****

**THE LINUX PROGRAMMING INTERFACE**

**A Linux and UNIX System Programming Handbook**

**MICHAEL KERRISK**

no starch press

San Francisco

*Translated by: Kevin*

***本资料仅供学习所用，请于下载后24小时内删除，否则引起的任何后果均由您自己承担。本书版权归原作者所有，如果您喜欢本书，请购买正版支持作者。***

目录

[前言 9](#_Toc291097830)

[主题 9](#_Toc291097831)

[目标读者 9](#_Toc291097832)

[Linux和UNIX 10](#_Toc291097833)

[使用和组织 10](#_Toc291097834)

[例子程序 11](#_Toc291097835)

[习题 12](#_Toc291097836)

[标准和可移植性 12](#_Toc291097837)

[Linux内核和C库版本 13](#_Toc291097838)

[其它语言使用编程接口 13](#_Toc291097839)

[关于作者 13](#_Toc291097840)

[致谢 13](#_Toc291097841)

[许可 14](#_Toc291097842)

[网站和例子程序源代码 14](#_Toc291097843)

[反馈 14](#_Toc291097844)

[第1章 历史和标准 15](#_Toc291097845)

[1.1 UNIX和C简史 15](#_Toc291097846)

[1.2 Linux简史 18](#_Toc291097847)

[1.2.1 GNU项目 19](#_Toc291097848)

[1.2.2 Linux内核 20](#_Toc291097849)

[1.3 标准化 25](#_Toc291097850)

[1.3.1 C编程语言 25](#_Toc291097851)

[1.3.2 第一个POSIX标准 26](#_Toc291097852)

[1.3.3 X/Open公司和开放组织 27](#_Toc291097853)

[1.3.4 SUSv3和POSIX.1-2001 28](#_Toc291097854)

[1.3.5 SUSv4和POSIX.1-2008 30](#_Toc291097855)

[1.3.6 UNIX标准时间线 31](#_Toc291097856)

[1.3.7 实现标准 32](#_Toc291097857)

[1.3.8 Linux、标准、和Linux标准基础 33](#_Toc291097858)

[1.4 小结 34](#_Toc291097859)

[第2章 基础概念 36](#_Toc291097860)

[2.1 操作系统的核心：内核 36](#_Toc291097861)

[2.2 Shell 39](#_Toc291097862)

[2.3 用户和组 40](#_Toc291097863)

[2.4 单一目录层次、目录、链接、和文件 41](#_Toc291097864)

[2.5 文件I/O模型 45](#_Toc291097865)

[2.6 程序 46](#_Toc291097866)

[2.7 进程 46](#_Toc291097867)

[2.8 内存映射 50](#_Toc291097868)

[2.9 静态和共享库 51](#_Toc291097869)

[2.10 进程间通信和同步 52](#_Toc291097870)

[2.11 信号 53](#_Toc291097871)

[2.12 线程 54](#_Toc291097872)

[2.13 进程组和shell工作控制 54](#_Toc291097873)

[2.14 会话、控制终端、和控制进程 55](#_Toc291097874)

[2.15 伪终端 56](#_Toc291097875)

[2.16 日期和时间 56](#_Toc291097876)

[2.17 客户端-服务器体系架构 57](#_Toc291097877)

[2.18 实时 58](#_Toc291097878)

[2.19 /proc文件系统 58](#_Toc291097879)

[2.20 小结 59](#_Toc291097880)

[第3章 系统编程概念 60](#_Toc291097881)

[3.1 系统调用 60](#_Toc291097882)

[3.2 库函数 63](#_Toc291097883)

[3.3 标准C库；GNU C库（glibc） 64](#_Toc291097884)

[3.4 系统调用和库函数的错误处理 65](#_Toc291097885)

[3.5 本书示例程序的说明 68](#_Toc291097886)

[3.5.1 命令行选项和参数 68](#_Toc291097887)

[3.5.2 常用函数和头文件 68](#_Toc291097888)

[3.6 可移植问题 79](#_Toc291097889)

[3.6.1 特性测试宏 79](#_Toc291097890)

[3.6.2 系统数据类型 82](#_Toc291097891)

[3.6.3 各种可移植问题 85](#_Toc291097892)

[3.7 小结 87](#_Toc291097893)

[3.8 习题 88](#_Toc291097894)

[第4章 文件I/O：通用I/O模型 89](#_Toc291097895)

[4.1 概述 89](#_Toc291097896)

[4.2 I/O的通用性 92](#_Toc291097897)

[4.3 打开文件：open() 92](#_Toc291097898)

[4.3.1 open()的flags参数 95](#_Toc291097899)

[4.3.2 open()的错误 99](#_Toc291097900)

[4.3.3 creat()系统调用 100](#_Toc291097901)

[4.4 读取文件：read() 101](#_Toc291097902)

[4.5 写入文件：write() 102](#_Toc291097903)

[4.6 关闭文件：close() 103](#_Toc291097904)

[4.7 改变文件偏移：lseek() 103](#_Toc291097905)

[4.8 通用I/O模型之外的操作：ioctl() 109](#_Toc291097906)

[4.9 小结 110](#_Toc291097907)

[4.10 习题 110](#_Toc291097908)

[第5章 文件I/O：更多细节 111](#_Toc291097909)

[5.1 原子性和竞争条件 111](#_Toc291097910)

[5.2 文件控制操作：fcntl() 115](#_Toc291097911)

[5.3 打开文件状态标志 115](#_Toc291097912)

[5.4 文件描述符和打开文件之间的关系 116](#_Toc291097913)

[5.5 复制文件描述符 116](#_Toc291097914)

[5.6 指定偏移位置的文件I/O：pread()和pwrite() 116](#_Toc291097915)

[5.7 Scatter-Gather I/O：readv()和writev() 117](#_Toc291097916)

[5.8 截断文件：truncate()和ftruncate() 117](#_Toc291097917)

[5.9 非阻塞I/O 117](#_Toc291097918)

[5.10 超大文件I/O 117](#_Toc291097919)

[5.11 /dev/fd目录 117](#_Toc291097920)

[5.12 创建临时文件 117](#_Toc291097921)

[5.13 小结 117](#_Toc291097922)

[5.14 习题 117](#_Toc291097923)

[第6章 进程 118](#_Toc291097924)

[第7章 内存分配 119](#_Toc291097925)

[第8章 用户和组 120](#_Toc291097926)

[第9章 进程凭证 121](#_Toc291097927)

[第10章 时间 122](#_Toc291097928)

[第11章 系统限制和选项 123](#_Toc291097929)

[第12章 系统和进程信息 124](#_Toc291097930)

[第13章 文件I/O缓冲 125](#_Toc291097931)

[第14章 文件系统 126](#_Toc291097932)

[第15章 文件属性 127](#_Toc291097933)

[第16章 扩展属性 128](#_Toc291097934)

[第17章 访问控制列表 129](#_Toc291097935)

[第18章 目录和链接 130](#_Toc291097936)

[第19章 监控文件事件 131](#_Toc291097937)

[第20章 信号：基础概念 132](#_Toc291097938)

[第21章 信号：信号处理器 133](#_Toc291097939)

[第22章 信号：高级特性 134](#_Toc291097940)

[第23章 定时器和睡眠 135](#_Toc291097941)

[第24章 进程创建 136](#_Toc291097942)

[第25章 进程结束 137](#_Toc291097943)

[第26章 监控子进程 138](#_Toc291097944)

[第27章 程序执行 139](#_Toc291097945)

[第28章 进程创建和程序执行的更多细节 140](#_Toc291097946)

[第29章 线程：介绍 141](#_Toc291097947)

[第30章 线程：同步 142](#_Toc291097948)

[第31章 线程：线程安全和线程存储 143](#_Toc291097949)

[第32章 线程：线程取消 144](#_Toc291097950)

[第33章 线程：更多细节 145](#_Toc291097951)

[第34章 进程组、会话和任务控制 146](#_Toc291097952)

[第35章 进程优先级和调度 147](#_Toc291097953)

[第36章 进程资源 148](#_Toc291097954)

[第37章 Daemon 149](#_Toc291097955)

[第38章 编写安全的特权程序 150](#_Toc291097956)

[第39章 能力 151](#_Toc291097957)

[第40章 登录会计 152](#_Toc291097958)

[第41章 共享库基础 153](#_Toc291097959)

[第42章 共享库高级特性 154](#_Toc291097960)

[第43章 进程间通信简介 155](#_Toc291097961)

[第44章 管道和FIFO 156](#_Toc291097962)

[第45章 System V IPC介绍 157](#_Toc291097963)

[第46章 System V消息队列 158](#_Toc291097964)

[第47章 System V信号量 159](#_Toc291097965)

[第48章 System V共享内存 160](#_Toc291097966)

[第49章 内存映射 161](#_Toc291097967)

[第50章 虚拟内存操作 162](#_Toc291097968)

[第51章 POSIX IPC介绍 163](#_Toc291097969)

[第52章 POSIX消息队列 164](#_Toc291097970)

[第53章 POSIX信号量 165](#_Toc291097971)

[第54章 POSIX共享内存 166](#_Toc291097972)

[第55章 文件锁 167](#_Toc291097973)

[第56章 Sockets：介绍 168](#_Toc291097974)

[第57章 Sockets：UNIX Domain 169](#_Toc291097975)

[第58章 Sockets：TCP/IP网络基础 170](#_Toc291097976)

[第59章 Sockets：Internet Domain 171](#_Toc291097977)

[第60章 Sockets：服务器设计 172](#_Toc291097978)

[第61章 Sockets：高级主题 173](#_Toc291097979)

[第62章 终端 174](#_Toc291097980)

[第63章 可选I/O模型 175](#_Toc291097981)

[第64章 伪终端 176](#_Toc291097982)

[附录A：跟踪系统调用 177](#_Toc291097983)

[附录B：解析命令行参数 178](#_Toc291097984)

[附录C：转换NULL指针 179](#_Toc291097985)

[附录D：内核配置 180](#_Toc291097986)

[附录E：更多信息来源 181](#_Toc291097987)

[附录F：部分习题解答 182](#_Toc291097988)

[参考书目 183](#_Toc291097989)

[索引 184](#_Toc291097990)

# 前言

## 主题

本书描述Linux编程接口——Linux（UNIX操作系统的一种免费实现）提供的系统调用、库函数、和其它底层接口。这些接口被直接或间接地使用在Linux上运行的每个程序中。它们允许应用程序完成各种任务：如文件I/O、创建删除文件和目录、创建新进程、执行程序、设置定时器、本机进程和线程间通信、通过网络连接的不同机器进程间通信等等。这些底层接口有时候也叫做系统编程接口。

尽管本书关注于Linux，但我也非常注意标准和可移植性问题，清晰地区分了Linux特有的接口、多数UNIX实现共有的特性、以及POSIX和Single UNIX Specification标准定义的特性。因此本书也提供了UNIX/POSIX编程接口的详尽描述，能够适用于编写UNIX系统应用或跨平台应用的程序员。

## 目标读者

本书主要面向以下读者：

* 为Linux、UNIX、或者其它遵循POSIX的系统开发应用的程序员和软件设计师；
* 在Linux、UNIX、或其它操作系统之间移植应用的程序员；
* Linux或UNIX系统编程课程的教师和高年级学生；
* 希望深入理解Linux/UNIX编程接口，以及系统软件是如何实现的系统管理员和“高级用户”。

我假设你拥有一定的编程经验，但不要求系统编程经验。我还假设你了解C编程语言，并且知道如何使用shell和常用的Linux或UNIX命令。如果你是Linux/UNIX的新手，你会发现第2章非常有用，我们以程序员的视角来讲述Linux和UNIX的基础概念。

## Linux和UNIX

本书原本可以纯粹地讲解标准UNIX（也就是POSIX）系统编程，因为UNIX和Linux的大多数特性都是相同的。不过虽然编写可移植程序是很好的目标，理解Linux对标准UNIX编程接口的扩展也是非常重要的。理由之一是Linux非常流行；其二是有时候为了性能、或使用标准UNIX没有的功能，我们不得不使用非标准的扩展（所有UNIX实现都提供类似的非标准扩展）。

因此本书在适用于标准UNIX的程序员时，还提供了Linux特定编程特性的详细描述。这些特性包括：

* epoll，获得文件I/O事件通知的机制；
* inotify，监控文件和目录改变的机制；
* 能力，授予进程一组超级用户能力的机制；
* 扩展属性；
* i-node标志；
* clone()系统调用；
* /proc文件系统
* Linux对文件I/O、信号、定时器、线程、共享库、进程间通信、和socket的特殊实现细节。

## 使用和组织

你至少可以按两种方式来使用本书：

* 作为Linux/UNIX编程接口的介绍手册。你可以从头到尾阅读本书。后续章节建立在之前章节的基础之上，我尽量避免依赖后续章节的情况。
* 作为Linux/UNIX编程接口的索引参考手册。详细的索引和频繁的交叉引用，允许你随机地阅读任何主题。

我把本书分为以下几部分：

1. 背景和概念：UNIX、C和Linux的历史；UNIX标准简介（第1章）；以程序员的视角介绍Linux和UNIX的基本概念（第2章）；Linux和UNIX系统编程的基本概念（第3章）。
2. 系统编程接口的基础特性：文件I/O（第4章和第5章）；进程（第6章）；内存分配（第7章）；用户和组（第8章）；进程凭证（第9章）；定时器（第10章）；系统限制和选项（第11章）；获取系统和进程信息（第12章）。
3. 系统编程接口的高级特性：文件I/O缓冲（第13章）；文件系统（第14章）；文件属性（第15章）；扩展属性（第16章）；访问控制列表（第17章）；目录和链接（第18章）；监控文件事件（第19章）；信号（第20章到第22章）；定时器（第23章）。
4. 进程、程序、和线程：进程创建、进程结束、监控子进程、执行程序（第24章到第28章）；POSIX线程（第29章到第33章）。
5. 进程和程序的高级主题：进程组、会话、任务控制（第34章）；进程优先级和调度（第35章）；进程资源（第36章）；daemon（第37章）；编写安全的特权程序（第38章）；能力（第39章）；登录会计（第40章）；共享库（第41章到第42章）。
6. 进程间通信（IPC）：IPC简介（第43章）；管道和FIFO（第44章）；System V IPC——消息队列、信号量、共享内存（第45章到第48章）；内存映射（第49章）；虚拟内存操作（第50章）；POSIX IPC——消息队列、信号量、共享内存（第51章到第54章）；文件锁（第55章）。
7. Socket和网络编程：IPC和socket网络编程（第56章到第61章）。
8. 高级I/O主题：终端（第62章）；可选I/O模型（第63章）；伪终端（第64章）。

## 例子程序

我用短小但完整的例子程序来阐述多数接口的使用方法，这些例子都被设计为很容易就能从命令行体验，来查看不同的系统调用和库函数如何工作。所以本书包含大量的示例代码——大概15000行C代码和shell会话日志。

尽管阅读和试验例子程序是不错的起点，掌握本书讨论的概念最有效的方法是编写代码，按你的想法修改例子程序，或者编写新程序都可以。

本书的所有源代码都可以在网站上下载。源代码包含许多书中没有的程序。这些程序的目的和细节在注释中都有相关描述。我提供了Makefile编译这些程序，以及一个README文件，给出了例子程序更多的细节信息。

源代码采用GNU Affero 通用公共授权版本3，可以自由分发和修改。源代码中也包含一份该协议的拷贝。

## 习题

多数章节都以一组习题结束，其中一些是要你按不同方式来试验例子程序，另外一些是该章讨论过的概念相关的问题，还有就是要求你来编写代码以巩固你对本书的理解。你可以在附录F找到部分习题的解答。

## 标准和可移植性

贯穿整本书，我都对可移植性问题特别地关注。你会发现很多相关标准的引用，特别是POSIX.1-2001和Single UNIX规范版本3（SUSv3）标准。同时你还将看到这些标准最新修订的细节改变，也就是POSIX.1-2008和SUSv4标准。（由于SUSv3是更大的修订版本，也是本书编写时最广泛有效的UNIX标准，本书讨论的标准大多是SUSv3，并标注出SUSv4不同的地方。除非我明确地提到，你可以假设我们对SUSv3规范的描述也适用于SUSv4）。

对于那些不是标准的特性，我会指出在不同UNIX实现间的差别。我还会突出那些Linux特定的特性，以及Linux与其它UNIX对系统调用和库函数实现上的细小差别。当某个特性我没有明确指出是Linux专有时，你也通常可以假设它在多数或所有UNIX上都有实现。

本书大多数例子程序我都在Solaris、FreeBSD、Mac OS X、Tru64 UNIX、和HP-UX上测试通过（除了那些Linux独有的特性）。为了提高代码在这些系统上的可移植性，本书网站上提供的某些例子程序有一些额外的代码。

## Linux内核和C库版本

本书主要关注Linux 2.6.x系列，这是本书写作时最广泛使用的内核版本。Linux 2.4的某些细节也会提到，我也会指出Linux 2.4和2.6的区别。当Linux 2.6.x系列出现了新特性时（例如2.6.34），我也会特别指出相应的内核版本号。

至于C库，本书则主要关注于GNU C库（glibc）版本2。当然，glibc 2.x系列版本存在差异时，我也会特别指出。

在本书即将印刷时，Linux内核刚刚发布了2.6.35版本，glibc则已经发布2.12版本。本书完全适用于这两个软件版本。Linux内核和glibc将来接口的变化，会在本书的网站上列出。

## 其它语言使用编程接口

尽管例子程序用C语言编写，你也可以在其它编程语言中使用本书讨论的接口——例如编译型语言C++、Pascal、Modula、Ada、FORTRAN、D；解释型语言Perl、Python、Ruby等。（Java则需要采用一种不同的方式JNI）。不同的语言要获取必要的常量定义和函数声明，需要使用不同的技术（C++除外），另外传递函数参数时可能也需要一点额外的工作。此外就没有太大的区别了，核心概念其实都是一样的。因此即使你使用其它的编程语言，你也会发现本书提供的信息是适用的。

## 关于作者

（略）

## 致谢

（略）

## 许可

电子工程学会和开放组织非常友好地许可我引用IEEE Std 1003.1, 2004版本，以及信息技术标准——可移植操作系统接口（POSIX），开放组织基本规范Issue6。完整的标准可以在<http://www.unix.org/version3/online.html>上在线查阅。

## 网站和例子程序源代码

你可以在<http://www.man7.org/tlpi>上找到关于本书更多的信息，包括勘误表和例子程序的源代码。

## 反馈

我非常欢迎代码bug报告、代码改进建议、以及代码可移植性的提高。同样我也欢迎本书的bug报告和改进建议。由于Linux编程接口总是在变化，我也非常高兴能获得关于本书将来版本的改进意见，包括新特性和变化特性。

Michael Timothy Kerrisk

Munich, Germany and Christchurch, New Zealand

August 2010

[mtk@man7.org](mailto:mtk@man7.org)

# 第1章 历史和标准

Linux是UNIX操作系统家族的成员之一。在计算机的术语里，UNIX已经拥有很悠久的历史。第1章的前半部分简述UNIX的历史。我们首先描述UNIX系统和C编程语言的起源，然后讲述导致Linux发展成为今天这个样子的两个关键因素：GNU项目和Linux内核的开发。

UNIX系统最显著的特点之一是它的开发不是被一个厂商或组织控制。相反许多商业和非商业组织都为UNIX的发展做出了贡献。UNIX也因此增加了许多革新的特性，但同时也导致UNIX各个实现之间的分歧越来越大，编写一个能运行于所有UNIX实现的应用也变得非常困难。于是产生了UNIX的标准化运动，我们将在本章后半部分进行讨论。

## 1.1 UNIX和C简史

第一个UNIX由贝尔实验室（电话公司AT&T的一个部门）的Ken Thompson在1969年开发完成（Linus Torvalds也正是在这一年出生）。这个UNIX是用汇编为Digital PDP-7微计算机编写。UNIX这个名字和MULTICS（Multiplexed Information and Computing Service）有关，后者是AT&T与麻省理工学院（MIT）和通用电子之前合作开发的操作系统项目。（由于该项目最初的失败，没有能够开发出一个有用的系统，当时AT&T已经退出项目）。Thompson的新操作系统从MULTICS中借用了一些设计，包括树型结构文件系统、对命令解释执行采用独立的程序（shell）、以及把文件当作无结构的字节流。

在1970年， UNIX使用汇编语言为新的Digital PDP-11微计算机重新编写，这个PDP-11的遗留痕迹至今仍然可以在多数UNIX实现中找到，包括Linux。

不久之后，Dennis Ritchie，Thompson在贝尔实验室的一个同事，设计和实现了C编程语言。这是一个进化的过程，C起源于更早的解释语言B，最初由Thompson实现了B语言，并从一个更早的语言BCPL中借鉴了许多想法。到1973年，C已经成熟到UNIX内核几乎可以全部使用其重写。UNIX也因此成为最早使用高级语言编写的操作系统，使其迁移到其它硬件体系架构成为可能的重要因素。

C语言的这个起源，解释了C和C++成为今天最广泛的系统编程语言的原因。之前广泛使用的语言都是为其它目的而设计的：FORTRAN为工程师和科学家完成数学任务；COBOL为商业系统处理面向记录的数据流。C填补了一个空白，和FORTRAN、COBOL不一样的是，C语言是几个人为了一个目标而设计的：开发一个高级语言来实现UNIX内核和相关的软件。和UNIX操作系统本身一样，C由专业的程序员为自身所设计。所产生的语言是小巧、高效、强大、简洁、模块化、注重实效、和一致的。

UNIX第一至第六版

在1969年到1979年间，UNIX发布了一系列版本。本质上就是AT&T对UNIX开发进展的一个快照。UNIX最初的六个版本发布时间如下：

* 第一版，1971年11月：此时UNIX还运行在PDP-11上，已经拥有一个FORTRAN编译器，和许多今天依然在使用的工具，包括ar, cat, chmod, chown, cp, dc, ed, find, ln, ls, mail, mkdir, mv, rm, sh, su, who。
* 第二版，1972年6月：UNIX安装在AT&T内部的10台机器上。
* 第三版，1973年2月：这个版本包含一个C编译器和管道的最初实现。
* 第四版，1973年11月：第一个几乎全部用C编写的版本。
* 第五版，1974年6月：此时UNIX已经安装在超过50个系统中。
* 第六版，1975年5月：这是第一个在AT&T范围外广泛使用的版本。

在这些版本发布的过程中，UNIX的使用和声望得到了扩展，首先在AT&T内部，随后在外部。Communications of the ACM杂志发表的一篇关于UNIX的论文也为此做出了巨大贡献。

当时AT&T正在接受美国电话系统对其垄断的政府制裁。AT&T与美国政府的协议禁止其销售软件，这也意味着AT&T不能把UNIX作为产品销售。相反，从1974年的第五版开始，特别是第六版，AT&T授权大学免费使用UNIX。针对大学的UNIX发布版包含文档和内核源代码（当时大约10000行）。

AT&T对大学发布UNIX极大地促进了UNIX的使用和流行，到1977年UNIX已经运行在500个地方，包括125所美国大学和其它一些国家。当时的商业操作系统非常昂贵，而UNIX为大学提供了一个交互式多用户的操作系统，即便宜又强大。同时UNIX还给大学计算机科学研究提供UNIX操作系统的源代码，他们可以修改并提供给学生学习和体验。很多学生学习了UNIX之后，就成为了UNIX的布道者。其它则加入或组建自己的公司，销售运行着UNIX操作系统的计算机工作站。

**BSD和System V的诞生**

1979年1月UNIX发布了第七版，改进了系统的可靠性，提供了一个增强的文件系统。这个发布版还包含一些新的工具，包括：awk, make, sed, tar, uucp, Bourne shell, 和FORTRAN 77编译器。第七版的发布对于UNIX来说具有重要意义，因为从这一刻起，UNIX产生了两个重要的变种：BSD和System V，它们的起源我们马上就会简要地描述。

Thompson在1975/1976学年回到自己的母校，加州大学伯克利分校担任客座教授。在那里他和几个毕业生为UNIX增加了许多新特性。（其中一个学生Bill Joy，随后与别人一起组建了Sun Microsystems，成为UNIX工作站市场早期参与者）。Berkeley开发了许多新的工具和特性，包括C shell、vi编辑器、改进的文件系统（Berkeley Fast File System）、sendmail、Pascal编译器、新的Digital VAX体系架构下的虚拟内存管理等。

在Berkeley Software Distribution（BSD）的授权许可下，这个版本的UNIX，包括它的源代码，被广泛地发布出去。1979年发布了第一个完整发行版3BSD（更早的Berkeley-BSD和2BSD，只是增加Berkeley开发的新工具，而不是完整的UNIX发行版）。

到1983，加州大学伯克利的计算机系统研究组织（Computer Systems Research Group）发布了4.2BSD。这是一个重大的发行版，因为它包含了完整的TCP/IP实现，包括socket应用编程接口（API）和许多网络工具。4.2BSD和它的前任4.1BSD被广泛发布于全世界的许多大学。它们也构成了Sun公司的UNIX变种，SunOS（1983首次发布）的基础。其它重要的BSD发布包括1986年的4.3BSD，以及1993年的最终发布版：4.4BSD。

与此同时，US反托拉斯诉讼强制AT&T解散（法律诉讼起于1970年代中期，1982年解散生效），由于在电话系统中不再垄断，公司被允许运营UNIX。结果就是1981年System III的诞生。AT&T的UNIX支持组（USG）负责开发System III，它雇佣了数百名开发者来增强UNIX，和开发UNIX应用（著名的有document preparation package和软件开发工具）。随后在1983年发布了System V(5)的第一个版本，一系列的小发布版后最终是1989年的System V发布版4（SVR4），到这时System V已经吸收了BSD的许多特性，包括网络基础设施。System V授权给许多商业厂商，这些厂商使用System V作为自己UNIX实现的基础。

因此到1980年代末，除了各种BSD发布版在大学广泛使用，UNIX还在许多硬件上拥有各种商业实现：包括Sun的SunOS及随后的Solaris、Digital的Ultrix和OSF/1（经过一系列的改名和收购之后，成为了今天的HP Tru64 UNIX）、IBM的AIX、Hewlett-Packard（HP）的HP-UX、NeXT的NeXTStep、Apple Macintosh的A/UX、Microsoft和SCO为Intel x86-32体系架构开发的XENIX。（本书将Linux的x86-32实现统一称为Linux/x86-32）。这种状况和当时典型的私有硬件/操作系统的方式完全不同，后者通常是厂商只生产一个或少数私有计算机芯片体系架构，然后在上面销售自己的私有操作系统。多数厂商系统的这种私有属性，意味着购买受限于一个厂商。切换到另一种私有操作系统和硬件平台会非常昂贵，因为需要迁移现有应用并进行相关的重新训练。这个因素再加上各个厂商便宜的单用户UNIX工作站，使得可移植的UNIX系统对商业应用非常具有吸引力。

## 1.2 Linux简史

Linux这个术语通常引用基于Linux内核的完整的类UNIX操作系统。不过这是错误的叫法，因为典型商业Linux发行版的许多关键组件，都起源于另一个项目，这个项目比Linux要早好几年。

### 1.2.1 GNU项目

Richard Stallman是一个天才程序员，曾工作于MIT，他在1984年开始考虑实现一个"Free" UNIX。Stallman对"free"的观点是精神上的自由，并且定义在法律层面上，而不仅仅是免费（参考<http://www.gnu.org/philosophy/free-sw.html>）。无论如何，Stallman倡导的自由也就意味着软件（如操作系统）应该免费或非常便宜。

Stallman大大影响了厂商对私有操作系统系统附加的限制。这些限制意味着购买计算机软件通常不包含源代码，而且通常不能对该软件进行复制、修改、和分发。Stallman指出这种形式鼓励程序员互相竞争并且保密自己的工作，而不是互相合作和共享成果。

于是Stallman创建了GNU项目（GNU's not UNIX），目标是开发一个完整、自由、类UNIX的系统，包含一个内核和所有相关的软件包，并且鼓励其它人参与该项目。到1985年，Stallman成立了自由软件基金会（FSF），这是一个旨在支持GNU项目以及其它自由软件开发的非赢利组织。

GNU项目的一个重要成果就是GNU General Public License(GPL)的产生，这也是Stallman对自由软件精神的具体化。Linux发行版的多数软件，包括内核都按GPL（或者类似的许可）授权。GPL授权的软件必须使源代码自由可用，而且允许按GPL许可自由地重新发布。GPL授权的软件允许自由地修改，但是修改后的软件必须同样遵循GPL许可。如果修改后的软件以可执行方式发布，作者必须同时允许以不超过发布的代价获得修改过的源代码。GPL第一版发布于1989年，目前的版本3发布于2007年。版本2发布于1991年，目前使用最广泛，也是Linux内核采用的授权。

GNU项目最初并没有开发出一个可用的UNIX内核，但确实创建了许多其它程序。由于这些程序设计成在类UNIX操作系统中运行，它们可以也确实被用在现有的UNIX实现中，有些还迁移到其它操作系统。GNU项目最著名的程序有Emacs文本编辑器、GCC（最早是GNU C编译器，不过现在重新命名为GNU编译器集合，包含C、C++和其它语言的编译器）、Bash shell、和glibc（GNU C库）。

在1990年代初期，GNU项目已经拥有了一个几乎完整的系统，除了一个关键的组成：可用的UNIX内核。GNU项目开始规划一个野心勃勃的内核设计，被称为GNU/HURD，基于Mach微内核。不过HURD远远达不到可发布的程度。（在本书写作之时，HURD的工作仍在继续，目前只能运行在x86-32体系架构下）。

万事俱备，只欠东风。GNU项目已经创建了完整UNIX系统所需的一切，只差一个最重要的内核了。

### 1.2.2 Linux内核

Linus Torvalds在1991年还是芬兰郝尔辛基大学的一名学生，当时他想为自己的Intel 80386 PC编写一个操作系统。在Linus的课程学习过程中，他接触了Minix，由Andrew Tanenbaum在1985年左右开发的类UNIX操作系统内核，后者是荷兰某大学的教授。Tanenbaum创造了Minix，并提供完整的源代码，用作大学操作系统设计课程的教学工具使用。Minix内核可以在386系统中构建和运行，但是由于主要目的是教学工具，Minix设计成很大程度上独立于硬件体系架构，因此不能完全发挥386处理器的能力。

于是Torvalds启动了自己的项目，开始为386创建一个高效、全功能的UNIX内核。几个月之后，Torvalds开发了一个基本的内核，允许自己编译和运行许多GNU程序。然后在1991年10月5日，Trovalds开始在网上请求其它程序员的帮助，发出了下面这段被广泛引用的声明，他在comp.os.minix Usenet新闻组上发布了自己内核的0.02版：

你是否怀念 minix-1.1 版时的日子？那时人们干劲十足，自己编写设备驱动程序。你是否手头正缺少一个很好的项目，并且非常渴望为符合自己的需要动手修改一个操作系统？当几乎所有的程序都能在Minix上运行时，你是否感到非常失望？不再有为了调通一个巧妙的程序而整夜不睡觉的夜猫子？那么本消息（邮件、公告）可能正是为你而发布的:-)。

正如我一个月前所提到的，我正在开发一个用于 AT-386 微机类似于Minix 的操作系统。它目前已经达到了可用的程度(当然，能不能用还依赖于你的具体要求)，而且我很高兴把源代码拿出来广泛发布。目前它的版本是0.02(加上已经编制好的(很小的)补丁程序，就是0.03)，但是我已经在它上面成功地运行了 bash/gcc/gnu-make/gnu-sed/压缩程序等。

该小巧项目的源程序可以在nic.funet.fi(128.214.6.100)上/pub/OS/Linux 目录中找到。该目录中含有一些README文件以及几个在Linux下运行的二进制执行程序(bash, update和gcc，你还能要求什么呢:-)。提供了完整的内核源代码，而且没有使用minix的代码。库文件的源代码仅是部分免费的，所以目前不能给出。照内核现在的样子，系统已经可以进行编译，并且已经可以运行。二进制执行程序（bash和gcc）的源代码可以在同一个地方的/pub/gnu目录中找到。

当心！警告！注意！这些源代码仍然需要minix-386系统来进行编译（需要 gcc-1.40，1.37.1可能也能用，但没有试过），并且如果你想运行它的话还需要minix来进行设置，所以对没有minix的人来说，它至今它还不是一个独立的系统，不过我正在朝这方面努力着。你还需要有些骇客的本事来设置它，所以对那些希望一个minix-386取代品的人来说，就不用考虑Linux了。它目前主要是供对操作系统感兴趣的骇客使用的，并且有能使用minix的386机器。该系统需要一个AT兼容硬盘（IDE硬盘当然更好）以及EGA/VGA显示卡，如果你还感兴趣的话，就使用ftp下载README/RELNOTES文件看看，并且/或者给我EMAIL告之其它信息。

我能够（当然，几乎是）听到你问自己“为什么？”，Hurd将在近年（或者两年、或者下个月，谁知道）内推出，而且我已经有了minix。这是一个骇客为骇客们写的程序，在开发过程中我已经得到了快乐，而某些人可能也乐意阅读它，甚至为自己的需要而修改它。它仍然很小，足以理解、使用和修改，我正期望你可能有的任何建议和说明。 我也对为minix系统编写过工具软件/库函数的任何人的反馈信息感兴趣。如果你的软件是可以自由发布的(在版权下甚至公共域内)，那么我很希望得到你们的消息，这样我就可以将它们加入到Linux系统中。现在我正使用着Earl Chews的stdio（Earl，谢谢你的很好而又能使用的系统），很欢迎这种类似的软件。你的版权当然会保留着，如果你乐意我使用你的代码，就请告知。

Linus

按照传统UNIX克隆采用的X字母结尾命名惯例，这个内核最终命名为Linux。最初Linux采用更加受限制的授权，不过Torvalds很快就将Linux许可更换为GNU GPL协议。

Linus的请求帮助得到热烈影响。很多程序员加入Linux的开发，添加了许多特性，例如增强的文件系统、网络支持、设备驱动、和多处理器支持等。到1994年3月，开发者们发布了1.0版本，1995年3月发布了Linux 1.2，1996年6月发布了Linux 2.0，1999年1月发布了Linux 2.2，2001年1月发布了Linux 2.4。2001年11月开始内核2.5的开发，到2003年12月发布了Linux 2.6。

**BSD**

值得一提的是1990年代前期，另一个免费的UNIX也已经能够用于x86-32体系架构。Bill和Lynne Jolitz对一个已经很成熟的BSD系统向x86-32做了迁移，名叫386/BSD。迁移基于BSD Net/2发布版（1991年6月），是4.3BSD的一个版本，把所有AT&T私有的源代码都替换或移除掉。Jolitz夫妇把Net/2迁移到x86-32，并重写了缺失的代码，在1992年2月发布了386/BSD的第一个版本（V0.0）。

在经历了最初短暂的成功和流行之后，386/BSD的工作由于各种原因而停滞。随着大量patch逐渐积压得不到处理，两个开发团队应运而生，分别创建了自己基于386/BSD的发布版：NetBSD，强调在各种硬件之间保持可移植性；FreeBSD，强调性能，也是现代BSD中最流行的一个。NetBSD的第一个发布版是1993年4月的0.8；FreeBSD的首张CD-ROM（版本1.0）发布于1993年12月。另外还有一个OpenBSD，派生自NetBSD项目，在1996年发布了最初的2.0版本，OpenBSD特别强调安全性。到2003年中期，一个新的DragonFly BSD又从FreeBSD 4.x分离而出。DragonFly BSD采用了不同于FreeBSD 5.x的方式，特别为对称多处理器（SMP）体系架构设计。

如果不提到UNIX系统实验室（USL，负责开发和销售UNIX的AT&T子公司）和伯克利之间的诉讼，那我们对于BSD的讨论就不是完整的。在1992年初，合并成立了伯克利软件设计公司（BSDi，今天是Wind River的一部分），开始发布一个商业支持的BSD UNIX：BSD/OS，基于Net/2发行版和Jolitz夫妇的386/BSD增强功能。BSDi以995美元发布二进制和源代码，并且建议潜在客户使用他们的电话号码1-800-ITS-UNIX。

1992年4月，USL向BSDi正式提出诉讼，试图阻止BSDi销售包含USL私有源代码和商业秘密的产品。USL同时还要求BSDi停止使用迷惑性的电话号码。这个官司最终扩大为要求加州大学赔偿。法院最后判决同意了USL的两个主张，并驳回了其它请求。接着马上加州大学向USL提出反诉讼，声称USL未经许可在System V中使用了BSD代码。

官司正在悬而未决的时候，Novell收购了USL，其CEO（Ray Noorda）开始公开声明自己希望双方在市场上而不是法院里竞争。诉讼最终得以在1994年1月终结，加州大学必须移除Net/2发布版18000个文件中的3个，并对其它少数文件做一些很小的修改，另外还要对大约70个文件增加USL版本声明，而且这些文件不能够再次发布。这个修改后的系统在1994年6月发布为4.4BSD-Lite（加州大学发布的最后一个版本是1995年6月的4.4BSD-Lite版本2）。从这时开始，法律条款要求BSDi、FreeBSD、NetBSD用修改后的4.4BSD-Lite源代码替换Net/2。尽管这导致BSD派生开发的一定延迟，但也使这些系统通过三年的开发，从加州大学计算机系统研究组织发布Net/2后重新同步到一起。

**Linux内核版本号**

和多数自由软件项目一样，Linux采用尽早发布、经常发布的模型，因此新的内核修订频繁更新（有时候几乎每天）。随着Linux用户群的增长，对发布模型进行了一定的修改，以减少对现有用户的影响。具体来说，从Linux 1.0发布之后，内核开发者就采用了固定的内核版本命名规范，每个发布版本统一命名为x.y.z：其中x表示主版本号；y表示在该主版本号下的副版本号；而z则是副版本号下的修订版本号（通常是很小的改进和bug修复）。

在这样一种模型下，通常会有两个内核版本总是处在开发过程中：一个是稳定版，用于生产系统，其主版本号为偶数；另一个是开发版，相对来说不稳定一些，主版本号一般是下一个奇数。理论上（实践中并不总是）所有新特性都只应该添加在当前开发版内核中，而稳定版的修订系列严格限制为很小的改进和bug修复。当内核开发者认为开发版本适合发布时，就会成为新的稳定版，并赋予一个偶数版本号。例如2.3.z开发内核最终形成了2.4稳定内核版本。

2.6内核发布之后，开发模型发生了变化，主要目的是解决稳定版内核发布时间间隔太长导致的问题和挫折（Linux 2.4.0和2.6.0之间差不多有三年时间）。关于改善开发模型的谈论时不时都有进行，但是核心细节基本保持如下：

* 不再有稳定和开发版的明确区分。每个新的2.6.z发布都可以包含新特性，而且都经历增加新特性，然后通过几个候选发布版达到稳定的生命周期。当候选版本足够稳定时，就发布为内核2.6.z版本。发布周期大约三个月。
* 有时候稳定的2.6.z发布版需要小的patch来修复bug或安全性问题。如果这些修复有足够高的优先级，而且这些patch也足够简单到不可能出错，那么不需要等待下一个2.6.z发布版，可以直接创建一个2.6.z.r发布版，这里的r序列号表示2.6.z内核的副修订版本。
* 额外的责任被转移到发行版厂商，来确保发行版内核的稳定性。

后面章节有时候遇到特殊的API时，会提及具体的内核版本（例如新的或修改的系统调用）。不过在2.6.z系列内核之前，多数内核变更都发生在奇数开发版中，我们通常会注明这个变化是在下一个稳定版中产生的，因为多数应用开发者都是使用稳定版内核而不是开发版内核。许多情况下，手册页则会精确地标注某个特性是在哪个开发版出现或修改的。

对于2.6.z系列内核出现的变化，我们会标注具体的内核版本号。当我们说某个特性是内核2.6的新特性时，如果不带z修订号，就表示这个特性是在2.5开发内核中实现的，首次出现在稳定内核版本2.6.0。

**移植到其它硬件体系架构**

在Linux最初的开发阶段，高效地实现Intel 80386是主要目标，而不是与其它处理器体系架构的可移植性。但是随着Linux越来越流行，开始向其它处理器体系架构进行移植，最开始是Digital Alpha芯片。Linux能够支持的硬件体系架构非常多，而且还在不断增长。包括但不限于：x86-64、Motorola/IBM PowerPC和PowerPC64、Sun SPARC和SPARC64（UltraSPARC）、MIPS、ARM（Acorn）、IBM z系列（以前的System/390）、Intel IA-64（Itanium）、Hitachi SuperH、HP PA-RISC、和Motorola 68000。

**Linux发行版**

准确地说，Linux这个术语只是指Linus Torvalds和其它开发者开发的内核。但是通常我们说的Linux则包括内核，加上大量其它软件（工具和库），它们一起组成了完整的操作系统。在Linux最早期的时代，用户需要自己组合所有这些软件，创建文件系统，正确地存放和配置文件系统中的所有软件。这需要大量时间和专业知识。结果就是Linux发行版市场的兴起，发行版自动化处理大多数安装过程，创建文件系统并安装内核和其它必需的软件。

最早的发行版出现于1992年，包含了MCC Interim Linux（Manchester Computing Centre，UK）、TAMU（Texas A&M 大学）、和SLS（SoftLanding Linux系统）。现存最老的商业发行版是1993年出现的Slackware；非商业的Debian发行版大约也在那时候出现，随后是SUSE和红帽。当前非常流行的Ubuntu发行版于2004年发布。今天许多发行版公司都雇佣了大量程序员，继续为自由软件项目做出贡献，或者发起新的项目。

## 1.3 标准化

1980年代后期，众多的UNIX实现也带来一个问题。某些UNIX实现基于BSD，其它则基于System V，某些特性则同时来自这两个变种。此外每个商业厂商都为自己的UNIX实现增加了额外的特性。结果就是从一个UNIX实现向另一个移植软件变得非常困难。这种状况为C编程语言和UNIX系统的标准化施加了积极的压力，标准化可以使应用在平台间移植就得非常简单。我们来看一看相关的标准。

### 1.3.1 C编程语言

在1980年代早期，C已经存在了10年之久，而且在多数UNIX系统和其它操作系统中都已经被实现。各种不同实现之间存在许多细小的差别，部分原因是C语言某些方面如何工作，并没有在事实上的标准中（Kernighan和Ritchie在1978年出版的C编程语言一书）详细描述（书中老式的C语法有时候也称为传统C或者K&R C）。此外，1985年产生的C++突出了C语言中缺乏的某些不影响兼容性的改进或增强，比如函数原型、结构体赋值、类型限定符（const和volatile）、枚举类型、和void关键字。

这些因素驱动了C语言的标准化，最终在1989年通过了美国国家标准协会（ANSI）的C标准（X3.159-1989），随后又在1990年被采纳为国际标准组织（ISO）标准（ISO/IEC 9899:1990）。除了定义C语言的语法和语义，该标准还描述了标准C库，包括stdio函数、字符串处理函数、数学函数、各种头文件等等。这个版本的C被称为C89或ISO C90，Kernighan和Ritchie的C编程语言第二版（1988）对标准做了完整描述。

ISO在1999年接受了C标准的新修订（ISO/IEC 9899:1999；参考<http://www.open-std.org/jtc1/sc22/wg14/www/standards>）。这个标准通常称为C99，对C语言和标准库做了一定的修改。包括增加long long和bool数据类型、C++风格注释（//）、受限指针、以及变量长度数组。（在本书写作的时候，还在对C标准进行进一步的修订，非正式地命名为C1X。新标准有望在2011年获得批准）。

C标准与操作系统实现完全无关；也就是说并没有绑定于UNIX系统。这表示使用纯标准库编写的C程序应该可以在任何计算机和操作系统之间移植。

### 1.3.2 第一个POSIX标准

POSIX术语（可移植操作系统接口）表示了一组标准，由电子电气工程协会（IEEE）组织开发，特别是其下属的可移植应用标准委员会（PASC，<http://www.pasc.org/>）。PASC标准的目标是在源代码层面上提高应用的可移植性。

POSIX标准对于我们来说关系最紧密的是第一个POSIX标准，称为POSIX.1（或者全称POSIX 1003.1），以及随后的POSIX.2标准。

**POSIX.1和POSIX.2**

POSIX.1在1988年成为IEEE标准，然后在1990年经过很小的修订，被采纳为ISO标准（ISO/IEC 9945-1:1990）。（原始的POSIX标准没有在线提供，但可以在IEEE的网站<http://www.ieee.org/>上购买）。

POSIX.1定义API提供明确的服务，而且遵循该标准的操作系统必须提供该API。这样的操作系统才可以获得POSIX.1依从的证明。

POSIX.1基于UNIX系统调用和C库函数API，但是并没有要求特定实现一定要与这个接口绑定。这意味着这些接口可以被任何操作系统实现，不必非得是UNIX操作系统。实际上有些厂商已经增加了API到自己私有的操作系统中，获得了依从POSIX.1的证明，同时又大体上保持底层操作系统不变。

原始POSIX.1标准的很多扩展也很重要。1993年通过的IEEE POSIX 1003.1b（POSIX.1b，正式名称是POSIX.4或者POSIX 1003.4），包含了对基础POSIX标准的许多实时扩展。1995年通过的IEEE POSIX 1003.1c（POSIX.1c），定义了POSIX线程。1996年通过了POSIX.1标准的修订版（ISO/IEC 9945-1:1996），核心内容保持不变，但整合了实时与线程扩展。IEEE POSIX 1003.1g（POSIX.1g）定义了网络API，包括socket；1999年通过的IEEE POSIX 1003.1d（POSIX.1d）和2000年通过的POSIX.1j，定义了额外的实时扩展。

另外一个相关的标准，POSIX.2（1992，ISO/IEC 9945-2:1993）标准化了shell和许多UNIX实用工具，包括C编译器的命令行接口。

**FIPS 151-1和FIPS 151-2**

FIPS是联邦信息处理标准的简称，是US政府为采购计算机系统而制定的一组标准。1989年公布了FIPS 151-1。这个标准基于1988年的IEEE POSIX.1标准和ANSI C标准草案。FIPS 151-1和POSIX.1（1988）的主要区别是FIPS标准强制要求某些POSIX.1指定可选的特性。因为US政府是主要的计算机系统采购商，多数计算机厂商都确保自己的UNIX系统遵循FIPS 151-1版本的POSIX.1标准。

FIPS 151-2对应于1990年POSIX.1的ISO版本，其它则保持不变。现在已经过时的FIPS 151-2在2000年2月取消标准。

### 1.3.3 X/Open公司和开放组织

X/Open公司是国际计算机厂商组成的集团，采纳或改编现有标准来产生综合的开放系统标准。它创建了X/Open可移植指南，基于POSIX标准的一系列可移植指南。这个指南的首个重要发布版是1989年的Issue 3（XPG3），随后1992年发布了XPG4，并在1994年重新修订，生成了XPG4的版本2，这个标准同时整合了AT&T System V接口定义Issue 3的重要部分，我们在1.3.7节会再加描述。这个修订版本也被称为Spec 1170，其中1170指的是标准定义的接口数量（函数、头文件、和命令）。

当Novell在1993年初获得了AT&T的UNIX系统业务后（后来又自己丢失了这块业务），把UNIX商标的权利转移给了X/Open（转移的计划发布于1993年，但法律要求延迟到1994初才完成）。XPG4版本2也因此重新包装为Single UNIX Specification（SUS或SUSv1），有时候也叫UNIX 95。包括XPG4版本2、X/Open Curses Issue 4版本2规范、和X/Open网络服务（XNS）Issue 4规范。Single UNIX规范的版本2（SUSv2，<http://www.unix.org/version2/online.html>）发布于1997年，实现并通过验证这个规范就可以称为UNIX 98。（这个标准有时候也被称为XPG5）。

到1996年，X/Open与开放软件基金会合并组成了开放组织。几乎所有与UNIX系统有关联的公司或组织现在都是开放组织的成员，继续开发API标准。

### 1.3.4 SUSv3和POSIX.1-2001

从1999年开始，IEEE、开放组织、和ISO/IEC Joint技术委员会就Austin公共标准修订组织（CSRG，<http://www.opengroup.org/austin/>）进行合作，目标是修订和巩固POSIX标准和Single UNIX规范。（Austin组织由于1998年9月在德克萨斯洲的奥斯丁举行开幕式而得名）。结果在2001年12月批准了POSIX 1003.1-2001，有时候直接称为POSIX.1-2001（随后被采纳为ISO标准ISO/IEC 9945:2002）。

POSIX 1003.1-2001替代了SUSv2、POSIX.1、POSIX.2、和其它早期POSIX标准草案。这个标准也被称为Single UNIX规范版本3，本书后面通常使用SUSv3来引用它。

SUSv3基本规范大概有3700页，分成以下四个部分：

* 基本定义（XBD）：这部分包含定义、术语、概念、和头文件内容规范。一共提供了84个头文件规范。
* 系统接口（XSH）：这部分的开头描述了许多有用的背景信息。中间大部分内容包含许多函数的规范（实现为系统调用或库函数）。这部分总共包含了1123个系统接口）。
* Shell和实用工具（XCU）：这部分规范了shell的操作和许多UNIX命令。总共规定了160个实用工具。
* Rationale（XRAT）：这部分包含与前面几个部分相关联的文本信息和阐述。

此外SUSv3还包含X/Open CURSES Issue 4版本2（XCURSES）规范，规定了curses屏幕处理API相关的372个函数和3个头文件。

SUSv3总共规定了1742个接口。相比较POSIX.1-1990（包含FIPS 151-2）才规定了199个接口，而POSIX.2-1992则规定了130个实用工具。

SUSv3可以在<http://www.unix.org/version3/online.html>上找到。实现并通过SUSv3验证的系统则称为UNIX 03。

原始的SUSv3批准之后，经过了一些小的变化和改进。结果就是Technical Corrigendum Number 1的出现，这些改进最后在2003年被整合到SUSv3修订版，而Technical Corrigendum Number 2的改进则被整合到2004修订版。

**POSIX依从、XSI依从、和XSI扩展**

历史上SUS（和XPG）标准与相应的POSIX标准存在差异，并组织为POSIX的功能超集。除了规定额外的接口，SUS标准还强制要求实现许多POSIX可选的接口和行为。

这种差异在POSIX 1003.1-2001中更为微妙，它同时是IEEE和开放组织技术标准（也是早期POSIX和SUS标准的合并）。这个文档定义了两个级别的依从：

* POSIX依从：定义了依从实现必须提供的接口基准。允许实现提供其它可选接口。
* X/Open系统接口（XSI）依从：要依从于XSI，实现必须符合所有POSIX依从的要求，同时还必须提供许多POSIX可选的接口和行为。实现必须达到这个级别的依从，才能从开放组织获得UNIX 03商标。

XSI依从要求的额外接口和行为合称为XSI扩展。它要求支持的特性包括：线程、mmap()和munmap()、dlopen API、资源限制、伪终端、System V IPC、syslog API、poll()、和登录会计。

在后面章节中，当我们说SUSv3依从时，指的是XSI依从。

**未规定和软规定**

有时候我们会谈到某个接口在SUSv3中“未规定”或“软规定”

对于未规定的接口，意思是虽然可能在背景注解或rationale文本中提到过，但在正式标准中根本没有定义。

对于软规定的接口，则指的是虽然接口包含在标准中，但其重要细节未明确规定（通常是由于委员会成员因现有实现的差异而无法达成一致）。

当使用未规定或软规定的接口时，我们很难保证能够迁移到其它UNIX实现。无论如何，少数情况下这种接口在不同实现间还是比较一致的，这时我们会明确地标注这一点。

**遗留特性**

有时候我们会提到SUSv3标记某个特性是遗留的。这个术语表示这个特性只是为了兼容老的应用而保留，应该避免在新应用中使用。在许多情况下，都有其它API提供等价的功能。

### 1.3.5 SUSv4和POSIX.1-2008

2008年Austin组织完成了POSIX.1和Single UNIX规范的修订。和之前版本的标准一样，它也包含基本规范和XSI扩展。我们把这个修订版称为SUSv4。

SUSv4的变化比SUSv3要少很多。最重要的改变如下：

* SUSv4为一些函数增加了新的规范。在本书中涉及的新规范函数包括：dirfd(), fdopendir(), fexecve(), futimens(), mkdtemp(), psignal(), strsignal(), utimensat()。其它一些文件相关的函数（例如18.11节描述的openat()）是现有函数（如open()）的类似物，区别是它们根据文件描述符来解释相对路径，而不是根据进程的当前工作目录来解释相对路径。
* 有些SUSv3规定为可选的函数在SUSv4中成为强制要求。例如SUSv3中的很多XSI扩展函数现在成为SUSv4的基本标准。这些函数包括dlopen API（42.1节），实时信号API（22.8节），POSIX信号量API（第53章），和POSIX定时器API（23.6节）。
* SUSv3的某些函数被标记为过时。包括asctime(), ctime(), ftw(), gettimeofday(), getitimer(), setitimer(), siginterrupt()。
* 某些SUSv3标记为过时的函数从SUSv4中移除。包括gethostbyname(), gethostbyaddr(), vfork()。
* SUSv3规范的一些细节在SUSv4中进行了修改。例如许多函数被添加到异步信号安全函数列表（表21-1）。

在本书的后面部分，我们会在相关主题被讨论时标注SUSv4的变化。

### 1.3.6 UNIX标准时间线

图1-1总结了前面章节描述的各种标准之间的关系，并按年代顺序排列了所有标准。在这个图中，实线表示标准之间直接继承；而虚线表示某个标准影响了另一个标准，并被整合到另一个标准中，或者推迟为其它标准。

网络标准的情况比较复杂，网络的标准化开始于1980年代末，由POSIX 1003.12委员会标准化socket API、X/Open传输接口（XTI）API（基于System V传输层接口的另一个网络编程API）、以及许多相关的API。这个标准酝酿了很多年，也就是POSIX 1003.12重命名为POSIX 1003.1G期间。最终批准于2000年。

在开发POSIX 1003.1g的同时，X/Open也在开发自己的X/Open网络规范（XNS）。该规范的首个版本XNS Issue 4是首个Single UNIX规范的一部分。后面还有XNS Issue 5，属于SUSv2的一部分。XNS Issue 5和当前的POSIX.1g（6.6）草案本质上是一样的。再后面是XNS Issue 5.2，与XNS Issue 5和POSIX.1g草案不一样的地方是标记XTI API为过时的，并包含了因特网协议版本6（IPv6），后者大约在1990年代中期设计。XNS Issue 5.2组成了SUSv3网络部分的基础，现在已经被废弃。相同的原因，POSIX.1g也很快被废除标准资格。



*图1-1：各种UNIX和C标准之间的关系*

### 1.3.7 实现标准

除了上面独立或多方组织产生的标准，有时候我们会提到两个实现标准，由最终的BSD发布版（4.4BSD）和AT&T System V发布版4（SVR4）定义。后一个实现标准由AT&T的System V接口定义（SVID）出版而正式化。1989年AT&T出版了SVID Issue 3，定义了UNIX实现要通过System V版本4验证，必须提供的接口。（SVID可以在<http://www.sco.com/developers/devspecs/>上在线查看）。

### 1.3.8 Linux、标准、和Linux标准基础

Linux（内核、glibc、和工具）开发致力于遵循各种UNIX标准，特别是POSIX和Single UNIX规范。但是在本书写作时，还没有哪个Linux发行版获得开放组织的“UNIX”标志。主要的问题是时间和代价。每个厂商的发行版都需要经历依从测试来获得这个认证，而且每个发行版的新版本也需要重新测试。无论如何，Linux能够在UNIX市场上如此成功，得益于Linux对各种标准事实上的接近依从。

对于多数商业UNIX实现来说，相同的公司开发和发行操作系统。而Linux则不同，各个发行版的实现是分开的，而且由多个组织（包括商业和非商业）处理Linux发行版。

Linus Torvalds并没有为某个特定的Linux发行版单独贡献，也没有认可某个Linux发行版。再加上其它个体也在负责Linux的开发，情况就更加复杂了。许多Linux内核和其它自由软件项目的开发者，都受雇于不同的Linux发行版公司，或者工作于对Linux非常感兴趣的公司（如IBM和HP）。这些公司都能够影响Linux的发展方向，但又无法控制Linux的发展。当然Linux内核和GNU项目也有许多贡献者是自愿工作的。

由于存在多个Linux发行版，而且内核实现并不能控制发行版的内容，因此没有“标准”的商业Linux这回事。每个Linux发行商的内核通常都基于内核主版本的某个快照，并应用许多patch而形成。

这些patch一般或多或少都是由于商业需求而提供，目的是提高市场竞争力。有些情况下这些patch后来也被内核采纳。实际上有些新内核特性最初就是由发行公司开发，在成为内核主版本的一部分之前，已经先出现在他们的发行版中。例如Reiserfs日志文件系统版本3先是某些Linux发行版的一部分，然后才被2.4主内核采纳。

上面这些描述的要点是，不同Linux发行版公司提供的系统存在差异（大多数的差异都很小）。从更小的范围来讲，这种实现间的分裂和UNIX早期发生的分裂是一样的。Linux标准基础（LSB）已经在努力，希望能够保证各个Linux发行版之间的可移植性。为了达到这个目标，LSB（<http://www.linux-foundation.org/en/LSB>）开发和推广了一组Linux系统的标准，目的在于确保二进制应用（编译过的程序）可以在任何LSB依从的系统中运行。

## 1.4 小结

UNIX系统最早于1969年在Digital PDP-7微计算机中由贝尔实验室的Ken Thompson实现。UNIX操作系统和它的双关语名字一样，从早期的MULTICS系统中吸收了许多想法。1973年UNIX被移植到PDP-11微计算机中，并用C重新编写，C语言由贝尔实验室的Dennis Ritchie设计和实现。由于法律阻止销售UNIX，AT&T转而向大学发布了完整的系统。这个发布包括源代码，在大学迅速流行起来，因为它提供了便宜的操作系统，并且可以让计算机科学院和学生学习和修改其源代码。

加州大学伯克利分校在UNIX系统的开发中扮演了关键角色。在那里Ken Thompson和一些毕业生扩展了UNIX操作系统。1979年伯克利发布了自己的UNIX系统BSD。这个发布版在学院广泛普及，并成为几个商业实现的基础。

同时AT&T垄断的解体，允许公司开始销售UNIX系统。这就产生了另一个主要的UNIX变种：System V，同样也成为几个商业实现的基础。

两个不同的因素促成了GNU/Linux的开发，其中一个因素是GNU项目，由Richard Stallman成立。到1980年代末，GNU项目已经创建了一个几乎完整的自由UNIX实现。缺少的只是可以工作的内核。1991年，Linus Torvalds受到Andrew Tanenbaum编写的Minix内核的启发，为Intel x86-32体系架构创建了一个可以工作的UNIX内核。Torvalds邀请其它程序员加入，来改进这个内核。许多程序员积极响应，于是Linux被扩展和移植到大量硬件体系架构下。

不同UNIX和C实现在1980年代末存在的可移植性问题，直接促成了标准化进程。1989年C语言标准化（C89），1999年进一步修订标准（C99）。对操作系统接口的首个标准化尝试产生了POSIX.1，并于1988年批准为IEEE标准，1990年批准为ISO标准。在整个1990年代，草拟了许多标准，包括各种版本的Single UNIX规范。2001年POSIX 1003.1-2001和SUSv3结合的标准得到批准。这个标准巩固和扩展了许多早期的POSIX标准和早期的Single UNIX规范。2008年完成了一个不那么广泛应用的标准修订，结合了POSIX 1003.1-2008和SUSv4标准。

和多数商业UNIX实现不同，Linux的实现和发行是分离的。因此没有单一的“官方”Linux发行版。每个Linux发行商都提供当前稳定版内核的某个快照，并增加许多patch。LSB开发和促进了一组Linux系统标准，目的是确保二进制应用在不同Linux发行版之间的可移植性，这样编译后的程序就可以在相同硬件的任何LSB依从系统中运行。

**更多信息**

（略）

# 第2章 基础概念

本章介绍Linux系统编程相关的许多概念。目标是那些主要工作于其它操作系统，或者对Linux和其它UNIX实现只有有限经验的读者。

## 2.1 操作系统的核心：内核

操作系统这个术语通常表示两个不同的意思：

* 表示整个软件包系统，是管理计算机资源的中心软件，包含所有标准软件工具，如命令行解释器、图形用户界面、文件工具、和编辑器。
* 狭义的含义则指管理和分配计算机资源（如CPU、RAM、和设备）的核心软件。

内核这个术语通常则代表第二种意思，本书所说的操作系统也是这种意思。

尽管没有内核也可以在计算机中运行程序，但内核能够极大地简化编写和使用其它程序，并增强程序员的能力和灵活性。内核通过提供软件分层来管理有限的计算机资源。

**内核执行的任务**

内核主要执行以下任务：

* 进程调度：计算机只有一个或少数中央处理单元（CPU）来执行程序指令。和其它UNIX系统一样，Linux是抢先式多任务操作系统，多任务表示多个进程（正在运行的程序）可以同时在内存中，而且每个都可以使用CPU。抢先式表示由内核进程调度器支配哪个进程获得CPU，以及确定进程使用CPU的时间。
* 内存管理：虽然计算机内存容量在近十来年变得非常庞大，但软件的体积也相应地快速增长，因此物理内存（RAM）仍然是一种有限的资源，内核必须以公平和有效的方式使多个进程间共享物理内存。和多数现代操作系统一样，Linux采用了虚拟内存管理机制（6.4节），这个技术有两个主要的优点：
  + 进程与其它进程以及内核隔离，因此一个进程不能读取和修改另一个进程以及内核的内存。
  + 内存中只保留某个进程的部分，因此降低了每个进程的内存需求，允许更多进程同时存在于RAM中。这也提高了CPU利用率，因为增强了这样一种可能性，任何时候至少有一个进程可以让CPU执行。
* 文件系统管理：内核提供文件系统，允许创建、读取、更新、删除文件等等操作。
* 创建和终止进程：内核可以装载新程序到内存中，为其提供运行所需的相关资源（CPU、内存、文件访问等）。每个正在运行的程序就是一个进程。一旦某个进程完成执行，内核确保它使用的资源被释放，并可以提供给接下来的程序使用。
* 设备访问：计算机系统中附加的设备（鼠标、显示器、键盘、磁盘和磁带设备等等）允许计算机与外界进行交流，提供输入和输出功能。内核为程序提供标准化和简化的接口访问设备，同时为多个进程使用设备进行仲裁。
* 网络：内核代表用户进程传输和接收网络信号（包）。这个任务包括将网络包路由至目标系统。
* 提供系统调用应用编程接口（API）：进程可以向内核请求执行不同的任务，使用内核入口也就是系统调用。Linux系统调用API是本书的主要主题。3.1节详细描述了进程执行系统调用时的步骤。

除了上面这些特性，多用户操作系统（如Linux）通常还给用户提供虚拟私有计算机的抽象；每个用户都可以登录到系统中，并与其它用户大体上独立操作。例如每个用户有自己的磁盘存储空间（home目录）。此外用户还可以运行程序，每个程序都能获得共享的CPU，并在自己的虚拟地址空间中操作，这些程序还可以独立的访问设备和通过网络传输信息。内核解决潜在的硬件资源访问冲突，因此用户和进程通常感觉不到冲突的存在。

**内核模式和用户模式**

现代处理器体系架构通常允许CPU至少在两种不同模式下操作：用户模式和内核模式（有时候也称为超级模式）。通过硬件指令就可以在不同模式间切换。相应地虚拟内存也被划分为用户空间和内核空间等区域。当运行在用户模式中时，CPU只能访问标记为用户空间的内存；试图访问内核空间内存会导致硬件异常。当运行在内核模式中时，CPU可以同时访问用户和内核空间内存。

有些操作只有进程处于内核模式时才能执行。例如执行halt指令来停止系统、访问内存管理硬件、发起设备I/O操作等。通过把操作系统放在内核空间中，操作系统实现可以确保用户进程无法访问内核的指令和数据结构，或者阻止用户进程执行有害操作。

**进程VS内核对系统的视角**

在每天的许多编程工作中，我们习惯于按面向进程的方式来思考。但是考虑到本书后面讲解的许多主题，调整我们的视角，从内核的角度来观察会非常有帮助。为了使对比更加明显，我们首先考虑进程视角，然后是内核视角。

一个运行系统通常有许多进程。对于每个进程，很多事情都在异步发生。执行进程并不知道自己什么时候CPU时间用完，其它进程被调度获得CPU，以及自己何时再次被调度，也不知道发生的顺序如何。信号递送和进程间通信事件由内核仲裁，对进程来说可能在任何时间发生。许多事情对进程是透明的。进程不知道自己在RAM中的位置，也不知道自己哪部分内存空间在内存中或是在交换区域（磁盘的保留区域，用来补充计算机的RAM）。类似地，进程也不知道自己访问的文件被存放于磁盘驱动器的位置；进程只是简单地通过名字来引用文件。进程的操作相互独立，不能直接与其它进程通信。进程自己也不能创建新进程，甚至无法终止自己。最后进程也不能直接与计算机的输入输出设备交互。

相比之下，运行系统的内核则知道和控制了所有一切。内核为系统中所有运行进程提供协助。内核决定哪个进程获得CPU访问权，什么时候获得，使用多长时间。内核维护一组进程数据结构，包含所有运行进程的所有信息，并根据进程创建、状态变化、进程终止来更新这些数据结构。内核维护所有底层的文件数据结构，允许程序使用文件名访问文件，并转换为磁盘中的物理位置。内核同时还维护每个进程虚拟内存到物理内存映射，以及到磁盘交换区域映射的数据结构。进程间的所有通信都通过内核提供的机制来完成。根据进程的请求，内核创建新进程或结束现有进程。最后内核（特别是设备驱动）执行所有与输入输出设备的交互，为用户进程传递信息。

本书后面我们讲到“进程可以创建另一个进程”、“进程可以创建管道”、“进程可以向文件写入数据”、“进程可以通过调用exit()终止”，请记住内核仲裁所有这些动作，这些句子只不过是“进程可以请求内核创建另一个进程”的简称。

## 2.2 Shell

Shell是特殊的程序，它读取用户输入的命令，并执行适当的程序来响应这些命令。Shell有时候也被称为命令解释器。

login shell表示用户首次登录时，为运行shell而创建的那个进程。

虽然在某些操作系统中命令解释器是内核的部分，但在UNIX系统中，shell实际上是用户进程。存在许多不同的shell，相同计算机的不同用户可以同时使用不同的shell。比较重要的几个shell如下：

* Bourne shell（sh）：这是被广泛使用的最古老的shell，由Steven Bourne编写。它是UNIX第7版的标准shell。Bourne shell包含许多其它所有shell拥有的特性：I/O重定向、管道、文件名自动生成、变量、环境变量操作、命令替换、后台命令执行、和函数。所有后来的UNIX实现都包含Bourne shell，同时也提供其它某些shell。
* C shell（csh）：这个shell由加州大学伯克利分校的Bill Joy编写。名字的来源是这个shell和C编程语言有许多相似的流控制。C shell提供Bourne shell没有的几个有用的交互特性，包括命令历史、命令行编辑、任务控制、和别名。C shell和Bourne shell不保持向后兼容。尽管BSD的标准交互shell是C shell，shell脚本（马上讲到）通常都是按Bourne shell编写，这样才能在所有UNIX实现中保持可移植。
* Korn shell（ksh）：这个shell由AT&T贝尔实验室的David Korn编写，是Bourne shell的继承者。与Bourne shell保持向后兼容的同时，增加了与C shell类似的交互特性。
* Bourne again shell（bash）：这个shell是GNU项目对Bourne shell的重新实现。提供了类似于C shell和Korn shell的交互特性。bash shell理论上的作者是Brian Fox和Chet Ramey。Bash可能是Linux系统使用最广泛的shell（Linux中Bourne shell是由bash提供的尽可能相似的模拟）。

shell不仅仅为交互用户设计，也可以解释shell脚本，后者是包含shell命令的文本文件。为了实现这个目的，每个shell都有类似于编程语言的机制：变量、循环和条件控制语句、I/O命令、和函数。

每个shell都执行类似的任务，只在语法上存在区别。不管我们讲哪个特定shell的操作，我们通常都只说“shell”，所有shell都按这种方式进行操作。本书的多数例子都需要使用bash，但是除非特别提到，读者可以假设这些例子可以在其它Bourne shell中同样工作。

## 2.3 用户和组

系统的每个用户都有唯一标识，用户可能属于某个或几个组。

**用户**

系统的每个用户都有唯一的逻辑名（用户名）和相应的用户ID（UID数字）。对于每个用户，系统的password文件（/etc/passwd）都有一行对其进行定义，还包含以下额外信息：

* 组ID：数字的组ID，用户加入的第一个组。
* home目录：用户登录后的初始目录。
* 登录shell：用来解释用户命令的shell名称。

这个密码记录可能还包含用户的密码，以加密形式存储。但是由于安全原因，通常密码会存放在单独的shadow密码文件中，只对超级用户可读。

**组**

从管理的角度来讲（特别是控制文件和其它系统资源的访问），把用户组织为组是非常有用的。例如工作于同一个项目的团队成员，需要共享相同的一组文件，就可以把所有成员添加到同一个组。在早期UNIX实现中，用户只能加入一个组。BSD允许用户同时加入多个组，这个想法被其它UNIX实现和POSIX.1-1990标准接受。每个组由系统组文件（/etc/group）一个单独的行定义，主要包括以下信息：

* 组名：组的唯一名称。
* 组ID（GID）：与该组相关联的ID数值。
* 用户列表：逗号分隔的用户登录名列表，这些用户都属于这个组（没有在这里标识的用户也可以在自己的密码文件记录中添加该组）。

**超级用户**

超级用户拥有系统的特别权限。超级用户的用户ID是0，通常登录名是root。在典型的UNIX系统中，超级用户可以绕过系统的所有权限检查。例如超级用户可以访问系统的任何文件，无论文件的权限如何设置；也可以向系统中的任何用户进程发送信号。系统管理员使用超级用户执行许多管理性的任务。

## 2.4 单一目录层次、目录、链接、和文件

内核维护一个单一层次的目录结构，来组织系统中的所有文件。（这和Microsoft Windows明显不同，后者的每个磁盘分区都有自己的目录层次）。层次的最底部是root目录，名为“/”（斜线）。所有文件和目录都是root目录直接或间接的子目录。图2-1显示了这种文件结构的一个例子：



*图2-1：Linux单一目录层次的子集*

**文件类型**

目录是一种特殊的文件，它的内容是文件名加上相应文件索引的表格。这种文件名+引用的关联就称为链接，而文件可以有多个链接，因此在相同或不同的目录下，可以有文件的多个名字。

目录可以同时包含文件和其它目录的链接。目录之间的链接组成了图2-1所示的目录层次。

每个目录都至少包含两项：“.”（点），链接到目录本身；“..”（点点），链接到父目录，也就是层次中上面那个目录。每个目录（除了root）都有父目录。对于root来说，“..”链接到root目录本身（因此“/..”等同于“/”）。

**符号链接**

和普通链接一样，符号链接也提供名字到文件的映射。但是普通链接是在目录列表中的文件名-指针项，而符号链接则是特殊的文件，它的内容是另一个文件的名字。（换句话说，符号链接有文件名-指针项，指针引用的文件内容是另一个文件的名字）。后一个文件通常称为符号链接的目标，通常也称符号链接“指向”或“引用”目标文件。当在系统调用中指定路径时，多数情况下内核会自动“解引用”（跟随）路径中的每个符号链接，使用实际的文件名替换该符号链接指针。如果符号链接的目标本身也是一个符号链接，那么这个过程可能产生递归。（内核强制解引用的数量限制，以避免环形符号链接）。如果符号链接引用的文件不存在，就称为dangling链接。

通常把普通链接和符号链接分别称为硬链接和软链接。为什么要使用两种类型的链接？我们在后面第18章会做出解释。

**文件名**

在多数Linux文件系统中，文件名最多可以有255个字符长度。文件名可以包含任何字符，除了斜线（/）和null字符（\0）。但是只使用字母和数字，以及“.”（点）、“\_”（下划线）、“-”（连字符）是明智的。这65个字符集[-.\_a-zA-Z0-9]在SUSv3中被称为可移植文件名字符集。

我们应该避免使用不可移植的文件名字符，因为这些字符在shell、正则表达式、或其它上下文中可能有特殊含义。如果一个文件名包含特殊含义的字符，那么这些字符就必须被转义。通常是在前面加上反斜线（\）来表示这些字符不要按特殊含义来解析。在无法使用转义机制的情况下，这个文件名就是不可用的。

我们应该避免以连字符（-）来开始一个文件名，因为这样的文件名可能会被shell错误地解析为命令行参数。

**路径名**

路径名是以可选的“/”开始，包含一系列以“/”分隔的文件名的字符串。除掉最后那个文件名，这串字符就标识了一个目录（或者一个指向目录的符号链接）。路径的最后那个文件名可以是任何文件，也可以是目录。在最后一个“/”之前的所有部分有时候称为路径的目录部分，紧跟最后那个“/”的名字就称为文件，或路径的base部分。

路径名以从左向右的顺序读取；每个文件名都存在于路径名之前那部分所标识的目录。字符“..”可以用在路径名的任何位置，来引用当前位置路径的父目录。

路径名描述了一个文件在单一目录层次架构中的具体位置，可以是绝对或相对路径：

* 绝对路径：开始于“/”，指定了相对于根目录的位置。例如图2-1中的绝对路径：/home/mtk/.bashrc、/usr/include、和/（根目录的路径名）。
* 相对路径：指定相对于进程当前工作目录（下面会介绍）的文件位置，和绝对路径的区别在于不以“/”开始。在图2-1中，相对于目录usr，文件types.h的相对路径就是include/sys/types.h；相对于目录avr，文件.bashrc则可以使用相对路径../mtk/.bashrc来引用。

**当前工作目录**

每个进程都有一个当前工作目录（有时候称为进程的工作目录或当前目录）。这是进程在单一层次目录架构中的“当前位置”，从这个目录开始解析所有的相对路径。

进程继承父进程的当前工作目录。login shell设置自己的当前工作目录为用户密码文件项的home目录。可以使用“cd”命令修改shell的当前工作目录。

**文件所有权和权限**

每个文件都关联到一个用户ID和组ID，定义了该文件的所有权，和文件所属于的组。文件所有权用来确定对于不同用户的访问权限。

要访问一个文件，系统把用户划分为三种类型：文件所有者（user）、文件组ID相匹配的用户（group）、和其它所有用户（other）。每种类型的用户都有三个权限位可以设置（总共9个权限位）：读权限允许读取文件内容；写权限允许修改文件内容；执行权限则允许执行该文件，这个文件要么是程序，要么是某种解释器可以处理的脚本（通常但不一定总是shell）。

这些权限也可以为目录设置，不过含义稍微有些不同：读权限允许列出目录的内容（也就是文件名）；写权限允许修改目录的内容（添加、移除、和修改文件名）；执行权限（有时候称为查找权限）允许访问目录中的文件（还要取决于文件本身的权限设置）。

## 2.5 文件I/O模型

UNIX的I/O模型的一个显著特点就是通用I/O概念。这意味着相同的一组系统调用（open(), read(), write(), close()等等）可以执行所有文件类型的I/O操作，包括设备（内核把应用I/O请求转化为适当的文件系统或设备驱动操作，来执行目标文件或设备的I/O操作）。因此采用这些系统调用的程序可以工作于任何文件类型。

内核本质上只提供一种文件类型，顺序字节流，如果是磁盘文件（磁盘或磁带设备），则可以通过lseek()系统调用进行随机访问。

许多应用和库把换行字符（ASCII码10，有时候也称为linefeed）解释为一行文本的终结符并开始下一行。UNIX系统没有文件结束字符（end-of-file）；读取文件无返回数据时表示到达文件末尾。

**文件描述符**

I/O系统调用通过文件描述符来引用已打开的文件，通常是一个很小的非负整数。文件描述符一般通过调用open()获得，传入路径参数指定要对哪个文件执行I/O操作。

通常进程由shell启动时会继承三个已经打开的文件描述符：描述符0是标准输入，进程把它那里获得输入；描述符1是标准输出，进程向它写入输出数据；描述符2是标准错误，进程向它写入错误信息，并通知异常或错误情况。在交互式shell或程序中，这三个描述符通常都连接到终端。在stdio库中，这三个描述符对应于文件流stdin, stdout, stderr。

**stdio库**

C程序通常采用标准C库中的I/O函数执行文件I/O。这一组函数称为stdio库，包括fopen(), fclose(), scanf(), printf(), fgets(), fputs()等等。stdio函数在I/O系统调用（open(), close(), read(), write()等等）之上。

## 2.6 程序

程序通常有两种存在形式。第一个是源代码，使用编程语言编写（如C），是人类可读的一系列程序语句。程序要被执行，源代码必须转化为第二种形式：二进制机器语言指令，这样计算机才能理解。（这和脚本形成对比，后者是包含许多命令的文本文件，直接由shell或其它命令解释器等程序处理）。程序的这两种含义通常认为是同义的，因为编译和链接最终会将源代码转化为语义相同的二进制机器代码。

**过滤器**

过滤器通常指的是那些从stdin读取输入，执行一些转化后，再将结果写入stdout的程序。例如cat, grep, tr, sort, wc, sed和awk。

**命令行参数**

在C语言中，程序可以访问命令行参数，即程序运行时提供的命令行。要访问命令行参数，程序的main()函数必须如下定义：

int main(int argc, char \*argv[])

argc变量包含命令行参数的总数，单个的参数由argv数组的字符串指针引用。其中第一个字符串argv[0]，标识了程序本身的名字。

## 2.7 进程

最简单地说，进程就是执行中的程序。当程序被执行时，内核装载程序代码到虚拟内存中，为程序变量分配空间，并设置内核数据结构来记录该进程的许多信息（例如进程ID、终止状态、用户ID、和组ID等）。

从内核的视角来看，进程是内核必须为其共享许多计算机资源的实体。由于资源是有限的（如内存），内核一开始只分配一定的资源给进程，然后在进程的生命周期过程中，根据进程的需要和整个系统的负载情况，来调整这些分配。当进程终止时，进程使用的所有资源都会被回收，并提供给其它进程重新使用。其它一些资源（如CPU和网络带宽），还必须在所有进程中公平地共享。

**进程内存布局**

进程逻辑上划分为以下部分，称为段（segment）：

* 文本（Text）：程序的指令。
* 数据（Data）：程序使用的静态变量。
* 堆（Heap）：程序可以动态分配额外内存的一个区域。
* 堆栈（Stack）：随着函数调用和返回自动扩展和缩小的一小段内存，为本地变量和函数调用链接信息分配存储空间。

**进程创建和程序执行**

进程可以使用fork()系统调用创建新的进程。调用fork()的进程称为父进程，新创建的进程就是子进程。内核通过复制父进程来创建子进程。子进程获得父进程的数据、堆栈、和堆的拷贝，并且随后可以进行修改，而不影响父进程。（程序的文本，存放于只读内存区域，由父子进程共享）。

调用fork()后，子进程要么执行父进程代码中的另一组函数；或者更常见的是使用execve()系统调用装载和执行一个全新的程序。execve()系统调用销毁现有的文本、数据、堆栈、和堆段，并根据新程序代码的新段进行替换。

有几个C库函数基于execve()系统调用实现，每个都提供稍微不同的接口，但是功能是一样的。所有这些函数都以相同的exec字符串开头，区别在哪里目前并不重要，我们使用exec()来引用所有这些函数。不过要明确一点，Linux中并没有名为exec()的函数。

通常我们使用动词exec来描述execve()和相关库函数执行的操作。

**进程ID和父进程ID**

每个进程都有唯一的整数类型的进程标识符（PID）。每个进程同时还有一个父进程标识符（PPID），标识了创建自己的那个进程。

**进程终止和终止状态**

进程可以按两种方式终止：使用\_exit()系统调用（或者相关的exit()库函数）自己请求终止；或者被信号kill而终止。前一种情况进程会产生一个终止状态，一个很小的非负整数，父进程可以使用wait()系统调用来检查这个值。如果调用\_exit()，进程可以显式地指定自己的终止状态。如果进程被信号杀掉，终止状态根据引起进程终止的信号类型来决定。（有时候我们把传递给\_exit()的参数称为进程的退出状态，以区别于终止状态，后者要么是传递给\_exit()的值，要么是信号kill进程产生的值）。

习惯上终止状态0表示进程成功退出。非0状态表示发生了某种错误。多数shell都可以通过$?变量来获得最后执行程序的终止状态。

**进程用户和组标识符（凭证）**

每个进程都有一组相关的用户ID（UID）和组ID（GID）。包括：

* 实际用户ID和实际组ID：标识进程所属的用户和组。新进程继承父进程的实际用户ID和实际组ID。login shell从系统密码文件相应的域获得实际用户ID和实际组ID。
* 有效用户ID和有效组ID：这两个ID（再加上下面的附加组ID）用来确定进程访问受保护资源时的权限，如文件和进程间通信对象。通常进程的有效ID和相应的实际ID相同。修改有效ID是允许进程获得其它用户和组的权限的一种机制，马上我们就会讲到。
* 附加组ID：这些ID标识进程属于的额外的组。新进程继承父进程的附加组ID。login shell从系统组文件中获取自己的附加组ID。

**特权进程**

在UNIX系统中特权进程的有效用户ID是0（超级用户）。这样的进程可以绕过内核实施的权限限制。相反非特权（或无特权）则是其它用户的进程。这种进程的有效用户ID非0，并且受内核的权限规则控制。

特权进程创建的进程也拥有特权，例如由root用户启动的login shell。另一种使进程拥有特权的方法是通过设置用户ID机制，允许进程使用程序文件拥有者的身份执行该进程。

**能力**

从内核2.2开始，Linux对特权进行了划分。每种特权操作都与特定的能力相关联，只有进程拥有相应的能力，才能执行该特权操作。超级用户进程（有效用户ID等于0）的所有能力都被启用。

赋予进程一组能力子集，可以使其执行某些超级用户才允许的操作，同时又防止其执行其它特权操作。

第30章详细讨论了能力，在本书的后面部分，当提到特定操作只能由特权进程执行时，我们通常会标识出相应的能力。能力的名字以前缀CAP\_开始，例如CAP\_KILL。

**init进程**

系统启动时，内核会创建一个特殊的init进程，它是所有进程的父进程，通常是/sbin/init程序文件。系统中的所有进程都是init或其后代创建的（通过fork()）。init进程的ID总是1，并且以超级用户权限运行。init进程不能被kill（超级用户也不行），只有系统关机时它才会终止。init的主要任务是创建和监控运行系统需要的所有进程（更多细节请参考init(8)手册页）。

**Daemon进程**

daemon是一种特殊用途的进程，daemon的创建和处理与其它进程相同，但是有以下区别：

* 长期运行，daemon进程通常在系统引导时启动，一直运行到系统关机。
* 后台运行，没有控制终端，不能读取输入也无法进行输出。

daemon的典型例子是syslogd，为系统记录日志信息；以及httpd，通过HTTP提供web网页服务。

**环境列表**

每个进程都有一个环境列表，是进程的用户空间内存中维护的一组环境变量。这个列表的每个元素都包含一个名字和相应的值。当通过fork()创建新进程时，继承父进程的环境。因此环境提供了一种父进程向子进程传递信息的机制。当进程使用exec()替换原有程序时，新的程序要么继承老程序的环境，要么使用exec()调用指定的新环境参数。

环境变量在多数shell中都是通过export命令来创建（C shell使用setenv命令），例子如下：

$ export MYVAR='Hello world'

C程序可以使用一个external变量（char \*\*environ）来访问环境，还有许多库函数允许进程获得和修改环境中的值。

环境变量有许多用途。例如shell定义和使用了大量变量，可以被shell执行的脚本和程序访问。包括变量HOME（指定了用户登录目录的路径）、变量PATH（指定了一组目录，shell执行用户输入的命令时会在里面查找相应的程序）。

**资源限制**

每个进程都要消耗资源，例如打开的文件、内存、CPU时间。进程可以使用setrlimit()系统调用设置自己消耗各种资源的上限。每个资源限制都有两个关联的值：软限制，限制了进程可以消耗的资源数量；硬限制，是软限制可以调整的上限。非特权进程可以把软限制设为0到相应的硬限制，但是只能降低硬限制。

当新进程创建时，会继承父进程的资源限制设置。

shell的资源限制可以使用ulimit命令进行调整（C shell使用limit）。这些限制值会被shell执行命令创建的子进程继承。

## 2.8 内存映射

使用mmap()系统调用可以在调用进程的虚拟地址空间中创建新的内存映射。内存映射有以下两种类型：

* 文件映射把文件区域映射到调用进程的虚拟内存中。一旦映射完成，就可以通过相应内存区域来访问文件内容。当需要时会自动从文件装载到内存页面中。
* 匿名映射则没有相应的文件。相反所有映射的页面都初始化为0。

一个进程映射的内存可以和另一个进程共享。可能是两个进程同时映射一个文件的相同区域，或者子进程继承父进程的映射。

当两个或多个进程共享相同的页面时，每个进程都可能看到其它进程对页面内容的修改，具体则取决于映射是私有还是共享的。当映射是私有的时，对映射内容的修改对于其它进程是不可见的，也不会修改到底层的文件。当映射是共享的时，对映射内容的修改对于其它共享该映射的进程是可见的，而且会更新底层的文件。

使用内存映射有许多目的，包括装载可执行文件来初始化进程的文本段、分配新的内存（置0）、文件I/O(内存映射I/O)、和进程间通信（通过共享映射）。

## 2.9 静态和共享库

对象库是已编译对象代码的文件，包含一组可被应用程序调用的函数（通常是逻辑相关的一组函数）。把一组函数的代码放在一个单独的对象库中，简化了程序创建和维护的工作。现代UNIX系统提供两种对象库：静态库和共享库。

**静态库**

静态库（有时候称为archive）是早期UNIX系统唯一支持的库类型。静态库本质上是结构化的已编译对象模块。要使用静态库中的函数，我们在构建程序时使用链接命令来指定该库。链接器为应用程序引用的所有函数找到相应的静态库模块，然后从静态库中提取出所需的对象模块，并复制到最终的可执行文件中。我们称这样的程序是静态链接的。

每个静态链接的程序都从库中复制了需要的对象模块，这种方式导致了一些缺点。其中之一就是不同可执行文件中的对象代码重复浪费了磁盘空间。当使用相同静态库的多个程序一起执行时，也浪费了内存空间；每个程序都会有相同的函数拷贝在内存中。此外如果库函数需要修改，那么在重新编译该函数并添加到静态库中后，所有使用该函数的应用都必须重新与库进行链接。

**共享库**

共享库是为了解决静态库的问题而设计的。

如果程序链接到共享库，那么就不会复制对象模块到可执行文件中，相反链接器会在可执行文件中插入一条记录，表示运行时需要使用这个共享库。当可执行文件装载到内存时，程序调用动态链接器确保所有需要的共享库都能够找到并装载到内存中，然后执行动态链接或resolve到相应的函数定义。在运行时，只有一份共享库需要保存在内存中，所有运行程序都使用这份拷贝。

共享库只包含唯一的已编译函数，可以节省磁盘空间。同时可以极大地确保程序能够轻松地使用更新版本的函数。只需要重新构建共享库，现有程序在下次运行时就可以自动使用到最新的函数定义。

## 2.10 进程间通信和同步

Linux系统运行着许多进程，许多是相互独立进行操作的。但某些进程则需要合作才能完成自己的任务。这些进程需要能够与其它进程进行通信，并同步各自的动作。

进程间通信的一个方法是通过读取和写入相关信息到磁盘文件中。但是对于许多应用来说，这样做太慢也不够灵活。

因此Linux和所有现代UNIX实现一样，提供一组丰富的进程间通信机制，包括以下这些：

* 信号，用来指示发生了某个事件。
* 管道（shell用户熟知的“|”操作符）和FIFO，用来在进程间传输数据。
* socket，用来在进程间传输数据，既可以在同一计算机中，也可以在通过网络连接的不同计算机中进行通信。
* 文件锁，允许进程锁住文件的某个区域，阻止其它进程读取和更新该区域的文件内容。
* 消息队列，用来在不同进程间交换消息（数据包）。
* 信号量，用来同步进程间的动作。
* 共享内存，允许两个或多个进程共享一块内存。当一个进程修改共享内存的内容时，所有进程都可以立即看到这个修改。

UNIX系统的IPC机制数量繁多，有些功能存在重叠，部分原因是各种UNIX系统变种不同发展，以及各种标准的要求导致。例如FIFO和UNIX域socket本质上执行相同的功能，都允许相同系统的不相关进程之间交换数据。现代UNIX系统拥有这两种机制，因为FIFO来自System V，而socket来自BSD。

## 2.11 信号

尽管我们在上一节把信号列为IPC机制之一，信号通常还在许多其它情况下被使用。值得我们进一步详加讨论。

信号通常被描述为“软件中断”。信号的到来通知进程发生了某些事件或者异常条件。信号的种类非常多，每个都标识了不同的事件或异常条件。每个信号类型都由一个整数标识，并使用符号名SIGxxxx来定义。

信号可以由内核发送给进程，也可以是其它进程发送（需要适当的权限），甚至可以自己给自己发送信号。例如当发生以下情况时，内核会给进程发送信号：

* 用户用键盘输入中断字符（通常是Control-C）。
* 进程的某个子进程终止。
* 进程设置的定时器（alarm时钟）过期。
* 进程试图访问非法内存地址。

在shell中，kill命令可以向进程发送信号。kill()系统调用则为程序提供相同的功能。

当进程接收到一个信号时，它可以根据不同的信号类型，采取以下动作：

* 进程忽略信号
* 进程被信号kill
* 进程暂时挂起，稍后在收到特别的信号后再继续。

对于多数信号类型，除了接受默认的信号动作，程序可以选择忽略信号，或者创建一个信号处理器。信号处理器是由程序员定义的函数，当信号到来时会被自动调用。这个函数可以根据信号产生的条件执行适当的动作。

从信号产生到被递送至进程，这段时间称信号是“未决”的。通常未决信号会尽快在进程下次被调度时递送至进程；或者如果进程正在运行，则会立即递送。但是通过添加信号到进程的信号掩码中，也可以阻塞该信号。如果信号产生时被阻塞，就会一直保持未决状态，直到被解除阻塞（从信号掩码中移除）。

## 2.12 线程

在现代UNIX系统中，每个进程都可以有多个执行线程。你可以把线程想象成共享相同虚拟内存，以及其它许多属性的进程。每个线程都执行同一个程序代码文件，并且共享相同的数据区域和堆。但是每个线程拥有自己的堆栈，里面存放本地变量和函数调用链接信息。

线程可以通过全局对象来互相通信。线程API提供了条件变量和mutex，主要是用来允许线程通信和动作同步，特别是保护共享变量的访问。线程也可以使用2.10节描述的IPC机制进行通信和同步。

使用的线程的主要优点是多个线程间共享数据非常容易（通过全局变量）；以及某些算法使用多线程实现更加自然。此外多线程应用还可以明显地利用并行处理和多核硬件的能力。

## 2.13 进程组和shell工作控制

shell执行的每个程序都会启动一个新的进程。例如shell创建三个进程来执行下面这个管道命令（按文件大小排序显示当前工作目录下的文件列表）：

$ ls -l | sort -k5n | less

所有主流shell，除了Bourne shell，都提供job控制的交互特性，允许用户同时执行和操作多个命令或管道。在job控制的shell中，管道中的所有进程都置于一个新进程组或job中。（shell命令行只包含一条命令时，新的进程组只包含一个进程）。该进程组中的每个进程都拥有相同的整数值进程组标识符，这个值和进程组中的进程组领导者的进程ID相同。

内核允许对进程组的所有成员进行许多操作，例如递送信号。job控制shell使用这个特性允许用户挂起或继续管道中的所有进程，下一节我们会描述。

## 2.14 会话、控制终端、和控制进程

会话是进程组（job）的一个集合。会话中的所有进程拥有相同的会话标识符，会话领导者是创建会话的那个进程，会话ID就是它的进程ID。

会话主要用于job控制shell。job控制shell创建的所有进程组都属于相同会话，shell就是会话领导者。

会话通常会有一个关联的控制终端。当会话领导者进程第一次打开终端设备时建立控制终端。如果是交互式shell创建的会话，那就是用户登录时的终端。一个终端只能作为一个会话的控制终端。

会话领导者打开控制终端之后，自己也就成为这个终端的控制进程。如果终端连接断开（例如关闭了终端窗口），控制进程会收到一个SIGHUP信号。

在任何时候，会话中的一个进程组是前台进程组（前台job），它可以从终端读取输入和写入输出。如果用户在控制终端中按下中断字符（通常是Ctrl-C）或者挂起字符（通常是Ctrl-Z），终端设备就会发送一个kill或挂起信号到前台进程组。会话可以有任意数量的后台进程组（后台job），在命令后面加上“&”字符可以创建后台进程组。

job控制Shell提供一组job相关的命令，包括列出所有job、向job发送信号、把job在前后台之间切换。

## 2.15 伪终端

伪终端是连接在一起的一对虚拟设备，称为master（主）和slave（从）。这对设备提供IPC通道，允许在两个设备间双向传输数据。

伪终端的关键是slave设备提供了类似终端的接口，这样就可以把一个面向终端的程序连接到slave设备，然后使用另一个程序连接到master设备，来驱动这个面向终端的程序。由驱动程序写入的输出经过终端驱动正常的输入处理（例如在默认模式下，回车被映射到换行），然后作为输入传递给连接到slave设备的那个面向终端的程序。面向终端的程序向slave设备写入的所有东西都会作为输入传递给驱动程序（也需要经过正常的终端输出处理）。换句话说，驱动程序按终端的惯例为用户处理相关的功能。

伪终端可以用在各种应用中，最显著的是实现X Window系统登录的终端窗口，以及提供网络登录服务，例如telnet和ssh。

## 2.16 日期和时间

进程一般会关心两种时间类型：

* 实际时间，一般从某个标准时间点开始计量（日历时间）；或者从某个固定点开始，通常是进程启动时（逝去时间或墙上时钟时间）。在UNIX系统中，日历时间是从1970年1月1日0点（Universal Coordinated Time，简称UTC）开始按秒计量，再以英国格林威治经线按时区进行调整。这个时间与UNIX系统的诞生比较接近，被称为Epoch。
* 进程时间，也称为CPU时间，是进程从启动开始总共使用的CPU时间。CPU时间又进一步划分为系统CPU时间、内核模式代码执行时间（执行系统调用和内核代表进程执行其它服务）、以及用户模式代码执行时间的用户CPU时间（例如执行普通程序代码）。

time命令可以显示管道中进程执行所花费的实际时间、系统CPU时间、和用户CPU时间。

## 2.17 客户端-服务器体系架构

在本书的一些地方，我们会讨论客户端-服务器应用的设计和实现：

客户端-服务器应用分为两个组件：

* 客户端，通过发送消息请求服务器执行某种服务。
* 服务器，接收客户端请求，执行适当的动作，并发送反馈信息给客户端。

有时候，客户端和服务器可能需要进行请求和返回的扩展对话。

一般客户端应用与用户交互，而服务器应用则提供某些共享资源的访问。通常会有许多客户端进程与一个或少数几个服务器进程通信。

客户端和服务器可以同时在同一台主机，也可以通过网络存在于不同机器上。客户端和服务器之间的互相通信，需要使用2.10节讨论的IPC机制。

服务器可以实现许多服务，例如：

* 提供数据库或其它共享信息资源的访问。
* 提供跨网络的远程文件访问。
* 封装某些业务逻辑。
* 提供共享硬件资源（如打印机）的访问。
* web页面服务。

把服务封装在一个服务器中有许多好处，例如：

* 高效，由服务器管理资源并提供服务，比在每台计算机中提供相同资源要便宜而且高效。
* 可控、协同、和安全，通过把资源（特别是信息资源）控制在单一位置，服务器可以控制资源的协同访问（如两个客户端不能同时更新相同的信息块），也可以使资源仅对选定客户端可用，提高安全性。
* 在多样环境中操作，在网络环境下，存在许多各不相同的客户端，服务器可以运行在不同的硬件和操作系统平台中。

## 2.18 实时

实时应用是那些必须及时响应输入的应用。最常见的输入是外部传感器或特殊的输入设备，输出则是控制某些外部硬件。常见的需要实时响应的应用有：自动化组装流水线、银行ATM、以及飞机导航系统。

尽管许多实时应用要求快速响应输入，但实时定义的关键是应用必须确保能够在最后期限之前响应输入。

要提供实时响应，特别是要求短时间内响应，要求底层操作系统提供支持。多数操作系统都不能够原生地提供实时支持，因为实时响应的需求和多用户共享时间的需求互相冲突。虽然UNIX变种有提供实时特性，传统的UNIX系统并不是实时操作系统。Linux的实时变种也有，而且目前内核也正在向完全原生支持实时应用的方向发展。

POSIX.1b定义了一组POSIX.1扩展来支持实时应用。包括异步I/O、共享内存、内存映射文件、内存锁、实时时钟和定时器、可选调度策略、实时信号、消息队列、和信号量等。尽管标准没有严格限定实时，多数UNIX实现现在都支持上面的部分或全部特性（在本书写作之时，Linux已经支持我们讨论的所有这些POSIX.1b特性）。

## 2.19 /proc文件系统

和某些其它UNIX实现一样，Linux也提供一个/proc文件系统，挂载在/proc目录下，它包含许多目录和文件。

/proc是虚拟的文件系统，它以文件系统的文件和目录的方式，提供内核数据结构的访问接口。这样就可以轻松地查看或修改许多系统属性。另外有一些/proc/PID形式的目录（PID是进程ID），允许我们查看系统每个运行进程的信息。

/proc文件系统的内容一般是人类可读的文本形式，可以被shell脚本解析处理。程序可以简单地open和read，也可以write需要的文件。多数情况下，程序必须拥有特权才能修改/proc目录下的文件内容。

在我们讨论许多Linux编程接口的时候，我们会同时描述相关的/proc文件。12.1节提供了/proc文件系统的更多信息。没有任何标准对/proc文件系统进行了定义，因此我们对其的讨论是特定于Linux的。

## 2.20 小结

在这一章，我们查看了许多Linux系统编程相关的基础概念。理解这些概念能够为读者提供Linux或UNIX的一定经验，使读者拥有足够的背景知识来开始学习系统编程。

# 第3章 系统编程概念

本章讲解系统编程的许多必备主题。首先介绍系统调用及其执行的详细步骤，然后考虑库函数及其与系统调用的区别，同时结合讲解（GNU）C库。

当我们调用系统调用或库函数时，总是应该检查它的返回值，来确定调用是否成功。我们描述了如何检查函数返回值，并介绍了一组错误诊断函数，它们用在本书的多数示例代码中。

最后我们考察许多与可移植编程相关的问题，特别是使用SUSv3提供的特性测试宏和标准系统数据类型。

## 3.1 系统调用

系统调用是进入内核的受控入口点，允许进程请求内核代表进程执行某些动作。内核通过系统调用API为应用程序提供一系列服务。这些服务包括：创建新进程、执行I/O操作、创建进程间通信用的管道等等（syscalls(2)手册页列出了Linux的所有系统调用）。

在描述系统调用工作的细节之前，我们先看一些基本要点：

* 系统调用把处理器状态从用户模式切换到内核模式，这样CPU才能访问受保护的内核内存。
* 系统调用是固定的。每个系统调用都由一个唯一的数值标识（这个数值通常对应用不可见，应用使用系统调用的名字来标识）。
* 每个系统调用都可以有一组参数，指定用户空间和内核空间之间要传递的信息。

从编程的角度来看，调用系统调用和调用C函数是非常相似的。但是在幕后，执行系统调用需要许多步骤。为了解释系统调用的步骤，我们来看下x86-32硬件体系架构下系统调用的每一个步骤：

1. 应用程序通过调用C库的包装函数发起系统调用。
2. 包装函数必须把系统调用的所有参数传递给系统调用陷阱处理例程（马上讲到）。这些参数是通过堆栈传递给包装函数的，但是内核要求参数存放在特定的寄存器中。包装函数把参数拷贝到这些寄存器中。
3. 由于所有系统调用都以同样的方式进入内核，内核必须采用某种方法来标识不同的系统调用。因此包装函数会把系统调用数值也复制到特定的CPU寄存器（%eax）。
4. 包装函数执行一个trap机器指令（int 0x80），这样就会把处理器从用户模式切换到内核模式，并从系统trap向量的0x80位置开始执行代码。更加现代的x86-32体系架构实现了sysenter指令，比传统的int 0x80 trap指令提供更快的进入内核模式的方法。从2.6内核和glibc 2.3.2开始支持使用sysenter。
5. 作为trap到0x80位置之后的响应，内核调用system\_call()例程（位于汇编文件arch/i386/entry.S）来处理这个trap。这个处理器：
   1. 把寄存器的值保存到内核堆栈中（6.5节）。
   2. 检查系统调用数值的有效性。
   3. 调用适当的系统调用服务例程，使用系统调用数值作为索引，从系统调用服务例程表中得到（内核变量sys\_call\_table）。如果系统调用服务例程需要参数，它会首先检查参数的有效性；例如，它会检查地址指向用户内存的合法位置。然后服务例程执行请求的任务，可能包括：修改参数指定地址的值，在用户内存和内核内存之间传输数据（例如I/O操作）。最后，服务例程返回一个结果状态给system\_call()例程。
   4. 从内核堆栈还原寄存器的值，并把系统调用返回值存放在堆栈中。
   5. 返回到包装函数，同时把处理器切回至用户模式。
6. 如果系统调用服务例程的返回值表示出现错误，包装函数就使用这个值设置全局变量errno（3.4节）。包装函数然后返回至调用方，提供一个整数返回值表示系统调用成功还是失败。

在Linux中，系统调用服务例程通常返回非负值表示成功，返回负值表示错误，这个错误值的绝对值就是相应的errno常量。当服务例程返回了负数值时，C库包装函数把它取正，并复制给errno，然后包装函数返回-1表示出现了错误。

这个惯例假设系统调用服务例程在成功时不会返回负数值。但是对于少数几个服务例程这个假设并不成立。一般来说这并不存在问题，因为取反后的errno值也没有超过合法的负数返回值范围。但是这个惯例确实导致了一个问题：fcntl()系统调用的F\_GETOWN操作，我们会在63.3节描述。

图3-1使用execve()系统调用阐明了上面的步骤。在Linux/x86-32上，execve()的系统调用数值为11（\_\_NR\_execve）。因此在sys\_call\_table向量中，条目11包含了sys\_execve()的地址，也就是这个系统调用的服务例程。（在Linux中，系统调用服务例程通常命名为sys\_xyz()，其中xyz就是正在讨论的这个系统调用）。

前面段落给出的信息已经超过了学习本书后面知识的需要。但是它说明了很重要的一点，即使是一个简单的系统调用，也需要完成许多工作，因此系统调用存在很小但仍然可观的开销。

作为系统调用开销的一个例子，我们来考虑getppid()系统调用，它只是简单地返回调用进程的父进程ID。在作者的x86-32 Linux 2.6.25系统中，调用getppid()一千万次大约需要2.2秒才能完成，大约每次调用需要0.3微秒。在相同的系统中，一千万次C函数调用（简单地返回一个整数）只需要0.11秒，大约是调用getppid()时间的二十分之一。当然，多数系统调用的开销比getppid()要大得多。

从C程序的角度来看，调用C库包装函数和调用相应的系统调用服务例程是等价的，因此在本书的剩余部分，我们使用“调用系统调用xyz()”来表示“调用包装函数来调用系统调用xyz()”。



*图3-1：执行系统调用的步骤*

附录A描述了strace命令，它可以用来跟踪应用发起的系统调用，可以作为调试程序时使用。

## 3.2 库函数

库函数指的就是标准C库的函数。这些函数的作用是各种各样的，包括打开文件、转换时间到人类可读的格式、以及比较两个字符串。

许多库函数不使用系统调用（例如字符串操作函数）。另外一些库函数则基于系统调用之上。例如fopen()库函数使用open()系统调用来打开文件。通常库函数设计用来提供比底层系统调用更加友好的接口。例如printf()函数提供输出格式和数据缓冲，而write()系统调用只是输出一块字节。类似地，malloc()和free()函数执行许多记录工作，使得分配和释放内存的任务比直接使用底层brk()系统调用要简单得多。

## 3.3 标准C库；GNU C库（glibc）

在不同UNIX实现中，标准C库也有不同的实现。Linux中最常用的实现是GNU C库（glibc, <http://www.gnu.org/software/libc/>）。

**确定系统中glibc的版本**

有时候我们需要确定系统中glibc的版本。我们可以在shell中运行glibc共享库，就把它当成是一个可执行程序。当我们把这个库当作可执行文件运行时，它会显示许多信息，包括版本号：

$ /lib/libc.so.6

GNU C Library stable release version 2.10.1, by Roland McGrath et al.

Copyright (C) 2009 Free Software Foundation, Inc.

This is free software; see the source for copying conditions.

There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A

PARTICULAR PURPOSE.

Compiled by GNU CC version 4.4.0 20090506 (Red Hat 4.4.0-4).

Compiled on a Linux >>2.6.18-128.4.1.el5<< system on 2009-08-19.

Available extensions:

The C stubs add-on version 2.1.2.

crypt add-on version 2.1 by Michael Glad and others

GNU Libidn by Simon Josefsson

Native POSIX Threads Library by Ulrich Drepper et al

BIND-8.2.3-T5B

RT using linux kernel aio

For bug reporting instructions, please see:

<http://www.gnu.org/software/libc/bugs.html>.

在某些Linux发行版中，GNU C库没有安装在/lib/libc.so.6路径下。有一个方法可以确定库的位置，就是对一个链接到glibc的可执行程序（多数可执行程序都会链接），运行ldd（列出动态依赖）命令。然后我们就可以从库依赖列表中找到glibc共享库：

$ ldd myprog | grep libc

libc.so.6 => /lib/tls/libc.so.6 (0x4004b000)

应用程序有两个办法可以确定GNU C库的版本：测试常量宏；或调用一个库函数。从2.0版本开始，glibc定义了两个常量：\_\_GLIBC\_\_和\_\_GLIBC\_MINOR\_\_，可以用来在编译时使用（#ifdef语句）。在安装了glibc 2.12的系统中，这两个常量的值是2和12。但是这些常量的作用有限，因为某个程序可以在这个系统编译，但拿到另一个系统去运行，两个系统安装了不同版本的glibc。为了处理这个可能性，程序可以调用gnu\_get\_libc\_version()函数来确定系统当前使用的glibc的版本。

|  |
| --- |
| #include <gnu/libc-version.h>  const char \*gnu\_get\_libc\_version(void);  返回一个null结尾的静态字符串，包含GNU C库版本号 |

gnu\_get\_libc\_version()函数返回一个字符串指针，例如”2.12”。

我们还可以使用confstr()函数得到\_CS\_GNU\_LIBC\_VERSION配置的值来获得版本信息。这个调用返回“glibc 2.12”形式的字符串。

## 3.4 系统调用和库函数的错误处理

几乎每个系统调用和库函数都会返回一个状态值，表示调用成功或失败。我们应该检查这个状态值来查看调用是否成功。如果调用失败了，就采取适当的措施——至少程序应该显示错误消息，警告发生了未预料的错误。

尽管为了节省打字时间，我们经常受诱惑而忽略这些检查（特别是许多UNIX和Linux例子程序都不检查返回值），这是负经济的作法。因为有时候我们没有对一个“不太可能失败”的系统调用检查返回值，结果就是浪费许多小时用于调试错误。

少数几个系统调用确实永远不会失败。例如getpid()总是会成功地返回进程ID，\_exit()总是会终止一个进程。这种系统调用的返回值就不需要检查啦。

**处理系统调用错误**

每个系统调用的手册页都注明了可能的返回值，并显示哪些返回值表示错误。通常-1表示错误，因此可以用以下代码检查系统调用的返回值：

fd = open(pathname, flags, mode); /\* system call to open a file \*/

if (fd == -1) {

/\* Code to handle the error \*/

}

...

if (close(fd) == -1) {

/\* Code to handle the error \*/

}

当系统调用失败时，它设置全局整型变量errno为一个正数值，标识具体发生的错误。包含<errno.h>头文件来提供errno的定义，以及许多错误数值的常量定义。所有错误的符号名都以E开头。每个手册页的ERRORS节列出了该系统调用可能的errno值。下面是一个简单的例子，使用errno来诊断系统调用错误：

cnt = read(fd, buf, numbytes);

if (cnt == -1) {

if (errno == EINTR)

fprintf(stderr, "read was interrupted by a signal\n");

else {

/\* Some other error occurred \*/

}

}

系统调用和库函数成功时不会重置errno为0，因此如果之前的调用出现了错误，这个值会被设为非0值并保持到下次出错。此外SUSv3甚至还允许成功的函数调用设置errno为非0值（很少函数这样做）。因此当检查错误时，我们应该首先检查函数返回值是否表示出错，然后才检查errno来确定具体的错误原因。

少数系统调用（如getpriority()）成功时返回-1是合理的。要确定这种调用是否发生错误，我们需要在调用前设置errno为0，调用完成后再检查errno值。如果调用返回-1并且errno非0，就发生了错误（有些库函数也是这样）。

系统调用失败后的常见动作是根据errno值打印一条错误消息。perror()和strerror()库函数提供了这个功能。

perror()函数打印msg参数指向的字符串，紧跟着打印对应于当前errno值的错误消息。

|  |
| --- |
| #include <stdio.h>  void perror(const char \*msg); |

处理系统调用失败的最简单方法如下：

fd = open(pathname, flags, mode);

if (fd == -1) {

perror("open");

exit(EXIT\_FAILURE);

}

strerror()函数返回errnum参数指定的错误值相对应的错误字符串。

|  |
| --- |
| #include <string.h>  char \*strerror(int errnum);  返回对应于errnum的错误字符串 |

strerror()返回的字符串可能是静态分配的，这意味着它的值可能会被随后的strerror()调用覆盖。

如果errnum指定了不被认可的错误数值，strerror()返回一个字符串“Unknown error nnn”。在某些其它实现中，strerror()在这种情况下返回NULL。

由于perror()和strerror()函数是区域敏感的（10.4节），错误描述会按本地语言显示出来。

**处理库函数错误**

不同的库函数返回不同的数据类型，并且以不同的值表示错误。（查看每个函数的手册页）。按我们的想法，库函数可以划分为以下几类：

* 有些库函数采用系统调用一样的方式返回错误：-1返回值，并设置errno来指示错误。例如remove()函数，用来移除一个文件（使用unlink()系统调用）或目录（使用rmdir()系统调用）。这类库函数的错误处理和系统调用的错误处理一样。
* 有些库函数返回其它值表示错误，并且也设置errno来指示特定的错误。例如fopen()返回NULL指针表示出错，并根据底层系统调用错误来设置errno的值。perror()和strerror()函数可以用来诊断这种错误。
* 其它库函数完全不使用errno。这种函数的错误诊断和处理要根据该函数的手册页描述来进行。对于这一类型的函数，使用errno, perror(), strerror()来诊断错误是不行的。

## 3.5 本书示例程序的说明

在这一节中，我们描述本书示例程序经常采用的惯例和特性。

### 3.5.1 命令行选项和参数

本书的许多示例程序依赖于命令行选项和参数，来确定自己的行为。

传统的UNIX命令行选项包括一个起始连字符，一个字母标识选项，以及一个可选的参数。（GNU实用工具提供一个扩展的选项语法，包括两个起始连字符，紧跟一个字符串标识选项，以及可选的参数）。要解析命令行选项，我们使用标准的getopt()库函数（附录B描述）。

我们的每个有命令行选项的示例程序，都为用户提供了一个简单的帮助机制：如果以--help选项调用，程序会显示命令行选项和参数的使用信息。

### 3.5.2 常用函数和头文件

多数示例程序都包含了同一个头文件，该文件包含常用的定义，以及一组常用的函数。我们在这一节讨论头文件和函数。

**常用头文件**

清单3-1是本书几乎所有程序都要使用的头文件。这个头文件包含了许多其它头文件，提供给许多示例程序使用，定义了一个Boolean数据类型，定义了计算最小和最大值的宏。使用这个头文件，我们的示例程序会更加短小简洁。

*清单3-1：多数示例程序使用的头文件*

----------------------------------------------------------------------------------------- lib/tlpi\_hdr.h

#ifndef TLPI\_HDR\_H

#define TLPI\_HDR\_H /\* Prevent accidental double inclusion \*/

#include <sys/types.h> /\* Type definitions used by many programs \*/

#include <stdio.h> /\* Standard I/O functions \*/

#include <stdlib.h> /\* Prototypes of commonly used library functions,

plus EXIT\_SUCCESS and EXIT\_FAILURE constants \*/

#include <unistd.h> /\* Prototypes for many system calls \*/

#include <errno.h> /\* Declares errno and defines error constants \*/

#include <string.h> /\* Commonly used string-handling functions \*/

#include "get\_num.h" /\* Declares our functions for handling numeric

arguments (getInt(), getLong()) \*/

#include "error\_functions.h" /\* Declares our error-handling functions \*/

typedef enum { FALSE, TRUE } Boolean;

#define min(m,n) ((m) < (n) ? (m) : (n))

#define max(m,n) ((m) > (n) ? (m) : (n))

#endif

----------------------------------------------------------------------------------------- lib/tlpi\_hdr.h

**错误诊断函数**

为了简化示例程序的错误处理，我们使用错误诊断函数，如清单3-2所示：

*清单3-2：常用错误处理函数声明*

---------------------------------------------------------------------------------- lib/error\_functions.h

#ifndef ERROR\_FUNCTIONS\_H

#define ERROR\_FUNCTIONS\_H

void errMsg(const char \*format, ...);

#ifdef \_\_GNUC\_\_

/\* This macro stops 'gcc -Wall' complaining that "control reaches

end of non-void function" if we use the following functions to

terminate main() or some other non-void function. \*/

#define NORETURN \_\_attribute\_\_ ((\_\_noreturn\_\_))

#else

#define NORETURN

#endif

void errExit(const char \*format, ...) NORETURN ;

void err\_exit(const char \*format, ...) NORETURN ;

void errExitEN(int errnum, const char \*format, ...) NORETURN ;

void fatal(const char \*format, ...) NORETURN ;

void usageErr(const char \*format, ...) NORETURN ;

void cmdLineErr(const char \*format, ...) NORETURN ;

#endif

---------------------------------------------------------------------------------- lib/error\_functions.h

要诊断系统调用和库函数的错误，我们使用errMsg(), errExit(), err\_exit(), 和errExitEN()。

|  |
| --- |
| #include "tlpi\_hdr.h"  void errMsg(const char \*format, ...);  void errExit(const char \*format, ...);  void err\_exit(const char \*format, ...);  void errExitEN(int errnum, const char \*format, ...); |

errMsg()函数向标准错误打印一条消息。它的参数列表和printf()是一样的，除了errMsg()会自动添加一个换行字符到输出字符串中。errMsg()函数打印当前errno错误值对应的错误信息，包括错误名字，如EPERM；加上strerror()返回的错误描述；再随后是参数列表格式化后的输出字符串。

errExit()函数和errMsg()类似，但同时还会终止程序，它调用了exit()，或者如果环境变量EF\_DEMPCORE设置为非空字符串，会调用abort()来产生一个core dump文件，以便于调试（22.1节解释core dump文件）。

err\_exit()函数类似于errExit()，但有以下两个区别：

* 它在打印错误消息之前不冲洗标准输出。
* 它通过\_exit()而不是exit()终止进程。这样会使进程不冲洗stdio缓冲区，也不调用退出处理器，直接终止进程。

err\_exit()的区别的细节到第25章就会变得清晰，我们在那里会讨论\_exit()和exit()的区别，以及子进程如何对待stdio缓冲区和退出处理器。现在我们只说明一点，父进程出现错误需要终止时，不应该冲洗子进程的stdio拷贝，也不应该调用exit处理器，这时候使用err\_exit()就非常有用了。

errExitEN()函数和errExit()函数是相同的，但是它不打印当前errno错误对应的错误消息，它打印errnum指定的错误对应的错误消息。

我们主要在采用POSIX线程API的程序中使用errExitEN()。和传统UNIX系统调用不一样（返回-1表示错误），POSIX线程函数通过返回错误数值来诊断错误（POSIX线程函数返回0表示成功）。

我们可以使用下面代码来诊断POSIX线程函数：

errno = pthread\_create(&thread, NULL, func, &arg);

if (errno != 0)

errExit("pthread\_create");

但是这样做不高效，因为errno宏在多线程环境下会扩展为一个函数调用，并且返回一个可以修改的左值。因此第次使用errno都会引起函数调用。errExitEN()函数允许我们编写更加高效地错误处理代码，等价于上面代码：

int s;

s = pthread\_create(&thread, NULL, func, &arg);

if (s != 0)

errExitEN(s, "pthread\_create");

要诊断其它类型的错误，我们使用fatal(), usageErr(), 和cmdLineErr()。

|  |
| --- |
| #include "tlpi\_hdr.h"  void fatal(const char \*format, ...);  void usageErr(const char \*format, ...);  void cmdLineErr(const char \*format, ...); |

fatal()函数用来诊断通用错误，包括不设置errno的库函数。它的参数列表和printf()一样，除了它也会在输出末尾自动添加换行字符。它打印格式化后的输出到标准错误，然后和errExit()一样终止程序。

usageErr()函数用来诊断命令行参数用法的错误。它的参数也和printf()一样，并且打印字符串Usage: 然后是格式化后的输出文本到标准错误，最后通过调用exit()来终止程序。（有些示例程序提供扩展的usageErr()函数，命名为usageError()）。

cmdLineErr()函数类似于usageErr()，但是只用在命令行参数诊断中。

我们的错误诊断函数实现如清单3-3所示：

*清单3-3：所有示例程序使用的错误处理函数*

---------------------------------------------------------------------------------- lib/error\_functions.c

#include <stdarg.h>

#include "error\_functions.h"

#include "tlpi\_hdr.h"

#include "ename.c.inc" /\* Defines ename and MAX\_ENAME \*/

#ifdef \_\_GNUC\_\_

\_\_attribute\_\_ ((\_\_noreturn\_\_))

#endif

static void

terminate(Boolean useExit3)

{

char \*s;

/\* Dump core if EF\_DUMPCORE environment variable is defined and

is a nonempty string; otherwise call exit(3) or \_exit(2),

depending on the value of 'useExit3'. \*/

s = getenv("EF\_DUMPCORE");

if (s != NULL && \*s != '\0')

abort();

else if (useExit3)

exit(EXIT\_FAILURE);

else

\_exit(EXIT\_FAILURE);

}

static void

outputError(Boolean useErr, int err, Boolean flushStdout,

const char \*format, va\_list ap)

{

#define BUF\_SIZE 500

char buf[BUF\_SIZE], userMsg[BUF\_SIZE], errText[BUF\_SIZE];

vsnprintf(userMsg, BUF\_SIZE, format, ap);

if (useErr)

snprintf(errText, BUF\_SIZE, " [%s %s]",

(err > 0 && err <= MAX\_ENAME) ?

ename[err] : "?UNKNOWN?", strerror(err));

else

snprintf(errText, BUF\_SIZE, ":");

snprintf(buf, BUF\_SIZE, "ERROR%s %s\n", errText, userMsg);

if (flushStdout)

fflush(stdout); /\* Flush any pending stdout \*/

fputs(buf, stderr);

fflush(stderr); /\* In case stderr is not line-buffered \*/

}

void

errMsg(const char \*format, ...)

{

va\_list argList;

int savedErrno;

savedErrno = errno; /\* In case we change it here \*/

va\_start(argList, format);

outputError(TRUE, errno, TRUE, format, argList);

va\_end(argList);

errno = savedErrno;

}

void

errExit(const char \*format, ...)

{

va\_list argList;

va\_start(argList, format);

outputError(TRUE, errno, TRUE, format, argList);

va\_end(argList);

terminate(TRUE);

}

void

err\_exit(const char \*format, ...)

{

va\_list argList;

va\_start(argList, format);

outputError(TRUE, errno, FALSE, format, argList);

va\_end(argList);

terminate(FALSE);

}

void

errExitEN(int errnum, const char \*format, ...)

{

va\_list argList;

va\_start(argList, format);

outputError(TRUE, errnum, TRUE, format, argList);

va\_end(argList);

terminate(TRUE);

}

void

fatal(const char \*format, ...)

{

va\_list argList;

va\_start(argList, format);

outputError(FALSE, 0, TRUE, format, argList);

va\_end(argList);

terminate(TRUE);

}

void

usageErr(const char \*format, ...)

{

va\_list argList;

fflush(stdout); /\* Flush any pending stdout \*/

fprintf(stderr, "Usage: ");

va\_start(argList, format);

vfprintf(stderr, format, argList);

va\_end(argList);

fflush(stderr); /\* In case stderr is not line-buffered \*/

exit(EXIT\_FAILURE);

}

void

cmdLineErr(const char \*format, ...)

{

va\_list argList;

fflush(stdout); /\* Flush any pending stdout \*/

fprintf(stderr, "Command-line usage error: ");

va\_start(argList, format);

vfprintf(stderr, format, argList);

va\_end(argList);

fflush(stderr); /\* In case stderr is not line-buffered \*/

exit(EXIT\_FAILURE);

}

---------------------------------------------------------------------------------- lib/error\_functions.c

enames.c.inc文件如清单3-4所示。这个文件定义了一个字符串数组ename，是每个可能的errno值对应的符号名。我们的错误处理函数使用这个数组来打印出某个错误数值对应的符号名。这是由于strerror()并不打印错误的符号常量名。打印出符号名让我们可以更加容易地在手册页中找到错误原因。

注意ename数组的某些字符串是空的，对应的是那些未使用的错误值。此外有些字符串包含两个名字并用斜线分开，这对应于那些两个符号名拥有相同的错误数值。

*清单3-4：Linux错误名（x86-32版）*

---------------------------------------------------------------------------------- lib/ename.c.inc

static char \*ename[] = {

/\* 0 \*/ "",

/\* 1 \*/ "EPERM", "ENOENT", "ESRCH", "EINTR", "EIO", "ENXIO", "E2BIG",

/\* 8 \*/ "ENOEXEC", "EBADF", "ECHILD", "EAGAIN/EWOULDBLOCK", "ENOMEM",

/\* 13 \*/ "EACCES", "EFAULT", "ENOTBLK", "EBUSY", "EEXIST", "EXDEV",

/\* 19 \*/ "ENODEV", "ENOTDIR", "EISDIR", "EINVAL", "ENFILE", "EMFILE",

/\* 25 \*/ "ENOTTY", "ETXTBSY", "EFBIG", "ENOSPC", "ESPIPE", "EROFS",

/\* 31 \*/ "EMLINK", "EPIPE", "EDOM", "ERANGE", "EDEADLK/EDEADLOCK",

/\* 36 \*/ "ENAMETOOLONG", "ENOLCK", "ENOSYS", "ENOTEMPTY", "ELOOP", "",

/\* 42 \*/ "ENOMSG", "EIDRM", "ECHRNG", "EL2NSYNC", "EL3HLT", "EL3RST",

/\* 48 \*/ "ELNRNG", "EUNATCH", "ENOCSI", "EL2HLT", "EBADE", "EBADR",

/\* 54 \*/ "EXFULL", "ENOANO", "EBADRQC", "EBADSLT", "", "EBFONT", "ENOSTR",

/\* 61 \*/ "ENODATA", "ETIME", "ENOSR", "ENONET", "ENOPKG", "EREMOTE",

/\* 67 \*/ "ENOLINK", "EADV", "ESRMNT", "ECOMM", "EPROTO", "EMULTIHOP",

/\* 73 \*/ "EDOTDOT", "EBADMSG", "EOVERFLOW", "ENOTUNIQ", "EBADFD",

/\* 78 \*/ "EREMCHG", "ELIBACC", "ELIBBAD", "ELIBSCN", "ELIBMAX",

/\* 83 \*/ "ELIBEXEC", "EILSEQ", "ERESTART", "ESTRPIPE", "EUSERS",

/\* 88 \*/ "ENOTSOCK", "EDESTADDRREQ", "EMSGSIZE", "EPROTOTYPE",

/\* 92 \*/ "ENOPROTOOPT", "EPROTONOSUPPORT", "ESOCKTNOSUPPORT",

/\* 95 \*/ "EOPNOTSUPP/ENOTSUP", "EPFNOSUPPORT", "EAFNOSUPPORT",

/\* 98 \*/ "EADDRINUSE", "EADDRNOTAVAIL", "ENETDOWN", "ENETUNREACH",

/\* 102 \*/ "ENETRESET", "ECONNABORTED", "ECONNRESET", "ENOBUFS", "EISCONN",

/\* 107 \*/ "ENOTCONN", "ESHUTDOWN", "ETOOMANYREFS", "ETIMEDOUT",

/\* 111 \*/ "ECONNREFUSED", "EHOSTDOWN", "EHOSTUNREACH", "EALREADY",

/\* 115 \*/ "EINPROGRESS", "ESTALE", "EUCLEAN", "ENOTNAM", "ENAVAIL",

/\* 120 \*/ "EISNAM", "EREMOTEIO", "EDQUOT", "ENOMEDIUM", "EMEDIUMTYPE",

/\* 125 \*/ "ECANCELED", "ENOKEY", "EKEYEXPIRED", "EKEYREVOKED",

/\* 129 \*/ "EKEYREJECTED", "EOWNERDEAD", "ENOTRECOVERABLE", "ERFKILL"

};

#define MAX\_ENAME 132

---------------------------------------------------------------------------------- lib/ename.c.inc

**解析数字命令行参数的函数**

清单3-5中的头文件提供了两个函数的声明，这两个函数被用来解析命令行参数的整数值：getInt()和getLong()。使用这些函数而不是atoi(), atol()和strtol()的主要优点是它们提供数值参数的基本验证检查功能。

|  |
| --- |
| #include "tlpi\_hdr.h"  int getInt(const char \*arg, int flags, const char \*name);  long getLong(const char \*arg, int flags, const char \*name);  都返回arg转化为数值形式 |

getInt()和getLong()函数把字符串arg转化为int或long。如果arg不包含合法的整数字符串（只有数字和+-），则这些函数会打印一条错误消息，并终止程序。

如果name参数非NULL，它会包含一个字符串标识arg中的参数。这个字符串被包含在这些函数的错误消息显示中。

flags参数提供getInt()和getLong()函数的某些控制功能。默认这些函数都认为字符串包含带符号十进制整数。通过“|”一个或多个清单3-5中的GN\_\*常量到flags中，我们可以选择其它进制，也可以限制数值的范围非负或大于0。

getInt()和getLong()函数的实现如清单3-6。

*清单3-5：get\_num.c的头文件*

---------------------------------------------------------------------------------- lib/get\_num.h

#ifndef GET\_NUM\_H

#define GET\_NUM\_H

#define GN\_NONNEG 01 /\* Value must be >= 0 \*/

#define GN\_GT\_0 02 /\* Value must be > 0 \*/

/\* By default, integers are decimal \*/

#define GN\_ANY\_BASE 0100 /\* Can use any base - like strtol(3) \*/

#define GN\_BASE\_8 0200 /\* Value is expressed in octal \*/

#define GN\_BASE\_16 0400 /\* Value is expressed in hexadecimal \*/

long getLong(const char \*arg, int flags, const char \*name);

int getInt(const char \*arg, int flags, const char \*name);

#endif

---------------------------------------------------------------------------------- lib/get\_num.h

*清单3-6：命令行数值参数解析函数*

---------------------------------------------------------------------------------- lib/get\_num.c

#include <stdio.h>

#include <stdlib.h>

#include <string.h>

#include <limits.h>

#include <errno.h>

#include "get\_num.h"

static void

gnFail(const char \*fname, const char \*msg, const char \*arg, const char \*name)

{

fprintf(stderr, "%s error", fname);

if (name != NULL)

fprintf(stderr, " (in %s)", name);

fprintf(stderr, ": %s\n", msg);

if (arg != NULL && \*arg != '\0')

fprintf(stderr, " offending text: %s\n", arg);

exit(EXIT\_FAILURE);

}

static long

getNum(const char \*fname, const char \*arg, int flags, const char \*name)

{

long res;

char \*endptr;

int base;

if (arg == NULL || \*arg == '\0')

gnFail(fname, "null or empty string", arg, name);

base = (flags & GN\_ANY\_BASE) ? 0 : (flags & GN\_BASE\_8) ? 8 :

(flags & GN\_BASE\_16) ? 16 : 10;

errno = 0;

res = strtol(arg, &endptr, base);

if (errno != 0)

gnFail(fname, "strtol() failed", arg, name);

if (\*endptr != '\0')

gnFail(fname, "nonnumeric characters", arg, name);

if ((flags & GN\_NONNEG) && res < 0)

gnFail(fname, "negative value not allowed", arg, name);

if ((flags & GN\_GT\_0) && res <= 0)

gnFail(fname, "value must be > 0", arg, name);

return res;

}

long

getLong(const char \*arg, int flags, const char \*name)

{

return getNum("getLong", arg, flags, name);

}

int

getInt(const char \*arg, int flags, const char \*name)

{

long res;

res = getNum("getInt", arg, flags, name);

if (res > INT\_MAX || res < INT\_MIN)

gnFail("getInt", "integer out of range", arg, name);

return (int) res;

}

---------------------------------------------------------------------------------- lib/get\_num.c

## 3.6 可移植问题

在这一节，我们讨论编写可移植系统程序的主题。介绍SUSv3定义的特性测试宏和标准系统数据类型，然后再查看其它一些可移植问题。

### 3.6.1 特性测试宏

许多标准支配着系统调用和库函数API的行为（1.3节）。其中一些标准由标准组织如开放组织（Single UNIX规范）定义，另一些则由两个历史上重要的UNIX实现定义：BSD和System V Release 4（以及System V接口定义）。

有时候当编写可移植程序时，我们可能希望头文件只暴露特定标准的定义（常量、函数原型等）。我们可以在编译程序时定义一个或多个特性测试宏，来实现这个功能。我们在包含任何其它头文件之前定义这些宏：

#define \_BSD\_SOURCE 1

或者也可以使用C编译器的-D选项：

$ cc -D\_BSD\_SOURCE prog.c

下面的特性测试宏由相关标准规定，因此在支持这些标准的所有系统中使用它们是可移植的：

\_POSIX\_SOURCE

如果定义了（无论什么值），暴露POSIX.1-1990和ISO C（1990）标准的定义，这个宏已经被\_POSIX\_C\_SOURCE取代。

\_POSIX\_C\_SOURCE

如果定义为1，和\_POSIX\_SOURCE的效果相同。如果定义为大于或等于199309，同时还暴露POSIX.1b（实时）定义。如果定义为大于或等于199506，还暴露POSIX.1c（线程）定义。如果定义为值200112，同时还暴露POSIX.1-2001基础规范定义（不包括XSI扩展）。（glibc 2.3.3之前的版本，不把200112解释为\_POSIX\_C\_SOURCE）如果定义为值200809，还暴露POSIX.1-20008基础规范（glibc 2.10版本之前不能解释200809值）。

\_XOPEN\_SOURCE

如果定义（任何值），暴露POSIX.1, POSIX.2, 和X/Open（XPG4）定义。如果定义为500或更大，还暴露SUSv2（UNIX98和XPG5）扩展。设置为600或更高，额外地暴露SUSv3 XSI（UNIX03）扩展和C99扩展。（glibc 2.2以前无法解释600值的\_XOPEN\_SOURCE）设置为700或更高，还同时暴露SUSv4 XSI扩展。（glibc 2.10之前无法解释\_XOPEN\_SOURCE为700）。500，600和700分别对应于SUSv2，SUSv3和SUSv4，分别由于X/Open规范的Issues 5，6和7而得名。

下面这些特性测试宏是glibc专有的：

\_BSD\_SOURCE

如果定义（任何值），暴露BSD定义。定义这个宏同时也定义\_POSIX\_C\_SOURCE的值为199506。显式地设置这个宏，当标准冲突时，会优先选择BSD定义。

\_SVID\_SOURCE

如果定义（任何值）。暴露System V接口定义（SVID）。

\_GNU\_SOURCE

如果定义（任何值），暴露前面所有宏提供的所有定义，以及许多GNU扩展。

当GNU C编译器不带特殊选项调用时，默认会定义：\_POSIX\_SOURCE，\_POSIX\_C\_SOURCE = 200809（glibc 2.5到2.9是200112，glibc 2.4及更早是199506），\_BSD\_SOURCE，和\_SVID\_SOURCE。

如果定义了某个宏，或者编译器按标准模式调用（cc -ansi或cc -std=c99），则只提供请求的定义。有一个例外：如果\_POSIX\_C\_SOURCE没有定义，并且编译器不以标准模式调用，则\_POSIX\_C\_SOURCE被定义200809（或者上面所说的更早版本）。

定义多个宏是附加的，因此我们可以使用下面cc命令来显式地选择默认的宏设置：

$ cc -D\_POSIX\_SOURCE -D\_POSIX\_C\_SOURCE=199506 \

-D\_BSD\_SOURCE -D\_SVID\_SOURCE prog.c

<features.h>头文件和feature\_test\_macros(7)手册页提供了更多信息，关于每个特性测试宏精确的数值及含义。

**\_POSIX\_C\_SOURCE、\_XOPEN\_SOURCE、和POSIX.1/SUS**

POSIX.1-2001/SUSv3只规定了\_POSIX\_C\_SOURCE和\_XOPEN\_SOURCE两个特性测试宏，并要求依从标准的应用分别把它们的值定义为200112和600。定义\_POSIX\_C\_SOURCE为200112表示依从POSIX.1-2001基础规范（依从POSIX，但不包括XSI扩展）。定义\_XOPEN\_SOURCE为600则表示依从SUSv3（XSI依从，基础规范加XSI扩展）。类似的描述也适用于POSIX.1-2008/SUSv4，后者要求这两个宏的值分别定义为200809和700。

SUSv3规定设置\_XOPEN\_SOURCE为600时，同时也应该提供\_POSIX\_C\_SOURCE设置为200112的所有特性。因此应用依从SUSv3（XSI）只需要设置\_XOPEN\_SOURCE。SUSv4也做了类似的规定，设置\_XOPEN\_SOURCE为700时也提供\_POSIX\_C\_SOURCE设置为200809的所有特性。

**函数原型和示例源代码中的特性测试宏**

手册页描述了要使特定常量定义或函数声明在头文件中可见，必须要设置的特性测试宏。

本书的所有示例源代码都编写成可以使用默认GNU C编译器选项或如下选项进行编译：

$ cc -std=c99 -D\_XOPEN\_SOURCE=600

本书中的每个函数原型都表示使用默认编译器选项或上面cc命令可以编译。手册页提供了每个函数定义需要的特性测试宏的更多精确描述。

### 3.6.2 系统数据类型

许多数据类型的实现都使用标准C类型来表示，例如进程ID、用户ID、和文件偏移量等。虽然直接使用C基本类型（如int和long）来声明变量也可以，但这样做会降低跨UNIX系统的可移植性，原因如下：

* 基本类型的大小在不同UNIX实现中是不一样的（例如long可能是4个字节，也可能是8字节）。甚至相同UNIX系统的不同编译环境下类型大小也不一样。此外不同的实现可能使用不同的类型来表示相同的数据。例如进程ID在某个系统可能是int，但在另一个系统却可能是long。
* 即使在单一的UNIX实现中，不同版本用来表示某个数据的类型也可能不一样。显著的例子是Linux中的用户和组ID，在Linux 2.2和更早的版本，这些值以16位表示，但在Linux 2.4及后面版本，它们却是32位的值。

为了避免这样的可移植问题，SUSv3规定了许多标准系统数据类型，并要求UNIX实现正确地定义和使用这些类型。

每个类型都使用C语言的typedef特性定义。例如pid\_t数据类型用来表示进程ID，在Linux/x86-32下这个类型如下定义：

typedef int pid\_t;

多数标准系统数据类型的名字都以“\_t”结尾，而且多数定义在头文件<sys/types.h>中，少数其它则定义在另外的头文件中。

应用应该使用这些类型定义，来可移植地声明这些变量。例如下面声明允许应用在所有SUSv3依从的系统中正确地表示进程ID：

pid\_t mypid;

表3-1列出了我们在本书中会遇到的一些系统数据类型。对于表中某些类型，SUSv3要求类型实现为“算术”类型。这意味着实现可以选择整数或浮点数（实数或复数）作为底层类型。

*表3-1：部分系统数据类型*

|  |  |  |
| --- | --- | --- |
| **数据类型** | **SUSv3类型要求** | **描述** |
| blkcnt\_t | 带符号整数 | 文件块计数（15.1节） |
| blksize\_t | 带符号整数 | 文件块大小（15.1节） |
| cc\_t | 无符号整数 | 终端特殊字符（62.4节） |
| clock\_t | 整数或浮点 | 系统时间时钟滴答（10.7节） |
| clockid\_t | 算术类型 | POSIX.1b时钟和定时器函数的时钟标识符（23.6节） |
| comp\_t | SUSv3无定义 | 压缩的时钟滴答（28.1节） |
| dev\_t | 算术类型 | 设备数字，包括主和副数字（15.1节） |
| DIR | 无类型要求 | 目录流（18.8节） |
| fd\_set | 结构体类型 | select()的文件描述符集（63.2.1节） |
| fsblkcnt\_t | 无符号整数 | 文件系统块计数（14.11节） |
| fsfilcnt\_t | 无符号整数 | 文件计数（14.11节） |
| gid\_t | 整数 | 数字的组标识符（8.3节） |
| id\_t | 整数 | 保存标识符的通用类型；至少足够大保存pid\_t, uid\_t, gid\_t |
| in\_addr\_t | 32位无符号整数 | IPv4地址（59.4节） |
| in\_port\_t | 16位无符号整数 | IP端口号（59.4节） |
| ino\_t | 无符号整数 | 文件i-node数值（15.1节） |
| key\_t | 算术类型 | System V IPC键（45.2节） |
| mode\_t | 整数 | 文件权限和类型（15.1节） |
| mqd\_t | 无类型要求，但不能是数组类型 | POSIX消息队列描述符 |
| msglen\_t | 无符号整数 | System V消息队列允许的字节数（46.4节） |
| msgqnum\_t | 无符号整数 | System V消息队列消息计数（46.4节） |
| nfds\_t | 无符号整数 | poll()的文件描述符数量（63.2.2节） |
| nlink\_t | 整数 | 某个文件的硬链接计数（15.1节） |
| off\_t | 带符号整数 | 文件偏移量或大小（4.7和15.1节） |
| pid\_t | 带符号整数 | 进程ID，进程组ID，会话ID（6.2、34.2、34.3节） |
| ptrdiff\_t | 带符号整数 | 两个指针的差 |
| rlim\_t | 无符号整数 | 资源限制（36.2节） |
| sa\_family\_t | 无符号整数 | socket地址家族（56.4节） |
| shmatt\_t | 无符号整数 | System V共享内存段的连接进程计数（48.8节） |
| sig\_atomic\_t | 整数 | 可以被原子访问的数据类型（21.1.3节） |
| siginfo\_t | 结构体类型 | 信号来源相关的信息（21.4节） |
| sigset\_t | 整数或结构体类型 | 信号集（20.9节） |
| size\_t | 无符号整数 | 对象的字节大小 |
| socklen\_t | 至少32位整数类型 | socket地址结构体的字节大小（56.3节） |
| speed\_t | 无符号整数 | 终端行速度（62.7节） |
| ssize\_t | 带符号整数 | 字节大小或指示错误 |
| stack\_t | 结构体类型 | 可选信号堆栈的描述（21.3节） |
| suseconds\_t | 带符号整数，允许范围[-1，1000000] | 微秒的时间间隔（10.1节） |
| tcflag\_t | 无符号整数 | 终端模式标志位掩码（62.2节） |
| time\_t | 整数或浮点 | 日历时间，从Epoch开始的秒数（10.1节） |
| timer\_t | 算术类型 | POSIX.1b时间函数定时器标识符（23.6节） |
| uid\_t | 整数 | 数值的用户标识符（8.1节） |

我们在后面讨论表3-1中的数据类型时，通常会说“[SUSv3规定]某个类型是整数类型”。这意味着SUSv3要求这个类型定义为整数，但并没有要求特定的本地整数类型（如short, int, long等）。（通常我们不关心Linux到底使用什么本地数据类型来表示标准系统数据类型，因为可移植应用不应该依赖于此）。

**打印系统数据类型的值**

当我们要打印表3-1中系统数据类型的数值时（如pid\_t和uid\_t），我们必须小心不要在printf()中引入表示依赖。表示依赖的存在是由于C参数提升规则，会把short值转化为int，但保持int和long类型参数不变。这意味着根据不同的系统数据类型，int或long会传递给printf()调用。但是由于printf()无法在运行时确定其参数类型，调用方必须使用%d或%ld格式说明符来显式提供类型信息。问题是简单地在printf()中指定说明符会引入表示依赖。通常的解决方案是使用%ld说明符并且总是把相应的值强制转化为long，如下：

pid\_t mypid;

mypid = getpid(); /\* Returns process ID of calling process \*/

printf("My PID is %ld\n", (long) mypid);

上面技术有一个例外。由于off\_t数据类型在某些编译环境下是long long，我们把off\_t的值转化为long long并且使用%lld说明符，5.10节会再加描述。

### 3.6.3 各种可移植问题

在这一节，我们来考虑编写系统程序时，可能遇到的其它一些可移植问题。

**初始化和使用结构体**

每个UNIX实现都指定了一组标准结构体，用在许多系统调用和库函数中。例如sembuf结构体，它用来描述semop()系统调用对信号量的操作：

struct sembuf {

unsigned short sem\_num; /\* Semaphore number \*/

short sem\_op; /\* Operation to be performed \*/

short sem\_flg; /\* Operation flags \*/

};

尽管SUSv3规定了结构体（如sembuf），但意识到下面两点是很重要的：

* 通常并没有规定结构体中域定义的顺序。
* 某些情况下，额外的实现特定域可能会添加到这类结构体中。

因此下面这样使用结构体初始化是不可移植的：

struct sembuf s = { 3, -1, SEM\_UNDO };

虽然这个初始化能够在Linux中工作，但其它实现中sembuf结构体的域定义顺序可能不同，这段代码将无法工作。要可移植地初始化结构体，我们必须显式地使用赋值语句，如下所示：

struct sembuf s;

s.sem\_num = 3;

s.sem\_op = -1;

s.sem\_flg = SEM\_UNDO;

如果你使用C99，那么可以采用结构体初始化的新语法来编写等价的初始化：

struct sembuf s = { .sem\_num = 3, .sem\_op = -1, .sem\_flg = SEM\_UNDO };

如果我们要把结构体的内容写到文件中，也需要考虑成员定义的顺序。为了实现可移植，我们不能简单地执行二进制写入。相反必须按特定顺序把结构体的域一个一个地写入到文件。

**使用不是所有实现都提供的宏**

某些情况下，可能不是所有UNIX实现都定义了某个宏。例如WCOREDUMP()宏（检查子进程是否产生了core dump文件）被广泛实现，但SUSv3却没有对其定义。因此这个宏可能在某些UNIX实现中不可用。为了处理这种可能性，我们可以使用C预处理器的#ifdef指令，如下面例子：

#ifdef WCOREDUMP

/\* Use WCOREDUMP() macro \*/

#endif

**跨实现所需头文件的差异**

在某些情况下，许多系统调用和库函数需要的头文件在不同UNIX实现上是不一样的。在本书中，我们会明确显示Linux和SUSv3的头文件要求。

本书的某些函数会包含一个特殊的头文件，伴随着注释/\* For portability \*/。这表示头文件不是Linux或SUSv3所要求，而是由于某些其它（特别是老的系统）实现要求包含它，为了可移植我们需要包含它。

## 3.7 小结

系统调用允许进程向内核请求服务。相比用户空间的函数调用，即使是最简单的系统调用也需要大量的开销，因为系统必须临时切换到内核模式来执行系统调用，内核必须验证系统调用参数，并在用户内存和内核内存间传输数据。

标准C库提供许多函数，完成各种各样的任务。某些库函数采用系统调用来完成自己的工作；其它则完全在用户空间中执行任务。在Linux中，常用的标准C库实现是glibc。

多数系统调用和库函数返回一个状态来表示调用是否成功。我们总是应该检查这个返回状态。

我们介绍了一组本书中使用的示例函数，这些函数执行的任务包括诊断错误和解析命令行参数。

我们讨论了许多能够帮助我们编写可移植系统程序的准则和技术。

当编译应用时，我们可以定义许多特性测试宏，来控制头文件暴露的定义。如果我们想确保程序依从于某个特定标准，特性测试宏就非常有用。

我们可以使用许多标准定义的系统数据类型，而不是系统本地C类型，来提高系统程序的可移植性。SUSv3规定了许多系统数据类型，各个UNIX实现都应该支持，应用程序也应该采用这些系统数据类型。

## 3.8 习题

3-1. 当使用Linux特定的reboot()系统调用来重启系统时，第二个参数magic2必须指定为某个魔法数字（例如LINUX\_REBOOT\_MAGIC2）。这些数字的意义是什么？（把它们转换为十六进制会提供线索）。

# 第4章 文件I/O：通用I/O模型

现在我们开始学习系统调用API最重要的部分之一。文件是很好的学习起点，因为它们是UNIX哲学的核心。本章关注于执行文件输入和输出的系统调用。

我们首先介绍文件描述符的概念，然后介绍构成通用I/O模型的系统调用。这些系统调用包括打开和关闭文件、读取和写入数据。

目前我们只关注于磁盘文件I/O。但是本章讲解的多数材料都可以应用于后续章节，因为相同的系统调用被用来执行所有文件类型的I/O操作，例如管道和终端。

第5章扩展了本章的讨论，提供更多文件I/O的细节。另外一个文件I/O的重要方面（缓冲），也值得拥有自己的一章，第13章讲解了内核和stdio库的缓冲机制。

## 4.1 概述

所有执行I/O的系统调用都需要使用文件描述符，后者的类型是非负整数（通常很小）。文件描述符用来引用所有类型的打开文件，包括管道、FIFO、socket、终端、设备、和普通文件。每个进程都有自己的一组文件描述符。

通常多数应用程序都希望能够使用表4-1所列的三个标准文件描述符。这三个描述符由shell在程序启动前自动打开；更精确地说，是程序继承了shell的文件描述符，而shell保持这三个文件描述符总是打开（在交互式shell中，这三个文件描述符通常指向shell正在运行的终端）。如果命令行指定了I/O重定向，则shell确保在程序启动之前相应地修改文件描述符。

*表4-1：标准文件描述符*

|  |  |  |  |
| --- | --- | --- | --- |
| **文件描述符** | **用途** | **POSIX名字** | **stdio流** |
| 0 | 标准输入 | STDIN\_FILENO | stdin |
| 1 | 标准输出 | STDOUT\_FILENO | stdout |
| 2 | 标准错误 | STDERR\_FILENO | stderr |

在程序中要引用这些文件描述符，可以直接使用数值（0，1，2），更好的做法是使用<unistd.h>定义的POSIX标准名字。

尽管变量stdin, stdout, stderr最初引用进程的标准输入、标准输出、标准错误，但是可以使用freopen()库函数把它们改为引用任何文件。freopen()在执行操作的同时，可能还会修改底层打开文件流的文件描述符。换句话说，比如对stdout执行freopen()之后，再假设底层的文件描述符还是1就不再是安全的了。

下面是执行文件I/O的四个关键系统调用（编程语言和软件包通常间接地通过I/O库来使用这些系统调用）：

* fd = open(pathname, flags, mode) 打开pathname指定的文件，它返回一个文件描述符，在随后的调用中引用这个已经打开的文件。如果文件不存在，open()可以创建它，根据flags掩码参数的设置而定。flags参数还指定了文件是打开读取、写入、还是二者均有。如果创建了一个新文件，mode参数指定该文件的权限。如果open()调用不创建文件，则忽略mode参数，可以省略。
* numread = read(fd, buffer, count) 最多从fd指向的文件中读取count字节，并存储读取的数据到buffer。read()调用返回实际读取的字节数。如果没有更多的字节可以读取（如遇到文件尾），read()返回0。
* numwrite = write(fd, buffer, count) 从buffer缓冲区中写入count字节到fd指向的文件。write()调用返回实际写入的字节数，可能小于count。
* status = close(fd) 在所有I/O操作结束之后调用，可以释放fd文件描述符以及相关的内核资源。

在我们深入这些系统调用的细节之前，先提供清单4-1中一个简短的演示。这个程序是cp命令的简单版本。它复制第一个参数指向的现有文件到第二个参数指向的新文件。

我们可以如下使用清单4-1的程序：

$ ./copy oldfile newfile

*清单4-1：使用I/O系统调用*

--------------------------------------------------------- fileio/copy.c

#include <sys/stat.h>

#include <fcntl.h>

#include "tlpi\_hdr.h"

#ifndef BUF\_SIZE /\* Allow "cc -D" to override definition \*/

#define BUF\_SIZE 1024

#endif

int

main(int argc, char \*argv[])

{

int inputFd, outputFd, openFlags;

mode\_t filePerms;

ssize\_t numRead;

char buf[BUF\_SIZE];

if (argc != 3 || strcmp(argv[1], "--help") == 0)

usageErr("%s old-file new-file\n", argv[0]);

/\* Open input and output files \*/

inputFd = open(argv[1], O\_RDONLY);

if (inputFd == -1)

errExit("opening file %s", argv[1]);

openFlags = O\_CREAT | O\_WRONLY | O\_TRUNC;

filePerms = S\_IRUSR | S\_IWUSR | S\_IRGRP | S\_IWGRP |

S\_IROTH | S\_IWOTH; /\* rw-rw-rw- \*/

outputFd = open(argv[2], openFlags, filePerms);

if (outputFd == -1)

errExit("opening file %s", argv[2]);

/\* Transfer data until we encounter end of input or an error \*/

while ((numRead = read(inputFd, buf, BUF\_SIZE)) > 0)

if (write(outputFd, buf, numRead) != numRead)

fatal("couldn't write whole buffer");

if (numRead == -1)

errExit("read");

if (close(inputFd) == -1)

errExit("close input");

if (close(outputFd) == -1)

errExit("close output");

exit(EXIT\_SUCCESS);

}

--------------------------------------------------------- fileio/copy.c

## 4.2 I/O的通用性

UNIX I/O模型的显著特性之一就是通用I/O的概念。这意味着相同的四个系统调用——open(), read(), write(), close()——用来执行所有文件类型的I/O操作，包括终端设备等。因此如果使用这些系统调用编写了一个程序，那这个程序对任何文件都是可以工作的。例如，下面都是清单4-1程序的合理用法：

$ ./copy test test.old 复制普通文件

$ ./copy a.txt /dev/tty 复制普通文件到终端

$ ./copy /dev/tty b.txt 复制终端输入到普通文件

$ ./copy /dev/pts/16 /dev/tty 复制另一个终端的输入

UNIX确保每种文件系统和设备驱动都实现了相同的I/O系统调用，来实现I/O的通用性。由于文件系统和设备的特定细节完全由内核处理，我们编写应用程序时可以忽略设备相关的因素。当需要访问文件系统或设备的特定特性时，可以使用ioctl()系统调用（4.8节），提供访问通用I/O模型之外特性的接口。

## 4.3 打开文件：open()

open()系统调用要么打开现有文件，要么打开一个新文件。

|  |
| --- |
| #include <sys/stat.h>  #include <fcntl.h>  int open(const char \*pathname, int flags, ... /\* mode\_t mode \*/);  成功时返回文件描述符，失败返回-1 |

要打开的文件由pathname参数指定。如果pathname是一个符号链表，那么首先会解引用（找到实际的文件）。成功时open()返回一个文件描述符，用来后续调用引用这个文件；如果发生错误，open()返回-1并设置errno为合适的值。

flags参数是一个位掩码，指定文件的访问模式，可以选择使用表4-2中的某个常量定义：

早期UNIX实现使用数字0，1，2而不是表4-2中显示的名字。多数现代UNIX实现都定义这些常量为这些值。因此我们可以认为O\_RDWR不同于O\_RDONLY | O\_WRONLY，后者的组合是一个逻辑错误。

*表4-2：文件访问模式*

|  |  |
| --- | --- |
| **访问模式** | **描述** |
| O\_RDONLY | 打开文件只能读取 |
| O\_WRONLY | 打开文件只能写入 |
| O\_RDWR | 打开文件同时读取和写入 |

当open()用来创建新文件时，mode位掩码参数指定文件的权限。（mode\_t数据类型在SUSv3中定义为整数类型）。如果open()调用不指定O\_CREAT，mode参数可以忽略。

我们会在后面15.4节详细地讨论文件权限，在那里我们会知道新文件的权限不仅仅依赖于mode参数，还同时依赖于进程的umask（15.4.6节），和父目录的默认访问控制列表（17.6节）。到那里，我们还会说明mode参数可以指定为数值（通常是八进制），或者使用表15-4所列常量掩码的“位或”。

清单4-2显示了使用open()的一个例子，使用了前面描述的flags位掩码：

*清单4-2：open()的使用例子*

-----------------------------------------------------------------------

/\* Open existing file for reading \*/

fd = open("startup", O\_RDONLY);

if (fd == -1)

errExit("open");

/\* Open new or existing file for reading and writing, truncating to zero

bytes; file permissions read+write for owner, nothing for all others \*/

fd = open("myfile", O\_RDWR | O\_CREAT | O\_TRUNC, S\_IRUSR | S\_IWUSR);

if (fd == -1)

errExit("open");

/\* Open new or existing file for writing; writes should always

append to end of file \*/

fd = open("w.log", O\_WRONLY | O\_CREAT | O\_TRUNC | O\_APPEND,

S\_IRUSR | S\_IWUSR);

if (fd == -1)

errExit("open");

-----------------------------------------------------------------------

**open()返回的文件描述符数值**

SUSv3规定如果open()成功，要确保使用进程未用文件描述符中最小数值的那个。我们可以使用这个特性来确保文件以某个特定的文件描述符打开。例如下面代码确保文件使用标准输入（文件描述符0）来打开：

if (close(STDIN\_FILENO) == -1) /\* Close file descriptor 0 \*/

errExit("close");

fd = open(pathname, O\_RDONLY);

if (fd == -1)

errExit("open");

由于文件描述符0没有被使用，open()确保使用这个描述符来打开文件。在5.5节，我们会使用dup2()和fcntl()来达到类似的结果，但对所用文件描述符拥有更加灵活的控制。在那一节里，我们还展示了一个例子，演示控制打开文件使用的文件描述符有什么用处。

### 4.3.1 open()的flags参数

在清单4-2某些open()的使用中，我们包含了文件访问模式之外的flags标志（O\_CREAT, O\_TRUNC, O\_APPEND）。下面我们来详细讨论flags参数。表4-3总结了flags可以“或”的所有常量定义，最后一列表示这些常量是否SUSv3或SUSv4标准定义。

*表4-3：open()调用flags参数的值*

|  |  |  |
| --- | --- | --- |
| **标志** | **作用** | **SUS?** |
| O\_RDONLY  O\_WRONLY  O\_RDWR | 打开为只能读取  打开为只能写入  打开为同时读写 | v3  v3  v3 |
| O\_CLOEXEC  O\_CREAT  O\_DIRECT  O\_DIRECTORY  O\_EXCL  O\_LARGEFILE  O\_NOATIME  O\_NOCTTY  O\_NOFOLLOW  O\_TRUNC | 设置“close-on-exec”标志（Linux 2.6.23开始）  如果文件不存在则创建  文件I/O绕过缓冲区缓存  如果pathname不是目录则失败  和O\_CREAT一起使用：创建唯一的文件  在32位系统中打开超大文件  read()时不更新文件的最后访问时间（Linux 2.6.8开始）  不让pathname成为控制终端  不解引用符号链接  截断现有文件为0长度 | v4  v3  v4  v3  v3  v4  v3 |
| O\_APPEND  O\_ASYNC  O\_DSYNC  O\_NONBLOCK  O\_SYNC | 写入总是追加至文件末尾  I/O可操作时产生一个信号  提供同步的I/O数据完整性（Linux 2.6.33开始）  非阻塞模式打开  使文件写入同步 | v3  v3  v3  v3 |

表4-3中的常量可以分为以下几组：

* **文件访问模式标志**：包括前面讨论过的O\_RDONLY, O\_WRONLY, 和O\_RDWR。可以使用fcntl()的F\_GETFL操作获得设置的值（5.3节）。
* **文件创建标志**：这些标志显示在表4-3的第二部分。它们控制open()调用的各种行为，以及控制随后进行的I/O操作的行为。这些标志不能修改也无法取得设置的值。
* **打开文件状态标志**：这些标志是表4-3最后那部分。它们可以使用fcntl()的F\_GETFL和F\_SETFL操作来获得和修改（5.3节）。这些标志有时候也简单地称为文件状态标志。

从内核2.6.22开始，目录/proc/PID/fdinfo下的Linux特定文件可以被读取，来获取系统中任何进程的文件描述符信息。进程的每个打开文件描述符在这个目录下都有一个文件，文件名就是描述符的数值。该文件中的pos域显示了当前文件偏移（4.7节）。flags域是一个八进制数字，显示了文件访问模式标志和打开文件状态标志。（要解码这个数字，我们需要查看C库头文件中这些标志的数值）。

flags常量的细节如下：

**O\_APPEND**

写入总是追加到文件末尾。我们在5.1节讨论这个标志的重要性。

**O\_ASYNC**

当文件描述符的I/O变得可操作时产生一个信号。这个特性叫做“信号驱动I/O”，只在某些文件类型中可用，例如终端、FIFO、和socket。（SUSv3没有规定O\_ASYNC标志，但多数UNIX实现都提供该标志或老的FASYNC标志）。在Linux中，调用open()时指定O\_ASYNC标志没有效果。要启用信号驱动I/O，我们必须使用fcntl()的F\_SETFL操作来设置该标志（5.3节）。（其它某些UNIX实现也是一样）。更多O\_ASYNC标志的信息请参考63.3节。

**O\_CLOEXEC（Linux 2.6.23开始）**

为新打开的文件描述符启用close-on-exec标志（FD\_CLOEXEC）。我们在27.4节描述FD\_CLOEXEC标志。使用O\_CLOEXEC标志允许程序避免使用额外的fcntl()的F\_SETFD操作来设置close-on-exec标志。也是多线程程序避免竞争条件的重要手段。当一个线程打开文件描述符，然后试图设置close-on-exec标志，这时另一个线程调用fork()然后再调用exec()，就会出现竞争条件。（假设第二个线程调用fork()和exec()的时间，正好在第一个线程打开文件描述符和使用fcntl()设置close-on-exec标志之间）。这种竞争条件会导致打开的文件描述符被无意地传递给不安全的程序。（我们会在5.1节更详细地讨论竞争条件）。

**O\_CREAT**

如果文件不存在，就创建一个新的空白文件。即使文件以只读模式打开，这个标志也是有效的。如果我们指定O\_CREAT，就必须为open()调用提供mode参数；否则新文件的权限会被设置为堆栈中的随机值。

**O\_DIRECT**

允许文件I/O绕过缓冲区缓存。13.6节详细描述了这个特性。必须设置\_GNU\_SOURCE特性测试宏，才能在<fcntl.h>中启用这个常量的定义。

**O\_DIRECTORY**

如果pathname不是目录则返回错误（errno等于ENOTDIR）。这个标志是专门为实现opendir()（18.8节）而特别设计的。必须定义\_GNU\_SOURCE特性测试宏，才能在<fcntl.h>中启用这个常量定义。

**O\_DSYNC（Linux 2.6.33开始）**

按照同步I/O数据完整性的要求来执行文件写入。参考13.3节关于内核I/O缓冲的讨论。

**O\_EXCL**

这个标志结合O\_CREAT一起使用，表示如果文件已经存在，就不应该打开它；相反open()应该失败，并设置errno为EEXIST。换句话说，这个标志允许调用者确保由本进程创建该文件。检查是否已经存在和创建该文件的操作是“原子的”。我们会在5.1节讨论“原子”的概念。当O\_CREAT和O\_EXCL同时指定时，如果pathname是一个符号链接，则open()也会失败（errno为EEXIST），SUSv3规定了这个行为，这样特权应用可以在已知的位置创建文件，杜绝由于符号链接导致文件被创建在不同的位置（例如系统目录），从而解决了这个安全问题。

**O\_LARGEFILE**

支持打开超大文件，这个标志用在32位系统操作超大文件。尽管SUSv3并没有规定这个标志，其它一些UNIX实现也支持O\_LARGEFILE标志。在64位Linux实现中（如Alpha和IA-64），这个标志没有作用。更多信息请参考5.10节。

**O\_NOATIME（Linux 2.6.8开始）**

读取文件时不更新文件的最后访问时间（15.1节描述的st\_atime域）。要使用这个标志，调用进程的有效用户ID必须匹配文件拥有者，或者进程拥有特权（CAP\_FOWNER）；否则open()会以EPERM错误失败。（实际上，当使用O\_NOATIME标志打开文件时，要匹配文件用户ID的并不是进程有效用户ID，而是进程的文件系统用户ID，9.5节会详细描述）。O\_NOATIME标志是非标准的Linux扩展，要在<fcntl.h>中暴露它的定义，必须定义\_GNU\_SOURCE特性测试宏。O\_NOATIME标志主要用于索引和备份程序，能够极大地降低磁盘活动，因为重复的磁盘来回seek，不需要读取文件内容和更新文件i-node的最后访问时间（14.4节）。使用mount()的MS\_NOATIME标志（14.8.1节）和FS\_NOATIME标志（15.5节）也可以达到类似O\_NOATIME的功能。

**O\_NOCTTY**

如果被打开的文件是终端设备，则阻止它成为控制终端。34.4节详细讨论控制终端。如果被打开的文件不是终端，则这个标志没有作用。

**O\_NOFOLLOW**

通常如果pathname是一个符号链接，open()会自动进行解引用。但是如果指定了O\_NOFOLLOW标志，则pathname是符号链接时open()将失败（errno设为ELOOP）。这个标志非常有用，特别是特权程序，可以确保open()不会解引用符号链接。要从<fcntl.h>中暴露这个标志的常量定义，必须定义\_GNU\_SOURCE特性测试宏。

**O\_NONBLOCK**

以非阻塞模式打开文件，请参考5.9节。

**O\_SYNC**

以同步I/O模式打开文件。参考13.3节内核I/O缓冲的相关讨论。

**O\_TRUNC**

如果文件已经存在并且是普通文件，则将其截断为0长度，并销毁所有数据。在Linux中，无论打开文件为读取还是写入，都会对文件进行截断（两种情况下，都必须拥有文件的写权限）。SUSv3没有对O\_RDONLY和O\_TRUNC标志的组合做出规定，但多数UNIX实现的行为都和Linux一样。

### 4.3.2 open()的错误

如果打开文件时出现了错误，open()返回-1，并设置errno为错误原因。以下是可能出现的错误（上面描述flags参数时已经提到一些错误了）：

EACCES

文件的权限不允许调用进程以flags指定的模式打开文件，或者由于目录权限，文件不能被访问；或者文件不存在并且无法被创建。

EISDIR

指定的文件是目录，调用方试图以写入模式打开它，这个操作是不允许的。（换句话说，打开目录来读取有时候是有用的。我们在18.11节会提供相关的例子）。

EMFILE

进程达到允许打开文件描述符数量的资源限制（RLIMIT\_NOFILE，36.3节描述）。

ENFILE

已经达到系统级的打开文件描述符数量限制。

ENOENT

指定的文件不存在，又没有指定O\_CREAT标志；或者指定了O\_CREAT，但pathname中的某个目录不存在；或者pathname是符号链接，指向不存在的路径（摇摆链接）。

EROFS

指定的文件在只读文件系统中，调用方却试图打开来写入。

ETXTBSY

指定的文件是可执行文件（程序），当前正在执行中。不允许修改（打开写入）正在运行程序关联的可执行文件。（我们必须首先终止这个程序，然后才能修改可执行文件）。

当我们后面讨论其它系统调用和库函数时，我们通常不会像上面这样列举出所有可能的错误（这个错误列表可以在系统调用和库函数相应的手册页找到）。在这里列出来有两个理由：首先，open()是本书详细讲解的第一个系统调用，上面列表说明系统调用或库函数可能由于各种原因失败；其次，open()为什么会失败本身也是非常有趣的，我们访问文件时需要考虑和检查各种情况。（上面列表是不完整的，更多失败原因请参考open(2)手册页）。

### 4.3.3 creat()系统调用

在早期UNIX实现中，open()只有两个参数，而且不能用来创建新文件。使用creat()系统调用来创建和打开新文件。

|  |
| --- |
| #include <fcntl.h>  int creat(const char \*pathname, mode\_t mode);  返回文件描述符；出错返回-1 |

creat()系统调用可以创建和打开pathname指定的新文件，或者如果文件已存在，则打开它并截断为0长度。creat()返回一个文件描述符，供后续系统调用使用。调用creat()等价于下面open()调用：

fd = open(pathname, O\_WRONLY | O\_CREAT | O\_TRUNC, mode);

由于open()的flags参数提供了打开文件的更多控制（如指定O\_RDWR而不是O\_WRONLY），目前creat()已经废弃，不过在老程序中还可以见到它。

## 4.4 读取文件：read()

read()系统调用从描述符fd引用的文件中读取数据：

|  |
| --- |
| #include <unistd.h>  ssize\_t read(int fd, void \*buffer, size\_t count);  返回读取的字节数，EOF返回0，错误时返回-1 |

count参数指定读取的最大字节数（size\_t数据类型是无符号整型）。buffer参数指定内存缓冲区的地址，用来存放读取的数据。这个缓冲区至少必须有count字节大小。

系统调用并不为调用方分配缓冲区内存来返回信息。相反我们必须自己分配合适大小的内存缓冲区，并传递指针给系统调用。有些库函数则确实会分配内存缓冲区，用来返回信息给调用方。

成功调用read()返回实际读取的字节数，如果遇到“end-of-file”则返回0，错误时返回-1。ssize\_t数据类型是带符号整数类型，用来返回字节数，或错误时返回-1。

调用read()可能读取少于请求的字节数。对于普通文件来说，可能的原因是我们已经接近文件末尾，只能读取剩余的字节。

当read()应用于其它文件类型时（如管道、FIFO、socket、终端），也存在许多读取少于请求字节数的情况。例如默认情况下，read()从终端读取字符最多只到换行字符（\n）。我们在随后章节讲解其它文件类型时还会仔细考虑这些情况。

使用read()从终端获取一系列输入字符，我们可以使用如下代码：

#define MAX\_READ 20

char buffer[MAX\_READ];

if (read(STDIN\_FILENO, buffer, MAX\_READ) == -1)

errExit("read");

printf("The input data was: %s\n", buffer);

这段代码的输出可能会很奇怪，包含了实际输入字符串之外的许多字符。这是因为read()不会在字符串的末尾自动增加printf()函数需要的null终止字符。稍微思考一下，我们就能明白read必须这么做，因为read()可能用于任何文件读取任何数据。有时候输入可能是文本，其它情况下输入可能是二进制整数或C结构体等二进制形式。read()没有办法进行区分，因此不能简单地使用C的null终止字符惯例。如果输入缓冲区末尾要求有null终止字符，我们必须显式地手工增加。

char buffer[MAX\_READ + 1];

ssize\_t numRead;

numRead = read(STDIN\_FILENO, buffer, MAX\_READ);

if (numRead == -1)

errExit("read");

buffer[numRead] = '\0';

printf("The input data was: %s\n", buffer);

由于null终止字符要求额外的一个字节内存，buffer的大小必须至少是我们需要读取最大字符的长度加1。

## 4.5 写入文件：write()

write()系统调用向打开文件写入数据。

|  |
| --- |
| #include <unistd.h>  ssize\_t write(int fd, void \*buffer, size\_t count);  返回实际写入的字节数，出错时返回-1 |

write()的参数类似于read()：buffer是待写入数据的地址；count是buffer的字节数；fd指向数据需要写入的文件。

成功时write()返回实际写入的字节数，可能小于count。对于磁盘文件来说，这种“部分写入”的可能原因是磁盘已满，或进程达到文件大小的资源限制。（36.3节描述的RLIMIT\_FSIZE限制）。

## 4.6 关闭文件：close()

close()系统调用关闭一个已打开的文件描述符，释放该文件描述符以供进程随后使用。当进程终止时，所有打开的文件描述符都会自动被关闭。

|  |
| --- |
| #include <unistd.h>  int close(int fd);  成功时返回0；失败返回-1 |

通常手工显式地关闭文件描述符是良好的实践，因为这样做可以提高代码应对以后修改的可读性和可靠性。此外文件描述符是消耗性资源，如果不关闭文件描述符，可能导致进程用完所有描述符。当编写长期运行需要处理许多文件的程序时（如shell或网络服务器），这就是一个特别重要的问题。

和其它系统调用一样，调用close()也应该检查相关的错误，如下所示：

if (close(fd) == -1)

errExit("close");

这样可以捕获到诸如关闭未打开文件描述符，两次关闭相同的文件描述符等错误。还能捕获到特定文件系统在关闭操作时诊断出来的错误条件。

NFS（网络文件系统）会提供文件系统特定的错误。如果发生了NFS提交错误，意味着数据没有到达远程磁盘，这个错误就会通过close()调用传送给应用。

## 4.7 改变文件偏移：lseek()

对于每个打开的文件，内核记录了一个文件偏移量，有时候也称为读写偏移或指针。这个偏移是下一个read()或write()将操作的文件位置。文件偏移是相对于文件起始的顺序字节位置，文件的第一个字节即是偏移0。

当文件被打开时，文件偏移设置为文件的开头，并随着read()和write()调用自动调整为刚刚读取或写入的下一个字节。因此连续的read()和write()调用可以顺序地穿过一个文件。

lseek()系统调用可以调整文件描述符fd引用文件的偏移，设置为offset和whence指定的位置。

|  |
| --- |
| #include <unistd.h>  off\_t lseek(int fd, off\_t offset, int whence);  成功时返回新的文件偏移，出错返回-1 |

offset参数指定字节数（SUSv3规定off\_t数据类型为带符号整数类型）。whence参数指示offset的基点，可以取如下值之一：

SEEK\_SET

文件偏移设为文件起始位置后的offset字节。

SEEK\_CUR

文件偏移调整为相对当前文件偏移的offset字节。

SEEK\_END

文件偏移设为文件大小加offset。换句话说，offset相对于文件末尾来解释。

图4-1显示了whence参数是如何被解释的。

在早期UNIX实现中，使用了0，1，2整数，而不是SEEK\*常量。老版本的BSD使用不同的名字：L\_SET, L\_INCR, L\_XTND。



*图4-1：解释lseek()的whence参数*

如果whence是SEEK\_CUR或SEEK\_END，offset可以为正也可以为负；如果是SEEK\_SET，则offset必须非负。

成功调用lseek()返回新的文件偏移。下面调用获取当前文件偏移，而不修改文件偏移：

curr = lseek(fd, 0, SEEK\_CUR);

有一些UNIX实现（不是Linux）有非标准的tell(fd)函数，作用和上面讲的lseek调用是一样的。

下面是lseek()调用的一些例子，后面的注释描述了新的文件偏移：

lseek(fd, 0, SEEK\_SET); /\* 文件起始位置 \*/

lseek(fd, 0, SEEK\_END); /\* 文件末尾的下一个字节 \*/

lseek(fd, -1, SEEK\_END); /\* 文件末尾 \*/

lseek(fd, -10, SEEK\_CUR); /\* 当前位置的前10字节处 \*/

lseek(fd, 10000, SEEK\_END); /\* 文件末尾之后的10001字节 \*/

调用lseek()只是简单地调整内核中文件描述符相关联的文件记录偏移值，不会引起任何物理设备访问操作。

我们在后面5.4节会更加详细地讨论文件偏移、文件描述符、和打开文件之间的关系。

不是所有文件类型都能使用lseek()，对管道、FIFO、socket、或终端应用lseek()是不允许的；lseek()会失败，并设置errno为ESPIPE。反过来对某些可调整偏移的设备应用lseek()是可以的，例如磁盘或磁带设备都可以seek到指定位置。

lseek()中的“l”表示最早offset参数和返回值都是long。早期UNIX实现还提供一个seek()系统调用，相应地使用int参数和返回值。

**文件空洞**

如果一个程序seek超过了文件末尾，然后又执行I/O，会发生什么呢？这时候read()会返回0，表示end-of-file。但是令人吃惊的是，超过文件末尾任意位置写入字节是可以的。

之前的文件末尾与新写入字节之间的空间被称为“文件空洞”。从编程的角度来看，空洞中是存在字节的，从空洞读取会返回全0（null字节）的数据。

不过文件空洞不会占用任何磁盘空间。文件系统不会为空洞分配任何磁盘块，除非之后有数据写入到空洞中。文件空洞的主要优点是稀疏文件会消耗更少的磁盘空间，不需要为null字节分配实际的磁盘块。Core dump文件（22.1节）是包含大量空洞的典型例子。

文件空洞不消耗磁盘空间的说法需要稍微澄清。在多数文件系统中，文件空间是以块的单位来分配的（14.3节）。块大小依赖于文件系统，不过通常1024，2048或4096字节。如果空洞存在于块中，而不是块的边界，那还是会分配一个完整的块来存储数据，对应于空洞的部分空间则填充null字节。

多数UNIX文件系统支持文件空洞的概念，但许多非UNIX本地文件系统（如Microsoft VFAT）却不支持，在这些不支持文件空洞的文件系统中，显式的null字节会被写入到文件。

空洞的存在意味着文件的正常大小可能会大于它占用的磁盘存储空间（某些情况下会大很多）。向文件空洞写入字节会减少磁盘的可用空间，因为内核会分配块来存储这些数据，而文件的大小则不会改变。这种情况并不常见，但无论如何你需要知道有这么个问题。

SUSv3规定了一个函数posix\_fallocate(fd, offset, len)，可以确保在磁盘中为描述符fd引用的文件分配offset和len指定的空间。这允许应用确保之后的write()操作不会因为磁盘空间耗尽而失败（如果有空洞这种情况可能会发生）。历史上glibc对这个函数的实现是在每个块中写入0字节。从内核2.6.23开始，Linux提供了一个fallocate()系统调用，可以更高效地确保分配必需的空间，新的glibc posix\_fallocate()实现就使用了这个系统调用。

14.4节描述空洞在文件中是如何表示的，15.1节描述stat()系统调用，可以告诉我们文件的当前大小，以及为文件实际分配的块数量。

**示例程序**

清单4-3演示了使用lseek()以及read()和write()的一个程序。第一个命令行参数是要打开的文件名，剩下的参数指定要对文件进行的I/O操作。每个操作都是一个字母以及相关的值（没有空格）：

* s(offset)：从文件起始seek offset字节。
* r(length)：从文件的当前偏移读取length字节，并显示为文本。
* R(length)：从文件的当前偏移读取length字节，并显示为十六进制。
* w(str)：写入str字符串到文件的当前偏移。

*清单4-3：read(), write(), lseek()演示*

----------------------------------------------------fileio/seek\_io.c

#include <sys/stat.h>

#include <fcntl.h>

#include <ctype.h>

#include "tlpi\_hdr.h"

int

main(int argc, char \*argv[])

{

size\_t len;

off\_t offset;

int fd, ap, j;

char \*buf;

ssize\_t numRead, numWritten;

if (argc < 3 || strcmp(argv[1], "--help") == 0)

usageErr(

"%s file {r<length>|R<length>|w<string>|s<offset>}...\n",

argv[0]);

fd = open(argv[1], O\_RDWR | O\_CREAT,

S\_IRUSR | S\_IWUSR | S\_IRGRP | S\_IWGRP |

S\_IROTH | S\_IWOTH); /\* rw-rw-rw- \*/

if (fd == -1)

errExit("open");

for (ap = 2; ap < argc; ap++) {

switch (argv[ap][0]) {

case 'r': /\* Display bytes at current offset, as text \*/

case 'R': /\* Display bytes at current offset, in hex \*/

len = getLong(&argv[ap][1], GN\_ANY\_BASE, argv[ap]);

buf = malloc(len);

if (buf == NULL)

errExit("malloc");

numRead = read(fd, buf, len);

if (numRead == -1)

errExit("read");

if (numRead == 0) {

printf("%s: end-of-file\n", argv[ap]);

} else {

printf("%s: ", argv[ap]);

for (j = 0; j < numRead; j++) {

if (argv[ap][0] == 'r')

printf("%c", isprint((unsigned char) buf[j]) ?

buf[j] : '?');

else

printf("%02x ", (unsigned int) buf[j]);

}

printf("\n");

}

free(buf);

break;

case 'w': /\* Write string at current offset \*/

numWritten = write(fd, &argv[ap][1], strlen(&argv[ap][1]));

if (numWritten == -1)

errExit("write");

printf("%s: wrote %ld bytes\n", argv[ap], (long) numWritten);

break;

case 's': /\* Change file offset \*/

offset = getLong(&argv[ap][1], GN\_ANY\_BASE, argv[ap]);

if (lseek(fd, offset, SEEK\_SET) == -1)

errExit("lseek");

printf("%s: seek succeeded\n", argv[ap]);

break;

default:

cmdLineErr("Argument must start with [rRws]: %s\n", argv[ap]);

}

}

exit(EXIT\_SUCCESS);

}

----------------------------------------------------fileio/seek\_io.c

下面shell会话日志演示了清单4-3程序的使用，显示了当我们从文件空洞中读取字节时的情况：

$ touch tfile 创建新的空白文件

$ ./seek\_io tfile s100000 wabc seek到100000偏移，写入“abc”

s100000: seek succeeded

wabc: wrote 3 bytes

$ ls -l tfile 检查文件大小

-rw-r--r-- 1 mtk users 100003 Feb 10 10:35 tfile

$ ./seek\_io tfile s10000 R5 seek到10000，从空洞读取5字节

s10000: seek succeeded

R5: 00 00 00 00 00 空洞中的字节全为0

## 4.8 通用I/O模型之外的操作：ioctl()

ioctl()系统调用是一个通用机制，可以执行本章前面描述的通用I/O模型之外的文件和设备操作。

|  |
| --- |
| #include <sys/ioctl.h>  int ioctl(int fd, int request, ... /\* argp \*/);  成功时返回request相关的值，出错返回-1 |

fd参数是打开的文件描述符，也是request要执行控制操作的那个文件。设备相关头文件定义的常量可以传递给request参数。

上面的省略号（…）是标准C符号，表示ioctl()的第三个参数argp可以是任何类型。request参数的值允许ioctl()确定自己需要的argp类型。通常argp是一个整型或结构体指针，有些情况下没有argp参数。

我们在后面章节会看到许多ioctl()的使用（比如15.5节）。

SUSv3对ioctl()的唯一规定是STREAM设备的控制操作（STREAM机制是System V特性，Linux主版本内核并不支持，不过已经开发了一些插件实现）。本书讨论的其它ioctl()操作都不是SUSv3规范。但是ioctl()调用很早的时候就一直是UNIX系统的一部分，因此我们后面讨论的一些ioctl()操作在许多UNIX实现中都可用。在我们讨论每个ioctl()操作时，会标明可移植性方面的问题。

## 4.9 小结

要对普通文件执行I/O操作，首先必须使用open()获得文件描述符，然后使用read()和write()执行I/O。在所有I/O操作结束之后，我们应该使用close()释放文件描述符和相关的资源。这些系统调用可以用于所有文件类型的I/O操作。

通用I/O模型要求所有文件类型和设备驱动实现相同的I/O接口，意味着程序不需要为特定文件类型编写代码，相同的代码可以用于任何类型的文件。

对每个打开的文件，内核都维护了一个文件偏移，用于确定下一个read或write将操作的文件位置。read和write会隐式地更新文件偏移，也可以使用lseek()显式地调整文件偏移，设置为文件内的任何位置，也可以超过文件末尾。向超过文件末尾的位置写入数据会创建文件空洞。从文件空洞读取的数据全部为0。

ioctl()系统调用提供标准文件I/O模型之外的设备和文件操作功能。

## 4.10 习题

4-1. tee命令读取标准输入直到end-of-file，并把输入复制到标准输出，以及命令行参数指定的文件中（我们在44.7节讨论FIFO时会展示该命令的使用例子）。请你使用I/O系统调用实现tee命令。默认情况下tee覆盖指定名字的现有文件。请你实现-a命令行选项（tee –a file），使tee追加文本到已经存在文件的末尾。（参考附录B对getopt()函数的描述，它可以用来解析命令行选项）。

4-2. 编写一个类似cp的程序，当用来复制包含空洞的文件时（null字节序列），要求在目标文件中也创建相应的空洞。

# 第5章 文件I/O：更多细节

在这一章，我们将扩展前一章对文件I/O的讨论。

我们将继续深入open()系统调用的讨论，解释原子性的概念——系统调用执行的动作是单一不可中断的步骤。原子性是许多系统调用能够正确执行操作的必要条件。

我们还介绍另一个文件相关的系统调用，多用途的fcntl()，并展现了它的一个用途：获取和设置打开文件状态标志。

接着我们学习内核用来表示文件描述符和打开文件的数据结构。理解这些结构体之间的关系，有助于我们随后章节解释文件I/O的许多微妙细节。基于这个模型，我们接下来解释怎样复制文件描述符。

然后我们考虑一些提供扩展读取和写入功能的系统调用。这些系统调用允许我们在文件的特定位置执行I/O，而不修改文件偏移；以及同时读取和写入程序的多个缓冲区。

我们简要地介绍了非阻塞I/O的概念，并描述了一些支持大型文件I/O操作的扩展接口。

由于许多系统程序需要使用临时文件，我们也学习几个创建和使用临时文件的库函数，这些函数随机生成唯一的临时文件名。

## 5.1 原子性和竞争条件

原子性是我们讨论系统调用操作时经常遇到的一个概念。所有系统调用都是原子执行的。也就是说内核确保一个系统调用的所有步骤都能以单一操作完整地结束，不会被其它进程或线程中断。

原子性是某些操作能够成功完成的必要条件。特别值得一提的是，原子性使得我们避免了竞争条件（有时候称为竞争危险）。两个进程（或线程）同时操作共享资源时，如果执行结果依赖于进程获得CPU访问的具体顺序，就产生了竞争条件。

在接下来的几页里，我们查看两个文件I/O相关的竞争条件，并演示如何使用open()的标志来确保相关文件操作的原子性，从而消除这些竞争条件。

在后面22.9节讨论sigsuspend()，和24.4节讨论fork()时，我们还会再次遇到竞争条件。

**互斥地创建文件**

在4.3.1节，我们说过指定O\_EXCL结合O\_CREAT标志，如果文件已经存在则open()将返回错误。这使得进程可以确保自己是新文件的创建者。检查文件是否存在，和创建该文件的过程是原子的。这一点非常重要，考虑清单5-1中的代码，我们没有使用O\_EXCL标志（在这段代码中，我们显示了getpid()返回的进程ID，可以让我们区分同一个程序同时运行的不同结果）。

*清单5-1：互斥打开文件的错误代码*

-------------------------------------------fileio/bad\_exclusive\_open.c

fd = open(argv[1], O\_WRONLY); /\* Open 1: check if file exists \*/

if (fd != -1) { /\* Open succeeded \*/

printf("[PID %ld] File \"%s\" already exists\n",

(long) getpid(), argv[1]);

close(fd);

} else {

if (errno != ENOENT) { /\* Failed for unexpected reason \*/

errExit("open");

} else {

/\* WINDOW FOR FAILURE \*/

fd = open(argv[1], O\_WRONLY | O\_CREAT, S\_IRUSR | S\_IWUSR);

if (fd == -1)

errExit("open");

printf("[PID %ld] Created file \"%s\" exclusively\n",

(long) getpid(), argv[1]); /\* MAY NOT BE TRUE! \*/

}

}

-------------------------------------------fileio/bad\_exclusive\_open.c

上面代码除了要烦琐地使用两次open()调用之外，还包含一个bug。假设进程调用了第一个open()，此时文件并不存在；但是等到进程第二次调用open()时，其它进程已经创建了这个文件。如果内核调度器认为进程时间片已经用完并将CPU控制权交给其它进程，如图5-1所示；或者两个进程同时运行在多核处理器系统中，这种情况就很有可能发生。图5-1假设两个进程都执行清单5-1中的代码。在这种场景下，进程A最终可能错误地认为自己已经创建了该文件，因为第二个open()无论文件是否存在都会返回成功。

虽然进程错误地认为自己是文件创建者的概率相对较低，但是无论如何这种可能性的存在，降低了代码的可靠性。操作结果依赖于两个进程的调度顺序，表明这是一个竞争条件。



*图5-1：互斥创建文件失败*

要演示上面代码存在的真正问题，我们可以替换清单5-1中已经注释掉的那行WINDOW FOR FAILURE，在文件存在检查和创建文件之间，加入一段长时间的延迟代码：

printf("[PID %ld] File \"%s\" doesn't exist yet\n",

(long) getpid(), argv[1]);

if (argc > 2) { /\* Delay between check and create \*/

sleep(5); /\* Suspend execution for 5 seconds \*/

printf("[PID %ld] Done sleeping\n", (long) getpid());

}

sleep()库函数挂起进程指定的秒数。我们在23.4节会讨论这个函数。

如果我们同时运行两次清单5-1中的程序，我们可以看到两个进程都声称自己已经成功创建该文件：

**$ ./bad\_exclusive\_open tfile sleep &**

[PID 3317] File "tfile" doesn't exist yet

[1] 3317

**$ ./bad\_exclusive\_open tfile**

[PID 3318] File "tfile" doesn't exist yet

[PID 3318] Created file "tfile" exclusively

$ [PID 3317] Done sleeping

[PID 3317] Created file "tfile" exclusively [Not true]

两个进程都声称创建了该文件，是因为第一个进程检查文件是否存在，到创建文件之间被中断。使用一个open()调用，指定O\_CREAT和O\_EXCL标志可以阻止这种情况的发生，确保检查和创建的步骤以原子操作进行（不可中断）。

**追加数据至文件**

另一个需要原子操作的例子是多个进程同时追加数据到相同文件（如全局日志文件）。要实现这个目的，我们可能会采用如下代码：

if (lseek(fd, 0, SEEK\_END) == -1)

errExit("lseek");

if (write(fd, buf, len) != len)

fatal("Partial/failed write");

但是这段代码面临前面例子同样的问题。如果第一个进程在lseek()和write()之间被中断，而第二个进程也正好在执行这段代码，则两个进程都会设置文件偏移为相同位置，然后当第一个进程重新被调度运行时，它就会覆盖第二个进程已经写入文件的数据。这里也存在一个竞争条件，因为结果依赖于这两个进程被调度的顺序。

要避免这个问题，就需要使seek到文件末尾下一个字节，和写入操作以原子方式进行。这就是以O\_APPEND标志打开文件要实现的功能。

某些文件系统（如NFS）不支持O\_APPEND。在这种情况下，内核会使用上面的非原子调用序列，结果就是刚刚描述过的可能污染文件。

## 5.2 文件控制操作：fcntl()

fcntl()系统调用可以对已打开的文件描述符执行许多控制操作。

|  |
| --- |
| #include <fcntl.h>  int fcntl(int fd, int cmd, ...);  成功时根据cmd返回，出错返回-1 |

cmd参数可以指定大量的操作。下面几节我们会介绍其中的几个，其余则留待后面章节详述。

正如省略号所示，fcntl()的第三个参数可以是不同类型，有时候也可以省略。内核使用cmd参数的值来确定自己需要的参数值类型（如果有的话）。

## 5.3 打开文件状态标志

fcntl()的一个作用是获取和修改文件的访问模式和打开文件状态标志（也就是open()调用中指定的flags参数值）。要获取这些值，我们为cmd指定F\_GETFL：

int flags, accessMode;

flags = fcntl(fd, F\_GETFL); /\* 第三个参数不需要 \*/

if (flags == -1)

errExit("fcntl");

然后我们可以如下测试文件是否以同步写入模式打开：

if (flags & O\_SYNC)

printf("writes are synchronized\n");

SUSv3要求只有open()指定的状态标志和fcntl() F\_SETFL指定的标志，才能设置到打开文件描述符中。但是Linux有一个地方偏离了这个规定：如果应用使用了5.10节打开超大文件的技术进行编译，则F\_GETFL获得的标志总是包含O\_LARGEFILE。

检查文件的访问模式则稍微复杂一些，因为O\_RDONLY(0), O\_WRONLY(1), O\_RDWR(2)常量并不对应于打开文件状态标志中的某个位。因此如果要检查访问模式，我们要用O\_ACCMODE常量对flags进行掩码，然后再与上面三个常量检测是否相等：

accessMode = flags & O\_ACCMODE;

if (accessMode == O\_WRONLY || accessMode == O\_RDWR)

printf("file is writable\n");

我们可以使用fcntl()的F\_SETFL命令来修改某些打开文件状态标志。可以修改的标志包括：O\_APPEND, O\_NONBLOCK, O\_NOATIME, O\_ASYNC, O\_DIRECT。试图修改其它标志会被忽略（某些UNIX实现允许fcntl()修改其它标志，如O\_SYNC）。

以下情况使用fcntl()修改打开文件状态标志特别有用：

* 文件不是由调用程序打开的，因此程序无法控制open()时使用的flags（如程序启动前打开的三个标准描述符）。
* 文件描述符不是使用open()系统调用获得。例如pipe()系统调用创建一个管道，并返回两个文件描述符分别引用管道的两端；socket()调用创建一个socket并返回一个文件描述符。

要修改打开文件的状态标志，我们先使用fcntl()来获得现有标志，然后修改相应的位，最后再次调用fcntl()来更新状态标志。因此要启用O\_APPEND标志，我们可以编写如下代码：

int flags;

flags = fcntl(fd, F\_GETFL);

if (flags == -1)

errExit("fcntl");

flags |= O\_APPEND;

if (fcntl(fd, F\_SETFL, flags) == -1)

errExit("fcntl");

## 5.4 文件描述符和打开文件之间的关系

到现在为止，看起来好像文件描述符和打开文件都是一一对应的。但是实际情况却并不是这样。可以有多个描述符引用同一个打开文件，而且这个特性非常有用。这些文件描述符可以由相同进程也可以由不同进程打开。

要理解这种关系，我们需要先学习内核维护的三个数据结构：

* 每个进程的文件描述符表；
* 系统级的打开文件说明表；
* 文件系统i-node表。

对于每个进程，内核都维护了一个打开文件描述符表。表中的每一项都记录了一个文件描述符的信息，包括：

* 一组控制文件描述符操作的标志（其实只有一个close-on-exec标志，27.4节讨论）；
* 打开文件说明的引用。

内核维护了一个系统级的所有打开文件说明表（这个表有时候也叫做打开文件表，它的每一项称为打开文件句柄）。一个打开文件说明存储了打开文件相关的所有信息，包括：

* 当前文件偏移（由open()和write()更新，或者lseek()显式修改）；
* 打开文件时指定的状态标志（open()的flags参数）；
* 文件访问模式（只读、只写、读写）；
* 信号驱动I/O相关的设置（63.3节）；
* 该文件i-node对象的引用。

每个文件系统都有一个该文件系统内所有文件的i-node表。第14章会更加详细地讨论i-node结构体和文件系统。现在我们只需要知道每个文件的i-node包含了以下信息：

* 文件类型（如普通文件、socket、FIFO）和权限；
* 指向文件锁列表的一个指针；
* 文件的许多属性，包括不同类型文件操作相关的大小、时间戳等。

这里我们简单地说明一下磁盘中和内存中i-node的区别。磁盘中的i-node记录了文件的持久属性，如文件类型、权限、和时间戳等。当访问文件时，就会在内存中创建一份i-node拷贝，而内存中的i-node则记录了引用i-node的打开文件描述符数量，以及i-node所在设备的主要（major）和次要（minor）ID。内存i-node还记录了文件打开相关的许多短暂属性，如文件锁。

图5-2阐明了文件描述符、打开文件、和i-node之间的关系。在这幅图中，两个进程都有若干打开的文件描述符。



*图5-2：文件描述符、打开文件、i-node的关系*

在进程A中，描述符1和20都引用同一个打开文件（标签23）。调用dup(), dup2(), fcntl()可能会导致这种情况出现（5.5节）。

进程A的描述符2和进程B的描述符2都引用同一个打开文件（标签73）。这种情况发生的原因包括：调用fork()（如进程A是进程B的父亲，反之亦然）；或者一个进程使用UNIX domain socket把打开描述符传递给了另一个进程（61.13.3节）。

最后，进程A的描述符0和进程B的描述符3引用不同的打开文件，但是这两个打开文件却又引用同一个i-node表项（标签1976）——换句话说就是同一个文件。这是由于两个进程各自对相同文件调用了open()，一个进程打开相同文件两次也会出现类似的情况。

我们可以从上面这些讨论得出以下结论：

* 引用同一个打开文件的两个不同文件描述符，共享相同的文件偏移。因此如果文件偏移被其中一个描述符改变（调用read(), write(), lseek()），这个改变对其它文件描述符也是可见的。不管两个文件描述符属于同一个进程还是不同进程，结果都是一样的。
* 使用fcntl() F\_GETFL和F\_SETFL操作获取和修改打开文件状态标志时（O\_APPEND, O\_NONBLOCK, O\_ASYNC），类似的范围规则同样适用。
* 相比之下，文件描述符标志（如close-on-exec标志）则是进程和文件描述符私有的。修改这些标志不会影响相同进程或其它进程的其它文件描述符。

## 5.5 复制文件描述符

## 5.6 指定偏移位置的文件I/O：pread()和pwrite()

## 5.7 Scatter-Gather I/O：readv()和writev()

## 5.8 截断文件：truncate()和ftruncate()

## 5.9 非阻塞I/O

## 5.10 超大文件I/O

## 5.11 /dev/fd目录

## 5.12 创建临时文件

## 5.13 小结

## 5.14 习题

# 第6章 进程

# 第7章 内存分配

# 第8章 用户和组

# 第9章 进程凭证

# 第10章 时间

# 第11章 系统限制和选项

# 第12章 系统和进程信息

# 第13章 文件I/O缓冲

# 第14章 文件系统

# 第15章 文件属性

# 第16章 扩展属性

# 第17章 访问控制列表

# 第18章 目录和链接

# 第19章 监控文件事件

# 第20章 信号：基础概念

# 第21章 信号：信号处理器

# 第22章 信号：高级特性

# 第23章 定时器和睡眠

# 第24章 进程创建

# 第25章 进程结束

# 第26章 监控子进程

# 第27章 程序执行

# 第28章 进程创建和程序执行的更多细节

# 第29章 线程：介绍

# 第30章 线程：同步

# 第31章 线程：线程安全和线程存储

# 第32章 线程：线程取消

# 第33章 线程：更多细节

# 第34章 进程组、会话和任务控制

# 第35章 进程优先级和调度

# 第36章 进程资源

# 第37章 Daemon

# 第38章 编写安全的特权程序

# 第39章 能力

# 第40章 登录会计

# 第41章 共享库基础

# 第42章 共享库高级特性

# 第43章 进程间通信简介

# 第44章 管道和FIFO

# 第45章 System V IPC介绍

# 第46章 System V消息队列

# 第47章 System V信号量

# 第48章 System V共享内存

# 第49章 内存映射

# 第50章 虚拟内存操作

# 第51章 POSIX IPC介绍

# 第52章 POSIX消息队列

# 第53章 POSIX信号量

# 第54章 POSIX共享内存

# 第55章 文件锁

# 第56章 Sockets：介绍

# 第57章 Sockets：UNIX Domain

# 第58章 Sockets：TCP/IP网络基础

# 第59章 Sockets：Internet Domain

# 第60章 Sockets：服务器设计

# 第61章 Sockets：高级主题

# 第62章 终端

# 第63章 可选I/O模型

# 第64章 伪终端

# 附录A：跟踪系统调用

# 附录B：解析命令行参数

# 附录C：转换NULL指针

# 附录D：内核配置

# 附录E：更多信息来源

# 附录F：部分习题解答

# 参考书目

# 索引