

Linux GNU C 程序观察

罗秋明 著



清华大学出版社



Linux GNU C 程序观察

罗秋明 著

清华大学出版社
北京

内 容 简 介

本书所讨论的内容是“C 语言程序设计”类课程的后续知识,涉及 C 程序在 Linux 环境下经过 GCC 编译/链接生成可执行文件以及在系统中运行的问题。本书能使读者在面对 C 程序的工程实践问题时,做到心中有数,处处不存疑。

全书共 7 章,第 1 章介绍环境准备,第 2 章介绍 C 程序的预处理、编译、汇编和链接的全过程,并介绍了一点关于 GCC 编译命令及编译选项、GDB 调试初步概念,第 3 章专注于编译环节,即从 C 到汇编的转换,第 4 章专注于链接过程,第 5 章介绍可执行文件在系统中运行时,观察进程与系统的关系、进程对库的调用、程序异常行为等问题,第 6、7 章介绍一些性能剖析方法,包括 GCC 自带工具、库函数打桩方法、valgrind 及 perf 工具的简单使用等,第 8 章介绍一个综合性的实例,即如何将 HDFS 文件系统使用的 gzip 压缩,从利用 zlib 库在 CPU 上计算转换成利用 FPGA 加速卡的过程。该实例涉及库的使用和修改、makefile 以及相应的 C 程序实现等多方面知识,让读者从一个工程需求的角度考察其方案与实现。每章后面都有一些练习题,其中有一个与 zlib 库相关的任务贯穿了各章,读者通过这个连贯的练习将各章知识融会贯通。

本书可以作为计算机及相关专业高年级本科生或研究生学习 Linux 环境下的 C 程序设计教学用书,对希望深入了解 Linux 内核的读者和相关开发人员也非常有参考价值。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

Linux GNU C 程序观察/罗秋明著. —北京:清华大学出版社,2020.1
ISBN 978-7-302-54549-1

I. ①L… II. ①罗… III. ①Linux 操作系统—程序设计 ②C 语言—程序设计 IV. ①TP316.85
②TP312.8

中国版本图书馆 CIP 数据核字(2019)第 290392 号

责任编辑:龙启铭
封面设计:何凤霞
责任校对:胡伟民
责任印制:沈 露

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>
地 址:北京清华大学学研大厦 A 座 邮 编:100084
社 总 机:010-62770175 邮 购:010-62786544
投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn
质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn
课 件 下 载: <http://www.tup.com.cn>, 010-83470236

印 装 者:北京嘉实印刷有限公司

经 销:全国新华书店

开 本:185mm×230mm

印 张:27.75

字 数:575 千字

版 次:2020 年 5 月第 1 版

印 次:2020 年 5 月第 1 次印刷

定 价:59.00 元

产品编号:081919-01

PREFACE

序

我

们在系统软件的教学和学生培养中,深感教材的缺乏。以往只能在项目实践中,让学生通过网络上的零散资料来完成相关知识的补充学习,然后才能参与到项目中。我们认为,计算机作为实践性很强的学科,如果课堂教学和实验不能紧密联系具体的系统,无法面对和解决工程问题,就不能算成功。Linux 系统作为一个开源的资源,为我们提供了良好的机会,可以将底层系统软件的相关技术细节完全呈现出来。为此,我们的第一步计划是提供最基本的一条学习通路,将应用程序和系统打通,形成系统软件技术学习丛书,其进阶学习流程如下。

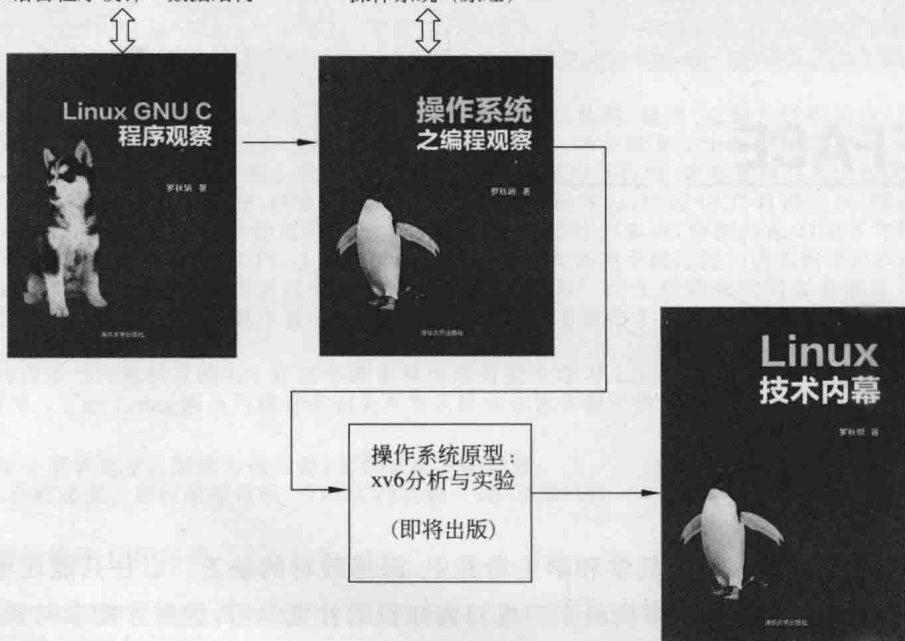
学生在完成 C 语言程序设计、数据结构和算法课程的学习之后,可以通过本书补充 C 程序与系统的知识。C 语言程序设计作为“上半部”知识,而本书作为“下半部”知识,从而形成 C 程序自身完整的知识结构。

然后将视角从一个程序扩展到整个系统中,需要面对多个进程并发的操作系统环境。此时仅靠本科操作系统原理性课程的学习仍是不够充分的。一方面,可以通过《操作系统之编程观察》(清华大学出版社,书号 978-7-302-48973-3)介绍的用 proc 文件系统提供的内核运行数据,直观地观察 Linux 操作系统的进程调度与均衡、进程间通信、内存管理和文件系统等行为,加深理论概念的认识;另一方面从《操作系统原型: xv6 分析与实验》(即将出版)对操作系统实现中的关键机制进行探索,掌握其编码实现的关键细节,弄懂操作系统编码实现的最核心知识。

最后,在有需要的时候学习《Linux 技术内幕》(清华大学出版社,书号 978-7-302-45100-6)。通过对真实的、完善的(相对于 xv6 的原型代码而言)、稳定的 Linux 内核代码

C语言程序设计、数据结构

操作系统（原理）



进行学习,掌握 Linux 内核实现细节并可以尝试根据工程需要对 Linux 系统进行修改增强。

上述 4 个相关联、递进的知识板块及学习安排,是我们在 PHPC(个人高性能计算机)系统研制的学生培养过程中积累下来的,希望能对有志于投身系统软件开发的读者有所帮助。

FOREWORD

前言

我们在当前的 C 语言程序设计教学工作中,对 C 语言的语法和编程技术虽然都已经讨论得非常充分,但是作为计算机的“系统观”的建立,只能说仅完成了一半的任务。从 C 语言如何转换到汇编语言进而生成机器码形式的可执行文件,以及可执行文件如何装入内存并在操作系统环境中运行的细节,对大多数完成本科课程学习的学生而言,仍未达到解惑的程度。学生也许可以通过在网络上找到的业界大牛们提供的零散材料,自行建立起相应的认识,但这毕竟是一个耗时和低效的学习过程。

本书希望将上述知识,组织成一个相对完整、便于学习与实践的材料,在计算机系统课程学习中(例如深圳大学的“计算机系统 2”)作为实验补充材料,让学生全面接触从 C 语言转换到汇编、进而生成机器码形式的可执行文件直至运行的全过程。在这种学习安排下,即使学生未修学编译原理课程,也能大致理解编译过程所使用的代码转换模板、链接中的符号解析和重定位等知识。除此之外,本书也介绍了程序在系统中运行的各种行为、代码调试和性能剖析工具的使用,对程序生成过程和运行过程都进行细致的观察——类似于电路与系统课程使用的万用表、示波器和频谱仪。有了这些“测量工具”后,C 语言的实验教学才能从当前的“犹抱琵琶半遮面”的境况,变得相对完整起来。

罗秋明
于深大荔园
2020.1

ACKNOWLEDGMENTS

致谢^①

感

谢深圳大学计算机与软件学院“计算机系统 2”课程组的老师,大家一起完成了广东省教育厅应用型人才培养课程建设项目“计算机系统系列核心课程”的实验内容和教学材料的准备工作,其中的部分工作正是本书的内容。特别感谢刘刚老师在相关实验的设计开发中给予的帮助。

还要感谢 2018 级的研究生杜海鑫、张靖、吴坤鑫和沙士豪三位同学,他们承担了部分书稿的整理、校对和实验代码的设计及检验等工作。其中,杜海鑫同学完成了第 8 章 zlib 的代码开发和部分撰写工作,并对第 4 章、第 5 章和第 8 章内容进行整理和校对。吴坤鑫同学提供了 7.2 节、7.3 节和 7.4 节材料。张靖同学负责第 1 章、第 2 章和第 3 章材料的校对,沙士豪同学负责第 6 章和第 7 章材料的校对。

在上述老师和同学的大力支持下,本书终于完稿并与读者见面。再次对他们表示衷心的感谢!

^① 本书获得深圳市科创委基础研究项目 JCYJ20170302153920897 云环境中的异构存储资源分配与性能优化研究、JSGG20170822110100205 基于开放技术的可信多路高端计算系统研发的资助。

CONTENTS

目 录

第 1 章 实验环境构建	1
1.1 安装 Linux	1
1.1.1 下载 CentOS7	1
1.1.2 CentOS7 安装	2
1.2 虚拟机安装 Linux	9
1.2.1 VirtualBox 安装	9
1.2.2 虚拟机配置	13
1.2.3 虚拟机安装 Linux	20
1.3 ssh 远程终端访问	20
1.3.1 PuTTY 客户端	21
1.3.2 无密码登录	24
1.3.3 Xming 图形终端	26
1.4 初次接触 Linux	28
1.4.1 简单操作	28
1.4.2 运行 HelloWorld 程序	33
1.5 小结	37
第 2 章 程序编译与运行	38
2.1 编译的各阶段	39
2.1.1 源代码	39

2.1.2	预处理	40
2.1.3	编译	44
2.1.4	汇编	46
2.1.5	链接	48
2.1.6	GCC 编译驱动	49
2.2	GCC 基本用法	51
2.2.1	C 语言标准	53
2.2.2	库的使用	54
2.2.3	搜索路径	60
2.2.4	编译警告	65
2.3	GDB 调试	70
2.3.1	代码准备	71
2.3.2	运行代码	73
2.3.3	查看变量和内存	77
2.3.4	图形前端 TUI	83
2.4	小结	84
	练习	84
第 3 章	数据、运算与控制	86
3.1	x86-64 ISA	86
3.1.1	寄存器	86
3.1.2	内存空间与 I/O 空间	91
3.2	数据	92
3.2.1	数据大小、字节序	92
3.2.2	数组、结构体和联合体	95
3.2.3	数据布局	98
3.3	运算	102
3.3.1	数据传送	102
3.3.2	算术/逻辑运算	104
3.3.3	加载有效地址	106
3.4	控制	107
3.4.1	条件跳转	107
3.4.2	函数调用	127

3.5 小结	159
练习	159
第4章 链接与可执行文件	161
4.1 生成可执行文件	161
4.1.1 样例代码	162
4.1.2 进程影像	164
4.1.3 ELF 文件与装入	168
4.2 可重定位目标文件	182
4.2.1 目标文件的节(section)	183
4.2.2 符号及重定位	187
4.2.3 符号表	196
4.3 静态链接	200
4.3.1 布局	200
4.3.2 符号解析	205
4.3.3 静态重定位	207
4.4 动态链接	214
4.4.1 样例代码	215
4.4.2 动态链接库	216
4.4.3 动态链接步骤	230
4.5 小结	250
练习	251
第5章 链接脚本与 makefile	252
5.1 二进制工具和链接脚本	252
5.1.1 binutils	252
5.1.2 链接器脚本	254
5.2 makefile	267
5.2.1 makefile 基本格式	267
5.2.2 makefile 规则	270
5.2.3 makefile 变量	274
5.2.4 文件指示	277
5.2.5 函数	279

5.2.6	make	281
5.3	小结	282
	练习	283
第 6 章	程序运行	284
6.1	装入与运行	284
6.1.1	ELF 装载器	284
6.1.2	内核代码	285
6.1.3	进程与线程	285
6.1.4	工作环境	287
6.2	基本行为观察	289
6.2.1	ptrace	289
6.2.2	strace	295
6.2.3	GDB 断点原理	300
6.2.4	ltrace	301
6.3	异常行为	304
6.3.1	非法操作	304
6.3.2	响应信号	309
6.3.3	core 文件	315
6.4	小结	325
	练习	326
第 7 章	性能剖析	327
7.1	打桩方法	327
7.1.1	源代码预处理时	328
7.1.2	静态链接时	330
7.1.3	运行加载时	332
7.2	gprof	334
7.2.1	工作原理	335
7.2.2	gprof 示例	335
7.2.3	性能数据解读	343
7.2.4	图形化显示(gprof2dot.py+graphviz)	348
7.3	gcov	349

7.3.1	基于函数分析的缺点	349
7.3.2	gcov 逐行分析	351
7.4	其他分析工具	355
7.4.1	Valgrind	355
7.4.2	perf	368
7.5	小结	375
	练习	376
第 8 章	综合实例：HDFS 中实现 zlib 库的旁路	377
8.1	项目需求	377
8.2	系统分析	378
8.2.1	整体方案	378
8.2.2	Hadoop 的 gzip JNI	379
8.2.3	zlib 分析	382
8.2.4	测定 z_stream 成员大小	385
8.3	编码实现	387
8.3.1	zlib 日志	387
8.3.2	Log4c	388
8.3.3	使用 libcprss.so 库	396
8.4	功能验证	398
8.4.1	准备输入文件	399
8.4.2	zlib 原生库的压缩	399
8.4.3	libcprss.so 库的压缩	401
8.5	小结	401
	附录	402

第 1 章

实验环境构建

由于需要在 Linux 环境中观察 C 程序的行为细节,因此需要先获得一个可访问的 Linux 系统。读者可以自己安装和配置一个 Linux 系统(真实机器或虚拟机都可以),也可以通过请 Linux 系统管理员为你开设一个账号等方式。如果读者已经使用过或安装和配置过 Linux 系统,可以直接跳过本章内容,从第 2 章开始阅读。

1.1 安装 Linux

这里以安装 CentOS7 为例,为读者展示从镜像下载到安装配置的各个步骤。其他的 Linux 发行版安装细节将不同,读者可以通过 Google 或 Bing 等搜索引擎查找相应的安装方法。

1.1.1 下载 CentOS7

首先访问 CentOS 官方网站(<https://www.centos.org/>),如图 1-1 所示。

然后单击“Get CentOS Now”按钮,进入下载 ISO 镜像文件的选择页面,可以下载 DVD ISO、Everything ISO 和 Minimal ISO,如图 1-2 所示。这三者对本书的编程实践而言差别不大。另外网页上也提供了 Torrent 等其他下载方式的选择。

接着单击“DVD ISO”按钮进入到下载链接的选择网页(如图 1-3),从中选择一个速度较快的下载即可。

单击其中一个链接将开始下载 CentOS7 的 ISO 文件(约 4.7GB)。在浏览器中将弹出一个保存对话框(不同浏览器界面会不一样),如图 1-4 所示。

直接单击“保存”按钮将文件保存到本机的某个目录下。然后将 CentOS-7-x86_64-



图 1-1 CentOS 官网



图 1-2 CentOS 的 ISO 镜像选择页面

DVD-1611.iso 镜像刻录成启动光盘、启动 U 盘或者通过 PXE 方式进行安装。

1.1.2 CentOS7 安装

下面介绍 CentOS7 的安装,这里先介绍字符登录界面的安装,后面介绍图形桌面的安装。读者请根据自己的喜好选择。

1. 简易安装

将刻录好的 CentOS7 安装启动盘插入光驱,重新启动计算机,将进入安装界面,如图 1-5 所示。

CentOS on the Web: CentOS.org | Mailing Lists | Mirror List | IRC | Forums

In order to conserve the limited bandwidth available .iso images are not downloadable from mirror.centos.org

The following mirrors should have the ISO images available:

Actual Country -

http://mirror.bit.edu.cn/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.yun-idc.com/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.bttc.net/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.cn99.com/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.aliyun.com/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.neusoft.edu.cn/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.zju.edu.cn/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.163.com/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.tuna.tsinghua.edu.cn/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirror.lzu.edu.cn/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://mirrors.nwsuaf.edu.cn/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://ftp.sjtu.edu.cn/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso

Nearby Countries -

http://ftp.tc.edu.tw/Linux/CentOS/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso
http://ftp.ksu.edu.tw/pub/CentOS/7/isos/x86_64/CentOS-7-x86_64-DVD-1611.iso

图 1-3 CentOS7 x86-64 ISO 下载链接

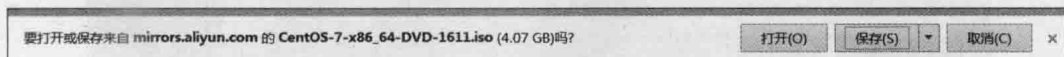


图 1-4 浏览器保存下载文件的对话框

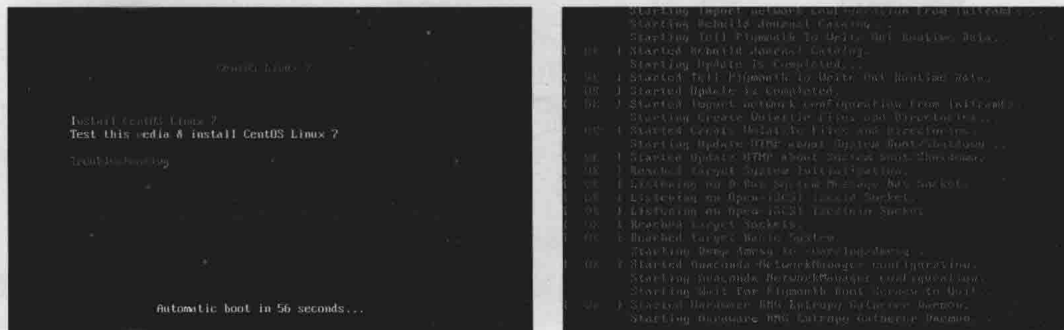


图 1-5 CentOS7 安装启动界面

选择第一项“Install CentOS Linux 7”并按回车键，等待片刻将出现图形的安装界面，如图 1-6 所示。在里面选择“中文”，然后再单击“继续”按钮进入下一窗口，如图 1-7 所示。

单击图 1-7 所示的“系统→安装位置”，进入后直接单击“完成”即可，此时图 1-7 的



图 1-6 语言选择



图 1-7 安装信息摘要

“开始安装”按钮变成激活可用状态。如果希望使用图形桌面,则需要单击进入“软件选择”进行必要的选择(参见图 1-12)。如果不需要图形桌面,则单击“开始安装”按钮进入下一步,如图 1-8 所示。



图 1-8 设置 ROOT 用户密码并创建普通用户

然后分别单击图 1-8 所示的两个带感叹号的图标,在相应的对话框中进行 ROOT 根用户密码设置和创建用户的设置。这两项工作完成后,图标上的感叹号将消失。窗口的底端有安装进度条(如图 1-9 所示),完成后在进度条下方出现“重启”按钮。

然后单击“重启”按钮重启系统,进入到 Linux 的字符登录界面,如图 1-10 所示。

输入前面设置的用户名及其密码登录到系统中,此时可以正式开始使用 Linux 系统。图 1-11 是登录后执行 `uname` 命令查看系统信息的输出,表明其 Linux 内核是 3.10.0 版本、x86_64 位的。

如果读者在前面安装选项中没有选 GCC 开发工具,此时可以用 `yum -y install gcc` 命令完成安装,其他所需的软件在后续学习中用到的时候再安装。

2. 图形桌面安装

在安装过程的“安装信息摘要”环节(见图 1-7),如果单击“软件选择”按钮可以进入图 1-12 所示的窗口,此时可选择使用图形桌面或安装更多的其他软件包。