——文件换名	380
57H ——读取/设置文件的日期和时间	380
59H ——取扩充错误	381

5AH —— 建立临时文件	382
58H —— 建立新文件	383
5CH —— 锁定/开锁文件访问	384
5E00H —— 取机器名	385
5E02H —— 设置打印机的配置	385
5E03H —— 取打印机的配置	386
5F02H —— 取重定向表项	387
5F03H —— 重定向设备	388
5F04H —— 取消重定向	389
62H —— 取程序段前缀地址	390
65H —— 取扩充的国别信息	390
66H —— 读取/设置全局代码页	392
67H —— 设置句柄计数	393
68H —— 提交文件	393
6CH —— 扩充的打开/建立	394

第八章 设备的输入/输出控制(IOCTL)编程实例

44H —— 设备的输入/输出控制(IOCTL)	397
TrackLayout(磁道布局)字段	408
读/写逻辑设备磁道	409
格式化/验证逻辑驱动器磁道(IOCTL 写)	410
取/设置访问标志状态	410
调用 AL=0EH	411
调用 AL=0FH	411

第三部分 附录:BIOS 扩充 扩展内存中断调用

附录 A IBM ROM BIOS 所提供的服务

INT 05H (5) 打印屏幕	414
INT 10H (16) 视频显示	415
AH=00H (0) 设置视频显示方式	415
AH=01H (1) 设置光标大小	416
AH=02H (2) 设置光标位置	416
AH=03H (3) 读取光标位置	416
AH=04H (4) 读取光笔位置	417
AH=05H (5) 设置工作显示页	417
AH=06H (6) 窗口向上滚动	418
AH=07H (7) 窗口向下滚动	418
AH=08H (8) 读取字符和特性	418

AH=09H (9) 写出字符和特性	419
AH=0AH (10) 写出字符	419
AH=0BH (11) 设置彩色调色板	420
AH=0CH (12) 显示一个像素	420
AH=0DH (13) 读取像素	420
AH=0EH (14) 以 TTY 方式写出字符	421
AH=0FH (15) 获得当前显示方式	421
INT 11H (17) 仪器	422
INT 12H (18) 内存大小	422
INT 13H (19) 磁盘	422
AH=00H (0) 重设磁盘系统	423
AH=01H (1) 取得磁盘状态	423
AH=02H (2) 读取磁盘扇区	423
AH=03H (3) 写入磁盘扇区	424
AH=04H (4) 验证磁盘扇区	425
AH=05H (5) 格式化磁盘磁道	526
INT 14H (24) 通讯	426
AH=00H (0) 设置串行口的起始值	426
AH=01H (1) 送出一个字符	427
AH=02H (2) 接收一个字符	428
AH=03H (3) 获得串行口状态	428
INT 15H (21) 录音机	429
AH=00H (0) 开启录音机马达	429
AH=01H 关闭录音机马达	430
AH=02H (2) 读数据段	430
AH=03H 写数据区段	430
INT 16H (22) 键盘	430
AH=00H (0) 读取下一个键盘字符	431
AH=01H (1) 检查字符是否准备好了	431
AH=02H (2) 获得功能转换状态	431
INT 17H 打印机	432
AH=00H (0) 输出字符到打印机	432
AH=01H (1) 启动打印机	432
AH=02H (2) 取得打印机状态	433
INT 18H (24) BASIC	433
INT 19H (25) 重新启动	434
INT 1AH (26) 时钟	434
AH=00H 读取目前计时器数值	434
AH=01H (1) 设置目前计时器数值	435

附录 B 扩展内存规范参考

B.1 EMS 功能一览表	436
B.2 EMS 错误信息一览表	446
B.2.1 检测 EMS 支持	447
B.2.2 EMS 编程注意点	448

附录 C 扩充内存规范参考

C.1 XMS 功能一览表	450
C.2 XMS 错误码一览表	454
C.2.1 测试 XMS 支持	455
C.2.2 XMS 编程建议	456

附录 D 硬件中断

INT 00H (0) 除以零	457
INT 01H (1) 单步执行	457
INT 02H (2) NMI	458
INT 03H (3) 断点	458
INT 04H (4) 溢出	458
INT 08H (8) 计时器脉冲	458
INT 09H (9) 按下键盘	458
INT 0BH (11) 串行口 1	458
INT 0CH (12) 串行口 0	459
INT 0DH (13) 硬盘驱动器	459
INT 0EH (14) 软盘驱动器	459
INT 0FH (15) 打印机	459
INT 1DH (29) 显示起始表	459
INT 1EH (30) 磁盘驱动器参数表	459
INT 1FH (31) 图形表格	460