

Mastering Red Hat Linux 9

红帽 Linux 9

从入门到精通

[美] Michael Jang 著

邱仲潘 等译

windecember.cn

本书全面覆盖使用红帽 Linux 作为
服务器或操作系统的知识



电子工业出版社
Publishing House of Electronics Industry
<http://www.phei.com.cn>

Mastering Red Hat Linux 9

红帽 Linux 9

最新推出“从入门到精通”系列丛书

Rational XDE从入门到精通
UML与Rational Rose 2002从入门到精通
Delphi 7从入门到精通
Java 2从入门到精通(J2SE 1.4版)
JavaScript从入门到精通(黄金版)
JSP从入门到精通
Visual Basic.NET从入门到精通
Visual C#.NET从入门到精通
Visual Basic.NET数据库编程从入门到精通
C#数据库编程从入门到精通
Visual Basic 6从入门到精通
Visual C++ 6从入门到精通
XML从入门到精通(黄金版)
ASP.NET与VB.NET从入门到精通
ASP.NET与C#从入门到精通
XSLT从入门到精通
PHP 4.1从入门到精通
Kylinx 2从入门到精通
Cisco路由器从入门到精通(第二版)
网络布线从入门到精通
网络安全从入门到精通(第二版)
网络安全积极防御从入门到精通
SQL Server 2000从入门到精通
SBS 2000服务器从入门到精通
Windows 2000 Server从入门到精通(第四版)
Windows Server 2003活动目录从入门到精通(第三版)
Windows XP家庭版从入门到精通(中文版)
Windows XP专业版从入门到精通(中文版)
Windows XP注册表从入门到精通
红帽Linux 9从入门到精通
Project 2002从入门到精通(中文版)
水晶报表Crystal Reports 9从入门到精通
Lotus Notes与Domino 6从入门到精通
AutoCAD 2002从入门到精通
Dreamweaver MX数据库从入门到精通
Autodesk VIZ 4从入门到精通

ISBN 7-5053-9127-5



9 787505 391277 >



从入门到精通

本书在如下方面为读者提供指导:

- 最新版本红帽Linux的安装、配置、安全和管理
- 重要的Linux命令
- 建立GNOME、KDE和基于GUI的应用程序
- Linux网络服务的配置和诊断

作者简介:

Michael Jiang获得了RHCE、Linux+和LCP认证,专门从事Linux及其认证的撰稿工作。他在计算机方面具有多年经验。他的著作涉及Linux、Linux认证、红帽Linux以及Windows 98/XP。

本书贴有激光防伪标志,凡没有防伪标志者,属盗版图书。

责任编辑:陈宇 陈双

ISBN 7-5053-9127-5/TP·5275

定价:75.00元

Mastering Red Hat Linux 9

红帽Linux 9从入门到精通

〔美〕 Michael Jang 著

邱仙菊 等译

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 提 要

本书是红帽Linux 9的完整指南。无论把Linux作为服务器还是桌面操作系统, 本书都提供了安装、配置与管理最新操作系统的实用信息。本书介绍的内容包括Linux安装, 命令行界面, Linux系统管理与配置, 诊断引导过程, 内核重新编译, 使用GNOME与KDE, 了解基本TCP/IP网络, 保护Linux防火墙, 设置安全远程访问, 安装和测试DNS、DHCP、CUPS与sendmail, 配置和查错FTP、NFS、Samba与Apache, 另外还介绍了Linux认证的要求。

本书适合于有兴趣学习红帽Linux的各层次读者。



Copyright©2003 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.

本书英文版由美国SYBEX公司出版, SYBEX公司已将中文版独家版权授予中国电子工业出版社及北京美迪亚电子信息有限公司。未经许可, 不得以任何形式和手段复制或抄袭本书内容。

版权贸易合同登记号: 01-2003-1086

图书在版编目 (CIP) 数据

红帽Linux 9从入门到精通/(美)江(Jang, M.)著;邱仲藩等译.一北京:电子工业出版社, 2003.10

书名原文: Mastering Red Hat Linux 9

ISBN 7-5053-9127-5

I. 红… II. ①江… ②邱… III. Linux操作系统 IV. TP316.89

中国版本图书馆CIP数据核字(2003)第079219号

责任编辑: 陈 宇 陈 双

印 刷: 北京天竺颖华印刷厂

出版发行: 电子工业出版社 <http://www.phei.com.cn>

北京市海淀区万寿路173信箱 邮编: 100036

北京市海淀区翠微东里甲2号 邮编: 100036

经 销: 各地新华书店

开 本: 787×1092 1/16 印张: 46.125 字数: 1180千字

版 次: 2003年10月第1版 2003年10月第1次印刷

定 价: 75.00元

凡购买电子工业出版社的图书, 如有缺损问题, 请向购买书店调换, 若书店售缺, 请与本社发行部联系。联系电话: (010) 68279077。质量投诉请发邮件至zlts@phei.com.cn, 盗版侵权举报请发邮件至dbqq@phei.com.cn。

谨将本书献给失去亲人的人们，我们的生活已经变了颜色，但日子还会好起来的。

亲爱的南希，我想你。我觉得快乐，是因为你的精神仍然活在我心里。我正在做你一直鼓励我做的善事。我要为我们俩好好活着。

致 谢

创作一本计算机书籍是许多人努力的成果。**Ellen Dendy**很有先见之明地提出了这本书的计划，**Linux**正领导着技术部门的复兴。**Brianne Agatep**从头到尾指导着本书的开发，努力使这项工作保持在轨道上。**Leslie Light**的优秀生产管理技巧使我在个人生活大受波折的时候能够专心写作。**Liz Welch**高超的编辑技巧使任何对**Linux**感兴趣的人都能阅读这本书。

如果没有小组中其他成员专心和艰苦的努力，本书也不可能成形。感谢**Jill Niles**、**Maureen Forys**、**Ted Laux**与**Elizabeth Campbell**。

对本书和对我的新生活特别重要的是，我要特别感谢**Elizabeth Zinkann**，她是非凡的技术编辑专家、逻辑**Linux**专家和我的好朋友，她不仅是我见过的最高超的**Linux**技术编辑，而且在我渡过心理困境期间一直耐心倾听和给予帮助。

建立一个操作系统需要一个团队。感谢全世界几千位开发人员投入时间把**Linux**建成挑战垄断的操作系统。其中两位还帮我建立了本书的一些新的图形应用程序：**Rob Buis**建立了**KDE**项目，**Jody Goldberg**建立了**GNOME**项目。

个人方面，感谢**Donna**，感谢你的爱与支持。谢谢你帮我理解到，我们总是会想念离去的亲人，谢谢你鼓励我重新寻找生活与爱。你是我新生活中的爱！谢谢你给我带来了我们共同的新记忆。

我充满希望，因此我能生活下去。

译 者 的 话

本书翻译过程中得到了周阳生、刘文红、邹能东、彭振庆、黄志坚、李耀平、郭王旋等同志的大力帮助，刘文琼、邱冬金、邱燕明、黄素平等同志完成了本书的录入工作，刘云昌、刘联昌兄弟帮助进行了书稿与打印稿的校对，在此深表感谢。

前 言

据《商业周刊》2003年3月3日称，Linux是“在漫长而痛苦的技术困境中少数几个欣欣向荣的技术产品之一”。

Red Hat Linux是一流的Linux发行版本。本书帮助你在工作和生活中有效地利用Red Hat Linux 9，可以作为服务器，也可以作为桌面操作系统。

Linux不仅便宜，而且可靠，还很安全。利用Linux，可以得到所要的计算应用，费用只是其他操作系统的一小部分。你不必担心许可证费用，而且可以用手头的工具建立定制方案。

在这个信息技术预算紧张的时代，各公司越来越因为经费有限而转向Linux。财经界的巨子Goldman Sachs、Merrill Lynch和Morgan Stanley等公司都转向Linux了。Amazon与Google之类的大型公司也用Linux支持自己的系统。IBM公司和惠普公司靠Linux产生了几十亿美元的收入。这种例子真是不胜枚举。

尽管Linux的核心是命令行界面，但红帽子公司开发了一系列优秀的图形工具，可以帮助其他操作系统管理员方便地过渡到Linux。Linux是为网络建立的，是of TCP/IP定制的，而TCP/IP是互联网上的基本协议。

Red Hat Linux是最著名的Linux发行版本，包括办公室组件和专用服务等应用程序，很容易使每台计算机节省几百美元。

Linux是自由的选择，可以免费下载Red Hat Linux 9，可以从第三方支付一些名义费用取得，可以购买Red Hat Linux，从而得到红帽子公司文档与支持。在前言末尾将介绍其中每一个选项。但是，不管你使用哪个版本，本书都可以帮你充分利用Red Hat Linux的功能。

本书内容

本书分八大部分，每个部分解决不同的技能，帮你充分利用Red Hat Linux的功能。你可以从头到尾阅读本书，也可以在需要时查找特定技能的相关内容。

安装Red Hat Linux 第1章介绍Linux作为桌面、作为小公司服务器和作为企业服务器的角色。如果你准备在多台计算机上安装Linux，则要认真阅读第2章，因为你要保证硬件支持Linux。第3章介绍用图形用户界面在本地安装Red Hat Linux，而第4章介绍如何在网络上安装Linux。第5章介绍如何使安装过程自动化，如果要在多台计算机上安装Red Hat Linux，则这个方法非常方便。

Linux基础 为了深入了解Linux，需要知道如何使用命令行界面。第6章介绍如何进行文件系统导航，学完之后就很容易使用命令行界面了。第7章介绍如何组织文件系统。第8章介绍如何利用命令行shell。

基本Linux管理 由于Linux是为网络建立的，因此也提供了几个管理工具。要管理这个多用户系统，就要知道如何生成、组织和管理用户与组（第9章）。我们还介绍如何

用Red Hat Package Manager和up2date安全地安装、升级和管理应用程序（第10章）。作为管理员，你要深入了解引导过程（第11章）和Linux内核（第12章），还要知道如何自动化、管理和诊断基本服务（第13章）以及如何备份系统（第14章）。

X窗口管理 桌面用户需要图形用户界面（GUI）。尽管普通用户不能修改基本X窗口配置（第15章），但管理员需要能够熟练操作。两大Linux GUI桌面环境的基础是：GNOME（第16章）和KDE（第17章）。可以在这些GUI桌面环境中安装几个有用的应用程序，包括多办公室组件（第18章）。不太熟悉命令行界面的管理员可以利用第19章介绍的图形化Red Hat管理工具。

基本Linux网络 Linux是为网络建立的，是为TCP/IP定制的，而TCP/IP是互联网上的基本协议。我们将介绍Linux中用到的基本TCP/IP知识，第20章介绍基本TCP/IP协议，第21章介绍用于局域网（LAN）的TCP/IP命令，第22章介绍网络安全基础。

Linux网络服务 Linux要为网络上所有计算机服务。作为管理员，你要知道如何配置远程访问（第23章）。TCP/IP网络需要域名和IP地址，它们被组织在DNS与DHCP服务器中（第24章）。网络用户还要打印（第25章）和使用E-mail（第26章）。

Linux文件共享服务 用户在计算机之间共享文件。Red Hat Linux中有多种共享文件的方法。可以为文件设置NTFS服务器（第27章）。如果管理的计算机网约运行Linux和其他UNIX操作系统，则可以和NFS、NIS服务器共享目录和配置文件（第28章）。如果网络中还有Microsoft Windows计算机，则可以让Linux计算机作为这个网络上的客户机或服务器（第29章）。最后，Apache是互联网中最普及的Web服务器，针对Linux进行了优化（第30章）。

附加认证基础材料 Sybex的网站（www.sybex.com）中还提供了各种Linux证书的附加材料。许多读者学习Linux是为了增加就业机会。如今，已经有这方面的Linux证书。三大主要的Linux证书项目是CompTIA的Linux+考试，SAIR的Linux认证专业人员与管理、LPI的Level I考试。网站上附加的第1章概述了这些考试，针对具有六个月到两年经验的Linux用户。网站上附加的第2章主要介绍Red Hat证书要求，包括Red Hat认证技术员和Red Hat认证工程师。

附录 本书是你Linux学习过程的一部分。书后的附录详细列出了每个管理员要在命令行界面中熟悉的几个命令。在Sybex的站点（www.sybex.com）中还有三个其他的附录材料。网站上附加的第3章简要列出了更多联机资源，第4章是GNU通用许可证文件，第5章按组介绍Red Hat Linux包，详细介绍了comps.xml文件，其中提供了Red Hat Linux安装的基础。

本书使用的约定

如果你刚开始使用Sybex公司的书籍，则应熟悉本书使用的一些约定。

- Linux命令（如ls）和文件（如/etc/passwd）放在段落主体中时，以内联代码形式偏移。
- 较长的命令与代码清单分行组织。命令行用散列号（#）显示。

```
# mkbootdisk 2.4.20-8
```


- 散列号 (#) 也在程序文件中表示说明语句，作者尽量区别不同情境。

```
# System initialization
```

- 有时，输入的代码取决于版本号之类的变量，这时会将代码显示为斜体字：

```
# mkbootdisk kernel_version
```

- 由于印刷的限制，我们用续行箭头 (↵) 将命令行分隔如下：

```
passwd chat = *New*password* %n\n *Retype*new*password* %n\n *passwd:
↵*all*authentication*tokens*updated*successfully*
```

但输入时仍要在一行中输入。

- 如果代码中一个项目显示为黑体字，则表示要在命令行界面输入这个内容以取得指定的输出：

```
# /usr/lib/yp/ypinit -m
```

这时我们要构造运行NIS服务器的主机表。RH9在NIS服务器的主机表中。请一行一行增加其他主机名。完成之后，输入<control D>。

- 加号表示键组合，例如Ctrl+Alt+F2表示要同时按这几个键。
- URL省略http://用省略斜杠，使用短简洁，同时避免不良的分行。例如，Linux文档项目的主页为www.fkdp.org，技术上应为http://www.fkdp.org/。但在根居Apache之类的服务器软件和Web浏览器的默认设置，这两者通常没有差别。
- 介绍Linux GUI时，命令箭头指向菜单或子菜单选项。例如，Main Menu►Graphics►The Gimp表示单击Main Menu按钮，移到Graphics菜单，然后单击The Gimp。

说明：说明通常提供主题以外的其他信息。

提示：提示则用于帮助常规使用，如配置应用程序。

警告：警告指出应用程序、操作系统、硬件等的危险。

取得Red Hat Linux 9

为了方便起见，我们的选配光碟中提供了Red Hat Linux 9的一个版本，共两张光碟。由于空间所限，本书选配光碟中并没有提供Red Hat Linux 9的162个软件包。其中一些软件包对Linux管理员很重要，如第12章介绍的kernel-source-* RPM。此外，该版本中另外25个软件包或者内容不多，或者已经过时。

如果从本书选配光碟安装Red Hat Linux 9，则这个过程会跳过第3章和第4章介绍的有些步骤。因此，建议使用Red Hat Linux 9的完整版本，共三张光碟。可以用三种方法取得Red Hat Linux 9的完整版本：

- 可以免费下载三张Red Hat Linux 9安装光碟，然后将数据写入空白光碟中（如果有光碟刻录机）。奇妙的是，下载的光碟实际上比购买的Red Hat Linux软件具有更新一些的软件包。
- 可以从第三方资源购买三张Red Hat Linux 9安装光碟。

- 可以购买正式的Red Hat Linux 9个人版或专业版软件。安装Red Hat Linux 9之后，可以用第10章介绍的up2date实用程序确保在计算机上安装最新软件包。此外，如果要按第4章介绍的方法，通过FTP连接安装Red Hat Linux 9，则建议使用第27章介绍的vsFTP服务器。

下载Red Hat Linux 9

如果你使用电缆调制解调器或DSL适配器之类的高速Internet连接，则可以下载三张Red Hat Linux 9安装光碟。建议使用gFTP之类的FTP客户机。Microsoft Windows用户可以使用WS FTP与Cute FTP之类的FTP客户机。任何GUI FTP客户机上的步骤都差不多。

说明：我曾经想在电话调制解调器上下载Red Hat Linux，结果花了将近两天时间才下载了第一张安装光碟。下载之后才发现，数据搞乱了。如果通过电话调制解调器连接Internet，则建议从红帽子公司或第三方购买Red Hat Linux。

要下载Red Hat Linux 9光碟，就要有一个FTP客户机，硬盘上要有足够的空间（三张Red Hat Linux 9安装光碟至少要求2.1GB自由空间），还要有下列信息：

FTP站点 尽管标准FTP站点是ftp.redhat.com，但这个FTP站点通常太忙。还有许多镜像站点，可以从www.redhat.com/download/mirror.html取得。通过镜像站点访问可能速度更快（特别是在美国以外的地方）。但要确认下载的Red Hat Linux版本与镜像站点版本之间通常会有一个时间差。

用户名与口令 下载Red Hat Linux 9光碟的FTP站点（包括ftp.redhat.com）通常允许匿名访问。在这些站点中，用户名为anonymous，口令为你的E-mail地址（但这不是必需的）。

FTP服务器上的目录 FTP服务器上的目录随所用FTP站点不同而不同。尽管Red Hat Linux光碟文件应在/pub/redhat/linux目录的某个子目录中，但可能需要浏览一下才能找到。

正确的光碟 在下面的表中可以看到六张Red Hat Linux 9光碟，代码名为Shrike：

```
shrike-i386-disc1.iso
shrike-i386-disc2.iso
shrike-i386-disc3.iso
shrike-i386-SRPMS-disc1.iso
shrike-i386-SRPMS-disc2.iso
shrike-i386-SRPMS-disc3.iso
```

前三张Shrike光碟是二进制安装光碟，是计算机上安装Red Hat Linux所需要的。后三张Shrike光碟包含相关的源代码。

在有些FTP站点中，还可能看到其他光碟，包括Red Hat Linux文档和一张扩展救援光碟。

一台光碟刻录机 Red Hat Linux 9光碟放在一个大文件中。需要有光碟刻录软件和光驱，将数据写入可写光碟中。Linux中有几个不错的光碟刻录软件，见第14章和第16章介绍。

其他指令见红帽子公司站点：www.redhat.com/download/howto_download.html。

带Red Hat Linux 9安装文件的第三方光碟

并不是每个人都有高速Internet连接。如果没有高速Internet连接,则更实用的方法是购买带Red Hat Linux 9安装文件的第三方光碟,三张通常只要10美元左右(或更少)。

可以在directory.google.com站点找到这些经销商的名录,可以单击Computers►Software►Operating Systems►Linux►Companies►Resellers访问这个名单。

说明: 通用许可证(见Sybex公司站点上Web Chapter 4或www.gnu.org/copyleft/gpl.html)允许免费下载和自由发布Red Hat Linux 9,可以销售下载的光碟。光碟内容可以和Red Hat Linux 9一致。但如果你不是红帽子公司,则经销光碟时不能称其为Red Hat Linux。

取得Red Hat Linux 9产品

可以从www.redhat.com站点和许多计算机经销商那里购买完整的Red Hat Linux版本。有两个选项:

- Red Hat Linux 9个人版共七张光碟:安装软件包放在三张光碟上,另外三张光碟上是每个包的源代码,还有一张光碟包括HTML与PDF格式的文档。这个版本有30天的Web安装支持和30天的单机Red Hat Network订阅期。
- Red Hat Linux 9企业版共九张光碟:安装软件包放在三张光碟上,另外三张光碟上是每个包的源代码。其他光碟包括文档、办公室与多媒体应用程序和系统管理工具。所有这些信息也在DVD中提供。这个版本有60天的电话与Web安装支持和60天的单机Red Hat Network订阅期。

其他版本也带有支持,见第1章介绍,详细清单见www.redhat.com/software站点。

欢迎反馈

我们出版此书是为了满足读者的需求,只有读者才能判断我们是否成功了。如果你有什么需要的课题在书中没有介绍,或发现有任何错误,请到www.sybex.com站点寻找本书页面,并单击Submit a Review链接,提出宝贵意见。当然,如果本书能帮你更快更好地使用Red Hat Linux,或我们介绍了你特别喜欢的特性,也请告诉我们。无论是好是坏,你的反馈都有助于我们推出更好的下一版。

目 录

第一部分 安装Red Hat Linux	1
第1章 Red Hat Linux简介	1
Red Hat Linux 9简介	2
UNIX与Linux简史	5
了解内核	8
为什么选择Linux	9
Linux计算机的角色	11
小结	14
第2章 准备硬件	15
创建硬盘分区	15
在同一计算机上安装Microsoft与Linux	17
为什么考虑硬盘	21
检查兼容硬件	22
准备硬件检查表	26
BIOS提示	28
小结	29
第3章 本地安装Linux	31
用引导盘启动	31
检查安装光碟	36
一步一步安装Red Hat Linux	38
运行红帽子安装主体	78
安装查错	86
登录	90
升级Red Hat Linux	91
小结	94
第4章 通过网络安装Linux	95
准备NFS服务器	95
准备Apache Web服务器	98
准备FTP服务器	100
通过网络安装Linux	101
查错网络安装	135
小结	136

第5章	用Kickstart安装Linux	137
	用comps.xml文件组织包	137
	分析默认Kickstart的配置	147
	使用GUI Kickstart Configurator	154
	从软盘运行Kickstart	164
	小结	165
第二部分	Linux基础	167
第6章	从命令行开始	167
	探索导航命令	167
	建立文件与目录	169
	管理文件	173
	操纵文件	176
	使用vi编辑器	178
	了解其他文本编辑器	180
	小结	182
第7章	文件系统简介	183
	了解文件系统层次标准	183
	管理分区	185
	使用格式与杂志	189
	修改/etc/fstab文件	195
	探索逻辑卷管理系统	196
	小结	198
第8章	有效利用shell	199
	管理shell	199
	配置shell	201
	shell的秘密	204
	小结	210
第三部分	基本Linux管理	211
第9章	安全管理用户与组	211
	基本用户与组管理	211
	管理用户账号	215
	阴影口令组	219
	配额	220
	使用专用组	223
	小结	224
第10章	用RPM管理包	226
	简化安装与升级	226

使用源代码RPM包	230
RPM包安全性	233
更新RPM包	235
特殊主体: up2date	235
小结	238
第11章 配置与查错引导过程	239
探索基本引导过程	239
了解默认配置文件	240
查错与使用救援盘	247
小结	252
第12章 升级与重新编译内核	253
为什么要升级和重新编译内核	253
简单升级	254
Tarball与补丁包	257
定制内核	258
设置配置菜单	262
内核的不同编译	266
引导装入器更新	283
小结	285
第13章 管理细节	286
使用cron监控程序	286
使用at监控程序	289
服务管理	290
查错日志	292
进程管理	297
小结	299
第14章 备份系统	300
探索备份概念	300
介质选择	302
使用备份与恢复命令	303
了解RAID	310
小结	315
第四部分 管理X窗口	317
第15章 管理X客户机与X服务器	317
使用基本配置工具	317
了解配置文件	328
查错X窗口	337
小结	339

第16章	GNOME	340
	基本GNOME界面	340
	了解其他GNOME项目	352
	小结	377
第17章	KDE	378
	使用基本KDE界面	378
	KDE控制中心	383
	了解KDE实用程序	400
	小结	416
第18章	GUI应用程序	417
	了解OpenOffice	417
	了解GNOME Office	424
	使用Koffice	429
	使用图形应用程序	434
	小结	441
第19章	红帽子图形前端	442
	用基本配置实用程序进行设置	443
	用网络配置实用程序连接	448
	使用系统管理实用程序	456
	使用服务配置实用程序	465
	小结	467
第五部分	Linux联网基础	469
第20章	TCP/IP基础	469
	搜索网络基础	469
	了解协议栈	471
	学习TCP/IP基础	473
	使用IP地址	476
	小结	479
第21章	在局域网中管理Linux	480
	了解网络硬件	480
	在局域网上配置计算机	482
	配置公网与专网	485
	建立Internet连接	489
	网络查错	493
	小结	495
第22章	保护Linux网络	497
	了解最佳做法	497
	使用可插入验证模块 (PAM)	499

建立防火墙	501
设置IP伪装	508
入侵检测	508
查错访问问题	511
小结	512
第六部分 Linux网络服务	515
第23章 远程访问与xinetd服务	515
使用典型扩展服务	515
用TCP包装器控制访问	519
了解安全Shell	521
查错访问问题	523
小结	524
第24章 DNS与DHCP	526
配置DNS服务器	526
使用DNS客户机	536
设置DNS服务器	536
使用DHCP与BOOTP客户机	539
小结	540
第25章 用CUPS与LPD打印	542
使用IPP（Internet打印协议）	542
配置CUPS（公共UNIX打印系统）	543
使用LPD（行打印监控程序）	565
小结	572
第26章 邮件服务	574
介绍一般电子邮件服务	574
配置sendmail	576
使用入站电子邮件服务器	584
配置邮件客户机	585
小结	591
第七部分 Linux文件共享服务	593
第27章 FTP客户机和服务器	593
使用FTP客户机	593
配置安全FTP服务器	597
生成匿名FTP服务器	601
用实名配置WU-FTP	603
小结	608

第28章	Linux共享服务：NFS与NIS	610
	配置NFS服务器	610
	使用NFS客户机	617
	配置NIS服务器	618
	使用NFS客户机	624
	小结	626
第29章	利用Samba	627
	沟通Linux与Microsoft Windows	627
	配置Samba客户机	629
	了解Samba配置文件	632
	Samba Web管理工具（SWAT）	648
	redhat-config-samba工具	655
	小结	657
第30章	Web服务	659
	探索Web服务器选项	659
	了解Apache基础	660
	配置Apache	661
	配置Red Hat GUI Apache实用程序	685
	集成Red Hat Content Accelerator	693
	小结	695
附录	Linux命令手册	697

第一部分 安装Red Hat Linux

第1章 Red Hat Linux简介

Linux可以很好地运行计算机，它可靠、安全、灵活，很容易安装，而且比人们想像的容易使用，它很容易定制，是针对网络建立的。由于可以免费下载最新的完整**Linux**操作系统，因此价格是合理的。

对许多人而言，**Linux**就是**Red Hat Linux**。其实不完全对。**Linux**是由全世界的志愿社区开发软件，最初的工作主要是由伯克利大学（www.usf.org）启动的。**Linux**最初是作为**UNIX**操作系统的克隆而开发的，如今则更是如此。**Linux**已经演变成满足许多不同用户的要求，包括航天工程师、电影制作者、理论物理学家和消费者。是的，包括消费者。甚至沃尔玛公司也在销售装有**Linux**版本的计算机。

严格地说，**Linux**只是个内核，是操作系统中支持软件与硬件通信的部分。但这是一个多么精彩的内核。可以通过无数种方法定制，可以更新特性。只要配置正确，就可以在计算机上优化有效的速度。

Red Hat Linux是个发行版本，包括**Linux**操作系统和几个免费应用程序，包括特性完整的办公组件以及满足大多数用户要求的图形和多媒体程序。相比之下，微软的程序使用户为每台计算机都要花上几百美元。

Linux很快成为替代**Microsoft Windows**的主要产品。作为服务器，它包括配置与管理各种网络所需的所有工具。它有一些大公司支持，到本书编写时，包括**Oracle**、戴尔和惠普公司。**IBM**公司已经在**Linux**中投入几十亿美元。越来越多的公司用**Linux**作为服务器，作为桌面操作系统。

说明：如果你专门使用Apple Macintosh机器，记住，最新的Mac OS X是从与**Linux**密切相关的**BSD**（伯克利标准版本）操作系统开发出来的。

Linux背后没有一家公司，但可以得到**Linux**方面的支持。红帽子公司提供很好的支持系统，其他公司也会提供支持。如果你参与**Linux**社区，则会有几千个开发人员愿意伸出手来帮助你。本章介绍下列主题：

- **Red Hat Linux 9**简介
- **UNIX**与**Linux**简史
- 分析内核
- 为什么选择**Linux**

• Linux计算机的角色

Red Hat Linux 9简介

Red Hat Linux 9不仅是个操作系统，而且是个完整的发行版本，包括各种命令、实用程序和应用程序。从光碟中安装附加软件包非常容易。只要从因特网下载所要的软件包，就可以使Red Hat Linux版本保持更新。

其他Red Hat Linux产品

到本书编写时，Red Hat Linux有多个版本，它们都包括Red Hat Linux 9的基本软件，可以用前言中介绍的目录下载。每个版本还有其他特性，如光碟与支持，但这是要支付费用的。到本书编写时，可以得到的特性包括：

Red Hat Linux 9.0个人版

前言中曾介绍过，Red Hat Linux 9.0个人版共七张光碟，安装软件包放在三张光碟上，另外三张光碟上是每个包的源代码，还有一张光碟包括HTML与PDF格式的文档。它包括个人桌面、工作站、服务器和定制配置中安装Red Hat Linux所要的文件。这个版本有30天的Web安装支持和60天的单机Red Hat Network订阅期。

Red Hat Linux 9.0专业版

Red Hat Linux 9.0专业版共九张光碟，安装软件包放在三张光碟上，另外三张光碟上是每个包的源代码。其他光碟包括文档、办公室与多媒体应用程序和系统管理工具。所有这些也在DVD中提供。这个版本有60天的电话与Web安装支持和60天的单机Red Hat Network订阅期。

尽管可以将任何Red Hat Linux版本安装成服务器，但下列Red Hat Linux版本是为多个CPU的服务器设计，其预订包括预订期间的免费更新特性。

Red Hat Enterprise Linux WS（工作站）

Red Hat Enterprise Linux WS（工作站）包括Red Hat Linux 9.0中的组件，并将特性定制成适用于Red Hat Enterprise Linux Servers（企业服务器）。这个操作系统在64位Itanium 2工作站中提供。

Red Hat Enterprise Linux ES（基本服务器）基础版

这个Red Hat Linux版本支持基本服务器，只限于两个CPU和4GB内存。基本版包括下载、基本安装与配置支持（90天）和一年内通过红帽子企业网络的支持。

Red Hat Enterprise Linux ES（基本服务器）标准版

这个Red Hat Linux版本支持基本服务器，只限于两个CPU和4GB内存。标准版包括下载、基本安装与配置支持和一年内通过红帽子企业网络的支持。

Red Hat Enterprise Linux AS（高级服务器）标准版

Red Hat Enterprise Linux AS（高级服务器）标准版包括Red Hat Enterprise Linux ES服务器的组件与支持，加上一年的安装支持、配置支持、高级配置支持和系统管理支持。

Red Hat Enterprise Linux AS（高级服务器）黄金版

Red Hat Enterprise Linux AS（高级服务器）黄金版包括Red Hat Enterprise Linux AS（高级服务器）标准版的组件与支持，加上高可用性群集支持和一级严重问题的不间断应急支持，见相关许可证中定义。

其他红帽子产品

还有一些其他红帽子产品，包括高度安全的Stronghold Enterprise Apache Server和专门为IBM公司eServer平台设计的版本。

基本硬件要求

表1.1列出了Red Hat Linux 9的基本硬件要求。这些要求不是绝对的，例如，我用命令行界面运行Red Hat Linux 9时，只要16MB内存。其他硬件要求见第2章介绍。

表1.1 基本硬件要求

类型	基本要求
CPU	奔腾级 文本方式建议：200MHz Pentium III以上 图形方式建议：400MHz Pentium III级以上
内存	文本方式工作站为64MB，图形工作站为128MB（建议用192MB）
硬盘	475MB（不包括交换空间和其他文件），其他类型安装见第3章介绍

这些基本硬件要求假设是使用最基本服务的独立Linux计算机。旧版Red Hat Linux甚至可以在更少内存的Intel 386机器上安装。如果要安装其他软件、配置图形用户界面（GUI）或建立服务器，则要求相应增加。

新特性

红帽子公司不断更新软件和增加新特性。最重要的是更新最新内核与服务。下面列出了红帽子最近增加的主要功能：

- Linux内核2.4.20版本，包括Linux 2.5测试系列内核中经过证明的改进和几个更新驱动程序。
- CUPS（常用UNIX打印系统），现已代替LPD成为默认的打印服务器，详见第25章介绍。
- Apache 2.0.40，现已成为标准Red Hat Linux Web服务器，详见第30章。
- iptables，现已成为默认的防火墙工具（详见第22章介绍）。
- OpenOffice，完全特性的Microsoft Office式应用程序，详见第18章介绍。
- XFree86 Version 4.3支持其他图形适配器，还包括对RandR、X Resize、Rotate与Reflect扩展的支持（www.xfree86.org/~keithp/talks/randr/protocol.txt）。

红帽子还配置了几个其他Linux发行版本中没有的工具。可以在GNOME与KDE之类的图形用户界面（GUI）中通过命令行界面的redhat-config-*命令启动这些工具。例如，redhat-config-samba可以配置Samba服务，使Linux可以在Microsoft Windows网络中使用。Samba见第29章介绍。

基本组件

Linux可以分成很多模块。Linux的模块性质使开发人员可以独立而高效地工作。他们可以复用与重新配置这些模块，得到不同结果。Linux至少有六类模块：内核、网络、init、监控程序、shell与实用程序、X窗口。

内核

内核是任何操作系统最重要的部分，使Linux和安装的任何软件可以和计算机硬件进行通信。内核通过专用设备驱动程序与硬件进行通信。例如，装载软盘时，特定内核驱动程序向软驱发消息并从软驱接收消息。

如果安装的新硬件在启动Linux时没有探测到，则可以在内核中增加一个驱动程序模块，见第11章介绍。如果要对新硬件下载驱动程序，则也要在内核中增加这个驱动程序模块。

内核的其他部分管理Linux文件系统和磁盘缓冲区之类的区域存放的任何数据。启动Linux时，内核装入保护方式的内存中。关于内核的配置与编译方法，见第12章介绍。

网络

Linux计算机通常在网络中或服务器网络中很多。这些计算机作为用户的工作站或客户机，有些作为服务器，控制不同工作站中多个用户共享的资源。在这类网络中，客户机向服务器请求所要的项目，如文件与应用程序。在Linux网络中，客户机甚至可以请求X Window信息。换句话说，可以将Linux客户机上的终端设置成从Linux服务器访问GUI数据。

Linux操作系统的网络模块保证客户机/服务器通信尽量顺利。理想情况下，客户机/服务器之间的连接是无缝的。如果网络速度足够快，则用户无法区别本地服务与网络服务。

由于网络模块与内核装入同一区域中，因此网络模块出现故障时，可能要重新启动Linux。第20章到第22章将介绍Linux网络基本知识。

init模块

一般来说，Linux程序只能用另一个Linux程序启动。例如，登录Linux终端程序mingetty。但终端程序又由谁启动呢？在计算机上启动Linux时，内核装入并启动init程序。然后init程序装载硬盘和启动终端程序。登录终端程序时，它启动命令行界面shell。

在计算机上启动Linux之后，init程序监视任何关闭计算机的信号，如不间断电源（UPS）发出的电源故障信号和重新启动命令。init程序的细节及/etc/inittab文件的控制见第11章介绍。

监控程序

Linux带有一系列服务。这些服务是后台运行的程序，在需要时启动。许多Linux服务也称为监控程序。在Linux中，可以同时运行几十个监控程序，准备启动网络、提供Web页面、打印文件和连接其他Linux或Windows计算机。典型的监控程序包括：

- Apache是互联网上最著名的Web服务器，也称为httpd。Apache见第30章介绍。
- Samba（也称为smbd）是个网络服务，使Linux可以和Microsoft Windows计算机通信。

- 打印监控程序管理与打印机的通信。CUPS监控程序是cupsd，见第25章介绍。本书将详细介绍各个Linux监控程序。

提示：Linux中的大小写是很重要的，例如常用UNIX打印系统的缩写为CUPS，而CUPS监控程序是cupsd。

Shell与实用程序

任何与内核通信的Linux程序和实用程序都是用户方式程序，包括Shell与实用程序。用户方式程序并不直接与硬件通信（内核才直接与硬件通信），换句话说，这些程序崩溃时并不影响Linux操作系统的基本操作。用户方式程序有三种基本类型：

- 登录程序将用户ID与用户Shell和其他个性化设置相关联，如X Window和Web浏览器。
- Shell程序是Linux命令解释器。最常见的Linux shell是bash，即Bourne Again Shell的简称。
- 实用程序是Shell中使用的小型命令。

第6章到第8章将介绍Bourne Again Shell的基本知识与相关命令。

X Window

Linux从不同程序模块建立图形用户界面。GNOME与KDE之类的GUI窗口管理器和所有GUI应用程序都是在X Window的基础上建立的。第15章到第19章将介绍X Window的基础和相关应用程序。

UNIX与Linux简史

Linux最初是从UNIX仿制而成的。换句话说，Linux开发人员建立系统时并没有使用建立UNIX的那些编程指令（也称源代码）。由于Linux是从UNIX仿制而成的，因此可以在这两个操作系统中使用大致相同的命令行命令。

尽管UNIX应该不难在个人计算机上采用，但Linux的开发有重要的历史原因。Linux的开发方式推动了今天的Linux开发人员、公司与用户的工作方式。

UNIX与Internet

过去，计算机非常昂贵，只能在大学和大公司中使用。当时对这些早期的计算机要求很高。为了支持这些要求，一些计算机科学家开发了分时的概念，即多个用户同时连接一台计算机。

尽管如今计算机已经更强大也更便宜了，但我们仍然要用到分时的概念。如今，管理员相当熟悉分时的概念，称这种系统为多用户系统。一个网络通常包括多台服务器，你的用户名在所有这些服务器上相同。事实上，可以说我们都是世界上最大的网络——Internet上的分时用户。

下面看看Linux发展史上的一些故事。

Multics

一个早期的分时项目是Multics（多路复用信息与计算服务），是麻省理工学院、AT&T公司贝尔实验室（现在改为朗讯公司）和通用电气公司的联合项目。尽管1969年贝尔实验室撤出这个项目，但他们的两位开发人员Ken Thompson与Dennis Ritchie仍然关注着今天我们看到的多用户操作系统。

UNIX

直到20世纪70年代初，Thompson与Ritchie仍然继续开发工作。他们成功的关键也许是用C语言编写内核和几个基本命令，包括Bourne shell中的命令。

1969年开发UNIX时，AT&T公司是美国的垄断经营者，许多法院指令和规定协议使AT&T公司无法参与计算机业务。

1974年，AT&T公司把UNIX系统送给加利福尼亚大学，只收了手册费和磁带费，使UNIX很快在几所大学普及。但是，政府规定AT&T公司不能够从中赚钱。

协作环境

贝尔实验室曾经有过许多开拓性研究，这个公司有一些高智商人员在从事基础问题方面的工作。贝尔实验室希望在学术界得到良好声誉，由于政府不允许AT&T公司以软件赚钱，因此公司保留UNIX许可证，将操作系统和源代码提供给大学，只收取少量费用。作为交换，AT&T公司的律师要求许可证中明确指出UNIX是没有担保的，这种发布方法被称为开放源代码。

时间安排得非常好，当时许多大学都在不同计算机中使用UNIX源代码。包括大型机、小型机和微型机。

与此同时，美国国防部的高级研究项目局（ARPA）要建立全国通信网络，以防核战争。这个ARPA网络中的大多数大学都使用UNIX操作系统。TCP/IP是在UNIX操作系统中建立的，最终成为ARPA网的通信协议。ARPA网最终发展成为今天的互联网。UNIX及其派生的Linux等操作系统是Internet上的关键部分。

AT&T认可法令

整个20世纪80年代，AT&T公司保留UNIX许可证。1982年美国政府处理AT&T反托拉斯案时，一个条款是：允许AT&T公司进入计算机业务，称为AT&T认可法令。这样，AT&T公司就可以销售UNIX操作系统和源代码，得到所有版权保护。

编程人员使用UNIX时希望继续保持开放源代码操作系统的好处。UNIX编程人员希望能够定制软件，学术机构希望共享结果。当时UNIX用户的知识水平很高，使开放源代码软件意义重大。

具有讽刺意味的是，AT&T公司并没有成功销售UNIX，最终出售了这个操作系统的权利，卖给SCO集团，其拥有SCO（原名为Caldera）Linux发行版本。

说明：SCO集团最近正为UNIX和IBM公司打官司，这是有争议的，许多Linux社区人士都把这看成是一种威胁。

UNIX变体

当时，由于财政限制，大学没钱购买专属的UNIX，不希望学术自由受到版权限制。一般来说，学术机构更希望共享所有数据。为此，1983年Douglas Comer开发了Xinu（把UNIX倒过来拼写），演示了一个课堂上使用的操作系统。1986年，Andrew Tannenbaum开发了Minix，是UNIX的克隆变体，是免费的。和Linux一样，Minix也不用UNIX源代码，因此没有侵犯AT&T公司的UNIX版权。

在AT&T认可法令之前，加利福尼亚大学的Bill Joy就已经开始研究UNIX。他还开始研究BSD（伯克利标准版本），它和UNIX一样是按开放源代码许可证发布的。后来的UNIX版本中引入了多个BSD实用程序。1982年，Joy开始创办Sun公司。

还有另外几个UNIX式的操作系统，见表1.2。

表1.2 UNIX式的操作系统

操作系统	描述
AIX	IBM公司开发的高级交互式执行操作系统，利用Power4与RS64 IV（64位PowerPC芯片）之类的高端CPU
BSD	伯克利标准版本，是Linux的开放源代码替代品
HP-UX	是惠普公司开发的，版本11i是为64位RISC和Itanium CPU开发的
IRIX	是Silicon Graphics公司为64位CPU开发的
Linux	UNIX的免费操作系统的克隆
Solaris	Sun公司为UltraSPARC CPU开发的
Tru64	原名为Digital UNIX，对64位CPU进行了优化
UNIXWare	AT&T公司的UNIX后续者，现属于SCO集团

一个明显的趋势是，许多公司的许多服务器都改用Linux。尽管本书基于32位Red Hat Linux内核，但也可以使用64位Red Hat Linux内核。

自由软件基金会

一些学术社区的工作最终演变成了反叛。在最初阶段，这是Richard Stallman领导的自由软件基金会（FSF）主导的（详见自由软件基金会Web站点www.fsf.org）。

1984年，Richard Stallman开始了GNU的Not UNIX（GNU）项目。他在导言性消息中指出了关心的焦点，“如果我喜欢一个程序，我就要把这个程序和其他喜欢它的人共享”。Richard Stallman的目的是建立一个强烈鼓励软件自由共享的组织。为了实现这个理想，Richard Stallman需要一个操作系统，使AT&T用版权控制的代码能够免费提供。

自由软件基金会开发了通用许可证（GPL），建立一个自由软件实体，防止使用者生成专属的封闭源代码系统。这个许可证仍然保护着今天的Linux，见Web上第4章的介绍，可在Sybex站点www.sybex.com找到。

1991年，自由软件基金会克隆了UNIX式操作系统中除内核以外的所有主要组件。

通用许可证

Richard Stallman开发的通用许可证（GPL）将原先UNIX提供的东西提供给一般软件社区。他要开发一个许可证，防止使用者生成专属的封闭源代码系统。GNU软件是按通用许可证条件发布的。尽管Web上第4章介绍了通用许可证，但也可以看看通用许可证的三大原则：

- 所有GPL软件发布时要提供全部源代码，源代码应有清晰的文档。
- 加进GPL软件的所有软件都要有清晰的文档。如果新软件与GPL软件互动，则整个软件包应作为GPL软件发布。
- 任何GPL软件都没有担保。

Linux开发内核

1991年，Linus Torvalds还是个芬兰的研究生，不喜欢新的386 CPU计算机上提供的操作系统，因此建立了一个内核，使有些操作系统组件可以和计算机硬件进行通信。1995年，几家公司把Linux开发的内核集成到自由软件基金会的GPL软件中，建立了第一个Linux发行版本。

说明：Richard Stallman和自由软件基金会人员认为Linux操作系统应该称为GNU/Linux，因为它把Linux内核组合到了大量GNU许可的程序、命令和实用程序。

了解内核

任何操作系统的生命都是始于内核，终于内核。如果正确配置，则任何操作系统都会像一场迷人的芭蕾舞表演，硬件可以随叫随到。遇到问题时，内核可能减慢或停止计算机。

利用Linux内核，可以配置硬件、文件系统、网络支持，等等。你也可以在内核式的另一模块中配置硬件驱动程序。

配置内核

如果要重新配置内核，则一定要熟悉图1.1所示的Linux内核配置菜单。可以看出，通过内核可以配置不同的硬件组件，如SCSI、USB设备。菜单中的每个按钮打开一个子菜单。

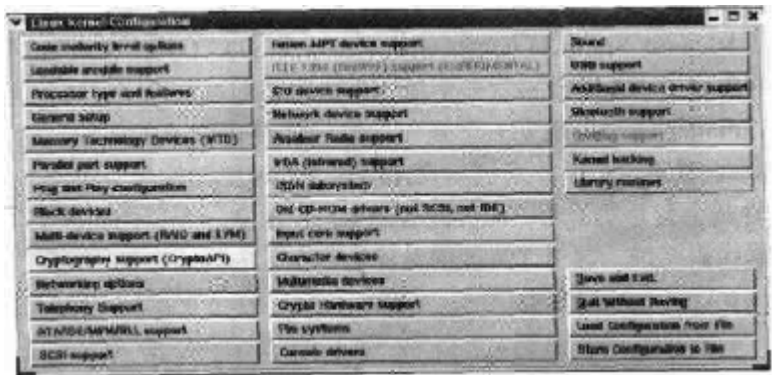


图1.1 Linux内核配置菜单

还有一些内核选项与硬件没有直接关系，如Networking Options选项与Code Maturity Level Options。例如，在网络选项菜单中，可以将Linux设置成使用不同的网络协议。第12章详细介绍了这个过程。

/proc文件系统

/proc目录是内存中存放的虚拟文件系统，记录Linux内核与计算机互动的方式。其中几个文件记录Linux内核如何读取硬件。阅读正确的文件时，可以看到不同组件的硬件设置。关于/proc的详细信息，见第11章。

模块化与一体化

可以在Linux内核的主体中设置每个硬件驱动程序，称为一体化内核。但大多数配置中有几百个硬件驱动程序。如果把所有硬件驱动程序都放在一个内核文件中，则会使硬件驱动程序长度大增，从而使系统过载。更有效的方法通常是配置模块化内核。计算机启动之后，装入不同的内核模块，通常与不同硬件组件相关联。图1.2显示了作者的桌面计算机例子。

Module	Size	Used by	Not tainted
sr_mod	44400	1 (autoclean)	
sr_mod	18168	0 (autoclean)	
parport	428	4 (autoclean)	
parport_pc	1907	1 (autoclean)	
parport	428	0 (autoclean)	
parport	37056	1 (autoclean) [parport_pc lp]	
autofs	13268	0 (autoclean) (unused)	
8139too	18088	1	
8139too	3912	0 [8139too]	
ipt_REJECT	3736	6 (autoclean)	
iptables_filter	2412	1 (autoclean)	
iptables	14868	2 [ipt_REJECT iptables_filter]	
ide-scsi	12240	0	
scsi_mod	107128	2 [sr_mod ide-scsi]	
ide-cd	35772	0	
cdrom	33696	0 [sr_mod ide-cd]	
loop	12152	0 (autoclean)	
keybdev	2976	0 (unused)	
mousedev	5492	1	
hid	22148	0 (unused)	
input	5888	0 [keybdev mousedev hid]	
usb-uhci	25412	0 (unused)	
usbcore	78432	1 [hid usb-uhci]	
ext3	84960	7	
jbd	52020	7 [ext3]	
raid5	18888	1	
Xor	9020	0 [raid5]	
lvn-mod	62176	3	

图1.2 Linux模块

可以看出，有硬件模块（如usbcore支持USB硬件），也有软件模块（如smbfs支持Samba文件系统）。第11章详细介绍了如何管理内核模块。如果要想自己的内核是模块化内核，见第12章。

为什么选择Linux

Linux通常与Microsoft Windows进行比较，Linux还可以代替表1.2介绍的其他UNIX操作系统。对许多用户与组织而言，Linux有四大优点：成本、可靠性、灵活性和支持。

成本

可以从互联网上免费下载Red Hat Linux, 而其他UNIX式操作系统的成本可能达到几千美元, 差别是明显的, 而与Microsoft操作系统的连续许可证成本一比, 差别更大。

仅仅考虑操作系统的价格是不够的, 还要考虑其他成本, 包括安装、配置与支持时间。

Red Hat Linux 9的安装选项适合不同情形, 包括家庭桌面计算机到网络服务器。更多信息见第3章。只要拥有一个操作系统发行版本, 就可以在各种不同计算机上安装Linux。

说明: 红帽子公司还基于最初的Red Hat Advanced Server推出了几个重量级服务器产品, 包括与Red Hat Linux 9中相似的软件, 并增加了红帽子公司的Stronghold Enterprise Secure Web服务器。更多信息见www.redhat.com站点。

Red Hat Linux还有一个成本优势: 光碟中带有许多特性完整的应用程序。例如, OpenOffice是个特性完整的办公应用程序, 具有大多数用户需要的所有特性。红帽子公司还提供了另外几个免费应用程序, 可以帮你省下几百美元。

安装

下面几章介绍Linux安装时, 可以看到安装过程并不复杂。如果在—组计算机上安装Red Hat Linux, 则可以用第5章介绍的启动方法将引导过程自动化。

由于大多数PC机上都能顺利安装Red Hat Linux 9, 因此第2章对硬件的介绍好像是多余的, 但如果管理员要负责在多台计算机上安装Linux, 则错误的成本是很高的。

配置

要想使用任何操作系统, 都要进行安装和配置。无论在家里配置桌面计算机、为用户配置工作站还是为公司网络配置服务器, 基本配置过程都是相同的。Linux的命令行工具提供了巨大的灵活性, 可以满足大多数Linux专家的要求。

利用第19章介绍的redhat-config-*工具, Red Hat Linux提供了图形化工具, 使其他操作系统的管理员更容易过渡到Linux操作系统。

可靠性

Linux是可靠的, 据说有的Linux服务器运行好几个月都不需要重新启动。想一想, 能够不重新启动计算机而停止一个失败的程序该多好, Linux就有这个功能。

Linux并不完美, 也可能发生错误。本书将会介绍查错技术。如果引导Linux时遇到问题, 则可以用Red Hat Linux安装光碟解决大多数系统问题(而不必重新安装Linux)。

灵活性

Linux是灵活的操作系统。RPM(红帽子包管理)系统很容易在需要时增加更多软件。关于RPM系统和rpm命令的更多信息, 见第10章介绍。第19章介绍的redhat-config-packages工具使软件管理过程更加简化。

可以用第12章介绍的方法优化Linux内核。优化Linux内核能使其其中的一切操作运行速度更快, 包括引导过程和联网。利用正确的技术, 总是能够方便地访问工作内核, 相反, 改变

Microsoft Windows注册表时发生的小小错误就可能造成灾难。

Linux很容易升级。可以用最新内核、应用程序和其他软件更新旧版Linux，第10章介绍的rpm和up2date工具可以帮你进行升级。

支持

Linux具有很好的支持。但是，许多管理员和IT经理担心没有像Microsoft公司一样的单一公司支持。但要记住，Microsoft支持是要花钱的。

如果购买正式的Red Hat Linux套件，则可以得到限量支持。还可以从红帽子公司或其他第三方厂家购买更多支持，如Linuxcare公司（www.linuxcare.com）。Linux背后的一些大公司（如IBM公司）也对其系统中安装的Red Hat Linux提供支持。

还有另外两个Linux支持资源。由于Linux是开放源代码的，因此管理员通常能够解决许多问题，他们可以联机了解内幕。也许互联网新闻组数据库中已经提供了问题的答案，可以通过groups.google.com访问。

Linux计算机的角色

可以将Linux配置成服务器或桌面计算机。Linux是灵活的，可以在许多本来要扔掉的旧式计算机上安装。

红帽子公司还提供了另外几个程序和应用程序，可以改进企业和小公司的Linux桌面功能。

Linux服务器

Linux是针对网络建立的，可以作为服务器，管理网络上许多不同类型的资源。表1.3列出了可以配置的几个Linux服务。许多服务都有自己的监控程序，有些则与第23章介绍的扩展互联网服务监控程序（xinetd）相关联。

表1.3 Linux服务器的服务

服务	描述	所在章节
crond	按计划运行脚本	第13章
cups	管理CUPS（常用UNIX打印系统）	第25章
httpd	Apache Web服务器	第30章
named	域名服务	第24章
nfs	网络文件系统服务器	第28章
sendmail	常用E-mail传输主体	第26章
smb	Samba，使Linux计算机成为Microsoft Windows网络成员	第29章
sshd	安全Shell	第23章
vsftpd	超安全FTP监控程序	第27章
xinetd	扩展互联网服务监控程序	第23章
ypserv	网络信息服务（NIS）服务器	第28章

Linux通常安装在旧式计算机中。可以将Linux计算机设置成有限功能的服务器。许多情况下,这并不要求太多内存或硬盘空间。例如,可以将Linux计算机设置为打印服务器或防火墙,而不必为此购买专用硬件。

Linux桌面

Linux是很好的桌面系统。第11章到第17章将会介绍,Linux提供了与任何Microsoft Windows版本中相同的基本GUI应用程序和配置工具。

此外,三大办公组件可以代替Microsoft Office。Mozilla与Konqueror是完全特性的Web浏览器,也可以在Linux中安装Netscape与Opera。Evolution可以代替Microsoft Outlook。

人们正在考虑安装Linux桌面。到本书编写时,沃尔玛公司正在销售的五种不同计算机都装有Lindows(www.lindows.com),这个Linux版本可以运行几个Microsoft Windows应用程序。美国以外的国家也正在考虑安装Linux桌面。

游戏制造商正在建立在Linux上玩游戏的方式。Tux Games是个联机商店(www.tuxgames.com),具有有趣的游戏仓库,甚至有个Sims for Linux版本,是TransGaming技术公司(www.transgaming.com)提供的。

Linux应用程序不一定能满足每个人的需求。在个人财务领域,我认为GNUcash比不上最新版的Quicken。www.linuxliberal.com/Software/Financial/Personal_Finance/站点列出了其他Linux个人财务程序。

如果需要几个Microsoft Windows程序,则可以用多种方法解决。CrossOver Office(www.codeweavers.com)可以运行Microsoft Office 97/2000、Quicken、Lotus Notes,等等。可以在Linux的虚拟计算机中建立Microsoft Windows,这是VMWare(www.vmware.com)或Win4Lin(www.trelos.com)提供的。

桌面Red Hat Linux

红帽子公司最近开始用8.0版本推动桌面市场。据红帽子公司产品市场部主任Erik Troan称,公司正在转向个人和公司市场的Red Hat Linux桌面。至少,目前红帽子公司正在关注财务机构和电话中心之类的市场。公司还关注高端用户,他们需要重量级软件,如CAD(计算机辅助设计)和应用程序。

为此,红帽子公司在用相似的外观配置GNOME与KDE,将GNOME与KDE变成Bluecurve。

GNOME是GNU网络对象模型环境,见第16章介绍;KDE是K桌面环境,见第17章介绍。这是目前Linux中最常用的两个GUI桌面。还有这两个桌面的改进GUI工具,见第18章介绍。

桌面用户会喜欢Red Hat Linux 9提供的各种应用程序,包括:

- OpenOffice, 完全特性的办公软件组件。
- Mozilla和Konqueror, 与Microsoft Internet Explorer具有相同特性的Web浏览器。
- Internet实用程序,如Instant Messenger、新闻客户端机、远程桌面,等等。
- 多媒体应用程序,可以全速写入光碟和DVD。

尽管Red Hat Linux桌面图形实用程序还没有Paint Shop Pro那样的CMYK（青红黄黑四种颜色）图形软件，但几个电影工作室已经在Linux计算机上建立了动画和特殊效果。

说明：CMYK（青红黄黑）四色模型比原先的RGB（红绿蓝）标准在高端图形应用程序中更常用。

小企业Red Hat Linux

Red Hat Linux也是小企业和组织的优势选项，可以在所有桌面和服务器的服务器上安装，从而不必另外增加成本去安装操作系统和应用程序。

Red Hat Linux很容易在网络上配置，即使具有Microsoft Windows计算机。甚至可以将Red Hat Linux配置成Microsoft Windows式网络中的主域控制器（PDC）。正确配置Samba之后（见第29章），其他Microsoft计算机就看不到任何差别。

只要正确配置，就很容易将网络连接到互联网。还可以用防火墙和其他网络工具的适当设置防止互联网上的许多危险。

企业Red Hat Linux

许多公司使用改进的Red Hat Linux版本，如红帽公司的企业服务器系列产品。配上其他工具，如Oracle数据库和Stronghold Web服务器，可以使Red Hat Linux成为强大的企业工具。

Amazon.com公司因为转向Red Hat Linux而节省了几百万美元。Google搜索引擎数据库在运行Red Hat Linux的8000多台服务器群集中运行。其他大机构也先后转向Red Hat Linux，如BP、Kenwood和麻省理工学院。在一个红帽公司案例分析中，丰田公司将计算机转入Red Hat Linux之后实际上使支持成本更低了一些。

问题报告

Linux的工作正在进行。开发人员不断为新的软件和硬件增加与修改特性。也许在你的Linux之旅中，也会遇到一、两个问题。可以用四种方法找到解决方案：

新闻组 前面曾介绍过，许多用户在不同新闻组中提出遇到的问题。Google搜索引擎把最近的新闻组消息放到groups.google.com上的可搜索数据库中。如果你要向新闻组提问，最好使用第16章和第17章介绍的新闻组阅读器。也可以用Google界面发表消息（需要先注册）。

邮件清单 红帽公司提供了不同主题与版本的一系列邮件清单，可以到www.redhat.com/mailling-lists/注册。几个不同应用程序的开发人员也维护了自己的邮件清单，可以到其Web站点中寻找。

红帽公司支持 如果你购买了正式Red Hat Linux拷贝，则可以对遇到的问题得到一定支持。这个支持可能只限于购买的版本。

缺陷报告 如果你能肯定问题出在Red Hat Linux本身，则可以向红帽公司提交缺陷报告。进入bugzilla.redhat.com站点并单击Login Now按钮。如果还没有建立账号，要建立账号。然后可以搜索Bugzilla数据库，看看别人是否已经向红帽公司提交了相同的缺陷报告，如果没有，而你已经查遍了其他资料，则可以通过红帽公司的Bugzilla系统提交一个缺陷报告。

小结

Linux是UNIX的克隆，主要由自由软件基金会推动，其关键是Linus Torvalds建立的Linux内核。Linux大部分通过通用许可证（GPL）保护。

随着Red Hat Linux 9的发布，企业和政府都在考虑如何减少成本。Linux至少最初成本比Microsoft Windows之类的其他操作系统低得多。Red Hat Linux和大多数著名Linux发行版本一样，走在这个改变的前列。

Red Hat Linux 9和所有其他Linux发行版本一样，有相同的基本组件：内核、初始化、监控程序、用户方式shell与实用程序、网络和X窗口。它将最新改变加进Linux内核，并改进打印、Web服务等特性。redhat-config-*图形工具使其他操作系统管理员更容易过渡到Linux。

Linux的关键是内核，是相当可定制的，模块化使其变得非常灵活。

Linux有四大优点：成本、可靠性、灵活性和支持。我相信，Linux在这四个方面都比其他操作系统好。

Red Hat Linux可以在计算中起重要作用。传统上，它用做服务器，即使许多旧式计算机也能很好地工作。红帽子公司正在增加工具，使其适合作为桌面操作系统。这种灵活性使Red Hat Linux成为小公司的可行方案。Red Hat Linux还可以用于大企业，用于计算机群集，满足重量级需求。

下一章介绍如何让计算机准备使用Red Hat Linux。安装通常能在大多数现代计算机中顺利进行。但如果在网络上的两台或多台计算机中安装Red Hat Linux，则错误成本很高。如果你要在网络上负责安装Linux，则要对计算机上的硬件有更多了解。

第2章 准备硬件

大多数现代计算机中通常能顺利安装Red Hat Linux。如果在新计算机上安装Red Hat Linux, 则只要在正确的驱动器中插入安装光碟, 将计算机BIOS设置成从光碟启动, 然后重新启动计算机, 就可以了。Red Hat Linux安装程序会启动和自动探测大多数硬件。

如果PC机相对较新, 至少有奔腾级CPU, 但计算机硬件不是最新的, 你永远不必担心Linux驱动程序。虽然至少要阅读第一节关于磁盘分区的内容, 但本章大部分内容可以跳过。

但是, 如果你的PC机包含专属硬件, 没有Linux驱动程序, 或你的PC机硬件很新, 还没有相应的Linux驱动程序, 或你的PC机太旧, 容易出现硬件冲突, 则在网络上安装Linux时错误成本很高。

这时, 最好详细列出PC机上的硬件表, 然后检查兼容硬件表。只要稍做调整, 并不需要安全匹配。只要有正确的资料, 配置一个致命的“Winmodem”也不是太难。

许多Linux用户将计算机设置为“双引导”方式, 可以在引导过程中启动Red Hat Linux或Microsoft Windows (或另一操作系统)。准备引导只从Microsoft Windows的计算机时, 需要多做一些工作。本章介绍下列课题:

- 创建硬盘分区
- 在同一计算机上配置Microsoft与Linux
- 为什么考虑硬件
- 检查兼容硬件
- 准备硬件检查表
- BIOS提示

创建硬盘分区

最新硬盘通常很大。分区可以将硬盘配置成较小的块。如果正确配置, 则分区可以帮助保护系统。例如, 如果有人在FTP服务器上过载文件, 则正确分区能保证系统仍然有运行的空间。

如果硬盘较小(不到4GB), 则需要提高效率。如果分成太多区, 则一些其他类型的文件可能得不到足够的空间。

可以将每个物理硬盘组织成主分区、扩展分区和逻辑分区, 具体细节取决于要配置普通IDE(集成驱动电路)硬盘还是SCSI(小型计算机系统接口)硬盘。

Linux组织成目录。可以按文件系统层次标准将不同目录装载到分区上。第7章介绍FHS(文件系统层次标准)和典型的Red Hat Linux分区配置。

分区类型

甚至可以用同一硬盘的不同分区配置不同的操作系统。每个文件系统可以格式化成不同类型，如红帽子第三扩展文件系统（ext3）或Microsoft公司的FAT32。这样，硬盘有四种分区方式：

主分区 一个硬盘最多有四个不同的主分区。一个主分区是活动主分区，可以包括一个引导装入器，如GRUB。如果将Linux目录装载到主分区，则称为卷。

扩展分区 如果四个主分区还不够，则可以将一个主分区变成扩展分区。扩展分区又可以进一步分成需要的多个逻辑分区。但扩展分区上不能装载目录。

逻辑分区 扩展分区可以分成需要的多个逻辑分区。虽然扩展分区中不可以建立Linux目录，但是可以在逻辑分区中建立Linux目录。因此，逻辑分区也是“卷”，Microsoft将其称为“逻辑盘”。

交换分区 Linux中通常设置一个交换分区作为硬盘上虚拟内存的专用区。交换分区不是什么特殊的分区，可以装载到主分区或逻辑分区。虽然交换分区的合适长度没有统一的标准，但红帽子公司建议将交换分区设置成内存的两倍。

分区名

Linux的硬盘分区命名规则很简单。命名系统也适用于任何不要求直接连接声卡的光碟。名称的前两个字母反映磁盘类型：如果是普通IDE硬盘，则为hd；如果是SCSI硬盘，则为sd。

第三个字母取决于硬盘的位置。第一个硬盘指定为a，第二个硬盘指定为b，等等。换句话说，如果主控制器连接两个不同的物理IDE硬盘，则第二个盘（从盘）称为hdb。相反，SCSI硬盘的字母对应于指定的ID号。例如，如果有两个SCSI硬盘，ID为0和1，则ID为0的SCSI硬盘称为sda，ID为1的SCSI硬盘称为sdb。命名时，光碟和DVD也归类为硬盘。

第四个位置的字母反映了磁盘如何分区。由于最多可以有四个主分区，因此指定为1、2、3、4。第一个生成的逻辑盘在位置5，即使只有一个主分区。

每个分区与/dev目录中的一个Linux设备文件相关联。在分区中装载目录时，将其与设备文件相关联。表2.1列出了不同分区设备文件的例子。

表2.1 不同分区设备文件的例子

名称	描述
/dev/hda3	主IDE控制器的硬盘上的第三个主分区，根据配置情况，可能是扩展分区
/dev/sdc8	第二个SCSI硬盘上的第四个逻辑分区
/dev/hdb7	主IDE控制器从盘上的第二个逻辑分区
/dev/sda1	第一个SCSI硬盘上的第一个主分区
/dev/hdb	由于没有编号，指连接主IDE控制器从盘位置的CD或DVD
/dev/sdc	由于没有编号，指连接SCSI接口第三个位置的CD或DVD

在IDE盘中，最多有16个分区。在SCSI盘中，最多有15个分区。

在同一计算机上配置Microsoft与Linux

在同一计算机上配置Microsoft与Linux有许多好处。到本书编写时，有的软件只能在Microsoft Windows中使用。运行许多业务的软件只适用于Microsoft Windows。用户过渡到Linux时，希望旧的Microsoft操作系统还在那里。

也可以用其他办法，如使用两台不同计算机。可以使用WINE（Wine Is Not an Emulator）项目中生成的软件，从而可以在Linux中使用一些Microsoft软件。可以使用相关软件，如Xandros、Lindows或CodeWeavers（CrossOver Office）提供的软件。甚至可以在Linux第三方专属虚拟机应用程序中安装Microsoft Windows，如VMWare与Win4Lin。

但是，最常见的方法是双引导配置。换句话说，可以在同一计算机上建立两个不同操作系统。例如，图2.1显示了标准GRUB菜单，可以启动Red Hat Linux或Microsoft Windows Server操作系统。



图2.1 双引导配置

双引导配置可以把不同操作系统放在不同物理硬盘上，也可以重新配置现有硬盘上的自由空间。这时，要仔细按照稍后“步骤”一节介绍的过程操作，之前一定要备份数据。错误在所难免，遇到灾难时应能够恢复。

简单方法：新硬盘

本节介绍在现有计算机上安装Linux的简单方法。BIOS能够自动探测第二个硬盘，这时你知道红帽公司的安装程序Anaconda也能够自动探测第二个硬盘。

只要将改变局限在新的空盘上，就可以减少风险。可以配置和格式化分区，而不会影响现有硬盘上的Microsoft Windows数据。

警告：Red Hat Linux服务器安装的默认设置是删除所有硬盘上的所有数据，即使其中包括Microsoft Windows。

到本书编写时, Red Hat Linux只可以直接安装到普通IDE与SCSI硬盘中。尽管可以使用USB、IEEE 1394或并行端口连接的硬盘存储Linux目录, 但Anaconda可能不支持在这些硬盘上安装Red Hat Linux。

说明: IEEE 1394系统还有个专属名称FireWire (Apple公司的商标) 和iLink (Sony公司的商标)。

警告: 增加新硬盘还有一个好处: Anaconda不能在有坏块的硬盘上安装Red Hat Linux 9。

便宜的方法: 现有硬盘

并不是每个人都有第二个硬盘。即使有, 计算机中也不一定有地方装这个硬盘。许多在双引导配置中安装Linux与Microsoft Windows的人要用现有硬盘上的自由空间。

如果要用现有硬盘上的自由空间安装Red Hat Linux, 则要按照下列基本步骤。记住, 出现错误时, 可能危及当前数据。这只是基本步骤, 下面将详细介绍双引导配置过程。

1. 在Microsoft Windows物理硬盘上腾出空间。大多数情况下, 可以使用Microsoft公司的Disk Defragmenter程序。Linux所需的空间量见第3章介绍。
2. 划出Microsoft Windows数据所在的分区, 可以用第一张Red Hat Linux安装光碟上的FIPS.EXE文件进行。如果喜欢, 也可以使用第三方工具。一定要为Microsoft Windows分区内存留足够空间。

说明: FIPS (第一互动分区分割器) 只能分割主分区。到本书编写时, 它不能划分NTFS文件系统格式的分区。

3. 如果需要, 用fdisk重新组织新分区。也可以在运行Anaconda时进行。如果使用Microsoft公司的FDISK.EXE程序, 则只能生成一个主分区。

如果要用现有硬盘上的自由空间, 则需要进行一些计划。一定要保证具有要安装的所有Red Hat Linux程序和软件包所需的空间。记住, 要包括后面准备安装的其他应用程序和数据所要的其他自由空间。第3章将详细介绍自由空间要求。一定要保证Microsoft Windows操作系统及其虚拟内存所要的足够空间。

图2.2显示了一个例子, 这是一个20GB的硬盘, Microsoft Windows有5GB文件。可以将这个硬盘分为两个各为10GB的分区, 第一个分区提供Microsoft Windows操作系统及其虚拟内存所要的足够空间, 第二个分区提供从Red Hat Linux安装光碟安装所要的空间。

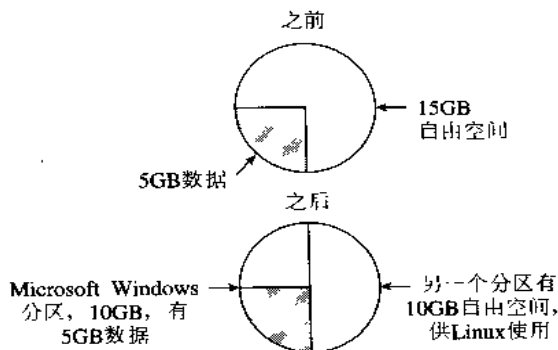


图2.2 硬盘双引导情形

提示：Microsoft Windows要求有虚拟内存所要的足够空间，而Linux不要求这种自由空间，因为Linux虚拟内存通常放在另一个交换分区中。根据我的经验，如果文件所占空间超过60%，则Microsoft Windows无法很好地工作。但这只是一个准则，因为本书不准备介绍如何优化Microsoft Windows。如果需要这方面的更多信息，可以阅读Sybex公司提供的这方面的系列丛书，它们都已由电子工业出版社翻译成中文并出版，包括《Windows 98从入门到精通》、《Windows 2000 Professional从入门到精通（第二版）》、《Windows XP家庭版从入门到精通》和《Windows XP专业版从入门到精通》。

说明：有些Linux用户喜欢另一个实用程序parted。可以用这个GNU程序增加、删除、缩放和格式化分区。我希望它最终能增加mkfs、fips与fdisk的功能。到本书编写时，它立即改变磁盘，因此我认为它比fdisk工具更危险。一个优点是，它和Partition Magic或System Commander一样可以缩放现有分区。关于实用程序parted的更多信息，见GNU项目站点www.gnu.org/software/parted。

步骤

有了总体概念之后，下面介绍为Linux准备硬盘的具体步骤。我们假设Linux要在已经安装Microsoft Windows的物理盘上安装。

警告：本节使用FIPS。使用时要小心，FIPS是“统计没有担保”的。我使用时通常没问题，但FIPS很容易让外边的人设陷阱。

我们假设你的硬盘组织成只有一个分区，所有空间分配给Windows C:盘。也可以在其他盘没有提供足够空间时使用这些步骤。

如果硬盘已经有两个或多个分区，则可以在Microsoft Windows中看到C盘和D盘。如果能把所有文件移到C盘而仍然有虚拟内存所要的足够空间，则可以跳过这个步骤，只要记下每个盘的长度，帮助在Linux安装过程中进行标识。

要为Linux准备硬盘，步骤如下：

1. 寻找硬盘容量和现有文件占用的空间量。确定要为Microsoft Windows和Red Hat Linux分配的空间量。
2. 整理硬盘。使用Disk Defragmenter，通常在Windows Start菜单的Programs>Accessories>System Tools文件夹中提供。具体步骤和位置随Microsoft Windows版本不同而不同。
3. 准备分区分割器。如果想使用FIPS.EXE，将其和RESTORRB.EXE与ERRORS.TXT一起复制到Microsoft Windows或MS-DOS引导盘中。也可以用Partition Magic或System Commander之类的第三方分区分割器所带的引导盘。在其余步骤中，我们假设使用FIPS。

说明：可以从www.bootdisk.com提供的下载中生成MS-DOS引导盘。我喜欢用Microsoft Windows 98引导盘。

4. 用引导软盘重新启动计算机。看到DOS A:\提示时，运行FIPS命令。
5. 遇到一个禁止在多任务环境中使用FIPS的警告时，可以看到“按任意键继续”的命令。

如果有多个硬盘，则要进行选择；它们按引导顺序列出，类似于下面所示。第一个盘为计算机上的第一个IDE或SCSI盘。选择一个盘。

Which Drive (1=0x80/2=0x81)

6. 然后可以看到一个分区表（如图2.3），列出四个主分区。如果四个主分区都使用，则FIPS失败，因为它只能分割主分区。如果可以分割多个分区，则可按编号进行选择。

Part.	bootable	Head	Cyl.	Sector	System	Head	Cyl.	Sector	Sector	Sectors	MB
1	yes	1	0	1	83h	127	24	63	63	201537	98
2	no	0	25	1	83h	127	476	63	201600	3644928	1779
3	no	0	477	1	82h	127	524	63	2848528	387672	189
4	no	0	0	0	00h	0	0	0	0	0	0

图2.3 FIPS分区表

7. 如果看到下列消息，则表示要选择一个主分区。进行选择并继续（如果选择扩展分区，则FIPS无法处理，因此终止）。

Which Partition do you want to split (1/2/3)?

8. 扫描选择的分区，显示这个分区的基本信息，然后询问是否将引导扇区和根扇区的备份拷贝写进可引导软盘中。这是个好主意。对这两个问题回答Yes。可以看到类似于Writing file a:\rootboot.000的消息。记住这个文件。如果遇到问题，则可以用RESTORRB.EXE命令恢复原先的分区表。
9. 现在可以定义如何分割分区。利用箭头键可以改变现有分区和新分区大小。记住新分区大小。

Old partition	Cylinder	New Partition
2075.3 MB	280	932.8 MB

10. 准备好之后，按Enter键确认两个新分区。旧分区中保留现有数据。然后FIPS测试新分区要占用的空间。如果是空的，则FIPS显示一个新分区表，类似于图2.3。然后要确定是否继续或重新编辑分区表 (...to continue or re-edit the partition table (c/r)?)。如果按r，则回到第6步；如果按c，则接受改变并继续。
11. 最后，程序询问是否继续 (...you want to proceed (y/n)?) 将新分区模式写入磁盘中。
12. 将新分区模式写入磁盘后，就可以安装Linux了。新分区应在Red Hat Linux安装过程中显示。如果一切顺利，则显示空的新分区，是FIPS生成的长度。

关于FIPS的更多信息见其Web站点www.igd.fhg.de/~aschaefer/fips。

为什么考虑硬盘

支持Linux的开发社区干得很漂亮，对各种主要PC硬件生成了驱动程序。许多（几乎大部分）新组件都可以在发布后几个月内得到Linux驱动程序。事实上，许多硬件厂家在硬件中包括Linux驱动程序或在Web站点中提供下载。随着Linux即插即用功能的进步，大多数硬件都能自动探测和自动配置。因此，许多情况下，在计算机上安装Red Hat Linux时，不需要担心硬件。

但是，还是可能遇到问题。如果计划在一组计算机上安装Linux，则硬件问题的成本是很高的。并不是所有硬件都是为Linux建立的（或为Microsoft Windows XP建立的），并不是所有硬件都具有Linux驱动程序。

硬件问题的成本是很高的

是的，随着时间的推移，硬件的成本不断下降，但是，计划在一组计算机上安装时，替换每个网卡不仅迅速增加硬件成本，也会迅速增加每台计算机所要的劳动力成本。

有些计算机更加昂贵。如果显卡配置发生错误，则很容易烧掉连接显示器的电路。如果显示器是桌面显示器，则成本可能更贵。因此，至少应该记录显示卡和显示器的规范。

如果配置显示卡时发生错误，则发送的信号可能超出显示器的能力，无论Linux计算机还是Microsoft Windows计算机都一样。

说明：大多数情况下，现代显示器会告诉你所犯的错误。

显示卡向显示器发信号时，按特定频率和刷新率发送。显示器能处理的频率和刷新率有限，超出范围时可能烧掉连接显示器的电路。尽管有些显示器具有保护性线路，但何必去冒这个风险呢？

并不是所有硬件都是为Linux建立的

有些厂家发布硬件的源代码，有些代码甚至是按通用许可证（GPL）条件发布的。这样，Linux开发人员就很容易设计这个硬件组件中的驱动程序。

但是，并不是所有硬件都是为Linux建立的。例如，Winmodems与Winprinters是专为Microsoft Windows设计的调制解调器与打印机，它们明确使用Microsoft Windows驱动程序库工作。由于Microsoft公司不发布驱动程序库的源代码，因此Linux开发人员很难设计这个硬件组件的驱动程序。奇怪的是，由于Microsoft Windows XP的变化，许多Winmodems与Winprinters甚至也无法在最新Microsoft操作系统中使用。

提示：许多Linux书籍建议干脆避免Winmodems，但这不一定是必要的，我就有一个Winmodems，Linux在我的桌面计算机和便携计算机上都能识别。

有时Linux开发人员还来不及生成最新组件的驱动程序。到本书编写时，三类组件的Linux驱动程序还不完善：USB、IEEE 1394和IEEE 802.11无线系统。尽管Linux能很好地支持USB 1.x组件，但USB 2.0则要求内核支持EHCI（改进型主机控制器接口），Red Hat Linux 9提供的内核仍然处于试验阶段。

Linux对一些IEEE 1394设备的支持也还只有试验性驱动程序。普通无线网络（IEEE 802.11b）的Linux支持很好，IEEE 802.11a-11g的驱动程序还在开发之中。本章稍后“可疑硬件”一节将会介绍这些最新驱动程序开发者的主页。

提示：从8.0版本开始，Red Hat Linux不能再在386和486级CPU上安装。

检查兼容硬件

红帽子公司站点中还有兼容硬件的最新信息。访问这个站点中的硬件兼容性部分<http://hardware.redhat.com/hcl>，如图2.4所示。Linux兼容硬件通常组织成HCL（硬件兼容性列表）。



图2.4 红帽子公司硬件兼容性列表

红帽子公司在几个不同PC机上测试了硬件。但是，公司还是依赖于其他Linux开发人员的工作。红帽子公司把硬件分成四类，见表2.2。

表2.2 红帽子公司硬件兼容性列表

类别	描述
认证	这类硬件已经在红帽子公司的正式认证项目中测试过，支持Linux
兼容	红帽子公司人员已经在正式认证项目之外审查过这个硬件
社区知识	别人发现这个硬件与Linux兼容，尽管红帽子公司也可能在安装光碟中包括这些硬件的驱动程序，但红帽子公司并不支持
不支持	这类硬件已经在红帽子公司的正式认证项目中测试过，不支持Linux

下面几节介绍每类硬件的例子。

认证硬件

认证硬件是经过Red Hat Linux正式测试的。一般来说，列为红帽子公司认证的是整个系统（如IBM公司的服务器），而不是单个组件。但也有一些例外。

在红帽子公司HCL Web页面中，可以单击Hardware Compatibility List链接，在红帽子公司HCL的搜索引擎中导航。这个搜索引擎很简单。找到硬件之后，可以找到红帽子公司对组件的审查情况。例如，图2.5显示了红帽子公司对D-Link网卡的审查情况。

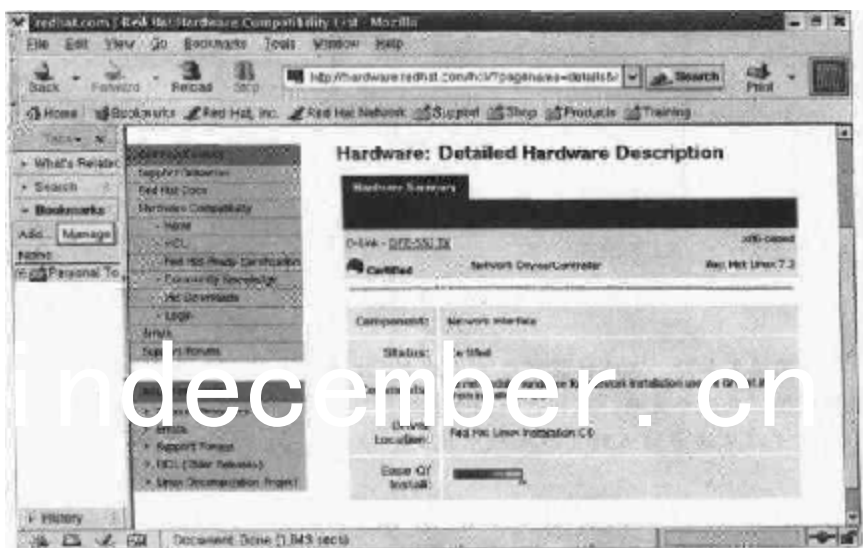


图2.5 红帽子公司对D-Link网卡的审查情况

从这个Web页面可以看出，D-Link DFE-550 TX网卡是认证的，使用sundance.o驱动程序，在Red Hat Linux安装光碟中。如果在网络上安装Linux，则可以通过drvnet.img安装驱动程序软盘安装Red Hat Linux，很容易安装。换句话说，可以通过这个网卡安装Red Hat Linux。只要让计算机读取驱动程序软盘，见第3章介绍。最后，注意这个网卡是对Red Hat Linux 7.2测试的，尽管这个网卡应该能适用于新版Red Hat Linux，但也不一定。

兼容硬件

认证硬件与兼容硬件之间还有一些微妙的差别。认证硬件通常包括整个系统，而兼容硬件则包括各个组件，如CPU、硬盘、图形卡和网卡。很难测试这些组件的每一种组合，未知交互可能影响与任何操作系统的兼容性。

红帽子公司对许可用户提供“兼容硬件”的有限Red Hat Linux支持。很容易在红帽子公司HCL表中找到兼容硬件。只要导航到<http://hardware.redhat.com/hcl>并在支持链接中单击HCL。在页面底部，可以看到四个标签，帮你搜索红帽子公司HCL。

我对已知与Red Hat Linux 8.0兼容的显示设备进行了高级搜索，结果如图2.6所示。

同便携电脑上的使用经验。Linux-Mobile-Guide提供了配置便携电脑和其他移动设备的详细信息，网址为<http://tuxmobil.org/howtos.html>。

网卡 Red Hat Linux适用于大多数标准网卡。但随着网络速度的增加，新的网卡不断开发，也许Red Hat Linux 9光碟中找不到各种千兆或10倍千兆以太网网卡的最新驱动程序。最新Linux网卡驱动程序的开发工作由Scyld Computing公司负责，网址为www.scyld.com/network。

打印机 Winprinter和Winmodem一样很难配置，具有更多特性的新打印机也以极快的速度不断推出。www.linuxprinting.org站点的开发人员投入大量工作，开发新的打印驱动程序和配置文件。

扫描仪 Scanner Access Now Easy (SANE) 主页提供了为Linux配置普通扫描仪与USB扫描仪的详细提示与技巧，目前其主页网址为www.mostang.com/sane。

声卡 Linux中的声卡很难配置。例如，有些声卡需要多DMA信道，有些则可以配置成仿真一个声霸卡。Red Hat Linux声卡支持的最新信息见Advanced Linux Sound Architecture (ALSA) 项目站点www.alsa-project.org。

USB 尽管Red Hat Linux可以在安装过程中探测基本USB键盘与鼠标，但目前USB设备的Linux支持还很不理想。随着PC机将外部设备转入USB与IEEE 1394标准，Linux开发人员会对行和外部器件生成新驱动程序，到本书编写时，IEEE 1394与USB 2.0标准的高速设备的支持仍然处于试验阶段。USB支持的最新信息见Linux USB项目站点www.linux-usb.org。

Winmodems 前面曾介绍过，Winmodems利用Microsoft Windows驱动程序库支持其功能。但是，Linmodem项目人员也在开发能够无缝地使用许多Winmodems的Linux驱动程序。许多驱动程序已经加进Red Hat Linux 9中。许多Winmodems可以通过Linux即插即用系统自动探测。但并不是所有Winmodems都适用于Linux，最新信息见www.linmodems.org站点。

社区知识硬件

Linux操作系统是全世界许多开发人员集体劳动的结果。Linux社区的人们把自己组成几个组。前面曾介绍过，其中许多组专门生成和更新特定硬件的驱动程序。这个进展会在其Web站点和邮件清单中记录。

如果要了解Linux硬件的最新社区知识，则可以用四种方法进行研究。Linux Hardware HOWTO文档提供了Linux硬件兼容性的总体视图，但不一定包括最新硬件信息。更多数据可以从许多硬件特定Linux支持小组的站点取得，见上节介绍。其中许多小组还有开放邮件清单，开发人员用其交换最新工作信息。最后，用户还可以在Internet新闻组中询问有关硬件的问题。<http://groups.google.com>提供了可搜索的新闻组数据库。

说明：向邮件清单或新闻组询问有关的问题之前，先要自己分析分析。许多Linux开发人员都要上班，没时间回答文档中已经有答案的问题，如www.tldp.org站点的LDP HOWTO文档。事实上，如果浪费他的时间，许多Linux开发人员会表示愤怒。因此，向邮件清单或新闻组询问有关的问题之前，先要检查相关主题的文档。可以搜索新闻组和邮件清单数据库，看看你的问题是否已经有答案。

准备硬件检查表

最好能收集计算机上每个硬件组件的信息。本节提供所要信息的检查表。标识硬件之后，可以检查红帽子公司和其他Web站点提供的驱动程序与配置提示。

至少要先取得图形卡和显示器的技术规范，之后再安装Red Hat Linux。安装Linux之后，测试每个硬件组件。列出很难配置的组件或工作不理想的组件。探测的组件通常在`/proc`目录中配置，见第11章介绍。下次安装Red Hat Linux时，就有了现成的驱动程序和配置命令。如果在另一组计算机上安装Red Hat Linux，则这是个好办法。

下面几节介绍的信息是要对每个硬件组件收集的信息。然后我们介绍如何将每个组件与特定驱动程序相关联，最后要提供一个表，可以填入需要的数据。

收集信息

开始在计算机上安装Red Hat Linux之前，要记住几个基本事项。我们不需要知道每个硬件组件的一切，大多数信息都会在安装过程中自动探测。检查表2.3所列的优先级硬件表。

表2.3 优先级硬件表

组件	所需信息
CPU	Red Hat Linux 9至少要求200MHz的Pentium级CPU。如果需要GUI，则至少要有400MHz的Pentium II级CPU。此外，如果不是Intel（或兼容）CPU，则要另一组安装软件包
内存	需要的内存量取决于是否在计算机上使用GUI，是否多用户。对命令行界面，64MB内存可能就够了，但要在计算机上使用GUI，则至少要有128MB内存（最好192MB）
图形卡	需要了解图形卡的几个信息。Linux XFree86服务器软件包有一个数据库，可以根据机型和版本配置图形卡。如果Linux不认识这个卡，则要单独配置已知的显示内存和水平、垂直刷新率
显示器	要知道显示器功能，包括分辨率和水平、垂直刷新率。如果图形卡刷新信号的能力超过显示器，则要小心，设置不当时可能把显示器烧掉

换句话说，至少要对计算机上的优先级硬件了解技术规范、机型和版本。

收集驱动程序

大多数硬件组件的驱动程序已经放在Red Hat Linux安装光碟中，大多数驱动程序都会在Linux安装过程中自动配置。

但是，Red Hat Linux并没有包括所有硬件的驱动程序。Microsoft操作系统也没有包括所有硬件的驱动程序。可以用两种方法收集其他驱动程序，一种方法是基于社区知识，见前面介绍；一种方法是基于硬件厂家生成的驱动程序。

许多硬件厂家对Linux很友好。记住，IBM公司已经在Linux开发中投资几十亿美元。许多厂家紧跟潮流，也提供了硬件的Linux驱动程序。许多Linux驱动程序可以从厂家的Web站点下载。通常，这个站点还会提供文档与说明。

一旦有了驱动程序之后，就可以用`insmod`之类的命令安装。可以用`/etc/modules.conf`中的正确命令保证下次启动Linux时安装这个驱动程序。关于这个过程的更多信息，见第11章。

硬件检查表

为了方便起见，本节提供一个PC机上要收集的硬件信息表。表2.4中列出了需要收集信息的硬件。

一定要特别注意不符合即插即用标准的任何设备。可能要在BIOS中对这类硬件保留IRQ端口或I/O地址。

表2.4 硬件检查表

组件
CPU类型，速度
RAM内存，MB数
键盘，制造商，机型
鼠标，协议，制造商，机型，按钮
硬盘1长度
分区与装载点，如/home与/dev/cd1
硬盘2长度
分区与装载点，如/var与/dev/sdb1
硬盘3长度
分区与装载点，如/usr与/dev/sdc1
硬盘4长度
分区与装载点，如/boot与/dev/hda1
CD-ROM，类型
光碟刻录机，类型
DVD-ROM，类型
SCSI卡，制造商，机型
网卡制造商，类型，机型，速度
网卡2，制造商，类型，机型，速度
电话调制解调器，制造商，机型，速度
图形卡，内存，制造商，机型，水平与垂直刷新
显示器，制造商，机型，水平与垂直刷新
显示器2，制造商，机型，水平与垂直刷新
声卡，制造商，机型，芯片集
USB设备1，制造商，机型
USB设备2，制造商，机型
USB设备3，制造商，机型
USB设备4，制造商，机型
IEEE 1394设备1，制造商，机型
IEEE 1394设备2，制造商，机型

BIOS提示

计算机BIOS中可以配置三个内容。一个是硬盘的引导顺序。一个是引导序列，如，可以将BIOS配置成从相应光碟引导Red Hat Linux安装程序。最后一个是保留关键通信信道，如保留IRQ端口或I/O地址。

BIOS菜单多种多样，因此无法具体指出如何配置BIOS。配置BIOS的方法取决于BIOS菜单和已经安装的升级项目。

通常，要检查BIOS菜单，可以在计算机的初始嘟嘟声后，按键盘上的F1、F2或Del之类的键。有时可以在引导过程中看到图2.7所示的菜单。



图2.7 PC启动菜单

有时菜单是隐藏的，可能被计算机或主板厂家的屏幕隐藏。可以按键盘上的F1、F2或Del之类的键。如果这些命令无法启动BIOS菜单，则可以检查PC机或主板文档。在BIOS菜单中，应能看到探测到的IDE盘。

说明：对有些Compaq与Acer计算机，要按Ctrl+Alt+Esc组合键才能打开BIOS菜单。

IDE硬盘

在标准PC机上，最多可以有四个IDE盘。可能是硬盘，也可能是CD/DVD盘，BIOS菜单中应能探测出来。

如果安装了IDE硬盘而BIOS菜单中没有探测出来，则可能有硬件问题。关于查错PC硬件安装的详细信息，见Sybex公司出版的“Complete PC Upgrade and Maintenance Guide, 2003 Edition”。

标准PC机有两个IDE卡，一个主卡，一个副卡。每个卡可以连接两个不同的IDE硬盘，一个主盘，一个从盘。Linux将这些设备与特定的设备文件相关联，见表2.5。

表2.5 Linux IDE硬盘设备文件

IDE硬盘	设备文件
主卡主盘	/dev/hda
主卡从盘	/dev/hdb
副卡主盘	/dev/hdc
副卡从盘	/dev/hdd

SCSI硬盘

SCSI标准有几种，SCSI-1、SCSI-2与SCSI-3标准最多与8个或16个设备相关联，最高数据传输速率为80Mb/s。每个SCSI设备有一个ID，指定在PC机上的优先级。

SCSI硬盘可以内置或外置，大多数新的BIOS至少可以在引导序列菜单中探测SCSI硬盘。在旧的PC机上，可能需要SCSI BIOS。

说明：IEEE 1394盘在技术上是没LUN号的SCSI硬盘。到本书编写时，不能从IEEE 1394盘引导Linux。

引导序列

在LINUX菜单中，可以看到引导序列（Boot Sequence）选项，可以自行引导顺序。PC机的BIOS依次检查这些盘，寻找Linux启动文件与内核的/boot目录。可以将PC机配置成先检查任何探测到的盘。但要BIOS设置成检查特定盘上的/boot目录。

如果IDE盘连接主卡主盘和主卡从盘的连接点，则/boot要安装在这些盘中的一个（/dev/hda或/dev/hdb），即使这些连接点之一连接了CD/DVD也是这样。如果有两个IDE主盘，则事实上，Red Hat Linux安装程序强制在其中一个盘上配置/boot。

如果有一个IDE主盘和一个SCSI盘，则SCSI要安装在其中一个盘上。SCSI盘的ID应为0。

如果没有IDE主盘而有两个或多个SCSI盘，则SCSI要安装在前两个SCSI盘之一上，ID为0或1。

非即插即用硬盘

尽管Linux能够探测大多数即插即用硬件，但有些遗留设备不符合即插即用标准。在许多新的BIOS菜单中，可以对这些硬件保留IRQ端口和I/O地址。例如，旧的网卡可能需要标准端口（如IRQ 10）和标准I/O地址（如0x300）。如果能保留IRQ端口和I/O地址，则可以在安装Linux之后相应配置这个网卡。

小结

安装Red Hat Linux之前，要先准备硬件。可能要对Linux准备IDE或SCSI盘上的硬盘分区。如果同一计算机上要配置Linux和另一个操作系统（如Microsoft Windows），则需要特殊配置。

如果已经安装Microsoft Windows, 则最简单的方法是在另一个空硬盘上安装Linux。Red Hat Linux安装程序Anaconda要探测新的空硬盘和在这个盘上配置分区。如果没有另一个硬盘, 则第一个盘上要有足够的空间。利用Microsoft Windows Disk Defragmenter可以腾出更多空间。利用FIPS实用程序可以将现有分区一分为二。然后可以在新建分区的自由空间中安装Linux。

Red Hat Linux能够探测大多数当前PC硬件。通常, 安装Red Hat Linux时不必担心硬件。Red Hat Linux 9个人版共七张光碟: 安装软件包放在三张光碟上, 另外三张光碟上是每个包的源代码, 还有一张光碟包括HTML与PDF格式的文档。有些硬件可能在安装过程中存在风险, 特别是与图形系统相关的硬件。

红帽子公司可以帮你寻找兼容硬件。红帽子公司把硬件分成四类: 认证、兼容、社区知识和不兼容。社区知识硬件可能要增加其他工作, 几个地方可以取得驱动程序、指令和建议。

至少要收集CPU、内存和图形系统的信息。几个地方可以取得驱动程序, 包括社区知识中提到的地方, 以及几个硬件制造商的Web站点。我们提供硬件检查清单和表格, 帮你收集PC机中其他组件的数据。

为了准备PC机, 至少要检查BIOS中的设置。PICS可以帮你配置IDE与SCSI硬盘。Linux /boot目录应安装到特定的盘上。用引导序列处理这些盘。许多BIOS菜单还可以对非即插即用的遗留设备保留IRQ端口和I/O地址。

下一章介绍从本地Linux安装光碟的安装文件, 用不同引导方法安装Red Hat Linux。安装Linux之后, 很容易注册计算机, 取得红帽子公司网络上的更新。

第3章 本地安装Linux

本章介绍用图形桌面安装Red Hat Linux的过程，从安装光碟一步一步进行安装。大多数情况下，只要将PC机设置成从第一个Red Hat Linux安装光碟启动，重新启动计算机，然后按提示做即可。也可以根据特定规范定制Red Hat Linux。

Red Hat Linux安装程序称为Anaconda。这是个非常灵活的程序，可以适应各个引导盘，也可以适应网络源，见第4章介绍。如果从光碟安装，则Anaconda中有个mediacheck选项，检查安装光碟的完整性。如果能识别前面安装的Red Hat Linux，则它支持升级。

本章主要介绍从光碟按图形方法安装的过程，要求计算机上有128MB内存。如果要在网络上安装Red Hat Linux或使用Anaconda文本方式安装过程，见第4章介绍。

安装完成之后，我们将介绍如何诊断典型安装问题。然后介绍第一个图形和文本登录屏幕。

如果将Red Hat Linux设置成默认按图形方式登录，则首次重新启动计算机时可以看到firstboot设置，可以和网络时间服务器同步日期与时间、搜索声卡、向红帽子公司网络注册计算机和安装其他软件。

由于空间限制，Red Hat Linux的有些组件在本书选配的Red Hat Linux发表版（两张光碟）中没有提供。完整版本可以免费下载（见本书前言介绍），也可以从红帽子公司或第三方经销商那里购买。尽管发表版适用于大多数安装，但本章演示用标准的三张光碟的Red Hat Linux进行安装。

本章介绍下列内容：

- 用引导盘启动
- 检查安装光碟
- 一步一步安装Red Hat Linux
- 运行Red Hat Linux安装主体
- 安装查错
- 登录
- 升级Red Hat Linux

用引导盘启动

大多数情况下，可以直接从光碟安装Red Hat Linux，只要在BIOS菜单中将设置重新配置成直接从光碟启动，见第2章末尾介绍。但是，有时需要用引导盘启动：

- 无法将BIOS配置成直接从光碟启动。
- 无法从第一张Red Hat Linux安装光碟读取引导文件。
- 从另一源安装Red Hat Linux，如通过网络从远程计算机安装（见第4章介绍）。如果能够从光碟引导，则最好为此生成很少的boot.iso光碟。

如果要从引导盘安装Red Hat Linux, 则根据所选的安装方法与硬件, 可能要一到四张三寸软盘。

可以从第一张Red Hat Linux安装光碟/image目录的img文件生成这些软盘。这个目录中的关键文件如表3.1所示。

表3.1 Red Hat Linux安装映像

映像文件	描述
bootdisk.img	所有本地与网络安装的标准引导盘
drvblock.img	块(存储)设备的驱动程序光碟
drvnet.img	网卡驱动程序光碟
pcmciaadd.img	PCMCIA硬件驱动程序光碟
boot.iso	带驱动程序的集成引导盘, 不能放在一张三寸软盘中, 但可以安装到一张光碟

本节与第4章引导盘部分密切相关, 也有一定重复之处。

生成引导盘或驱动程序盘

Red Hat Linux提供了四个实用程序, 可以帮您生成引导盘和驱动程序盘。其中两个(dd和cat)适用于Linux, 两个(C:\AWR\SETUP\CDROM\KTEV\IN.EXE)适用于Microsoft Windows。Linux实用程序是标准命令, 可以从其他Linux或UNIX计算机上运行, 映像文件和Microsoft Windows实用程序放在第一张Red Hat Linux安装光碟中。

如果目前运行Linux计算机, 则可以按下列步骤生成引导盘。记住, 可能还需要一张或几张驱动程序盘, 见下面几节介绍。

1. 在命令行界面中, 找到映像文件。例如, 如果用下列命令装载第一张Red Hat Linux安装光碟:

```
# mount /mnt/cdrom
```

则映像文件位于/mnt/cdrom/images目录中。

2. 将一张三寸软盘插入软盘驱动器中。不要对这个盘使用mount命令。
3. 用下列命令将引导盘映像bootdisk.img转换成软盘上的一系列文件(/dev/fd0设备与计算机上第一个软驱相关联):

```
# dd if=/mnt/cdrom/images/bootdisk.img of=/dev/fd0
# cat /mnt/cdrom/images/bootdisk.img > /dev/fd0
```

4. 对images目录中可能需要的任何驱动程序盘重复这些步骤。

如果在Microsoft Windows中, 要从命令行界面生成引导盘, 则可以用这些步骤生成这个盘。记住, 可能还要对一个或两个驱动程序盘重复这些步骤, 见下面几节介绍。

1. 将第一张Red Hat Linux安装光碟插入光碟驱动器中, 假设为F:盘, 如果盘号不同, 只要换成相应盘号。
2. 打开MS-DOS提示。单击Start▶Run。在Run对话框的文本框中输入CMD, 并按Enter键, 从而打开一个命令提示窗口。
3. 在命令提示窗口中输入F:并按Enter键。

4. 启动RAWRITE.EXE实用程序并运行下列命令，出现提示时将一张三寸软盘插入软盘驱动器中：

```
F:\>/DOSUTILS/RAWRITE.EXE
Enter disk image source file name: /IMAGES/BOOTDISK.IMG
Enter target diskette drive: A:
Please insert a formatted diskette into drive A:, and press -ENTER-:
```

5. 对images目录中可能需要的其他磁盘映像重复这些步骤。

也可以用图形化RAWRITEWIN.EXE实用程序，用Microsoft Windows生成引导盘。记住，可能还要对一个或两个驱动程序盘重复这些步骤，见下面几节介绍。

1. 将第一张Red Hat Linux安装光碟插入光碟驱动器中，假设为H:盘，如果盘号不同，只要换成相应盘号。
2. 访问RAWRITEWIN.EXE实用程序。打开Microsoft Windows Explorer，单击Start▶Run。在Run对话框的文本框中输入EXPLORER并按Enter键，从而打开Microsoft Windows Explorer。
3. 导航到H:盘，然后访问DOSUTILS文件夹中的RAWRITEWIN文件夹，然后双击RAWRITEWIN1.XF实用程序（是的，RAWRITEWIN文件夹与RAWRITEWIN.1XF实用程序的拼写不同）。
4. 这就打开了RawWrite对话框，如图3.1所示。如果需要，单击Write标签。单击Image File文本框右边的按钮，可以在Open对话框中从H:\IMAGES目录访问所选的映像文件。

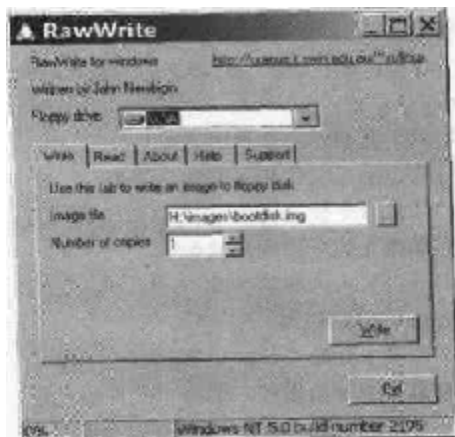


图3.1 用RawWrite生成引导盘

5. 将一张三寸软盘插入软盘驱动器中并单击Write。对所要的其他磁盘映像重复这些步骤。

分析Red Hat Linux引导盘

无论用什么方法生成Red Hat Linux 9引导盘，其目的和内容都是相同的。它从第一张Red Hat Linux安装光碟images目录中的bootdisk.img文件生成，用于引导计算机。在这个

盘中，syslinux.cfg文件提供后续内容的地图，如图3.2所示。

```
default linux
prompt 1
timeout 600
display boot.msg
F1 boot.msg
F2 options.msg
F3 general.msg
F4 param.msg
F5 rescue.msg
F7 snake.msg
label linux
kernel vmlinuz
append initrd=initrd.img
label text
kernel vmlinuz
append initrd=initrd.img text
label expert
kernel vmlinuz
append expert initrd=initrd.img
label ks
kernel vmlinuz
append ks initrd=initrd.img
label lowres
kernel vmlinuz
append initrd=initrd.img lowres
```

图3.2 Linux引导地图

仔细看看这个文件。表3.2给出了关键命令，有助于解释syslinux.cfg文件。

表3.2 syslinux.cfg文件关键命令

命令	描述
default	指定默认引导选项。这里默认为linux
prompt	设置引导提示
timeout	配置引导盘自动启动默认选项之前的延迟时间（单位为1/10秒），通常设置为600（一分钟）
display	指向屏幕上要显示的初始消息文件
Fx option.msg	设置与特定消息文件相关联的功能键
label command	指定与特定命令相关联的动作
kernel	设置引导盘上的压缩内核映像名
append	增加引导盘装入内核的参数
initrd	指定Initial RAM磁盘
text	在文本方式中开始安装，见第4章
expert	在专家方式中开始安装，要指定硬件驱动程序
ks	用Kickstart文件开始安装，见第5章介绍
lowres	用基本VESA（SVGA）驱动程序和640×400低分辨率图形方式开始安装

可以看出，默认用Initial RAM盘装入压缩内核vmlinuz。从图3.2可以看出，其他选项增加不同参数。

提示：可以用一张Red Hat Linux引导盘作为救援盘。利用第11章介绍的方法，可以用它从几种故障恢复，如引导配置文件搞乱时。

分析存储设备驱动程序盘

要安装Red Hat Linux, Anaconda首先要探测到连接计算机的硬盘。标准引导盘（来自bootdisk.img）通常能够识别连接PC机的IDE、SCSI和一些USB硬盘，所要的驱动程序集成在压缩内核中。

因此，可能要从第一张Red Hat Linux安装光碟images目录的drvblock.img文件中生成一个三寸软盘。用本章前面介绍的任何方法生成这个盘，它会在软盘中装入五个文件，见表3.3介绍。

表3.3 存储设备驱动程序盘（drvblock.img）中的文件

文件	描述
modinfo	包含一系列设备驱动程序和描述
modules.cgz	具有modinfo中列出的所有驱动程序的压缩版本
modules.dep	有一个相关性表，换句话说，就是每个设备所需的其他驱动程序
pcitable	对每个设备配置PCI设置
rhdd-6.1	将这个驱动程序盘标为“Supplemental Block Device Drivers”（补充块设备驱动程序）

分析网络设备驱动程序盘

要通过网络安装Red Hat Linux, Anaconda首先要探测到连接计算机的网卡。标准引导盘（来自bootdisk.img）不包括任何网络驱动程序，因此要有网络安装的补充驱动程序盘。

可以从第一张Red Hat Linux安装光碟images目录的drvnet.img文件中生成一个三寸软盘。用本章前面介绍的任何方法生成这个盘，它会在软盘中装入五个文件，与表3.3介绍的文件功能相似。尽管内容不同，但文件名仍然一样。

分析PCMCIA驱动程序盘

在便携电脑上安装Red Hat Linux时通常会产生特殊问题。便携电脑通常利用PCMCIA卡，个人计算机内存卡国际学会（PCMCIA）指定PCMCIA卡连接网络、SCSI设备，等等。这些信用卡大小的卡通常称为PC卡。自然，红帽子公司提供了大部分主要PCMCIA套接、网络和SCSI驱动程序，放在pcmciaadd.img文件中。

可以从第一张Red Hat Linux安装光碟images目录的pcmciaadd.img文件中生成一个三寸软盘。用本章前面介绍的任何方法生成这个盘，它会在软盘中装入五个文件，与表3.3介绍的文件功能相似。尽管内容不同，但文件名仍然一样。

引导ISO

第一张Red Hat Linux安装光碟images目录中还有一个文件值得一提：boot.iso。我们用第14章介绍的cdrecord命令从这个3.5MB文件生成引导光碟，适合同时进行网络安装，不必跑来跑去，装载与卸载引导盘和驱动程序盘。

将boot.iso文件刻录到光碟中时，其内容与标准Red Hat Linux引导盘非常相似，但有两点不同：所有文件都在一个isolinux子目录中，与后面所介绍的驱动程序盘相关联的驱动程序合并初始内存磁盘映像文件initrd.img中。

检查安装光碟

从安装光碟开始安装Red Hat Linux之前，要先检查光碟完整性，保证光碟中的所有软件包完整。在Red Hat Linux光碟的1500多个软件包中，只要有一个软件包不好，就可能使安装失败。

检查安装光碟的方法有两个，一个是用linux mediacheck命令开始引导过程，一个是根据光碟上的二进制码采用统计方法检查。

说明：笔者还没有进行检查就完成了Red Hat Linux安装过程，完成所有Red Hat Linux配置工作之后，我发现安装到第三张光碟时失败了，因为其中有一个软件包不好。没有办法，只好从头开始。

用mediacheck检查安装光碟

要检查安装光碟，可以从引导盘或第一张安装光碟引导计算机。在图3.3所示的引导提示下，运行linux mediacheck命令。

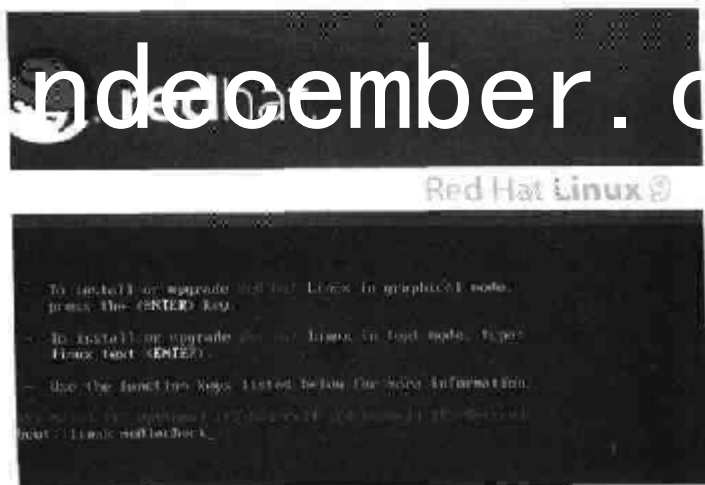


图3.3 用mediacheck启动

说明：在linux mediacheck安装屏幕中，可以用Tab键在选项之间切换，可以按键盘上的Enter键转入下一步。

然后，Anaconda继续安装基本内核。出现的第一个提示如图3.4所示，可以检查安装光碟的完整性。如果选择Skip，则Anaconda继续安装，如果选择OK，则检查安装光碟。

说明：如果你的光碟是从下载的.iso文件生成的，则不必运行linux mediacheck命令，就会立即出现图3.4的提示。前言中详细介绍了如何下载与生成Red Hat Linux安装光碟。

这个方式不限于Red Hat Linux 9的光碟，也可以用Red Hat Linux 9的mediacheck特性检查Red Hat Linux 8安装光碟。下一个屏幕如图3.5所示，可以选择测试当前在光驱中的光碟或将其弹出，测试另一张安装光碟。

插入所要的Red Hat Linux光碟，加亮显示Text并按Enter键。测试通常需要几分钟，然后Anaconda标识光碟，对其评分为Pass或Fail。如果需要，对结果做出反应并按Enter键。

Anaconda会打开另一个屏幕，如图3.6，可以测试另一张Red Hat Linux安装光碟或插入第一张安装光碟，然后继续安装。



图3.4 检查安装光碟完整性



图3.5 准备测试

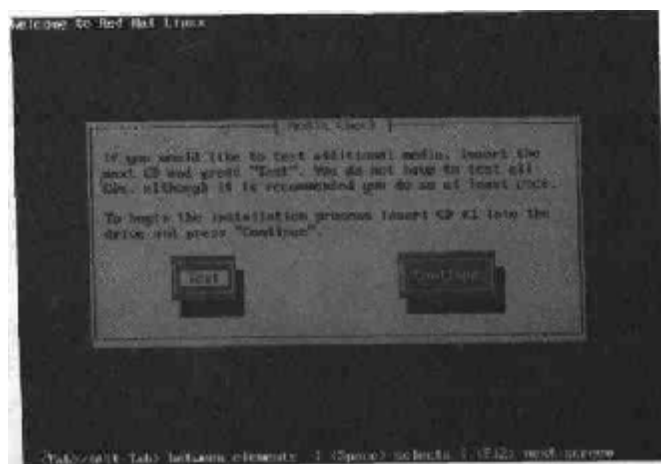


图3.6 继续测试或开始安装

用md5sum检查安装光碟

可以直接检查每个Red Hat Linux安装光碟相关的MD5签名。MD5算法检查数字化签名，可以在Linux中对下载的Red Hat Linux安装光碟（.iso格式）采用md5sum命令。例如，如果下载的第一张安装光碟文件名为disc1.iso，则可以运行下列命令：

```
# md5sum disc1.iso
abb3dd2cd1cd1b92b5e85b0d556b8e12 disc1.iso
```

得到的32位字母数字字符串应与MD5SUMS-ftp.i386文件中指定光碟的字符串相符。它与Red Hat Linux安装光碟的.iso文件在同一个FTP目录中。更多信息见前言中介绍。

一步一步安装Red Hat Linux

检查安装光碟之后，就可以在计算机上安装Red Hat Linux 9了。实际安装过程不一定像本章介绍的这么复杂，我只是想介绍Anaconda提供的所有功能。我们把这个过程分成六节：

- 选择安装提示选项：描述第一个安装引导提示下能做什么。
- 配置基本参数：可以用键盘和鼠标检查选项，以及配置安装过程中Anaconda使用的语言。
- 设置硬盘：详细介绍如何用Disk Druid按不同格式配置不同类型的分区。
- 配置安装细节：可以检查Red Hat Linux安装的配置细节。
- 选择包组：介绍Red Hat Linux中可以安装的各个包组和各个包的选项。
- 管理安装后步骤：帮助配置X窗口和对新系统生成定制引导盘。

这些步骤假设从安装光碟安装Red Hat Linux。如果通过网络连接安装Red Hat Linux，见第4章。

本节假设已经按第2章的介绍改变了BIOS，从第一个Red Hat Linux安装光碟引导。如果还没有，确保BIOS至少先从软盘启动，或生成一个引导盘。还要记住，这个安装基于已经安装了Microsoft Windows 98的桌面计算机。笔者按第2章介绍的方法对硬盘采用FIPS，生成大约有6GB自由空间的空分区。

说明：可以通过NFS（网络文件系统）连接开始图形化安装过程。关于设置NFS网络安装的更多信息，见第4章，然后回到这里介绍的图形化安装过程。

选择安装提示选项

开始安装过程时，可以从两个地方启动计算机：从第一张Red Hat Linux安装光碟或从引导盘，两者都打开相同的开始屏幕，如图3.7所示。遇到这个屏幕时，在60秒钟内按F2键，否则Red Hat Linux自动开始图形方式安装。

可以看到有几个菜单，我们将介绍不同安装屏幕。第一个屏幕中是基本选项，可以选择按图形方式或文本方式安装Red Hat Linux。我们将在本章介绍图形方式，在第4章介绍文本方式。按F5键时，Anaconda打开Rescue Mode Help屏幕，与安装无关，将在第11章介绍。



图3.7 安装提示

准备好后，可以按Enter键开始图形方式安装，或输入text并按Enter键开始文本方式安装。大多数情况下，这些选项是最佳选项。

但是，如果安装期间遇到问题，你可以重新开始，试试其他选项。因此，要转入“安装程序引导选项”一节，检查引导提示下可以运行的各种命令。

安装程序引导选项

从图3.7所示的安装提示屏幕中，按F2键进入安装程序引导选项菜单，如图3.8。表3.4简要介绍了这个菜单中的不同选项。



图3.8 安装程序引导选项

可以在文本方式中运行任何安装选项，只要将linux换成text即可。

表3.4 安装程序引导选项

选项	描述
linux noprobe	不自动探测硬件而开始安装过程，要从清单中选择任何SCSI硬盘和网卡的驱动程序
linux mediacheck	从文本方式提示开始安装过程，可以检查红帽子安装光碟的完整性。默认情况下，在图形方式中继续
linux rescue	在救援方式中引导基本Linux系统，试探测当前Linux安装。详见第11章
linux dd	开始安装过程，出现驱动程序盘提示，适用于第三方驱动程序
linux askmethod	开始安装过程，可以选择语言和键盘，然后可以选择本地或网络安装选项
linux updates	支持用定制安装更新盘升级
linux lowres	用低分辨率图形方式（640×400）开始安装，也称为VGA（视频图形卡）

一般引导/内核参数帮助

在Red Hat Linux安装开始屏幕中按F3键，进入一般引导帮助菜单，如图3.9，其中不包括任何特定选项，但比引导提示下丰富得多。



图3.9 一般引导帮助

引导提示下，可以在linux或text后面增加其他变元。例如，linux upgradeany命令搜索和提供Linux发现的任何计算机的升级，独立于/etc/redhat-release文件中的内容。表3.5列出了表3.4中没有介绍的几个变元。

表3.5 引导提示安装变元

变元	描述
apm=off	在安装过程中关闭APM（高级电源管理）特性
display=ip_addr:0	将安装显示转发到IP地址为ip_addr的计算机。为此，一定要保证接收计算机允许远程X窗口访问，关于xhost命令的更多信息，见第15章介绍

(续表)

变元	描述
expert	提示选择驱动程序盘, 支持可操作硬盘分区。如果在SCSI硬盘上安装, 则至少要提供相关驱动程序盘
ide=nodma	在硬盘之类的IDE (集成驱动电子) 设备上关闭DMA (直接内存访问) 寻址
isa	提示确认Anaconda检测到正确ISA (行业标准体系结构) 盘或类似设备
mem=xyzM	指定特定内存量, 在一些旧式计算机中, 可能要将Anaconda使用的内存限制在128MB。在计算机与显示卡共享内存时, 可能要指定可用内存
nmi_watchdog=1	在后面介绍的一个消息屏幕中增加内核调试消息
nopcmcia	避免安装PCMCIA控制器, 如果从不通过PCMCIA连接控制的光碟安装Red Hat Linux, 则不用Anaconda寻找PCMCIA控制器
nousb	阻止Anaconda安装USB支持
reboot=b	修改内核重新启动方法, 否则有些安装可能在最后一步之前死机
resolution=a × b	指定安装显示方式, 如640 × 480或1024 × 768
serial	在安装期间启动串行控制台支持
skipddc	避免ddcprobe命令, 否则将采集则显示器和图形卡。第5章详细介绍ddcprobe的信息
upgradeany	查找要升级的Linux安装, 独立于/etc/redhat-release内容

说明: 支持在具有Intel 440GX芯片集BIOS的计算机上安装的apic变元不再提供, 也不再需要, 因为现在已经自动支持。

按F4键时, Anaconda转入内核参数帮助菜单, 如图3.10。其中的信息与一般引导帮助菜单相似。表3.4和表3.5中的几个变元可以传递到内核中。有些是直接的, 如mem=128M, 有些则间接工作, 如noprobe, 可以指定PC机关键组件的硬件地址。

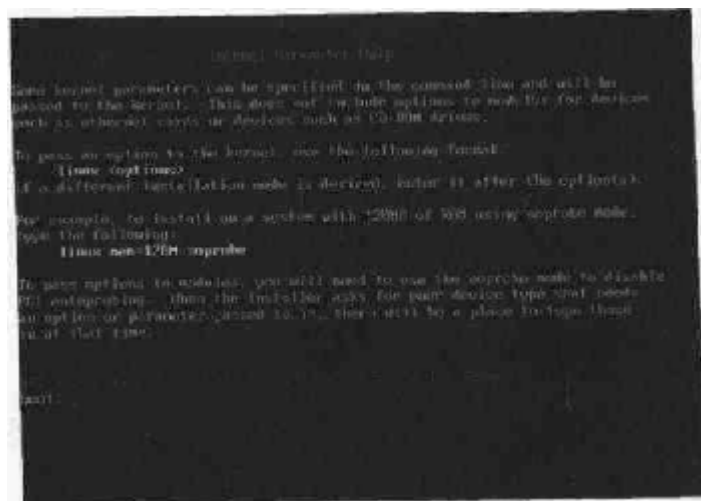


图3.10 内核参数帮助

配置基本参数

现在要实际开始安装了。除非前面几节遇到了特定问题，否则只要在安装引导提示下按Enter键，即可在图形方式中开始Red Hat Linux安装过程。

说明：如果开始安装时在引导提示下输入linux mediacheck命令，或从下载的.iso文件生成的光碟开始安装，则Anaconda会提示检查光碟完整性，见前面介绍。

Anaconda会检查系统，看看是否符合图形安装的要求。第一个安装光碟的RELEASE-NOTES文件中将会介绍，其要求至少128MB内存。我试过在64MB内存的机器上进行图形安装，也能够进行，但速度太慢了，我终于半途放弃。如果内存不到64MB，则Anaconda自动默认为文本方式安装。

然后它检查系统进行图形安装的其他要求：显示卡、显示器和鼠标。可以看到如下所示的消息：

```
Running anaconda, the Red Hat Linux system installer - please wait...
Probing for video card: Intel 810
Probing for monitor type: S/M 955DF
Probing for mouse type: Generic - Wheel Mouse (PS/2)
Attempting to start native X server
Waiting for X server to start...log located in /tmp/X.log
1...2...3...4...5.... X server started successfully.
```

看到的消息列出Anaconda发现的硬件。如果遇到问题，则可以检查日志文件/tmp/X.log。这个消息有点不同寻常之处，一旦安装Red Hat Linux之后，这个文件实际消失。稍后将介绍这个文件。

如果系统上的硬件能通过测试，则可以看到第一个Anaconda安装屏幕，如图3.11。



图3.11 图形安装开始

基本图形安装屏幕的左窗格中有一些帮助说明。如果单击**Release Notes**，则会打开**Release Notes**窗口，如图3.12，其中包括第一张Red Hat Linux安装光碟**Release Notes**文件中的测试。

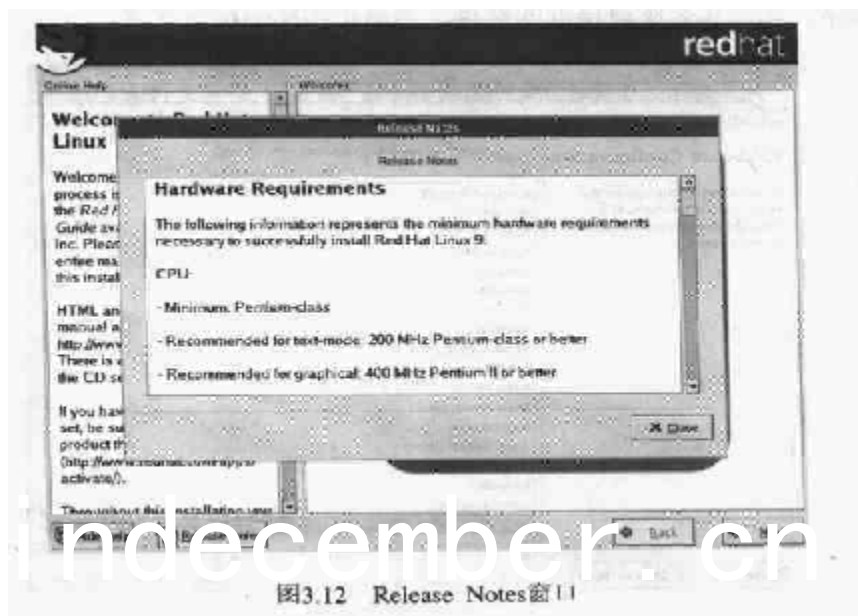


图3.12 Release Notes窗口

阅读版本说明，这样有助于了解Red Hat Linux 9。完成之后，单击**Close**退出版本说明，然后单击**Next**按钮继续。Anaconda打开**Language Selection**屏幕，如图3.13，可以选择其余安装过程使用的20种语言或方言之之一。这并不确定安装Red Hat Linux之后使用的语言，见稍后介绍。本章余下部分假设使用英语。单击**Next**按钮继续。

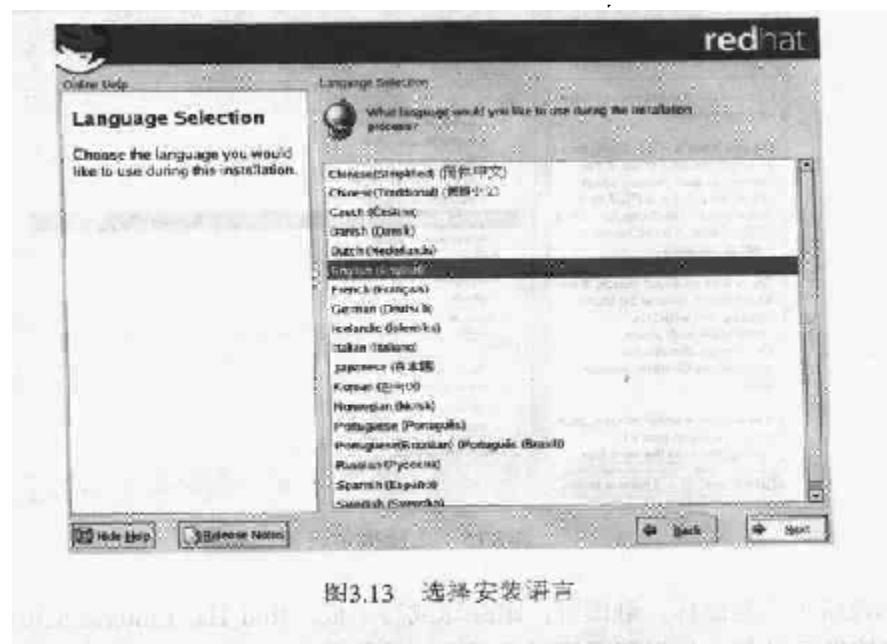


图3.13 选择安装语言

现在看看图3.14所示的Anaconda屏幕，可以选择系统使用的55种键盘之一。如果Anaconda探测到你的键盘，则会加亮显示。你的选择决定了安装Red Hat Linux之后的默认键盘。安装Red Hat Linux之后可以改变默认键盘，只要使用第19章介绍的redhat-config-keyboard实用程序。选择与系统最接近的键盘，然后单击Next按钮继续。

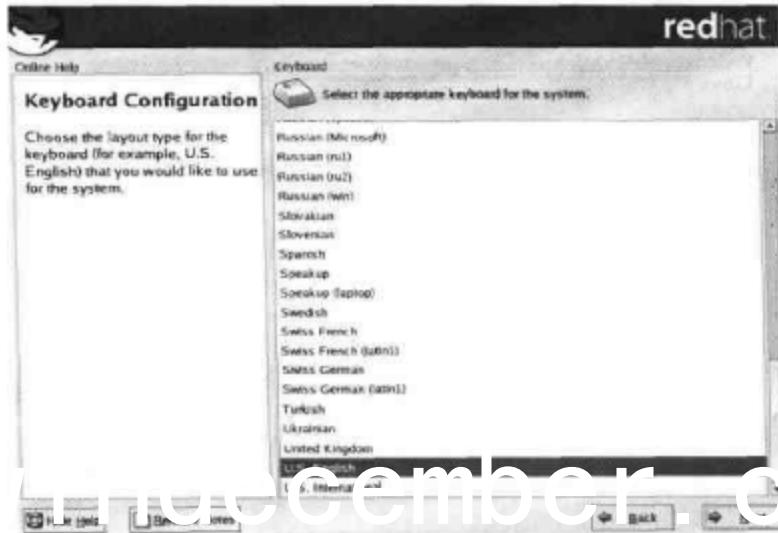


图3.14 选择键盘

然后检查Mouse Configuration屏幕，如图3.15。这个屏幕的标题名不符实，可以用Anaconda配置几种不同类型的指示设备。

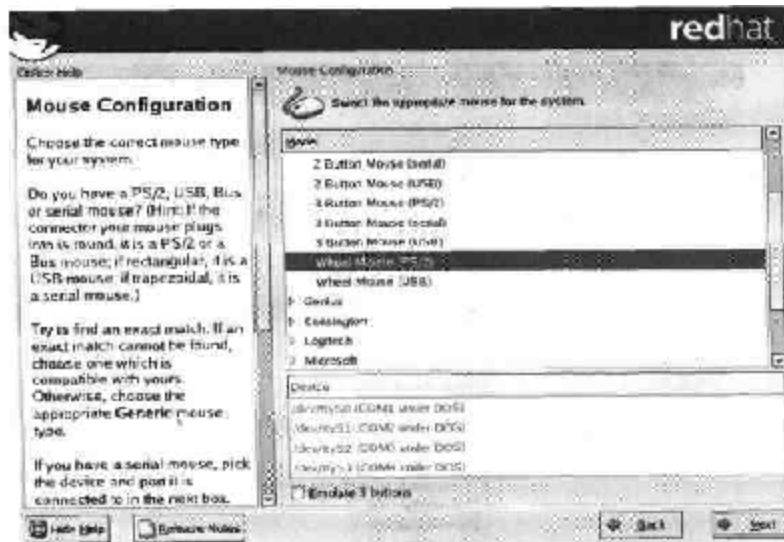


图3.15 选择指示设备

指示设备可以是鼠标、触摸屏、跟踪球或写字板。Red Hat Linux甚至可以使用通过USB端口连接的指示设备。如果配置通过串行端口连接的指示设备，则会激活Device文本框，可

以选择相应的串口设备。

如果使用双键鼠标，则要激活Emulate 3 Buttons选项，从而通过同时按两个鼠标键模拟中间键的功能。但是，如果有鼠标轮，则可以试按鼠标轮。单击时，Red Hat Linux可能已经把它识别为第三个键。

如果Anaconda检测到指示设备，则应在屏幕上加亮显示。安装Red Hat Linux之后，可以用第19章介绍的redhat-config-mouse实用程序改变默认指示设备。选择与系统最接近的指示设备，然后单击Next按钮继续。

如果计算机上包括旧版Red Hat Linux，则可以看到Upgrade Examine屏幕。升级见本章末尾介绍。如果看到图3.16的屏幕，则要选择Perform A New Red Hat Linux Installation并单击Next按钮继续。

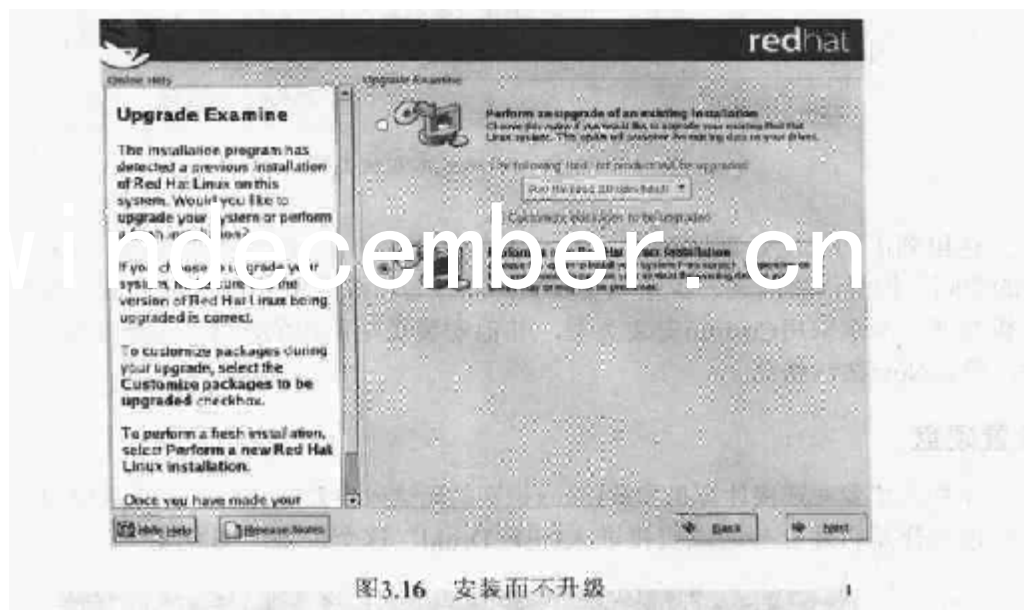


图3.16 安装而不升级

选择安装类型

图3.17显示了四种基本安装类型。每个选项支持不同类型的计算机，与不同类型的软件包组相关联。表3.6总结了每种安装类型的基本特征。

说明：长度要求往往大于安装过程中可能看到的要求。根据依赖性，还要安装其他文件，见Web上第5章详细介绍。

表3.6 安装类型

选项	描述
Personal Desktop	配置PC桌面或便携电脑使用的图形化桌面环境。默认配置安装的文件将近1700MB
Workstation	配置带软件开发与系统管理工具的图形化桌面环境。默认配置安装的文件将近2100MB
Server	对用做服务器的PC机配置文本桌面环境，默认配置安装的文件将近850MB
Custom	设置完全可定制的安装过程，默认配置安装的文件将近1500MB

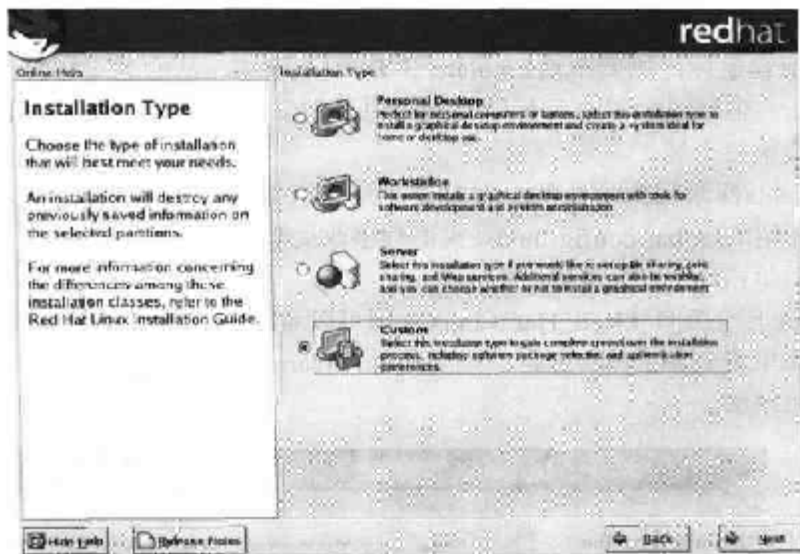


图3.17 四种基本安装类型

这里列出的长度是默认长度，不包括分区和其他个人或第三方文件、应用程序的空间。但是，可以进一步定制要安装的软件包，改变所要的磁盘空间。选择适合需要的安装类型。本章采用Custom安装类型，其他安装类型所用的步骤大致相同。选择Custom之后，单击Next按钮继续。

设置硬盘

下面几步要对连接计算机和被Linux识别的所选硬盘建立分区。一旦选择安装类型之后，就可以选择是否建立分区或直接进入Disk Druid，这个屏幕如图3.18所示。

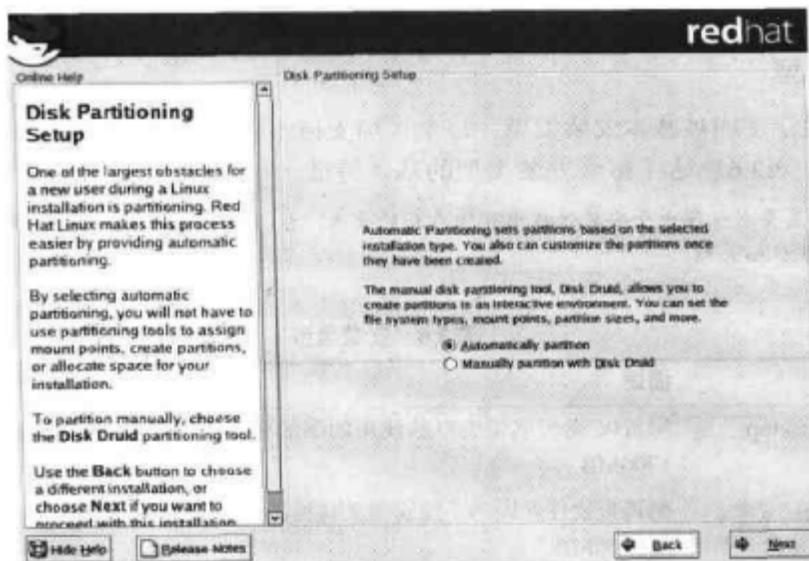


图3.18 选择自动或手工分区

我们选择自动分区，然后进入Disk Druid，看看Anaconda能做些什么。如果选择Manually Partition With Disk Druid，则Anaconda跳过下一步。进行选择，然后单击Next按钮继续。

Anaconda要求输入在哪里采用自动分区。从图3.19可以看出，有几个选项，见表3.7。

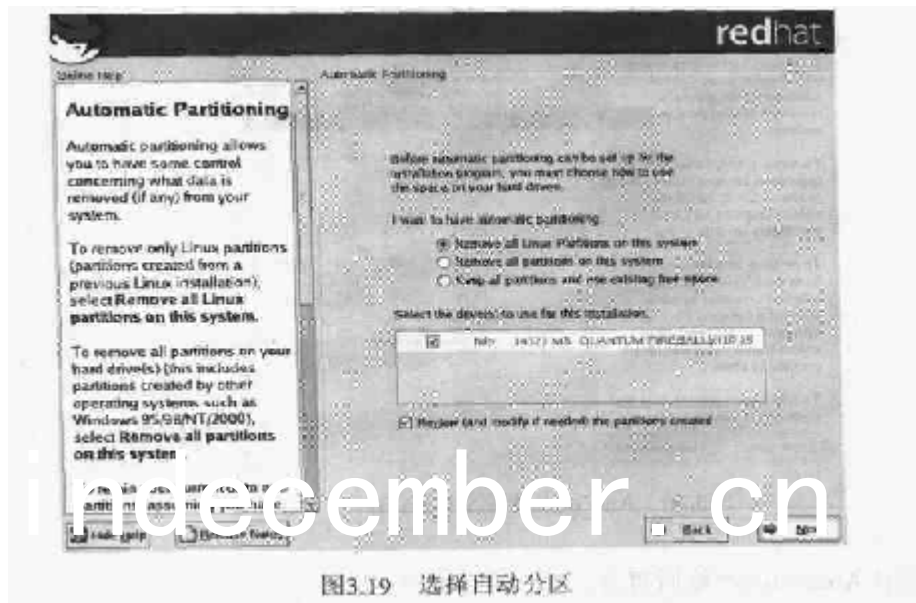


图3.19 选择自动分区

表3.7 自动分区选项

选项	描述
Remove All Linux Partitions On This System	删除当前配置的所有格式化为Linux文件系统的分区，适用于所有选择的硬盘
Remove All Partitions On This System	删除所选硬盘上的所有分区。如果有Microsoft Windows之类的另一操作系统，则这个动作删除该操作系统
Keep All Partitions And Use Existing Free Space	不删除任何分区，在没有分配给分区的硬盘空间中试图配置Red Hat Linux
Select the Drive(s) To Use For This Installation	列出计算机上识别的硬盘，自动分区只适用于选择的盘。hda之类的设备名见第2章介绍
Review (And Modify If Needed) The Partitions Created	选择这个选项时，下一个安装步骤显示Disk Druid中Anaconda建议的分区配置

警告：如果将Red Hat Linux作为服务器与Microsoft Windows之类的操作系统双引导，则要小心。Anaconda默认为Remove All Partitions On This System选项，会删除计算机上的所有Microsoft Windows分区。

本安装中，我们选择Remove All Linux Partitions On This System选项，继续，并选择Review (And Modify If Needed) The Partitions Created选项（如果不选择这个选项，则Anaconda跳过后面的Disk Druid菜单）。进行选择，然后单击Next按钮继续。

Anaconda删除任何分区之前，会发出一个警告消息。如果让Anaconda删除Linux分区，则会出现图3.20所示的消息。

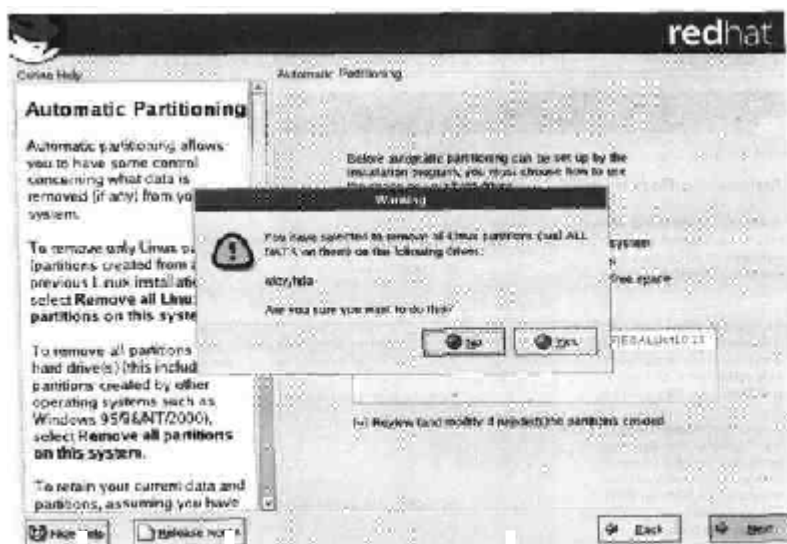


图3.20 Anaconda删除分区时，会发出一个警告消息

如果让Anaconda删除所有分区，则会出现类似警告。一定要确保这些分区确实要删除，然后才能单击Yes按钮继续。

说明：还可能遇到/boot分区的警告。如果计算机上已经有Microsoft Windows之类的另一个操作系统，则Anaconda可能无法在硬盘上最理想的区域（1024柱面以下）安装/boot分区。一些旧计算机上的BIOS无法找到这个柱面以上的/boot分区中放置的Linux引导文件。即使计算机受到影响，至少也可以用两种方法解决这个问题。可以从引导盘引导Linux，也可以安装第三方引导装入器，如Partition Magic与System Commander。

用Disk Druid建立分区

Disk Druid是Anaconda的半自动磁盘分区实用程序。图3.21显示了桌面计算机用Disk Druid自动分区的结果。

可以想像，这是个双引导安装，/dev/hda1分区格式化为Microsoft的FAT32文件系统格式，/dev/hda5上配置的交换分区长度为这个桌面计算机内存长度的两倍。

说明：如果安装Red Hat Linux的计算机上已经安装Microsoft Windows，则Anaconda把FAT16与FAT32分区显示为vfat类型。

Disk Druid屏幕分成几个部分，上方是计算机识别的硬盘配置的当前分区图，然后是一系列命令按钮，可以不断试验，下方是每个盘和分区上的数据，见表3.8介绍。

表3.8 Disk Druid磁盘定义

列	描述
Device	列出每个硬盘和分区的设备文件
Mount Point/RAID/Volume	指定分区装载的目录

(续表)

列	描述
Type	指定分区文件系统
Format	指定要格式化的盘（如果选择）
Size	列出分区长度（MB）
Start	指定分区的开始柱面
End	指定分区的结果柱面

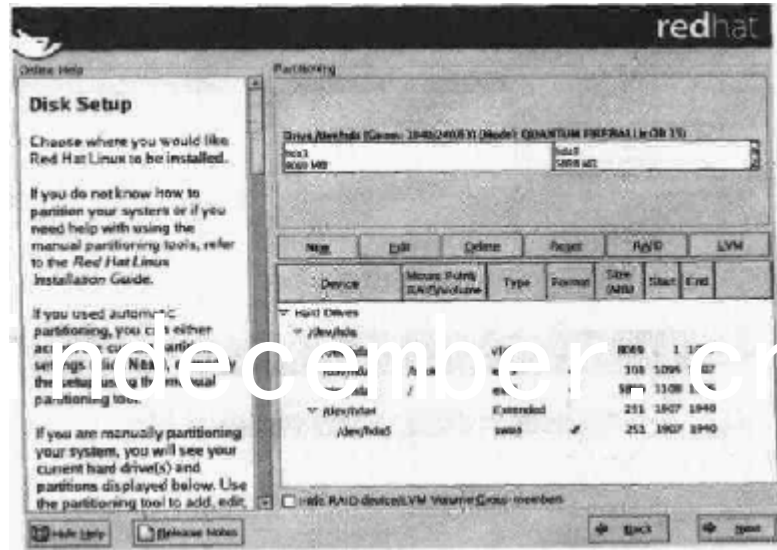


图3.21 Disk Druid自动分区的结果

在屏幕下方，可以选择Hide RAID Device/LVM Group Members。如果激活这个选项，则不会显示RAID或逻辑卷组中的分区。关于RAID的更多信息，见第14章，关于逻辑卷组的更多信息，见第7章。

下面介绍图3.21列出的每个命令选项。我们使用下面几节介绍的配置进行演示。由于所列硬盘中目前没有空间，因此要先删除一个分区。

删除一个分区

要删除一个分区，加亮这个分区并单击Delete按钮。在图3.21所示的例子中，我们加亮/dev/hda3分区并单击Delete按钮。删除分区之前，会要求确认，如图3.22。

这样就从删除分区得到了自由空间。

增加分区

硬盘中要有自由空间才能增加分区。如果硬盘中有自由空间，则可以单击New，打开Add Partition对话框，如图3.23，表3.9列出了图中每个项目。

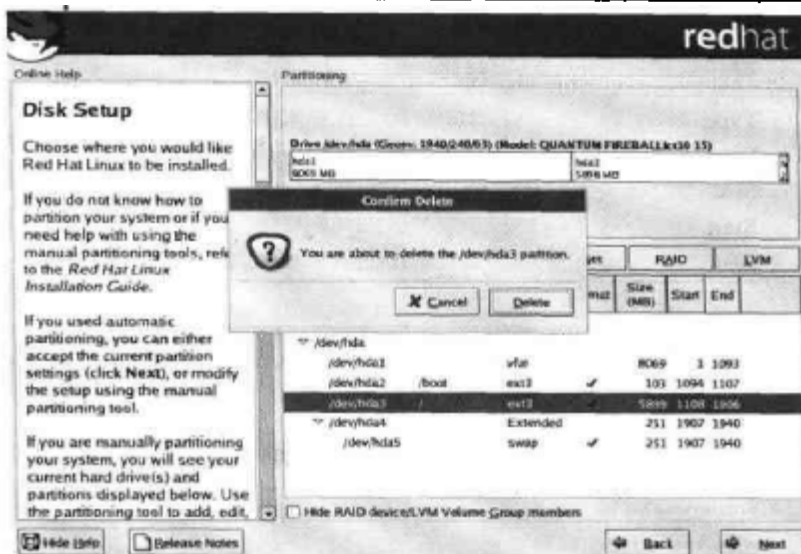


图3.22 确认删除分区



图3.23 增加分区

表3.9 Add Partition对话框选项

选项	描述
Mount Point	指定分区上要装载的目录，对可装载目录，见第7章介绍的文件系统层次标准。这不适用于LVM、RAID或交换类型的文件系统
File System Type	设置分区格式，可以选择Linux ext2或ext3标准、Linux交换格式、LVM（逻辑卷管理器）物理卷、软件RAID卷或Microsoft Windows vfat格式
Allowable Drives	指定与分区相关联的硬盘设备

(续表)

选项	描述
Size (MB)	指定分区长度 (MB)
Fixed Size	设置指定的分区长度
Fill All Space Up To (MB)	如果硬盘上有自由空间, 则这个分区的长度增加到指定极限
Fill To Maximum Allowable Size	填充硬盘上其余自由空间
Force To Be A Primary Partition	一般来说, 引导目录应放在1024柱面以下的主分区中
Check For Bad Blocks	对不可读扇区设置分区物理检查

提示: 在硬盘上设置分区时, 记住IDE硬盘最多16个分区, SCSI硬盘最多15个分区。超出这个极限时, 开始不会遇到问题, 但看上去安装完成时, 其实已经出问题了。

本章增加四个LVM分区、四个软件RAID分区, 并把其余空间作为一个根 (/) 目录分区。单击RAID与LVM按钮演示能做的工作时, 可以看到这个工作。

编辑分区

编辑分区与增加分区非常相似。例如, 图3.24演示了将根 (/) 目录加亮与编辑分区时发生的情形。屏幕中的信息与图3.23一致。该图详细列出了编辑分区窗口的内容。

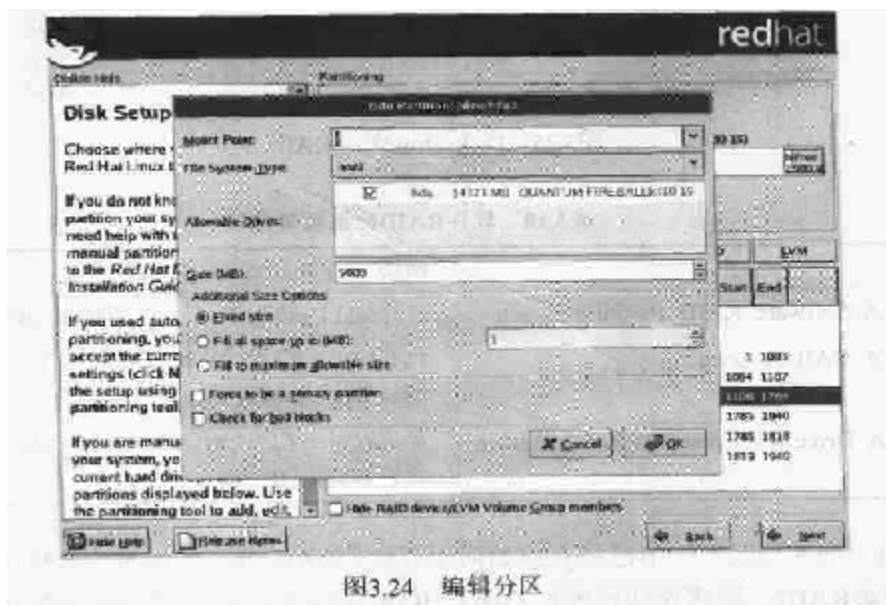


图3.24 编辑分区

警告: Anaconda不能在有坏块的硬盘上安装Red Hat Linux 9。

复位分区表

所做的任何改变都要到分区格式化时才写入。如果要恢复硬盘上原先的分区表, 只要单击Reset, 还有一个确认机会。一旦确认之后, 分区表即返回开始Disk Druid时的分区表。

建立RAID

配置软件RAID分区之后，可以生成RAID阵列。理想情况下，RAID阵列中的软件分区应在不同物理硬盘上，然后，一个硬盘发生故障时不会破坏RAID 1或RAID 5阵列中的数据。详细信息见第14章。

单击RAID，Disk Druid打开图3.25所示的RAID选项屏幕。可以看出，这个窗口包含三个选项，如表3.10所示。

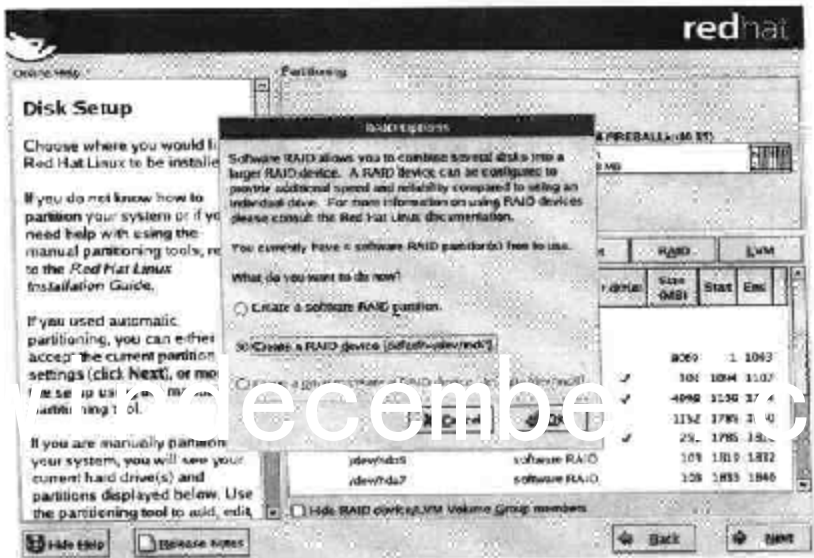


图3.25 Disk Druid软件RAID选项

表3.10 软件RAID配置菜单选项

选项	描述
Create A Software RAID Partition	打开Add Partition窗口，显示软件RAID文件系统类型
Create A RAID Device	打开Make RAID Device窗口，可以指定RAID设备的软件RAID格式化分区
Clone A Drive To Create A RAID Device	如果有两个不同的物理硬盘，则可以从一个盘向另一个盘复制RAID设备

前面“增加分区”一节已经介绍如何生成软件RAID分区。如果计算机上有多个硬盘，要认真考虑RAID，则建议阅读硬件RAID HOWTO文献，网址为www.tldp.org。

本安装选择Create A RAID Device选项。单击OK按钮之后，Disk Druid打开Make RAID Device窗口，如图3.26所示。

如图所示，我对/home/mj目录生成RAID设备。这是个RAID 5设备，格式化为Linux ext3文件系统。由于RAID 5至少要求三个成员分区，因此可以用一个多余分区设置。如果一个分区坏了，则RAID 5在多余分区上自动重建所要的数据。

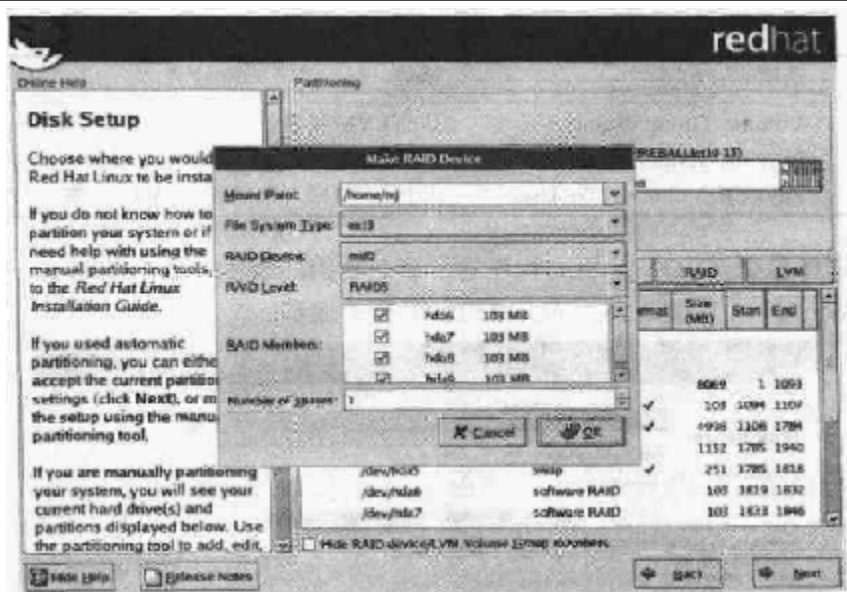


图3.26 建立 RAID设备

建立LVM

配置LVM物理卷之后，可以生成LVM卷组。LVM在单硬盘中更实用。由于组中可以增加和删除LVM物理卷，因此可以对/usr之类的目录指定的分区增加或减少长度。更多信息见第7章介绍。

单击LVM，Disk Druid打开图3.27所示的Make LVM Volume Group屏幕。表3.11列出了图中每个可配置选项。

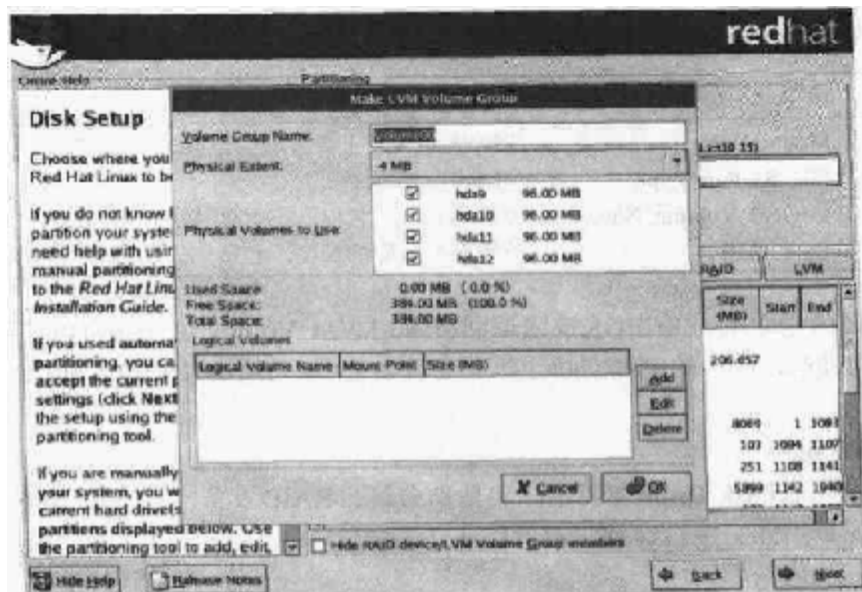


图3.27 建立LVM卷组

表3.11 建立LVM卷组选项

选项	描述
Volume Group Name	设置LVM卷组名
Physical Extent	指定与这个卷组相关联的磁盘空间块
Physical Volumes To Use	列出LVM格式物理卷（PV）

一定要选择卷组（VG）要用的物理卷。命名卷组，然后单击Add按钮，从而打开Make Logical Volume窗口，如图3.28。表3.12列出了有关选项。

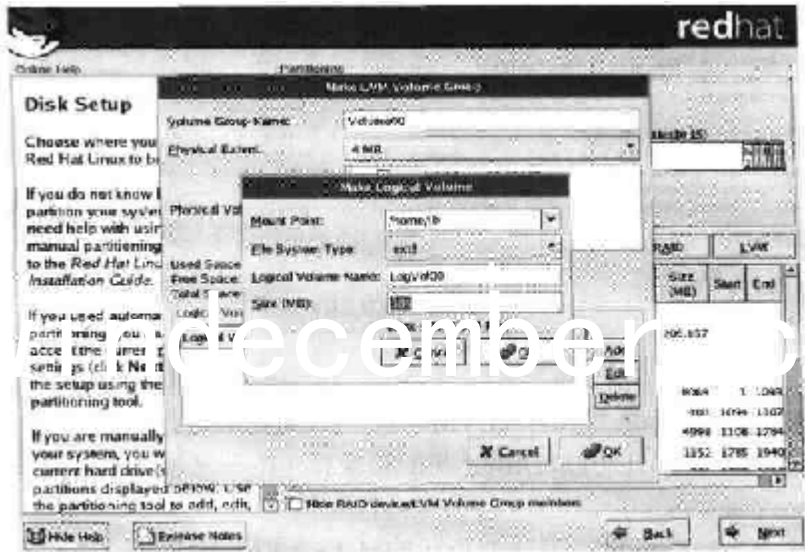


图3.28 建立逻辑卷

表3.12 建立逻辑卷选项

选项	描述
Mount Point	逻辑卷（LV）上要装载的目录
File System Type	与LV相关联的格式
Logical Volume Name	逻辑卷的任意名称
Size（MB）	逻辑卷要分配的长度，包括加进逻辑卷中的物理卷

生成逻辑卷之后，单击OK按钮返回Make LVM Volume Group窗口。注意，自由空间量减去了加进逻辑卷中的物理空间。建立逻辑卷之后，单击OK按钮回到主Disk Druid窗口。

离开Disk Druid

最后结果在Disk Druid中显示，包括新分区、RAID设备阵列和LVM卷组，如图3.29。完成之后，单击Next按钮继续。离开Disk Druid。

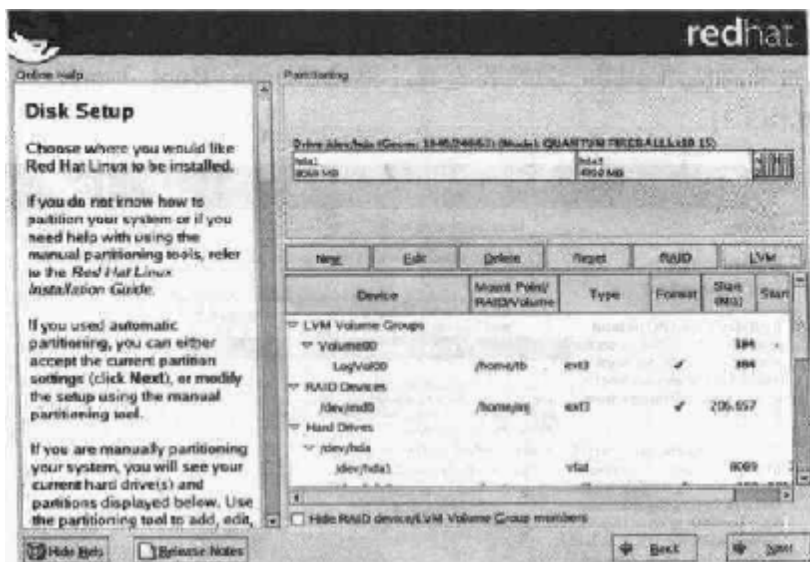


图3.29 Disk Druid中显示修改的分区表

配置安装细节

下面要介绍Disk Druid与包组选择之间的Red Hat Linux安装过程细节。这里内容丰富多样，包括引导装入器配置和验证配置。

引导装入器配置

完成Disk Druid工作之后，就要进行引导装入器配置，其在首次启动计算机时出现。Anaconda会打开Boot Loader Configuration屏幕，如图3.30。

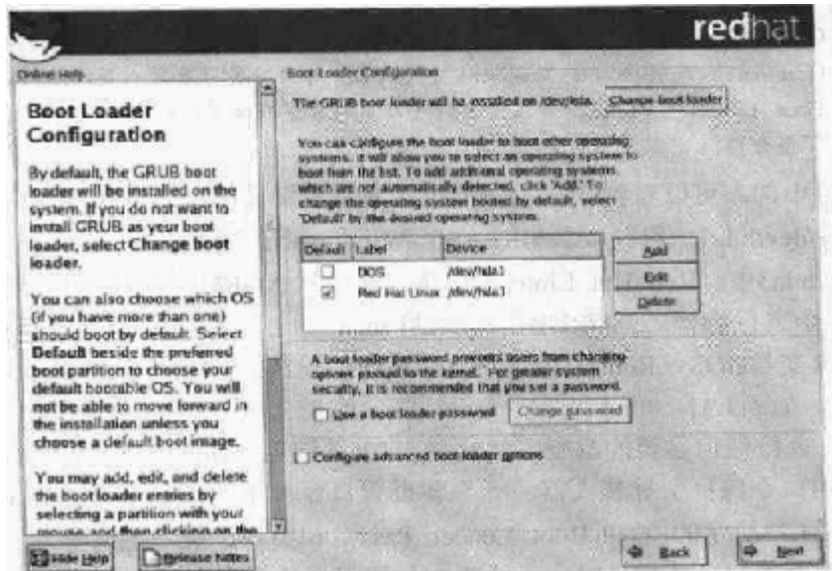


图3.30 Boot Loader Configuration屏幕

默认GRUB屏幕顶部的消息显示GRUB安装在第一个IDE硬盘（/dev/hda）的主引导记录（MBR）中。如果要使用不同的引导装入器，单击Change Boot Loader打开Change Boot Loader窗口，如图3.31。

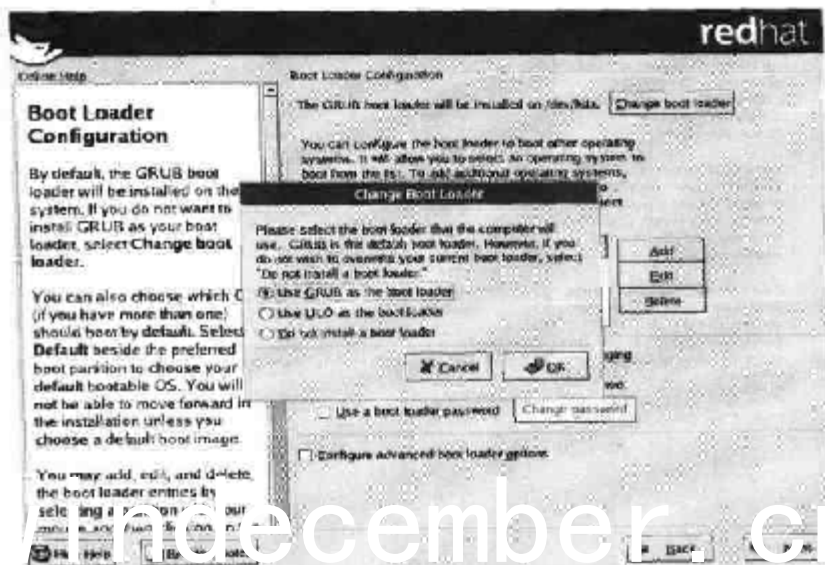


图3.31 选择引导装入器

说明：Red Hat Linux中的引导装入器有时称为bootloader，有时称为boot loader。

Red Hat Linux中可以安装引导装入器GRUB或LILO（Linux Loader）。如果已经安装引导装入器而不想覆盖，则要选择Do Not Install A Boot Loader选项。进行选择并单击OK按钮，也可以单击Cancel按钮保持默认引导装入器，返回主Boot Loader Configuration屏幕。

说明：GRUB或LILO（Linux Loader）可以和其他引导装入器一起使用，如Partition Magic、System Commander或Microsoft Windows NTLDR。选择安装引导装入器，选择Configure Advanced Boot Loader Options，并在具有引导目录的分区中安装GRUB或LILO（Linux Loader），见下节介绍。

在屏幕中部，可以看到，Anaconda正在双引导配置中安装Red Hat Linux。标为DOS的分区设备/dev/hda1中已经安装Microsoft Windows操作系统，主Red Hat Linux文件安装在分区/dev/hda3中。Red Hat Linux是默认，其中默认GRUB配置表示，如果10秒钟内不在GRUB菜单中进行选择，则GRUB自动启动Linux。

可以改变与DOS或Red Hat Linux相关联的设置，为此要加亮设置并选择Edit，打开Image窗口，如图3.32，可以在其中编辑标签、改变分区设备、把相关操作系统设置为默认操作系统。进行任何必要的改变，然后单击OK按钮返回Boot Loader Configuration屏幕。

可以用口令保护引导装入器。如果要设置口令，单击Use A Boot Loader Password选项，打开图3.33所示的Enter Boot Loader Password窗口，提示两次输入所要口令。这个口令使别人在重新启动计算机时，无法改变你的引导装入器配置文件。

最后，激活屏幕底部的Configure Advanced Boot Loader Options，单击Next按钮继续。

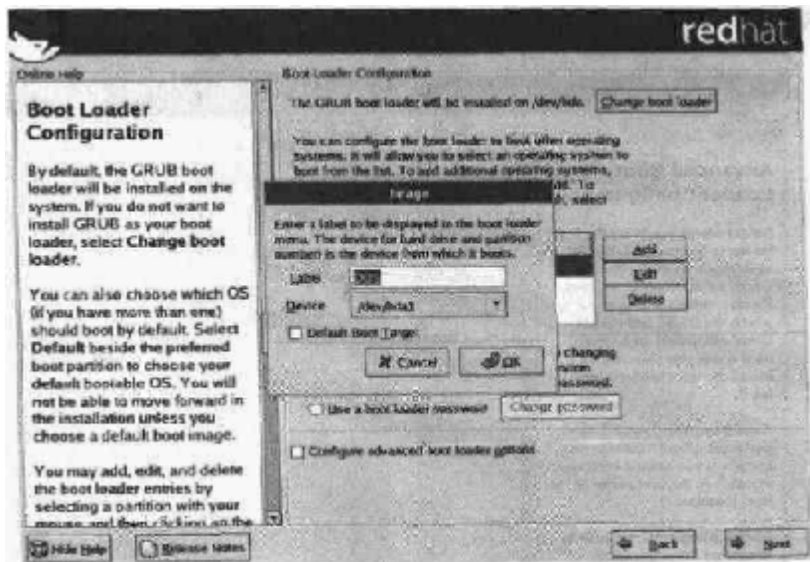


图3.32 引导装入器映像属性

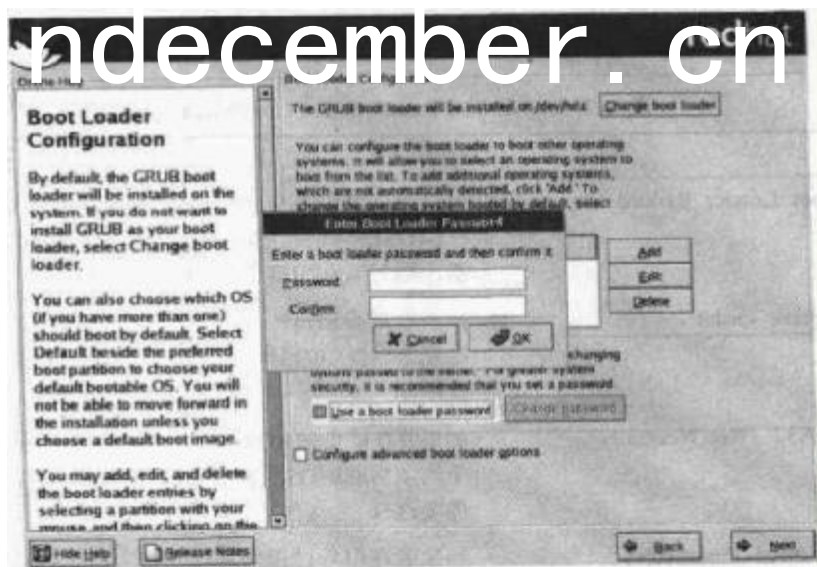


图3.33 Enter Boot Loader Password窗口

高级引导装入器配置

如果单击Next按钮继续，则会打开图3.34所示的Advanced Boot Loader Configuration屏幕，可以配置与引导装入器相关的另外几个内容，见表3.13。进行任何改变，然后单击Next按钮继续。

网络配置

现在可以配置Anaconda探测的任何网卡。默认情况下，网卡设置成从DHCP（动态主机配置协议）服务器自动取得网络参数。如果网络上有DHCP服务器，则可以分配主机名和向

计算机提供网关和DNS服务器的IP地址。

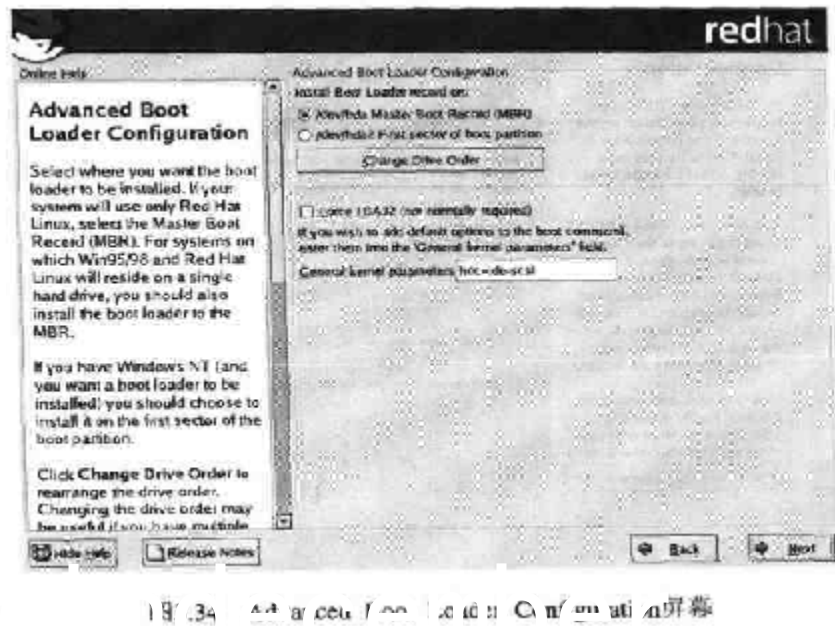


表3.13 Advanced Boot Loader Configuration选项

选项	描述
Install Boot Loader Record On	可以在硬盘的主引导记录（MBR）中配置引导装入器，其在BIOS指向该盘时运行。如果MBR中有另一个引导装入器，则可以在引导分区的第一扇区中装入引导装入器
Change Drive Order	如果物理盘超过两个，则可能要重排硬盘顺序，保证BIOS检查适当盘中的引导装入器。第2章详细介绍了这个BIOS硬盘限制
Force LBA32 (Not Normally Required)	如果要在硬盘的1024以上柱面中装载引导目录，则可以用这个选项帮助BIOS找到Linux引导文件。在新的硬盘中通常不需要这样
General Kernel Parameters	如果要在引导过程中将参数传入Linux内核，则可以在这里指定。在图3.34的例子中，Anaconda自动增加光碟刻录机的SCSI仿真模块

即使是家庭网络，也可能有DHCP服务器。许多高速互联网路由器/电缆MODEM/DSL适配器就是用DHCP服务器装备的。详见硬件文档。

我们显示图3.35的网络配置屏幕，并介绍表3.14所列的基本选项。图中显示的两个网络设备是以太网网络适配器eth0与eth1。

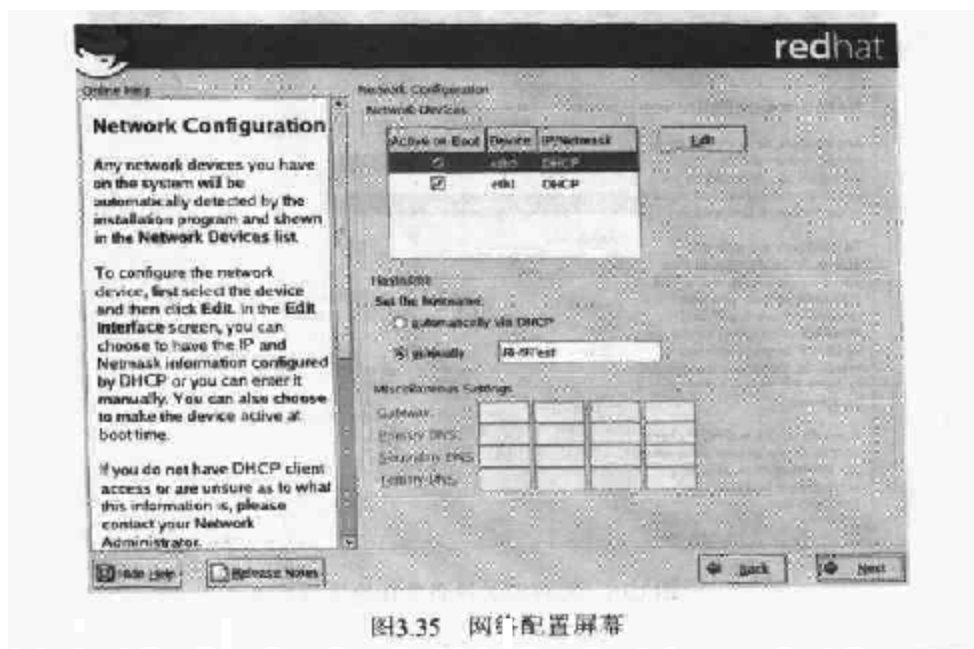


图3.35 网络配置屏幕

表3.36 网络配置选项

选项	描述
Active On Boot	选择这个选项时，在引导过程中激活相关的网络设备
Edit Starts the Edit Interface	加亮设备的设备窗口，可以用静态IP地址手工配置网卡
Hostname	可以对这台计算机指定主机名，否则由网络上的DHCP服务器完成这个工作
Gateway	注意网络外部消息的网关IP地址，如果手工配置网卡，则可以设置这个网关
Primary DNS	列出网络上DNS服务器的IP地址，如果手工配置网卡，则可以设置这个IP地址
Secondary DNS	列出网络上另一DNS服务器的IP地址
Tertiary DNS	列出网络上另一DNS服务器的IP地址

如果喜欢对网卡指定静态IP地址，则可以加亮所要设备和单击Edit，其打开Edit Interface Device窗口，如图3.36。

要设置静态IP地址，取消Configure Using DHCP选项，然后可以输入所选的IP地址和网络掩码。关于专用网络IP地址的准则，见第20章介绍。进行所要的改变，然后单击OK按钮返回网络配置屏幕。

如果安装Red Hat Linux之后改变了主意，则可以用第19章介绍的redhat-config-network实用程序编辑配置。

完成之后，单击Next按钮继续。

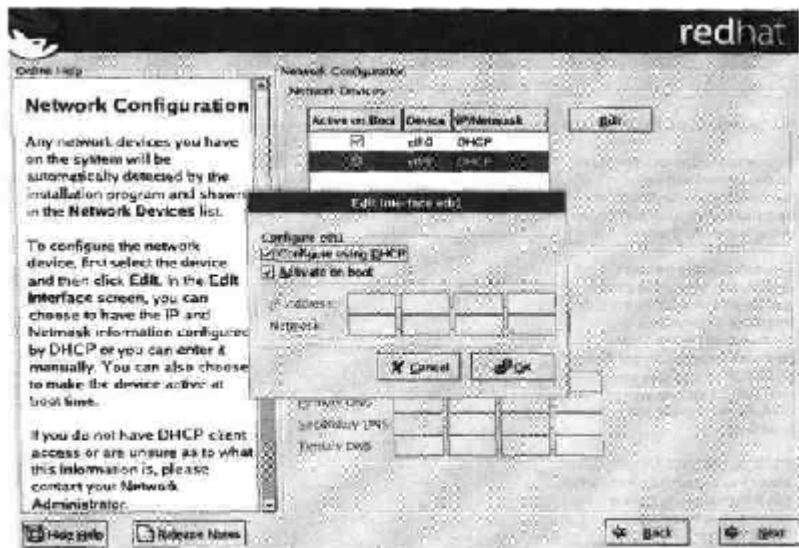


图3.36 配置网关设备的IP地址信息

防火墙配置

现在要进行Red Hat Linux的防火墙配置。这对网关计算机特别重要，其可能提供局域网与互联网之间的联系。在这种情况下，最好把防火墙放在网关计算机上，防止互联网对局域网的侵入。在Red Hat Linux 9中，其在/etc/sysconfig/iptables中生成基于iptables的防火墙。图3.37显示了网关计算机一个可能的配置，下面介绍这些配置选项。

High 配置高度安全的防火墙，阻止几乎所有进入的通信流，只有一个外部DNS服务器发来的消息可以通过，其支持与互联网的连接。

Medium 配置中等安全的防火墙，阻止TCP/IP端口0到1023的通信流，阻止可以访问NFS服务器、本地X窗口服务器与X字体服务器的端口的通信流。

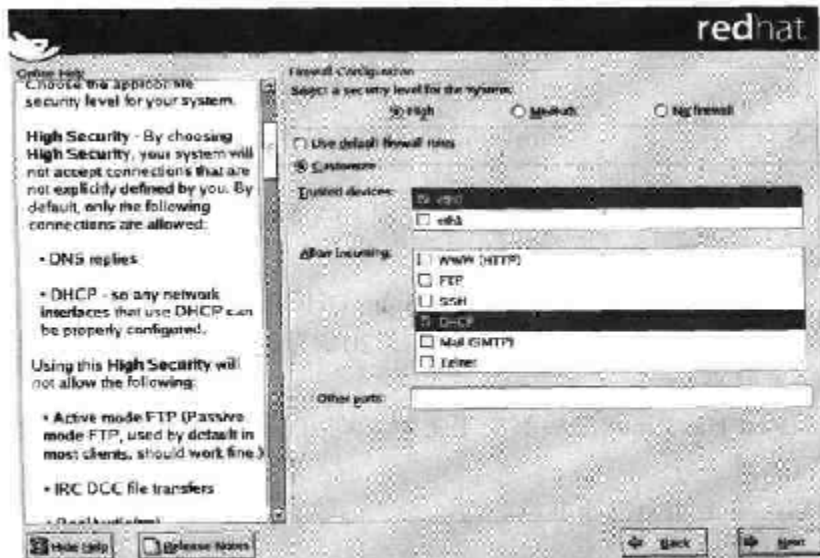


图3.37 防火墙配置

No Firewall 在这台计算机上关闭所有iptables防火墙命令。

Use Default Firewall Rules 采用默认高级或中级安全防火墙，不修改这台计算机上的所有网卡。

Customize 可以对这台计算机上的一个或几个网卡指定不同规则。

Trusted Devices 列出这台计算机上的网络设备，这里是eth0与eth1。通常对连接局域网而不是连接互联网的以太网卡关闭防火墙，这里eth0是信任设备。

Allow Incoming 如果计算机上有一台服务器，则可以允许来自其他网络的输入通信流。例如，如果计算机上有一台Web服务器，则可以通过与Web（HTTP）通信流相关的TCP/IP端口，开放输入数据（见第30章）。其他选项与FTP（文件传输协议，见第27章）、SSH（安全Shell，见第22章）、Sendmail之类的邮件服务器（见第26章）或Telnet（见第23章）相关。

默认情况下，即使高度安全防火墙也允许与DNS（域名服务）服务器相关的通信流进入，帮你导航互联网和DHCP（动态主机配置协议）服务器，使你可以从局域网以外取得IP地址信息。关于这些服务的更多信息，见第24章。

Other Ports 如果要通过防火墙访问其他服务，则要在相关文本框中输入相应端口和协议。例如，如果要用HTTPS协议连接安全Web服务，则要在该文本框中输入下列内容：

```
https:tcp,https:udp
```

安装Red Hat Linux之后，可以用第16章介绍的GNOME Lokkit向导、第19章介绍的redhat-config-securitylevel或第22章介绍的iptables命令，改变防火墙设置。进行所要的改变，然后单击Next按钮继续。

说明：这不影响与第23章介绍的xinetd服务相关联的任何防火墙，或与本书介绍的各个网络服务相关联的任何防火墙。

其他语言支持

在图3.38所示的安装屏幕中，可以在安装Red Hat Linux之后设置默认语言。可以看到，有些语言包括各种国家方言。

如果需要不同语言或其他语言，则可以相应选择。如果将Anaconda配置成安装多个语言，则可以单击Select The Default Language For The System框旁边的下拉箭头，从这些语言中选择默认语言。安装Red Hat Linux之后，可以用第19章介绍的redhat-config-language改变默认语言。进行所要改变，然后单击Next按钮继续。

选择时区

在这个安装屏幕中，可以配置计算机的基本时间设置。安装之后，还可以进一步配置。如果利用本章稍后介绍的firstboot实用程序，或第19章介绍的redhat-config-time，则可以将这台计算机设置成与中央时间服务器同步的时间。

选择时区的屏幕有两个标签，Location标签如图3.39。

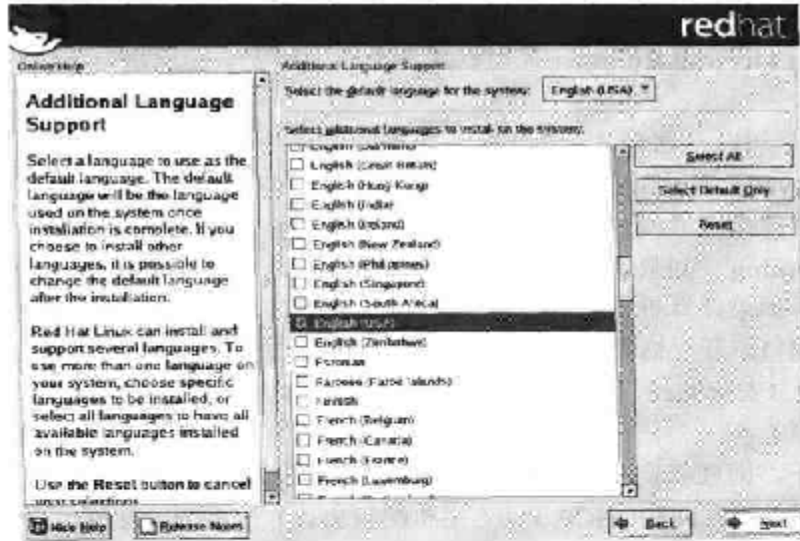


图3.38 选择语言

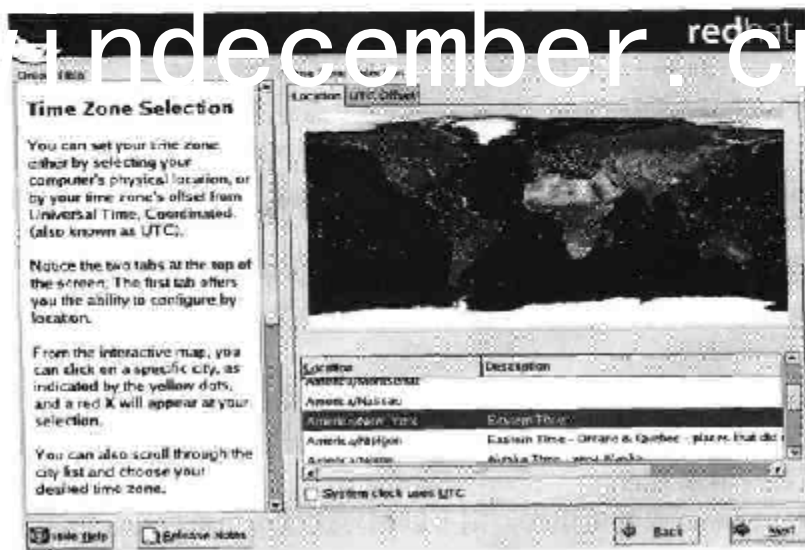


图3.39 选择时区地点

要选择与一个地点相关联的时区，可以单击地图，或从滚动窗口中选择时区地点。除非计算机处于双引导配置，还有Microsoft Windows之类的另一个操作系统，否则应激活System Clock Uses UTC选项。进行选择，然后单击UTC Offset标签，如图3.40。UTC是格林威治平均时间的法文缩写。

在UTC Offset标签中，选择与时间相应的偏差，例如，美国西海岸时间比格林威治平均时间晚八个小时，对应于UTC-8。如果在美国，还可以激活Use Daylight Saving Time (US Only) 选项。进行选择，然后单击Next按钮继续。

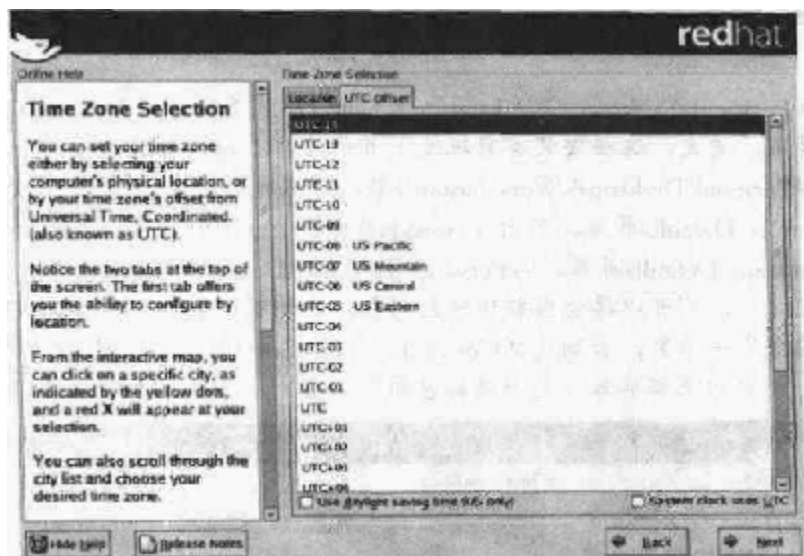


图3.40 UTC Offset标签

设置根用户口令

根用户也称为超级用户，根用户可以在Linux计算机上进行任何操作。在图3.41所示的根用户口令安装屏幕中，输入所要口令，要输入两次。红帽子软件要求，这个过程中输入的根用户口令至少由6个字母数字字符构成。

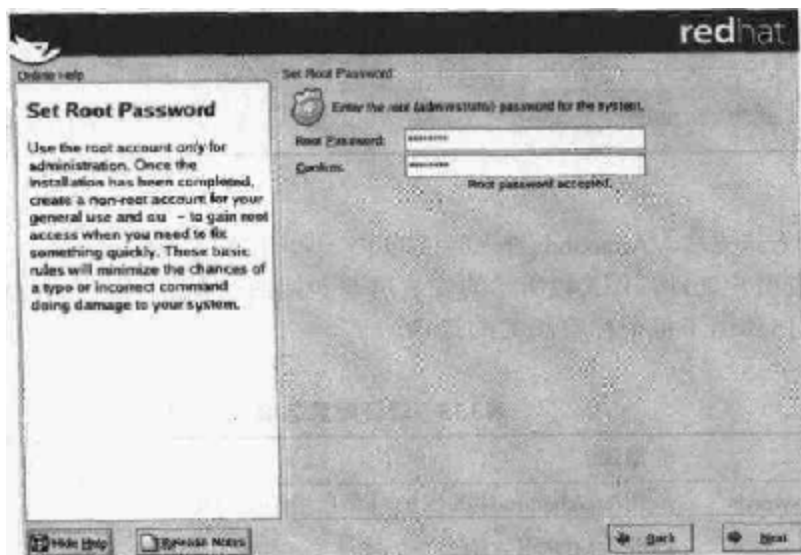


图3.41 设置根用户口令

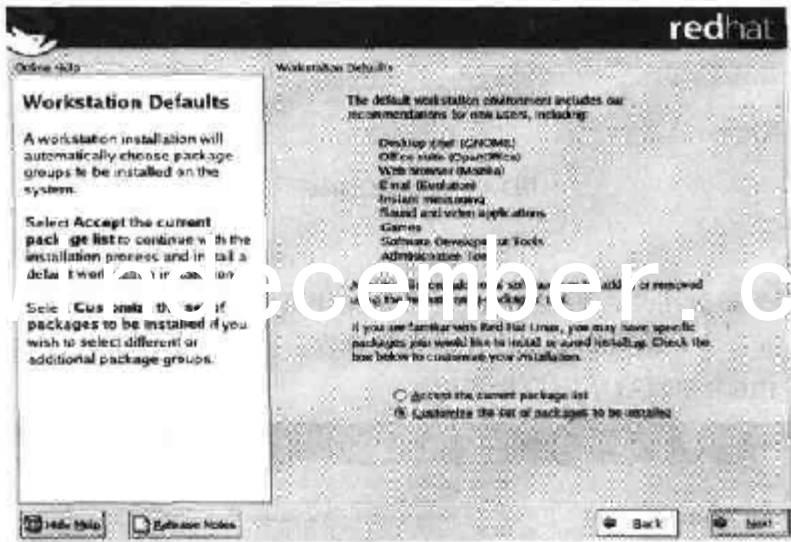
最好的口令要组合数字和大小写字母，可能要用PC攻克程序计算几天或几个星期才能找到这种口令。但这种口令不一定会很难记，我常常用自己喜欢的句子缩写生成口令。例如，Ieic3teM表示“I eat ice cream 3 times every Monday”。

输入所要的根用户口令，然后单击Next按钮继续。

非定制安装

如果选择Personal Desktop、Workstation或Server安装类型，则Anaconda移到另外两个不同的安装屏幕。首先，这些安装类型跳过了节介绍的Configure Authentication屏幕。

如果选择Personal Desktop或Workstation安装，则这时Anaconda提供一个Personal Desktop或Workstation Defaults屏幕，列出Anaconda在Red Hat Linux中默认安装的一些软件。下面是Workstation Defaults屏幕，与Personal Desktop Defaults屏幕的样子差不多。如果选择这两种安装之一，则可以接受当前软件包列表，这时可以直接进入Ready To Install屏幕（见“准备安装”一节），否则选择Customize The Set Of Packages To Be Installed选项，进入第一个包组选择屏幕（见“选择包组”一节）。



验证配置

进入命令行方式之后，Anaconda进入验证的下一步，出现验证配置屏幕，可以配置Red Hat Linux如何检查用户证件。图3.42所示的安装屏幕包括四个标签：NIS、LDAP、Kerberos 5与SMB。表3.15列出了每个标签相关的选项。

表3.15 验证配置选项

选项	描述	标签
Shadow Passwords	用/etc/shadow中的保护口令启用阴影口令组件	N/A
MD5	允许MD5形式的口令加密	N/A
Enable NIS	触发使用NIS（网络信息服务），对局域网提供用户名与口令的公共数据库，详见第28章	NIS
NIS Domain	在这个文本框中输入NIS域名	NIS
Use Broadcast To Find NIS Server	选择这个选项时向网络上其他计算机发送广播消息，标识NIS服务器	NIS
NIS Server	如果关闭广播选项，则设置网络的NIS服务器名	NIS

(续表)		
选项	描述	标签
Enable LDAP	启用验证的LDAP（轻量级目录辅助协议）和相关局域网数据库	LDAP
LDAP Server	设置LDAP数据库所在服务器名	LDAP
LDAP Base DN	允许用LDAP区别名（DN）查找账号信息	LDAP
Use TLS Lookups	让计算机用TLS（传输层安全）向LDAP服务器发送加密用户名与口令	LDAP
Enable Kerberos	允许使用麻省理工学院开发的Kerberos 5系统，支持用户名与口令的强加密	Kerberos 5
Realm	允许访问Kerberos支持网络	Kerberos 5
KDC	可以访问KDC（密钥分配中心）服务器，发出Kerberos验证票	Kerberos 5
Admin Server	允许用kadmin实用程序访问Kerberos服务器	Kerberos 5
Enable SMB Authentication	允许用SMB（Samba）服务器进行验证，如Microsoft Windows Server操作系统	Kerberos 5 SMB
SMB Server	可以设置用用户认证和验证的SMB服务器名	SMB
SMB Workgroup	可以指定与SMB验证服务器相关联的工作组或域	SMB

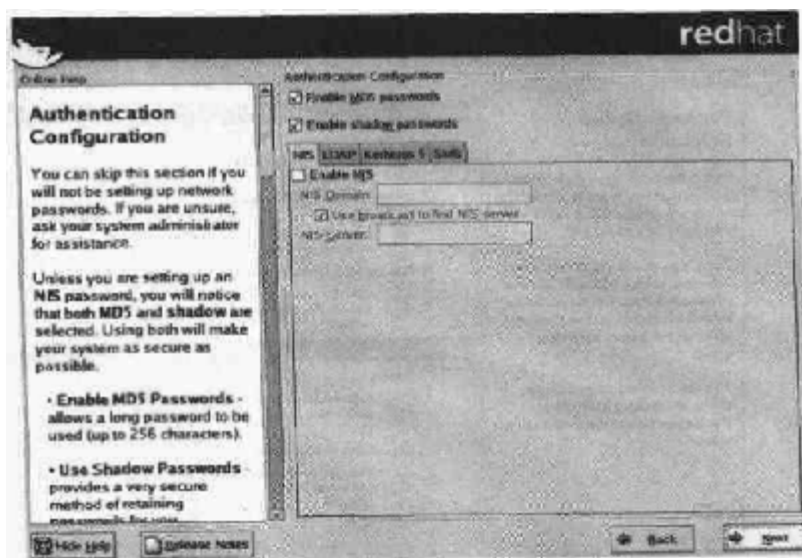


图3.42 验证配置屏幕

除非网络特别需要这些服务，否则默认配置就足够了。例如，图3.43演示了如何将系统连接到工作组或域Group1中SMB（Samba）服务器Master1上的用户名与口令数据库。

进行必要的改变，然后单击Next按钮继续。

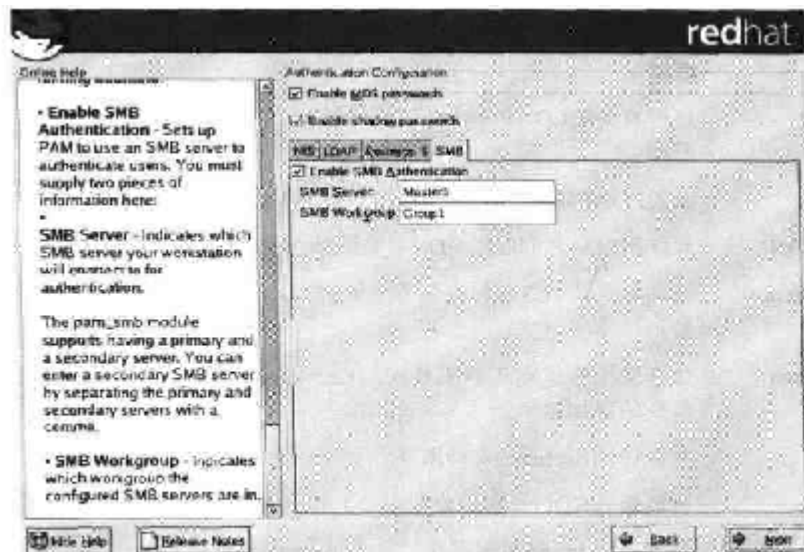


图3.43 配置SMB（Samba）验证

选择包组

最后要选择和Red Hat Linux一起安装的内容。我们已经配置了除图形系统以外的一切。现在要看看选择包组的安装屏幕，如图3.44。

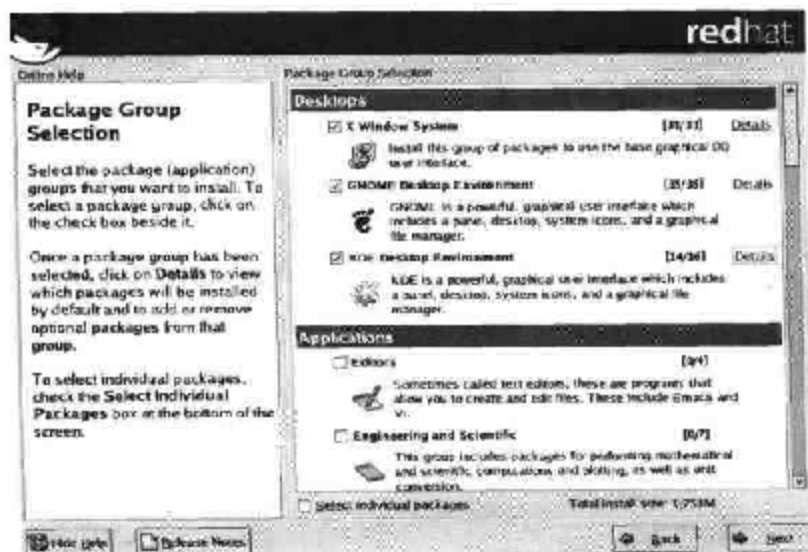


图3.44 选择包组

包与组

如果你不熟悉Linux，则下面要介绍一些基本知识。红帽子公司把软件组织成包，称为RPM（红帽子包管理器），红帽子Linux安装光碟中大约有1500个RPM，其中许多RPM是相互依赖的。例如，要安装与GNOME桌面相关联的大多数软件包，就要安装Linux X Window Server。

安装Red Hat Linux时，即使熟练用户通常也不想在安装过程中选择这1500个RPM，因此红帽子公司把RPM组织成包组，在选择包组的安装屏幕中显示。

换句话说，RPM也称为包，红帽子公司把常用的RPM放在一起，形成包组。

红帽子包组对应于第一张Red Hat Linux安装光碟中的comps.xml配置文件，在/RedHat/base目录中。Web上的第5章将详细介绍这些文件，见Sybex公司Web站点www.sybex.com。

选择所要的包组。如果不想安装Games与Entertainment之类的包组，则可以将其取消，从而节省空间。如果需要了解每个包组中各个包的详细信息，见Web上第5章。

Anaconda图形安装把包组分成五大类，有三个桌面组，如图3.44。表3.16总结了这些组。

表3.16 桌面包组

包组	描述
X Window System	安装基本XFree86 Server、字体和几个GUI配置文件
GNOME Desktop Environment	增加使用GNOME桌面所需的软件包
KDE Desktop Environment	增加使用KDE桌面所需的软件包

看看每个包组右边的包数。例如，图3.44中，看看与KDE桌面环境包组相关的包数，说明这个包组中会安装14个包。在这个数字右边单击Details，可以打开Details For 'KDE Desktop Environment'窗口，如图3.45。

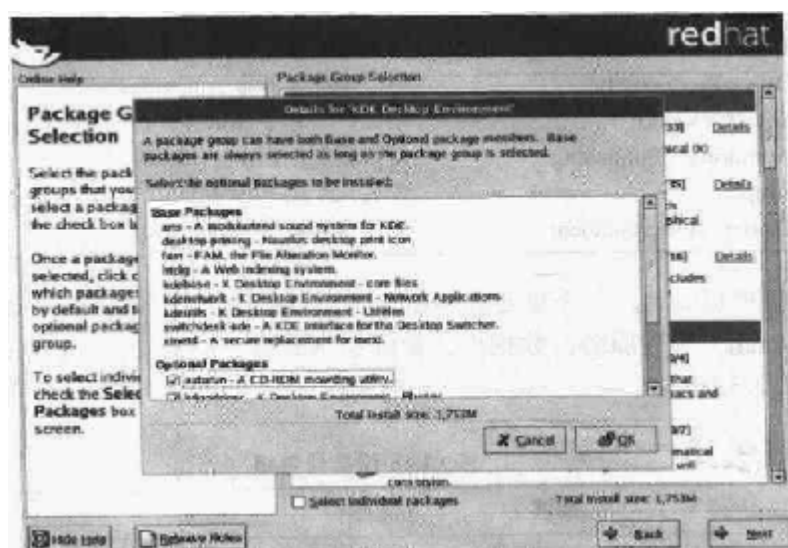


图3.45 KDE桌面环境包组

在Details For 'KDE Desktop Environment'窗口中，包分为两大类：基本与可选。基本包是KDE桌面工作所必需的，而可选包则增加更多特性。

下一类包组是Applications（应用程序），图3.46列出了部分应用程序。应用程序包括基本文本编辑器、互联网连接实用程序、游戏，等等。这个类别的包组见表3.17。

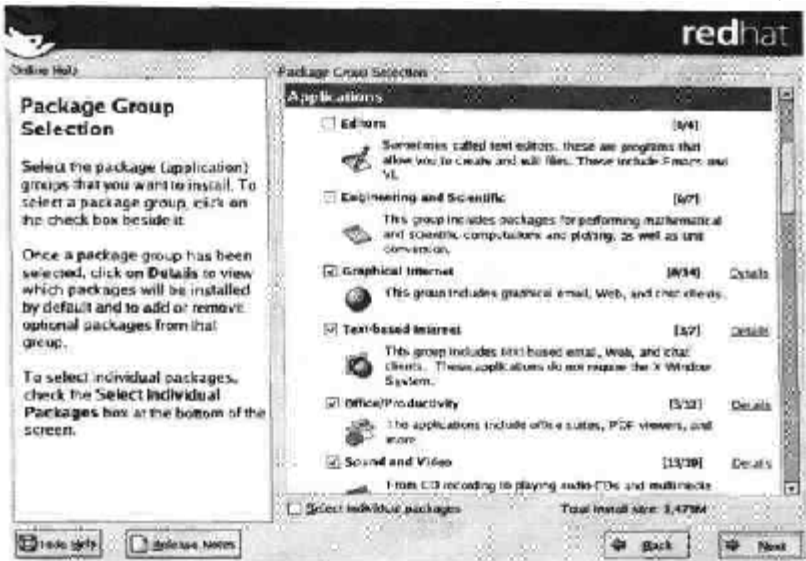


图3.46 应用程序包组

表3.17 应用程序包组

包组	描述
Editors	包括改进vi与Emacs的包
Engineering与Scientific	增加数学计算与图表的程序
Graphical Internet	安装各种图形化网络通信工具
Text-based Internet	安装命令行网络通信工具
Office/Productivity	可以增加各种办公应用程序与组件
Sound与Video	增加一系列多媒体包、浏览器和配置工具
Authoring与Publishing	支持生成DocBook页面的包
Graphics	安装几个图形程序与支持库
Games与Entertainment	增加各种视频和棋类游戏

对Linux管理员而言，一个重要的包组类别是Servers（服务器）。不同服务器可以提供Web站点、E-mail、文件服务、数据库、新闻组等服务。图3.47显示了部分清单。这个类别的每个包组见表3.18。

表3.18 服务器包组

包组	描述
Server Configuration Tools	安装几个红帽子图形化配置工具
Web Server	增加Apache和相关包，向其他计算机上的浏览器提供Web页面
Mail Server	增加各种E-mail服务器与实用程序
Windows File Server	可以让计算机以客户机或服务器形式连接Microsoft Windows网络
DNS Name Server	增加软件，用于建立DNS（域名服务）服务器或相关缓冲名称服务器
FTP Server	增加vsFTP文件服务器，其支持匿名访问

(续表)

包组	描述
SQL Database Server	安装配置PostgreSQL与MySQL服务器数据库的包
News Server	增加InterNet News包, 其支持Usenet式新闻组系统
Network Servers	安装各种网络服务器, 包括DHCP、NIS与Telnet

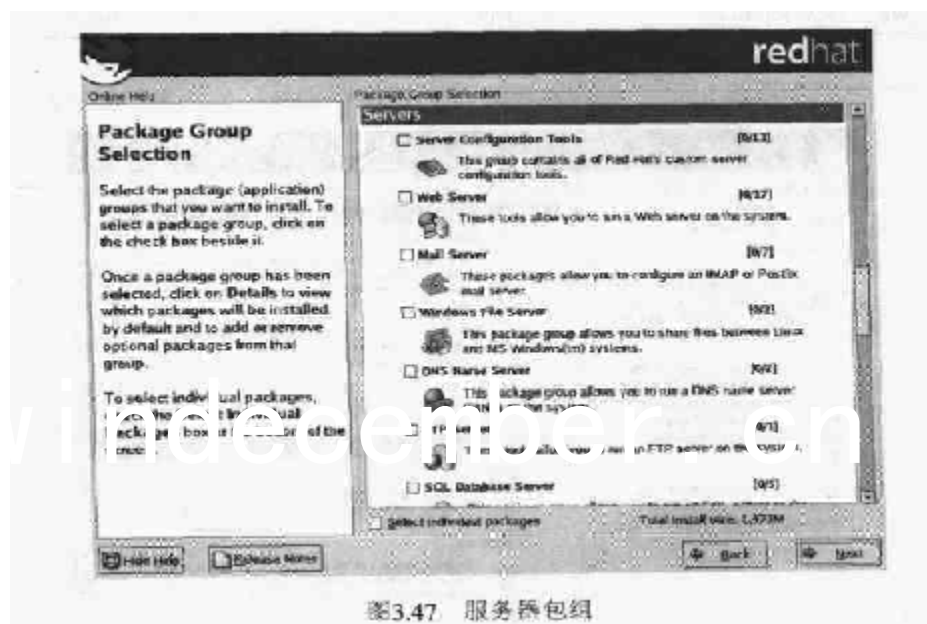


图3.47 服务器包组

有几个Linux开发包组。虽然你可能不是开发人员,但最终也会用到这个组中的许多包。例如,为了编译Linux内核,就需要Kernel Development与Development Tools包组中的包。图3.48显示了开发包组中的包,表3.19介绍开发包组。

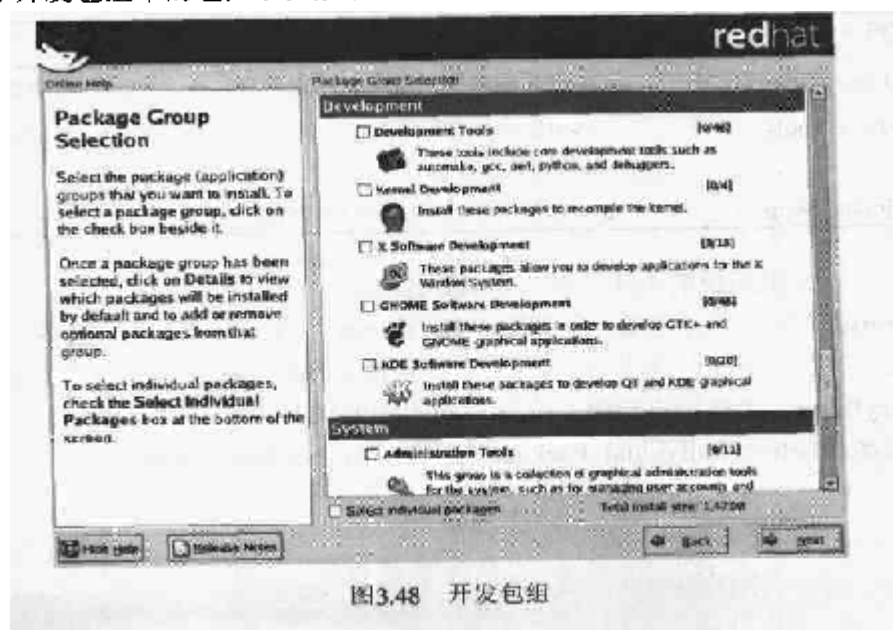


图3.48 开发包组

表3.19 开发包组

包组	描述
Development Tools	安装包工具、语言库，等等
Kernel Development	安装头和内核源代码
X Software Development	增加与Linux XFree86图形系统相关联的开发库、头和文档
GNOME Software Development	增加与GNOME桌面环境相关联的开发库、头和包括文件等
KDE Software Development	增加与KDE桌面环境相关联的开发库、头和包括文件等

最后一类包组是系统包组，包括管理、系统和打印工具，如图3.49与表3.20。

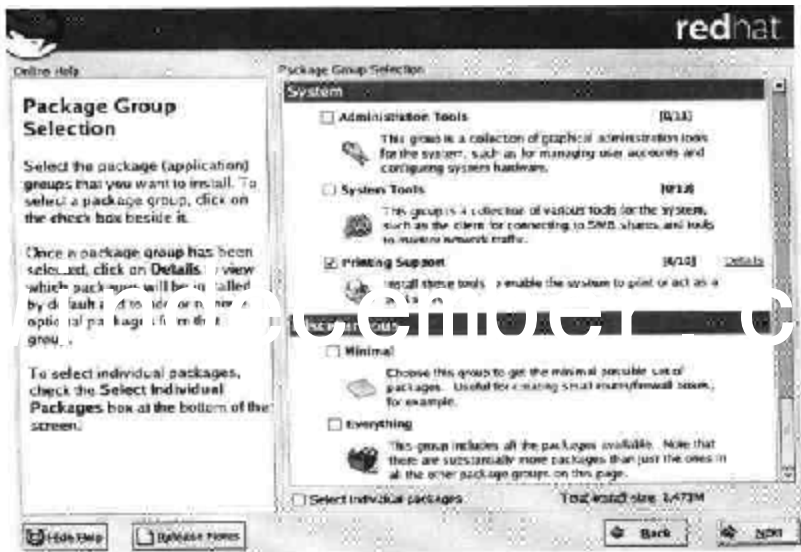


图3.49 系统包组

表3.20 系统包组

包组	描述
Administration Tools	安装图形实用程序，可以管理口令、包、内核参数，等等
System Tools	可以管理各种应用程序，如amanda客户机（用于备份）和gnome-lokkit（用于防火墙）
Printing Support	包括安装CUPS（公用UNIX打印系统）所要的包

最后，在包组选择清单底部有两个其他选项：

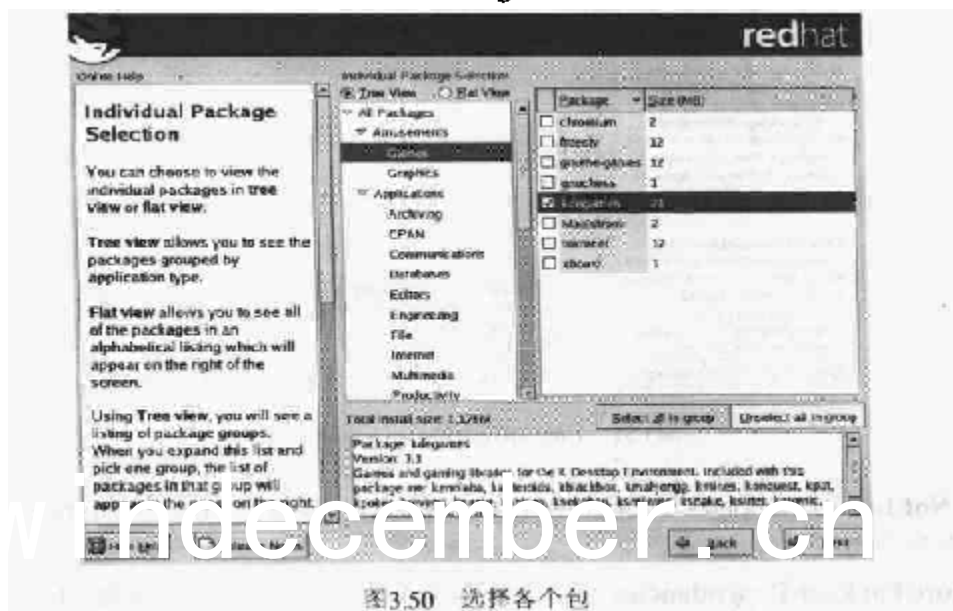
Minimal 取消所有包组。安装Red Hat Linux之后，可以再安装需要的包。这个选项可以提高安全性。一般来说，如果不安装到计算机上，就不会成为安全漏洞。

Everything 选择所有包组，文件空间大约要5GB。

本章激活Select Individual Packages选项，单击Next按钮继续。

选择各个包

还可以用各个RPM进一步定制安装。这个工作并不像想像的那么麻烦：一旦选择包组之后，也就安装了图3.50中所示Individual Package Selection屏幕的相应RPM。



从图中可以看出，**kdegames RPM**包已经准备安装。到本书编写时，这是选择安装KDE桌面环境包组时的默认情况。如果选择游戏与娱乐包组，则也会选择其他游戏包。如果要了解包的细节，则可以将其加亮显示，即可在右下角窗格中看到其描述。

假设公司不允许PC机上放游戏，则要删除kdegames RPM包，将其取消。可以随意浏览其他包类别，完成之后，单击Next按钮继续。

屏幕中可能出现下列消息:

```
checking dependencies in packages selected for installation...
```

依赖性就是一个包的工作离不开另一个包。例如，要使用Mozilla Web浏览器、XFree86 X Window Server和OpenOffice组件之类的Linux应用程序，就要安装Perl编程语言。

如果选择的RPM包具有依赖性，则可以看到图3.51所示的Unresolved Dependencies屏幕。

我们取消kdegames RPM包，这时就可以看到一开始就选择它的原因：如果没有它，kdeaddons RPM就无法工作（kdegames RPM包中有一些语言库，是kdeaddons RPM包所需要的）。此外，kdeaddons RPM包增加了Konqueror（KDE Web浏览器）、noatun（KDE媒体播放器）和Kate（KDE文本编辑器）的功能。

现在要进行选择，是违反公司政策在这台计算机上安装**kdegames RPM**包，还是遵守公司政策，部分丢失上述**KDE**应用程序中的功能？这个选择反映在图3.51所示的三个选项：

Install Packages To Satisfy Dependencies 安装Unresolved Dependencies屏幕中列出的所有包。

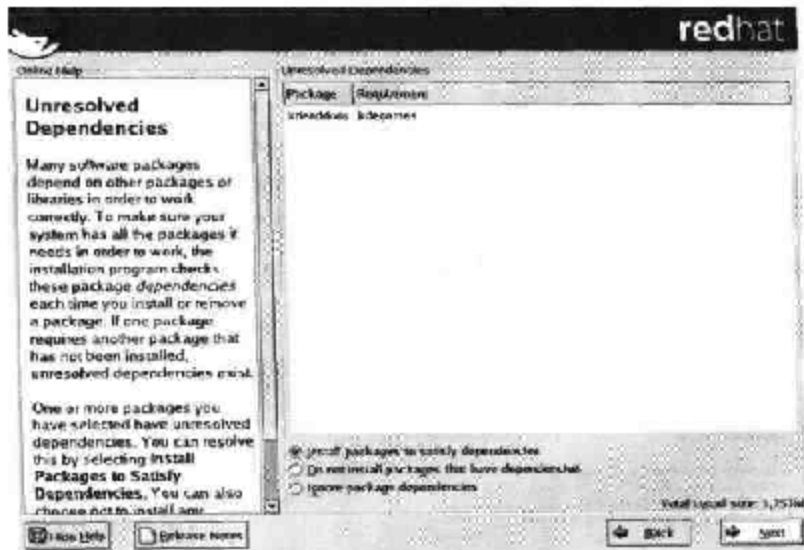


图3.51 Unresolved Dependencies屏幕

Do Not Install Packages That Have Dependencies 不安装Unresolved Dependencies屏幕中列出的所有包。

Ignore Package Dependencies 保留原先的选择，但这时kdeaddons RPM包所安装的软件可能无法工作。

这里的选择取决于公司政策和需要的软件。是满足功能，还是满足公司政策？进行选择，然后单击Next按钮继续。

准备安装

最后，终于可以让Anaconda在计算机上安装Linux了。Anaconda中包括我们定义的分区、我们选择的包组和其他设置。如图3.52所示，单击Next按钮继续。Anaconda即开始按你的选择安装Red Hat Linux 9。

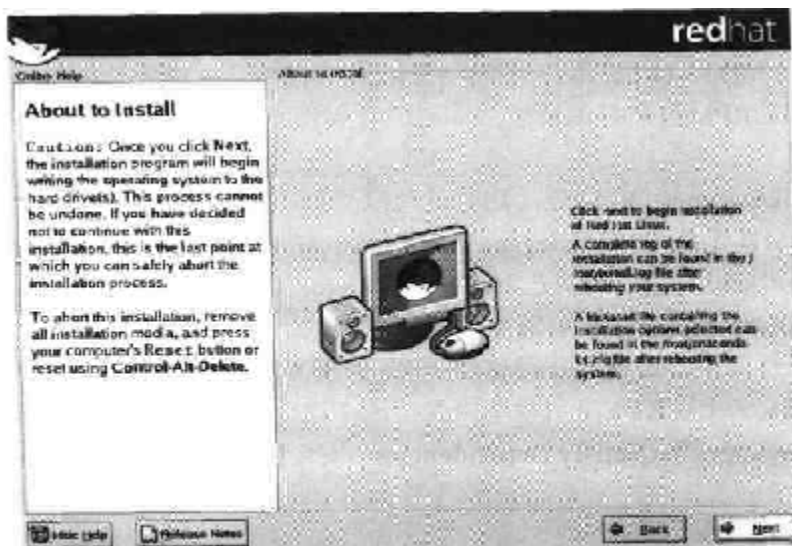


图3.52 准备安装

记住所列的组件。安装完成之后，可以在`/root/install.log`中检查安装的RPM。`/root/anaconda-ks.cfg`文件可以帮你用第5章介绍的Kickstart系统在其他计算机上重复这个安装。

准备好后，单击Next按钮继续。

Anaconda安装Linux

最后，Anaconda开始安装过程。首先，可以看到一系列消息：

```
Formatting / file system . . .
Formatting /boot file system . . .
Transferring install image to hard drive
Setting up RPM transaction
Starting install process, this may take several minutes
Preparing to install . . .
```

这时Anaconda用所选文件系统目录将分区格式化，然后将基本安装模板作为映像传递到硬盘上。它设置要安装的RPM表，然后开始从安装源（这里是Red Hat Linux安装光碟）向硬盘传输数据。然后可以看到图3.53所示的屏幕，不断更新安装进程。

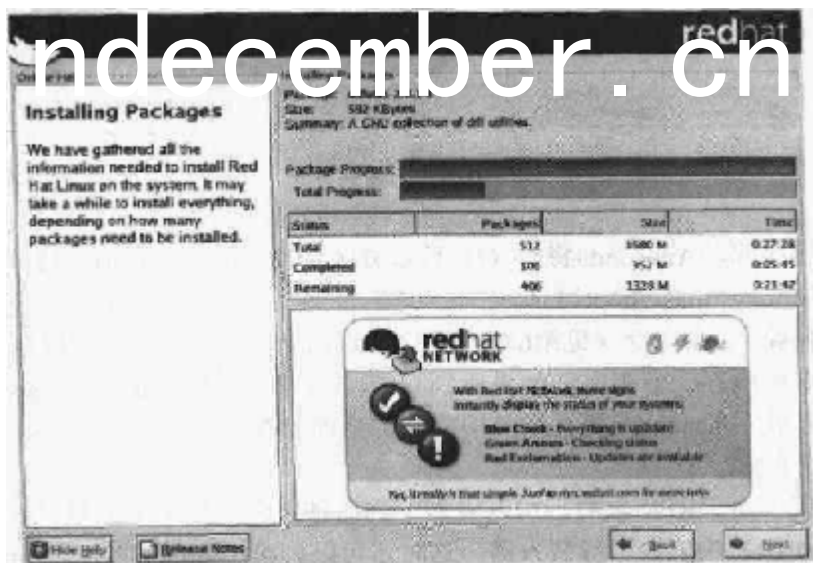


图3.53 安装进程

Red Hat Linux安装光碟有三张（请阅读本章开头和本书前言中关于出版版的两张光碟的说明）。随着安装的进行，Anaconda可能要访问第二或第三张Red Hat Linux安装光碟。安装停止时，出现图3.54所示的消息，按照指令做，然后单击OK按钮继续。

这时可以检查安装过程对系统进行了哪些改变。到第二个虚拟控制台，按Ctrl+Alt+F2键组，在命令提示下检查磁盘使用情况：

```
-/bin/sh-2.05b# df
Filesystem 1k-blocks    Used Available Use% Mounted on
rootfs           6120      3594      2176  63% /
```

```

/dev/root.old 6120 3594 2176 63% /
/tmp/cdrom 653312 653312 0 100% /mnt/source
/tmp/hda3 5037736 1648884 3132948 35% /mnt/sysimage
/tmp/hda2 102486 8608 88586 9% /mnt/sysimage/boot

```

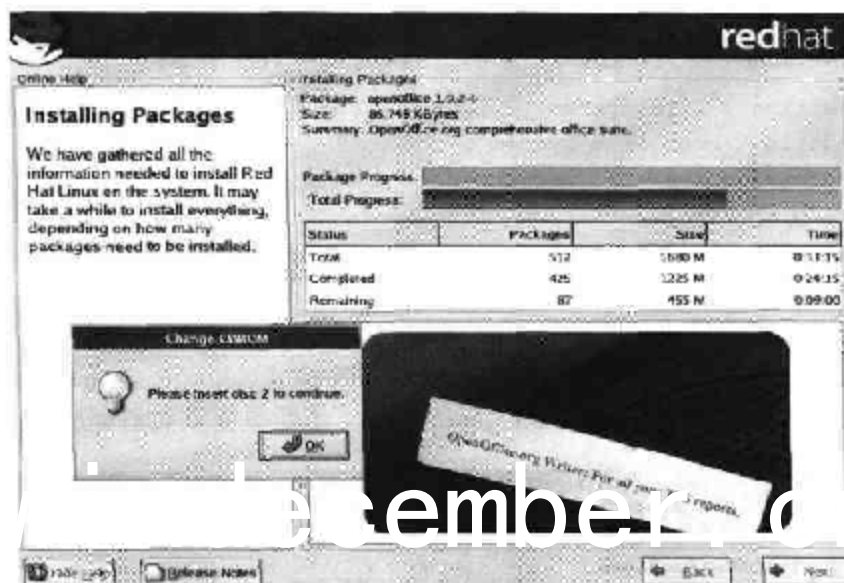


图3.54 安装停止

这个输出表明，Anaconda将根（/）目录分区装载到/mnt/sysimage目录，并将引导目录分区装载到/mnt/sysimage/boot目录。

可以用bash shell命令（见第6章、第7章和第8章介绍）导航这些目录，看看Anaconda已经安装了哪些内容。事实上，如果遇到问题，则可以检查/mnt/sysimage/root/install.log内容。这个日志表示Anaconda要在系统中安装的当前RPM。如果安装冻结，则可能是光碟上的特定RPM有问题。

安装所要的全部RPM之后，可以看到下列消息，表示Anaconda可以进入下一步，在主引导记录（MBR）中安装引导装入器。这时还可以到第二个虚拟控制台/mnt/sysimage/etc目录中寻找引导装入器配置文件。安装完成之后，可以到所要地址/etc目录中寻找文件。如果使用GRUB，则其在grub.conf文件中。

```

Performing post install configuration
Installing bootloader

```

进行安装后配置

Anaconda已经在计算机上安装了Red Hat Linux，但我们的工作还没有完成，还要对系统生成引导盘和配置图形。下一个屏幕如图3.55。

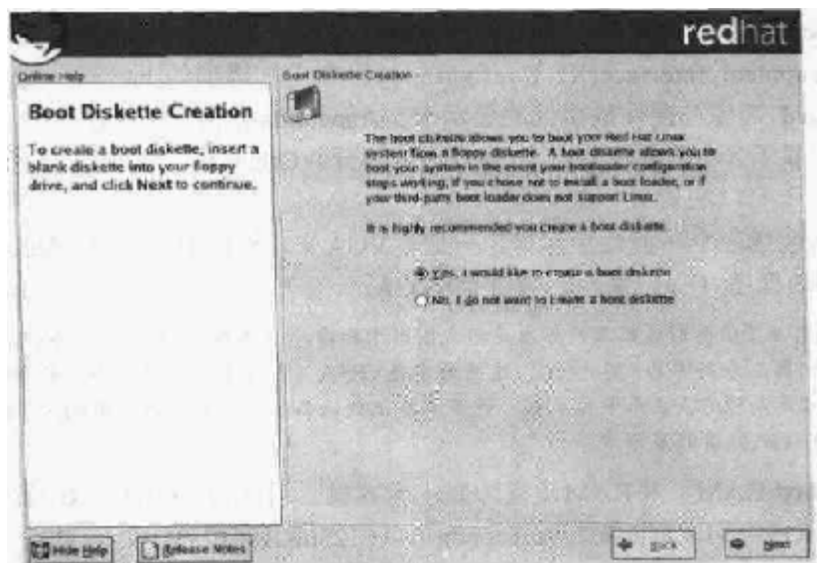


图3.55 生成引导盘

生成引导

最好要生成引导盘，这是对系统定制的最佳救援盘。

如果有软盘驱动器，则可以在Boot Disk Creation屏幕中选择Yes，然后单击Next按钮继续。程序提示插入软盘，并警告软盘上的所有数据均会被删除。按照指令做，单击Make Boot Disk，从而运行mkbootdisk命令，见第11章介绍。

配置显示卡

如果安装了X窗口软件，则Anaconda会提示配置图形系统，如图3.56。可以跳过这个过程，后面再用第15章介绍的redhat-config-xfree86实用程序配置。

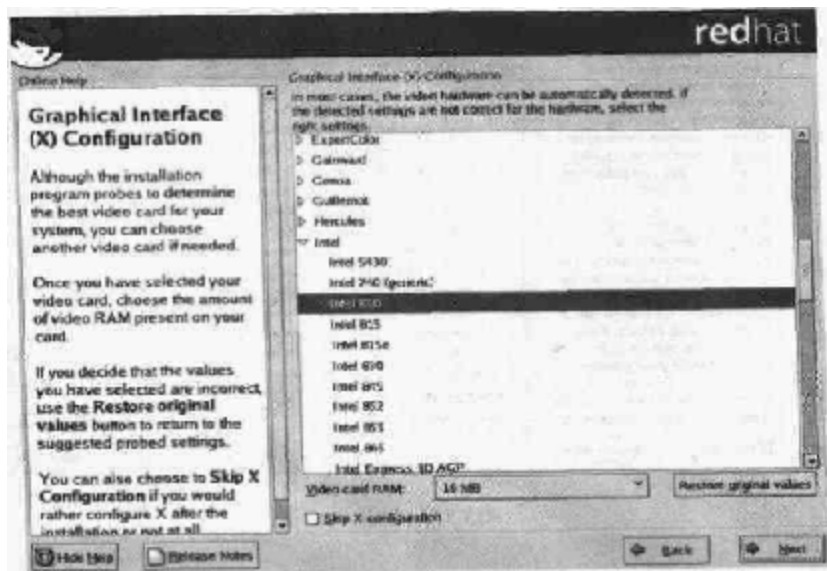


图3.56 配置图形系统

如果Anaconda在这个过程开始时探测到硬件,则会加亮显示探测到的图形卡,以及卡的内存量。**Graphical Interface(X) Configuration**屏幕中的选项如下:

Video Card 选择与硬件最接近的显示卡。Anaconda可能会选择显示卡。卡按厂家进行组织。如果看不到你的显示卡,则可能在表开头**Other**下面的制造商名单中。另外大多数新显示卡可以配置成一般性显示卡。

这个部分包括三个一般性显示卡:一般性VGA兼容显示卡、非支持VGA兼容显示卡和VESA驱动程序(一般性),等价于SVGA。

说明: VGA(显示图形适配器)标准是旧式图形卡标准,分辨率为640×480。SVGA指超级显示图形适配器,分辨率为800×600。这些标准是VESA(显示电子标准协会)维护的,标准VESA驱动程序与SVGA显示卡相关联。许多不能识别的高性能卡都可以使用VESA方式,如符合XGA与SXGA标准的显示卡。

Video Card RAM 将RAM设置为显示卡容量。如果显示卡共享普通内存,则一定要使其与BIOS中的设置匹配。Anaconda可以用256KB到128MB的增量设置显示卡内存。

Restore Original Values 如果进行了多处改变之后要恢复原先探测到的配置,则要单击这个按钮。

Skip X Configuration 如果这时不想配置图形系统,则可以启用这个选项并单击Next按钮继续。后面还可以用 `xconfig -xirc 316` 配置图形系统。

大多数情况下,不需要进行任何改变。进行所要改变,然后单击Next按钮继续。

配置显示器

还要在计算机上配置X窗口系统时,下一个任务是使用图3.57所示的**Monitor Configuration**屏幕。

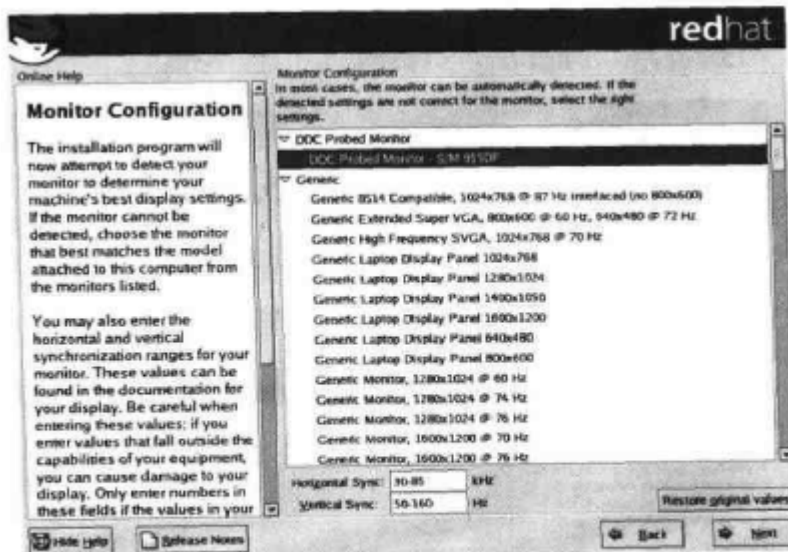


图3.57 配置显示器

Anaconda探测系统时，可能已经探测到显示器，这样就会在DDC Probed Monitor部分加亮显示。如果这是个错误的显示器，则可以从表中选择显示器，其按厂家和机型进行分类。如果表中看不到你的显示器，则可以选择各种一般性显示器。

每个显示器都有水平同步率与垂直同步率。认真检查显示器文档。如果这里设置的值超过显示器能力，则显示卡发出的信号可能把显示器电路烧掉。

如果试验之后要返回Anaconda探测的值，则可以单击Restore Original Values。大多数情况下，不需要进行任何改变。进行所要改变，然后单击Next按钮继续。

定制图形

已经到达最后一步了。现在要把显示卡与显示器的配置设置集成起来。图3.58显示了定制图形配置屏幕。

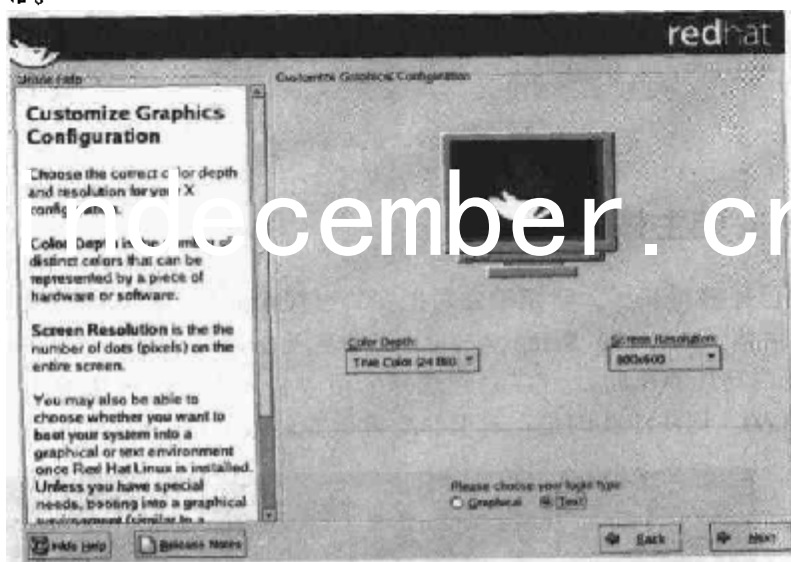


图3.58 定制图形配置屏幕

这个屏幕中的选项包括：

Color Depth 指定每个像素相关联的颜色位数。例如，24位是真彩色，支持 $2^{24}=16\,777\,216$ 种不同颜色。根据显示卡与显示器的功能，可以对每个像素设置8位（256种颜色）或16位（65 536种颜色）。

Screen Resolution 设置显示器中显示的像素个数。屏幕分辨率按“水平×垂直”格式设置。例如，800×600分辨率表示水平方向为800像素，垂直方向为600像素。可用分辨率取决于显示器尺寸和显示卡内存。

Please Choose Your Login Type 配置Linux引导序列，影响/etc/inittab中的id变量，可以按第11章介绍的方法改变。如果选择Graphical，则Linux引导到图形登录屏幕；如果选择Text，则Linux引导到基于文本的虚拟控制台。这些选项在选择Personal Desktop与Workstation installation安装类型时不提供，它们都默认为图形登录屏幕。

进行选择，然后单击Next按钮继续。安装完成后，如图3.59。单击Exit重新启动计算机。

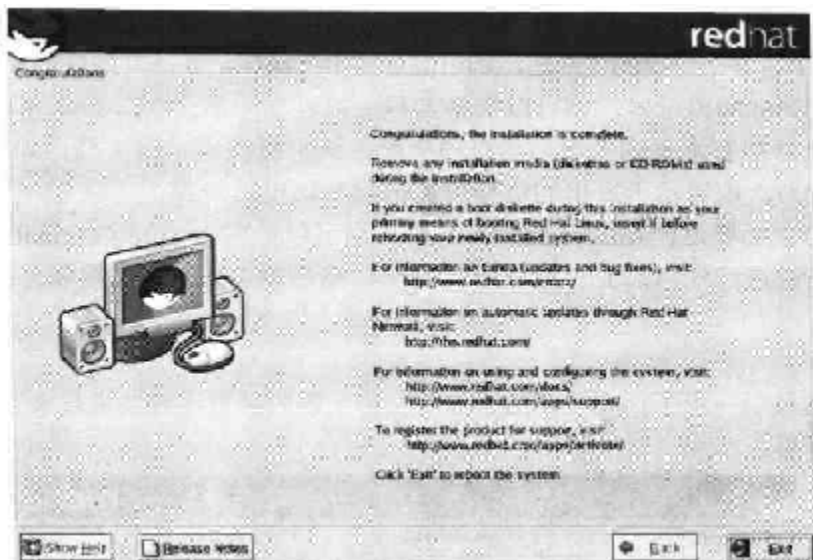


图3.59 安装完成

运行红帽安装主体

安装过程已经够漫长了。红帽子公司把安装过程中的几个配置活动移到新程序中，称为红帽子安装主体（Red Hat Setup Agent），也称为firstboot。

首次重新启动计算机时，可以看到选择的引导装入器。默认情况下，引导装入器为GRUB，如图3.60。记住，我们是在双引导配置中安装Red Hat Linux。



图3.60 GRUB引导装入器

安装过程的最后曾介绍过，有两种登录方式：文本方式和图形方式。典型的文本方式登录如下：

Red Hat Linux release 9 (Shrike)

Kernel 2.4.20-8 on an i686

RH9Test login:

但是，如果安装过程最后选择图形方式登录，则会进入图3.61所示的红帽子安装主体。登录图形屏幕之前，Red Hat Linux引导过程不允许进行任何工作。



图3.61 红帽子安装主体

红帽子安装主体可以配置用户账号、建立与时间服务器的连接、探测声音卡、注册红帽子公司网络 and 增加其他软件。

如果选择文本方式登录，则可以用firstboot命令启动红帽子安装主体。

说明：如果选择文本方式登录，则运行级为3，运行telinit 5命令并登录Linux GUI，然后可以在GUI命令行界面中运行firstboot命令。

单击Forward按钮继续。

生成普通用户

可以生成个人用户账号，如图3.62。在Username文本框中输入登录名。然后在Full Name文本框中输入标识信息。在最后两个文本框中输入相同的口令，然后单击Forward按钮继续（Vaclav Havel是刚刚离任的捷克共和国总统）。

增加所选用户，然后单击Forward按钮继续。

指定日期与时间

是的，Red Hat Linux安装过程中已经指定日期与时间。这里的差别在于，这个firstboot屏幕可以让计算机与中央时间服务器同步。请选择Enable Network Time Protocol选项，如图3.63。



图3.62 生成个人用户账号



图3.63 指定时间服务器

如果计算机连接互联网，则可能要从Delaware大学NTP上的授权Web站点www.eecis.udel.edu/~ntp选择NTP服务器，其中有个链接，列出全世界的活动NTP服务器名单。后面可以用第19章介绍的redhat-config-time实用程序改变设置。注意，我的计算机指向北卡罗莱纳大学的时间服务器。

为了保证下次启动Linux时NTP监控程序还能继续工作，红帽子安装主体在第3级和第5级运行级中激活NTP监控程序，并通过生成的任何防火墙提供一个路径。关于运行级的更多信息，见第11章。关于防火墙的更多信息，见第22章。

指定时间服务器，然后单击Forward按钮继续。如果计算机连接互联网，则firstboot会与选择的时间服务器联系。

声音卡

红帽子安装主体自动探测计算机上安装的任何声音卡。如果成功，则可以看到声音卡的厂家、机型和模块，如图3.64所示。如果声卡连接扬声器，则可以单击Play Test Sound按钮。

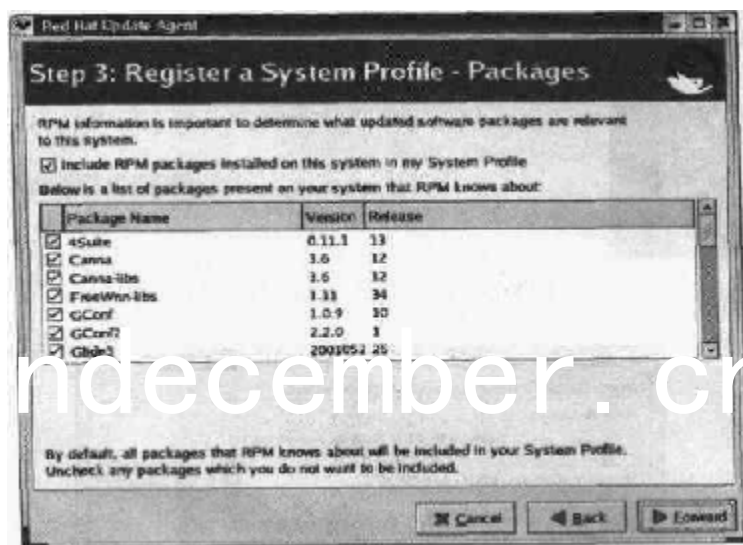


图3.64 红帽子安装主体自动探测声音卡

firstboot播放声音之后，出现一个提示，询问“是否听到了样本声音”。如果没有听到，单击No，则会出现一个消息，表示声音卡没有激活；否则单击Yes返回红帽子安装主体，然后单击Forward按钮继续。

注册红帽子公司网络

计算机注册红帽子公司网络时，可以将计算机设置成接收最新软件升级与补丁包。红帽子安装主体描述图3.65所示的选项。

到本书编写时，有六级服务：Demo、Basic、Enterprise、Enterprise Linux AS Developer、Enterprise Linux WS Basic和Enterprise Linux ES Basic。演示级是免费的，但要求经常注册和更新。要注册基础服务级，就要购买Red Hat Linux 9软件包或预订红帽子网络rhnl.redhat.com。企业服务级的要求也差不多。红帽子公司还为教育机构提供基于网络的支持，详见红帽子网络Web站点。

我们注册演示账号，选择“Yes, I Want To Register My System With Red Hat Network”并单击Forward按钮继续，打开Red Hat Network Configuration窗口，如图3.66所示，可以看到，这个窗口有三个标签。



图3.65 向红帽子网络注册计算机

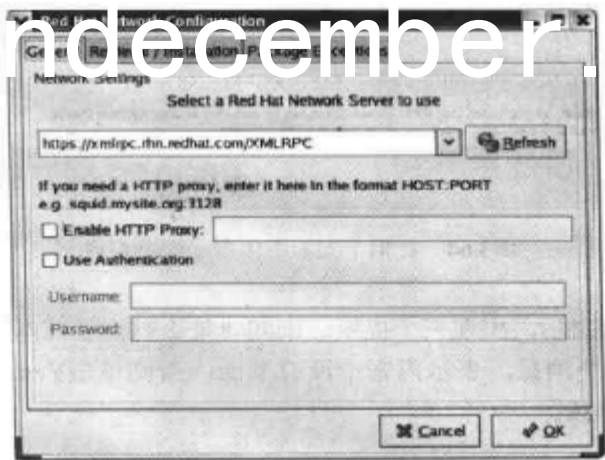


图3.66 Red Hat Network Configuration窗口

在General标签中，输入与服务级相应的红帽子网络服务器。也许文本框中已经提供一个服务器。如果建立演示账号，则可以用显示的默认服务器。如果计算机通过代理服务器连接互联网，则要输入必要的连接信息。现在单击Retrieval/Installation标签，如图3.67所示，表3.21列出了其中的选项。

表3.21 红帽子网络Retrieval/Installation标签选项

选项	描述
Do Not Install Packages After Retrieval	从数据库中将新包下载到指定的包存储目录，不安装这些包
Do Not Upgrade Packages When Local Configuration File Has Been Modified	不升级已经配置的服务包，可以在控制方式中测试升级的包

(续表)

选项	描述
Retrieve Source RPM Along With The Binary Package	下载源代码和每个包
Use GPG To Verify Package Integrity	用GNU隐私卫士检查每个下载的包（见第22章）
After Installation, Keep Binary Packages On Disk	安装之后保留RPM包
Enable RPM Rollbacks	可以返回升级前的配置
Override Version Stored In System Profile	忽略与旧版Red Hat Linux相关联的红帽子网络配置，其可能在这台计算机上有文件
Package Storage Directory	指定RPM的目录

现在单击Package Exceptions标签，如图3.68。这里可以指定不通过红帽子网络升级的包和文件名，至少要你批准之后才能升级。注意，这个表中列出了升级的kernel* RPM包。

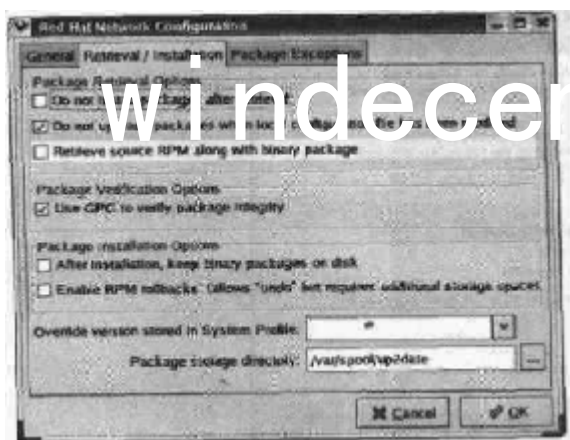


图3.67 指定要更新的包

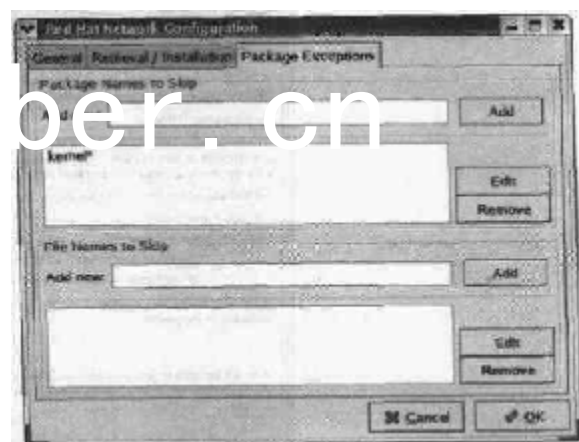


图3.68 不升级的包和文件名

完成红帽子网络配置改变之后，单击OK按钮，打开红帽子更新主体，见第10章介绍。单击Forward按钮继续。首次运行红帽子更新主体时，可以看到第1步是红帽子隐私声明。阅读红帽子隐私声明，然后单击Forward按钮继续，进入第2步登录屏幕，如图3.69。

输入登录信息并单击Forward按钮继续。可以通过这个屏幕设置新登录，或登录现有红帽子网络账号，从而进入第3步，注册计算机。图3.70显示了我向红帽子网络提交的系统配置。必要时改变配置，然后单击Forward按钮继续。

这时，红帽子注册向导收集RPM清单，并将其放在系统配置文件中，如图3.71。可以取消不想告诉红帽子的任何软件包。准备好后，单击Forward按钮继续。

如果愿意将系统配置文件发送给红帽子公司，则在下一个屏幕中单击Forward按钮继续。如果已经成功地向红帽子网络注册，则这个过程按第10章介绍up2date实用程序时那样继续。

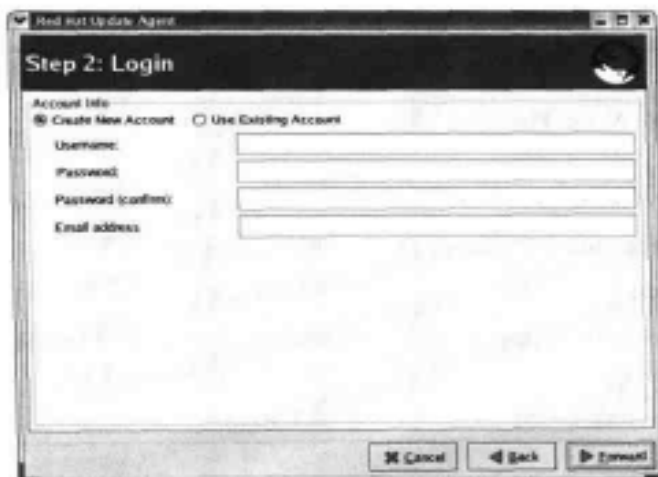


图3.69 红帽子更新主体登录屏幕

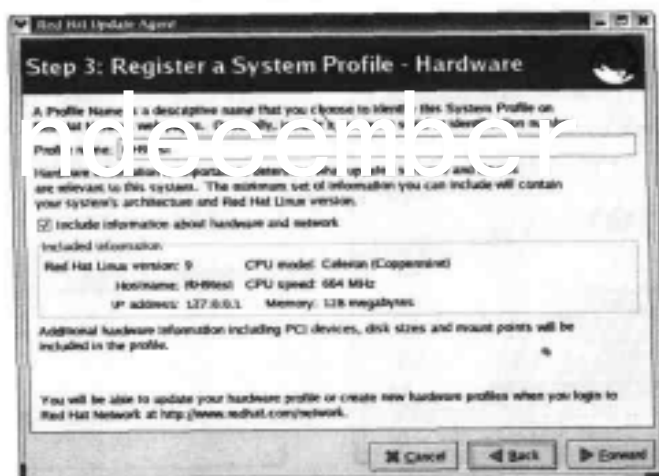


图3.70 注册计算机

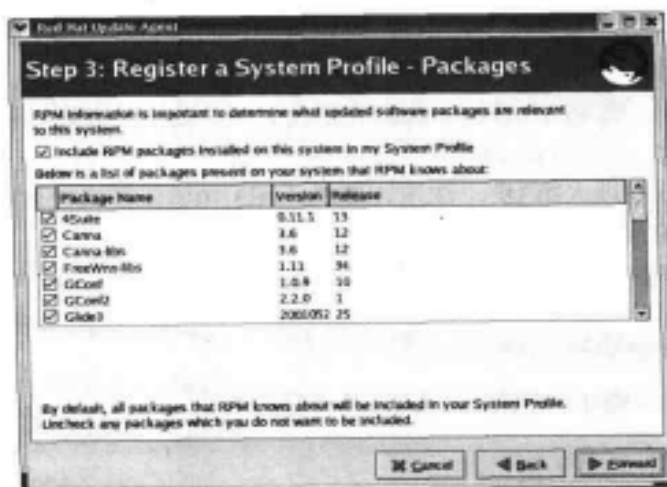


图3.71 系统配置文件中的RPM

其他安装

如果还要在Red Hat Linux中安装其他软件包，则可以在这时进行。如图3.72所示，可以从Red Hat Linux文档光碟、Red Hat Linux安装光碟或其他光碟安装其他包。

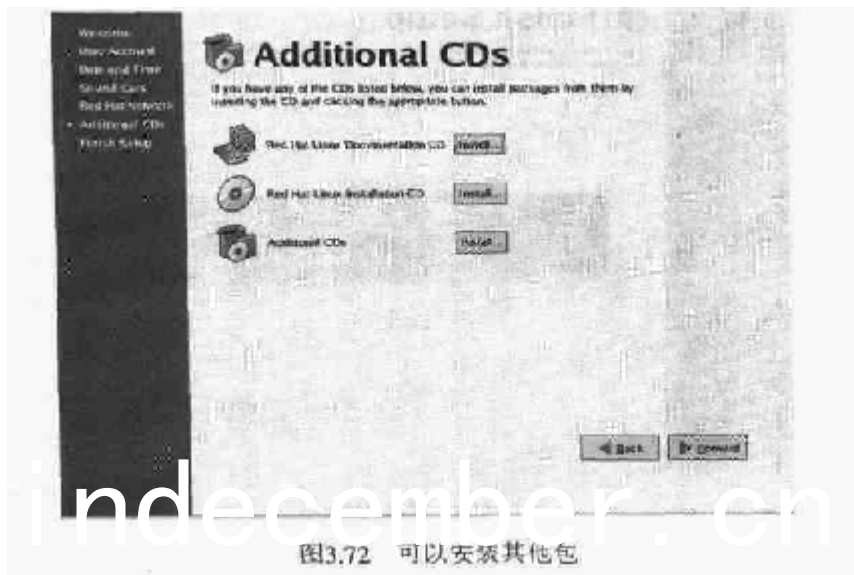


图3.72 可以安装其他包

插入相应光碟，单击Install，然后按提示做。本节用与redhat-config-packages实用程序相关联的软件组织新软件的安装。图3.73显示了安装Red Hat Linux文档光碟的结果。选择要安装的文档，然后单击Forward按钮继续。按照提示做，firstboot自动从光碟中安装所要的文档。

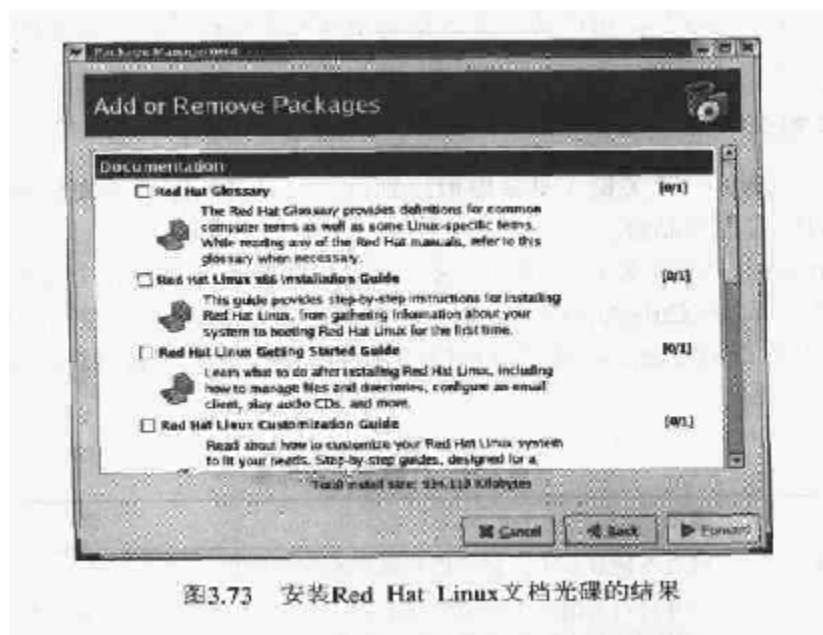


图3.73 安装Red Hat Linux文档光碟的结果

如果要从安装光碟中增加更多RPM，则要插入第一张Red Hat Linux安装光碟，并单击Install，从而启动第19章介绍的redhat-config-packages实用程序。单击Forward按钮继续。这时可以看到图3.74所示的Finish Setup屏幕，可以看到，系统已经准备设置和使用了。



图3.74 安装完成

安装查错

查错的标准方法就是收集所有可以得到的数据。Red Hat Linux是个著名的操作系统。人们随时在网上交换相关问题的信息。一旦收集到数据之后，就可以标识问题的征兆，通过本地用户组或网络与Linux社区联系。

要访问大量查错数据，可以访问安装期间出现的虚拟控制台。收集的数据可能反映某个主要问题，见下节介绍。

安装虚拟控制台

查错安装问题的一个关键工具是虚拟控制台。一旦开始图形化安装过程之后，就可以访问五种不同的虚拟控制台。

如果Red Hat Linux安装遇到问题，这个问题也许并不明显。几个文本安装屏幕可能提供了重要消息。可以按Ctrl+Alt+Fn命令取得这些消息，其中n是虚拟控制台号码：1、2、3、4、5或7。一旦检查消息之后，就可以按Ctrl+Alt+F7命令返回安装屏幕。表3.22描述了安装屏幕。

表3.22 红帽子安装屏幕

屏幕	描述
Ctrl+Alt+F1	检查本地显示卡、显示器和鼠标的探测消息
Ctrl+Alt+F2	打开具有有限命令功能的bash shell，例如，df命令可以显示装载目录和分区，其他bash命令见本书第6章、第7章和第8章介绍

(续表)

屏幕	描述
Ctrl+Alt+F3	浏览安装日志，包括与硬件探测相关联的消息，这里还有读光碟和装入驱动程序时的问题。安装过程中，这个信息记录到/tmp/anaconda.log文件中
Ctrl+Alt+F4	转入系统消息日志，包括格式化与装载分区目录之类的消息。安装过程中，这个信息记录到/tmp/syslog文件中
Ctrl+Alt+F5	显示其他消息，如文件系统标题、块、格式和杂志。只能在Anaconda格式化分区之后访问
Ctrl+Alt+F7	返回图形安装屏幕

说明：安装过程中改变屏幕时，有些键盘要求用键盘左边的Ctrl与Alt键。

安装虚拟控制台和/tmp/syslog目录中的日志文件存放在RAM盘中，因此重新启动计算机时或完成安装过程后会删除。

图形探测消息

本章前面介绍了成功安装时第一个控制台的消息。但有可能遇到问题，特别是具有不相符的图形硬件时。首先看看我的笔记本中出现的消息：

```
You do not have enough RAM to use the graphical installer. Starting text mode.
```

这个消息很简单，如果看到这个消息，则要在计算机上增加更多内存，之后才能进行图形化安装。好在文本方式安装（见第4章介绍）能够满足大部分要求。有时图形硬件不符合要求，则会出现下列消息：

```
Running anaconda, the Red Hat Linux system installer - please wait...
Probing for video card: Unsupported VGA Compatible
Probing for monitor type: Unknown monitor
Probing for mouse type: Generic - Wheel Mouse (PS/2)
Attempting to start native X Server
Waiting for X server to start...log located in /tmp/X.log
1...2...3...4...5...X SERVER FAILEDAttempting to start VESA driver X server X
➡ startup failed, falling back to text mode
```

这些消息也很简单，表示这个计算机不包括符合VESA（SVGA）标准的图形硬件。

日志文件

安装过程中很容易访问日志文件，只要利用第二个虚拟控制台。按Ctrl+Alt+F2键组打开bash提示：

```
~/bin/sh-2.05b#
```

这里可以输入所选的bash命令。通过这个界面，可以访问前面安装的任何文件。前面曾看到/tmp/X.log文件的消息，用vi /tmp/X.log命令将其打开，则可以看到图3.75所示的文件。

```

XFree86 Version 4.3.0 (Red Hat Linux release: 4.3.0-2)
Release Date: 27 February 2003
X Protocol Version 11, Revision 0, Release 6.6
Build Operating System: Linux 2.4.20-3bigmem 1686 [ELF]
Build Date: 27 February 2003
Build Host: porky.devel.redhat.com

Before reporting problems, check http://www.XFree86.org/
to make sure that you have the latest version.

Module loader present
OS Kernel: Linux version 2.4.20-3800T (bhcompil@porky.devel.redhat.com) (gcc ve
rsion 3.2.2 20030222 (Red Hat Linux 3.2.2-5)) #1 Thu Mar 13 17:31:36 EST 2003
Markers: (--) probed, (**) from config file, (==) default setting,
(++) from command line, (!!) notice, (II) informational,
(WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(++) Log file: "/tmp/ramfs/X.log", Time: Wed Mar 26 11:54:54 2003
(++) Using config file: "/tmp/XF86Config.test"
(EE) Failed to load module "glx" (module does not exist, 0)
(EE) Failed to load module "record" (module does not exist, 0)
error opening security policy file /etc/X11/Xserver/SecurityPolicy
Could not init font path element unix/:7100, removing from list!
cat: //Xauthority: No such file or directory

```

图3.75 X配置日志

注意文件底部的说明语句，指向/tmp/ramfs/X.log文件，其中提供该计算机上图形问题的其他信息。/tmp目录中还提供了其他重要的日志文件，见表3.23。

表 3.23 安装过程中的日志文件

日志文件	描述
anaconda.log	与第三个虚拟控制台相关联的硬件探测日志
isoinfo	当前光碟的MD5校验和
modules.conf	已安装的模块清单
syslog	引导日志，对应于dmesg（见第11章）
X.log	图形配置日志文件
XF86Config.text	基本X窗口配置文件

硬件探测消息

第三个虚拟控制台中提供几个硬件探测消息。安装过程中，可以用Ctrl+Alt+F3命令取得这个虚拟控制台，也可以在第二个虚拟控制台中看到/tmp/anaconda.log中的整个消息清单。记住，随着安装的继续，Anaconda会不断地在这个文件中增加信息。

如果遇到硬件问题，则通常很明显，例如，下列消息表示Anaconda读取一个光驱时遇到问题：

```
<4>hdb: cdrom_decode_status: error=0x51{DriveReady SeekComplete Error}
```

尽管这个消息可能表示光碟媒体问题或硬件问题，但通常能够表示问题所在。

有些硬件消息比较微妙：

```

/tmp/yenta_socket.o: init_module
Hint: insmod errors can be caused by incorrect module parameters, including
      > invalid IO or IRQ parameters.
You may find more information in syslog or the output from dmesg.

```

我知道，yenta_socket.o模块与我的PCMCIA硬件有关，但还要进一步研究，才能发现我的引导盘中缺少i82365 PCMCIA模块。就像一条不会叫的狗，我发现Anaconda根本没有装

入关键PCMCIA模块时，才知道问题所在。如果我不熟悉自己便携电脑中的硬件，则根本猜不出这个问题。

系统消息日志

标准Linux安装消息日志中有相当标准的引导消息，这里通常不会遇到问题。例如，任何没有探测到的硬件都不会在系统消息日志中出现。

这样，要通过这个消息日志找问题，就要有一定判断能力。例如，如果安装了512MB内存，而消息说，只探测到128MB内存，则说明有问题。

这个日志与第四个安装虚拟控制台相关联，可以用Ctrl+Alt+F4命令访问。也可以在第二个虚拟控制台中看到/tmp/syslog中的消息。记住，随着安装的继续，Anaconda会不断地在这个文件中增加信息。

其他消息

Anaconda在实际开始Red Hat Linux安装之前，将分区格式化。如果分区没有配置足够的空间，则会出现错误消息，要再次开始这个过程。前面的表3.6列出了与每个安装选项相关联的标准文件长度要求。

Red Hat Linux在计算机上开始安装软件包时，可以用Ctrl+Alt+F5命令检查这个虚拟控制台。图3.76所示的视图包括Anaconda如何格式化根（/）目录文件系统的消息。

```
This filesystem will be automatically checked every 20 mounts or
100 days, whichever comes first. Use tune2fs -c or -l to override.
tune2fs 1.32 (09-Nov-2002)
Setting maximal mount count to -1
Setting interval between check 8 seconds
tune2fs 1.32 (09-Nov-2002)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
26184 inodes, 104391 blocks
5219 blocks (5.00%) reserved for the super user
First data block=1
13 block groups
8192 blocks per group, 8192 fragments per group
2000 inodes per group
Superblock backups stored on blocks:
    8193, 24577, 40961, 57345, 73729

Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 27 mounts or
100 days, whichever comes first. Use tune2fs -c or -l to override.
tune2fs 1.32 (09-Nov-2002)
Setting maximal mount count to -1
Setting interval between check 8 seconds
■
```

图3.76 Anaconda格式化消息

在这个过程的后面，Anaconda显示一个GRUB提示，可以修改引导装入器配置。但是，GRUB配置文件grub.conf可以通过第二个虚拟控制台配置，见前面的介绍。

包状态

Linux安装时，一个常见的问题是RPM包没有正确复制。

安装过程中可能涉及到许多包，这可能是第一千个包。如果Anaconda突然发现这个包有问题，则安装停止。除非手头有替换媒体（如复制光碟），否则就没有办法了，只能重新

开始安装。

安装进行之后，可以在屏幕上跟踪安装状态。图形和文本方式安装都会标识当前所安装的包。还有一个解救的办法，一旦安装开始后，可以通过第二个虚拟控制台找到当前清单，在/mnt/sysimage/root目录的install.log文件中。

如果能标识有问题的包，则可以替换这个包。可以在光碟上的包清单中替换，也可以再次将包下载到中央网络安装源。

特别是，如果通过Internet下载Red Hat Linux安装光碟，则可能有许多原因会造成问题。可能是Internet上某个地方临时电源不稳定，也可能是下载的硬盘具有坏扇区，也可能是光碟文件复制到有缺陷的磁盘中，等等。从下载的光碟安装Red Hat Linux通常没有麻烦（我经常这么做），但也有它的风险。

登录

现在你和计算机都准备好使用Linux了。如果你是Linux专家（或想成为Linux专家），则可以从命令行界面登录如下：

```
Red Hat Linux release 9 (Shrike)
Kernel : 2.4.20-8 on i686
RH9Test login: username
Password:
Last login: Wed Mar 19 15:33:00 on tty1
[username@RH9Test username]#
```

这样就进入了命令行界面，这是本书的重点界面。

如果你不熟悉Linux，则可以在图形化登录提示下登录，如图3.77所示。



图3.77 图形登录屏幕

许多Linux管理员充分利用图形用户界面。默认的Red Hat Linux GUI是GNOME（GNU网络对象模型环境）。GNOME中很容易启动命令行界面。右单击桌面上任何空白的区域，

并从弹出菜单中选择New Terminal, 从而打开默认GNOME终端命令行界面, 如图3.78所示。

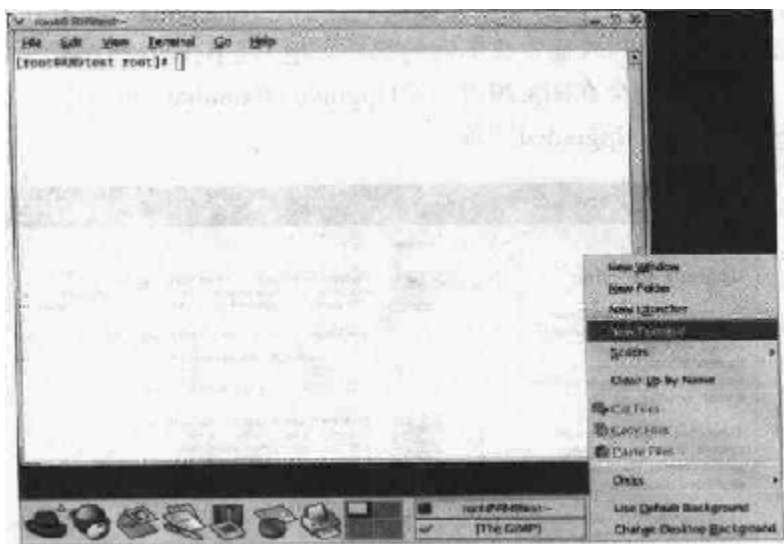


图3.78 GNOME命令行终端

现在就可以开始学习Linux了。

升级Red Hat Linux

如果过去在本地硬盘上装过Red Hat Linux, 则可能只需要升级。一个好的升级可以保存当前地址的配置与数据文件。尽管升级任何操作系统之前一定要先备份数据, 但不必花时间从备份恢复会方便得多。

通常, Anaconda会从/etc/redhat-release文件中探测到计算机上原先安装的Red Hat Linux。如果没有, 则可以在Anaconda引导提示下输入下列内容:

```
boot: linux upgradeany
```

允许升级

可以用Red Hat Linux 9安装光碟从6.2以上版本升级。如果要升级带Ximian GNOME的Red Hat Linux版本, 则会遇到特殊问题。这时红帽子公司建议采用下列方法之一:

- 先删除Ximian GNOME再开始升级。
- 升级到Red Hat Linux 9, 然后重新安装Ximian GNOME。
- 升级到Red Hat Linux 9, 然后从Red Hat Linux安装光碟升级所有Ximian GNOME RPM及其相应RPM。

如果当前使用Ximian GNOME, 则升级到Red Hat Linux 9, 而不采取这些措施时, Red Hat Linux会警告GNOME不稳定。

进行升级

升级和普通安装一样地开始。从光碟或软盘引导Anaconda的问题并没有改变。图形化安装的前几步是相同的。与普通安装不同的第一个地方是配置鼠标之后。如果Anaconda发现旧版Red Hat Linux, 则会在图3.79所示的Upgrade Examine屏幕中标识。我们激活了Customize Packages To Be Upgraded选项。

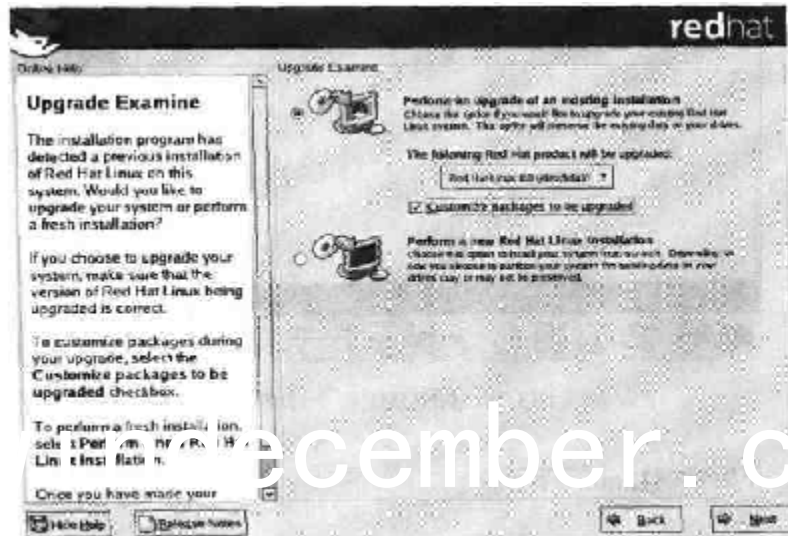


图3.79 寻找旧版Red Hat Linux

单击Next按钮继续。下一个屏幕可以从旧版GRUB或LILO更新引导装入器。从图3.80可以看出, 可以跳过更新过程或生成全新的引导装入器配置。进行选择, 然后单击Next按钮继续。

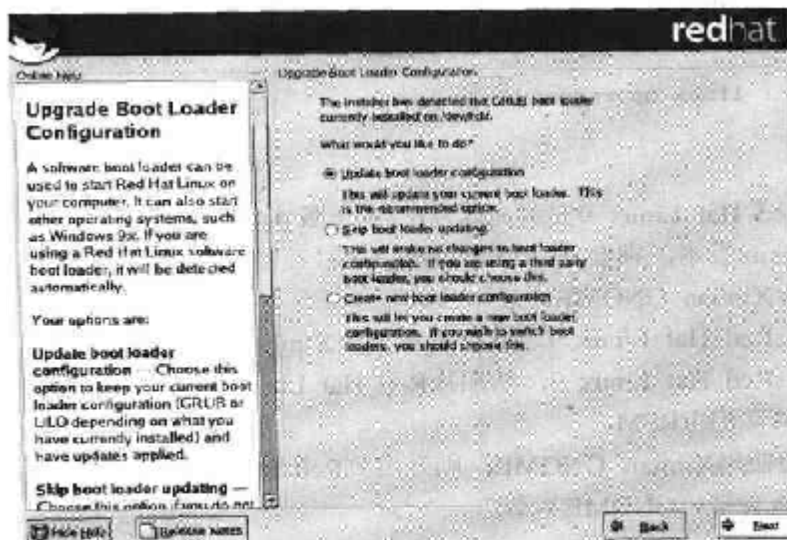


图3.80 更新引导装入器

现在, Anaconda要花一些时间检查系统中当前的包。它从清单中检查要更新的包。如果前面启用了Customize Packages To Be Upgraded选项, 则下一步进入Individual Package Selection菜单, 如图3.81。可以浏览菜单, 带有复选标志的包要升级。

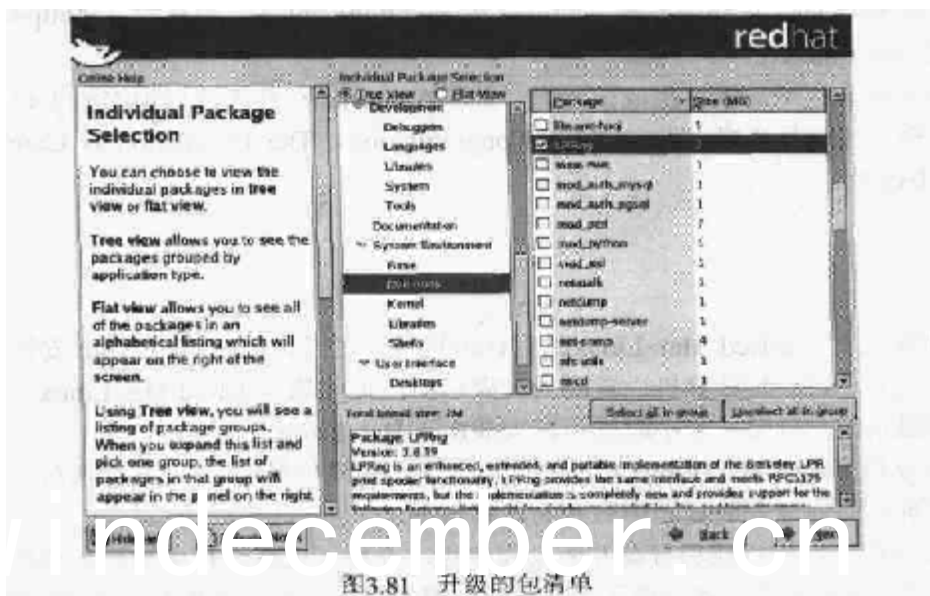


图3.81 升级的包清单

这里, 惟一需要升级的监控程序是LPRng (是旧的行打印监控程序)。第25章将会介绍, CUPS是新的默认打印服务。因此, 可以对这个包的升级进行决策。进行选择, 然后单击Next按钮继续。如果有依赖性, 则可以像普通Anaconda安装过程中一样看到 (这个屏幕见图3.51)。否则出现About To Upgrade屏幕, 如图3.82。准备好后, 单击Next按钮继续, 开始升级。

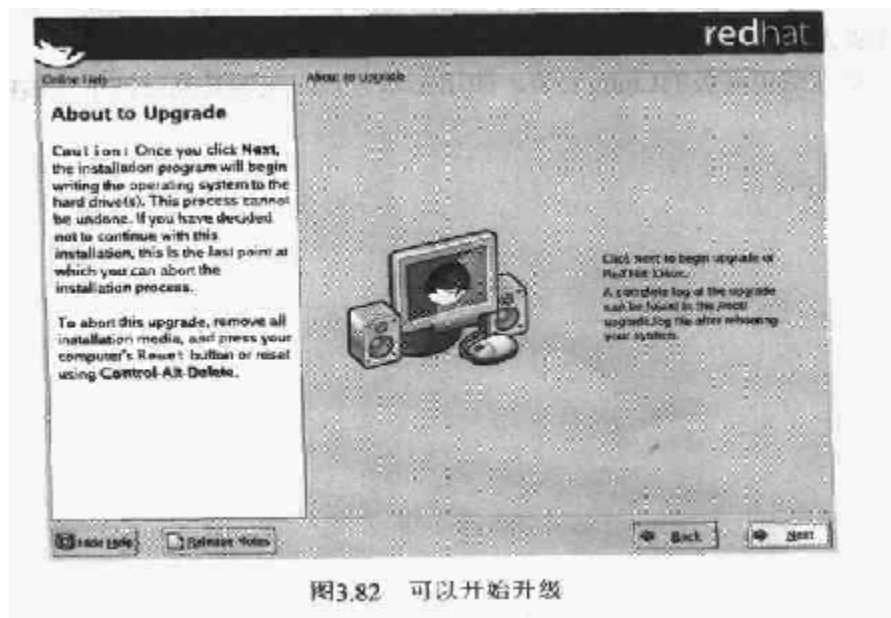


图3.82 可以开始升级

升级过程和安装时一样进行。这个过程会快一些，如果从较新的系统升级，则Anaconda可能只要升级少量包。

如果升级影响任何带配置文件的服务，则找到原配置文件，扩展名为.rpmsave。例如，如果升级影响Apache Web服务器，则可以在/etc/httpd/conf目录中看到，原httpd.conf文件保存为httpd.conf.rpmsave。

安装升级包之后，提示生成引导盘。如果Anaconda在升级过程中安装了新内核，则特别需要这样。按照其余提示做，遇到“Congratulations, The Installation Is Complete”消息时，单击Exit按钮。

小结

在计算机上安装Red Hat Linux时有许多选项。通常，Red Hat Linux安装并不复杂。大多数情况下，只要将计算机设置成从光碟启动，插入第一张Red Hat Linux安装光碟，按照简单的提示做，只要一个小时就可以安装Red Hat Linux。

本章介绍了Red Hat Linux安装的几种变形。如果你想成为Linux管理员，则本章应该有助于了解如何处理安装过程中遇到的各种情形。

本章介绍了如何生成引导盘和驱动程序。介绍了安装过程中如何用各种方法测试下载光碟和检查各种选项，还介绍了如何导航红帽子安装主体，帮助用户通过图形化登录屏幕完成桌面Linux配置。

可以用许多良好的资源查错安装，可以在Anaconda工作时使用这些资源。要利用这些资源，可以浏览/tmp目录中的日志文件和访问安装虚拟控制台。

登录Red Hat Linux之后，就可以用命令行界面学习整个Linux社区中的知识。

Anaconda还可以帮助从Red Hat Linux 6.2以上版本升级，可以定制要升级的包，可以更新引导装入器，可以保存前面修改的任何配置文件。

下一章介绍更高级的Linux安装，使用文本方式，主要是通过网络安装Red Hat Linux。

第4章 通过网络安装Linux

本章适用于Linux系统管理员和网络中连接多台Linux计算机的人。尽管第3章介绍的安装过程很不错，但从光碟安装需要大量时间，特别是安装到多台计算机时。为了节省时间，可以通过网络安装Red Hat Linux。通过网络安装的另一个好处是不必坐在那里，等待向计算机中插入另一张Red Hat Linux光碟。

本章假设你已经按照第2章的要求准备好计算机。例如，如果计划双引导Red Hat Linux与Microsoft Windows，则要用第2章介绍的方法为Linux保留足够的自由内存空间。

我们将介绍从三种网络服务器安装Linux：NFS（网络文件系统）、FTP（文件传输协议）和Web（通过Apache）。我们介绍如何在每种服务器上建立Red Hat Linux安装文件。尽管可以在不同操作系统中建立这些服务器，但我们将介绍建立每个服务的基础。每个服务的详细配置将在后面几章介绍。

本章还要详细介绍网络安装过程，从引导到一步一步的文本方式安装。为什么要用文本方式安装？速度快！且安装的时间是短暂的。我们还将介绍升级现有Linux安装时的微妙差别。最后，我们将介绍查错网络安装的方法。

学完第4章和第5章之后，你就可以同时在多台计算机上安装Red Hat Linux。本章介绍下列主题：

- 准备NFS服务器
- 准备HTTP服务器
- 准备FTP服务器
- 通过网络安装Linux
- 查错网络安装

准备NFS服务器

本节介绍配置NFS服务器，从光碟安装Red Hat Linux。配置服务器时，可以在Red Hat Linux安装了今后要用到的RPM包之后，使用共享NFS目录。

这里假设已经有Linux或UNIX计算机并安装了相应的NFS服务。我们将介绍建立NFS安装服务器所需的基本命令，但NFS工作的细节不在本章介绍，而放到第28章。

我们还假设你以根用户身份进行改变。

复制文件

第一步要建立具有Red Hat Linux安装文件的目录。需要一个/RedHat目录，其中有base与RPMS子目录。要将第一个Red Hat Linux安装光碟中的文件复制到/RedHat/base目录，将三张安装光碟中的RPM包复制到/RedHat/RPMS目录。

这个过程实际上很简单:

1. 找到Red Hat Linux安装文件的空间, 大约需要2GB空间。
2. 生成另一目录, 保证它在有足够空间的分区中。关于管理分区的更多信息, 见第7章。
本练习中将这个目录命名为/mnt/inst。

```
# mkdir /mnt/inst
```

3. 装载第一张Red Hat Linux 9安装光碟。

```
# mount -r /dev/cdrom /mnt/cdrom
```

4. 从光碟中复制相应文件:

```
# cp -ar /mnt/cdrom/RedHat /mnt/inst
```

5. 卸载第一张安装光碟。装载第二张Red Hat Linux安装光碟, 并从光碟中复制相应文件:

```
# umount /mnt/cdrom
```

```
# mount -r /dev/cdrom /mnt/cdrom
```

```
# cp -ar /mnt/cdrom/RedHat /mnt/inst
```

6. 重复第5步, 从第三张光碟中复制相应文件。

```
# umount /mnt/cdrom
```

```
# mount -r /dev/cdrom /mnt/cdrom
```

```
# cp -ar /mnt/cdrom/RedHat /mnt/inst
```

现在就有了Red Hat Linux安装源。

也可以从共享NFS目录的.iso文件中安装Red Hat Linux, 但本书没有介绍这个方法, 因为我认为这没什么用。尽管我们可以装载.iso文件, 像普通Red Hat Linux安装光碟一样, 但这个方法在安装Red Hat Linux之后无法提供单个RPM包来源。

共享目录

如果在计算机上安装了NFS, 则可以导出带Red Hat Linux安装文件的共享目录。导出在/etc/exports配置文件中建档, 可以在所选的文本编辑器中将其打开。

说明: Linux中有几个文本编辑器, 关于vi文本编辑器的更多信息, 见第6章。

根据上节的工作, 我们共享Red Hat Linux安装文件所在的/mnt/inst目录, 非常简单, 只要按照下列步骤去做:

1. 在/etc/exports中增加下列行:

```
/mnt/inst      *(ro,sync)
```

保证星号之后没有空格, 否则NFS可能产生误解。将改变保存到/etc/exports中。

2. 然后用下列命令导出共享目录:

```
# exportfs -a
```

3. 这样就可以保证NFS准备共享目录了。停止这个服务。如果NFS还没有运行, 则后面的消息好像生成错误消息, 别管它。

```
# service nfs stop
```

4. 从光碟中复制适当文件（这个过程可能需要几分钟）：

```
# service nfs start
```

5. 检查导出内容。用下列命令显示可以装载的目录：

```
# showmount -e
```

6. 如果安装过程中安装了防火墙，最好将其关闭。尽管可以在防火墙上打洞，但这需要更复杂的技巧（见第23章）。目前只要用下列方法“刷新”Linux计算机上的所有防火墙规则：

```
# iptables -F
```

（如果你的Linux版本较老，则可能要用ipchains -F命令）。

这样就已经建立了Red Hat Linux安装文件所在的/mnt/inst目录，并用NFS共享。

说明：如果要在下次引导Linux时继续共享安装目录，则可以利用chkconfig --level 2345 nfs命令。

关于chkconfig命令的详细信息，见第13章。

安装参数

要使用已经共享的NFS目录，需要两件事，NFS服务器地址和/RedHat目录地址。NFS服务器地址可以是计算机名（如NFSserver）或完全限定域名（如www.example.com）。但这要求工作的DNS（域名服务）服务器，并不适合所有网络。

也可以使用NFS服务器IP地址。如果不知道NFS服务器IP地址，则可以运行ifconfig命令，得到图4.1所示的输出。

```
(root@RH9Test root)# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:40:F4:DC:05:98
          inet addr:10.252.113.63  Bcast:10.252.113.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:191 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:37979 (37.0 Kb)  TX bytes:10859 (10.6 Kb)
          Interrupt:5 Base address:0x8000

lo        Link encap:Local loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16384  Metric:1
          RX packets:4210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4210 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:280966 (280.2 Kb)  TX bytes:280966 (280.2 Kb)

(root@RH9Test root)#
```

图4.1 NFS服务器IP地址

其中最重要的信息是IP地址，图4.1中为10.252.113.63。关于IP地址和本节其他概念的详细信息，见第20章。总之，运行的NFS服务器中建立共享目录之后，要在安装过程中使用下列信息：

NFS服务器IP地址 如果网络上有工作的DNS服务器，则也可以使用计算机名或完全限定域名。

/RedHat目录地址 根据本章前面采取的动作，这是/mnt/inst。如果在不同目录中建立Red Hat Linux安装文件，则/RedHat目录地址相应改变。

本章稍后“文本方式步骤”一节将介绍其如何工作。

准备Apache Web服务器

本节介绍配置Apache Web服务器，从光碟安装Red Hat Linux。配置服务器时，可以在Red Hat Linux安装了今后要用到的RPM包之后，使用Web站点上的目录。

这里假设已经有Linux或UNIX计算机，并安装了相应的Apache (httpd) 服务。我们将介绍建立Apache (httpd) 安装服务器所需的基本命令，但Apache工作的细节不在本章介绍，而放到第30章。

我们还假设你以根用户身份进行改变。

复制文件

第一步要建立具有Red Hat Linux安装文件的目录。需要一个/RedHat目录，其中有base与RPMS子目录。要将第一个Red Hat Linux安装光碟中的文件复制到/RedHat/base目录，将三张安装光碟中的RPM包复制到/RedHat/RPMS目录。

这个过程实际上很简单：

1. 找到Red Hat Linux安装文件的空间，最好与/var目录相联系。大约需要2GB空间。
2. 生成该目录，保证它有足够空间的分区中。关于管理分区的更多信息，见第7章。

本练习中将这个目录命名为/var/www/html/inst。

```
# mkdir /var/www/html/inst
```

3. 装载第一张Red Hat Linux 9安装光碟（可能要几分钟）：

```
# mount /dev/cdrom /mnt/cdrom
```

4. 从光碟中复制相应文件：

```
# cp -ar /mnt/cdrom/RedHat /var/www/html/inst
```

5. 卸载第一张安装光碟。装载第二张Red Hat Linux安装光碟，并从光碟中复制相应文件：

```
# umount /mnt/cdrom
```

```
# mount /dev/cdrom /mnt/cdrom
```

```
# cp -ar /mnt/cdrom/RedHat /var/www/html/inst
```

6. 重复第5步，从第三张光碟中复制相应文件：

```
# umount /mnt/cdrom
```

```
# mount /dev/cdrom /mnt/cdrom
```

```
# cp -ar /mnt/cdrom/RedHat /var/www/html/inst
```

现在就有了Red Hat Linux安装源。

与NFS或硬盘安装不同的是，不能用Apache服务器从.iso文件安装Red Hat Linux。

共享目录

如果计算机上安装了Apache Web服务器，则现在可以共享相关目录。默认情况下，标准文件在/var/www/html中存放。假设使用上节指定的目录，则Red Hat Linux安装过程中只

要指定`/inst`目录即可。

这个过程比NFS中更简单，只要保证用下列命令启动Apache：

```
# service httpd start
```

然后检查用所选择的Web浏览器导航到`http://localhost`时，是否得到“Test Page”。

建立共享之后，可以通过Web服务器下载各个Red Hat Linux包。图4.2显示了这个方法。导航到`http://yourwebserver/inst/RedHat`，单击RPM目录，然后可以单击上节装入的RPM。可以将RPM下载到本地计算机上。

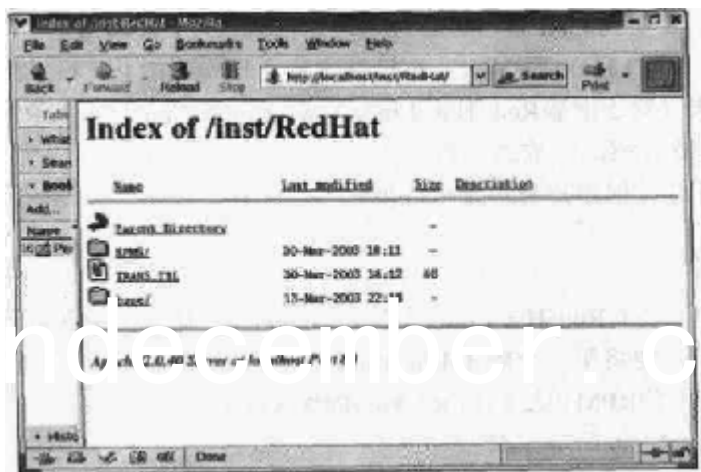


图4.2 通过Web浏览器访问RPM

和NFS中一样，要保证本地计算机上的防火墙不会阻止访问Web服务器。最简单的方法是用下列方法“刷新”Linux计算机上的所有防火墙规则：

```
# iptables -F
```

如果你的Linux版本较老，则可能要用`ipchains -F`命令。

这样就已经建立了Red Hat Linux安装文件所在的`/mnt/inst`目录，并用Apache Web服务器共享。

说明：如果要在下次引导Linux时继续运行Apache，则可以利用`chkconfig --level 2345 httpd on`命令。

关于`chkconfig`命令的详细信息，见第13章。

安装参数

要使用已经共享的Apache目录，需要两件事：Apache Web服务器地址和RedHat目录地址。Apache Web服务器地址可以是计算机名（如Webserver）或完全限定域名（如`www.example.com`）。但这要求工作的DNS（域名服务）服务器，并不适合所有网络。

也可以使用Web服务器IP地址。如果不知道Web服务器IP地址，则可以运行`ifconfig`命令，得到图4.1所示的输出。

关于IP地址和本节其他概念的详细信息，见第20章。总之，运行的Web服务器中建立共享目录之后，要在安装过程中使用下列信息：

Apache web服务器IP地址 如果网络上有工作的DNS服务器, 则也可以使用计算机名或完全限定域名。

/RedHat目录地址 根据本章前面采取的动作, 这是inst。

本章稍后“文本方式步骤”将介绍其如何工作。

准备FTP服务器

本节介绍配置FTP服务器, 从光碟安装Red Hat Linux。配置服务器时, 可以在Red Hat Linux安装了今后要用到的RPM包之后。如何连接同一个FTP服务器。

这里假设已经有Linux或UNIX计算机并安装了相应的FTP服务。在Red Hat Linux中, 这包括vsftpd-*或(对于旧版Red Hat Linux)wu-ftpd-*和anonftp-* RPM包。FTP服务器配置的细节不在本章介绍, 而放到第27章。

我们还假设你以根用户身份进行改变。

复制文件

第一步要建立具有Red Hat Linux安装文件的目录。需要一个/RedHat目录, 其中有base与RPMS子目录。要将第一张Red Hat Linux安装光碟中的文件复制到Red Hat base目录, 将三张安装光碟中的RPM包复制到/RedHat/RPMS目录。

这个过程实际上很简单:

1. 找到Red Hat Linux安装文件的空间, 最好与/var目录相联系。大约需要2GB空间。
2. 生成另一目录, 保证它在有足够空间的分区中。关于管理分区的更多信息, 见第7章。

本练习中将这个目录命名为/var/ftp/pub/inst。

```
# mkdir /var/ftp/pub/inst
```

3. 装载第一张Red Hat Linux 9安装光碟:

```
# mount /dev/cdrom /mnt/cdrom
```

4. 从光碟中复制相应文件:

```
# cp -ar /mnt/cdrom/RedHat /var/ftp/pub/inst
```

5. 卸载第一张安装光碟。装载第二张Red Hat Linux安装光碟, 并从光碟中复制相应文件:

```
# umount /mnt/cdrom
```

```
# mount /dev/cdrom /mnt/cdrom
```

```
# cp -ar /mnt/cdrom/RedHat /var/ftp/pub/inst
```

6. 重复第5步, 从第三张光碟中复制相应文件:

```
# umount /mnt/cdrom
```

```
# mount /dev/cdrom /mnt/cdrom
```

```
# cp -ar /mnt/cdrom/RedHat /var/ftp/pub/inst
```

现在就有了Red Hat Linux安装源。

与NFS或硬盘安装不同的是, 不能用FTP服务器从.iso文件安装Red Hat Linux。

共享目录

如果计算机上安装了FTP服务器，则现在可以共享相关目录。默认情况下，标准文件在/var/ftp/pub中存放。假设使用上节指定的目录，则Red Hat Linux安装过程中只要指定/inst目录即可。

这个过程比NFS中更简单，只要保证用下列命令启动FTP：

```
# service vsftpd start
```

并在登录FTP服务器之后检查是否能进入相应目录。

说明：在Red Hat Linux 9之前，vsftpd是个xinetd服务，可以按第23章介绍的方法激活。

建立共享之后，可以通过FTP服务器下载各个Red Hat Linux包。详见第10章介绍。

和NFS中一样，要保证本地计算机上的防火墙不会阻止访问Web服务器。最简单的方法是目前只要用下列方法“刷新”Linux计算机上的所有防火墙规则：

```
# iptables -F
```

如果你的Linux版本较老，则可能要用ipchains -F命令。

说明：ipchains命令与Linux内核v2.2关系最密切，但有些Linux内核为v2.4的计算机也运行ipchains，包括Red Hat Linux 7.1与7.2及以后的版本。

这样就已经建立Red Hat Linux安装文件所在的/mnt/inst目录并用FTP服务器。

说明：如果要在下次引导Linux时继续运行Apache，则可以利用chkconfig --level 2345 vsftpd命令。关于chkconfig命令的详细信息，见第13章。

安装参数

要使用已经共享的FTP目录，需要两件事：FTP服务器地址和/RedHat目录地址。FTP服务器地址可以是计算机名（如Webserver）或完全限定域名（如www.example.com）。但这要求工作的DNS（域名服务）服务器，并不适合所有网络。

也可以使用FTP服务器IP地址。如果不知道FTP服务器IP地址，则可以运行ifconfig命令，得到图4.1所示的输出。

关于IP地址和本节其他概念的详细信息，见第20章。总之，运行的FTP服务器中建立共享目录之后，要在安装过程中使用下列信息：

FTP服务器IP地址 如果网络上有工作的DNS服务器，则也可以使用计算机名或完全限定域名。

/RedHat目录地址 根据本章前面采取的动作，这是/pub/inst。

本章稍后“文本方式步骤”将介绍其如何工作。

通过网络安装Linux

通过网络安装Red Hat Linux时，通常不用Red Hat Linux安装光碟，因此要一个引导盘。红帽子公司提供了引导盘映像，可以写入软盘或光碟中。

有了引导盘之后，就可以开始Red Hat Linux网络安装过程。本章使用文本方式安装，因为第3章已经介绍过图形方式。无论何种情况，从FTP与Apache服务器安装时，不能进行图形方式安装。

Red Hat Linux安装程序是Anaconda。可以定制Anaconda安装过程，省略游戏之类的安装选项，详见第5章介绍。

建立引导盘

红帽子公司在第一张安装光碟的/images目录中提供了引导盘映像，甚至可以用第一张安装光碟作为网络引导盘。可以用两个基本文件生成安装引导盘，还有几个驱动程序映像，可以生成三寸驱动程序软盘。

表4.1简要介绍了/images目录中提供的文件。

表4.1 引导映像

文件名	描述
bootdisk.img	所有本地与网络安装的标准引导盘
cd-vblock.img	CD（存储）设备的驱动程序盘
cd-vnet.img	网卡驱动程序盘
pcmciaadd.img	PCMCIA硬件驱动程序盘
boot.iso	带驱动程序的集成引导盘，不能放在一张三寸软盘中，但可以安装到一张光碟

可以用三种方法将.img文件写入三寸软盘。如果有Linux计算机，则可以用cat或dd命令。例如，可以用下列命令将bootdisk.img文件内容写入三寸软盘。这些命令假设第一张Red Hat Linux安装光碟装载到/mnt/cdrom目录：

```
# dd if=/mnt/cdrom/images/bootdisk.img of=/dev/fd0
# cat /mnt/cdrom/images/bootdisk.img > /dev/fd0
```

第二种方法是在Microsoft Windows中将这此映像文件内容写入三寸软盘。关键实用程序在第一张Red Hat Linux安装光碟的/dosutils目录中。这个界面的命令行版本为RAWRITE.EXE。在Microsoft Windows中，打开一个DOS命令行窗口，插入第一张Red Hat Linux安装光碟。如果光碟为E盘，则运行下列命令：

```
E:\>DOSUTILS\RAWRITE
Enter disk image source file name: E:\IMAGES\BOOTDISK.IMG
Enter target diskette drive: A:
Please insert a formatted diskette in drive A: and press -ENTER- :
```

也可以从boot.iso文件生成引导光碟，详见第14章介绍的cdrecord命令。甚至可以用第一张Red Hat Linux 9开始网络安装，但要记住用linux askmethod或text askmethod命令安装。

文本方式引导

我们将介绍文本方式网络安装。上节曾介绍过，引导盘有三个选项：

- 将bootdisk.img文件内容写入三寸软盘

- 从boot.iso文件生成引导光碟
- 第一张Red Hat Linux安装光碟

三种情况都会出现图4.3所示的菜单。



图4.3 Red Hat Linux安装菜单

第3章介绍了图形方式安装Red Hat Linux，主要针对普通用户。现在要详细介绍管理员的做法。从初始菜单可以看出，其中还有另外几个菜单。可以按F2键取得Installer Boot Options菜单，如图4.4。



图4.4 安装引导选项

这个菜单列出了boot:提示下可以输入的一些选项，表4.2介绍这些选项。

表4.2 安装程序引导选项

选项	描述
linux noprobe	不自动探测硬件而开始安装过程，要从清单中选择任何SCSI硬盘和网卡的驱动程序
linux mediacheck	从文本方式提示开始安装过程，可以检查红帽子安装光碟的完整性。默认情况下，在图形方式中继续
linux rescue	在救援方式中引导基本Linux系统，试探测当前Linux安装。详见第11章
linux dd	开始安装过程，出现驱动程序光碟提示，适用于第三方驱动程序
linux askmethod	开始安装过程，可以选择语言和键盘，然后可以选择本地或网络安装选项

(续表)

选项	描述
linux updates	支持用定制安装更新盘升级
linux lowres	用低分辨率图形方式（640×480）开始安装，也称为VGA（视频图形卡）

说明：可以在文本方式中运行任何安装选项，只要将linux换成text即可。也可以用linux text或text命令在文本方式中开始安装。

换句话说，如果从bootdisk.img软盘或boot.iso光碟开始安装过程，则要输入下列命令：

```
boot: linux text
```

如果从第一张安装光碟开始安装过程，则要输入下列命令：

```
boot: text askmethod
```

引导提示下还可以指定一些硬件的参数。图4.5所示的内核参数帮助屏幕提供了基本方法。详细信息可以在另一台Linux计算机上用man bootparam命令查阅。



图4.5 内核参数帮助屏幕

文本方式步骤

现在要开始安装过程了，我们要一步一步介绍。我们根据从bootdisk.img安装盘开始的方法，详细介绍文本方式安装过程。其他安装过程更简单。

提示：这节非常长。如果想一下子读完，最好先歇一会儿。

- 1. 用bootdisk.img文件生成的Red Hat Linux安装软盘启动计算机，见前面“建立引导盘”一节。
- 2. 出现提示时，输入下列命令：

```
boot: linux text
```

说明：如果使用第一张Red Hat Linux安装光碟，则要在引导提示下输入text askmethod。

可以看到一系列消息，安装基本内核和Anaconda安装程序的文本方式版本。

3. 从图4.6所示的Choose A Language屏幕中选择语言。默认为英语，但安装Red Hat Linux时也可以使用另外18种语言和方言。可以用向上和向下箭头键进行选择。选择语言之后，用Tab键加亮显示OK按钮，然后按Enter键或按F12键继续。

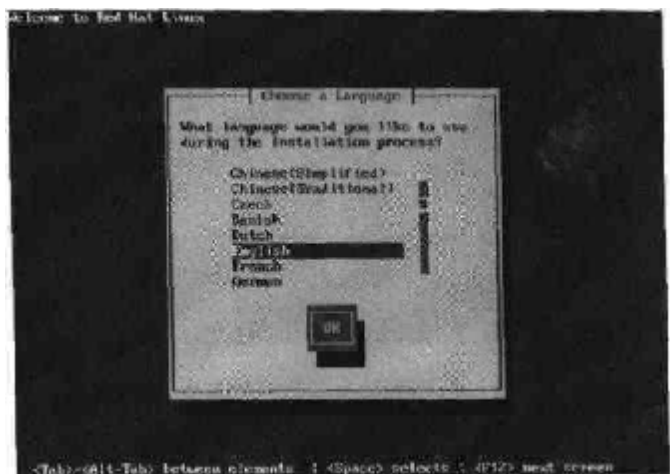


图4.6 选择语言

说明：对于每个文本方式菜单，可以用Tab键在选项之间移动。进行选择后，会亮显示OK按钮，并按Enter键或按F12键继续。如果某个设置可以来回切换，则可以加亮显示所要设置并按空格键。

4. 从Keyboard Type屏幕中选择键盘，如图4.7。默认为美式键盘，但也可以将Keyboard Type安装用60多种不同键盘设置，其中许多键盘是针对其他语言定制的。选择键盘之后，按F12键继续。

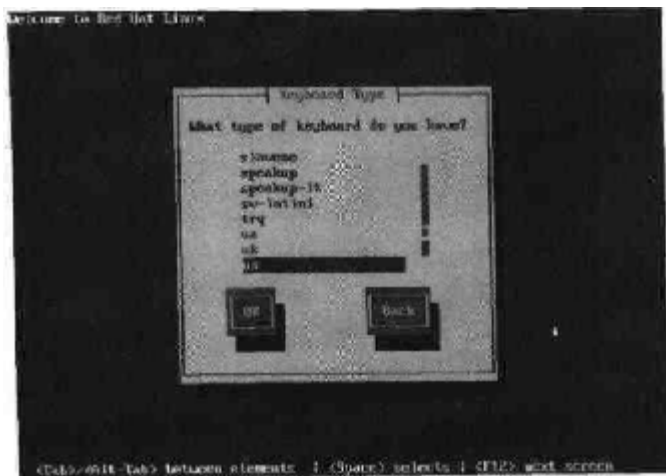


图4.7 选择键盘

5. 从图4.8选择网络安装方法。前面曾介绍过，可以从NFS、FTP或HTTP（Apache）服务器安装。进行选择，然后按F12键继续。



图4.8 选择网络安装方法

说明：如果有多个网卡，则可以看到一个菜单，可以选择不同网卡，如eth0与eth1。很难简单判断哪个网卡连接哪个网络。如果选错网卡，则后几步会出现错误消息。可能需要一个试错过程。如果选错网卡，则可以在菜单中的Back选项，可头选择其他网卡。

6. 基于bootdisk.img的安装盘可能还需要其他驱动程序，如图4.9。选择Use A Driver Disk并按Enter键继续。如果看不到No Driver Found屏幕，则表示从第一张Red Hat Linux安装光碟或基于boot.iso的光碟启动，这时可以跳到第10步。



图4.9 No Driver Found屏幕

7. 由于需要新驱动程序，因此可以选择一个驱动程序盘，如图4.10。可以用前面“建立引导盘”一节生成的驱动程序盘。这时选择fd0。如果能用第一张Red Hat Linux安装光碟作为驱动程序盘，则可以选择与光碟相关联的设备，通常是hdb或hdc。进行选择，然后按F12键继续。



图4.10 选择驱动程序盘

8. 在图4.11所示的提示下插入与网卡或硬盘相应的驱动程序盘（软盘或光碟）。如果两者都需要，则会提示对另一个盘重复这个过程。

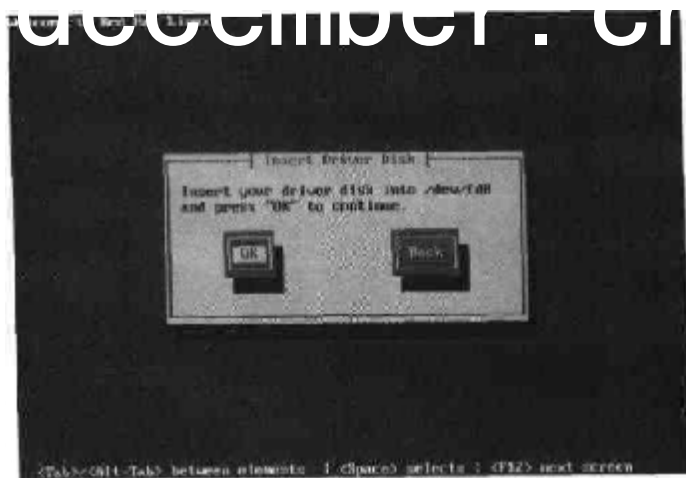


图4.11 插入驱动程序盘

9. 如果需要不同驱动程序盘，则可以看到图4.12所示的错误屏幕。选择**Load Another Disk**并按Enter键继续。如果继续看到同一消息，则可能是驱动程序盘搞乱了，或不支持你的硬件。回到第7步。如果没有看到错误屏幕，则转到第10步。

10. 现在已经安装网卡与硬盘的驱动程序，就可以建立与网络服务器的连接。在图4.13所示的TCP/IP配置屏幕中，要建立计算机的TCP/IP设置。

如果网络中有DHCP（动态主机配置协议）服务器，则可以激活**Use Dynamic IP Configuration (BOOTP/DHCP)**设置，否则要设置系统的关键IP地址信息。这时，加亮设置并按空格键将其取消。关于IP地址的更多信息，见第20章。进行选择，然后按F12键继续。如果有第二个网卡，则要对第二个网卡重复这个过程。

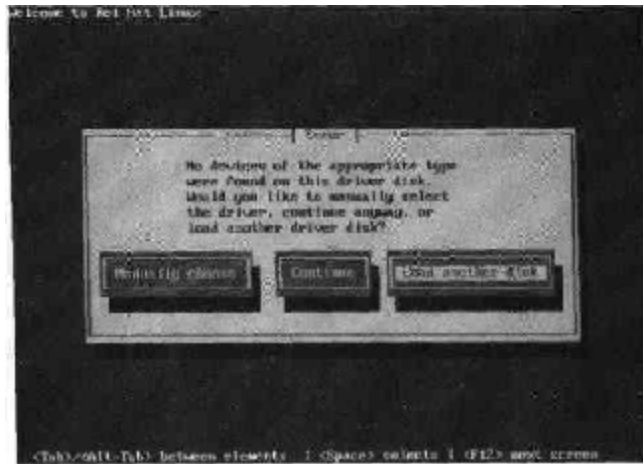


图4.12 提示插入另一驱动程序盘

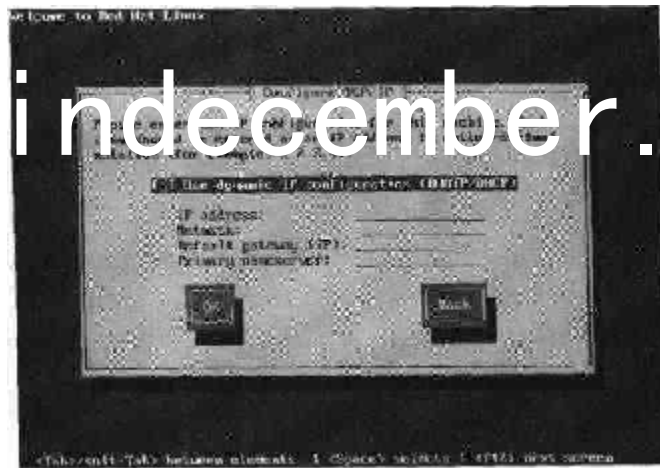


图4.13 TCP/IP配置屏幕

提示：如果有家庭网络，则可能已经有DHCP服务器。许多硬件路由器都有自己的DHCP服务器，如电缆调制解调器与DSL适配器的硬件路由器。如果有这些组件，则可以检查与这个硬件路由器相关联的文档。确保指定的IP地址匹配网络所配置的子网。

11. 下一步随从NFS、Apache HTTP或FTP服务器，安装而稍有不同。无论如何，都要指定服务器的名称或IP地址以及安装文件地址。图4.14、图4.15和图4.16分别演示了每种服务器中要输入的内容，对应于本章前面建立的服务器设置。例如，图4.14要求将RedHat目录安装到NFS服务器的/mnt/inst目录中。图4.15和图4.16基于前面的设置，将安装文件复制到HTTP或FTP服务器中。

如果从FTP服务器安装，则从图4.16可以看出，可以从非匿名FTP服务器安装，即只有用户名和口令。如果选择这个选项，则会提示输入用户名和口令。

12. 如果成功连接了任何网络服务器，则最终可以看到下列消息：

```
Running anaconda, the Red Hat Linux System installer - please wait
```



图4.14 NFS设计

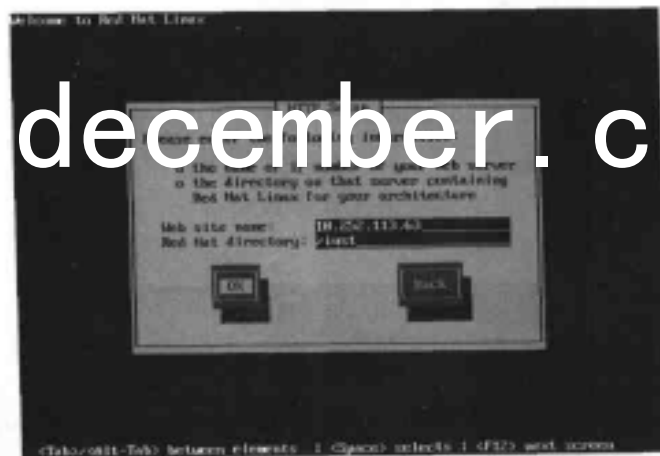


图4.15 HTTP设置



图4.16 FTP设置

然后是图4.17所示的欢迎屏幕。后面的步骤独立于所用的安装服务器。选择OK按钮继续。

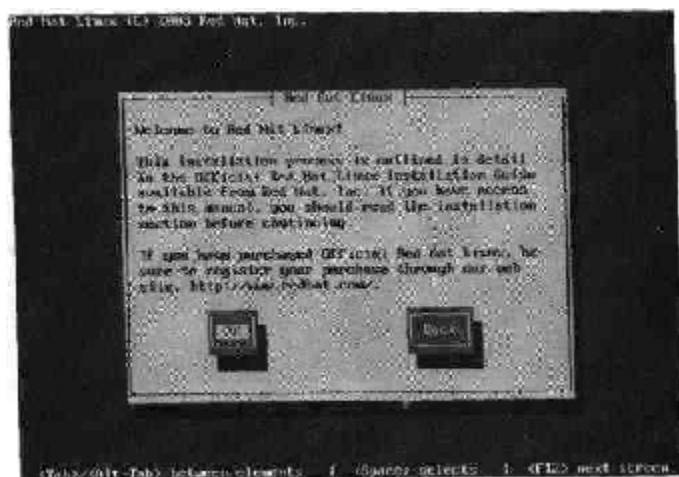


图4.17 欢迎屏幕

说明：如果已经安装Red Hat Linux 9.0，则此屏幕会出现一个警告，并可以停止安装过程。

13. 从图4.18所示的Mouse Selection屏幕选择一个鼠标。可以选择40多种指导设备，包括几个连接USB接口的指导设备。大多数情况下，如果选择双键鼠标，则自动选择Emulate 3 Buttons选项。

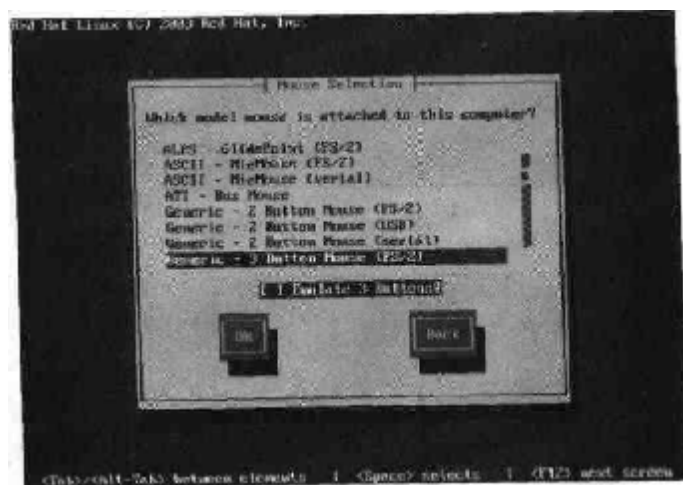


图4.18 Mouse Selection屏幕

说明：Emulate 3 Buttons选项可以同时按左右键而模拟中间键功能。可以通过空格键选择与取消这个选项。

14. 如果在已经有旧版Red Hat Linux的计算机上安装Red Hat Linux，则会出现图4.19所示的System To Upgrade屏幕。如果准备升级现有Red Hat Linux安装，则选择这个选项。如果选择Reinstall System，则可以在同一空间中安装全新的Red Hat Linux。



图4.19 System To Upgrade屏幕

如果选择升级现有Red Hat Linux安装，则阅读下节内容，否则选择Reinstall System并按F12键继续。

15. 选择Installation Type，图4.20显示了四种安装类型选项。每个选项有不同的默认包组，见下面的“安装选项”旁白。本组选择是定制安装，与其他选项相关的步骤大致相同。进行选择，并按F12键继续。



图4.20 安装类型选项

安装选项

Red Hat Linux标准安装选项有四个：Personal Desktop、Workstation、Server与Custom。尽管每种情况都可以定制安装，但每个选项与一组默认包组相联系。每个包组有一组RPM包，建档在comps.xml文件中，见Web上第5章介绍，见Sybex公司web站点www.sybex.com。

其他Red Hat Linux版本还有Laptop安装选项，增加与标准便携电脑硬件相关的包。这些包现在已经加进Personal Desktop和Workstation安装选项中。

下面列出默认安装的包组，供参考：

组	个人桌面计算机	工作站	服务器	定制
Administration Tools	*	*	*	
Authoring and Publishing				
DNS Name Server				
Development Tools		*		
Editors	*	*		
Engineering and Scientific				
FTP Server				
GNOME Desktop Environment	*	*		*
GNOME Software Development		*		
Games and Entertainment	*	*		
Graphical Internet	*	*		*
Graphics	*	*		*
KDE Desktop Environment				
KDE Software Development				
Kernel Development				
Mail Server				
Network Servers				
News Server				
Office/Productivity	*	*		*
Printing Support	*	*	*	*
SQL Database Server				
Server Configuration Tools			*	
Sound and Video	*	*		*
System Tools				
Text-based Internet	*	*	*	*
Web Server			*	
Windows File Server			*	
X Software Development		*		
X Window System	*	*		*
安装文件大致长度	1700MB	2100MB	850MB	1500MB

16. 然后选择Disk Partitioning Setup，如图4.21。如果选择Autopartition，则Red Hat Linux会根据所要的包、内存和硬盘上的分区长度自动配置分区。如果选择Disk Druid，则跳到第18步。进行选择，并按Enter键继续。

说明：如果这是新盘，则可能出现一个警报，表示无法阅读分区表。这时可以初始化硬盘。要确认在这个硬盘上安装Red Hat Linux。

17. 如果选择让Red Hat Linux将系统自动分区，则可以看到图4.22所示的自动分区窗口。如果在具有Linux与Microsoft Windows分区的计算机上安装Red Hat Linux，

则要格外小心。服务器安装的默认选项是删除Microsoft Windows操作系统。表4.3列出了这些选项。进行选择并按F12键继续。

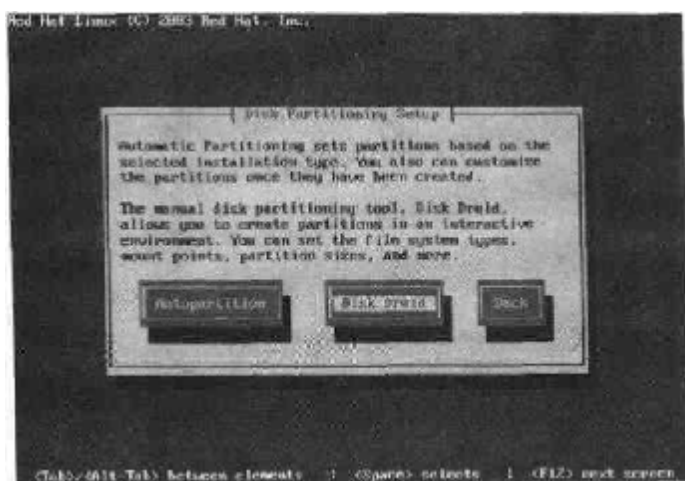


图4.21 磁盘分区设置



图4.22 自动分区

表4.3 自动分区选项

选项	描述
Remove All Linux Partitions On This System	删除格式化为Linux文件系统的所有分区，不影响格式化为其他文件系统的所有分区，如Microsoft Windows文件系统
Remove All Partitions On This System	删除这台计算机上的所有分区
Keep All Partitions And Use Existing Free Space	假设硬盘上具有未分区自由空间，如果没有，则这个选项会产生错误消息
Which Drive(s) Do You Want To Use For This Installation?	如果有多个物理硬盘，则可以选择安装Red Hat Linux的盘

18. 要确认选择，如图4.23。如果对选择满意，则选择Yes并按Enter键继续。

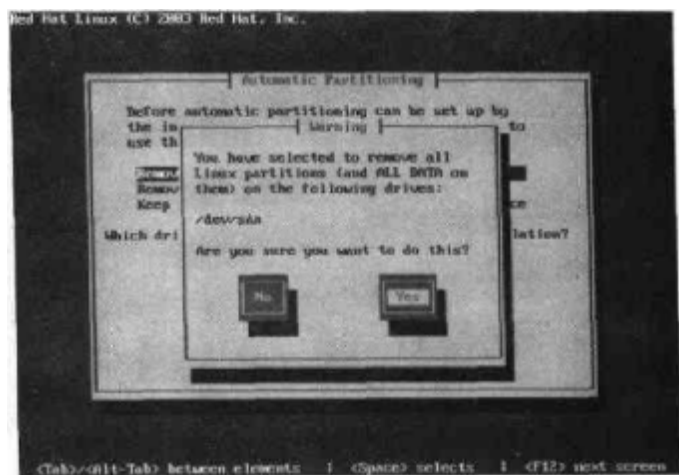


图4.23 删除分区之前出现的警告

19. 进入Disk Druid屏幕，可以检查Anaconda进行的自动分区选项。图4.24显示了192MB内存和4GB硬盘的计算机上的默认服务器配置。如果空间允许，则Red Hat Linux通常指定内存空间的两倍空间作为交换分区。

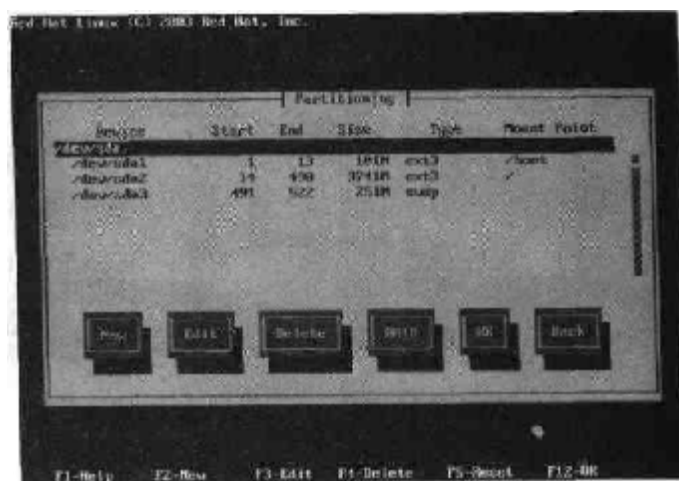


图4.24 默认服务器配置

20. 可以编辑配置的分区。例如，如果配置如图4.24，则可以加亮显示与根 (/) 目录相关联的/dev/sda2。然后可以用Tab键加亮Edit并按Enter键继续，进入Add Partition窗口，可以改变与/dev/sda2相关联的设置。图4.25显示了这个菜单，表4.4列出了菜单中的选项。
21. 也可以增加新分区。例如，我增加/var目录的分区，帮助控制其余自由空间，如图4.26。



图4.25 编辑配置的分区

表4.4 Add Partition窗口选项

选项	描述
Mount Point	指定分区在根文件系统下的目录，对可装载目录，见第7章介绍的文件系统层次结构
File System Type	设置分区格式，可以选择Linux ext2或ext3标准、Linux交换格式、LVM（逻辑卷管理器）物理卷、软件RAID卷或Microsoft Windows式vfat格式
Allowable Drives	指定与分区相关联的硬盘设备
Size (MB)	指定分区长度（MB）
Force To Be A Primary Partitoun	一般来说，引导目录应放在1024柱面以下的主分区中
Check For Bad Blocks	对不可读扇区设置分区物理检查

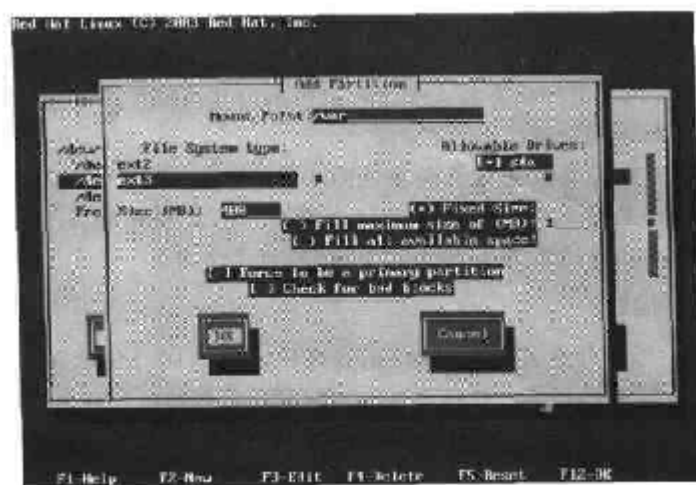


图4.26 增加新分区

22. 如果配置两个或多个软件RAID分区，则可以配置一个RAID设备。在前面图4.24的主Disk Druid屏幕中，选择RAID并按Enter键。如果有足够的软件RAID分区，则可以看到Make RAID Device菜单，如图4.27。

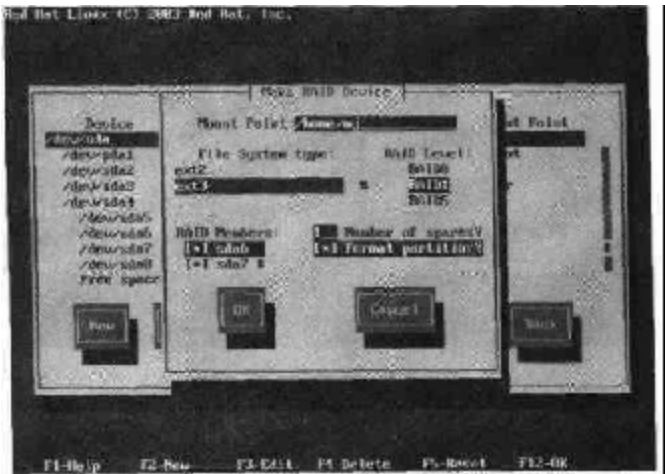


图4.27 Make RAID Device菜单

这里笔者生成RAID1级设备，有三个RAID成员分区sda6、sda7和sda8。由于RAID1只求两个分区，因此有一个多余分区。关于RAID的更多信息，见第14章。

说明：Red Hat Linux文本方式菜单不能手工配置逻辑卷管理器（LVM）文件系统，但第3章介绍的图形方式安装和第5章的Kickstart安装中可以。

分区长度

Red Hat Linux安装过程中的一个重要决策是分区长度与个数。第3章和第7章会介绍，可以将不同目录装载到不同的硬盘分区。这样有保护作用，因为许多分区连接可能会使计算机崩溃。

如果硬盘空间只有2GB到3GB以下，则选择很简单。硬盘上没有更多空间，因此只能对根目录、引导目录和交换分区进行划分。这些典型分区配置见第7章介绍。

如果还有更多空间，则可以更加灵活。可以对不同目录配置不同分区。第7章将会介绍，有些目录不能装载到不同分区。

下面列出一些可能要装载的目录和安装Red Hat Linux中一切所需的最小空间要求（可能大于特定目录中安装的文件长度）。记住，用户、应用程序和日志文件通常还要更多空间。例如，大型Web站点通常每天产生几个GB的日志文件。

目录	描述
/boot	包含引导文件，包括Linux内核，默认100MB应该足够
/	顶层根目录，包括没有在不同分区装载的所有目录。除了不同分区装载的所有目录外，根目录中的其余目录在“一切”安装中大约占110MB文件
/home	包括除根用户之外所有用户的主目录，选择长度时，要考虑当前与未来用户的长期需要

/home/mj	限制特定用户可用的空间量，也可以使用第9章介绍的配额
/opt	包含许多第三方应用程序的文件，在“一切”安装中大约占17MB文件
/tmp	包括经常自动删除的文件，适合下载在“一切”安装中大约占5MB文件
/usr	包含许多程序和大量数据，在“一切”安装中大约占5300MB空间。有些第三程序也需要这个目录中的空间
/var	包括日志文件和打印假脱机的目录，这个目录中应留足几百MB自由空间。在“一切”安装中大约占210MB文件

23. 根据需要生成和删除其他分区。我生成了一系列分区，如图4.28完成之后，按F12键继续。

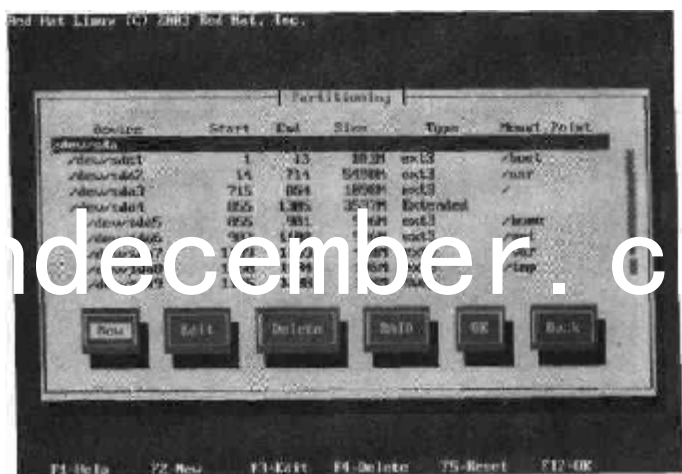


图4.28 分区配置

24. 现在可以选择引导装入器。有三个选择，如图4.29。默认为GRUB（大一统引导装入器），是第11章介绍的默认另一选项是LILO（Linux装入器），是旧版Red Hat Linux的默认。可以选择另一引导装入器，如与专属Partition Magic或System Commander程序相关的引导装入器。由于Red Hat Linux已经让LILO（Linux装入器）过时，因此要用默认GRUB引导装入器。进行选择，然后按F12键继续。

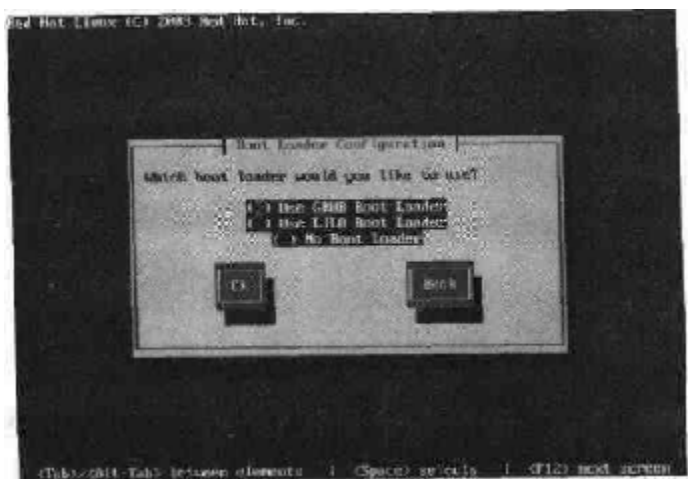


图4.29 选择引导装入器

说明：引导装入器既称为boot loader，也称为bootloader。

说明：可以用软盘作为引导装入器。但一定要在Red Hat Linux实际在系统中安装包之后在第40步建立引导盘。

25. 如果有与内核相关联的特殊参数，则可以在第二个引导装入器配置屏幕中输入，如图4.30。可以输入前面“文本方式引导”一节介绍的内核参数。Red Hat Linux也许会自动输入这些参数。例如，在第3章的相应图形屏幕中，Red Hat Linux包括hdc=ide-scsi参数，是许多IDE光驱所要求的。进行选择，然后按F12键继续。

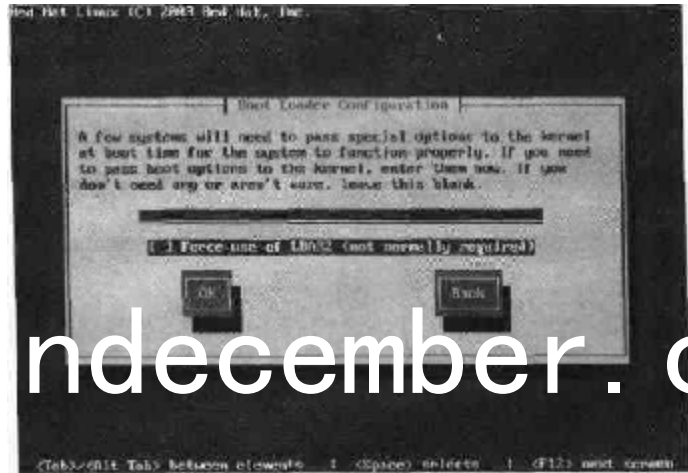


图4.30 第二个引导装入器配置屏幕

说明：通常，我们不需要激活Force Use Of LBA32选项。逻辑块寻址（LBA）使Linux可以访问硬盘上1024柱面以外的空间。它在大多数计算机上默认激活，GRUB能够自动探测。即使没有激活，也不要写，只要/boot目录所在分区在硬盘上1024柱面以内。

26. 如果使用GRUB，则可以设置口令，使用户实际访问计算机时无法在单用户方式中引导，改变根口令。这是个好主意。激活Use A GRUB Password选项并输入所要口令，如图4.31，然后按F12键继续。

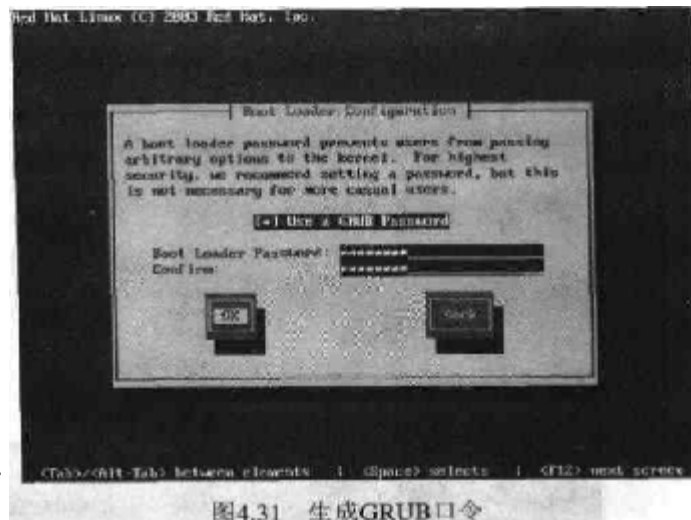


图4.31 生成GRUB口令

说明：如果口令不匹配，则会出现警告。按Enter键之后，回到原来的屏幕，可以再次输入口令。

27. 然后可以选择计算机的默认操作系统。如果只在计算机上使用Red Hat Linux，则没关系，只有一个选择。但如果Anaconda发现计算机上还有其他操作系统，则要设置默认操作系统。例如，图4.32所示的屏幕可以选择默认操作系统为DOS或Red Hat Linux。

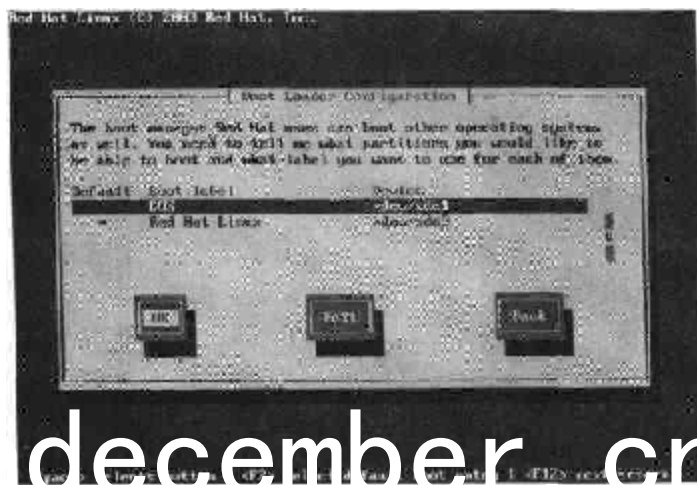


图4.32 选择默认操作系统

这里，分区/dev/sda1的操作系统是Microsoft Windows NT 4。关于这个GRUB工作的更多信息，见第11章。选择默认操作系统，用Tab键选择OK，然后按Enter键继续。

28. 然后可以设置引导装入器地址，通常应放在硬盘的主引导记录（MBR）中。但是，如果计算机上已经有另一个引导装入器，则可能要选择引导分区第一扇区（First Sector Of Boot Partition），对应于引导目录所在分区。图4.33显示了典型选择。进行选择，然后按F12键继续。

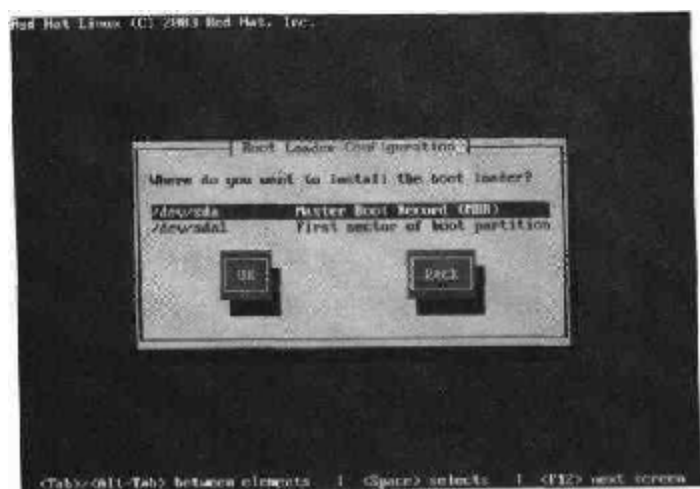


图4.33 设置引导装入器地址

说明：如果有多个硬盘，则要小心。典型PC机上的BIOS只能找到前两个IDE（hda和hdb）或SCSI（sda和sdb）硬盘上的引导目录。SCSI盘的ID号应为0或1。如果同时有IDE与SCSI硬盘，则要在第一个这些盘上，SCSI盘的ID号应为0。

29. 现在可以完成网络配置了。由于从网络服务器安装，因此已经输入这个计算机的基本IP地址信息。如果对图4.34所示设置感到满意，则可以按F12键继续（注意这里对网卡eth0进行配置）。否则取消Use BOOTP/DHCP，可以改变表4.5所示设置。

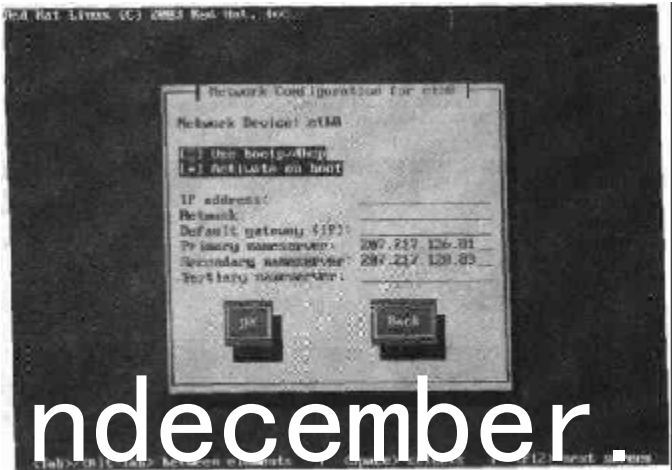


图4.34 完成网络配置

说明：如果有多个网卡，则要对下一个网卡重复第29步。

- 30. 如果设置静态IP地址，则会看到主机配置窗口，可以指定计算机的主机名。指定主机名，然后按F12键继续。
- 31. 然后可以配置计算机的防火墙。局域网内的计算机已经在防火墙保护之下，通常不需要配置防火墙。但如果在连接互联网之类另一网络的计算机上安装Red Hat Linux，则防火墙至关重要。如图4.35所示，有三个防火墙配置。本安装中配置高度安全的防火墙。加亮这个选项，然后按空格键选择。

表4.5 网络配置设置

设置	描述
Use BOOTP/DHCP	让计算机寻找本地或远程网络上的DHCP服务器，BOOTP协议可以从远程网络上的DHCP服务器取得IP地址信息
Active On Boot	选择这个选项时在引导过程中激活相关的网络设备
IP Address	配置与这个网卡相关联的IP地址，更多信息见第20章介绍
Netmask	网络掩码或子网掩码，更多信息见第20章介绍
Default Gateway (IP)	注意网络外部消息的网关IP地址，如果手工配置网卡，则可以设置这个网关
Primary Nameserver	列出网络上DNS服务器的IP地址；地址可以在局域网之外
Secondary Nameserver	列出网络上另一DNS服务器的IP地址；地址可以在局域网之外
Tertiary Nameserver	列出网络上另一DNS服务器的IP地址；地址可以在局域网之外

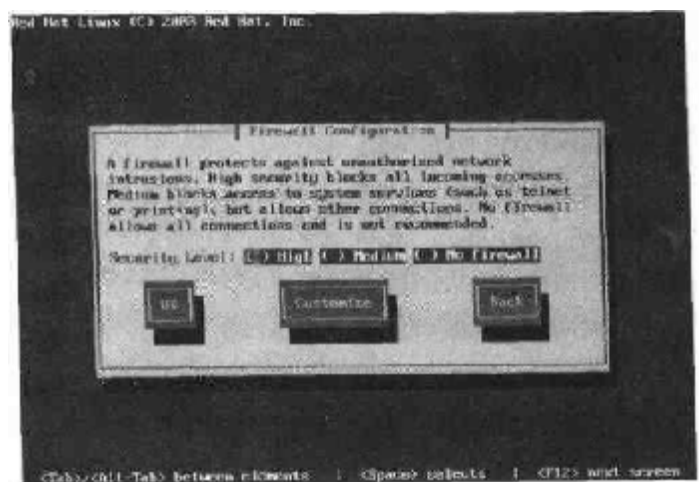


图4.35 配置防火墙

说明：即使标准Red Hat Linux高度安全防火墙也允许计算机从DNS服务器取得信息，这对浏览互联网至关重要。只要在安装过程前面至少一个nameserver指定了IP地址即可。

32. 现在来定制防火墙。它可以在第4.6节用第4.2章介绍的方法定制防火墙。选择High之后，用Tab键加亮选择Customize，然后按Enter键打开Firewall Configuration - Customize屏幕，如图4.36。表4.6列出了图中的选项。进行必要的改变，然后按F12键返回图4.35所示的基本Firewall Configuration屏幕。再次按F12键继续。

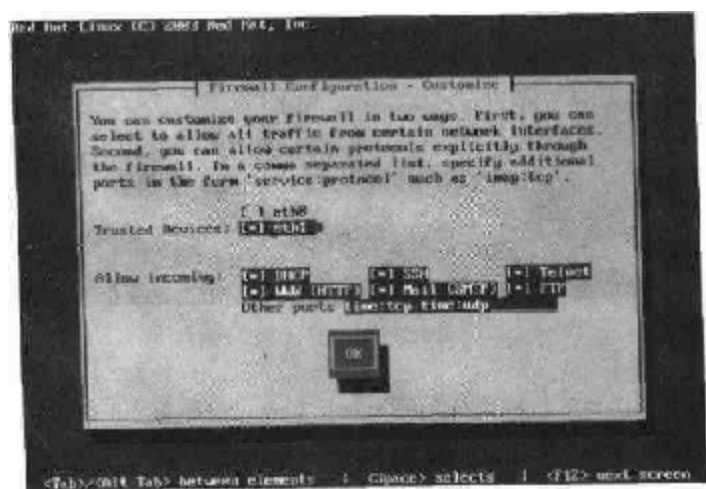


图4.36 定制防火墙

表4.6 定制防火墙的选项

选项	描述
Trusted Devices	可以激活一个网卡，作为信任设备，适用于有多个网卡时，建立的任何防火墙无法阻止任何通信流通过任何设备传递。通常对连接内部网络的网卡激活这个选项

(续表)

选项	描述
DHCP	允许输入DHCP信息, 允许外部DHCP服务器对网络上的计算机指定IP地址信息, 对BOOTP访问很重要
SSH	允许安全Shell访问, 允许用这个服务进行加密远程连接, 见第23章介绍
Telnet	允许安全Shell访问, 允许用这个服务进行明文远程连接, 见第23章介绍
WWW	允许对网络上的Web服务器进行请求
Mail	允许对网络上的发送电子邮件服务器进行请求
FTP	允许对网络上的FTP服务器进行请求
Other Ports	允许数据经过/etc/services中描述的其他TCP/IP端口, 格式为服务: 协议, 如time:tcp和time:udp

33. 这一步可以定义Red Hat Linux中安装的语言。从图4.37可以看出, 默认安装美式英语, 但支持120种不同语言和方言。如果选择Select All, 则安装所有语言的支持。如果选择Reset, 则只安装美式英语。进行选择, 然后按F12键继续。



图4.37 选择支持的语言

说明: 如果选择多个语言, 则可以看到Default Language屏幕, 可以选择系统的默认语言。

34. 然后可以选择计算机的硬件时钟设置和时区。图4.38显示了这些选项。如果选择Hardware Clock Set To GMT, 则要将PC机BIOS时钟设置为格林威治平均时间。此外, 还要选择与当地最接近的时区。

说明: 激活Hardware Clock Set To GMT选项的好处是, 后面Linux可以按夏时制调整时间。但如果计算机中有另一操作系统(如Microsoft Windows), 则这个设置会改变时钟。

35. 选择系统的根口令。我们用这个口令登录根用户或超级用户账号。如图4.39所示进行选择, 然后按F12键继续。

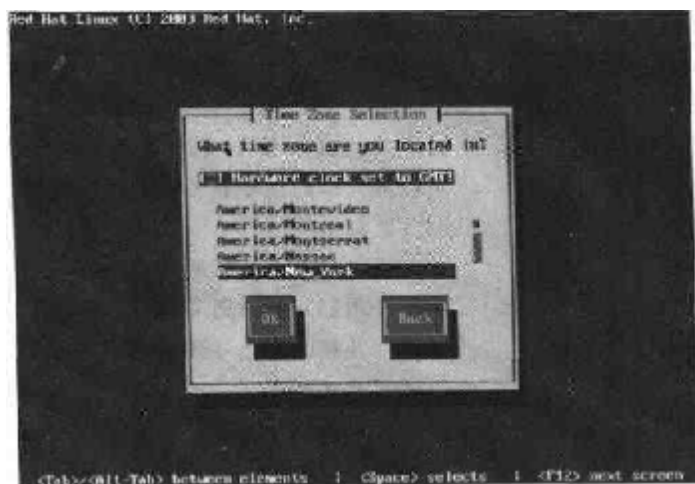


图4.38 选择时区



图4.39 生成根口令

分支步骤

第35步之后，根据安装类型的不同可能有所不同。如果第15步选择Personal Desktop或Workstation安装，则可以看到定制软件选择的屏幕。如果激活这个选项，则可以到第36步，出现图4.41所示的视图，否则跳到第39步。

如果选择定制安装，则出现图4.40的验证配置屏幕，下面列出了相关选项。

如果选择服务器安装，转入第36步。

选项	描述
Use Shadow Passwords	用/etc/shadow中的保护口令启用阴影口令组件
Enable MD5 Passwords	允许MD5形式的口令加密
Enable NIS	触发使用NIS（网络信息服务），对局域网提供用户名与口令的公共数据库，详见第28章

NIS Domain	在这个文本框中输入NIS域名
Request Server via Broadcast	选择这个选项时向网络上其他计算机发送广播消息，标识NIS服务器
Or Use:	如果关闭广播选项，则设置网络的NIS服务器名
Enable LDAP	启用验证的LDAP（轻量级目录帮助协议）和相关局域网数据库
LDAP Server	设置LDAP数据库所在服务器名
LDAP Base DN	允许用LDAP区别名（DN）查找账号信息
Use TLS Connections	让计算机用TLS（传输层）安全向LDAP服务器发送加密用户名与口令
Enable Kerberos	允许使用麻省理工学院开发的Kerberos 5系统，支持用户名与口令的强加密
Realm	允许访问Kerberos支持网络
KDC	可以访问KDC（密钥分配中心）服务器，发出Kerberos验证票据
Admin Server	允许用kadmin实用程序访问Kerberos服务器

36. 现在选择要安装的包且。如图4.4所示，可以安装类型定制了默认组，见前面的“安装选项”旁白。可以进一步定制安装，选择或取消包组。每个包组见Web上第5章详细介绍。

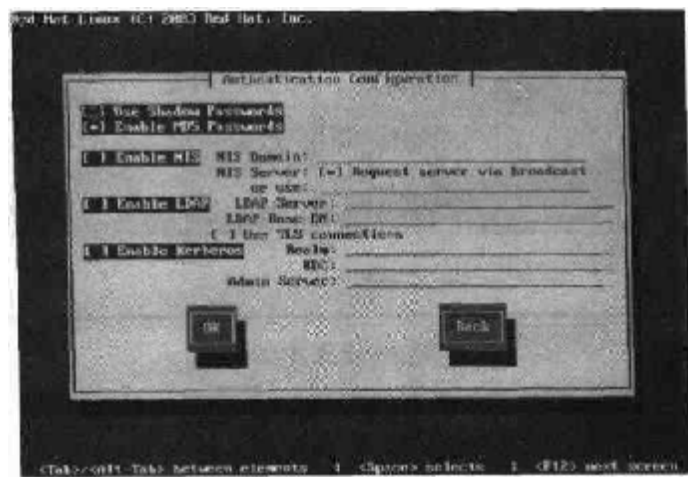


图4.40 验证配置

如果要进一步定制安装，可以激活Select Individual Packages选项。本章已经完成这个工作，转入第37步。

说明： 安装的包组不是最终的，还可以用第11章介绍的rpm命令和第19章介绍的redhat-config-packages实用程序安装各个包。



图4.41 选择安装的包组

37. 可以选择要安装的包。例如，如图4.42所示，可以在Editors包组中选择各个包。图的右边显示了每个包（及包组）的当前长度，可以帮你判断硬盘上是否有足够的空间。进行安装，然后按F12键继续。

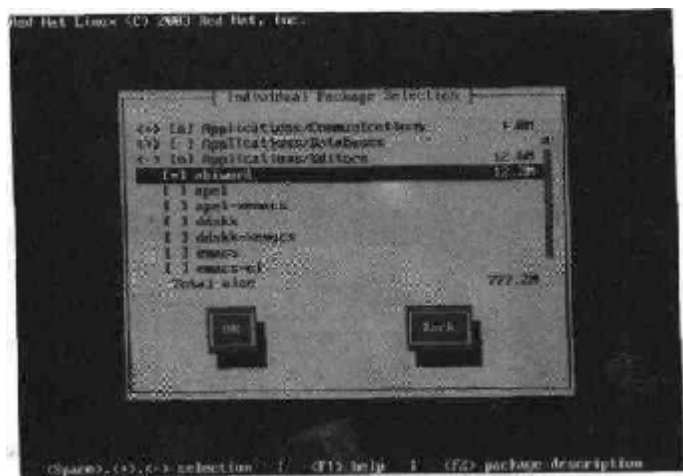


图4.42 选择各个包

38. Anaconda检查所选包的依赖性。图4.43所示的例子列出了没有满足的依赖性。从图中可以看出，要使用control-center与firstboot包，首先要安装metacity与xscreensaver包。表4.7列出了其中的选项。通常要选择Install Packages To Satisfy Dependencies选项。进行选择，然后按F12键继续。
39. 这时还有最后一次机会可以阻止Anaconda开始在系统中安装Red Hat Linux，如图4.44。文件/root/install.log包含已安装包的完整清单。如果已经准备好，则可以加亮OK按钮并选择F12键继续。

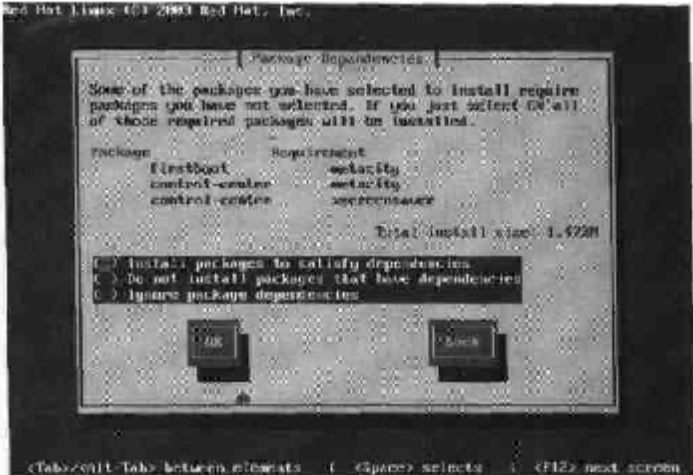


图4.43 满足包依赖性

表4.7 包依赖性选项

选项	描述
Install Packages To Satisfy Dependencies	添加安装表Requirement列中的包
Do Not Install Packages That Have Dependencies	删除安装表Package列中的包
Ignore Package Dependencies	不改变包安装表，但与相关包有关的程序可能失败



图4.44 准备安装Red Hat Linux

这时Anaconda格式化所选分区，可能要几分钟才能开始安装过程。图4.45显示了安装过程。可以跟踪当前安装状态。

安装过程完成后，Anaconda自动进行安装后配置。根据网络速度和安装的包个数与长度，整个安装过程可能要花费几分钟或几小时。最后，就可以进行下一步。

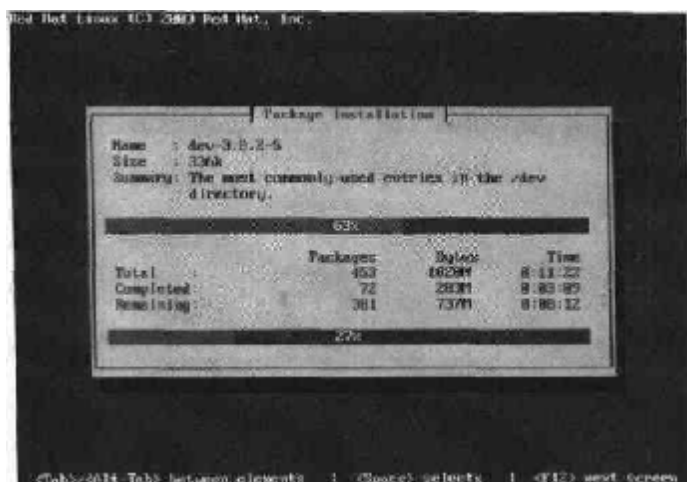


图4.45 安装过程

40. 这时可以生成引导盘，这是个好主意。如果引导装入器或主引导记录（MBR）不慎搞坏了，则可以用引导盘启动Red Hat Linux。在图4.46的菜单中，选择Yes生成引导盘。在后面的菜单中，插入软盘后选择Make Boot Disk。

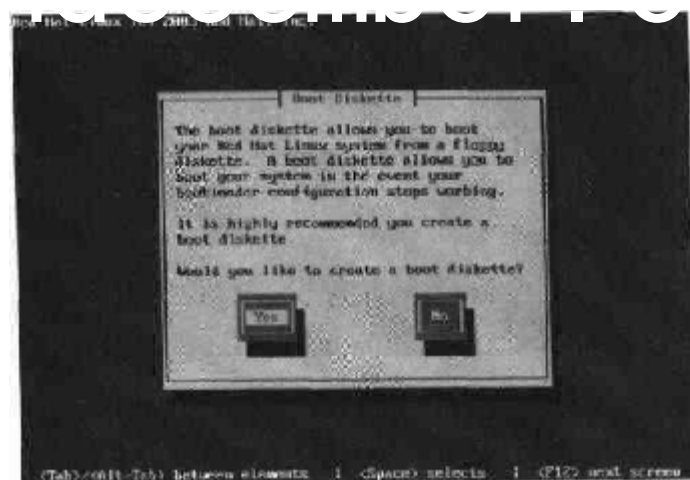


图4.46 生成引导盘

41. 下面要配置图形系统。图4.47所示的显示卡配置菜单演示了Red Hat Linux探测的显示卡信息。如果不想在此时配置图形系统，则可以选择Skip X Configuration并按Enter，转入第45步。
42. 如果对当前设置不满意，则可以改变配置。例如，可以加亮显示卡的Change选项并按Enter键打开Video Card菜单，如图4.48。
- 这里有一系列显示卡，大多数是专属的。如果找不到所要的机型和版本，则可以试用同一制造商的不同显示卡，或选择Unsupported VGA Compatible或VESA Driver（Generic）。这些选项对应于默认VGA与SVGA驱动程序。选择适当的驱动程序，然后按F12键继续。

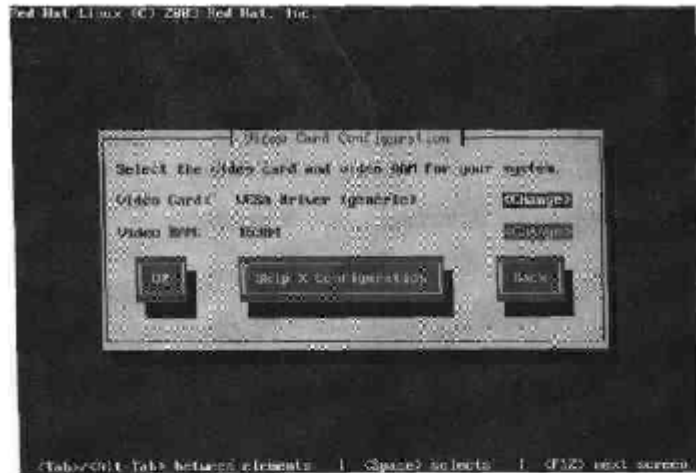


图4.47 显示卡配置菜单

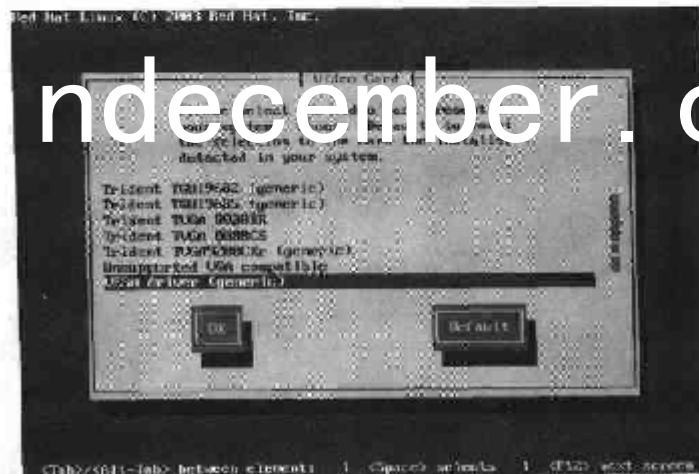


图4.48 选择显示卡

说明：VGA（显示图形适配器）标准是旧式图形卡标准，SVGA指超级显示图形适配器，红帽子的SVGA驱动程序是VESA。这些标准是VESA（显示电子标准协会）维护的，标准VESA驱动程序与SVGA显示卡相关联。

43. Red Hat Linux可能没有探测到与显示卡相关联的所有内存。这时，可以加亮显示内存的Change选项并按Enter键打开Video RAM菜单，如图4.49。选择显示卡的显示内存，然后按F12键继续，回到显示卡配置菜单。如果对整个配置感到满意，则可以按F12键继续。
44. 配置显示卡时，还要配置显示器。在图4.50所示配置显示器的屏幕中，可以指定显示器机型和版本，以及允许的水平同步率（HSync Rate）和垂直同步率（VSync Rate）。
45. 如果对当前配置不满意，则可以进行改变。例如，可以加亮显示器的Change选项并按Enter键打开Monitor菜单，如图4.51。

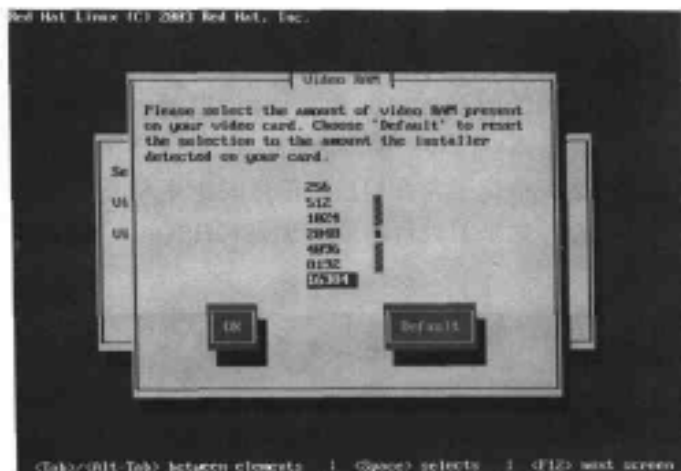


图4.49 选择显示卡的显示内存



图4.50 配置显示器

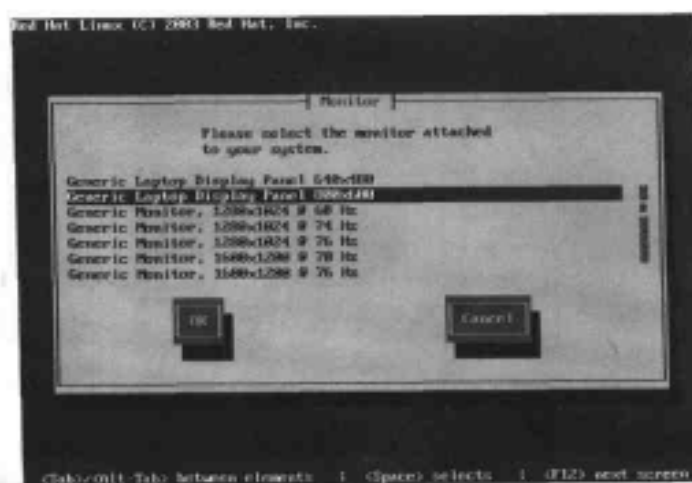


图4.51 指定显示器

可以看到这里有一系列显示器，大多数是专属的。如果找不到所要的机型和版本，则可以试用同一制造商的不同显示卡，或选择各种一般性显示器，包括几种便携电脑的显示器。选择适当的驱动程序，然后按F12键继续，回到显示器配置屏幕。

46. 然后要改变允许的显示器同步率，如图4.52。水平同步率是系统在屏幕中重画一条水平线所要的时间量，单位通常用kHz；垂直同步率是系统重画整个屏幕所要的时间量，单位通常用Hz。如果要进行改变，加亮与HSync和VSync Rates相关的Change选项并按Enter键。

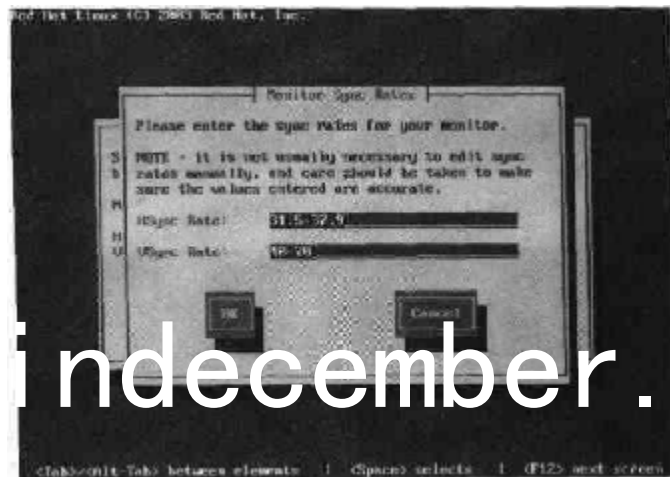


图4.52 设置显示器同步率

警告：一定要小心，尽量查阅显示器文档。如果指定的水平或垂直同步率太高，则显示卡发出的信号可能永久损坏显示器。

根据需要改变显示器同步率，然后按F12键回到Monitor屏幕。如果对整个配置感到满意，则可以按F12键继续。

47. 然后要指定几个默认值。如图4.53的X定制菜单所示，可以指定颜色深度、分辨率和默认登录方式。



图4.53 选择图形启动默认

48. 如果对当前配置不满意, 则可以进行改变。例如, 可以加亮显示器的**Change**选项并按**Enter**键打开**Color Depth**菜单, 如图4.54。选择所要的颜色深度并按**F12**键回到**X**定制菜单。

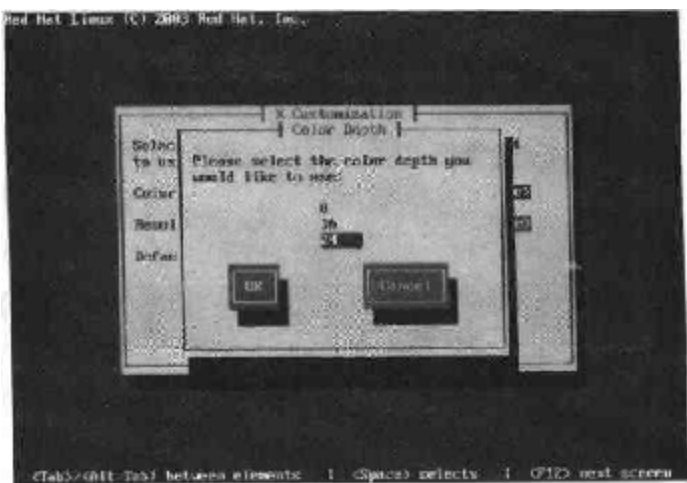


图4.54 选择所要的颜色深度

49. 现在可以改变分辨率, 如图4.55。加亮选择所要分辨率, 然后按**Enter**。

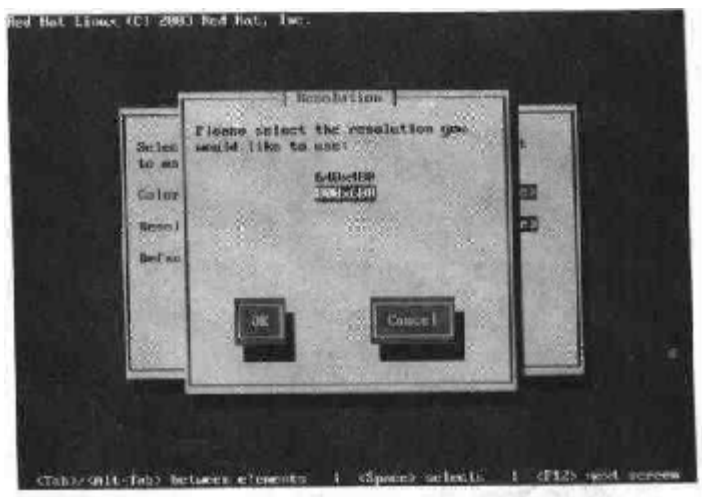


图4.55 选择所要分辨率

分辨率基于显示卡内存、指定的颜色深度和显示器规范。选择所要分辨率, 并按**F12**键回到**X**定制菜单。

50. **X**定制菜单中还可以改变Linux系统的默认登录方式, 其改变/etc/inittab文件中的默认运行级, 见第11章介绍。可以设置成文本或图形控制台登录。图形控制的视图见第15章。进行选择, 然后按**F12**键继续。
51. 最后, 安装与基本配置已经完成, 可以看到图4.56所示屏幕。按**Enter**键时, **Anaconda**重新启动计算机。重新启动计算机之后, 可以看到选择的引导装入器。

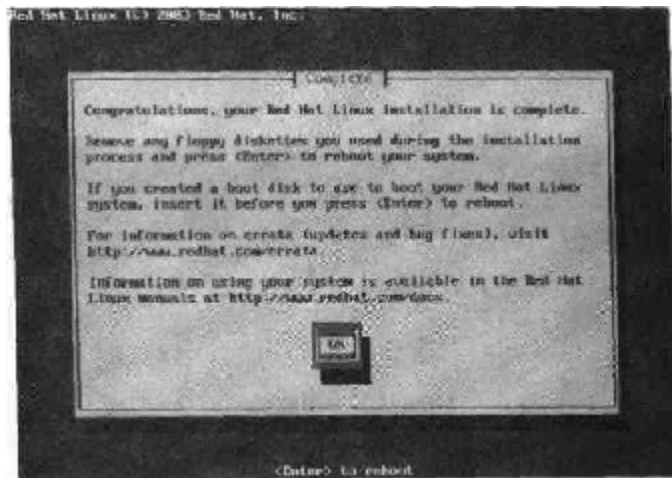


图4.56 安装完成

说明：如果第50步配置成在图形控制中登录，则Red Hat Linux重新启动并打开firstboot实用程序。步骤和视图与第3章末尾，“红帽子安装主体”一节介绍的相同。

文本方式升级

还可以升级旧版Red Hat Linux。如果Anaconda探测到旧版本，则会打开System To Upgrade菜单，前面在安装过程的第14步已经见过。为了方便起见，图4.57重复这个菜单。这里不准备介绍详细步骤，因为这些详细步骤与文本方式安装中大致相同。

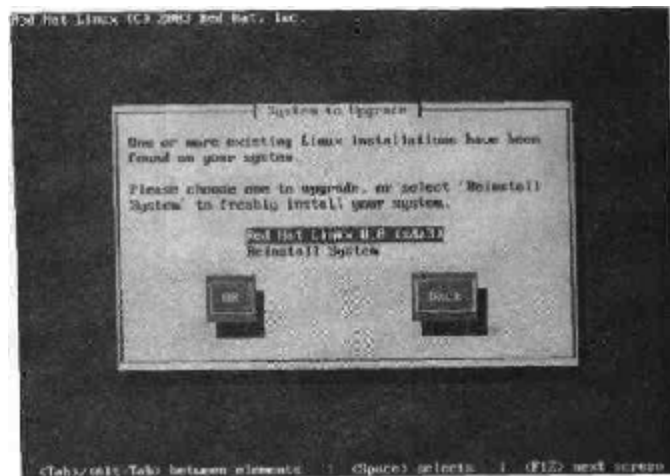


图4.57 System To Upgrade菜单

这时，Anaconda发现引导目录`/dev/sda3`分区中安装的Red Hat Linux 8.0相关联。如果只要将包升级到Red Hat Linux 9，则可以选择这个选项并按F12键继续。

说明：如果旧版Linux的分区格式化为第二扩展文件系统（ext2），则升级时可以将其转换成RH Linux 9的默认第三扩展文件系统（ext3）。关于文件系统的更多信息，见第7章介绍。

然后可以选择是否定制要升级的包。例如，如果从Red Hat Linux 7.2升级，则可能没有准备将Web服务器从Apache 1.3.x改成2.0.x。这时，就要定制升级，如图4.58。否则Anaconda自动安装新版包（如有）。进行选择，然后按F12键继续。

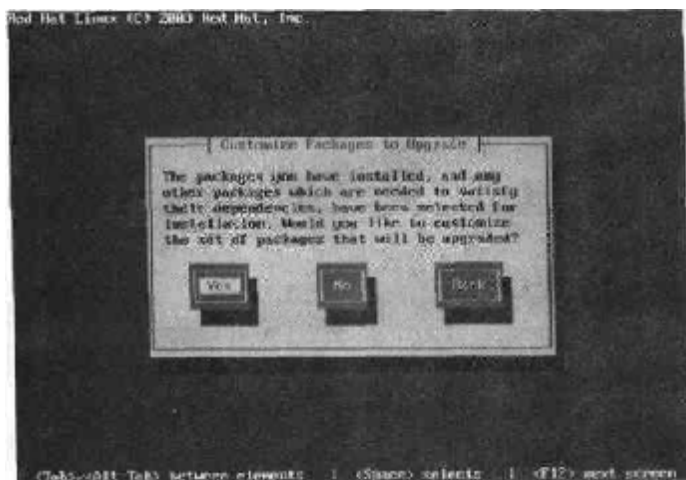


图4.58 定制要升级的包

后一个屏幕可以升级或新装引导装入器。如图4.59所示，有三个选项，见表4.8。如果有特殊引导装入器配置文件（如具有特殊内核项目），则不能用Create New Boot Loader Configuration选项将其删除。

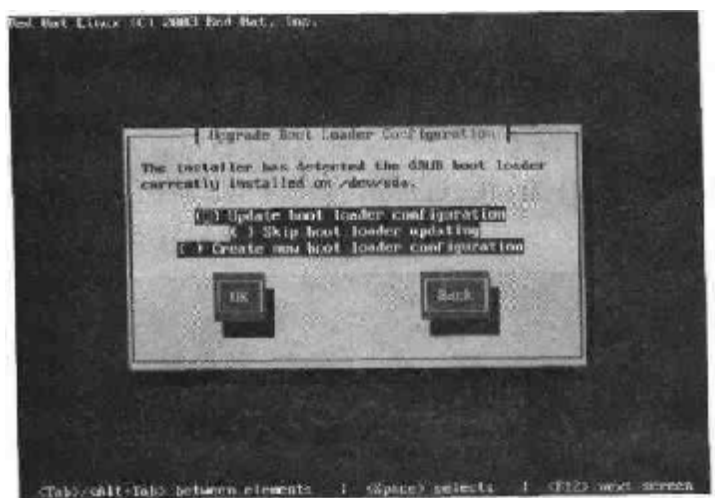


图4.59 升级引导装入器

表4.8 引导装入器升级选项

选项	描述
Update Boot Loader Configuration	升级引导装入器包而不改变配置文件
Skip Boot Loader Updating	不升级引导装入器包也不改变配置文件
Create New Boot Loader Configuration	升级引导装入器包而且改变配置文件

我们选择第一个选项。进行选择, 然后按F12键继续。假设定制要升级的包, 则Anaconda会读取系统中的当前包, 这个过程在我升级不带GUI的Red Hat Linux 8.0系统时花掉了大约20分钟。

完成升级评估过程后, 进入Individual Package Selection屏幕, 如图4.60。这个菜单中选择的包只限于计划的更新。例如, 从图中可以看到, 对这个特定系统, Anaconda升级ash shell。

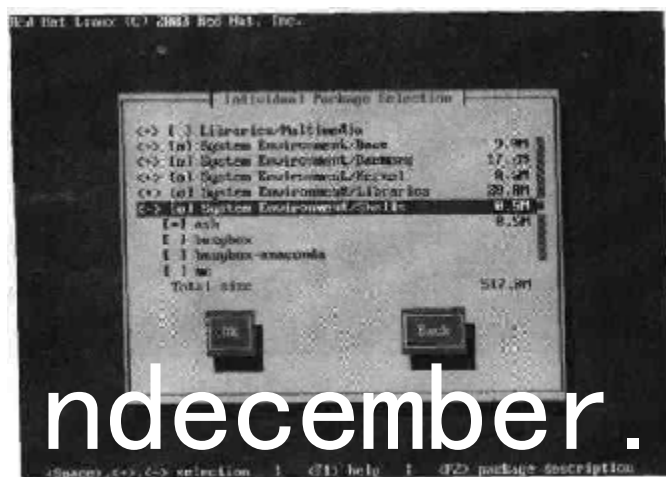


图4.60 升级与选择包

可以选择与取消各个包。如果升级服务器, 则要特别注意System Environment/Daemons类别。如果有Apache与Samba之类的可靠服务, 则至少目前不一定要升级。进行所要的改变, 并按F12键继续。

Anaconda检查依赖性。如果发现, 则完成与图4.43相似的过程。这个过程可能要几分钟。完成之后, 出现Upgrade To Begin屏幕, 如图4.61。按F12键之后, Anaconda即开始升级过程。

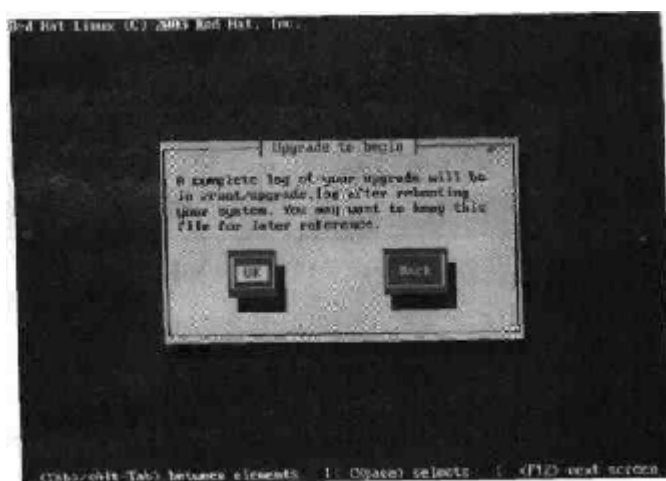


图4.61 开始升级过程

查错网络安装

如果无法通过网络安装Red Hat Linux, 则可以检查几个地方。第一, 大多数网络问题都是物理问题。Red Hat Linux默认安装一个防火墙, 这个防火墙也可能出问题。如果没有正确的地址设置, 则计算机无法找到安装服务器。最后, 还有一些便携电脑通过网络安装Red Hat Linux的特殊问题。

检查消息

如果Red Hat Linux安装遇到问题, 问题甚至可能与网络无关。几个文本安装屏幕可能提供了重要消息。可以按Ctrl+Alt+Fn命令取得这些消息, 其中n是虚拟控制台号码: 1、2、3、4、5或7。表4.9列出了安装屏幕。

表4.9 红帽子安装屏幕

屏幕	描述
Ctrl+Alt+F1	检查本地显示卡、显示器和鼠标的探测消息
Ctrl+Alt+F2	打开具有各种命令功能的it is shell, 例如, df命令可以显示表制目录和分区, 其他bash命令见本书第6章、第7章和第8章介绍
Ctrl+Alt+F3	浏览安装日志, 包括与硬件探测相关联的消息, 这里还有读光碟和装入驱动程序时的问题
Ctrl+Alt+F4	转入系统消息日志, 包括格式化与装载分区目录之类的消息
Ctrl+Alt+F5	显示其他消息, 如文件系统标题、块、格式和杂志

检查网络

大多数网络问题都是物理问题。如果网络无法工作, 则首先要检查电缆、连接和其他硬件问题。

可以用几个命令测试物理条件。例如, 对另一计算机的IP地址使用ping命令, 可以测试两台计算机之间的连接。第21章介绍了基本网络查错方法。

服务器上的防火墙

Red Hat Linux默认安装防火墙。但如果接受默认安装, 则无法从这个计算机访问安装文件, 至少无法用本章介绍的网络协议(NFS、HTTP与FTP)访问。如果仍然有网络问题, 则应该登录和检查服务器计算机中的Red Hat Linux安装文件。

如果服务器也运行Red Hat Linux 7.3以上, 则可以用两个命令检查防火墙:

```
# iptables -L
```

这个iptables命令列出该计算机当前采用的任何规则。如果有现有规则, 则可以用下列命令从当前配置中将其“刷新”:

```
# iptables -F
```

安装完成后，可以用`service iptables restart`命令重新启用防火墙。防火墙见第22章详细介绍。

地址设置

不太熟悉IP地址的用户可能出错。例如，如果对计算机设置静态IP地址，则要保证几个事项正确：

- 计算机IP地址应与局域网在同一网络上。
- 计算机网络掩码（或子网掩码）应符合局域网中每台其他计算机。

尽管有正确的默认网关和DNS服务器IP地址很方便，但这不是成功地通过网络安装Red Hat Linux所必需的。关于IP地址的详细工作方法，见第20章介绍。

通过网络安装到便携电脑

通过网络安装到便携电脑时通常不会有问题，但与标准网络安装有一定差别。便携电脑网卡通常在PC卡槽上（也称为PCMCIA，基于个人计算机内存卡国际协会的标准）。

PC卡要求自己的驱动程序，从`pcmciaadd.img`文件生成的驱动程序盘装入。本章前面曾介绍过，驱动程序映像文件位于第一张Red Hat Linux安装光碟的`/images`目录中。

有许多PCI/CLM网卡，Red Hat Linux驱动程序集中的文件不一定能够满足它们的要求。例如，既要有PCMCIA槽，又要有PCMCIA网卡。如果遇到问题，可以用`Ctrl+Alt+F3`命令打开安装日志屏幕，可以从这里找到问题。

小结

本章通过网络安装Red Hat Linux。需要另一台计算机保存安装文件。我们介绍了配置三种网络服务的过程：NFS、HTTP与FTP。具体步骤很简单，每个服务的细节见后面章节介绍。

然后我们介绍了引导盘和驱动程序盘的各种选项，并介绍了文本方式安装过程的详细步骤，还简要介绍了升级过程。

如果网络安装遇到问题，则可以从安装消息屏幕找到线索。如果是网络问题，则通常是物理问题，还可以用几个命令检查网络。一个常见的错误是安装服务器中的活动防火墙阻止通信流。另一个常见的错误是IP地址信息错误。最后，通过网络安装到便携电脑时可能发生特殊问题。

下一章介绍Kickstart自动安装过程。一旦建立Kickstart文件之后，就可以用相同的网络安装服务器同时在几台计算机上安装Red Hat Linux。

第5章 用Kickstart安装Linux

前面几章介绍了Linux的本地安装与远程安装。可以用多种方法定制Red Hat Linux，都要求大量的用户输入。这样，管理员负责在一组计算机上安装Red Hat Linux时，要花大量时间在这组计算机上安装和定制Linux。为此，红帽子公司开发了Kickstart系统，可以将安装过程自动化。利用Kickstart系统，可以管理每台计算机上的包组安装和各个RPM包。

第3章和第4章曾介绍过，包集成组，如GNOME Desktop Environment与Graphics组。这些包组被组织在第一张Red Hat Linux安装光碟/RedHat/base目录的comps.xml文件中。我们将详细介绍这个文件，可以编辑这个文件，定制用户安装Red Hat Linux的方式。

我们已经介绍过依赖性。一些包和包组中的软件要安装了另一些软件时才能工作。这些依赖性也记录在comps.xml文件中。

在计算机上安装Red Hat Linux 9时，Anaconda在/root目录中留下一个默认Kickstart文件anaconda-ks.cfg。可以用这个文件对其他计算机生成标准Kickstart文件。此外，红帽子公司还提供了一个GUI Kickstart Configuration，可以轻易地根据需要定制Kickstart文件。

生成Kickstart文件之后，可以在引导盘上设置这个文件。只要用软盘重新启动计算机。一旦装入基本内核之后，就可以在本地或通过网络安装Red Hat Linux。本章介绍下列主题：

- 用comps.xml文件组织包
- 分析默认Kickstart文件
- 使用GUI Kickstart Configurator
- 从软盘执行Kickstarting

用comps.xml文件组织包

Red Hat Linux安装程序Anaconda用comps.xml文件设置安装。这个文件位于第一张安装光碟或网络源的/RedHat/base目录中，是用XML编写的，XML主要用于Web页面，它的标志类似于Web页面的标准语言HTML。

说明：安装Red Hat Linux之后（在标准Intel类型PC机上），还可以在/usr/share/comps/i386目录中找到comps.xml文件。如果可能，在文本编辑器中打开这个文件，按照本章这个部分的内容学习。

comps.xml文件分成四大段。第一段是强制包组，通常是每个Red Hat Linux安装都要安装的，然后是安装过程中可以选择的各个包组。第三，这些组按类别组织，可以在图形安装过程中看到，也可以用第19章介绍的redhat-config-packages实用程序检查。最后，还有一列依赖性，是其他包所需要的包。

了解comps.xml文件之后，可以编辑这个文件。例如，可以增加一段自己的特殊包组，也可以删除或隐藏不让用户在计算机上安装的包组，如图形和游戏。

说明：Red Hat Linux是通过红帽子包管理器（RPM）组织的，红帽子软件集合在扩展名为.rpm的RPM文件中。comps.xml文件中组织RPM包时，按包组来组织。

基本comps.xml段

comps.xml文件中每一段有一个标准组织。和HTML文件一样，每一段有开始标志（如<group>）和结束标志（如</group>）。每一组有个标识符，例如：

```
<id>dialup</id>
```

然后下面几行确定用户是否可以选这个组，这个组是否默认安装：

```
<uservisible>>false</uservisible>
```

```
<default>>true</default>
```

这些组合表示这个特定组是默认安装的。由于安装过程中用户无法看到这个包组，因此Anaconda自动安装这个包组。

如果看不到这两个标志，则<uservisible>为真，<default>为假。换句话说，显示相关包组，但安装过程中不能选择。

每个组有一个名称和一个描述，comps.xml文件包括不同语言的版本。这些命令列出KDE包组名（用德语名称），并使用同一语言的缩写描述：

```
<name>KDE Desktop Environment</name>
```

```
<translatable:lang="de">KDE Desktop Umgebung</translatable:lang>
```

```
<description>IDesktopumgebung</description>
```

有些包组其有依赖性。例如，图形组依赖于base与base-x组，表示为下列命令（我们为了简洁起见而省略了几个命令）：

```
<group>
  <id>graphics</id>
  <name>Graphics</name>
  <grouplist>
    <groupreq>base</groupreq>
    <groupreq>base-x</groupreq>
  </grouplist>
</group>
```

最后，每一组有相关的包，用<packagelist>标志表示。有些包是强制的（mandatory），即没有它不行。例如，如果没有samba-client与samba RPM包，则Windows File Server包组无法工作：

```
<packagelist>
  <packagereq type="mandatory">samba-client</packagereq>
  <packagereq type="mandatory">samba</packagereq>
</packagelist>
```

有些包是默认的或可选的。安装过程中选择各个包的用户可以选择或取消这些包。

最后，大多数comps.xml文件包括一系列相关性。例如，下面是第26章介绍的m4宏处理器的一系列相关性：

```
<package>
  <name>m4</name>
```



```

<dependencylist>
  <dependency>bash</dependency>
  <dependency>info</dependency>
  <dependency>glibc</dependency>
</dependencylist>
</package>

```

除非知道具体意图，否则不要去编辑相关性表，否则安装的程序可能缺少必要的基本软件，如shell和语言编译器。

强制组

comps.xml文件中有两个强制包组：Core与Basic。核心组包括Linux中不可或缺的RPM包，表5.1列出了一些核心Linux包，完整清单见Web上第5章，在Sybex公司Web站点www.sybex.com。

表5.1 一些核心Linux包

包	描述
bas-sysinit	Red Hat Linux中安装的第一个包，永远不能删除
bash	Novell Argon Shell默认Red Hat Linux命令解释器
cpio	档案实用程序，见第14章介绍
e2fsprogs	基本Linux文件系统管理命令
filesystem	标准目录布局
glibc	标准C语言库
grub	默认Linux引导装入器，见第11章介绍
hotplug	用于USB与IEEE 1394设备
iputils	包括ping之类的基本网络命令的包
kbd	用于管理控制台、字体和键盘
kernel	Linux内核
libgcc	支持GNU C语言编译器的包
passwd	包括passwd命令的包
procps	系统信息实用程序，如ps
raidtools	用于配置软件RAID设备
rpm	包括红帽子包管理器（RPM）的包，见第10章介绍
setup	一些基本/etc配置文件，如passwd、group、profile
vim-minimal	vi编辑器

基本组中的RPM包使Red Hat Linux对管理员有用。表5.2列出了其中几个包，完整清单见Web上第5章。

表5.2 一些基本Linux包

包	描述
at	支持at与批处理命令，见第13章介绍
bind-utils	包含检查DNS服务器的命令，见第24章介绍

(续表)

包	描述
crontabs	用于经常性计划任务, 见第13章介绍
dhclient	包含DHCP (动态主机配置协议) 客户机
ftp	包含FTP (文件传输协议) 命令行客户机
kudzu	包含红帽子硬件探测工具
nfs-utils	包含NFS (网络文件系统) 命令, 见第28章介绍
openssh-clients	用于SSH (Secure Shell) 客户机连接
quota	可以设置配额, 见第9章介绍
sudo	可以对某些用户配置根权限
telnet	包含Telnet命令行客户机
up2date	包含红帽子更新主体, 见第10章介绍
ypbind	包含NIS (网络信息服务) 客户机, 见第28章介绍

这些包组加起来将近有450MB文件。comps.xml文件中还有一组总是要安装的, 就是拨号网络支持 (Dialup Networking Support)。下面看看Red Hat Linux安装过程中看到的其他包组。

包组

本节详细介绍每个包组, 帮你确定计算机上要安装的软件包集合。每个组中完整的包清单见Web上第5章介绍。

Red Hat Linux安装过程中不一定能看到所有这些组, 前面曾介绍过, 可以将comps.xml配置成不显示一个或几个组。

本节的包顺序对应于编写本书时comps.xml文件中的顺序, 发布Red Hat Linux 9时可能会有所改变。这个顺序与Red Hat Linux安装过程中看到的顺序不同。

有些包组依赖于其他包组。例如, 要使用Office/Productivity包组, 就要先安装X Window System包组。这个组中的一个组件OpenOffice还要求安装另外几个包, 见comps.xml文件依赖性部分。

打印支持

也许令人奇怪的是, 打印支持包放在comps.xml文件的这么前面。这个包中相关的字体是GUI中需要的, 打印支持还包括与CUPS和LPD服务相关的基本驱动程序和实用程序, 见第25章介绍。这个组默认安装。

X窗口系统

X Window System包组包括XFree86 Server和Linux计算机上配置GUI所要的相关包, 包括一些基本redhat-config-*实用程序, 用于管理日期、网络、服务运行级配置、声音、用户、打印机和X窗口。

如果要安装GNOME与KDE之类的桌面, 则需要这个包组。这个组默认安装, 要用到打印支持包组, 主要是用它的字体。

comps.xml中的其他命令可能用ID引用这个组。例如，下列命令引用X窗口系统包组的<id>:

```
<id>base-x</id>
```

拨号网络支持

Dialup Networking Support包组包括基本文本实用程序，用于通过电话调制解调器连接。其他GUI互联网连接实用程序要用到这个包（见第16章、第17章和第21章）。这个包组总是在Red Hat Linux 9中安装。

GNOME桌面环境

GNOME Desktop Environment包组包含运行GNOME桌面环境所需的软件，包括文本编辑器、计算器之类的基本应用程序。

如果用户需要GUI环境，则要安装GNOME与KDE，为此还要安装X窗口系统包组。GNOME是默认Red Hat Linux桌面，见第16章介绍。

KDE桌面环境

KDE Desktop Environment包组包含运行KDE桌面环境所需的软件，包括文本编辑器、计算器之类的基本应用程序。和GNOME桌面环境中一样，要安装X窗口系统包组。KDE是其他Linux发行版本中最常见的桌面，见第17章介绍。

Graphical Internet

Graphical Internet包组包括与互联网连接相关的基本GUI实用程序，包括Mozilla Web浏览器和Evolution邮件管理器，以及几个聊天和相关实用程序。尽管本书不是关于GNOME与KDE的，但其中许多实用程序都会在第16章到第18章介绍。

Text-Based Internet

还有许多实用程序可以在文本控制台连接互联网。例如，lynx是个Web浏览器，具有丰富的特性，pine是个过时的电子邮件客户机，已经被mutt取代。

声音与视频

Sound and Video包组集中了声卡的控制、配置与命令功能，包括几个工具，可以在光碟和DVD上录制数据和多媒体。

图形

Graphics包组中的几个实用程序可以管理图片、屏幕图形和其他图形，包括GIMP和相关数据，见第18章介绍。GIMP大量用于生成本书的屏幕图形。

如果需要图形，显然还要安装X窗口系统包组。

办公/生成

Office/Productivity包组包括两组特性丰富的办公组件OpenOffice与Koffice，还包括与GNOME Office相关联的办公室应用程序，以及另外几个应用程序，如项目管理器。这些组件见第18章介绍。

邮件服务器

mail servers包组包括几个邮件服务器。可选包可以帮助管理讨论清单、过滤不要的电子邮件，等等。关于sendmail与IMAP邮件服务器的更多信息，见第26章。

网络服务器

Network Server包组中的各种服务器可以管理局域网。这些网络服务器包括DHCP（管理IP地址信息）和telnet-server（接受Telnet连接），等等。关于这些网络服务器的更多信息，见本书第五部分到第七部分。

新闻服务器

News Server包组只有一个包InterNetNews（inn）。这个服务器可以建立一个新闻服务器，相当于Usenet讨论清单服务器。可以通过邮件管理程序访问。从com.us.rn中检查依赖性表时，可以看到inn还要求inews包的新闻。

Windows File Server

Windows File Server包组也很简单，只要用samba与samba-client包连接Microsoft Windows-based网络和与网络上其他计算机共享。检查依赖性表时，可以看到它要求samba-common RPM包。Samba将在第29章详细介绍。

服务器配置工具

红帽子公司最近建立了几个配置工具，以redhat-config-*开头，其中*表示功能。Server Configuration Tools包组可以用这些配置工具配置几个服务器。虽然comps.xml中没有指定，但大多数配置工具都要求运行X窗口界面。

说明：一个不要求运行X窗口界面的工具是redhat-config-xfree86，它从普通命令行界面建立自己的GUI。

FTP服务器

FTP Server包组很简单，包括一个Very Secure FTP Daemon包，可以设置具有不同安全级的FTP服务器。FTP配置将在第23章介绍。

SQL数据库服务器

SQL Database Server包组可以运行使用结构化查询语言（SQL）的数据库服务器。提供的数据库服务器PostgreSQL与MySQL都是关系型数据库服务器的基础。这些服务器没有在本书介绍，详见Ian Gilfillan的著作“Mastering MySQL 4”（Sybex公司出版，2002，该书中文版已由电子工业出版社出版，书名为《MySQL 4从入门到精通》）。

Web服务器

Web Server包组有两个不同的Web服务器Apache (httpd) 与TUX, 见第30章介绍。这个包组还有几个Apache模块。

DNS名称服务器

DNS Name Server包组有两个包: bind是Linux上的标准DNS服务器, caching-nameserver包支持计算机上的DNS服务器缓冲。DNS见第24章介绍。

写作与发表

Authoring and Publishing包组包括Linux的自然发表格式DocBook, 这是标记文本文件的格式, 可以将文档转换成几种不同格式, 包括HTML、RTF与TeX。DocBook系统不在本书介绍, 详见“DocBook: The Definitive Guide”, Reilly公司出版。

工程与科学

Engineering and Scientific包组包括一系列计算包, 有些与线性代数有关, 帮你解复杂方程。由于本书不是工程专著, 因此不准备介绍这些包。

编辑器

Editors包组中有两个最常用的Linux文本编辑器: vi和Emacs。如果安装Emacs或GUI版本xemacs, 则Red Hat Linux自动安装相关的包组。介绍这些编辑器的专著很多。第6章将简要介绍vi。

关于Emacs的更多信息, 见“GNU Emacs Manual”, 作者Richard M. Stallman (GNU出版, 2002)。

Emacs

Emacs组包括Emacs文本编辑器和几个编辑LISP与SGML语言的包。

Xemacs

Xemacs组中的三个包使Emacs可以在GUI中工作。

系统工具

System Tools包组中有各种客户机和诊断软件。例如, 第22章将会介绍, Ethereal可以在网络上阅读明文消息。第29章将会介绍, 可以用几个与samba-client相关的工具阅读Microsoft Windows-based网络上的共享目录。

管理工具

Administration Tools包组中的redhat-config-*实用程序不能放进其他组中, 包括各种工具, 如键盘配置和用户管理工具。关于这些管理工具的细节, 见第19章。

游戏

Linux中的游戏可以在GUI中安装。我个人不安装游戏，因为或对这些简单游戏兴趣不大。但是，有些管理员认为游戏能帮助新用户更快熟悉Linux。这个games包组中包括与GNOME和KDE桌面相关联的游戏。

ISO8859支持

可以安装两个不同的ISO8859字体集。ISO8859-2与东欧语言相关，ISO8859-9与土耳其语相关。这些组中包括75和100dpi（每英寸点数）的字体。

说明：ISO是国际标准化组织（www.iso.ch）。奇怪的是，这个缩写不符合其正式称呼（法文版称呼）。

各个语言支持

还有另外几个包组，可以按自然语言使用Linux。每个语言组都有字体，可能还有拼写检查器和翻译的手册页。到本书编写时，支持西西里字母、巴西葡萄牙语、英式英语、加拿大英语、卡特兰语、中文、捷克语、丹麦语、荷兰语、爱沙尼亚语、芬兰语、法语、德语、希腊语、希伯来语、匈牙利语、冰岛语、意大利语、日语、朝鲜语、挪威语、波兰语、葡萄牙语和乌克兰语。

说明：其中一些语言要求不同字体，例如乌克兰语要求西西里字母包、土耳其语要求ISO8859-9包。

开发工具

如果要进行任何软件开发工作，则至少需要Development Tools包组中的一些包。尽管本书不是介绍编程的，但第12章也要用到这个包组中的一些包来编译Linux内核。

其中automake包可以生成Makefile式配置脚本，binutils包可以包括二进制管理实用程序，gcc是个GNU C语言编译器。这个包组还要求安装开发库包组。

开发库包组

Development Libraries包组中的各种开发程序具有广泛用途。这些库包括kudzu-devel（支持红帽子硬件管理实用程序）和openssl-devel，后者可以配置SSH服务器，见第23章介绍。如果要改进任何这类应用程序，则可能要安装这个包组。

内核开发

如果准备修改或重新配置Linux内核，则要安装Kernel Development包组。这个包组中包括kernel-source包，这个包组还要求安装开发工具包组。关于这些包和管理内核的更多信息，见第12章。

遗留软件开发

红帽子公司最近升级了GNU C语言编译器。如果要使用需要旧版包的软件，则可以使用kernel-source包组中的遗留包。

X软件开发

如果使用XFree86软件,则可能要安装X Software Development包组。这个组中的包可以对X窗口系统开发应用程序。由于还有其他桌面,因此这个组不要求与GNOME或KDE软件开发包组相关的软件。

GNOME软件开发

如果对GNOME桌面开发应用程序,则要安装GNOME软件开发包组。其中两个关键的包是gtk+-devel, The GIMP工具库(GTK+)和fontconfig-devel,用于管理桌面字体。尽管GTK+是对The GIMP建立的,但也可以开发GNOME应用程序。

KDE软件开发

如果对KDE桌面开发应用程序,则要安装KDE软件开发包组。其中两个关键的包是cups-devel与qt-devel,前者用于CUPS打印服务器,后者用于Qt语言工具库。Qt是GTK+工具库的KDE版本,用于开发KDE应用程序。

说明: Qt是个C++语言工具库,可以生成GUI应用程序,是 TrollTech (www.trolltech.com) 开发的,与苹果公司的QuickTime无关。这里的Qt不是QuickTime的缩写。

包组类别

comps.xml文件将每个包组分成几个类别,第3章已经介绍了这些类别的用法。表5.3列出了标准包组类别。

表5.3 包组类别

类别	描述
Applications	可以安装各种包组,包括Graphical Internet, Editors与Office Suites
Desktops	配置X窗口和GNOME与KDE桌面环境的安装
Development	可以增加各种开发工具包组
Servers	可以选择不同服务器包组,包括web, mail与FTP服务
System	可以设置管理员或系统工具与打印支持

例如,桌面类别中的包组如下,可以在计算机上安装GUI时使用:

```
<category>
  <name>Desktops</name>
  <subcategories>
    <subcategory>base-x</subcategory>
    <subcategory>gnome-desktop</subcategory>
    <subcategory>kde-desktop</subcategory>
  </subcategories>
</category>
```

桌面类别包括base-x、gnome-desktop与kde-desktop。根据<id>变量(在comps.xml文件开头),这对应于下列包组: X Window System, GNOME Desktop Environment和KDE Desktop Environment。

依赖性

依赖性就是一个软件包（如内核源代码）的工作要求安装另一个包（如C语言编译器）。依赖性是在comps.xml文件的重要部分。例如，下列段列出了XFree86-75dpi-fonts包的三个依赖性：

```
<package>
  <name>XFree86-75dpi-fonts</name>
  <dependencylist>
    <dependency>bash</dependency>
    <dependency>XFree86-font-utils</dependency>
    <dependency>chkfontpath</dependency>
  </dependencylist>
</package>
```

通常，Red Hat Linux不安装XFree86-75dpi-fonts包，除非已经安装bash shell，安装字体的XFree86-font-utils和配置字体目录的chkfontpath包。

Anaconda开始安装Red Hat Linux之前，要先检查所有依赖性。这里，如果还没有安装依赖的包，则Anaconda会选择要安装的包，然后可以接受或拒绝Anaconda的选择。

编辑例子

可以生成自己的组。例如，Red Hat Linux光碟中不再包括Netscape。但如果你下载或安装了Netscape RPM，则可以将其放进网络安装的/RedHat/RPMS目录中。

然后可以增加下列命令，生成Netscape组：

```
<group>
  <id>netscape</id>
  <name>Netscape Browser</name>
  <description>This group is for Netscape.</description>
  <uservisible>true</uservisible>
  <default>>false</default>
  <packagelist>
    <packagereq type="optional">netscape</packagereq>
  </packagelist>
</group>
```

这些命令使Netscape成为Red Hat Linux文本方式安装过程中的可选包组选项。为了在图形安装过程中提供Netscape，就要增加下列命令将其放在一个组类别中：

```
<subcategories>
  <subcategory>netscape</subcategory>
</subcategories>
```


分析默认Kickstart的配置

安装Red Hat Linux时,选择的配置保存在/root目录的anaconda-ks.cfg文件中。本节要分解笔者桌面计算机中这个文件的例子。这个文件的开头如图5.1所示。

```
# Kickstart file automatically generated by anaconda.

install
lang en_US.UTF-8
langsupport --default en_US.UTF-8 en_US.UTF-8
keyboard us
mouse genericmouse/2 --device psaux
xconfig --card "Intel 810" --videoram 16384 --hsync 90-85 --vsync 90-160 --resol
ution 800x600 --depth 24 --startxonboot --defaultdesktop gnome
network --device eth0 --bootproto static --ip 10.252.113.84 --netmask 255.255.25
5.0 --gateway 10.252.113.119 --nameserver 207.217.126.81 --hostname RH81Test
network --device eth1 --bootproto static --ip 10.252.113.63 --netmask 255.255.25
5.0 --gateway 10.252.113.113 --nameserver 207.217.126.81 --hostname RH81Test
rootpw --iscrypted $15vJ8yUL9r$3nE5M/hx2wT/ge/o.0Sm/1
firewall --medium --trust=eth0
authconfig --enablesdow --enablemd5
timezone America/New_York
bootloader --location=mbr --append hdc=ide=acsi
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
# not guaranteed to work
#clearpart --linux --drives=hda
#part / --fs=ext3 --size 487 --as %PC
```

图5.1 典型anaconda-ks.cfg文件

每个Kickstart文件可以分成几类命令。我们将在下面几节介绍anaconda-ks.cfg文件。Kickstart文件中的命令顺序不一定是这样。

编辑完这个文件之后,将其保存成ks.cfg。本章末尾将介绍如何在软盘上建立这个文件。

安装并命令

可以设置安装参数。例如,可以指定安装开始的日期和时间。每次登录Linux时,都会显示/etc/motd文件:

```
#pre
echo "My Kickstart Installation started on `"/bin/date`" >/etc/motd
```

预安装命令要放在Kickstart文件末尾,放在任何%post安装命令之前。

当然,脚本还可以更复杂些,但只能使用Kickstart文件磁盘提供的命令。本章末尾将会介绍,Kickstart文件通常复制到红帽子安装引导盘中,包括基本内核和有限个数的bash shell命令。

基本配置

启动Red Hat Linux安装过程只需要几个基本命令。下列命令来自我的anaconda-ks.cfg文件:

```
install
lang en_US.UTF-8
langsupport --default en_US.UTF-8 en_US.UTF-8
```

```
keyboard us
mouse genericwheelp/2 --device psaux
timezone America/New_York
bootloader --location=mbr --append hdc=ide-scsi
```

如果要在一系列其他计算机上安装Linux，则最好使用相同语言、键盘类型和鼠标。如果这样，则不必做任何修改。下面一一介绍这些命令，供读者参考。

Install

第一个命令很简单，事实上它太简单，难于支持自动安装。换句话说，这个命令没有指定红帽子安装文件的来源：

```
install
```

可以用下列命令将Kickstart设置成到光碟或硬盘上寻找安装文件：

```
cdrom
harddrive --partition=hdb1 --dir=/install
```

本节假设Red Hat安装目录在/install目录中，服务器的IP地址为192.168.0.1。

harddrive命令在计算机的第二个IDE硬盘上寻找Red Hat目录，可以在第一个主分区(hdb1)的/Us.all目录中找到。或者用下列命令从远程计算机的NFS共享目录安装：

```
nfs --server=192.168.0.1 --dir=/install
```

也可以用下列命令从远程FTP或Web服务器的红帽子安装文件安装：

```
url --url ftp://username:password@192.168.0.1/install
url --url http://192.168.0.1/install
```

如果从匿名FTP服务器安装，则不需要用户名和口令。

提示：如果用静态IP地址配置安装Red Hat Linux，则有些计算机从网络上寻找安装文件时可能遇到问题。可以按本章稍后“网络设置”一节介绍的命令设置DHCP访问。

lang与langsupport

下一个命令指定安装过程中使用的语言以及Red Hat Linux要安装的语言文件。例如，下列命令用标准美式英语安装Red Hat Linux：

```
lang en_US.UTF-8
```

还有几个其他语言代码，可以从/usr/X11R6/lib/X11/locale目录的locale.alias文件中找到清单。如果运行自动安装，则不必看任何安装屏幕。但如果启动Red Hat Linux时想看到标准美式英语作为安装语言，可以用下列命令：

```
langsupport --default en_US.UTF-8 en_US.UTF-8
```

其他语言包括法语(fr_FR)、德语(de_DE)和朝鲜语(ko_KR.eucKR)。计算机上安装的语言会在anaconda-ks.cfg文件中显示。可以选择几种其他语言，详见Red Hat Linux定制指南，在红帽子文档光碟中或www.redhat.com站点。

说明：要取得联机Red Hat Linux 9手册，导航到www.redhat.com/docs/manuals/linux/RHL-9-Manual/。

Keyboard

Kickstart文件中的Keyboard命令很简单，标准美国键盘所要的命令如下：

```
keyboard us
```

anaconda-ks.cfg文件中的Keyboard命令应与安装相符。但也可以选择几十种不同键盘，如法语（fr）和西班牙语（es），完整清单见Red Hat Linux定制指南。

Mouse

Kickstart文件中的mouse命令表示指示设备。可以是触摸屏或写字板。例如，下列命令表示一般性PS/2鼠标，连接标准PS/2端口（psaux）：

```
mouse genericwheelpsaux --device psaux
```

如果要配置双键鼠标，仿真第三个中间键，则可以在这个命令末尾加上--emulthree开关。第3章曾介绍过，同时按两个键可以仿真第三个中间键。

还有其他类型的鼠标，如标准USB鼠标（genericusb），Microsoft鼠标（microsoft）和Logitech鼠标（logitech）。完整清单见红帽子定制指南。

Timezone

Timezone命令很简单，指定与计算机相关联的时区。如果Linux是安装的唯一操作系统，则要将硬件时钟设置为格林威治平均时间（--utc），使Mouse可以处理夏时制变化。典型的Timezone命令如下：

```
timezone --utc America/New_York
```

说明：UTC表示统一协调时间，满足一些人不愿提到格林威治的要求。

Bootloader

要用GRUB或LILO之类的引导装入器启动Red Hat Linux。Bootloader命令指定地址和可能需要的其他内核参数：

```
bootloader --location=mbr --append hdc=ide-scsi
```

这个命令让Kickstart在主引导记录（mbr）中安装引导装入器，并向内核发送光碟刻录机的配置消息。使Linux可以使第二个主IDE盘（hdc）像个SCSI工具（ide-scsi）。

说明：关于内可以添加的更多命令，可以运行man bootparam命令。

图形

Kickstart文件中的图形命令xconfig可能很复杂，但其实不是太难。由于我们不必在Red Hat Linux中配置X窗口系统，因此不需要xconfig命令。

下面从我的Kickstart文件中分析xconfig命令：

```
xconfig --card "Intel 810" --videoram 16384
➤ --hsync 30-85 --vsync 50-160 --resolution 800x600
➤ --depth 24 --startxonboot --defaultdesktop gnome
```

其指定一个特定显示卡Intel 810。如果其他计算机也有相同的卡和显示器，则应该可以对Kickstart文件保存这些设置。但是，如果需要进行改变，则可以参照表5.4的xconfig设置。

表5.4 Kickstart xconfig设置

设置	描述
--card "name"	指定显示卡版本和机型
--videoram amount	指定显示内存量
--hsync range	列出水平频率范围 (kHz)
--vsync range	列出垂直同步范围 (MHz)
--resolution horxvert	指定显示器分辨率
--depth num	指定每个像素颜色数
--defaultdesktop gnome	将GNOME设置为默认GUI桌面
--startxonboot	在安装完成后启动X窗口
--noprobe	指定安装过程不能探测显示器

提示：如果不想用这个Kickstart文件配置X窗口，则可以添加skipx命令，否则Anaconda停止安装过程，就可以配置X窗口。

网络设置

本节假设计算机上有一个网卡。但大多数情况下，Kickstart过程用网络上远程计算机中的红帽子安装文件。因此，需要如下所示命令在计算机上配置网卡：

```
network --device eth0 --bootproto dhcp
```

这个命令假设有个以太网网卡，网络上有个DHCP服务器。如果DHCP服务器在远程网络上，则使用BOOTP协议，只要将上述命令中的dhcp换成bootp。关于以太网的更多信息，见第20章；关于DHCP服务器和BOOTP的更多信息，见第24章。

也可以指定静态IP地址信息。第3章曾介绍过，这包括IP地址（--ip）、网络掩码（--netmask）、网关地址（--gateway）和DNS服务器IP地址（--nameserver）。还可以用下列命令指定这台计算机的主机名（--hostname）：

```
network --device eth0 --bootproto static --ip 192.168.12.20 --netmask
➤ 255.255.255.0 --gateway 192.168.12.11 --nameserver 207.217.126.81
➤ --hostname RH9test
```

说明：Kickstart文件中的network命令应放在一行中。

根口令

每个Red Hat Linux安装要求设置一个根口令。这是个简单命令，可以用下列两种方式之一进行配置：

```
rootpw Big747Ap
rootpw --iscrypted $1$ZIVd1QpJ$ptS2UJkTRngOTacYN22vR1
```

第一个方法以明文形式包括口令，如果使用本地Kickstart文件，则可以这样。但如果使用远程Kickstart文件，则最好将口令加密，见第二个例子。

防火墙

Kickstart文件中可以配置防火墙。在安装过程中曾介绍过，防火墙有三种：

```
firewall --high
firewall --medium
firewall --disabled
```

假设要标准高度安全防火墙，则可以进行定制。例如，如果有两个网卡eth0与eth1，则可以用下列命令关闭一个网卡上的防火墙：

```
firewall --high --trust=eth1
```

有几个标准服务可以让其穿过防火墙，包括DHCP配置消息（--dhcp）、安全Shell连接（--ssh）、Telnet连接（--telnet）、接收电子邮件（--smtp）、Web页面向内请求（--http）和FTP服务器输入连接（--ftp）。

可以让其他服务穿过防火墙，只要知道端口号和相关协议。例如，下列命令设置的高度安全防火墙允许普通与安全Web页面的外部请求：

```
firewall --high --http --port 443:tcp
```

数字是/etc/services文件中定义的TCP/IP端口，见第20章介绍。

验证选项

验证就是检查用户证件。通常，这只是检查用户名和口令。但也可以用几种方法配置这个过程。默认Kickstart命令用MD5加密设置阴影口令：

```
authconfig --enablesshadow --enablemd5
```

验证选项有几个，例如，可以设置NIS支持（--enablenis）、指定NIS域名（--nisdomain=name）、允许Kerberos口令（--enablekrb5）和检查Samba与Microsoft Windows服务器口令（--enablesmbauth）。大多数选项都在Red Hat Linux定制指南中。

硬盘分区设置

Anaconda将配置写入anaconda-ks.cfg时，默认关闭硬盘设置。如果对下列命令感到满意，则可以删除#号将其激活：

```
#clearpart --linux --drives=sda
#part /boot --fstype ext3 --size=100 --ondisk=sda
#part / --fstype ext3 --size=700 --grow --ondisk=sda
#part swap --size=192 --grow --maxsize=384 --ondisk=sda
```

第一个命令（clearpart）删除第一个SCSI硬盘（sda）任何现有Linux格式分区中的所有数据（--linux）。标准服务器安装从所有格式化分区中删除所有数据（--all）。

下一个命令对/boot目录设置分区（part），要在第一个SCSI硬盘上（--ondisk=sda）格式化（--fstype）成ext3文件系统，长度为100MB。

下一个命令将根目录 (/) 配置成第一个SCSI硬盘上的至少700MB长度。但是，这里设置了可增长标志 (-grow)，使分区可以填上第一个SCSI硬盘的可用空间。

这个设置中最后一个命令配置第一个SCSI硬盘上的交换分区，长度至少192MB，最大长度 (--maxsize) 为384MB。

还可能更有更丰富的硬盘配置。例如，下列命令对/boot、/usr、/home、root(/)与/var目录和交换分区配置单独的分区：

```
#clearpart --linux
#part /boot --fstype ext3 --noformat --onpart hda2
#part /usr --fstype ext3 --size=2500
#part /home --fstype ext3 --size=1000
#part / --fstype ext3 --size=1000
#part /var --fstype ext3 --size=500
#part swap --size=256
```

此外，下列命令对四个不同分区配置RAID阵列，配置两个适合逻辑卷管理 (LVM) 的物理卷：

```
#part raid.44 --size=100
#part raid.42 --size=100
#part raid.40 --size=100
#part raid.38 --size=100
#part pv.36 --size=100
#part pv.34 --size=100
```

最后，下列raid命令在三个分区的RAID5阵列中 (一个多余) 设置/home/mj目录。volgroup与logvol命令对/home/ez目录配置LVM组：

```
#raid /home/mj --fstype ext3 --level=RAID5 --spares=1 raid.44 raid.42 raid.40 raid.38
#volgroup Volume00 pv.36 pv.34
#logvol /home/ez --fstype ext3 --name-LogVol100 --vgname=Volume00 --size=192
```

包与组

当遇到%packages命令时，后面的项目指定要安装的包和组。本段的第一行应当如下，其指定五个包组：

```
%packages --resolvedeps
@ Administration Tools
@ Authoring and Publishing
@ DNS Name Server
@ Graphical Internet
@ Text-based Internet
```

第一行的--resolvedeps开关保证Red Hat Linux安装所选包的所有依赖包。否则Anaconda会停止安装过程，询问是否要解决依赖性。

这些命令从本章第一节介绍的comps.xml文件中搜索指定名称的组，其以comps.xml文件中的<name>变量为依据。每个组中要安装<packagereq type="mandatory">指定的包。其他

包可能是“default”或“optional”，这些包可以在Red Hat Linux安装过程中选择或取消。选择的结果得到下列格式的RPM包名表：

```
printman
libtool-libs
-gnomemeeting
gdbm
gnome-audio
tk
bzip2-libs
-ncftp
```

从这个表中，安装printman、libtool-libs、gdbm、gnome-audio、tk与bzip2-libs RPM包。Gnomemeeting与ncftp RPMs包通常属于安装的包组之一（Graphical Internet与Text-Based Internet），每个名称前面的负号表示不是通过这个Kickstart文件安装的。

安装后命令

安装Linux之后，Kickstart进行文件末尾的安装后脚本处理。可以运行各种脚本，默认语言基于bash shell。要指定不同的脚本语言，用下列命令：

```
post --initrd exec /usr/lib/typid
```

可以从远程计算机复制多个配置文件。例如，下列脚本从指定IP地址的计算机复制XF86Config文件：

```
mkdir /mnt/source
mount 192.168.0.1:/etc /mnt/source
cp /mnt/source/etc/X11/XF86Config /root
```

其假设通过NFS与指定IP地址的计算机共享/etc目录。

另一个简单命令保证Kickstart安装过程完成后系统重新启动：

```
reboot
```

其他命令

Kickstart文件中有大量命令。表5.5列出了基本Kickstart命令。

表5.5 基本Kickstart命令

命令	描述
auth	指定验证选项，同authconfig
bootloader	指定引导装入器地址，--useLilo安装LILO而不是GRUB
clearpart	删除当前分区，可以指定--linux或--all
device	可以对特定设备设置硬件参数
driverdisk	如果需要另一驱动程序盘，则可以将其装入现有分区，如driverdisk hda2 --type=vfat
firewall	可以设置基本防火墙配置
install	可以指定基本安装参数，包括红帽子安装文件源代码
interactive	通过Kickstart文件交互式运行，同autostep
keyboard	指定键盘类型

(续表)

命令	描述
lang	指定安装语言
langsupport	指定要安装的语言
logvol	增加逻辑卷分区
mouse	增加指示设备
network	配置本地网卡
part	生成指定分区, 同partition
raid	配置软件RAID设备
reboot	安装完成后重新启动系统
rootpw	指定这个系统的根口令
skipx	跳过X窗口配置过程
text	在文本方式中运行安装
timezone	指定这台计算机的时区
upgrade	升级现有Linux系统
volgroup	建立LVM组
xconfig	指定X窗口和图形卡配置细节
zerombr	覆盖任何现有分区表, 包括所有引导装入器

说明: 许多命令都有大量开关。本书介绍一些主要开关。如果需要更多信息, 见Red Hat Linux 9配置指南。

使用GUI Kickstart Configurator

还可以用另一种方法生成定制Kickstart配置文件, 用GUI Kickstart Configurator。可以在GNOME与KDE之类的GUI中启动GUI Kickstart Configurator。

打开命令行界面, 运行redhat-config-kickstart命令打开GUI Kickstart Configurator, 如图5.2。

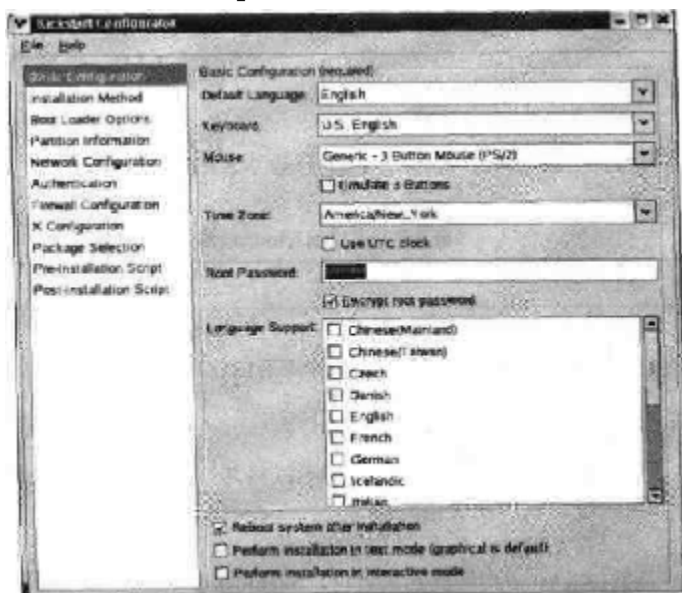


图5.2 GUI Kickstart Configurator

说明：如果需要在GNOME与KDE中启动命令行界面的更多信息，见第16章和第17章。

可以看出，左边的列包含11个菜单，将在下面几节介绍。如果安装过Red Hat Linux或读过本书第一年，则应该已经熟悉许多选项。

如果要从现有配置启动，单击File►Open File，然后从出现的菜单中选择/root/anaconda-ks.cfg之类的文件。

基本配置菜单

基本配置菜单如图5.2，包括几个基本设置，见表5.6简要介绍。

表5.6 Kickstart Configurator基本配置菜单

选项	描述
Default Language	指定安装过程中要用的语言，大约有20种
Keyboard	指定键盘类型，可以选择50种键盘
Mouse	选择计算机的鼠标或其他指示设备
Emulate 3 Buttons	如果有双键鼠标，则这个选项可以同时按两个键模拟中间键
Time Zone	指定时区
Use UTC Clock	在没有Microsoft windows之类的双引导操作系统时，可以用这个选项将硬件时钟设置为格林威治平均时间
Root Password	输入所要根口令
Encrypt Root Password	加密Kickstart文件中输入的根口令
Language Support	对运行Linux计算机安装字体和语言文件
Reboot System After Installation	在Kickstart文件中增加重新启动命令
Perform Installation In Text Mode	在文本方式中运行安装过程
Perform Installation In Interactive Mode	可以调试Kickstart安装过程

安装方法菜单

在Kickstart Configurator中选择Installation Method，可以打开图5.3所示的安装方法菜单。

这些选项是一目了然的。可以将Kickstart配置成安装新Red Hat Linux或升级Red Hat Linux。也可以指定安装文件的本地（CD-ROM或硬盘）或网络（FTP、HTTP、NFS）源。

引导装入器选项菜单

引导装入器选项菜单可以配置系统中引导装入器的类型和地址。第11章将会介绍，Linux的基本引导装入器有两种：GRUB与LILO。从图5.4可以看出，引导装入器选项菜单分为四个部分。

如果已经有第三方引导装入器（例如来自Partition Magic或System Commander），则可以在引导分区第一个扇区安装GRUB与LILO。如果喜欢LILO，而且在这台计算机上升级Linux，则可以选择Upgrade Existing Boot Loader而保留LILO。

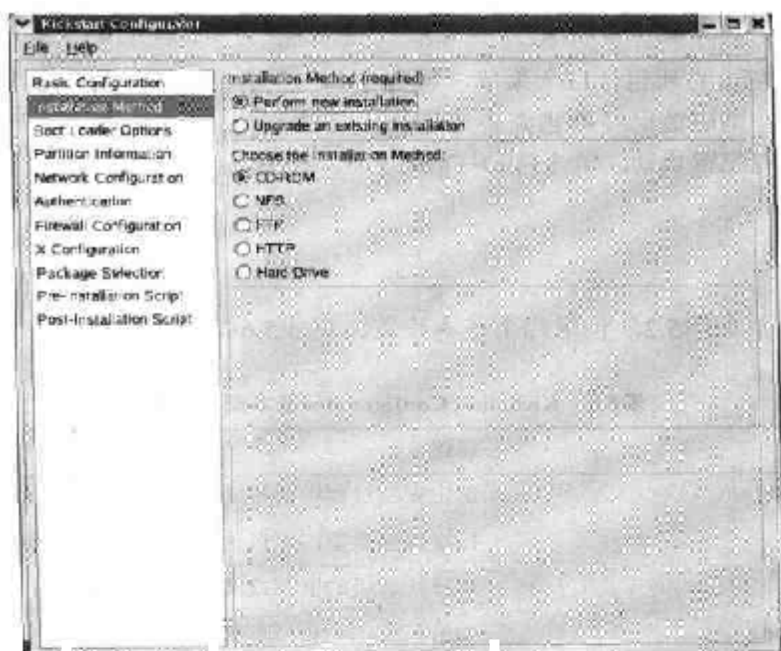


图5.3 Kick start 安装方法菜单

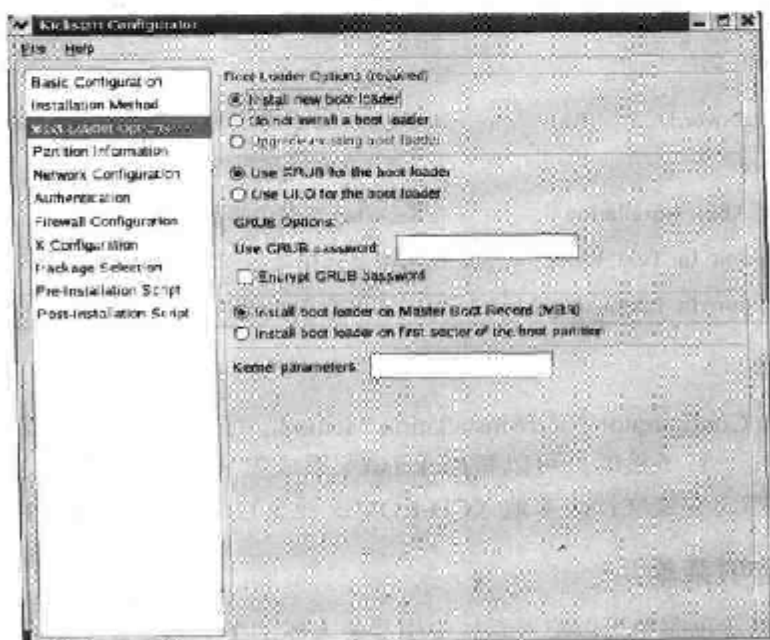


图5.4 引导装入器选项菜单

可以选择GRUB与LILO作为引导装入器。如果选择LILO，则可以让其按线性方式（linear）读硬盘，对大硬盘很方便。还可以强制使用lba32方式，帮助Linux在旧硬盘的1024柱面以外寻找/boot目录中的启动文件。

通常，引导装入器安装在MBR（主引导记录）中。如果喜欢用另一个引导装入器，则可以在引导分区第一个扇区安装GRUB与LILO。

也可以将硬件参数传入内核。这通常在Linux自动探测硬件遇到问题时有用。可以指定各种参数，见bootparam手册页定义。

说明：Linux中的手册页是个手册，介绍命令和配置文件。例如，要读取/etc/fstab的手册页，打开Linux命令行界面，并运行man fstab命令。

引导装入器还有更多选项，见下节介绍。

分区信息菜单

分区信息菜单中可以配置需要的大多数分区，如图5.5。

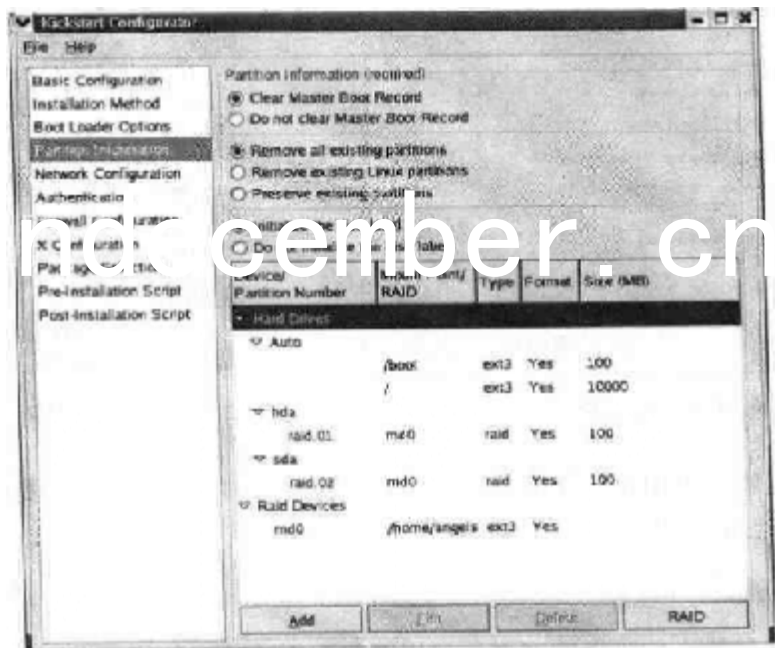


图5.5 分区信息菜单

这个菜单第一部分可以设置硬盘的基本参数。Clear Master Boot Record选项可以从硬盘中删除任何现有引导装入器，相当于Kickstart中的zerombr=yes命令。

如果硬盘有现有分区，则可以选择只删除Linux分区，也可以删除硬盘上的所有分区。如果在带新硬盘的计算机上安装Linux，则还要选择Initialize The Disk Label。

说明：如果升级Red Hat Linux，则通常使用现有分区，这个菜单的所有选项取消。

单击Add按钮打开Partition Options对话框，如图5.6。如果你熟悉第3章介绍的Disk Druid，则不难理解这里的选项。如果需要这些选项的更多信息，请看第3章。

除了Disk Druid中的选项外，这个对话框中还有下面两个选项：

Use Recommended Swap Size Red Hat Linux可以配置推荐的交换分区，通常是内存长度的两倍。

Use Existing Partition 如果知道目标计算机的分区布局，则可以指定hdal之类的分区。第2章介绍了分区命名规则。

到本书编写时，Kickstart Configurator不支持对LVM分区生成卷组。但仍然可以按前面介绍的方法将LVM条件加进实际Kickstart文件中。

也可以设置RAID设备。如果已经配置RAID分区。则可以单击RAID，在RAID选项窗口中，选择Create A RAID Device并单击OK按钮继续，从而打开Make RAID Device对话框，如图5.7所示。

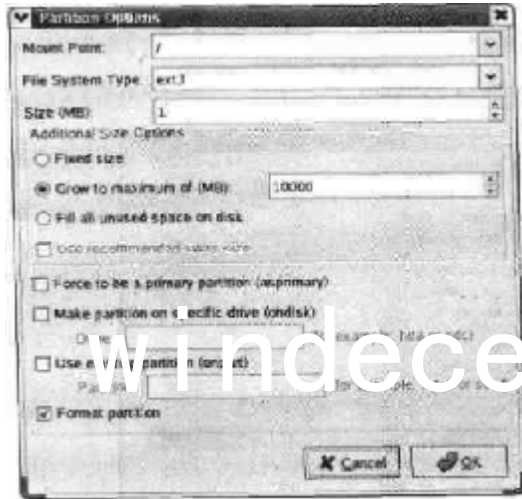


图5.6 Partition Options对话框

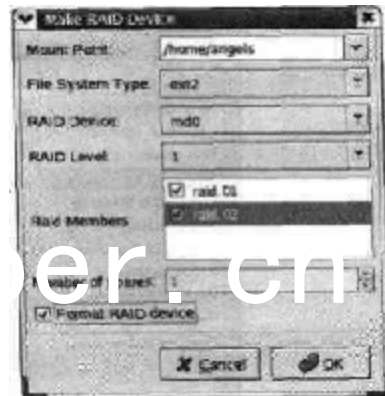


图5.7 Make RAID Device对话框

如果有足够的RAID分区数，则这个对话框支持生成0、1、5级RAID。关于这些不同级的RAID要求，见第14章介绍。

网络配置菜单

要配置计算机上的以太网网卡，使用网络配置菜单。如果有不同类型的网卡，则要直接编辑Kickstart配置文件。从图5.8可以看出，可以增加、编辑或删除各种网络设备。

增加或编辑网络设备时，其打开Network Device Information对话框，如图5.9所示。

每个网络设备可以配置几个不同设置：

Network Device 单击下拉箭头设置为17个以太网网络设备之一，是eth0到eth16。

Network Type 可以选择静态IP配置的网络类型，也可以从本地DHCP服务器或从远程DHCP服务器中使用BOOTP取得网络设备的数据。如果选择静态IP网络类型，则可以对这个网络设备配置网址信息。

IP Address 网卡的IPv4地址。

Netmask 局域网的网络掩码。

Gateway 将网络与互联网之类外部网络连接的计算机或路由器IP地址。

Name Server 连接网络的DNS服务器IP地址。

关于每个设置的更多信息，见第20章。

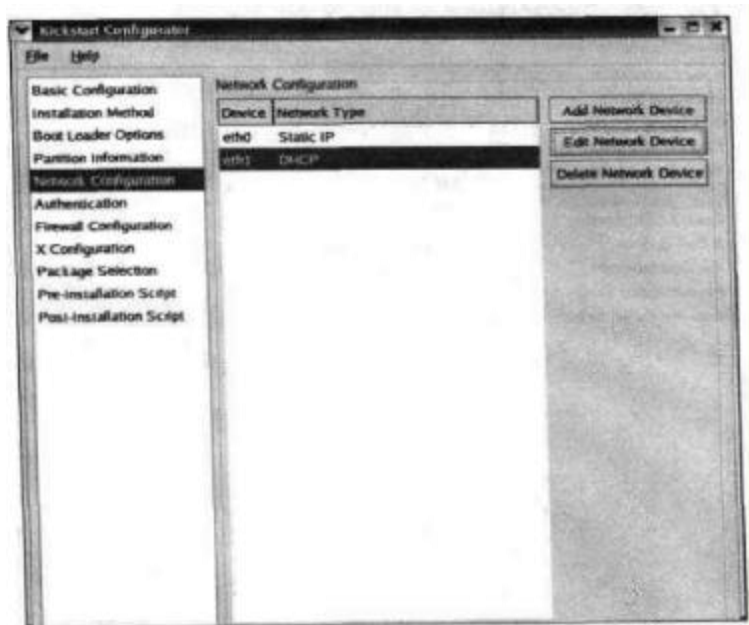


图5.8 网络配置菜单

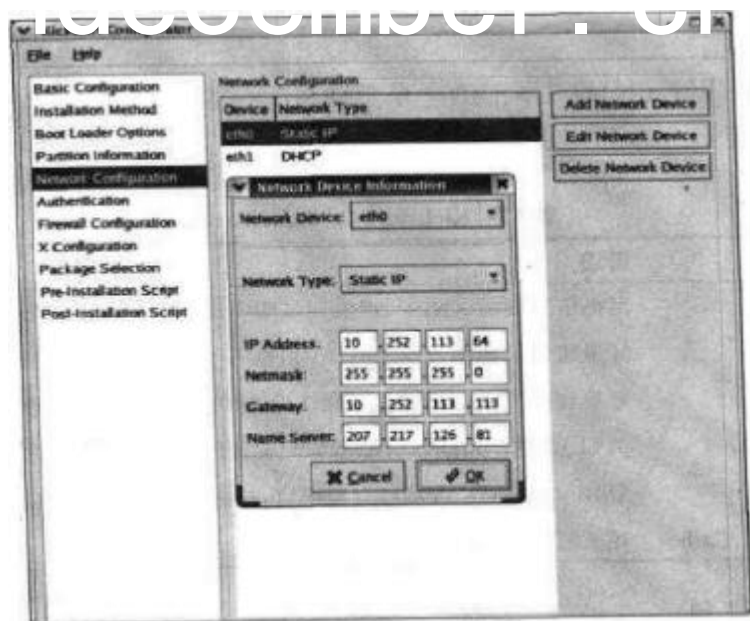


图5.9 编辑网络设备

验证配置菜单

前面曾介绍过，验证通常描述计算机如何检查用户名与口令。图5.10显示了基本验证配置菜单。

默认情况下，Kickstart配置两种口令安全性。阴影口令属于第9章介绍的阴影口令组，MD5是对用户口令采用的一种加密。

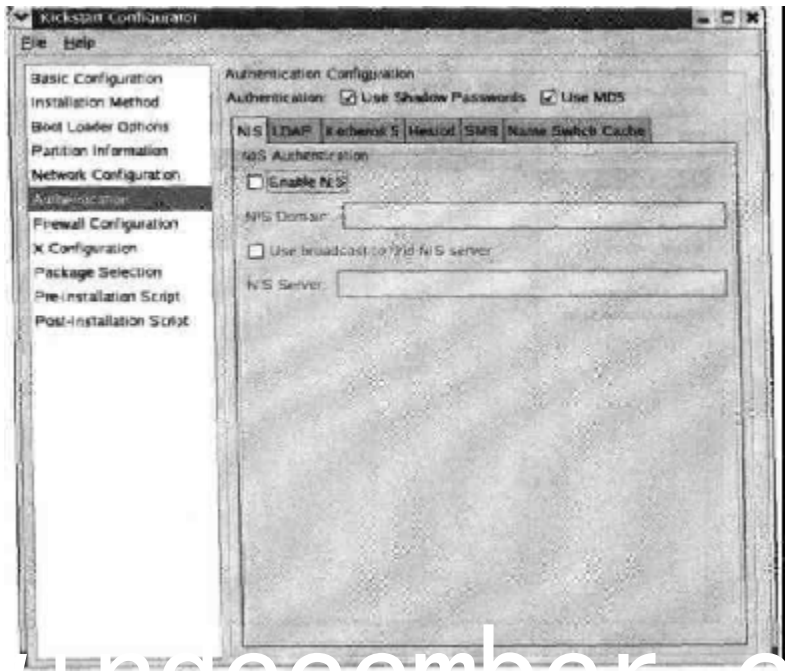


图 5.10 验证设置菜单

从图5.10可以看出，这个窗口有一系列标签，表示不同形式的验证。现将其在表5.7中列出。

表5.7 Kickstart Configurator验证选项

选项	描述
NIS	网络信息服务（NIS）提供局域网中用户名与口令的公共数据库，详见第28章
LDAP	轻量级目录帮助协议（LDAP）也用于验证，与局域网数据库相联系
Kerberos 5	是麻省理工学院开发的，提供检查用户证件的强加密方法
Hesiod	类似于NIS，用DNS分配基本配置文件中保存的信息
SMB	SMB（Samba）选项可以使用Microsoft Windows网络上的其他服务器进行验证
Name Switch Cache	相关监控程序ncsd通过NIS支持验证

防火墙配置菜单

第3章与第4章安装Red Hat Linux时已经介绍防火墙配置菜单。从图5.11可以看出，可以选择三种基本防火墙配置：High、Medium或Disabled。

如果选择配置防火墙，则可以进行定制。可以在Trusted Devices文本框中选择设备名，从防火墙中排除某个网卡（如eth0）。此外，可以允许几种不同类型的服务器通信流进入网络：web（WWW）、FTP、Secure Shell（SSH）、DHCP接收邮件（SMTP）与Telnet。

Other Ports文本框可以根据/etc/services增加其他端口。

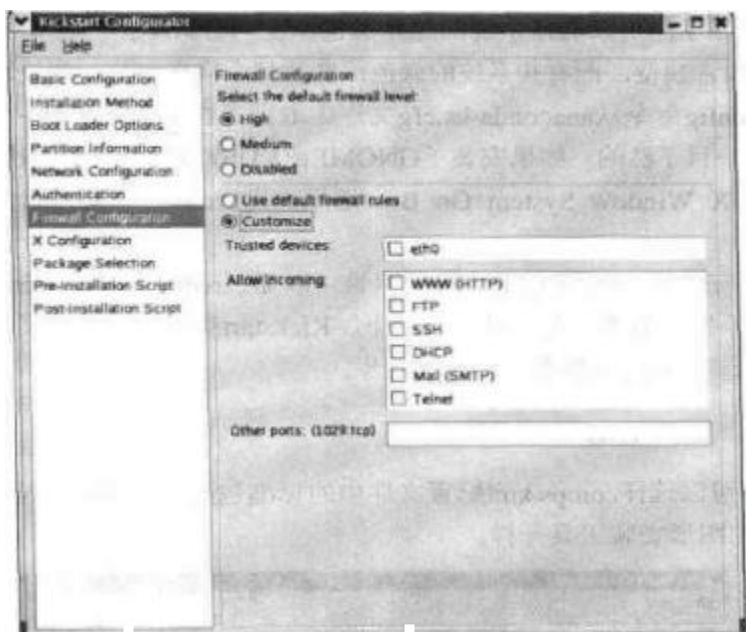


图5.11 防火墙配置菜单

X配置菜单

X配置菜单与redhat-config-xfree86工具非常相似。如果要通过Kickstart配置X窗口，则可以选择Configure The X Window System，激活图5.12所示的三个标签。

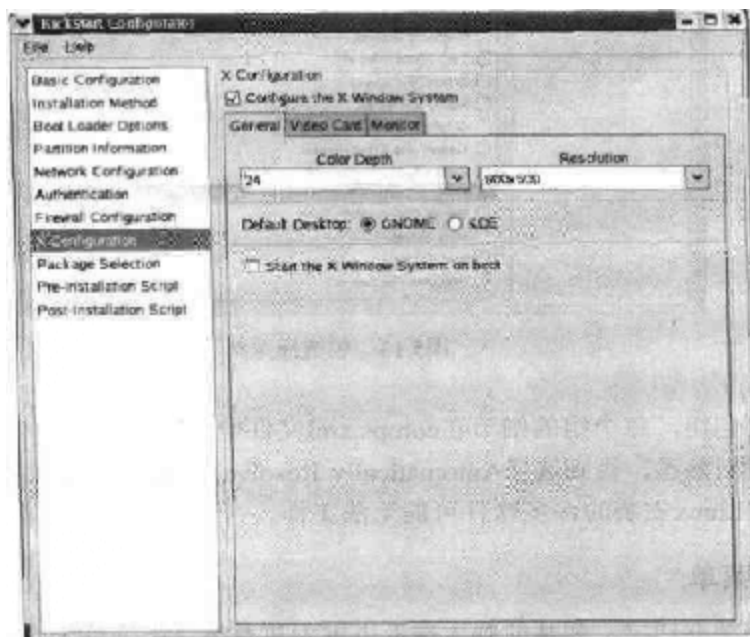


图5.12 X配置菜单

在General标签中,可以选择系统的总体颜色深度与分辨率。一定要小心,有些系统的颜色深度为每个像素24位,而有些系统的颜色深度为每个像素32位。假设计算机反映目标硬件,则只好用xconfig命令从anaconda-ks.cfg文件中取得工作配置。

其他选项是一目了然的。如果安装了GNOME或KDE,则可以将其设置为默认桌面。如果启用Start The X Window System On Boot选项,则Linux打开第15章介绍的显示管理器之一。

Video Card与Monitor标签包括的数据库也可以通过redhat-config-xfree86工具取得。第15章介绍了这个系统的更多信息。默认情况下, Kickstart探测显示卡与显示器,也可以用这个工具激活设置,包括显示器水平与垂直同步。

包选择菜单

包选择菜单可以选择comps.xml配置文件中的标准包组。如图5.13所示,窗口的组织与Red Hat Linux的图形安装工具一样。

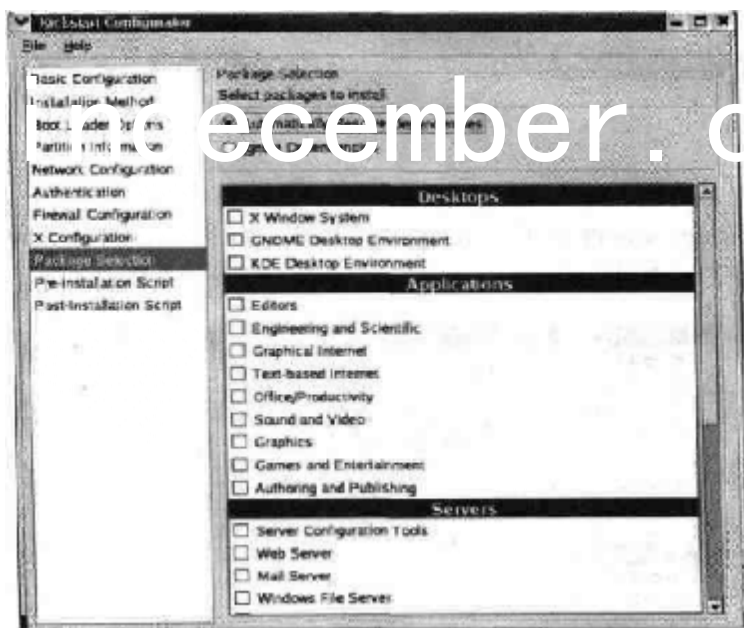


图5.13 包选择菜单

选择所要包组,每个组的细节在comps.xml文件中。

除非你特别熟悉,否则选择Automatically Resolve Dependencies,保证安装基础软件,否则Red Hat Linux安装的许多软件可能无法工作。

安装前脚本菜单

本章前面曾介绍过,安装前脚本帮你设置安装参数。由于脚本在安装Red Hat Linux之前运行,因此可用的命令很有限。可以用Kickstart Configurator生成安装前脚本,如图5.14。

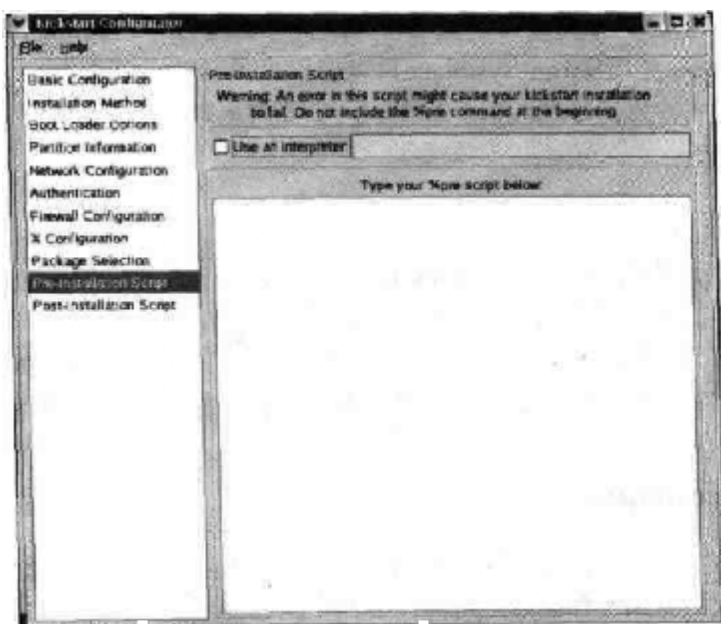


图5.14 安装前脚本菜单

默认脚本语言是bash。如果要使用不同语言的命令，则可以激活Use An Interpreter文本框，然后输入另一语言模块的地址，如/usr/bin/python。测试脚本，如果有错，则Kickstart安装可能失败。

安装后脚本菜单

安装后脚本可以对每个配置增加参数。也可以用Kickstart Configurator生成安装后脚本，如图5.15。

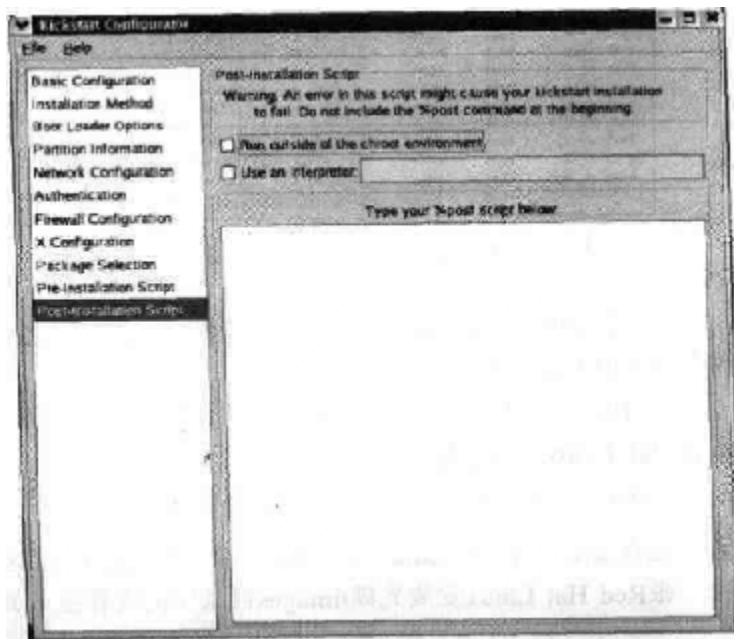


图5.15 安装后脚本菜单

安装后脚本在chroot环境中运行。换句话说,安装过程中,标准Linux根目录装载到/mnt/sysimage目录。Chroot环境使/mnt/sysimage目录像根目录一样。

关于Chroot环境的更多信息,见第27章。一定要测试脚本,如果有错,则Kickstart安装可能失败。

下一步

进行改变之后,要将改变保存到Kickstart文件中。为此,单击File►Save File并将文件保存在所选目录中。下节将会介绍,它将文件命名为ks.cfg。

如果有些内容无法加进配置文件中(如LVM分区),则可以在文本编辑器中打开ks.cfg文件,增加这些内容。我们在本章前面检查了Kickstart文件的基本配置与命令。

从软盘运行Kickstart

有了Kickstart文件之后,就可以从安装引导盘开始Red Hat Linux安装过程。Red Hat Linux发现和装入Kickstart文件之后,可能需要一个驱动程序盘。激活所要的驱动程序之后,Anaconda用Kickstart文件中的指令自动安装Red Hat Linux。然后可以删除安装盘与驱动程序盘,用其启动计算机上开始这个过程。

换句话说,可以同时多台计算机上安装Red Hat Linux。

引导盘上的文件

Kickstart文件通常很小,放在标准Red Hat Linux安装软盘中。图5.16显示了bootdisk.img引导盘中的标准文件。注意我在这个盘中放了我的ks.cfg文件。

```
[root@RH9Test root]# ls -l /mnt/floppy/
total 1414
-rwxr-xr-x 1 root root 342 Mar 13 21:58 boot.msg
-rwxr-xr-x 1 root root 957 Mar 13 21:58 general.msg
-rwxr-xr-x 1 root root 570110 Mar 13 21:58 initrd.img
-rwxr-xr-x 1 root root 1305 Mar 27 14:38 ks.cfg
-r-xr-xr-x 1 root root 7836 Mar 13 21:58 ldlinux.sys
-rwxr-xr-x 1 root root 730 Mar 13 21:58 options.msg
-rwxr-xr-x 1 root root 869 Mar 13 21:58 param.msg
-rwxr-xr-x 1 root root 531 Mar 13 21:58 rescue.msg
-rwxr-xr-x 1 root root 549 Mar 13 21:58 snake.msg
-rwxr-xr-x 1 root root 5420 Mar 13 21:58 splash.las
-r-xr-xr-x 1 root root 495 Mar 13 21:58 syslinux.cfg
-rwxr-xr-x 1 root root 855693 Mar 13 21:58 vmlinuz
[root@RH9Test root]#
```

图5.16 bootdisk.img引导盘中的标准文件

用第3章介绍的方法生成Red Hat Linux安装光碟。将生成的任何Kickstart文件更名为ks.cfg,将这个文件复制到安装光碟中。

但是,安装引导盘中的空间不足以放下驱动程序。如果需要其他驱动程序,则可以使用安装引导盘和Red Hat Linux安装光碟。

说明: 有些公司购买的PC机不带光碟驱动程序,防止用户自己装入软件。

如果计算机没有光碟驱动程序,则Linux要装入的任何驱动程序需要更多软盘。第2章曾介绍过,可以从第一张Red Hat Linux安装光碟/images目录中的文件生成其他软盘。根据配

置情况，可能要从下列一个或几个映像生成软盘：drvnet.img、drvblock.img与pcmciaadd.img。

安装过程

有了安装软盘之后，将带Kickstart文件的Red Hat Linux安装软盘插入相应软驱中。如果可能，插入第一张Red Hat Linux安装光碟。重新启动计算机，从安装软盘或光碟引导。看到第一个安装屏幕时，可以看到引导提示，可以输入下列命令：

```
[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: linux ks=floppy
```

如果已经正确配置ks.cfg文件并从光碟引导启动，则可以在计算机读取启动内核和相应驱动程序之后取出软盘和光碟，安装会自动继续。

如果不从光碟启动，则要在提示下插入相应驱动程序软盘。提示屏幕与第4章显示的的驱动程序屏幕相似。

测试Kickstart

Kickstart可以在具有类似或相同硬件配置的一组计算机上安装Red Hat Linux。如果要在大量计算机上安装Red Hat Linux，则可能要整个晚上呆在办公室中，保证一切顺利进行，也可以在一台或两台计算机上测试Kickstart安装过程，然后用这个Kickstart充满信心地在网络上其他计算机上安装Red Hat Linux。

小结

前几章介绍了安装Red Hat Linux的过程比较复杂。Anaconda是Red Hat Linux安装程序，需要大量用户输入。本章介绍如何用Kickstart自动安装Red Hat Linux。有了相应的Kickstart文件之后，就可以将软盘或光碟插入PC机中，然后输入一个简单命令，让安装自动进行。

为了演示如何配置Kickstart文件，我们分析了comps.xml文件，其把Red Hat Linux包分成几个组。

然后我们检查了计算机的默认Kickstart配置，保存在/root目录的anaconda-ks.cfg文件中。将这个文件稍做修改，就可以让Kickstart在另一计算机上建立相同的配置。

Kickstart Configurator提供了生成定制Kickstart文件中的GUI界面。尽管生成基本配置能够节省时间，但可能还要在文本编辑器中对生成的文件增加几个命令。

对Kickstart文件感到满意之后，可以将其保存在Red Hat Linux安装引导盘的ks.cfg文件中。可以使用第一张Red Hat Linux安装光碟或所要驱动程序的驱动程序盘。如果正确配置了ks.cfg文件，则可以用一个简单命令开始安装。除非要插入另一个驱动程序盘，否则可以离开计算机，Red Hat Linux会自动安装。

下一章开始介绍Linux的命令行界面，然后我们介绍导航与管理Linux的基本命令。

第二部分 Linux基础

第6章 从命令行开始

尽管Red Hat Linux中有几个集成GUI工具，但控制Linux的最好方法是使用命令行界面。命令行界面比GUI工具有更多选项。由于命令行界面没有GNOME与KDE之类的桌面开销，因此速度更快。Linux社区仍然对命令行情有独钟。因此，如果想真正学习Linux，则一定要知道命令行界面的用法。

本章介绍的是几个不同命令，基于第8章要介绍的Bourne Again Shell (bash)。有些命令可以导航到不同Linux目录，有些命令可以创建和删除Linux文件。有些命令可以按不同方式阅读或搜索文件，有些命令可以充分利用文件特征。

命令行界面的关键之一是vi编辑器，在检查引导失败之类的错误时，这是惟一可用的编辑器。本章介绍下列内容：

- 探索导航命令
- 设置文件与目录
- 管理文件
- 操纵文件
- 使用vi编辑器
- 了解其他文本编辑器

探索导航命令

有两个基本导航命令可以在shell中移动。cd命令可以在目录之间移动。ls命令可以显示目录内容（包括其他目录）。但是，进入不同Linux目录之前，可以用pwd命令显示当前位置。导航命令的输出取决于绝对路径，绝对路径指定相对于顶层根目录（/）的目录地址。

pwd

pwd命令（表示当前工作目录）很简单。在命令行界面输入这个命令后，就可以看到当前目录的绝对路径。例如：

```
# pwd
/etc/httpd/conf
```

这个输出表示当前目录为/etc/httpd/conf，这是Apache配置文件的默认地址。

cd

cd命令改变目录。如果你熟悉MS-DOS，则可以发现MS-DOS与Linux的cd命令之间有几个相似之处。表6.1显示了典型的cd命令。

说明：Linux是大小写相关的，注意本章表中较小的大写字母表示小写字母。

表6.1 CD命令

命令	结果
cd ..	上移一层目录。例如，如果当前在/home/mj目录，则移到/home目录
cd ../..	上移两层目录。例如，如果当前在/etc/rc.d/rc0.d目录，则移到/etc目录。 还可以上移多层目录，直到根目录 (/)
cd /home/mj	移到用户mj的主目录
cd ~	移到自己的主目录，适用于任何用户

说明：如果你对Linux不太熟悉，则要记住目录、计算机和域名之间用斜杠 (/) 分开，而不是用反斜杠 (\)。

ls

ls命令非常灵活，不仅可以列出当前目录中的文件与目录，而且可以用正确选项找到文件权限与长度。这个命令可以检查拥有权，区别不同文件类型和按多种方式排序结果。表6.2列出了这个命令的一些例子。

表6.2 LS命令

命令	结果
ls	按字母顺序列出当前目录中所有非隐藏文件
ls -a	按字母顺序列出当前目录中所有文件，包括隐藏文件
ls -r	按字母顺序的逆序列出当前目录中所有非隐藏文件
ls -F	按类型列出所有文件，每个文件末尾的字符表示类型。例如，斜杠 (/) 表示目录，星号 (*) 表示可执行文件，@号表示链接文件
ls -i	列出带inode编号的文件。inode编号表示文件在卷中的地址。具有相同inode编号的两个或多个文件是同一文件的不同名称
ls -l	列出当前目录中的所有文件，包括当前目录 (.) 和父目录 (..) ，包括长度、拥有者和权限，称为长列表格式
ls -t	按文件最后修改时间列出文件，最新的文件放在前面
ls -u	按文件最后访问时间列出文件，最新的文件放在前面

也许其中最重要的是ls -l，列出当前目录中的所有文件，包括长度、拥有者和权限。图6.1显示了这个命令的结果例子。

```

-rw-r--r-- 1 root root 35 Feb 25 18:18 updfstab.conf
-rw-r--r-- 1 root root 870 Feb 25 18:18 updfstab.conf.default
lrwxrwxrwx 1 root root 34 Mar 26 10:19 vfontcap -> ../usr/share
/VfLib/2.25.6/vfontcap
lrwxrwxrwx 1 root root 37 Mar 26 13:41 vfontcap.js -> ../usr/sh
are/VfLib/2.25.6/vfontcap.js
drwxr-xr-x 3 root root 4096 Mar 26 10:24 vrs
drwxr-xr-x 2 root root 4096 Mar 26 13:41 vsftpd
-rw-r--r-- 1 root root 125 Feb 28 14:21 vsftpd.ftputers
-rw-r--r-- 1 root root 361 Feb 28 14:21 vsftpd.user_list
-rw-r--r-- 1 root root 864 Feb 25 10:53 warnquota.conf
-rw-r--r-- 1 root root 23954 Jan 25 22:00 webalizer.conf
-rw-r--r-- 1 root root 23930 Jan 25 22:09 webalizer.conf.sample
-rw-r--r-- 1 root root 4022 Jan 25 03:18 wgetrc
drwxr-xr-x 2 root root 4096 Mar 26 14:43 wordtrans
drwxr-xr-x 17 root root 4096 Mar 26 11:05 X11
-rw-r--r-- 1 root root 289 Feb 24 18:10 xinetd.conf
drwxr-xr-x 2 root root 4096 Mar 26 13:38 xinetd.d
drwxr-xr-x 2 root root 4096 Mar 26 10:31 xsl
-rw-r--r-- 1 root root 4912 Feb 20 10:08 xpdfrc
-rw-r--r-- 1 root root 361 Mar 26 10:47 yp.conf
-rw-r--r 1 root root 1626 Jan 25 03:38 ypserf.conf
drwxr-xr-x 2 root root 4096 Mar 26 13:43 zebra
[root@RH9Test etc]#

```

图6.1 当前目录中的长列表格式 (ls -l)

可以看出，长列表包括当前目录中每个文件的权限、拥有者、组拥有者、长度、修改时间和名称。

路径管理

描述文件位置时，可以指定相对路径或绝对路径。绝对路径相对于根目录 (/) 描述文件位置。例如，可以输入下列命令，取得启动几个Linux监控程序的脚本：

```
# cd /etc/rc.d/init.d
```

第一个目录前面的正斜杠表示是个绝对路径。可以从Linux中任何地方输入这个命令，进入这个目录。有时输入的命令没有正斜杠：

```
# cd etc/rc.d/init.d
```

这时Linux会在你的主目录中寻找这些目录。例如，如果你的主目录为/home/mj，则Linux会寻找/home/mj/etc/rc.d/init.d目录。除非把这些文件放在主目录的深层中，否则Linux什么也找不到。

相对与绝对路径还适用于其他命令。例如，可以用下列命令列出/etc/rc.d/init.d目录中的监控程序：

```
# ls /etc/rc.d/init.d
```

但是，如果使用相对路径，则当前目录很重要。例如，如果pwd命令的输出为/home/mj，则下列命令是行不通的，除非有个/home/mj/etc/rc.d/init.d目录：

```
# ls etc/rc.d/init.d
```

建立文件与目录

Linux中很容易生成文件。可以从现有文件复制，也可以从编辑器或另一应用程序中保存所选的文件名。还有一个特殊命令，可以生成空文件。删除文件也很容易，简直太容易了，

甚至有些删除文件的命令非常危险。

尽管Linux目录只是个特殊文件，但Linux中具有生成与删除目录的特定命令。首先，我们介绍文件管理命令，然后再介绍生成与删除目录的特定命令。

touch

有时只需要在Linux中生成空文件。例如，对用户或组激活配额之前，要在目标目录中生成空文件aquota.user或aquota.group。利用touch命令很容易生成空文件。下列命令在/home目录中生成这些空文件：

```
# touch /home/aquota.user /home/aquota.group
```

touch命令还可以改变现有文件的时间标志。使用不带开关的touch命令时，文件的最后访问时间变成当前时间。例如，假设现在是4月15日11时21分，则运行下列命令后：

```
# touch /root/f0601.tif
```

对f0601.tif文件运行ls -l命令时，可以看到下列输出：

```
-rw-r--r--  1 root root  883823 Apr 15 11:21 f0601.tif
```

其他开关可以改变文件相关的时间（如-t）。

cp

复制命令最简单的形式是cp file1 file2。发出这个命令时将file1内容复制到目标文件file2中。目标文件得到新的生成日期和inode编号。其他复制命令可以覆盖目标文件。甚至可以用cp命令的开关复制一个或多个子目录的内容。表6.3列出了cp命令的例子。

表6.3 CP命令

命令	结果
cp file1 file2	将file1内容复制到目标文件file2中，目标文件得到新的生成日期和inode编号
cp file* Dir1	将多个文件复制到一个目录
cp -f file1 file2	如果文件file2已经存在，则这个命令覆盖其内容时不发出提示
cp -i file1 file2	如果文件file2已经存在，则这个命令覆盖其内容时会先发出提示
cp -p file1 file2	将file1内容复制到目标文件file2中，目标文件保持原有的生成日期和inode编号
cp -r Dir1 Dir2	将目录Dir1及其子目录内容复制到Dir2。这个效果是递归的，换句话说，如果Dir1的子目录中还有子目录，则也复制其中的文件和目录
cp -u file1 file2	如果文件file2已经存在，但file1更新，则这个命令覆盖其内容时不发出提示

说明：inode是每个Linux分区中对文件使用的标识符。每个文件有一个inode，inode包括文件的元数据，包括权限、长度、最后访问时间和文件所在的磁盘块。如果inode搞乱或搞错，则Linux无法找到相关的文件。此外，同一文件具有相同的inode号。但由于不同分区不可能有相同inode号，因此从一个分区向另一个分区复制文件时，不能使用cp -p file1 file2命令。

mv

如果要在Linux中更名文件，则要移动文件。mv命令改变文件名。除非将文件移到不同的卷，否则文件的一切保持相同，包括inode。有四个关键的mv命令，见表6.4。

表6.4 MV命令

命令	结果
mv file1 file2	将文件名从file1变成file2。如果源与目标文件在同一卷中，则文件的inode号不变
mv file* Dir1	将多个文件移到一个目录
mv -f file1 file2	如果文件file2已经存在，则这个命令覆盖其内容时不发出提示
mv -i file1 file2	如果文件file2已经存在，则这个命令覆盖其内容时会先发出提示

提示：有些Linux用户生成的文件名为小写字母，如file1，而目录以大写字母开头，如Dir1。这不是必要的规则，标准Linux目录以小写字母开头，如/bin。

rm

rm命令可以删除文件与目录。因为许多Linux系统建议，只在必要时才在根用户或超级用户方式下运行Linux。这个命令的小小错误就很容易删除所有Linux文件。例如，假设要删除根目录（/）中一组临时目录的信息：a.tmp、b.tmp与c.tmp。本来要使用rm -r *.tmp命令，但你不小心输入下列命令：

```
# rm -r * .tmp
```

由于星号与.tmp之间有一个空格，使shell认为要递归删除所有目录，然后删除.tmp文件，结果非常糟糕。

为此，红帽子公司将下列别名配置为根用户的别名：

```
alias rm='rm -i'
```

这个别名保证，用rm命令（包括rm -r）时，shell提示先确认之后再删除任何文件。有些Linux发行版本将这个别名设置为根用户的shell变量。表6.5列出了关键rm命令。

提示：可以用alias命令找到默认别名。

表6.5 RM命令

命令	结果
rm file1	删除file1而不提示确认，但这个命令不会覆盖alias rm='rm -i'，其要求确认
rm -d Dir1	删除Dir1而不提示确认，但这个命令不会覆盖alias rm='rm -i'，其要求确认
rm -i file1	提示用户确认之后删除file1
rm -f file2	如果文件file2已经存在，则这个命令覆盖其内容时不发出提示，甚至覆盖alias rm='rm -i'
rm -r *	递归删除文件，如果当前目录中还有子目录，则也删除其中的文件和目录。但这个命令不会覆盖alias rm='rm -i'，其要求确认

以根用户身份管理

Linux社区中一个争论很激烈的问题是Linux管理员可否以根用户身份登录。根用户发生错误时可能破坏或删除系统中的文件。此外，以根用户身份登录还可能向在系统中转入“特洛伊木马程序”的人暴露根用户口令。

另一方面，红帽子软件使根账号的使用变得安全。好的别名使用户更难因为意外而删除关键文件。NFS中的root_squash之类的默认使其他计算机上的根用户无法破坏你的系统。可以用GRUB引导装入器和BIOS的口令进一步保护系统。由于我知道红帽子公司的人经常使用根账号，因此我也在本书中使用根账号。

如果以根用户身份登录，则一定要小心。不要没有退出就离开系统，否则别人可能改变口令，随意访问你的系统。不要在系统中提供读取或控制根用户工作的服务，如AT&T公司的VNC（虚拟网络计算）环境。

ln

除了复制与移动文件之外，还可以链接文件。链接很常见，特别是在不同运行级启动的程序。链接文件时，生成了当前现有文件的另一个路径。例如，如果你和同事都在使用文件project，则可以在主目录中生成一个链接文件。假设project文件在/home/jm目录中。要生成mj的主目录中文件的链接，使用下列命令。

```
# ln /home/jm/project /home/mj/project
```

使用其中一个文件时，改变与结果可以从两个目录中显示和访问。这也称为硬链接。使用硬链接时，由于两个文件保持相同inode号，因此两个文件是一致的。如果删除原文件，则硬链接文件保留，保持原文件的所有信息。

说明：ln file1 file2命令与cp -p file1 file2命令得到相同结果。除非文件位于不同分区，否则file1与file2保持相同inode号。

链接的一个重要选项是符号化方式，可以看到链接文件。例如，如果运行下列命令：

```
# ln -s /home/jm/project /home/mj/project
```

则可以在文件的长列表（ls -l）中看到链接文件，称为软链接。如果删除原文件则软链接指向空文件，原文件中的信息丢失。

mkdir与rmdir

可以想像，mkdir命令可以生成目录。生成的目录不一定要基于当前目录。如果需要，也可以建立多级目录。还可以对生成的目录指定所选权限。表6.6列出了关键的mkdir命令。

表6.6 MKDIR命令

命令	结果
mkdir -p Dir1/Dir2	生成目录Dir2。如果Dir1不存在，则-p开关让Linux也生成这个目录。两者都作为当前目录的子目录
mkdir -m 755 /usr/Dir3	生成目录Dir3，作为/usr目录的子目录。权限（755）是拥有者rwx，组中的其他成员和别人为r-x

`rmdir`命令可以删除目录。删除的目录不一定要基于当前目录。如果需要，也可以删除多级目录。例如，下列命令可以删除目录`Dir1`与`Dir3`：

```
# rmdir -p Dir1/Dir3
```

如果`Dir3`是空的，则这个命令删除该目录。如果`Dir1`目录中的惟一文件是`Dir3`，则这个命令也删除`Dir1`。

管理文件

Linux中有几个命令可以按不同方式读文件。可以验证不同类型的文件，可以从上或从下读文件。可以只读几行，也可以读取整页或整个文件。还可以计算文件中的行数、字数和字母数字字符数。此外，Linux还可以用选择的搜索选项搜索文件。

由于二进制文件中很难定义行和单词，因此这些命令更适合文本文件。

file

尽管有些发行版本用不同颜色区别文件类型，但Linux没有标准扩展。可执行文件不一定以`.exe`结尾，文档文件不一定以`.doc`结尾。file命令可以浏览每个文件的类型，如图6.2。

```
boot.log:      ASCII English text
cron:          ASCII text
cups:          directory
cnews:         ASCII text
gdm:           directory
httpd:         directory
ksyms.O:       ASCII text
lastlog:       Non-ISO extended-ASCII text, with no line terminators
maillog:       ASCII text
mailman:       setgid directory
messages:      ASCII English text
news:          directory
pgsql:         empty
rpmkys:        ASCII text
samba:         directory
scrollkeeper.log: ASCII text
secure:        ASCII text
spooler:       empty
squid:         directory
vbox:          directory
wtmp:          GLS_BINARY_ISO_FIRST
XFree86.0.log: ASCII English text
zebra:         directory
[root@RHBTst log]#
```

图6.2 浏览每个文件的类型

从图6.2可以看出，要具有正确的权限才能浏览文件的类型。

cat

接合（cat）命令将文件文本发送到标准输出。可以对任何文件使用`cat`命令。下列命令将文件文本发送到屏幕上：

```
# cat file
```

这个命令很灵活，甚至可以用`cat file1 file2`命令依次读取多个文件。

head与tail

head与**tail**命令是一个硬币的两面。**head**命令提供文件开头几行的视图，而**tail**命令提供文件最后几行的视图。可以用开关指定要显示的文件量。例如，下列命令显示**bully.txt**文件的前十五行：

```
# head -n15 bully.txt
```

如果将**head**换成**tail**，则命令显示**bully.txt**文件的后十五行。表6.7列出了这些命令使用的主要开关。

表6.7 HEAD与TAIL命令

命令	结果
head 400b bully.txt	显示文件bully.txt的前400个字节
tail 4k bully.txt	显示文件bully.txt的后4KB字节
head 3m bully.txt	显示文件bully.txt的前3MB字节
tail -n22	显示文件bully.txt的后22行

more与less

more与**less**命令不像**head**与**tail**命令一样相反，而是都从文本文件开头开始。对文本文件运行这些命令时，可以一次一页地浏览文件内容。**less**命令更灵活，可以用键盘上的Page Up与Page Down键，在任何大文本文件中上下滚动。

由于这些命令可以一点一点地读文本，因此可以比**vi**之类的文本编辑器更快打开文件。**less**命令还有一些**vi**文本编辑器的优点，可以用一些**vi**命令搜索文本。

每个命令有两组选项。下列命令对文件**bigfile**设置行号：

```
# less -N bigfile
```

打开文本文件之后，可以运行其他命令，见表6.8。

表6.8 用LESS打开文本文件之后可以运行的命令

命令	结果
space	按键盘上的空格键在屏幕上向前一页
page up	在屏幕上向前一页
page down	在屏幕上向前一页
#z	#表示一个数。例如，8z在文件中前移八行。如果不用数字，则这个命令等于space命令
/abc	在文件中搜索文本字符串abc。这个命令来自vi文本编辑器

more与**less**命令也称为分页器，可以用键盘上的Page Up与Page Down键一页一页地浏览文本文件。完成之后，只要按q键退出这个浏览方式。

权限

从ls -l的输出可以看出，每个文件有相关的拥有者、组和一系列权限（例子见图6.1）。每个文件相关的权限对拥有者、组和Linux计算机上的一切其他人指定。下面的项目是假想文件abc采用ls -l命令得到的输出：

```
-rwxrw-r-- 1 root root 1213 Feb 2 09:39 abc
```

权限基于输出最左边的字符。这10个字符确定不同用户能对这个文件干什么。

如果第一个字符不是连字符（-），则不是普通文件，可能是目录（d）或另一文件的链接（l）。

其余字符可以每三个组成一组。这三个字符是rwx，换句话说，文件abc的拥有者可以读（r）、写（w）和执行（x）这个文件。

后三个字符是rw-，即与文件拥有者同一组的用户可以读（r）和写（w），但不能执行这个文件。

最后三个字符是r--。不与文件拥有者同一组的用户可以读（r）这个文件，但不能写，也不能执行。

可以用下列命令设置任何文件的这些权限

```
# chmod 764 abc
```

权限用三位代码设置。上述命令中，第一位（7）设置拥有者权限，第二位（6）设置拥有者组权限，第三位（4）设置别人的权限。每个数字表示拥有者、组与别人的所有权限，见表6.9。

表6.9 数字权限

权限	数字	基础
r	4	= r(4)
w	2	= w(2)
x	1	= x(1)
rx	5	= r(4) + x(1)
rw	6	= r(4) + w(2)
wx	3	= w(2) + x(1)
rwx	7	= r(4) + w(2) + x(1)

再看看与文件abc相关的权限。由于第一位数是7，因此这个文件的拥有者具有读（r）、写（w）和执行（x）这个文件的权限。由于第二位是6，因此组中其他用户具有读（r）、写（w）权限。由于第三位是4，因此别人只有读（r）权限。

提示：chown与chgrp是两个密切相关的命令，根用户可以用其改变文件拥有者和组拥有者。例如，chown mj abc命令使用户mj成为文件abc的拥有者。

umask

生成新文件或目录时，得到的权限取决于umask值。在命令行界面中输入umask，可以看到权限的当前数字掩码值：

```
# umask
0022
```

要了解这个数字，就要明确权限的数字值。umask中第一个数当前未用，因此实际umask为022。

下面举一个例子。如果给每个人文件与目录的权限，则所有用户都具有读、写、执行权限，前面曾介绍过，这些权限对应于数字7（r+w+x = 4+2+1）。作用于所有用户，即得到777。也可以用下列命令对所有用户设置文件abc的同一权限：

```
# chmod 777 abc
```

习惯上，其对应于umask值000。但是，umask不能对任何文件配置执行（x=1）权限。因此，umask值022对应于权限644或rw-r--r--。换句话说，对于新文件，拥有者有读、写权限，组成员有读权限，所有其他用户有读权限。

操纵文件

可以用几个命令了解和搜索不同文件。wc命令可以取得文件中的行数、字数和字符数。find与locate命令可以搜索特定文件。grep命令可以不打开文件而搜索文件中的文本字符串。slocate与egrep命令是这些命令的变形。

wc

wc命令很简单。对任何文件，可以用wc命令取得文件中的行数、字数和字符数。例如，可以检查showoff文本文件，如下：

```
# wc showoff
1914   9298   76066
```

这些数字分别表示文件中的行数、字数和字符数。可以用表6.10所示的命令取得各个值。

表6.10 WE命令举例

命令	结果
wc -l showoff	文件showoff中的行数
wc -w showoff	文件showoff中的字数
wc -c showoff	文件showoff中的字符数

find

find命令可以从目录与子目录中搜索所选文件。例如，如果要寻找文件fig0606.tif，可以使用下列命令：

```
# find / -name fig0606.tif
```

这个**find**命令从根目录及所有子目录中搜索**fig0606.tif**文件。这个搜索可能需要较长时间。如果有更多信息，则可以将根目录（/）换成更具体的低层目录。

利用这个命令，还可以在搜索时使用通配符，如星号（*）和问号（?）。

locate与slocate

另一个搜索命令是**locate**命令。这个命令搜索数据库中的文件。默认情况下，如果计算机上一直运行Linux，则每天凌晨4点2分刷新与**locate**命令相关的数据库。如果要搜索的文件在上次更新数据库时还没有生成，则**locate**命令能更快找到文件。

在Red Hat Linux中，**locate**命令实际上是更安全**slocate**命令的软链接。数据库根据**/etc/cron.daily/slocate.cron**脚本的指示进行更新。下面看看这个脚本中的默认命令：

```
/usr/bin/updatedb -f "nfs,smbfs,ncpfs,proc,devpts" \  
-e "/tmp,/var/tmp,/usr/tmp,/aft,/net"
```

从**updatedb**手册页可以看到，**-f**开关排除几个文件系统类型，**-e**开关排除几个只能让根用户访问的目录。可以定制这个脚本，排除其他目录（如**/root**）和文件系统类型（如**vfat**）。

有了**locate**数据库之后，将会更加灵活。例如，如果使用下列命令，则返回包括文本字符串**fig0**的所有文件：

```
# locate fig0
```

locate命令就像搜索关键字前后加了星号一样。

grep

grep命令可以方便地搜索文件。系统管理员可能有个长长的用户名单。如果要从**/etc/passwd**文件中搜索用户**michael jang**，则可以使用下列命令：

```
# grep "michael jang" /etc/passwd  
mj:x:500:500:michael jang:/home/mj:/bin/bash
```

这个响应表示有个用户**michael jang**，并包括这个用户的主目录与默认**shell**。如果搜索字符串在多行中出现，则所有行都会显示。甚至可以用**grep**命令搜索一系列文件，命令如下：

```
# grep mj *  
# grep -c bash /etc/passwd
```

第一个命令寻找当前目录中所有文件中的字符串**mj**。第二个命令使用**-c**开关，计算包括单词**bash**的行数。

命令组合

我们经常把多个Linux命令放在一行中。例如，如果使用**find**命令时，知道结果会有大量文件，则可以用**grep**之类的命令来搜索结果。具体地说，假设要在系统中寻找一些**.html**文件，则可以用下列命令：

```
# find / -name *.html
```

但终端屏幕中出现几百个文件时，可能让你无所适从。这时可以使用命令组合：

```
# find / -name *.html | grep bookmark
```

这个命令搜索find命令结果中的字符串“bookmark”，只在屏幕中输出包含这个字符串的文件。其他命令组合包括：

```
# who | grep mj
# ps aux | grep mozilla
```

第一个命令who列出当前登录Linux系统的所有用户。将结果管道（|）到grep mj命令时，可以看到用户mj当前登录系统的次数。

第二个命令ps列出Linux系统中当前运行的进程。三个开关aux（ps命令开关不需要连字符）产生很长的进程表，因为它包括所有用户（a）运行的进程，带有用户名（u），独立于虚拟终端（x）。要用grep之类的工具搜索这些进程。这个命令组合返回具有单词mozilla的所有进程。

使用vi编辑器

Linux利用大量文本文件进行配置。因此，要用一个文本编辑器来配置Linux，vi编辑器看起来比较陌生，即使在Linux社区中也算不上最普及的编辑器。使用一、两个字母的命令非常古怪，但如果要用引导盘恢复系统，则vi是唯一可用的编辑器。

用vi编辑器打开文件很简单。例如，如果要打开/etc/inittab文件，则可以用下列命令：

```
# vi /etc/inittab
```

使用vi的基本方法有三种，默认为命令方式，插入方式用于插入文本，几个特殊字符可以用执行方式执行普通shell命令。

命令方式

在vi中打开文件时，第一个方式就是命令方式。我们用命令方式滚动文本、搜索不同文本字符串和删除特定字符、字、行。

vi中可以使用行号，为此要在编辑器中用下列命令激活，得到图6.3所示的结果。

```
:set nu
```

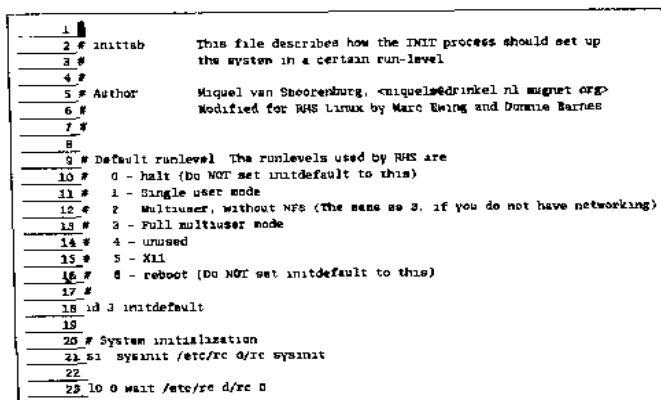


图6.3 带行号的vi

移动

尽管当前vi版本可以使用键盘上的方向键（箭头、Page Up、Page Down），但这个编辑器是为没有这些键的旧式键盘设计的。四个小写字母可以代替键盘上的方向键：

h 向左
j 向下
k 向上
l 向右

Page Up、Page Down键分别使用Ctrl+B（back）与Ctrl+F（forward）。

如果已经知道所要的行号，则可以用G命令。单独使用G命令时，转到文件最后一行。加个行号时（如20G），可以转到所要的行。和Linux shell一样，大小写很重要，这个命令一定要用大写G。

删除文本

vi中删除文本很简单。有三个删除命令与光标当前位置有关：

x 删除当前字符，包括空格或制表符
dw 删除当前单词
dd 删除当前行

如果不小心删错了内容，则可以用u命令撤销最后一个命令。

搜索文本

vi中搜索文本很容易，只要用斜杠开关。例如，如果要在文件中搜索单词dollar，输入下列命令：

```
/dollar
```

光标加亮显示文件中找到的第一个这个单词。要移到下一个实例，输入n。记住，vi编辑器中的大小写很重要。

插入方式

如果要在文件中插入文本，用插入方式。为此可以使用几种方法，取决于光标当前位置（见表6.11）。

表6.11 插入方式选项

命令	动作	说明
i	Insert	插入输入的一切，从光标当前位置开始
a	Append	插入输入的一切，从光标当前位置后一个字符开始，而A命令，插入输入的一切，从光标当前位置行末开始
o	Open	插入输入的一切，从光标当前位置下一行开始，而O命令插入输入的一切，从光标当前位置上一行开始
cw	Change word	删除与光标当前位置对应的单词（或空格），从这个单词开始插入文本

无论什么时候，很容易进入插入方式，只要在键盘上按Esc键即可。

执行方式

可以在vi编辑器内运行普通shell命令，只要在命令前面加上:!即可。例如，如果生成脚本，则可能要知道某个文件的目录地址。可以用下列命令列出/etc/cron.daily目录中的文件：

```
:!ls /etc/cron.daily
```

普通执行方式以冒号(:)开始。执行方式有几个相关的文件管理命令，包括:q（退出文件）和:w（将当前文本写入文件）。表6.12列出了不同方式中的几个基本vi命令。

提示：如果要从vi退出而不保存任何改变，则可以用!q命令。

表6.12 基本的vi命令

命令	描述
a	在当前光标位置后面开始插入方式
A	开始插入方式，添加到当前行末尾
cw	删除当前单词，然后进入插入方式，以便替换这个单词
dw	删除当前单词，而不进入插入方式
dd	删除当前行
G	将光标移到行末
15G	将光标移到第15行
h	将光标移到左边一格
I	进入插入方式
o	进入插入方式，打开当前光标下一行
O	进入插入方式，打开当前光标上一行
:q	退出vi，如果要从vi退出而不保存任何改变，则可以用:q!命令
r	用输入的下一个字符替换当前字符
:set nu	激活当前文件和行号
u	取消最后的改变
:w	写入当前文件
Esc	退出插入方式
/system	搜索当前文件中的单词系统

了解其他文本编辑器

显然，vi不是Linux中唯一的文本编辑器。另外三大文本编辑器是emacs、pico与joe，当前Red Hat Linux都没有默认安装。由于本书不是专门介绍文本编辑器的，因此这里只是简单介绍一下这些文本编辑器。

emacs

emacs也许是目前Linux/UNIX世界上最普及的文本编辑器。安装emacs RPM包之后，可以用其打开文本文件，像vi一样。例如，要在emacs中打开/etc/inittab文件，只要运行下列命令：

屏幕底部显示了可用的命令。可以看出，可以通过Get Help屏幕取得帮助和其他命令，可以用Ctrl+g命令打开。

joe

另一个常用的Linux/UNIX文本编辑器是joe，称为“Joe自己的文本编辑器”。安装joe RPM包之后，可以用其打开文本文件。例如，要在joe中打开/etc/inittab文件，只要运行下列命令：

```
# joe /etc/inittab
```



图6.6 joe文本编辑器

从图6.6可以看出，在GUI中打开joe时会打开一个控制符驱动的界面。但是，打开帮助的不是F1键，而是Ctrl+k h命令。屏幕顶部显示了可用的命令。

小结

本章介绍了命令行界面可以使用的一些基本命令。导航命令可以在Linux目录结构中移动，其他命令可以生成、复制、移动、删除和链接文件与目录。

要管理文件，就要将文件进行分类。也可以按不同方法读取每个文件中的文本。Linux可以操纵文本文件，计算行数、字数与字符数，搜索系统中的特定文件，搜索特定文件中的文本。命令组合可以帮你集中所需的信息。

也许最重要的Linux文本编辑器是vi。尽管这不是最普及的文本编辑器，但如果要恢复Linux系统，则这是惟一可用的文本编辑器。vi文本编辑器有三种方式：命令方式、插入方式和执行方式。另外三大文本编辑器是emacs、pico与joe。

知道基本shell和vi编辑命令之后，第7章要介绍Linux目录结构和设置一些关键配置文件。下一章还要介绍如何管理、格式化、标识和查错不同的硬盘分区。利用逻辑卷管理（LVM），还可以根据要求增大和缩小分区。

第7章 文件系统简介

Linux中的一切都配置成文件。第6章介绍了普通文件和其他文件的链接。我们看到，目录只是特殊类型的文件。此外，硬件设备驱动程序和分区也用文件表示。Linux文件的组织系统称为文件系统层次标准（FHS）。

文件系统通常装载到特定分区。Linux服务器通常在不同分区中有几个文件系统。可以用fdisk或Disk Druid生成分区，将其格式化成几种标准之一。如果在/etc/fstab中归档结果，则引导过程中Linux会按这里的指定装载分区。

将硬盘分成不同分区时，会失去一定的灵活性，很难扩展/home之类的专用文件系统可用的空间。逻辑卷管理（LVM）系统使文件系统长度可以扩大。本章介绍下列内容：

- 了解文件系统层次标准
- 管理分区
- 使用格式与杂志
- 使用 `/etc/fstab`
- 分析逻辑卷管理

了解文件系统层次标准

安装Linux时，可以将所有Linux目录装载到一个分区中，也可以将任何Linux目录建成不同文件系统，将其装载到不同分区。

建立不同分区可以限制系统的风险。例如，Apache之类的Web服务器中可能累积日志文件，很快超过几个GB，很容易用光硬盘上的所有自由空间。用户无法保存文件，Linux没有空间准备打印作业，从而造成混乱。

但是，如果将正确目录装载到不同分区中，则用户工作和文件保存不会因为日志文件填满分区而受到影响。

基本Linux目录结构

对Linux系统选择分区之前，首先要熟悉Linux目录选项。Red Hat Linux根据文件系统层次标准（FHS）将文件组织成目录：

/ 顶层根目录。所有其他目录都在文件系统层次的根目录之下。换句话说，它们是子目录。任何没有在另一分区中装载的目录自动放在根目录卷中。

/bin 包含基本命令行实用程序。不能在另一分区配置这个目录，否则无法在linux rescue方式中访问这些实用程序。

/boot 包括Linux启动计算机时所要的命令与文件，如统一引导装入器（GRUB）、初始内存盘和Linux内核。如果硬盘较大（超过8GB），则可以把/boot装载到另一分区，这样可以保证启动计算机时能够访问Linux引导文件。

/dev 列出可用的设备驱动程序。例如，如果装载软驱，则可以将/dev/fd0装载到/mnt/floppy之类的目录中。不能将这个目录装载到另一分区。

/etc 包含基本Linux配置命令，包括口令、Apache和Samba之类监控程序和X窗口有关的配置命令。

/home 包括除根用户以外的所有用户的主目录。如果将这个目录装载到另一分区，则要留足空间让每个用户增加文件。

/initrd 配置启动期间初始内存盘使用的空目录。不要将这个目录装载到另一分区。如果删除这个目录，则Red Hat Linux不能启动，会出现kernel panic消息。这个目录不属于FHS的一部分。

/lib 列出几个不同应用程序和Linux内核所需的程序库。不能将这个目录装载到另一分区。

/lost+found 包含孤儿文件。fsck之类的实用程序在这个目录中放上空的不可标识文件（或部分文件）。这个目录不是FHS的一部分。

/misc 指定共享NFS目录的公共装载点，这个目录不是FHS的一部分。

/mnt 软盘（/mnt/floppy）、CD-ROM（/mnt/cdrom）与Zip盘（/mnt/zip）等可拆介质的公共装载点。

/opt 包含Sun StarOffice与Corel WordPerfect之类的第三方应用程序的标准位置。

/proc 包括当前运行的所有内核相关进程。这个目录中的有些文件列出当前资源分配，如/proc/interrupts列出当前分配的中断请求（IRQ）端口。

/root 根用户主目录，/root目录是根目录（/）的子目录，不能另外装载这个目录。

/sbin 包含许多系统管理命令，不能另外装载这个目录。

/tftpboot 支持无盘工作站，也称为远程终端。无盘工作站从Linux终端服务器装载这个目录。这个目录不是FHS的一部分。

/tmp 作为临时文件的专用存储地址，也是下载文件的好地方。默认情况下，/etc/cron.daily/tmpwatch脚本从这个目录中清除超过10天的文件。

/usr 包括所有用户可用的程序与数据，包含许多子目录。例如，与OpenOffice相关联的程序安装在/usr/bin中。

/var 包含变量数据，包括日志文件和打印假脱机。在Linux服务器中，这个目录经常装载到另一分区。

说明：顶层根目录（/）不同于根用户的主目录/root。事实上，/root目录是根目录（/）的子目录。

有些目录要装载到另一分区。例如，把/home装载到另一分区后，就可以保证这个目录总是能访问该分区空间。此外，把/var装载到另一分区后，可以防止过大的日志文件抢占其他目录中文件所要的空间。下面几节将详细介绍这个方法。

分区模式

我们知道，Linux提供了各种建立分区的方法。为了帮助建立分区，可以使用几种标准分区模式。默认情况下，安装Red Hat Linux时，至少要在不同分区建立两个目录：根目录（/）和/boot。/boot目录通常装载到另一分区，因为如果把/boot目录中的文件存放到1024柱面以上的硬盘中，则许多Linux脚本无法启动。

说明：对大多数新计算机，只要启用LBA，就可以在1024柱面以上的硬盘中配置/boot目录，见第3章介绍（LBA指逻辑块寻址，是BIOS寻址硬盘柱面、磁头和扇区的方法）。

在服务器配置中安装Red Hat Linux时，默认包括几个装载目录：/home、/usr与/var。如果在不同物理硬盘中安装不同Linux目录，则可以用其他配置。表7.1包含了几个Linux分区配置。

表7.1 几个Linux分区配置

装载目录	说明
/、swap	一个硬盘的计算机上的典型配置
/、/boot、swap	具有大硬盘的计算机上的典型配置，是配置Red Hat Linux 9个人桌面版与工作站版时的默认配置
/、/boot、/var、swap	日志文件长度造成问题时可用的配置（如来自Web服务器），可以防止过大的日志文件抢占其他目录中的文件所要的空间
/、/boot、/home、swap	Linux服务器中具有几个其他用户的主目录时可用的配置。利用配额之类的其他方法可以限制各个用户占用的空间量

管理分区

将硬盘分区时，要将其组织成扇面，然后可以格式化。每个硬盘至少要有一个分区。事实上，可以把标准硬盘分成15个或16个不同分区，取决于它是IDE还是SCSI盘。

可以在硬盘上配置三种分区：

主分区 IDE与SCSI盘中可以建立最多四个主分区。一个主分区为活动分区，应包括引导装入器，如GRUB、Linux引导装入器（LILO）或Windows NT/2000/XP引导装入器。

扩展分区 如果需要更多分区，则可以将一个主分区变成扩展分区。然后将扩展分区进一步分解为逻辑分区。

逻辑分区 可以将扩展分区进一步分解为逻辑分区。SCSI盘最多可以有11个逻辑分区，而IDE盘最多可以有12个逻辑分区。

第3章在Red Hat Linux安装过程中用Disk Druid生成了不同分区。但安装Linux之后无法使用Disk Druid，而只能使用fdisk实用程序。

用fdisk实用程序增加分区

fdisk实用程序是管理分区的传统工具。尽管Linux fdisk实用程序的功能与同名的DOS工具相似，但样子不同，更加灵活，可以在现有盘上管理空余空间，可以在硬盘上配置最多四个主分区。利用fdisk实用程序可以改变分区类型，变成100多种不同类型，包括FAT32、Novell NetWare、Linux Logical Volume Manager、Linux Swap和标准Linux分区。

增加新硬盘

Linux管理员要知道如何在服务器中增加新硬盘。实际连接硬件之后,确保PC机能通过BIOS或其他方法识别这个硬件。如果PC机不能识别这个硬件,则可能是新硬件或连接有间题。

增加新硬盘之后,要进行设置与配置。fdisk实用程序是基本硬盘配置工具,如图7.1所示,其中配置两个不同的物理硬盘。

```
[root@RH9Desk root]# fdisk -l

Disk /dev/sda: 4293 MB, 4293598100 bytes
255 heads, 63 sectors/track, 522 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1 *          1           13       104391    83  Linux
/dev/sda2             14          474      3702982+   83  Linux
/dev/sda3            475          522       385500    62  Linux swap

Disk /dev/sdb: 1073 MB, 1073741824 bytes
128 heads, 32 sectors/track, 512 cylinders
Units = cylinders of 4096 * 512 = 2097152 bytes

Disk /dev/sdb doesn't contain a valid partition table
[root@RH9Desk root]#
```

图7.1 fdisk实用程序配置两个不同的物理硬盘

可以看出,fdisk -l命令列出本地计算机上的分区表。这里有两个不同的物理SCSI硬盘,指定为/dev/sda与/dev/sdb。/dev/sda硬盘中有几个不同分区。

注意/dev/sda中的柱面数,由于其与最后一个/dev/sda分区的最后一个柱面相同,因此可以看出第一个SCSI硬盘上没有建立其他分区的时间了。

如图7.1所示,没有与/dev/sdb相关联的分区。从fdisk -l命令的输出可以看出,第二个SCSI硬盘没有包含有效分区表。现在要对其进行一些配置。用下列命令通过fdisk实用程序打开第二个SCSI硬盘:

```
# fdisk /dev/sdb
```

说明: 根据PATH变量的值,可能要对fdisk之类的命令指定完全路径。如果fdisk命令本身不能工作,可以试试/sbin/fdisk。关于PATH变量的详细信息,见第8章。

如果这是全新的硬盘,则可以看到一个消息,表示硬盘不包含有效分区表。如果看不到消息,则可能是已经有人用过这个硬盘。无论如何,下面都会看到fdisk实用程序提示:

```
Command (m for help):
```

按m命令,可以看到fdisk实用程序的选项。表7.2列出了其中较重要的命令。

表7.2 FDISK实用程序命令

命令	结果
a	设置或清除可引导标志,至少要使前两个硬盘之一的一个主分区可引导
d	删除分区。实际删除分区之前,要选择分区号
l	列出已知分区类型,大约有100多种不同分区类型
m	显示可用的fdisk实用程序命令

(续表)

命令	结果
n	配置新分区
p	列出当前分区表
q	退出fdisk实用程序而不保存改变
t	可以改变分区系统ID。还要有分区号和已知分区类型的分区类型ID可以用（命令l列出）
v	验证当前分区表
w	写入改变和退出fdisk实用程序。执行这个命令之后才能将改变写入分区表

下面回到手头的工作：配置新硬盘。我们在fdisk实用程序中，首先要建立新分区。发出n命令。fdisk实用程序可以选择生成主分区或扩展分区。如果已经有扩展分区，则fdisk实用程序可以生成逻辑分区。

```
Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
```

首先用p命令生成主分区，作为第一个主分区，从第一个可用柱面开始。可以用柱面、KB或MB来指定分区长度。见图7.2所示序列。第一个分区配置成100MB，从柱面1开始。可以看出，这里100MB对应于49个柱面。

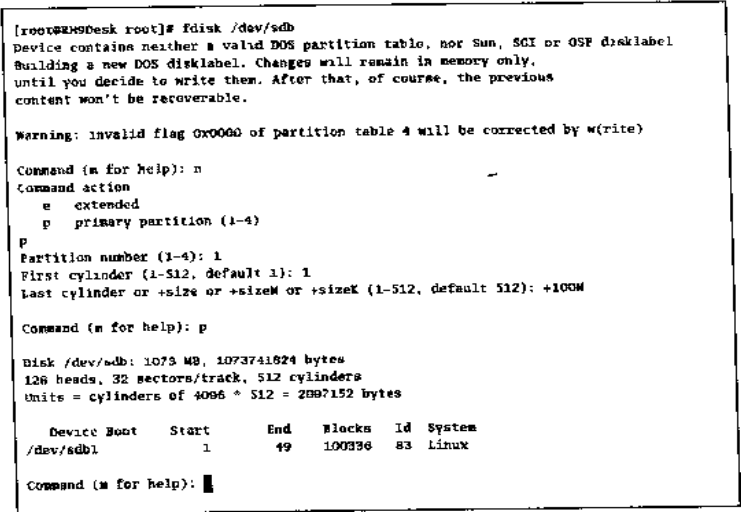


图7.2 生成主分区

可以继续这个过程，直到配置了所需空间，或对新硬盘分配的所有空间。完成分区配置之后，用w命令保存改变。如果要重新开始，则用q命令退出而不保存改变。

使用新分区之前，要先将其格式化为ext2、ext3或VFAT系统。这个过程将在本章稍后详细介绍。

管理现有硬盘

如果在很大的硬盘上安装Red Hat Linux, 则可能还会有一些多余空间。记住, 硬盘上可以配置最多15或16个不同分区, 取决于该盘是IDE还是SCSI盘。本节要切换可引导分区, 增加一个新的扩展分区, 然后增加和删除一个逻辑分区。

让分区可引导很简单。在fdisk实用程序中, 运行a命令。选择相应主分区, fdisk实用程序即会增加可引导标志。图7.3显示了这个过程。

```
(root@RH0Desk root)# fdisk /dev/sdb

Command (m for help): p

Disk /dev/sdb: 1073 MB, 1073741824 bytes
128 heads, 32 sectors/track, 512 cylinders
Units = cylinders of 4096 * 512 = 2097152 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1             1           49       100336    83  Linux

Command (m for help): a
Partition number (1-4): 1

Command (m for help): p

Disk /dev/sdb: 1073 MB, 1073741824 bytes
128 heads, 32 sectors/track, 512 cylinders
Units = cylinders of 4096 * 512 = 2097152 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1             1           49       100336    83  Linux
```

图7.3 让分区可引导

可以在计算机前两个硬盘之一的可引导分区上安装GRUB或LILO之类的引导装入器。

根据图7.2所示的配置, 新硬盘中还有463个自由柱面。Boot列下面的空间是空的, 标为Linux分区。

熟悉fdisk实用程序后, 生成扩展分区和逻辑分区很简单。但是, 也可以选择不同柱面。图7.4显示了一组命令, 可以生成扩展分区和逻辑分区。

```
Command (m for help): n
Command action
  e   extended
  p   primary partition (1-4)
e
Partition number (1-4): 4
First cylinder (50-512, default 50): 200
Last cylinder or +size or +sizeM or +sizeK (200-512, default 512): 512

Command (m for help): n
Command action
  l   logical (5 or over)
  p   primary partition (1-4)
l
First cylinder (200-512, default 200): 200
Last cylinder or +size or +sizeM or +sizeK (200-512, default 512): +300M

Command (m for help): p

Disk /dev/sdb: 1073 MB, 1073741824 bytes
128 heads, 32 sectors/track, 512 cylinders
Units = cylinders of 4096 * 512 = 2097152 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1             1           49       100336    83  Linux
/dev/sdb4            200          512       641024     5  Extended
/dev/sdb5            200          349       294896    83  Linux

Command (m for help):
```

图7.4 生成扩展分区和逻辑分区

注意, 第一个逻辑分区/dev/sdb5的柱面包含在扩展分区的柱面中。逻辑分区空间应当包含在扩展分区的空间中。

修改分区表

fdisk实用程序可以配置LVM的交换空间分区, 以及其他操作系统的分区。

用Linux fdisk实用程序生成新分区时, 其默认建立带Linux标志的新分区。可以将每个分区配置成基本Linux格式: ext2、ext3、xfs、reiserfs等等。但是, 还有几个其他标注分区的方法。

用fdisk实用程序打开要改变的分区所在的硬盘, 如图7.4。

在fdisk实用程序中, 用t命令改变分区标志。要选择分区名, 然后输入所要系统的十六进制码。例如, 下列命令将/dev/sdb5逻辑分区变成Linux交换系统:

```
Command (m for help): t
Partition number (1-5): 5
Hex code (type L to list codes): 82
Changed system type of partition 5 to 82 (Linux swap)
```

从图7.5可以看出, 可以将分区设置成适用于各种不同的操作系统。

```
Command (m for help): t
Partition number (1-5): 5
Hex code (type L to list codes): L

0 Empty          1c Hidden Win95 FA 70 DiskSecure Mult bb Boot Wizard hid
1 FAT12          1e Hidden Win95 FA 75 PC/IX          be Solaris boot
2 XENIX root     24 NEC DOS          80 Old Minix      c1 DRDOS/sec (FAT-
3 XENIX usr      30 Plan 9          81 Minix / old Lin c4 DRDOS/sec (FAT-
4 FAT16 <32M     3c PartitionMagic 82 Linux swap   c6 DRDOS/sec (FAT-
5 Extended       40 Venix 80286      83 Linux        c7 Syrix
6 FAT16          41 PPC PReP Boot   84 OS/2 hidden C: da Non-FS data
7 HPFS/NTFS      42 SFS              85 Linux extended db CP/M / CTOS / .
8 AIX            4d QNX4.x          86 NTFS volume set de Dell Utility
9 AIX bootable   4e QNX4.x 2nd part 87 NTFS volume set df BootIt
a OS/2 Boot Manag 4f QNX4.x 3rd part 8e Linux LVM      e1 DOS access
b Win95 FAT32    50 OnTrack DM      93 Amoebs        e3 DOS R/O
c Win95 FAT32 (L 51 OnTrack DM6 Aux  94 Amoebs BBT     e4 SpeedStor
e Win95 FAT16 (L 52 CP/M          9f BSD/OS        eb BeOS fs
f Win95 Ext'd (L 53 OnTrack DM6 Aux  a0 IBM Thinkpad hi ee EFI GPT
10 OPUS          54 OnTrackDM6      a5 FreeBSD       ef EFI (FAT-12/16/
11 Hidden FAT12  55 EZ-Drive         a6 OpenBSD       f0 linux/PA-RISC b
12 Compaq diagnost 56 Golden Bow      a7 NextSTEP      f1 SpeedStor
14 Hidden FAT16 <3 5c Priam Edisk       a8 Darwin UPS    f4 SpeedStor
16 Hidden FAT16  61 SpeedStor     a9 NetBSD        f2 DOS secondary
17 Hidden HPFS/NT 63 GND HURD or Sys ab Darwin boot   fd Linux raid auto
18 AIX SmartSleep 64 Novell Netware b7 BSDI fs        fe LANtapes
1b Hidden Win95 FA 65 Novell Netware b8 BSDI swap      ff BST

Hex code (type L to list codes):
```

图7.5 可用的fdisk实用程序分区系统

本章稍后将介绍最后步骤, 使新分区准备接收数据。但首先, 分区的标志可以帮助Linux用/etc/fstab装载我们需要的分区。下面看看具体做法。

使用格式与杂志

从图7.5可以看出, 可以用许多方法对不同操作系统格式化文件系统。此外, 还可以用不同方法格式化Linux分区。最新Linux版本中的杂志特征可以促进设备崩溃时快速恢复。每个过程对分区建立不同类型的标志。

基本Linux格式

前面曾介绍过，可以用几种不同方法格式化文件系统。Red Hat Linux当前默认的是第三个扩展文件系统ext3，但也可以使用许多不同的Linux文件系统。表7.3列出了主要Linux文件系统格式。

Linux正在转入杂志文件系统。杂志记录所有即将发生的改变，如要写入磁盘的数据。如果设备崩溃，则Linux可以检查杂志中即将发生的改变，而不需要检查磁盘，从而节省大量时间。

表7.3 主要Linux文件系统格式

格式	描述
ext2	第二扩展文件系统，是2001年之前Red Hat Linux的标准。如果旧系统使用ext2分区，则很容易转换成ext3文件系统格式
ext3	第三扩展文件系统，是Red Hat Linux的当前默认，包括杂志，其记录所有即将发生的改变，如要写入磁盘的数据
reiserfs	Reiser文件系统，基于与Linux扩展文件系统不同的设计
xfs	Slicon Graphics文件系统格式，支持超大磁盘

还有几个其他文件系统格式，包括ext、bfs、minix、xia与jfs，这些文件系统格式在现行Linux操作系统中很少使用。

格式化分区

Linux将mkfs命令配置成格式化Linux分区的前端。如果已经正确地格式化分区，则只要使用这个命令，Linux就会将分区重新格式化为相同文件系统，否则要用-t开关指定要建立的文件系统类型。还可以先检查坏块，之后再格式化，为此要使用-c开关。

这些命令很简单。例如，下列命令将/dev/sdb1分区格式化为指定的文件系统类型：

```
# mkfs -t ext2 /dev/sdb1
# mkfs -t ext3 /dev/sdb1
# mkfs -t vfat /dev/sdb1
# mkfs -t reiserfs /dev/sdb1
```

另一种生成ext3文件系统的方法是使用下列命令（-j生成杂志）：

```
# mkfs -j /dev/sdb1
```

如果对Linux交换空间格式化分区，则可以用mkswap命令。例如，如果要将/dev/sdb5设置为交换分区，则只要使用下列命令：

```
# mkswap /dev/sdb5
```

调整

很容易将格式化为ext2文件系统的旧分区转换成ext3。事实上，ext3文件系统与ext2基本相同，惟一的差别是ext3文件系统包括杂志。

因此, 如果对ext2文件系统生成杂志, 则其自动变成ext3文件系统。只要使用tune2fs -j命令即可。例如, 下列命令将格式化为ext2文件系统的/dev/hda1分区转换成ext3:

```
# tune2fs -j /dev/hda1
```

磁盘管理

Linux中有两个非常相似的磁盘管理命令: du和df。du(目录使用)命令列出当前目录及其下面的每个文件所用空间量。df(磁盘自由)空间命令列出每个硬盘卷上的自由空间量。图7.6列出了Linux用户在主目录中运行du命令时的输出。

左边看到的数字是文件长度(KB数), 是df与du命令的默认设置。右边显示相应文件。例如:

```
1941  ./gimp/tmp
```

第一个点号表示从当前目录开始, 斜杠(/)移到子目录, 这里是gimp。换句话说, 子目录gimp/tmp有1941 KB磁盘空间。

df命令显示计算机上每个文件系统有多满。如图7.7所示, df -m命令访问每个文件系统, 并将结果用MB数表示, 包括任何其他文件系统, 如当前装载的软盘和光碟。

-m开关将结果用MB*表示, 而-k开关将结果用KB数表示。

```
16  ./gnome-desktop
12  ./metacity/sessions
16  ./metacity
4   ./gimp-1.2/brushes
4   ./gimp-1.2/generated_brushes
4   ./gimp-1.2/gradients
182 ./gimp-1.2/palettes
4   ./gimp-1.2/patterns
4   ./gimp-1.2/plugin-ins
4   ./gimp-1.2/modules
4   ./gimp-1.2/scripts
4   ./gimp-1.2/tmp
4   ./gimp-1.2/curves
4   ./gimp-1.2/levels
4   ./gimp-1.2/fractalexplorer
4   ./gimp-1.2/gfig
4   ./gimp-1.2/gflare
4   ./gimp-1.2/gimpressionist/Brushes
4   ./gimp-1.2/gimpressionist/Paper
4   ./gimp-1.2/gimpressionist/Presets
16  ./gimp-1.2/gimpressionist
564 ./gimp-1.2
4   ./book
1120 .
[root@RH9Desk root]#
```

图7.6 运行du命令时的输出

```
[root@RH9Test root]# df -m
Filesystem      1M-blocks    Used Available Use% Mounted on
/dev/sda5        494         85       388  19% /
/dev/sda1        99          20        84  10% /boot
/dev/sda3       728         17       672   3% /home
none            62           0        61   0% /dev/shm
/dev/sda2      1984       1244       640  67% /usr
/dev/sda6       548         51       470  10% /var
/dev/cdrom       640         641        0 100% /mnt/cdrom
//laptop2/downloads 22889      8792    14097  39% /root/downloads
/dev/fd0         1           2          0  95% /mnt/floppy
[root@RH9Test root]#
```

图7.7 df -m命令输出

扩展分区数据

Linux列出每个分区的大量数据, 可以用e2label与dumpe2fs之类的命令访问。安装Red Hat Linux时, 安装过程生成的Linux分区自动得到相应的标志数据。例如, 这个命令得到下列结果:

```
# e2label /dev/sda1
/boot
```

本章稍后将会介绍, 标志很重要。默认的/etc/fstab使用磁盘标志。GRUB配置文件中也可以找到磁盘标志。但用fdisk配置新分区和用mkfs将其格式化时, 这两个命令都不增加标

志。因此，如果要在/dev/sdb1分区中装载/home/mj目录，则要用下列命令增加标志：

```
# e2label /dev/sdb1 /home/mj
```

也可以用dumpe2fs命令得到分区的更多信息。图7.8显示了具有/home/mj标志的分区。

```
dumpe2fs 1 32 (09-Nov-2002)
Filesystem volume name: <none>
Last mounted on: <not available>
Filesystem UUID: 3922f241-1d2a-42d8-b801-d0a104b230ef
Filesystem magic number: 0xEF53
Filesystem revision #: 1 (dynamic)
Filesystem features: has_journal filetype sparse_super
Default mount options: (none)
Filesystem state: clean
Errors behavior: Continue
Filesystem OS type: Linux
Inode count: 26208
Block count: 104448
Reserved block count: 5222
Free blocks: 97006
Free inodes: 26187
First block: 1
Block size: 1024
Fragment size: 1024
Blocks per group: 8192
Fragments per group: 8192
Inodes per group: 2048
Inode blocks per group: 256
Filesystem created: Fri Mar 7 07:01:03 2003
Last mount time: n/a
```

图7.8 用dumpe2fs命令显示文件系统属性

甚至可以用dumpe2fs输出中的Last Mount Time变量检查这个分区最后装载的时间，这里的n/a表示这个分区没有装载目录。

装载目录

读取和写入Linux分区之前，首先要装载目录。需要指定分区、所装载目录和分区的格式。mount命令的典型语法如下：

```
# mount -t format partition directory
```

format可以配置分区格式，如ext2、ext3或vfat。partition是要装载的硬盘设备，如/dev/sda1或/dev/hda1。directory也称为装载点，是对这个分区分配的Linux目录结构，如/boot、/home或/var。

换句话说，可以用下列命令将/home/mj目录装载到格式化ext3文件系统的/dev/sdb1分区：

```
# mount -t ext3 /dev/sdb1 /home/mj
```

这比通常的命令更复杂。/etc/filesystems配置文件中列出了格式，mount命令可以检查这个文件，找出与/dev/sdb1分区相应的格式。因此只要使用下列命令即可：

```
# mount /dev/sdb1 /home/mj
```

还可以进一步简化。如果在/etc/fstab配置文件中增加下列语句，则只要指定分区或目录即可：

```
/dev/sdb1 /home/mj ext3 defaults 1 2
```

这时可以使用下列命令：

```
# mount /dev/sdb1
# mount /home/mj
```

有时要卸载目录。例如，在许多计算机中，Linux会锁定光碟驱动器，直到用如下命令卸载目录：

```
# umount /mnt/cdrom
```

注意，这个命令是umount，而不是unmount。

查错

查错文件系统故障比Linux启动问题更复杂。第11章将会介绍，可以用现成的方法检查启动问题，而查错文件系统故障时更加困难，可能是文件搞乱、块不整齐、配置文件有错或硬件坏了。

文件系统问题通常要在引导过程中查错。Linux可能无法装载特定分区，或文件系统完整性检查遇到某种故障。无论哪种情况，都可以看到一个消息，表示fsck操作失败，要输入根用户口令以访问Linux。图7.9显示了一个例子。

```
nit al eiv L'P V q u a r : [ OK ]
initializing USB mouse. [ OK ]
Checking root filesystem
/: clean, 73416/463072 files, 300960/925745 blocks [ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Activating swap partitions: [ OK ]
Finding module dependencies: [ OK ]
Checking filesystems
fsck.ext3/dev/sdb1:
The superblock could not be read or does not describe a correct ext2
filesystem. If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
e2fsck -b 8193 <device>
/boot: clean, 41/26104 files, 12727/104391 blocks
Bad magic number in super-block while trying to open /dev/sdb1
fsck

*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** When you leave the shell,
Give root password for maintenance
(or type Control-D to continue): _
```

图7.9 Linux对文件系统问题的响应

fsck命令是个重要工具，Linux定期用其自动检查系统中的大多数分区。如果没有文件系统完整性问题，则只要调整参数和重新装载文件系统，如根目录（/）。

fsck命令

fsck命令可以检查和修复Linux文件系统，和mkfs一样，它是相关文件系统专用命令的前端，如fsck.ext2、fsck.ext3与fsck.reiserfs。如果文件系统的格式已知，则只要fsck命令就够了。如果分区格式化为ext3，则自动调用fsck.ext3命令。表7.4列出了fsck命令的几个关键开关。

表7.4 fsck命令的几个关键开关

开关	说明
-a	不加提示而自动修复目标文件系统，只在/etc/rc.sysinit中使用
-b superblock	使用不同的超块，可以用dumpe2fs命令列出可选超块
-A	检查/etc/fstab中列出的所有文件系统
-R	使用-A时，跳过根目录 (/) 文件系统
-y	fsck提出一个方案时，将默认答案设置为yes

警告：不要在装载分区中运行fsck命令，否则可能造成严重的文件系统损坏。

如果怀疑有问题，则可以在任何非装载分区运行fsck命令。一般来说，要接受修复任何文件系统问题的默认建议。尽管有些数据可能丢失，但这个过程能使分区再次可以引导，然后可以再整洁地重新启动Linux。

说明：顺便说一句，fsck命令的拼读多种多样，可以说是FS检查，也可以说是对一个分区运行fisk命令。

自动分区检查

默认情况下，fsck命令不再定期运行（但可以用tune2fs -o count /dev/partition命令改变。要寻找特定分区的装载数量信息，可以用dumpe2fs命令。图7.10显示了定期分区检查的输出信息。

```
Inode blocks per group: 255
Filesystem created: Wed Mar 26 05:06:00 2003
Last mount time: Wed Mar 26 15:16:24 2003
Last write time: Wed Mar 26 15:16:24 2003
Mount count: 8
Maximum mount count: -1
Last checked: Wed Mar 26 05:06:00 2003
Check interval: 0 (<none>)
Reserved blocks uid: 0 (user root)
Reserved blocks gid: 0 (group root)
First inode: 11
Inode size: 128
Journal UUID: <none>
Journal inode: 8
Journal device: 0x0000
First orphan inode: 0

Group 0: (Blocks 1-8192)
Primary superblock at 1, Group descriptors at 2-2
Block bitmap at 3 (+2), Inode bitmap at 4 (+3)
Inode table at 5-259 (+4)
0 free blocks, 2014 free inodes, 2 directories
```

图7.10 定期分区检查的输出信息

装载与重装

第11章介绍救援方式时的一个选项是，在只读方式中装载根目录 (/) 之类的文件系统。进行必要的改变之后，可以在读写方式中装载这个文件系统。也可以在只读方式中用usr之类的程序装载文件系统。

最终可能要改变/etc/fstab配置文件和重新启动Linux。但可以先用所要选项重装目录，测试所做改变。例如，如果要在读写方式中重装根目录 (/) ，用下列命令：

```
# mount -o remount,rw /
```


如果要在只读方式中重装/usr，用下列命令：

```
# mount -o remount,ro /usr
```

记住，这个命令所做的改变要重新启动Linux之后才生效，除非相应地修改/etc/fstab文件。

修改/etc/fstab文件

Linux在引导过程中用/etc/fstab文件按不同方式装载分区和目录。如图7.11所示，每个文件系统有几个相关的参数。这些参数确定文件系统如何装载、数据如何读取、文件系统有哪些相关用户权限，等等。

LABEL=/	/	ext3	defaults	1 1
LABEL=/boot	/boot	ext3	defaults	1 2
none	/dev/pts	devpts	gid=5,mode=620	0 0
LABEL=/home	/home	ext3	defaults	1 2
none	/proc	proc	defaults	0 0
none	/dev/shm	tmpfs	defaults	0 0
LABEL=/usr	/usr	ext3	defaults	1 2
LABEL=/var	/var	ext3	defaults	1 2
/dev/sdb1	/home/mj	ext3	defaults	1 2
/dev/sda7	swap	swap	defaults	0 0
/dev/cdrom	/mnt/cdrom	iso9660	noauto,owner,kudzu,ro	0 0
/dev/floppy	/mnt/floppy	autofs	noauto,owner,kudzu	0 0

图7.11 /etc/fstab确定文件系统如何装载

可以看出，/etc/fstab中每一行有六个不同字段。表7.5列出了这些字段，从左到右进行介绍。

表7.5 /etc/fstab字段

列号	字段	描述
1	Label	要安装的文件系统（如/usr）或分区（如/dev/sdb1）
2	Mount Point	要装载的分区或文件系统所在目录
3	Format	文件系统格式类型，如ext2、ext3与reiserfs
4	Mount Options	默认选项包括rw（读写）、suid（SUID 权限）、dev（终端与磁盘之类的块设备）、exec（二进制文件）、auto（自动装载）、nouser（只有根用户可以装载）和async（数据异步读写）
5	Dump Value	1表示文件系统自动写入磁盘
6	Filesystem Check Order	需要fsck的文件系统，根文件系统为1，本地计算机上的其他文件系统为2，交换、虚拟、光碟、软盘和远程目录为0

大多数情况下，用LABEL=/之类的清单检查计算机上的分区数据，寻找要装载的实际分区设备，如/dev/hda3。

还有其他装载选项，如usrquota与grpquota（设置配额）、noauto（保证Linux引导时不寻找光碟或软盘）和user（让任何用户装载文件系统，如光碟）。

探索逻辑卷管理系统

如果没有逻辑卷管理系统（LVM），则安装Red Hat Linux期间一定要确定如何将硬盘分区。一旦硬盘分区之后，就很难扩大各个分区空间。

例如，假设在另一分区中建立/home目录。事先计划了10个用户所需的空间。但随着公司扩大，需要20个用户所需的空间。如果没有逻辑卷管理系统，则很难扩大/home分区长度，需要备份/home中的文件，寻找具有足够空间的分区，然后将文件恢复到这个分区。

逻辑卷管理系统可以在不同文件系统之间重新分析磁盘空间块。利用逻辑卷管理系统，就可以在/var之类的文件系统中还有多余空间时，将多余空间分配给/home目录。

可以在安装Red Hat Linux期间生成逻辑卷管理系统卷组，见第3章介绍。也可以用下面几节介绍的方法，生成和管理逻辑卷管理系统卷组。即使安装Red Hat Linux期间已经生成逻辑卷管理系统卷组，也请继续阅读下文。如果不能用本章介绍的命令增加与减少逻辑卷长度，则逻辑卷管理系统也没什么用。

基础

逻辑卷管理系统实际上是硬盘中不同物理段的映像。集合到一个逻辑卷之后，/home与/usr之类的文件系统可以装载到这个卷中。逻辑卷可以重新组织，包括增加的硬盘空间。

下面简要介绍逻辑卷管理系统的功能，要了解逻辑卷管理系统的工作，首先要了解几个基本定义：

物理卷（PV, Physical volume） 物理卷通常对应于硬盘上的标准主分区或逻辑分区。

物理块（PE, Physical extent） 物理块是磁盘空间块。物理卷分成几个等长的物理块。

逻辑块（LE, Logical extent） 逻辑块是磁盘空间块。逻辑卷管理系统中的逻辑块长度与这个系统中的物理块长度相同，每个逻辑块对应于特定物理块。

逻辑卷（LV, Logical volume） 逻辑卷是逻辑块的集合，可以在逻辑卷中装载/usr与/boot之类的文件系统。

卷组（VG, Volume group） 系统中的逻辑卷集合起来即可形成卷组。配置逻辑卷管理系统时，大多数命令都是针对卷组的。

生成物理卷

首次实现逻辑卷管理系统时，最好在新硬盘上配置。安装硬盘之后，先不要安装任何分区。可以在整个硬盘上建立一个逻辑卷管理系统。例如，如果硬盘是辅助IDE接头上的从盘，则Linux设备为/dev/hdd。要在这个盘上建立物理卷，用下列命令：

```
# pvcreate /dev/hdd
```

如果已经用fdisk之类的实用程序建立分区，则可以在特定分区上建立物理卷。首先运行fdisk实用程序，改变所要分区的系统ID。进入fdisk实用程序菜单之后，可以用下列命令改变硬盘上的假想分区号：

```
Command (m for help): t
Partition number (1-15): 1
Hex code (type L to list codes): 8e
```

不要对需要保留数据的任何分区使用这个命令。一旦改变Linux逻辑卷管理系统类型，就可以用下列命令生成物理卷：

```
# pvcreate /dev/hdd1
```

配置两个或多个物理卷之后，下一步要生成卷组。

生成卷组

卷组是一个或几个硬盘上配置的物理卷的集合。增加更多物理卷时，可以将其加进现有卷组。

生成卷组很简单，甚至可以用下列命令指定所要的卷组名（如programs）：

```
# vgcreate programs /dev/hdd1 /dev/sd1
```

生成卷组之后，可以用下列命令将物理卷加进现有卷组：

```
# vgextend programs /dev/sd1
```

然后将卷组组织成物理卷中可以建立的块。

生成逻辑卷

最后要生成逻辑卷，装载/home与/var之类的文件系统。但首先要知道卷中物理块的长度。为此可以使用vgdisplay命令。用上节生成的卷组时，命令如下：

```
# vgdisplay programs
```

图7.12显示了样本输出。可以看出，其中包括这个组的最大逻辑卷与物理卷个数、卷组长度和卷组中的物理块长度（图中为4MB）。

```
[root@rh19 root]# vgdisplay programs
--- Volume group ---
VG Name                programs
VG Access               read/write
VG Status               available/resizable
VG #                    0
MAX LV                  256
CUR LV                  0
Open LV                 0
MAX LV Size             255.99 GB
Max PV                  256
Cur PV                  2
Act PV                  2
VG Size                 392 MB
PE Size                 4 MB
Total PE                98
Alloc PE / Size         0 / 0
Free PE / Size          98 / 392 MB
VG UUID                 QqCwYF-KzDI-6ynj-Dny6-zjnx-13Lu-25kHeF

[root@rh19 root]#
```

图7.12 卷组细节

然后即可用下列命令生成所要长度的逻辑卷：

```
# lvcreate -l num_of_PEs programs -n logicvol
```

上例中新的逻辑卷名为logicvol。由于物理块长度为4MB，因此，如果要建立200MB的logicvol逻辑卷管理系统分区，则可以将num_of_PEs改成50。

这样就生成了新设备/dev/programs/logicvol。现在可以像任何其他硬盘分区一样，格式化和装载这个设备。例如，下列命令将其格式化为ext3文件系统，将其装载到/tmp目录：

```
# mkfs -j /dev/programs/logicvol
# mount -t ext3 /dev/programs/logicvol /tmp
```

现在很容易增加/dev/programs/logicvol设备长度。假设还有多余的物理块，则只要用lvextend命令。下列命令将/dev/programs/logicvol长度增加到了300MB：

```
# lvextend -L300M /dev/programs/logicvol
```

小结

本章介绍了Linux中文件与文件系统的工作原理。文件组织成独特的FHS（文件系统层次标准）结构。FHS中的不同目录具有不同功能，可以容纳多目录装载到不同分区。

fdisk实用程序是基本Linux分区管理实用程序。利用这个实用程序，可以管理现有硬盘或新装硬盘上的空余空间。可以生成新分区，确定新分区长度，设置与改变分区的Linux格式。

有了新分区之后，可以用mkfs命令格式化。很容易将分区格式化成Red Hat Linux标准格式——ext3文件系统，只要用mkfs -j命令即可。甚至可以用tunefs -j命令将现有ext2文件系统转换成ext3分区。Red Hat Linux经常用fsck命令查错分区。

/etc/fstab是个关键的文件系统配置文件，定义不同分区的装载与检查方法。

利用逻辑卷管理系统，可以根据分区在卷组中的配置，改变分区长度。

了解基本文件系统知识后，下一章继续介绍shell。我们将介绍如何有效利用shell。

第8章 有效利用shell

前面两章介绍了导航与管理Red Hat Linux的许多基本命令。本章介绍如何有效利用shell。

默认Red Hat Linux shell是bash（是Bourne Again Shell的简称）。尽管还有另外几个shell，但bash是自由软件基金会（www.fsf.org）建立的默认shell，因此是与Linux关系最密切的shell。

如果你已经熟悉Korn、C与Z之类的不同shell，则可以安装相应RPM包，使用这些shell。它们很容易打开，ksh、csh与zsh命令分别自动打开这三个shell，出现的提示有所不同。和其他UNIX操作系统一样，Linux也适用于所有这些shell。但是，如果你首次进入UNIX操作系统，则建议使用bash，这是Linux的默认shell，大多数联机Linux文档都是针对这个shell的。

本章介绍如何管理bash的基本内容，然后介绍shell的秘密，帮你在复杂环境中巧妙利用不同的bash命令。最后，我们要利用环境与shell变量，简化向bash shell的过渡。本章包括下列内容：

- 管理shell
- 配置shell
- shell的秘密

管理shell

Bourne Again Shell（bash）是Linux操作系统的用户界面。可以用bash命令运行程序、管理文件，通过Linux内核与硬件互动。可以用几个局部和系统文件、变量配置bash。

bash之类的shell也称为命令行解释器，是响应特定命令的用户界面，如ls、cd与cp。shell还响应生成的程序与脚本。

使用这些命令时，记住Linux是大小写相关的。换句话说，ls命令列出当前目录中的文件，而LS、Ls或lS命令在当前Linux shell中没有意义。

bash shell的两个帮助作用基于过去的命令和简化长命令完成，称为互动性与命令完成特性。

互动性

互动性可以访问过去的命令，也可以和当前命令互动。可以用Home和箭头之类的键纠正输入错误，甚至可以使用文本编辑器中的命令。

互动与历史

可以和过去的命令互动。打开命令行界面，输入history命令。如果过去用过这个命令行界面，则可以看到图8.1所示的结果。

```

80 mount
81 fdisk -l
82 quota
83 df
84 alias
85 mount
86 mkdir /mnt/source
87 mount '//laptop3/redhat' /mnt/source
88 ls
89 df
90 ps
91 vi /etc/passwd
92 cat /etc/inittab
93 fdisk -l
94 switchdesk kde
95 man dnf2fs
96 rpm -q kernel-source
97 redhat-config-xfree86
98 mount
99 df
100 mozilla &
101 alias
102 history
root@RH9Desk root]#

```

图8.1 过去的命令

默认情况下，可以用几种方法重复过去的命令。最简单的方法是用键盘上的向上与向下箭头键。到命令行界面中，按向上箭头键，可以看到过去的命令，按逆序排列。这个清单甚至还包含上次会话中使用的命令。可以用向下箭头键将这个过程逆转。

如果记住最近命令的第一个字母，则可以用感叹号(!)回叫这个命令。例如，根据图8.1中history命令的输出，如果输入!r，则shell会回叫上次使用的以r字母开头的命令，并运行这个命令，这里是redhat-config-xfree86。

这个特性非常灵活，可以增加更多信息，如!rp。根据图8.1中history命令的输出，这时运行rpm -q kernel-source命令。如果输入env | more命令，则可以找到HISTSIZE=1000语句，表示可以回溯和重新运行过去1000条命令。

互动与编辑器

还可以和当前或过去命令的细节互动。例如，下列命令中有个输入错误：

```
# rpm -Vvh /mnt/cdrom/RedHat/RPMS/sendmail-*
```

实际上要输入rpm -Uvh命令，但你又不想重输整行。好在没必要删除整行命令，而可以用Home和箭头之类的键，将光标移到命令开头，纠正输入错误。

也可以使用文本编辑器中的命令。例如，如果将vi设置为默认命令行编辑器，则可以运行下列命令：

```
# set -o vi
```

说明：set命令比较不直观，set -o editor启用编辑器，而set +o editor关闭编辑器。这个命令中的编辑器可以是emacs或vi。

现在可以使用vi编辑器命令。默认情况下，我们是在命令行界面的插入方式中。第6章曾介绍过，可以按Esc键切换到命令方式。然后可以对这个语句采用所选的vi编辑器命令。表8.1列出了一些第6章没有介绍的vi编辑器命令。

表8.1 更多vi编辑器命令

命令	描述
Home	移到行开头
b	左移一个单词
w	右移一个单词

记住，还有其他vi编辑器命令，例如cw，删除当前单词并开始插入方式。

命令完成

bash shell还可以用Tab键完成命令，只要输入命令的一部分。例如，要用ypdomainname命令寻找系统的NIS域名，输入下列字母：

```
# ypd
```

然后用Tab键完成命令。如果有多个以ypd开头的命令，则可以再次按Tab键，得到这些命令的清单。

配置shell

任何shell都有两组配置文件，一组是系统级的，影响Linux计算机上的所有用户；一组是用户特定的，存放在用户的主目录中。

根据发行版本情况，bash有两个基本的系统级配置文件：`/etc/bashrc`与`/etc/profile`。这些配置文件包含两组不同变量：shell变量与环境变量。前者只在特定shell中固定（如bash中），后者在不同shell中固定。

换句话说，shell变量是局部的，而环境变量是全局的。

shell变量

默认Red Hat Linux的`/etc/bashrc`配置文件如图8.2所示，设置两个基本shell变量：umask的默认值和命令行界面的光标位置出现的提示。

```
# /etc/bashrc

# System wide functions and aliases
# Environment stuff goes in /etc/profile

# by default, we want this to get set.
# Even for non-interactive, non-login shells.
if [ "id -gn" = "id -un" -a "id -u" -gt 99 ]; then
    umask 002
else
    umask 022
fi

# are we an interactive shell?
if [ "$PS1" ]; then
    if [ -x /usr/bin/tput ]; then
        if [ "x`tput kbs`" != "x" ]; then # We can't do this with "dumb" terminal
            stty erase tput kbs
        elif [ -x /usr/bin/wc ]; then
            if [ " `tput kbs/wc -c` " -gt 0 ]; then # We can't do this with "dumb" te
                stty erase tput kbs
            fi
        fi
    fi
    case $TERM in
        xterm*)
            if [ -e /etc/sysconfig/bash-prompt-xterm ]; then
                PROMPT_COMMAND=/etc/sysconfig/bash-prompt-xterm
            fi
        ;;
    esac
fi

"/etc/bashrc" 561, 1497C
```

图8.2 `/etc/bashrc`文件

这些配置文件使用每个用户主目录中的可定制文件，默认包括**.bash_history**、**.bash_logout**、**.bash_profile**与**.bashrc**。尽管可以定制每个文件，但其中包含几个默认。每个文件前面的点号将其从正常搜索中隐藏。可以用**ls -a**命令浏览隐藏文件。

.bash_history 包括前面的bash命令历史。一些管理员不喜欢这个文件，因为从中可能猜出你用的命令。可以在**.bash_profile**文件中加上**HISTFILESIZE=0**，切断这个过程，如图8.3所示。

```
mount '//laptop3/redhat' /mnt/source
mkdir /mnt/source
mount '//laptop3/redhat' /mnt/source
ls
df
ps
vi /etc/passwd
cat /etc/inittab
fdisk -l
switchdesk kde
man dmp2fs
rpm -q kernel-source
redhat-config-xfree86
mount
df
mozilla &
alias
history
mount -o userxname=michael '//laptop3/ml3' book
quota
vi /etc/passwd
vi .bash_logout
vi .bash_history
```

图8.3 .bash_history中有大量过去的命令

.bash_logout 设置何时退出shell的命令。默认情况下，其中有一个clear命令，从当前终端窗口删除前面的命令。图8.4显示了简单的默认**.bash_logout**文件的样本。

```
~/.bash_logout
clear
#
# This file is read by bash when the shell exits.
#
# The commands in this file are executed with /bin/sh.
#
# .bash_logout' 3L, 24C                                2.0-1      All
```

图8.4 主目录.bash_logout

.bash_profile 从**.bashrc**文件取得更多配置数据。将**/bin**目录加进**PATH**，如图8.5。如果增加**HISTFILESIZE=0**变量，则记住将其加进这个文件的导出表中。

.bashrc 从**/etc/bashrc**文件取得基本配置数据。对根用户，这个文件增加**rm**、**mv**与**cp**命令的别名，防止意外删除文件，如图8.6。


```
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
    . ~/.bashrc
fi

# User specific environment and startup programs


PATH=$PATH:$HOME/bin
BASH_ENV=$HOME/.bashrc
USERNAME="root"

export USERNAME BASH_ENV PATH


--
-
-
-
-
-
-
-
-
".bash_profile" 15L, 234C
```

图8.5 主目录.bash_profile

```

1 .bashrc
2
3 # Set up if alias is found
4
5 alias mv='mv -i'
6 alias cp='cp -i'
7 alias mv='mv -i'
8
9 # Source global definitions
10 if [ -f /etc/bashrc ]; then
11     . /etc/bashrc
12 fi
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

```

图8.6 主目录.bashrc

对shell变量运行**export**命令时，实际上使其变成全局变量（或环境变量）。全局变量也可以在程序中使用。

说明: 记住, 如果不在主目录的.bash文件中记录, 则下次登录Linux时, 设置返回原先的配置。

环境变量

默认环境变量很多，可以用`env`命令浏览。其中有些通过`/etc/profile`设置，包括文件名颜色、安全`shell`设置、默认终端与显示变量。表8.2列出了一些标准环境变量。

表8.2 一些标准环境变量

环境变量	说明
SHELL	默认shell
LANG	默认语言

(续表)

环境变量	说明
BASH_ENV	bash shell的环境变量，通常在~/.bashrc中
DISPLAY	X窗口使用的控制台，DISPLAY=:0对应于控制台F7，DISPLAY=:1对应于F8，DISPLAY=server:0向远程计算机发送GUI应用程序
COLORTERM	GUI中的默认终端，通常是gnome-terminal
PATH	Linux自动从路径中搜索所有目录，寻找所要命令，按回显\$PATH命令的输出顺序搜索。/etc/profile自动在根用户的PATH中增加几个目录
USER	自动设置当前登录用户的用户名
LOGNAME	通常设置为\$USER
MAIL	设置为特定\$USER的标准邮件目录
HOSTNAME	设置为/bin/hostname命令输出
HISTSIZE	设置为history命令记住的命令数
INPUTRC	设置为默认键盘映像，详见/etc/inputrc

环境变量很容易复位。其中最重要的是PATH。假设在/opt/data/db/programs目录中增加了几个脚本，不想在每次运行这些程序时显示完整目录路径，则可以用下列命令将这个目录加进PATH中：

```
# PATH=$PATH:/opt/data/db/programs
```

现在，要运行/opt/data/db/programs/script1之类的程序，只要输入script1并按Enter键。但要记住，为了使改变保存起来，就要修改主目录中的.bash_profile配置文件，反映PATH的改变。要在PATH中寻找当前目录，用echo \$PATH命令。

shell的秘密

bash shell可以使用几个方法。例如，可以将一个命令的输出定向到一个文件或另一命令。shell可以建立别名，定义所选的命令。还可以将运行程序移到后台，从而不必打开另一虚拟终端或控制台。

mash shell很灵活，可以用不同命令管理bash命令的输入。例如，可以用两种通配符表示多个文件。Linux可以用引号管理命令输入。

其他的可以方便地移到任何主目录，设置别名以简化管理，在Linux目录树中快速上下移动。

数据流

Linux中的数据流有三种：输入、输出和错误。这些概念也称为标准输入（stdin）、标准输出（stdout）和标准错误（stderr）。

标准输入通常来自键盘。例如，如果运行ls c*命令，则c*是ls命令的标准输入。

标准输出是命令的结果。例如，输入ls之后看到的文件是标准输出，通常定向到显示器。

如果没有标准输出，则可能有一个错误消息，这就是标准错误数据流，通常也定向到显示器。

可以用两个基本方法定向输入、输出和错误。可以将一个数据流引入到另一个命令，也可以在数据流与文件之间进行改方向。

改向输入与输出

通常，标准输入来自键盘。但如果数据放在一个文件中，则不必重新一一输入，而可以将这个数据文件用小于号(<)改向到程序中。例如，下列命令将database_data文件改向到database_program中：

```
# database_program < database_data
```

许多情况下，要把标准输出保存在一个文件中。例如，下列命令用大于号(>)将标准输出保存在文件filelist中：

```
# ls > filelist
```

覆盖文件filelist中的任何数据。也可以用双大于号(>>)将数据添加到文件filelist末尾：

```
# ls >> filelist
```

同一命令中可以组合这些改向箭头。例如，如果database_program程序产生大量输出，则可以保存起来，后面再慢慢分析：

```
# database_program < database_data > database_output
```

标准错误输出可以帮助诊断程序故障。例如，如果程序在半夜运行，则可以将这个程序的标准错误定向到一个文件中，以便发生错误时找到线索。例如，下列命令将标准错误定向到文件errorlog中：

```
# database_program < database_data 2> errorlog
```

同样，也可以用双大于号(>>)将数据添加到文本errorlog末尾：

```
# database_program < database_data 2>> errorlog
```

提示：检查标准错误时，注意2>和2>>的字符之间不能有空格。

文件描述符与数据流

这个说明是为编程人员提供的。shell中的进程处理文件时，会建立一个文件描述符。系统调用这些程序，帮助管理这个进程。

标准文件描述符有三个：0、1、2。文件描述符0对应于标准输入，或大于号(>)。文件描述符1对应于标准输出，或小于号(<)。文件描述符2对应于标准错误，在bash shell中为2>。

输出与输入管道

就像stdin、stdout、stderr和特定文件之间可以改向一样，也可以将这些数据流改向到其他命令。如果要检查大量文件的权限，则可以使用两个不同命令：

```
# ls -l > tempfiles
# more tempfiles
```

第一个命令取得当前文件列表，将结果存放在tempfiles文件中。第二个命令读取tempfiles文件，一次读一屏。由于文件列表可能经常改变，因此应删除过时的tempfiles文件。

但这样效率很低。也可以用管道符号 (|) 组合这些命令，这个字符在美式键盘的反斜杠上方。例如，下列命令等价于上述两个命令：

```
# ls -l | more
```

管道 (|) 取得ls -l命令的标准输出，将其作为标准输入发送到more命令，而不需要生成和删除任何临时文件。

后台运行

Linux是个多任务系统。如果不想打开更多终端和虚拟控制台，则可以用一个命令行运行多个程序。例如，编译内核时，有些步骤可能需要几个小时。如果在后台运行程序，则不必等待，可以运行其他程序。

可以用两种方法在后台运行程序。例如，假设当前目录中有个脚本test。这个脚本在一小时内发警报。我们要运行test程序，但不想等上一个小时。为此，可以运行下列命令：

```
# ./test &
```

和号 (&) 将程序放到后台执行。程序继续运行，你又回到命令行界面。

说明：./programname命令在当前目录中运行程序，如果当前目录不在PATH中，则这是运行本地程序的最简单方法。

如果程序要计算pi的值，算到无穷位，则这个程序要很久才能完成。如果没有使用&号，则要用另一种方法将程序放到后台执行。Ctrl+Z命令暂停运行程序，bg将程序放到后台执行。

特殊shell字符

可以用特殊shell字符规定标准输出。也许你已经在shell中指定了一些特殊字符，可以用stty -a命令检查，得到图8.7所示的输出。

```
[root@RH9Desk root]# stty -a
speed 38400 baud; rows 24; columns 80; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D; eol = M-^?; eol2 = M-^?;
start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R; werase = ^W; lnext = ^V;
flush = ^O; min = 1; time = 0;
-parenb -parodd cs8 hupel -cstopb cread -cllocal -crtscts
-ignbrk brkint -ignpar -parmrk -inpck -istrip -inlcr -igncr icrnl ixon -ixoff
-iuic ixany inaxbel
opost -olcuc -ocrnl onlcr -onocr -onlret -ofill -ofdel n10 cr0 tab0 bs0 vt0 ffo
tsig icanon ixexten echo echoe echok -echonl -noflsh -xcase -tostop -echoprt
echoctl echoke
[root@RH9Desk root]#
```

图8.7 特殊shell字符

这个输出显示了一些特殊字符和设置。输出中，折号 (^) 对应于键盘上的Ctrl键。例如，intr = ^C设置表示用Ctrl+c键组合中断运行程序。表8.3列出了一些默认特殊字符，这些只是默认特殊shell字符，还可以定制特殊字符，用于不同命令。

提示：输入shell字符的方式与`stty -a`命令输出不同。例如，`eof`字符显示为`^D`（大写D），而实际上要按`Ctrl+d`（小写d）退出终端。

表8.3 特殊shell字符

字符	描述
<code>^C</code>	中断与停止运行程序
<code>^_\</code>	发送退出命令
<code>^D</code>	停止标准输入，退出控制台
<code>^Z</code>	暂停运行程序

还有几个带连字符和不带连字符的设置。例如，`igncr`设置忽略回车符，而`-igncr`设置表示不忽略回车符。换句话说，按键盘上的`Enter`键时，`shell`提供新提示。`echo`设置表示在终端上显示键盘中输入的内容。

可以用`stty`命令指定不同的特殊字符集合。例如，要用`Ctrl+x`而不是`Ctrl+z`停止程序，用下列命令：

```
# stty susp ^X
```

警告：`stty`命令非常危险。例如，如果输入`stty -echo`命令，则不会在终端上显示键盘中输入的任何内容，要输入`tttyo.hk`命令之后才能恢复原样配置。如果黑客在登记配置文件中输入`stty -echo`命令，则会让人百思不得其解。

代词符与主目录

`bash shell`中的一个关键字符是代词符（`~`），表示当前登录用户的主目录。在大多数标准美式键盘中，可以看到这个代词符和反撇号（```）在一起，在`Tab`键上方。

可以在大多数`bash shell`命令中使用代词符。例如，用户可以用`cd ~`命令导航到自己的主目录，也可以用`ls ~`命令列出主目录中的文件。表8.4列出了几个使用代词符的命令例子。

表8.4 使用代词符的命令例子

命令	结果
<code>cd ~</code>	导航到自己的主目录
<code>cd ~/.kde</code>	移到主目录中的 <code>.kde</code> 目录。例如，如果用户名为 <code>mj</code> ，则移到 <code>/home/mj/.kde</code> 目录
<code>ls ~</code>	列出主目录中的文件
<code>tar czvf homebk.tar.gz ~</code>	备份主目录中的文件
<code>~/yourprogram</code>	运行主目录中的程序 <code>yourprogram</code>

也可以在Linux脚本中使用，因为代词符可以帮助配置Linux服务器上的脚本，所有用户都可以使用。

连接点号

点号是`bash shell`中与斜杠同样重要的工具。点号（`.`）表示当前目录，而双点号（`..`）可以移到父目录。

可以在许多bash命令中使用点号。例如，如果服务脚本在/etc/rc.d/init.d目录中，则不一定需要输入每个命令的完整路径，而可以运行./iptables状态命令，检查防火墙的当前状态。

通配符

Linux命令中有两个特殊字符，是Microsoft通配符的变形，分别是星号（*）与问号（?）。星号（*）表示多个字母或数字，而每个问号表示一个字母数字字符。例如，如果运行下列命令，则可以得到以字母a开头的所有文件的清单：

```
# ls a*
```

如果有个文件a，则其会在清单中，相反，如果运行下列命令，则可以得到以字母a开头的两个字符的文件清单：

```
# ls a?
```

如果有个文件a，则其不在清单中，但文件ab、ac、ad在这个清单中。也可以用下列命令进行更复杂的文件搜索：

```
# ls ?at?
```

这个命令返回cate、kata与nate之类的文件名，而不返回Catherine、matador与cat之类的文件名。

甚至可以用方括号（[]）定义更详细的特殊字符。例如，如果要显示目录中f0801.tif到f0806.tif之间的所有文件，则可以用下列命令：

```
# ls f080[1-6].tif
# ls f080[123456].tif
```

提示：在Linux世界中，使用通配符的技术也称为全局化。

Shell中的斜杠

Shell中的斜杠（/）表示根目录，多个斜杠可以在子目录间导航，如/etc/rc.d/init.d。

反斜杠（\）是个特殊字符。例如，如果要在/etc/shadow文件中找一个星号（*），则可以用下列命令：

```
# grep * /etc/shadow
```

但这个命令在/etc/shadow所在的当前目录中寻找每个文件。

这是因为，星号是个通配符，根据上下文，寻找几乎一切内容。这时可以使用反斜杠（\）。将反斜杠（\）放在特殊字符前面，可以转义特殊字符。

换句话说，下列命令实际上在/etc/shadow文件中找一个星号（*）：

```
# grep \* /etc/shadow
```

反斜杠还有其他用处，例如列出双单词目录，如Microsoft的My Documents。例如，如果要从远程计算机的/mnt/win1目录装载Microsoft Windows盘，则可以用下列命令列出该目录中的文件：

```
# ls /mnt/win1/My Documents
```

这个命令寻找两个不同目录/mnt/win1/My与Documents。问题是，单词My与Documents之间有空格。增加反斜杠时，shell忽略这个空格，列出My Documents目录中的文件清单：

```
# ls /mnt/win1/My\ Documents
```

引号

键盘上有三种引号：单引号（'）、双引号（"）和反引号（`）。用于标准输入时，它们完成不同功能。

这些引号之间的差别是对变量有不同作用，包括变量（如\$NAME）和shell命令（如date）。对任何引号对，shell将引号中的一切发送到命令中。下例中，使用echo命令，具体差别如下：

单引号 shell不处理任何变量与命令。

双引号 shell处理变量（如\$NAME），但不处理任何命令。

反引号 shell把引号中每个单词作为一个命令。如果是变量，则先求值，然后作为一个命令处理。这样，如果\$NAME在反引号中，则要处理，然后把结果作为一个命令求值。

下面举一个例子加以说明。假设NAME=Michael。记住date命令返回当前日期和时间。第一个命令没有引号，shell解释\$NAME变量，但不运行date命令：

```
# echo Welcome $NAME, the date is date
Welcome Michael, the date is date
```

下一个命令把输入放在单引号中，使shell不处理任何变量与命令：

```
# echo 'Welcome $NAME, the date is date'
Welcome $NAME, the date is date
```

下一个命令把输入放在双引号中，结果与没有引号时相似：

```
# echo "Welcome $NAME, the date is date"
Welcome Michael, the date is date
```

最后一个命令放在反引号中，shell要解释命令：

```
# echo "Welcome $NAME, the date is `date`"
Welcome Michael, the date is Fri Jan 17 15:52:02 EST 2003
```

别名

另一个最重要的shell变量是别名。输入alias命令时，就得到可以替换的命令表。图8.8显示了根用户的别名例子。

```
[root@RH9Desk root]# alias
alias cp='cp -i'
alias l.='ls -d .* --color=tty'
alias ll='ls -l --color=tty'
alias ls='ls --color=tty'
alias mv='mv -i'
alias rm='rm -i'
alias which='alias | /usr/bin/which --tty-only --read-alias --show-dot --show-ti
lde'
[root@RH9Desk root]#
```

图8.8 根用户的别名

前面曾介绍过，这个清单是cp、mv和rm命令的别名，可以防止不小心删除文件。很容易生成其他别名。例如，下列命令使rx成为redhat-config-xfree86命令的别名：

```
# alias rx=redhat-config-xfree86
```

现在，输入rx命令时，bash shell调用redhat-config-xfree86实用程序。可以用unalias命令逆转这个过程。例如，下列命令删除redhat-config-xfree86的别名：

```
# unalias rx
```

提示：可以对经常使用的复杂命令建立别名。例如，alias le='ls -ltr /etc | more'命令可以在检查/etc配置文件时非常方便。如果要保存别名的改变，则可以将其加进主目录的.bashrc文件中。

小结

尽管bash shell中包括大量命令，但bash shell的细节很简单。互动性使它很容易回叫过去的命令。命令完成特性可以用几个键加Tab键寻找所要的命令。

Shell与环境变量在/etc和用户主目录的一些基本配置文件中维护。这些变量确定命令界面的基本设置。其他变量确定历史容量、默认终端、标准电子邮件目录，等等。

Shell有几个秘密，包括三个基本数据流：标准输入、标准输出和标准错误。还可以在后台运行命令。特殊shell字符及置终端参数。可以用Ctrl键在键盘上进行不同操作。代词符(~)表示任何用户主目录。

点号和双点号可以在Linux文件系统层次中导航。通配符可以标识文件与命令，甚至不需要知道全名。斜杠可以在目录间导航，而反斜杠则改变星号、问号等特殊字符的含义。单引号、双引号与反引号可以按不同方式处理变量和命令。别名可以更名容易忘记的命令。

第二部分就讲完了，我们已经介绍了Linux的基础。第三部分要介绍几个基本管理功能。第9章介绍如何管理用户与组。Red Hat Linux用阴影口令组、配额、用户专用组模式管理用户与组，从而提高安全性。

第三部分 基本Linux管理

第9章 安全管理用户与组

Linux管理员的关键任务之一是维护用户与组。即使计算机是只有一个专门用户的工作站，至少也要在计算机上维护根用户账号和普通账号。

用户与组用/etc目录中的几个基本文件配置。Red Hat Linux生成用户时，可以直接编辑这些文件，也可以使用一些基本命令。无论使用哪种方法，都可以用其他命令和配置文件管理用户账号及其口令。

阴影口令组使Linux可以提供另一层保护（按用户和组）。配额规定用户在系统中可以使用的空间量和文件数。

Red Hat Linux可以用不同方法组织组，称为用户专用组模式。这样可以提高用户安全性，因为用户可以得到自己的专用组。如果需要，仍然可以对各个组设置共享目录。本章介绍下列内容：

- 基本用户与组管理
- 生成用户
- 使用阴影口令组
- 设置配额
- 生成用户专用组

基本用户与组管理

Linux系统中每个人都要有一个用户账号。每个账号的权限取决于命令与目录。Linux用户账号用组进行组织。尽管默认用户是默认组的惟一成员，但可以将用户组织到新组中，可以根据不同组配置不同权限。

Red Hat Linux中的用户账号在/etc/passwd中组织，/etc/shadow使其口令更加安全。对Red Hat Linux组，相应文件为/etc/group与/etc/gshadow。

生成新用户账号时，默认参数在/etc/login.defs中配置，配置文件通常从/etc/skel目录复制到新用户的主目录。

说明：普通用户有自己的账号，通常为了减少风险，要避免普通用户得到根用户权限。但是，如果你是Linux计算机的管理员，则可能要以根用户身份登录，见第6章介绍。

/etc/passwd

Linux用户可以分成三组：管理用户、服务用户和普通用户。每个用户具有一定的权限。普通用户与管理用户具有用户名、口令和主目录。所有用户都通过/etc/passwd文件中的语句进行配置，如图9.1所示。

```
ftp x 14 50 FTP User /var/ftp /sbin/nologin
nobody x 99 99 Nobody / /sbin/nologin
ntp x 38 38 /etc/ntp /sbin/nologin
apache x 48 48 Apache /var/www /sbin/nologin
rpc x 32 32 Portmapper RPC user / /sbin/nologin
vcsa x 69 69 virtual console memory owner /dev /sbin/nologin
nsd x 28 28 NSCD Daemon / /sbin/nologin
sshd x 74 74 Privilege-separated SSH /var/empty/ssh /sbin/nologin
rpm x 37 37 /var/lib/rpm /bin/bash
mailnull x 47 47 /var/spool/queue /sbin/nologin
snmp x 51 51 /var/spool/queue /sbin/nologin
rpcuser x 29 29 RPC Service User /var/lib/nfs /sbin/nologin
nfsnobody x 65534 65534 Anonymous NFS User /var/lib/nfs /sbin/nologin
pcap x 77 77 /var/arpwatch /sbin/nologin
xfs x 43 43 X Font Server /etc/X11/fs /sbin/nologin
named x 25 25 Named /var/named /sbin/nologin
gdm x 42 42 /var/gdm /sbin/nologin
desktop x 80 80 desktop /var/lib/menu/kde /sbin/nologin
postfix x 69 69 /var/spool/postfix /sbin/nologin
squid x 23 23 /var/spool/squid /dev/null
usb_lser x 00 00 W. J. Lee /var/usb/lser /bin/bash
j x 00 00 Mic. J. Jiang /home/j /bin/bash
m x 01 01 M. J. Ott /home/m /bin/bash
```

图9.1 /etc/passwd文件

图中的最后两行包含普通用户的项目。可以看出，用户名与ftp、apache和squid之类的服务相联系。每个项目有七个列，用冒号(;)分开。表9.1介绍了每个列。

表9.1 /etc/passwd项目

列号	功能	说明
1	Username	登录名
2	Password	如果这个字段包含一个x，则在/etc/shadow中存放加密口令
3	User ID	红帽子用户ID，从500开始
4	Group ID	红帽子组ID，通常与用户ID匹配
5	Extra information	常用于用户实名
6	Home directory	通常是/home/username
7	Default shell	用户登录后看到的shell

/etc/shadow

Red Hat Linux中的/etc/shadow文件增加了口令安全性。默认情况下，这个文件只有根用户能够读取。如果用标准命令生成新用户，则也把基本信息加进这个文件中，这是基于/etc/login.defs文件中的默认（见本章稍后介绍）。图9.2显示了/etc/shadow文件。

可以看出，最后两行的项目对/etc/passwd中显示的普通用户与服务用户相同。这里，每个用户项目有八列，用冒号分开。表9.2显示了这些列。

表9.2 /etc/shadow项目

列号	功能	说明
1	Username	登录名
2	Password	加密口令
3	Number of days	上次口令改变时间，从1970年1月1日算起的天数
4	Minimum password life	在这么长的天数内不能改变口令
5	Maximum password life	在这么长的天数后必须改变口令
6	Warning period	口令到期之前的这么多天会出现警告
7	Disable account	如果口令到期后这么多天还不使用账号，则无法登录
8	Account expiration	如果到这个日期不用账号，则无法登录。可以用YYYY-MM-DD格式，也可以用从1970年1月1日算起的天数

/etc/group

Red Hat Linux组配置文件与用户配置文件相似，但只有四列。图9.3中可以看到/etc/group中有两个普通用户名，与/etc/passwd和/etc/shadow中相同。在/etc/group中，它们是组名。注意，组mj和组jm的组ID与前两个配置文件中同名用户的用户ID相匹配。

```
# # 119:9 0 9999:7
ircd * 119:9 0 9999:7
r.p 119:19 0 9999:7
apache 119:19 0 9999:7
rpc 119:19 0 9999:7
vcsw 119:19 0 9999:7
nsd 119:19 0 9999:7
sshd 119:19 0 9999:7
rpm 119:19 0 9999:7
mailnull 119:19 0 9999:7
ownsp 119:19 0 9999:7
rpcuser 119:19 0 9999:7
nfsnobody 119:19 0 9999:7
pcap 119:19 0 9999:7
xfs 119:19 0 9999:7
named 119:19 0 9999:7
gdm 119:19 0 9999:7
desktop 119:19 0 9999:7
postfix 119:19 0 9999:7
squid 119:19 0 9999:7
webalizer 119:19 0 9999:7
mj $1$Yp8h q5K$1b7m01DvzbDCDwn0RIJzo/ 11920 0 9999:7
jm $1$VfwM4pCG$PrEpTyZhZkq879zHfKnDF1 11920 0 9999:7
```

图9.2 /etc/shadow文件

```
rpc x 32
floppy x 19
vcsw x 69
nsd x 28
sshd x 74
rpm x 37
mailnull x 47
ownsp x 51
slorate x 21
rpcuser x 29
nfsnobody x 85534
pcap x 77
xfs x 43
named x 25
gdm x 42
desktop x 60
postdrop x 90
postfix x 69
squid x 28
webalizer x 67
mj x 500
jm x 501
Sharing x 800 jm,mj
```

图9.3 /etc/group文件

注意最后一个项目Sharing组（共享组）。可以看出，用户mj与jm是这个组的成员。表9.3列出了/etc/group中的列。

表9.3 /etc/group项目

列号	功能	说明
1	Group name	默认情况下，红帽子用户是同名组的成员
2	Password	如果这个字段包含一个x，则在/etc/shadow中存放加密口令
3	Group ID	默认情况下，红帽子用户ID与组ID相同
4	Members	包括同一组中其他成员的用户名

/etc/gshadow

Red Hat Linux的/etc/gshadow组配置文件相当于用户的/etc/shadow文件，指定相应组的加密口令和特定组的管理员权限。图9.4显示了样本/etc/gshadow文件。

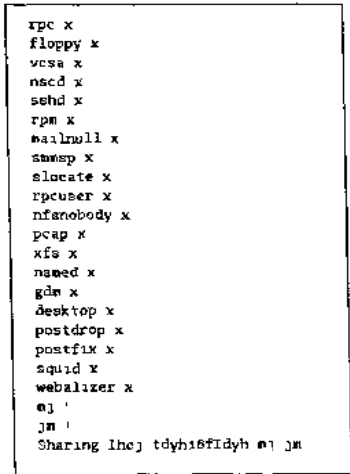


图9.4 /etc/gshadow文件

注意Sharing组与/etc/group中的差别。表9.4列出了/etc/gshadow的列。

表9.4 /etc/gshadow项目

列号	功能	说明
1	Group name	可以生成其他组
2	Password	加密组口令，用gpasswd命令增加
3	Group administrator	可以管理组中用户的用户
4	Group members	包括同一组中其他成员的用户名

/etc/skel

用户有一组默认配置文件和目录。第8章介绍了bash shell中的一些配置文件。这些文件的默认清单在/etc/skel目录中，很容易用ls -la /etc/skel命令检查，如图9.5。这个清单随安装的内容不同而不同。

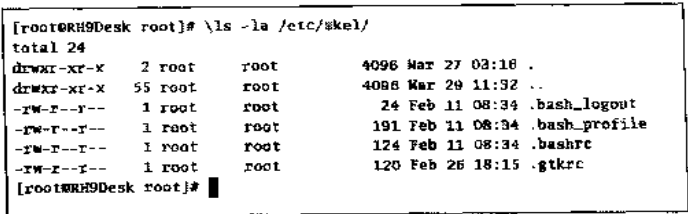


图9.5 /etc/skel中的默认主文件

提示：如果有一列标准文件，如新用户的公司政策，则可以将其复制到/etc/skel文件中。所有用户的主目录中都会得到这些文件的拷贝。

/etc/login.defs

生成新用户时，基本参数来自/etc/login.defs配置文件。Red Hat Linux所带的版本包括电子邮件目录、口令寿命、用户ID与组ID号、生成主目录的设置。这个文件中的默认变量是一目了然的：

```
MAIL_DIR    /var/spool/mail    # Default mail directory
PASS_MAX_DAYS 99999          # Password max life
PASS_MIN_DAYS 0              # Password min life
PASS_MIN_LEN 5               # Min password length
PASS_WARN_AGE 7              # Warning before expiration
UID_MIN     500              # Lowest User ID number
UID_MAX     60000            # Highest User ID number
GID_MIN     500              # Lowest Group ID number
GID_MAX     60000            # Highest Group ID number
CREATE_HOME yes
```

不用说，可以通过其他配置文件来设置这些配置，例如，可以编辑/etc/shadow文件，管理口令寿命。图9.6显示了这个文件的一个拷贝。

```
# "REQUIRED"
# Directory where mailboxes reside, _or_ name of file, relative to the
# home directory.  If you _do_ define both, MAIL_DIR takes precedence.
# QMAIL_DIR is for Qmail
#QMAIL_DIR Maildir
MAIL_DIR    /var/spool/mail
#MAIL_FILE  .mail

# Password aging controls:
# PASS_MAX_DAYS Maximum number of days a password may be used.
# PASS_MIN_DAYS Minimum number of days allowed between password changes.
# PASS_MIN_LEN  Minimum acceptable password length.
# PASS_WARN_AGE Number of days warning given before a password expires.
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN 5
PASS_WARN_AGE 7

# Min/max values for automatic uid selection in useradd
UID_MIN 500
UID_MAX 60000
# Min/max values for automatic gid selection in groupadd
GID_MIN 500
GID_MAX 60000

# If defined, this command is run when removing a user.
#USERDEL_CMD /usr/sbin/userdel_local
# If useradd should create home directories for users by default
CREATE_HOME yes
```

图9.6 /etc/login.defs文件

管理用户账号

Linux管理员管理用户账号时有三个基本工作，包括增加新用户、删除用户和管理现有用户的访问参数。尽管可以使用Red Hat Linux图形工具（见第19章的redhat-config-users），但大多数管理员喜欢从命令行界面完成这些功能。

命令行界面与GUI之间的争议

大多数Linux管理员喜欢用命令行界面完成管理功能，尽管好像与Microsoft Windows 管理员大相径庭，但这是有一定道理的：

- 命令行界面工具更灵活，使用命令行界面通常比使用GUI时具有更多选项。
- 命令行界面更快，不必等待Linux处理GUI或将另一个GUI工具放到屏幕上。
- GUI工具只是个前端，换句话说，建立和运行的Linux GUI工具对应于shell中的命令。
- GUI工具是另一层软件，也是另一个出错源。
- GUI工具不显示所有错误。命令行界面提供的错误消息可以在控制台看到，而GUI工具可能不在图形桌面中显示这些错误。

增加用户

Red Hat Linux中增加用户的基本方法有三种：

- 直接编辑/etc/passwd文件，在新用户主目录中增加所要的文件。
- 使用一些此方面的命令，如useradd。
- 打开图形前端Red Hat Configuration，见第13章介绍。

也可以用newusers命令，其配置选项与passwd格式相同的批处理文件增加整组用户。

直接方法

可以看看生成新用户所要的步骤，以便了解与现有用户相关的每个参数。本例中，假设对James K. Polk（美国总统，1845~1849）建立一账号，计划对其指定用户ID和组ID为600（如果600已经被占用，则换成另一个500到60 000之间的未用值）。按下列步骤生成新用户：

1. 在文本编辑器中打开/etc/passwd文件。
2. 另建一行，最简单的方法是从当前用户中复制相应信息。
3. 改变用户名、用户ID、组ID和主目录。在第一列插入用户名jkg，第三列插入用户ID 600，第四列插入组ID 600，第五列插入James K Polk，第六列插入主目录/home/jkg。确保输入的信息（除了shell）相对于/etc/passwd文件中的其他项目是惟一的。将文件改变保存起来。
4. 在文本编辑器中打开/etc/shadow文件。另建一行，最简单的方法是从当前用户中复制相应信息。在第一列插入用户名jkg。将文件改变保存起来。这是个只读文件，在vi中，可以用wq!命令覆盖只读设置。
5. 在文本编辑器中打开/etc/group文件。另建一行，最简单的方法是从当前用户中复制相应信息。在第一列插入用户名jkg。第三列插入组ID 600。
6. 设置新用户的主目录。对用户jkg，命令如下：

```
mkdir -p /home/jkg
```

7. 让新用户能访问其主目录。这里，用下列命令指定拥有权：

```
chown jkg /home/jkg  
chgrp jkg /home/jkg
```

8. 用`passwd jkp`命令指定新口令。向新用户提供这个口令。告诉他，可以自己用`passwd`命令指定新口令。
9. 复制基本初始化文件，通常存放在`/etc/skel`目录中（第8章介绍了这些文件，如`.bashrc`与`.bash_profile`）。用下列命令改变新用户标识：

```
su - jkp
```

用下列命令复制这些文件：

```
cp /etc/skel/. * /home/jkp  
command.
```

10. 将`/etc/skel`中的任何子目录复制到`/home/jkp`中。例如，可以用下列命令复制`/etc/skel/.kde`目录：

```
cp -r /etc/skel/.kde /home/jkp
```

11. 改变从`/etc/skel`目录所复制文件的用户与组拥有权。
12. 退出`jkp`用户账号，将用户名与口令告诉新用户。
13. 假设使用默认阴影口令组，则要运行`pwconv`与`grpconv`命令。这些命令将在本章稍后介绍。

使用useradd

使用`useradd`命令生成新用户要简单得多。例如，要建立`jkp`的新账号，只要输入下列命令：

```
# useradd jkp
```

这个命令对用户`jkp`设置`/etc/login.defs`配置文件中描述的默认值，并从`/etc/skel`目录复制文件，修改这些文件的拥有权。但还要按上节第8步介绍的方法对`jkp`指定新口令。

检查`/etc/passwd`、`/etc/shadow`与`/etc/group`配置文件，验证`useradd`命令是否在这些文件中增加了新用户`jkp`的项目。

使用newusers

`newusers`命令可以处理用户名与口令批处理文件中的大量用户，采用与`/etc/passwd`文件相同的格式。惟一的差别是口令列要求用加密口令，可以对已知用户从`/etc/passwd`或`/etc/shadow`项目中复制。如果生成文件`new-batch`中的一列新用户，则可以用下列命令建立这些用户：

```
# newusers new-batch
```

`new-batch`文件的格式应与`/etc/passwd`相同，口令应以明文形式输入。因此，如果保存这个批处理文件，则要保证其安全。可以将其隐藏、加密或删除。任何人得到用户名和明文口令清单，都很容易攻击你的系统。

提示：复制加密口令之类的文本很简单，可以自己试试。用一个文本编辑器打开`/etc/shadow`文件，加亮选择口令。然后从文本编辑器退出。右键单击鼠标，可以看到所加亮的内容。打开所选文件，在插入方式中再次右键单击鼠标，可以看到加密口令的另一个拷贝。

删除用户

可以直接删除用户，也可以使用`userdel`命令，甚至可以临时将用户取消，同时保留该用户主目录中的文件。

提示：将用户取消很简单，只要在`/etc/passwd`文件中将目标用户的口令换成星号（*），这个用户就无法再用任何口令登录其账号，即使使用默认Red Hat Linux阴影口令组，情况也是如此。

直接方法

删除用户比增加用户更简单，只要从相应配置文件中删除这个用户的项目，然后删除该用户的主目录。基本步骤如下：

- 从`/etc/passwd`文件中删除这个用户的项目。
- 从`/etc/group`文件中删除这个用户的项目。
- 从`/etc/shadow`文件中删除这个用户的项目。
- 从`/etc/gshadow`文件中删除这个用户的项目。
- 保存所要的文件，然后删除该用户的主目录。

用命令删除

用命令删除用户时，需要两步。`userdel`命令很简单。如果用户James K. Polk刚刚离开公司，则可以将他的账号取消。从他的主目录中取得和保存需要的任何文件，然后运行下列命令：

```
# userdel -r jkp
```

这个命令从`/etc/passwd`文件中删除`jkp`的信息。`-r`开关删除`/home/jkp`目录，包括其中的任何文件和子目录。

但可能还要用`groupdel`命令删除这个用户的组，否则下一个增加的用户的用户ID和组ID不相符，从而会在今后管理新用户时造成问题：

```
# groupdel jkp
```

用chage命令管理用户访问

可以用`chage`命令管理用户口令。它可以根据口令寿命规定指定`/etc/shadow`中的信息。事实上，`chage`命令可以改变这个文件中的设置。可以从表9.5检查`chage`命令的开关。

表9.5 chage命令

命令	结果
<code>chage -m days user</code>	将口令的最短寿命设置为days天
<code>chage -M days user</code>	将口令的最长寿命设置为days天
<code>chage -l days user</code>	设置锁定账号之前，账号可以不活动的天数
<code>chage -E date user</code>	设置账号无法访问之前的天数
<code>chage -W days user</code>	设置提前days天的警告，表示口令要改变
<code>chage -l user</code>	列出当前用户的口令与账号信息，普通用户可以对自己的账号运行

日期可以用YYYY-MM-DD格式，也可以用1970年1月1日算起的天数。

阴影口令组

阴影口令组提供管理Linux用户与组的所有命令，包括本章已经介绍的命令。默认情况下，Red Hat Linux用这个阴影口令组和/etc/shadow与/etc/gshadow文件中的加密口令提供更多的安全性。这些文件要求用命令转换相应/etc/passwd与/etc/group配置文件中的口令。

这些加密口令文件的权限比/etc/passwd与/etc/group文件更严格，只有根用户才能浏览这些文件，根用户默认不能写入这些文件。

但是，如果口令出现问题，则这样增加的安全性也无济于事，见下节介绍。

说明：一个主要的口令测试程序是crack，cracklib* RPM包中提供了一个版本。只能用它测试用户口令的安全性。

强口令

默认情况下，Red Hat Linux不提倡使用简单口令，如单词或abcd之类的简单模式。一个现成的口令攻破程序只要几分钟就可以攻破这种简单口令。相反，最好的口令应该组合大写字母、小写字母和数字，同样的程序要好几个星期才能攻破这种口令。要建立强口令，一个简单的方法是利用自己喜欢的句子，例如running表示“I ran a 1 minute mile on Wednesday”。

说明：使用passwd命令时，新口令要输入两次。如果两次口令不相符，则会出现一个警告消息。按Enter键之后，进入原先的提示，可以重新输入。

转换用户口令

阴影口令组中可以用两个命令转换用户口令：pwconv与pwunconv。

pwconv 转换现有/etc/passwd文件。/etc/passwd文件中的现有口令换成“x”，加密口令、用户名和其他相关信息传输到/etc/shadow文件中。如果最近生成新用户时在文本编辑器中编辑/etc/passwd文件，则可以再次运行这个命令，转换新用户的口令。即使其他口令已经在/etc/shadow文件中加密，也可以这么做。

pwunconv 口令转换/etc/passwd，并删除/etc/shadow文件。注意，这样也会删除/etc/shadow文件中保存的任何口令寿命信息（见前面介绍的chage命令）。

转换组口令

前面曾介绍过，可以在/etc/group中配置组管理员，用gpasswd指定相应口令。有了组口令之后，与普通用户口令具有相同的安全问题。阴影口令组中可以用两个命令转换组口令：grpconv与grpunconv。

grpconv 转换现有/etc/group文件，相关信息传输到/etc/gshadow文件中。

grpunconv 与上一命令正好相反，和pwunconv命令一样，这个命令也删除任何现有的/etc/gshadow文件。

配额

配额使各个用户和组无法占用分区上的全部空间。Linux管理员通常用磁盘配额，规定一个用户的电子邮件、Web站点文件、FTP文件等可以占用的空间量，使各个用户和组无法占用分区上的全部空间，挤压根目录和/boot之类的关键目录所要的空间。如果这些目录没有足够的磁盘空间，则可能使Linux崩溃。

可以通过限定inode数而配置配额。每个inode与特定文件相关联。也可以设置绝对极限（KB数）。换句话说，可以限制用户与组放在系统中的文件个数，也可以对用户与组放在系统中的数据量设置绝对极限。

配额可以监视系统的使用模式。

配置

默认情况下，Red Hat Linux中安装和激活了quota RPM包。如果不能确定，可以运行下列命令：

```
rpm -q quota
```

如果已经安装和激活了quota RPM包，则可以在屏幕的相应输出中看到包名和版本号。如果需要，可以按第10章介绍的方法安装这类RPM包。

配额通常在内核中激活。激活之后，可以在特定分区中对用户与组配置配额。无论哪种情况，都要用/etc/fstab中的活动配额设置重新装载目标目录。配置配额设置后，可以自己激活配额，其在下次重新启动时在/etc/rc.d/rc.sysinit中激活。

内核说明

尽管默认Red Hat Linux内核支持配额，但这个设置不一定适用于从其他来源下载的内核。好在很容易检查相应的内核设置。

下载内核源代码时，文件保存在/usr/src/linux或/usr/src/linux-2.4目录中。Red Hat Linux内核下载到不同目录中，链接到/usr/src/linux-2.4。关于内核源代码的更多信息，见第12章。

说明：下一个Linux内核版本计划于2003年某个时间推出（到本书编写时，可能称为2.6或3.0）。发布之后，内核源代码可能放到/usr/src/linux-2.6或/usr/src/linux-3.0目录中。这个新内核的许多特性已经加进Red Hat Linux 9.0内核中。

标识内核源代码所在目录后，这个目录中应该有一个.config文件。如果没有，则表示这个内核还没有对你的计算机进行编译。这时，用下列命令搜索这个文件中的CONFIG_QUOTA设置：

```
# grep CONFIG_QUOTA /usr/src/linux-2.4/.config
```

如果内核源代码在不同目录中，则要相应改变这个命令。可以在标准输出中看到下列结果之一：

```
CONFIG_QUOTA=y  
CONFIG_QUOTA=n
```

换句话说，配额支持活动（y）或非活动（n）。如果配额支持为非活动，则要将其编译到内核中，详见第12章介绍。

说明：内核版本应与引导装入器配置文件/boot/grub/grub.conf中的设置相关联。关于引导装入器与内核之间的关系，见第12章介绍。

使用配额

要对特定用户生成配额，需要六个步骤：

1. 修改/etc/fstab，对所选文件系统激活配额选项。
2. 重新装载文件系统，使改变生效。
3. 在该文件系统开头建立aquota.user文件。例如，如果在/home中生成配额，则生成/home/aquota.user文件。
4. 扫描相应文件系统，用quotacheck命令生成基本配额文件。
5. 用edquota命令，对特定用户采用配额限制。
6. 最后，用quotaon命令激活配额。

下面几节详细介绍这些步骤。

修改/etc/fstab与重新装载

修改/etc/fstab很简单，从这个配置文件中取出一行，这里设置/home为另一分区的文件系统：

```
LABEL=/home /home ext3 defaults 1 2
```

好在/etc/fstab中还有增加用户配额设置usrquota的空间。/etc/fstab中的空间很紧缺，因为如果这个代码换行，则引导过程可能无法工作。因此加上用户配额设置后，这个/etc/fstab语句如下：

```
LABEL=/home /home ext3 defaults,usrquota 1 2
```

现在可以重新装载/home目录，使改变生效。好在不需要改变运行级或用救援盘重新启动，只要用下列命令在/home中激活/etc/fstab改变：

```
# mount -o remount /home
```

建立aquota.user文件

利用touch命令很容易建立所要的配额文件。本节在/home文件系统中生成配额时，在/home目录中生成空白aquota.user文件。最简单的方法是使用touch命令：

```
# touch /home/aquota.user
```

一定要设置这个文件的安全性，只能让根用户访问。由于这个文件不用执行，因此可以使用下列命令：

```
# chmod 600 /aquota.user
```

进行配额检查

现在可以用`quotacheck -avum`命令生成相应的配额文件。其扫描（-a）`/etc/tab`中支持配额的文件系统，生成冗长（-v）输出，检查用户配额（-u）和重新装载扫描的文件系统（-m）。

对用户使用usrquota

然后对特定用户设置配额。对用户使用`usrquota`命令。例如，如果要对用户`ez`设置配额，运行下列命令：

```
# edquota ez
```

默认情况下，其在vi编辑器中打开用户`ez`的配额信息文件，例如：

```
Disk quotas for user ez (uid 512)
Filesystem blocks    soft    hard inodes soft hard
/dev/sda3      4        0        0      1    0    0
```

可以看出，`ez`的主目录中使用四个数据块（KB）和一个inode。可以在每个类别中设置硬极限或软极限。什么是硬极限或软极限？

软极限 软极限是对用户分配的最大空间量或inode数。如果没有一个延展期，则这是硬极限。可以用`edquota`命令设置延展期。

硬极限 如果有延展期，则硬极限是对用户分配的空间量或inode数的绝对极限。

如果设置100MB软极限和110MB硬极限，则可以编辑`ez`的配额如下：

```
Disk quotas for user ez (uid 512)
Filesystem blocks    soft    hard inodes soft hard
/dev/sda3      4 100000 110000      1    0    0
```

启用配额

最后一步是启用配额，很简单。我们已经完成必要的配置工作，只要用下列命令，对`/home`文件系统中所有配置的用户启用配额即可：

```
# quotaon /home
```

也可以用`quotaoff /home`命令取消同一文件系统中的配额。

组配额

生成组配额和生成用户配额一样容易，差别可以在六步骤中指出：

1. 修改`/etc/fstab`，对所选文件系统激活配额选项。对于组配额，要在目标文件系统的选项中增加`grpquota`设置。
2. 重新装载文件系统，使改变生效。这时用`mount -o remount filesystem`命令。
3. 在该文件系统开头建立`aquota.user`文件。例如，如果在`/home`中生成配额，则生成`/home/aquota.group`文件。
4. 扫描相应文件系统，用`quotacheck`命令生成基本配额文件。用`-avgm`开关，`-g`配置组配额。

5. 用edquota命令对特定组采用配额限制。
6. 最后，用quotaon命令激活配额。

在rc.sysinit中激活

在Red Hat Linux中配置配额之后，操作系统可以在下次重新启动时生效。配额检查与激活命令放在默认的/etc/rc.d/rc.sysinit启动脚本中，图9.7显示了相关部分，其中还转换了与Linux内核2.2相关的配额文件2.2（quota.user与quota.group）。

```
# check remaining quotas other than root
if [ X'$_RUN_QUOTACHECK' -X1 -X /sbin/quotacheck ], then
    if [ X /sbin/convertquota ], then
        # try to convert old quotas
        for mountpt in `awk 'F4 ~ /quota/{print $2}' /etc/mtab`, do
            if [ -f "$mountpt/quota.user" ], then
                action "$Converting old user quota files " \
                    /sbin/convertquota -u $mountpt && \
                    rm -f $mountpt/quota.user
            fi
            if [ -f "$mountpt/quota.group" ], then
                action "$Converting old group quota files " \
                    /sbin/convertquota -g $mountpt && \
                    rm -f $mountpt/quota.group
            fi
        done
        action "$Checking local filesystem quotas " /sbin/quotacheck -aRnug
    fi
fi

if [ X'$_IN_QUOTA_22' -X1 ], then
    action "$Activating local Linux 2.2 quotas " /sbin/quotaon -aug
fi

"/etc/rc.d/rc.sysinit" /94L, 22605C 530, 2-16 69%
```

图9.7 在rc.sysinit中激活配额

对其他用户采用配额

可以对多个用户设置相同配额。edquota命令可以对一系列用户设置相同配额。假设我们已经对用户ez配置配额，则可以用下列命令将相同的限制复制给其他用户，这里是mj、jm和tp：

```
# edquota -up ez mj jm tp
```

配额监视

配置配额之后，可以报告谁使用磁盘空间和inode，以及占用了多少空间。repquota命令按用户（-u）和组（-g）提供配额报告。还可以用repquota -a命令得到所有文件系统的报告。

如果要检查各个用户（-u）和组（-g），则可以用quota命令。各个用户可以用这个命令检查自己的状态。

使用专用组

Red Hat Linux用独特方式组织用户和组，提高安全性。本节介绍Red Hat Linux专用组模式，然后详细介绍如何生成具有公共目录的安全组。

红帽子模式

本章开头曾介绍过，每个人的用户ID要与组ID在/etc/passwd中匹配。但这通常只适用于Red Hat Linux和联盟发行版本，另一种模式是每个用户具有相同的组ID号，通常是100。换句话说，在有些发行版本中，每个用户默认属于同一组。

红帽子模式更适合于几种配置。例如，ISP的用户可以使自己的文件隐藏起来，不让同一ISP的其他用户看到。但是，仍然可以对所选用户配置共享目录。

配置共享目录

有时要让用户共享文件。有些用户可能来自相同部门，或共同处理一个项目。为此可以建立一个组和一个目录，使这个组的所有成员能够阅读所有导入的文件。

最简单的方法可以举一个例子。假设要对项目成员Tom、Adnan、Carlos与Libby建立一个组和一个共享目录。下列步骤要生成用户并建立一个组和一个共享目录，然后设置组ID（SGID）位，使组中任何用户可以将文件复制到共享目录，可以从共享目录阅读文件。

1. 用useradd username命令在系统中生成Tom、Adnan、Carlos与Libby账号。记住对每个用户指定口令。
2. 用groupadd project命令生成项目组。编辑/etc/group，将新用户加进这个组中。
3. 设置新的共享目录/home/project，用chmod 770 /home/project命令使拥有这个目录的用户与组具有完全权限（rwx）。
4. 用chmod g+s /home/project命令在共享目录中配置SGID位，使拥有目录的组中的所有用户具有拥有者权限。
5. 以某个用户的身份登录。从用户主目录向/home/project复制文件。以组中另一个用户的身份登录，能否对第一个用户复制的文件进行任何处理？

提示：可以组合两个chmod命令。chmod 2770 /home/project命令配置指定权限并将SGID位加进这个目录。

小结

本章介绍了Red Hat Linux中管理用户与组的基础，首先介绍配置文件。/etc/passwd与/etc/group包含用户与组的基本信息，而/etc/shadow与/etc/gshadow在更安全的文件中包括加密口令和口令寿命参数。根据/etc/login.defs中的参数，新用户指定一个主目录并复制/etc/skel中的文件。

可以直接生成用户与组，编辑相应配置文件，也可以用useradd与groupadd之类的命令更有效地生成用户与组。可以用几乎一样的userdel与groupdel命令删除用户与组。可以用chage命令管理用户口令规定。

这种用户、组与相关命令的系统称为阴影口令组。利用适当的强口令，这个阴影口令组可以提高用户与组的账号安全性。pwconv与grpconv命令将/etc/passwd与/etc/group文件转换成符合这种阴影口令组格式，而pwunconv与grpunconv命令正好相反，逆转这个过程。

可以管理用户所需的配额。Linux配额可以用inode和特定分区所占的文件空间限制用户。根据所要文件系统的配额修改/etc/fstab文件之后，很容易配置配额。配置配额之后，Red Hat Linux自动在启动时激活配额。

最后，Red Hat Linux的用户专用组模式提供了更多安全性，将各个用户隔离到不同组中。但是，仍然可以用共享目录把用户组织在公共组中。

下一章介绍Red Hat Linux如何用红帽子包管理器管理包。这个系统取得了巨大成功，已经在其他多种Linux发行版本中广泛采用。

第10章 用RPM管理包

红帽子包管理器（RPM）提供了标准化方式，可以对各种实用程序和应用程序组织所要的软件。红帽子包管理器使红帽子公司很容易地把Linux组织成不到两千个包，而不是几万个文件。

用红帽子包管理器增加新程序和应用程序非常简单。这个系统取得了巨大成功，已经在其他多种Linux发行版本中广泛采用，包括SuSE与SCO（原名Caldera）。

管理员需要安装、升级、删除和维护许多不同的RPM包。红帽子包管理器还包括依赖性信息，帮助安装需要的包。红帽子公司增加新特性或提供更安全的软件时，可以升级现有包。

尽管我们安装的红帽子包管理器采用二进制格式，但红帽子公司提供了每个包的源代码。可以用`rpmbuild`命令组织和建立这些包，变成二进制格式，使任何人都能安装。也可以从其他标准包系统建立二进制格式RPM，称为`tarball`。

红帽子包管理器的一个好处是可以验证包和其依赖项。如果文件被人修改过，则正确的`rpm`命令可以标出改变的文件。

红帽子包管理器系统具有丰富的特性。本章只是介绍一点皮毛，提供我认为对Linux管理员最重要的技巧。

红帽子公司还通过`Rawhide`系统存储最新的RPM包，也可以用`up2date`命令根据当前可升级的RPM包数据库更新所选的RPM包。本章介绍下列内容：

- 简化安装与升级
- 使用源RPM
- 了解验证与列表过程
- 特殊主体`up2date`

简化安装与升级

安装与升级是管理RPM包的根本。安装RPM包时，就是在系统中增加新软件。升级RPM包时，就是在相关软件中更新最新特性。

安装与升级RPM包之前，要知道系统中是否已经有所要的包。RPM查询还可以提供包的描述信息，验证和列出与这个包相关的文件。

可以从本地或远程源安装与升级RPM包。从远程地点访问二进制RPM包时，要提供用户名/口令组合。

RPM包还包括依赖性信息。例如，内核源代码RPM包要有GNU C语言编译器。由于内核源代码具有依赖性，因此要先安装GNU C语言编译器，再安装内核源代码。

如果要检查特定文件，则要安装标准Red Hat Linux RPM包数据库，以便标识要安装的包。

查询

rpm命令的查询方式有许多。最简单的形式可以用这个命令寻找已安装包的版本。增加更多开关，可以用其浏览汇总信息、列表文件、验证内容，等等。

简单查询

最简单的形式是rpm -q packagename查询。例如，可以用这个命令寻找已安装包的版本，其中包含几个基本配置文件。只要运行下列命令：

```
# rpm -q setup
setup-2.5.25-1
```

信息查询

查询可以提供包的更多信息。例如，rpm -qi packagename命令可以得到安装包的汇总信息，其输出如图10.1，显示了特定包的大量信息。

```
[root@RH9Desk root]# rpm -qi setup
Name       : setup                      Relocations: (not relocatable)
Version    : 2.5.25                    Vendor: Red Hat, Inc.
Release    : 1 on 17 Feb 2004 / 11.45 35
Build Date: Mon 31 Mar 2003 04:10:15 PM EDT      Build Host: usffy.peri.redhat.com
Group      : System Environment/Base           Source RPM: setup-2.5.25-1.src.rpm
Size       : 34927                           License: public domain
Signature  : DSA/SHA1, Mon 24 Feb 2003 12:56:03 AM EST, Key ID 219180cddb42a60e
Packager   : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary    : A set of system configuration and setup files.
Description:
The setup package contains a set of important system configuration and
setup files, such as passwd, group, and profile.
[root@RH9Desk root]#
```

图10.1 包的汇总信息

标识拥有者

假设听说可以从某个文件升级，但不知道用什么RPM包，这时可以用rpm -qf filename命令标识包名。例如，如果要标识/etc/passwd配置文件所在的包名，只要运行下列命令：

```
# rpm -qf /etc/passwd
setup-2.5.25-1
```

注意要指定相应文件的完整路径。

列表RPM中的文件

如果对--个包不够了解，则可以用rpm -ql packagename命令列出包中的文件。这个表中确认某个配置文件或命令是否在这个包中。如果要升级，则这个信息有助于了解升级有什么风险。图10.2的例子列出了setup RPM包中的文件。

提示：包升级总是有风险的。如果配置了一个监控程序，然后在升级时将其覆盖，则可能丢失定制信息。尽管RPM会用.rpm*扩展名保存配置文件，但最好备份关键配置文件。有时同一包使用两个版本会比升级更安全。第12章将介绍升级Linux内核时这样处理的例子。

```
[root@RH9Desk root]# rpm -ql setup
/etc/bashrc
/etc/csh.cshrc
/etc/csh.login
/etc/exports
/etc/filesystems
/etc/group
/etc/host.conf
/etc/hosts.allow
/etc/hosts.deny
/etc/inputrc
/etc/ntpd
/etc/passwd
/etc/printcap
/etc/profile
/etc/profile.d
/etc/protocols
/etc/securetty
/etc/services
/etc/shells
/usr/share/doc/setup-2.5.25
/usr/share/doc/setup-2.5.25/uidgid
/var/log/lastlog
[root@RH9Desk root]#
```

图10.2 列出setup RPM包中的文件

RPM包与CPU

许多RPM包是针对特定CPU建立的。例如，许多RPM包的扩展名为i386.rpm或.noarch.rpm。尽管Red Hat Linux 9不能在使用Intel 386级CPU的计算机上安装，但具有i386.rpm扩展名的RPM包可以在具有Intel兼容奔腾级CPU的Red Hat Linux计算机上安装。

具有其他扩展名的RPM包也对不同CPU进行了优化。如果可能，应安装与CPU类型相关联的RPM包。要找到CPU标识符，输入uname -p命令。表10.1列出了一些可选的RPM扩展名。

表10.1 RPM扩展名

扩展名	CPU
noarch.rpm	不依赖于CPU，可以在所有计算机上安装
i386.rpm	基于Intel 386 CPU，这些RPM包可以在所有Intel兼容计算机上安装
i486.rpm	用于带Intel 486 CPU的计算机（随时）
i586.rpm	用于带Intel 586 CPU的计算机
i686.rpm	用于带Intel 686 CPU的计算机
ia64.rpm	用于带Intel Itanium 64位CPU的计算机
alpha.rpm	用于带HP Alpha CPU的计算机，最初是DEC公司开发的
athlon.rpm	基于AMD Athlon CPU
ppc.rpm	用于带Apple PowerPC CPU的计算机
s390.rpm	用于基于S/390 CPU的IBM服务器
sparc.rpm	用于带Sun系统公司SPARC CPU的计算机

基本安装

安装新的RPM包很简单，只要用rpm -i packagename-versionnumber命令即可。如果系统中还没有这个包，则其自动安装。通常，要从Red Hat Linux安装光碟之类的来源安装RPM包，装载到/mnt/cdrom。装载源之后，可以用下列命令安装setup RPM包：

```
# rpm -i /mnt/cdrom/RedHat/RPMS/setup-*
```

星号是个合适的通配符，因为RPM包经常更新，但实际包名通常保持不变。如果多个包以setup-*开头，则可以用这个命令一起安装。

如果有你喜欢的联机RPM包来源，则可以直接从这个来源安装。例如，如果要从abcd服务器的RedHat/RPMS目录安装lynx RPM包，则可以用下列命令：

```
# rpm -ivh ftp://abcd/RedHat/RPMS/lynx-*
```

-i扩展安装，-v与-h扩展设置带散列的冗长输出，因此可以监视安装进程。有些FTP服务器要求用户名和口令。如果安装lynx RPM包，用户名为anonymous，口令为efgh，则可以用下列命令：

```
# rpm -ivh ftp://anonymous@ftp.redhat.com/pub/redhat/linux/rawhide/i386/RPMS/  
↳lynx-  
Password for anonymous@ftp.redhat.com:
```

屏幕上不显示提示输入的口令。尽管可以在rpm命令中增加口令，但最好别这么干，因为这样会在屏幕上显示口令，以明文形式在互联网上传输。

甚至可以用这个命令安装多个包的最新版本。但这个命令通常无法在互联网工作。如果要可靠地安装包，则应离线安装。本章末尾介绍的Rawhide包是红帽子公司提供的最新包。

说明：红帽子公司开发新版RPM包时，将其存放在Rawhide包中。可以在红帽子公司FTP站点及其镜像站点中找到这些包。到本书编写时，它们存放在/pub/redhat/linux/rawhide/cputype/RedHat/RPMS目录中，其中cputype表示系统的CPU类型，如i386与sparc。

升级

包升级总是有风险的。如果配置了一个监控程序，然后在升级时将其覆盖，则可能丢失定制信息。升级的软件也可能与系统中安装的其他应用程序存在互动问题。

但是，RPM包经常需要升级。有时你或用户需要新特性，可能要通过软件升级来解决安全问题，可能要升级的软件（如编译器）处理其他新包的升级版本（如内核）。

升级有两个相关开关：-U与-F。这两个开关都可以升级RPM包，差别体现在没有已安装的RPM包时。这时rpm -U packagename命令安装新包，而rpm -F packagename命令不安装新包。

一般来说，最好在升级和全新安装RPM包时包括-v（冗长）和-h（散列标志）开关。例如，如果是从装载光碟升级安装的lynx RPM版本，则可以用下列命令监视安装进程（用散列标志）和可能出现的错误消息：

```
# rpm -Uvh /mnt/cdrom/RedHat/RPMS/lynx-*
```

依赖性

升级和全新安装RPM包时，可能遇到错误消息。也许最常见的rpm错误消息与依赖性有关。

RPM依赖性就是，一个包的工作要求已经安装另一个包。包的源代码中列出需要的其他RPM包，换句话说，就是它所依赖的包。可以看看安装kernel-source RPM包时的依赖性例子：

```
# rpm -Uvh /mnt/cdrom/RedHat/RPMS/kernel-source-*
warning: /mnt/cdrom/RedHat/RPMS/ kernel-source-2.4.20-11.i386.rpm: Header V3 DSA
signature: NOKEY, key ID 89da07a
error: Failed dependencies:
    gcc >= 2.96-98 is needed by kernel-source-2.4.20-11
Suggested resolutions:
    gcc-3.2.2-5.i386.rpm
```

这个输出表明我要先安装gcc (GNU C Compiler) 包。可以同时安装这两个包，也可以先装gcc包。如果觉得这样太麻烦，则也可以用rpm --nodeps开关忽略依赖性。只要在使用kernel-source包之前安装了gcc包，就不会有问题。一种方法是使用下列命令：

```
# rpm -Uvh --nodeps /mnt/cdrom/RedHat/RPMS/kernel-source-*
# rpm -Uvh /mnt/cdrom/RedHat/RPMS/gcc-3*
```

删除

利用-e开关很容易删除RPM包。甚至不需要知道包的版本号。例如，可以使用下列命令删除kernel-source RPM包：

```
# rpm -e kernel-source
```

由于不需要指定要删除的RPM包路径，因此可以用同一命令删除多个包：

```
# rpm -e kernel-source gcc
```

RPM包数据库

我们查找文件和命令时，发现计算机中还没有安装。你知道，Red Hat Linux文件是用RPM包组织的。有时，不难猜出要安装的RPM包，例如smbclient命令属于samba-client-* RPM包。但是，如果要寻找与某些隐藏程序库相关联的RPM包，则很难找到正确的包。

这时就要用到RPM包数据库。安装之后，即可用rpmdb-redhat-* RPM包，寻找与当前Red Hat Linux版本中安装的每个文件相关联的RPM包。

例如，如果要寻找与/etc/exports相关联的包，则可以用下列命令，只要事先安装了rpmdb-redhat-* RPM包：

```
# rpm --redhatprovides /etc/exports
setup-versionnumber
```

使用源代码RPM包

Linux的一个关键特性是很容易访问源代码。由于Red Hat Linux是用RPM包建成的，因此可以访问源代码RPM包 (SRPM)。源代码RPM包中包括建立二进制RPM包所需的代码与指令，然后可以在Red Hat Linux计算机上安装。

处理源代码需要rpm-build RPM包。尽管rpm命令仍然提供管理源代码RPM包的遗留支持，但今后要用rpmbuild命令完成这个功能。

要了解如何使用源代码RPM包，就要知道默认目录结构，知道.spec文件用于建立二进制RPM包。

目录

习惯上，源代码RPM包很容易看出，其扩展名为.src.rpm。源代码RPM包中包括规范和其他文件，可以在不同/usr/src/redhat子目录中建立。建成二进制文件的任何源代码RPM包也在同一目录结构中设置。表10.2列出了五个关键源代码RPM包目录。

表10.2 源代码RPM包目录

目录	功能
/usr/src/redhat/BUILD	处理的源代码在这里解包和建立
/usr/src/redhat/RPMS	从源代码RPM包生成的二进制RPM包放在这里
/usr/src/redhat/SOURCES	包含实际源代码
/usr/src/redhat/SPECS	包括控制RPM包建立过程的文件
/usr/src/redhat/SRPMS	已经建立过程中产生的源代码RPM包

要将源代码RPM包分解成这些目录，就要安装这个包。例如，如果要使用anonftp包，则要安装相关的.src.rpm文件。例如，如果已经装载一个源代码RPM包的红帽子光碟，则可以使用下列命令：

```
# rpm -i /mnt/cdrom/RedHat/SRPMS/anaconda-*.src.rpm
```

规范文件

管理源代码RPM包的关键是规范文件。安装源代码RPM包之后，应能在/usr/src/redhat/SPECS目录中找到它的规范文件。这个规范文件控制包的建立方法，以及安装与删除RPM包时的配置命令。

规范文件中的关键部分是%prep、%build与%install，可以建立源代码和二进制RPM包。一个重要变量是Requires或BuildRequires，列出要先安装的其他包。规范文件中的其他典型部分包括：

%define 包括基本参数，如包的顶层目录地址。例如，这一段中可能看到ROOT /var/ftp。这个段中包括RPM包的基本汇总信息。安装这个RPM包时，rpm -qi packagename命令可以显示这个内容。

%package 列出依赖于这个特定RPM包的包。

%description 提供rpm -qi packagename命令的更多信息。

%prep 包括档案与补丁包的准备命令。

%setup 包含解包档案的处理命令。

%build 建立要编译的代码。

%install 增加命令，实际建立文件，在定义好的目录中安装包。

%clean 包括从系统中删除任何中间文件的基本命令。

%post 包含安装后脚本，如修改用户账号的脚本。

%postun 包含删除包之后的脚本。

%pre 包含安装前脚本，如准备目录的脚本。

%preun 包含删除包之前的脚本。

%triggerin 包含复制的其他包的部分。

%config 列出/etc的配置文件。

规范文件并不像最初看起来那么难。通常，它们包含普通Linux命令与描述，可以在文本编辑器中修改。

从Tarball建立二进制RPM包

可以从Tarball建立二进制RPM包，但首先要有一个规范文件。上节曾介绍过，这有一定难度。

说明：Tarball是单个文件的包或一组文件的档案。将Tarball解包时，包中的文件复制到计算机上。这样，Tarball相当于Microsoft Windows中的压缩zip文件档案。Tarball通常以压缩形式出现，扩展名为.tar.gz、.tgz或.tar.bz2。

要了解这个过程，一个办法是阅读不同的规范文件。例如，下面是dosemu spec文件的摘要：

```
%define vimver 5.8
%define vim vim58
Summary: A DOS emulator.
Name: dosemu
Version: 1.1.1
Release: 3
Exclusivearch: %{ix86}
License: distributable
Group: Applications/Emulators
Source0: ftp://ftp.dosemu.org/dosemu/dosemu-%{version}.tar.bz2
...
Patch0: dosemu-0.66.7-config.patch
...
%package -n xdosemu
Requires: dosemu = %{PACKAGE_VERSION}
Summary: A DOS emulator for the X Window System.
Group: Applications/Emulators
```

这个文件来自dosemu-*.src.rpm包。这个系统很简单，从代码中可以看出版本号、源代码URL、相对路径以及汇总描述。还可以看到xdosemu包需要dosemu，从而建立RPM包依赖性。

建立二进制RPM包

建立二进制RPM包时只需要有源代码（可以从源代码RPM包或tarball取得）和一个规范文件。可以从头开始建立规范文件，也可以从源代码RPM包修改现有规范文件。

可以用两种基本方法建立二进制RPM包:

```
# rpmbuild -ba packagename.spec
# rpmbuild -bb packagename.spec
```

第一个命令 (`rpmbuild -ba`) 生成源代码和二进制RPM包, 第二个命令 (`rpmbuild -bb`) 只生成二进制RPM包。

说明: `rpm -ba`与`rpm -bb`命令不再适用于Red Hat Linux 9, 其功能已经移到`rpm-build.*` RPM包中的`rpmbuild`命令。

RPM包安全性

学习使用RPM包之后, 很容易形成依赖。黑客很可能在网上发布的RPM包中发表病毒或特洛伊木马程序。`rpm`命令可以用Pretty Good Privacy (PGP) 系统 (见下节介绍) 检查RPM包的完整性。还可以验证包内容或特定文件内容。

RPM包与PGP系统

RPM系统使用与电子邮件安全性相关的PGP系统作为安全标准。PGP系统是Phil Zimmermann开发的, 是供专用密钥与公用密钥系统。在Red Hat Linux中, 使用PGP系统的GNU方式称为GNU隐私卫士 (GPG, GNU Privacy Guard)。

这一切的关键是红帽子GPG密钥, 默认安装成`/usr/share/doc/rpm-version/RPM-GPG-KEY`。如果没有安装, 则可以从下列来源取得:

- 从Red Hat Linux安装光碟主目录中。如果在默认位置安装光碟, 则密钥在`/mnt/cdrom/RPM-GPG-KEY`中。
- 从`www.redhat.com`站点, 到本书编写时, 其在`www.redhat.com/solutions/security/news/publickey.html`页面中。

然后要导入GPG的公用密钥。例如, 如果从安装光碟导入, 则要用下列命令导入到`/var/lib/rpm/Pubkeys`文件:

```
# rpm --import /mnt/cdrom/RPM-GPG-KEY
```

说明: `rpm --import`是个新命令, 如果你使用7.3以前的旧版Red Hat Linux, 则可能要使用`gpg --import publickey`命令。

验证包

现在可以验证任何RPM包的真正Red Hat Linux签名。例如, 可以先验证内核源代码的完整性, 再重新编译。要对`/tmp`目录中的`kernel-sources` RPM包完成这个工作, 用下列命令:

```
# rpm -K /tmp/kernel-source-*.rpm
/tmp/kernel-sources-versionnumber.rpm: (sha1) dsa sha1 md5 gpg OK
```

其用指定加密模式验证`kernel-source` RPM包的完整性, 包括GPG。

验证文件

可以用原先的配置检查文件。例如，如果黑客改变计算机上的文件，则你希望知道。每个文件可以与原文件进行多方面的对比。通过RPM包安装的每个文件相关的数据存放在/var/lib/rpm目录下的RPM包数据库中。

如果怀疑某个命令没有按预期方式工作，则可以用RPM包数据库进行检查。下面以mount命令为例。可以用下列命令检查mount命令的完整性：

```
# rpm -Vf /bin/mount
```

如果没有看到任何输出，则说明这个命令与原先安装的命令相符。

如果有人篡改了mount命令，则可能看到如下输出：

```
# rpm -Vf /bin/mount
SM5....T    /bin/mount
```

这个命令检查/bin/mount的九个不同属性。如果遇到表10.3所示的字母之一，则说明这个命令与原先安装的命令有所不同。这里的例子说明文件长度、权限、MD5校验和以及文件修改时间发生了改变。

表10.3 rpm文件验证问题

输出	失败测试
S	文件长度不匹配
M	方式（不同权限与文件类型）
5	MD5校验和错误
L	符号链不对
D	设备号错误
U	用户拥有权改变
G	组拥有权改变
T	文件修改时间不匹配
?	文件不可读
c	配置文件标志

有时“失败”并不是问题。例如，如果修改了/etc/inittab文件，则可能看到下列验证失败消息：

```
# rpm -Vf /etc/inittab
..5....T c /etc/inittab
```

但这个“失败”并不是问题，例如，我在这个配置文件中修改initdefault变量之后看到这个结果。换句话说，由于改变文件内容，因此MD5校验和改变，而且文件修改时间不同于计算机上安装initdefault时的时间。

更新RPM包

红帽子公司在Rawhide包中保存最新RPM包，可以用任何FTP客户机方便地访问。到本书编写时，可以在红帽子公司FTP服务器的/pub/redhat/linux/rawhide目录中找到Rawhide RPM包。

如果要更新特定RPM包，可以从Rawhide下载到/tmp之类的目录中。备份当前配置，因为它与这个包有关。如果可能，用rpm命令安装（-i）而不是升级（-U）新包。如果遇到任何问题，则更容易从原先的配置恢复。第12章介绍Linux内核升级过程中，会看到这个过程例子。

特殊主体：up2date

除了Rawhide之外，还有一个红帽子更新主体，其文本命令为up2date。这节假设已经按第3章介绍的方法注册到红帽子公司网络。注册时，要发送系统中安装的RPM包清单。利用红帽子更新主体，可以检查红帽子数据库中的新RPM包，让其安装到系统中。

要启动红帽子更新主体，可以在命令行界面中输入up2date命令。图10.3假设计算机已经注册到红帽子公司网络，而且在GUI界面中启动了up2date。

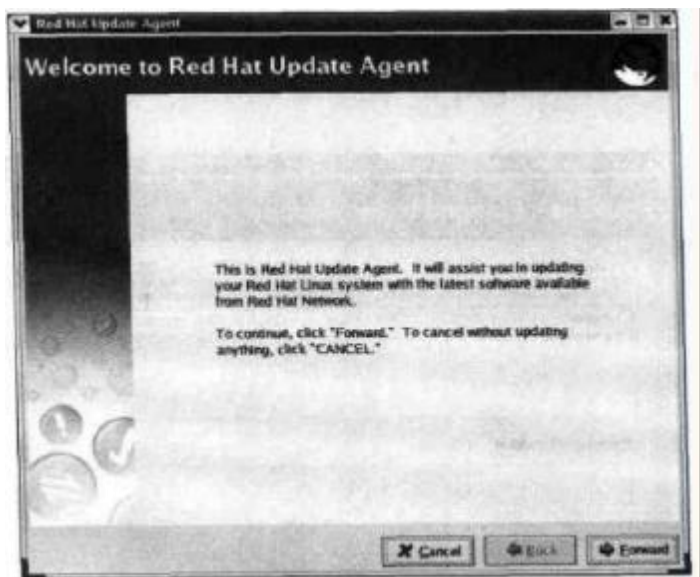


图10.3 启动红帽子更新主体

否则可能看到红帽子公司网络配置窗口，以及登录红帽子公司网络的窗口，并要传输计算机上所安装包的基本信息与清单，详见第3章。

假设已经注册，则可以看到图10.4所示的红帽子更新通道对话框。可以看出，这个对话框中列出了Red Hat Linux 9的通道。单击Forward按钮继续。

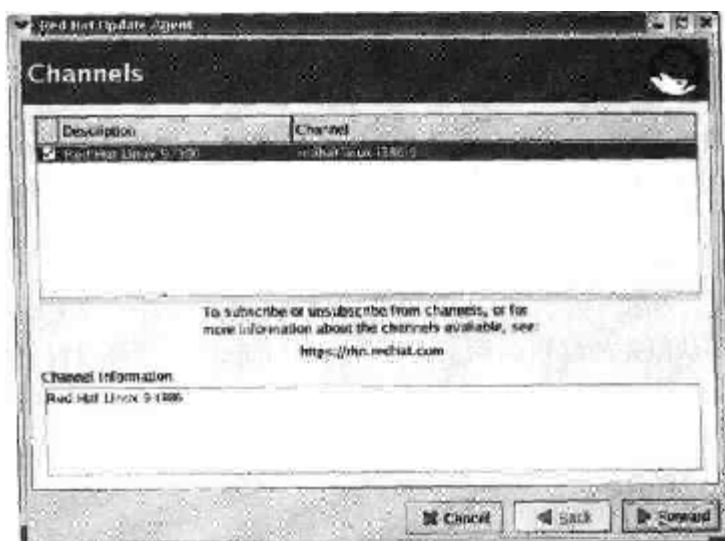


图10.4 红帽子更新通道

说明：如果未活动的红帽子公司用户（Domain ID），则这些计算机只限于一个用户。会删除当前计算机上的这个账号之后，才能注册新计算机。

然后up2date检查红帽子公司网络上的RPM包，将其与安装的RPM包进行比较。假设注册过程中指定要跳过RPM包，且这些包有更新版本，则可以看到图10.5所示的屏幕（到本书编写时，内核2.4.21版还没有推出）。这时可以安装这些包。进行所需的选择，然后单击Forward按钮继续。



图10.5 指定跳过包

下一步要检查可用的更新，换句话说就是可以安装的新RPM包。图10.6配置Mozilla Web浏览器的更新（你的选择可能不同）。进行所需的选择，然后单击Forward按钮继续。

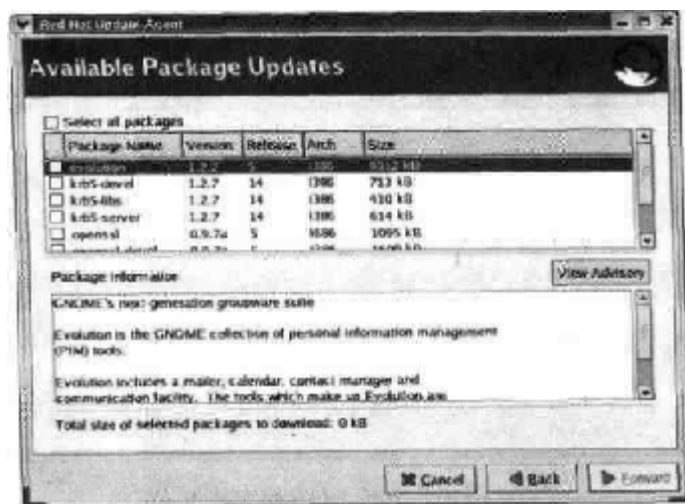


图10.6 可用的更新

前面曾介绍过，可能有RPM包依赖于。如果需要安装其他包，则up2date会列出这些包。

假若想继续工作，则可以单击Forward按钮继续。这时红帽子更新主体开始下载所要的RPM包及其依赖包，如图10.7。

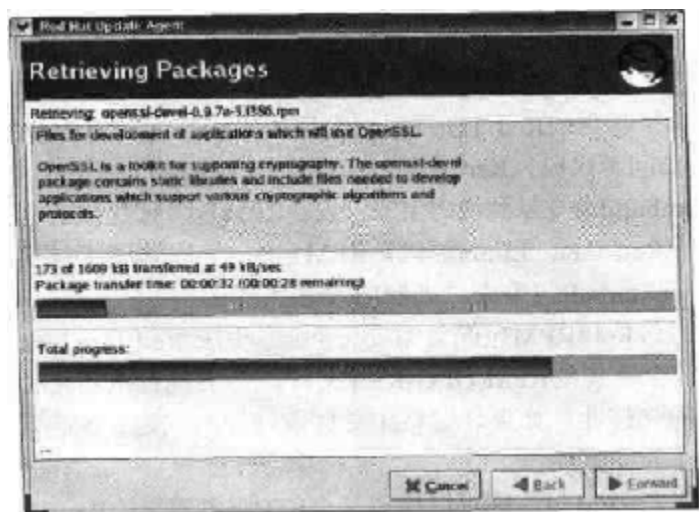


图10.7 下载所要的RPM包及其依赖包

包下载到Linux计算机之后，up2date开始安装包，这时系统如图10.8所示。安装完成后，可以看到一个对话框，列出up2date在计算机上安装的RPM包。

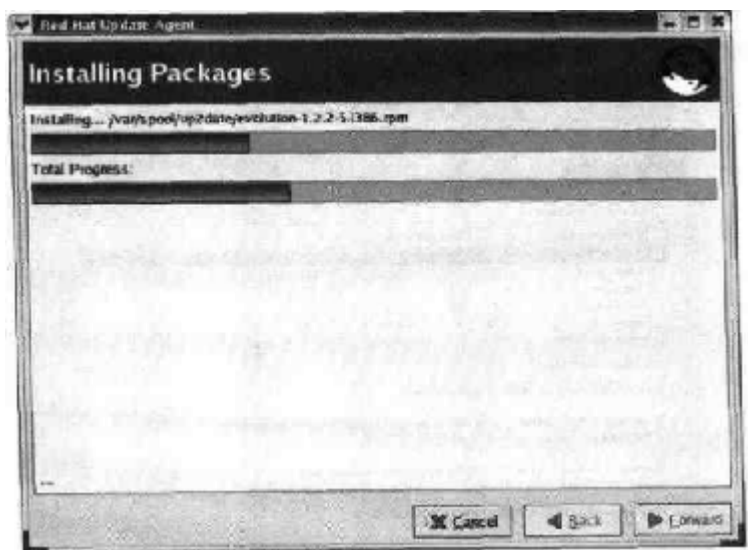


图10.8 up2date开始安装包

小结

如果在Red Hat Linux中安装新软件，则要知道如何管理RPM包。可以用rpm命令从光碟之类的本地源或FTP与HTTP服务器之类的远程源安装与升级新包。

rpm命令很灵活。使用正确的开关后，就可以查询状态、列出文件或包的拥有权。正确配置的RPM包还会列出依赖性。例如，如果Linux内核源代码需要GNU C语言编译器，则rpm命令默认不允许先安装kernel-source包。如果要寻找正确的RPM包，则可以使用rpmdb-redhat-* RPM包，其提供了与当前Red Hat Linux发行版本相关的所有RPM包的数据库。

Linux很容易访问源代码。Red Hat Linux用源代码RPM包支持这个特性。安装rpm-build包之后，可以用rpmbuild命令从源代码生成二进制RPM包，只要有正确配置的规范文件即可。

规范文件放在Red Hat Linux源代码RPM包中，可以根据需要进行修改。也可以建立自己的规范文件，从tarball包生成二进制RPM包。

人们很容易过份依赖RPM包而忽略安全问题。因此Red Hat Linux支持PGP系统，只要从几个地方取得一个真正的RPM-GPG-KEY文件，然后就可以用rpm -K packagename命令验证任何RPM包的完整性。如果怀疑特定文件或命令有问题，则还可以用rpm -Vf filename命令验证特定文件的完整性。

如果要寻找最新RPM包，则可以检查某个FTP服务器上的Rawhide目录，红帽子公司首先在这里发布最新更新，也可以用红帽子更新主体自动完成这个过程。

下一章介绍引导过程的分析细节。介绍Linux引导过程时，我们将介绍如何查错各种引导问题。最后，可以用红帽子安装光碟中的linux rescue方式对付大多数引导问题，以便修复任何损坏的文件。

第11章 配置与查错引导过程

有时Red Hat Linux可能无法启动计算机。如果遇到kernel panic之类的消息，不要头痛。也许根本不必从备份恢复系统。如果知道基本引导配置文件，则很容易迅速诊断和解决大多数引导问题。

要了解Linux引导配置文件的工作方法，就要了解基本引导过程，从硬件探测到运行级管理。

然后就可以了解管理硬件的关键引导配置文件的细节，如寻找内核、启动诊断和在不同运行级初始化服务。

如果遇到问题，则安装过程中生成的引导盘（有没有生成？）通常能够解决大多数问题。否则Red Hat Linux安装引导盘或安装光碟可以提供丰富的救援方式。本章介绍下列主题：

- 探索基本引导过程
- 了解默认配置文件
- 总结与使用建议

探索基本引导过程

介绍Red Hat Linux配置文件的细节之前，一定要先对这个过程有个总体了解。尽管小改动可能使Red Hat Linux无法引导，但了解总体有助于更快找到问题。

启动Linux计算机时，这个过程涉及三个基本步骤。首先要通过BIOS（基本输入/输出系统）初始化硬盘并由Linux探测硬件。BIOS指向Linux引导装入器。一旦启动引导装入器，它就会打开内核。然后它启动init程序，这是第一个程序，装入内核，并转入初始化其他启动程序。最后，Linux找到默认运行级，启动所有相关过程。

本章稍后将详细介绍每个过程的细节。

初始化硬件

尽管本书不是介绍计算机硬件的，但最好对硬件有个基本了解，然后可以更方便地判断问题是硬件问题还是Linux问题。

标准PC机上的一切都是由BIOS启动的。第一步是一系列嘟嘟声，称为通电自检（POST），检查与基本硬件的连接，寻找与IDE和SCSI盘相联系的其他BIOS，并可能探测系统中的其他硬件。

提示：如果对CompTIA的Linux+考试感兴趣，则要对PC机硬件有大量知识。详见Sybex公司出版的“Complete PC Upgrade and Maintenance, 2003 Edition”。

Linux通过引导装入器启动装入过程后，开始用kudzu实用程序探测硬件，然后用/etc/modules.conf中存储的设置增加与硬件相关的模块。可以用dmesg命令分析结果。如果遇到硬件问题，则不难从dmesg的输出中看到问题所在。

引导装入器

基本Linux引导装入器有两种：**GRUB**（统一引导装入器）和**LILO**（Linux引导装入器），前者是Red Hat Linux的默认，后者已经过时，今后的Red Hat Linux版本中可能将其删除。

无论哪个引导装入器，都有四个作用：

1. 选择操作系统（如果计算机上安装了多个操作系统）。
2. 标识相应引导文件所在的分区。
3. 找到内核。
4. 运行初始内存盘，设置内核与相关模块。

运行级

运行级是Linux中组织初始化软件的特定方式。不同服务在不同运行级中启动与停止。启动Red Hat Linux时，它从/etc/inittab中确定默认运行级，然后指向/etc/rc.d的相关子目录，标识要启动与停止的服务。

了解默认位置文件

硬件引导装入器和运行级都有关键启动配置文件。硬件配置文件可以确定探测到的内容。引导装入器可以跟踪内核、初始内存盘和计算机上任何其他操作系统的位置。每个运行级的目录可以帮助定制Linux计算机上的启动与停止过程。

硬件探测

一旦GRUB或LILO找到引导文件后，下一步是建立Linux内核与计算机硬盘之间的连接。Linux硬件探测分为几个部分。首先，Linux要从BIOS中取得基本硬件的相关数据，然后用kudzu实用程序检查系统上的新硬件。假设有默认模块化内核，则它插入/etc/modules.conf文件中与专用硬件相关的任何模块。可以用dmesg命令检查与这个过程相关的消息。

内核连接

dmesg命令可以在Linux启动时显示内核与硬件如何互动。它用BIOS启动，用相关信息寻找CPU、硬盘、PCI设备和通信端口，在相应分区启动相应文件系统，最后配置与键盘和鼠标相关的其他基本设备。图11.1是dmesg的输出摘要。

从样本输出可以看到一个CPU和128MB内存。如果实际上安装了多个CPU和更多内存，则这个输出表明Linux没有探测到其他硬件。

Kudzu

Kudzu的当前版本是Linux支持即插即用硬件的成果。过去，在Linux中使用即插即用硬件是有风险的。现在，它可以顺利管理任何新硬件。

```

linux version 2.4.20-8 (bhcompile@porky.devel.redhat.com) (gcc version 3.2.2 200
3022Z (Red Hat Linux 3.2.2-5)) #1 Thu Mar 13 17:54:28 EST 2003
BIOS-provided physical RAM map:
BIOS-e820: 0000000000000000 - 000000000000f800 (usable)
BIOS-e820: 000000000000f800 - 0000000000000000 (reserved)
BIOS-e820: 000000000000ca00 - 000000000000cc00 (reserved)
BIOS-e820: 000000000000dc00 - 000000000000e000 (reserved)
BIOS-e820: 000000000000e400 - 0000000000010000 (reserved)
BIOS-e820: 0000000000010000 - 000000000000bef000 (usable)
BIOS-e820: 000000000000bef000 - 000000000000befc00 (ACPI data)
BIOS-e820: 000000000000befc00 - 000000000000bf0000 (ACPI NVS)
BIOS-e820: 000000000000bf0000 - 00000000000c000000 (usable)
BIOS-e820: 00000000000c000000 - 00000000000fec10000 (reserved)
BIOS-e820: 00000000000fec10000 - 00000000000fec01000 (reserved)
BIOS-e820: 00000000000fec01000 - 0000000000000000 (reserved)
OMB HIGHMEM available.
192MB LOWMEM available.
On node 0 totalpages: 40152
zone(0): 4096 pages.
zone(1): 45056 pages.
zone(2): 0 pages.
Kernel command line: ro root=LABEL=/
Initializing CPU#0

```

图11.1 dmesg输出摘要

Kudzu寻找计算机上的不同端口。如果探测并识别了新硬件，则把相关信息加进/etc/sysconfig/kernel文件中，以便支持已识别的硬件。

如果需要特殊设备驱动程序，则把技术规范加进/etc/modules.conf中。下次启动计算机时，Linux在引导过程中读取这个文件，装入所要的驱动程序。

加进新硬件之后，为了保证Red Hat Linux能够正确探测到这个硬件，只要运行Kudzu命令。如果需要更多配置，则可以采用redhat-config-mouse的文本版本（见第19章），步骤与过时的mouseconfig实用程序相似。极少数情况下，可能还会提示增加IRQ端口、I/O地址、DMA信道等信息。

内核与硬件

Linux中很容易看到Linux内核如何看待硬件。只要看看/proc目录。如表11.1所示，/proc中的各种文件提供了连接Red Hat Linux的硬件信息。

表11.1 /proc目录中的一些硬件文件

文件	描述
apm	高级电源管理电池状态
cpuinfo	探测的CPU
dma	指定的DMA信道
ide	指定连接的IDE设备的目录
interrupts	指定的IRQ端口
ioports	指定的I/O地址
modules	安装的驱动程序模块，与lsmod的输出相同
partitions	基本分区信息
pci	探测的PCI设备
scsi	指定连接的SCSI设备的目录

这个信息相当详细。例如，图11.2显示了`/proc/cpuinfo`文件，其中不仅显示了CPU的速度与实际速度，而且显示cpu family，可以帮助找到系统使用的最优Linux内核。我使用`kernel-versionnumber.i686.rpm`包。这个用法见下一章介绍。

```
processor       0: 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 11
model name     : Intel(R) Pentium(R) III Mobile CPU      1200MHz
stepping       : 2
cpu MHz        : 1386.351
cache size     : 32 KB
fdiv_bug       : no
hlt_bug        : no
i00f_bug       : no
coma_bug       : no
fpu            : yes
fpu_exception  : yes
cpuid level    : 2
wp             : yes
flags           : fpu vme de pse tsc msr pae mce cx8 sep mtrr pge mca cmov pat p
se36 mmx fxsr sse
bogomips       : 2366.82
~
~
~
"/proc/cpuinfo" [readonly] 19L, 401C
```

图11.2 CPU详细信息在文件

/etc/modules.conf设置

有时Red Hat Linux的内核配置设置需要一些帮助。有时不同组件的默认即插即用设置可能会相互干扰。这时就要用到`/etc/modules.conf`配置文件。Linux在这里存储不同硬件组中的驱动程序、设备和地址设置。下面是`/etc/modules.conf`文件摘要：

```
alias eth0 pcnet32
alias usb-controller usb-uhci
options sb io=0x220 irq=5 dma=1 dma16=5 mpu_io=0x330
```

注意，其定义第一个以太网、USB控制器和声霸卡（sb）的驱动程序。Linux探测更多硬件时，这个文件的重要性不断下降。

改变`/etc/modules.conf`文件时，可以立即测试结果。例如，如果要寻找声霸卡的正确设置，则可以使用下列命令：

```
# modprobe sb
```

如果没有看到任何错误消息，则可以再次检查`lsmod`命令。也许声卡已经安装，否则要从错误消息中认真检查下一步的线索，可能是试验不同的硬件设置。

列出模块

可以验证红帽子软件是否能够探测你的硬件。除了浏览前面介绍的`/proc`目录内容外，还可以用`lsmod`命令检查安装的模块。例如，图11.3显示了用这个命令列出计算机上的一系列模块。


```
[root@RH9Desk root]# lsmod
Module                Size  Used by    Not tainted
usbfs                 44368  1 (autoclean)
ide-cd                 35708  0 (autoclean)
cdrom                  33728  0 (autoclean) [ide-cd]
parport_pc            19076  1 (autoclean)
lp                     8996  0 (autoclean)
parport                37056  1 (autoclean) [parport_pc lp]
autofs                 13268  0 (autoclean) (unused)
pcnet32                18240  1
mii                     3976  0 [pcnet32]
keybdev                2944  0 (unused)
mousedev              5492  1
hid                    22148  0 (unused)
input                  5856  0 [keybdev mousedev hid]
usb-uhci               26348  0 (unused)
usbcore                78784  1 [hid usb-uhci]
ext3                   70784  2
jbd                    51892  2 [ext3]
BusLogic              100796  3
sd_mod                 13452  6
scsi_mod              107128  2 [BusLogic sd_mod]
[root@RH9Desk root]#
```

图11.3 lsmod命令列出计算机上的一系列模块

可以看出，每个模块有个文件长度（字节数）。有些模块是相互依赖的。例如，要注意pcnet32网络驱动程序模块需要mii模块。换句话说，如果用下列命令删除mii模块，则会出现下列错误消息：

```
# rmmod mii
mii: Device or resource busy
```

如果从计算机上删除pcnet32网卡，则下次计算机启动时，Linux不会安装这两个模块。也可以关闭网络，然后依次删除这两个模块：

```
# rmmod pcnet32
# rmmod mii
```

安装模块也一样容易。例如，如果要安装新的3Com EtherLink网卡，而Linux没有探测到，则可以用下列命令安装相应模块：

```
# insmod 3c589_cs
```

如果成功，则不会出现任何错误消息，可以用lsmod命令检查结果。输出中会出现网卡模块。

引导装入器

前面曾介绍过，Red Hat Linux默认引导装入器为GRUB，比LILO有多处改进，包括：

- 口令保护。
- 易于在引导过程中编辑。可以试验不同引导参数，而不必永久改变GRUB配置文件。
- 可以从硬盘的主引导记录（MBR）区引导Windows NT操作系统。
- 支持LBA（逻辑块寻址）方式，可以帮助计算机寻找/boot文件，特别是硬盘中1024柱面以上位置的文件。

LILO已经过时，红帽子公司计划在今后删除Red Hat Linux中的LILO。因此，本书不再介绍这个旧的引导装入器。

下面看看/boot/grub/grub.conf中的典型GRUB配置文件，如图11.4。

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda2
#          initrd /initrd-version.img
#boot=/dev/sda
password --md5 $1$61hul/$uu0q208r M0Tj2KluR8QV1
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-8)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
    initrd /initrd-2.4.20-8.img
title DOS
    rootnoverify (hd0,0)
    chainloader +1
-
-
```

图11.4 双引导GRUB配置文件

表11.2列出了图11.4中显示的变量。

表 11.2 变量与GRUB设置

变量	说明
password	口令保护GRUB，使用--md5开关时，可以按加密格式输入口令
default	指定默认操作系统。如果为0，则没有用户输入时，自动启动第一段中显示的操作系统
timeout	设置GRUB启动默认之前的时间极限（秒数）
splashimage	指定默认GRUB映像
title	设置GRUB菜单中显示的选项
root	指定/boot文件所在分区
kernel	指定Linux内核地址
initrd	指向初始内存盘地址
rootnoverify	对Windows XP之类的敏感操作系统指定引导文件所在分区
chainloader	+1表示对指定分区中第一个扇区寻找引导文件

GRUB中的/boot变量不容易理解，因为它实际上指的是/boot目录。注意与根相关的数据，如(hd0,0)与(hd0,1)。这个数据指向该操作系统的引导文件所在分区。

如果找不到硬件，则尽量使用前面介绍的硬件模块。但可能要向Linux提供一些寻找引导过程中关键硬件的帮助信息，如硬盘或其SCSI控制器。这时，应在kernel行中指定模块。例如，如果对旧式Adaptec控制器指定IRQ端口9、IO地址0x330、SCSI号7，则可以在grub.conf配置文件的kernel行中增加下列命令：

```
kernel /vmlinuz-2.4.20-2.2 ro root=LABEL=/ aha152x=0x330,9,7
```

引导硬盘显示为/dev/sda说明，因此，root (hd0,1) 指向第一个SCSI硬盘第二个分区（即/dev/sda2）中的Linux引导文件。同样，root (hd0,0) 设置指向第一个SCSI硬盘第一个分区（即/dev/sda1）中的DOS引导文件。

说明：为了方便起见，/etc/grub.conf链接实际引导装入器的配置文件/boot/grub/grub.conf。

提示：Linux中root一词有多个含义，根用户的主目录为/root，而顶层根目录则是/。在GRUB中，root变量实际上指的是/boot目录所在分区。因此，GRUB配置文件中看到的“/”实际上是/boot目录。

在GRUB中增加口令

如果Red Hat Linux安装过程中没有增加GRUB，则很容易在GRUB中增加安全MD5口令。只要使用grub-md5-crypt命令，在提示下输入所要口令。可以看到一系列奇怪的字符，可以将其复制到配置文件中，如图11.2所示。

很容易从命令行复制这个口令，只要用鼠标加亮选择口令，在文本编辑器中打开/etc/grub.conf，在所到位置右单击鼠标，然后Linux即会自动插入加亮的MD5口令。如果系统在GNOME终端中，也可以右单击打开一个弹出菜单，从中复制和粘贴加亮选择的文本。

/etc/inittab

Linux现在要初始化系统中的关键文件、进程和应用程序。主控配置文件为/etc/inittab。在喜欢的文本编辑器中打开这个文件。这个文件中的关键变量是initdefault，其他变量设置Linux环境的重要部分。图11.5显示了我的/etc/inittab文件。

```
# inittab      This file describes how the INIT process should set up
#             the system in a certain run-level.
#
# Author:      Miguel van Sjoenenburg, <miguels@drinkel.nl.nuget.org>
#             Modified for RHEL Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHEL are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
#
# System initialization.
#
# 10:0:wait:/etc/rc.d/rc 0
# 11:1:wait:/etc/rc.d/rc 1
# 12:2:wait:/etc/rc.d/rc 2
# 13:3:wait:/etc/rc.d/rc 3
# 14:4:wait:/etc/rc.d/rc 4
# 15:5:wait:/etc/rc.d/rc 5
# 16:6:wait:/etc/rc.d/rc 6
#
# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
#
# When our UPS tells us power has failed, assume we have a few minutes
# of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
of::powerfail:/sbin/shutdown -f -h 42 "Power Failure: System Shutting Down"
```

图11.5 /etc/inittab文件

initdefault变量设置默认运行级，在引导Linux时启动。例如，下列语句将计算机配置成在运行级3中启动：

```
id:3:initdefault
```

Red Hat Linux有六个标准运行级，见表11.3（Red Hat Linux不用运行级4）。下节介绍在运行级3中启动Linux时的情形。

表11.3 Red Hat Linux标准运行级

运行级	功能
0	停止, 关闭Linux, init停止计算机上当前运行的所有服务
1	单用户方式, 不联网, init只是启动单个用户登录Linux系统所需的程序, 本章稍后将会介绍, 可以在单用户方式中修复关键文件等
2	多用户方式, 不能访问NFS, init启动程序, 使多个用户可以同时登录Linux系统
3	多用户网络方式, 多用户运行级之后, init启动计算机上的网络监控程序
5	图形登录, init启动网络程序, 然后启动X窗口程序, 可以分成客户机和服务器
6	重新启动, 按/etc/inittab中id命令定义的运行级关闭Linux和重新启动计算机

其他Linux发行版本可能使用不同的标准运行级。

警告: 不要将默认运行级设置为0或6, 否则计算机会在启动Linux时关闭或进入重新启动的循环。

标准Red Hat Linux /etc/inittab文件中有几个其他重要命令。下列命令

```
.          si::sysinit:/etc/rc.d/rc.sysinit
```

运行rc.sysinit脚本, 激活配置的网卡, 配额, 安装文件系统, 激活LVM (逻辑卷管理) 与RAID分区, 装入硬件模块, 等等。简而言之, rc.sysinit运行Linux激活服务。

为了帮助Microsoft Windows用户, /etc/inittab把Ctrl+Alt+Del键组与shutdown命令相关联。

提示: 如果设置Linux服务器, 则可能要将ca::ctrlaltdel:/sbin/shutdown -t3 r now命令标为说明语句, 以免因为一个用户的错误而关闭整个系统。

默认情况下, Red Hat Linux用/etc/inittab设置六个虚拟终端控制台: tty1到tty6。可以按Ctrl+Alt+Fn访问不同的虚拟控制台, 其中n是虚拟控制台编号。Red Hat Linux允许配置最多12个虚拟控制台, 其在/etc/inittab中的命令如下:

```
1:2345:respawn:/sbin/mingetty tty1
```

这个命令在Linux以运行级2、3、4、5启动时配置第一个虚拟控制台 (tty1)。

提示: 如果刚刚编辑/etc/inittab, 则不一定要重新启动。例如, 如果增加了虚拟控制台, 则可以用telinit q命令促使Linux重读/etc/inittab文件。

第一个进程: init

第一个进程init与/etc/inittab密切相关。它在几个不同运行级中工作, 主要脚本在/etc/rc.d目录中。例如, 如果运行init 5命令, 则Linux运行/etc/rc.d/rc5.d目录中的脚本。

启动一个运行级

下面要介绍Red Hat Linux如何用initdefault变量启动一个运行级。前面曾介绍过, Red Hat Linux通常在运行级3启动, 即完全多用户方式。Linux读取所要运行级时, 启动相关的脚本。在这里, 下列命令启动运行级3的所有脚本:

```
13:3:wait:/etc/rc.d/rc 3
```

这个命令指向与指定运行级相关的脚本，然后依次执行kill与start脚本。很容易比较两个不同运行级，只要检查相应目录中的脚本清单。图11.6比较了运行级3与运行级1的脚本。

[root@RH9Desk root]# \ls /etc/rc.d/rc3.d/				
K05ssslauthd	K95firstboot	S13portmap	S28autofs	S90cups
K15htptd	S05kudzu	S14nfslock	S45sshd	S90xfs
K20nfs	S06vmware-tools	S17keytable	S56rawdevices	S95anacron
K25irda	S08iptables	S20random	S56xinetd	S95atd
K35smb	S09lsm	S24pcmcia	S60sendmail	S97rhnsd
K35winbind	S10network	S25netfs	S85gpm	S99local
K74ntpd	S12syslog	S26apmd	S90crond	
[root@RH9Desk root]# \ls /etc/rc.d/rc1.d/				
K09rhnsd	K15gpm	K35smb	K74apmd	K88syslog
K05anacron	K15htptd	K35winbind	K74ntpd	K90network
K05atd	K20nfs	K44rawdevices	K75netfs	K91lsm
K05ssslauthd	K25irda	K50xinetd	K80random	K92iptables
K10cups	K25sshd	K60crond	K86nfslock	K95firstboot
K10xfs	K30sendmail	K72autofs	K87portmap	K95kudzu
[root@RH9Desk root]#				

图11.6 资源控制脚本

说明：计算机上的kill与start脚本随安装的服务和这个运行级中激活的服务不同而不同。

目录很简单，kill脚本以K开头，而start脚本以S开头。这些脚本按显示的顺序执行。但也有一些差别。运行级3要启动超过25个服务，大部分与网络有关。运行级1停止几乎每个服务，只运行单用户方式所需的服务。单用户方式不需要网络和多用户配置。

说明：记住，S05lsm启动一个服务，而K15ntpd会停止另一个服务。关于服务管理的更多信息，见第13章。

查错与使用救援盘

系统管理员要检查和编辑几个配置文件。进行改变时，可能发生错误。例如，如果编辑GRUB配置文件时发生错误，则下次启动Linux时会出现下列消息：

```
root (hd0,1)
Filesystem type is ext2fs, partition type 0x83
kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
Error 15: File not found
Press any key to continue
```

这只是许多引导问题中的一个。安装过程中生成的引导软盘也许能帮上你的忙。如果找不到这个盘，则可以使用mkbootdisk命令。

但是，引导盘并不是包医百病的灵丹妙药，如果没有引导盘，则Red Hat Linux还提供了其他自动恢复选项。可以使用任何标准的安装引导盘，包括用第一个安装光碟恢复Linux系统。根据不同的问题，可以选择自动化恢复过程，也可以单用户方式中启动Linux。

提示：红帽子公司有时还提供一个优化救援盘，可以从ftp.redhat.com站点下载，其中有emacs与pico之类的文本编辑器和Telnet与FTP之类的网络实用程序。检查红帽子公司FTP站点的文件rescue-cd.iso，用第14章介绍的方法建立光碟。

专用引导盘

解决指定问题的最简单方法是使用引导盘。Red Hat Linux安装期间生成的引导盘就是为此定制的。只要没有改变分组组织方式，定制引导盘就可以启动Linux系统。

利用mkbootdisk versionnumber命令很容易建立新的引导盘，它使用与Linux内核相关联的版本号。例如，如果/boot目录中显示的内核为vmlinuz-2.4.21-13，则可以用下列命令在三寸软盘上建立定制引导盘：

```
# mkbootdisk 2.4.21-13
Insert a disk in /dev/fd0. Any information on the disk will
be lost. Press <Enter> to continue or ^C to abort: _
```

记住要尽快测试定制引导盘，而不要到想恢复Linux系统时才发现这个盘不行。

救援方式

定制引导盘并不能解决所有Linux引导问题。好在还有别的办法。即使丢失了定制引导盘，红帽子的linux rescue方式通常也能进入Linux系统。一旦启动Linux之后，可以恢复或修复任何损坏的文件。

提示：如果用linux rescue方式，就要访问Red Hat Linux的文件。如果从网络引导盘启动，则需要/RedHat目录的地址和位置，见第4章的例子。

可以从Red Hat Linux安装引导盘启动linux rescue方式。如果没有安装引导盘，则可以从ftp.redhat.com站点或其镜像站点下载。甚至可以在Microsoft Windows计算机上用RAWRITE.EXE实用程序生成安装引导盘，见第3章介绍。只要在安装Red Hat Linux的引导提示下输入linux rescue，如下：

```
boot: linux rescue
```

也许你会问，自己到底做对了没有，因为Red Hat Linux会进行标准安装的前两步：语言与键盘类型。如果使用Red Hat Linux安装软盘，则会进入图11.7所示的屏幕，还要输入Red Hat Linux安装文件地址（本地或网络）。更多信息见第4章介绍。

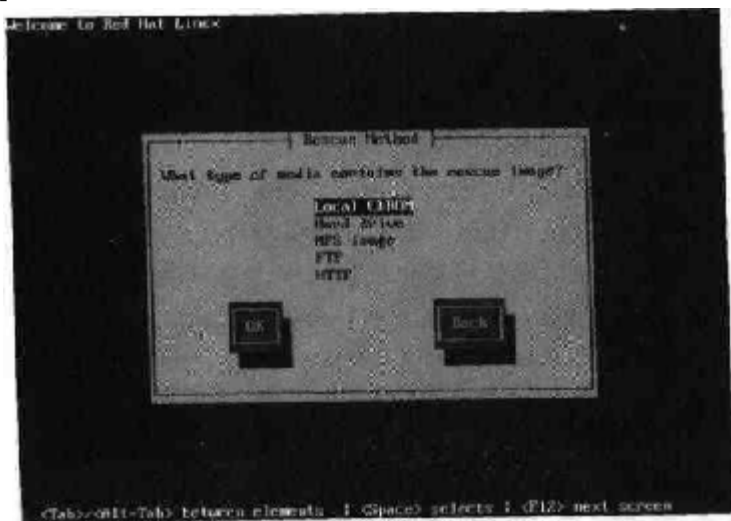


图11.7 输入Red Hat Linux安装文件地址

这时linux rescue方式出现一个菜单，有三个选项：

Continue 如果选择这个选项，则Red Hat Linux搜索硬盘中的安装文件。所有找到的文件系统都装载成/mnt/sysimage的子目录，可以看成是自动化救援方式。

Read-Only 如果选择这个选项，与上一选项差不多，只是找到的文件系统都装载成只读方式，可以看成是只读救援方式。

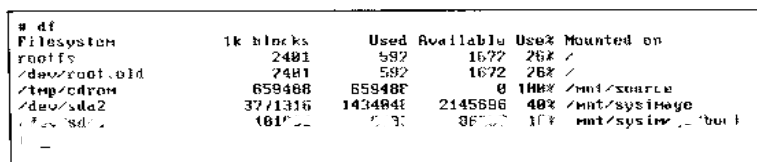
Skip 如果选择这个选项，则直接出现单用户方式的根shell提示，不查找可用的文件系统。可以看成是手工救援方式。

进行必要的改变之后，输入exit命令。根据需要重复，直到看到一个终止信号消息。

Linux卸载所有文件系统，然后自动重新启动计算机。

自动化救援方式

如果自动化救援方式成功，则Red Hat Linux将/etc/fstab中所有相应文件系统都装载成/mnt/sysimage的子目录。这时，df命令可以反映装载的目录，如图11.8所示。



Filesystem	1k blocks	Used	Available	Use%	Mounted on
rootfs	2481	592	1672	26%	/
/dev/root.old	2481	592	1672	26%	/
/tmp/cdrom	659488	659488	0	100%	/mnt/source
/dev/sda2	371316	143484	214588	40%	/mnt/sysimage
/dev/sda1	161728	0	161728	0%	/mnt/sysimage/boot

图11.8 救援方式装载

图11.8中，光碟装载到/mnt/source，/dev/sda2装载到/mnt/sysimage，而/dev/sda1装载到/mnt/sysimage/boot。尽管很容易看到/dev/sda1与/boot相关联，/dev/sda2与根目录(/)相关联，但可以用partitiondevice命令确认，如下：

```
# e2label /dev/sda1
/boot
```

如果自动化救援方式无法装载所有文件系统呢？这时可能看到如下所示的错误消息：

```
Error mounting filesystem on sdc1: Invalid argument
```

只要简单地继续自动化救援方式。Linux会尽量装载更多文件系统，这里可以处理/dev/sdc1之类的卸载文件系统的任何损坏部分。

如果有一个或多个卸载文件系统，则首先要检查fstab配置文件和格式本身的完整性。这时可以用vi编辑器检查fstab，但由于根目录(/)实际装载到/mnt/sysimage，因此fstab配置文件要用下列命令打开：

```
# vi /mnt/sysimage/etc/fstab
```

为了清理损坏的卸载文件系统，也可以用fsck devicename命令。例如，要检查/dev/sdc1，用下列命令：

```
# fsck /dev/sdc1
```

提示：如果要在linux rescue方式中访问Linux手册页，则可以运行chroot /mnt/sysimage命令，其恢复顶层根目录(/)为层次顶层，激活Linux手册页的标准路径。

只读救援方式

只读救援方式与自动化救援方式的惟一差别在于找到的文件系统都装载成只读方式，这适合有大量文件系统时，如典型的Red Hat Linux服务器安装。

可以在只读方式中重装任何需要的文件系统。例如，下列命令以读写方式在根目录（/）中重装分区设备/dev/sda2:

```
# mount -w -o remount /dev/sda2 /
```

说明：这个命令等价于第7章介绍的mount -o remount, rw /命令。

手工救援方式

有时linux rescue方式找不到任何文件系统。别担心，问题可能只是/etc/fstab中简单的名称错误。这时可以使用手工救援方式。

手工救援方式在内存盘中装入最基本的根映像和内核，然后发出一个根shell提示（#），不装载任何文件系统，只能使用基本命令集，如mount、mkdir、mv、cp、rm、fdisk与fsck。装载目录之后，还可以用vi编辑器根据需要改变文件。

记住，这只是Linux的最基本版本，能用的命令不多。

在手工救援方式中，第一步是在/root/sysimage之类的临时地址装载与根目录（/）相关联的分区。这样就可以从bin、sbin和usr/sbin之类的目录访问更多命令。

单用户方式

另一种方式是单用户方式，可以登录损坏的Linux系统。如果Linux能够找到根目录（/）文件系统，则可以在单用户方式中启动Linux。前面曾介绍过，单用户方式也称为运行级1，只需要两个服务。

进行必要的改变之后，不必重新启动。exit命令自动转入/etc/inittab中定义的默认运行级，init 3或init 5命令也可以立即启动相应运行级。单用户方式还可以改变根口令。如果忘记了口令，则可以在单用户方式中运行passwd命令，输入的口令即成为新的根口令。

有时会在引导过程中遇到一些问题，如/etc/fstab文件损坏或文件系统无法装载。这时可以看到图11.9所示的提示。在提示下输入根口令时，Linux启动单用户方式。

```
Setting clock (utc) Sat Mar 29 13:39:37 EST 2003      [ OK ]
Loading default keymap (us):                        [ OK ]
Setting hostname RH9Desk:                           [ OK ]
Initializing USB controller (usb-uhci):             [ OK ]
Mounting USB filesystem:                             [ OK ]
Initializing USB HID interface:                     [ OK ]
Initializing USB keyboard:                          [ OK ]
Initializing USB mouse:                             [ OK ]
Checking root filesystem
WARNING: couldn't open /etc/fstab: No such file or directory
/:
The superblock could not be read or does not describe a correct ext2
filesystem. If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
e2fsck -b 8193 <device>

fsck ext2: Is a directory while trying to open /
[ OK ]

*** An error occurred during the file system check
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue): _
```

图11.9 退回单用户方式

也可以从GRUB菜单中启动单用户方式。前面曾介绍过,很容易用口令保护GRUB。如果看不到图11.10所示的GRUB编辑选项,则可以输入P命令,然后输入GRUB口令。



图11.10 GRUB编辑选项

加亮选择Linux操作系统,然后按a命令修改内核变量。GRUB进入下列语句:

```
grub append> ro root=LABEL=/  
grub append>
```

这时可以在这行末尾增加命令,如single、1或init=/bin/sh,如图11.11。



图11.11 为单用户方式修改GRUB

按Enter键时,Red Hat Linux在单用户方式中启动,即运行级为1。这时可以对卸载盘执行fsck、编辑配置文件、检查LVM分区状态,等等。

小结

本章介绍了Linux引导过程。基本引导过程首先从计算机BIOS开始。探测系统中的基本硬件之后，它指向Linux引导装入器（GRUB），可以选择一个操作系统。选择Red Hat Linux时，引导装入器启动内核。然后/etc/inittab文件启动默认运行级的相关进程。

可以在Linux安装期间或之后用mkbootdisk命令生成定制引导盘。即使引导过程中遇到几个问题，也可以用它启动Linux。但是，也可以使用linux rescue方式，其用到一张Red Hat Linux安装引导盘。在不同的linux rescue方式中，可以对卸载盘执行fsck、编辑配置文件，等等。也可以在单用户方式中启动Linux，从而解决其他问题，如丢失根口令。

说明：按照红帽子术语，分区检查通常用命令名表示，如可以fsck一个分区。

下一章介绍Linux内核的细节。了解内核的细节之后，就不难修改、重新编译和实现新的Linux内核。

第12章 升级与重新编译内核

重新编译内核的想法让许多Linux用户望而生畏。的确如此，重新编译发生错误可能使系统无法启动。如果没有适当的备份，则恢复也很困难。但是，只要采取一些预防措施，就可以避免内核重新编译的风险。了解基本步骤之后，这个过程就不太困难了。

升级内核有一个简单步骤，只要安装与CPU对应的下一版红帽子Linux内核RPM包即可。红帽子Linux内核RPM包会自动更新引导装入器，因此可以用新版或旧版内核启动Linux。

红帽子Linux内核RPM包不一定包括最新更新。最新Linux内核是以tarball格式提供的，而小的升级则只需要使用补丁包。本章将介绍这两个选项。

可以定制和重新编译已经在计算机上的内核，也可以下载、定制和重新编译新内核。由于选项很多，使这个过程看上去比较复杂。本章介绍三种不同的内核配置工具。

本章根据GUI内核配置工具，详细分析可以进行的改变。这个工具组织成配置菜单、存储设备、网络、其他硬件支持和其他软件支持几个类别。

我在此处包括了几个不同的内核版本。Red Hat Linux 9发布的Linux内核版本是2.4.20。本章的有些版本号可能更高，反映了你或同事已经进行的改变。

进行所要改变之后，还要编译新内核，这个过程很简单。编译内核之后，要将其复制到相应目录中。至少目前还要将其配置到引导装入器中，就像新旧内核是两个不同操作系统一样。本章介绍下列内容：

- 为什么要升级和重新编译内核
- 选择简单方法
- 探索tarball与补丁包
- 设置配置菜单
- 了解内核的各个部分
- 编译新配置
- 更新引导装入器

为什么要升级和重新编译内核

Red Hat Linux所带的内核适用于大多数软件和硬件，但有时还是需要改变内核：

驱动程序 你要利用新驱动程序，可能是新装的硬件，或者是要试验一个文件系统。

缺陷 当前Linux内核的某个缺陷可能影响操作系统的运行。

特性 新内核可能提供改进的硬件支持，如IEEE 1394 FireWire录像机。也许可以连接802.11a无线网络。

安全 可能要抵抗新发现的安全漏洞。

长度 为了使系统加速，可能要删除不必要的驱动程序，从而减少内核长度。

需要改变内核时，要依次考虑下列事项：

1. 重新编译现有内核。新内核及相关源代码会占用大量空间。新内核不一定适用于现有软件。现有内核也许能够完成所要的工作。
2. 补充现有内核。可以用补丁包对Linux内核进行小的升级。补丁包会加进当前内核源代码中。例如，只要一个补丁包就可以将内核从2.4.20升级到2.4.21。
3. 安装新内核。安装新内核包之后，还要配置和编译新内核。

内核版本号

Linux内核用vmlinuz-2.4.23之类的名称存放在/boot目录中。所有内核的版本号采用major.minor.patch编号格式。这里，第一个数（2）指第二大版本；第二个数（4）有两个含义：是指定大版本的第四个小版本，偶数表示生产版（而奇数表示测试版）；第三个数（23）表示指定小版本的第二十个补丁包。

Red Hat Linux内核的版本号稍有不同，如2.4.23-10。可以看出，这里多一个数，是建立（build）号。每个“建立”可以增加少量新驱动程序或缺陷修复。一些Red Hat Linux内核还有个带“pp”、“pre-patch”的数字，是一个内核的测试版本。

如果在生产计算机上安装新内核，则不要安装小版本为奇数的内核，如2.5.22，这是测试版，不适用于实际使用。此外，`makeauth (p)` 为奇数版本的风险也很大。

简单升级

Red Hat Linux很容易“升级”内核。如果你愿意使用“库存”的红帽子包的内核RPM包，则可以非常方便地安装下一个内核版本。

此外，如果安装红帽子包内核RPM包，则新内核加进引导装入器中，就像是另一个操作系统。如果新内核遇到问题，则还可以重新启动并在引导装入器中选择旧内核。

安装最新Red Hat Linux内核

尽管可以升级RPM包，但最好安装最新Red Hat Linux内核RPM包。是的，这样就会同时安装两个Linux版本。图12.1显示了一个例子，这个网络上的RPM包装载到/mnt/source目录。

```
[root@RHLS root]# rpm -ivh /mnt/source/RPMS/kernel-2.4.20-8.i686.rpm
error: Failed dependencies:
  SysVinit < 2.84-13 conflicts with kernel-2.4.20-8
  pam < 0.75-48 conflicts with kernel-2.4.20-8
  vixie-cron < 3.0.1-73 conflicts with kernel-2.4.20-8
  cups < 1.1.17-13 conflicts with kernel-2.4.20-8
[root@RHLS root]# rpm -Uvh /mnt/source/RPMS/SysVinit-2.84-13.i386.rpm
Preparing... [100%]
1:SysVinit [100%]
[root@RHLS root]# rpm -Uvh /mnt/source/RPMS/pam-0.75-48.i386.rpm
Preparing [100%]
1:pam warning: /etc/pam.d/system-auth created as /etc/pam.d/system-auth.rpmnew
[100%]
[root@RHLS root]# rpm -Uvh /mnt/source/RPMS/vixie-cron-3.0.1-74.i386.rpm
Preparing... [100%]
1:vixie-cron [100%]
[root@RHLS root]# rpm -e cups cups-drivers
warning: /etc/xinetd.d/cups-lpd saved as /etc/xinetd.d/cups-lpd.rpmnew
warning: /etc/cups/printers.conf saved as /etc/cups/printers.conf.rpmnew
warning: /etc/cups/classes.conf saved as /etc/cups/classes.conf.rpmnew
[root@RHLS root]# rpm -ivh /mnt/source/RPMS/kernel-2.4.20-8.i686.rpm
Preparing... [100%]
1:kernel [100%]
[root@RHLS root]#
```

图12.1 安装最新Red Hat Linux内核RPM包

可以看出,较高的内核版本有时要求升级或暂时删除其他包。升级是有风险的,因为这样更难恢复。但是,这些包对Linux内核并不重要。因此,即使遇到最糟的情况,也只要删除升级的包,然后重新安装原先的RPM包。

还有几个红帽子kernel-* RPM包,可以根据CPU进行定制。Red Hat Linux内核RPM包文件按下列格式组织:

kernel-versionnumber.cputype.rpm

表12.1列出了不同CPU类型的红帽子定制内核。红帽子公司可能没有在对CPU定制的内核RPM格式中提供最新Linux内核。为了寻找cputype,可以用下列命令:

```
# uname -p
```

说明:本章余下部分将用x表示文件与目录中的版本号。

表12.1 定制红帽子内核

CPU类型	描述
alpha	适用于HP alpha CPU, 原先是DEC公司开发的
athlon	适用于AMD Athlon CPU
i386	一般Intel内核。适用于i386、i586与i686 CPU
i586	适用于Intel 586 CPU
i686	适用于Intel 686 CPU
ia64	适用于Intel Itanium 64位CPU
ppc	适用于Power PC CPU
ppc64	适用于Power PC 64位CPU
s390	IBM服务器专用CPU
s390x	s390的64位版本
sparc	Sun系统公司为Solaris操作系统开发的

说明:记下安装的RPM包。从/root/install.log开始,这是计算机安装Red Hat Linux时安装的RPM清单。

很容易安装新内核RPM包。图12.1显示了典型步骤,所用的命令可能不同。例如,如果内核RPM文件名为kernel-2.4.22.i686.rpm,位于/mnt/source目录中,则只要运行下列命令:

```
# rpm -ivh /mnt/source/kernel-2.4.22.i686.rpm
```

如果图12.1中出现Failed dependencies错误,则先要安装错误消息中列出的包。要安装或升级的实际包取决于新内核要求和已经安装的包。

安装另一内核时,要在/boot目录中安装几个文件。这些文件和旧内核的相应文件存放在一起。表12.2总结了这些文件。

新内核会自动安装,多么容易。下节介绍新装的内核对引导装入器有什么影响。

表12.2 内核相关/boot文件

文件	描述
config-*	内核配置文件
initrd-*	初始内存盘, 使内核可以在引导过程开始时访问驱动程序
module-info-*	这个内核可用的硬件模块清单
System-map-*	具有不同功能的内核映射
vmlinuz-*	内核
vmlinuz-*	内核的压缩版

引导装入器更新

Red Hat Linux内核RPM包自动更新活动引导装入器, 不管它是GRUB还是LILO。每个引导装入器的详细信息见第11章介绍。图12.2显示修改后的grub.conf文件, 有两个不同内核。

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
# all kernel and initrd paths are relative to /boot/, eg.
# root (hd0,0)
# kernel /vmlinuz-2.4.20-9 ro root=/dev/sda
# initrd /initrd-2.4.20-9.img
#boot=,dev,=sda
default=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-9)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-9 ro root=LABEL=/
    initrd /initrd-2.4.20-9.img
title Red Hat Linux (2.4.20-8)
    root (hd0,0)
    kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
    initrd /initrd-2.4.20-8.img
title DOS
    rootnoverify (hd0,1)
    chainloader +1
"/etc/grub.conf" 25L /05C
```

图12.2 修改后的grub.conf文件

这个grub.conf文件好像可以选择三个不同操作系统:

- Red Hat Linux (新内核号)
- Red Hat Linux (旧内核号)
- DOS (通常是Microsoft Windows的某个版本)

记住, 内核是操作系统的核心。因此, 安装新内核时, 实际上是安装Linux的另一个版本, 但这两个版本使用几乎相同的实用程序、程序和命令。

还可以看到default=1命令, 实际把第二段作为默认操作系统。换句话说, 如果10秒钟内不选择另一操作系统(timeout), 则GRUB自动引导旧的Red Hat Linux内核。

图12.3显示了结果, 可以看到相关GRUB菜单。注意第二个Red Hat Linux版本(使用原内核号)是加亮显示的。

说明: 默认Red Hat Linux引导装入器为GRUB。Red Hat Linux安装程序把LILO版本保存在/etc/lilo.conf.anaconda中, 如果在/etc/lilo.conf中复制这个文本, 则Red Hat Linux内核RPM包也会自动升级LILO。



图12.3 修改的GRUB菜单

Tarball与补丁包

使用Red Hat Linux的tarball包的一个缺点是，它不一定在最新内核中包括最新特性。如果需要真正的最新内核，则可能要下载和处理Tarball包。关于tar命令的更多信息，见第14章，下面介绍具体步骤。

下载源代码

Linux内核是不断发展的，随着新特性的出现，Linus Torvalds领导的松散志愿小组会确定新内核何时推出测试版本与生产版本。可以从kernel.org因特网站点下载相关结果。如果无法访问www.kernel.org或ftp.kernel.org站点，则可以选择www.kernel.org/mirrors中列出的镜像站点。

图12.4演示从zeus-pub.kernel.org下载Linux内核2.4.20的过程。这个包很大，大约有33MB，因此在普通电话MODEM上下载时可能要花几个小时。

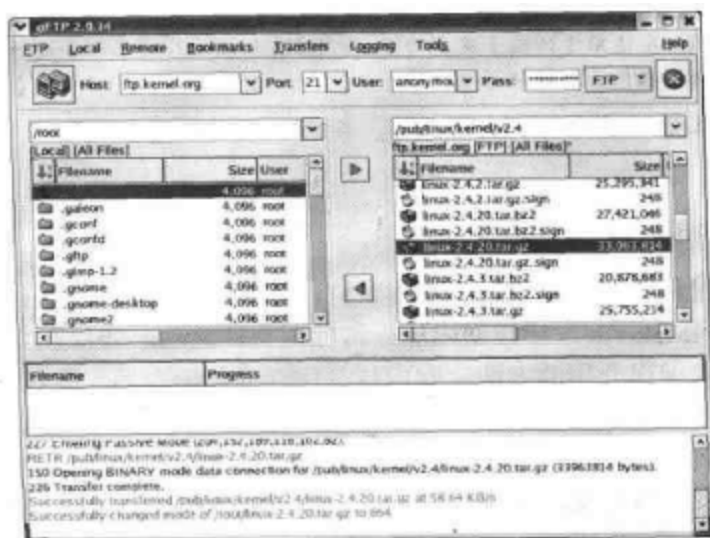


图12.4 下载内核tarball

安装

下载内核tarball包之后，安装过程很简单。下载的包应有linux-x.tar.gz之类的名称。安装步骤如下：

1. 将内核tarball包复制到/usr/src目录中。例如，如果包在当前目录中，则运行下列命令：

```
# cp linux-x.tar.gz /usr/src
```

2. 导航到/usr/src目录并打开tarball包。可以用下列命令在/usr/src/linux-x目录中打开大量文件：

```
# cd /usr/src
# tar xzvf linux-x.tar.gz
```

3. 导航到/usr/src/linux-x目录中。本章稍后将介绍如何打开与使用Linux内核配置菜单。然后要编译和安装新内核。

补丁包选项

如果只是为了升级最新改变，则安装和编译新内核显得太麻烦了。假设计算机上已经安装Linux内核2.4.10，现在要升级到Linux 2.4.11并安装安全补丁，则可以使用另一种方法：可以安装内核补丁包。

说明：我们假设你已经通过kernel-source-* RPM包安装了当前内核的源代码。本章稍后的表12.3将介绍所要的其他RPM包。

可以从kernel.org因特网站点或镜像站点下载内核补丁包。到本书编写时，补丁包与普通内核放在同一目录中，名称为patch-x.gz。

下载补丁包之后，将其复制到/usr/src目录中，然后即可用下列命令升级内核：

```
# zcat patch-x.gz | patch p0
```

这个命令读取压缩的补丁包文件，标识与当前Linux内核源代码的差别，然后根据需要更新文件。如果遇到问题，则会在内核源代码目录/usr/src/linux-x的*.rej文件中记录。

说明：补丁包不一定适用于红帽子建立的Linux内核。红帽子公司已经加进一些补丁包内容，因此可能在升级过程中出现错误。

然后可以按本章稍后介绍的方法定制、编译和安装补丁包内核。

定制内核

定制内核的过程很长。本节介绍基本步骤，本章稍后要详细介绍使用图形配置菜单的步骤。首先要编辑Makefile，标注新内核；清理源文件之后，要保存当前配置。

然后要用本章前面介绍的方法定制内核。保存当前配置后，要组织依赖性和建立新的内核映像。

这时已经对内核进行了必要的改变，激活所要的设置，包括相应硬件模块，通过关掉不要的项目而减少内核长度，保存改变。下一步要编译和建立新的内核。

内核不同，所要的步骤也不同。首先要阅读/usr/src/linux-x目录中的README文件，看看这个过程有什么大变化。

准备源代码

也许你已经下载新内核，也许只要对当前使用的内核改变几个设置。无论哪种情况，都要准备源代码。

记住，源代码位于/usr/src/linux-x目录中，其中x表示内核的linux-versionnumber。导航到这个目录，依次阅读下面几节的内容。

提示：修改和重新编译Linux内核时，一定要按顺序执行下列指令。遇到问题时，可以参考Linux Kernel HOWTO文档，站点为www.tldp.org。

Makefile文件

用喜欢的文本编辑器打开位于/usr/src/linux-x目录中的Makefile文件。这个文件的前四行如下：

```
VERSION = 2
PATCHLEVEL = 1
SUBLEVEL = 2
EXTRAVERSION = something
```

如果你不熟悉Linux内核，则可能不太理解。Makefile文件中的标号与标准内核编号格式不一致：PATCHLEVEL是内核的小版本号，而SUBLEVEL是内核的补丁包修订号。

EXTRAVERSION是Linux加到内核文件末尾的内容，可以在这个过程结束时传输到/boot目录中，也可以帮助标识引导装人器（如GRUB）中的新内核。

将EXTRAVERSION变量变成能够识别的内容。本章将Makefile文件中的该行变成如下：

```
EXTRAVERSION = sugaree
```

提示：注意EXTRAVERSION变量，如果sugaree后面有多余空格，则会在内核模块配置过程中产生错误。

保存当前内核配置

如果没有修改过内核，则红帽子公司已经提供当前内核配置文件。前面曾介绍过，它在/boot/config-x文件中。如果从“库存”内核RPM包安装另一个Red Hat Linux内核，则情况也是如此。

如果前面已经重新编译内核，则当前内核配置放在位于/usr/src/linux-x目录中的隐藏文件.config中。将它保存起来，下节介绍的步骤会删除这个文件。

无论哪种情形，都要备份当前配置。这些文件很小，可以放在普通软盘上。

清理源代码

准备Makefile文件之后，就要清理源代码。如果还没有进入/usr/src/linux-x目录，请进入这个目录。下列命令用Makefile脚本，清理与内核源代码编译有关的文件和目录：

```
# make mrproper
```

提示：本章每个make命令都可能在几千行代码中运行。尽管有些只要几分钟，但有些可能要几个小时，特别是在低速计算机上，因此一定要有耐心。

标准开始点

从ftp.kernel.org之类非红帽子源下载内核时，可能要调整几百个设置，匹配当前Red Hat Linux配置。这个过程是很麻烦的。

也可以对内核设置Red Hat Linux开始点，也称为基线配置。基线Linux内核有四个基本选项，是相互排斥的：

保存的.config文件 如果有前面保存的.config文件，则可以将其恢复到/usr/src/linux-x目录。

/boot/config-x文件 这个文件包含从RPM包安装时或安装Red Hat Linux时的内核配置。可以将其复制到/usr/src/linux-x/.config文件。

当前配置 用make oldconfig命令，在/usr/src/linux-x/.config文件中设置当前配置。

/usr/src/linux-x/configs中的相应文件 configs子目录中包括一系列配置文件，是针对不同CPU定制的。可以将与内核最接近的文件复制到/usr/src/linux-x/.config文件。

定制配置

我们已经介绍过三个定制内核配置的菜单：make config、make menuconfig和make xconfig。选择一个菜单，用前面介绍的方法和条件对内核进行必要的改变。一般来说，要进行如下的改变：

- 使用模块。保证其在可装入模块支持菜单中启用，也可以用一体化内核，但可能对于系统来说太大。
- 一定要在处理器类型与特性菜单中指定正确CPU。
- 删除不必要的设备与模块。这样可以减少内核与相关驱动程序的文件长度。例如，如果不准备将Linux计算机与电台相联，则不必安装与“业余爱好者电台支持”相关的模块。
- 如果不能肯定，就不要删除。假设从基线或标准内核配置开始，则许多设置是相互依赖的。删除错误的设备之后，可能使内核无法使用。

说明：过去的内核需要对称多重处理（SMP）支持，即使计算机只有一个CPU。但Red Hat Linux 9所带的内核不再要求这样。

进行改变之后，保存配置。默认情况下，make工具可以将设置保存到/usr/src/linux-x目录中的.config文件。

生成依赖性

现在可以强制源代码读取Linux内核配置。下列命令可以解决所有依赖性。它取得新的.config文件中的设置，并用其定制源代码：

```
# make dep
```

说明：make dep过程在我的660MHz计算机上花了五分钟，你的CPU速度与内核长度可能有所不同，因此所要时间也不同。

建立内核映像

满足依赖性之后，就可以建立内核映像。这个过程可能要几分钟，也可能要整个晚上，取决于CPU速度。可以压缩映像，以便放进引导盘或救援盘中。要生成压缩内核映像，运行下列命令：

```
# make bzImage
```

可以看到长长的一系列消息。这个命令完成之后，注意下列消息：

```
warning: kernel is too big for standalone boot from floppy
```

如果看到这个消息，则可能无法用第11章的mkbootdisk命令生成引导盘。如果要想减小内核，则可能要再次启动make xconfig过程，删除更多设置。

说明：make bzImage过程在我的660MHz计算机上花了十五分钟，你的CPU速度与内核长度可能不同，因此所要时间也不同。

你不需要定制引导盘。许多情况下，可以在救援方式中用Red Hat Linux安装引导盘启动系统。关于linux rescue过程的更多信息，见第11章。

提示：linux rescue方式中的Red Hat Linux安装引导盘不一定能挽救所有系统，可能要对新内核定制引导盘。

记录上一消息中指出的目录，稍后将需要这个信息。目前，先假设重新编译内核版本2.4.20-8：

```
/usr/src/linux-2.4.20-8/arch/i386/boot
```

说明：如果你的PC机不用Intel 32位CPU，则目录中的i386可能有所不同。

编译之后

现在可以将内核移到/boot目录并更新引导装入器。前面曾介绍过，新内核在/usr/src/linux-2.4.20-8/arch/i386/boot目录中。将其复制到/boot目录，命名为vmlinuz-2.4.20sugaree。

还要建立初始内存盘。根据指定的内核版本和EXTRAVERSION值，可以使用下列命令：

```
# mkinitrd /boot/initrd-2.4.20sugaree.img 2.4.20sugaree
```

建立模块

这时我们假设已经在内核中配置了模块支持。下一步要建立模块。第一个命令组织各个/usr/src/linux-x子目录中已经配置的模块：

```
# make modules
```

说明：make modules过程在我的660MHz计算机上花了四十五分钟，你的CPU速度与内核长度可能不同，因此所要时间也不同。

下一个命令在/lib/modules/2.4.20-4目录中组织模块：

```
# make modules_install
```

说明：make modules_install过程在我的660MHz计算机上花了三十分钟。

提示：如果遇到错误消息“when making multiple links, last argument must be a directory”，则应检查/usr/src/linux-x/Makefile中的EXTRAVERSION变量。也许是该行末尾多了一个空格。

下面就可以根据三个配置菜单之一，准备定制内核的细节了。

设置配置菜单

如果要按任何方式定制内核，就要有个配置菜单。文本、终端图形、GUI格式提供不同菜单。每个菜单要求一系列包：内核的源代码和语言库、图形配置屏幕的语言库。

内核RPM包

表12.3列出了几个与内核建立有关的RPM包，其中有些提供源代码，有些与内核配置和处理所要的语言和库有关。按第10章介绍的方法用rpm命令安装这些包。

表12.3 内核RPM包

包	描述
binutils-*	必要的二进制实用程序
cc-*	GNU C 语言编译器
gcc-*	C语言编译器
glibc-devel-*	用于开发需要C语言库的程序（如内核）
glibc-kernheaders-*	内核C语言头文件
kernel-source-*	内核源文件
ncurses-*	终端上表示图形的语言库，用于make menuconfig
ncurses-devel-*	ncurses屏幕的头文件
tcl-*	TCL脚本语言，用于TK，make xconfig需要
tk-*	TCL使用的GUI文件，make xconfig需要

提示：如果遇到与kernel-headers相关的Failed dependencies错误消息，则要安装kernheaders-* RPM包。许多依赖性显式表明需要的RPM包，而与kernel-headers相关的依赖性则不然。

如果重新配置现有内核，则不需要安装kernel-x.cputype.rpm包，本章后面进行编译时，实际上要从其他一些包生成新内核。

如果愿意在文本方式中定制内核，则不需要ncurses*或tcl-*或tk-* RPM包。但内核中包含大量可以定制的设置，使图形化内核配置屏幕特别方便。下节将介绍这个特性。

建立菜单

安装正确的RPM包之后，要检查三个不同内核配置菜单中的选项。首先移到Linux内核源文件所在目录/usr/src/linux-versionnumber。为了方便起见，本章余下部分称其为/usr/src/linux-x目录。

提示：默认情况下，Red Hat Linux将/usr/src/linux-2.4目录链接到原内核的默认源代码目录。

/usr/src/linux-x目录中有个Makefile文件，可以配置内核。这个文件包含三个不同的内核配置工具：

- make config
- make menuconfig
- make xconfig

下面几节简要介绍这些工具，然后用make xconfig工具分析内核配置的细节。

先要转入计算机上的/usr/src/linux-x目录。如果不在这个目录中，则无法使用所列的make命令。

为什么要菜单

可以直接编辑配置文件。前面曾介绍过，第一个内核配置建档在/boot目录中的config-x文件中。这个文件包括所有设置，例如：

```
CONFIG_MODULES=y
CONFIG_3C359=m
# CONFIG_IRDA_DEBUG is not set
```

换句话说，CONFIG_MODULES设置集成到内核中，使内核可以使用模块化驱动程序。CONFIG_3C359=m命令将这个特定网卡驱动程序变成一个模块。红帽子软件探测到这个网卡时，可以用insmod命令（见第11章介绍）使用这个驱动程序。CONFIG_IRDA_DEBUG之类的未用元素保留在源代码库中之外，然而却是（#）的无完成说明语句，应该将该行忽略。

完成之后，要将文件保存到/usr/src/linux-x目录的.config中。然后就可以按本章稍后介绍的方法编译和安装内核。

提示：如果前面已经重新编译内核，则通常把设置保存在/usr/src/linux-x/.config文件中。前面的一个修改保存在/usr/src/linux-x/.config.old中。然后，这时最好把.config文件备份到另一个目录。

但由于这个文件有两千多行，分析每一行是个非常费时的过程，因此，可以用三个内核工具提供帮助。

make config

在/usr/src/linux-x目录中，make config命令启动内核配置工具，提示一系列问题，如图12.5所示。

```
[root@RH9Desk linux-2.4]# make config
rm -f include/asm
( cd include ; ln -sf asm-i386 asm)
/bin/sh scripts/Configure arch/i386/config.in
#
# Using defaults found in configs/kernel-2.4.20-1686.config
#
*
* Code maturity level options
*
Prompt for development and/or incomplete code/drivers (CONFIG_EXPERIMENTAL) [Y/n/?]
/Y
*
* Loadable module support
*
Enable loadable module support (CONFIG_MODULES) [Y/n/?]
Set version information on all module symbols (CONFIG_MODVERSIONS) [Y/n/?]
Kernel module loader (CONFIG_KMOD) [Y/n/?]
Y
*
* Processor type and features
*
Low latency scheduling (CONFIG_LOLAT) [Y/n/?]
Processor family (386, 486, 586/K5/5x86/6x86/6x86MX, Pentium-Classic, Pentium-MM
X, Pentium-Pro/Celeron/Pentium-II, Pentium-III/Celeron(Coppermine), Pentium-4, X
6/K6-II/K6-III, Athlon/Duron/K7, Elan, Crusoe, Winchip-C6, Winchip-2, Winchip-2A
/Winchip-3, CyrixIII/VIA-C3/VIA-C5) [Pentium-Pro/Celeron/Pentium-II] ]
```

图12.5 make config过程

它首先在/usr/src/linux-x目录中寻找.config文件。如果这个文件不存在, 则用uname -p标识CPU, 在/usr/src/linux-x/configs目录中寻找相应文件。所选文件中的设置成为默认值。

如果首次修改内核, 则可以使用/boot/config-x中已经安装的配置, 其中x表示内核版本号。用下列命令将其复制到/usr/src/linux-x/.config文件中:

```
# cp /boot/config-x /usr/src/linux-x/.config
```

然后会出现一系列问题。对每个问题, 最多有四个选项。Y和N很简单, 通常可以选择M, 在一个文件中提供相关驱动程序模块。如果输入问号, 则打开与该问题相关的帮助文件。

需要回答的问题有几百个, 如果只要改变第366个问题的设置, 则很容易错过, 而一旦错过, 就无法再回头, 只好按Ctrl+C键退出, 然后重新开始。为此, 另外两个make菜单更常用。

make menuconfig

进入/usr/src/linux-x目录之后, make menuconfig命令可以打开一个低分辨率图形菜单。只要按前面介绍的方法安装了ncurses* RPM包, 就可以看到图12.6所示的make menuconfig主菜单。

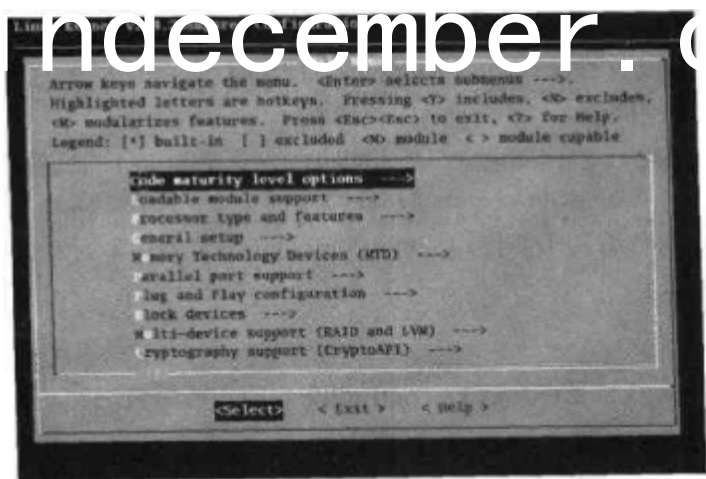


图12.6 make menuconfig主菜单

和make config一样, 这个选项也寻找/usr/src/linux-x目录中的.config文件。如果找不到, 则使用/usr/src/linux-x/configs目录中对CPU定制的*.config文件。

可以看出, 内核设置组织成菜单。可以加亮显示一个设置, 然后随时选择Help。但是, 并不是每个变量都有帮助信息。

加亮菜单选项并按Enter键, 可以检查详细配置选项。例如, 图12.7显示了一些无线局域网设备。可以看出, 有些提供模块, 有些内置在内核中。

说明: 可以从远程计算机上通过Telnet或SSH连接, 运行make menuconfig命令。这样既方便也危险。

关于Telnet或SSH的更多信息, 见第23章。

可以看出, make menuconfig命令还提供许多其他菜单。下节将详细介绍这些选项, 因为make xconfig菜单更容易在书中阅读。

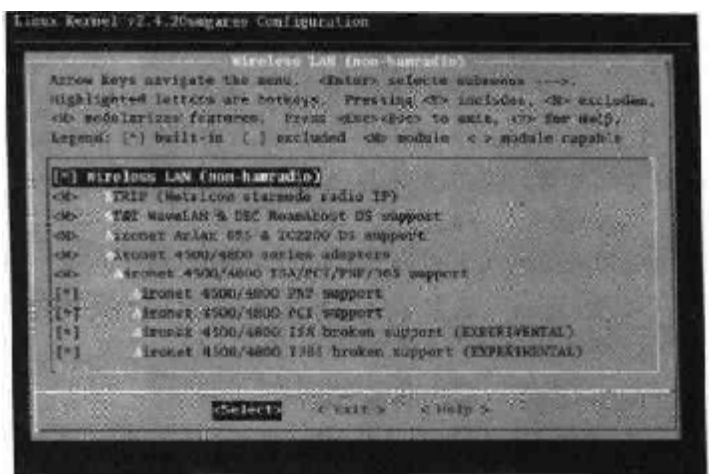


图12.7 无线局域网内核菜单

退出make menuconfig时，可以保存新配置。如果回答Yes，则这个工具将新的内核配置写入/usr/src/linux-x/config文件中。

make xconfig

在GUI界面和/usr/src/linux-x目录中，make xconfig命令可以提供高分辨率图形菜单。只要安装了tcl-*与tk-* RPM包，就可以看到图12.8所示的菜单。

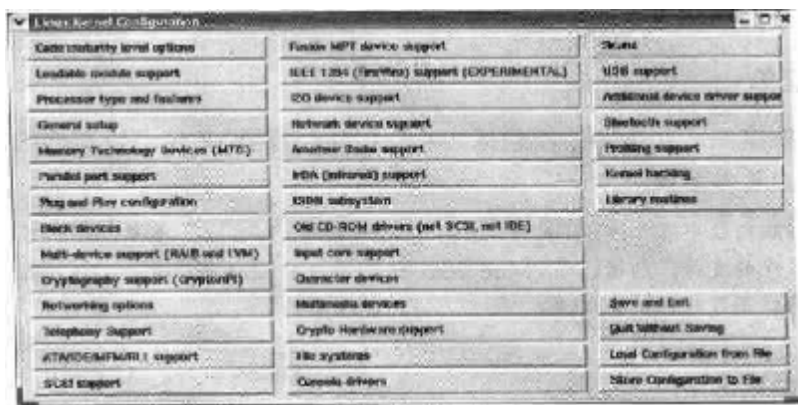


图12.8 Linux内核配置菜单

和make config一样，这个选项也寻找/usr/src/linux-x目录中的.config文件。如果找不到，则使用/usr/src/linux-x/configs目录中对CPU定制的*.config文件。如果要从不同的配置文件开始，则可以利用右下角的两个按钮。

可以看出，不同内核设置组织成不同部分。我们将在本章稍后详细介绍这些部分。对改变感到满意之后，可以单击Save And Exit选项，否则单击Quit Without Saving选项。

内核的不同部分

下面根据make xconfig Linux内核配置菜单的输出详细介绍内核的不同部分。这一节相当长，如果你准备全部阅读，不妨先休息一会儿。

这里共介绍35个内核菜单，分成六大部分：

- 基本配置菜单配置内核的基本部分，如CPU、ISA或PCI支持。一定要注意这些菜单，这里的错误可能使Linux无法识别外部设备，甚至无法识别CPU。
- 存储设备菜单处理各种存储设备相关的连接：硬盘、光碟、并行端口驱动器，等等。小心，要保证Linux能够识别你的硬盘。
- 网络菜单可以配置基本网络软件与网络硬件。
- 外部硬件包括与计算机机箱之外的硬件相关的菜单。
- 其他硬件支持与不属于任何类型的硬件相关。
- 其他软件支持包括文件系统、库之类的关键组件。

如果要在你的Linux计算机上进行操作，则要转入/usr/src/linux-x目录中，并运行make xconfig命令。进入每一段时，单击Linux内核配置菜单的相应按钮。

检查硬件内核设置时，应特别严格。如果不用相关硬件，则应关掉这个设置。如果今后可能增加这类硬件，则可以建立一个模块。这些动作可以减少内核长度，大大提高系统启动速度与性能。

警告：如果对一个活动内核或模块化内核设置不了解，不要将它关闭。有些看起来关系不大的内核参数对Linux的基本操作至关重要。

基本配置菜单

本节随意组织了几个菜单，包括与启动Linux、识别硬件、设置CPU、在内核中使用试验组件相关的基本参数。

说明：旧版内核中有个“Binary Emulation of Other Systems”菜单，用户可以配置仿真其他UNIX系统的支持，包括UNIXWare 7.x、SCO Open Server和Solaris 2.x。Red Hat Linux 9所带的内核不再提供这个选项。

代码成熟度级别选项

如果在生产环境中使用Red Hat Linux，则一定要将图12.9所示的设置设为n，否则可能不小心加进试验性内核驱动程序和设置。

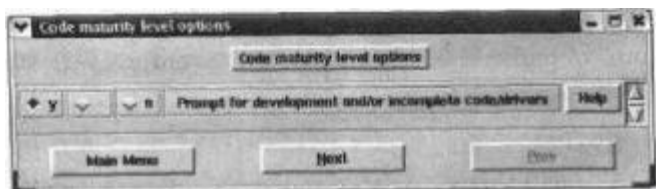


图12.9 代码成熟度级别选项

如果你是开发人员，则要小心。最好一次只试用一个试验性内核驱动程序，遇到问题时才知道原因在哪里。可以单击相关Help按钮得到每个变量的更多信息。这个菜单的配置帮助对话框如图12.10所示。

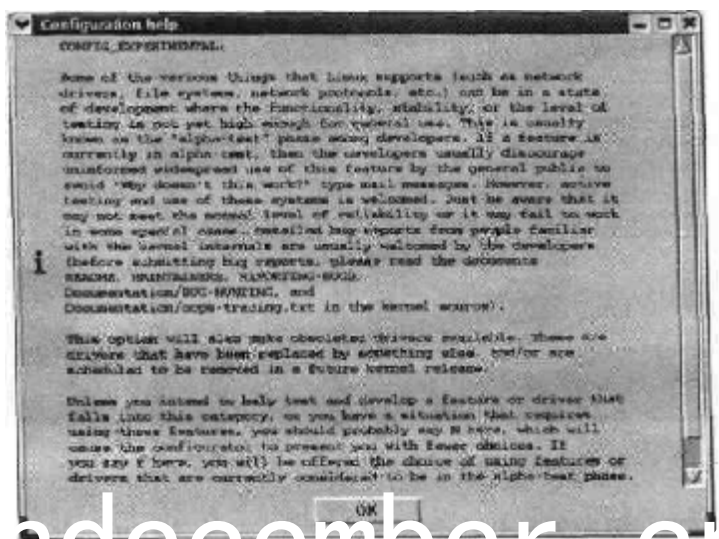


图12.10 配置帮助

可装入模块支持

通常，Linux发现系统上的新硬件时，会自动安装驱动程序模块（如果有）。这可以用图12.11所示的“可装入模块支持”选项启动。

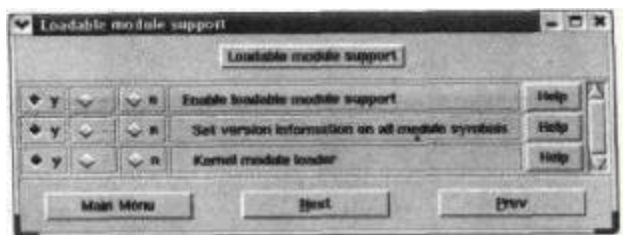


图12.11 可装入模块支持

所有这些选项基本上都应回答Yes，以便将硬件驱动程序模块与内核分开，使用不同来源的驱动程序和在需要时装入模块。

否则要在主内核中包括所有驱动程序，从而使内核太大。有些内核没有模块，称为一体化内核，结果非常大，旧式PC机中要引导Linux时根本无法装入。

处理器类型与特性

可以针对CPU定制Linux内核，相当于计算机上可以直接安装的不同种类kernel-x.cputype.rpm包。从图12.12可以看出，可以对各种CPU定制Linux内核。

如果表中没有你的CPU，则可以寻找最接近的匹配。如果你用Intel 32位CPU，则可以试试386，其基本内核适用于所有当前Intel 32位CPU。

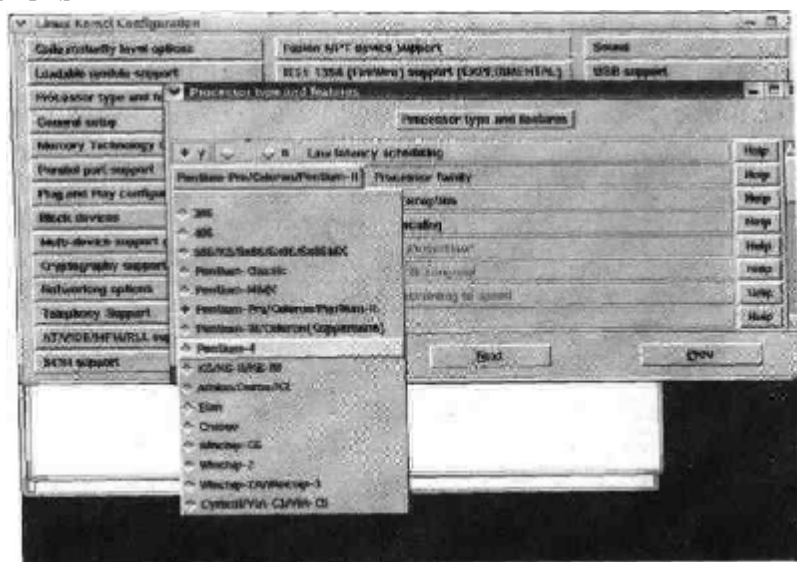


图12.12 处理器类型与特性

选择处理器之后，要配置另外几个变量，包括支持多个CPU的特殊模块，以及东芝或戴尔笔记本电脑的特殊特性。

一般设置

一般设置内核菜单如图12.13，提供内核的几个基本硬件、二进制与网络选项。请看看变量表，它们可以分成几类，有些是计算机上硬件类型的基本变量。这些类别包括：

网络支持 有些程序要求内核网络支持，即使你的计算机从不连接互联网或另一个网络。

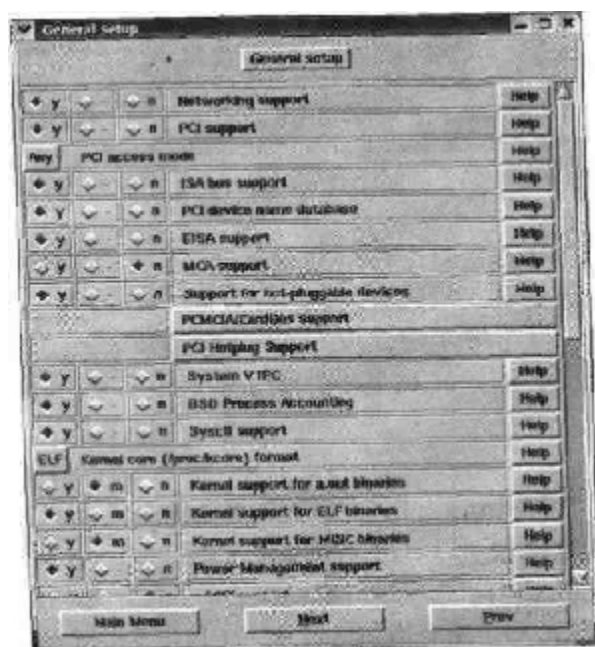


图12.13 一般设置

基本硬件支持 通常, Linux内核配置成支持PCI、ISA与PCMCIA卡。

热插拔支持 Linux可以配置成支持热插拔硬件,即可以在计算机运行时安装或拆除。

电源管理支持 Linux支持旧的APM(高级电源管理)系统,ACPI(高级配置电源接口)支持还处于试验阶段,即还不能用于生产计算机中。

说明: 在一般设置菜单中,单击PCMCIA/CardBus Support按钮,可以看到图12.14所示的子菜单。如果在笔记本电脑上使用Linux,则一定要激活相应的网桥。

存储设备

几个Linux内核菜单用于组织与文件和其他信息存储相关的设置。如果使用外部存储设备,见后面的“外部硬件”一节介绍的菜单。

内存技术设备

在Linux内核中,内存技术设备(MTD)包括可以在“固体状态”中存储信息的一切,如BIOS、数码相机闪存卡、只读芯片。记住,其中有些可以通过PCMCIA适配器安装。图12.15显示了基本菜单。

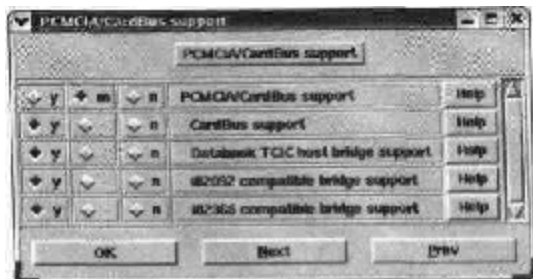


图12.14 PCMCIA/CardBus Support子菜单

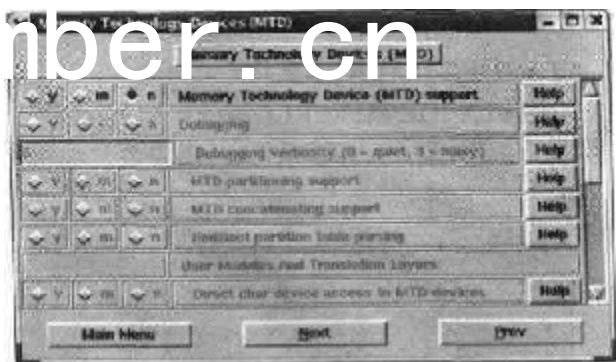


图12.15 内存技术设备

块设备

块设备可以在一个目录中装载存储单元,如软盘与硬盘。打开块设备菜单,可以看到图12.16所示的内容。向下滚动菜单,可以看到其支持软盘、普通IDE硬盘、共享网络盘和内存盘。

这些设置与ATA/IDE/MFM/RLL Support菜单中的设置密切相关。

多设备支持

第3章曾介绍过,Red Hat Linux支持RAID与LVM。这两个系统都需要多个分区。由于Linux对每个分区指定设备,因此把RAID与LVM看成多设备系统。如果要使用RAID与LVM,则要激活这些设置,如图12.17。

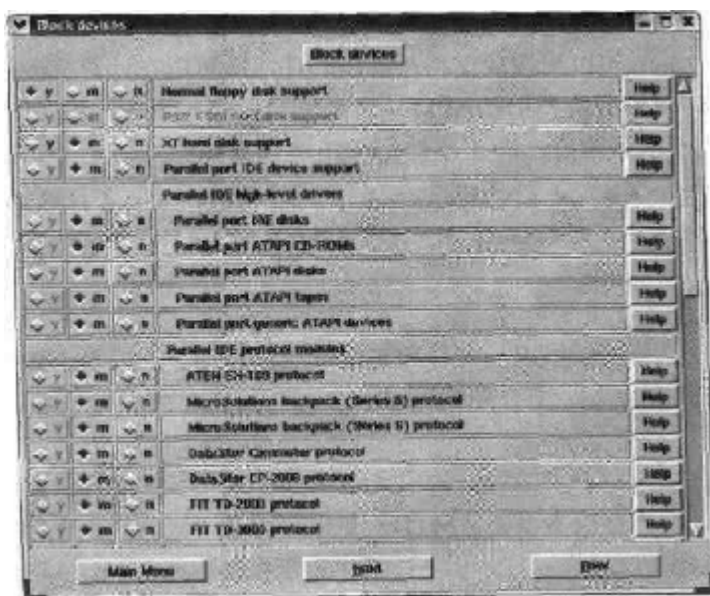


图12.16 块设备菜单

ATA/IDE/MFM/RLL支持

ATA/IDE/MFM/RLL是一串缩写，都与标准PC硬盘与光碟接口有关。如图12.18所示，可以使用IDE、ATA与ATAPI块设备按钮来调用一个子菜单，带有不同驱动器与芯片集的变量。

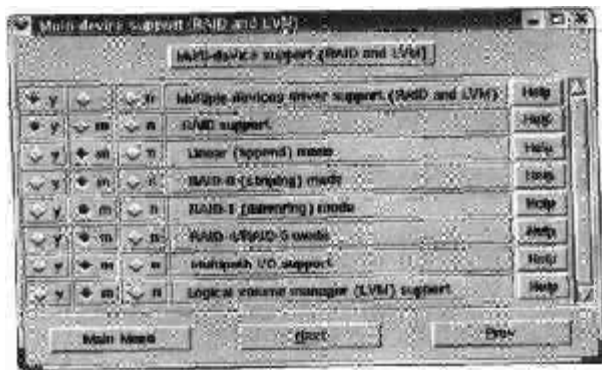


图12.17 多设备支持

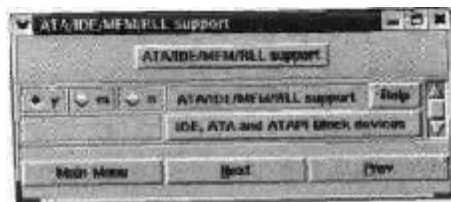


图12.18 ATA/IDE/MFM/RLL支持

SCSI支持

另一类存储设备的主要接口是SCSI（小型计算机系统接口）。SCSI支持内核菜单可以激活基本SCSI硬盘、磁带机和光碟系统的驱动程序与模块。在图12.19所示的SCSI支持内核菜单底部，可以看到两个子菜单：

- SCSI Low-Level Drivers菜单支持几个特定SCSI硬盘与RAID设备。
- PCMCIA SCSI Adapter Support菜单支持将计算机连接到SCSI设备的PCMCIA卡。

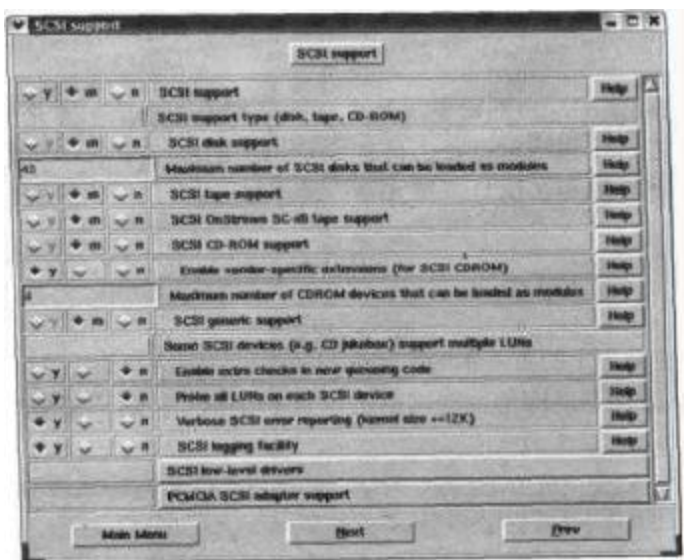


图12.19 SCSI支持内核菜单

旧式光驱驱动程序

旧式光碟驱动程序连接声卡。旧式光碟驱动程序（非SCSI，非IDE）菜单可以访问曾经用于这些光碟的Linux驱动程序。图12.20列出了几个可用的驱动程序。

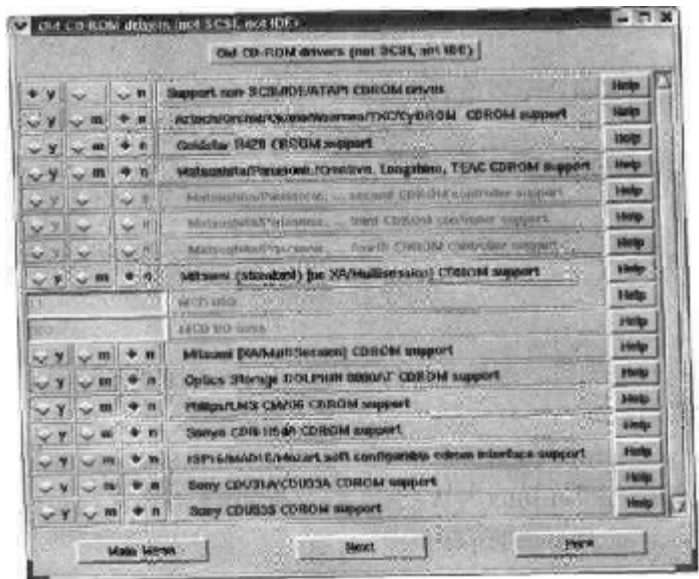


图12.20 旧式光碟驱动程序（非SCSI，非IDE）菜单

可以看出，旧式光碟驱动程序按版本和机型进行组织。如果你的旧式光碟驱动程序不在这个表中，则可以检查相应文档，试用具有类似版本和机型的驱动程序。记住，这些驱动程序已经不再支持，可能不太适用于最新Linux生产内核。

网络

Linux是为网络而建的，自然提供了几个与网络相关的内核配置菜单。可以通过几个网络菜单配置基本网络软件和特定设备。这些菜单不一定都与网络有严格关系。

关于基本网络协议的更多信息见第20章，关于Linux内核网络设置的其他重要章节还有第21章和第22章。

网络选项

网络选项菜单主要用于配置基本网络软件。尽管可以激活其他协议堆栈（如IPX/SPX），但许多选项都与Linux和互联网的主要网络协议TCP/IP相关。这个菜单很大，图12.21显示了其中一部分。



图12.21 网络选项

其中许多设置并不明显。例如，图12.21所示的IP: DHCP Support选项只用于远程Linux终端。记住，帮助菜单提供了每个选项的更多信息。几个子菜单如下：

- **IP: Netfilter Configuration**子菜单使内核可以用iptables、ipchains或ipfwadm支持防火墙。ipchains命令与Linux内核2.2相关，ipfwadm命令已经过时，与Linux内核2.0相关。第22章详细介绍当前iptables防火墙。
- **IPv6: Netfilter Configuration**子菜单可以在用这个更高级的IP地址系统时配置防火墙，见第20章。记住，IPv4目录仍然广泛使用。
- **Appletalk Devices**菜单可以通过TCP/IP网络与Apple计算机通信。
- **QoS And/Or Fair Queuing**菜单支持网络，可以用“Quality of Service”参数将消息排出优先级。
- **Network Testing**菜单可以发送预配置数据分组，检查系统容量。

网络设备

网络设备支持内核菜单可以对不同类型的网络适配器激活多个驱动程序。这也是个重要菜单，如图12.22。

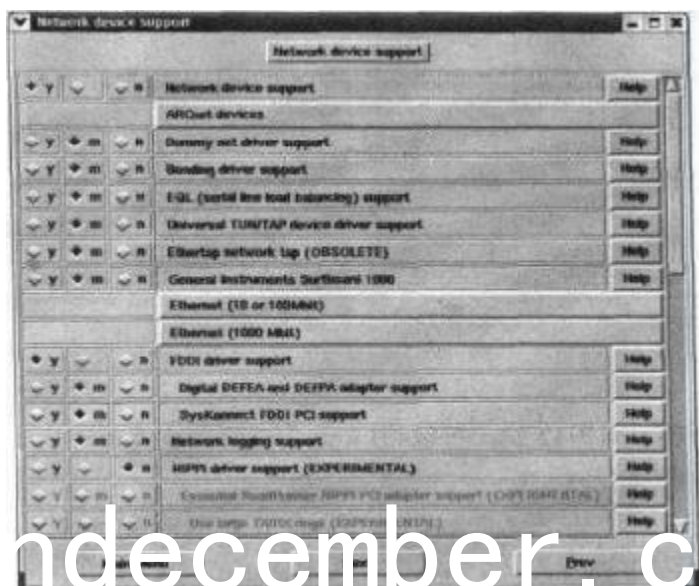


图12.22 网络设备支持内核菜单

这个菜单中包括基本网络驱动程序表，有几个网络特定驱动程序子菜单。可以看出，几种不同网络系统都建立了网卡，如以太网。这些子菜单包括：

- **ARCnet Devices** 可以使用对特定类型局域网建立的网卡。ARCnet是令牌环的变形，网络速度很慢（2.5Mb/s），因此目前已经基本不用。
- **Ethernet (10 Or 100Mbit)** 可以配置普通和快速以太网适配器。如果这个表中看不到你的适配器，则可以检查文档中的“克隆”。例如，许多旧式网卡使用Novell NE2000驱动程序。
- **Ethernet (1000Mbit)** 可以在Linux计算机上配置Gigabit Ethernet网卡。
- **Wireless LAN (Non-Hamradio)** 可以在PC机上配置基本无线网络，主要用于符合IEEE 802.11b标准的设备。蓝牙技术在另一菜单中支持。到本书编写时，还不支持IEEE 802.11a设备。
- **Token Ring Devices** 子菜单可以配置为这个旧式网络系统设计的特定网卡。尽管令牌环网络不太常用，但有人认为令牌环网络比以太网更可靠，因此在工厂之类的地方仍然可能看到令牌环网络。
- **Wan Interfaces** 可以配置广域网中连接两个远程局域网的网络设备。
- **PCMCIA Network Device Support** 可以让网卡支持这个标准，主要用于便携电脑。
- **ATM Drivers** 子菜单支持为ATM（异步传输方式）网络建立的网卡。ATM是快速以太网和Gigabit Ethernet的常见替换。

提示：如果对内核配置符合PCMCIA或PC Card标准的网卡，请检查PCMCIA网络设备支持菜单。

电话局支持

现代的电话公司将普通电话转换成数据，放到互联网之类的网络中发送。这个过程称为电话局。Linux支持几个电话局卡，主要用于帮助大企业将普通电话转换成数据。电话局支持菜单如图12.23。



图12.23 电话局支持

业余无线电台

业余无线电台菜单如图12.24，可以将Linux内核配置成支持连接业余无线电台。



图12.24 业余无线电台

计算机可以用AX.25协议通过业余无线电台联网。还有一个AX.25网络设备驱动程序子菜单，可以配置这种网络连接。

ISDN

早期电话网络通过ISDN（综合服务数字网）适配器连接数字计算机。这些连接在欧洲仍然很普及，通常是美国农村地区惟一的“高速”（128Kb/s）连接选项。图12.25所示的基本ISDN子系统菜单可以对ISDN配置几种网络和命令。

Linux内核ISDN子系统菜单包括几个子菜单：

- ISDN Feature Submodules子菜单可以配置虚拟ISDN卡，一些命令在欧洲连接中有用。
- Passive ISDN Cards子菜单可以配置消费者常用的适配器，与128Kb/s速度相关联。
- Active ISDN Cards子菜单可以配置高速ISDN适配器。

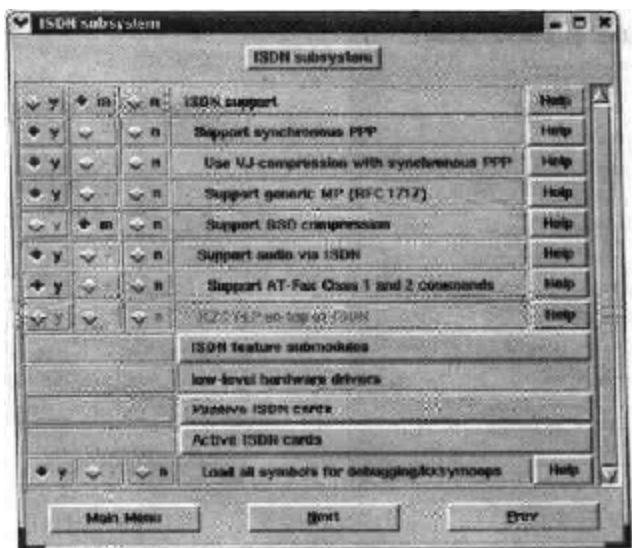


图12.25 ISDN子系统菜单

Fusion MPT

Fusion MPT设备支持是等待菜单中，用于LJ逻辑公司的高速SCSI设备，也有相关的局域网驱动程序，如图12.26。

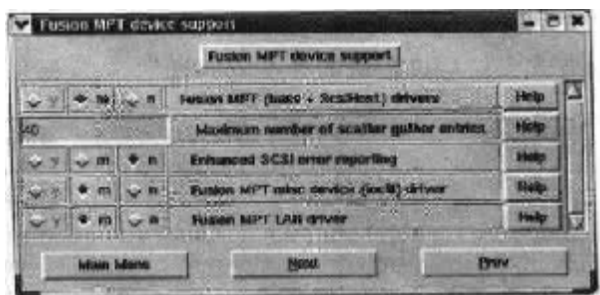


图12.26 Fusion MPT设备支持

红外支持

可以将Linux内核配置成支持符合红外数据协会（IrDA）标准的红外设备。从图12.27的菜单可以看出，有几个传输数据的红外协议。红外端口设备驱动程序子菜单可以在Linux内核或模块中包括相应硬件。

蓝牙技术支持

蓝牙技术规范基于网络的无线电技术，通常是33英尺（10米）左右的短距离传输，常用于手提电脑和手机之类的移动设备。有几个移动设备是用Linux建立的。蓝牙技术还可以连接网络中的普通计算机。图12.28显示了内核蓝牙技术支持菜单。

蓝牙设备驱动程序子菜单可以使用基本HCI（主机控制器接口）。不同驱动程序可以支持不同厂家的USB、串口和PCMCIA卡。

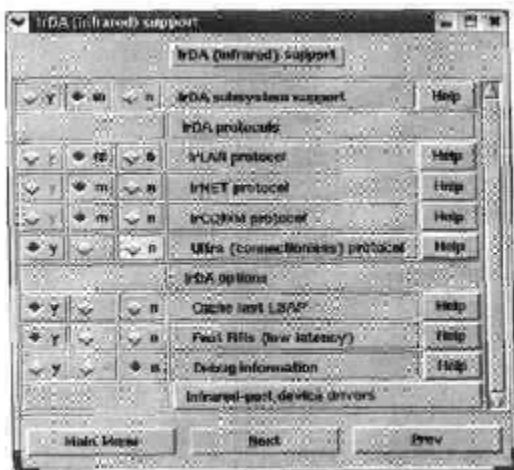


图12.27 红外支持

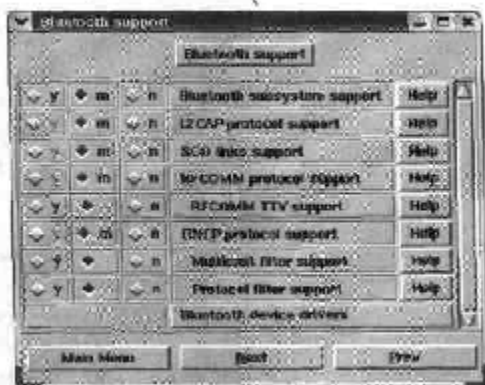


图12.28 内核蓝牙技术支持菜单

外部硬件

外部硬件有三个Linux内核菜单，其中两个与较新的USB和IEEE 1394标准有关，另一个针对较老的外部硬件：并口支持。

并口支持

并口通常称为打印机端口。从图12.29可以看出，可以按几种不同方法配置并口支持。例如，IEEE 1284传输方式支持与打印机的标准双向通信。

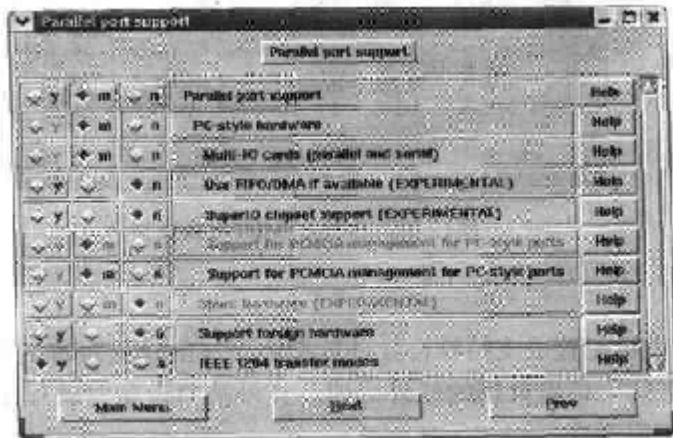


图12.29 并口支持

记住，并口不一定只有打印机。例如，有些硬盘和其他存储设备也可以连接并口。并口也是计算机同步和传输数据的一种方式。更多信息见“块设备菜单”部分。

USB支持

看起来所有未来的外部设备都会符合某种USB和IEEE 1394标准。这两个领域的新硬件都不断推出。Linux开发人员正在努力跟上这个形势。

Linux对USB的支持还非常不完善，USB 2.0标准设备的内核支持目前还处于试验性阶段。关于Linux与USB的更多信息见第2章和www.linux-usb.org站点。从图12.30的USB支持主菜单可以看出，各种主要USB硬件都有内核代码。

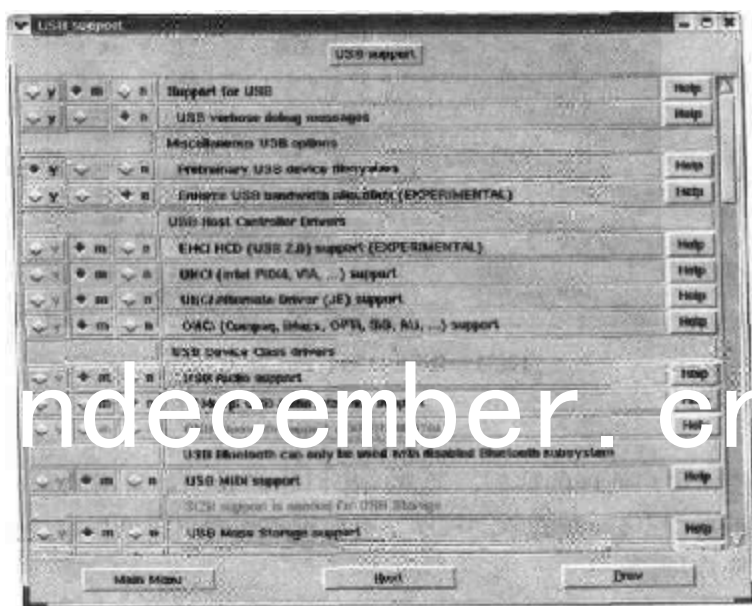


图12.30 USB支持

USB串行转换器支持子菜单可以配置串口适配器，可以将串行设备连接USB端口，如旧式鼠标。

IEEE 1394——FireWire/iLink

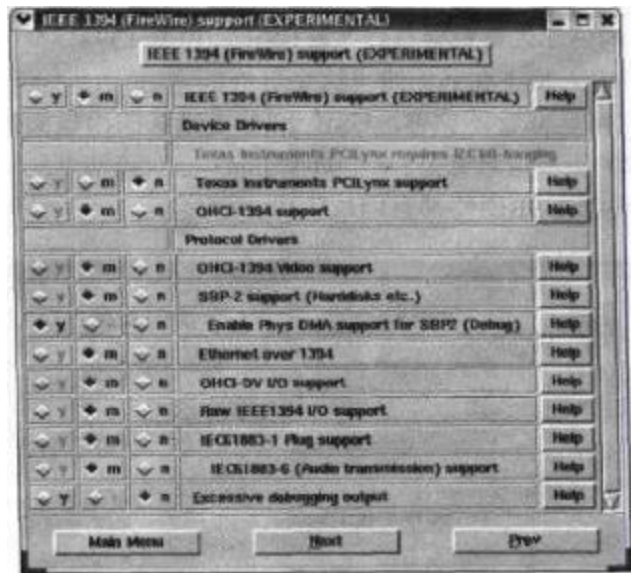
第2章曾介绍过，IEEE 1394硬件以其商标名FireWire与iLink著称于世。Linux对这些设备的支持还处于试验阶段。相关设备使用其高速（400Mb/s+）功能，如图12.31。

说明：如果在代码成熟度级别选项菜单中关闭开发驱动程序设置，则这个菜单不活动。

警告：处于试验阶段的代码不能在生产中使用。换句话说，其测试还不完全，相关内核组件不一定可行，可能影响系统其他部分，使用时风险自担。

其他硬件支持

有些硬件菜单很难归到某个类中，有些与本地和远程工作的终端、控制台相关，有些与即插即用、多媒体相关。



12.31 IEEE 1394 FireWire支持

字符设备

字符设备传输用户处理的数据，通常与串口相联系。最常用的字符设备是终端。可以对本地虚拟终端和远程终端配置驱动程序。有些远程终端可以使用串口和其他物理端口。图12.32显示了这些选项。

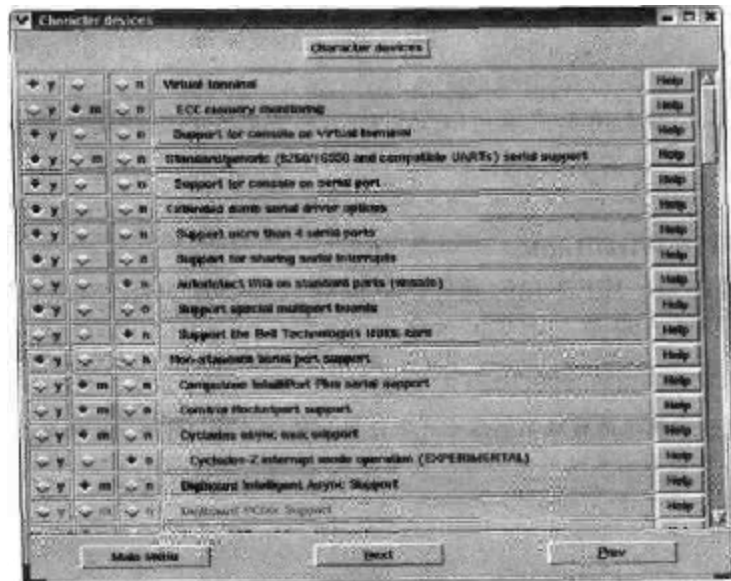


图12.32 字符设备

字符设备还包括一些奇怪的内核设置，如磁带机、图形卡、鼠标和游戏杆。几个子菜单包括：

- I2C Support是个串行总线协议，可以支持各种硬件，包括Linux视频内核设置。
- Hardware Sensors Support包括几个为显示器硬件设计的设备，基于Linux系统硬件显示项目的工作，其站点为www2.lm-sensors.nu/~lm78。
- Mice子菜单可以配置鼠标、触摸屏等基本指示设备支持。
- Joysticks和与PC机游戏端口相关的设备有关。
- Watchdog Cards常用于嵌入设备，在一定时间内设备输入时强制重新启动。
- Ftape与旧式磁带机有关，连接34引脚的软盘控制器，包括几个机型和版本的驱动程序。
- PCMCIA Character Devices子菜单可以仿真串口。

控制台驱动程序

控制台驱动程序很简单：可以支持图形屏幕中的控制台或文本方式终端。图12.33显示了控制台驱动程序菜单。

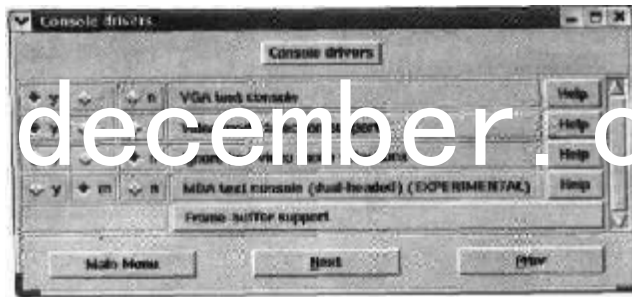


图12.33 控制台驱动程序

有一个帧缓冲支持子菜单，使应用程序可以通过缓冲区取得图形硬件，对Intel系统处于试验阶段，通常不需要。

输入内核支持

输入内核支持是与Linux人机接口设备（HID）交互所需要的。人机接口设备是个物理接口，将信号发送到计算机，包括键盘、鼠标和游戏杆。图12.34显示了输入内核支持菜单。

即插即用配置

内核中的Linux即插即用配置很简单。如图12.35所示，你可以激活基本即插即用配置，以及ISA即插即用设备所需的特殊命令。

I2O设备

I2O是智能输入/输出体系结构，使驱动程序可以分成硬件与操作系统模块。I2O常用于嵌入设备，大多数用户在Linux内核中不用或不需要I2O设备。图12.36显示了I2O设备支持菜单。

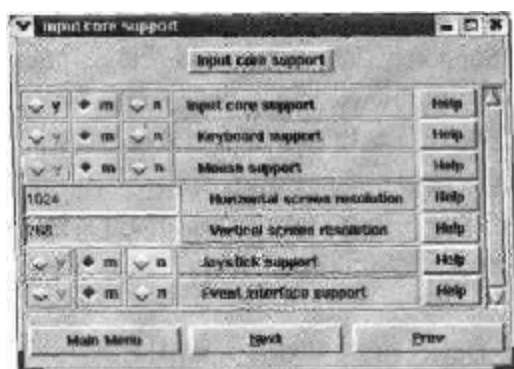


图12.34 输入内核支持



图12.35 即插即用配置

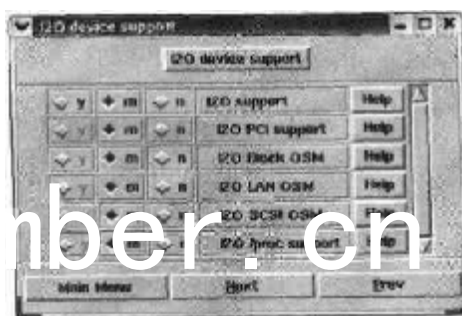


图12.36 I2O设备支持菜单

声音

Linux支持丰富的声卡。尽管Linux不支持每个声卡，但有些声卡可以使用相应的替换配置，如声霸卡。如果这个菜单中没有你的声卡的驱动程序，如图12.37，则可以检查文档，或与声卡厂家联系。

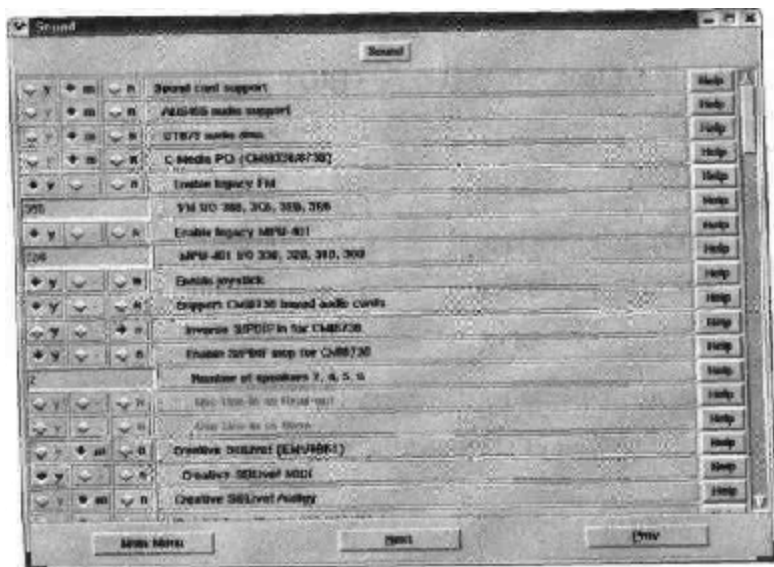


图12.37 声音

多媒体

与声音密切相关的是多媒体。多媒体设备菜单可能与你想像的不太相同，有一个Linux视频子菜单，要求字符设备菜单中具有I2C串行支持，还有一个电台适配器子菜单，包括计算机上可以安装的一系列普通电台。图12.38显示了多媒体设备菜单。

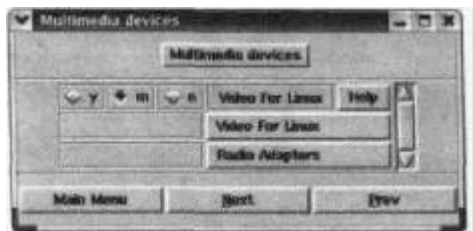


图12.38 多媒体设备菜单

加密

Linux内核还有软件与硬件加密菜单。加密硬件支持菜单如图12.39，可以支持Broadcom 5820芯片集，支持安全Web服务器。不要把它与图12.40的加密支持菜单混淆。

其他软件支持

其余内核菜单是很难分类的软件菜单，包括加密、文件系统、负荷配置、内核调试和库的基本接口。

加密

加密支持选项可以对Linux使用强加密，超过上面介绍的加密硬件支持菜单范围，不再局限于一个芯片集。加密支持（CryptoAPI）菜单如图12.40。



图12.39 加密硬件支持菜单

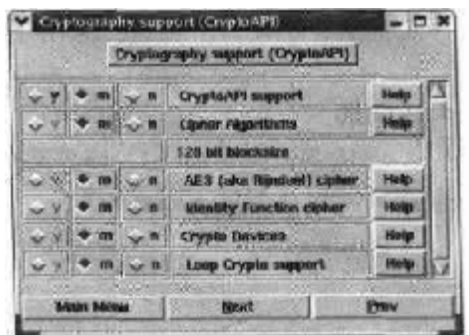


图12.40 加密支持（CryptoAPI）菜单

文件系统

Linux文件系统菜单可以配置Linux能读取的格式类型，以及每个分区上的配额。Linux支持多个文件系统格式，包括第7章介绍的许多格式。图12.41显示了文件系统菜单。

注意，Linux对几个文件系统的支持还是试验性的，包括将文件写入Microsoft NTFS文件系统的模块，标为“危险”。

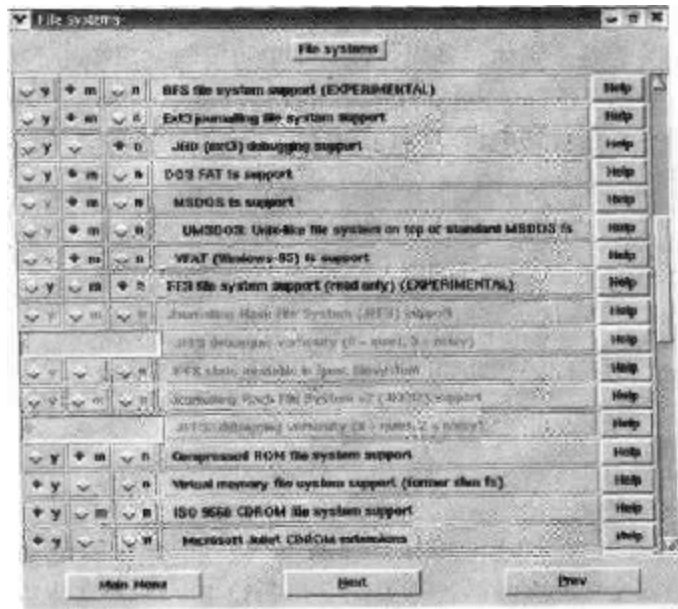


图12.41 文件系统

说明：文件系统一词可以称为file systems或filesystems。

警告：我不激活NTFS写入支持模块，相关帮助文件建议先备份NTFS卷，因为它可能被损坏。

负荷配置

最新Linux内核可以支持系统性能配置，基于OProfile系统，见<http://oprofile.sourceforge.net/about.php3>站点介绍，目前还是个内部试验软件。如果代码成熟度级别选项菜单中关掉了开发驱动程序设置，则这个菜单不活动。图12.42显示了配置支持菜单。

内核调试

内核调试菜单如图12.43，支持的驱动程序可以帮助调试驱动程序和其他内核问题。这个菜单通常是开发人员使用的。



图12.42 配置支持菜单

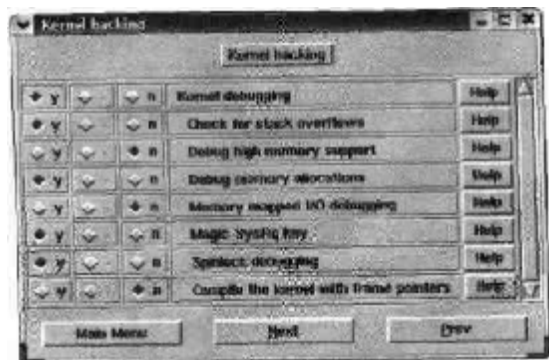


图12.43 内核调试

库程序

库程序菜单如图12.44，包括数据流的zlib压缩与解压缩支持。

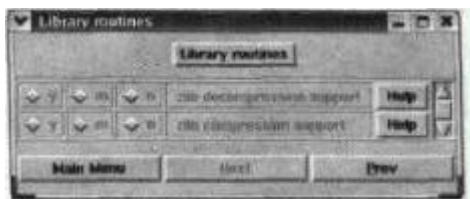


图12.44 库程序

引导装入器更新

GRUB是Red Hat Linux的默认引导装入器，但LILO仍然相当常用。重新编译内核时，要将引导装入器设置成从某个内核引导，就像它们是两个不同操作系统一样。尽管引导装入器更新不属于“建立”过程，但更新这些引导装入器的步骤非常简单。

更新GRUB

使用引导装入器CRUE，则可以在某个文本编辑器中打开`/etc/grub.conf`文件。如果Red Hat Linux是计算机上的唯一操作系统，则关键命令如下：

```
default=0
title Red Hat Linux (2.4.20-8)
    root (hd0,1)
    kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
    initrd /initrd-2.4.20-8.img
```

现在取得刚刚重新编译的内核。主要压缩内核文件为`vmlinuz-2.4.20-sugaree`，相应的初始内存文件为`initrd-2.4.20sugaree.img`。由于我们把这些文件安装在同一个`/boot`目录中，因此不改变任何其他参数。可以在第二段中加上新编译的内核：

```
default=0
title Red Hat Linux (2.4.20-8)
    root (hd0,1)
    kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
    initrd /initrd-2.4.20-8.img
title Red Hat Linux (2.4.20sugaree)
    root (hd0,1)
    kernel /vmlinuz-2.4.20sugaree ro root=LABEL=/
    initrd /initrd-2.4.20sugaree.img
```

记住，不用改变别的内容了。重新启动计算机时，可以在GRUB菜单中看到两个标题，如图12.45。由于`default=0`，因此第一段的旧内核仍然是默认内核。图12.2曾描述了类似的`grub.conf`版本，GRUB的详细分析见第11章。



图12.45 修改后的GRUB

更新LILO

假设引导加载器是LILO，则可以在文本编辑器中打开/etc/lilo.conf文件。如果Red Hat Linux是计算机上的唯一操作系统，则关键命令如下：

```
default=linux
image=/boot/vmlinuz-2.4.20-8
label=linux
initrd=/boot/initrd-2.4.20-8.img
read-only
append="root=LABEL=/"
```

现在取得刚刚重新编译的内核。主要压缩内核文件为vmlinuz-2.4.20sugaree，相应的初始内存文件为initrd-2.4.20sugaree.img。由于我们把这些文件安装在同一个/boot目录中，因此不改变任何其他参数。可以在第二段中加上新编译的内核：

```
default=linux
image=/boot/vmlinuz-2.4.20-8
label=linux
initrd=/boot/initrd-2.4.20-8.img
read-only
append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20sugaree
label=linux-sugaree
initrd=/boot/initrd-2.4.20sugaree.img
read-only
append="root=LABEL=/"
```

保存改变。对LILO，需要用lilo命令将改变写入硬盘的主引导记录（MBR）中。由于default设置为linux，因此LILO仍然自动引导旧内核，除非在LILO引导菜单中选择新内核。

小结

升级与重新编译Linux内核的想法初看起来让人望而生畏，尽管涉及的步骤很多，工作量很大，但这个过程并不复杂。

升级内核的最简单的方法是安装新的Red Hat Linux内核RPM包。安装而不升级时，新内核也自动升级引导装入器。如果是小升级，也可以下载和安装补丁包。

如果要改变内核配置，则过程比较复杂，主要步骤如下：

1. 下载新内核的源代码：ftp.kernel.org之类的Web站点上的tarballs或红帽子RPM包。
2. 安装与menuconfig、xconfig之类内核工具相关的RPM包。
3. 移到内核源代码所在目录。选择Makefile中的EXTRAVERSION值，备份任何当前隐藏.config文件。用make mrproper命令清理当前源代码。
4. 使用基线配置，有些在/boot中，有些在configs子目录中。也可以使用本地.config文件，或用make oldconfig命令生成另一文件。
5. 用make menuconfig或make xconfig打开内核配置编辑器。进行改变并保存。
6. 用make dep命令设置依赖性。
7. 用make bzImage命令生成压缩内核映像。它位于所在目录。
8. 将生成的内核复制到/boot目录中，命名为vmlinuz-xEXTRAVERSION，其中x表示内核版本号，EXTRAVERSION是Makefile中的变量。
9. 用make modules与make modules_install组织内核模块。
10. 用mkinitrd/boot/initrd-xExtraVersion命令生成新内核的初始内存盘。
11. 修改引导装入器：增加新内核和初始内存盘文件的段。

下一章要介绍其他管理功能。cron和at之类的作业管理器使管理员可以自动运行程序。其他关键管理任务包括日志文件分析和服务管理。

第13章 管理细节

管理计算机是个复杂的工作。即使在小组中，也要配置用户与组、生成备份、维护数据库，等等。许多管理工作是相当费时的。如果在上班时间运行这些任务，则可能占用大量系统资源，使用户无法正常工作。

可以改变工作时间，在晚上运行，但如果你要负责几个地方的管理工作呢？每个Linux管理员还要有自己的个人生活。

为了支持这些工作，Linux提供了cron和at监控程序，可以随时按计划将需要运行的程序自动化。at是一次性管理工具，而cron可以设置经常性定期运行的任务。

如果没有中间方案，则查错的第一个地方是日志文件。Linux日志通常放在/var/log目录中，提供系统活动的丰富信息。不同日志文件可以帮助监视安全、登录活动、监控程序状态，等等。

Linux管理员要熟悉几个基本命令。ps、top和kill可以帮助管理进程，who可以检查当前登录，nice与rnice命令可以对运行进程排成优先级，no top命令可以在退出top之后仍然运行程序。本章介绍下列内容：

- 使用cron监控程序
- 使用at监控程序
- 管理服务
- 日志查错
- 管理进程与用户

使用cron监控程序

如果你和计算机操作系统一样，不需要睡觉，则可以在晚上备份用户文件，可以在别人睡觉时转换日志和删除临时文件。

cron监控程序（也称为crond命令脚本）自动完成这个工作。Linux启动时，在后台进程中运行crond命令脚本，每分钟检查相应配置文件，看看是否要运行什么东西。

cron配置文件有两组，一组由全局配置文件/etc/crontab控制，一组基于用户用crontab命令生成的配置文件。

格式化cron

要了解cron如何工作，最好从基本cron配置文件/etc/crontab开始。这个文件指定几个环境变量，包括SHELL、PATH与HOME。下面一行一行地分析这个文件：

```
SHELL=/bin/bash
```

这个文件中的命令基于bash shell。

```
PATH=/sbin:/bin:/usr/sbin:/usr/bin
```

指定目录中有此文件的命令时，不需要完整目录路径。`/etc/crontab`中的PATH还确定搜索目录的顺序。例如，如果flight命令同时在/sbin与usr/bin目录中，则cron运行/sbin/flight命令。

```
MAILTO=root
```

每次cron命令脚本实际工作时，将通知邮寄给根用户。

```
HOME=/
```

与这个/etc/crontab配置文件相关的主目录为根目录 (/)。

```
# run-parts
```

run-parts命令运行指定目录中的每个脚本文件，从而可以组织需要定期运行的脚本。

```
01 * * * * root run-parts /etc/cron.hourly
```

这个命令在每天每小时过后一分钟运行/etc/cron.hourly目录中的每个脚本文件。

```
02 4 * * * root run-parts /etc/cron.daily
```

这个命令在每天凌晨4时2分运行/etc/cron.daily目录中的每个脚本文件。

```
22 4 * * 0 root run-parts /etc/cron.weekly
```

这个命令在每个星期天凌晨4时22分运行/etc/cron.weekly目录中的每个脚本文件。

```
42 4 1 * * root run-parts /etc/cron.monthly
```

这个命令在每月第一天凌晨4时42分运行/etc/cron.monthly目录中的每个脚本文件。

命令中的数字与星号好像比较古怪，下面要进行详细介绍。

cron语法

要有效利用cron，就要了解cron文件中每个命令左边的时间与日期字段。表13.1从左到右列出了五个字段。

表13.1 cron文件中的时间与日期字段

字段	取值范围
Minute	0~59
Hour	0~23，其中0是午夜，20是晚上8时
Day	1~31
Month	1~12
Day of week	0~7，其中0和7表示星期天

任何字段中的星号是通配符。例如，如果第一个字段包含星号，则特定任务在可能的每一分钟运行。

如果要指定时间范围，如上午8时到下午4时，则可以将第二个字段设置为8~16。如果要隔一天运行任务，则可以将第三个字段设置为*/2。可以看出，知道这五个字段（minute、hour、day、month、day of week）之后，cron文件中的每个字段就没有什么神秘之处了。

标准cron任务

安装Red Hat Linux时，标准配置中包括一组cron任务。这个配置可以按每小时、每天、每月或每周组织cron任务。每个类别放在不同目录中：`/etc/cron.hourly`、`/etc/cron.daily`、`/etc/cron.weekly`与`/etc/cron.monthly`。

下面介绍几个每天运行的标准cron任务：

logrotate 定期轮换日志。例如，Red Hat Linux轮换五周的日志，上一周的`/var/log/messages`项目放在`/var/log/messages.1`文件中。

slocate.cron 刷新与`locate`命令相关的数据库。默认情况下，数据库更新排除从其他计算机联网的目录以及几个临时目录。

tmpwatch 删除`/tmp`与`/var/tmp`目录中的文件。默认情况下，这些目录中的文件分别在240小时和720小时没有访问时删除。

用户cron任务

Linux用户也可以计划用户cron任务。例如，有人要在午夜管理数据库。只要这个用户没有在`/etc/cron.deny`表中（见本章稍后介绍），就可以用`crontab -e`命令启动自己的cron文件。

说明：crontab默认使用vi编辑器，但也可以将其设置为另一个编辑器。例如，如果要用Emacs编辑器编辑cron文件，则可以运行`export EDITOR=emacs`命令。

例如，假设将脚本`goodback`配置成备份主目录中的所有文件，则可以在每个星期天凌晨1时36分运行`goodback`。假设用户名为`ez`，脚本在默认主目录（`/home/ez`）中。则可以以`ez`身份登录，然后运行`crontab -e`命令。假设使用默认vi编辑器，则可以输入I进入插入方式，然后输入下列行：

```
36 1 * * 0 /home/ez/goodback
```

保存文件之后，可以用`crontab -l`命令检查文件内容。所有用户cron文件都存放在`/var/spool/cron`目录中，默认可以由拥有者和根用户访问。

说明：如果生成cron文件，则还要指定SHELL、PATH与HOME变量。最好还要设置MAILTO变量，在cron实际运行任务时取得通知。关于默认`/etc/crontab`文件的细节，见前面“格式化cron”一节。

脚本管理

运行cron任务时，就是运行脚本。这个可执行文件中的命令也可以在命令行界面中运行。也可以用文本编辑器将经常使用的命令放在一个文件中。保存这个文件，然后用`chmod +x script1`命令使其变成可执行文件。例如，假设文件在`/path/to`目录中，则可以随时输入`/path/to/script1`命令执行。如果有几个命令通常要同时运行，则可以将这个文件扩展成包括多个命令，从而大大节省时间。

将脚本保存到PATH目录中则更加高效。例如，假设用户名为`tb`。则运行`echo $PATH`命令，可以看到PATH目录中有个`/home/tb/bin`目录。如果将`script1`之类的脚本保存到该目

录中，则运行这个脚本时，只要运行script1命令即可。

记住，如果要把script1作为cron任务，则应按前面介绍的方法将相应目录加进PATH目录中。

cron安全性

默认情况下，所有用户都可以访问cron工具。要限制对cron的访问，可以生成/etc/cron.allow与/etc/cron.deny文件。这些文件有几种不同情形：

- 这两个文件都不存在时，每个用户都可以访问cron工具。
- 只有/etc/cron.allow中的用户可以访问cron工具，如果也有/etc/cron.deny文件，则忽略后一个文件。
- 如果/etc/cron.deny文件不存在，则/etc/cron.allow中的用户不可以访问cron工具。

使用at监控程序

cron任务的一个缺点是要计划成经常运行。有时只需要让特定任务运行一次，然后就用不上了。这时就要使用at监控程序。

设置的任务很简单，可以指定运行程序的时间，也可以用相关的batch命令在计算机比较空闲时启动任务。

这个监控程序有点像打印进程，把任务假脱机到/var/spool/at目录中，在所要时间执行。

at监控程序相当于另一个shell。运行at time命令时，它发送一个命令提示，可以输入任意命令和程序。at now + time命令可以在经过指定时间之后运行任务。

例如，假设处理一个大型数据库，要在别人不用系统时处理数据，如凌晨2时5分。先建立/home/mj/airplane脚本管理数据库，计划处理/home/mj/air-safe文件中的结果。正常方式是使用下列命令：

```
# at 2:05 tomorrow
at> /home/mj/airplane > /home/mj/air-safe
at> Ctrl-D
```

可以用几个不同方法在at time命令中设置时间，见表13.2。

表13.2 at监控程序时间参数

时间	例子	说明
Minute	at now + 5 minutes	任务在5分钟后运行
Hour	at now + 1 hour	任务在1小时后运行
Days	at now + 3 days	任务在3天后运行
Weeks	at now + 2 weeks	任务在两周后运行
Fixed	at midnight	任务在午夜运行
Fixed	at 10:30pm	任务在晚上10时30分开始
Fixed	at 1:00 5/12/03	任务在2003年5月12日凌晨1时开始

任务队列

输入任务之后，可以用`atq`命令将其放进队列中。可以看到，输出提供了任务号、负责用户和任务执行时间。用户名前面的字母（a或b）表示它是at任务还是batch任务：

```
# atq
8      2003-03-08 02:05 a mj
```

删除任务很容易，只要用`atrm jobnumber`命令。例如，下列命令从队列中删除第8个任务：

```
# atrm 8
```

批处理任务

`batch`任务是`at`任务的特殊版本，默认情况下，用`batch`命令生成的任务只在CPU需求低于CPU能力的80%时才运行。

`batch`命令相当于`at -q b`命令。

安全性

和`cron`监控系统一样，`at`使用`/etc/at.allow`与`/etc/at.deny`文件规定对系统的访问。默认情况下，Red Hat Linux安装空白`/etc/at.deny`文件，即所有用户都可以访问`at`系统。

只有`/etc/at.allow`中的用户可以访问`at`工具，如果也有`/etc/at.deny`文件，则忽略后一个文件。如果`/etc/at.deny`文件不存在，则`/etc/at.allow`中的用户不可以访问`at`工具。

服务管理

服务管理是Linux系统管理员的一个关键技能。可以用`/etc/rc.d/init.d`目录中的脚本启动与停止当前任务。此外，可以保证所选服务在特定间隔期间活动。

`/etc/rc.d/init.d`脚本

Red Hat Linux中安装的服务在`/etc/rc.d/init.d`目录中有自己的脚本。系统中通常有大量脚本，图13.1显示了我的桌面计算机上的服务脚本。

```
[root@RH9Test root]# ls /etc/rc.d/init.d/
acpid      dhcpcd     kdcrotate  netfs      postgresql snb         xfs
and        firstboot  keytable   network    pxe        snmpd       xinetd
anacron    functions  killall    nfs         radvd      snmpttrapd  ypbind
apmd       gpm        kprop      nfslock    random     spamassassin yppasswdd
atd        halt       krb524     nsd         rawdevices squid        ypserv
autofs     httpd      krb5kdc    ntpd        rhnsd      sshd        ypxfrd
bees5820   innd       kudzu      ospf6d     ripd       syslog      zebra
bgpd       iptables   lisa       ospfd      ripngd     tax
crond      irda       lpd        pcscia     saslauthd  vncserver
cups       isdn       mailman    portmap    sendmail   vftpd
dhcpcd     kadmin     named      postfix    single     winbind
[root@RH9Test root]#
```

图13.1 `/etc/rc.d/init.d`目录中的服务脚本

看看其中一些脚本。在文本编辑器中打开脚本，在每个脚本末尾，可以看到一系列命令，如图13.2。这个smb脚本管理Samba。不同脚本中的有些命令是不同的。

```
case "$1" in
start)
    start
    ;;
stop)
    stop
    ;;
restart)
    restart
    ;;
reload)
    reload
    ;;
status)
    rstatus
    ;;
condrestart)
    [ -f /var/lock/subsys/smb ] && restart ||
    ;;
*)
    echo $"Usage: $0 {start|stop|restart|reload|status|condrestart}"
    exit 1
esac
```

96,1-8 97%

图13.2 服务脚本内幕

从图13.2可以看出，可以对特定服务运行几个操作，见表13.3。这个表中只反映了图13.2的操作，不同脚本中的动作是不同的。

表13.3 服务脚本操作

操作	描述
start	启动服务，等价于服务脚本start命令
stop	停止服务，等价于服务脚本stop命令
restart	关闭服务，然后再次启动，等价于服务脚本restart命令
reload	使服务不重新启动而重读相关配置文件，等价于服务脚本reload命令
status	提供服务的当前状态，等价于服务脚本status命令
condrestart	如果服务锁定，则这个开关关闭服务，然后再次启动，等价于服务脚本condrestart命令

例如，如果要重新启动Samba，则可以以根用户身份运行下面两个命令：

```
# /etc/rc.d/init.d/smb restart
# service smb restart
```

激活不同运行级

可以让服务在不同运行级启动与停止。例如，图13.3是运行级3的服务。

从/etc/rc.d/rc3.d目录可以看出，Linux在运行级3启动时，删除Apache 3（K15httpd）。如果要在运行级3启动这个服务，则要在启动脚本中改变。标准方法是chkconfig命令。要列出与Apache（httpd）相关联的当前运行级，用下列命令：

```
# chkconfig --list httpd
httpd 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

```
[root@RHTest root]# \ls /etc/rc.d/rc3.d/
K05snd      K35vncserver  K65krb5kdc  S06iptables  S56randdevices
K09ac1authd K39winbind    K70nfs1000  S09iscn       S39xinetd
K12nailman  K36lisa       K70bcm5820  S10network    S58nupd
K15httpd    K45named      K74ypserv   S12syslog     S09nendmail
K15postgresql K56advsd      K74ypxfrd   S13portmap    S05passwdssm
K20nfs      K50nmapd      K84hgpd     S14nfslock    S85gn
K24lrda     K50nmaptrpd   K84ospfd    S17keytable   S90ctond
K25squid    K50rux        K84ospfd    S20random     S00cps
K28and      K50vsftpd     K84ripd     S24pcmcia     S00xfs
K34dircelay K54pxe        K84ripd     S25etfs       S95acton
K39ypasswd  K85kadmin     K85zebra    S26apd        S95td
K350hcpd    K65kprop      K95firstboot S28autofs     S07rhnsd
K35nab      K65krb324     S05kudzu    S55sshd       S99local
[root@RHTest root]#
```

图13.3 运行级3的服务

这个输出显示，Apache没有在任何运行级中启动。要启动Apache，就要在所要运行级中将其激活。例如，下列命令在运行级3和5启动这个服务，使用标准多用户和G级方式：

```
# chkconfig --level 35 httpd on
```

要确认这个效果，可以列出运行级3和5的文件，这里可以看到每个目录（/etc/rc.d/rc3.d和/etc/rc.d/rc5.d）中的S85httpd启动脚本。也可以只用下列命令：

```
# ls -l /etc/rc.d/rc3.d
```

```
httpd 0:off 1:off 2:off 3:on 4:off 5:on 6:off
```

有几个图形工具，例如，可以用ntsysv --level runlevel浏览不同运行级的服务。例如，ntsysv --level 5命令可以浏览第5运行级的服务，如图13.4。



图13.4 管理服务

查错日志

有一首老歌，与加利福尼亚州伯克利市的一家酒家有关：“在Linux酒家中，你可以找到几乎任何日志。”Linux日志文件的菜单是非常丰富的，可以按服务或按问题严重性配置日志。

我们已经在第3章介绍了安装日志文件的工作。本节介绍日志文件，看看Linux服务发生的情形。

日志文件由系统日志和内核日志监控程序syslogd与klogd控制，在/etc/syslog.conf文件中配置这两个监控程序默认活动。

日志文件类别

可以用系统日志文件诊断安装、引导、特定服务等问题。日志可以分成八大类，下面按重要性从大到小列出：

- emerg (emergency, 紧急)
- alert (警报)
- crit (critical, 关键)
- err (error, 错误)
- warning (警告)
- notice (通知)
- info (信息)
- debug (调试)

日志文件按Linux /etc/syslog.conf配置文件中的消息进行组织。图13.5显示了这个文件的默认Red Hat Linux版本。

```
# log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console
[]
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* /var/log/maillog

# Log cron stuff
cron.* /var/log/cron

# Everybody gets emergency messages
*.emerg *

# Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log
```

图13.5 /etc/syslog.conf文件

可以看出，大多数日志位于/var/log目录中。如果激活内核消息，则其通常发送到控制台（屏幕）。有些监控程序（如Internet Network News，互联网新闻监控程序）还在这个文件中包括其他技术细节。

日志通过标准cron任务logrotate维护。前面曾介绍过，它每周轮换日志文件。这样，/var/log/boot.log.1文件是上周的文件。

看看这个文件中第一个活动行，其指定与几个监控程序相关联的消息。例如，第一条语句`*.info`，将info级以上（notice、warning、err、crit、alert与emerg）的所有消息发送到相应日志文件。

系统日志

下面看看`/var/log`目录中的系统日志。`dmesg`文件包括与Linux启动相关的基本引导消息。`message`文件包括计算机上启动Linux之后的其他处理消息。`boot.log`文件列出与监控程序启动和停止相关的消息。`wtmp`可以帮助监视登录。

取得其余dmesg内容

第11章介绍了`/var/log/dmesg`如何确定Linux是否探测到硬件。这个文件末尾还有一个关键项目：Linux是否正确装载了文件系统与交换空间。如果装载成功，则可以看到如下消息：

```
EXT3 FS 2.4-0.9.19, 19 August 2002 on ide0(3,6), internal journal
Adding Swap: 257032K swap-space (priority -1)
kjournald starting. Commit interval 5 seconds
```

表示Linux在分区上成功地装载了带内部杂志的ext3文件系统。`kjournal`监控程序（`kjournald`）实际更新文件系统杂志。每个Linux分区都有类似行

其他/var/log/messages消息

`/var/log/messages`中记录了与硬件和服务相关联的其他消息。下面显示了两个例子：

```
Sep 23 11:03:00 RH9 kernel: sb: No ISAPnP cards found, trying standard ones...
Sep 23 11:03:00 RH9 kernel: SB 4.13 detected OK (220)
Sep 23 11:46:46 RH9 sshd(pam_unix) [1129]: session opened for user root by LOGIN(uid=0)
Sep 23 11:46:51 RH9 sshd(pam_unix) [1129]: session closed for user root
```

这个文件中每一行包括一些基本特征，如每个消息相关的日期、时间、主机名与服务。如果可能，还会列出用户名与进程标识符。

可以看到代码中的两个重要进步。第一，Red Hat Linux在引导过程中发现了声霸卡。第二，有人通过sshd顺利访问了RH9计算机，这是个安全shell监控程序。第22章将会介绍，安全shell监控程序是远程管理计算机的关键工具。

但也可能有安全漏洞。如果发现登录是没有授权的，则可能有黑客攻进系统。第22章介绍了如何保护Linux系统。

说明：在Linux世界中，hacker是好人，目的只是建立更好的软件，而Crackers则是要进攻系统的坏人。

分析/var/log/boot.log

启动与停止服务和监控程序时，会在`/var/log/boot.log`中列出。以图13.6为例，事实上，其中显示的第一行是1月15日关闭的最后消息。第二个消息是引导`/var/log/boot.log`时启动的第一个监控程序。

```

Mar 26 10:54:04 RH9Test syslog: syslogd startup succeeded
Mar 26 10:54:04 RH9Test syslog: klogd startup succeeded
Mar 26 10:54:04 RH9Test portmap: portmap startup succeeded
Mar 26 10:54:05 RH9Test nfslock: rpc.statd startup succeeded
Mar 26 10:54:05 RH9Test keytable: Loading keymap:
Mar 26 10:54:05 RH9Test keytable:
Mar 26 10:54:05 RH9Test rc: Starting keytable: succeeded
Mar 26 10:54:05 RH9Test random: Initializing random number generator: succeeded
Mar 26 10:54:05 RH9Test rc: Starting pcmcia: succeeded
Mar 26 10:54:06 RH9Test netfs: Mounting other filesystems: succeeded
Mar 26 10:54:06 RH9Test apmd: apmd startup succeeded
Mar 26 10:54:06 RH9Test autofs: automount startup succeeded
Mar 26 10:54:10 RH9Test sshd: RSA1 key generation succeeded
Mar 26 10:54:10 RH9Test sshd: RSA key generation succeeded
Mar 26 10:54:15 RH9Test sshd: DSA key generation succeeded
Mar 26 10:54:15 RH9Test sshd: succeeded
Mar 26 10:54:19 RH9Test xinetd: xinetd startup succeeded
Mar 26 10:54:20 RH9Test sendmail: sendmail startup succeeded
Mar 26 10:54:21 RH9Test sendmail: sm-client startup succeeded
Mar 26 10:54:21 RH9Test gpm: gpm startup succeeded
Mar 26 10:54:21 RH9Test crond: crond startup succeeded
Mar 26 10:54:24 RH9Test cups: cupsd startup succeeded
"/var/log/boot.log" 312L, 17876C

```

图13.6 /var/log/boot.log文件

有些服务还有其他参数。例如，图13.6中的keytable参数装入与键盘相关的keymap。此外，network服务的启动环境初始化。

探测远程登录

登录记录放在一个数据库文件/var/log/wtmp中。可以用utmpdump命令使这个文件变成可读格式。以图13.7为例，这是运行utmpdump/var/log/wtmp时的部分输出。注意IP地址128.99.1.64的登录。

```

] [Wed Mar 26 11:03:49 2003 EST]
[5] [02151] [x] [ ] [ ] [ ] [2.4.20-6] [ ] [0.0.0.0]
] [Wed Mar 26 11:03:49 2003 EST]
[6] [02145] [1] [ ] [LOGIN] [ ] [tty1] [ ] [0.0.0.0]
] [Wed Mar 26 11:03:49 2003 EST]
[6] [02149] [5] [ ] [LOGIN] [ ] [tty5] [ ] [0.0.0.0]
] [Wed Mar 26 11:03:49 2003 EST]
[6] [02150] [6] [ ] [LOGIN] [ ] [tty6] [ ] [0.0.0.0]
] [Wed Mar 26 11:03:49 2003 EST]
[6] [02146] [2] [ ] [LOGIN] [ ] [tty2] [ ] [0.0.0.0]
] [Wed Mar 26 11:03:49 2003 EST]
[6] [02147] [3] [ ] [LOGIN] [ ] [tty3] [ ] [0.0.0.0]
] [Wed Mar 26 11:03:49 2003 EST]
[6] [02148] [4] [ ] [LOGIN] [ ] [tty4] [ ] [0.0.0.0]
] [Wed Mar 26 11:03:49 2003 EST]
[7] [02204] [ :0 ] [root] [ ] [ :0 ] [ ] [128.99.1.64]
] [Wed Mar 26 11:04:33 2003 EST]
[8] [00000] [ :0 ] [ ] [ ] [ :0 ] [ ] [128.99.1.64]
] [Wed Mar 26 11:05:34 2003 EST]
[7] [02333] [ :0 ] [root] [ ] [ :0 ] [ ] [128.99.1.64]
] [Wed Mar 26 11:05:46 2003 EST]
[7] [02437] [ /0 ] [root] [ ] [ pts/0 ] [ ] [0.0.0.0]
] [Wed Mar 26 11:06:01 2003 EST]

```

图13.7 检查登录活动

警告：应知道局域网的IP地址。如果你的网络不包括图13.7所示的某些地址，而你没有任何远程用户，则要小心了。也许已经有人攻进你的系统。第22章将介绍如何阻止来自可疑网络的登录。

监控程序日志

大多数Linux监控程序都在/var/log目录中配置日志文件，如crond、httpd与smbd。每个日志文件可以显示特定服务成功或失败。图13.8显示了一个整洁的例子，是/var/log/cron文件的视图。

```
Mar 26 10:54:21 RH9Test crond[1944]: (CRON) STARTUP (fork ok)
Mar 26 10:54:26 RH9Test anacron[2037]: Anacron 2.3 started on 2003-03-26
Mar 26 10:54:26 RH9Test anacron[2037]: Will run job 'cron.daily' in 65 min.
Mar 26 10:54:26 RH9Test anacron[2037]: Will run job 'cron.weekly' in 70 min.
Mar 26 10:54:26 RH9Test anacron[2037]: Will run job 'cron.monthly' in 75 min.
Mar 26 10:54:26 RH9Test anacron[2037]: Jobs will be executed sequentially
Mar 26 11:01:00 RH9Test CROND[2062]: (root) CMD (run-parts /etc/cron.hourly)
Mar 26 11:23:15 RH9Test crond[1958]: (CRON) STARTUP (fork ok)
Mar 26 11:23:19 RH9Test anacron[2035]: Anacron 2.3 started on 2003-03-26
Mar 26 11:23:19 RH9Test anacron[2035]: Will run job 'cron.daily' in 65 min.
Mar 26 11:23:19 RH9Test anacron[2035]: Will run job 'cron.weekly' in 70 min.
Mar 26 11:23:19 RH9Test anacron[2035]: Will run job 'cron.monthly' in 75 min.
Mar 26 11:23:19 RH9Test anacron[2035]: Jobs will be executed sequentially
Mar 26 11:58:25 RH9Test crond[1961]: (CRON) STARTUP (fork ok)
Mar 26 11:58:30 RH9Test anacron[2039]: Anacron 2.3 started on 2003-03-26
Mar 26 11:58:30 RH9Test anacron[2039]: Will run job 'cron.daily' in 65 min.
Mar 26 11:58:30 RH9Test anacron[2039]: Will run job 'cron.weekly' in 70 min.
Mar 26 11:58:30 RH9Test anacron[2039]: Will run job 'cron.monthly' in 75 min.
Mar 26 11:58:30 RH9Test anacron[2039]: Jobs will be executed sequentially
Mar 26 12:01:00 RH9Test CROND[2376]: (root) CMD (run-parts /etc/cron.hourly)
Mar 26 12:24:05 RH9Test crond[1958]: (CRON) STARTUP (fork ok)
Mar 26 12:24:09 RH9Test anacron[2037]: Anacron 2.3 started on 2003-03-26
Mar 26 12:24:10 RH9Test anacron[2037]: Will run job 'cron.daily' in 65 min.
```

图13.8 /var/log/cron文件

从图13.8可以看出执行cron任务的日期和时间。本章前面曾介绍过，这是标准cron任务。尽管这里的时间与/etc/crontab中指定的不同，但这只是表明这台Linux计算机没有在指定时间运行。

下面是/var/log/httpd/access_log的摘要，显示Web服务器的一台客户机情况。例如，这台客户机在夏时制期间（-0400）从美国东部时区使用Lynx Web浏览器：

```
localhost.localdomain - -[23/Sep/2003:14:05:26 -0400] "GET / HTTP/1.0" 403 2898
➡ "-" "Lynx/2.8.5dev.7 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6b"
```

下列摘要（来自/var/log/samba/smbmount.log）显示通过Samba连接Microsoft Windows 共享：

```
[2003/09/23 13:53:32, 0] client/smbmount.c:send_fs_socket(383) mount.smbfs: entering
➡ daemon mode for service \\laptop2\downloads, pid 5711
```

在Red Hat Linux系统中增加更多监控程序时，/var/log目录中会出现更多日志文件。但是，日志文件也不一定放在/var/log目录中，这是由每个监控程序的配置文件确定的。

其他日志

/var/log目录中还有几个其他日志文件。增加更多服务时，会出现更多日志文件。因此，表13.4并不是完整的清单。

表13.4 /var/log日志文件

文件	功能
ksyms	导出内核符号，如驱动程序与模块
lastlog	根据lastlog -u username命令指定最后登录的时间与地点
maillog	与邮件服务器相关的一切，如sendmail的启动、关闭、别名和错误
news	与InterNetNews (INN) 服务器相关的日志文件目录
rpmkgs	当前安装的RPM包
scrollkeeper	用于文档，特别是GUI文档
secure	与安全连接相关的一切，如ssh与xinetd

进程管理

要管理Linux计算机，就要知道如何管理进程。

可以用几个关键工具在Linux中管理进程：**who**与**ps**。这些命令可以分别跟踪谁在连接、什么进程在运行。此外，**top**命令可以监视服务对计算机的需求。最后，**nohup**命令可以运行另一命令，使其在你退出计算机之后仍然运行。

如果任何用户在任何应用程序中遇到问题，则可以用**kill**命令停止这个应用程序。如果要运行其程序或进程，则可以用**nice**命令，提高与降低所运行程序的优先级。

进程与ps

ps命令显示什么进程或程序正在运行。单单输入**ps**命令时，可以看到安装相关的进程。如果输入**ps aux**，则可以看到Linux系统中运行的一切，包括监控程序。另一个重要变形是**ps 1**，返回每个当前运行进程的“长清单”。表13.5列出了这个命令显示的重要类别。

表13.5 ps-al输出类别

项目	说明
PID	进程标识符，每个进程与一个数据库相关联，称为进程标识符
PPID	父进程标识符，每个进程有个父进程（除了init）。如果不能删除一个进程，则可以删除其父进程
PRI	优先级值。优先级值高的程序更快得到CPU的注意，优先级值最高的程序PRI为-20，优先级值最低的程序PRI为19
STAT	进程当前状态，有三个选项：R（运行）、S（休眠）和SW（交换分区）

说明：**ps**是少数几个命令开关前面不用连字符的命令之一。

如果有一个程序失控，则要知道PID号才能停止这个程序。如果运行的程序一直等待CPU资源，则可以用其PID提高优先级。

进程与top

top命令可以监视服务对计算机的需求，特别是CPU和内存。例如，图13.9的**top**命令输出显示了系统内存不足时的情形。

```

1:38pm up 5:18, 1 user, load average: 0.22, 1.78, 0.74
65 processes: 60 sleeping, 5 running, 0 zombie, 0 stopped
CPU states: 12.7% user, 7.6% system, 0.0% nice, 79.5% idle
Mem: 34552K av, 37098K used, 528K free, 0K shrd, 312K buff
Swap: 183528K av, 5426K used, 139204K free, 14892K cached

```

PID	USER	PR	NI	SIZE	RES	SHARE	STAT	SCD	STEN	TIME	CMD	
1221	root	15	-1	13724	3476	2520	D	4	5.7	0.2	0:58	x
1286	root	15	0	4868	3524	2652	R		3.9	0.3	0:23	gnome-terminal
1270	root	15	0	5288	3992	3104	R		2.1	10.6	0:12	gnome-panel
1450	root	15	0	748	748	502	R		1.7	1.8	0:05	top
1452	root	15	0	14884	1236	9080	R		1.1	34.8	0:18	mozilla-bin
1278	root	15	0	8940	3652	3044	S		0.9	0.7	1:01	xhm-applet-gui
5	root	15	0	0	0	0	SW		0.5	0.0	0:05	ksmopd
1274	root	15	0	2684	1952	1836	S		0.1	5.1	0:01	magicedv
1	root	15	0	400	368	348	S		0.0	0.0	0:04	init
2	root	15	0	0	0	0	SW		0.0	0.0	0:00	keventd
3	root	15	0	0	0	0	SW		0.0	0.0	0:00	kupd
4	root	34	19	0	0	0	SW		0.0	0.0	0:00	ksoftirqd_CPU0
6	root	15	0	0	0	0	SW		0.0	0.0	0:00	bdflush
7	root	15	0	0	0	0	SW		0.0	0.0	0:00	kupdated
8	root	28	0	0	0	0	SW		0.0	0.0	0:00	mdrecoveryd
12	root	15	0	0	0	0	SW		0.0	0.0	0:03	kjournald

图13.9 top命令输出

本例中，性能不好，可以听到硬盘一直在忙个不停。从图13.9的输出表明，要减少硬盘负荷，可以限制Mozilla Web浏览器运行，也可以增加系统内存量。

如果运行多用户系统，则要注意与问题中提到的用户。

登录与who

管理员要经常检查登录情况，例如，下面的who命令输出显示了同一个人从两个不同地点登录：

```

mj      tty1      Mar 12 10:33
ywow    pts1      Mar 11 22:30 (192.168.0.12)
mj      pts0      Mar 11 22:45 (136.46.1.64)

```

由于用户mj从本地机和地址为136.46.1.64的远程计算机同时登录，因此可能有人冒充mj的用户名和口令，想攻击系统。

进程删除

Linux号称是不会崩溃的。据说，Linux支持的用户和Web站点可以一个月不重新启动。其原因之一是，系统管理员能够用kill命令管理程序。

例如，如果浏览互联网时，Mozilla Web浏览器死机了，则可以按下列命令删除这个程序：

1. 打开命令行shell。如果无法在X窗口中打开命令行shell，则可以用Ctrl+Alt+Fn命令打开新的虚拟控制台，其中n是1到6的值。
2. 运行ps aux | grep mozilla命令。用户名后面的数字是运行Mozilla的进程PID。本练习中，假设进程号为1789。
3. 运行kill PIDnumber命令。根据第2步的结果，实际命令为kill 1789。如果kill命令无法工作，则可以用ps aux | grep mozilla命令寻找PPID，可能要先删除这些进程。
4. 最后，还可以使用一个开关，即使会在内存中留下其他程序，也强制删除进程。

nice与renice

nice与**renice**命令可以按不同的相对优先级运行程序。任何程序的优先级可以取-20（最高）到19（最低）。**nice**程序启动另一个优先级不同的进程。例如，可以将Mozilla设置成在所有其他进程完成后启动，命令为**nice -n 19 mozilla**。如果要想Linux关注特定程序，则需取得其PID。一旦找到程序的PID后（本练习中，假设进程号为1789），就可以用**renice -10 1789**命令增加优先级。

说明：要了解优先级，记住Linux中的一切都是倒过来的。如果程序更重要，就用负数。

使用nohup

如果无法按所要优先级运行一个程序，则可以使用**nohup**命令，**nohup**命令可以运行另一个命令，使其在你退出计算机之后仍然运行。例如，假设要将一个.iso文件刻录到光碟中。记录到光碟是需要较长时间的，而你又要到学校接小孩了。

如果计算机上有光碟刻录机，则可以用**nohup**命令。要把redhatcd1.iso文件记录到光碟中，可以运行下列命令，然后退出你的用户账号，即可自动将文件记录到光碟，并在本地目录的nohup.out文件中写入消息：

```
# nohup cdrecord -v speed=4 drive=1,0,0 redhatcd1.iso
```

当然，这要求不关闭Linux计算机。关于cdrecord命令的更多信息，见下一章介绍。

小结

cron监控程序可以帮助经常性自动运行程序。Red Hat Linux通过/etc/crontab配置标准**cron**任务，在/etc/cron.hourly和/etc/cron.weekly之类的目录中配置时间。用户可以用**crontab**命令配置自己的**cron**任务，每个用户的配置存放在/var/spool/cron目录中。**cron**安全由/etc/cron.allow与/etc/cron.deny文件控制。

at命令与**cron**相似，但可以运行一次性任务。**batch**命令是**at**的变形，在系统需求低于系统功能的80%时运行指定任务。与**cron**相似，**at**安全由/etc/at.allow与/etc/at.deny文件控制。

管理Linux的另一个关键是基于日志文件。标准Linux日志文件在/etc/syslog.conf中配置，位于/var/log目录中。系统日志可以跟踪探测的硬件，分析登录活动。监控程序日志可以监视crond、httpd与smbd之类的监控程序的使用情况。还有其他日志文件，可以监视当前安装的RPM包、安全连接、新闻服务器，等等。

要管理Linux计算机，就要知道几个基本过程和用户安全命令。**ps**、**top**与**kill**命令可以寻找与删除失控的进程，**who**命令可以标识当前登录用户，**nice**与**renice**命令可以改变关键任务的优先级。

下一章要扩展Linux管理知识，介绍备份整个系统或部分系统的命令。

第14章 备份系统

如今个人计算机上的数据非常脆弱。管理员经常担心病毒影响网络上的数据。黑客攻击、电源不稳、机器故障、磁场和自然灾害等事故都可能破坏硬盘上的整个或部分数据。

备份系统的措施取决于具体情形。在多台计算机上对多个用户备份数据时需要更加小心。为了帮助公司从故障恢复，可以选择把数据存放在另一地点。

可以使用几种不同类型的备份介质。可以将关键数据备份到光碟上，也可以将整个计算机备份到一个或几个磁带机上。可录制DVD已经成为磁带机的可行替换。也可以用可拆硬盘和外部硬盘，其容量大，而且很容易存放在不同地点。

在大型网络中，可以备份到中央服务器。管理员可能要在一个地点从网络上所有服务器备份文件。工作站和桌面用户可能发现，负责任的Linux管理员在维护中央备份服务器，非常方便。

根据备份介质与方式不同，可以使用几个备份命令，如tar、cpio、dump与restore。也可以用正确配置的RAID在其他磁盘上备份数据。有时，可以备份到RAID盘，存放在远程安全地点。本章介绍下列主题：

- 探索备份概念
- 选择备份介质
- 使用备份与恢复命令
- 了解RAID

探索备份概念

备份策略的选择取决于愿意承担的风险。任何计算机备份的风险包含两个部分。第一，要了解数据和计算机可能发生什么情形，灾难包括文件搞乱和公司总部破坏。第二，要选择解决每种灾难的备份策略。策略（与成本）取决于数据重要性、用户对不同灾难的反应和需要以多快速度从备份恢复。最后，还要保证能从生成的备份恢复，而不能到实际需要时才发现行不通。

要了解风险的这几个部分，就要了解几种灾难情形和可用的数据与计算机备份级。

数据灾难情形

即使丢失一个文件也可能给用户造成灾难：例如，丢失商用飞机的工程图、硕士论文或正在创作的一本书的某一章都可能改变一个人的生活。

信息技术经理要计划每一级灾难，包括文件丢失和核战争（是的，有些公司的IT经理已经建立了核战争的备份计划）。表14.1列出了几种基本情形。

表14.1 数据灾难情形

情形	恢复策略
丢失用户文件	从/home文件系统备份恢复
丢失配置文件	从/etc备份恢复
丢失应用程序文件	重装备份或重新安装应用程序
分区损坏	从备份恢复分区或使用相应RAID级
硬盘损坏	从备份恢复硬盘或使用相应RAID级
计算机损坏	从其他计算机或磁带/光碟/DVD恢复数据
数据设备损坏	从远程地点存放的备份恢复
电磁数据丢失	从非磁性备份恢复

这里并没有列出全面的数据灾难情形。例如，网络问题也很困难，特别是用户无法访问服务器上的文件与应用程序时。当然，本书不准备介绍网络的灾难计划，但根本原理是相同的。

备份级

要确定哪些数据是至关重要的。如果是个人桌面用户，则可能只有几个关键文件，如文档。可以在每次改变这些文件时进行备份。

如果是计算机网络的Linux管理员，则要花更多经费保护与备份数据。但是，根据计算机网络中存储的数据量，每个晚上备份一次不一定合算。

下面几节介绍用Linux计算机作为个人桌面时，管理普通网络时和管理具有时间敏感数据的网络时可以做的工作。实际做法取决于数据重要性和资源可用性。

还要确定时间敏感数据的备份频率和大计算机群集中硬盘备份频率。

个人计算机用户

并不是所有用户都备份计算机。如果个人计算机用户只用计算机浏览互联网，则系统中没有什么不可替换的数据。对有些用户，灾难只是不方便，只要重新安装操作系统，然后再次连接网络即可。但是，如果你在计算机中保存财务记录之类的关键数据，则可以把自己看成Linux管理员，需要阅读下面几节的内容。

许多情况下，所有这些用户只要备份主目录中的文件。备份/etc中的配置文件有助于恢复许多定制设置。

有些用户喜欢备份Linux计算机上的所有文件和数据，这样就可以在发生灾难时顺利恢复，而不必增加时间配置系统。

Linux管理员

Linux管理员负责一组计算机时，一定要及时进行备份。例如，与新飞机设计相关的数据是经常改变的。

尽管恢复一天的工作并不太难，但恢复飞机公司一个星期或一个月的设计工作则是成本很高的。这时，可以在大容量介质上配置每次备份，如DVD或磁带。

这样，Linux管理员可以帮助疲劳的工程师恢复不小心删除的数据。如果发生大灾难，则管理员可以重新安装Linux，以及相应的工程软件，然后将设计文件恢复到相应目录中。

时间敏感数据

计算机是在时间敏感情形中使用的。例如，如果Linux管理员负责财务服务公司，则及时备份至关重要。例如，如果无法恢复与股市交易相关的数据，则后果非常严重。时间敏感信息需要实时备份，例如使用RAID。

这样，任何硬盘发生故障时都不会影响公司经营。利用可拆硬盘，还可以把RAID数据复制和存放在外部地址。

备份类型与频率

最简单的备份是备份计算机上的一切。但是，随着各个硬盘上的数据量增至几百GB，所要的时间也延长到几十小时。

尽管Linux计算机是多任务的，但备份负荷很大，可能影响用户性能。这样就形成了两个基本选择：只是偶尔备份整个计算机（如周末），或只是备份部分数据，如新文件或/home与/etc目录。

许多Linux管理员使用这两种理想的混合——Linux计算机的完整备份加上每天备份新文件。为此可以使用两种方法：

递增备份 递增备份包括上次完全备份以来生成或改变的所有文件。随着递增备份，长度也会不断增大。恢复系统时只要使用上次完全备份中的数据和最新递增备份。

差异备份 差异备份包括上次进行任何类型备份以来的所有文件改变。差异备份通常比递增备份小，但从差异备份恢复系统时更加困难，需要完全备份、递增备份（如有）和所有后续差异备份中的数据。

由于恢复数据需要更长时间，因此大多数Linux管理员使用某种形式的RAID。本章稍后将会介绍，RAID可以提供数据的近似实时冗余度。

介质选择

数据可以备份到任何能够记录信息的地方。有时甚至可以将关键配置文件打印到纸上，有些个人桌面用户发现三寸软盘就足够了。工作站用户可能需要更大的容量，如100MB Zip或230MB Bernoulli盘。这些用户只要备份关键文件，通常放在/home目录中。tar与cpio之类的命令可以备份特定文件或目录组，见本章稍后介绍。

如果需要备份GB或TB级数据（1TB = 1000GB），则有三种基本选项：磁带机、可写光碟/DVD和可拆硬盘。如果一个磁带或光碟无法备份硬盘，则可以用硬件将这些系统组织到磁带库和光碟/DVD“投币机”中。用硬盘备份的方法之一见本章稍后介绍，在“了解RAID”一节。

三种介质都可以复制和运输到安全的远程地点。如果一场大火或其他灾难将机房破坏，则可以用正确存储的正确介质重建公司并重开业务。美国的“9.11”事件对备份技术进行了大规模的测试。有些公司实时地将数据保存到远程地址，而有些公司则可以得到每小时或

每天的数据。

说明：还有许多其他第三方软件方案，如果数据量很大，要用到光碟“投币机”或大容量磁带机，则可能需要这些支持。www.storagesearch.com站点列出了第三方备份软件与硬件的厂家名单。

磁带机

如果经费允许，则可以买一个磁带机，以接近IEEE 1394硬盘的速度存储数据。到本书编写时，已经出现这样的系统，可以在一台磁带机中用100多个磁带盒存储30TB以上的数据。数据传输速度每小时近1000GB，因此一个周末就可以在这个磁带机中填进完全备份。

还有采用传统接口的低容量低成本磁带机，如采用并口、IDE和SCSI。使用这些接口的磁带机与使用这些接口的硬盘具有相似的设备名。

还有使用USB与IEEE 1394接口的磁带机。第2章曾介绍过，许多USB与IEEE 1394接口的支持还处于试验阶段，不一定能在Red Hat Linux 9中使用。

光碟/DVD备份

与磁带机相比，光碟/DVD备份大为逊色。一个光碟只能放650MB数据，一个DVD也只能放6GB数据。但是，已经出现一些“投币机”，可以将数据直接写入几百个磁盘中。

此外，光碟/DVD备份比磁带机有几个优点。在正确的环境条件下（即不在过热过湿环境中存储光碟），光碟/DVD备份可以保存十几年或更长时间。与硬盘和磁带机不同的是，光碟/DVD备份不会被磁场突然删除，不会受核爆炸的电磁脉冲影响。

使用备份与恢复命令

使用的命令取决于如何备份数据。一般性备份通常用tar或cpio命令，也可以用dump与restore命令转储或恢复磁带机数据。本地光碟的备份与mkisofs、cdrecord、dvdrecord命令相关。通过远程地址进行网络备份与恢复数据时，需要使用一些变形。

一般性备份

下面看备份一组文件的一般性备份命令。tar命令最初用于将文件与目录存档到磁带机中，cpio命令也复制文件与目录到档案中，或从档案中复制文件与目录。加上正确的选项后，可以用这些命令将文件备份到大多数介质。

说明：也可以用dd命令，直接将一个目录的内容转储到一个设备，例如/dev/fd0之类的软盘设备或/dev/st0之类的磁带机设备。关于dd命令的细节，见第3章介绍。

tar存档

第10章首次介绍了tar命令。这个命令很容易使用，其格式很容易压缩，是可下载的。这个命令可以代替RPM系统，包装程序与应用程序。使用正确的选项后，这个命令与Microsoft Windows的zip文件系统相似。

tar命令将一系列文件复制到一个大文件中。如果要备份mj主目录中的文件，则可以运行下列命令：

```
# tar cvzf mjbackup.tar.gz /home/mj
```

这个命令生成(c)一个备份,列出档案中的每个文件名(v=冗长),采用压缩格式(z=zip),放在文件(f)mjbackup.tar.gz中。/home/mj的子目录中的文件也保存在这个档案中。然后可以将这个档案文件保存到网络共享、磁带机之类的备份区域。

说明: 压缩tar档案通常用扩展名.tar.gz、.tgz或.tar.bz2。前两个扩展名都是用gzip命令压缩的tar档案,后一个扩展名基于bzip2的Burrows-Wheeler块排序压缩算法,数据压缩更加有效。

很容易用下列命令打开档案文件:

```
# tar tkvzf mjbackup.tar.gz
```

这个命令列出(t)档案中的文件,恢复时,它并不覆盖当前文件(k=保留旧文件)。在冗长(v)方式中,可以看到发生的一切。如果存储zip格式的文件,则要从zip(z)格式恢复,另外,它从备份文件mjbackup.tar.gz恢复。

表14.2列出了一些tar开关。注意,tar命令中第一个开关应当以c、t或x开头。

说明: tar命令是路径相关的。如果将文件用绝对路径保存到一个目录中(即开头为斜杠,如/home/mj),则可以从计算机上的任何位置将文件恢复到这个目录。如果使用相对路径(没有开头的斜杠,如home/mj),则文件不一定恢复到原址,而取决于当前工作目录。

可以用几个tar命令生成和提取档案。下面是一些典型命令,可以用表14.2所示的tar命令选项进行对照:

```
# tar xzvf download.tar.gz
# tar czvf backup.tar.gz /somedirectory
```

表14.2 tar命令选项

选项	功能
c	生成档案
d	比较档案与当前目录中的文件
f	使用下列档案文件名
j	压缩成bzip2格式
k	不覆盖当前文件
r	将文件添加到档案末尾
t	列出当前档案中的文件
v	冗长方式,列出进出档案的所有文件
z	Zip,按普通gzip格式压缩文件

说明: tar命令与ps相似,单字母选项前面不需要连字符。

cpio存档

cpio命令可以建档一类文件,与tar命令的不同之处在于,它处理标准输入和输出。顾名思义,cpio就是复制、输入和输出。

和tar命令一样,建档已知目录(及其子目录中的文件)很简单。例如,如果要备份mj主目录中的文件,用下列命令:

```
# find /home/mj | cpio -o > mjarch.cpio
```

但cpio命令有一个缺点，即来自标准输入，存档到标准输出。注意，标准输入是/home/mj目录中的所有文件，要管道到cpio命令。由于这时处理一类文件，因此可以用通配符将一组文件设置成标准输入。例如，下列命令从当前目录中的.tif文件建立档案：

```
# find *.tif | cpio -o > mjtifs.cpio
```

记住，find命令很灵活，下列命令从系统中的所有.tif文件建立档案：

```
# find / -name '*.tif' | cpio -o > mjtifs.cpio
```

很容易从cpio档案恢复文件。下列命令恢复mjarch.cpio中的文件：

```
# cpio -i < mjarch.cpio
```

和tar命令一样，cpio命令恢复从目录保存的文件时，取决于用相对路径还是绝对路径。

cpio命令的一个优点是可以直接将文件发送到外部源。例如，下列命令恢复mj主目录中的文件，并将其发送到SCSI磁带机：

```
# find /home/mj | cpio -o > /dev/st0
# cpio -i < /dev/st0
```

cpio命令有几个选项。表14.3列出了一些重要的cpio命令选项。

表14.3 cpio命令选项

选项	功能
-A	添加到档案末尾，与-F密切相关
-F	指定档案文件名，可以换成反向箭头(>)
-i	从档案文件或设备读取
-o	复制到档案文件或设备
-u	替换所有文件，即使其更新
-v	冗长方式

磁带转储与恢复

dump与restore命令使递增备份与差异备份很容易实现。dump可以取得目录内容，restore可以交互式将备份文件返回原址。

尽管这些命令最常用于磁带机，但也适用于其他介质。本节的例子用这些命令将主目录备份到软盘。

用dump命令存档

dump命令有三个基本选项级，详见附录。可以设置一系列命令，从主目录完全备份开始，然后是差异备份。例如，如果要用dump命令，将mao的主目录备份到/dev/nst0磁带机，可以用下列命令：

```
# dump 0f /dev/nst0 /home/mao
# dump 1f /dev/nst0 /home/mao
# dump 2f /dev/nst0 /home/mao
```

```
# dump 3f /dev/nst0 /home/mao
# dump 4f /dev/nst0 /home/mao
# dump 5f /dev/nst0 /home/mao
```

第一个命令使用0f选项，建立/home/mao目录的完全备份。后面的命令依次运行，只对上一备份之后改变的文件建立差异备份。

提示：为了加速备份，可以使用备份系统（如磁带机）允许的最大块长。例如，命令dump 0f /dev/nst0 /home/mao -b 2048使用的块长为2048字节。可以试用更大的块长来减少备份时间。但要记住，还要用相应restore命令验证试验结果。

也可以从完全备份开始，然后是增量备份，命令如下：

```
# dump 0f /dev/nst0 /home/mao
# dump 8f /dev/nst0 /home/mao
# dump 7f /dev/nst0 /home/mao
# dump 6f /dev/nst0 /home/mao
# dump 5f /dev/nst0 /home/mao
# dump 4f /dev/nst0 /home/mao
```

说明：你不用运行这六个命令。对于增量备份，只要保证下一个数（如4f）小于上一个增量备份命令，否则无法记录这个备份。

如果备份整个文件系统，则使用u选项，将历史存放在/etc/dumpdates里。例如，下列命令备份到整个根目录（/）文件系统：

```
# dump 0uf /dev/nst0 /
```

看看dump命令对/home/mao目录文件的处理，如图14.1。

```
[root@RH9Test root]# dump 0f /dev/fd0 /home/mao/
DUMP: Date of this level 0 dump: Fri Mar 28 10:54:02 2003
DUMP: Dumping /dev/hda3 (/ (dir home/mao)) to /dev/fd0
DUMP: Added inode 8 to exclude list (journal inode)
DUMP: Added inode 7 to exclude list (resize inode)
DUMP: Label: /
DUMP: Mapping (Pass I) [regular files]
DUMP: Mapping (Pass II) [directories]
DUMP: estimated 239 tape blocks.
DUMP: Volume 1 started with block 1 at: Fri Mar 28 10:54:03 2003
DUMP: dumping (Pass III) [directories]
DUMP: dumping (Pass IV) [regular files]
DUMP: Closing /dev/fd0
DUMP: Volume 1 completed at: Fri Mar 28 10:54:10 2003
DUMP: Volume 1 240 tape blocks (0.23MB)
DUMP: Volume 1 took 0:00:07
DUMP: Volume 1 transfer rate: 34 kB/s
DUMP: 240 tape blocks (0.23MB) on 1 volume(s)
DUMP: finished in 1 seconds, throughput 240 kBytes/sec
DUMP: Date of this level 0 dump: Fri Mar 28 10:54:02 2003
DUMP: Date this dump completed: Fri Mar 28 10:54:10 2003
DUMP: Average transfer rate: 34 kB/s
DUMP: DUMP IS DONE
[root@RH9Test root]#
```

图14.1 dump命令输出

dump命令有几个选项，表14.4列出了一些重要的dump命令选项。

表14.4 dump命令选项

选项	功能
0~9	转储级，0 = 完全备份，差异备份的转储号递增（如1、2、3），而增量备份转储号递减（如8、7、6）
A	建档备份目录表
f	将备份写入文件或设备
j level	压缩写入，要指定压缩级，如2或4
T date	指定日期，而不用/etc/dumpdates中显示的日期
u	备份成功后更新/etc/dumpdates

进行恢复

可以用两种方法从dump命令生成的备份恢复：交互式和直接恢复。无论哪种情况，都可以恢复整个备份，也可以只恢复需要的文件。

可以浏览dump命令备份的文件清单。如图14.2，下列命令列出备份mao主目录的文件：

```
# restore -tf /dev/fd0
```

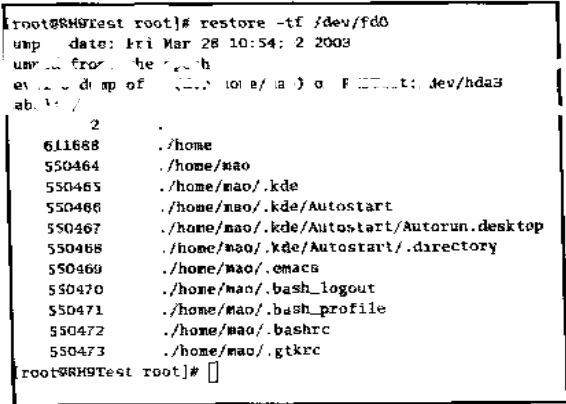


图14.2 备份文件

也可以用恢复方式搜索当前备份。如图14.3所示，-i选项进入交互方式，可以使用一些基本Linux导航命令。到本书编写时，restore交互方式不能使用ls命令的-l等选项。

restore命令有几个选项，表14.5列出了一些重要的restore命令选项。

表14.5 restore命令选项

选项	功能
-C	比较备份与当前文件
-f	指定文件
-i	允许备份的交互式恢复，恢复方式中有几个命令
-r	在全新格式化分区重建数据
-l	列出备份中的文件名

```

[root@RH9Test root]# restore -if /dev/fdd
restore > ls
:
home/

restore > cd /home/mao
restore > ls
./home/mao:
.bash_logout  .bashrc      .gtkrc
.bash_profile .emacs       .kde/

restore > help
Available commands are:
ls [arg] - list directory
cd arg - change directory
pwd - print current directory
add [arg] - add 'arg' to list of files to be extracted
delete [arg] - delete 'arg' from list of files to be extracted
extract - extract requested files
setmodes - set modes of requested directories
quit - immediately exit program
what - list dump header information
verbose - toggle verbose flag (useful with ls'')
prompt - toggle the prompt display
help or '?' - print this list
If no 'arg' is supplied, the current directory is used
restore > 

```

图14.3 交互式恢复

光碟/DVD备份命令

开始记录数据之前，要先检查Red Hat Linux能否识别这个硬件。这个工作通常很简单。然后可以生成适合光碟/DVD的文件，用相应命令记录。

检查硬件

向光碟与DVD记录数据之前，要先检查Red Hat Linux能否识别这个硬件。假设Red Hat Linux已经自动探测到正确的光碟，则可以用下列命令看到相应设置：

```

# cdrecord --scanbus
# dvdrecord --scanbus

```

Linux用SCSI盘进行刻录。但如果只有IDE盘，问题也不大，大多数情况下，Red Hat Linux默认自动配置SCSI仿真。换句话说，它能像SCSI盘一样写入IDE光碟或DVD刻录机。

利用这些命令，可以看到与scsibus相关的输出如下，尽管这个组件列为光碟（CD-ROM），但其像可写光碟（CD-RW）一样：

```
0,0,0 0) 'LG ' 'CD-RW CED-8083B ' '1.09' Removable CD-ROM
```

但是，如果遇到“No such file or directory”消息，则说明有问题。Red Hat可能无法对系统采用SCSI仿真。但我们可以自己进行SCSI仿真。首先在/etc/modules.conf中增加下列语句，忽略IDE设置：

```
options ide-cd ignore=ddb
```

如果可写光碟或DVD光碟在/dev/hdc之类的另一IDE设备上，则要相应替换。可以用dmesg | grep hd命令检查设备。用下列命令增加SCSI仿真模块，然后就可以了：

```
# modprobe -a ide-scsi
```

为了能够工作，要将相应SCSI设备文件（通常是/dev/scd0）链接到/etc/fstab中的/dev/cdrom。

例如，可以将/etc/fstab中的下列语句从第1版改成第2版：

```
/dev/cdrom /mnt/cdrom iso9660 noauto,owner,kudzu,rw 0 0
/dev/scd0 /mnt/cdrom iso9660 noauto,owner,kudzu,rw 0 0
```

也可以用下列命令直接链接设备文件：

```
# ln -s /dev/scd0 /dev/cdrom
```

如果遇到“File exists”错误，可以试试ls -l /dev/cdrom命令。Linux可能已经建立正确的链接。

建立映像

下一步要建立映像文件。无论录制到光碟或DVD，都可以用mkisofs命令生成映像文件。例如，假设要备份/home中的所有文件和目录，则可以使用下列命令，其中-r包括Rock Ridge扩展（支持UNIX文件系统），-J包括Joliet文件系统（使Microsoft操作系统中可以阅读这个文件），-T保留长文件名，-o表示输出：

```
# mkisofs -J -r -t -o newcd.iso /home
```

这样可能生成很大的文件。如果生成DVD的映像，则文件可能长达几个GB。最好检查这个文件的完整性。一种办法是像光碟与DVD一样装载映像文件。例如，对于光碟，下列命令可以将新生成的newcd.iso映像装载到/mnt/cdrom：

```
# mount -t iso9660 -o loop newcd.iso /mnt/cdrom
```

对于DVD，下列命令可以列出相应映像中的文件：

```
# isoinfo -i newdvd.iso -l
```

说明：DVD中刻录数据的命令还在开发之中，因此本章显示的命令可能发生改变。最新信息见dvdrttools项目的正式站点www.nongnu.org/dvdrttools。

刻录映像

现在要将映像刻录到空白的可写光碟中，可以使用cdrecord命令。对上节列出的项目，可以使用下列命令：

```
# cdrecord -v speed=2 dev=0,0,0 newcd.iso
```

-v选项可以看到Linux向光碟复制映像时发生的情形。如果遇到问题，则可以用这些消息诊断原因。图14.4显示了如何从第4章介绍的boot.iso文件生成红帽子安装引导光碟。从图中可以看出，运行这个命令时可以得到大量有用的消息。

向可写DVD复制映像时使用的命令也差不多：

```
# dvdrecord -v speed=1 -dao dev=0,1,0 newdvd.iso
```

其在Disk at Once（-dao）方式中以第一速度（speed = 1）刻录newdvd.iso映像，使用冗长方式，数据在一次操作中写入。

```
[root@RR0Test root]* cdrecord -v speed=2 dev=0,0,0 hant.iso
Cdrecord 2.0 (1686-pc-linux-gnu) Copyright (C) 1995-2002 Jrg Schilling
TOC Type: 1 = CD-ROM
scsiid: '0,0,0'
scsiid: 0 target: 0 lun: 0
Linux sg driver version: 3.1.24
Using libscg version 'schily 0.7'
cdrecord: Warning: using unofficial libscg transport code version (schily Red
Hat-scsi-linux-sg.c-1.75-RH '0(#)scsi-linux-sg.c 1.75 02/10/21 Copyright
1997 J. Schilling').
atapi: 1
Device type : Removable CD-ROM
Version : 0
Response Format : 1
Vendor info : 'LG '
Identifikation : 'CD-RW CED-8083B '
Revision : '1.09'
Device seems to be: Generic mmc CD-RW.
Using generic SCSI 3/mmc CD-R driver (mmc_cdr).
Driver flags : MMC SWABAUDIO
Supported modes: TAO PACKET SAO SAU/R96P SAO/R96R RAW/R16 RAW/R96P RAW/R96R
Drive buf size : 1024000 = 1000 KB
ELFO size : 4194304 = 4096 KB
Track 01: data 3 MB
Total size: 4 MB (00:24.13) = 1810 sectors
Lout start: 4 MB (00:26.10) = 1810 sectors
Current Secsize 2048
ATIP info from disk:
Indicated writing power: 5
Is not unrestricted
```

图 4.1 cdrecord 的输出

说明: 如果在GNOME中, 则插入空白可写光碟时, Nautilus自动打开burn:///窗口, 可以复制要写入光碟的文件和文件夹。其中有Write To CD按钮和易于理解的提示。

了解RAID

RAID有两个不同的含义, 冗余独立磁盘阵列和冗余廉价磁盘阵列, 但两者都不能准确描述RAID软件版本在Red Hat Linux中的工作方法。

冗余独立磁盘阵列表示RAID阵列中的每个磁盘在物理上独立。如果一个磁盘失败, 则阵列中的其他磁盘可以取代其功能。有几个RAID版本, 使Linux可以用其他工作盘, 重建任何故障盘上的数据。其中一个RAID版本包括两个独立硬盘, 存放一致信息。

RAID阵列中还可以包括多余硬盘。如果RAID 1或RAID 5硬盘中发生故障, 则Linux可以立即在空余盘上重建数据。

使用RAID阵列有三个好处:

高可用性 RAID阵列总是可以取得数据。只要有相应硬件, 甚至可以在计算机运行时改变硬盘。而在Red Hat Linux软件RAID阵列中, 是不可能这样的。

容错 对大多数硬件RAID阵列, 数据总是可以访问, 即使一个硬盘发生故障。可以对Red Hat Linux软件RAID阵列建立容错, 只需要在不同物理硬盘上配置阵列中的每个RAID分区。

故障切换 硬盘发生故障时, RAID系统可以自动切换到保留硬盘, 将数据自动传输到备份硬盘或分区。

RAID选项

Red Hat Linux中有三个RAID版本：RAID 0、RAID 1与RAID 5。简单地说，RAID 0可以加速硬盘访问，但没有容错功能。RAID 1用两个独立硬盘，存放一致信息，因此完全容错。RAID 5基于三个以上硬盘阵列，也提供容错。

第3章介绍Red Hat Linux安装时，详细介绍了基本RAID阵列的配置。

说明：尽管最新Linux内核也支持RAID 4，但Red Hat Linux安装程序不支持配置这个RAID版本。

RAID 4与RAID 5有一个差别。在RAID 4中，所有奇偶性信息存放在一个分区或一个硬盘中，而RAID 5中的奇偶性信息分布在阵列中所有硬盘上。

RAID 0

这个RAID级包括两个或多个分区或硬盘。虽然它们是分开的物理盘，但计算机可以使用每个盘上的缓冲区。这样，RAID 0可以加速硬盘读取和写入。

但是，RAID 0没有提供数据冗余度。换句话说，如果RAID 0中的任何分区或硬盘发生故障，则会丢失这个阵列中的所有数据。

说明：RAID 0也称为不带奇偶性的带区。

RAID 1

这个RAID级像个镜像，包括两个独立硬盘或分区，存放一致信息。两个独立硬盘使用RAID 1时，可以使用其中任一硬盘。一个硬盘发生故障时，另一个硬盘可以介入，而不会丢失数据。

RAID 1的缺点是数据写入磁盘时需要较长时间。对于RAID 1，要写入两个盘之后，数据写入才完成。RAID 1的硬件版本安全而昂贵，如果在所有计算机上实现RAID 1，则要购买和安装两倍的硬盘。

说明：RAID 1也称为“磁盘镜像”。

RAID 5

这一级RAID要求三个以上磁盘。RAID 5在阵列的所有磁盘之间均匀分配奇偶性信息。如果一个磁盘发生故障，则Linux可以从其余磁盘的奇偶性信息重新构造“丢失”的信息。尽管RAID 5磁盘失败时数据读取会减慢，但系统仍然继续运行。

如果RAID 5阵列中有多余硬盘，则Linux立即在这个多余磁盘上开始写丢失的信息。大多数情况下，这个RAID级通常更好，能保证数据完整性，而且保存奇偶性信息。

说明：RAID 5也称为“带奇偶性的数据带区”。

软件与硬件RAID

软件RAID可以在Red Hat Linux中配置，与硬件RAID稍有不同，因为它使用分区，而不用各个物理磁盘。如果在Red Hat Linux中使用RAID，则建议避免对单一RAID阵列使用同一硬盘上的分区，否则这个磁盘发生故障时，可能破坏RAID阵列中的所有数据。

有几个硬件RAID系统，只有它们自己的软件支持Linux。但是，本章介绍的原理适用于与Red Hat Linux相关的任何RAID版本。

专用RAID硬件可以保证，任一硬盘遇到任何致命的物理故障时，数据仍然能够保留。

生成RAID分区

安装Red Hat Linux之后，可以生成RAID分区。例如，假设有几个SCSI硬盘。我们在第一个SCSI硬盘/dev/sda上安装Red Hat Linux，另外三个硬盘用于一个RAID阵列：/dev/sdb、/dev/sdc与/dev/sdd。

说明：也可以在Red Hat Linux安装过程中生成RAID分区。详见第3章和第4章。

安装之后，生成新分区标准实用程序是fdisk。关于这个实用程序的详细信息，见第7章。

要在RAID中生成RAID阵列，就需要两个或多个长度大约相同的分区。如果阵列要在发生任何物理硬盘故障之后维持，则RAID阵列中每个分区应在不同的物理硬盘上。

有了RAID阵列的分区之后，可以用fdisk实用程序将分区变成适合RAID阵列的类型。例如，图14.5所示的命令将/dev/sdb1分区变成适合RAID阵列的类型。

```
root@RR19:~# fdisk /dev/sdb

Command (m for help): p

Disk /dev/sdb: 128 heads, 32 sectors, 512 cylinders
Units = cylinders of 4096 * 512 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1          205           300       196608    83  Linux
/dev/sdb2           52           102        104448    83  Linux
/dev/sdb3           1            51         104432    83  Linux

Partition table entries are not in disk order

Command (m for help): t
Partition number (1-4): 1
Hex code (type L to list codes): fd
Changed system type of partition 1 to fd (Linux raid autodetect)

Command (m for help):
```

图14.5 生成RAID分区

警告：不要对具有所需数据的分区改变文件类型，除非已经把数据备份到一个安全地址。用fdisk改变文件类型时，这个操作可能毁掉目前在该分区中存放的任何数据。

对RAID阵列生成磁盘和分区之后，就要将其格式化。第7章曾介绍过，要用mkfs -j partitiondevice命令，将新分区格式化为ext3文件系统。例如，下列命令可以格式化刚刚生成的分区：

```
# mkfs -j /dev/sdb1
```

重复这个步骤，生成需要的RAID分区。记住，要将RAID阵列中使用的所有分区格式化。

配置/etc/raidtab

有了需要的RAID分区之后，下一步是编辑RAID配置文件/etc/raidtab。这个文件很容易配置。下面几节介绍RAID 0、RAID 1与RAID 5阵列的配置例子。

/etc/raidtab文件中有几个命令，可以用于任何此类阵列，见表14.6。

表14.6 /etc/raidtab中的命令

命令	功能
raiddev	RAID设备文件名
raid-level	RAID阵列类型，通常是0、1、5
nr-raid-disks	对这个RAID阵列指定的磁盘数
nr-spare-disks	对这个RAID阵列指定的备份磁盘数
persistent-superblock	等于1时，Linux可以探测这个RAID阵列
chunk-size	要读写的数据量（KB）
parity-algorithm	RAID 5如何计算奇偶性
device	RAID分区的设备名
raid-disk	RAID阵列中对分区顺序指定的编号，从0开始
spare-disk	RAID阵列中对备份分区顺序指定的编号，从0开始

RAID 0 /etc/raidtab

RAID 0是不带奇偶性的磁盘带区。由于没有数据冗余度，因此这个RAID阵列不配置多余磁盘分区。下面的RAID 0 /etc/raidtab文件摘要配置的RAID阵列有两个分区，/dev/sda1与/dev/sdb1，具有大块长度（16KB），提高数据传输速度：

```
raiddev      /dev/md0
raid-level   0
persistent-superblock 1
chunk-size  16

nr-raid-disks   2
nr-spare-disks  0

device        /dev/sda1
raid-disk      0
device        /dev/sdb1
raid-disk      1
```

RAID 1 /etc/raidtab

RAID 1也称为磁盘镜像。由于其目标是冗余度，因此下列/etc/raidtab摘要中有一个多余磁盘分区。阵列中的两个分区是/dev/sda2与/dev/sdb2。多余分区是/dev/sdc2：

```
raiddev      /dev/md1
raid-level   1
persistent-superblock 1
chunk-size   4
```

```
nr-raid-disks 2
nr-spare-disks 1

device /dev/sda2
raid-disk 0
device /dev/sdb2
raid-disk 1
device /dev/sdc2
spare-disk 0
```

RAID 5 /etc/raidtab

RAID 5也称为带奇偶性的磁盘带区，可以使用大量磁盘或分区。由于它提供冗余度，因此下列/etc/raidtab摘要中有两个多余磁盘分区。阵列中的四个RAID分区是/dev/sda3、/dev/sdb3、/dev/sdc3与/dev/sdd3，两个多余磁盘分区是/dev/sde3与/dev/sdf3：

```
raiddev /dev/md2
raid-level 5
persistent-superblock 1
chunk-size 4

nr-raid-disks 4
nr-spare-disks 2

device /dev/sda3
raid-disk 0
device /dev/sdb3
raid-disk 1
device /dev/sdc3
raid-disk 2
device /dev/sdd3
raid-disk 3
device /dev/sde3
spare-disk 0
device /dev/sdf3
spare-disk 1
```

生成RAID设备

好了，基本完成了，我们已经生成了RAID阵列中所要的分区，设备为Linux RAID文件类型，已经格式化每个分区，已经在/etc/raidtab文件中设置了RAID阵列的配置。下面可以生成和格式化RAID设备。

例如，以上节生成的RAID 5配置为例。RAID设备文件为/dev/md2。我们要生成文件，然后将其格式化。然后可以在这个分区上装载所选文件系统。如果要让它在下次启动Linux时自动装载，则要将其加进/etc/fstab中。

下列命令生成和格式化RAID设备：

```
# mkraid -R /dev/md2
# mkfs -j /dev/md2
```


警告：mkraid -R raiddevice命令从与/etc/raidtab中raiddevice相关的所有分区删除所有数据。

装载RAID

这时我们已经可以将新的RAID阵列装载到所选文件系统。例如，如果要对主目录建立RAID，则可以将/home目录中的所有文件（包括隐藏文件）复制到另一地址，将新的RAID设备装载到/home，然后恢复文件，假设/tmp/home存在，则下列命令适用于刚刚生成的/dev/md2 RAID设备：

```
# cp -r /home /tmp/home
# mount /dev/md2 /home
# cp -r /tmp/home/home /
```

最后，为了保存改变，标注新设备，然后在/etc/fstab中增加相应项目。对上述目录和设备，首先要运行e2label /dev/md2 /home命令，然后在/etc/fstab中生成如下新项目：

```
LABEL=/home /home ext3 defaults 1 2
```

更新启动时，Linux自动在新的RAID设备/dev/md2中装载/home文件系统。

小结

数据很脆弱，备份很重要。选择数据保护策略之前，要先考虑各种灾害情形，标准情形包括丢失用户关键文件、完全删除数据、损坏计算机和电磁脉冲。

你的响应取决于要保护的计算机。如果是个人桌面用户，则主要灾难可能只是不方便。也许只要备份主目录中的文件就可以了。备份/etc中的配置文件可以在重装和重新配置Linux时节省时间。而负责整组计算机的管理人员则要更完整的备份。有时要有能够快速访问的介质，因为财务数据之类的信息对时间很敏感。

备份有三种不同类型：完全备份、递增备份和差异备份。完全备份就是完全备份整个计算机系统的所有文件。递增备份包括上次完全备份以来的所有数据。差异备份包括上次任何备份以来的所有数据。

备份可以使用各种介质，主要有磁带机和可写光碟/DVD。如果单个磁带和光碟无法提供足够的空间，则可以用“投币机”之类的设备将大量磁带和光碟集中到一台备份计算机上。

对磁带和其他介质，可以用tar、cpio、dump与restore之类的一般性备份和恢复命令。如果备份到光碟或DVD，则要用mkisofs命令生成要保存的文件的映像。然后可以用cdrecord与dvdrecord命令写入相应介质中。

另一种备份方法是RAID。RAID提供数据冗余度。换句话说，如果一个磁盘发生故障，则正确类型的RAID能保证不丢失数据。Red Hat Linux支持三种RAID：RAID 0不提供数据冗余度，RAID 1将一个硬盘镜像到另一磁盘，RAID 5也称为带奇偶性的带区。也可以使用硬件RAID。

在Red Hat Linux中，可以从一系列格式化为Linux raid autodetect文件类型的分区生成软件RAID阵列。在/etc/raidtab中配置设备之后，可以格式化和装载新的RAID设备。只要记住用e2label命令标注分区。还要在/etc/fstab中建档这个设备，以便下次启动时Linux将其自动装载。

第四部分要介绍如何在Red Hat Linux中管理X窗口。第15章详细介绍如何配置基本X客户机与X服务器，介绍配置工具和其影响的文件，然后介绍如何处理远程图形化应用程序。

第四部分 管理X窗口

第15章 管理X客户机与X服务器

新的Linux用户通常喜欢图形用户界面（GUI）。如果不是管理员，则用不上命令行的灵活性，而需要优化图形以设计飞机、生成电影、绘制统计数据，等等。一些普通用户希望更方便地从其他操作系统过渡。两个最重要的GUI是GNOME（见第16章）和KDE（见第17章）。

尽管大多数专业Linux管理员喜欢命令行界面，但他们应该认识到，许多用户希望使用GUI。为此，Red Hat Linux提供了XFree86页面（www.xfree86.org）开发的X客户机和X服务器系统。Linux GUI使用这种客户机/服务器结构。

安装Red Hat Linux时，也许你已经配置了X窗口和安装了GNOME或KDE。只要安装了基本X包，就可以用基本xf86config或redhat-config-xfree86工具在计算机上配置X窗口。

关键X窗口配置文件是XF86Config，在/etc/X11目录中，包括几个部分，将在下面详细介绍。还有另外几个重要的X窗口配置文件，可以帮助定制系统。本章介绍下列主题：

- 使用基本配置工具
- 了解配置文件
- 查错X窗口

使用基本配置工具

在计算机上配置X窗口时，要配置计算机的几个部分。不仅要配置图形，还要配置与图形屏幕互动的任何输入设备。这些组件包括：

- 显示器，包括水平与垂直频率、分辨率和刷新率
- 显示卡，指定内存量
- 鼠标或其他GUI指示设备
- 支持GUI的键盘

这些数据记录在/etc/X11/XF86Config中。可以直接编辑它。事实上，本章稍后将详细介绍这个文件。但是，这个文件使用的语言比较古怪，因此大多数人使用X窗口配置工具完成这个过程。

X窗口配置工具是redhat-config-xfree86。红帽子公司没有再提供原先的三个常用配置工具xf86config、Xconfigurator与XF86Setup。但是,由于xf86config放在X窗口包中,可以从www.xfree86.org安装,因此本章介绍这个工具。

如果Linux能探测到硬件,则可以用一个简单方法生成X窗口配置文件:用X -configure命令。

X窗口RPM包

通常,如果要安装多个包,则只要从第19章介绍的redhat-config-packages实用程序开始。其打开包组选择屏幕(见第3章),可以选择不同包组。但这个实用程序工作时要求事先安装一个GUI。

如果要安装X窗口RPM包,用rpm命令(见第10章介绍)安装base-x组件的包。这个组在第一张Red Hat Linux安装光碟/RedHat/base目录中的comps.xml文件内。为了方便起见,可以从Web上第5章了解这些包的详细清单,见Sybex公司站点www.sybex.com。

X窗口RPM包可能还不够,还要更多的GUI桌面支持包。第3章和第4章曾介绍过,GNOME 与KDE桌面要求不同的RPM包集合,可以从gnome-desktop与kde-desktop组的comps.xml文件中看到。

xf86config

传统Linux X配置工具xf86config使用命令行界面,不需要GUI即可启动,可以配置一些基本组件:鼠标、键盘、显示器和显示卡。

说明: xf86config不在Red Hat Linux 9中。但xf86config放在X窗口包中,可以从www.xfree86.org安装。

安装之后可以运行xf86config,其使用很简单,并且有可用显示卡的完整数据库。可以用下列步骤作为向导,因为其随选择硬件不同而不同:

1. 备份当前/etc/X11/XF86Config文件。如果这个过程中遇到问题,则可以从现有配置恢复。
2. 打开命令行界面,并用xf86config命令打开图15.1所示的入门窗口,其底部有个SuperProbe的引用。对于Red Hat Linux,其功能已经换成ddcprobe命令。按Enter键继续。

```
This program will create a basic XF86Config file, based on menu selections you
make

The XF86Config file usually resides in /usr/X11R6/etc/X11 or /etc/X11. A sample
XF86Config file is supplied with XFree86, it is configured for a standard
VGA card and monitor with 640x480 resolution. This program will ask for a
pathname when it is ready to write the file.

You can either take the sample XF86Config as a base and edit it for your
configuration, or let this program produce a base XF86Config file for your
configuration and fine-tune it.

Before continuing with this program, make sure you know what video card
you have, and preferably also the chipset it uses and the amount of video
memory on your video card. SuperProbe may be able to help with this.

Press enter to continue, or ctrl-c to abort
```

图15.1 xf86config入门窗口

3. 如图15.2所示, 后面的问题可以选择基本鼠标协议、在双键鼠标上仿真三键和指定设备名。在另一虚拟控制台中运行`ls -l /dev/mouse`命令(见第11章)。如果`/dev/mouse`链接实际鼠标端口, 则这个设备就足够了。按Enter键继续。

```

1  Microsoft compatible (2-button protocol)
2  Mouse Systems (3-button protocol)
3  Bus Mouse
4  PS/2 Mouse
5  Logitech Mouse (serial, old type, Logitech protocol)
6  Logitech MouseMan (Microsoft compatible)
7  MM Series
8  MM HitTablet
9  Microsoft IntelliMouse

If you have a two-button mouse, it is most likely of type 1, and if you have
a three-button mouse, it can probably support both protocol 1 and 2. There are
two main variations of the latter type: mice with a switch to select the
protocol, and mice that default to 1 and require a button to be held at
boot-time to select protocol 2. Some mice can be convinced to do 2 by sending
a special sequence to the serial port (see the ClearDTR/ClearRTS options).

Enter a protocol number: 4

If your mouse has only two buttons, it is recommended that you enable
Emulate3Buttons.

Please answer the following question with either 'y' or 'n'. Do you want to
enable Emulate3Buttons? y

Now enter the full device name that this mouse is connected to, for example
/dev/ttyO. If you are pressing this on a serial port, the default is /dev/mouse.

Mouse device: 

```

图15.2 配置鼠标

说明: 根据选择的鼠标协议, 可能出现一个或两个其他问题, 如是否要对Logitech鼠标启用ChordMiddle特性, 或是否要保证鼠标系统不默认为Microsoft兼容方式。更多信息见www.xfree86.org的文档部分。

4. 然后可以选择大约25种基本键盘。进行选择, 然后按Enter键继续。
5. 这时可以选择与键盘相关联的语言类型, 包括来自阿拉伯和越南的语言。进行选择, 然后按Enter键继续。然后可以输入特殊的配置名。按Enter键继续, 可以看到如下消息:

```
Please answer the following question with either 'y' or 'n'. Do you want to
select additional XKB options (group switcher, group indicator, etc)?
```

6. XKB选项主要适用于非英语用户, 特别是多字母键盘。但是, 这方面缺乏好的文档, 只有Ivan Pascal的资料放在www.tsu.ru/~pascal/en/xkb站点。如果使用单一语言键盘, 则输入并按Enter键继续。
7. 然后可以设置显示器规范。准备好显示器文档, 包括相应的水平与垂直同步范围。在提示下进行相应输入。遇到疑问时, 选择可用范围中的最低值。输入一个标识符, 然后按Enter键继续。
8. 现在可以配置显示卡。准备好卡文档, 如图15.3。也可以输入y查阅可用显示卡清单。如果你的卡在清单中, 则xf86config会处理所需的配置细节。
9. 显示卡有七百多种, 寻找显示卡并输入相应数字或输入9继续。确认卡的定义, 然后按Enter键继续。

```

Now we must configure video card specific settings. At this point you can
choose to make a selection out of a database of video card definitions.
Because there can be variation in Ramdac and clock generators even
between cards of the same model, it is not sensible to blindly copy
the settings (e.g. a Device section). For this reason, after you make a
selection, you will still be asked about the components of the card with
the settings from the chosen database entry presented as a strong hint.

The database entries include information about the chipset, what driver to
run, the Ramdac and ClockChip, and comments that will be included in the
Device section. However, a lot of definitions only hint about what driver
to run (based on the chipset the card uses) and are untested.

If you can't find your card in the database, there's nothing to worry about.
You should only choose a database entry that is exactly the same model as
your card, choosing one that looks similar is just a bad idea (e.g. a
GemStone Snail 64 may be as different from a GemStone Snail 64+ in terms of
hardware as can be).

Do you want to look at the card database? █

```

图15.3 xf86config与显示卡

10. 在提示下输入显示卡的内存量，输入一个标识符，然后按Enter键继续。
11. 现在可以对显示器/显示卡系统选择不同分辨率。例如，图15.4中，选项1、2和3可以改变8位、16位、24位颜色相关的默认分辨率，如果选择选项4，则跳到第13步。

```

For each step, a list of modes is shown. The default
resolution that the server will start with will be the first listed
mode that can be supported by the monitor and card.
Currently it is set to

"640x400" for 8-bit
"640x480" for 16-bit
"640x480" for 24-bit

Modes that cannot be supported due to monitor or clock constraints will
be automatically skipped by the server:

1. Change the modes for 8-bit (256 colors)
2. Change the modes for 16-bit (32K/64K colors)
3. Change the modes for 24-bit (24-bit color)
4. The modes are OK, continue

Enter your choice: 3

Select modes from the following list:

1. "640x400"
2. "640x480"
3. "800x600"
4. "1024x768"
5. "1280x1024"
6. "320x200"
7. "320x240"
8. "400x300"
9. "1152x864"

```

图15.4 xf86config分辨率

12. 选择与颜色设置相关的默认分辨率。然后可以在需要时选择“虚拟屏幕”，以便配置大于显示器处理能力的分辨率（如1800×1400）。回到第11步。
13. 选择默认颜色深度，标准选项为1、4、8、16、24和32位。
14. 如果对改变感到满意，则可以让xf86config将结果写入/etc/X11/XF86Config。从图15.5可以看出，还有其他选项。

```

I am going to write the XF86Config file now. Make sure you don't accidentally
overwrite a previously configured one.

Shall I write it to /etc/X11/XF86Config? n

Please answer the following question with either 'y' or 'n'.
Shall I write it to the default location, /usr/X11R6/etc/X11/XF86Config? n

Do you want it written to the current directory as 'XF86Config'? y

File has been written. Take a look at it before running 'startx'. Note that
the XF86Config file must be in one of the directories searched by the server
(e.g. /etc/X11) in order to be used. Within the server press
ctrl, alt and '+' simultaneously to cycle video resolutions. Pressing ctrl,
alt and backspace simultaneously immediately exits the server (use if
the monitor doesn't sync for a particular mode).

For further configuration refer to the XF86Config(5) manual page.

[root@RH9Test root]#

```

图15.5 xf86config将结果写入配置文件

说明：记住，Linux是大小写相关的。xf86config实用程序修改X窗口配置文件XF86Config，两者不是一回事。

redhat-config-xfree86

Red Hat Linux中配置X窗口的工具是redhat-config-xfree86。大多数情况下，甚至可以在标准命令行界面中运行这个工具，它会探测显示器与图形卡，打开带VESA界面的基本对话框。

说明：VESA（显示电子标准协会）开发的基本图形界面，相关的一般性设置也称为SVGA。

redhat-config-xfree86命令可以探测硬件，包括总体显示、显示器和显示卡部分。

探测硬件

redhat-config-xfree86打开显示设置窗口之前，先运行ddcprobe命令。也可以自己运行ddcprobe命令。图15.6显示了在我的桌面计算机上的结果。

```

[root@RH9Test root]# ddcprobe

Videocard DDC probe results
Description: Intel Corporation 810 Graphics Controller
Memory (MB): 1

Monitor DDC probe results
ID: SAM415b
Name: S/M 955DF
Horizontal Sync (kHz): 30-85
Vertical Sync (Hz): 50-160
Width (mm): 360
Height (mm): 270
[root@RH9Test root]#

```

图15.6 ddcprobe探测显示器与显示卡

总体显示

打开redhat-config-xfree86时，可以看到显示设置窗口，如图15.7。Display标签可以选择分辨率与颜色深度，其中的设置基于显示卡的功能，反映显示器的极限。

屏幕上方显示计算机上打开的GUI应用程序，可以看到应用程序在显示器中的样子。如果改变分辨率设置，则应用程序周围的虚线相应改变。

分辨率表示显示卡发送到显示器的点数，采用水平X垂直格式。例如分辨率800×600表示水平方向800点，垂直方向600点。其他分辨率清单可以单击Resolution下拉箭头打开。

颜色深度设置表示每一点的颜色数。例如，16位颜色表示每一点的颜色数为 $2^{16} = 65536$ 。其他颜色深度清单可以单击Color Depth下拉箭头打开。

显示卡

回到redhat-config-xfree86显示设置窗口，单击Advanced标签。如图15.8所示，屏幕下半部分包括显示卡设置（探测的显示内存已经正确）。

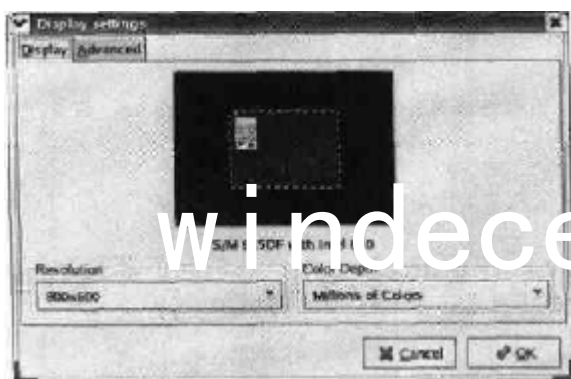


图15.7 Display标签

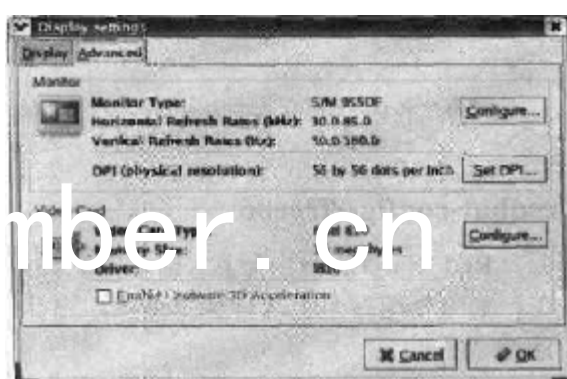


图15.8 Advanced标签

可以进一步配置显示卡。单击Advanced标签Video Card部分的Configure，进入显示卡设置窗口，如图15.9。

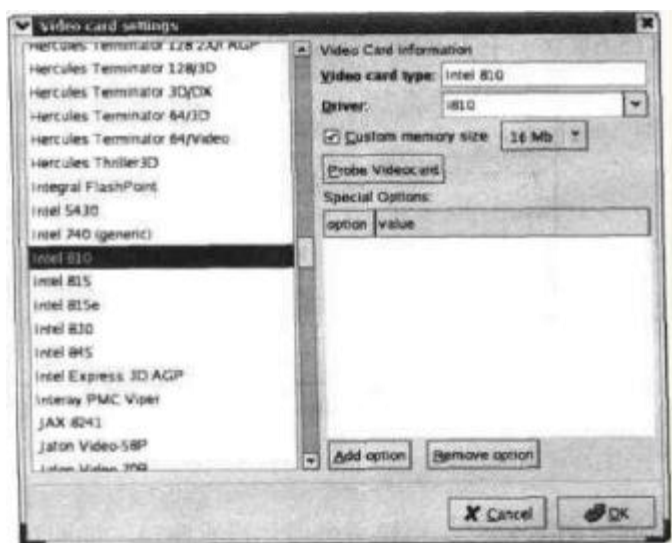


图15.9 显示卡设置

可以选择六百多种显示卡机型与版本。这时右上角自动出现显示卡类型与驱动程序。有时还可以在右下角看到特殊选项命令。

也可以单击Probe Videocard按钮,通常redhat-config-xfree86能够探测显示卡和自动选择相应驱动程序。

如果没有看到符合显示卡机型与版本的显示卡,则有几个办法:

- 选择VESA Driver (Generic)卡类型,指定标准设置(SVGA)和vesa驱动程序,适用于近几年建立的大多数显示卡。
- 选择Unsupported VGA Compatible卡类型,对系统指定vga驱动程序。
- 选择清单顶部的Custom,可以将显示卡厂家或第三方的Linux驱动程序加进显示模块目录/usr/X11R6/lib/modules/drivers。

使用机型特定或一般性驱动程序时,一定要选择Custom Memory Size设置。如果其不符合显示卡实际图形内存量,则要进行修改。

几个显示卡可以配置不同选项,如加速、深度与方向。可以使用Add Option按钮完成这个工作。进行选择,然后单击OK按钮继续。

说明: 如果需要关于可用选项的更多信息,可以取得显示卡机型与版本。移到www.xfree86.org/4.3.0/RELNOTES.html页面,并检查Video Drivers部分,可以看到显示卡机型与版本的链接。这里还记录了显示卡需要的XF86Config文件选项。

回到显示设置窗口Advanced标签看看Enable Hardware 3D Acceleration复选框。如果你的显示卡有这个三维加速功能,则应激活这个复选框。下面看看显示器。

显示器

redhat-config-xfree86工具还可以配置显示器的X服务器设置。打开显示设置窗口Advanced标签,然后单击Configure按钮打开显示器设置窗口,如图15.10。

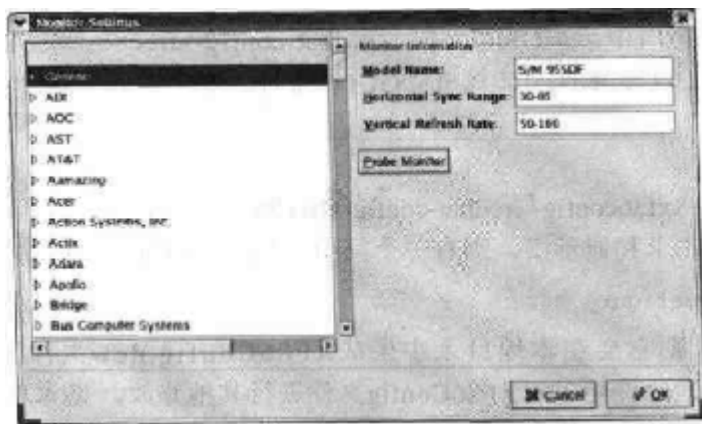


图15.10 显示器设置窗口

可以用redhat-config-xfree86配置100多个厂家的显示器。如果看到你的显示器厂家,单击厂家名旁边的箭头,打开这个厂家的一系列机型。

也可以单击**Probe Monitor**按钮寻找准确匹配。

如果找不到准确匹配, 则可以使用大量一般性显示器, 图15.11显示了其中一部分。可以看出, 其中还有便携电脑的设置。

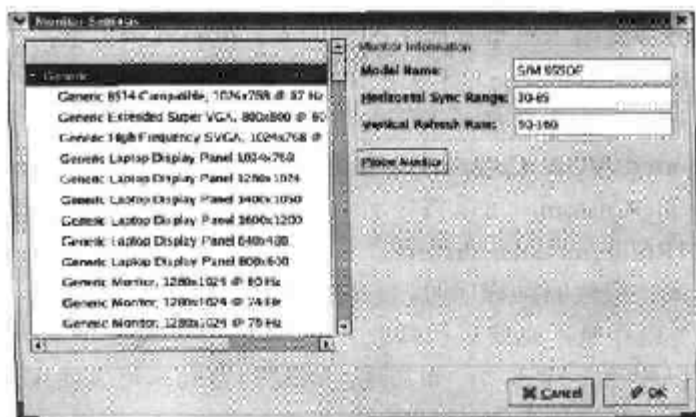


图15.11 一般性显示器设置

尽管可以定制显示器的水平同步范围和垂直刷新率, 但一定要格外小心。检查显示器文档。如果选择的数值太大, 则可能超过显示器能力, 把显示器破坏。尽管许多显示器能够防止这种过载, 但为什么要对新买的显示器或便携电脑屏幕冒这个险呢?

完成设置之后, 单击**OK**按钮回到**Advanced**标签。单击**Set DPI**按钮打开显示器**DPI**设置窗口, 如图15.12。

可以看出, 可以定制显示器屏幕上的图形尺寸。利用下拉框, 可以设置显示器宽度与高度(毫米或英寸)。如果单击**Look Up From Monitor**按钮, 则可以得到当前设置。进行所要改变, 然后单击**OK**按钮继续。

在显示设置窗口中单击**OK**按钮时, **redhat-config-xfree86**工具将改变保存到**/etc/X11/XF86Config**中。下次登录这个计算机的GUI界面时, 这个设置生效。

自动X配置

如果你不喜欢**xf86config**与**redhat-config-xfree86**, 则还有另一个选择。如果**XFree86**服务器能够探测到显示卡和显示器, 则有一个简单方法。可以使用下列命令:

```
# X -configure
```

如果成功, 则它会在本地目录中生成**XF86Config.new**文件。备份当前**/etc/X11/XF86Config**文件, 也许可以对**XF86Config**文件进行其他修改, 见本章稍后介绍。准备好之后, 用**XF86Config.new**文件覆盖**/etc/X11/XF86Config**文件。然后用**startx**命令测试结果。

switchdesk

在Red Hat Linux中, 默认桌面是GNOME。如果使用多个不同桌面, 则**switchdesk**实用程序可以方便地启动不同GUI。如果从GUI中运行**switchdesk**, 则可以看到图15.13所示的桌面切换器窗口。

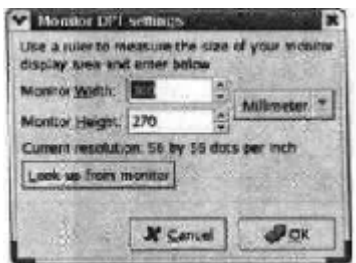


图15.12 显示器DPI设置窗口



图15.13 桌面切换器

桌面切换器窗口显示安装的GUI，可以在GNOME与KDE之类安装的桌面环境之间来回切换。

也可以在命令行界面中使用switchdesk。它很简单，例如，如果要用KDE作为默认桌面，则可以运行下列命令：

```
# switchdesk KDE
```

Linux GUI桌面

有几个Linux GUI桌面。switchdesk可以使用的一些主要选项如下：

- GNOME是默认Linux GUI桌面，表示GUI网络对象模型环境。
- KDE是另一个主要Linux GUI桌面，表示K桌面环境。
- fvwm（与fvwm95）窗口管理器是GNOME与KDE之前的标准Linux GUI桌面，由于它只需要少量内存，因此在内存稀缺时适用。
- Enlightenment是各大Linux GUI窗口管理器中最可配置的。
- twm窗口管理器非常简单，在Red Hat Linux中包括一个控制台屏幕。它也作为故障保险桌面环境，具有基本工具和程序。
- WindowMaker窗口管理器更加直观，大致像NeXTStep操作系统的GUI。

改变显示管理器

显示管理器是个登录管理器，提供用户登录Linux计算机时的图形界面。显示管理器有三个选项，其中两个与GNOME与KDE有关，第三个是一般性X窗口显示管理器。

可以在/etc/X11/prefdm中选择喜欢的显示管理器。关键变量是这个文件中的大约10行：

```
preferred=
```

根据显示管理器情况，可以将优选变量设置为下面的值：

```
preferred=gdm
preferred=kdm
preferred=xdm
```

分别选择GNOME显示管理器、KDE显示管理器和X显示管理器。下面一一介绍。

GNOME显示管理器

GNOME显示管理器如图15.14。



图15.14 GNOME显示管理器

除了简单登录界面（提示输入口令）外，还有三个菜单：

Language 如果安装了相应语言包，则可以单击这个菜单，选择会话语言。

Session 打开一个菜单，可以选择桌面。

Reboot 在重新启动计算机之前提示确认。

Shutdown 关闭计算机之前提示确认。

可以配置GNOME桌面管理器。打开一个GUI并运行`gdmsetup`命令，打开一个菜单，其中有五个标签，如图15.15。

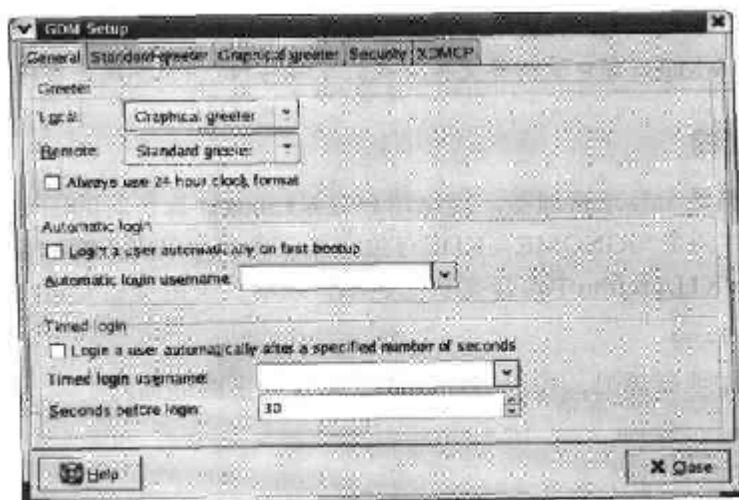


图15.15 GNOME桌面管理器设置窗口

这些标签可以用几种方法定制GNOME显示管理器：

- **General**标签可以配置本地和远程登录参数。
- **Standard Greeter**标签可以控制这个界面的样子，通常用于远程图形连接。
- **Graphical Greeter**标签可以选择图形化gdm界面的几个主题，可以安装红帽子公司开发的新主题、GNOME项目或Ximian之类第三方主题。
- **Security**标签可以规定根登录与远程登录和可用登录菜单。
- **XDMCP**标签可以配置这个显示管理器如何与远程用户通信。**XDMCP**指X显示管理器控制协议。

第17章将会介绍，可以通过**KDE**控制中心登录管理器设置配置**KDE**显示管理器。**X**显示管理器（**xdm**）没有相应的配置工具，但在`/etc/X11/xdm`目录中包括配置文件。

KDE显示管理器

也可以配置**KDE**显示管理器，如图15.16。这个显示管理器还有简单的登录界面和几个选项：

Session Type 可以选择不同桌面。

Go 发送输入的用户名和口令，以便验证。

Clear 删除用户名和口令框中的项目。

Menu 可以重新启动X服务器。

Shutdown 打开一个窗口，可以发送Turn Off Computer（poweroff）或Restart Computer（reboot）命令。

X显示管理器

最后，还可以配置**X**显示管理器，如图15.17。这是最简单的登录界面，只能登录到计算机。



图5.16 KDE显示管理器



图5.17 X显示管理器

定义

使用X窗口和GUI界面时，要记住几个定义。其中一些术语是密切相关和互换使用的，很容易引起混淆。

显示管理器 登录的图形界面。常用显示管理器包括**X**显示管理器（**xdm**），**GNOME**显示管理器（**gdm**）和**KDE**显示管理器（**kdm**）。

桌面 集成一系列工具和程序的窗口管理器。两个最常用的桌面是GNOME与KDE。GNOME桌面不一定要包括GNOME窗口管理器，例如，旧版Red Hat Linux在GNOME桌面中配置Enlightenment窗口管理器。

图形用户界面 (GUI) 用户与计算机互动的图形界面，组合X服务器和X客户机。

窗口管理器 特殊的X客户机，控制GUI窗口的外观和界面。

X客户机 GUI中运行的应用程序，可以从本地或远程计算机上运行。

X服务器 在本地计算机上生成GUI的驱动程序和程序。

了解配置文件

Linux X窗口有几个重要的配置文件和可执行程序。大多数人都知道从命令行界面启动X窗口的命令：

```
# startx
```

这个程序引用/etc/X11/xinit与/usr/X11R6/bin目录中的其他程序和配置文件。/etc文件可以对各个用户定制，使用用户主目录中的隐藏文件。

最重要的X窗口配置文件是/etc/X11/XF86Config 本节稍后将介绍这个文件。

startx

可以用三种方法打开Linux GUI界面。可以编辑/etc/inittab中的id变量，在引导Linux时在运行级5中启动，也可以用int 5命令从文本控制台进入运行级5（关于/etc/inittab与init的更少信息，见第11章）。这些方法都可以进入前面介绍的图形登录界面的。

第三种方法是运行startx命令，实际上是/usr/X11R6/bin目录中的一个可执行文件。可以在任何文本编辑器中打开startx。这个文件的开头如图15.18。

```
# This is just a sample implementation of a slightly less primitive
# interface than xinit. It looks for user xinitrc and xserverrc
# files, then system xinitrc and xserverrc files else lets xinit choose
# its default. The system xinitrc should probably do things like check
# for Xresources files and merge them in, startup up a window manager,
# and pop a clock and several xterms
#
# Site administrators are STRONGLY urged to write nicer versions
#
# $XFree86 xc/programs/xinit/startx.cpp,v 3.14 2002/01/28 18:19:50 tse Exp $

userclientrc=$HOME/.xinitrc
userserverrc=$HOME/.xserverrc
sysclientrc=/etc/X11/xinit/xinitrc
sysserverrc=/etc/X11/xinit/xserverrc
defaultclient=/usr/X11R6/bin/xterm
defaultserver=/usr/X11R6/bin/X
defaultclientargs=""
defaultserverargs=""
clientargs=""
serverargs=""
```

图15.18 startx文件

可以看出, 这个脚本包括几个变量, 首先查找请求用户主目录中的`.xinitrc`与`.xserverrc`文件。如果找不到这些文件, 则使用`/etc/X11/xinit`目录中的默认值。

说明: Red Hat Linux系统中默认不存在`/etc/X11/xinit/xserverrc`文件, `/etc/inittab`脚本用`X :0`命令在第一个可用的图形控制台中启动X服务器。

`defaultclient`与`defaultserver`是默认X客户机和默认X服务器, 默认`xterm`客户机用于`switchdesk`指定`twm`为默认桌面时。其他变量故意空着, 如果你对编程代码熟悉, 则可以看到这些变量如何赋值。

更多X窗口

可以本地或远程运行不同X窗口。第3章曾介绍过, X窗口有自己的虚拟控制台。如果在文本屏幕中, 运行GUI时, 可以用`Ctrl+Alt+F7`命令访问GUI。

如果有足够的内存, 则可以在本地计算机上运行第二个X窗口。`startx -- :1`命令打开第二个GUI, 可以用`Ctrl+Alt+F8`命令访问。

如果要从另一台计算机访问GUI应用程序, 则可以将计算机设置成从远程计算机接受X命令。关掉防火墙, 并用`xhost +computername`或`xhost +remoteipaddr`命令允许远程计算机登录(`remoteipaddr`表示远程计算机IP地址)。以后可以登录远程计算机和启动`gimp --display yzumpaddr:0.0`或`xclock --display yzumpaddr:0.0`之类的命令。

`display`开关不一致, 对`xclock`之类的命令, 只要一个连字符(`--display`), 而对`gimp`之类命令, 则要两个连字符(`--display`)。如果不能肯定, 则可以用`-h`开头运行命令, `xclock -h`或`gimp -h`。

/etc/X11

`/etc/X11`目录中包含几个重要配置文件和目录。表15.1列出了这些文件和目录。

表15.1 /etc/X11文件和目录

文件和目录	描述
<code>applink</code>	这个目录链接GUI开始菜单中出现的应用程序
<code>desktop-menus</code>	这个目录具有各种默认GUI菜单的设置
<code>fs</code>	这个目录具有字体服务器配置
<code>gdm</code>	这个目录具有GNOME显示管理器配置文件
<code>lbxproxy</code>	远程客户机的目录, 其使用X服务器的低带宽扩展(LBX)
<code>prefdm</code>	这个文件选择优选显示管理器
<code>proxymngr</code>	这个目录具有代理管理器使用的配置
<code>rstart</code>	这个目录具有远程启动客户机, 基于rsh
<code>serverconfig</code>	X服务器的配置设置目录
<code>starthere</code>	具有基本X桌面设置的目录
<code>sysconfig</code>	具有gnome-lokkit配置文件的目录
<code>twm</code>	这个目录具有twm配置文件, <code>system.twmrc</code>
<code>X</code>	链接X服务器应用程序的文件
<code>xdm</code>	这个目录具有X显示管理器配置文件
<code>XF86Config</code>	主X服务器配置文件

(续表)

文件和目录	描述
xinit	这个目录具有startx调用的默认X配置文件，在相应主目录中没有等价文件时使用
xkb	键盘配置目录
Xmodmap	键盘的默认配置文件
Xresources	这个配置文件调用登录屏幕的字体
xserver	这个目录具有SecurityPolicy配置文件
xsm	这个目录配置X会话管理器

本地配置文件

可以在用户主目录中设置X窗口配置文件。前面曾介绍过，startx从其中的两个文件`~/.xinitrc`与`~/.xserverrc`寻找启动Linux X窗口的设置。点号在主目录中隐藏这些文件名。

说明：第6章曾介绍过，可以用`ls -la`命令浏览任何目录中的隐藏文件。

前面曾介绍过，红帽子公司不用`xserverrc`文件，因此关键配置文件是`~/.xinitrc`，它也调用主目录中另外几个文件。

说明：现在，符号`~`（~）表示当前用户的家目录。

其他关键文件是`~/.Xclients`与`~/.Xclients-default`，switchdesk修改这些文件，使startx知道所要的桌面。如果了解这些文件如何工作，可以自己阅读这些文件。用前面介绍的switchdesk命令设置不同的默认桌面，看看对`~/.Xclients-default`有什么影响。

xinitrc

startx命令启动X服务器时，要调用字体、键盘设置和默认X客户机。

xinitrc文件是可执行shell脚本，可以使用/etc/X11/xinit目录中的默认，也可以进行定制，将其名称改成。xinitrc存放在自己的主目录中。下面详细分析默认xinitrc文件：

```
#!/bin/sh
# (c) 1999-2003 Red Hat, Inc.
userresources=$HOME/.Xresources
usermodmap=$HOME/.Xmodmap
userxkbmap=$HOME/.Xkbmap

sysresources=/etc/X11/Xresources
sysmodmap=/etc/X11/Xmodmap
sysxkbmap=/etc/X11/Xkbmap
```

前几行表示脚本余下部分需要的其他配置文件。稍后将会看到，如果没有user*变量文件，则xinitrc使用sys*文件：

```
# merge in defaults
if [ -f "$sysresources" ]; then
    xrdp -merge "$sysresources"
fi
```



```
if [ -f "$userresources" ]; then
    xrdp -merge "$userresources"
fi
```

这几行开始采用\$sysresources文件/etc/X11/Xresources。如果有有效\$userresources文件（~/Xresources），则组合每个文件中的设置：

```
# merge in keymaps
if [ -f "$sysxkbmap" ]; then
    setxkbmap `cat "$sysxkbmap"`
    XKB_IN_USE=yes
fi

if [ -f "$userxkbmap" ]; then
    setxkbmap `cat "$userxkbmap"`
    XKB_IN_USE=yes
fi
```

这儿行与上一段作用相同，但适用于指定的键盘映射文件，基于Xkbmap。但是，Red Hat Linux中通常没有这个文件，因此将其忽略。在xinitrc中，后面的段与Sun系统公司X服务器有关。Red Hat Linux不用，因此将其注释。后面的内容如下：

```
# xkb and xmodmap don't play nice together
if [ -z "$XKB_IN_USE" ]; then
    if [ -f "$sysmodmap" ]; then
        xmodmap "$sysmodmap"
    fi

    if [ -f "$usermodmap" ]; then
        xmodmap "$usermodmap"
    fi
fi

unset XKB_IN_USE
```

这一段检查/etc/X11/xinit中的Xmodmap文件或主目录中的隐藏版本。如果存在，则用其代替前面所述的Xkbmap文件。但要记住，Red Hat Linux中通常没有这个文件。

```
# run all system xinitrc shell scripts.
for i in /etc/X11/xinit/xinitrc.d/* ; do
    if [ -x "$i" ]; then
        . "$i"
    fi
done
```

这一段运行指定目录/etc/X11/xinit/xinitrc.d中的基本shell脚本。这些脚本可以包括xinput与xmbind之类的文件，见稍后介绍。

```
if [ -f $HOME/.Xclients ]; then
    [ -x /usr/bin/ssh-agent -a -z "$SSH_AGENT_PID" ] && \
    exec ssh-agent $HOME/.Xclients || \
```

```

        exec $HOME/.Xclients
    elif [ -f /etc/X11/xinit/Xclients ]; then
        [ -x /usr/bin/ssh-agent -a -z "$SSH_AGENT_PID" ] && \
            exec ssh-agent /etc/X11/xinit/Xclients || \
            exec /etc/X11/xinit/Xclients
    else

```

这些命令检查Xclients文件中的默认客户机，并建立SSH的验证主体（如果前面已经配置）。详见第23章。

```

        xclock -geometry 100x100-5+5 &
        xterm -geometry 80x50-50+150 &
        if [ -x /usr/bin/netcape -a -f /usr/share/doc/HTML/index.html ]; then
            netcape /usr/share/doc/HTML/index.html &
        fi
        if [ -x /usr/X11R6/bin/fvwm2 ]; then
            exec fvwm2
        else
            exec twm
        fi
    fi

```

如果没有Xclients文件，则这些命令建立默认客户机。注意这一段包括Netscape，xclock光碟中不再提供。这一段还使用xclock和xterm，前者是个一般化Linux GUI时钟，后者是个一般化命令行界面窗口。

也可以在主目录中生成自己的.xinitrc文件。一定要用相应chmod命令使用这个文件成为可执行文件。例如，可以在xterm文件中增加下列信息：

```

#!/bin/bash
xclock &
xterm &
gimp &
exec twm

```

这个文件从#!/bin/bash开始，假设后面的命令基于bash shell。其余命令启动标准Linux GUI时钟（xclock）、基本命令行界面窗口（xterm）和The GIMP（gimp），这是个GNU图形操纵程序。最后，代码启动一个简单窗口管理器界面twm（twm），结果用twm启动程序，如图15.19。

Xresources

用户主目录中通常有个.Xresources文件，以及/etc/X11目录中的默认Xresources文件。默认文件用一系列步骤寻找优选桌面。一般来说，如果没有GNOME或KDE，则Xresources寻找主目录中的.wm_style文件，可能调用旧式窗口管理器。

但这些是细节问题，主目录节中的.Xresources文件设置GUI界面中基本X客户机的颜色模式。



图15.19 .xinitrc文件中的操作

XF86Config

`/etc/X11/XF86Config` 文件中包含X服务器的配置。启动Linux GUI时，通过这个文件配置分辨率、音调、图形驱动程序、显示器、键盘、鼠标或其他指示设备的基本设置。这个文件包括几大部分，见下面介绍。

文件第一行表示是否通过Anaconda生成XF86Config:

```
# XFree86 4 configuration created by pyxf86config
```

或redhat-config-xfree86

```
# XFree86 4 configuration created by redhat-config-xfree86
```

说明: 在Red Hat Linux 8.0之前，默认X服务器配置文件是`/etc/X11/XF86Config-4`。这里之所以增加-4，是因为Red Hat Linux 8.0支持XFree86服务器的两个不同版本3.a.b与4.x.y。由于Red Hat Linux现在已经删除v3.a.b版本，因此也就取消了一4后缀。XFree86 4.x.y服务器包括除最老的图形卡以外所有图形卡的数据。

表15.2列出了XF86Config中的许多指令，下面几字节介绍XF86Config文件中可以看到的典型段落。

表15.2 `/etc/X11/XF86Config`文件中的常用指令

指令	描述
BoardName	指定对设备所赋名称，如显示卡
BusID	指定PCI或AGP显示卡位置（如果Linux没有探测到）
DefaultDepth	指定每个像素的默认颜色位数，通常为1、4、8、16、24或32
DisplaySize	列出水平与垂直屏幕长度（毫米）
Driver	对组件指定特定驱动程序
EndSection	表示一组命令结束
EndSubSection	表示一组命令小节结束

(续表)

指令	描述
FontPath	指定X字体位置, 可以指定特定文件, 也可以指定本地字体服务器的TCP/IP端口, 通常用unix/:7100
HorizSync	显示允许的显示器水平同步率范围
Identifier	允许命令组之间互动
InputDevice	可以指键盘和鼠标、触摸屏之类指示设备
Load	增加指定模块
Model Name	表示特定模型名, 和VendorName共用
Modes	指定允许的显示器分辨率
Module	列出X服务器要装入的服务器和字体模块
Monitor	指定与一个屏幕相关的显示器标识符
Option	表示不同硬件组件的许多选项之一
RgbPath	文本格式的数据库文件, 指定不同颜色的红、绿、蓝值
Section	表示一组命令的开头, 要有标号和相应的EndSection
SubSection	表示段中一组命令的开头
VendorName	指定厂家名
VertRefresh	显示允许的显示器垂直刷新率范围
Video Ram	表示显存容量

ServerLayout

ServerLayout段关联到不同输入设备与屏幕, 包括显示器与显示卡的组合配置。这里的例子汇总了计算机上的配置:

```
Section "ServerLayout"
    Identifier      "Default Layout"
    Screen 0       "Screen0" 0 0
    InputDevice    "Mouse0" "CorePointer"
    InputDevice    "Keyboard0" "CoreKeyboard"
    InputDevice    "DevInputMice" "AlwaysCore"
EndSection
```

换句话说, 这个特定ServerLayout段组合了Red Hat Linux安装程序Anaconda配置的Screen0、Mouse0、DevInputMice与Keyboard0设置。

Files

X服务器需要的文件, 与颜色和字体有关。我的计算机上例子如下:

```
Section "Files"
    RgbPath        "/usr/X11R6/lib/X11/rgb"
    FontPath       "unix/:7100"
EndSection
```

这个Linux段表示显示器的RGB式颜色位置, 并列出X字体服务器xfs的标准TCP/IP端口。RGB(红绿蓝)是传统的颜色图形标准。

说明: RGB (红绿蓝) 不太适合许多艺术和图形设计, 因此有些Linux应用程序支持CMYK (青红黄黑) 标准, 适合几大电影工作室, 包括梦工厂和迪斯尼。Linux CMYK程序有Houdini (www.sidefx.com) 和Maya (www.aliaswavefront.com)。

Module

Module命令装入字体和服务扩展模块。下面的字体模块很简单, 装入**Freetype** (True Type克隆) 和**Type1**字体。完整模块清单见`/usr/X11R6/lib/modules`目录。

```
Section "Module"
    Load "dbe"
    Load "extmod"
    Load "fbdevhw"
    Load "dri"
    Load "glx"
    Load "record"
    Load "freetype"
    Load "type1"
EndSection
```

InputDevice

InputDevice是用户向计算机发送信息时直接接触的一切, 也称为人机接口设备 (HID), 主要是键盘和鼠标, 但也可以包括跟踪球、触摸屏, 等等。从下面可以看出, 每个组件有一个**InputDevice**段。

```
Section "InputDevice"
    Identifier "Keyboard0"
    Driver      "keyboard"
    Option      "XkbRules" "xfree86"
    Option      "XkbModel" "pc105"
    Option      "XkbLayout" "us"
EndSection
```

第一个**InputDevice**指定键盘, 使用同名驱动程序。基本键盘规则指定的布局符合XFree86服务器的布局。机型与标准105键的键盘相关, 是标准美国布局。

```
Section "InputDevice"
    Identifier "Mouse0"
    Driver      "mouse"
    Option      "Protocol" "IMPS/2"
    Option      "Device" "/dev/psaux"
    Option      "ZAxisMapping" "4 5"
    Option      "Emulate3Buttons" "no"
EndSection
```

第二个**InputDevice**指定鼠标, 使用PS/2连接。设备驱动程序文件是`/dev/psaux`, 通常连接`/dev/mouse`。**ZAxisMapping**表示鼠标轮上下移动, 这里对应于标准鼠标键4和5。这些键不

是所有鼠标都有。键4对应于三键鼠标的滚动轮，键5对应于鼠标旁边的键。如果有多个鼠标或指示设备，则可能还有另一InputDevice段。

Monitor

Monitor段汇总与显示器相关的基本设置。下面设置来自我的计算机，非常简单，表示显示器机型、DisplaySize（毫米）和水平同步与垂直刷新率。dpms选项表示省电设置标准。

```
Section "Monitor"
    Identifier   "Monitor0"
    VendorName   "Monitor Vendor"
    ModelName    "S/M 955DF"
    DisplaySize  360      270
    HorizSync    30.0 - 85.0
    VertRefresh  50.0 - 160.0
    Option       "dpms"
EndSection
```

可以配置两个不同显示器，各有自己的定制设置。显示器和显示卡一起有自己的Screen段，见本章档后介绍。

Device

支持任何GUI的主设备是显示卡。下节标识特定卡（带有驱动程序）和相关显示内存。

```
Section "Device"
    Identifier   "Videocard0"
    Driver       "i810"
    VendorName   "Videocard vendor"
    BoardName    "Intel 810"
    VideoRam     16384
EndSection
```

如果有多个显示卡，则每个卡在XF86Config文件中另起一段。

Screen

Screen段组合相应段中的相应显示卡（Device）和显示器设置。与Device与Monitor行相关的名称来自其Identifier变量。

```
Section "Screen"
    Identifier   "Screen0"
    Device       "Videocard0"
    Monitor      "Monitor0"
    DefaultDepth  24
    SubSection "Display"
        Depth     16
        Modes      "1024x768" "800x600" "640x480"
    EndSubSection
EndSection
```

```

SubSection "Display"
    Depth    24
    Modes    "800x600" "640x480"
EndSubSection
EndSection

```

组合显示卡和显示器得到点音调（Depth）和分辨率（Modes）。下节配置两个不同SubSection“Display”段，注意每段有一个点音调和可能重叠的分辨率。

DRI

直接绘制接口（DRI）利用高端显示卡的三维加速功能，用于游戏和电影、计算机辅助设计模型所需的高端图形。下列DRI段很简单：

```

Section "DRI"
    Mode      0666
EndSection

```

0666与所有用户的读写文件权限相关联。如果在/etc/group中指定组，则可以限制三维绘制访问。例如，如果/etc/group中有个galley组，则可以用下列段限制访问：

```

Section "DRI"
    Group      "galley"
    Mode      0666
EndSection

```

查错X窗口

如果启动Linux GUI时遇到问题，则可以检查几个地方。本章主要介绍基本X配置工具，因此首先可以重新运行这个工具。

和大多数其他服务器一样，许多问题都可以从/var/log目录中的日志文件查出。有时可能在另一个地方显示，如另一控制台或另一计算机上。启动X服务器时的一个常见问题是字体。如果没有启动X字体服务器，则无法启动X窗口。

日志

Linux X窗口事件有两个基本文件，都在/var/log目录中。这个目录中的XFree86.0.log文件显示startx和相关命令与配置文件交互时发生的情形，特别是XF86Config。/var/log/messages文件可以标识X字体服务器问题。

即使没有遇到问题，也应分析这些文件。也许你会突然发现一个错误。了解这里的内容有助于使X窗口更快启动。

XFree86.0.log

图15.20是这个日志文件的摘要。如果阅读了前面介绍的XF86Config文件部分，则可以识别许多变量。

```

Markers (--) probed, (**) from config file, (==) default setting,
      (++) from command line, (!!) notice, (II) informational,
      (WW) warning, (EE) error, (NI) not implemented, (??) unknown
(==) Log file "/var/log/XFree86.0.log". Time Sun Dec 22 09:47:01 2002
(==) Using config file "/etc/X11/XF86Config"
(==) ServerLayout "Default Layout"
(**) |----Screen "Screen0" (0)
(**) |   |-->Monitor "Monitor0"
(**) |   |-->Device "Videocard0"
(**) |----Input Device "Mouse0"
(**) |----Input Device "Keyboard0"
(**) Option "XkbRules" "xfree86"
(**) XKB rules "xfree86"
(**) Option "XkbModel" "pc105"
(**) XKB model "pc105"
(**) Option "XkbLayout" "us"
(**) XKB layout "us"
(==) Keyboard CustomKeycode disabled
(**) |----Input Device "DevInputMice"
(**) FontPath set to "unix:/7100"
(**) RgbPath set to "/usr/X11R6/lib/X11/rgb"
(==) ModulePath set to "/usr/X11R6/lib/modules"
(==) using VT number 7
"XFree86.0.log" 825L. 32662C
31.10 2%

```

图15.20 XFree86.0.log文件

注意基于配置文件的行，前面有星号（**）。如果存在问题，则可以在XF86Config文件中修改这些行。在我的文件中，可以看到下列行：

```

(TI) I810(0): Not using default mode "320x175" (bad mode
➡ clock/interlace/doublescan)

```

这是个信息性（II）消息，不影响工作。但要注意警告（WW）和错误（EE）消息。

学会查错

查错过程可能很复杂，如果等出事了再想办法，则迟早要出事。可以试试，由于X窗口依赖于XF86Config文件，因此可以试验这个文件来了解可能的问题。如果知道第11章介绍的linux rescue方式，而且具有系统性，则可以试试这种方法。

试验任何配置文件之前，先要进行备份。这里要将/etc/inittab中的id变量设置为运行级3。如果XF86Config中遇到问题，则可以从命令行界面重新启动Linux。

试在语句前加“#”号，将文件中的不同命令标为说明语句，然后运行startx。有时X窗口能够顺利启动，用其他设置作为默认值，而有时X窗口可能根本无法启动。注意错误（EE）消息及其与XF86Config文件变化的关系。

完成之后，记住要恢复原先的配置文件。

/var/log/messages

除非运行X字体服务器，否则无法启动X窗口。这个服务和许多服务一样在/etc/rc.d/init.d目录中控制。

说明：主字体配置文件为/etc/font/font.conf。

/var/log/messages文件相当长。默认情况下，可以放上最多一个星期的Linux计算机启动与停止消息。如果是新问题，则从文件末尾开始找。启动过程中出现的第一个消息如下：

```
Dec 22 10:25:09 RH9Server kernel: Linux version 2.4.20-3
```


然后是下列xfs启动消息：

```
Dec 22 10:25:09 RH9Server xfs: xfs startup succeeded
```

如果没有看到这个消息，则会有字体问题。请看下列情形：

- 检查xfs服务状态。如果其停止，则要用`service xfs start`命令启动。确保xfs用相应`chkconfig`命令设置为自动启动，见第13章介绍。
- 检查`/etc/X11/XF86Config`中的`FontPath`变量，其应指向实际字体文件或TCP/IP端口7100。
- 确保`FontPath`中列出的文件实际存在。如果不存在，则可能要安装一些与XFree86相关的字体RPM包。这些包的名称格式为`XFree86-*-fonts-*`。
- 检查防火墙。如果阻止端口7100的本地访问，则X字体服务器无法将信息发到X窗口。

说明：不要把X字体服务器与SGI公司开发的xfs文件系统混起来，尽管它们使用相同的缩写。

小结

本章介绍了配置X窗口的基础。尽管许多Linux专家不喜欢也不需要图形用户界面，但对许多用户而言，这是个重要工具。可以吸引来自其他图形化系统的用户，如Microsoft Windows

也许安装Linux的过程中已经配置X窗口。如果还没有配置或需要改变设置，则可以使用两大工具`xf86config`与`redhat-config-xfree86`。红帽子用`redhat-config-xfree86`，`xf86config`可以从其他发行版本得到，也可以从www.xfree86.org下载新的XFree86服务器。

X窗口有几个关键配置文件，通过`startx`脚本调用。可以在主目录中生成各个设置，也可以让`startx`使用`/etc/X11`目录中的一般化设置。

也许关键配置文件是`/etc/X11/XF86Config`。一定要了解这个文件的基础，以便进行定制和查错可能遇到的一些问题。尽管X窗口要求X字体服务器xfs，但大多数问题在主X窗口日志文件`/var/log/XFree86.0.log`中。

下一章详细介绍Red Hat Linux的默认桌面GNOME。这是个完全特性GUI，具有Microsoft Windows的几乎所有特性。即使不用GUI，最好也要了解GNOME的好处，以便帮助用户。

第16章 GNOME

尽管Linux管理员可能不需要图形用户界面，但从Microsoft Windows转过来的用户需要。GNU社区的目标之一是让Linux操作系统在桌面上有竞争力。为此，Linux需要一个GUI，让Microsoft Windows用户更习惯。

为了达到这个目的，Red Hat Linux提供了GNOME，即GNU网络对象模型环境。GNOME不仅提供高性能GUI，而且提供办公组件之类的高性能软件，Microsoft用户要为此支付几百美元。当然，Linux也没有许可证费。第1章曾介绍过，这使许多公司与政府开始将Microsoft Windows换成Linux。

GNOME提供了GUI界面、控制小程序和几个重要应用程序。其中许多组件可以替换只有Microsoft Windows中才运行的昂贵的第三方应用程序。本章简要介绍GNOME桌面、控制中心以及Red Hat Linux 9中GNOME所带的应用程序。

但是，本章并没有全面介绍GNOME。OpenOffice之类的常用应用程序放到第18章介绍，redhat-config工具放到第9章介绍。

此外，红帽子的GNOME版本可以使用KDE应用程序与实用程序，见第17章。许多KDE工具可以直接从GNOME主菜单按钮访问。本章介绍下列主题：

- 使用基本GNOME界面
- 学习其他GNOME知识

基本GNOME界面

标准GNOME桌面具有当今所有GUI操作系统特性，包括面板、主菜单按钮和图标。可以根据需要定制每个组件，甚至可以对GNOME安装配置标准界面。可以通过GNOME控制中心控制和定制GNOME的外观。首次在Red Hat Linux中启动GUI时，可以看到图16.1所示的桌面。



图16.1 GNOME桌面

说明：Red Hat Linux中面板的作用相当于Microsoft Windows中的任务栏，主菜单按钮具有红帽子图标，相当于Microsoft的Start按钮。

GNOME概述

基本GNOME界面很简单，如图16.1所示，可以导航到主目录（用户名的主目录），**Start Here**按钮可以打开小程序、实用程序和应用程序，还有一个**Trash**文件夹。这三者都使用Nautilus，这是个“Explorer”式的图形shell，用于管理文件、GNOME配置和Linux系统中相关的任何GUI工具。本章稍后将再次使用Nautilus。下面几节介绍面板与GNOME控制中心中的按钮。

GNOME面板








GNOME面板中可以调用多个应用程序，在打开程序之间切换和在打开工作空间之间切换。图16.2显示了我的GNOME面板。这里GNOME面板包括左边七个图标，见表16.1介绍。

说明：工作空间相当于标准桌面，有自己的图标和打开程序。默认情况下，GNOME包括四个工作空间，其中三个工作空间的数据存放在多余显示内存中。



图16.2 GNOME面板

表16.1 GNOME面板图标

图标	描述
	单击这个按钮打开GNOME主菜单，可以访问应用程序和实用程序，相当于Microsoft Windows中的Start按钮
	可以打开Mozilla Web浏览器
	启动Evolution个人信息管理器，其功能相当于Microsoft Outlook
	打开OpenOffice Writer，其功能相当于Microsoft Word
	打开OpenOffice Impress演示管理器，其功能相当于Microsoft PowerPoint
	打开OpenOffice Calc电子表格程序，其功能相当于Microsoft Excel
	打开GNOME打印管理器

GNOME工作空间与打开程序

GNOME很灵活，可以将打开窗口放在几个工作空间。因此我们不需要打开和关闭窗口，只要通过切换工作空间来访问应用程序。例如，可以把OpenOffice Writer放在一个工作空间，把OpenOffice Impress放在一个工作空间，把Gimp图形程序放在一个工作空间，把终端窗口

放在一个工作空间。四个工作空间在面板上显示缩略图，如图16.3。



图16.3 四个GNOME工作空间

要切换到另一工作空间，单击相应缩略图。要将一个应用程序移到另一工作空间，单击应用程序左上角，可以看到图16.4所示的下拉菜单。



图16.4 移到工作空间2

还可以在面板上显示的打开应用程序之间切换。例如，图16.5所示的屏幕可以在三个打开应用程序之间切换。



图16.5 打开应用程序之间切换

其他GNOME面板项目

最后，面板右端还有两个图标。红色感叹号是红帽子网络警报图标，表示要用up2date连接红帽子网络，升级一些包（如果是蓝色复选标志，则系统已经用最新包更新）。up2date实用程序见第10章介绍。

如果单击面板上的日期和时间，则可以看到本月日历。如果右单击这个区并从弹出菜单选择Adjust Date & Time，则打开redhat-config-date实用程序，见第19章介绍。

很容易定制GNOME面板，只要右单击面板上的一个打开区域，然后在弹出菜单中单击Properties打开面板属性窗口，如图16.6。

利用GNOME面板属性窗口可以做几件事。可以改变面板尺寸与位置，可以默认隐藏，直到鼠标放在面板上。在Background标签中，可以设置面板本身的背景。

提示：许多Linux管理员在GNOME中使用命令行界面。要启动这个界面，右单击桌面，并从弹出菜单选择New Terminal打开gnome-terminal命令行窗口。也可以选择Main Menu►System Tools►Terminal打开这个命令行界面。

GNOME主菜单

下面要介绍GNOME主菜单。单击桌面左下角的红帽子，可以看到图16.7所示的菜单。

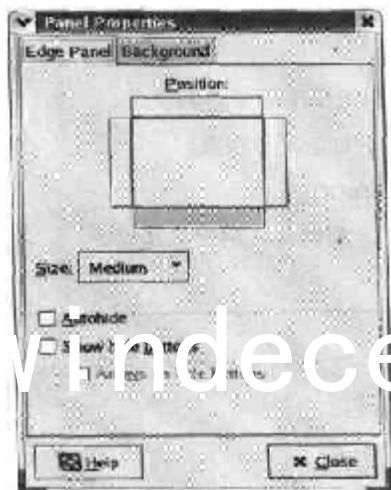


图16.6 GNOME面板属性窗口



图16.7 GNOME主菜单

可以看出，GNOME主菜单打开一系列其他命令和菜单，见表16.2简要介绍。我们将在本章和后面几章详细介绍其中一些菜单。这些菜单中的许多程序是针对KDE（K桌面环境）的，见第17章介绍。这个菜单中的主要应用程序（如办公组件与图形）将在第18章介绍。第19章将介绍红帽子特定管理工具。

表16.2 GNOME主菜单命令与子菜单

命令与子菜单	说明
Accessories	打开一组小程序，如文本编辑器和计算器
Documentation	进入从Red Hat Linux文档光碟装入的任何文档
Games	启动安装的任何游戏
Graphics	访问编辑、屏幕快照、传真、PDF阅读器等图形应用程序
Internet	一系列应用程序，可以在互联网之类的TCP/IP网络上通信
Office	打开与OpenOffice程序组相关的一系列应用程序，还可以通过这个菜单访问其他办公组件
Preferences	可以定制设置，通常与桌面有关
Programming	可以访问一组编程工具，奇怪的是，这个组中还包括Emacs

(续表)

命令与子菜单	说明
Sound & Video	增加多媒体应用程序, 包括光碟刻录程序
System Settings	可以访问许多redhat-config-*管理实用程序, 大多数要求根用户级访问
System Tools	启动各个管理工具的菜单
Help	在简化浏览器中打开GNOME帮助会话
Home Folder	启动Nautilus, 提供主目录中文件的视图
Network Servers	可以从其他计算机访问共享文件夹, 包括通过Samba访问Microsoft Windows 计算机
Run Program	打开Run Program对话框, 可以输入应用程序的文本名
Search For Files	打开搜索文件的Find命令前端, 从指定目录开始搜索
Open Recent	可以打开最近访问文档, 通常使用OpenOffice
Lock Screen	启动安全屏幕保护程序, 要返回桌面, 需要输入用户名和口令
Log Out	退出GNOME

如果看不到特定菜单, 则可能是没有安装相关软件包。例如 要看到Game 菜单, 一定要先安装kdegames-*与gnome-games-*之类的相关软件包。

GNOME控制中心

下面要介绍GNOME桌面的一些详细配置选项, 可以通过GNOME控制中心访问。可以从主菜单中选择Main Menu►Preferences►Control Center打开GNOME控制中心, 其打开Nautilus窗口, 有一系列图标, 如图16.8。每个图标与GNOME中可以使用的图形应用程序相关。控制中心图标打开另一个选项窗口。下面几节介绍其他小程序。



图16.8 GNOME控制中心

说明：GNOME控制中心中的小程序也可以通过Main Menu►Preferences子菜单访问。

About Myself

About Myself小程序打开用户信息窗口，如图16.9。可以输入与账号相关的其他信息，如电话号码和地点。这是chfn命令的前端，详细信息可以用finger命令访问。

Accessibility

Accessibility小程序打开键盘访问性选项窗口，如图16.10。如果要改变任何特性，可以激活Enable Keyboard Accessibility Features选项。



图16.9 用户信息窗口

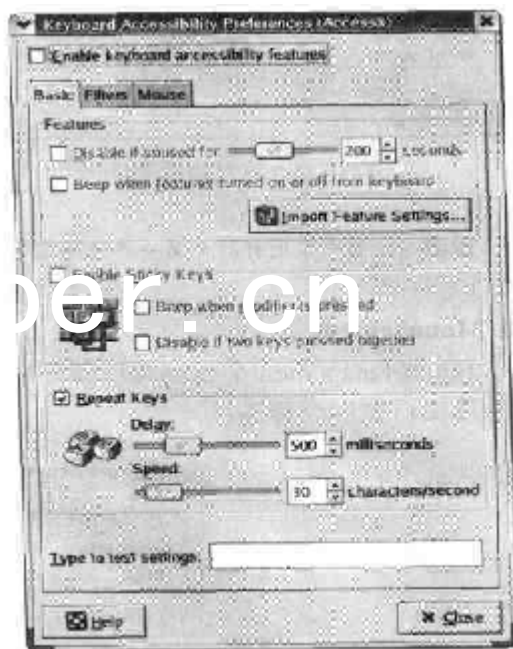


图16.10 键盘访问性选项窗口

这个窗口有三个标签。Basic标签可以定制键盘的标准设置。Filters标签可以检查输入，例如，如果输入时手指摇动，则Enable Bounce Keys选项可以忽略几毫秒之内重复的键击。Mouse标签可以管理屏幕上的鼠标指针速度。

Background

Background小程序打开图16.11所示的背景选项菜单，可以定制桌面背景中显示的图形和显示。要改变背景图形，单击Select Picture下面显示的图形。

CD Properties

CD Properties小程序打开光碟与DVD选项窗口，如图16.12。可以看出，其可以在光碟与DVD插入光驱时设置选项。默认情况下，数据光碟自动装载，声音光碟用gnome-cd播放，空白光碟可以访问Nautilus光碟刻录机。可以用不同Command文本框设置各个光碟与DVD命令。



图16.11 背景选项菜单

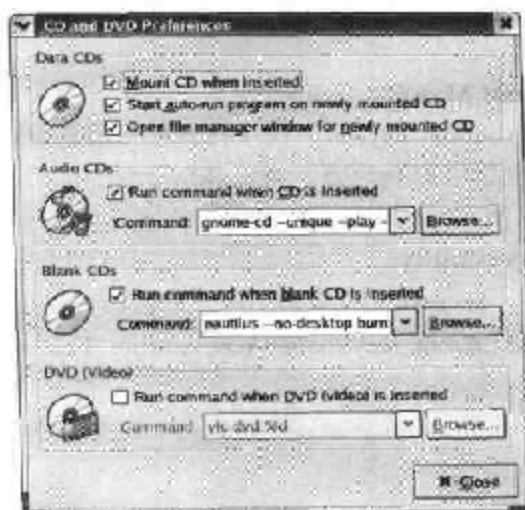


图16.12 光碟与DVD选项窗口

说明：控制中心图标打开另一个选项窗口。

File Management

File Management小程序可以管理Nautilus中文件视图的外观。如图16.13所示，文件管理选项窗口有四个标签：

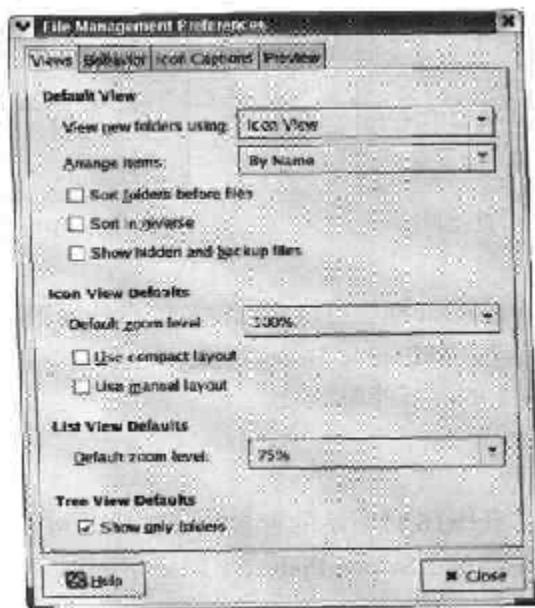


图16.13 文件管理选项窗口

- **Views**标签可以定制Nautilus中文件的外观。默认情况下，采用图标视图，可以包括图形文件的缩略图。

- **Behavior**标签可以确定单击文件时发生的情形。例如，可以设置选项，在单击可执行文件时运行这个文件。
- **Icon Captions**标签可以调整每个图标显示的信息。
- **Preview**标签可以确定Nautilus窗口中浏览文本、图形、声音和目录（文件夹）文件时的行为。

文件类型与程序窗口

文件类型与程序窗口如图16.14，可以将不同文件类型与特定程序相关联。文件标识依赖于扩展名，如.doc与.tif。如果要增加或改变与特定文件类型相关联的程序，可以选择这种文件类型并单击Edit。

说明：图16.14所示的HTML页面文件类型可以在Documents►World Wide Web中找到。

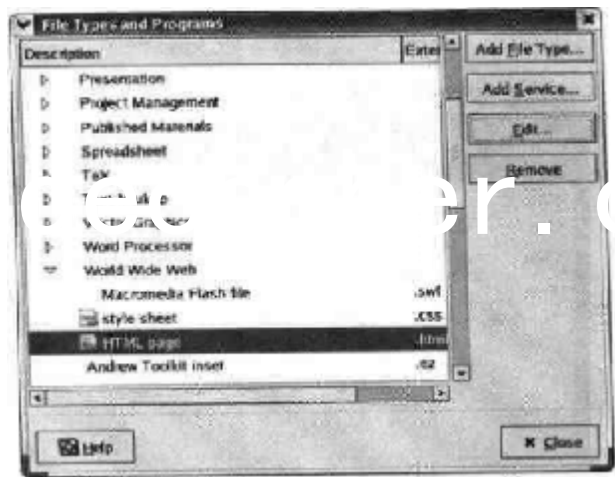


图16.14 文件类型与程序窗口

字体

字体选项程序窗口可以配置桌面上不同组件的默认字体，如图16.15。仍然可以指定不同应用程序和实用程序中的定制字体，如终端窗口。

Handheld PDA

Handheld PDA小程序是gnome-pilot的前端，可以同步GNOME与符合PalmPilot与PalmOS标准的手提设备间的数据。首次打开这个小程序时，它启动一个向导，可以定义支持物、设备和允许的用户。GNOME试验设置窗口如图16.16。

键盘

键盘选项窗口如图16.17，可以定制键盘对键击的响应。光标闪烁方式和键盘事件是否与声音相联系。

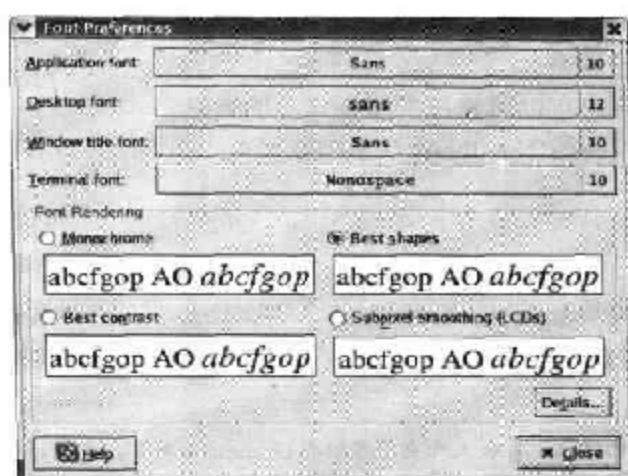


图16.15 字体选项程序窗口



图16.16 GNOME试验设置窗口



图16.17 键盘选项窗口

键盘快捷窗口

键盘快捷窗口如图16.18，列出键盘上不同控制键的功能，如Shift、Ctrl、Alt、Tab与Esc。有两组默认，一组针对GNOME，一组针对Emacs。

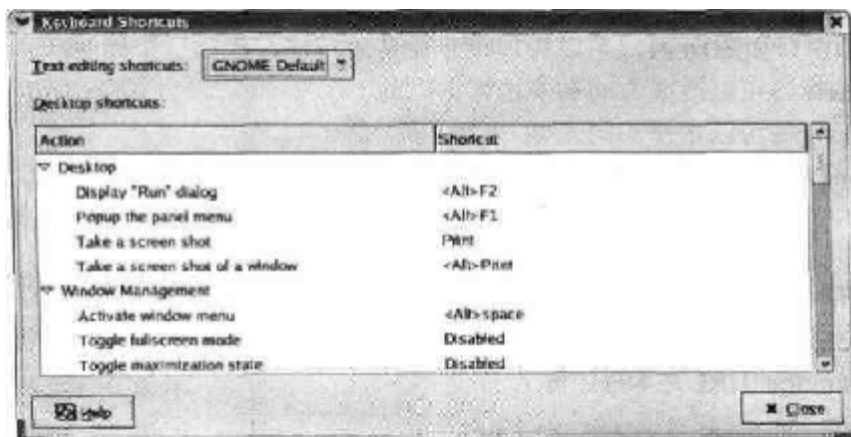


图16.18 键盘快捷窗口

如果要改变快捷方法，可以加亮这个快捷方法，按退格键，然后按下作为该操作快捷键的键。

登录照片窗口

登录照片窗口与第15章介绍的GNOME显示管理器（GDM）相关联，可以设置与GNOME显示管理器标准问题相关的一组照片，要用GNOME显示管理器登录时才会启动。

为了使用这个功能，就要在第15章介绍的Standard Greeter标签中启用GDM Setup菜单的Show Choosable User Images选项，然后出现图16.19所示的照片选择窗口，可以设置这个特定登录情形的照片。

说明：登录照片文件只限于64KB。

鼠标与工具栏

鼠标与工具栏选项窗口如图16.20，可以修改程序菜单中图标与文本的外观。

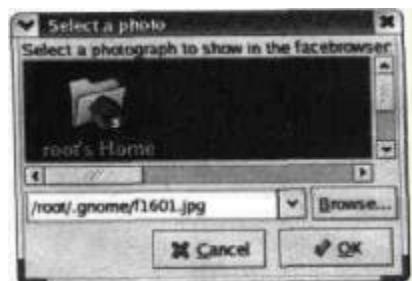


图16.19 为GNOME显示管理器选择照片

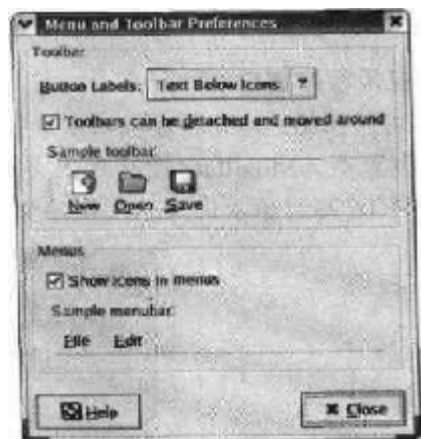


图16.20 鼠标与工具栏选项窗口

鼠标选项窗口

鼠标选项窗口如图16.21，可以管理指示设备的特性，包括三个标签：

- Buttons标签可以改变方向和双击延迟时间。
- Cursors标签可以选择不同光标。
- Motion标签可以管理光标速度和拖放行为。

网络代理

网络代理配置窗口可以设置外部网络连接的路径，通常连接互联网。如果网络上有代理服务器，则可以设置协议的地址，如图16.22。有些管理员提供自动代理配置链接，可以在Autoconfiguration URL文本框中输入。

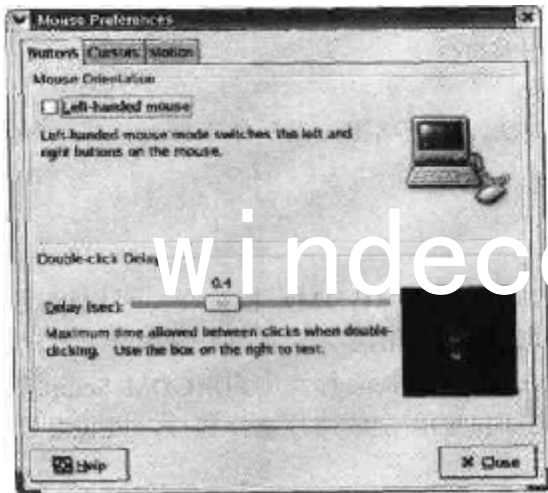


图16.21 鼠标选项窗口

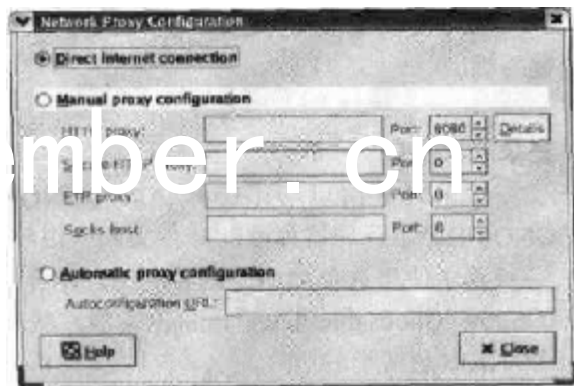


图16.22 网络代理配置窗口

Password

Password小程序很简单，可以改变当前用户账号的登录口令，是passwd命令的前端，可以输入当前口令，然后两次输入新口令。

优选应用程序窗口

可以在优选应用程序窗口中选择优选文本编辑器、Web浏览器、命令行界面终端。默认Web浏览器为Mozilla，没有默认文本编辑器，默认终端为gnome-terminal。

图16.23显示了优选应用程序窗口。

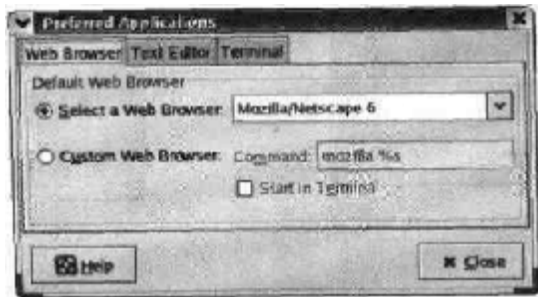


图16.23 优选应用程序窗口

Screensaver

通过Screensaver小程序可以配置所选的屏幕保护程序。屏保选项窗口如图16.24，可以配置随机或特定屏幕保护模式以及延迟时间和屏幕保护性能设置。



图16.24 屏保选项窗口

说明：GNOME不允许屏幕保护程序访问根用户，除非运行xhost +localhost命令。xhost命令见第15章介绍，可以对指定计算机进行网络访问。事实上，GNOME不鼓励根用户访问GUI。尽管本书使用根账号，但我没有离开启用根用户的计算机，因此不需要屏幕保护程序。

Sound

如果在计算机上配置了声卡，则可以用Sound小程序在遇到不同事件时激活声音，如收到电子邮件、登录、出错，等等。声音选项窗口如图16.25，可以对指定事件设置不同声音。

主题

主题选项窗口如图16.26，也很简单，显示的红帽子“Bluecurve”主题是红帽子桌面的默认主体。单击Details，可以对控制、窗口边框和图标设置不同主题。

窗口

窗口选项窗口如图16.27，可以设置GUI中的窗口行为。可以设置双击标题栏或与移动特定窗口相关的键时窗口的行为。

更多选项

GNOME控制中心还有More Preferences的链接，对下列三个项目打开不同窗口：CD数据库、面板和会话。本章稍后将介绍相关的选项窗口。



图16.25 声音选项窗口

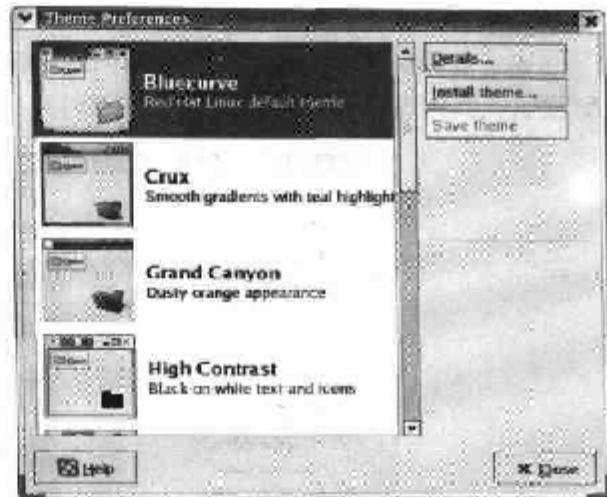


图16.26 主题选项窗口

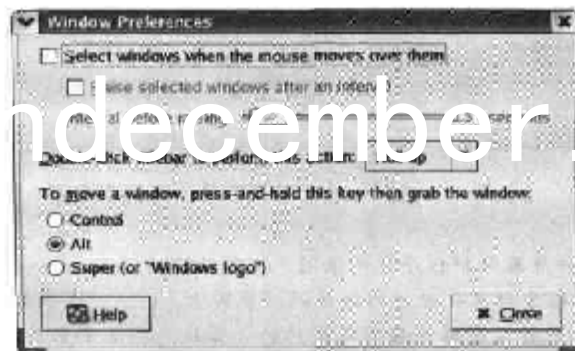


图16.27 窗口选项窗口

了解其他GNOME项目

GNOME还带有几个应用程序，可以通过主菜单按钮访问，分成几类：附件、互联网、选项、多媒体和系统工具。这还不是主菜单按钮可以访问的全部程序，其中许多会在后面三章介绍。尽管大多数实用程序基于GNOME项目工作，但也有几个第三方实用程序将在本节一起介绍。

附件

GNOME中的几个附件可以帮助进行简单计算工作，可以通过Main Menu►Accessories子菜单访问。如图16.28所示，这个菜单有一个More Accessories子菜单。这个子菜单中的大多数实用程序与KDE相关联，将在第17章介绍。

计算器

GNOME有一个简单科学计算器，如图16.29，响应键盘数字键中的项目。可以将结果复制到其他GUI应用程序。

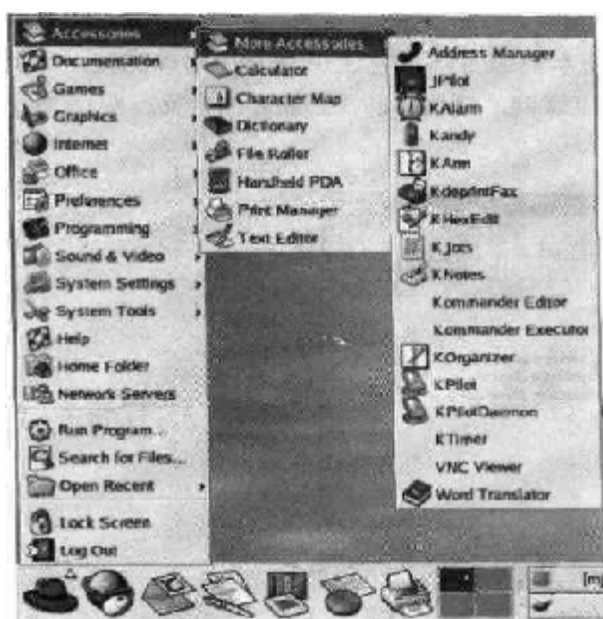


图16.28 附件菜单



图16.29 GNOME计算器

字符映射

字符映射应用程序如图16.30，可以使用几个罗马式字母的非英文语言，提供的接口可以在文档中包括特殊字符和升降调符。

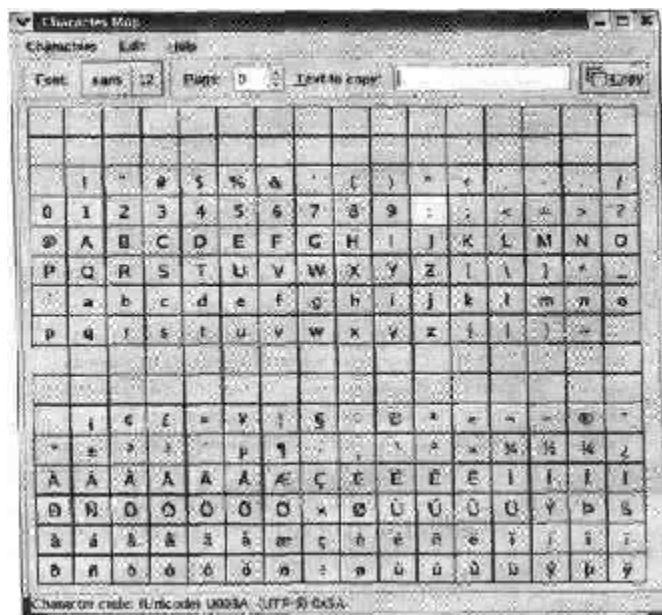


图16.30 GNOME字符映射

字典

GNOME字典可以访问dict.org站点的联机字典服务器。它使用TCP/IP端口2628, 因此URL前面没有“www”或“http”。只要连接互联网, 就很容易找到需要的定义。图16.31显示了一个例子。

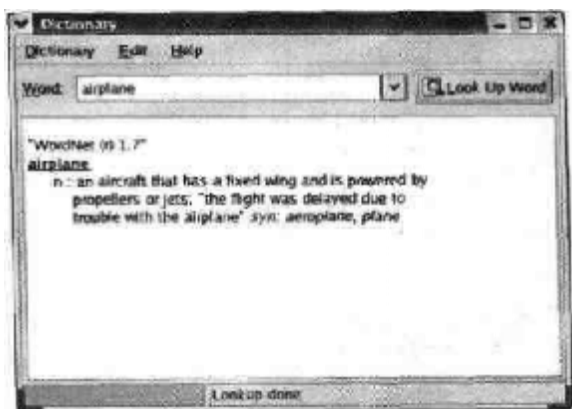


图16.31 GNOME字典

文件滚压器

GNOME文件滚压器的功能相当于Microsoft Windows中的各种Zip实用程序。换句话说, 可以从压缩档案中浏览和读取文件。图16.32显示了.tar.gz档案中文件视图的例子。

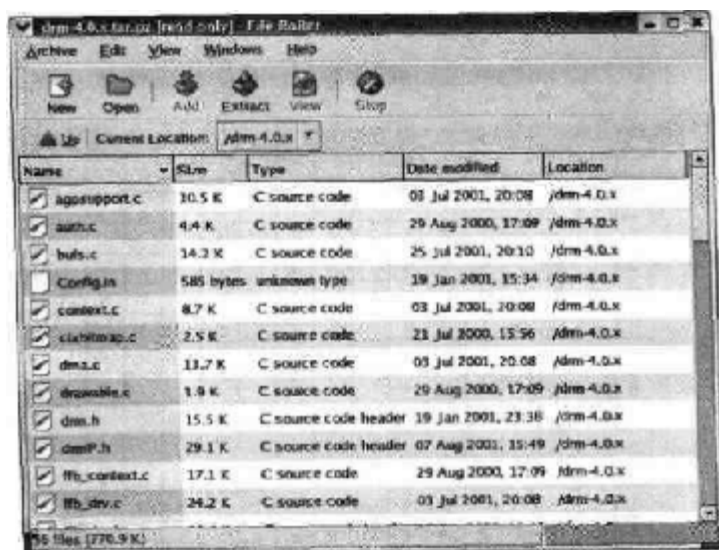


图16.32 GNOME文件滚压器

手提PDA

选择Main Menu►Accessories►Handheld PDA时, GNOME可以打开本章前面介绍的Pilot Link实用程序。

打印管理器

运行Main Menu►Accessories►Print Manager时，GNOME打开一个打印管理器，检查打印队列中的文档。如果要对适用文档有更多了解，可以单击Edit►Preferences。如果前面没有配置打印机，则GNOME打印管理器会启动第25章介绍的redhat-config-printer实用程序。

文本编辑器

gedit程序是标准GNOME GUI文本编辑器，是相当灵活的Linux文本编辑器，特别是比vi灵活得多。图16.33显示了/etc/fstab配置文件的gedit视图。

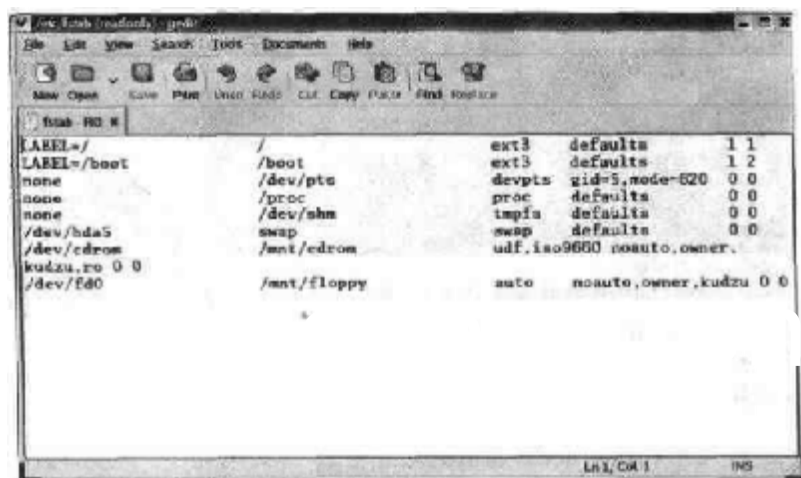


图16.33 gedit视图

gedit程序也很容易定制。单击Edit►Preferences打开选项菜单，可以定制文本外观。例如，可以用其修改字体、颜色、增加行号、配置打印设置和增加插件。

VNC浏览程序

AT&T公司的VNC（虚拟网络计算）提供了访问远程图形操作系统的方法。可以通过Main Menu►Accessories►More Accessories►VNC Viewer启动VNC客户浏览程序，VNC浏览程序和远程VNC服务器一起工作。

VNC浏览程序打开一个小VNC服务器窗口，可以输入远程服务器的IP地址与口令。如图16.34所示，我用其打开远程Windows 2000计算机的完全功能视图。

文档

Red Hat Linux有个Documentation菜单，很容易访问安装的任何Red Hat Linux 9文档。可以通过主菜单中的Documentation选项访问这个菜单，如图16.35。

选择其中的文档时，Red Hat Linux在默认Web浏览器中打开文档。

游戏

如果系统中安装了任何GNOME或KDE游戏包，则可以通过Main Menu►Games访问。

本节介绍更基本的程序，包括立即消息程序、聊天程序和其他连接实用程序。可以单击Main Menu►Internet访问Internet实用程序，有些可以通过Main Menu►Internet►More Internet Applications访问，如图16.36。许多实用程序是对KDE开发的，将在第17章介绍。



图16.36 Internet菜单

说明：图16.36中的许多应用程序都不属于GNOME或KDE，将在其他章节介绍，如Balsa与Ethereal。

视频会议

要启动GnomeMeeting，选择Main Menu►Internet►Video Conferencing。GnomeMeeting是特性完全的H.323兼容视频会议应用程序。换句话说，可以用它连接其他视频会议客户机，如Microsoft的NetMeeting。它支持声音和视频，即要有声卡和Linux支持的摄像头。图16.37显示了GnomeMeeting的基本屏幕。

说明：Linux支持的摄像头清单见Hardware HOWTO文档页面www.tldp.org/HOWTO/Hardware-HOWTO/other.html和QuickCam mini-HOWTO文档页面www.dkfz.de/Macromol/wedemann/mini-HOWTO-cqcam.html。

首次启动GnomeMeeting时，可以看到初次配置工具，否则可以单击Edit►Configuration Druid打开图16.38所示的屏幕。需要身份信息、连接类型（如Modem、ISDN或DSL适配器）和声音与视频设备驱动程序。还可以用GnomeMeeting将PC机连接普通电话网络，使用www.microtelco.com站点的MicroTelco账号。后面可以单击Edit►Preferences选项修改选项。

exmh

exmh程序是X窗口用户界面，用于UNIX式电子邮件处理器（MH），可以搜索内部消

息，如图16.39所示。如果按第25章介绍的方法配置sendmail，则可以答复或转发收到的任何消息。



图16.37 GnomeMeeting

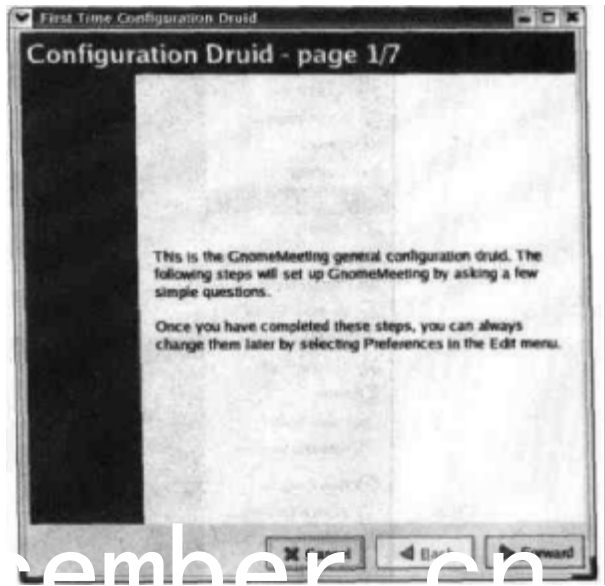


图16.38 GnomeMeeting初次配置工具

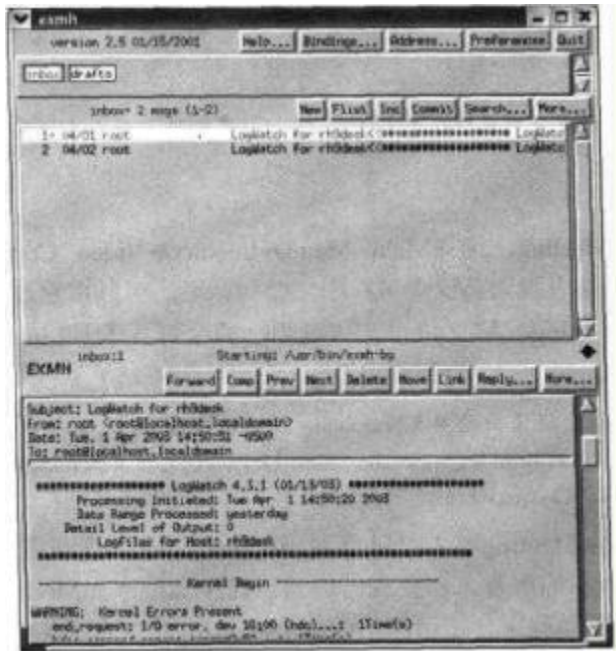


图16.39 exmh程序

首次打开exmh程序时，它检查是否有MH账号。如果没有，则向导会建立MH环境，在主目录中建立.mh_profile。

Galeon

尽管默认红帽子Web浏览器是Mozilla，但还有另一个GNOME浏览器，称为Galeon。首次打开这个浏览器时，其提示用Netscape或Mozilla的书签设置工具栏和网关的代理设置（如有）。

也可以将Galeon集成为正常（HTTP）页面、安全（HTTPS）Web页面、FTP站点和GNOME帮助的默认客户机，以及浏览本地目录中的文件。

从图16.40可以看出，Galeon的左窗格中不包括Mozilla的功能，有人认为这样能使界面更整洁。可以用Settings►Preferences命令编辑选项。

IRC

Linux有个互联网中继聊天（IRC）程序X-Chat，可以访问许多不同的聊天服务器，如图16.41。其他组可能有自己的IRC服务器，可以单击New Server按钮进行设置。

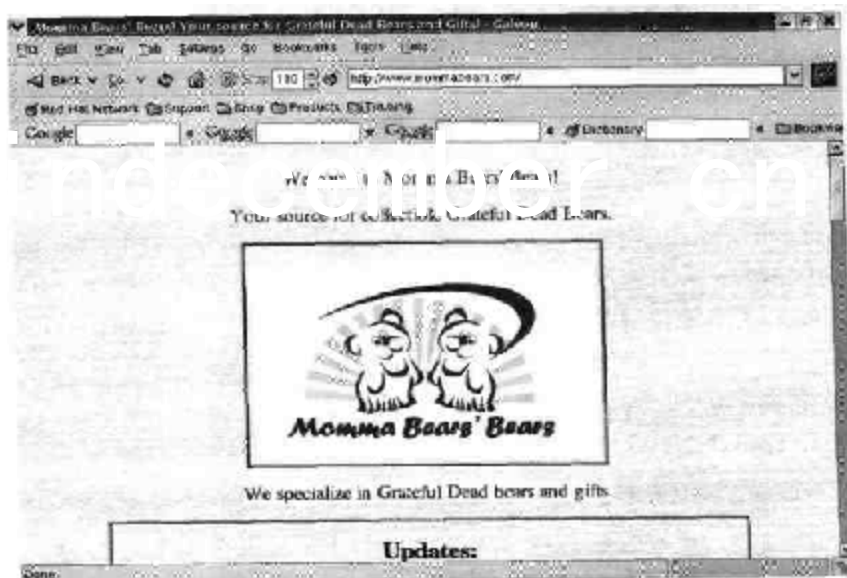


图16.40 GNOME Galeon浏览器

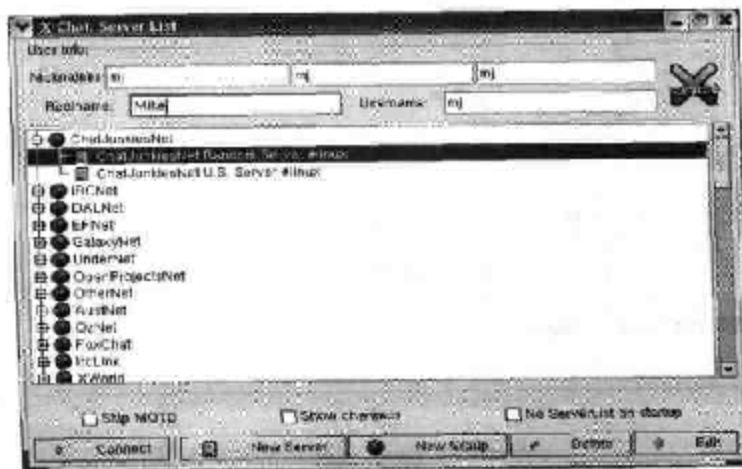


图16.41 X-Chat与IRC

配置X-Chat之后, 选择聊天服务器和单击Connect。如果有服务器, 则会进入聊天窗口, 如图16.42所示。



图16.42 聊天窗口

Pan

GNOME有个图形化新闻阅读器Pan, 如图16.43, 可以在不同新闻组中阅读和发表消息。

首次启动Pan时, 程序提示输入基本登录信息, 包括电子邮件地址、SMTP服务器和新闻服务器名。如果在本地计算机上使用sendmail, 则可以使用localhost, 否则用ISP的发送电子邮件服务器。

如果要改变发表的样子, 可以单击Tools►Posting Profiles。如果要改变或增加新闻服务器, 可以单击Tools►News Servers。

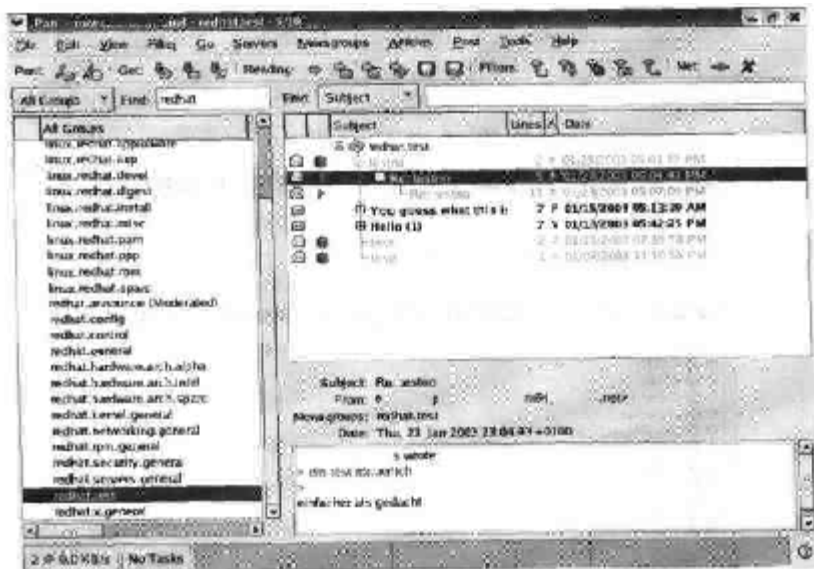


图16.43 Pan可以阅读和发表消息

远程桌面连接

如果有远程桌面服务器，则可以用远程桌面连接，如图16.44。它适用于带VNC服务器的计算机。远程桌面连接的优点是可以进入全屏方式。除了屏幕上方的小标题之外，桌面环境与远程计算机基本一致。

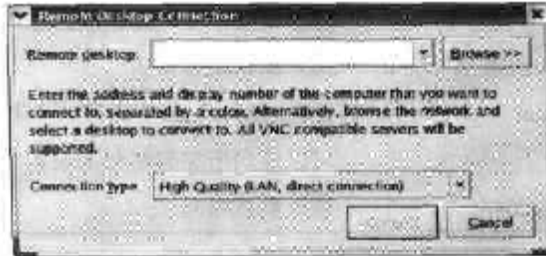


图16.44 建立远程桌面连接

Sylpheed

Sylpheed是个电子邮件客户端，用与GNOME相当的基本工具开发：GTK+（GNOME Tool Kit），是在日本开发的，因此有一个很强的日语界面。这是个轻量级邮件管理器，适用于任何Web浏览器。图16.45显示了一个配置版本。

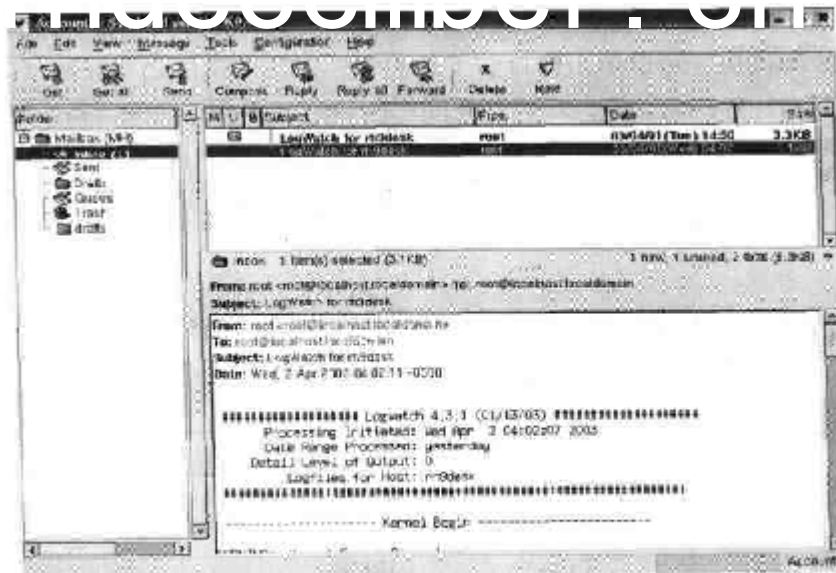


图16.45 Sylpheed邮件管理器

Sylpheed很容易配置，Configuration菜单提供了一系列菜单命令选项，如表16.3所示。

表16.3 Sylpheed配置选项

选项	描述
Common Preferences	包括文件夹地址、接口、答复默认、自动检查时间，等等

(续表)

选项	描述
Filter Setting	可以停止或转发具有某些特征的消息
Templates	支持一般性答复
Actions	可以指定命令，如译码某些消息
Preferences For Current Account	指定默认账号设置
Create New Account	可以对Sylpheed生成第二个电子邮件账号
Edit Accounts	可以编辑所配置账号的设置
Change Current Account	修改默认账号

Internet应用程序

本节介绍Linux用户经常在Internet上运行的三个基本应用程序，是红帽子默认程序：Web浏览器Mozilla、个人信息管理器Evolution和立即消息（IM）客户机Gaim，可以通过主菜单上的Internet子菜单访问。

Mozilla

Mozilla是默认红帽子Web浏览器，是个特性完全的Web浏览器，利用1998年Netscape公司发布的开放源代码。可以单击窗口右下角的图标在几个特性之间导航（如图16.46）。这些图标从左到右与Web浏览器、邮件与新闻组阅读器、Web页面编写器、地址簿和IRC聊天客户机相关联。



图16.46 Mozilla图标

每个特性还有相关的控制键，如表16.4所示。

表16.4 Mozilla特性

按键	特性
Ctrl+1	Navigator（浏览器）
Ctrl+2	邮件与新闻组
Ctrl+3	IRC聊天
Ctrl+4	编写器
Ctrl+5	地址簿

说明：Marc Andreessen开发Netscape Web浏览器时，Mozilla是一流的浏览器，他希望建立“Mosaic Godzilla”，因此浏览器项目的代码名为Mozilla。

Mozilla浏览器

默认Mozilla Web浏览器的外观与Netscape相似，如图16.47，包括与Netscape相关的命令，如“What's Related”旁白。



图16.47 Mozilla Web浏览器

可以定制各种Mozilla选项。单击Edit►Preference打开图16.48所示的选项窗口，Netscape用户应该熟悉这些选项。

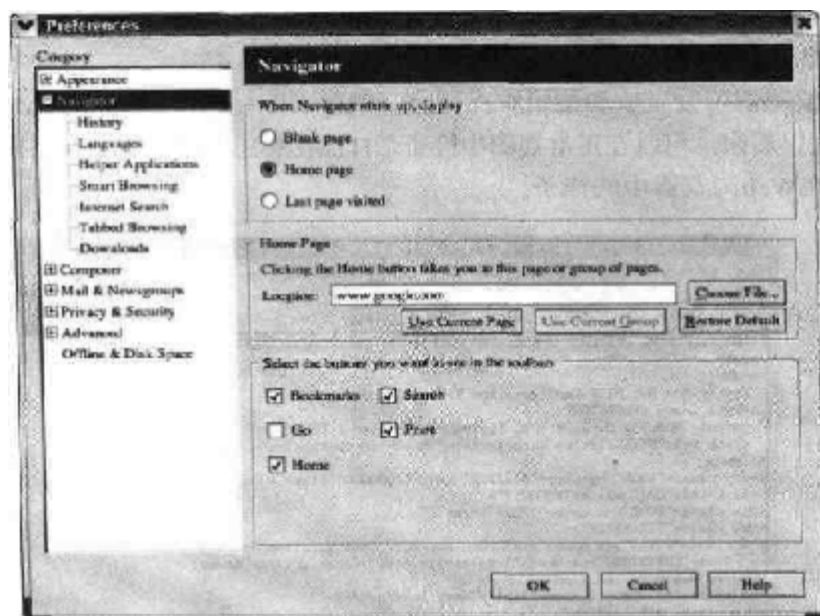


图16.48 设置Mozilla选项

Mozilla邮件与新闻组阅读器

首次打开Mozilla邮件与新闻组阅读器时，会提示设置邮件与新闻组账号。如果要增加更多账号，可以单击Edit►Mail And Newsgroups Account Settings。在打开的窗口中，单击Add Account。

对电子邮件账号,要输入姓名、邮件地址、接收POP或IMAP E-mail服务器和发送SMTP服务器,要从电子邮件账号的ISP那里取得这个信息。关于这些邮件协议的更多信息,见第26章。

配置之后, Mozilla包括基本功能的超链接, 如图16.49。

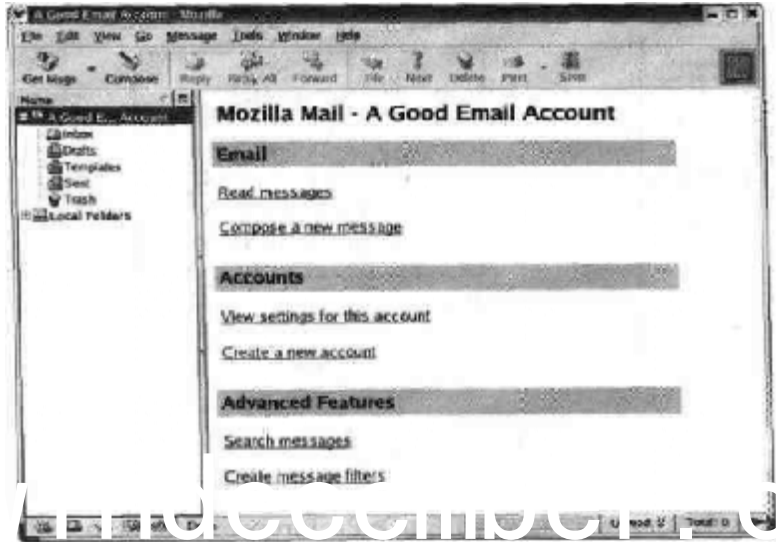


图16.49 Mozilla与电子邮件

Mozilla编写器

Mozilla编写器可以生成和编辑Web页面。例如, 图16.50的代码来自Mozilla实用程序的帮助文件。可以看出, 可以在正常视图中检查带HTML标志的Web页面, 来自HTML源代码, 可以预览其在Web浏览器中的样子。



图16.50 Mozilla编写器

Mozilla地址簿

Mozilla地址簿可以收集每个联系人的各种信息，如图16.51。

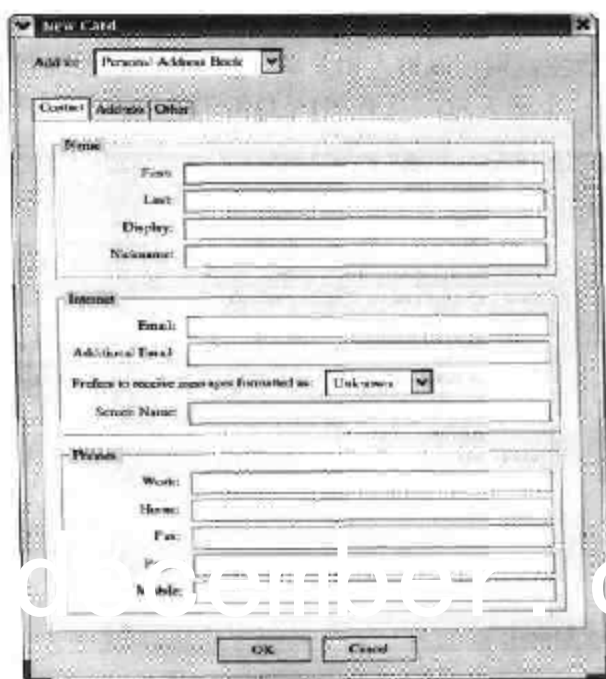


图16.51 Mozilla地址簿

Mozilla聊天客户机

Mozilla聊天也称为ChatZilla!，是基于链接的程序。启动Mozilla聊天程序时，可以看到图16.5所示的屏幕。可以单击一个可用网络，其在ChatZilla!屏幕中实际上是蓝色的。

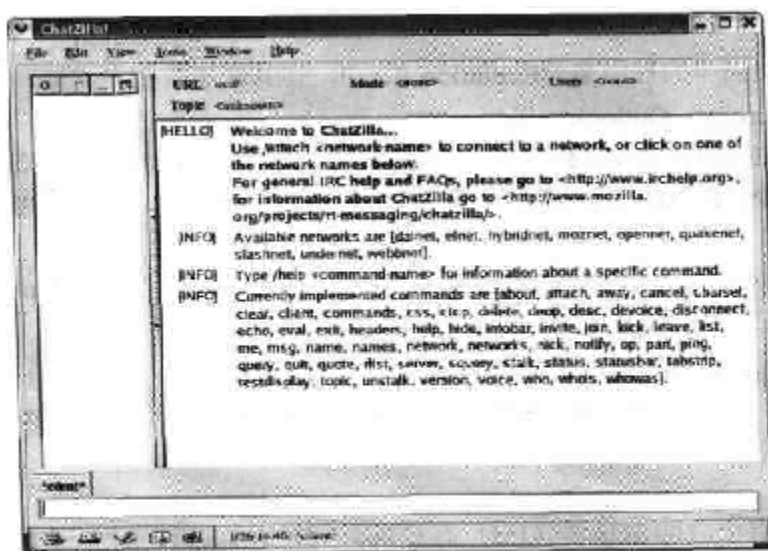


图16.52 ChatZilla!屏幕

例如, 要访问undernet IRC网络, 可以在ChatZilla!屏幕中单击其网络。登录服务器之后, 可以加入所选的闲聊天。有时可以在开始消息中看到一个链接, 例如:

```
/join #phoenix
```

如果知道所要的聊天室, 则可以输入相关命令, 这里用所要的聊天室数据替换phoenix。如果成功, 则可以看到一个聊天室, 具有图16.53所示的用户。

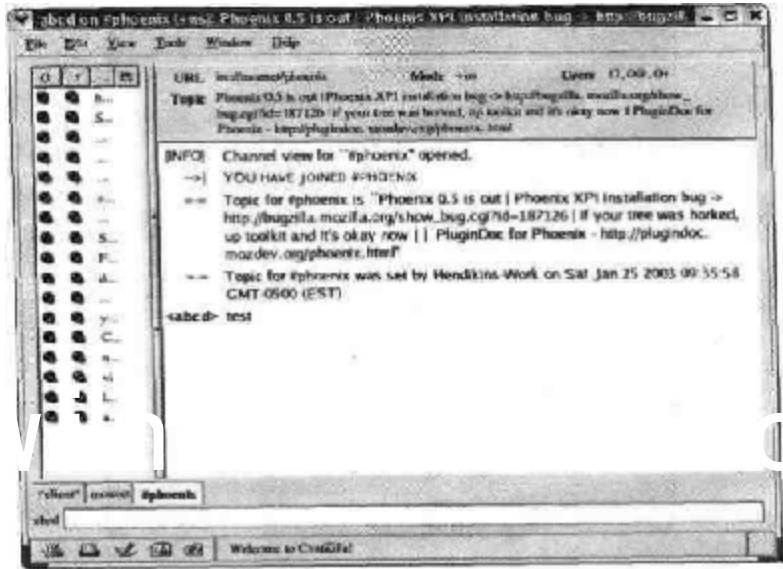


图16.53 与ChatZilla!通信

提示: 如果聊天客户机没有响应, 则可能是防火墙阻止了通信流可以通过端口6667用相应iptables命令设置聊天通信, 如第22章所示。

Evolution

GNOME桌面中的程序名为Evolution Email, 但其实还有更多功能, 可以作为个人信息管理器, 像Microsoft Outlook一样。

首次启动Evolution时, 提示配置你的配置文件。Evolution可以处理各种类型的标准电子邮件, 包括POP、IMAP与MH服务器, 它还要求标出时区, 并提示从其他格式导入地址簿和电子邮件。

从图16.54可以看出, Evolution汇总视图列出本地天气、电子邮件、约会和未来任务。另一个对Linux管理员很有用的特性是最新的红帽子勘误表。

说明: Ximian (www.ximian.com) 是Linux桌面产品的重要生产者, 为企业开发GUI桌面工具。他们还启动Mono项目, 目标是建立Microsoft的.NET平台的开放源代码实现版本。

立即消息器

GNOME有个立即消息器 (IM) 客户机, 可以连接各种不同的服务器, 包括America Online (AOL)、Yahoo!与Microsoft Network (MSN) 提供的服务器, 正式编写为Gaim, 表示某个著名IM程序的GNU版本 (这里不能指出)。实际上, 这个缩写并不合理, 因为与

专属IM程序不同的是，Gaim使用插件件，实际上是个程序适配器，可以连接几种不同类型的IM网络。图16.55显示了Gaim登录屏幕。



图16.55 Gaim登录屏幕

为了访问特定网络，要安装一个配置的插件件。在Gaim中，单击**Plugins**打开**Gaim - Plugins**窗口。在这个窗口中，单击**Load**，其中列出了`/usr/lib/gaim`目录中的插件件。表16.5列出了一些常用的插件件。

表16.5 Gaim插件件

插入件	立即消息网络
libicq.so	ICQ (即 “I seek you”)
libirc.so	Internet Relay Chat (IRC)
libmsn.so	Microsoft Network (MSN)
libyahoo.so	Yahoo! Messenger

关于所要登录信息的细节，见所选的IM提供者。屏幕名对应于账号，别名是IM聊天区看到的内容。

选项

Main Menu►Preferences子菜单中的大多数实用程序已经在本章介绍，GNOME控制中心时介绍。本节介绍与Main Menu►Preferences►More Preferences子菜单相关的实用程序。图16.56显示了这些菜单。



图16.56 选项菜单

CD数据库

一系列CD数据库（CDDDB）服务器提供了所喜欢的音乐光碟的其他信息。打开CD数据库选项窗口时，可以配置对这些服务器的访问，有些可以通过www.freedb.org访问，CDDDB主页为www.gracenote.com。

面板

面板选项窗口可以配置GNOME面板的行为以及面板中配置的任何“抽屉”。抽屉相当于主菜单按钮，可以配置所选菜单和应用程序的链接。

会话

会话窗口可以配置进入GNOME桌面时启动的程序，还可以配置GNOME启动时的行为，监视当前装入的程序。如图16.57所示，窗口中有三个标签，见表16.6。

表16.6 GNOME会话

标签	描述
Session Options	管理GNOME登录和退出过程中的行为
Current Session	列出GNOME中当前运行的程序
Startup Programs	列出启动GNOME时启动的程序

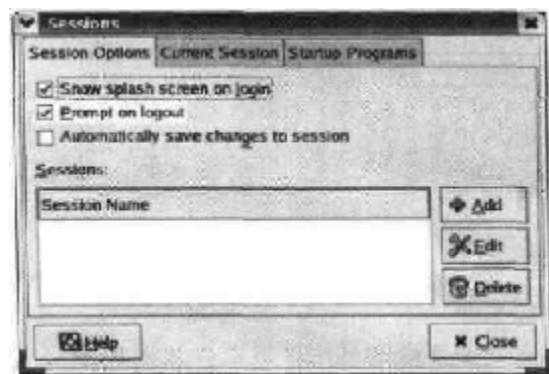


图16.57 GNOME会话管理

多媒体

单击Main Menu►Sound & Video时还有几个GNOME多媒体应用程序，如图16.58，包括各种声音与光碟播放器和声音控制实用程序。这个菜单中显示的一些多媒体应用程序与KDE相关，将在第17章介绍。

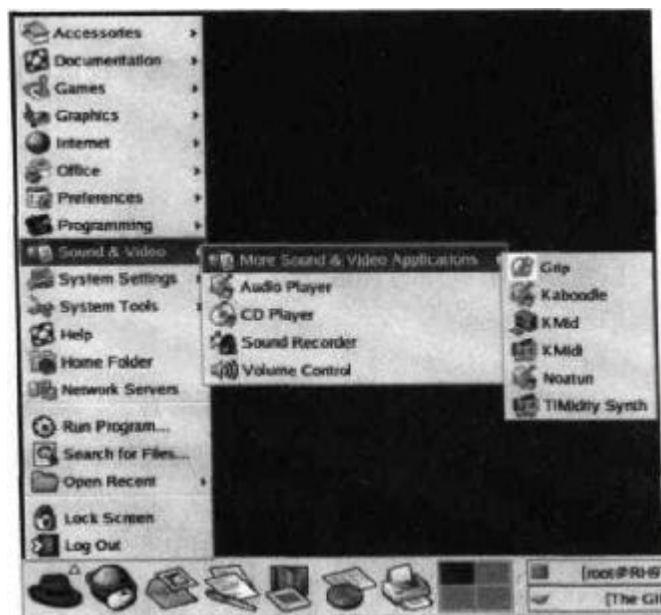


图16.58 多媒体菜单

声音播放器

声音播放器是个X多媒体系统(XMMS)。尽管多媒体播放器本身好像很简单(如图16.59),但可以建立虚拟录音工作室,可以混合不同声音。



图16.59 多媒体播放器

光碟播放器

GNOME光碟播放器是声音光碟的易用播放器。如图16.60,它的标准按钮可以播放和移动光碟磁道。

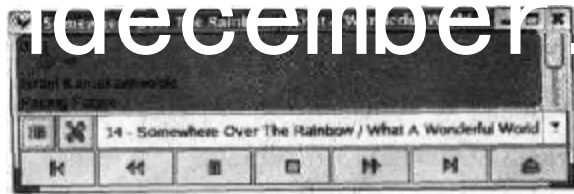


图16.60 光碟播放器

如果单击歌名,则可以从光碟中选歌。歌名左边的两个按钮可以编辑歌曲数据库和管理光碟播放器选项。

声音录制器

声音录制器录制来自声卡麦克风端口的声音。也可以播放录制的任何.wav文件声音。此外,它的混音功能可以控制多个声源的音量。

音量控制

gnome-volume-control实用程序可以控制多个声源的音量,如图16.61。

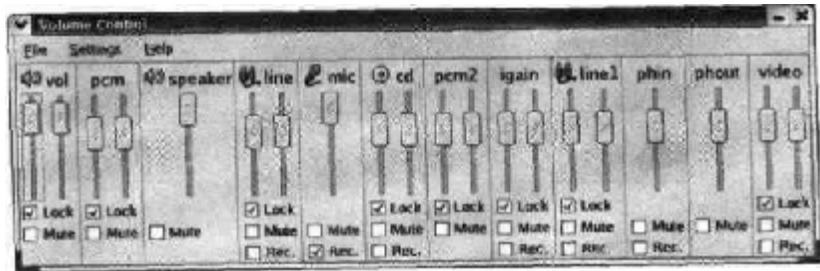


图16.61 GNOME音量控制

Grip

Grip (GNOME rip) 是个GNOME光碟播放器和刻录器，可以从光碟取得音乐或下载音乐，可以按所要顺序配置要进行刻录的音乐。如图16.62所示，它有几个配置标签，窗口底部还有标准光碟功能。表16.7简要介绍Grip配置标签。

文件通常保存成~/ogg目录中的.ogg格式，.m3u格式放在与艺术家姓名相关的子目录中。

说明：我们不鼓励也不默许非法录制音乐，本书只是介绍不同Linux程序的功能。

表16.7 Grip配置标签

标签	描述
Track	列出光碟上的声音磁道，双击歌名可以将其加进Rip表中
Rip	可以录制所选歌曲
Config	包括光碟、默认录制器、编码器等的各种配置参数
Help	显示与不同Grip功能相关的帮助按钮
About	列出Grip版本与主页

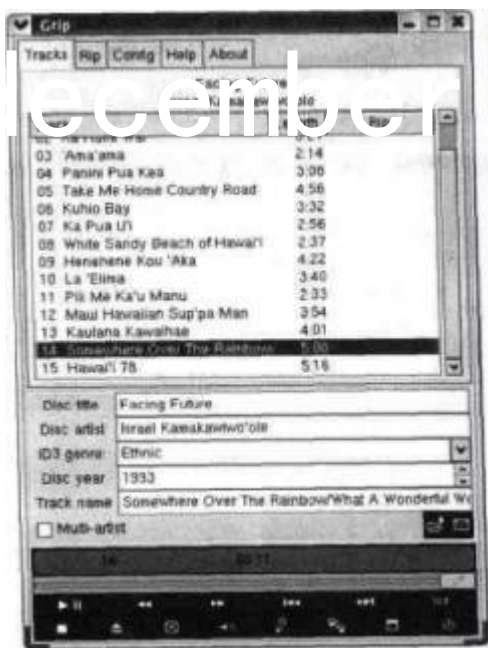


图16.62 GNOME光碟播放器和刻录器

系统工具

系统工具多种多样。许多redhat-config-*工具将在第19章介绍。本节介绍其他工具。图16.63显示了系统工具菜单。

X光碟写入器

X光碟写入器工具如图16.64，可以复制和写入音乐与数据光碟。使用X光碟写入器之前，首先要单击Setup从主菜单中进行配置，以便验证光碟探测、修改所录制映像文件的地址，等等。

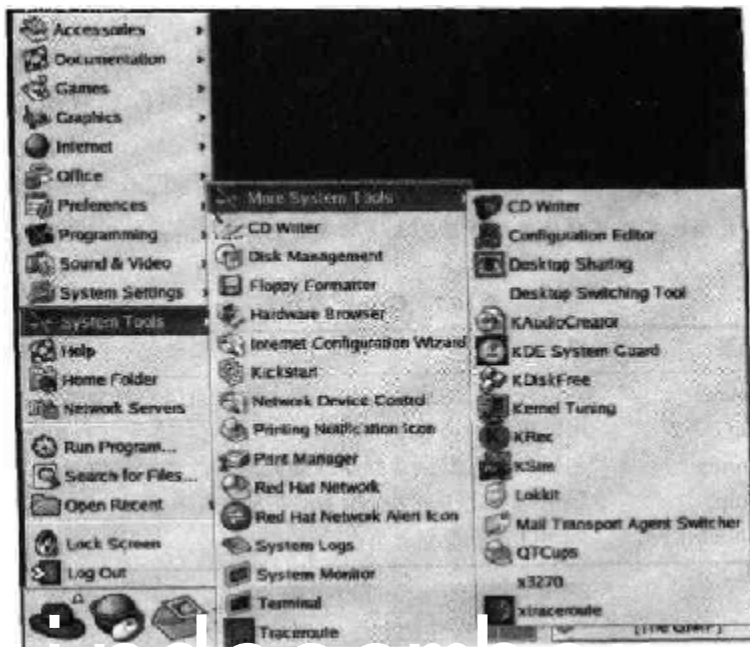


图 16.63 系统工具菜单

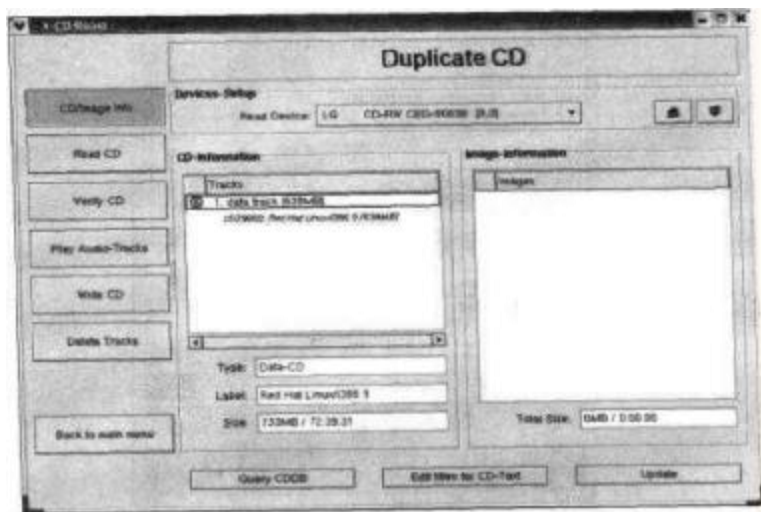


图16.64 X光碟写入器

磁盘管理

用户装载工具如图16.65，演示各种Linux文件系统的当前状态，基于/etc/fstab。可以用其装载或格式化/mnt/floppy之类文件系统。

软盘格式化

gfloppy工具可以格式化软驱中的软盘，可以选择安装的软驱，指定数据格式与长度、命名卷和在不同方式中格式化。

硬件浏览器

硬件浏览器演示了计算机上探测的设备，如图16.66。这个硬件浏览器仅仅提供信息，无法进行配置。

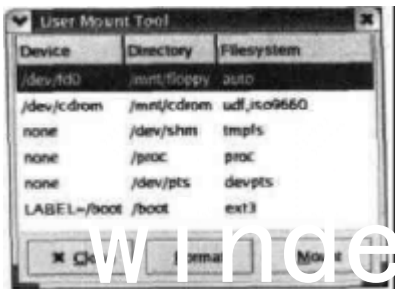


图16.65 用户装载工具

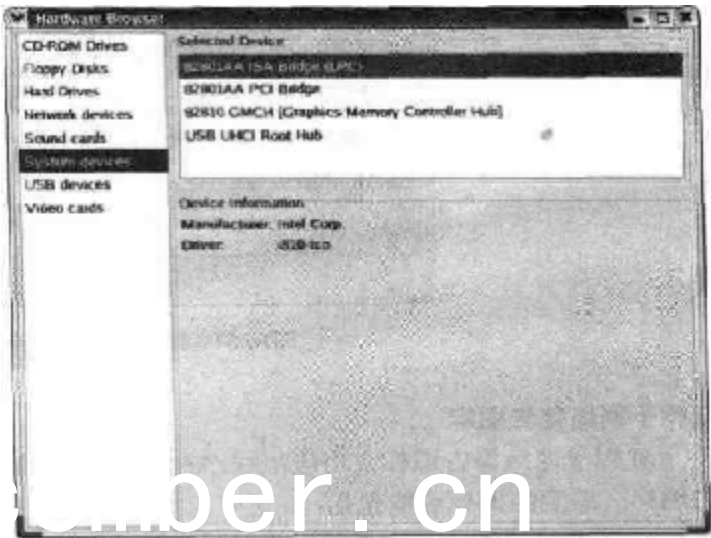


图16.66 硬件浏览器

打印通知图标

选择打印通知图标时，激活拖放式打印功能。

打印管理器

GNOME打印管理器可以控制与管理打印机和打印作业。如果没有配置任何打印机，则其启动redhat-config-printers实用程序，见第25章介绍。

红帽子网络

红帽子网络配置工具如图16.67，将up2date连接的默认设置为红帽子网络管理服务器。它有三个标签，如表16.8所示。

表16.8 红帽子网络配置标签

标签	描述
General	指定安全红帽子网络服务器的路径和网络中可能需要的任何代理服务
Removal / Installation	配置包读取、安装与验证设置
Package Exceptions	设置up2date过程中要跳过的RPM包与文件

说明：关于红帽子网络的更多信息，见第3章和第10章。

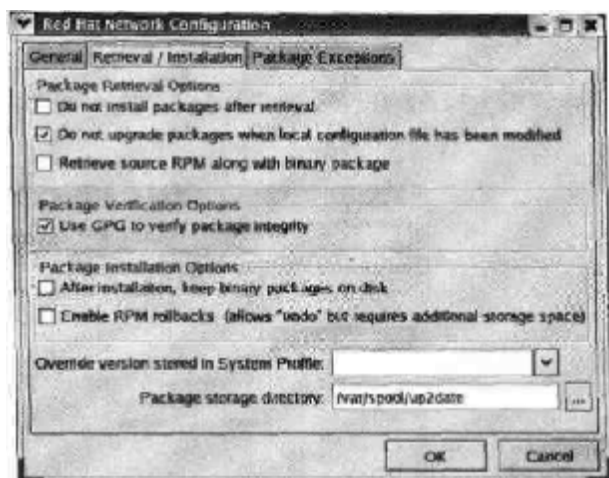


图16.67 红帽子网络配置工具

红帽子网络警告图标

红帽子网络警告图标实用应用程序在工具栏中增加一个圆形图标。默认已经有一个警告图标。看到的图标可能包括:

- 蓝色复选标志表示系统上的包是更新的。
- 绿色箭头对表示系统与红帽子网络通信。
- 红色感叹号表示红帽子网络中的最新包不在系统中。

系统监视器

GNOME系统监视器可以监视当前进程,以及CPU和交换分区用量,是top命令的定制前端。图16.68显示的系统监视器标签演示了系统负载。

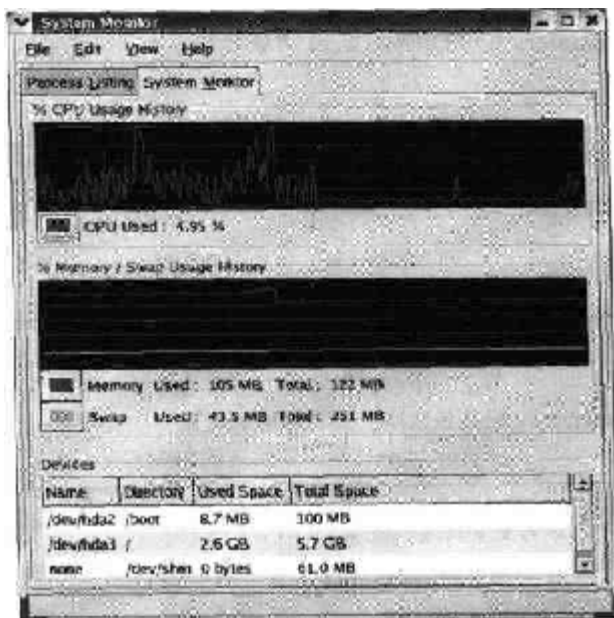


图16.68 GNOME系统监视器

终端

GNOME终端是GNOME桌面使用的标准命令行界面，采用黑白界面，很容易阅读。本书的大多数命令行屏幕图形都使用GNOME终端。

traceroute

traceroute命令有两个相关的系统工具，映射从计算机到目标的数据路径。图16.69用xtraceroute演示了我的计算机与Egypt Air站点之间的连接路径。

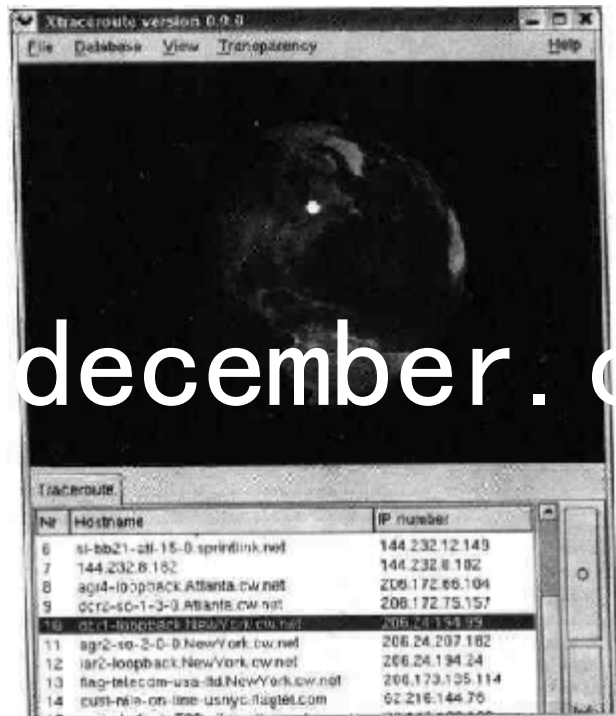


图16.69 跟踪网络路由

光碟写入器

GNOME光碟写入器称为GnomeToaster，如图16.70，可以配置声音和数据光碟，具有大量选项，支持拖放式复制。

配置编辑器

GConf是用户主目录中所有设置的配置编辑器。Microsoft Windows用户很熟悉图16.71的注册表式界面，修改时对运行GNOME也同样危险。但是，这是个综合界面，可以编辑GNOME设置而不必打开每个GNOME应用程序。

关于使用GConf的更多信息，见developer.gnome.org/feature/archive/gconf/gconf.html。

lokkit

lokkit实用程序可以配置防火墙。在命令行界面中，lokkit的功能与第19章介绍的redhat-

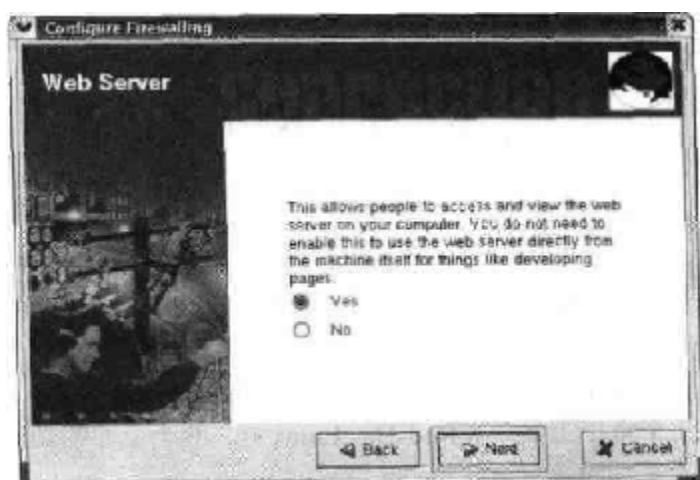


图16.72 lokkit实用程序可以配置防火墙

小结

本章简要介绍了GNOME桌面，它是Red Hat Linux的默认GUI。GNOME中有许多与Microsoft Windows中相似的工具，事实上，还可以在四个不同桌面上分配打开的程序。很容易根据需要配置GNOME桌面。

通过GNOME还可以得到大量功能，包括各种价值几百美元的软件。附件可以满足日常需要，Internet应用程序包括浏览器、邮件管理器和闲聊客户机，声音与视频实用程序可以管理、处理和录制多媒体，GNOME中有几个系统工具，可以帮助管理员管理系统。

下一章介绍最常用的Linux GUI桌面替换—KDE（K桌面环境）。如果你用过KDE，则可以看到，红帽子公司已经将其定制成GNOME的样子。

第17章 KDE

就像还有其他Linux发行版本一样，也还有其他Linux GUI桌面。也许最常用的Linux GNOME桌面替换是KDE（K桌面环境），两者都在Linux用户中非常普及。事实上，许多Linux用户喜欢KDE，包括我自己。尽管Red Hat Linux默认为GNOME，但各大Linux发行版本都允许安装这两个桌面环境。

红帽子公司在实现KDE和GNOME时都集成了“Bluecurve”主题，还在这两个桌面环境的主菜单中集成了几个常用工具。在Red Hat Linux中，两个桌面的功能是重合的，因此，桌面选择完全是个人爱好问题。

尽管KDE与GNOME之间的变化不像Linux与Microsoft Windows之间那么大，但这些桌面来自不同开发环境。KDE使用Qt工具库，是开放源代码许可证下发布的较新版本。大多数KDE开发都是以欧洲为中心的，因此在北美以外非常普及。例如，KDE已经被德国政府作为默认桌面GUI。

本章介绍KDE界面基础，以及与KDE相关的定制程序，我们详细介绍KDE控制中心的功能。从本章可以看到，KDE幕后的人们开发了几个优秀的管理工具，我认为其质量已经超过redhat-config-*工具。

此外，Red Hat Linux中的KDE实现可以使用GNOME应用程序和实用程序，见第16章介绍。如果已经读过第16章，则可以看到本章具有很大的相似性，反映了红帽子公司将Linux GUI标准化的努力。KDE（和GNOME、redhat-config-*）可以通过KDE K Menu按钮直接访问。本章介绍下列主题：

- 使用基本KDE界面
- 使用KDE控制中心
- 了解KDE实用程序

使用基本KDE界面

标准KDE桌面与其他各大GUI操作系统具有相同特征，包括面板、KDE K Menu按钮和图标。可以根据需要定制每个组件，也可以对KDE安装配置标准界面。可以通过KDE控制中心控制和定制KDE外观。如果已经安装KDE并将其设置为默认桌面，则可以打开图17.1所示的视图。

说明：Linux中的面板与Microsoft Windows中的任务栏功能相似。KDE K Menu按钮（表示为红帽子）的功能与Microsoft Start按钮相似，在GNOME中称为主菜单按钮。红帽子公司互换使用这些术语，本章也是这样。



图17.1 KDE桌面

KDE概述

基本KDE界面也很简单。如图17.1所示，包括一个Trash图标和一个软盘管理器，还可以直接访问主目录和访问Start Here目录。这些图标都使用Konqueror，是个“Explorer”式图形Shell，可以管理文件和KDE配置。默认Red Hat Web浏览器仍然是Mozilla，但KDE项目开发了Konqueror。

首次启动KDE时，可以看到“Kandalf's Useful Tips”，这些提示即使对经验不足的计算机用户也很有用。

说明：中间鼠标键在KDE中很有用。在桌面上试试，可以看到什么？在另一个图标上试试，可以看到什么？

下面几节介绍面板和KDE控制中心的按钮。

KDE面板








KDE面板可以调用几个应用程序、在打开程序间切换和在打开桌面间切换。图17.2显示了我的KDE面板，这里，KDE面板左边有六个图标，如表17.1所示。

说明：KDE中有四个标准桌面，也称为工作空间。每个工作空间有自己的图标和打开程序。一下子看不到四个工作空间，三个工作空间的数据存放在多余显示内存中，稍后将会看到，KDE桌面很容易定制。



图17.2 KDE面板

表17.1 KDE面板图标

图标	描述
	单击这个按钮打开KDE主菜单，可以访问应用程序和实用程序，相当于Microsoft Windows中的Start按钮
	可以打开Mozilla Web浏览器
	启动Evolution个人信息管理器，其功能相当于Microsoft Outlook
	打开OpenOffice Writer，其功能相当于Microsoft Word
	打开OpenOffice Impress演示管理器，其功能相当于Microsoft PowerPoint
	打开OpenOffice Calc电子表格程序，其功能相当于Microsoft Excel
	打开GNOME打印管理器

说明：OpenOffice应用程序组件也称为OpenOffice.org OOo，按GNU通用许可证和Sun公司行业标准源代码许可发布。

KDE工作空间与打开程序

KDE很灵活，可以将打开窗口放在几个工作空间。因此我们不需要打开和关闭窗口，只要通过切换工作空间来访问应用程序即可。例如，可以把GIMP图形程序放在一个工作空间，把OpenOffice Calc电子表格放在一个工作空间，把OpenOffice Writer放在一个工作空间，把终端窗口放在一个工作空间。四个工作空间在面板上显示缩略图，如图17.3。注意，活动工作空间加亮显示。



图17.3 四个KDE工作空间

要切换到另一工作空间，单击相应缩略图。要将一个应用程序移到另一工作空间，单击应用程序左上角，在出现的下拉菜单中选择To Desktop，可以看到图17.4所示的下拉菜单。



图17.4 移到工作空间2

还可以在面板上显示的打开应用程序之间切换。例如，图17.5所示的屏幕可以在三个打开应用程序之间切换。



图17.5 打开应用程序之间切换

其他KDE面板项目

最后，面板右端有三个图标。带“K”字样的剪贴板称为Klipper（KDE剪贴板工具），可以在应用程序之间进行复制和粘贴。要配置Klipper，右单击面板图标并从弹出菜单中选择Configure Klipper。

后面的空间可能包括三个图标之一：带感叹号的红色圆圈表示要连接红帽子网络，以检查更新，蓝色复选标志表示系统是更新的，绿色圆圈带箭头表示系统与红帽子网络通信。可以右单击图标，检查或配置与红帽子网络的连接。第10章详细介绍了用up2date使系统保持更新。根据运行的应用程序，这个区中可能还有其他图标。



如果单击面板上的日期和时间，则可以看到本月日历。如果右单击这个区，则可以打开一个菜单，配置时钟外观、时区和格式。

要定制KDE面板，只要单击面板中的打开区，选择Panel Menu►Configure Panel。图17.6显示了KDE控制模块窗口。

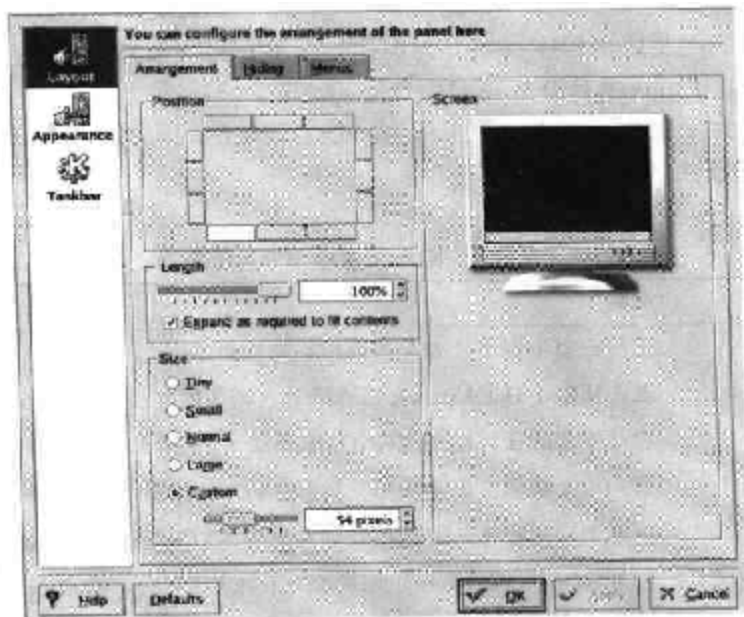


图17.6 KDE控制模块窗口

利用KDE面板属性窗口，可以做几件事。它们与面板外观、地址和主菜单命令的内容有关。

KDE主菜单

下面要介绍KDE主菜单。单击桌面左下角的红帽子，可以看到图17.7所示的菜单。



图17.7 KDE主菜单

可以看出，KDE主菜单打开一系列其他命令和菜单，见表17.2简要介绍。我们将在本章和后面几章详细介绍其中一些菜单。这些菜单中的许多程序是针对GNOME的，见第16章介绍。这个菜单中的主要应用程序（如办公组件与图形）将在第18章介绍。第19章将介绍红帽子特定管理工具。Linux游戏没有在书中介绍。

图17.7的KDE主菜单上方有三个小程序，是当前使用的应用程序。默认情况下，KDE最多存放五个最近使用的应用程序。

表17.2 KDE主菜单命令与子菜单

命令与子菜单	说明
Accessories	打开一组小程序，如文本编辑器和计算器
Documentation	进入从Red Hat Linux文档光碟装入的任何文档，见第16章
Games	启动安装的任何KDE或GNOME游戏
Graphics	访问用于编辑、屏幕快照、传真、PDF阅读器等图形应用程序
Internet	一系列应用程序，可以在互联网之类的TCP/IP网络上通信
Office	打开与OpenOffice程序组相关的一系列应用程序，KOffice放在这个目录的More Office Applications子菜单中
Other	许多有趣的KDE工具，许多在教育中使用
Preferences	可以定制设置，通常与桌面有关

(续表)

命令与子菜单	说明
Programming	可以访问一组编程工具, 奇怪的是, 这个组中还包括Emacs
Sound & Video	增加多媒体应用程序, 包括光碟刻录程序
System Settings	可以访问许多redhat-config-*管理实用程序, 大多数要求根用户级访问
System Tools	启动各个管理工具的菜单
Control Center	打开KDE控制中心, 是个综合配置与信息工具
Find Files	开始寻找文件的实用程序, 可以搜索文件和浏览文件属性
Help	在简化浏览器中打开KDE帮助会话
Home	启动Konqueror, 提供主目录中文件的视图
Run Command	打开Run Command对话框, 可以输入应用程序的文本名
Lock Screen	启动安全屏幕保护程序, 要返回桌面, 需要输入用户名和口令
Log Out	退出KDE

如果看不到特定菜单, 则可能是没有安装相关软件包。例如, 要看到Games菜单, 一定要先安装 `kde-games` 包。

KDE控制中心

下面要介绍KDE桌面的一些详细配置选项, 可以通过KDE控制中心访问。可以从主菜单中选择Main Menu►Control Center打开KDE控制中心, 其打开Control Center窗口, 有一系列图标, 如图17.8。可以看出, 控制中心可以配置计算机的各个方面, 包括外观、主题和Web浏览。下面几节介绍这个区中的每个工具。

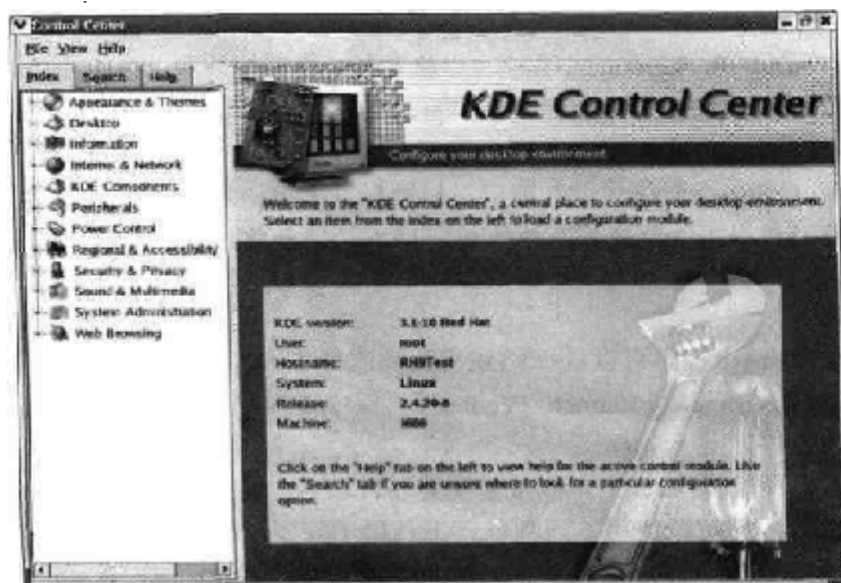


图17.8 KDE控制中心

改变配置时，可以单击Apply按钮，将改变写入 ~/.kde目录（第8章曾介绍过，~表示主目录）。

说明：KDE控制中心的有些小程序要求管理访问。如果是普通用户而非根用户，要求根权限时则会出现Administrator Mode按钮。如果要改变这些类型的设置，可以单击Administrator Mode按钮并在出现的Run As Root窗口中输入根口令。

外观与主题

KDE控制中心外观与主题部分可以定制KDE桌面的外观。可以用图17.9所示的各种功能定制桌面背景和窗口外观（窗口装饰）。

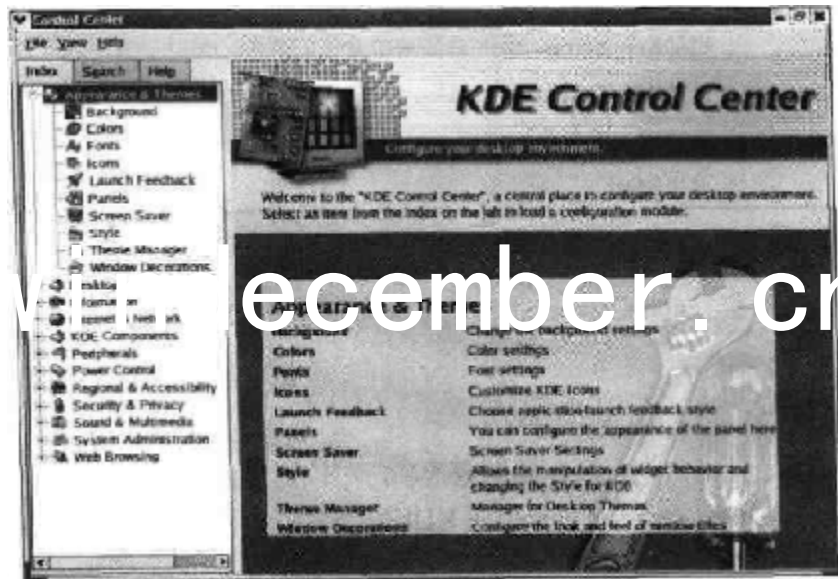


图17.9 外观与主题

Background Background小程序可以修改每个桌面的外观。在KDE中，其很容易定制。除非激活图17.10中的Common Background选项，否则可以对每个桌面配置不同背景与墙纸。

Colors Colors小程序可以对窗口、标题栏、菜单、按钮、链接等配置几个颜色模式。总共有25种以上的颜色模式，还可以导入其他颜色模式，见图17.11。

Fonts Fonts小程序可以配置桌面上不同位置的不同字体，如菜单、任务栏、窗口标题，等等。

Icons Icons小程序可以选择KDE桌面的图标模式。

Launch Feedback Launch Feedback小程序通常配置成在桌面上运行OpenOffice之类的应用程序时显示光标。

Panels 可以对面板上不同按钮配置不同颜色。K菜单按钮、应用程序、窗口标题和其他面板内容可以使用不同颜色。工具提示简要地描述图标功能，在光标放在图标上时显示。

Screen Saver KDE配置了多种屏幕保护程序，如图17.12。可以将屏幕保护程序设置成在一定非活动时间后启动，要输入口令才能返回桌面。

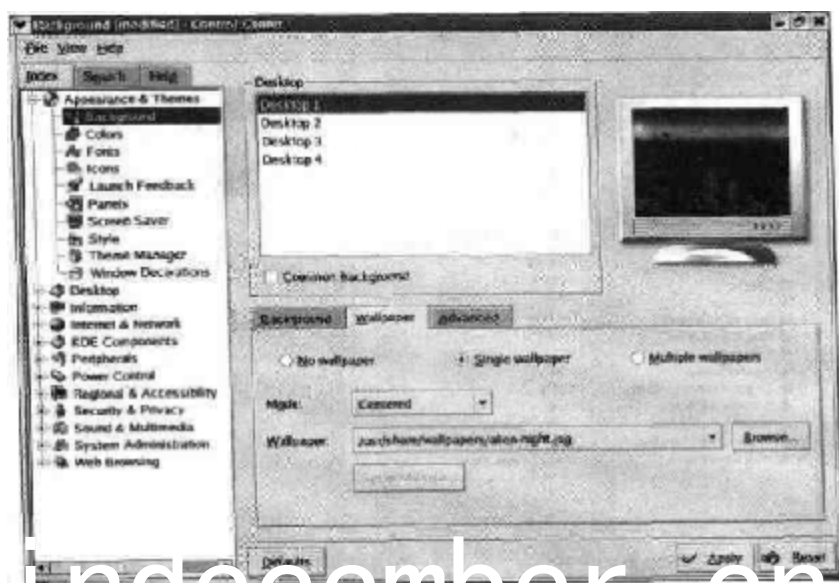


图17.10 配置桌面背景

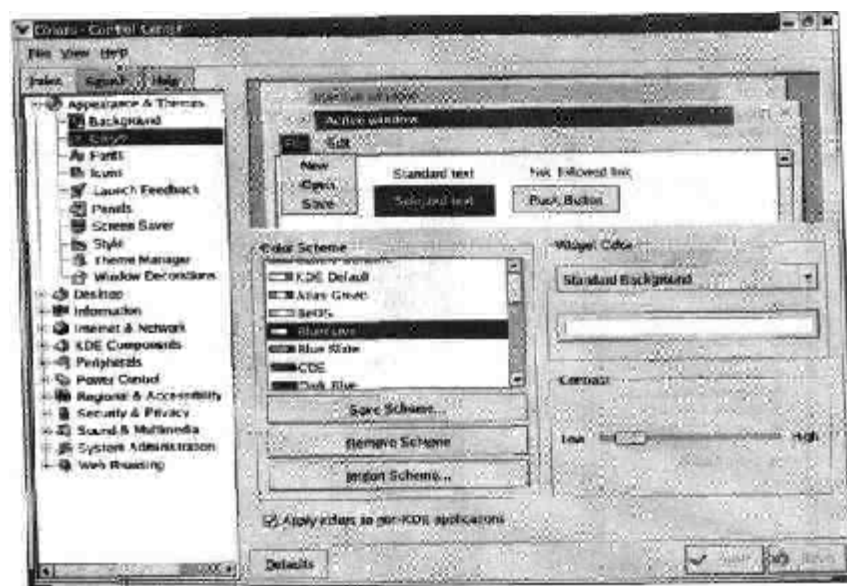


图17.11 配置桌面颜色

Style KDE可以配置与标签、按钮、复选框等相关的样式。可以选择二十多种不同样式，然后对所选样式配置不同效果。

Theme Manager 可以用不同主题配置桌面外观，如图17.13。红帽子KDE桌面默认为Bluecurve主题，但可以配置所选主题，定制其在桌面中采用的外观。

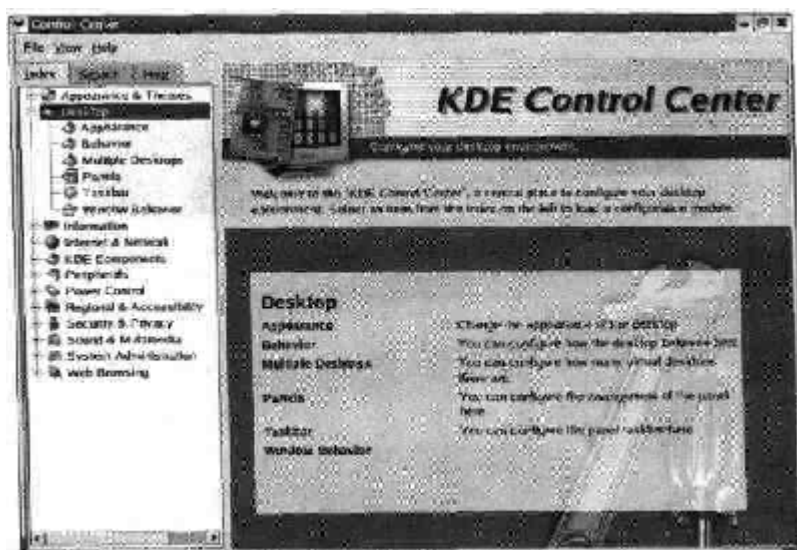


图17.14 桌面控件

Appearance Appearance 小程序可以设置在桌面的标准字体和文本颜色。

Behavior Behavior 小程序如图17.15，可以定制桌面图标和Konqueror中文件管理器视图的外观。还可以定制鼠标单击的响应和桌面上显示的设备图标。

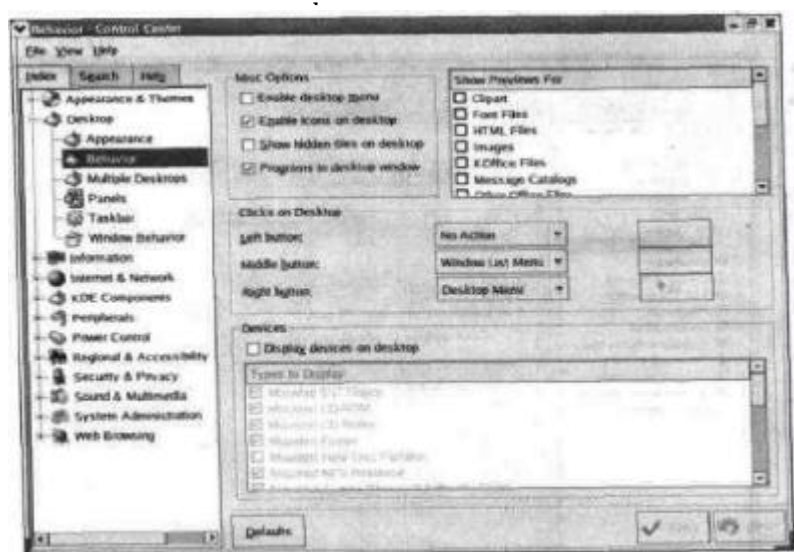


图17.15 桌面行为

Multiple Desktops 默认情况下，KDE有四个桌面，通过这个小程序可以配置最多16个不同桌面。

Panels 可以设置面板位置和长度，以及相关图标尺寸。可以将面板设置成隐藏。还可以在K菜单中建立不同设置。图17.16显示了这个小程序。

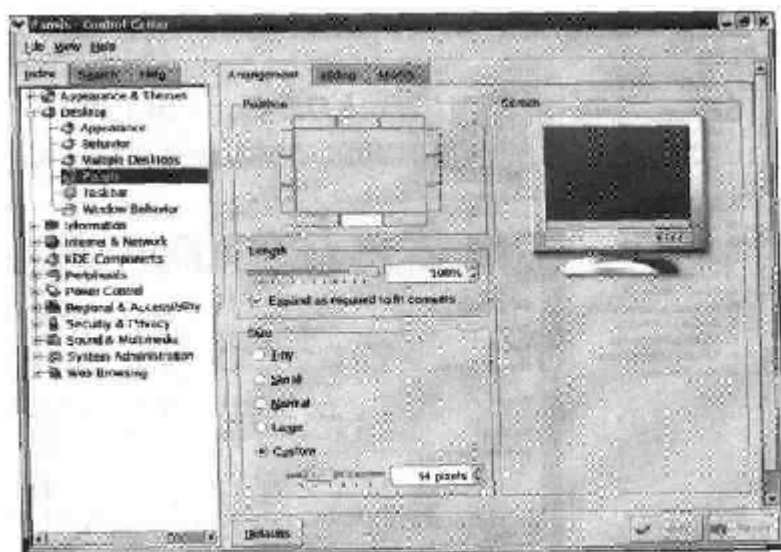


图17.16 设置面板

Taskbar: Taskbar 小程序可以确定打开应用程序的行为, 以及左、中、右鼠标键单击的相关操作。

Window Behavior Window Behavior 小程序如图17.17, 可以定制打开的窗口如何响应鼠标光标和如何移动。高级设置可以设置打开窗口的动画特性。

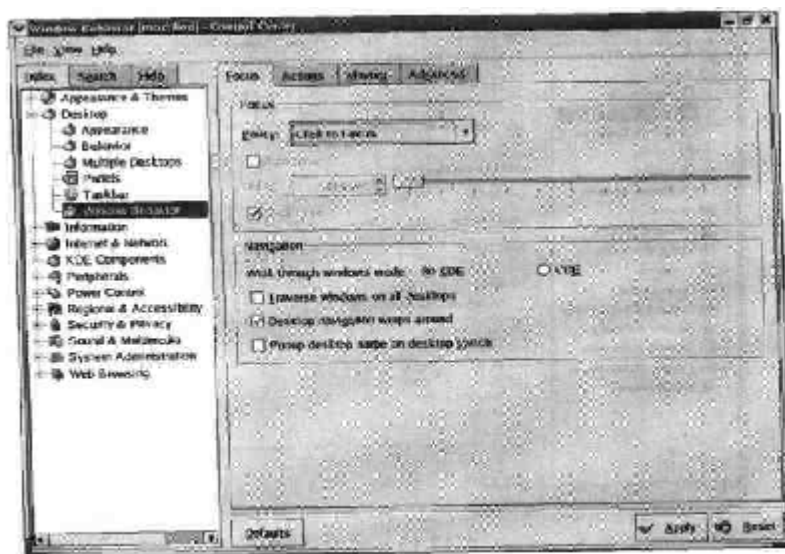


图17.17 设置窗口行为

信息

KDE控制中心的信息部分是探测到的硬件系统信息的图形化视图, 主要来自`/proc`目录, 见第11章介绍。图17.18显示了硬件信息表, 表17.3描述了KDE控制中心的硬件信息。

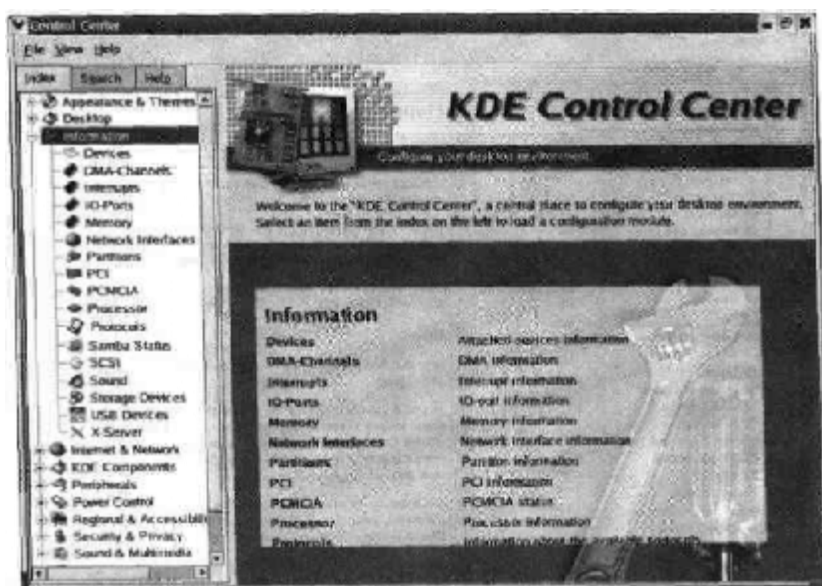


图17.18 硬件信息

表17.3 KDE控制中心的硬件信息

小程序	描述
Devices	列出从 <code>/proc/devices</code> 与 <code>/proc/misc</code> 中探测的设备文件
DMA-Channels	列出占用的直接内存地址信道，这个信息来自 <code>/proc/dma</code>
Interrupts	显示所有占用的中断请求（IRQ）信道，这个信息来自 <code>/proc/interrupts</code>
IO-Ports	列出输入/输出地址与相关硬件，这个信息来自 <code>/proc/iports</code>
Memory	显示当前内存与交换运行用量，数据用 <code>top</code> 命令取得，用于 <code>/proc/meminfo</code>
Network Interfaces	演示所探测网络适配器的当前IP地址和状态信息
Partitions	列出通过 <code>/etc/fstab</code> 装载的目录
PCI	列出探测的PCI卡、控制器和网桥，可能包括未配置硬件，如第二个网卡和Winmodems。这个信息来自 <code>/proc/pci</code>
PCMCIA	显示便携计算机可用的控制器，PCMCIA设备采用PCMCIA标准，也称为PC卡。这个信息来自 <code>/proc/pci</code>
Processor	显示所探测CPU的特性，这个信息来自 <code>/proc/cpuinfo</code>
Protocols	提供几个协议的定义，例子见图17.19
Samba Status	演示Samba客户机与服务器连接，包括其他计算机和共享Samba目录
SCSI	列出连接的SCSI设备
Sound	列出与声卡相关的信息
Storage Devices	显示装载的本地和网络存储设备，反映 <code>mount</code> 命令
USB Devices	显示安装的USB硬件
X-Server	演示图形配置，这个信息来自 <code>/etc/X11/XF86Config</code>

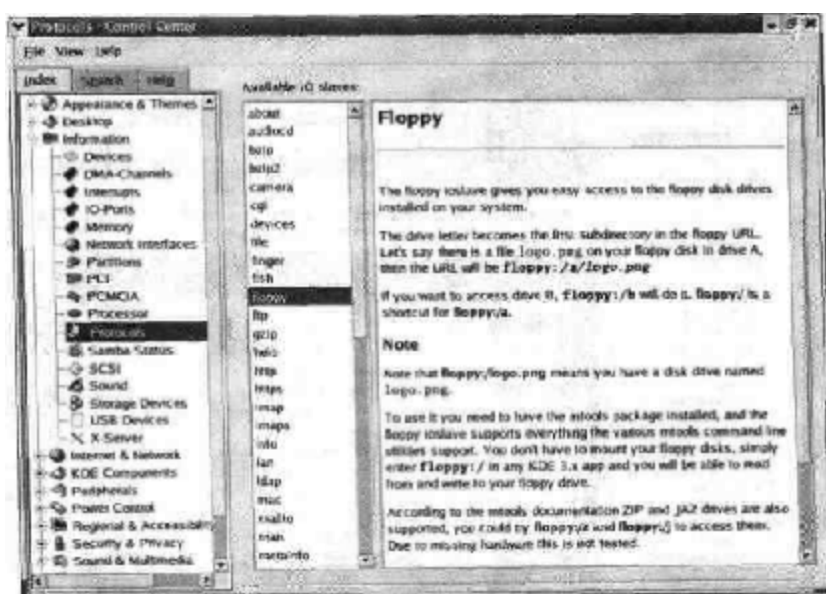


图17.19 KDE控制中心的协议定义

Internet与网络

KDE控制中心的Internet与网络部分可以配置网络与共享目录的参数。可以用图17.20所示功能，定制从电子邮件默认到代理服务器的一切。如果单击这个部分的项目而得到一个错误消息，则可能没有安装相关的软件包。

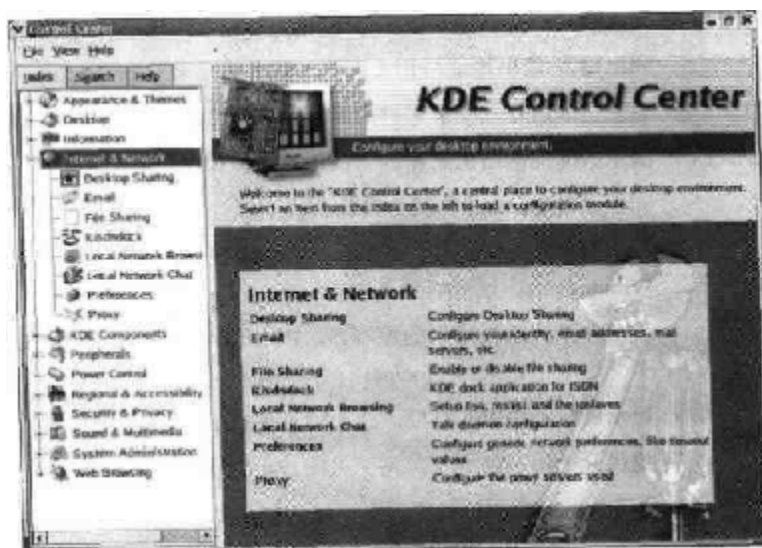


图17.20 Internet与网络

Desktop Sharing KDE Desktop Sharing小程序支持VNC（虚拟网计算）服务（见第16章介绍），使别人可以远程连接你的GUI。

Email Email小程序可以对发送电子邮件建立基本默认值，包括姓名、电子邮件地址、单位、答复地址和发送（SMTP）邮件服务器。

File Sharing 如果支持文件共享，则用户可以通过网络从主目录共享文件。支持的方法包括NFS（网络文件系统，见第28章）和Samba（见第29章）。

Kisdndock 这个小程序可以配置任何安装的ISDN服务。ISDN（综合服务数字网）是个数字化Internet连接选项，速度为普通电话MODEM的两倍左右。由于ISDN在欧洲很普及，因此，主要在欧洲开发的KDE提供了坚实的ISDN支持。

Local Network Browsing Local Network Browsing小程序可以设置默认用户名和口令，通过Samba网络连接共享目录和打印机。第29章将会介绍，这是从Microsoft Windows计算机连接共享目录和打印机的常见方法。

Local Network Chat Local Network Chat小程序可以对本地网络配置闲聊监控程序。

Preferences Preferences小程序确定连接Internet之类的外部网络时，KDE程序如何响应。例如，可以对低速Web站点配置超时值，可以配置被动方式（用于连接多个FTP服务器）。

Proxy 许多网络用代理服务器进行保护。如果你的计算机在这种网络中，则可以用这个小程序配置与该服务器相关的设置。然后可以连接Internet之类的外部网络。

KDE组件

KDE组件部分可以配置与各种KDE实用程序相关的基本参数，包括地址簿相关资源和退出KDE桌面时的设置。

图17.21显示了基本KDE组件。

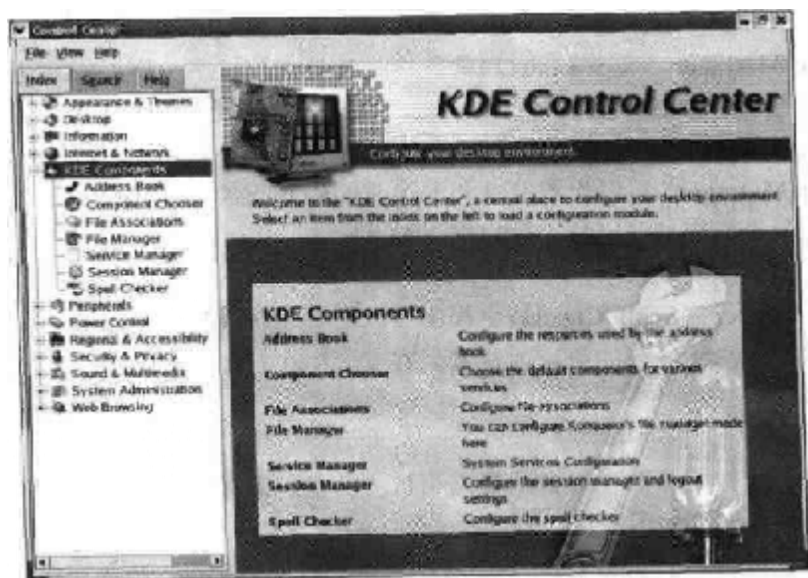


图17.21 KDE组件

Address Book KDE Address Book可以加入标准.vcf地址簿文件，也可以转换其他文件或LDAP（轻量级目录辅助协议）数据库中的地址簿。

Component Chooser KDE Component Chooser可以选择默认电子邮件客户机、嵌入文本编辑器和终端仿真程序。

File Associations KDE File Associations小程序可以设置与不同文件类型相关的应用程序。例如，图17.22显示了与.jpg图形文件相关的应用程序。

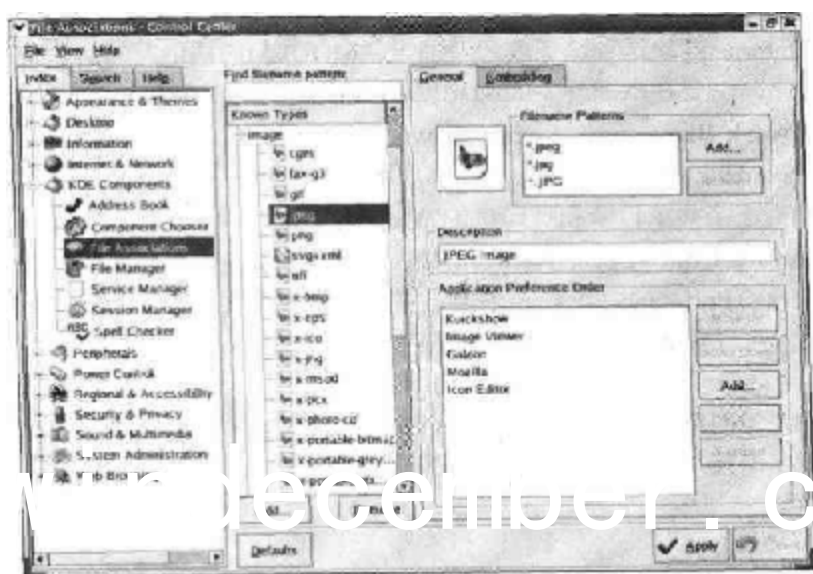


图17.22 KDE文件关联

File Manager KDE File Manager小程序配置Konqueror中的文件外观，包括字体、打开新目录时的行为、删除文件时的确认、小于配置尺寸的文件预览/缩略图。

Service Manager 就像Linux启动各种服务与监控程序一样，KDE也启动服务。有些KDE服务在启动KDE GUI时自动装入，有些则在需要时启动。可以通过这个小程序配置这些服务。

Session Manager 可以设置登录和退出时的KDE行为。具体地说，可以配置重新打开时KDE是否响应与退出时运行的相同实用程序。也可以指定计算机是否在Konqueror中存在、重新启动或关闭。

Spell Checker Spell Checker小程序可以配置系统的默认拼写检查程序。可用的拼写检查程序取决于安装的语言，这发生在安装Red Hat Linux时。

外设

外设部分可以配置四个设备：数码相机、键盘、鼠标或其他指示设备、打印机。KDE控制中心的外设部分如图17.23。

Digital Camera Digital Camera小程序可以配置数码相机，将其连接KDE桌面。例如，图17.24选择和配置一个数码相机设置。

Keyboard Keyboard小程序可以设置键盘响应的一些基本参数，包括重复速率、数字锁键的默认条件和键对其他活动类型的响应。

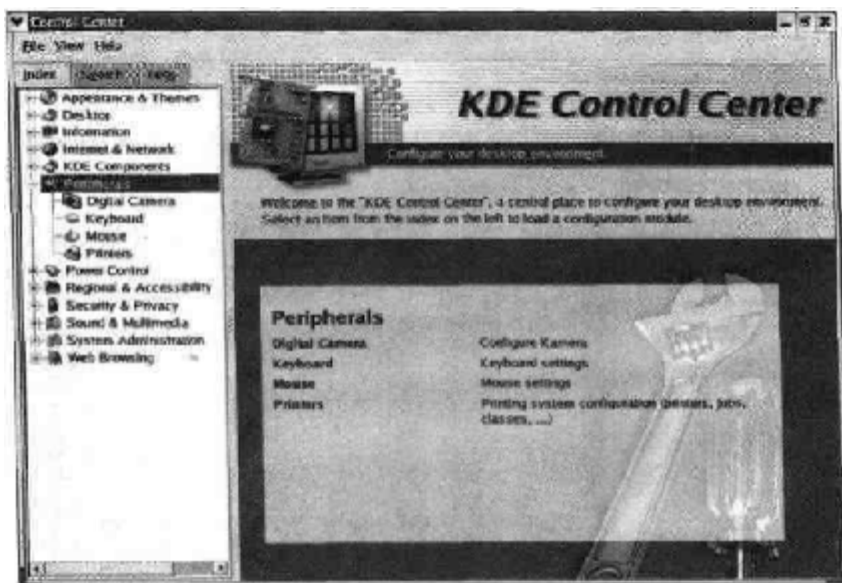


图17.23 KDE控制中心的外设部分

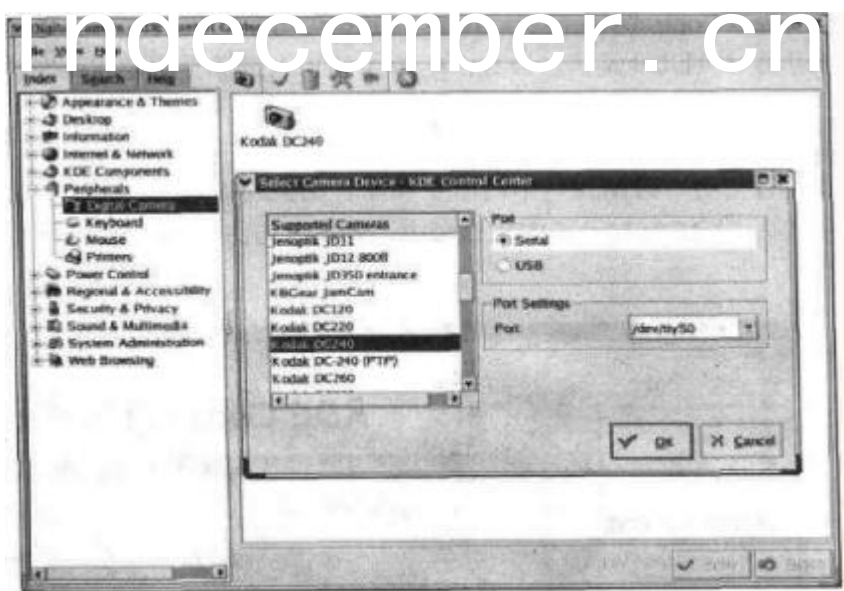


图17.24 在KDE控制中心配置数码相机

Mouse Mouse小程序配置鼠标键、单击与双击的效果和光标行为。还可以用数字键盘上的键移动光标。

Printers KDE中可以将打印作业发送到不同地址，包括传真或文件中。利用这个小程序，可以配置每个打印位置的特性，直到符合图形的颜色设置。

电源控制

电源控制部分可以控制电源管理设置，包括便携电脑的电源设置（如有）。图17.25显示了KDE控制中心的电源控制部分。

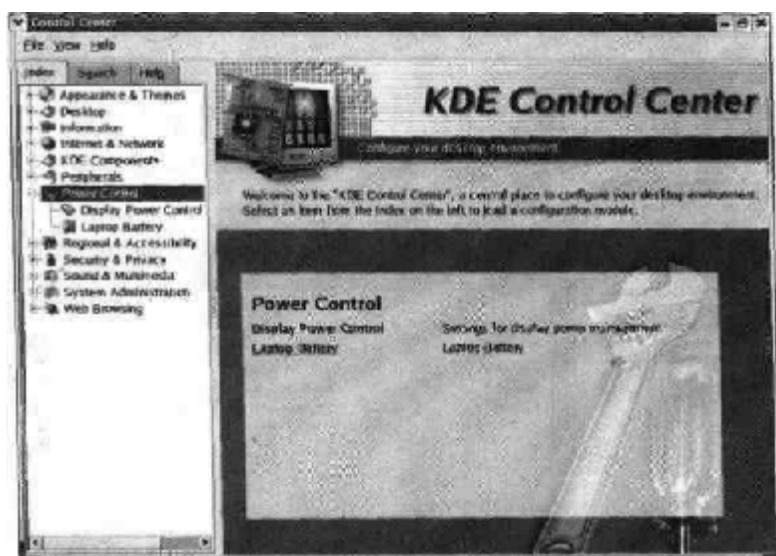


图17.25 KDE控制中心的电源控制

Display Power Control 小程序可以记录一些在充电期之后的准备、启动和断电方式。Laptop Battery 小程序可以设置状态检查、电源控制和电量低于指定水平时的操作。

地区与访问性

地区与访问性部分可以配置与不同国家和语言相关的格式，还可以设置键盘铃声和对不同控制键的响应。图17.26显示了KDE控制中心的地区与访问性部分，表17.4显示了相关小程序。

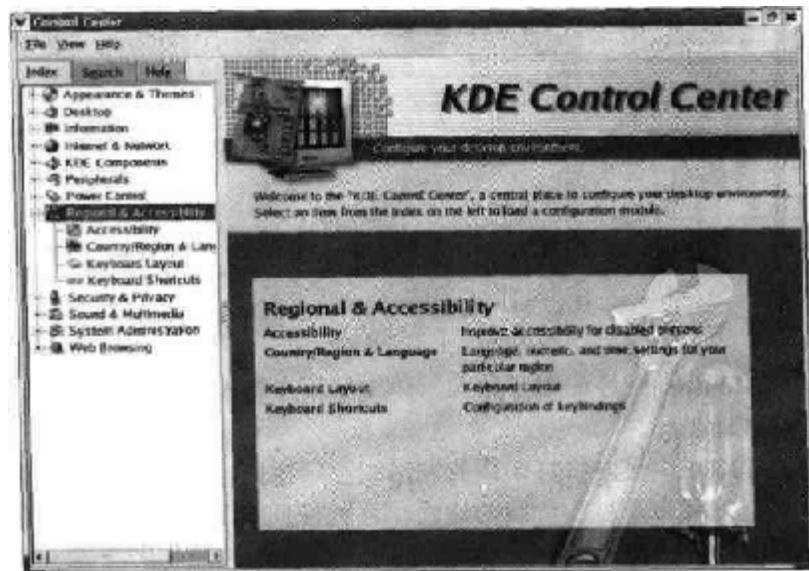


图17.26 KDE控制中心的地区与访问性部分

表17.4 地区与访问性部分的小程序

小程序	描述
Accessibility	配置键盘铃声设置和粘性、低速、回弹键
Country/Region & Language	支持定制数字、币值、日期与时间格式和测量系统
Keyboard Layout	可以设置不同国家键盘布局，以及和Alt、Ctrl、Shift、Caps Lock等控制键相关的快捷功能
Keyboard Shortcuts	支持对各种操作配置键盘快捷组合

安全与隐私

安全与隐私部分可以配置加密与口令设置。KDE控制中心的这个部分如图17.27。

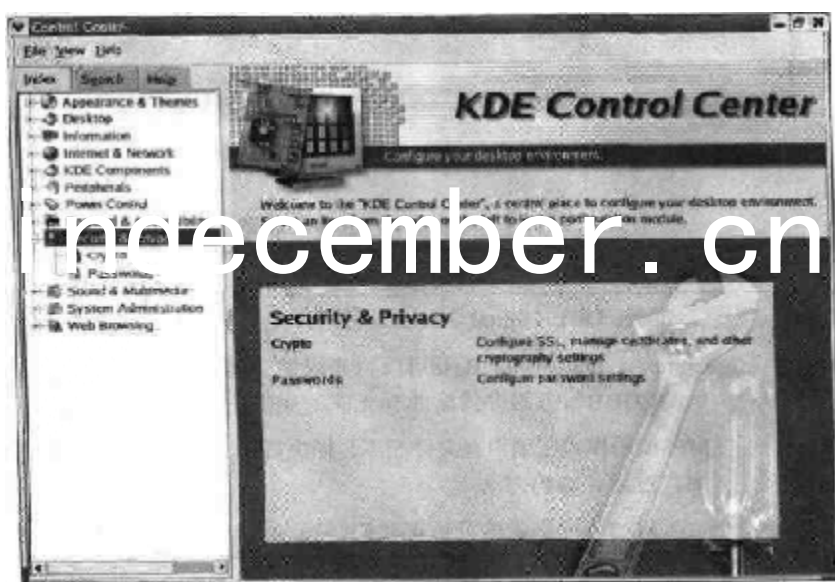


图17.27 KDE的安全与隐私

Crypto 小程序可以配置SSL（安全套接层）加密代码和证书，**Passwords** 小程序可以设置输入口令时回显的内容和KDE记住最近所输口令的时间。

声音与多媒体

声音与多媒体部分可以配置与声卡相关的设置，包括音乐文件、默认音量、混音器和输入速率。还可以配置系统铃声音量和不同事件相关的声音。KDE控制中心的声音与多媒体部分如图17.28。

Audio CD Audio CD小程序可以配置几种设置，见表17.5。

Mixer Mixer小程序可以配置音量、探测混音器和各个混音器的设备。

Sound System Sound System小程序可以配置KDE声音服务器，称为aRts，这是个模拟实时合成器。这个小程序有四个标签，见表17.6。

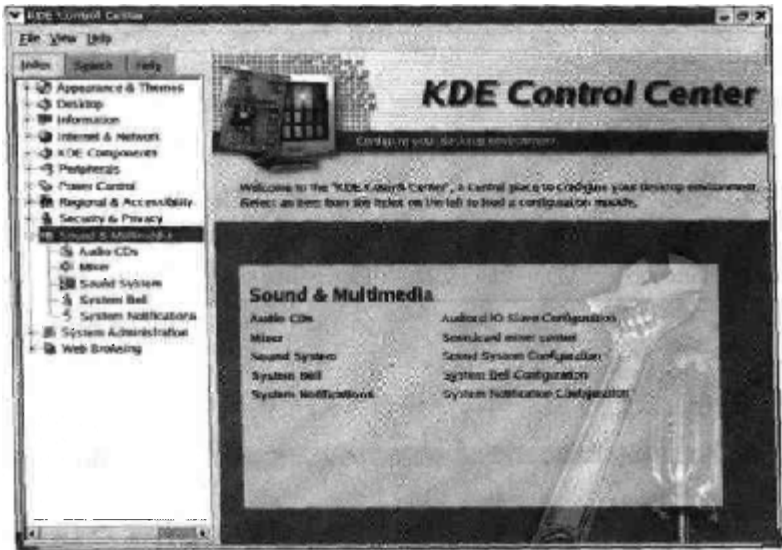


图17.28 KDE控制中心的声音与多媒体部分

表 17.7 Audio CD 小部件设置

类别	描述
CDDA	Compact Disk Digital Audio设置可以配置光碟设备探测与错误纠正
CDDDB	Compact Disk Data Base可以将光碟播放器设置成通过freedb.org等提供的CDDDB服务器寻找歌曲与光碟的更多信息
MP3	MP3编码模式压缩声音文件而不会损失质量，相关选项可以配置MP3压缩、过滤和编码方法
Ogg Vorbis	这是MP3压缩格式的开放源代码替换（这个名称来自视频游戏操作）

表17.6 Sound System标签

标签	描述
aRts	可以配置KDE声音服务器的基本设置，可以设置不同服务器消息级（err、warn、info、debug）的声音消息
Sound I/O	可以配置输入/输出、定制设备、质量和缓冲区长度
Mixer	设置与Audio CD小程序相同的信息
MIDI	可以根据音乐器材数字接口设置合成器接口

System Bell System Bell小程序可以配置这个警告设备的音量、音调和时间。

系统通知 可以对各种事件配置声音与文本消息，如图17.29，可以对表17.7所列的各种事件配置不同响应，可以单击窗口上方的下拉文本框，在不同类别间切换。

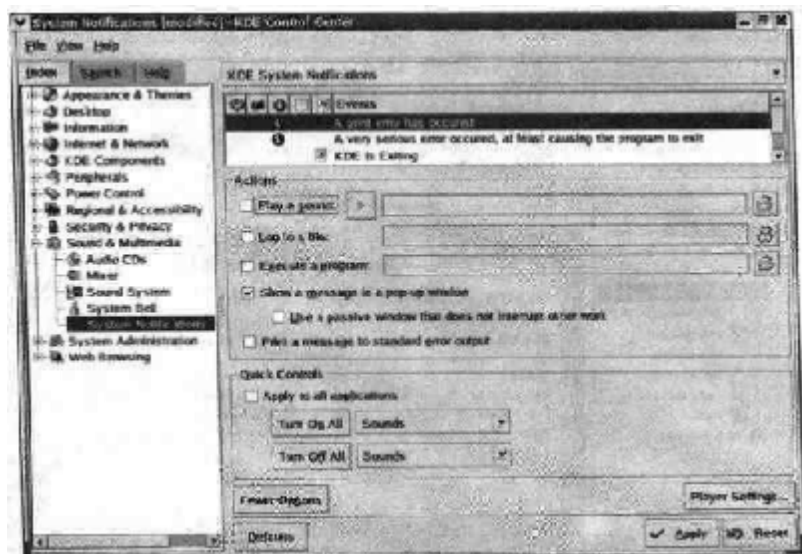


图17.29 KDE系统通知

17.7 与KDE桌面环境相关的声音事件

应用程序	描述
AOL IM Client	可以配置Gaim之类的立即消息器，对不同事件播放声音，适用于America Online的Instant Messenger插件配置Gaim
Desktop Sharing	可以在计算机与网络上其他计算机连接时配置声音事件
KDE Screen Ruler	可以在移动KDE屏幕标尺时配置声音，可以用K Menu►Graphics►More Graphics Applications►Screen Ruler访问
KDE System Guard	支持与这个实用程序中设置的极限相关的声音设置，通过K Menu►System Tools►More System Tools►KDE System Guard访问
KDE System Notifications	可以配置与KDE桌面中基本操作相关的声音
KInetD	可以在别人连接你的xinetd服务器时设置声音
KMail	可以在新邮件进入邮件程序时设置声音
KSirc	支持KSirc Internet中继聊天应用程序中的声音事件
News Ticker	类似于KMail，适用于有指导的新闻组
The KDE Window Manager	可以配置与KDE窗口相关基本操作有关的配音

如果安装了kdegames-* RPM包，则还可以修改与一些游戏相关的声音设置。

系统管理

System Administration小程序可以配置各种管理设置。KDE控制中心的系统管理部分如图17.30。

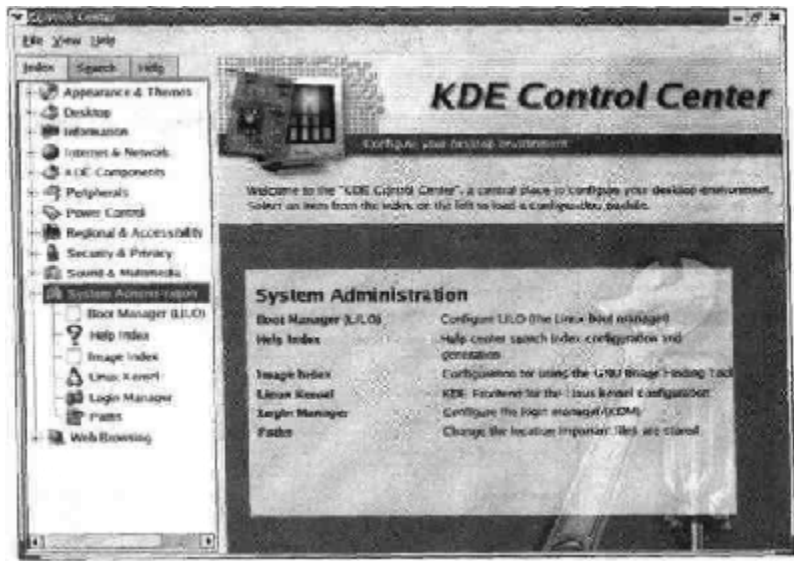


图17.30 KDE的系统管理

引导管理器 (LILO) 默认红帽子引导管理器是GRUB。但如果使用LILO，则可以用Boot Manager (LILO) 小程序作为修改/etc/lilo.conf的GUI前端。这里所做的改变在Expert标签中立即反映出来。

Help Index 这个小程序可以配置和建立与KDE帮助相关的索引。

Image Index 这个小程序可以配置GIFT (GNU图形查找工具)，搜索图形文件名和内容。

Linux Kernel 如果安装了kernel-sources-* RPM内核包，则这个小程序可以改变配置。

Login Manager 这个小程序可以配置KDE显示管理器kdm。和GDM设置实用程序一样，可以用各个标签设置基本外观、语言、字体、背景、会话、合法用户和自动登录设置，如图17.31。

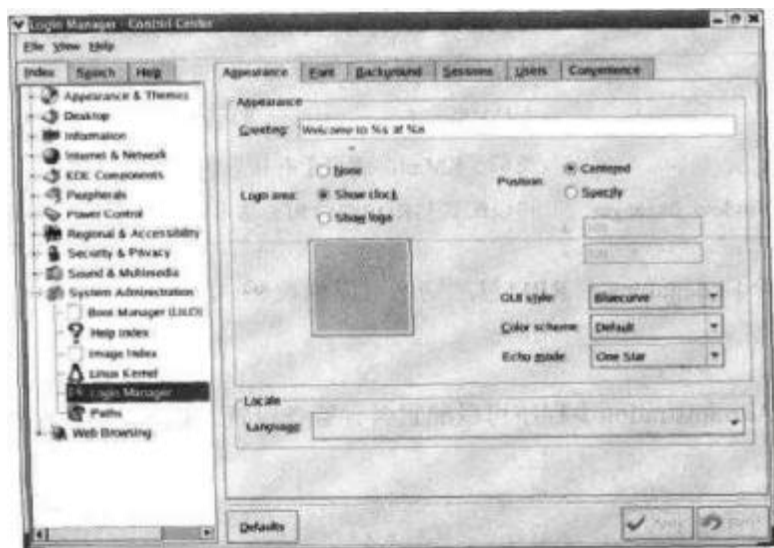


图17.31 KDE登录管理器

Paths 这个小程序可以配置桌面设置的目录路径、Trash文件夹、自动启动配置和本地文档。通常，它们都应放在主目录或其子目录中。

Web浏览

Web浏览小程序可以配置KDE Web浏览经历。这个部分的小程序和默认KDE Web浏览器Konqueror相联系。KDE控制中心的Web浏览小程序如图17.32，表17.8列出了各个小程序。

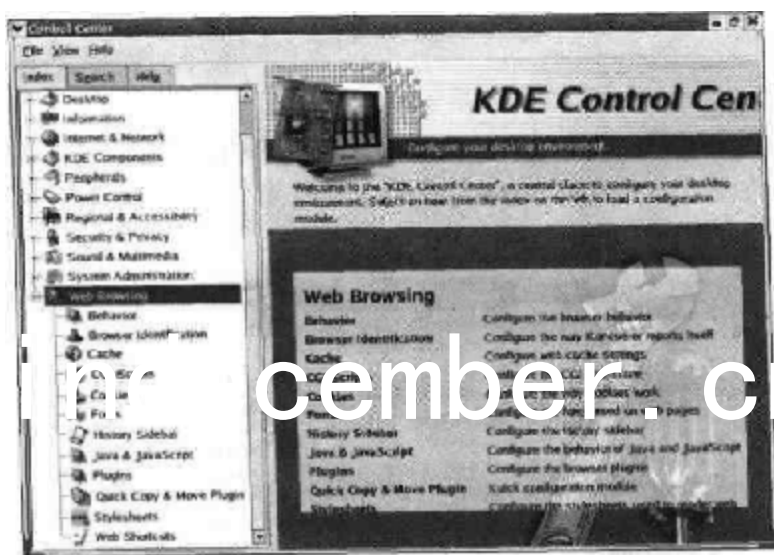


图17.32 Web浏览配置

表17.8 Web浏览小程序

应用程序	描述
Behavior	设置浏览器的光标、表单完成、图形、链接等行为
Browser Identification	可以定制浏览器标识自己的方式，甚至可以在特定Web站点将Konqueror标识为Microsoft Internet Explorer 6
Cache	可以对前面浏览的Web页面设置磁盘缓冲
CGI Scripts	支持访问CGI程序
Cookies	可以对不同Web站点的Cookie配置接受性政策
Fonts	可以设置与不同站点设置和语言相关的字体
History Sidebar	支持生成链接史
Java & JavaScript	可以按域启用Java可执行程序
Plugins	编译与浏览器相关的一系列插件
Quick Copy & Move Plugin	配置目录缓存参数
Stylesheets	支持CSS（级联样式单），使Web站点具有一致外观
Web Shortcuts	列出主要Web站点和搜索引擎的快捷缩写



图17.34 KDE字符选择器

手持PDA 手持PDA应用程序启动GNOME Pilot，见第16章介绍。

Kandalf's Tips Kandalf's Tips实用程序打开提示，可以在首次启动KDE时看到。图17.36显示了一个例子。

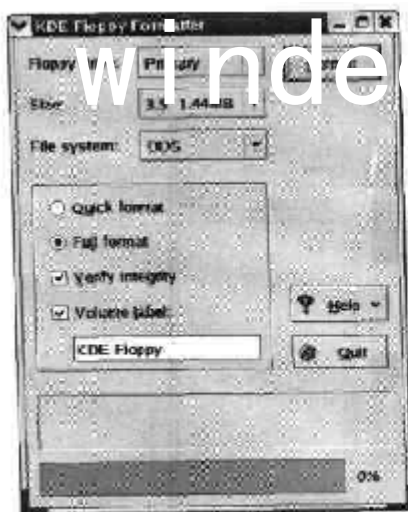


图17.35 软盘格式化工具



图17.36 Kandalf's Tips

Kate Kate是KDE的高级文本编辑器，可以编辑各种文本文件。如图17.37，Kate还提供了命令行界面的方便窗口。

Kdict Kdict是KDE字典，可以访问dict.org上的联机字典服务器，使用TCP/IP端口2628。只要连接互联网，就很容易找到所要的定义。图17.38显示了一个例子。

Kpager Kpager是KDE传呼机，打开一个小窗口，显示打开工作空间，其功能相当于KDE面板中看到的桌面工作空间视图。

打印作业 可以用KJobViewer管理打印队列中的当前作业。可以用不同功能保持、恢复、删除或移动任何当前打印作业。

打印管理器 打开第16章介绍的GNOME打印管理器实用程序。

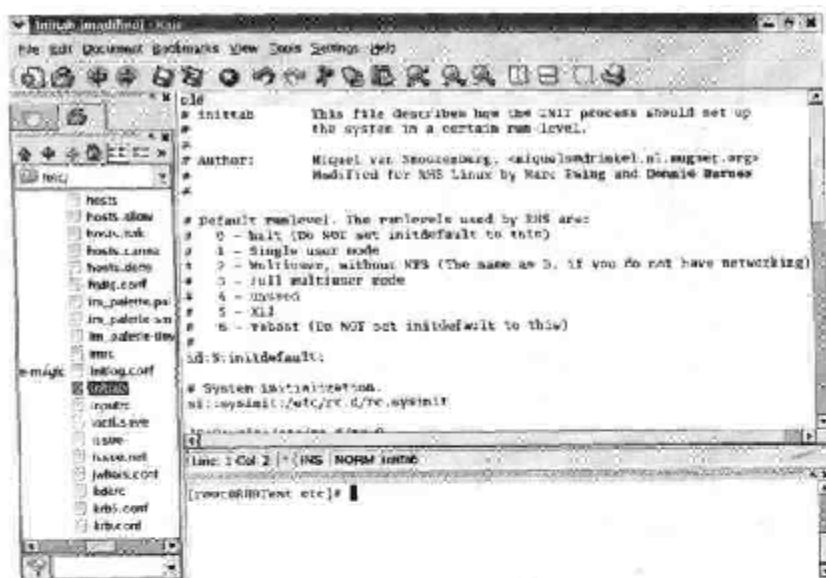


图17.37 在/etc/passwd中使用Kate

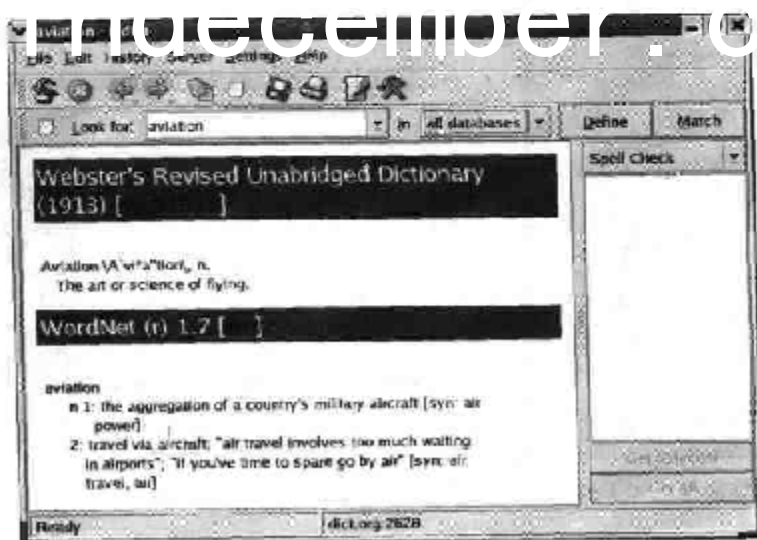


图17.38 联机字典

科学计算器 KCalc实用程序是可配置的计算器，可以通过数字键盘控制。可以在三角或统计方式中设置，各有不同函数。

更多附件

其他KDE附件主要是功能较少的小程序，见表17.9介绍。

表17.9 更多附件

附件	描述
Address Manager	KDE地址簿可以在地址簿中配置人们的联系信息。
JPilot	这个实用程序在符合PalmPilot与PalmOS标准的手持设备与KDE之间同步数据，图17.39是个样本视图
KAlarm	利用KDE个人警报消息和命令计划器，可以按时间表设置备忘或管理命令
Kandy	这个实用程序可以同步移动电话和KDE地址簿
KArm	这个实用程序可以跟踪不同任务所花的时间
KdeprintFax	这个实用程序是KDE Print的加入件，可以浏览打印到传真设备的文件
KHexEdit	这个实用程序是可定制的十六进制编辑器，可以显示和帮助在十六进制、八进制、二进制方式中编辑数据（对应于数学中的基数16、8、2），也可以在文本方式中显示文件
KJots	这个实用程序可以按组织方式记录短备注，生成的任何“簿”可以加入热键串
Notes	这个实用程序可以在桌面上增加一些短备注，以作备忘和发送电子邮件
KOrganizer	这是个方便的计划实用程序，如图17.39
KPilot	这个实用程序使用最新的Desktop HotSyncs软件，用于代替Palm桌面软件
KTimer	这个实用程序可以在指定延迟之后启动一个命令，默认为100秒
KWrite	这个实用程序是个文本编辑器，适合编程人员使用
Text Editor	这个实用程序是更基本的文本编辑器，KEdit是默认KDE文本编辑器
VNC Viewer	见第16章介绍
Word Translator	这个实用程序根据服务器增加其他字典，或增加与Babylon（ www.babylon.com ）相关的其他字典。见图17.40

其中几个实用程序将图标放在面板上的系统时钟旁边，如KOrganizer、KNotes与KAlarm。

Internet

KDE中有几个网络实用程序，可以帮助使用Internet，包括IRC客户机和MODEM连接实用程序，可以通过K Menu►Internet►More Internet Applications子菜单访问，如图17.41。几个GNOME应用程序已经在第16章介绍，如Mozilla、gFTP、Instant Messenger、Video Conferencing、Balsa、exmh、Galeon、IRC Client、Sylpheed和Evolution。第22章将介绍Ethereal。

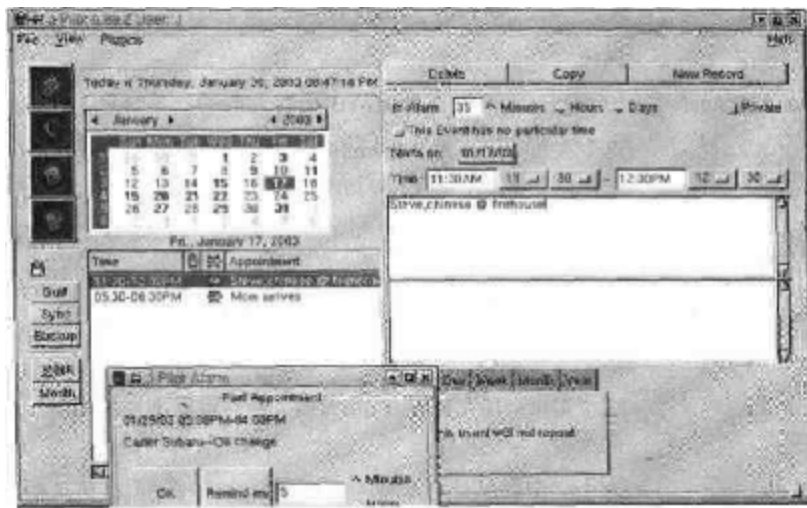


图17.39 同步JPilot与手持计算机

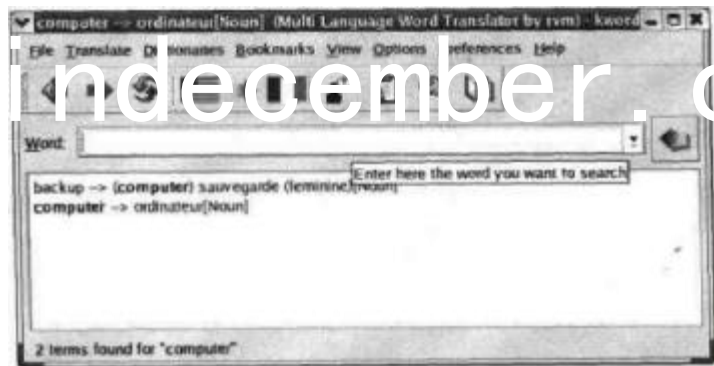


图17.40 KDE Word Translator

KGet KGet是KDE下载管理器，也称为Caitoo。集成到默认KDE Web浏览器Konqueror时，可以列出和监视、暂停与恢复下载。图17.42显示了样本下载过程。

Kisdndock 这个小程序可以配置任何安装的ISDN设备。ISDN是综合服务数字网，是个数字Internet连接选项，速度为普通电话MODEM的两倍。ISDN在欧洲很普及，因此主要在欧洲开发的KDE提供了坚实的ISDN支持。

如果还没有设置ISDN设备，则要先通过redhat-config-network-druid配置ISDN设备，见第21章介绍。

说明：redhat-config-network-druid实用程序的原名为internet-druid。

Kit 这个实用程序目前是AOL系统的KDE立即消息（IM）客户机。首次运行Kit时，会进入一个向导，可以建立AOL立即消息账号。新的Kit版本可能支持其他消息系统。

KMail 这是默认的KDE电子邮件客户机，是高度可定制的，可以用快捷键和工具栏上的操作进行配置。当然，还可以建立要用的电子邮件账号。

例如，可以用快捷键设置几个功能，如使用电子邮件过滤和标注消息、答复，等等。

可以使用一百多种快捷键，可以在主工具栏中配置所要的操作。

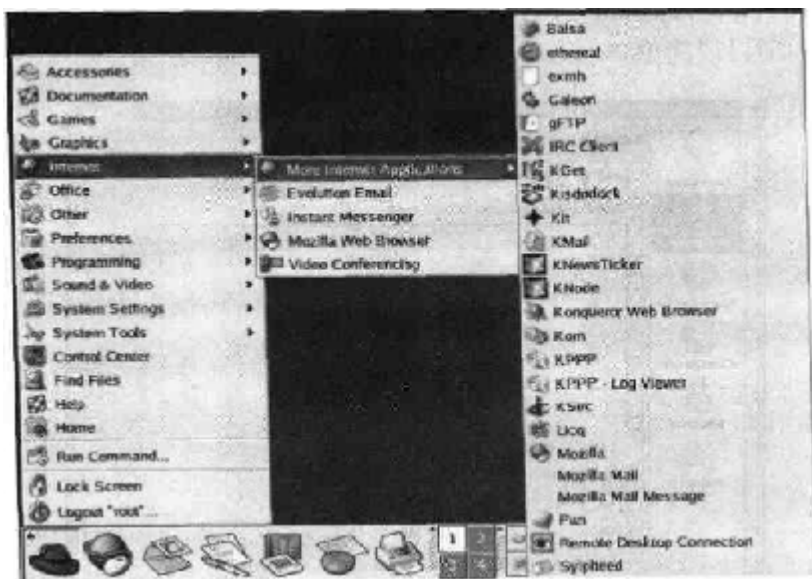


图17.41 更多Internet应用程序

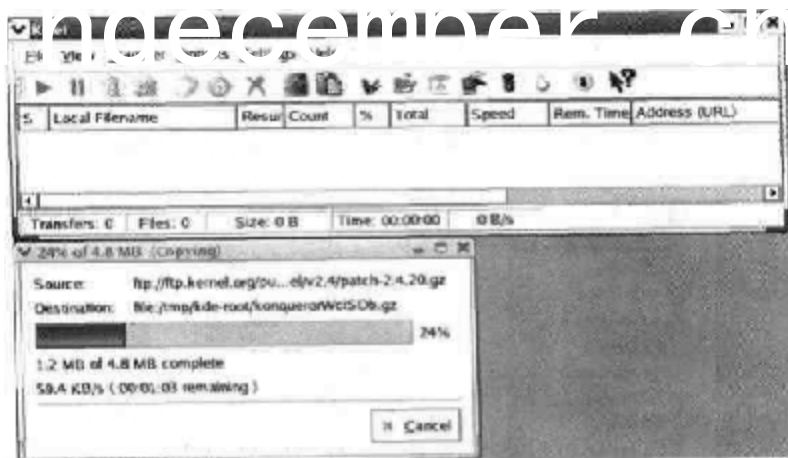


图17.42 KGet监视下载

配置新的电子邮件账号很简单。在KMail中，单击Settings►Configure KMail，打开Configure KMail对话框，在左窗格中单击Network，可以在图17.43所示的标签中配置发送与接收账号。

KNewsTicker 可以在面板中设置新闻提示。KNewsTicker可以访问几个不同的源。增加KNewsTicker的过程有所不同，不能用K菜单，而要直接加进面板中。要增加KNewsTicker，右单击面板中的空白区，并在弹出菜单中选择Add►Applet►KNewsTicker。

KNode 也可以用KNode作为默认新闻组阅读器，它和KMail一样，很容易配置。打开KNode之后，单击Settings►Configure KNode，打开Preferences - KNode对话框，单

击New，打开New Account - KNode对话框。如图17.44所示，KNode是高度可配置的，新闻账号的项目很简单。

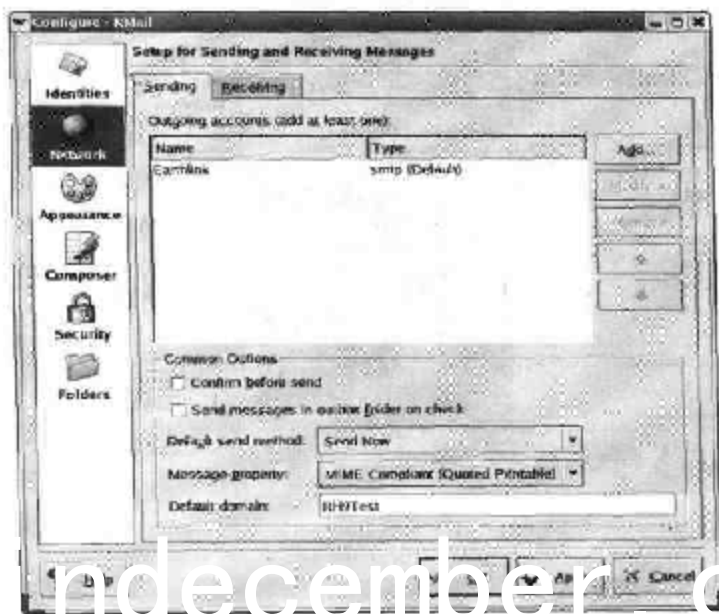


图17.43 配置KMail

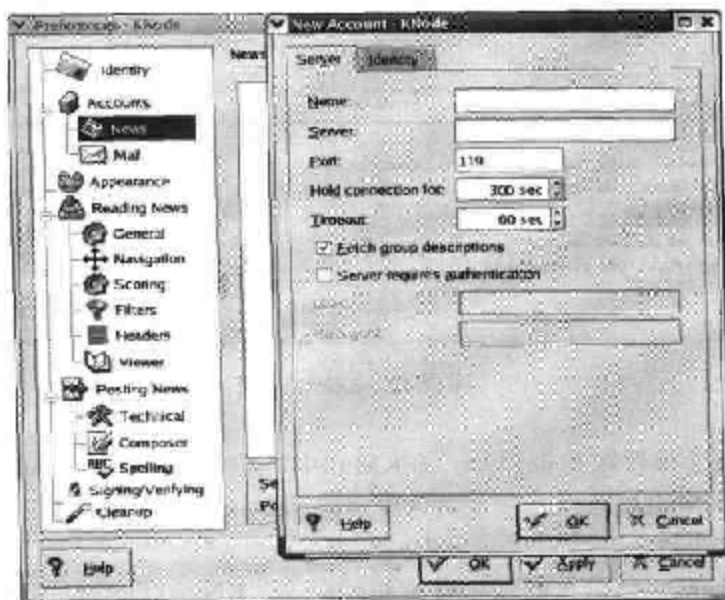


图17.44 配置KNode

Konqueror Web浏览器 Konqueror是默认KDE Web浏览器。和GNOME的Nautilus一样，它也可以浏览文件夹。我们已经在本章前面介绍KDE控制面板时，介绍过Konqueror配置选项。可以选择Settings►Configure Konqueror，配置这些设置。图17.45显示了基本浏览器，图17.46显示了配置选项。

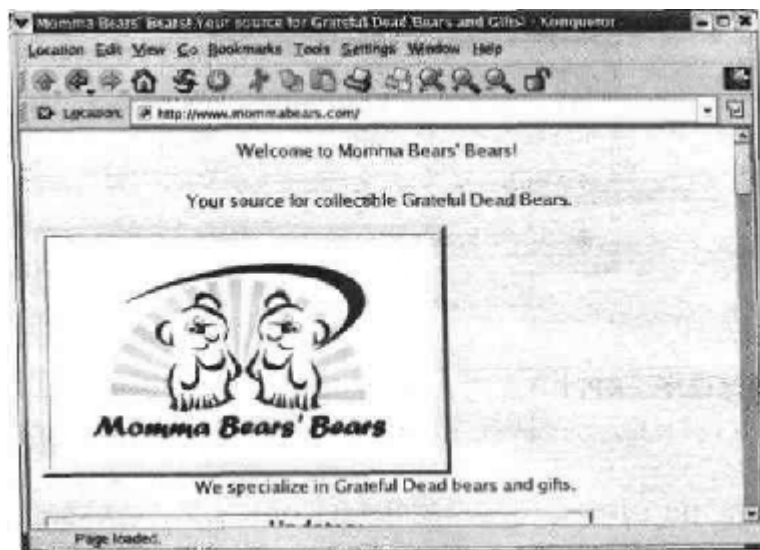


图17.45 Konqueror Web浏览器

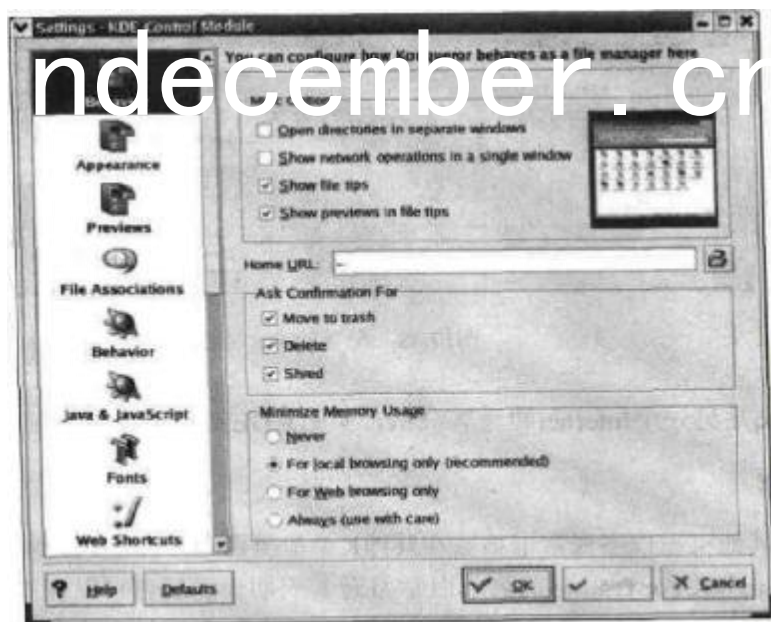


图17.46 通过KDE控制模块，配置Konqueror

Korn 如果要用一个实用程序监视邮箱，则可以启动Korn，这是个KDE邮件检查程序。配置所选账号（本地、POP3、IMAP4等等）之后，启动Korn。放进面板之后，它可以在固定时间间隔监视配置的邮箱，默认为5分钟。

KPPP KPPP是我喜欢的Linux GUI应用程序之一，主要用于在电话MODEM上连接ISP，是高度可配置的，可以对不同ISP或不同地址设置所选账号。如果无法配置MODEM，则KPPP可以试验不同设备。KPPP还包括日志与终端屏幕，可以帮助跟踪连接的性能。图17.47显示了主KPPP屏幕。



图17.47 KPPP

KPPP日志浏览程序 KPPP日志浏览程序启动当前月份的连接日志，在连接按分钟或按字节计费时特别有用。一些无线连接和欧洲电话MODEM连接通常按分钟或按字节计费。

KSirc 如果连接IRC闲聊室，则可以使用默认KDE聊天客户机KSirc。打开KSirc之后，可以选择Connect，配置新连接。如图17.48所示，可以选择聊天服务器组，选择服务器，输入必要的口令，然后单击Connect。如果连接成功，则可以看到聊天室所在的新窗口。

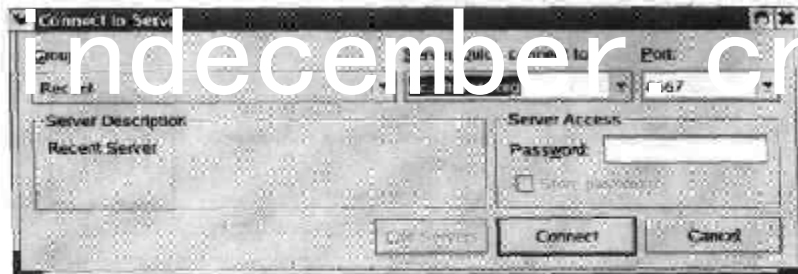


图17.48 配置KSirc

Licq Licq是另一个Internet聊天客户机，具有KDE支持。

其他实用程序

KDE中的其他实用程序通常很难放在其他K菜单类别中，许多其他实用程序在教育中有用，包括Kalzium和KVocTrain，前者可以学习元素周期表，后者可以提高词汇量。这些实用程序可以通过K Menu►Other子菜单访问，如图17.49。这个菜单中的有些实用程序不在KDE桌面中，本章不准备介绍。

FlashKard 这是个KDE词汇建立器。装入词汇表之后，可以自测表中单词的含义。
/usr/share/apps/kvotrain/examples目录的sample-de.kvtml中提供了德语的样本词汇表。

Kalzium Kalzium是个实用程序，表示前103个元素的元素周期表，如图17.50。每个元素有一个可单击按钮，提供这个元素的更详细信息，链接克罗地亚Split大学（www.ktf-split.hr/en/index.html）化学系的其他信息。

KEduca KEduca支持生成和修改基于表单的考试。可以用KEduca-Editor增加问题。更多信息见sourceforge.net/projects/keduca。

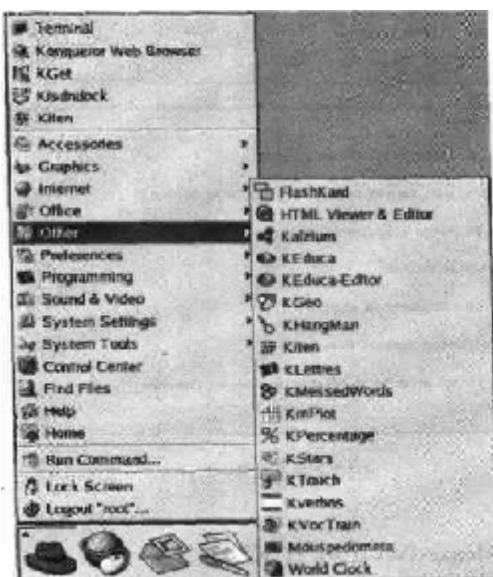


图17.49 其他KDE实用程序

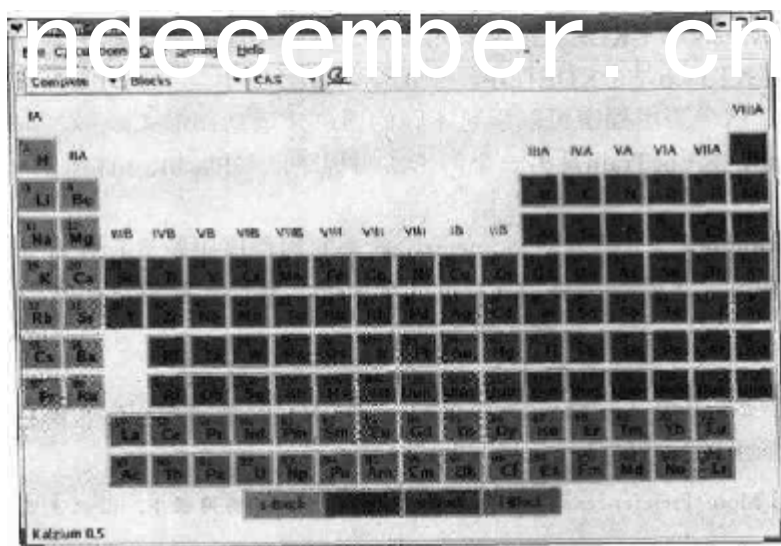


图17.50 KDE元素周期表

KGeo KGeo是个交互式KDE几何程序，帮助数学老师演示基本几何原理。

KHangMan KHangMan是猜字游戏的KDE版本。

Kiten Kiten是另一个互动字典，默认适用于日文和英语。图17.51显示了一个翻译例子。

KLettres KLettres是教字母表的KDE实用程序，目前可以配置成丹麦语、荷兰语和法语。

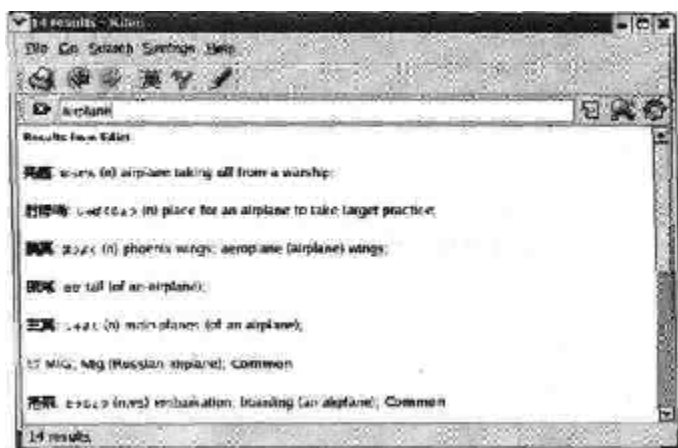


图17.51 将英语译成日文

KMessedWords KMessedWords是个KDE游戏。

KmPlot KmPlot是KDE数学函数绘图器，可以画出不同方程的图。

KPercentage KPercentage是个KDE实用程序，测验学生计算百分比的能力。

KStars KStars是个KDE天文学实用程序，能实时空图显示不同星座。

KTouch KTouch是个KDE程序，帮助学习接触类型。

Kverbos 这个实用程序可以学习不同的西班牙语动词形式。

KVocTrain KVocTrain是另一个闪卡实用程序，与FlashKard相似，也使用.kvtml数据库。

Mousepedometa 也称为KOdometer，这个实用程序跟踪光标在桌面上移动的距离。

World Clock 可以显示不同地点的当前时间，并显示在晴空中太阳的位置。

选项

KDE的选项子菜单（K Menu►Preferences）中有几个实用程序。图17.52所示的实用程序中只有几个是KDE实用程序，见表17.10介绍。

说明：由于More Preferences菜单中的实用程序都不是KDE实用程序，因此这里不做介绍。

表17.10 选项子菜单中的KDE实用程序

实用程序	描述
Configure Panel	打开Settings - KDE Control Module窗口，可以设置面板，见本章前面介绍
Desktop Settings Wizard	这个向导可以对KDE配置语言、地址、优选系统行为、特殊效果和风格

更多编程工具

KDE的K Menu►Programming►More Programming Tools子菜单中还有几个实用程序。图17.53所示的实用程序中只有几个是KDE实用程序，见表17.11介绍。

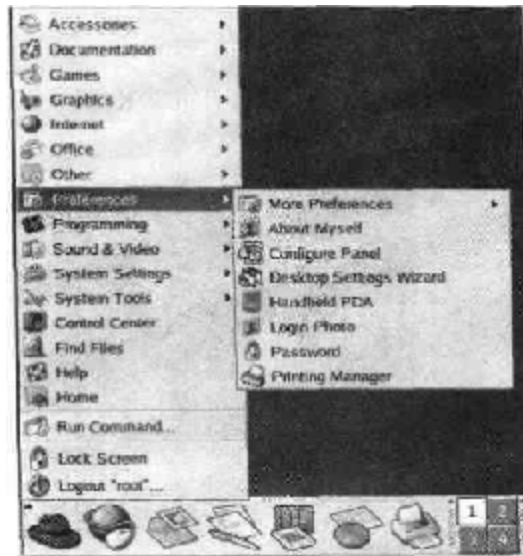


图17.52 选项菜单

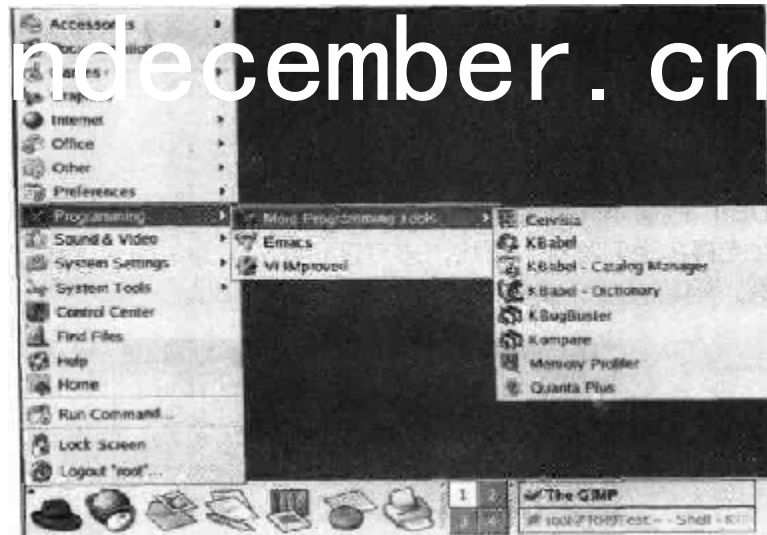


图17.53 更多编程工具

表17.11 KDE编程工具

工具	描述
Cervista	跟踪源代码不同版本的KDE工具，使用CVS（并发版本系统）
KBabel	支持对程序代码中的注释和其他指导使用其他语言
KBabel - Catalog Manager	合并KBabel目录
KBabel - Dictionary	也称为PO Compendium，列出一个项目的翻译消息
KBugBuster	支持缺陷管理，默认连接bugs.kde.org的KDE缺陷跟踪系统
Kompare	diff命令的KDE前端，检查文件之间的差别
Memory Profiler	监视程序的内存行为，包括内存泄漏
Quanta Plus	KDE的Web开发工具

多媒体

单击Main Menu►Sound & Video, 可以打开几个KDE多媒体应用程序。如图17.54, 其中包括不同声音、光碟播放器和声控实用程序。



图17.54 多媒体菜单

KsCD KDE小型/简单光碟播放器是声音光碟的易用播放器, 如图17.55所示, 其标准按钮可以在光碟磁道间移动和播放, 还可以访问前面介绍的光碟数据库(CDDDB)。如果单击歌名, 则可以从光碟中选歌。



图17.55 KDE光碟播放器

Sound Mixer 可以从几个不同源调节声音输入。

aRts Builder 前面曾介绍过, aRts是KDE声音服务器。这个图形的设计工具可以用几个声音特性配置连接。

aRts Control Tool 这个工具可以控制aRts声音服务器的不同设置。

Kaboodle Kaboodle是单个文件的媒体播放器, 如.wav格式文件。

KMid KDE MIDI/Karaoke文件播放器可以播放.mid与.kar文件, 只要声音具有原始MIDI文件的硬件支持。

KMidi KMidi是TiMidity合成器的前端(如图17.56)。如果声卡不提供MIDI支持, 则可以用这个工具播放.mid文件。还要有/etc/timidity.cfg配置文件, /usr/share/apps/

kmidi/config目录中提供了一个样本。如果启动这个工具时遇到错误,则应检查是否安装了arts-devel-* RPM包。

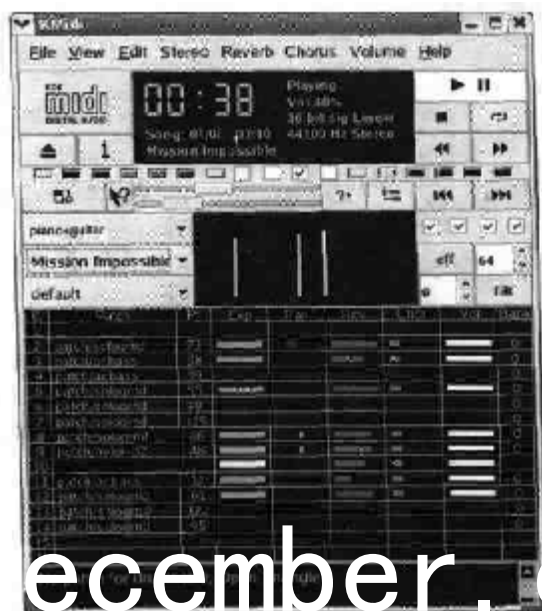


图17.56 KMidi

Noatun Noatun实用程序是aRts声音服务器的前端。启动时可能像是不工作。事实上,它在面板中增加一个图标。右单击这个图标,可以打开基本Noatun菜单。Noatun与第16章的XMMS声音播放器相似,具有调谐器和播放列表菜单。

TiMidity Synth 见KMidi。

系统工具

有几个KDE系统工具与第19章介绍的redhat-config-*工具无关。图17.57显示了这个菜单,本节介绍各种管理工具。

Create A Boot Disk 这个实用程序调用qmkbootdisk命令,帮助在3寸软盘上生成安装引导盘。详见第11章对mkbootdisk的介绍。界面很简单,见图17.58。

Desktop Sharing 这个实用程序原名为krfb,支持管理xinetd服务器。

File Manager 在Konqueror中打开当前用户的主目录。

KAudioCreator 这个实用程序位置不太对,实际上属于Sound & Video菜单中的其他多媒体应用程序。利用这个实用程序,可以从声音光碟复制磁道,写入所选光碟中。它还支持CDDDB访问,可以帮助寻找每个磁道的更多信息。

KDat 这个实用程序是个KDE磁带档案程序,基于tar命令。

KDE System Guard 这个实用程序也称为ksysguard,是KDE任务管理器和性能监视器。默认情况下,它根据top命令显示系统负荷的图形化视图。也可以建立图表,监视另外几个系统。图17.59显示了这个工具的基本视图。

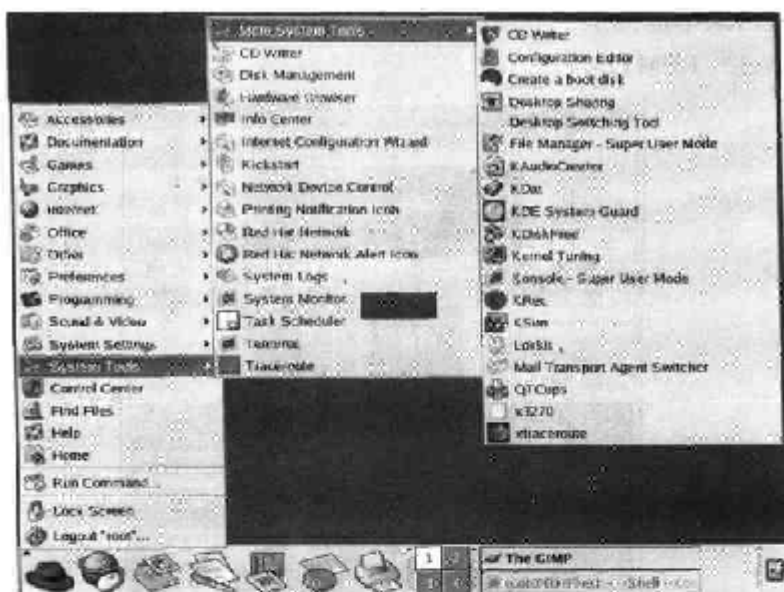


图17.57 更多系统工具



图17.58 生成引导盘

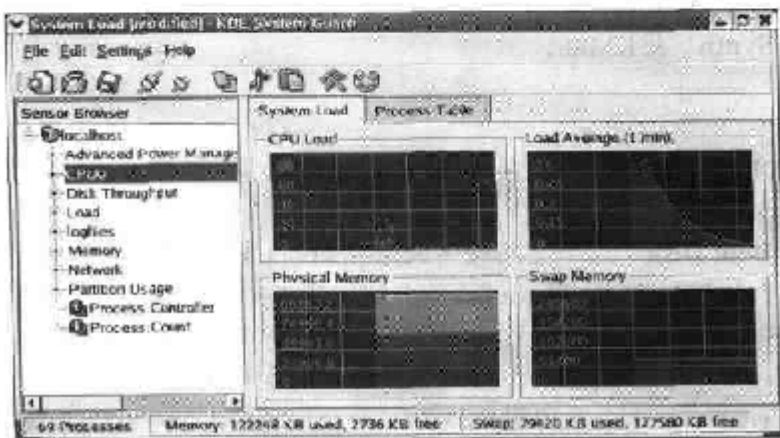


图17.59 KDE System Guard工具

KDiskFree 这个实用程序演示了所有装载分区中的自由空间，实际上是第7章介绍的df命令的演示前端。

Kernel Tuning 可以用内核修改/proc目录中存储的一些设置，见第11章介绍。例如，如果Linux计算机是个网关，则要启用IP转发。第21章介绍了一个方法，也可以通过这个实用程序设置，如图17.60。

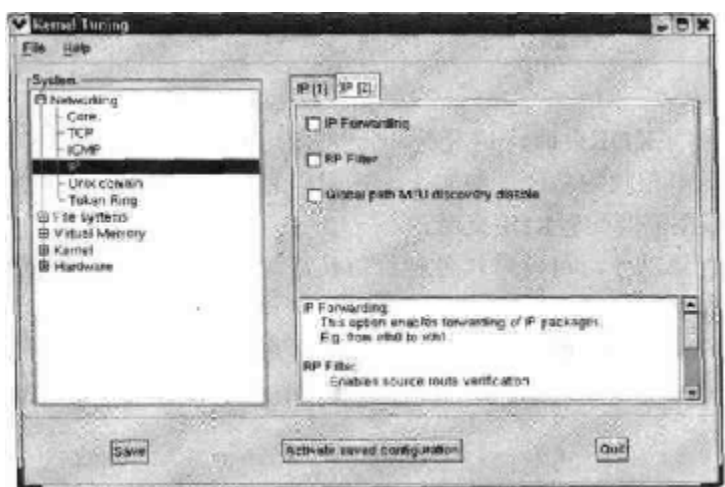


图17.60 Kernel Tuning工具

KRec 这个实用程序是KDE aRts声音服务器的录制前端，是个多媒体实用程序，实际属于Sound & Video菜单。

KSysd 这个实用程序是个系统监视器，是top命令的简单前端。这个命令放在KDE面板中，右单击Linux菜单栏，打开Linux配置菜单，如图17.61。可以看出，Linux是高度可配置的。

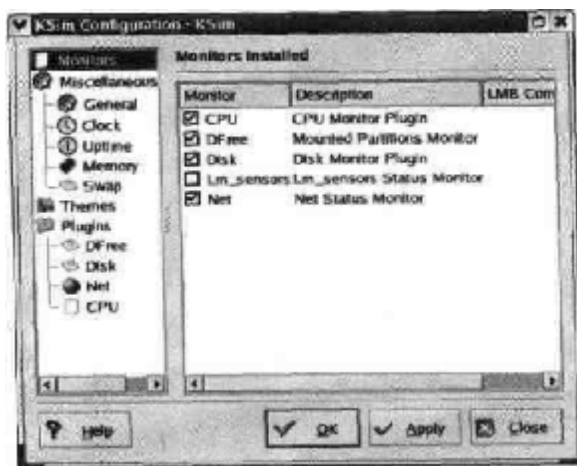


图17.61 Linux配置菜单

QTCups 到本书编写时，这个实用程序还放在Red Hat More System Tools子菜单中，但已经过时，换成KDEPrint实用程序，可以用kprinter命令从命令行界面启动。KDEPrint是KDE实用程序与计算机上活动的打印监控程序之间的接口。第25章将会介绍，默认打印服务为CUPS。

小结

本章简要介绍了KDE桌面，这是另一个主要Linux GUI，其中的许多工具提供与Microsoft Windows中相同的功能。事实上，还可以将打开应用程序分配到四个或多个不同桌面中。很容易根据需要配置KDE桌面。

KDE提供了大量功能，可以替代各种价值几百美元的软件。KDE提供了每天需要的附件。Internet应用程序包括浏览器、邮件管理器和聊天客户机。声音与视频实用程序可以管理、处理和录制多媒体。KDE中还有许多系统工具，可以帮助管理员管理系统。

下一章介绍一些更重要的Linux GUI应用程序，主要是办公组件和图形实用程序。

第18章 GUI应用程序

Red Hat Linux中有几个与Microsoft操作系统中类似的应用程序，其中最主要的是完全个性的办公组件。Red Hat Linux用这些程序代替每台计算机上价值几百美元的Microsoft Windows程序。

Linux办公组件通常包括字处理程序、电子表格、图形支持、演示管理器和项目计划器。有些组件还有更多内容。可能需要下载一两个应用程序，但它们和Linux所带的办公组件应用程序一样是免费提供的。本章要介绍的三个办公组件是OpenOffice、Koffice与GNOME Office。

Red Hat Linux还提供了几个图形应用程序，包括图形浏览器、扫描工具、屏幕捕获程序和与Adobe Acrobat Reader一样的文件浏览程序。

本章简要介绍每个应用程序，其中许多应用程序是相当复杂的，本身可以写成一本书。本章包括下列主题：

- 了解OpenOffice
- 了解GNOME Office
- 使用KOffice
- 使用图形应用程序

了解OpenOffice

Red Hat Linux的默认办公组件是OpenOffice，来自www.openoffice.org站点，是用Sun系统公司的StarOffice代码开发的，包括几个应用程序，见表18.1。

表18.1 OpenOffice应用程序

应用程序	描述
Calc	电子表格
Draw	框图生成器
Impress	演示管理器
Math	公式生成器
Printer Setup	管理打印机接口
Repair	安装程序
Writer	字处理程序

可以从所选GUI中打开已安装的OpenOffice应用程序。在GNOME中，单击Main Menu➤Office，然后从弹出菜单中选择应用程序。

说明：如果使用KDE，则K Menu按钮对应于GNOME Main Menu按钮。默认情况下，两者都在桌面左下角，都与红帽子图标相关联。本章的指令基于红帽子默认桌面GNOME，KDE中的指令可能稍有不同。

也可以从桌面下方的面板上直接启动三个OpenOffice应用程序。第16章和第17章曾介绍过，可以单击笔和纸图标启动OpenOffice Writer，可以单击条形图和幻灯图标打开OpenOffice Impress，可以单击饼形图图标打开OpenOffice Calc。

关于OpenOffice.org项目的更多信息，见Web站点www.openoffice.org。

OpenOffice Calc

也许第一个关键业务PC应用程序是电子表格。可以用电子表格定义各种数据。利用所选公式，可以让电子表格在不同情形中进行从统计分析到业务建模与预测的各种计算。

要打开OpenOffice Calc，选择Main Menu>Office>OpenOffice.org Calc或在GUI终端窗口中运行oocalc命令。图18.1显示了OpenOffice Calc和2000年美国人口统计的一些基本数据。

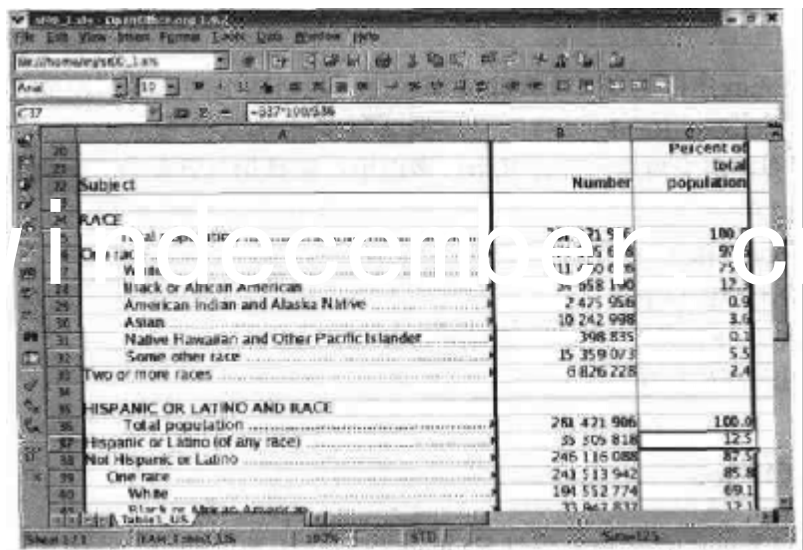


图18.1 OpenOffice Calc和人口统计数据

从图中可以看出，OpenOffice Calc具有电子表格外观，其功能与Microsoft Excel相似，包括几个工具栏，见表18.2。

表18.2 OpenOffice Calc工具栏

工具栏	描述
Formula	显示元位置和与其相关的公式
Function	配置基本功能，如打开、打印与撤销
Hyperlink	设置Web页面访问
Main	生成图表，支持格式与拼写检查，允许排序和组合
Object	支持格式选项，包括字体、间距、编号方式、边框与对齐方式

OpenOffice Calc适用于多种不同电子表格，见表18.3所示。可以看出，OpenOffice Calc可以处理多种应用程序中的电子表格，包括Microsoft Excel、StarOffice Calc、dBASE/FoxPro数据库，等等。还可以用逗号分隔格式的文本文件设置OpenOffice Calc（见下面的旁白）。

表18.3 OpenOffice Calc文件格式

格式	描述
.sxc	OpenOffice电子表格
.stc	OpenOffice电子表格模板
.dif	数据交换格式
.dbf	dBASE/FoxPro数据库文件
.xls	Microsoft Excel 97/2000/XP或Excel 95/5.0
.xlt	Microsoft Excel 97/2000/XP或Excel 95/5.0模板
.sdc	StarOffice Calc 5.0/4.0/3.0 (Sun StarOffice电子表格)
.vor	StarOffice Calc 5.0/4.0/3.0模板
.slk	符号链格式, 包括公式和单元与文件链接
.wks	Lotus 1-2-3
.csv	逗号分隔格式, 文本文件中的电子表格
.html	Web页面

逗号分隔格式

电子表格和其他数据表通常存在文本文件中用逗号分隔格式表示。换句话说, 下面行中的每个值可以导入到表格一行中的连续单元格中。

```
height, 60, 61, 44, 78, 56, 66
```

OpenOffice Draw

OpenOffice Draw可以管理不同格式的图形文件, 从AutoCAD文件到位图文件。换句话说, 从设计工程师到图形设计师, 每个处理图形的人都可以使用OpenOffice Draw设计工具。

要启动OpenOffice Draw, 选择Main Menu>Office>OpenOffice.org Draw或在GUI终端窗口中运行oodraw命令。图18.2显示了GNOME可以进行编辑的界面。

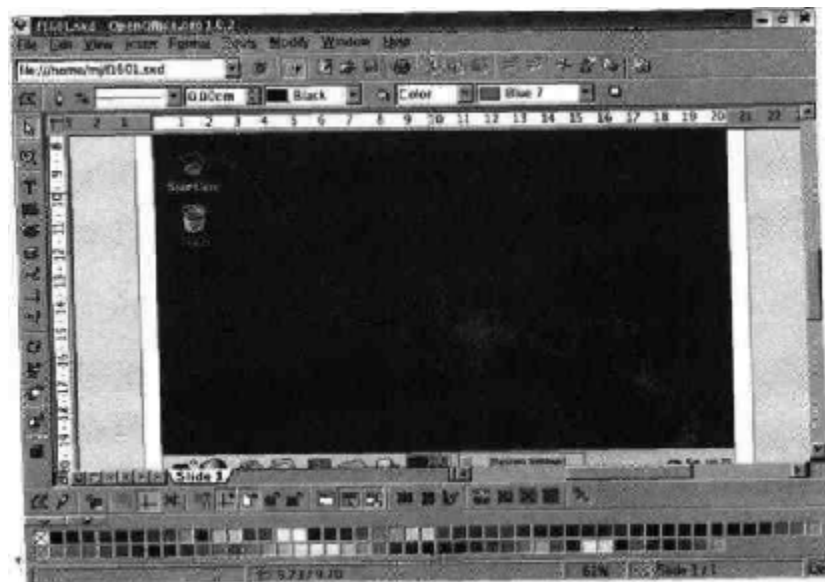


图18.2 OpenOffice Draw界面

从图中可以看出，OpenOffice Draw包括各种工具栏，有些可以管理颜色，有些可以绘制和增加对象。表18.4介绍了这些工具栏。

表18.4 OpenOffice Draw工具栏

工具栏	描述
Color	选择各种颜色
Function	配置基本功能，如打开、打印与撤销
Hyperlink	设置Web页面访问
Main	缩放、插入（文本和几何形体等）对象、对齐对象，等等
Object	配置栅格生成、文本编辑、旋转、颜色，等等
Option	支持编辑与绘制线型选项，包括厚度与颜色

OpenOffice Draw适用于多种不同的图形格式，见表18.5所示。可以看出，OpenOffice 图形可以处理几个应用程序中的图形表格，包括Microsoft Windows bitmap、StarOffice Draw、Adobe Photoshop，等等。还可以用逗号分隔格式的文本文件设置OpenOffice Draw。

表18.5 OpenOffice Draw支持的格式

格式	描述
.sxd	OpenOffice图形
.std	OpenOffice图形模板
.bmp	Microsoft Windows位图
.dxf	AutoCAD交换格式
.emf	改进元文件
.eps	包装PostScript
.gif	图形交换格式
.jpg	连接图形专家组规范格式
.met	OS/2元文件
.pbm	可移植位图
.pcd	Photo CD（Kodak）格式
.pct	Macintosh Pict图形
.pcx	Zsoft画刷
.pgm	可移植灰度图
.png	可移植网络图形
.ppm	可移植像素图
.psd	Adobe Photoshop
.ras	Sun光栅图形
.sda	StarOffice 5.0 Draw
.sdd	StarOffice 3.0 Draw
.sgf	StarWriter图形
.sgv	StarDraw 2.0图形
.svm	StarView元文件

(续表)

格式	描述
.tga	Truevision Targa
.tiff	标志图形文件格式
.vor	StarOffice 5.0/3.0 Draw模板
.wmf	Microsoft Windows元文件
.xbm	X位图
.xpm	X像素图

OpenOffice Impress

生成演示时，实际上是生成幻灯片。演示应用程序就是带图形的专用字处理程序，它支持室内或网上的幻灯片。可以像Microsoft PowerPoint或StarOffice Impress等其他应用程序一样用OpenOffice Impress建立演示。

要启动OpenOffice Impress，可以选择Main>Office>OpenOffice.org Impress或在GUI终端窗口中运行oointpress命令。图18.3显示了典型的演示程序开始界面。

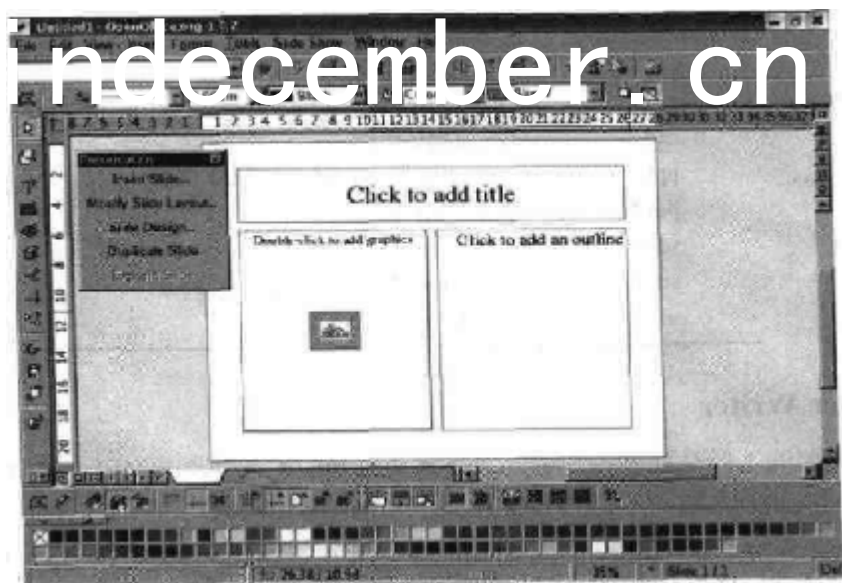


图18.3 OpenOffice Impress演示程序开始界面

从图中可以看出，OpenOffice Impress包括各种工具栏，有些可以管理颜色，有些可以绘图、管理文本和增加对象。表18.6介绍了这些工具栏。

表18.6 OpenOffice Impress工具栏

工具栏	描述
Color	选择各种颜色
Function	配置基本功能，如打开、打印与撤销
Hyperlink	设置Web页面访问

(续表)

工具栏	描述
Main	缩放、插入文本和几何形体等对象、对齐对象，等等
Object	配置栅格生成、文本编辑、旋转、颜色，等等
Option	支持编辑与绘制线型选项，包括厚度与颜色
Presentation	管理每个幻灯片的设计

首次启动OpenOffice Impress时，会出现AutoPilot Presentation向导，你可以从空白页、演示模板或现有工作开始工作。如果生成新演示，则OpenOffice Impress配置一个幻灯设计、输出媒介和基本演示注释。

OpenOffice Impress适用于其他演示格式，如表18.7所列。可以看出，OpenOffice演示可以处理其他应用程序数据，包括Microsoft PowerPoint，StarDraw，StarImpress和任何能够保存为.cgm格式的应用程序。

表18.7 OpenOffice Impress文件格式

格式	描述
.sxi	OpenOffice演示
.sti	OpenOffice演示模板
.sxd	OpenOffice图形
.ppt	Microsoft PowerPoint 97/2000/XP
.pot	Microsoft PowerPoint 97/2000/XP模板
.sda	StarDraw 5.0
.sdd	StarDraw 3.0/StarImpress 4.0/5.0
.vor	StarImpress 4.0/5.0模板

OpenOffice Writer

一个重要的工作是处理各种字处理格式文档。要用转换器将Microsoft Word文档转换成Corel WordPerfect文档，然后再转换成StarOffice Write文档。尽管大多数字处理程序（包括StarOffice Write）都内置了转换器，但每个字处理程序都有一些特殊特性，因此很难正确转换。

StarOffice Write在这方面干得很漂亮，但仍有几个行业包括出版待业。使用的特殊特性不能够用StarOffice Write正确处理，然而，对大多数应用程序和业务而言，StarOffice Write已经足够好了。

要启动StarOffice Write，选择Main Menu>Office>OpenOffice.org Writer或在GUI终端窗口中运行oowriter命令。StarOffice Write中生成的新文档可以包括Microsoft Word提供的所有特性。图18.4显示了典型文档。

从图中可以看出，StarOffice Write有三个基本工具栏，见表18.8。

OpenOffice Writer可以处理其他字处理程序中的文件，见表18.9。

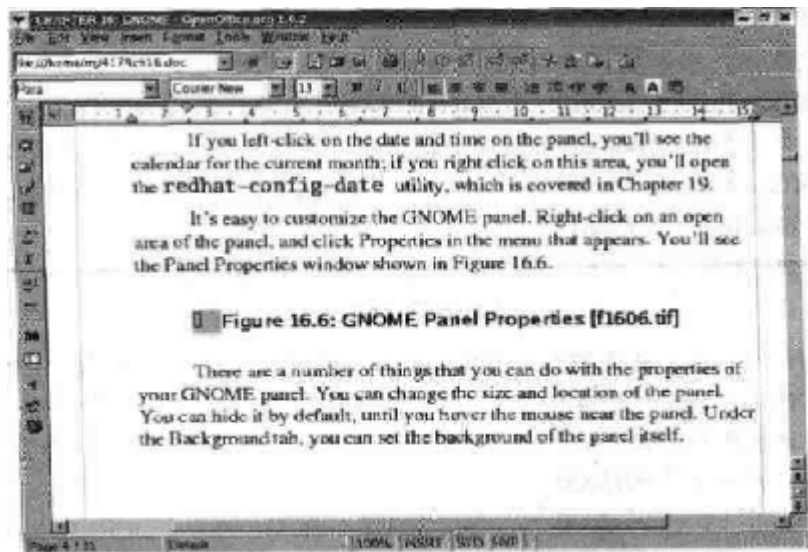


图18.4 StarOffice Write中的Microsoft Word文档

表18.8 OpenOffice Writer工具栏

工具栏	描述
Function	配置基本功能，如打开、打印与撤销
Hyperlink	设置Web页面访问
Main	缩放、插入文本和几何形体等对象、生成窗体，等等
Object	设置字体、样式、格式、加亮和颜色

表18.9 OpenOffice Writer文件格式

格式	描述
.sxw	OpenOffice “文本” 文档，其实不是文本格式
.stw	OpenOffice “文本” 文档模板
.doc	Microsoft Word 97/2000/XP以及Microsoft Word 95与6.0的替换.doc格式
.html	超文本标记语言，适合Web页面
.rtf	多信息文本格式，许多字处理程序都能阅读的通用格式
.sdw	StarWriter 3.0/4.0/5.0
.vor	StarWriter 3.0/4.0/5.0模板
.txt	普通文本，或使用编码分行符的.txt格式

说明：当熟练的Linux用户需要桌面发表功能时，他们往往使用文本工具。例如，TeX与LaTeX之类工具的文本命令可以格式化文本文件中的标题、斜体，等等。这没有什么特别之处，WordPerfect 5.2也开始设置了类似的文本命令。

其他OpenOffice工具

其他OpenOffice工具包括：

- **OpenOffice Math**让用户生成和建档不同复杂程度的方程，支持三角函数、积分、极限、指数等。可以从命令行运行oomath命令启动该程序。
- **OpenOffice Printer Setup**可以对OpenOffice组件中其他部分配置驱动器和打印格式。可以从命令行运行oopadmin命令启动该程序。
- **OpenOffice Repair**可以增加、删除和修复OpenOffice组件中的不同组件。可以从命令行运行oosetup命令启动该程序。

CrossOver Office

如果想转向Linux，又离不开这些Microsoft应用程序，则可以选择CodeWeavers公司的CrossOver Office，零售价为54.95美元，它使用WINE（WINE不是仿真程序）项目的一些工作使你能在Linux计算机上运行最常用的Microsoft Windows应用程序。这些应用程序包括：

- Microsoft Word 97/2000 *
- Microsoft Excel 97/2000 *
- Microsoft Outlook 97/2000
- Microsoft PowerPoint 97/2000 *
- Microsoft Visio 2000
- Microsoft Internet Explorer 5.0/5.5
- Intuit Quicken 2002
- Lotus Notes R5

据CodeWeavers公司称，标有星号的应用程序是“Gold Medal”，它们可以像在Microsoft Windows中一样顺利运行。有些应用程序在Linux中用CrossOver Office运行时可能有重大缺陷。详见www.codeweavers.com站点。

了解GNOME Office

GNOME Office套件中也有许多应用程序。尽管它们最初不是作为集成套件建立的，但现在已经集成起来了。GNOME Office包括GNOME项目中的小组开发的办公应用程序。表18.10简要列出了GNOME办公应用程序。

表18.10 GNOME办公应用程序

应用程序	描述
AbiWord	字处理程序
Agnubis	演示管理器，目前不提供RPM格式，因此不包括在Red Hat Linux中
Balsa	电子邮件客户机
Dia	框图程序
Evolution	个人信息管理器
Galeon	Web浏览器
GIMP	图形编辑器
GnuCash	个人财务管理器
Gnumeric	电子表格

(续表)

应用程序	描述
Guppi	绘图, 与Gnumeric密切相关
MrProject	项目管理工具
Sketch	向量绘图软件包, 不包括在Red Hat Linux中
Sodipodi	向量绘图软件包, 不包括在Red Hat Linux中
Toutdoux	项目管理工具, 不包括在Red Hat Linux中

这里不介绍所有工具, 例如第16章已经介绍Galeon与Evolution, 我们将在本章稍后介绍The GIMP。其中有些工具不包括在Red Hat Linux中, 例如, Agnubis演示管理器虽然属于GNOME Office套件, 但目前还在开发之中, 不提供RPM格式。

截止本书编写时, GNOME web站点www.gnome.org/gnome-office指出OpenOffice应用程序将放在GNOME Office套件中。但GNOME Office应用程序的开发还在继续。

说明: 许多GNOME Office应用程序是试验性的, 目前还不能在生产中使用。为了查看应用程序的状态, 只需打开应用程序, 然后选择Help>About application。一般来说, 版本为1.0以上的应用程序可以在生产中使用, 但也不绝对。大多数应用程序是由志愿者开发和维护的, 到V1.0发布以后也还在开发。

AbiWord

AbiWord是GNOME的字处理程序, 可以按多种格式打开和关闭文档, 其功能对大多数用户和应用程序是足够的。但是, 据我所见, 其对Microsoft Word文档的支持不如OpenOffice Writer。例如, 图18.5演示了将第16章的视图化为表的结果。

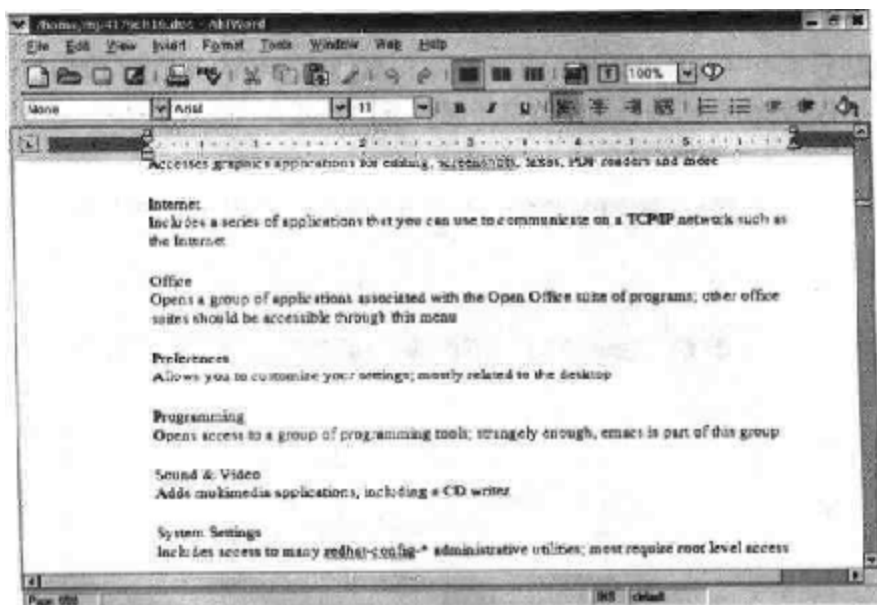


图18.5 AbiWord读取Microsoft Word文档

与大多数OpenOffice应用程序不同的是,选择AbiWord之前要选择Main Menu>Office>More Office Applications,也可以在GUI中用abiword命令启动AbiWord。这个字处理程序支持各种格式,见表18.11。

表18.11 AbiWord文档格式

格式	描述
.abw	自然格式
.aw	Applix Words
.awt	AbiWord模板
.dbk	DocBook
.doc	Microsoft Word
.fo	Extensible Stylesheet Language (扩展样式单语言)
.html, .htm	Hypertext Markup Language (超文本标记语言)
.xhtml	Extensible Hypertext Markup Language (扩展超文本标记语言)
.isc, .iscii	Indian script code for information interchange (印度信息交换脚本码)
.kwd	KOffice word文档
.latex	LaTeX, Lamport TeX文本文档格式工具
.pdb	Palatino
.psitext, .siwrtd	Postscript 文本格式
.rtf	Rich Text Format (多信息文本格式)
.txt, .text	文本,也可能是编码文本
.nws	新闻组格式文本
.wml	Wireless Markup Language (无线标记语言)

Balsa

Balsa是标准电子邮件管理器。和第16章和第17章介绍的其他电子邮件应用程序一样,它有标准文件夹视图和入站与出站的电子邮件视图。通常,它设置为本地账号。图18.6演示了根用户的人站电子邮件。

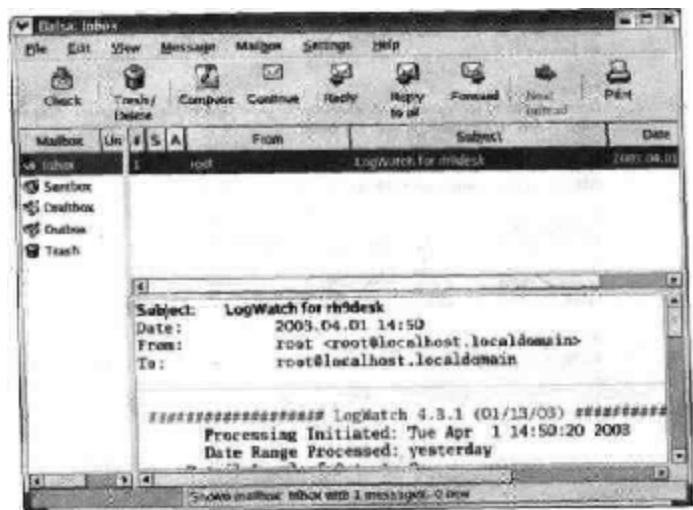


图18.6 Balsa电子邮件管理器

要启动Balsa, 选择Main Menu►Internet►More Internet Applications►Balsa, 也可以用balsa命令在GUI中从命令行界面启动。

首次运行Balsa时, 要输入电子邮件账号的入站与出站设置。以后可以从Settings菜单配置其他电子邮件地址, 只要对每个账号配置新的标识。

Dia

如图18.7所示, Dia是个框图编辑器。顾名思义, 它可以绘制框图。从图中可以看出, 它可以在框图中生成各种形状, 与Microsoft Visio相似。

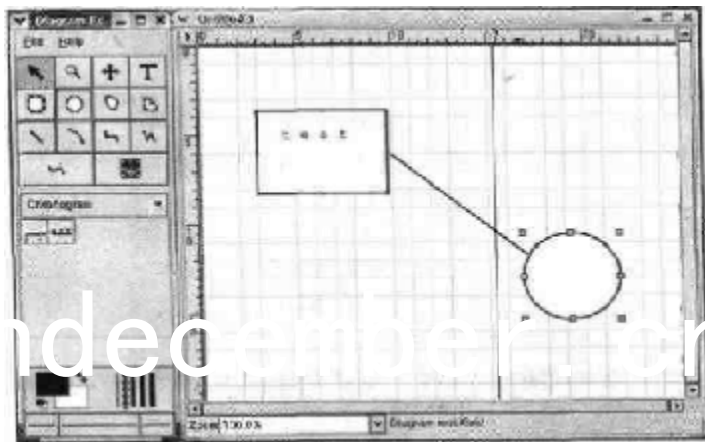


图18.7 Dia框图编辑器

要启动Dia, 选择Main Menu►Office►Dia Diagrams, 也可以用dia命令在GUI中从命令行界面启动。

GnuCash

GnuCash是个开放源代码的个人财务管理器, 可以处理Quicken文件。

要启动GnuCash, 选择Main Menu►Office►More Office Applications►GnuCash, 也可以用gnucash命令在GUI中从命令行界面启动。

首次运行GnuCash时, 其提示对资产、负债、收入和支出设置新账号。也可以从Quicken 2002导入文件。图18.8导入简单Quicken测试文件。

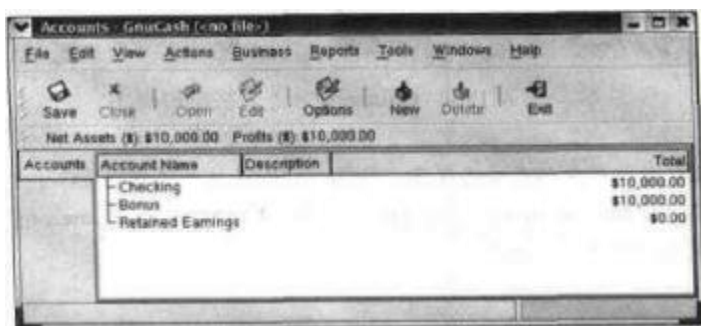


图18.8 GnuCash导入Quicken文件

Gnumeric

Gnumeric是个GNOME电子表格应用程序，如图18.9所示。和AbiWord一样，要启动Gnumeric，选择Main Menu>Office>More Office Applications>Gnumeric Spreadsheet，也可以用gnumeric命令从GUI命令行界面启动。这个电子表格支持各种格式，如表18.12所示。

表18.12 Gnumeric文件格式

格式	描述
.dif	数据交换格式
.dvi	groff文本处理器格式
.efs	试验性
.po	要求GNOME glossary插入件
.gnumeric	Gnumeric默认XML格式
.tex	LaTeX 2e文件
.xls	Microsoft Excel格式
.csv	导出到逗号分隔格式的文本
.me	来自Troff文本处理器格式

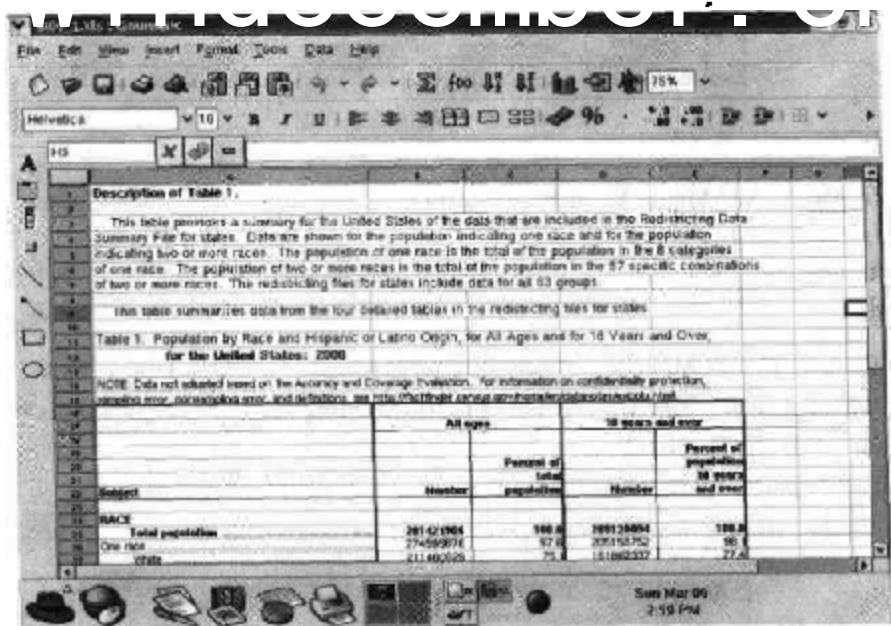


图18.9 Gnumeric电子表格应用程序

说明：电子表格的一个组件是绘图程序。与Gnumeric最接近的标准是Guppi，但到本书编写时，Guppi的主页（www.gnome.org/projects/guppi/）建议用www.gnome.org/projects/guppi/otherprogs.shtml站点的其他免费绘图程序。

MrProject

MrProject是GNOME项目管理应用程序。要启动MrProject, 选择Main Menu►Office►Project Management, 也可以用mrproject命令在GUI命令行界面启动。其中有设置项目的基本工具: 资源表、甘特图、任务表。它是独立的, 到本书编写时还不能从Microsoft Project之类其他项目管理应用程序导入或导出文件。

使用Koffice

还有第三个开放源代码办公套件, 是KDE人员开发的。Koffice应用程序最好运行在KDE中, 但其中许多也可以在GNOME中运行。启动每个Koffice应用程序的菜单步骤是相同的, 可以通过选择Main Menu►Office►More Office Applications访问。

说明: 如果使用KDE, 则K Menu按钮对应于GNOME Main Menu按钮。默认情况下, 两者都在桌面左下角, 都与红帽子图标相关联。

KOffice套件中有几个应用程序, 主要是一系列集成的应用程序。表18.13简要介绍了这些应用程序。

说明: 如果要安装KDE, 可以用第19章介绍的KDE configuration packages实用程序。如果已经安装KDE, 则可以用第15章介绍的switchdesk实用程序使其成为默认的GUI。

表18.13 KOffice应用程序

应用程序	描述
Karbon14	画线和画形体
KChart	支持画图表
KFormula	可以生成与编辑数学公式
Kivio	可以生成流程图
KOffice Workspace	打开其他KOffice应用程序的GUI前端
Kontour	支持画线和画形体, 类似于Karbon14
KPresenter	打开演示应用程序
KSpread	启动KDE电子表格程序
KThesaurus	开始KDE词典
Kugar	支持生成业务报表
KWord	打开KDE字处理程序

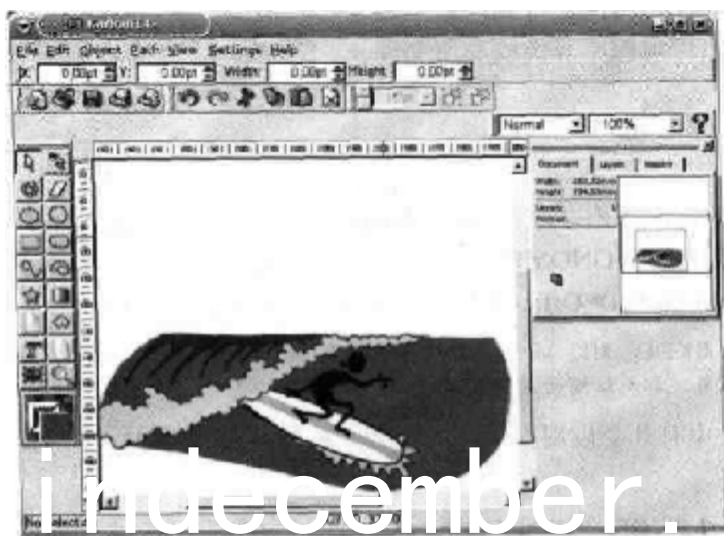
说明: 其中几个KOffice应用程序是试验性的, 目前还不能在生产中使用。要显示应用程序的状态, 打开应用程序, 然后选择Help►About application可以查看。一般来说, 版本为1.0以上的应用程序可以在生产中使用, 但也不一定。大多数应用程序是由志愿者开发和维护的, 甚至到V1.0发布以后也还在开发。

Karbon14

Karbon14是KDE绘图程序, 它包括几种基本绘图功能。要启动Karbon14, 选择Main Menu►Office►More Office Applications►Karbon14, 也可以用karbon命令从GUI命令行界

面启动。

到本书编写时，我用的Red Hat Linux 9版本包括Karbon14 v0.0.1，因此还不能在生产中使用。它的开发还在进行，但潜力巨大，这可以从图18.10看出，这是Karbon14的新版本。如果你从2003版的Red Hat Linux中更新koffice-* RPM包，很可能就是可用的。



(图18.10由Karbon14的开发人员之一——Rob Buis提供)

图18.10 Karbon14

KChart

KChart图表软件主要用于KDE电子表格应用程序KSpread。要启动KChart，选择Main Menu>Office>More Office Applications>KChart，也可以用kchart命令在GUI命令行界面启动。

生成图表后，很容易用饼形图、图表和彩色区等视图组织数据。图18.11显示了条形图。

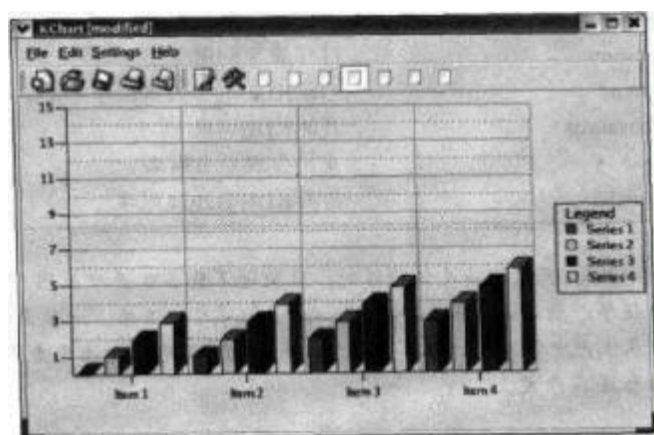


图18.11 KChart中的条形图

Kivio

Kivio是KDE框图编辑器，可以绘制框图，它类似于GNOME Dia和Microsoft Visio程序。要启动Kivio，选择Main Menu>Office>More Office Applications>Kivio，也可以用kivio命令从GUI命令行界面启动。

KPresenter

生成演示时，实际上是生成幻灯片。演示应用程序是带图形的专用字处理程序，它支持室内或网上的幻灯片演示。要启动KPresenter，选择Main Menu>Office>More Office Applications>KPresenter，也可以用kpresenter命令GUI命令行界面启动。

可以像Microsoft PowerPoint或StarOffice Impress等其他应用程序一样用OpenOffice Impress建立演示。

图18.12演示了从Microsoft PowerPoint文件导入的演示。

从图中可以看出，KPresenter包括各种工具栏，有些可以管理颜色，有些可以绘制、管理文本和增加对象。表18.14介绍了这些工具栏。

表 18.14 OpenOffice Impress 工具栏

工具栏	描述
Edit	包括编辑与缩放功能
File	增加基本文件、打印和幻灯显示功能
Format	包括管理直线与形体外观的功能
Insert	支持增加文本、表格、图形、直线，等等
Presentation	可以管理幻灯组织
Text	可以管理演示中的文本
Tools	增加缩放、旋转和对象管理功能

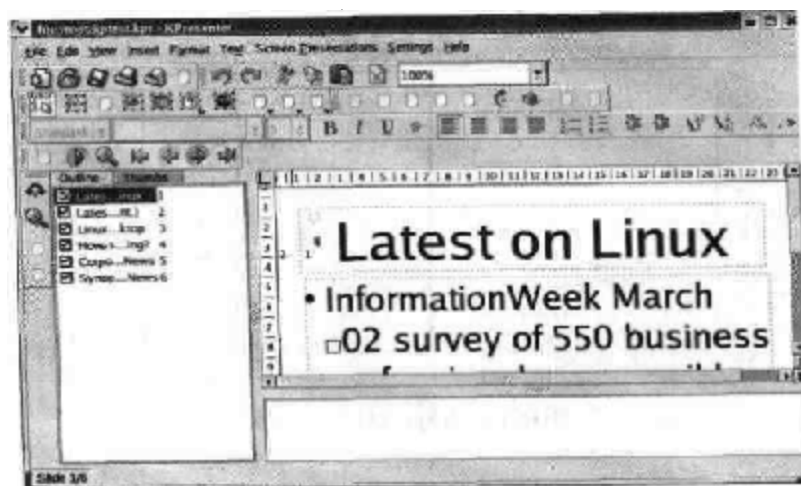


图18.12 在KPresenter中打开Microsoft PowerPoint文件

首次启动KPresenter时，可以选择使用不同模板或打开现有文档。如果这都不是你希望的，则KPresenter可以打开空白文档。

KPresenter只能导入KPresenter、XML与PowerPoint文件，但可以导出更多格式，包括KWord（.kwd）、HTML与RTF格式。

KSpread

可以用电子表格定义各种数据。利用所选公式，可以让电子表格在不同情形中进行从统计分析到业务建模与预测的各种计算。

要打开KSpread，选择Main Menu►Office►More Office Applications►KSpread或在GUI终端窗口中运行KSpread命令。图18.13显示了KSpread和2000年美国人口统计的一些基本数据。

从图中可以看出，KSpread具有电子表格外观，其功能与Microsoft Excel相似，它包括几个工具栏，见表18.15。

表18.15 KSpread工具栏

工具栏	描述
Color/Border	可以配置单元表格边框大小
Edit	已经编辑、排序与图表功能
File	增加基本文件与打印功能
Format	支持每个单元中文本与数字的基本格式
Math	可以配置单元的基本数学函数

Subject	Number	Percent of total population	Percent of population 18 years and over
RACE			
Total population	2,830,228,885	100	2,091,185,096
White	2,251,786,488	82.58	2,051,185,096
Black or African American	2,139,161,488	75.14	1,418,621,096
American Indian and Alaska Natives	2,479,991,096	12.39	2,172,721,096
Native Hawaiian and Other Pac. Is. Islanders	3,624,096	0.13	1,329,991,096
Hispanic or Latino	35,931,096	1.27	2,721,096
Other	1,124,096	0.04	2,418,621,096

图18.13 KSpread和人口统计数据

KSpread适用于多种不同电子表格，包括表18.16所示的文件格式。可以看出，KSpread可以处理几个应用程序中的电子表格，包括Microsoft Excel、Applix Spreadsheets、Gnumeric与Quattro Pro数据库，等等。还可以用逗号分隔格式的文本文件来设置KSpread。

表18.16 KSpread文件格式

格式	描述
.asa	电子表格格式
.csv	逗号分隔格式，文本文件中的电子表格
.gnumeric	Gnumeric电子表格格式
.html	Web页面
.ksp	KSpread电子报表
.wb2	Quattro Pro电子表格格式
.xls	Microsoft Excel 97/2000/XP或Excel 95/5.0

KWord

一个重要的工作是处理各种字处理格式。要用转换器将Microsoft Word文档转换成Corel WordPerfect文档和AbiWord文档。尽管大多数字处理程序都内置了转换器（包括KWord），但每个字处理程序都有一些特殊特性，它们之间很难正确转换。

但人们经常使用的几种特殊性也不能够用KWord正确处理。然而，对大多数应用程序和业务而言，KWord已经足够好了。KWord中生成的新文档可以包括Microsoft Word提供的所有特性。

要启动KWord，选择Main Menu->Office->More Office Applications->KWord，也可以用kword命令在GUI命令行界面启动。图18.14演示了典型文档。

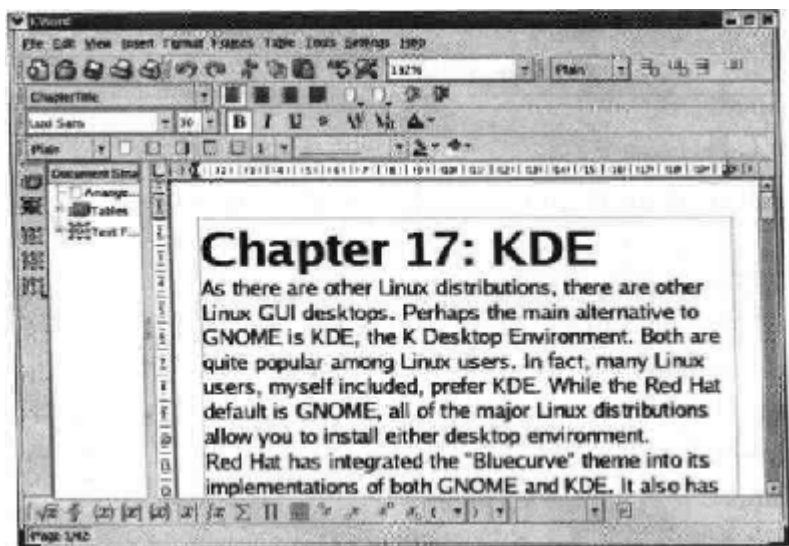


图18.14 KWord打开Microsoft Word文档

可以看出，KWord有五个默认工具栏File、Edit、Insert、Paragraph与Format。KWord中最多可以使用八个不同工具栏，如表18.17所示。

表18.17 KWord工具栏

工具栏	描述
Borders	可以配置边框外观
Edit	包括编辑、排序、缩放和尺寸功能
File	增加基本文件与打印功能
Format	支持文本与颜色的基本格式
Formula	包括数学函数
Insert	可以增加表格、图形和其他对象
Paragraph	支持样式、对齐与强调符
Table	可以在文档中建立表格

KWord可以处理其他字处理程序中的文件，见表18.18。

表18.18 KWord文件格式

格式	描述
.kwd	KWord文档
.doc	Microsoft Word
.html	超文本标记语言，适合Web页面
.t	多语言文本格式，几乎所有处理程序都能阅读的通用格式
.sam	AmiPro文档
.tex	TeX-格式文件
.txt	普通文本
.wpd	WordPerfect文档

其他KOffice工具

其他重要的KOffice工具可以通过Main Menu>Office>More Office Applications子菜单来访问：

- KFormula允许用户生成和建档不同复杂程度的方程，它支持三角函数、积分、极限、指数，等等。功能相当于OpenOffice Math。你可以从命令行用kformula命令开始。
- KOffice Workspace是其他KOffice应用程序的前端，可以用koshell命令启动。
- Kontour支持图形，也可以从扫描仪取得输入。可以用kontour命令启动。
- KThesaurus列出三类可比单词：同义词、更一般的单词和更特定的单词。可以用kthesaurus命令启动。
- Kugar是个报表管理器，相应的Kugar Designer是报表生成工具，样本文件在/usr/share/apps/kugar/templates目录中。

使用图形应用程序

Linux非常适合图形，几个大的运动图形工作室都在Linux计算机上产生动画和特殊效果。因此，下面介绍几个Linux图形应用程序。

Red Hat Linux 9有几个图形应用程序，包括PDF（可移植文档格式）阅读器、图形浏

览器和屏幕捕获程序。可以从Main Menu►Graphics and Main Menu►Graphics►More Graphics Applications子菜单来选择大多数图形应用程序。

图形文档阅读器

Linux中的三种图形文档格式为PDF（可移植文档格式）、PS（PostScript）和DVI（设备独立格式）。

下载Adobe Acrobat阅读PDF文档时，Red Hat Linux包括两个自然的PDF阅读器：xpdf与PS/PDF浏览器。PostScript（PS）文档格式也可以用GNOME Ghostview（GGV）阅读。可以用DVI Viewer、KViewShell阅读DVI（设备独立格式）文档。

说明：奇怪的是，KDE Fax Viewer，Kfax不用于收发传真，而只能浏览传真文件。关于Linux传真程序的更多信息，见www.cce.com/efax。

xpdf

要启动xpdf，选择Main Menu►Graphics►PDF Viewer，也可以用xpdf命令在GUI命令行界面启动。其打开一个没有工具栏的简单屏幕，可以右单击访问一些基本命令。如果要打开PDF文档，输入O，在图18.15所示的Open对话框中，可以访问打开的PDF文件。

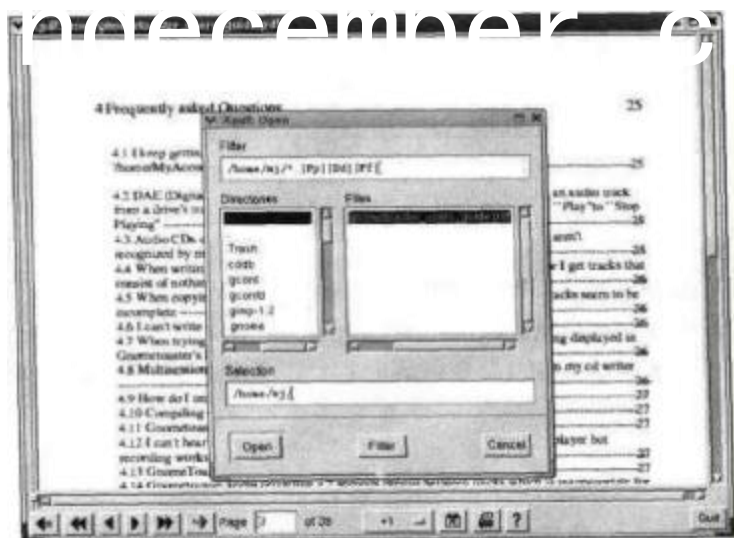


图18.15 访问PDF文件

文件打开之后，可以用屏幕下方的箭头键在文档间导航。也可以用表18.19所列的基本命令。还有其他命令，可以单击Question按钮访问。

表18.19 xpdf基本命令

命令	描述
o	打开新文件
f	寻找文本
n	转入下一页
p	转入上一页

PS/PDF Viewer

PS/PDF Viewer也称为KGhostView。要启动PS/PDF Viewer, 选择Main Menu►Graphics►More Graphics Applications►PS/PDF Viewer, 也可以用pdfviewer命令从GUI命令行界面启动。这个应用程序提供更直观的界面, 可以浏览PDF和PS文件, 如图18.16。

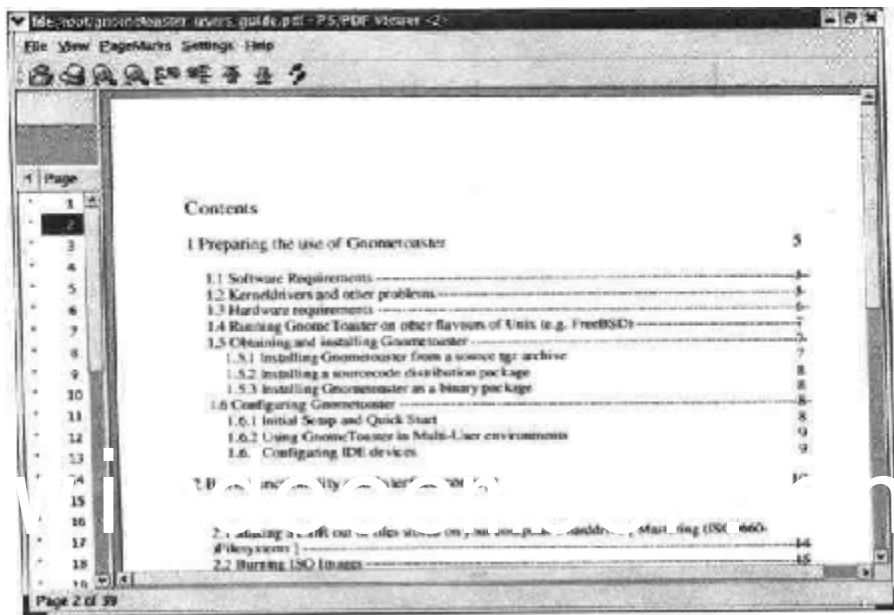


图18.16 用KGhostView浏览PDF文件

PostScript Viewer

PostScript Viewer也称为GNOME Ghostview (GGV), 也可以浏览PDF和PS文件。要启动PostScript Viewer, 选择Main Menu►Graphics►More Graphics Applications►PostScript Viewer, 也可以用ggv命令从GUI命令行界面启动。它与KGhostView一样直观, 窗口也很相似。

DVI Viewer

许多UNIX与Linux文档都需要从TeX处理成DVI (设备无关格式) 文件。这个DVI浏览器也称为KGhostView, 表面上与PDF相似, 因为它显示排版文档的GUI视图。

要启动这个应用程序, 运行kghostview命令。要得到这个应用程序的全部功能, 需要tetex-* RPM软件包, 如图18.17。

DVI浏览器还有其他形式。要启动DVI, 选择Main Menu►Graphics►DVI viewer; 要启动XDVI, 选择Main Menu►Graphics►More Graphics Applications►DVI viewer。

说明: TeX与LaTeX是UNIX与Linux中常用的格式语言, 可以按适合发表的格式设置文本文件。

图形浏览器

Red Hat Linux GUI包括几个图形浏览器。利用这些图形浏览器可以打开、操纵和编

辑现有图形。每种浏览器有不同功能：**GQview**可以生成缩略图，**Kuickshow**可以设置图形浏览器，**Icon Editor**可以管理不同GUI应用程序中图标的外观。

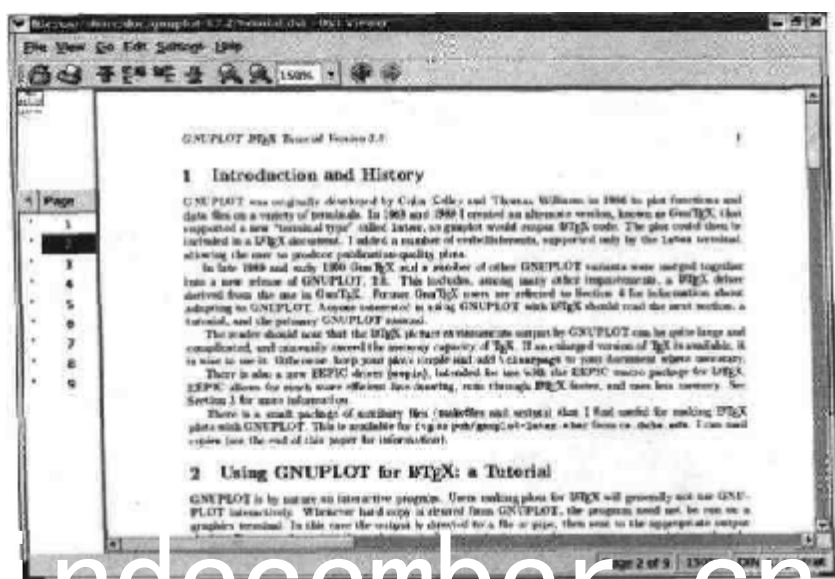


图18.17 浏览GUI文件

GQview

GQview是个图形文件浏览器，可以浏览各种图形、设置幻灯片、组织缩略图，等等。要启动**GQview**，选择**Main Menu>Graphics>GQview Image Viewer**，也可以用**gqview**命令从GUI命令行界面启动。如图18.18所示，基本界面很简单。

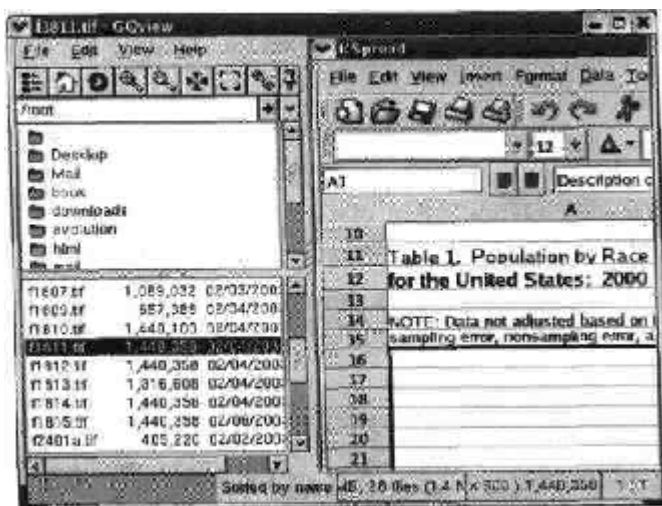


图18.18 用GQview浏览各种图形

Eye of GNOME

Eye of GNOME与**GQview**相似，也是个图形文件浏览器，可以浏览不同文件格式的图

形。但这个程序的编写功能有限，默认只能编写JPEG与PNG格式的文件。

要启动Eye of GNOME，选择Main Menu►Graphics►More Graphics Applications►Eye of Gnome Image Viewer，也可以用eog命令从GUI命令行界面启动。如图18.19所示，浏览图形文件的命令很简单。



图18.19 Eye of GNOME

图标编辑器

图标编辑器KIconEdit可以打开和修改各种图标的样子。要启动图标编辑器，选择Main Menu►Graphics►More Graphics Applications►Icon Editor，也可以用kiconedit命令从GUI命令行界面启动。

图形浏览器

图形浏览器KView和GQview与Eye of GNOME相似，也是个图形文件浏览器，可以输出不同文件格式的图形。要启动图形浏览器，选择Main Menu►Graphics►More Graphics Applications►Image Viewer，也可以用kview命令从GUI命令行界面启动。

Kuickshow

Kuickshow图形浏览器列出所选目录中的图形。要启动Kuickshow，选择Main Menu►Graphics►More Graphics Applications►Kuickshow，也可以用kuickshow命令从GUI命令行界面启动。

双击图形文件时，Kuickshow在另一窗口中打开图形。然后可以右击图形打开一个菜单，操纵图形的外观。图18.20显示了Kuickshow屏幕。

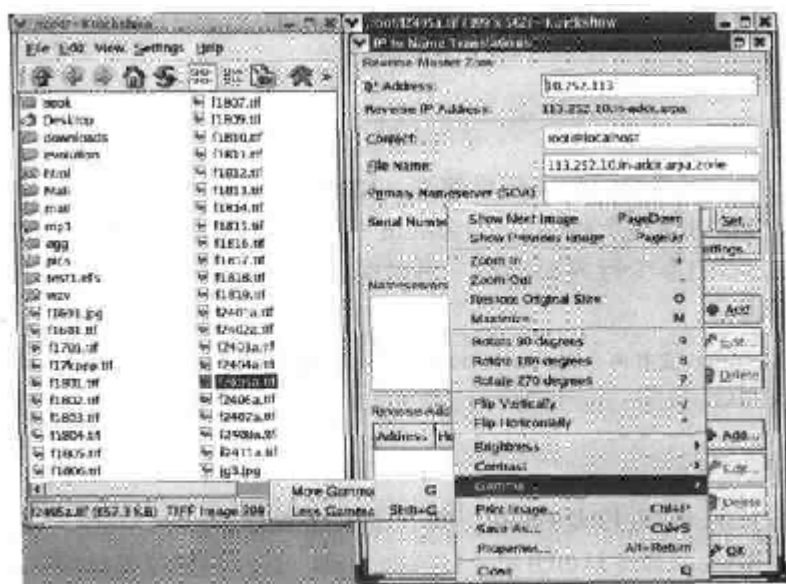


图18.20 Kuickshow图片管理器

Paint Program

Paint Program也称为KPaint，可以打开、增加和修改图形。要启动绘图程序，选择Main Menu►Graphics►More Graphics Applications►Paint Program，也可以用kpaint命令在GUI中从命令行界面启动。

图18.21显示了如何增加和剪切第16章第一幅图中的图形。

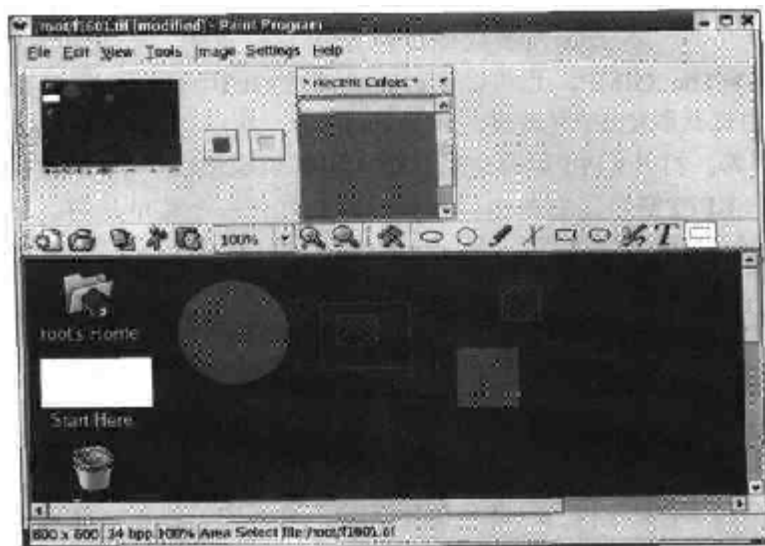


图18.21 用KPaint编辑图形

屏幕捕获程序

有时要记录屏幕上的设置。如果向别人描述问题，则可以建立包括桌面外观的图形。

有些程序的图形来自其他硬件，如数码相机和扫描仪，而有些图形直接来自桌面屏幕或活动桌面窗口。

数码相机

gphoto2-* RPM有几个GUI数码相机前端，KDE包为Kamera，标准红帽子软件包为Digital Camera Tool。要启动这个程序，选择Main Menu►Graphics►Digital Camera Tool，也可以用gpcam命令从GUI命令行界面启动。可以探测的数码相机清单并不完整，详细信息见www.gphoto.org站点。

说明：www.tldp.org站点有两个特殊的HOWTO文档：Kodak-Digitalcam-HOWTO与USB-Digital-Camera-HOWTO。

扫描

标准红帽子GUI扫描程序是xsane，要启动这个程序，选择Main Menu►Graphics►Scanning，也可以用xsane命令从GUI命令行界面启动。有些扫描仪无法用xsane探测，这时会提示这个消息，并且不打开xsane。

还有一个KDE扫描程序Kooka，支持xsane并拥有字符识别功能。要启动Kooka，选择Main Menu►Graphics►More Graphics Applications►Scan & OCR Forman，也可以用kooka命令从GUI命令行界面启动。

GIMP

我喜欢的Linux图形程序是GIMP，它是GNU图形操纵程序。许多Linux用户认为GIMP比Adobe公司的Photoshop和Jasc公司的Paint Shop Pro之类的高端图形程序更好用。GIMP放在GNOME办公套件中。本书的大多数图片都是用它配置的。要启动这个程序，选择Main Menu►Graphics►The GIMP，也可以用gimp命令在GUI中从命令行界面启动。

例如，第17章获取KPPP屏幕时，我启动GIMP，然后选择File►Acquire►Screen Shot打开Screen Shot屏幕。打开KPPP屏幕之后，单击屏幕瞬像窗口中的OK按钮，使光标变成加号(+)。我用它选择KPPP窗口。右单击屏幕瞬像时其打开一个菜单，可以将图形保存到所选文件中。图18.22显示了不同图形和结果。

另一个图形程序KcolorChooser

KColorChooser也称为KColorEdit，可以编辑调色板。要启动这个程序，选择Main Menu►Graphics►More Graphics Applications►Color Chooser，也可以用kcolorchooser命令从GUI命令行界面启动。

图18.23显示了DarkCyan（深青）在标准颜色模式中的位置。注意RGB（红绿蓝）的相对水平，每个颜色有不同红、绿、蓝值，这个值介于0到255之间。

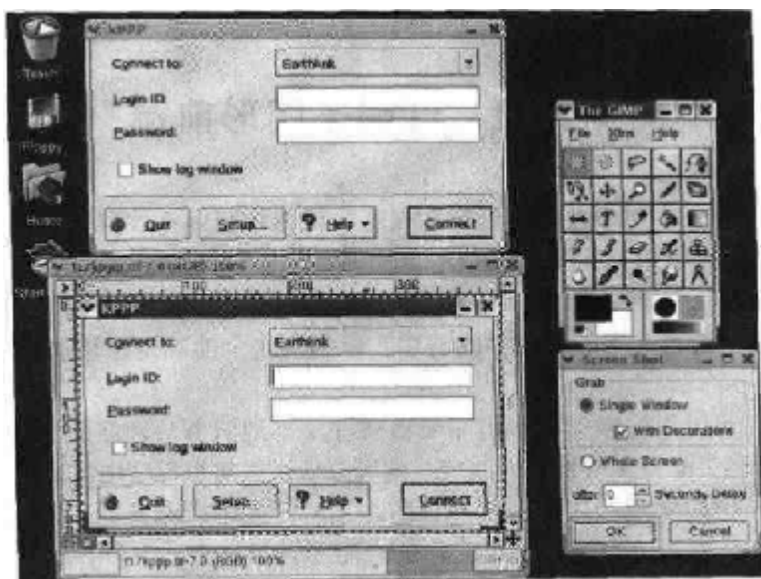


图18.22 C IMP



图18.23 用KColorChooser定义颜色

小结

Red Hat Linux带有各种特性完全的GUI应用程序。红帽子光碟中有三个办公套件和一些强大的图形应用程序。

Red Hat Linux所带的办公套件有OpenOffice、GNOME Office和KOffice。每个办公套件都有字处理程序、电子表格、绘图程序、框图生成器和演示管理器，还有项目管理工具、数学公式管理器和个人财务程序。

图形程序包括简单颜色管理器（如GQview）和完全特性的图形程序（如GIMP）。这个类别还包括GUI文档浏览器，如PDF、DVI与PS阅读器。

第19章将介绍红帽子公司建立的许多GUI管理工具，这些工具的实用程序名称通常以redhat-config-*开头，我们将按这个顺序来介绍。这些工具大部分可以从Main Menu►System Settings子菜单访问。

第19章 红帽子图形前端

本章介绍红帽子公司开发的图形前端程序，使得你可以在计算机和网络上管理与配置Linux。传统的Linux用户可能不太关心本章的内容，他们更喜欢从命令行界面工作。

传统的Linux用户认为，命令行能做更多工作。因为红帽子图形前端还在不断开发之中。事实上，它们只是编辑文本配置文件的前端。但是，这个前端可以帮助新的Linux用户过渡到Linux。

我们相信，可以用红帽子图形前端配置硬件、本地服务与网络服务和进行基本的系统管理。如果分析相关配置文件发生的改变，则可以从这些实用程序中学习更多的Linux知识。

但要记住，这些实用程序还很新，且还在不断开发中，因此使用图形实用程序后，应该检查配置文件，看看改变是否反映了你的意图。

要显示可用的实用程序清单，可以到命令行界面，输入redhat-config-，然后按Tab键两次。可以看到整个实用程序清单，如图19.1。当然，可以用看到的命令启动这些实用程序。其中一些实用程序在其他章节有介绍。

```
[root@RH9Desk root]# redhat-config-
redhat-config-bind          redhat-config-packages
redhat-config-bind-gui     redhat-config-printer
redhat-config-date         redhat-config-printer-gui
redhat-config-httpd       redhat-config-printer-tui
redhat-config-keyboard     redhat-config-proc
redhat-config-kickstart    redhat-config-rootpassword
redhat-config-language     redhat-config-samba
redhat-config-mouse        redhat-config-securitylevel
redhat-config-network      redhat-config-services
redhat-config-network-cmd  redhat-config-soundcard
redhat-config-network-druid redhat-config-time
redhat-config-network-gui  redhat-config-users
redhat-config-network-tui  redhat-config-xfree86
redhat-config-nfs
[root@RH9Desk root]# redhat-config-
```

图19.1 redhat-config-*图形实用程序

大多数实用程序也可以通过在GNOME选择Main►System Tools或在KDE中选择Main Menu►System Settings访问（如果使用KDE，则按钮仍然显示红帽子，只是它称为K Menu按钮而不是Main Menu按钮）。有几个实用程序要求管理权限，如果不是以根用户（或其他权限用户）身份登录，则会在需要时提示输入根口令。

如果命令行或主菜单中没有看到特定工具，则需要安装这个工具。大多数情况下，RPM包名与命令名相同，例如，Samba配置工具是redhat-config-samba，它来自redhat-config-samba-* RPM包。

由于redhat-config-*实用程序没有正式类别，因此我在本章对其随意分类。本章将介绍下列主题：

- 用基本配置实用程序进行配置
- 用网络配置实用程序连接
- 使用系统管理实用程序
- 使用服务配置实用程序

用基本配置实用程序进行配置

许多红帽子图形配置实用程序可以通过在GNOME中选择Main Menu►System Settings来访问。这些实用程序可以设置日期和时间、定制键盘、指定默认语言、定制鼠标功能和设置声卡，见表19.1。

表19.1 红帽子基本配置实用程序

实用程序	功能
redhat-config-date redhat-config-time	可以设置日期和时间以及NTP服务器连接
redhat-config-keyboard	可以设置系统的默认键盘
redhat-config-language	可以改变图形桌面的默认语言
redhat-config-mouse	可以定制鼠标和其他指示设备
redhat-config-soundcard	可以自动探测和配置声卡

设置日期与时间

对计算机正确地设置日期与时间非常重要。如果Internet商店的服务器分布在不同时区，则要在服务器之间同步时间。Red Hat Linux用TCP/IP协议栈中的NTP（网络时间协议）进行配置。

要启动Red Hat Date/Time Properties工具，选择Main Menu►System Settings►Date & Time，也可以用redhat-config-date和redhat-config-time命令从GUI命令行界面启动，从而打开日期/时间属性窗口，如图19.2。

可以自己设置日期与时间。接受任何改变之后，Linux改变计算机上的硬件时钟。也可以将其设置为与远程服务器时钟同步。利用NTP和网络连接，Linux可以发一个请求当前日期与时间的消息给中央时间服务器。

说明：如果把系统时钟的控制交给NTP服务器，则日期/时间属性窗口中不能独立设置时间。

无论如何，Red Hat Linux还可以设置与计算机相关的时区。从图19.3可以看出，可以将计算机设置为不同时区，其默认为标准美国东部时区，显示为America/New_York。可以将系统设置为几百个时区地点之一。

除非将计算机配置成和Microsoft Windows等类似的另一操作系统双重引导，否则应该激活System Clock Uses UTC选项。UTC是协调统一时间的法语缩写，它相当于格林威治平均时间。如果选择UTC，则Linux将硬件时钟设置为这个时间，计算当地系统时钟的时区差。

时区改变保存在/etc/sysconfig/clock文件中，任何指定的NTP服务器记录在/etc/ntp/ntpserver中。自然，也可以直接编辑这些文件。也许NTP服务器的权威Web站点是德拉华大学的站点www.eecis.udel.edu/~ntp，其中有一个链接，列出了全世界的活动NTP服务器。

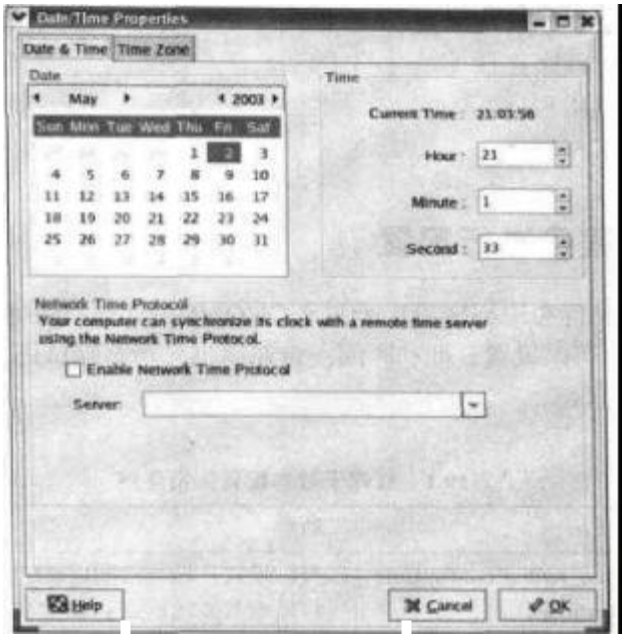


图19.2 日期/时间属性工具

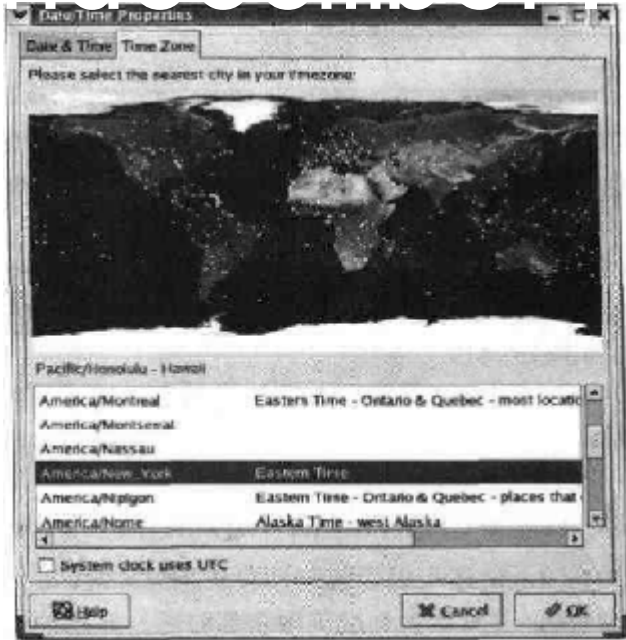


图19.3 设置时区

红帽子日期/时间属性工具自动将网络时间协议监控程序ntpd设置为下次使用组3和5启动Linux时启动。可以用下列命令进行验证：

```
# chkconfig --list ntpd
```

如果配置了防火墙，则红帽子日期/时间属性工具自动生成防火墙规则，使计算机可以

从外部NTP服务器接收数据。例如，如果用iptables -L命令列出防火墙规则，则可以在防火墙链中看到下列规则：

```
ACCEPT udp -- ns3.oit.unc.edu anywhere udp spt:ntp dpt:ntp
```

其中ns3.oit.unc.edu是时间服务器的完全限定域名。如果运行不同的时间服务器，则要换上相应域名。

配置键盘

可以对不同语言、方言和系统配置键盘。可以用红帽子键盘实用程序将键盘设置成最接近于系统的键盘。

要启动这个工具，选择Main Menu>System Settings>Keyboard，也可以用redhat-config-keyboard命令从GUI命令行界面启动，从而打开键盘选择窗口，如图19.4。

从图中可以看出，不同语言和国家位置有多个键盘可供选择。如果需要，选择最接近硬件的键盘，然后单击OK按钮。键盘改变保存在/etc/sysconfig/keyboard文件中。

说明：如果从文本方式控制台运行redhat-config-keyboard，则这个实用程序在蓝色文本方式低图形屏幕中显示相同选项，但顺序有所不同。

选择语言

可以用红帽子语言实用程序从所安装语言中选择图形默认。要启动这个程序，选择Main Menu>System Settings>Language，也可以用redhat-config-language命令从GUI命令行界面启动。其打开语言选择窗口，如图19.5。这个窗口通常包括安装过程中安装的语言。

如果安装Red Hat Linux时没有安装所要的语言，则可以现在安装所需语言相关的RPU包。要寻找相应清单，打开comps.xml文件，它在Red Hat Linux第一张安装光碟的/RedHat/base目录或/usr/share/comps/i386目录中。例如，如果要安装韩国语相关的包，则要找到这个文件的Korean部分（关于comps.xml中所带语言的信息，见Sybex公司Web站点www.sybex.com上的第5章）。

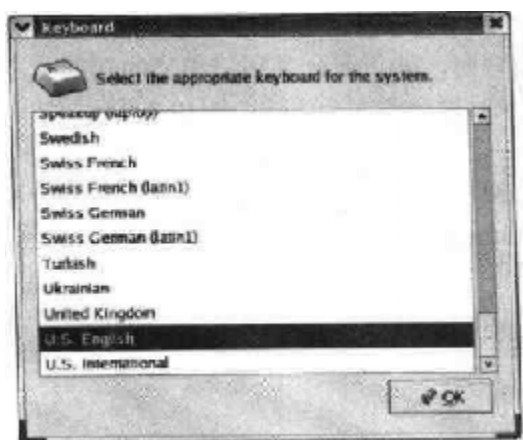


图19.4 键盘选择窗口



图19.5 语言选择窗口

```
<packagelist>
  <packagereq type="mandatory">nvi-m17n</packagereq>
  <packagereq type="optional" requires="kdelibs">kde-i18n-Korean</packagereq>
  <packagereq type="optional" requires="man-pages">man-pages ko</packagereq>
  <packagereq type="optional" requires="XFree86">ami</packagereq>
  <packagereq type="optional" requires="XFree86">hanterm-xf</packagereq>
  <packagereq type="mandatory">h2ps</packagereq>
  <packagereq type="mandatory">nhp</packagereq>
  <packagereq type="mandatory">ttfonts-ko</packagereq>
</packagelist>
```

从这个清单中安装最新的强制RPM包，然后打开/etc/sysconfig/i18n文件。修改相应地方的SUPPORTED变量。/usr/X11R6/lib/X11/locale目录中列出了不同的语言和字符集。例如，这个目录中韩国语相关的语言场景和字符类型如下：

```
ko_KR.UTF-8
```

现在打开/etc/sysconfig/i18n文件，按下列格式增加相应地方的SUPPORTED变量：

```
language_locale.chartype:language_locale:language
```

对所列韩国语相关的语言、场景和字符类型，就是：

```
ko_KR.UTF-8:ko_KR:ko
```

图19.6显示了结果，这里显示我的/etc/sysconfig/i18n文件。这个文件包括中文、美式英语、法语和韩语的设置。

```
LANG="en_US.UTF-8"
SUPPORTED="zh_CN.GB18030:zh_CN:zh:en_US.UTF-8:en_US:en:fr_FR.UTF-8:fr_FR:fr:ko_KR.UTF-8:ko_KR:ko"
SYSFONT="latarcyrheb-sun16"
-
-
-
```

图19.6 /etc/sysconfig/i18n文件中的语言设置

下次打开redhat-config-language实用程序窗口时，即可看到韩国语相关的选项。选择另一语言时，redhat-config-language会表示下次登录时这个改变会生效。图19.7显示了结果，是韩语版的GNOME桌面。

有些应用程序要求自己的语言包和设置，这些内容超出了redhat-config-language和本书范围，要了解这些，可以查阅Linux Documentation Project (www.tldp.org) 中几个语言特定的HOWTO文件。

提示：KDE控制中心有自己的语言配置小程序，见第17章介绍。

配置鼠标

可以配置多种类型的指示设备，最常用的指示设备是鼠标，配置过程中，这些术语可以交换使用。要配置默认指示设备的设置，启动红帽子鼠标配置实用程序。



图19.7 韩语版的GNOME桌面

要启动这个程序，选择 **System Menu** → **System Settings** → **Mouse**，也可以用 `redhat-config-mouse` 命令从 GUI 命令行界面启动。打开鼠标配置窗口，如图 19.8。

默认设置基于当前的/etc/sysconfig/mouse文件，任何改变都记录在这里。如果使用双键鼠标，则有必要激活Emulate 3 Button Click选项，使鼠标可以在同时按左右键时仿真中间鼠标键的功能。第17章曾介绍过，KDE用中间鼠标键打开弹出命令的菜单。

如果鼠标连接串行端口，则可以选择Serial Devices按钮打开一个菜单，选择实际使用的串行设备。如果过去在这个计算机上使用Microsoft操作系统，则应将鼠标设置为表19.2所示的相关Microsoft COM端口。

表19.2 鼠标串行设备

设备文件	描述
/dev/ttyS0	对应于Microsoft COM1端口
/dev/ttyS1	对应于Microsoft COM2端口
/dev/ttyS2	对应于Microsoft COM3端口
/dev/ttyS3	对应于Microsoft COM4端口

提示：这些串行设备还可以配置电话MODEM。如果在Microsoft Windows窗口中已经配置电话MODEM，则要特别注意与其相关的COM端口。如果运行ls -l /dev/modem命令，则可以看到表19.2所示相关设备文件的链接。

如果改变并关闭redhat-config-mouse, 则Linux停止并重新启动鼠标控制台。

提示： 如果不用GUI运行redhat-config-mouse，则红帽子Linux可以在文本控制台中自动启动这个实用程序的文本方式版本。

设置声卡

Red Hat Linux可以配置多种声卡。要设置默认声卡，可以启动红帽子声卡配置实用程序。

要启动这个程序，选择Main Menu>System Settings>Soundcard Detection，也可以用redhat-config-soundcard命令从GUI命令行界面启动，从而打开声音设备窗口，如图19.9。

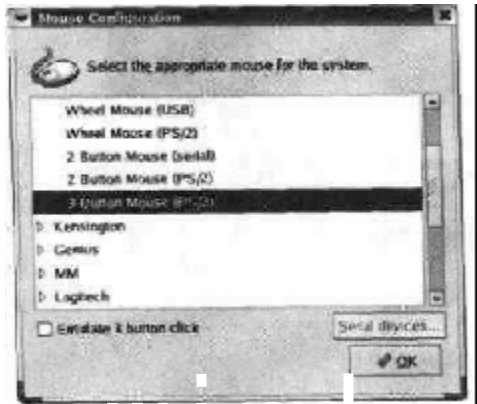


图19.8 配置鼠标

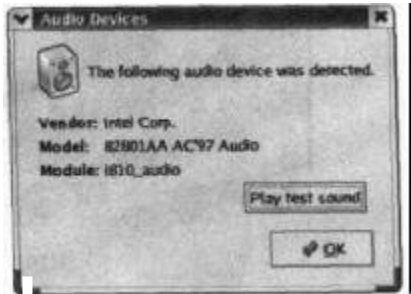


图19.9 设置声卡

如果redhat-config-soundcard在系统中发现声卡，则可以在声音设置窗口中看到卡的型号和版本。如需测试结果，可以单击Play Test Sound选项。假设有声卡并连接音箱，则可以听到一个声音，并看到一个确认窗口。确认结果，然后在声音设备窗口中单击OK按钮。如果Linux要安装声卡的特殊内核模块，则所做改变将被写入/etc/modules.conf文件中。

说明：到本书编写时，如果安装sndconfig-* RPM包，则可以从命令行用sndconfig实用程序配置声卡。它更灵活，可以为声卡设置特定硬件地址。但是，红帽子公司已经把sndconfig作废，并准备在今后的Red Hat Linux版本中将其完全删除。由此可见，红帽子公司对redhat-config-soundcard充满信心。

用网络配置实用程序连接

许多图形实用程序可以将计算机与网络相连，有些可以配置各种网络服务。尽管这些实用程序会在相关章节详细介绍，但这里还是简要介绍每个红帽子网络图形工具。

表19.3总结了红帽子网络图形工具，记住，这只是个任意清单，它列出了本节介绍的实用程序。

表19.3 红帽子网络图形工具

实用程序	功能
redhat-config-network-druid	帮助配置网络连接
redhat-config-network-tui	帮助从文本控制台配置网络连接
redhat-config-network	列出与配置的网络适配器相关的设置

(续表)

实用程序	功能
redhat-config-network-gui	
redhat-config-httpd	可以配置Apache web服务器
redhat-config-bind	可以配置DNS服务器
redhat-config-nfs	可以配置NFS服务器
redhat-config-samba	可以配置Samba服务器
Samba Web Administration Tool	可以通过Web界面配置Samba服务器

基本网络配置

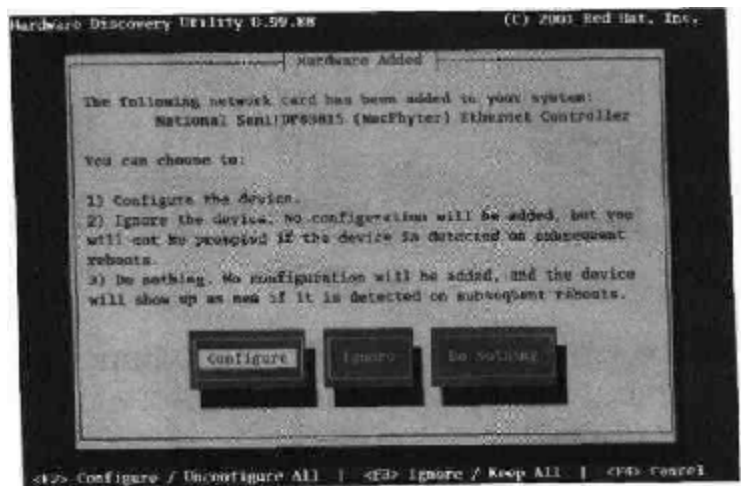
两个基本的网络配置工具是redhat-config-network和redhat-config-network-druid。它们控制计算机上网络设备的配置。

要启动redhat-config-network-druid，选择Main Menu►System Tools►Internet Configuration Wizard。打开Add New Device Type窗口，如图19.10。

图 19.10

如果Red Hat Linux没有探测到网卡，可以启动红帽子硬件探测实用程序——Kudzu。Kudzu可以探测到新安装的硬件，包括网卡。

Kudzu在引导过程中自动运行。但如果刚刚在便携电脑PCMCIA槽中安装PC卡之类的新网卡，则可能需要再次运行Kudzu。如果发现新硬件，则会让你配置硬件，如下图所示。



说明：第21章将介绍如何用redhat-config-network-druid设置电话MODEM。

本节用它配置第二个（未探测到的）以太网连接。在窗口中加亮显示Ethernet Connection并单击Forward按钮继续，打开图19.11所示的窗口，可以检查发现的以太网卡。如果Linux已经控制到第二个以太网卡，则你很方便。图19.11假设Linux没有发现这个卡，则选择Other Ethernet Card并单击Forward按钮继续。

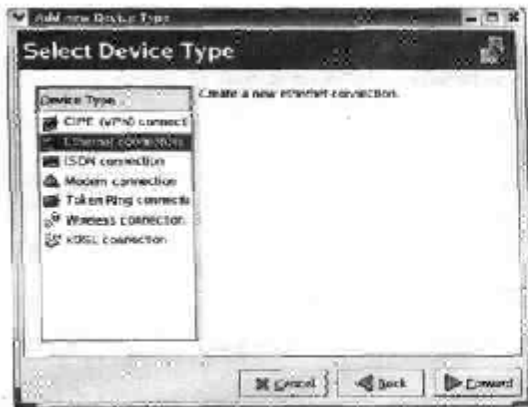


图19.10 增加新的网络设备

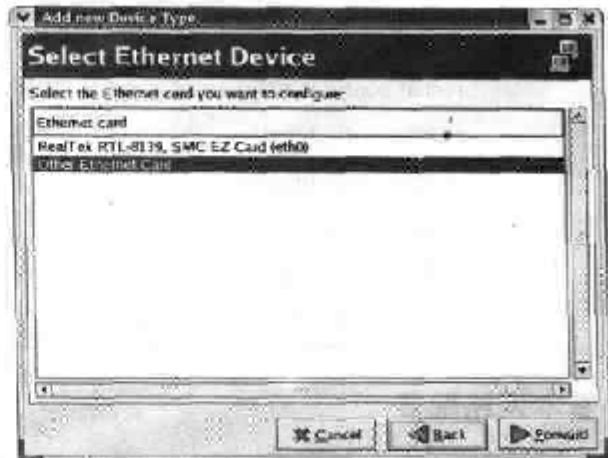


图19.11 选择以太网卡

现在可以设置与第二个以太网卡相关的设备驱动器和硬件地址。图19.12可以指定与新卡相关的驱动器和硬件资源。

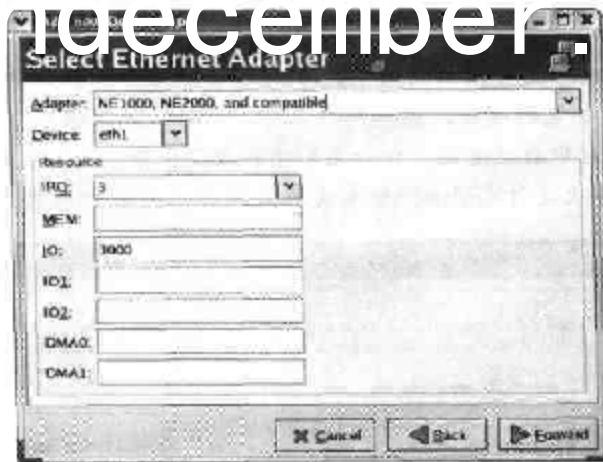


图19.12 设置设备驱动器和硬件地址

最后，可以配置新卡的网络设置。如图19.13，可以用DHCP或BOOTP服务器（关于DHCP或BOOTP的详细信息，见第24章）。Dialup选项通常只适用于已经配置电话MODEM时，与连接ISP的电话MODEM相关联。

也可以设置静态IP地址。关于指定IP地址的更多信息，见第20章。

确认改变之后，进入网络配置窗口，如图19.14。这是redhat-config-network工具，可以通过选择Main Menu►System Settings►Network访问。

首次配置一个网卡时，它是不活动的。可以通过引导过程，或加亮并单击Activate按钮将它激活，如图19.14。如果设置的配置不错，则显示的状态从Inactive变成Active。

每个网卡的配置保存在ifcfg-ethn目录中。以太网网卡的配置文件为ifcfg-ethn，其中n是卡的编号，通常是0或1。

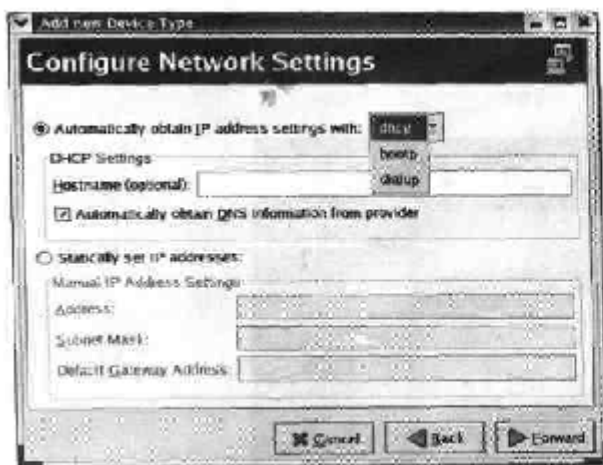


图19.13 IP地址设置

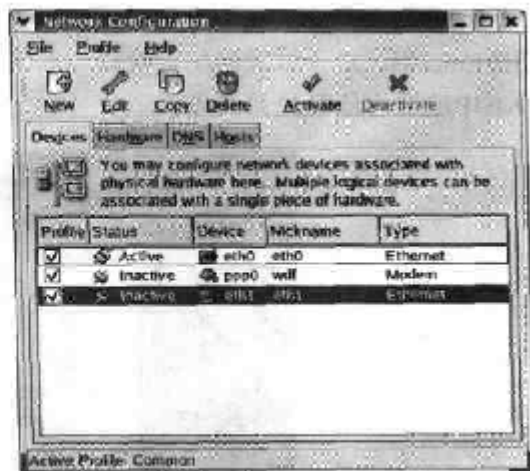


图19.14 网络配置窗口

补充网络配置

在图19.4所示的网络配置窗口中还可以进行更多设置。可以看出，这个窗口还有三个标签：

Hardware标签列出每个配置的网络设备。

DNS标签可以设置计算机主机名，最多可以有三个不同DNS服务器和一个DNS搜索路径。主机名保存在/etc/sysconfig/network中，DNS服务器信息保存在/etc/resolv.conf中。

可以设置主机名、域名和相应IP地址数据库。这里的改变保存在/etc/hosts中。

文本方式网络配置

Linux计算机上可以用文本方式进行网络配置。用redhat-config-network-tui命令启动图19.15所示的文本方式网络配置窗口，可以设置以太网、电话MODEM或ISDN适配器等网络设备。

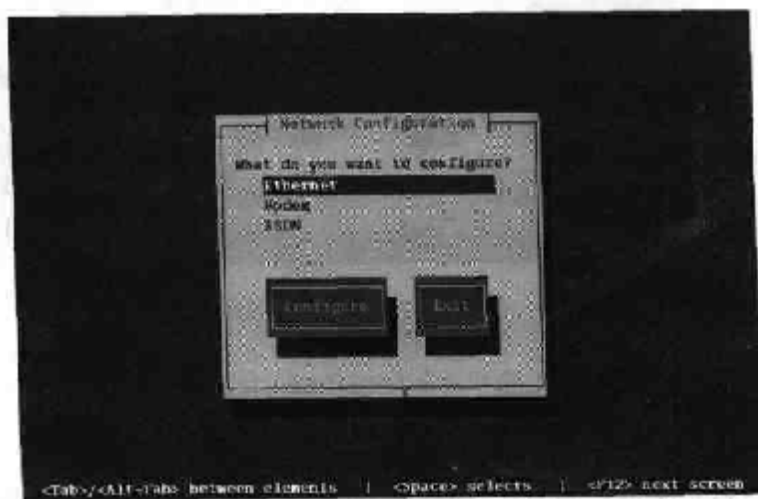


图19.15 文本方式网络配置

如果要用这个实用程序建立以太网连接,则加亮这个选项,按Tab键加亮Configure,然后按Enter键,进入以太网配置窗口,如图19.16。关于DHCP的更多信息见第24章,关于设置静态IP地址的信息见第20章。



图19.16 文本方式中配置以太网网卡

和图形方式中一样,改变保存在/etc/sysconfig/networking/devices目录中。配置文件是ifcfg-ethn,其中n是卡的编号,通常是0或1。

如果用redhat-config-network-tui设置电话MODEM,则回到图19.15的窗口,加亮MODEM选项,按Tab键加亮Configure,然后按Enter键,进入MODEM配置窗口,如图19.17。

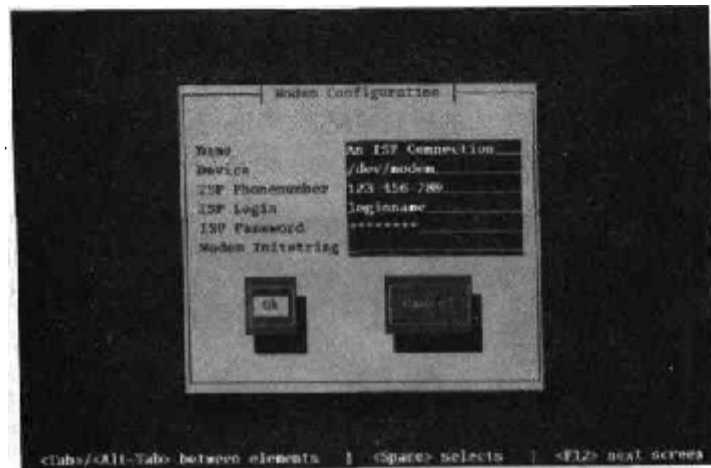


图19.17 配置MODEM连接

可以设置所选名称。如果正确探测到MODEM,则其应链接到/dev/modem上。其余信息可以从ISP那里取得,通常不必填写MODEM Initstring字段。

关于每个选项的更多信息,见第21章。如果MODEM能工作,则改变保存在/etc/sysconfig/networking/devices目录中。配置文件是ifcfg-ethn,其中n为MODEM的编号。

如果要用MODEM设置ISDN适配器, 则回到图19.15的窗口, 加亮ISDN选项, 按Tab键加亮Configure, 然后按Enter键, 进入ISDN配置窗口, 如图19.18。

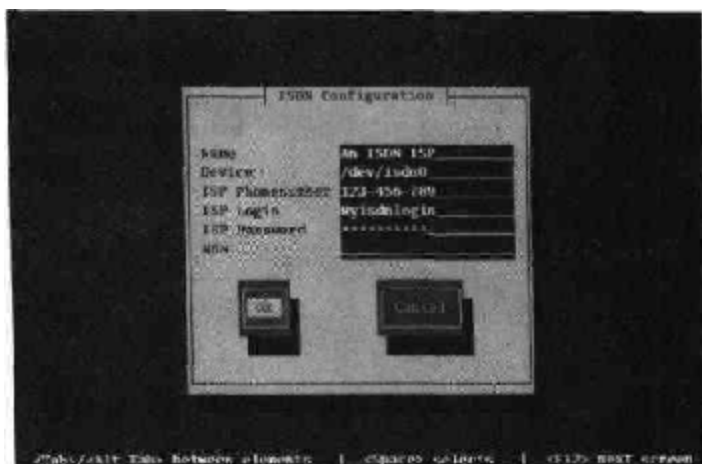


图19.18 配置ISDN适配器

根据ISP的指示配置适配器, 应包括MSI(多用户号), 通常由ISP提供。如果ISDN适配器能工作, 则改变保存在/etc/sysconfig/networking/devices目录中, 配置文件是ifcfg-ethn, 其中n是适配器的编号。

说明: ISDN表示综合服务数字网, 是旧的电话数字标准。消费者ISDN适配器在欧洲比较普及, 根据系统情况, 通常支持的数据传输速率为128或144Kb/s。

Apache

可以用redhat-config-httpd实用程序在计算机上配置Apache服务器。首先要从GNOME桌面上选择Main Menu>System Settings>Server Settings>HTTP Server启动这个实用程序, 打开Apache配置窗口, 如图19.19。关于这个实用程序的详细信息, 见第30章。

如果已经配置Apache服务器, 则可以用它来检查配置内容, 它读写主Apache配置文件/etc/httpd/conf/httpd.conf中的关键变量。

域名服务 (DNS)

可以用redhat-config-bind实用程序在计算机上配置域名服务 (DNS) 服务器。首先从GNOME桌面上选择Main Menu>System Settings>Server Settings>Domain Name Service启动这个实用程序, 打开域名服务配置窗口, 如图19.20。关于这个实用程序的详细信息, 见第24章。

如果已经配置了DNS服务器, 则可以用这个实用程序检查配置内容, 它读取主DNS配置文件/etc/named.conf和/etc与/var/named目录中的相关文件。

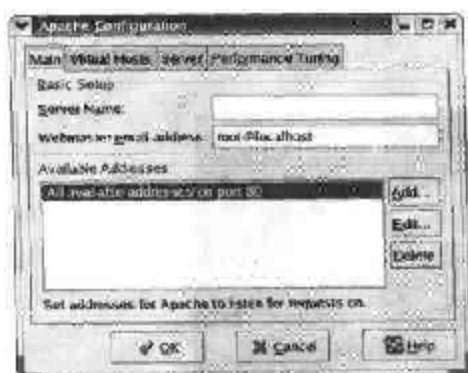


图19.19 Apache配置窗口

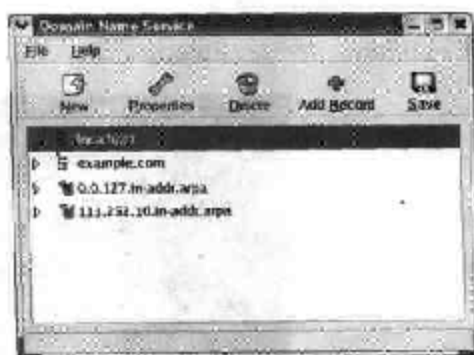


图19.20 DNS配置窗口

网络文件系统 (NFS)

可以用redhat-config-nfs实用程序在计算机上配置网络文件系统(NFS)服务器。首先要从GNOME桌面上选择Main Menu>System Settings>Server Settings>NFS Server启动这个实用程序,打开NFS配置窗口如图19.21。关于这个实用程序的详细信息,见第24章。

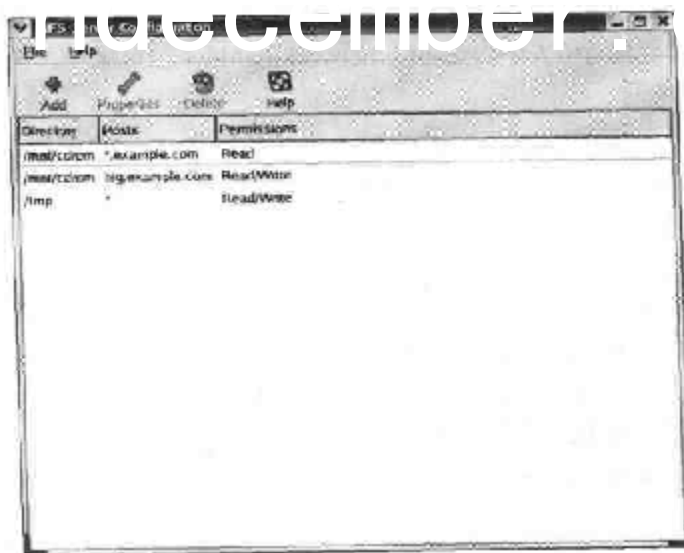


图19.21 NFS配置窗口

如果已经配置了NFS服务器,则可以用这个实用程序检查配置内容,它读取NFS配置文件/etc/exports中的关键变量。

Samba

有两个不同的Samba图形配置实用程序:redhat-config-samba与samba-swat。redhat-config-samba是个图形红帽子工具,它将Linux计算机配置为Microsoft Windows网络上的Samba服务器。可以从GNOME或KDE桌面选择Main Menu>System Settings>Server Settings>Samba Server启动,打开Samba服务器配置窗口,如图19.22。

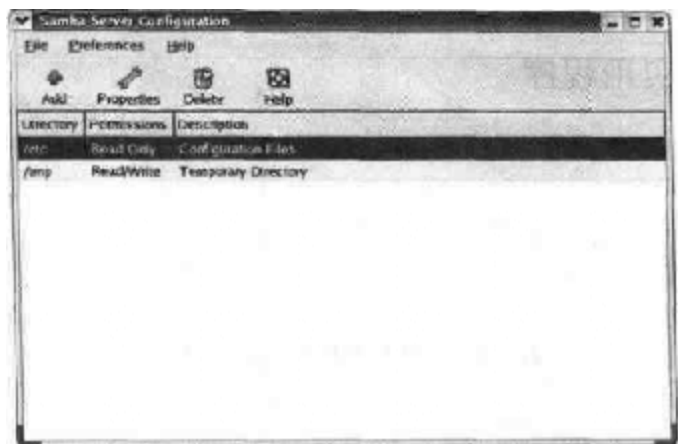


图19.22 Samba服务器配置窗口

另一个工具是Samba人员开发的，是个Web工具，可以将Linux计算机配置为Microsoft Windows网络上的Samba服务器，并进行详细配置。打开所选浏览器并导航到localhost: 901。如果激活了正确的服务，则在默认浏览器中打开Samba Web管理工具（SWAT），如图19.23。



图19.23 Samba Web管理工具

Samba Web管理工具要求事先安装samba-swat-* RPM包和启用/etc/xinetd.d/swat配置文件中的服务。

这两个实用程序都是前端，可以帮助配置主Samba配置文件——/etc/samba/smb.conf和/etc/samba目录中的其他配置文件。关于这两个实用程序的详细描述，见第29章。

使用系统管理实用程序

红帽子公司开发了另外几个图形实用程序，以帮你完成Linux系统进行日常的管理工作。它们开发处于不同阶段，红帽子公司发布新版本和新包时应该会有所改进。

表19.4汇总了红帽子图形化系统管理实用程序。记住，这只是本地介绍的实用程序清单，也可以把本章介绍的其他实用程序归类为系统管理实用程序。

表19.4 红帽子图形系统管理实用程序

实用程序	功能
redhat-config-packages	管理RPM包组
redhat-config-rootpassword	改变根用户口令
redhat-config-users	增加与维护用户
redhat-config-xfree86	配置GUI
redhat-logviewer	检查当前日志文件
redhat-update-gnome-font-install	更新字体
redhat-update-gnome-font-install2	更新字体
redhat-config-kickstart	建立自动安装的Kickstart文件
redhat-config-securitylevel	配置防火墙
redhat-config-proc	改变/proc中的内核设置
authconfig-gtk	设置验证
authconfig	使用authconfig-gtk的文本方式版本

管理RPM包组

可以用redhat-config-packages实用程序检查、安装和删除当前Linux系统中的RPM包。从GNOME桌面选择Main Menu>System Settings>Add/Remove Applications，打开包管理窗口，如图19.24。

如果按第3章介绍的图形方法安装Red Hat Linux，则已经见过图19.24，其中包括与图形安装过程中相同的包组组织。

可以选择每个组中的各个包进行安装或删除。例如，我们看看与KDE桌面环境相关的包。在相关项目的最右端，单击Details打开KDE桌面环境包细节窗口，如图19.25。

可以看出，包分为两类：标准包和多余包。标准包对应于Web上第5章介绍的comps.xml文件中定义的强制包，多余包对应于comps.xml文件中定义的默认包或可选包。

这样，可以取消所选包或包组。进行选择，然后单击Close按钮。单击包管理窗口的Update时，这个实用程序保证没有不满足的依赖性。从系统中删除取消的包之前，还有一次机会取消这个操作（如图19.26）。可以单击Show Details检查要删除的包。

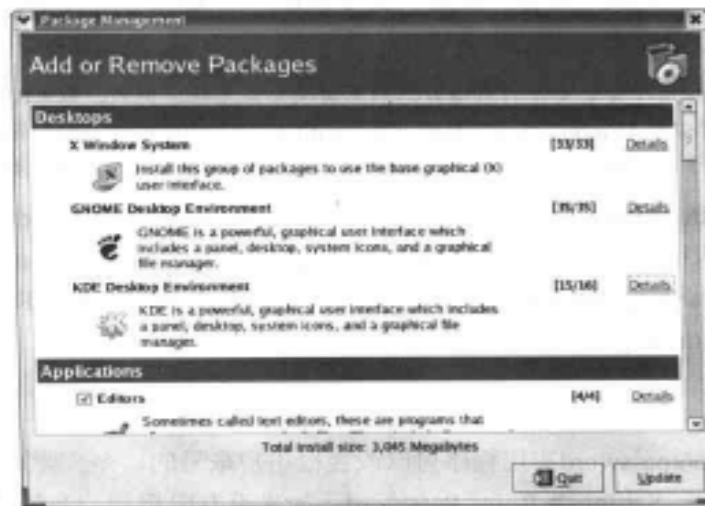


图19.24 包管理窗口

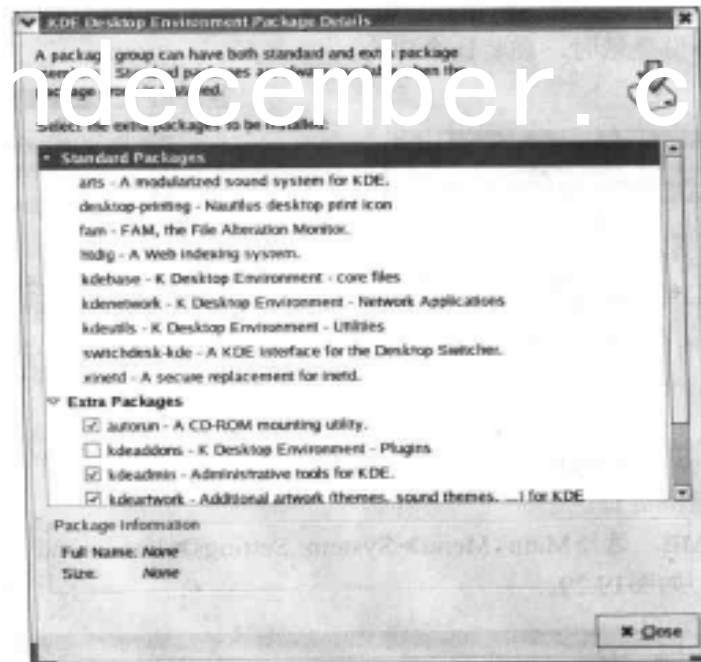


图19.25 KDE桌面环境包细节窗口

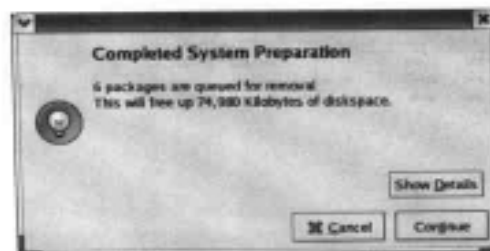


图19.26 删除取消的包之前

增加新包要复杂得多，因为它要求访问安装RPM。如果从命令行启动redhat-config-packages，则这个实用程序会提示插入光碟。

提示：如果具有红帽子安装文件的网络源，则不需要安装光碟。例如，如果RPM包所在的/RedHat/RPMS目录装载到/mnt/source，则可以运行redhat-config-packages --tree=/mnt/source命令。只要通过网络访问RPM，就可以启动redhat-config-packages和用这个源安装指定的包。

另一种启动redhat-config-packages的方法是使用redhat-cdinstall-helper --tree=/mnt/cdrom命令。程序提示插入红帽子第一张安装光碟之后，才能进入redhat-config-packages实用程序。

Linux每周在/var/log/rpmpkgs中登记所安装RPM包的更新表。安装Red Hat Linux时的原表存放在/root/install.log中。

根口令

redhat-config-rootpassword实用程序可以改变根用户账号的口令。要启动GNOME，选择Main Menu>System Settings>Root Password。如果没有以根用户身份登录，则会提示输入根口令，如图19.27所示。

假设输入了正确口令（或以根用户身份登录），则可以看到根口令对话框，如图19.28。下次要以根用户身份登录时，需要这个口令。

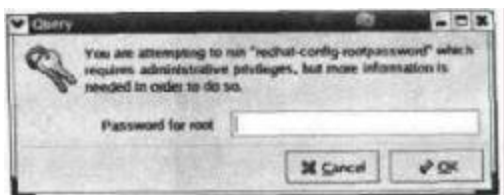


图19.27 要有根口令才能改变口令

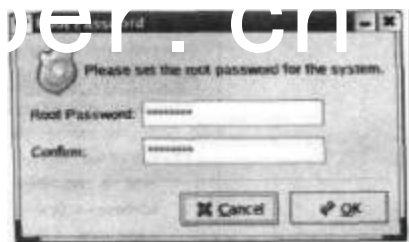


图19.28 根口令对话框

配置用户

可以用redhat-config-users实用程序管理Linux系统中有账号的用户与组。第9章介绍了其影响配置文件的更多信息。

要启动GNOME，选择Main Menu>System Settings>Users and Groups。打开红帽子用户管理器窗口，如图19.29。

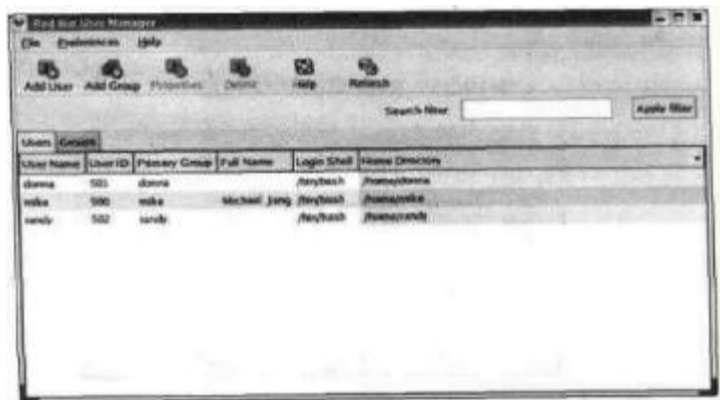


图19.29 红帽子用户管理器窗口

可以看出, 这个窗口有两个标签。Users标签列出系统中的当前用户, 来自/etc/passwd。了解这个文件的读者很容易看出其类别。要增加用户, 单击Add User打开生成新用户对话框, 如图19.30。

生成新用户对话框可以输入新用户信息和口令。通常, 新用户得到一个自动编号的用户ID, 这里是503。如果激活Specify User ID Manually选项, 则可以设置所选用户号。

可以对每个用户增加更多账号信息。加亮显示一个用户并单击Properties, 打开用户属性对话框, 如图19.31。



图19.30 生成新用户对话框

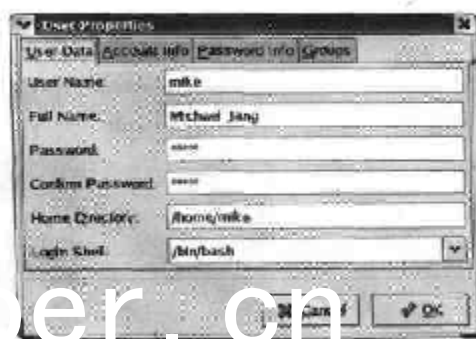


图19.31 用户属性对话框

用户属性对话框有四个标签, 见表19.5。

表19.5 用户属性对话框标签

标签	描述
User Data	列出用户的基本数据, 这个信息存放在/etc/passwd与/etc/shadow中
Account Info	可以锁定和/或设置账号有效日期, 这个信息存放在/etc/shadow中
Password Info	可以设置口令有效期参数, 这个信息存放在/etc/shadow中
Groups	可以设置用户的组成员关系, 这个信息存放在/etc/group中

单击OK按钮回到红帽子用户管理器窗口。然后选择Groups标签, 其中列出了/etc/group中的当前组。单击Add Group打开生成新组的对话框, 如图19.32。默认情况下, 每个用户是自己的组成员, 具有相同ID号。例如, 用户donna的用户ID为501, 组donna的组ID为501。这是第9章介绍的用户专用组模式。

生成特殊组时, 最好指定与用户不同范围的编号。我生成名为angels的组。从Groups标签中选择angels之后, 单击Properties按钮打开组属性对话框。在图19.33所示的Group Users标签中, 可以将所选用户加进这个新组, 这里是nancy与randy。

GUI配置

红帽子图形配置工具是redhat-config-xfree86, 见第15章详细介绍。要启动GNOME, 选择Main Menu>System Settings>Display。打开显示设置窗口, 如图19.34。

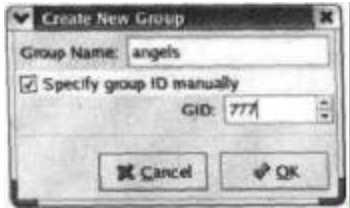


图19.32 生成新组对话框



图19.33 将用户加进组



图19.34 显示设置窗口

大多数情况下，即使Red Hat Linux安装过程中没有安装图形包，也可以从终端窗口运行`redhat-config-xfree86`。进行改变之后，可以在`/etc/X11/XF86Config`中看到结果。如果你用过`redhat-config-xfree86`，则可以在文件顶端看到下列说明：

```
# XFree86 4 configuration created by redhat-config-xfree86
```

如果Red Hat安装过程中只配置了X窗口，则可以看到下列说明：

```
# XFree86 4 configuration created by pyxf86config
```

日志浏览器

红帽子带有标准日志文件的图形化浏览器——`redhat-logviewer`。要启动GNOME，选择Main Menu►System Tools►System Logs。打开系统日志窗口，如图19.35。

注意左边的日志清单和右边的特定日志文件。可以从感叹号（警报图标）和“失败”消息看到，网络时间协议监控程序`ntpd`可能有问题。

可以用这个工具搜索特定消息：输入要搜索的术语，`redhat-logviewer`立即隔离任何带搜索术语的消息。也许你能认识到，这个搜索功能是`grep`命令的功能。

`redhat-logviewer`配置成从标准地址浏览日志文件。如果单击Edit►Preferences打开选项对话框，则可以改变日志相关的文件和指定触发警报图标消息。

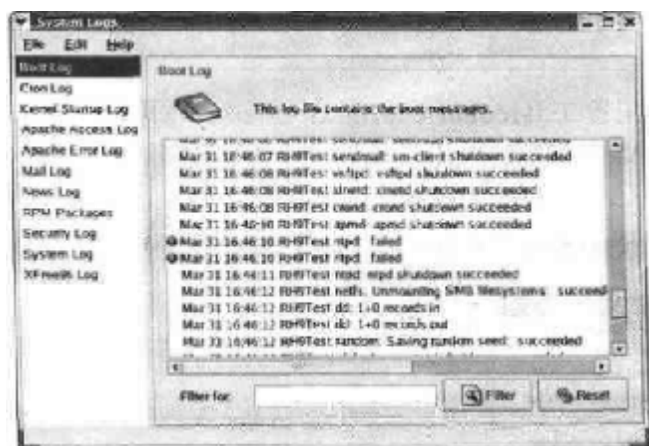


图19.35 系统日志窗口

redhat-logviewer日志文件的标准地址见表19.6。

表19.6 redhat-logviewer日志文件的标准地址

日志名	文件地址
Boot	/var/log/boot.log
Cron	/var/log/cron
Kernel Startup	/var/log/dmesg
Apache Access	/var/log/httpd/access_log
Apache Error	/var/log/httpd/error_log
Mail	/var/log/maillog
News	/var/log/spooler
RPM Packages	/var/log/rpmpkgs
Security	/var/log/secure
System	/var/log/messages
XFree86	/var/log/XFree86.0.log

如果清单中缺少某个日志文件，则可能是前面没有启动这个服务。例如，如果图19.35中看不到Apache的访问日志，则可能计算机还没有启动或访问Apache Web服务器。

字体

有两个实用程序与字体有关：

```
# redhat-update-gnome-font-install
# redhat-update-gnome-font-install2
```

两者都支持GNOME应用程序打印的字体。第一个实用程序生成的字体映射用于打印GNOME应用程序，更新下列字体配置文件：

```
/etc/gnome/fonts/gnome-print-rpm.fontmap
/etc/gnome/libgnomeprint-2.0/fonts/libgnomeprint-rpm.fontmap
```

Kickstart

红帽子Kickstart配置工具redhat-config-kickstart，在第5章已经详细介绍过。要启动GNOME，选择Main Menu►System Tools►Kickstart。打开Kickstart Configurator窗口，如图19.36。

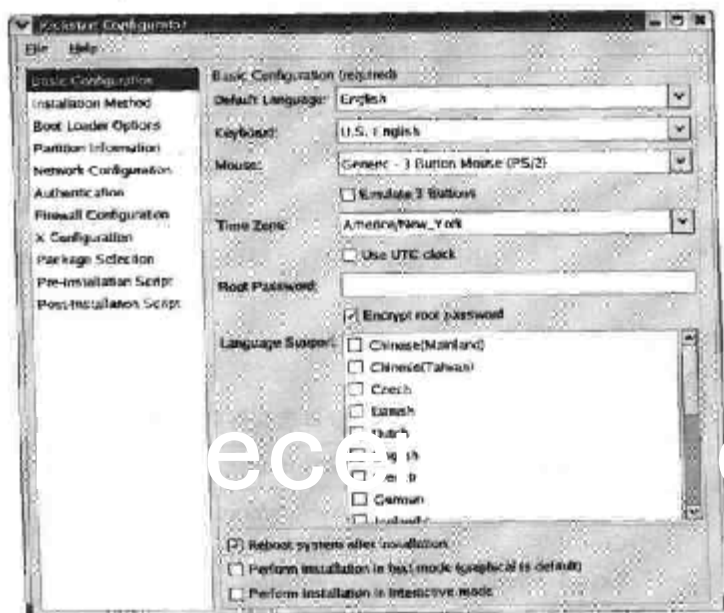


图19.36 Kickstart Configurator

通常，Kickstart文件应保存在ks.cfg中，/root/anaconda-ks.cfg提供了一个模型Kickstart文件，保存了基于本地计算机上如何安装Red Hat Linux的信息。

安全级

红帽子防火墙配置工具是redhat-config-securitylevel，与第3章和第4章安装过程中使用的工具相同。要启动GNOME，选择Main Menu►System Settings►Security Level。打开安全级配置窗口，如图19.37。

总之，可以对计算机配置三级防火墙的保护：高、中、无。

还可以进一步定制防火墙。例如，如果一个网卡只连接本地网络，则可能要使用信任设备，通过信任设备的通信流不能采用防火墙规则。此外，可以将防火墙定制成允许与安全级配置窗口显示的协议相关联的入站数据。

如果使用默认的iptables防火墙命令，则任何改变都将写入/etc/sysconfig/iptables中。关于防火墙和iptables命令的更多信息，见第22章。

redhat-config-securitylevel实用程序与第16章介绍的GNOME iokkit防火墙向导密切相关。两者都可以用相同的基本参数生成基于iptables的防火墙。

调整内核

红帽子内核调整工具redhat-config-proc可以修改/proc目录中的设置。这个目录中的有些文件已经在第11章详细介绍过。到本书编写时，只能从GUI命令行界面启动这个实用程序，而没有GNOME主菜单项目可以启动它。图19.38显示了内核调整窗口。

警告：使用redhat-config-proc时一定要小心。至少要先备份当前的/etc/sysctl.conf文件。任何改变都可能影响内核功能，从而使Linux无法工作。

在图19.38的设置中，可以启用IP转发，使Linux计算机作为两个或多个网络之间的网关。所作改变写入/etc/sysctl.conf文件。



图19.37 防火墙配置工具

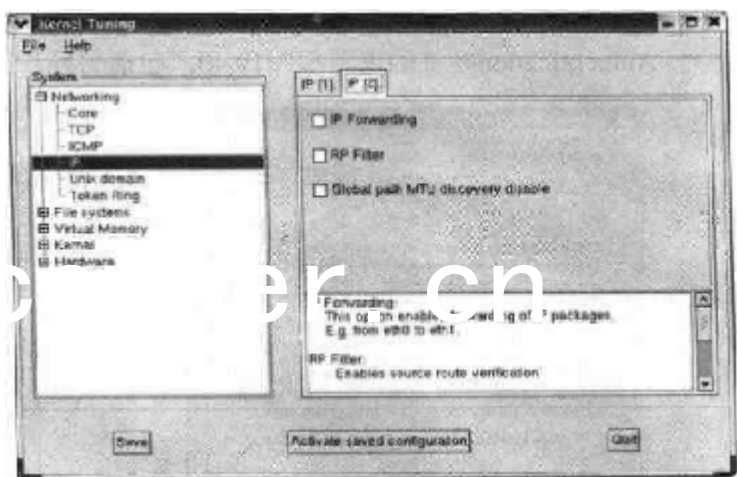


图19.38 调整内核

验证

红帽子设置用户名和口令数据库的工具是authconfig-gtk，实际上与第3章和第4章安装过程中使用的工具相同。要启动GNOME，选择Main Menu►System Settings►Authentication，也可以用gnucash命令从GUI命令行界面启动。打开验证配置窗口，如图19.39。

根据安装类型，可能已经在第3章和第4章安装过程中设置过这些内容。由于你也可能第一次看到这个项目，因此这里详细介绍。首先，表19.7列出了User Information标签的设置。

表19.7 验证配置窗口中的User Information标签

设置	描述
Cache User Information	设置存储用户设置的本地服务器
Enable NIS Support	通过NIS服务器配置验证
Configure NIS	打开一个窗口，可以输入NIS域和服务名
Enable LDAP Support	通过LDAP（轻量级目录辅助协议）配置用户信息访问

(续表)

设置	描述
Configure LDAP	打开一个窗口，可以启动TLS（传输层安全）——SSL（安全套接层）协议的正式名称，以及启用LDAP搜索数据库和服务
Hesiod	配置验证信息和DNS中的其他配置文件，功能与NIS相似
Configure Hesiod	打开一个窗口，可以指定Hesiod LHS和Hesiod RHS，前者是DNS服务器名的前缀，后者是DNS服务器名的后缀。例如，如果DNS服务器地址为nameserv.mommabears.com，则LHS为nameserv RHS为mommabears.com

Authentication标签的设置如图19.40，包括另外几个配置选项，见表19.8。

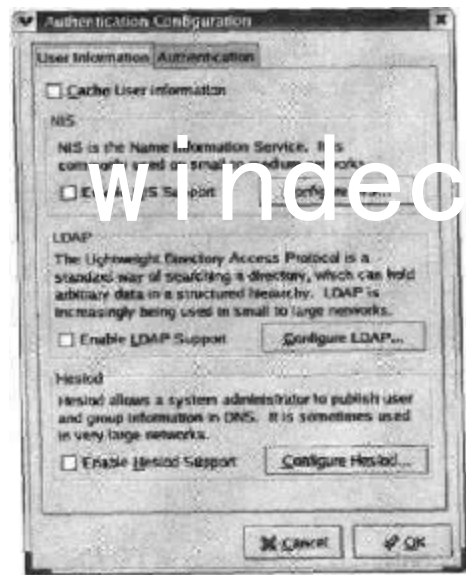


图19.39 设置用户信息数据库



图19.40 配置其他用户名/口令

表19.8 验证配置窗口中的Authentication标签

设置	描述
Enable LDAP Support	通过LDAP（轻量级目录辅助协议）配置用户验证
Configure LDAP	打开一个窗口，可以启动TLS（传输层安全）——SSL（安全套接层）协议的正式名称，以及启动LDAP搜索数据库和服务
Use Shadow Passwords	启用阴影口令组，口令、账号数据和组信息被保护在/etc/shadow与/etc/gshadow中
Use MD5 Passwords	配置MD5形式的口令加密
Enable Kerberos Support	用麻省理工学院开发的这个协议，设置检查用户证件的强加密

(续表)

设置	描述
Configure Kerberos	打开一个窗口，可以设置Kerberos域，通常是域名的大写。Kerberos域控制器（KDC）是Kerberos服务器名，使用TCP/IP端口1188，任何Kerberos管理服务器使用TCP/IP端口749
Enable SMB Support	在Microsoft Windows网络上用Microsoft Windows或Samba服务器设置验证
Configure SMB	打开一个窗口，可以设置Microsoft Windows网络的工作组或域控制器名

任何改变都会写入/etc/sysconfig/authconfig的配置文件中。

提示：如果要配置Kerberos 5，则要将计算机配置为中央NTP服务器，见前面介绍的Kerberos实用程序。

验证配置实用程序也有个文本方式的版本，可以用authconfig命令启动。它有两个文本方式屏幕，可以输入与本节相同的信息。

使用服务配置实用程序

红帽子公司还开发了另外几个图形实用程序，可以完成与各种Linux服务管理有关的日常工作，包括服务运行级管理、打印机和邮件服务器，见表19.9。

表19.9 红帽子服务配置

实用程序	功能
redhat-config-service	可以管理不同运行级中激活的服务
redhat-config-printer	启动打印机配置实用程序，适用于CUPS与LPD监控程序
redhat-config-printer-tui	redhat-config-printer实用程序的文本方式版本
redhat-switch-printer	可以在打印监控程序间切换
redhat-switch-printer-nox	redhat-switch-printer的文本方式版本
redhat-switch-mail	可以在sendmail与Postfix等邮件服务器之间切换
switchdesk	可以切换默认GUI桌面

设置服务级

红帽子服务配置实用程序是redhat-config-service。实际上它是运行第13章介绍的chkconfig命令的一种方式。要启动GNOME，选择Main Menu>System Settings>Server Settings>Services。打开服务配置窗口，如图19.41。

服务配置窗口在/etc/inittab定义的默认运行级中打开。加亮选择服务，可以看到窗口右边显示相关监控程序的描述及其当前状态。

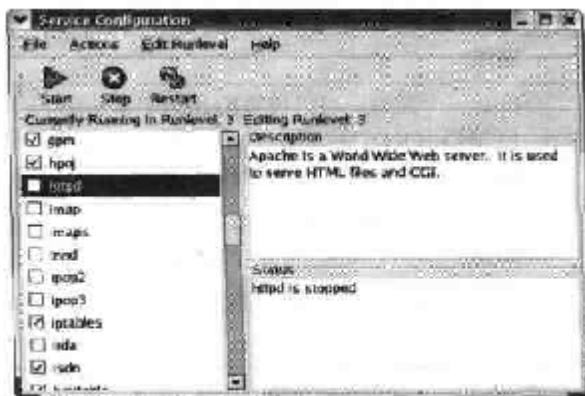


图19.41 设置服务级

在Actions菜单中，可以启动、停止或更新一个服务，对应于下列命令之一：

```
# service servicename stop
# service servicename start
# service servicename restart
```

在Edit Runlevel菜单中，可以将运行级更改为1、4或5。任何改变都将保存到`/etc/rc.d/rcn.d`目录中，其中`n`是运行级。活动监控程序与启动脚本相关联，主导监控程序与删除脚本相关联。下次启动Linux时，它读取每个目录中的启动与删除脚本。关于运行级和每个相关目录中脚本的更多信息，见第13章。

配置打印机

红帽子打印机配置工具是`redhat-config-printer`，它是编辑活动打印监控程序配置文件的前端。第25章将会介绍打印监控程序CUPS或LPD。要启动GNOME，选择Main Menu►System Settings►Printing。打开打印机配置窗口，如图19.42。

也可以用`redhat-config-printer-gui`命令启动这个实用程序。运行`redhat-config-printer-tui`命令可以得到文本方式控制台版本。关于这个实用程序的更多信息，见第25章。

切换打印监控程序

第25章将会介绍，Red Hat Linux 9中有两个主要的打印监控程序CUPS和LPD。红帽子打印机系统的交换器是`redhat-switch-printer`。假设两个系统都已经安装，则可以用其切换活动打印监控程序。要启动GNOME，选择Main Menu►System Settings►More System Settings►Printer System Switcher。打开图19.43所示的切换打印监控程序。

运行`redhat-switch-printer-nox`命令可以得到文本方式控制台版本。相应运行级改成要的打印监控程序。

切换邮件主体

第26章将会介绍，Red Hat Linux 9提供了几个邮件服务器监控程序。红帽子邮件系统交换器是`redhat-switch-mail`。假设安装了多个邮件系统，则可以用它切换活动邮件服务监

控程序。到本书编写时,只能从GUI命令行界面启动这个实用程序,没有相应的GNOME主菜单项目。图19.44显示了得到的redhat-switch-mail窗口。相应运行级改成所要的邮件监控程序。

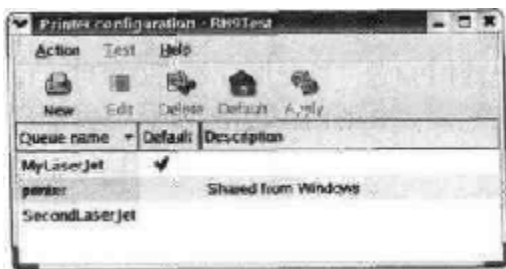


图19.42 打印机配置窗口

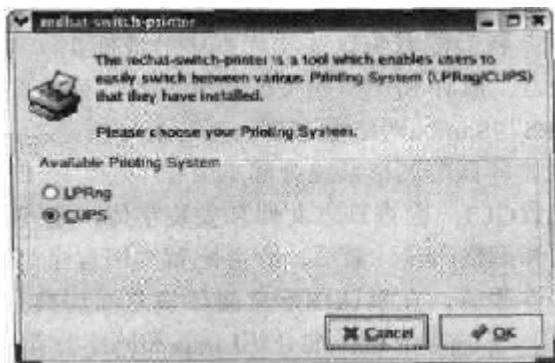


图19.43 切换打印监控程序

切换桌面

第15章曾介绍过,Red Hat Linux 9有四个GUI桌面,包括GNOME、KDE与twm(在窗口中显示为TWI D)。红帽子桌面交换器为switch desk。假设安装了多个GUI桌面,则可以用其切换默认的GUI。要启动GNOME,选择Main Menu>System Settings>More System Settings>Desktop Switching Tool。打开桌面交换器窗口,如图19.45。每个用户的默认桌面在主目录中的/.Xclients-default文件中列出。

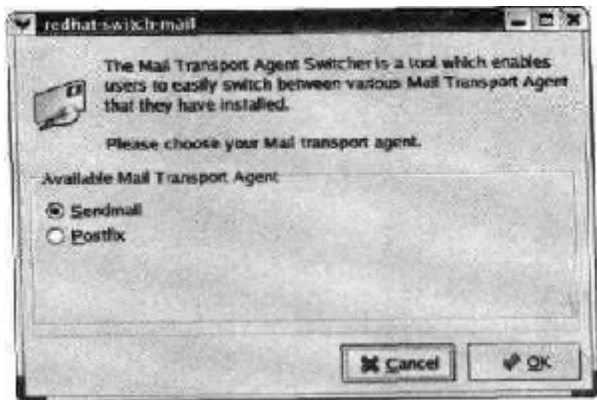


图19.44 切换邮件主体



图19.45 切换默认GUI桌面

小结

本章介绍了红帽子公司生成的图形实用程序,它们可以帮助管理Linux桌面。大多数所要的命令以redhat-config-开头。

记住,图形实用程序只是前端,换句话说,它们可以帮你改变各个配置文件,但不能

完成文本编辑器中的所有改变。这些实用程序还很新，因此一定要检查相关配置文件中的结果。

但是，图形实用程序是新的Linux管理员很好的学习工具。管理员可以在图形实用程序中进行改变，然后检查相关配置文件中的结果。

我们随意将这些实用程序分成四类。基本配置实用程序可以配置与系统时钟、键盘、语言、鼠标和声卡相关的基本设置。网络配置实用程序可以设置新网卡和Apache、DNS、NFS与Samba网络服务器。

不同的图形系统管理实用程序还可以安装和删除RPM包、管理根口令、设置用户与组、配置GUI、检查日志文件和安装字体，还可以配置自动安装的Kickstart文件、设置定制防火墙和调整内核。最后，服务配置实用程序可以在不同运行级管理服务，改变默认的打印机和邮件服务，在默认图形桌面环境之间切换。

下一章开始详细介绍Linux和网络。第20章介绍TCP/IP协议栈与IP地址理论，还介绍局域网网件配置专用IP地址的工具。后面几章介绍局域网件管理Linux、保护Linux网络，等等。

第五部分 Linux联网基础

第20章 TCP/IP基础

许多开发UNIX操作系统的人也参与了网络开发，因此使得这个网络最终成为了Internet。他们设计TCP/IP作为标准网络协议组。由于Linux是UNIX的克隆，因此它也是针对TCP/IP定制的。但是，TCP/IP只是现代网络的几个协议栈之一。

TCP/IP名称表示它的两个组成协议：TCP（传输控制协议）和IP（Internet协议）。TCP/IP实际上包括几百个协议，称为TCP/IP协议套件。

详细介绍TCP/IP之前，先要介绍计算机网络的一些基本知识，包括大网和小网。我们需要标识网络上每一台计算机，需要有传输数据的标准方法。还有其他几个协议栈，本章将介绍其中两个：NetBEUI与IPX/SPX。

NetBEUI是NetBIOS改进主用户接口，是Microsoft与IBM公司开发的。IPX/SPX名称也表示它的两个组件协议：IPX（网间网分组交换）和SPX（顺序分组交换）。和TCP/IP一样，IPX/SPX也包括大量协议。

为了帮助软件设计人员开发不同协议，需要指定标准的通信层，这是通过ISO（国际标准化组织）的OSI网络模型实现的，OSI指开放标准互联模型。

尽管TCP/IP常常使用OSI网络模型，但许多设计人员常常采用与之相似的四层协议栈概念。否则许多TCP/IP服务要求几个不同OSI层的软件。

如果你对这些理论不感兴趣，则可以直接跳到TCP/IP的功能，从IP地址开始。IP地址有两个版本，IPv4地址至今还在美国广泛使用，但新的IPv6已经在世界其他地方普及。本章介绍下列主题：

- 搜索网络基础
- 了解协议栈
- 学习TCP/IP基础
- 使用IP地址

搜索网络基础

网络是指包括两个或多个相互通信的计算机系统。从某种程度说，所用的“媒介”并不重要。可以用并行电缆、电话MODEM、以太网网卡、无线适配器或任何媒介联网，只要

能让计算机交换信息即可。如果能直接或通过集线器连接这些计算机，则可以建立一个局域网（LAN）。每个局域网通常有个特殊的IP地址，称为网址。

局域网连接距离很近的计算机，如同一幢大楼或同一办公室中的计算机。互连网络包括两个或多个局域网。有些互连网络是广域网（WAN）。广域网包括两个或多个位于不同地点的网络。最大的广域网是Internet。

说明：任何由同一小组管理的网络或网络组称为一个域（domain）。例如，可以将两个不同网络——linux.sybex.com与windows.sybex.com配置成属于sybex.com域。

局域网与广域网

Linux局域网通常用IEEE 802.3标准配置，也称为以太网。这种网络比电话MODEM快得多。标准以太网可以使计算机的通信速度高达10或100Mb/s（Ethernet与Fast Ethernet），而许多地方已经采用了Gigabit Ethernet（1000Mb/s）和正在开发更快的网络（10Gb/s Ethernet）。

说明：以太网是个商标名，这个网络的正确名称来自电子与电器工程师学会实现的标准IEEE 802.3。Fast Ethernet和Gigabit Ethernet也有类似名称：IEEE 802.3u与IEEE 802.3ae。

但以太网上两台计算机之间的距离只限于几百米，这取决于连接类型。实际上，尽管局域网覆盖的范围有限，但局域网的速度非常快。相反，广域网中的局域网间连接可以跨几千里，但连接速度通常有限。即使高速广域网连接通常也只限于1.4Mb/s以下。

说明：广域网连接速度的限制取决于成本。Internet广域网主干可以传递几十个Gb的数据，但成本很高，因此要由广域网的客户分享这个“带宽”。

Internet

即使你从来没有建立网络，但也可能从Internet经历中对网络有所了解。连接Internet时，大多数用户和许多Linux管理员都是通过Internet服务提供者（ISP）子网的。如果你负责一个大的网络，则可能直接连接Internet，因此自己就是个ISP。

我们通过ISP的网关连接Internet，这台计算机连接ISP和整个Internet。搜索www.mommabears.com之类的域名时，计算机要寻找相应的计算机地址。在Internet中，这个地址称为IP地址，通常存放在域名服务（DNS）服务器中。

域

安装Red Hat Linux时，要输入主机名（如computer1）或完全限定域名（FQDN，如www.mommabears.com）。除非计算机提供信息或直接连接Internet，否则使用的名称并不重要。如果使用完全限定域名，则要保证在网络的每台计算机上安装Linux时使用相同域名。

有些ISP也可能对你的Internet连接指定特定完全限定域名。这是电缆MODEM和DSL（数字用户线）适配器之类高速连接中常见的做法。

可以把域分解为几个子域。每个子域可以表示不同局域网。例如，linux.mommabears.com、windows.mommabears.com与other.mommabears.com可以表示三个不同的局域网。

主机名

除了网络上的完全限定域名之外，还可以使用主机名（如computer1）。计算机的完全

限定域名把主机名和域名组合在一起。例如，如果计算机的主机名为berkeley，域名为california.now，则完全限定域名为berkeley.california.now。每个主机名或完全限定域名与一个数字地址相关联，如IP地址。

硬件地址

计算机通过网卡上的硬件地址相互联系。硬件地址形如00-60-08-8D-41-93，是十六进制数。每个网卡配置唯一的十六进制硬件地址。配置TCP/IP网络时，将一个硬件地址与一个IP地址相联系。

说明：十六进制数用16个数表示：0，1，2，3，4，5，6，7，8，9，a，b，c，d，e与f。

了解协议栈

可以看出，网络上的计算机要有不同要素才能相互通信。它们需要域名、数字地址和硬件地址，还要有连接管理器和与邮件、Web页面、文件服务器等相关的应用程序协议。这些元素可以通过协议栈进行分类。

协议栈实际上就是分配劳动。有些协议与邮件和DNS等应用有关。有些指定域名、IP地址和硬件地址。有些加密数据。管理二进制数据流和或控制远程登录会话。

这种分配劳动的方法有两大类，一种是OSI网络模型，另一种是基于TCP/IP的网络模型，前者将在本节介绍，后者放在本章稍后介绍。本节还将介绍另外几个协议栈，如NetBEUI与IPX/SPX。

提示：支持OSI还是TCP/IP的争论和支持Linux还是Microsoft Windows的争论一样激烈。尽管纯粹主义者反对用OSI描述TCP/IP协议，但这个方法对学习很有帮助。

OSI层

OSI网络模型共七层。计算机在网络上发送消息之前，要通过这些层将消息变成1和0，然后才能在网络上发送。每一层相关的程序完成不同功能，如加密、校错和路由。

下面简要介绍图20.1所示OSI网络模型的每一层，特别注意每层的编号。

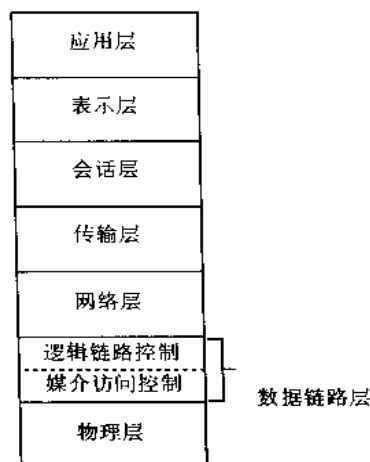


图20.1 OSI网络模型

应用层 应用层（7）协议从所用程序开始转换过程。例如，HTTP是个应用层协议，从Mozilla之类Web浏览器转换数据。网关计算机可以在网络之间转换应用。

表示层 表示层（6）协议将数字和字母变成低级计算机代码。一个例子是ASCII码，它表示英语键盘上的数字和字母。表示层还有加密协议，如安全套接层（SSL）。

会话层 会话层（5）协议管理网络上所花的时间。这些协议定义任何特定时间由哪台计算机发送和接收消息。例如，网卡的会话层软件确定数据是单向移动（半双工）还是同时双向移动（全双工）。

传输层 传输层（4）协议可以重发消息，直到得到返回收据（即确认），也可以按最佳路径向目标计算机发消息。两个主要TCP/IP传输层协议是TCP和UDP。传输层协议还开始将消息分解为数据包。TCP在数据包开头增加确认请求，而UDP则不然。

数据包生命期

除非消息很小，否则计算机网络并不同时发送整个消息。从传输层开始，网络将消息分解为数据包。在OSI的下层，数据包可能进一步分解为更小的数据包或单元。有些协议可能通过Internet上的不同路由发送各个数据包或单元，每个数据包包括地址信息，保证消息在正确的目标计算机上按顺序重新汇合起来。

例如，以太网数据包在数据链路层发送，它只包含最多1513字节，包括1500字节数据和18字节（以上）的地址信息，保证数据包到达网络上正确的目标计算机。

网络设计的细节非常丰富网络设计的标准参考资料是“Computer Networks”一书，它的作者Andrew Tanenbaum，由Prentice Hall 2002年出版。

网络层 网络层（3）协议实际将数据从一台计算机移到另一台计算机，从一个网络移到另一个网络。IP协议是个网络层协议。消息要靠IP地址才能在网络间移动。路由器在网络层管理网络通信流。

数据链路层 数据链路层（2）协议主要用于保证消息到达正确的目标计算机，数据链路层通常分为两个子层：逻辑链路控制（LLC）和媒介访问控制（MAC）。LLC协议保证消息正确无误地按顺序到达目标计算机，称为帧同步和错误校验。MAC协议帮助计算机相互通信。因此网卡的硬件地址也称为MAC地址。交换机和网桥可以在这一层管理网络通信流。

物理层 物理层（1）协议将数据转换成0和1以便在计算机间通信，并控制网络的物理方面，如电缆与接头。

说明：购买网络硬件时，记住销售工程师通常按层指定组件。例如，标准交换机在第二层工作，而基本路由器在第三层工作。但是，这个边界并不严格。例如，有些交换机包括路由或传输功能，因此称为第三层或第四层交换机。

NetBEUI

NetBEUI是NetBIOS扩展主用户接口，是Microsoft与IBM公司合作开发的。NetBEUI基于NetBIOS（网络基本输入/输出系统）。NetBIOS中有一系列命令，使计算机可以发送和接收数据以及网络上其他计算机共享目录中的信息。

NetBEUI与NetBIOS的主要缺点是不可路由。换句话说，不能将NetBEUI网络与Internet之类的另一个网络连接。NetBEUI网络只限于255台计算机。

但是，Microsoft公司已经让NetBIOS命令适应TCP/IP与IPX/SPX之类的可路由网络协议栈。如果你是个网络管理员，且你的网络中包括Microsoft计算机，则有必要知道几个基本NetBIOS命令，如net view与net use。

使用Samba时，可以利用与NetBIOS命令相关的服务器消息块（SMB）格式。第29章将介绍Linux系统可用的命令。由于Samba实际上是NetBIOS的Linux/UNIX版本，因此如果你发现Samba命令直接对应于net view与net use之类的NetBIOS命令，不必感到惊讶。

IPX/SPX

和TCP/IP一样，IPX/SPX也包括大量协议。IPX/SPX是Novell公司开发的，它支持NetWare程序这样的网络操作系统。

许多旧网络仍然使用NetWare。但NetWare也支持TCP/IP，因此即使连接NetWare网络，也不一定需要采用IPX/SPX。

IPX/SPX是可路由的，旧版Microsoft Windows中，如果要在多个网络上配置计算机，IPX/SPX是惟一选择。

如要建立连接IPX/SPX网络，则需要安装netware-*, ipx utils-*与netpfs-*.LPM包。第一个包使Linux计算机可以作为NetWare网络上的文件与打印服务器。第二个包支持IPX/SPX，最后一个包中的命令可以使计算机在NetWare网络上作为客户机。

说明：还有许多协议套件，如IBM公司的系统网络体系结构（SNA）、施乐网络系统（XNS）、DEC网络（DECnet）。DEC现在已经被惠普公司并购。

学习TCP/IP基础

TCP/IP是当今主流的网络协议套件。即使Novell公司也已经在NetWare服务器中使用多年，Microsoft公司也使用TCP/IP，虽然其开发了NetBIOS套件。TCP/IP是Internet上的通用语言，因此通常只要知道这个协议套件就够了。

TCP/IP模型

TCP/IP网络模型分为四层，与OSI模型大致对应，如图20.2所示。TCP/IP应用层的功能相当于OSI模型前三层。TCP/IP链路层相当于OSI模型后两层。

自然，TCP/IP层更适合不同的TCP/IP协议。例如，第27章介绍的FTP安全版本：它管理客户机与服务器之间的通信，是个OSI会话层功能；它将数据转换成ASCII或二进制代码，是个OSI表示层功能；它还转换FTP命令，这又是个OSI应用层功能。

主要协议

TCP/IP协议有几百个，我们已经见过许多，如FTP、HTTP、SMTP、SNMP、TCP、IP。下面几节详细介绍其中几个协议。

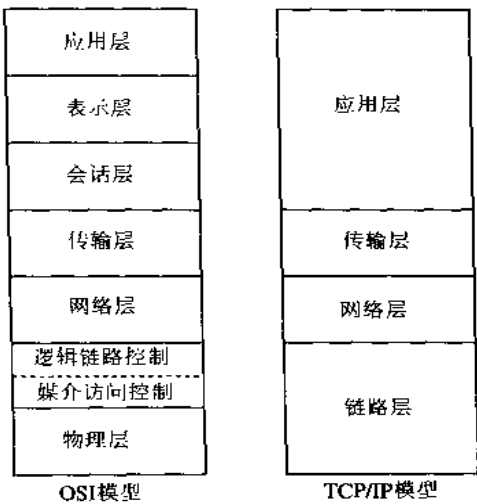


图20.2 TCP/IP网络模型

TCP/IP应用层协议

TCP/IP应用层协议为系统管理员提供/etc/services。从图20.3可以看出，这个文件包括服务名（如ftp、ssh与smtp）、相关端口号和相关说明。

```
# 21 is registered to ftp, but also used by fsp
ftp      21/tcp
ftp      21/udp      fsp fspd
ssh      22/tcp
ssh      22/udp      # SSH Remote Login Protocol
telnet   23/tcp
telnet   23/udp
# 24 - private mail system
smtp     25/tcp      mail
smtp     25/udp      mail
time     37/tcp      timeserver
time     37/udp      timeserver
rlp      39/tcp      resource
rlp      39/udp      resource      # resource location
nameserver 42/tcp      name
nameserver 42/udp      name      # IEN 110
nicname  43/tcp      whois
nicname  43/udp      whois
tscacs   49/tcp
tscacs   49/udp      # Login Host Protocol (TACACS)
re-mail-ck 50/tcp      # Remote Mail Checking Protocol
re-mail-ck 50/udp      # Remote Mail Checking Protocol
domain   53/tcp      # name-domain server
```

图20.3 /etc/services

TCP/IP有65 536个可用端口，每个端口就像个电视频道。将Linux计算机指向正确的端口时，可以收到与这个端口相关的数据。著名端口由Internet号码指定机构（www.iana.org）指定。典型端口80用于HTTP（Web页面）、21用于FTP通信、110用于POP3 E-mail通信。表20.1列出了几个重要TCP/IP应用层协议及其端口。

表20.1 TCP/IP应用层协议

协议	端口	描述
FTP	21	文件传输协议，对文件收发进行优化
SSH	22	安全Shell，加密计算机之间的通信
Telnet	23	以明文形式连接远程计算机
SMTP	25	发送邮件的简单邮件传输协议
HTTP	80	Web页面的超文本传输协议
POP3	110	接收邮件的邮局协议
SNMP	161	诊断网络的简单网络管理协议
HTTPS	443	安全HTTP
IPP	631	Internet打印协议，与公共UNIX打印系统（CUPS）相关
SWAT	901	Samba web管理工具
NFS	2049	Linux/UNIX计算机之间通信的网络文件服务协议

TCP/IP传输层协议

两个最重要的传输层协议是TCP与UDP，两者都取完全限定域名（如www.sybex.com）并将消息发送到这些计算机。TCP也称为传输控制协议，它一直发送消息，直到从目标计算机收到确认。TCP是面向连接的协议。

相反，UDP也称为用户数据报协议，它发送所用的网络很可靠，不会丢失数据或丢失的数据不重要，不需要确认。UDP是无连接的协议。

TCP/IP网络层协议

关键网络层协议是IP（Internet协议），它通常与192.168.32.142之类的IP地址相关关联。本章末尾将详细介绍IPv4和IPv6地址。

还有另一个重要的TCP/IP网络层协议，就是Internet控制消息协议（ICMP），它与ping实用程序密切相关，可以检查计算机与网络中每个组件之间的连接。第21章将介绍ping实用程序和其他相关的实用程序。

说明：TCP/IP网络层也称为Internet层。

TCP/IP链路层协议

TCP/IP链路层协议和网络技术密切相关，如以太网、令牌环以及ATM。在这里要组织网络分组。一旦组织网络分组之后，它们组成位流（0和1），然后通过网络电缆或其他传输媒介发送这些位流。

当前网络的重点是以太网，但你也可能遇到另外一些重要的网络技术。下面简要介绍几种重要网络技术：

Ethernet 普通以太网遵循IEEE 802.3标准，数据传输的理论最高速度为10Mb/s。由于以太网数据包在忙网络中要等待以避免冲突，因此实际速度通常不到理论最高速度的一半。

Fast Ethernet 快速以太网遵循IEEE 802.3u标准，数据传输的理论最高速度为100Mb/s。要求用五类线以上的电缆。

Gigabit Ethernet 千兆位以太网遵循IEEE 802.3ae标准，数据传输的理论最高速度为1000Mb/s。要求用光纤之类的传输媒介。

Token Ring (令牌环) 令牌环遵循IEEE 802.5标准，数据传输的理论最高速度为16Mb/s。由于只有取得令牌的计算机才能传输数据，因此比以太网更高效，至少相对于最高速度而言是这样。

Asynchronous Transfer Mode (ATM, 异步传输方式) ATM网络是高速网络的常用技术，传输速率在155Mb/s与622Mb/s左右。尽管ATM支持还是试验性的，但Linux Hardware-HOWTO中已经列出了ATM网卡。开发人员正在研究传输速率达2Gb/s以上的ATM网络。

Point-to-Point Protocol (PPP, 点对点协议) 介绍网络协议时，少不了要介绍为普通电话MODEM服务的协议。尽管PPP速度只限于56kb/s（在美国为53kb/s），但它曾经是我们的好伙伴。如果你使用高速Internet访问，请记住，到本书编写时，美国还有20%的Internet用户使用电缆MODEM和DSL适配器之类的“高速”服务。

说明：TCP/IP链路层也称为网络访问层。

重要服务定义

本节介绍几个重要TCP/IP网络服务。如果你对不熟悉TCP/IP，则可以阅读这个清单了解其提供的服务。尽管后面几章会详细介绍这些服务的配置，但最好先对下列服务有个基本了解：

域名系统 (DNS, Domain Name System) 域名系统是个数据库，包括完全限定域名（如linux1.mommabears.com）如IP地址（如192.168.1.231）。连接Internet和搜索www.redhat.com之类站点时，Linux计算机要查找DNS服务器。一旦找到IP地址之后，就把这个信息加进请求中。然后可以在网络之间发送消息，直到该信息到达红帽子公司Web站点。

动态主机配置协议 (DHCP, Dynamic Host Configuration Protocol) 可以对网络上每台计算机指定IP地址，但要小心，如果对两台计算机指定相同的IP地址，则网络会失败。动态主机配置协议将这个过程自动化。

地址解析协议 (ARP, Address Resolution Protocol) 地址解析协议将IP地址与计算机网卡的硬件地址相联系，这些硬件地址也称为MAC地址。网络上的计算机通过硬件地址相互通信。如果IP地址分配给错误的MAC地址，则网络会遇到故障。

使用IP地址

TCP/IP网络上每台计算机都有IP地址之后才能相互通信。你或者你的ISP可以指定永久IP地址，也可以从DHCP服务器“租借”IP地址。连接Internet时，ISP对你的计算机指定唯一的IP地址。

要设置网络的IP地址，需要有网络地址和网络掩码。网络地址和网络掩码相同的IP地址在同一局域网上。网络地址分成五大类，网络掩码定义特定网络地址，可以分配的IP地址范围。

每个连接其他网络的网络都要为这个连接提供一个网关IP地址。在Linux中, 可以用/etc/hosts.allow和/etc/hosts.deny文件或相应的iptables与ipchains防火墙命令限制网络访问。

IPv4

20世纪70年代以来使用的IP地址标准是IPv4, 它使用32位地址。这32位共构成40亿个地址 ($2^{32}=4\,294\,967\,296$), 这在Internet初创阶段是相当够用的。但是, 如今这个地址已经不够了。尽管目前Internet已经在向IPv6过渡, 但过渡完成后, 仍然会使用IPv4地址。

事实上, 对许多专用局域网, IPv4地址更容易理解和配置。我相信, IPv4地址将在多年内继续广泛使用。下一章要介绍如何用IPv4地址方便快捷地配置专用IP网络。

可以用两种方法指定IPv4地址: 二进制方法和点号十进制格式。下面是二进制方法指定的典型IPv4专用网址:

```
11000000 10101000 00000001 00100000
```

复杂吗? 这是计算机读取数据的方式, 而人们更习惯于十进制格式。很容易将这些位转换成十进制格式: 上述IPv4地址的点号十进制格式为192.168.1.32。但并不是任何人都能熟练进行这种转换。下面花点时间介绍如何将这些转换成十进制格式。

IPv4地址的位

位是二进制数位。二进制数只有两个数字0和1, 很容易在计算机中表示。只要一个开关、电脉冲或光脉冲即可。开关关时为0, 开时为1。

习惯上, 8位构成一个字节。在ASCII系统中, 英语键盘上每个字母和数字与一个字节相对应。因此32位IPv4地址组成四个8位组, 下列地址中有4个字节:

```
11000000 10101000 00000001 00100000
```

下面把每个字节的位进行分解。一个字节中第一个数00000001等于十进制记数的1, 而00000010=2, 00000011=3, 等等。表20.2列出了几个例子。

下面看看上述地址的第一个字节11000000, 由于10000000=128而01000000=64, $128+64=192$, 因此得到这个IP地址的第一个数为192。下一个数10101000, 为 $128+32+8=168$, 同样, 00000001=1, 00010000=32。因此, 可以得到点号十进制格式的IPv4地址192.168.1.32。

极限情况下, 二进制数11111111为255。

表20.2 字节与普通数

字节	普通数
00000000	0
00000001	1
00000010	2
00000100	4
00001000	8
00010000	16
00100000	32
01000000	64
10000000	128

地址类

IPv4地址范围为0.0.0.0到255.255.255.255，可以分为五大类地址——A到E。可以从A、B、C类分配IP地址。表20.3列出了五类地址的地址范围。

表20.3 IPv4地址类

类	范围	说明
A	1.0.0.0 to 127.255.255.255	最多允许网络中有1600万台计算机
B	128.0.0.0 to 191.255.255.255	最多允许网络中有65 000万台计算机
C	192.0.0.0 to 223.255.255.255	最多允许网络中有254万台计算机
D	224.0.0.0 to 239.255.255.255	用于多目广播
E	240.0.0.0 to 255.255.255.255	用于试验

注意，即使在A、B、C类网络中，也不是每个地址都可以使用。有四类地址不能指定给直接连接Internet的计算机：

- 任何IPv4地址网络中第一个地址保留作网络地址。
- 任何IPv4地址网络中最后一个地址保留作广播地址。
- 地址1.7.0.0是可路由地址。
- 有一组IPv4地址是专用地址，用于通过防火墙连接Internet的专用局域网。

下一章详细介绍每种地址，还要介绍网络地址与广播地址以及网络或子网掩码。这些概念将在连接Internet的专用IP网络情境中介绍。

IPv6

听起来似乎很奇怪，IPv4地址多达40亿个，怎么还不够？但实际上所有IPv4地址组都已经分配出去。尽管你也许能从ISP那里取得自己的IPv4地址（通常要加钱），但人们正在将Internet转向IPv6。

IPv6地址有128位，包括340 000 000 000 000 000 000 000 000 000 000 000个地址。为了便于过渡，每个IPv4地址指定一个特定的IPv6地址。这样至少还留下 3.4×10^{38} 个地址。而你的IPv4地址还可以在IPv6中使用。

IPv6地址的配置使IPv4地址很容易转换。例如，下列IPv4地址：

```
192.168.1.32
```

实际上与下列IPv6地址一致：

```
::192.168.1.32
```

但是，IPv6地址采用十六进制记数法，使用16个数0，1，2，3，4，5，6，7，8，9，a，b，c，d，e与f表示。下面是个IPv6地址例子：

```
4aed:0a21:3c53:7dab:0000:0000:0000:0451
```

IPv4地址很容易转换成十六进制记数法。例如，将上述IPv4地址转换成二进制格式：

```
11000000 10101000 00000001 00100000
```

由于 $2^4=16$ ，即可以把4个位表示为一个十六进制数。因此，可以将IPv4地址组成4位（半字节）：

```
1100 0000 1010 1000 0000 0001 0010 0000
```

然后将其转换成十进制记数法：

```
12 0 10 8 0 1 2 0
```

等价于下列十六进制记数法：

```
c0a8:0120
```

对应的IPv6地址为：

```
0000:0000:0000:0000:0000:0000:c0a8:0120
```

小结

UNIX与最终成为Internet的网络是并行开发的。TCP/IP已经成为Internet的通用语言。Linux是UNIX的克隆，因此很适合在Internet上通信。

一个网络由两台以上计算机相互通信。局域网连接距离很近的计算机，而广域网则连接远隔万里的局域网。最大的广域网是Internet。由于成本较低，因此局域网通常比广域网更快。无论如何，都要配置完全限定域名、主机名、IP地址和硬件地址才能在网络上通信。

TCP/IP之类网络语言也称为协议栈。NetBEUI与IPX/SPX之类主要协议栈包括几十种不同协议。协议通常分为OSI七层网络模型中某一层的协议。

由于TCP/IP是Internet语言，所以它是主要的网络协议套件。TCP/IP网络模型包括四层，能够更好地描述不同TCP/IP协议与服务的功能，如FTP、HTTP、SNMP、TCP、UDP、IP、Ethernet与ATM。其他关键TCP/IP网络服务包括DNS、DHCP与ARP。

每个在TCP/IP网络上通信的计算机都需要一个IP地址。标准IP地址系统为IPv4。IPv4将地址分为五类。由于IPv4地址已经不够，因此Internet最终要过渡到IPv6。但是，IPv4地址仍然非常普及，而且每个IPv4地址都有一个对应的IPv6地址。

下一章要利用这些TCP/IP协议和IP地址配置计算机和网络，还要介绍如何将Linux局域网连接到Internet上。

第21章 在局域网中管理Linux

学习了第20章介绍的网络理论之后，现在就可以把这些应用到Linux计算机与网络实践中。

首先要了解一些基本网络硬件。集线器连接局域网中的不同计算机；交换机将局域网分段，帮助控制网络中的通信流；路由器连接不同网络，并根据需要引导通信流。

然后在Linux计算机上，要配置网卡并保证其连接正确的网卡地址，为此要使用ifconfig和arp命令。可以用不同命令在普通网络和网络信息系统（NIS）网络中配置计算机的主机名。如果已经正确安装Red Hat Linux，则可以在/etc/hosts、/etc/host.conf、/etc/sysconfig/network与/etc/resolv.conf之类的文件中看到正确的网络设置。

我们接着要介绍使用IPv4专用地址的局域网。IPv4地址至今仍然广泛使用的原因之一是很容易配置局域网。有了正确的路由配置和一个公用IPv4地址，就可以将这个局域网连接到Internet。

Red Hat Linux中的一些工具可以使你的计算机连接到Internet。尽管有些是图形工具，但有些只能在命令行界面中使用。这些工具在红帽子自己的/etc.net配置向导和m nicom中。

最后，如果网络遇到故障，则可以用几个命令查错产生的问题。netstat命令可以测量通过不同TCP/IP端口的通信流，ping命令可以检查连接，最后，traceroute命令可以直观地显示消息经过不同网络（特别是Internet）时的路由。本章介绍下列主题：

- 了解网络硬件
- 在局域网上配置计算机
- 配置公网与专网
- 建立Internet连接
- 网络查错

了解网络硬件

在介绍网络中如何配置Linux之前，首先要考虑网络的物理布局。尽管本书是关于Linux的，但大多数网络故障都是物理故障。最常见的网络故障是连线松掉、电缆没接上、集线器或路由器尘埃太多，等等。根据第20章介绍的OSI网络模型，要考虑局域网上的五类硬件：

- 物理层传输媒介
- 物理层集线器
- 数据链路层交换机
- 网络层路由器
- 应用层网关

传输媒介

计算机在传输媒介中用1和0发送数据。数据可能是铜线上的电脉冲、光纤上的光脉冲

或空气中的无线电波。传输媒介处于OSI模型的物理层。

无论用什么方法传输信号，都有一定的范围限制。例如，如果两台计算机和集线器之间的双绞线长度超过指定的最大电缆长度——328英尺（100米），则以太网网络无法有效工作。简单地说，下面是铜线和光纤之类物理媒介要注意的几个问题：

连接 要检查连接，许多网络故障都是因为电缆没有正确插入。

长度 网络有一定范围。标准“五类线”网络电缆使得快速以太网网络在超过100米的电缆长度上不能达到最高功能。

安装 电缆不要弯曲得太厉害。弯曲得太厉害可能使部分电缆拉伸，从而降低其传递数据的能力。

集线器

集线器是大多数现代局域网的中心。连接的集线器实际上是带套接的框。正确连线之后，可以将计算机与每个套接连接。多台计算机连接集成器时，其配置就像轮子中央向外的辐线，称为星形配置（我不太明白为什么不把集线器叫做辐线配置）。

随着距离增加，数字信号会衰减。集线器可以重建数字信号，将其按原有强度传输。由于集线器只处理计算机通信中的0和1，因此它也是在OSI模型的物理层工作。

交换机

交换机常用于将大局域网分解为两个或多个不同的逻辑网段。交换机保存局域网中硬件地址的数据库，换句话说，它在OSI模型的第二层工作。

两台计算机之间首次建立连接之后，它们用硬件地址继续通信。由于交换机知道局域网上的硬件地址，因此可以重传每个消息（像集线器），将其定向到目标计算机。

说明：旧式交换机有时也称为网桥，两者都在OSI模型的第二层（数据链路层）工作。

路由器

路由器在两个或多个局域网之间传输数据。路由器在每个局域网上有一个网卡。在TCP/IP网络中，每个网卡有一个IP地址。这样，路由器在OSI模型的网络层工作。

许多情况下，`/etc/sysconfig/network`之类文件中配置的网关地址应为连接网络的路由器的IP地址。

也可以将Linux计算机配置成路由器。首先需要两个或多个网卡，连接不同网络。然后要在内核中启用IP转发功能。这在IPv4配置中很简单，只要在`/proc`目录中改变一个设置即可：

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

如果需要，可以在局域网中配置路由器，以完成与交换机或集线器相同的功能。为了保证下次启动Linux时这个改变还在，可以打开`/etc/sysctl.conf`文件，验证下列变量设置为1：

```
net.ipv4.ip_forward = 1
```

网关

大多数情况下，Linux假设路由器与网关的功能是相同的。例如，如果网络通过路由器

的以太网网卡eth0连接外部网络，则可以在/etc/sysconfig/networking/devices目录下的ifcfg-eth0文件中用GATEWAY IP地址指定与局域网的连接。

但是，网关还有不同的用途，因为它可以用来连接使用不同协议栈（如TCP/IP与IPX/SPX）的局域网。网关在OSI应用层工作。

在局域网上配置计算机

尽管Red Hat Linux通常将计算机配置成连接局域网，但也可能需要改变配置。假设便携电脑上的Linux要连接另一网络，或者要从不同部门获取了一些计算机，还可能是计算机上安装了另一网卡，要保证每个网卡配置正确，甚至可能是Red Hat Linux没有探测到你的网卡，需要改变配置。

通常Red Hat Linux在安装过程中配置网卡。只要一个可探测网卡与Linux驱动器以及动态主机配置协议（DHCP）服务器即可。也可以手工输入IP地址和主机名信息。如果连接到NIS网络，则要在安装过程中输入相应名称。第28章将详细介绍NIS。

遇到问题时，一定要知道到哪里可以查找Linux计算机的网络配置问题。一些基本命令包括ifconfig与arp（配置网卡）以及与主机名相关的各种命令。

还要了解本地的网络配置工作。/etc/sysconfig/network文件是一系列重要的Linux网络配置文件中的一个。

用ifconfig配置

也许关键Linux网络配置命令是ifconfig，它在/sbin目录中。利用这个命令的正确选项，可以指定IP地址、硬件端口和网络掩码，以及激活和冻结网卡。很容易检查当前的网络配置。如图21.1所示，我的计算机上有两个活动网络组件：一个以太网网卡（eth0）和一个回环设备（lo）。可以看出，eth0包括局域网的连接信息。回环设备可以保证Linux正确连接TCP/IP协议栈。

```
[root@RH9Test root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:40:F4:3C:05:58
          inet addr:10.252.113.3  Bcast:10.252.113.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1640 (1.6 Kb)  TX bytes:1832 (1.5 Kb)
          Interrupt:5 Base address:0x8000

lo        Link encap:Local Loopback
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:67692 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67692 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4624266 (4.4 Mb)  TX bytes:4624266 (4.4 Mb)

[root@RH9Test root]#
```

图21.1 ifconfig输出

很容易为网卡指定新的IP地址。下列命令对eth1指定新的IPv4地址：

```
# ifconfig eth1 10.122.238.3
```

本章稍后将会介绍，这个IP地址的标准网络掩码为255.0.0.0。还可以用新IP地址指定不同的网络掩码：

```
# ifconfig eth1 netmask 255.255.255.0 10.122.238.3
```

过去，Red Hat Linux在对第二个（及以后的）网卡指定IRQ端口和I/O地址时会遇到问题。现在可以为网卡指定不同硬件地址。例如，下列命令对计算机上第三个以太网网卡指定IRQ 9和I/O地址0x300：

```
# ifconfig eth1 irq 9
# ifconfig eth1 io_addr 0x300
```

从图21.1可以看出，这些设置对应于ifconfig输出中的Interrupt与Base address设置。如果遇到错误，则中断或地址可能已经分配，或是为即插即用设备保留。

可以用这个命令激活和冻结网络适配器。例如，下列命令激活和冻结网络适配器eth0：

```
# ifconfig eth0 down
# ifconfig eth0 up
```

用arp配置

地址解析协议（ARP）将IP地址与网卡上的硬件地址相关联。计算机连接网络上的另一台计算机之后，要交换硬件地址，然后存放在ARP数据库中。因此可以用arp命令在自己的计算机中找到这个ARP数据库（标识一个问题）：

```
# arp
Address      HWtype HWaddress      Flags Mask  Iface
192.168.7.2  ether  00:12:B5:64:3B:B2  C          eth0
RH9laptop    ether  00:60:0B:8A:41:93  C          eth0
192.168.7.2  ether  52:A5:CB:32:52:A2  C          eth0
experimental ether  00:20:78:09:D3:6A  C          eth0
```

根据建立连接的方式，Address列中列出远程计算机的IP地址或名称。计算机名来自/etc/hosts。HWtype列显示网络适配器类型，HWaddress列按十六进制格式列出网络适配器硬件的地址。

这个输出显示有重复的IP地址，可能阻碍网络上的通信。可以用arp -d computename命令删除ARP表中相关计算机的项。一定要将computename换成出现故障的计算机名或IP地址。

主机名命令

许多主机名命令可以定义或列出不同网络中的计算机名。表21.1列出了这些主机名命令。除了dnsdomainname命令之外，其余命令都可以设置计算机名。例如，命令hostname ilovehackers将计算机名设置为ilovehackers。

表21.1 主机名命令

命令	功能
hostname	列出或设置本地计算机上的主机名
domainname	列出或设置NIS域名
dnsdomainname	列出网络上DNS服务器的完全限定域名
nisdomainname	见domainname
ypdomainname	见domainname

网络配置文件

Red Hat Linux中有许多网络配置文件，包括其他Linux发行版本中常用的基本配置文件，如/etc/hosts、/etc/resolv.conf与/etc/host.conf。Red Hat Linux还有一些新的配置文件，在/etc/sysconfig目录中，可以用来确定基本网络设置。

提示：红帽子公司正在努力汇总配置数据，特别是与网络设置相关的数据，放到/etc/sysconfig目录中。如果不知道要到哪里找配置数据，则可以从这个目录开始。

静态主机名——/etc/hosts

在ARPANET出现的初期，这个全球网络上只有几台计算机。这些计算机运行UNIX，用/etc/hosts文件作为计算机名和IP地址的静态数据库。当有新主机要加进这个网络时，很容易改变/etc/hosts文件，并在所有计算机上共享这个文件的拷贝。

尽管Internet中已经不可能用/etc/hosts完成任务，但/etc/hosts仍然是小型网络的可行方案。只要保证局域网上每台计算机具有相同的/etc/hosts文件拷贝，就能够满足网络要求。

这个文件相当简单：每一行有一个IP地址、一个完全限定域名（FQDN）和一个主机名：

```
192.168.23.121    linux1.mommabears.com    linux1
```

DNS服务器——/etc/resolv.conf

如果不用/etc/hosts，也可以使用域名服务（DNS）服务器。在Linux中，DNS通过伯克利因特网名称域（BIND）实现，使用named监控程序（DNS将在第24章详细介绍）。如果有DNS服务器的IP地址，则可以在/etc/resolv.conf配置文件中输入这个IP地址。

这个文件很简单，每个DNS服务器称为一个名称服务器，这个文件将名称服务器与IP地址相关联。如果将网络连接到ISP，则要在文件中增加ISP的DNS服务器IP地址，语句如下：

```
nameserver 207.217.126.81
```

搜索顺序——/etc/host.conf

有两个主机名与IP地址的数据库：/etc/hosts和DNS服务器，顺序由/etc/host.conf确定。通常，这个文件中只有如下一行：

```
order hosts,bind
```

它将Linux计算机配置成先在/etc/hosts文件中搜索正确的IP地址，然后再检查关联（BIND），上节曾介绍过，这是DNS服务器的Linux名称。甚至可以在这个表中包括NIS服务器，见第28章介绍的/etc/nsswitch.conf。

基本网络设置——/etc/sysconfig/network

基本网络设置数据放在/etc/sysconfig/network中。如果网络遇到问题，则可以检查这个文件。文件开头可以看到NETWORKING=yes，其他变量如表21.2所示。并不是所有这些变量都要在这个配置文件中出现，如果使用DHCP服务器，则有些变量是不必要的，有些变量可能位于/etc/sysconfig/networking/devices目录中的网络适配器特定文件中。

表21.2 /etc/sysconfig/network变量

变量	描述
NETWORKING	取值为yes/no，要让Red Hat Linux运行网络，就要取yes
HOSTNAME	计算机的主机名
GATEWAY	计算机的网关IP地址
GATEWAYDEV	用网关连接网络的网络设备，如eth1,如果计算机上有多个网卡，则需要这个网络设备
NISDOMAIN	NIS系统的域名，如有的话

配置公网与专网

第20章介绍了IPv4地址的一些基本知识。下面要介绍如何在配置连接到Internet的局域网时使用IPv4地址。

配置连接到Internet的局域网时，不能随便选择任何IP地址。内部网络可以随意使用一组专用IP地址，但连接到Internet时至少要有有一个公用IP地址。网络上的每台计算机可以同时用这个公用IP地址访问Internet。

但是，大多数公用IP地址已经被用光，余下的也通常由ISP分配。

说明：公用IP地址用于Internet上计算机与网络之间的通信。另一方面，独立的专用网络可以使用相同的专用IP地址。为了避免混淆，专用IP地址不能在Internet上通信。

可以用专用IP地址配置局域网，并在网关计算机上配置一个公用IP地址，将局域网与Internet相联。为了得到Internet上的公用IP地址，要与ISP联系。可以取得带子网或网络掩码的静态IP地址，也可以从DHCP服务器取地址。

网络定义

局域网中定义IP地址时常用到下面几个基本定义。

网址 每个IP地址分为两个部分：网址和主机地址。192.168.22.0之类的网址惟一标识一个特定网络。假设是C类网，则标识IP地址范围为192.168.22.1到192.168.22.254。

网络掩码 网络掩码是特殊的IP地址（也称子网掩码），可以定义局域网上可用的IP地址范围。三个标准的网络掩码是255.0.0.0、255.255.0.0与255.255.255.0。

广播地址 广播地址是个特殊的IP地址，它让网络上所有计算机通信，是网络上最后一个IP地址。例如，如果网址为192.168.22.0，网络掩码为255.255.255.0，则广播地址

为192.168.22.255。

专用IP地址 专用IP地址是在专用局域网中使用的，可以通过带公用IP地址的计算机用局域网上的专用IP地址连接Internet。不同局域网可以使用同一专用IP地址。但是，不能用专用IP地址直接连接Internet。

公用IP地址 公用IP地址直接连接Internet。

无类域间路由（CIDR） 无类域间路由（CIDR）方法可以指定非标准网络掩码，从而可以分割或组合标准IP地址范围。

专用IP网

要在网络内部用专用IP地址设置计算机，就要有网址和网络掩码。这两个参数定义了IP地址范围。第20章曾介绍过，专用IP地址有三个标准范围，见表21.3。

表21.3 专用IP地址范围

范围	类	描述
10.0.0.1-10.255.255.254	A	这个域中可支持1600万台计算机
172.168.0.1-172.168.255.254	B	这个域中可支持65 000台计算机
192.168.0.1-192.168.255.254	C	这个域中可支持254台计算机

选择网址和网络掩码时，通常选择表21.3所示IP地址组之一的子集。例如，如果网址为10.0.0.0，网络掩码为255.255.255.0，则地址范围为10.0.0.0到10.0.0.255，共256个不同地址。这些地址构成一个子网。

但是，第20章曾介绍过，10.0.0.0是保留网址，而10.0.0.255是广播地址，这些地址不能分配给特定计算机。这样，这个子网中只能对实际计算机分配254个地址。

网络掩码

网络掩码可以确定特定IP地址是否在同一局域网中，还可以区别网址与主机地址。将网址和网络掩码放在一起时，可以定义计算机可以分配的主机地址范围。

表21.4显示了一些网址、主机地址和网络掩码的例子。“可用主机地址”列定义了内部网络可以指定的IP地址。

表21.4 样本网址和网络掩码

网址	网络掩码	可用主机地址	可以分配的主机地址范围
10.0.0.0	255.0.0.0	10.0.0.1~10.255.255.254	16 777 214
10.21.92.0	255.255.255.0	10.21.92.1~10.21.92.254	254
10.182.0.0	255.255.0.0	10.182.0.1~10.182.255.254	65 534
172.168.78.0	255.255.255.0	172.168.78.1~172.168.78.254	254
172.168.0.0	255.255.0.0	172.168.0.1~172.168.255.254	65 534
192.168.3.0	255.255.255.0	192.168.3.1~192.168.3.254	254

从这个信息可以得到IP地址的下列规则：

- 网络IP地址不能作为特定计算机的主机地址。这个地址在可用主机地址范围之前。
- 网络掩码中的255通常对应于网址。例如，如果IP地址为10.162.4.23，而网络掩码为255.255.255.0，则网址为10.162.4.0。这个IP地址的主机部分为23。这个规则的例外见“无类域间路由（CIDR）”一节。
- IP地址范围中最后一个地址保留为广播地址。例如，表21.4的最后一个例子中，广播地址为192.168.3.255。
- 标准网络掩码为255.0.0.0、255.255.0.0与255.255.255.0。其他网络掩码见“无类域间路由（CIDR）”一节。

配置网络

在局域网中设置TCP/IP之前，要选择一组地址。根据前面几节介绍的知识，可以选择专用网址和网络掩码。将两个地址放在一起时，就可以得到局域网上每台计算机可以指定的IP地址范围。

也许最常见的网络掩码是255.255.255.0，前面曾介绍过，这个网络掩码可以选择254个IP地址。换句话说，如果网址为10.168.0.0，则这个网络掩码可以对网络上的计算机指定10.168.0.1、10.168.0.2、10.168.0.3到10.168.0.254的地址。

记住，网络范围中第一个地址是保留网址（这里是10.168.0.0），最后一个地址是广播地址（这里是10.168.0.255）。

可以指定的IP地址有两个选择，可以用ifconfig之类的命令将其赋予各台计算机，即同时要手工增加DNS服务器和默认网关的IP地址，也可以在DHCP服务器中设置可用主机地址范围。第24章将会介绍，DHCP服务器可以将IP地址“租借”给网络上的每台计算机。这个服务器还可以传递与网络中DNS服务器和网关地址相关的信息。

网关计算机

在网络中，网关计算机连接局域网和另一网络，如Internet。在典型的局域网中，只有一台计算机直接连接另一网络，这台计算机有两个或多个网卡：一个连接局域网，其他的连接其他网络。每个网卡指定一个IP地址。网关地址是局域网中网卡的IP地址。

为了演示这个配置，请看图21.2，其显示五台计算机的局域网。集线器与Internet之间的计算机是网关计算机。这个局域网中所有其他计算机的网关地址为10.190.18.3，是这个局域网中网关计算机的地址。

网关计算机上的另一网卡取得Internet上的公用IP地址，这里是62.33.23.122。

无类域间路由（CIDR）

无类域间路由不是个简单课题，但如果按下列步骤一一分析，则很快就可以掌握这个概念。

大多数情况下，IPv4网络中需要的网络掩码只有255.0.0.0、255.255.0.0和255.255.255.0。这些网络掩码分别与A类网、B类网和C类网相关。

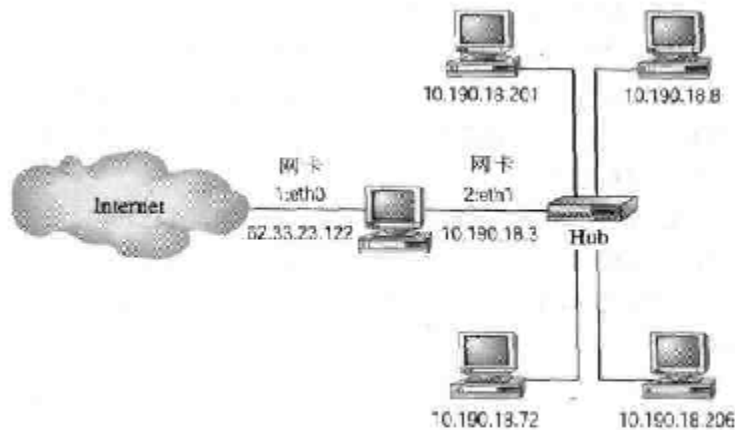


图21.2 分配IP地址

利用这三个网络掩码很容易区别网址与主机地址。例如，如果远程网络上的一台计算机的IP地址为192.168.38.48，而网络掩码为255.255.255.0，则网址为192.168.38.0。这个局域网中其他计算机的IP地址为192.168.38.1到192.168.38.254。

位与字节

为了理解无类域间路由（CIDR），要了解IPv4地址中的位与字节。IPv4地址中有32位，组成四个0到255之间的数，对应于4个字节。一个字节共八位，每位表示一个不同数。上面一行将位表示成字节，下面一行将位表示成十进制数。

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

例如，如果字节为10000000，则对应的值为128。如果字节为00010000，则对应的值为16。如果字节为11111111，则对应的值为128+64+32+16+8+4+2+1=255。

例如，假设要用网址192.168.38.0设置一个C类网。局域网中可能不需要254个IP地址，但如果你负责两幢大楼中的两个局域网，则可以使用无类域间路由（CIDR）。这时可以用CIDR按不同方式划分IP地址。

要了解无类域间路由的工作，下面回头看看位。下面两个IP地址是192.168.38.48与255.255.255.0的二进制表示：

```
11000000 10101000 00100110 00110000
11111111 11111111 11111111 00000000
```

前面曾介绍过，网络掩码中的255对应于网址，这里是192.168.38.0。表示成位时，网络掩码中的1对应于网址：

```
11000000 10101000 00100110 00000000
```

说明：注意255.255.255.0对应于IPv4地址的24位。在CIDR符号中，这个网址和网络掩码可以表示成192.168.38.0/24。

最后8位没有包括, 因此得到 $2^8=256$ 个主机地址, 从0开始。0指定为主机网址结尾, 255指定为主机广播地址, 这两个地址不能分配给特定计算机, 因此, 这个局域网中可以提供254个地址。下面看看网络掩码增加一位的情形:

```
11000000 10101000 00100110 00110000
11111111 11111111 11111111 10000000
```

网络掩码中1表示的区域表示192.168.38.0的网址, 但只有最后七位没有包括, 因此理论上只有 $2^7=128$ 个主机地址, 从0到127。因此这个网络的网址为192.168.38.0, 广播地址为192.168.38.127, 网络掩码为255.255.255.128。

说明: 看看255.255.255.128与IPv4地址中25位的对应关系。在CIDR符号中, 这个网络和网络掩码可以表示为192.168.38.0/25。

看看IP地址192.168.38.166的这个网络掩码:

```
11000000 10101000 00100110 10110000
11111111 11111111 11111111 10000000
```

利用同样的原理, 这个网络的网址为192.168.38.128, 广播地址为192.168.38.255。记住, 这两个IP地址都不能分配给特定计算机, 因此只有126个主机地址。

CIDR网络掩码53.255.255.0可以使用192.168.38.0网络上的254个计算机地址, 而网络掩码变成255.255.255.128之后, 只能在两个不同局域网中配置126个主机地址。

建立Internet连接

尽管高速Internet连接的广告打得很响, 但大多数家庭用户仍然通过56kb/s电话MODEM连接Internet。但是, 高速Internet连接的成本已经降下来, 适合小公司建立Internet连接。高速Internet连接也称为宽带网。

宽带连接服务有几种, 包括卫星网、红外网、无线网、电缆MODEM和数字用户线(DSL)服务。这些服务以144kb/s以上速度发送和接收数据。由于这种竞争, 许多电话公司降低了T1线(1.544Mb/s)和综合服务数字网(ISDN, 128Kb/s以上)之类传统宽带服务的成本。

大多数情况下, 连接宽带服务和计算机连接路由器一样。宽带提供者提供或出售路由器。你可以用第24章介绍的方法连接其DHCP服务器, 也可以使用网关和DNS服务器的IP地址。

也许Linux文本方式的电话MODEM接口的最佳范例是minicom。红帽子公司开发了自己的Internet配置向导, 可以帮你建立电话MODEM连接和宽带连接。

Internet配置向导

红帽子公司的Internet配置向导不同于Microsoft公司的同名工具。可以在GNOME与KDE中用控制台命令redhat-config-network-druid启动。从图21.3可以看出, 这时打开增加新类型设备的窗口, 其中的选项可以配置各种不同网络设备。尽管本节的重点是普通电话MODEM连接, 但我们也简要介绍其他选项。



图21.3 Internet配置向导

CIPE (VPN) Connection 连接加密IP包装 (CIPE) 也称为VPN (虚拟专用网)，它在Internet之类公共网络上建立安全的网络连接。这个选项可以设置连接两端的IP地址和相应的加密密钥。

Ethernet Connection 这个选项可以指定以太网连接的驱动器、设备名 (如eth1) 和各种资源，如这个网卡的IRQ端口、I/O地址与DMA信道。这些设置用ifconfig命令帮助Linux探测到这个网卡并与其通信。还可以将网卡设置成从DHCP服务器取得IP地址信息，或者自己配置这些设置。如果DHCP服务器在远程网络上，则通常要指定BOOTP协议。

ISDN Connection 和以太网连接一样，这个选项指定ISDN适配器的驱动器和资源。由于ISDN在欧洲特别普及，因此这个设置对欧洲的几种不同国家进行了定制。

Token Ring Connection 这是令牌环连接的前端，与以太网配置选项相似。

Wireless Connection 这是无线连接的前端，与以太网配置选项相似。其余设置允许你设置网络的无线信道和/或加密密钥。

xDSL Connection DSL连接有好几种，上装和下载速度各不相同。无论哪种情况，都可以用这个实用程序配置以太网适配器的连接，使用宽带ISP的用户名和口令。也适用于大多数电缆MODEM连接。

下面用Internet配置向导配置MODEM。在设备类型窗口中，选择MODEM Connection并单击Forward按钮继续。向导探测MODEM。如果没有探测到，而计算机上确实有MODEM，则可以按第2章介绍的Winmodems方法处理。无论结果如何，都会进入图21.4所示的MODEM选择窗口，可以配置MODEM的设备、波特率和其他选项。

说明：Linux MODEM设备通常可以转换成Microsoft COM端口。例如，/dev/tty0=COM1，/dev/tty1=COM2，等等。图21.4所探测的MODEM是在与COM3相关的设备文件上探测的。因此，如果MODEM在Microsoft操作系统中能工作，则可以找到其COM端口，并使用相应的Linux设备。

波特率通常应为MODEM连接速度的两到四倍。对56Kb/s的MODEM (美国为53Kb/s)，通常要选择波特率为115 200或230 400b/s。MODEM会压缩这个数据流。在Flow Control文本框中，通常保持默认值Hardware (CRTSCTS)。对设置满意之后，单击Forward按钮继续。

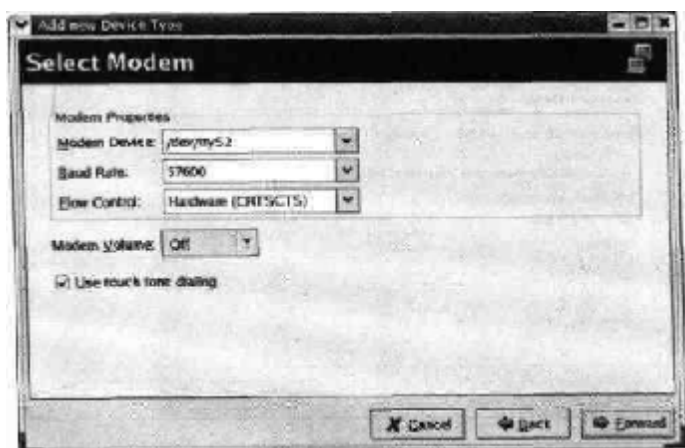


图21.4 MODEM选择窗口

提示：为了检查与所探测到MODEM相关的设备，运行`ls -l /dev/modem`命令，它与实际MODEM设备文件`/dev/ttyx`相关联。

在下一个窗口中，可以增加ISP的访问号、登录名和口令，如图21.5。只要有这个信息，就不必担心Internet提供者列表中是否有你的国家（如来自欧洲的T-Online账号，单击T-Online账号设置按钮，然后填入T-Online提供的提示）。

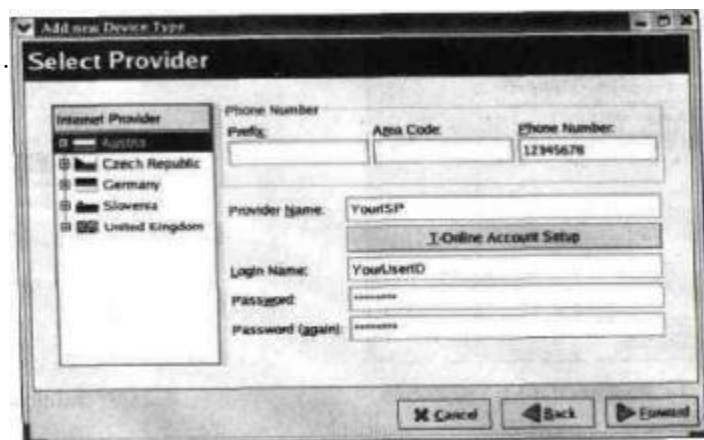


图21.5 指定ISP

然后再次单击Forward按钮继续。下一个窗口是IP设置对话框，如图21.6。通常，ISP自动提供拨号电话MODEM连接的IP地址设置。如果ISP指定静态IP地址，则还要指定子网掩码和网关地址，可以在这个窗口中输入。

单击Forward按钮继续，在下一个窗口中单击Apply。可以看到网络配置窗口有网卡设置。图21.7所示的ppp0设备是非活动的，但这只是表示MODEM还没有连接。加亮MODEM并单击Activate。如果MODEM启用声音，则可以听到其拨号ISP的声音。

准备切断MODEM连接时，回到网络配置窗口，加亮MODEM并单击Deactivate。

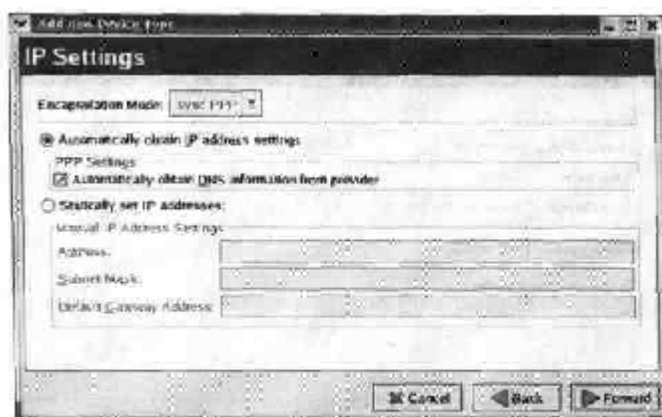


图21.6 IP设置对话框

使用minicom

MODEM连接的一个传统命令行工具是minicom，可以用minicom -s命令以根用户身份开始配置这个实用程序，打开minicom配置菜单，如图21.8。

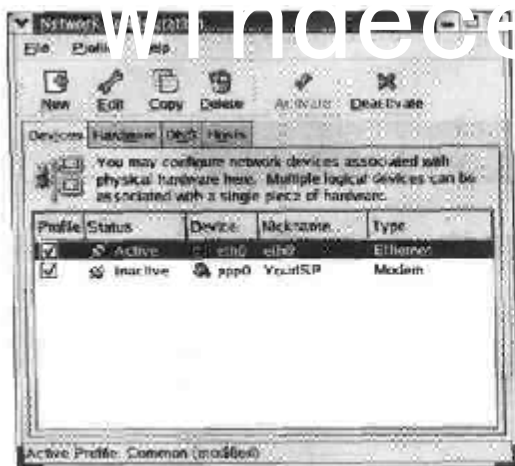


图21.7 激活MODEM



图21.8 minicom配置菜单

使用minicom之前，要先将其配置成连接MODEM。选择Serial Port Setup菜单并按Enter键，可以看到图21.9所示的菜单。根据MODEM的情况，可能还要改变下列设置：

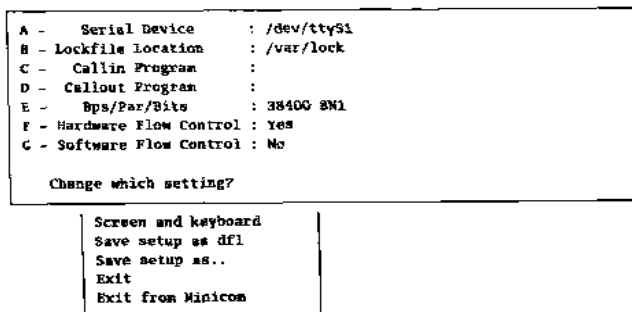


图21.9 配置串口

Serial Device 与MODEM相关联的设备。如果`ls -l /dev/modem`命令能显示与设备的连接, 如`/dev/ttyS0`, 则使用这个设备; 否则可能要采用试错方法。

Bps/Par/Bits MODEM的数据设置。位/秒(b/s)数据速率应为MODEM速度的两到四倍, 因为目前MODEM会压缩数据。除非使用旧式MODEM, 否则奇偶性(Par)和停止位(Bits)应匹配默认值8N1。

检查MODEM文档中的其他任何需要改变的设置, 如b/s或硬件流控制。配置完成后, 一定要从原菜单中选择Save Setup As df1。要开始MODEM查错, 选择Exit(不是Exit from Minicom)。这样就会初始化MODEM并进入主minicom屏幕。

最简单的测试是拨号到ISP。为此, 只要输入atdt命令以及ISP的号码。图21.10显示了这个过程的一个例子。



```
Welcome to minicom 2.00.0

OPTIONS: History Buffer, F-key Macros, Search History Buffer, IISn
Compiled on Jun 23 2003, 16:41:20.

Press CTRL-A Z for help on special keys.

AT S7=35 S0=0 L1 V1 X4 Ael E1 Q6
OK
atdt2612085
(CARRIER 3346)

! NOTE: D1: D/ 5A

CONNECT 9600
Authorized Use Only - Unauthorized Use is Prohibited - Sprint-IP

sdn-ar-00mctar000t slot:10/mod:2

User Access verification
Login/Username: 
```

图21.10 用minicom连接

说明: minicom实用程序用终端MODEM软件相关的常见命令。例如, atdt是“Attention, use Touch-Tone dialing”的简写。

网络查错

本书介绍了许多查错技术。网络查错也一样。遇到问题时, 需要收集数据、确定并隔离原因、研究症状, 如果这些都不行, 还可以采用科学方法。

前面曾介绍过, 许多网络问题的原因来自于物理设备的连接不好、电缆问题、电源问题, 等等。检查物理问题之后, 还可以使用Linux中的几个查错命令。`netstat`命令可以收集数据, 而`ping`与`traceroute`命令则可以隔离问题。

检查网络状态

为了检查网络状态你必须做如下两步。第一, 运行`ifconfig`命令, 保证网卡还在工作。前面曾介绍过, 可以用`ifconfig eth0 up`命令激活`eth0`网卡。如果网卡工作, 则下一步要用

netstat命令检查网络状态。

这个命令显示路由表、代理与外部网络的连接、接口统计信息，等等。例如，netstat -a命令显示所有可用连接。如图21.11所示，Local Address列显示名称与号码，对应于前几章介绍的TCP/IP端口。Foreign Address列可以看到本地计算机与另外两台计算机之间建立的telnet、http与ssh连接。

```
[root@RH9Test root]# netstat -a | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
tcp        0      0 0 *:1024                  *:*                      LISTEN
tcp        0      0 0 RH9Test:1025            *:*                      LISTEN
tcp        0      0 0 RH9Test:783             *:*                      LISTEN
tcp        0      0 0 *:sunrpc                 *:*                      LISTEN
tcp        0      0 0 *:x11                    *:*                      LISTEN
tcp        0      0 0 *:ssh                     *:*                      LISTEN
tcp        0      0 0 RH9Test:ipp             *:*                      LISTEN
tcp        0      0 0 RH9Test:smtp             *:*                      LISTEN
tcp        0      0 1 10.252.113.3:2836       RH9Test:ipp             SYN_SENT
tcp        0      0 0 10.252.113.3:2831       laptop2:netbios-ssn     ESTABLISHED
udp        0      0 0 *:1024                  *:*                      LISTEN
udp        0      0 0 *:687                    *:*                      LISTEN
udp        0      0 0 *:bootpc                 *:*                      LISTEN
udp        0      0 0 *:bootpc                 *:*                      LISTEN
udp        0      0 0 *:sunrpc                 *:*                      LISTEN
udp        0      0 0 *:631                    *:*                      LISTEN
udp        0      0 0 10.252.113.1:ntp        *:*                      LISTEN
udp        0      0 0 RH9Test:ntp              *:*                      LISTEN
udp        0      0 0 *:ntp                     *:*                      LISTEN
Active UNIX domain sockets (servers and established)
```

图21.11 netstat -a命令输出

路由表列出了计算机到网络上或网络外另一计算机的当前配置路径。Linux用这些路径寻找要连接的计算机。可以用netstat的变形检查路由表。图21.12显示了一个相当简单的路由表，包括三种不同类型的IP地址，见表21.5。

```
[root@RH9Test root]# netstat -nr
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
10.252.113.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 lo
0.0.0.0 10.252.113.113 0.0.0.0 UG 0 0 0 eth0
[root@RH9Test root]#
```

图21.12 路由表

表21.5 路由表

目标	说明
192.168.0.0	这个网络上的地址不需要网关，因为它在当前局域网上
127.0.0.0	回环地址不需要网关，因为它在当前计算机上
0.0.0.0	用192.168.0.113作为这个路由表中前面没有指定网关的所有IP地址的默认网关（可以在目标列中用默认值代替0.0.0.0）

如果需要，可以用route命令增加路由表中的路由。例如，假设刚刚增加了另一个局域网，网址为10.0.0.0，网络掩码为255.255.0.0，要将其连接另一网卡eth1。则可以用下列命令

将其加进路由表中:

```
# route add -net 10.0.0.0 netmask 255.255.0.0 dev eth1
```

用ping与traceroute检查连接

网络上遇到特定问题,如用户不能访问Web或电子邮件时,首先要与用户联系。根据你对浏览器和电子邮件管理器的知识,看看用户是否知道如何访问所要的服务。可能还要通过ssh或telnet登录到这个用户的计算机,亲自检查这个用户的计算机。

Linux中有许多工具可以检查大多数基本网络连接,包括应用程序所要的连接。这些命令工具基于ping和traceroute命令。诊断网络连接时,试使用下列命令。如果其能够工作,则按Ctrl+C键停止响应:

1. `ping 127.0.0.1`: 检查回环地址的连接。如果看到连续响应,如64 bytes from 127.0.0.1...,则说明TCP/IP已经在计算机上正确安装。

提示:除了连续ping,也可以用`ping -c 4 ip_address`命令向目标计算机发送四个ping分组,然后自动停止。甚至可以设置`alias ping='ping -c 4'`,关于alias命令的更多信息,见第8章。

2. `ping your_ip_address`: 换成网卡定义的IP地址,这个地址从ifconfig命令输出取得。如果看到类似的连续响应,则已经正确配置IP地址。
3. `ping your_host_name`: 换上计算机的主机名,这个地址通常在/etc/sysconfig/network中。如果看到类似的连续响应,则已经正确配置计算机的主机名。
4. `ping another_ip_address`: 将another_ip_address换成局域网中另一台计算机的IP地址。可以用ifconfig命令找到Linux计算机的IP地址(相应的Microsoft Windows命令为IPCONFIG)。如果看到类似的连续响应,则局域网上能够顺利通信,这两台计算机至少配置了相同网址和网络掩码。接下来可以试试局域网上默认网关的IP地址。
5. `ping another_hostname`: 将another_hostname换成连接网络的计算机名。如果是连接Internet,则一个例子是`ping www.Sybex.com`。如果能够工作,则说明已经正确配置了局域网网关或路由器,可以和局域网进行通信。
6. `traceroute another_hostname`: 使用连接网络上的另一名称。如果连接Internet,则可以试试`traceroute www.Sybex.com`命令。看看从你的计算机访问Sybex公司Web站点时间经过的路径。诊断网络互联问题时,这个命令可能在目标终止,或在有问题的网关或路由器上停止。

例如,如果ping局域网网关或路由器IP地址时遇到问题,则要检查网络上其他一些计算机的IP地址。如果无法连接局域网上的其他计算机,则可能是电缆或连接问题;否则可能是路由器计算机的硬件问题。

小结

本章介绍了用Linux配置局域网的一些基本步骤。局域网上可以使用许多基本硬件组件。传输媒介通常是铜线或光纤电缆。集线器将计算机连接到局域网。交换机常用于将局域网分成段。路由器可以在两个或多个局域网之间传输数据。网关可以在不同协议栈之间转换,如

TCP/IP与IPX/SPX。

由于几个原因，可能要改变Linux安装期间设置的网络配置。也许配置网卡最关键的命令是ifconfig。可以用ifconfig指定硬件端11和IP地址信息。甚至可以用它激活或冻结网卡。arp命令可以检查重复的IP地址。hostname命令可以设置不同网络服务看到的计算机名。一些关键网络配置文件是/etc/hosts、/etc/resolv.conf、/etc/host.conf与/etc/sysconfig/network。

局域网中可以使用IPv4地址。只要对局域网上的计算机指定一个专用IP地址范围。利用正确的网络掩码，可以选择A类、B类和C类范围的专用IP地址。然后只要一个公用IP地址将局域网连接Internet。可以用CIDR和非标准网络掩码配置IP网络。

尽管宽带连接对企业是成本更有效的选项，但大多数Internet用户仍然通过电话MODEM连接。红帽子公司开发的Internet配置向导可以帮助配置几种类型的网络适配器，包括电话MODEM。也可以用minicom实用程序从命令行界面配置Internet连接。

进行网络查错时，首先要记住，大多数网络问题都是物理问题。检查电缆与连接。如果仍不能解决问题，则要收集数据、找出问题原因并研究问题症状。

如果这些办法都行不通，则要回头取得手头数据，采用科学方法。Linux中有几个命令可以收集数据和查找问题原因，包括ifconfig、netstat、ping与traceroute。minicom命令可以保证网络适配器处于工作状态，netstat命令可以检查当前的网络连接和路由表，ping与traceroute命令可以检查网络中的连接。

了解了网络配置的基本知识后，第22章将介绍保护网络的最佳做法。Red Hat Linux中有两个关键安全系统：可插入验证模块（PAM）和防火墙。

第22章 保护Linux网络

安全对任何计算机网络都很重要。各种黑客都在寻找网络上的漏洞，有些只是找趣儿，而另一些则想攻击网络，实现其罪恶目的。

本章首先对网络安全的最佳做法进行一般性概述，其中一些最佳做法要求很好的Linux技巧，可以从本章学到。本章介绍加密、防火墙、口令与物理安全的概念。而其他重要技巧需要权衡利弊，只能从实践中学习。

Red Hat Linux不仅在用户登录时要求验证，还在用户使用某些命令与服务时要求验证。可插入验证模块（PAM）可以对任何情形进行动态配置。

防火墙可以用iptables命令配置，可以对每个TCP/IP信道上的每个服务定制系统。这些命令都不难理解，只要知道如何将其分解为各个成分就可以。一旦了解了iptables命令之后，就可以建立所需要的防火墙，保护系统且不会拒绝用户需要的服务。

与防火墙密切相关的是伪装，即向Internet上其他主机隐藏局域网内计算机的真实身份。伪装也是iptables的一个功能。

由于任何安全系统都不是十全十美的，因此需要经常检查是否有人侵入。Ethereal之类的工具可以检查网络上明文形式显示的内容。可以浏览wtmp之类的日志文件，看看是否有非授权用户。其他工具（如Tripwire）可以探测到关键文件的改变。

安全性也可能太过份。如果用户不遵循口令政策，则可能是因为这些政策过于严格。如果用户无法得到所要服务，则可能是防火墙太强了。本书另外几章还会详细介绍安全需求，包括加密和相应的配置网络服务。本章介绍下列课题：

- 了解最佳做法
- 使用可插入验证模块（PAM）
- 建立防火墙
- 设置IP伪装
- 入侵检测
- 查错访问问题

了解最佳做法

可以采用如下几个步骤保护网络。一些基本做法要求的是常识而不是高深的计算机知识。计算机的配置方式可以提高安全性，加密可以保护网络上传输的数据，适当位置的适当口令可以保护用户账号与计算机，防火墙也可以提供不同程度的网络保护。

物理步骤

保护计算机和网络硬件的方法取决于它们的价值和所处环境的风险。

在家庭网络中，最好把集线器和路由器放在小孩碰不到的地方，放在喝咖啡时不会溅

到的地方。一般来说，不必担心有人用物理方法攻入家庭网络。

在公司网络中，则要防止计算机被有意或无意损坏。根据需要，可能要把服务器、路由器、交换机与集线器放在上锁的机房中。安全房中还可以放置一些备份媒介。但一定要保证这些地方有正确的环境控制（如空调），以提高系统寿命。

提示：一定要记住配置，以便从头开始重装Linux时使用。

在军队和其他有高度安全需求的设置中，可能要采取更强的措施，如拆掉或锁住可以连接存储硬件的软盘驱动器和端口。根据需要，可以对服务器、网络硬件和 workstation 配置不同的物理安全级。此外，还可以把内部网络与Internet隔离，增加其安全性。

在任何安全设置中，还可以使用其他基本安全系统，如警报、门卫、摄像头、ID系统等类似设备。

加密

网络上发送的敏感数据必须加密。大多数情况下，加密就是用专用密钥打乱发送的数据。在连接的另一端，要向用户提供公用密钥，以便将数据解密。

安装Red Hat Linux时可以对口令、不同服务和其他系统设置不同的安全级。系统中可以增加的加密类型如下

MD5口令 Linux最多支持256个字符的长口令。

隐蔽口令组 这种口令在/etc/shadow中加密口令，通常只能让根用户访问。隐蔽口令组默认是激活的（详见第9章介绍）。

Kerberos 这个加密系统满足网络上发送口令的需求。利用这个系统，客户机和服务器都使用TGS（给票服务）的授权。Kerberos是个完全功能的加密系统，不适用于隐蔽口令组，只与本章稍后介绍的PAM系统部分兼容。Kerberos是麻省理工学院开发的。

GNU隐私门卫 常用于加密电子邮件，使用Linux版本的PGP系统。GNU隐私门卫也可以验证下载内容（如RPM包）的合法性。详细信息见第10章。

RSA与DSA 数字签名算法（DSA）与安全Shell（SSH）网络相关。关于SSH与这些算法的更多信息，见第23章。

口令安全

口令安全至少有三级：计算机、引导装入器和Linux登录。在每一级口令安全中，要确定是否需要口令、使用何种口令和口令改变的频率。第9章介绍了用户口令相关的问题与选项。

计算机口令

现代PC机的BIOS中有个选项，可以建立访问BIOS菜单的口令。BIOS中包括各种选项，包括网络启动计算机，这一操作只是记录输入的口令。但BIOS的其他改变可能破坏系统数据。

但是，至少在标准PC机上，修改BIOS时要求实际访问这台计算机。换句话说，如果系统是物理安全的，则不需要BIOS口令。

引导装入器口令

前面曾介绍过，引导装入器有两种：GRUB和LILO。大多数用户喜欢GRUB，因为它可以使用口令保护。否则用户可以改变引导装入器配置文件，通过在单用户方式中启动Linux改变根口令，甚至可以访问双引导配置中的其他操作系统（如Microsoft Windows）。关于默认Red Hat Linux引导装入器GRUB的更多基本信息，见第11章。利用第11章介绍的方法，可以用口令保护其他操作系统的访问。例如，如果计算机包括Microsoft Windows的双引导配置，则可以在GRUB配置文件/boot/grub/grub.conf的相应段中增加一个口令如下：

```
title DOS
    lock
    password --md5 sf934^(^$asjl
    rootnoverify (hd0,0)
    chainloader +1
```

lock命令使任何人都无法启动相关操作系统，试图启动都会造成“must be authenticated”的错误消息。增加这个代码后，为了启动一个系统，你首先要输入编辑GRUB的口令，选择DOS选项，并输入启动这个操作系统的MD5口令。

防火墙与DMZ

防火墙有三种基本类型：一种检查进入网络的每个分组，根据数据类型进行决策；另一种基于Samba、NFS与Apache之类的服务，我们在相关章节已经介绍过，不同服务有不同形式的访问控制，因此也可以作为防火墙；还有一种基于与xinetd监控程序相关联的服务，见第23章介绍。

Red Hat Linux的主要防火墙工具是iptables。本章稍后将会介绍，iptables可以阻止标识的通信流，也可以配置成阻碍大部分通信流，只允许需要的服务经过。在网关计算机上配置防火墙时，它常常作为堡垒主机。

可以对不同计算机设置不同的防火墙保护级。例如，有Web服务器，可能需要配置两个不同的防火墙，如图22.1。对防火墙I，可以配置最基本的保护，包括避免Web服务器典型问题的命令，如所谓“ping到死机”。对于防火墙II，可以配置完全保护，在Internet上保护网络。关于防止网络中“ping到死机”和其他问题的更多信息，见本章稍后。

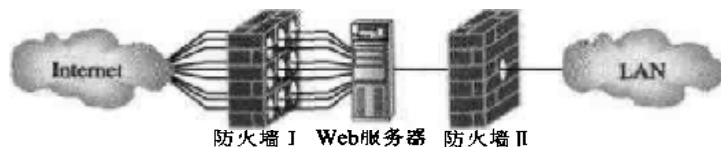


图22.1 配置两个不同的防火墙

说明：ping到死机是一种拒绝服务（DOS）攻击，用ping命令发送大量数据，使其他网络消息无法到达目标服务器。

使用可插入验证模块（PAM）

另一级安全基于可插入验证模块。这些模块通常用于限制特定应用程序的访问，如halt

与redhat-config-network，只让根用户访问。不同模块可以按用户、口令或访问地址控制访问。控制标志确定传递一个PAM命令行是否足以限定用户对特定应用程序的访问。

说明：与PAM相关联的定义通常是重叠的。本章调用PAM模块的命令是应用程序，而PAM模块文件中的命令是命令行。

基本配置

PAM中有一系列动态可装入模块，可以针对特定应用程序进行定制。PAM配置文件存放在/etc/pam.d目录中，各个模块存放在/lib/security目录中，并在/usr/share/doc/pam-version/txts目录中建档。

PAM命令行按下列格式组织：

```
module_type control_flag module_location arguments
```

下节介绍模块与控制标志。模块位置就是文件位置，通常在/lib/security中。变元与每个模块相关联。

模块类型

PAM模块类型共四种，都与用户验证相关：

口令模块 Linux登录控制台不让用户多次尝试登录。这是因为，PAM口令模块设置登录次数和口令的长度极限。

会话模块 这类模块生成应用程序设置。例如，PAM会话模块可以限制特定用户登录Linux服务器的次数。

账号模块 这类模块根据政策管理访问。例如，PAM账号模块可以根据用户表、时间和口令有效期允许或拒绝访问。

验证模块 验证模块检查用户标识。例如，PAM验证模块可以提示输入用户名和口令。这些模块有一个公共变元service=system-auth，调用system-auth PAM包的用户名与口令。

控制标志

每个PAM命令行的控制标志有四种，见表22.1，它们用于确定模块命令成功或失败时应用程序的操作。

表22.1 PAM控制标志

控制标志	描述
optional（可选）	这个模块不重要，除非所有其他模块也有可选控制标志
required（必须）	如果这个模块失败，则与这个文件相关的应用程序也会失败
requisite（必要）	如果这个模块失败，则立即停止验证过程，不能使用这个命令，PAM文件中后面的命令忽略
sufficient（充分）	如果这个模块成功，则立即停止验证过程，可以使用这个命令，PAM文件中后面的命令忽略

PAM举例

要了解PAM模块的工作原理，最好一行一行分析PAM配置文件。所有PAM配置文件默认位于/etc/pam.d。下列代码例子基于这个目录中的redhat-config-xfree86文件。注意这个配置文件与第15章介绍的配置实用程序同名。下面一行一行分析这个PAM配置文件：

```
auth sufficient pam_rootok.so
```

验证模块类型表示这个命令行要检查用户标识。充分控制标志表示如果这个命令行成功，则可以运行应用程序。如果用户是根用户，则/lib/security目录中的pam_rootok.so模块返回PAM_SUCCESS。换句话说，如果根用户运行redhat-config-xfree86，则不运行这个文件中的其他命令行就能启动应用程序。

```
auth sufficient pam_timestamp.so
```

这个命令也使用验证模块类型和充分控制标志。pam_timestamp.so模块通常对过去5分钟内运行了sudo命令的普通用户返回PAM_SUCCESS。

```
auth required pam_stack.so service=system-auth
```

这个命令使用验证模块类型和必须控制标志。如果满足service=system-auth变元，则pam_stack.so模块返回PAM_SUCCESS。system-auth模块要求用户输入根口令。

```
session required pam_permit.so
```

这个命令使用会话模块类型和必须控制标志。pam_permit.so模块总是返回PAM_SUCCESS，因此继续到下一行。

```
session optional pam_xauth.so
```

这个命令使用会话模块类型和可选控制标志。pam_xauth.so模块不返回成功或失败，可选标志使这个命令行与这个文件关系不大。但是，可以增加调试变元，将访问请求记录到/var/log/messages^[1]。

```
session optional pam_timestamp.so
```

这个命令也使用会话模块类型和可选控制标志。pam_timestamp.so模块更新任何时间标志文件，通常在/var/run/sudo目录中。这个文件中还有一个命令：

```
account required pam_permit.so
```

这个命令使用账号模块类型和必须控制标志。pam_permit.so模块总是返回PAM_SUCCESS。

建立防火墙

任何配置成防止数据进入系统或局域网的命令和配置文件都是防火墙。其中有些命令和配置文件在其他章节有所介绍。主要的Linux防火墙工具是iptables。不同iptables命令可以链接起来。每个命令可以阻止或允许与特定协议相关联的数据。

其他防火墙命令

iptables的两个遗留的替代命令是ipfwadm与ipchains。ipfwadm命令与Linux内核2.0.x相关，现已过时。ipchains命令与Linux内核2.2.x相关，在当前2.4.x内核中仍然支持。

许多好的防火墙都基于ipchains。如果使用这些防火墙，则要采取下列操作：

1. 用service iptables stop命令关闭iptables服务。
2. 用rmmod命令删除ip_tables和相关模块。
3. 安装ipchains-* RPM包。
4. 用insmod命令激活ipchains.o模块。

然后将ipchains规则加进/etc/sysconfig/ipchains，并用service ipchains start命令激活。要确保下次启动Linux时激活ipchains而不是iptables，可以用相应chkconfig命令进行检查。

数据方向与iptables

iptables命令在三个方向规定数据通信流：in、out和through。换句话说，可以将iptables配置成阻止数据从外部网络进入，也可以配置成阻止数据离开计算机，还可以配置成阻止数据经过计算机，即介于局域网和另一网络（如Internet）之间。

防火墙链

没有一个到处都适用的奇妙的iptables命令。大多数防火墙都是把一系列iptables命令链接成一条链。下面看一个相当简单的防火墙：基于安装Red Hat Linux期间建立的高度安全防火墙。图22.2所示的信息来自/etc/sysconfig/iptables，Red Hat Linux在这里存储所有防火墙命令。

```

# Firewall configuration written by lokkit
# Manual customization of this file is not recommended.
# Note: ifup-post will punch the current nameservers through the
#       firewall; such entries will *not* be listed here.

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Lokkit-0-50-INPUT - [0:0]
-A INPUT -j RH-Lokkit-0-50-INPUT
-A RH-Lokkit-0-50-INPUT -i lo -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -s 207.217.126.81 --sport 53 -d 0/0 -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -s 207.217.120.83 --sport 53 -d 0/0 -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp --syn -j REJECT
-A RH-Lokkit-0-50-INPUT -p udp -m udp -j REJECT
COMMIT

```

图22.2 iptables防火墙

目前只要注意这个文件中显示的四种不同链：INPUT、FORWARD、OUTPUT和RH-Lokkit-0-50-INPUT。前三种链是默认链，允许所有通信流经过防火墙。前面加-A的所有命令都将添加到RH-Lokkit链末尾。下面几节要详细介绍iptables命令及其选项。

iptables格式

下面详细介绍iptables命令。这个命令的内容非常丰富，可以用一本书来介绍其所有选项。本章稍后将介绍伪装选项，这里先介绍几个重要选项。iptables命令的格式非常特别：

```
iptables -t table option pattern -j target
```

第一个选项基于-t表格选项。有两个基本表：**filter**与**nat**。**nat**表支持与伪装相关的网址转换（NAT）。**filter**表可以阻止或允许特定类型的网络通信流。由于默认为-t过滤，因此防火墙配置文件中通常不指定这个选项。

iptables选项

记住，默认链有三个：**INPUT**、**OUTPUT**与**FORWARD**。iptables有四个主要选项：列表（-L）、添加（-A）或删除（-D）特定文件以及刷新（-F）链上的所有规则。

iptables -L命令列出所有链上的所有当前规则。如果防火墙很复杂，则可能要列出特定链的规则。例如，iptables -L INPUT命令列出与进入计算机的数据相关的所有防火墙规则。图22.3显示了当前防火墙规则的样本清单。

```
[root@RH9Test root]# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
RH-Lokkit-0-50-INPUT all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination
RH-Lokkit-0-50-INPUT all -- anywhere anywhere

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain RH-Lokkit-0-50-INPUT (2 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT udp -- rns1.earthlink.net anywhere udp spt:domain
ACCEPT udp -- rns3.earthlink.net anywhere udp spt:domain
REJECT tcp -- anywhere anywhere tcp flags:SYN,RST,ACK/
SYN reject-with icmp-port-unreachable
REJECT udp -- anywhere anywhere udp reject-with icmp-p
ort-unreachable
[root@RH9Test root]#
```

图22.3 当前防火墙规则

要增加新规则，通常要将其添加到一个链末尾。例如，下列命令限制每秒在这台计算机上转发的ping命令数据量，从而防止“ping到死机”的问题：

```
# iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --
limit 1/s -j ACCEPT
```

要删除现有规则，首先要找出链以及规则在链中的位置。例如，如果要删除与图22.3中rns3.earthlink.net相关的规则，则要注意它是RH-Lokkit-0-50-INPUT链中第三条规则，因此相应命令如下：

```
# iptables -D RH-Lokkit-0-50-INPUT 3
```

如果还不明白，可以再看一些例子。例如，如果要删除FORWARD链中的一系列规则，则可以运行下列命令：

```
# iptables -F FORWARD
```

这个命令比较危险；如果运行iptables -F命令而不指定链，则会删除每个链中的所有规则。表22.2列出了基本iptables选项。

提示：如果不小心刷新了iptables链，则仍然可以从/etc/sysconfig/iptables中得到原先的链。可以用service iptables reload命令让Linux重新读取这些规则。

表22.2 iptables选项

选项	功能
-A chain rule	将一个规则添加到链末尾
-D chain number	从指定链中删除指定规则
-F chain	从指定链中删除或刷新所有规则
-I chain number rule	在指定链的指定编号位置插入一个规则
-L chain	列出指定链中的当前规则
-N chain	开始新的非标准链
-X chain	删除用户定义链

iptables的模式

下面要介绍iptables命令的步骤。前面介绍了一个链中要采取的操作。下面要指定链中要匹配的模式。模式可以匹配消息发送者或源的IP地址、TCP/IP端口或协议。

IP地址模式

以上面防止“ping到死机”的命令为例。由于某种原因，假设要控制来自IP地址199.88.77.66的ping命令，则可以使用下列命令：

```
# iptables -A FORWARD -s 199.88.77.66 -p icmp --icmp-type
➤ echo-request -m limit --limit 1/s -j ACCEPT
```

注意这里使用-s选项，为源IP地址作准备。可以逆转效果，控制除该IP地址之外其他每个地址的ping命令，为此可以使用感叹号，如下：

```
# iptables -A FORWARD -s !199.88.77.66 -p icmp --icmp-type
➤ echo-request -m limit --limit 1/s -j ACCEPT
```

感叹号让iptables把后面的项目看成例外。换句话说，这个命令适用于Internet上除指定IP地址的计算机之外的每一台计算机。

可以指定局域网之类的IP地址范围。下列命令将普通网址和CIDR符号的网址以及子网掩码组合起来（关于CIDR（无类域间路由）的介绍，见第21章）：

```
# iptables -A FORWARD -s 199.88.77.0/255.255.255.0 -p
➤ icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
# iptables -A FORWARD -s 199.88.77.0/24 -p icmp --icmp-type
➤ echo-request -m limit --limit 1/s -j ACCEPT
```

表22.3列出了iptables命令中的一些其他开关。

表22.3 iptables命令的开关

开关	功能
--dport port	指定目标TCP/IP端口号
--icmp-type message	可以指定ICMP消息类型，echo-request对应于ping命令发送的消息
-j action	表示满足命令要求时采取的操作，通常为ACCEPT、DROP、REJECT或LOG
--limit time	设置特定消息允许的速率，可以是秒、分、时、天：如2/s表示每秒2个消息
-m condition	检查匹配数据，可以是tcp与udp之类协议，也可以是极限之类的条件
-p protocol	检查tcp与udp之类的协议的数据
-s ip_address	指定源IP地址
--sport port	设置源TCP/IP端口
--tcp-flags fl1,...	检查TCP数据包中的标志： SYN（同步）数据包是客户端发送，并要求答复 ACK（确认）数据包确认同步请求 A FIN（完成）数据包是通信中最后一个分组 RST（复位）数据包告诉客户端请求已被拒绝 例如：--tcp-flags SYN、RST、ACK SYN寻找SYN、RST与ACK数据包，但只传递带SYN标志的数据包

TCP/IP协议模式

iptables命令检查进入、离开或经过计算机的每个数据包。可以让这个命令检查特定协议。最常用的协议模式基于TCP、UDP与ICMP。-p选项指定协议。例如，对前面的命令阻止“ping到死机”，可使用-p icmp选项，因为ping与ICMP协议相关（关于ICMP的详细信息，见第20章）。

TCP/IP端口模式

第20章曾介绍过，TCP/IP端口有65000多个。许多端口是标准服务专用的。例如，下列命令防止199.88.77.0/24网络用TCP分组连接端口21，这个端口与FTP服务相关联：

```
# iptables -A FORWARD -s 199.88.77.0/24 -p tcp --dport 21 -j REJECT
```

iptables操作

假设生成的iptables命令要在进入、离开和经过计算机的数据中寻找某种模式，并在找到匹配后，告诉iptables对这个数据分组进行什么处理。

iptables找到匹配后，-j命令让链跳到下列四个结论之一：ACCEPT、DROP、REJECT或LOG。表22.4将介绍这些操作。

表22.4 iptables的操作

操作	说明
-j ACCEPT	允许匹配指定特征的分组进入、离开和经过计算机
-j DROP	阻止匹配指定特征的分组进入、离开和经过计算机
-j REJECT	阻止匹配指定特征的分组进入、离开和经过计算机，并向发出消息的计算机发一个消息
-j LOG	在/var/log/messages中登记分组匹配记录

综合起来

分解iptables命令之后，就可以建立所要的防火墙规则了。可以使用第19章介绍的redhat-config-firewall之类的工具，但GUI工具没有提供所要的控制水平。至少要知道如何从防火墙链中增加和删除规则。

从没有防火墙开始

作为试验，假设计算机开始没有防火墙。这里假设局域网有两台或多台计算机。如果/etc/sysconfig/iptables中有需要保存的防火墙规则，可以进行备份。加上前面介绍的“ping到死机”规则，修改这个规则，使其删除局域网中的任何ping请求。

下列步骤假设局域网地址为192.168.0.0/24，当然这也可以换成你所使用的局域网的网址和网络掩码。

- 1. 备份当前防火墙，将/etc/sysconfig/iptables复制到主目录中的文件中。
- 2. 用iptables -F命令刷新当前防火墙规则。
- 3. 添加“ping到死机”规则，使其删除局域网中的任何ping请求：

```
# iptables -A INPUT -s 192.168.0.0/24 -p icmp --icmp-type echo-request -j DROP
```
- 4. 试在本地计算机上使用ping 127.0.0.1命令，确保其仍然可以工作。
- 5. 到局域网中另一台计算机上，试ping第一台计算机的IP地址。这时可以在一切停止之前看到一个ping消息。
- 6. 如果需要，恢复原先的/etc/sysconfig/iptables文件。

如果喜欢试验，可以再试一次，例如在iptables命令末尾使用-j REJECT选项。看看从局域网中另一台计算机上运行ping命令时的情形。

插入防火墙规则

回到图22.3描述的高度安全防火墙。如果今后在计算机上安装一个Web服务器，则要对防火墙规则稍作修改。当前防火墙包括下列规则：

```
Chain RH-Lokkit-0-50-INPUT (1 references)
target    prot opt source                destination
ACCEPT    all  --  anywhere              anywhere
ACCEPT    udp  --  rns1.earthlink.net    anywhere udp spt:domain
ACCEPT    udp  --  rns3.earthlink.net    anywhere udp spt:domain
```



```

REJECT    tcp  --  anywhere          anywhere tcp flags:SYN,RST,ACK/SYN reject-
➡ with icmp-port-unreachable
REJECT    udp  --  anywhere          anywhere udp reject-with icmp-port-
➡ unreachable

```

为了接收经过TCP/IP端口80的数据，需要插入一个iptables规则。根据前面介绍的条件可以得出：

- 我们在RH-Lokkit-0-50-INPUT链中插入规则。使其成为链中第二条规则（-I RH-Lokkit-0-50-INPUT 2）。
- 由于Web站点连接需要答复，因此要求TCP数据包（-p tcp）。
- 我们从/etc/services知道，Web站点连接使用端口80（-m tcp --dport 80）。
- 来自客户机的Web站点请求，应有SYN标志。应检查RST与ACK标志，保证不是来自作为服务器的计算机的请求（--tcp-flags SYN, RST, ACK SYN）。
- 最后，要接收符合所有这些条件的数据包（-j ACCEPT）。

综合起来，可以得到下列命令：

```

# iptables -I RH-Lokkit-0-50-INPUT 2 -p tcp -m tcp
➡ --dport 80 --tcp-flags SYN,RST,ACK SYN -j ACCEPT

```

增加这个命令之后，可以在iptables链中看到下列结果：

```

Chain RH-Lokkit-0-50-INPUT (1 references)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
ACCEPT     tcp  --  anywhere              anywhere
➡ tcp dpt:http flags:SYN,RST,ACK/SYN
ACCEPT     udp  --  rms1.earthlink.net    anywhere udp spt:domain
ACCEPT     udp  --  rms3.earthlink.net    anywhere udp spt:domain
REJECT     tcp  --  anywhere              anywhere
➡ tcp flags:SYN,RST,ACK/SYN reject-with icmp-port-unreachable
REJECT     udp  --  anywhere              anywhere
➡ udp reject-with icmp-port-unreachable

```

如果这些改变符合你的要求，则保存所做的改变。

保存配置改变

可以用service iptables save命令将配置改变保存到/etc/sysconfig/iptables中。

尽管iptables是Red Hat Linux 9的默认，但最好检查防火墙的服务状态。为此可以使用chkconfig命令。例如，下列命令显示Linux启动iptables服务时的运行级：

```

# chkconfig --list iptables
iptables 0:off 1:off 2:on 3:on 4:on 5:on 6:off

```

如果看到iptables服务没有激活（和使用正确的运行级），则可以将其激活。例如，下列命令在下次从运行级2、3、5启动Linux时激活iptables：

```

# chkconfig --level 235 iptables

```

说明：记住，Red Hat Linux通常不使用运行级4，详见第11章。

设置IP伪装

IP伪装可以隐藏局域网上计算机的IP地址，通过将这些IP地址换成网关计算机上的公共IP地址，从而防止局域网上的计算机被直接攻击。

说明：IP伪装是一种网址转换（NAT）。另一种实现网址转换的方式是使用代理服务器。

IP伪装与防火墙通常在局域网上的同一台计算机上配置，是局域网与Internet等外部网络之间的网关。因此，iptables开发人员提供了几个配置IP伪装的命令选项。

功能

第21章曾介绍过，可以通过配置网关计算机来连接局域网与Internet等外部网络。假设连接Internet，则可以在局域网中使用专用IP地址，而在连接Internet的网卡上使用公共IP地址。

然后，为了完成连接，要按第21章介绍的方法在网关计算机上配置IP转发。然后要在防火墙中增加相应的iptables命令。

设置IP伪装之后，任何从局域网内连接Internet站点都通过网关计算机发送数据包。例如，假设有个用户要寻找一个Web站点，则源地址为局域网中计算机的IP地址，换成网关计算机的公共IP地址。iptables命令对该数据包指定一个非标准的TCP/IP端口。然后网关计算机缓存源IP地址和分配的TCP/IP端口。

防火墙收到Web站点的数据时，进行的过程正好相反。分配的端口与缓冲区进行匹配。从缓冲区中取得源计算机的IP地址并将其加进Web站点数据中。然后网关计算机将数据包发送到源计算机。

IP伪装命令

下面再看看iptables命令的格式。前面曾介绍过，默认表为filter表，是与iptables相关的防火墙功能：

```
iptables -t table option pattern -j target
```

但是，可以通过-t nat选项，用iptables配置伪装。例如，下列命令假设网址为10.0.0.0/24，网关上直接连接Internet的网卡为eth2：

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth2 -j MASQUERADE
```

这个命令改变发往Internet的数据包的IP地址（-A POSTROUTING），这个改变只适用于局域网上的专用IP地址（-j MASQUERADE）。

入侵检测

入侵检测的标准方式有两种，一种是检查/var/log/wtmp文件中的登录，另一种是检查日志文件的活动，看看Linux系统上的通信流何时最少。

但是，人们入侵系统的方式之一是读取用户在网络上以明文形式发送的口令。检查网

络通信流的一个重要工具是Ethereal，这个协议分析器支持Linux/UNIX与Microsoft Windows，位于Red Hat Linux的etherel-* RPM包中。

用Ethereal检测

协议分析器一个更通俗的名称是窃听器。Ethereal之类的协议分析器记录（或窃听）网络通信流。如果在以太网网络中，则可以记录局域网所有计算机之间的所有通信。

如果消息以明文形式传输，则Ethereal可以将其转换成可读格式。例如，以图22.4为例，Ethereal可以浏览各种网络分组。注意加亮显示的19号数据包。

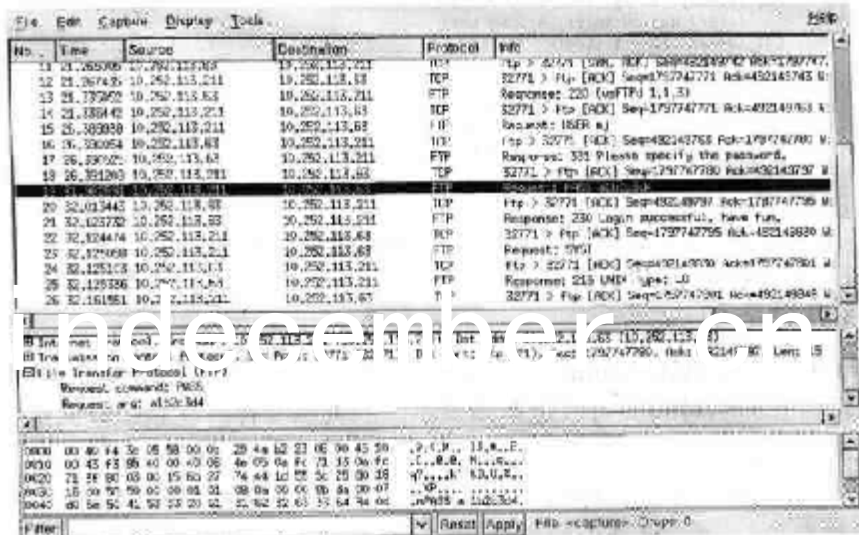


图22.4 Ethereal显示口令

可以看出，数据包19是用户mj连接本地FTP服务器时输入的口令：a1b2c3d4。

由此可见，网络的物理安全非常重要：如果黑客能够实际访问局域网，则可以用Ethereal连接计算机，检测到任何人使用局域网上的明文服务器时所用的口令。

Ethereal并不是黑客使用的最先进武器，如果你能用Ethereal探测到明文口令，则黑客也能够读到这个口令。

安装etherel-* RPM包之后，可以用etherel命令启动这个工具。

检查登录

最好检查日志文件中的可疑活动。例如，/var/log/wtmp文件中提供了登录记录。由于这是个二进制文件，因此需要使用二进制阅读器utmpdump。要阅读这个文件的记录，可以使用utmpdump/var/log/wtmp命令。图22.5显示了登录活动的输出摘要。

注意图22.5中的second-to-last项目。可以看出，源IP地址为128.99.1.64，如果它不属于授权用户和网络，则要小心了。也许有人想入侵你的系统。然后要考虑增加iptables防火墙命令，阻止这个IP地址或相关IP网络的访问。

```

    ] [Fri Mar 28 10:21:34 2003 EST]
[5] [02082] [5 ] [      ] [2.4.20-8 ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[5] [02083] [6 ] [      ] [2.4.20-8 ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[5] [02084] [x ] [      ] [2.4.20-8 ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02078] [1 ] [LOGIN ] [tty1   ] [      ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02079] [2 ] [LOGIN ] [tty2   ] [      ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02080] [3 ] [LOGIN ] [tty3   ] [      ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02081] [4 ] [LOGIN ] [tty4   ] [      ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02082] [5 ] [LOGIN ] [tty5   ] [      ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[6] [02083] [6 ] [LOGIN ] [tty6   ] [      ] [0.0.0.0
    ] [Fri Mar 28 10:21:34 2003 EST]
[7] [02138] [:0 ] [root  ] [:0    ] [      ] [128.99.1.64
    ] [Fri Mar 28 10:21:51 2003 EST]
[7] [02246] [:0 ] [root  ] [pts/0 ] [0.0.0
    ] [Fri Mar 28 10:22:25 2003 EST]

```

图22.5 登录活动的输出摘要

Tripwire与可疑活动

第13章介绍了/etc/syslog.conf文件如何配置日志文件。大多数日志文件存放在/var/log目录中，日志项目都标明时间。可以定期浏览不同的日志文件，在系统或网络中应该没有活动时检查存在的可疑活动。

但是，高水平的黑客会让你以为系统中一切都是正常的。例如，具有根用户访问权限的黑客可能替换掉/var/log目录中的文件。

检查文件完整性的一个重要工具是Tripwire。到本书编写时，这个软件有开放源代码版本，也有商业版本。开放源代码版本在红帽子安装RPM包中，并且在www.tripwire.org中有建档，商业版本可以从Psionic技术公司（www.psionic.com）的TriSentry套件中取得。

Tripwire可以检查系统中关键配置文件的完整性。要有效利用这个工具，就要尽快安装，它不能在黑客攻进系统和改变系统关键文件之后探测不良改变。

安装Tripwire之后，要对它进行配置并生成一个基本数据库，然后Tripwire RPM包所带的cron作业可以每天检查文件。

安装Tripwire

安装Tripwire很简单，只要运行安装脚本/etc/tripwire/twinstall.sh即可。这个脚本采用文本格式，甚至可以用文本编辑器修改安装文件地址。它包括Tripwire许可证（GPL）的拷贝。

运行默认脚本时，会提示增加本地和站点口令，即加密访问Tripwire所用的口令。安装过程中，twinstall.sh脚本还在/etc/tripwire目录中生成配置文件和政策文件。

然后用tripwire --init命令初始化Tripwire数据库。这个命令可能要几分钟时间用政策文件tw.pol建立初始化数据库，可能指出几个错误，因为它搜索的文件中可能有几个还没有安装。

可以编辑/etc/tripwire/twpol.txt，更新Tripwire政策文件。例如，如果还没有安装Z shell，

则可以删除/bin/zsh的引用。改变完成后，可以用下列命令更新Tripwire政策文件：

```
# tripwire --update-policy /etc/tripwire/twpol.txt
```

提示：安装Tripwire之后，它就会成为保卫系统的重要工具。黑客可能通过改变各种Tripwire文件而隐藏自己的踪迹。为了防止这种情形，可以使用一些安全媒介或只读媒介。例如，有些管理员将Tripwire文件写入只读光碟中。

Tripwire工作

假设从Red Hat Linux RPM包安装了Tripwire，则它会每天检查数据库。事实上，/etc/cron.daily目录中有个tripwire-check检查脚本。第13章曾介绍过，这个脚本默认通过/etc/crontab在每天凌晨4时2分运行。

可以编辑这个文件，保存输出。例如，可以将tripwire命令的输出定向到一个日志文件：

```
/usr/sbin/tripwire --check >> /var/log/tripwire
```

得到的输出很有趣。为了本书的写作，我暂时删除/sbin/poweroff文件，然后再运行tripwire-check检查脚本。在/var/log/tripwire中，可以得到下列输出：

```
-----
File Name: Critical Utility Binaries ( /sbin/poweroff )
Security Level: 100
-----

Removed:
"/sbin/poweroff"
```

尽管这个警告好像是小问题，但它告诉你有人从Linux系统中删除了poweroff命令。

查错访问问题

安全性也可能太强。任何阻止用户取得所要服务的安全措施都可能弊大于利。

如果用户需要一个服务，而安全措施阻止使用这个服务，则要进行选择。为了解决这个问题，可以提供可接受的替代，也可以按某种方法放松安全措施。

有时，用户报告某个服务无法工作，其实是安全性问题。例如，iptables DROP选项产生的输出可能让用户费解。

过于安全

阻止用户取得所要服务的安全措施通常可能弊大于利，但有些服务相当危险，可以提供可接受的替代。

例如，如果用户要通过Telnet连接远程计算机，则最好让用户了解第23章介绍的安全shell实用程序。通常不能让用户以明文形式在网络上发送口令。

又如第28章要介绍的网络文件系统(NFS)要访问几个不同的TCP/IP服务：nfs、portmap、rpc.mountd和rpc.nfsd。NFS使用TCP/IP端口2049，而标准Red Hat Linux防火墙还防止端口111，与RPC监控程序相关联。

否定与拒绝

用户要访问被禁止的服务时，iptables中的DROP与REJECT选项产生不同结果。例如，可以实现下列防火墙链，防止192.168.0.0/24网络上的用户通过Telnet连接：

```
# iptables -A INPUT -s 192.168.0.0/24 -p tcp -dport 23 -j DROP
# iptables -A INPUT -s 192.168.0.0/24 -p tcp -dport 23 -j REJECT
```

提示：端口23是Telnet服务的TCP/IP端口。可以从/etc/services查找标准TCP/IP端口。

现在看看192.168.0.0/24网络上的用户通过Telnet连接设置为DROP请求的服务器时看到的结果：

```
# telnet RHL9
Trying 192.168.0.34
```

用户看到这个输出时，可能抱怨Telnet无法工作。现在看看192.168.0.0/24网络上的用户通过Telnet连接设置为REJECT请求的服务器时看到的结果：

```
# telnet RHL9
Trying 192.168.0.34
telnet: connect to address 192.168.0.34: Connection refused
```

用户看到这个输出时，通常能了解服务器RHL9不允许Telnet连接。用户询问原因时，你可以告诉用户，可以选择SSH之类替换选项。

小结

也许你很幸运，你管理的网络没有连接任何其他网络，特别是Internet。你的服务器和网络组件可以锁在安全的机房里。你的用户可以信任。这时，你就不需要保护Linux网络了。

但是，大多数局域网都与其他网络连接。许多用户要通过Internet连接进行工作。但是，任何Internet访问都可能使局域网系统暴露在黑客攻击之下。

网络安全有一些最佳做法，如提供不同程度的计算机与网络组件物理安全性，对Web服务器和内部局域网配置不同级别的防火墙，用Kerberos和GPG之类的不同协议加密通信，用MD5和隐蔽口令加密口令，在BIOS和Linux引导装入器中提供不同程度的口令安全。

PAM（可插入验证模块）可以限制对特定应用程序的访问，如/etc/pam.d目录中定义的应用程序。这个目录中的文件与不同应用程序相关联。四种PAM（可插入验证模块）模块是口令、会话、账号与验证。每个模块有四种控制标志之一：可选、必须、必要与充分。这些控制标志确定模块的响应。

Red Hat Linux主要的防火墙实用程序是iptables。不同iptables命令可以连接成链，用于三个方向的数据：INPUT、OUTPUT与FORWARD。可以将iptables配置成匹配不同模式的IP地址、TCP/IP端口以及防止“ping到死机”的模式。防火墙命令匹配一个模式时，可以将iptables设置为ACCEPT、DROP、REJECT或LOG。

还可以对iptables配置IP伪装，这是一种NAT（网址转换），隐藏局域网中访问Internet等外部网络的计算机的地址。每个外走分组与一个未用端口号相关联，局域网得到答案时，

用这个端口号标识请求计算机。

可以用几种方法探测Linux计算机上的入侵。一种是检查/var/log/wtmp中的登录，一种是使用Tripwire RPM包。还可以用Ethereal检查通信流，显示用户是否以明文形式在网络上发送口令。

当然，安全也可能太过份。任何使用户无法访问所需服务的措施都是太强的。这样配置的iptables可能使用户费解。

下一章要介绍通过网络访问计算机的其他方式。有些是不安全的，如远程Shell与Telnet。另一方面，安全Shell是相当安全的，因为它使用口令等加密通信。还可以用tcp_wrappers访问控制文件保护非安全服务。

第六部分 Linux网络服务

第23章 远程访问与xinetd服务

如果用户能够从远程地址读取文件和运行程序，则网络是高效的。如果用户经常需要远程访问，则要考虑配置一些Linux远程访问服务。

可以通过几种不同方式从远程地址访问Linux计算机。这些远程访问服务是由扩展Internet服务监控程序xinetd控制的。这个监控程序监听与FTP和Telnet等服务相关联的端口。如果安装了相应的服务器，则xinetd可以在请求时启动这些服务。

xinetd监控程序控制几个远程访问服务的操作，包括远程Shell（RSH）、Telnet、FTP和POP3。安装这些服务之后，每个服务都在/etc/xinetd.d目录中有一个配置文件。可以通过这些配置文件激活每个服务，许多情况下，也可以建立服务特定的防火墙。

利用TCP包装系统，可以对xinetd服务配置详细的防火墙。要控制对单个或所有xinetd服务的访问，可以定制/etc/hosts.allow与/etc/hosts.deny文件。还可以按第22章介绍的方法用iptables防火墙控制访问。

一些xinetd服务以明文形式发送消息。第22章介绍了这样会给口令带来风险。另一种远程访问Linux计算机的方法是安全Shell（SSH）。安全Shell监控程序可以配置专用与公用密钥，用于在网络上加密消息。

有了所有这些安全措施之后，诊断服务问题有时不一定很容易。如果用户无法访问一个服务器，则可能要一个一个检查可用的防火墙。也可能是这个服务没有激活，或不同的iptables命令或TCP包装器阻止访问。本章介绍下列主题：

- 使用典型扩展服务
- 用TCP包装器控制访问
- 了解安全Shell
- 查错访问问题

使用典型扩展服务

有几个基本服务是由xinetd控制的，这些服务包括RSH、Telnet、POP3与FTP，等等。关于当前安装的xinetd服务清单，见/etc/xinetd.d目录。

Xinetd监控程序包括两级配置文件，一个是/etc/xinetd.conf，用来设置基本参数。默认情

况下，它从/etc/xinetd.d中的配置文件查找服务的特定参数。

许多xinetd服务是不加密的，但有自己的安全级。如果使用每个服务相关的安全措施来限制信任用户与计算机的使用，则风险有限。Linux管理员要判断这样对你和公司是否合适。

xinetd配置文件

第一个扩展Internet服务的监控程序配置文件是/etc/xinetd.conf。这个文件中的设置对xinetd管理的所有服务设置基本参数。默认情况下Red Hat Linux配置文件很简单，如图23.1。

```
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    instances                = 60
    log_type                  = SYSLOG authpriv
    log_on_success            = HOST PID
    log_on_failure            = HOST
    cps                       = 25 30
}

include /etc/xinetd.d

.
.
.
.
.
.
"/etc/xinetd.conf" 161, 289C
```

图23.1 /etc/xinetd.conf配置文件

表23.1介绍了这个文件中显示的参数。可以看出，这个文件用instances控制xinetd负载、指定日志参数、停止过量连接和包括/etc/xinetd.d中的文件。

可以在/etc/xinetd.d目录下的任何其他配置文件中配置这些参数。需要IP地址时，可以使用普通符号或CIDR符号。

表23.1 xinetd.conf参数

命令	描述
instances	活动xinetd服务器的最大个数
log_type	指定日志，SYSLOG authpriv按第13章介绍的/etc/syslog.conf指定日志
log_on_success	指定服务启动和停止时的日志信息，重要参数包括PID、HOST与USERID
log_on_failure	指定用户请求的服务无法启动时的日志信息，重要参数包括HOST与USERID
cps	控制输入连接率，如果连接超过每秒25个，则将xinetd关闭30秒，从而减慢攻击xinetd服务的速度

(续表)

命令	描述
includedir	读取指定目录中的每个文件，作为xinetd配置文件
only_from	指定允许访问服务的IP地址
no_access	指定不允许访问服务的IP地址
access_times	指定允许访问服务的时间，例如access_times=08:00~23:00表示上午8时到晚上11时可以访问服务

激活xinetd服务

激活xinetd服务的方法有两种：直接编辑相应配置文件，或用相应的chkconfig命令激活。例如，如果安装了telnet-server-* RPM包，则可以在文本编辑器中打开/etc/xinetd.d目录中的telnet配置文件。这些配置文件包含下列关键参数：

```
disable = yes
```

换句话说，这个服务默认关闭。可以用下列语句启动服务：

```
disable = no
```

要进行这个改变，可以直接编辑相应配置文件，也可以用下列命令（其中service_name是要激活的服务名（如Telnet））：

```
# chkconfig service_name on
```

当然，可以用下列命令逆转这个过程：

```
# chkconfig service_name off
```

进行修改之后，要用下列命令让xinetd重新读取相应配置文件：

```
# service xinetd reload
```

也可以重新启动Linux，从而重新启动xinetd，使其重新读取相应的配置文件。但我们很少重新启动Linux。

提示：service命令可以运行/etc/rc.d/init.d目录中的任何脚本。例如，service xinetd reload命令的功能等价于/etc/rc.d/init.d/xinetd reload。

远程Shell

如果多台计算机上具有相同账号，则可以用远程Shell（RSH）方便地连接所选计算机上的不同账号。例如，启用和正确配置远程Shell之后，可以访问不同Linux计算机上的不同账号。RSH要求客户端安装rsh-* RPM包，服务器上安装rsh-server-* RPM包。

远程Shell有四个命令，称为r命令：rsh、rlogin、rexec和rcp。安装RSH服务器之后，前三个命令都在/etc/xinetd.d目录中有自己的配置文件。可以用前面介绍的方法激活所要的r命令。记住要重新装入xinetd服务。下列命令使用户mj可以在计算机RHL9上打开自己的账号：

```
[mj] $ rlogin RHL9
Password:
Last login: Tue Mar 17 10:27:43 from tty2
```

这里用户mj要输入自己的口令，但这也不是必要的：他可以在每台计算机上的主目录中生成一个.rhosts文件。只要其中包括客户机和服务器的计算机名，就不必输入自己的口令。Linux管理员也可以在/etc/hosts.equiv中加入相同的信息，每个在两台计算机上有账号的用户就不必输入自己的口令即可检查其他计算机上的文件。

访问远程计算机上的不同账号也同样简单，下列命令访问RHL9上用户lula的账号：

```
[mj] $ rlogin -l lula RHL9
Password:
Last login: Tue Mar 17 10:29:26 from tty2
```

换句话说，如果黑客知道Linux服务器上的账号，又能够改写这台计算机上的.rhosts或/etc/hosts.equiv文件，则很容易访问所要的文件。

如果要生成.rhosts或/etc/hosts.equiv文件，则应设置其不可变标志。完成之后，就无法删除这些文件。为此可以使用chattr +i filename命令，如下：

```
# chattr +i .rhosts
# chattr +i /etc/hosts.equiv
```

但是，如果黑客取得了根用户访问权限，则可以用chattr -i /etc/hosts.equiv命令取消其不可变标志。

Telnet

Telnet服务是连接远程计算机的最简单方式。许多用户都熟悉这个服务，并且它很容易使用。Telnet可以迅速配置几个不同的Linux终端。此外，利用Telnet还可以配置其他xinetd服务。但是，它以明文形式发送消息（包括口令），因此，Telnet的使用只限于安全的网络。

在Red Hat Linux中，Telnet客户机与服务器RPM包是分开的：telnet-*和telnet-server-*。

一旦建立网络连接之后，Telnet和任何其他Linux命令行界面一样。一个优点是，Telnet可以支持不同操作系统，图23.2显示了从Windows XP操作系统用Telnet连接Linux计算机的例子。

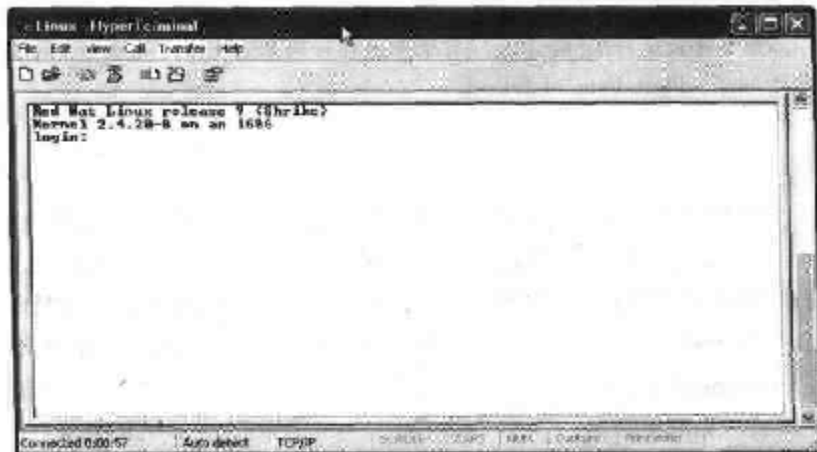


图23.2 从Windows XP操作系统用Telnet连接Linux计算机

如果Telnet连接或终端遇到问题, 则Telnet客户机可能发生了故障, 所管理的Linux服务器会发出终端消息。下列命令可以将环境变量设置为旧的标准终端程序:

```
TERM=vt100
```

和其他xinetd服务一样, 要通过/etc/xinetd.d/telnet配置文件激活这个服务并重新装入xinetd之后才能激活Telnet服务器。然后可以用telnet hostname命令从其他计算机访问这个服务。

FTP服务器

文件传输协议(FTP)是TCP/IP协议套件中最古老的协议之一。由于文件传输协议专用于传输文件, 因此在文件传输方面仍然比HTTP之类的新协议更高效。我下载文件建立Red Hat Linux光碟时, 用的就是FTP服务器。

第27章将详细介绍FTP服务器, 因此这里只介绍激活要求。一个最常用的FTP服务器是WU-FTP, 是华盛顿大学圣路易斯分校维护的, 现已不再放在Red Hat Linux中, 但可以从其FTP站点ftp.wu-ftp.org或SpeakEasy RPM库站点www.rpmfind.net下载。可以想象, 安装wu-ftp-* RPM包时, 它会在/etc/xinetd.d目录中安装wu-ftp配置文件。

和其他xinetd服务一样, 要在wu-ftp配置文件中设置disable = yes将其激活。

其他超级服务器服务

还有另外几个xinetd服务器, 包括finger、pop3s与imaps, 前者可以取得特定用户的更多信息, 后两者可以让远程用户通过服务器安全地访问电子邮件。表23.2列出了一些基本xinetd服务, 但这个清单并不完整。

表23.2 基本xinetd服务

服务	功能
amanda	配置备份用的高级马里兰自动网络磁盘档案器
finger	可以取得特定用户的更多信息, 通过chfn指定, 并存放在/etc/passwd中
imap	支持远程访问IMAP4邮件服务器
ipop3	支持远程访问POP3邮件服务器
rlogin	允许使用rlogin命令
rsh	配置RSH服务器
swat	支持Samba Web管理工具, 见第29章
telnet	设置Telnet服务器
wu-ftp	配置WU-FTP服务器, 见第27章

用TCP包装器控制访问

防止系统被黑的最佳方法是关闭或删除尽可能多的服务。例如, 如果没有安装Telnet服务器RPM, 则黑客无法用Telnet命令攻击你的系统。

如果不马上需要某个xinetd服务, 则可以在/etc/xinetd.d目录中将其冻结。大多数情况下, 只要在相关配置文件中关闭其他服务, 只留下必须的服务。

但是,有些用户在远程地点时要访问电子邮件,因此需要Telnet。如果需从远程地点访问大文件,则FTP服务器仍然是Internet上传输文件的最有效方法。

可以用TCP包装器配置所有这些服务的访问控制。

控制访问

可以用两种方法降低Linux计算机的风险。一种是控制用户/计算机对服务的访问,可以通过配置文件控制,有些位于/etc/xinetd.d目录中,另一些文件与不同服务相关,将在后面几章介绍;另一种方法是用TCP包装器通过/etc/hosts.allow与/etc/hosts.deny文件控制计算机的访问。

可以在这些文件中增加不同的规则。这些规则按下列顺序读取:

1. TCP包装器读取/etc/hosts.allow文件,如果显式允许访问,则提供访问权。
2. TCP包装器读取/etc/hosts.deny文件,如果显式拒绝访问,则指定计算机上的用户无法启动这个服务。
3. 如果两个文件中都没有这个计算机名或IP地址,则自动提供访问,xinetd启动服务。
4. 如果两个文件中都有这个计算机名或IP地址,则/etc/hosts.allow文件中的规则优先。

例如,如果配置的规则显式在/etc/hosts.allow中对计算机A打开服务,而在/etc/hosts.deny中对其拒绝服务,则计算机A取得访问权。

此外,任何改变保存到这些文件时立即生效,而不需要重新启动或重新装入xinetd监控程序。

xinetd防火墙

/etc/hosts.allow与/etc/hosts.deny与特定类型的语法相关联。首先,和其他脚本中一样,不读取空行和以#开头的说明语句。这些文件中的每个命令行采用下列配置:

监控程序: 客户机: spawn命令

换句话说,指定服务器监控程序时,可以将其与一组主机名或IP地址相关联。找到匹配时,也可以触发一个命令,如向用户或日志项目中发一个消息。

这个命令行的最简单例子如下:

ALL: ALL

以上的例子适用于所有监控程序和所有计算机。这些选项很复杂,因此最好一个一个地介绍。

TCP包装器监控程序

可以指定各个监控程序,但要记住监控程序名不一定与你想像的一样。例如,Telnet监控程序的名称为in.telnetd。

如果要指定多个监控程序,只要将它们放在空格分开的清单中。例如,下列/etc/hosts.deny文件中的语句阻止所有用户访问本地Telnet和RSH服务器:

in.telnetd in.rshd: ALL

如果不知道监控程序名,则可以查阅/etc/xinetd.d目录中的配置文件,这些配置文件把监控程序名作为服务器变量。

TCP包装器客户机

可以用主机名或IP地址指定TCP包装器命令中的不同计算机名或客户名。还可以使用几个通配符参数。

可以用几种方法指定主机名。可以一个一个指定，例如，下列命令阻止计算机sugaree与delilah访问本地Telnet和RSH服务器：

```
in.rshd in.telnetd: sugaree delilah
```

也可以指定计算机的完全限定域名（FQDN），如sugaree.mommabears.com完全限定域名可以使用通配符。例如，只包括.mommabears.com前面的点号可以指定mommabears.com网络上的所有计算机。

可以指定不同计算机，例如下列语句中的规则适用于mommabears.com网络中除delilah.mommabears.com以外的所有计算机：

```
in.rshd: .mommabears.com EXCEPT delilah.mommabears.com
```

IP地址也可以采用这些原则。例如，下列语句的规则适用于192.168.0.0网络中除192.168.0.102以外的所有计算机，它将应用于IP地址为192.168.0.0到192.168.0.255的所有计算机：

```
in.rshd: 192.168.0. EXCEPT 192.168.0.102
```

说明 192.168.0.0/24之美CIDE符号为语句 in.rshd: allow @/etc/hosts deny 3件。

表23.3列出的通配符可以代替主机名、完全限定域名和IP地址，使用起来很方便。

表23.3 TCP包装器通配符

通配符	应用
ALL	所有计算机，包括localhost
EXCEPT	规则的例外
KNOWN	已知计算机，例如来自DNS或/etc/hosts
LOCAL	具有单个主机名的计算机，这个名称不能带点号
PARANOID	主机名或完全限定域名和IP地址不符的计算机
UNKNOWN	不在/etc/hosts或DNS数据库中的计算机

TCP包装器命令

通常，启动xinetd服务的所有企图都会自动加进/var/log/messages中。可以用spawn命令运行另一个Shell命令。例如，下列命令向指定地址发一个警报电子邮件：

```
in.telnetd: ALL: spawn /bin/mail -s "Telnet security alert" mj@example.com
```

另一个常见用法是向/var/log中的日志文件发一个特殊消息，标识有人试图访问服务的日期和时间。

了解安全Shell

如果担心有人截取你的明文网络通信流，则可以安装安全Shell（SSH）。由于安全Shell可以在任何网络上加密通信，因此可以代替RSH命令和Telnet。

安装SSH

SSH几个组件RPM包，见表23.4。可以用第10章介绍的rpm命令安装所要的包。

表23.4 安全Shell包

包	功能
openssh-*	安全Shell客户机与服务器的核心文件
openssh-askpass-gnome-*	GNOME中支持口令管理的文件
openssh-askpass-*	GUI中支持口令管理的文件
openssh-clients-*	连接安全Shell服务器的客户机文件
openssh-server-*	安全Shell服务器

提示：甚至可以在Microsoft Windows计算机上使用安全Shell，到本书编写时，Open SSH包的自由版本可以从Network Simplicity站点www.networksimplicity.com下载。安装和配置之后，它像Linux版的SSH一样工作。

SSH配置

主要的SSH配置文件是`/etc/ssh/sshd_config`。尽管默认配置文件适合大多数情形，但可以调整特殊TCP/IP端口在这个配置文件中的设置，例如限制对不同IP地址的访问、调整加密密钥长度、覆盖RSH验证和启用Kerberos。

安装相应的软件包之后，下一步要生成公用与专用的加密密钥。专用密钥要放在Linux服务器上安全的地方。公用加密密钥可以让别人加密要发给你的消息。而你要发的消息也可以用专用密钥加密，其中包括公用密钥，让目标计算机解密消息。这些密钥基于非常大的随机数（512位以上），黑客用个人计算机时要几个星期才能攻破。

生成公用与专用加密密钥时有两个基本SSH命令：`ssh-keygen -t rsa`与`ssh-keygen -t dsa`。这些命令可以根据RSA安全公司的算法或数字安全算法生成密钥。

这两个命令默认都在用户主目录的ssh子目录中生成专用与公用密钥，即`~/.ssh`，见表23.5。并提示生成一个口令。如果不设置口令，则黑客可能窃取你的专用密钥。有时黑客可能用你的数字标识使用你的信用卡或用你的名义签合同。

表23.5 默认SSH密钥文件

算法	专用密钥	公用密钥
DSA	<code>~/.ssh/id_dsa</code>	<code>~/.ssh/id_dsa.pub</code>
RSA	<code>~/.ssh/id_rsa</code>	<code>~/.ssh/id_rsa.pub</code>

样本会话

在客户机和服务器上安装正确的RPM包并生成相应SSH密钥之后，就可以开始使用安全shell了。如果需要，可以检查SSH服务器是否运行，只要发出`service sshd status`命令即可。

现在就可以直接连接另一计算机上的账号。例如，假设你是用户**tblair**，在两台计算机

上都有账号，则可以用`ssh sugaree.mommabears.com`命令连接这台计算机，一定要将其换成自己的计算机名或IP地址。

首次用ssh（或相关命令）连接时，可以看到如下消息：

```
The authenticity of host 'sugaree.mommabears.com' can't be
➡ established. RSA key fingerprint is
➡ 34:21:d2:3c:34:83:40:23:d2:c2:9f:34:90:e3:a3. Are
➡ you sure you want to continue connecting (yes/no)?
```

选择Yes，并输入远程计算机上的口令以完成连接，然后即可使用远程计算机，并对两台计算机之间的消息进行加密。也可以登录另一账号（如vputin），如下：

```
# ssh vputin@sugaree.mommabears.com
```

也可以使用与SSH相关联的安全FTP服务。如果用户vputin的账号上有一组RPM，而且你有他的口令，则可以用安全FTP服务从他在远程计算机上的主目录中下载文件。例如，下列命令登录这个账号，然后将新的GNU C语言编译器源代码下载到本地/tmp目录：

```
# sftp vputin@sugaree.mommabears.com
sftp> get gcc-3.9-8.src.rpm /tmp
```

查错访问问题

有了这么多层保护之后，要了解访问问题，就需要进行一定的探测工作。下列步骤适用于用户无法访问计算机上的服务时：

- 保证服务已经安装
- 检查服务是否激活
- 检查与这个服务相关的安全配置文件
- 如果是xinetd服务，则要检查/etc/hosts.allow与/etc/hosts.deny文件
- 用iptables -L命令检查iptables防火墙链

保证安装服务

检查是否安装了服务很简单，第20章曾介绍过，可以用`rpm -q packagename`命令检查安装RPM包与否。

记住，人们通常把服务组织在不同的客户机和服务器的RPM包中。例如，Telnet、FTP与SSH有不同的客户机和服务器RPM包。

检查服务是否激活

使用/etc/rc.d/init.d目录中的脚本很简单。第13章曾介绍过，每个服务监控程序都在这个目录中有一个脚本，可以用`/etc/rc.d/init.d/script status`命令检查。也可以使用`service script status`命令。

如果对一个xinetd服务不确定，则可以检查/etc/xinetd.d目录中的相关配置文件。默认情况下，这些服务设置`disable = yes`，使服务关闭。

还要记住用chkconfig之类工具保证在下次重新启动Linux时激活这个服务。例如，下列命令验证Linux在运行级2、3、5启动时是否激活httpd:

```
# chkconfig --list 235 httpd on
```

xinetd服务的语法稍有不同，因为这些服务在每个激活xinetd的运行级中已经被激活:

```
# chkconfig swat on
```

检查服务特定安全文件

许多服务有自己的配置文件，可以限制或控制访问。Apache与Samba之类的服务可以配置成在主配置文件中限制不同用户与计算机的访问。WU-FTP之类的xinetd服务有自己的配置文件，如/etc/ftpaccess。服务特定安全文件将在每个服务相关的章节详细介绍。

检查扩展xinetd安全文件

我们已经介绍如何通过/etc/hosts.allow与/etc/hosts.deny限制访问。记住，也可以用类似命令通过/etc/xinetd.d配置文件限制访问。

检查防火墙iptables等

可以在Red Hat Linux安装过程中或安装之后配置防火墙。安装之后，可以使用lokkit或redhat-config-securitylevel实用程序。每个Red Hat Linux特定工具都提供了默认高级和中级的安全选项，并可由此得到相同的iptables链。

说明：当然，可以用第22章介绍的方法用自己的iptables命令配置防火墙。

与两个防火墙相关的规则阻止大多数主要TCP/IP端口对计算机的访问。例如，要允许访问计算机上的Apache服务器，可以按第22章介绍的方法设置相应iptables命令，也可以用/etc/services工具将防火墙定制成接受相应TCP/IP端口的数据（这里正确端口为80，可以在/etc/services中查找到不同的TCP/IP端口）。

小结

用户经常要从远程地点取得文件。工程师在手提电脑上的文件可能不是解决客户问题所需的配置文件。Linux提供了一组不同的远程访问服务，其中许多都属于扩展的Internet服务监控程序xinetd。

xinetd监控程序控制服务访问并实时启动不同服务。可以通过/etc/xinetd.conf文件和/etc/xinetd.d目录中的各个服务文件控制服务访问。新的xinetd服务默认关闭，三个主要的xinetd远程访问服务是FTP、Telnet和RSH。

xinetd服务的访问通过TCP包装器控制，其利用/etc/hosts.allow与/etc/hosts.deny中的配置命令。可以对特定服务配置命令，寻找特定计算机或网络。发现匹配时，还可以将这些命令设置成运行shell命令，发送一个警告或将此信息发送到日志文件。

另一个加密远程通信的服务是安全Shell(SSH)。不同的openssh-* RPM包可以用RSA或DSA加密算法加密网络通信。利用这种公用/专用密钥系统时，一定要用口令保护专用密钥。

可以用SSH命令打开远程计算机上的账号，甚至可以安全地连接支持SSH的FTP服务器。

查错远程访问问题是比较难的，因为防火墙多种多样。也许是由于没有安装或激活服务。许多服务有自己的安全相关配置文件，要检查这些配置文件，可以通过/etc/hosts.allow与/etc/hosts.deny保护xinetd服务。当然，也可以用iptables配置防火墙。

第24章将介绍两大Linux服务器及其客户机的详细配置：DNS（域名服务）和DHCP（动态主机配置协议）。

第24章 DNS与DHCP

两个关键的Linux服务可以帮助计算机管理主机名和IP地址。DNS（域名服务）通常配置成主机名或域名与IP地址的数据库。DHCP（动态主机配置协议）可以将IP地址租借给局域网上的不同计算机。和大多数其他Linux服务一样，DNS与DHCP也有客户机和服务器。

Linux DNS服务器基于伯克利因特网名称域（BIND）软件，可以通过/etc与/var/named中的一系列文件进行配置，也称为名称服务器，使用named监控程序。任何配置成使用TCP/IP的Linux计算机默认配置为DNS客户机。查找一个Web站点时，计算机是个DNS客户机，查找DNS服务器中的相关IP地址，就可以知道向Internet上什么地方发消息。

DHCP服务器可以租借IP地址和提供其他关键信息，使计算机可以在局域网上定义自己。DHCP服务器可以配置信息，使计算机可以访问外部网络、寻找其他重要服务器，等等。近年来，Red Hat Linux多次改变DHCP客户机名称，但功能仍然是一样的。它从DHCP服务器取得IP地址，并从DHCP服务器中收集其他重要信息。本章介绍下列主题：

- 配置DNS服务器
- 使用DNS客户机
- 设置DHCP服务器
- 使用DHCP与BOOTP客户机

配置DNS服务器

DNS（域名服务）服务器是灵活的数据库，它包括完全限定域名（FQDN，如www.sybex.com）和IP地址（如63.99.198.12）。Linux DNS基于伯克利因特网名称域（BIND）软件，支持着Internet上的大多数DNS服务器。

一个DNS服务器不可能保存Internet中的所有FQDN与IPv4地址。如果DNS服务器的数据库中沒有FQDN，则可以引用其他DNS服务器。一旦服务器找到正确的IP地址之后，就把FQDN和IP地址加进数据库中。

DNS通过基本配置文件/etc/named.conf与/etc/named.custom配置，也可以通过/var/named目录中的详细配置文件/etc/named.conf与/etc/named.custom配置。最好直接编辑这些文件以配置DNS。

但是，到本书编写时，红帽子公司鼓励用redhat-config-bind配置DNS服务器。配置DNS并不简单，对于经验不多的Linux管理员，redhat-config-bind也许是更好的选项。这个工具要求GNOME与KDE之类的GUI。

包

并不是所有DNS需要的RPM包都默认安装。表24.1列出了所要的RPM包，第10章曾介绍过，可以用rpm -q packagename命令可以检查其是否已经安装。一旦安装了所要的RPM包之后，可以用rpm -ql packagename命令显示相关的文件。

表24.1 DNS所要的RPM包

包	功能
bind-*	DNS名称服务器软件
bind-devel-*	DNS开发工具，不必需
bind-utils-*	dig与host之类的DNS工具
caching-nameserver-*	缓存DNS服务器的基本配置文件，包括样本/etc/named.conf与/var/named/localhost.zone文件
redhat-config-bind-*	红帽子GUI DNS配置工具，是必需的

DNS概念

前面曾介绍过，一个DNS服务器不可能保存Internet中的所有FQDN与IP地址。由于相关数据量很大，因此不可能集中所有的DNS信息。因此，DNS服务器组织成区域。每个DNS服务器有自己的负责区域。DNS服务器基于组织FQDN的方式。

从基本FQDN `www.mommabears.com` 开始，其包括根区域（不是.com，而是.com中点号的右边部分）。

说明 `/etc/named/named.conf` 中列出了DNS信息，而在 `caching-nameserver-*` RPM包中。

然后是.com、.net、.org等，称为顶层域。这里mommabears是.com的子域，www是Momma Bears Web服务器所在的计算机名（或别名）。

mommabears.com网络上的主DNS服务器是这个区域的权威服务器。相反，mommabears.com是这个DNS服务器的转发（或基本）主域。

这些数据库域还要支持逆过程。换句话说，应能从FQDN找到IP地址，也应能从IP地址找到FQDN。逆向数据库称为逆主域。

可以配置四种不同类型的DNS服务器。第21章曾介绍过，所用的任何DNS服务器的IP地址都应在/etc/resolv.conf中列出。

主DNS服务器 主DNS服务器是特定域（如sybex.com）的权威服务器，如sybex.com。从sybex.com网络上的计算机查询IP地址时，通常访问这台服务器。其他DNS服务器从这个主DNS服务器中寻找sybex.com中其他网络与计算机的地址。

从DNS服务器 寻找sybex.com中其他网络与计算机的地址时，也可以查询该DNS服务器，它从主DNS服务器中取得FQDN/IP地址数据库。

缓存DNS服务器 缓存DNS服务器存储最近请求的IP地址。如果局域网中有缓存DNS服务器，而DNS服务器在远程网络上，则计算机可以从缓存DNS服务器迅速取得答案。

转发DNS服务器 转发DNS服务器不存储任何FQDN/IP地址信息，而是在/etc/named.conf中存储其他DNS服务器的IP地址。

初始DNS配置

通常，我鼓励用户在命令行界面中配置Linux服务。如果这样，则可以更了解服务和更好地为网络定制服务。

但是，红帽子公司重新配置DNS配置文件，鼓励用户使用红帽子GUI DNS配置工具redhat-config-bind。即使主DNS配置文件中的简单错误也可能使DNS无法运行。如果你不太熟悉Linux，则可以用redhat-config-bind编辑/etc/named.conf，将这类错误减到最少。如果要进一步定制DNS服务器，则可以在/etc/named.custom文件中增加其他信息。这个格式与第25章介绍的LPD打印机配置文件相似。

提示：不一定要使用redhat-config-bind，也可以直接编辑/etc/named.conf。但后面通过redhat-config-bind进行的任何改变都会覆盖加进/etc/named.conf中的内容。如果喜欢直接编辑/etc/named.conf，则不要安装redhat-config-bind-*RPM包。还可以跳过下面介绍的DNS配置文件的章节。

配置主DNS服务器

要配置主DNS服务器，打开所选GUI，打开文本控制台窗口，并输入redhat-config-bind命令，从而打开图24.1所示的域名服务窗口。首次安装DNS时，惟一的项目是本地计算机中的项目。

说明：也可以在GNOME或KDE中选择Main Menu（或K Menu）►System Settings►Server Settings►Domain Name Service。

配置主DNS服务器时，需要配置/etc/named.conf和/var/named中的各个文件。在域名服务窗口中单击New按钮。在域类型选择窗口中，选择Forward Master Zone选项。输入域名，如果没有，则可以用一般性域名example.com，如图24.2。

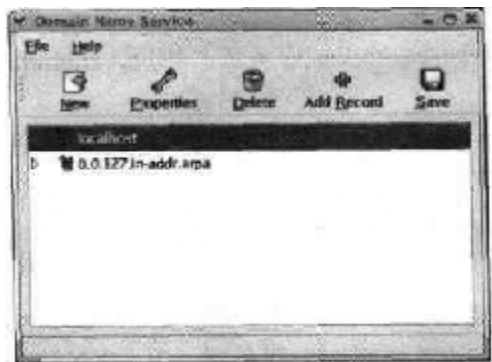


图24.1 域名服务窗口

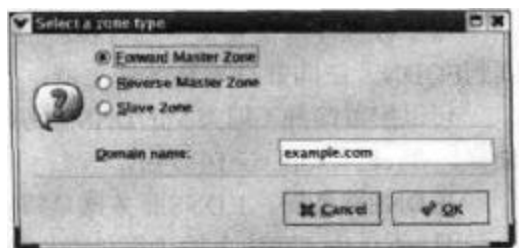


图24.2 域类型选择窗口

单击OK按钮打开名称/IP转换窗口，如图24.3。在这个窗口中，输入主名称服务器（SOA，即DNS服务器）的主机名。记住在主机名后面加上点号。

还要输入DNS服务器的IP地址。单击Add按钮打开增加记录窗口，单击图24.4所示的Nameserver标签。在Domain Name文本框中，输入DNS服务器计算机的主机名，注意完全限定域名的其他部分已经填入。并注意信息已经默认加进逆向地址表中。在Served By文本框中，输入DNS服务器计算机的IP地址。完成之后，两次单击OK，回到域名服务窗口。

现在要增加逆向主域。单击New，这时从域类型选择窗口选择Reverse Master Zone。这时文本框显示“IP Address (first 3 Octets)”。IPv4地址包括四个数，称为四段。例如，如果网络IP地址为10.252.113.0，则在这个文本框中输入10.252.113并单击OK按钮，打开新的IP/名称转换窗口，如图24.5。



图24.3 添加DNS服务器

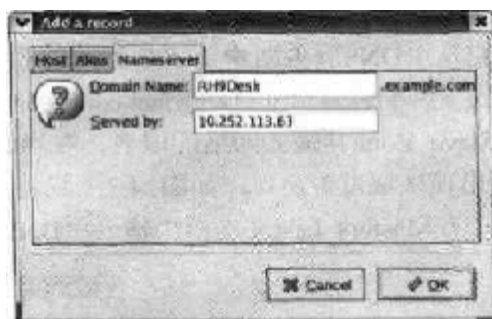


图24.4 添加DNS服务器记录

要重新输入主名称服务器（SOA）信息，还要在Nameserver部分单击Add，至少把这个DNS服务器的IP地址加进表中。单击OK并根据需要重复。

然后在Reverse Address Table部分单击Add（打开新的逆向区指针窗口），如图24.6。在这个窗口中，输入局域网上的计算机IP地址及其主机名或完全限定域名。



图24.5 添加逆向主域

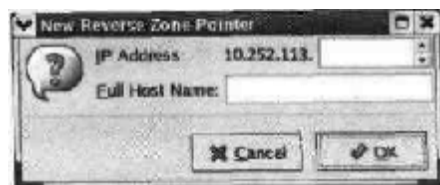


图24.6 添加逆向主域信息

重复这个过程，直到把局域网上的所有计算机加进逆向地址表。记住网络上DNS服务器所在的计算机。单击OK退出IP/名称转换窗口。这样就生成了主DNS服务器。要保存配置，单击Save按钮，即把配置保存在/etc/named.conf和各种/var/named文件中。

现在可以用本章稍后“启动DNS”一节介绍的指令启动DNS，也可以用redhat-config-bind配置从DNS服务器，或直接编辑相应的配置文件，配置所有DNS服务器。

从DNS服务器

也可以用redhat-config-bind生成从DNS服务器。根据定义，从DNS服务器在另一计算机上，它从主DNS服务器中寻找数据库信息。

在另一台计算机上启动redhat-config-bind，单击New，在域类型选择窗口中（如图24.2），选择Slave Zone并输入网络的域名，在当前例子中为example.com。然后单击OK按钮。

出现从域设置窗口，如图24.7。域名和数据库文件名在Name与File Name文本框中自动出现。在Masters List文本框中输入主DNS服务器的IP地址，然后单击Add。



图24.7 从域设置窗口

DNS配置文件

DNS服务器需要几个配置文件：`/etc/named.conf`和`/var/named`目录下的各种数据库文件。可以用redhat-config-bind生成这些配置文件的设置，也可以用文本编辑器直接编辑这些文件。下面详细介绍这些文件。

DNS `/etc/named.conf`

主DNS的配置文件是`/etc/named.conf`。图24.8显示了这个文件工作的例子，它是通过redhat-config-bind建立的。可以在任何文本编辑器中方便地生成这个文件。但是，如果使用redhat-config-bind，则一定要将其他参数加进`/etc/named.custom`中。

可以一条命令一条命令地分解这个文件。首先，下列命令只让本地计算机上的用户用rndc命令维护这个DNS服务器：

```
controls {  
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };  
};
```

说明：大多数管理员用第23章介绍的SSH连接远程DNS服务器。但也可以在`/etc/named.conf`中将controls一行设置成局域网内其他计算机的IP地址与名称。然后可以用rndc（名称服务器控制实用程序），远程管理DNS服务器。


```

# Generated automatically by redhat-config-bind, alchemist et al.
# Any changes not supported by redhat-config-bind should be put
# in /etc/named.custom
#
controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

include "/etc/named.custom";

include "/etc/rndc.key";

zone "0.0.127.in-addr.arpa" {
    type master;
    file "0.0.127.in-addr.arpa.zone";
};
zone "113.252.10.in-addr.arpa" {
    type master;
    file "113.252.10.in-addr.arpa.zone";
};

zone "localhost" {
    type master;
    file "localhost.zone";
};
zone "example.com" {
    type master;
    file "example.com.zone";
};

```

图24-0 /etc/named.conf

然后include指令增加指定文件的内容:

```

include "/etc/named.custom";
include "/etc/rndc.key";

```

选项options指定DNS数据库文件所在的目录,通常是/var/named:

```

options {
    directory "/var/named";
};

```

说明: 如果使用redhat-config-bind, 则options命令在/etc/named.custom文件中。

这个DNS服务器具有基本授权域。Localhost计算机的IP地址为127.0.0.1, 默认为授权域。局域网(这里是example.com)的域是第二个授权域。逆向域(表示为in-addr.arpa语句)也是DNS数据库的重要部分。由于这些是逆向IP地址, 因此0.168.192.in-addr.arpa域基于网址192.168.0.0。

```

zone "0.0.127.in-addr.arpa" {
    type master;
    file "0.0.127.in-addr.arpa.zone"
};
zone "0.168.192.in-addr.arpa" {
    type master;
    file "0.168.192.in-addr.arpa.zone"
};
zone "localhost" {
    type master;

```

```
        file "localhost.zone"
    };
    zone "example.com" {
        type master;
        file "example.com.zone"
    };
```

但这并不包括整个Internet的数据库，一定要让DNS服务器能够访问这个数据库。它在 `caching-nameserver-*` RPM包的 `/var/named/named.ca` 文件中提供。要在 `/etc/named.conf` 配置文件中增加下列段，将其他查询指向Internet的根服务器：

```
zone "." {
    type hint;
    file "named.ca"
};
```

说明：如果使用 `redhat-config-bind`，则这个zone命令在 `/etc/named.custom` 文件中。

如果这是 `example.com` 网络的第二个（从）DNS服务器，则首先要从主DNS服务器取得信息（如果DNS服务器的IP地址不同，则要相应替换）。

```
zone "example.com" {
    type slave;
    file "example.com.zone";
    masters {
        192.168.0.213
    }
};
```

如果这是单向DNS服务器，则对所有域可能看到不同的options语句，其中转发器是其他DNS服务器（可能是ISP）的IP地址：

```
options {
    directory "/var/named";
    forward only;
    forwarders {
        10.11.12.13;
        10.11.12.14;
        10.11.12.15;
    };
};
```

最后，配置缓存DNS，要有 `caching-nameserver-*` RPM包。它所带的 `/etc/named.conf` 版本适合大多数情形。惟一的问题是会不会有防火墙阻止向其他DNS服务器的请求。如果有，则要从这个命令开头删除两个斜杠号，这是说明语句符：

```
// query-source address * port 53
```

第22章曾介绍过，即使默认高度安全Linux iptables防火墙也允许DNS请求通过TCP/IP端口53。如果没有这个命令，则其他DNS服务器的请求可能会被阻止，因为最新的BIND版本通常使用其他端口。

DNS数据库文件

支持DNS服务器的数据库文件默认位于/var/named目录。存储的文件取决于域名、网络IP地址和是否支持普通或缓存DNS服务器。表24.2列出了一些可能看到的文件。

表24.2 /var/named中的DNS数据库文件

文件	功能
0.0.127.in-addr.arpa.zone	指定localhost计算机的逆向域文件
netaddr.in-addr.arpa.zone	指定局域网的逆向域文件，其中netaddr是网址的前三段（倒过来），如192.168.4.0网络的文件为4.168.192.in-addr.arpa.zone
domain.zone	指定局域网的域文件，将domain换成example.com之类的地址
localhost.zone	指定的域文件
named.ca	列出Internet根服务器，来自caching-nameserver-* RPM
named.local	指定PTR，是localhost的逆向域记录

现在看看正向和逆向域数据库文件。图24.9是假想的局域网example.com的域文件。

```

$TTL 86400
@      IN      SOA      RHDDesk. root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )

;
;
;

@      IN      NS       10.252.113.63

RHSLaptop      IN      A       10.252.113.55
RHSTest        IN      A       10.252.113.211
laptop2         IN      A       10.252.113.121
-

```

图24.9 假想的局域网example.com的域文件

可以看出，这个文件中有几个奇怪的命令，实际上把RH9设置为example.com域的名称服务器（ns），网络上还有另外三台计算机。

可以在这个网络中配置另外几种类型的服务器。例如，下列语句设置两个不同的邮件服务器，数值越低，优先级越高：

```

MX      10 mail.example.com ; Primary Email Server
MX      20 mail2.example.com ; Secondary Email Server

```

如果在同一台计算机上配置不同服务器，则要设置别名。例如，下列命令在FTP服务器的同一台计算机上配置新闻服务器和Web服务器：

```

ftp      IN      A       192.168.0.34
www      IN      CNAME   ftp
news     IN      CNAME   ftp

```

表24.3介绍了这个区域文件中的一些命令。

表24.3 DNS区域文件命令

命令	描述
\$TTL	指定这个数据库中的记录删除之前的存活时间（TTL），通常单位为秒，也可以用3D表示三天
@	设置本地计算机的引用
IN	指定Internet类数据
SOA	开始授权，指定这个域的DNS服务器
root.localhost	包含这个DNS的管理员电子邮件地址，也指root@localhost
serial	指定与这个文件相关联的序列号，改变DNS配置时应当将其更新，否则其他DNS服务器可能忘记你的DNS服务器存在
refresh	指定这个区域主DNS服务器两次检查之间的时间间隔（秒数）
retry	设置第一次连接失败时重新连接DNS服务器的时间间隔。如果刷新时无法访问DNS服务器，则经过这么多秒之后再重试
expire	指定保持时间。如果更新与重试都已访问DNS服务器，则经过这么多秒之后停止该区域的活动
ttl	设置该DNS服务器中各个记录的存活时间
NS	指定名称服务器（即DNS服务器）名称
A	包含这个主机名与IP地址的地址记录
CNAME	指定规范名称，是不同主机名的别名
MX	指定邮件服务器
PTR	包含逆向域文件中的指针（或逆向记录）

下面看看图24.10的逆向域文件。可以看出，其中包含与普通DNS数据库文件相同的基本命令。PTR记录看上去有点怪。

为了寻找IP地址，需要PTR记录号和文件名。例如，第一个PTR记录号从编号121开始，完全限定域名为laptop2.example.com。与文件名113.252.10.in-addr.arpa.zone相关联时，表示laptop2.example.com的IP地址为10.242.113.121。

启动DNS

配置DNS之后，要试验新服务器。最简单的方法是在Red Hat Linux中使用DNS服务脚本。记住，named是运行Linux DNS服务器的监控程序：

```
# service named start
```

然后要看看它是否工作。第21章曾介绍过，DNS服务器的IP地址通常在/etc/resolv.conf中列出。启动名称服务器之后，可以看到它如何工作。试用dig命令（DNS查找实用程序）查找Internet上特定的完全限定域名。

```

$TTL 86400
@      IN      SOA      RH9Desk.example.com.  root.localhost (
                        3 : serial
                        28800 : refresh
                        7200 : retry
                        604800 : expire
                        86400 : ttl
                        )

@      IN      NS       10.252.113.63.

121    IN      PTR      laptop2.example.com.
122    IN      PTR      laptop3.example.com.
63     IN      PTR      RH9Desk.example.com.
-
-
-
-
-
-

```

图24.10 逆向域文件

图24.11显示了其如何工作。注意下方的SERVER行，表示其来自本地网络上的DNS服务器，IP地址为10.252.113.63。

```

[root@RH9Desk root]# dig www.monmabears.com

; <> DiG 9.2.1 <> www.monmabears.com
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 64701
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;www.monmabears.com.                IN      A

;; ANSWER SECTION:
www.monmabears.com.                1685    IN      A      58.36.97.32

;; AUTHORITY SECTION:
monmabears.com.                    1685    IN      NS      ns9.hosting4u.net.
monmabears.com.                    1685    IN      NS      ns.hosting4u.net.
monmabears.com.                    1685    IN      NS      ns2.hosting4u.net.

;; Query time: 282 msec
;; SERVER: 10.252.113.63#53(10.252.113.63)
;; WHEN: Mon Mar 3 18:03:29 2009
;; MSG SIZE rcvd: 118

[root@RH9Desk root]#

```

图24.11 dig命令

如果对结果表示满意，则要保证下次重新启动Linux时启动named监控程序。用chkconfig --level 235 named命令保证这个监控程序在运行级2、3、5中启动。

提示：引导过程中启动DNS时，还可以在/var/log/messages文件中检查启动消息。如果遇到问题，如/etc/named.custom中发生语法错误，则可以在这里看到消息。

使用DNS客户机

如果将计算机配置成在Internet上通信，则已经将其设置成了DNS客户机。访问其他计算机时，要查找主机名和IP地址数据库。

第21章曾介绍过，有两个主机名和IP地址数据库：`/etc/hosts`和DNS中列出的DNS服务器。计算机搜索的数据库及其搜索顺序由`/etc/host.conf`文件确定，其通常包括一行：`order hosts,bind`。即计算机首先在`/etc/hosts`中寻找IP地址，然后搜索DNS中列出的DNS服务器，可以按第21章介绍的指令进行配置。

不需要其他配置。

设置DHCP服务器

DHCP（动态主机配置协议）可以自动向网络上所有的TCP/IP计算机提供通信所需的信息，包括路由器、DNS服务器、其他名称类型服务器和基本IP地址信息。

要设置DHCP服务器，就要保证网卡能够处理多目广播请求。如果使用旧式Microsoft Windows计算机，则还要来广播地址设置为专用IP。然后可以配置DHCP配置文件：`/etc/dhcpd.conf`。如果要对远程网络使用这个DHCP服务器，则还要在局域网之间的路由器/网关上配置`dhcrelay`。`dhcrelay`监控程序支持BOOTP协议。但首先看看需要的RPM包。

包

DHCP所要的RPM包并没有全部默认安装。表24.4列出了所要的RPM包，第10章曾介绍过，可以用`rpm -q packagename`命令检查其是否已经安装。一旦安装所要的RPM包之后，可以用`rpm -ql packagename`命令显示相关的文件。

表24.1 DHCP所要的RPM包

包	功能
dhcp-*	DHCP服务器软件
dhcp-devel-*	DHCP开发工具，不必需
dhclient-*	DHCP客户机软件

基本配置

Linux计算机配置成DHCP服务器时要求网卡能够处理多目广播请求，并要求启用全部为1的广播地址。

也许网卡与内核已经支持多目广播，可以用`ifconfig`命令检查，看看网卡的输出。在相关IP地址下面，可以看到下列内容：

```
UP BROADCAST RUNNING MULTICAST MTU:1500 METRIC:1
```

如果这一行中没有看到MULTICAST，则要在内核中重新配置多目广播支持。详见第12章。

可能还要配置广播地址的路由255.255.255.255。Microsoft Windows 95之类旧式客户机要监听这个广播地址，否则它们不知道DHCP服务器的存在。如果DHCP服务器要为网络上的旧式客户机服务，则要运行下列命令：

```
# route add -host 255.255.255.255 dev eth0
```

配置文件：/etc/dhcpd.conf

现在可以配置DHCP服务器主配置文件：/etc/dhcpd.conf。我们从dhcp-* RPM中的样本文件——/usr/share/doc/dhcp-versnum目录中的dhcp.conf.sample开始。这个样本列出几个IP地址，可能需根据你的网络做出相应改变。

要对DHCP服务器有更多了解，最好详细分析这个文件。下面是样本文件的摘要。第一行使动态DNS可以更新到最新的“临时”标准。这里显示了几个IP地址。如果你的网络使用不同IP地址，则需要相应改变：

```
ddns-update-style interim;
```

也许你不想让各个用户更新DNS服务器中的主机名或IP地址项目，因此要使用下列命令：

```
ignore client-updates;
```

也可以用命令allow client-updates允许用户更新DNS服务器中的主机名或IP地址项目。

下一行设置允许IP地址的默认范围。其中有些地址会在后面的命令中为特定计算机保留：

```
subnet 192.168.0.0 netmask 255.255.255.0 {
```

如果你的局域网连接另一个局域网，则在连接两个局域网的路由器上需要有个网关IP地址。下列命令指定网关IP地址：

```
option routers 192.168.0.1;
```

下列命令很简单，指定子网掩码，也称网络掩码：

```
option subnet-mask 255.255.255.0;
```

如果对网络配置NIS权威数据库，则可以指定这个域（代替下面这个命令中的domain.org）。关于NIS的更多信息见第28章。

```
option nis-domain "domain.org";
```

自然，网络可能还有个域名。根据本章介绍的例子，可能是example.com。在这个命令中，用域名代替这个命令中的domain.org：

```
option domain-name "domain.org";
```

如果局域网中设置了DNS服务器，则要在这里列出其地址。它可以帮助这个DHCP服务器寻找你的DNS服务器，并在必要时进行更新。可以用类似语句标识入站与出站的电子邮件服务器（option pop-server或smtp-server）、Web服务器（option www-server）或日志文件专用服务器（option log-server）：

```
option domain-name-servers 192.168.1.1;
```

下一条语句帮助网络保持同步。时间单位为秒，相对于GMT（格林威治标准时间）。换句话说，美国东部标准时间为比GMT晚18000秒或5小时。如果在其他时区，也应换成相应值。

```
option time-offset -18000; # Eastern Standard Time
```

有些计算机时钟比较快。电池电力不足时，计算机时钟会减慢。如果同一进程（如Web服务器）由几台计算机运行，则一定要同步这些计算机时钟。为此可以使用NTP（网络时间协议）服务器，已经在第19章用redhat-config-time实用程序配置。这个语句可以调用所选的NTP服务器：

```
option ntp-servers 192.168.1.1;
```

有些Linux计算机配置成Microsoft Windows网络的成员。不同计算机的Microsoft名称服务之一基于NetBIOS名称，称为Windows Internet名称服务（WINS）：

```
option netbios-name-servers 192.168.1.1;
```

可以将DHCP服务器配置成“p节点”计算机，换句话说，它从WINS服务器和LMHOSTS文件寻找名称解析：

```
option netbios-name-type 2;
```

可以配置这个DHCP服务器可以对远程网络上的计算机分配的IP地址范围。这些地址应在定义的网址范围中。

```
range dynamic-bootp 192.168.0.128 192.168.0.254
```

DHCP服务器临时分配IP地址。更新IP地址的第一个时间是default-lease-time（秒）：

```
default-lease-time 21600
```

IP地址必须更新的时间为max-lease-time（秒）：

```
max-lease-time 43200
```

可以根据特定计算机网卡的硬件地址分配固定IP地址。这里next-server变量指可替换的DNS服务器（host ns）：

```
host ns {
    next-server marvin.redhat.com
    hardware ethernet 12:23:34:45:AB:CD
    fixed-address 207.175.42.254
}
```

对局域网定制这个文件之后，将其保存在/etc/dhcpd.conf中。

启动DHCP服务器

要运行Linux DHCP服务器，需要一个已经有IP地址的网卡，如果需要，可以用ifconfig命令分配IP地址，见第21章介绍。

启动DHCP服务器很容易，只要用service dhcpd start之类的命令运行dhcpd脚本。记住要用chkconfig之类的命令保证下次启动Linux时启动DHCP服务器。

DHCP服务器与远程网络

将DHCP服务器配置成对远程网络保留的一系列IP地址时（见上节的range dynamic-bootp变量），DHCP服务器需要帮助。通常，网络之间的网关或路由器会阻止DHCP消息，这时要实现BOOTP协议，在网关或路由器上打开一条通道，让DHCP在局域网之间通信。

要设置BOOTP，在网关或路由器上安装来自dhcp-* RPM包的dhcrelay监控程序。然后可以在/etc/sysconfig/dhcrelay配置文件中配置命令选项。例如，这个文件中的下列命令使dhcrelay可以监听网卡eth0与eth1。DHCPSEVERs至少要连接其中一个网卡。然后可以指定需要连接远程DHCP服务的网络的任何网卡。

```
INTERFACES="eth0 eth1"
DHCPSEVERs="192.168.0.213"
```

记住启动dhcrelay脚本并且用chkconfig保证下次启动Linux时激活dhcrelay。

提示：一个常见的错误是只指定需要连接远程DHCP服务的局域网的网络适配器。记住要包括连接DHCP服务器所在局域网的适配器。

租借数据库

网络上的计算机开始从DHCP服务器取得地址信息后，结果会在/var/lib/dhcp/dhcpd.leases中建档。图24.12显示了这个文件的一个例子，其中显示对局域网上不同网卡的硬件地址分配的IP地址。

```
# All times in this file are in UTC (GMT), not your local timezone.  This is
# not a bug, so please don't ask about it.  There is no portable way to
# store leases in the local timezone, so please don't request this as a
# feature.  If this is inconvenient or confusing to you, we sincerely
# apologize.  Seriously, though - don't ask.
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-v3.0pl1

lease 192.168.0.254 {
    starts 1 2002/10/14 14:35:09;
    ends 1 2002/10/14 20:35:09;
    binding state active;
    next binding state free;
    hardware ethernet 00:60:08:8d:41:93;
}
lease 192.168.0.253 {
    starts 1 2002/10/14 14:37:59;
    ends 1 2002/10/14 20:37:59;
    binding state active;
    next binding state free;
    hardware ethernet 00:10:b5:64:3b:b2;
}
~
```

图24.12 /var/lib/dhcp/dhcpd.leases

使用DHCP与BOOTP客户机

配置DHCP客户机很简单。配置完网络之后，要让网卡的启动脚本查找DHCP服务器。配置完成之后，计算机下次启动时会广播一个寻找DHCP服务器的请求。

自然, 要保证启用网络。检查/etc/sysconfig/network文件, 其中应包括下列项目:

```
NETWORKING=yes
```

现在修改网卡配置文件, 通常在/etc/sysconfig/network-scripts目录中。如果网卡为eth0, 则文件名为ifcfg-eth0, 文件中应包括下列项目:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

BOOTPROTO变量有两个替换值: bootp与dialup。这些替换值很容易理解, 前者表示DHCP服务器在远程网络上, 后者为拨号连接配置设备, 如连接Internet上的ISP。

改变配置文件之后, 要将计算机作为新DHCP客户机启动, 最简单的方法是使用dhclient命令, 结果如图24.13所示。

```
[root@RH9Test root]# dhclient
Internet Software Consortium DHCP Client V3.0p11
Copyright 1985-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP

Listening on PF/eth1/00:10:b5:64:3b:b2
Sending on PF/eth1/00:10:b5:64:3b:b2
Listening on PF/lo/
Sending on PF/lo/
Listening on LPF/eth0/00:40:f4:3c:05:58
Sending on LPF/eth0/00:40:f4:3c:05:58
Sending on Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 7
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
DHCPOFFER from 10.252.113.113
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 10.252.113.113
bound to 10.252.113.3 -- renewal in 125720 seconds.
[root@RH9Test root]#
```

图24.13 租借IP地址

说明: 红帽子公司近年来多次改变DHCP客户机名称, 曾经用过的名称包括dhcpcd与pump。

小结

两个关键服务可以帮助Linux计算机在Internet之类TCP/IP网络上通信: DNS与DHCP。本章介绍如何对这两个服务配置客户机与服务器。

DNS服务器是完全限定域名与IP地址的数据库, 可以配置主、从、缓存和转发DNS服务器。红帽子公司鼓励用redhat-config-bind配置主DNS配置文件/etc/named.conf和/var/named中的几个文件。如果使用这个工具, 则需要在/etc/named.custom中增加特殊配置选项。配置DNS服务器之后, 可以启动named监控程序, 控制DNS, 所用命令为service named start。

一般来说, 设置DNS客户机时不需要特殊配置。通常, DNS客户机先搜索/etc/hosts, 之后再转入/etc/resolv.conf中指定的DNS服务器。

DHCP可以管理网络上的IP地址。还可以在/etc/dhcpd.conf配置文件中设置其他基本网络信息, 如网关、DNS服务器、NIS服务器和SMTP服务器。只要DHCP服务器具有带IP地址的

网卡，就可以用`service named dhcpd`命令启动它。可以用`dhcrelay`监控程序将网关计算机配置成在网络之间传输DHCP消息。设置DHCP服务器之后，可以用`dhclient`命令租借地址。租借地址存放在`/var/lib/dhcp/dhcpd.leases`数据库中。

配置DHCP客户机很简单，关键文件是`/etc/sysconfig/network-scripts`目录中网卡的配置文件。如果局域网中有DHCP服务器，则可以用`dhclient`命令立即取得其IP地址消息。

下一章介绍Linux中的两大打印系统：**CUPS**（公共UNIX打印系统）和**LPD**（行打印监控程序）。

第25章 用CUPS与LPD打印

安装Red Hat Linux时，它并不自动探测打印机，因此所有的管理员都要知道关于打印机配置的一些细节。

Red Hat Linux有两大打印系统：CUPS（公共UNIX打印系统）和LPD（行打印监控程序），前者是目前默认的打印服务，后者是Red Hat 8.0以前的默认打印服务。红帽子所带的软件可以在CUPS系统中使用LPD命令与应用程序。

CUPS基于Internet打印协议（IPP）1.1版，管理员可以将网络打印机组织成组。CUPS把打印机组称为类。CUPS包括Web配置界面，也可以应用于单个本地计算机。

也可以通过Web界面组织大量打印机，但为了理解网络的含义，需要理解相关配置文件的内容。`/etc/cups`配置文件中的语言看起来比较怪，但与第30章介绍的Apache Web服务器配置文件语言非常相似。

相反，LPD来自BSD操作系统，适合小型网络上的单台打印机。红帽子公司已经让LPD过时，即今后的Red Hat Linux版本中可能将其删除。

说明：BSD操作系统也称为伯克利标准发行版本。和Linux一样，它也是UNIX的先驱。

利用CUPS，没必要放弃LPD中建立的任何应用程序。如果你熟悉LPD，则仍然可以使用CUPS。它的xinetd服务可以使用lpr、lpq之类的标准LPD命令。选择所要的打印服务器之后，要安装并激活相应的软件包。如果选择CUPS作为打印监控程序，则可以对需要LPD式命令的应用程序激活cups-lpd监控程序。本章介绍下列主题：

- 使用IPP（Internet打印协议）
- 配置CUPS（公共UNIX打印系统）
- 配置LPD（行打印监控程序）

使用IPP（Internet打印协议）

过去，UNIX与Linux之类的联盟系统在处理打印机界面时不太一致。AT&T公司、惠普公司和Sun公司等都建立自己的UNIX版本，因此也建立了专属的打印机界面。尽管Linux能够很好地适应LPD包，但新的行业标准基于IPP（Internet打印协议）。

CUPS是Linux与UNIX中使用IPP的方式。IPP是Novell公司与Xerox公司开发的，有四大目标：

- 帮助用户寻找网络上可用的打印机
- 将打印作业发送到IPP配置打印机
- 读取打印作业状态
- 取消打印作业

CUPS可以将打印作业发送到特定URI，如parallel:/dev/lp0。

说明：URI是统一资源标识符，URL（统一资源定位器）是URI的子集。众所周知，Web浏览器中用URL指向ftp://ftp.redhat.com与http://www.sybex.com之类的站点。URI可以指向更多内容，如mailto:abc@def.ghi、smb://comp1/printername或parallel:/dev/lp1。

CUPS以几种不同方式实现IPP（Internet打印协议）。表25.1所列的几个标准也许是LPD用户比较熟悉的。这里显示的标准操作并不全面，更详细的信息见CUPS开发商Easy Software Products公司的站点www.easysw.com。

表25.1 CUPS功能

操作	描述
Print	将文件发送到特定URI的打印机
Validate	保证作业有正确优先级、打印机，等等
Create	设置空打印作业
Send	将文件作为打印作业发去处理
Cancel	取消打印作业
Pause	停止打印机操作
Resume	恢复打印机操作
Purge	从打印机假脱机文件中清除作业

此外，CUPS还有一些位于标准LPD系统之上的管理功能。表25.2列出了其中一些功能。同样，这并不是一个完整的列表。

表25.2 特殊CUPS功能

操作	描述
CUPS-Get-Default	寻找默认打印机的URI
CUPS-Get-Printers	寻找CUPS在网络上配置的所有打印机的URI
CUPS-Add-Modify-Printers	通过CUPS增加或修改打印机
CUPS-Delete-Printer	从CUPS类中删除打印机
CUPS-Get-Classes	寻找每个CUPS类中的打印机类型
CUPS-Add-Modify-Class	增加新打印机类型或修改现有打印机类型
CUPS-Delete-Class	删除现有CUPS打印机类型
CUPS-Accept-Jobs	设置特定打印机或打印机类型以开始接受打印作业
CUPS-Reject-Jobs	设置特定打印机或打印机类型以开始拒绝打印作业

有了这些基本概念之后，下面介绍如何在计算机和网络上配置CUPS。

配置CUPS（公共UNIX打印系统）

许多情况下，CUPS（公共UNIX打印系统）很容易配置。由于CUPS是默认的，只要安装了正确的包，则计算机上可能已经激活CUPS。CUPS打印机上可以使用许多LPD命令，只要激活xinetd管理的监控程序cups-lpd即可。

可以通过TCP/IP端口631上的Web界面配置许多CUPS打印机，这个端口是IPP的通信信道。但是，如果配置一组CUPS打印机，则要知道如何直接编辑/etc/cups目录中的CUPS配置文件。

检查当前CUPS RPM包，如果还没有安装，则要安装这些包。表25.3列出了CUPS RPM包。

表25.3 CUPS RPM包

包	描述
cups-*	主CUPS包，包括基本命令和默认配置文件
cups-libs-*	这个包可以用access CUPS命令，而不必用lpr之类的LPD命令
cups-devel-*	CUPS开发库
cups-drivers-*	CUPS打印机的驱动器，可能要从www.rpmfind.net之类的第三方源下载这些包，redhat-config-printer-*包和命令提供了许多打印机驱动器
foomatic-*	独立于假脱机程序的打印机数据库，支持redhat-config-printer
hpijs-*	针对惠普打印机优化的打印机驱动器

卜节开始Web界面，然后详细介绍/etc/cups中的每个配置文件。最后，我们要介绍一些基本CUPS命令以及使用LPD命令的cups-lpd服务。

说明：CUPS文件、监控程序和脚本的名称比较古怪。CUPS监控程序是cupsd，在/usr/sbin目录中。但Red Hat Linux可以用/etc/rc.d/init.d目录中的cups脚本启动和停止CUPS。最后，主CUPS配置文件为cupsd.conf，在/etc/cups目录中。

图形配置

可以在所选Web浏览器中设置CUPS打印机。也许CUPS RPM包已经安装，cups监控程序已经激活。这样，只要在TCP/IP端口631打开所选的本地浏览器。

说明：可以从远程计算机上的Web浏览器中运行CUPS配置程序。但这要求这两台计算机之间没有防火墙，至少不能阻止端口631。尽管我们不鼓励采用这个做法，但如果你在通过防火墙与外部网络分开的局域网中，则这个风险是可以接受的。

升级：从LPD到CUPS

如果你使用Red Hat 8.0或更早的版本，则默认打印服务器可能是LPD。如果升级到Red Hat 9，则它不会自动改变打印服务器，计算机上仍然激活LPD。

假设要升级到CUPS，则要保证启动Linux时不再激活lpd监控程序，然后保证在相应运行级中激活cupsd监控程序（在/usr/sbin目录中）。可以使用下列命令：

```
# chkconfig --level 2345 lpd off
# chkconfig --level 2345 cups on
```

实际使用cups打印机之前，要运行redhat-switch-printer，以便从LPD切换到CUPS（LPD的包名为LPRng，即下一代行打印请求）。

自然，如果刚刚安装Red Hat Linux 9。要使用LPD，则可以将这个过程倒过来。

打开所选的浏览器，指向http://localhost:631。图25.1显示了Mozilla Web浏览器中的结果。

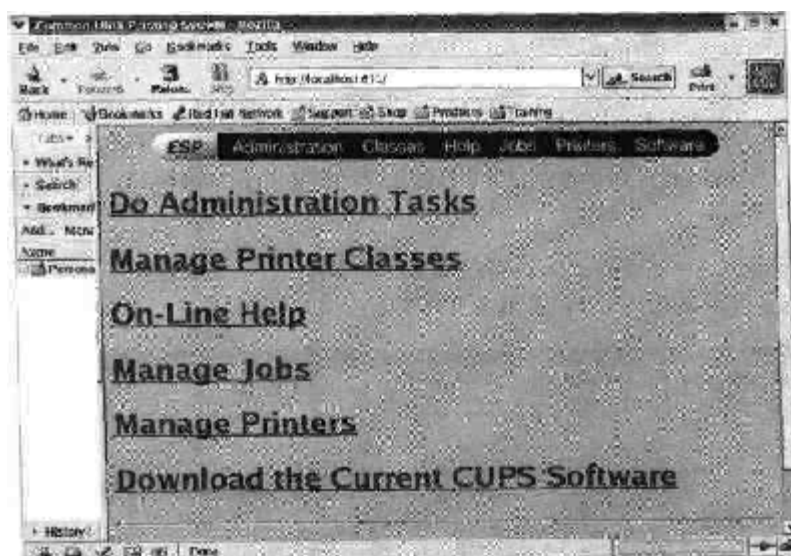


图25.1 CUPS打印机配置器

提示：浏览器窗口可能有以下消息：“The connection was refused when attempting to contact servername.631”。这行说明没有安装CUPS或防火墙阻止了对631的访问。

可以看到，有六个不同命令选项，Web页面上方的ESP链接指向CUPS的开发人员，即Easy Software Products公司的站点www.easysw.com。其他选项很简单，见表25.4。

表25.4 CUPS配置菜单选项

选项	描述
ESP	导航到www.easysw.com
Administration: Do Administration Tasks	可以增加或管理打印机、类和打印作业
Classes: Manage Printer Classes	可以增加或管理打印机组，作为类
Help: On-Line Help	包括与CUPS相关的HTML与PDF手册
Jobs: Manage Jobs	可以管理CUPS系统中的当前打印作业
Printers: Manage Printers	可以增加或管理各个打印机
Software: Download The Current CUPS Software	导航到www.cups.org，可以取得最新CUPS包

由于Administration链接提供全方位的配置界面，因此我们可以按相反的顺序介绍这些选项（除ESP以外）。

提示：继续学习之前，先备份/etc/cups目录中的文件，本章稍后要使用这些文件的原有格式。

可以用本章稍后介绍的redhat-config-printer工具配置或编辑所选的打印机。它适用于CUPS与LPD，只要激活一个监控程序（而不同时激活两个监控程序）。它在Red Hat的Printer GUI Tool部分。

提示: redhat-config-printer工具可以方便地访问针对厂家和机型定制的各种打印驱动器。

下载CUPS

如果要下载CUPS的最新版本,则可以从CUPS Web站点www.cups.org下载,如图25.2。到本书编写时, www.cups.org站点的可下载版本只提供tarball格式,可能没有对Red Hat Linux定制。

说明: www.cups.org站点由Easy Software Products公司维护,其主页为www.easysw.com。但要记住,CUPS是开放源代码软件,采用通用许可证(GPL)。

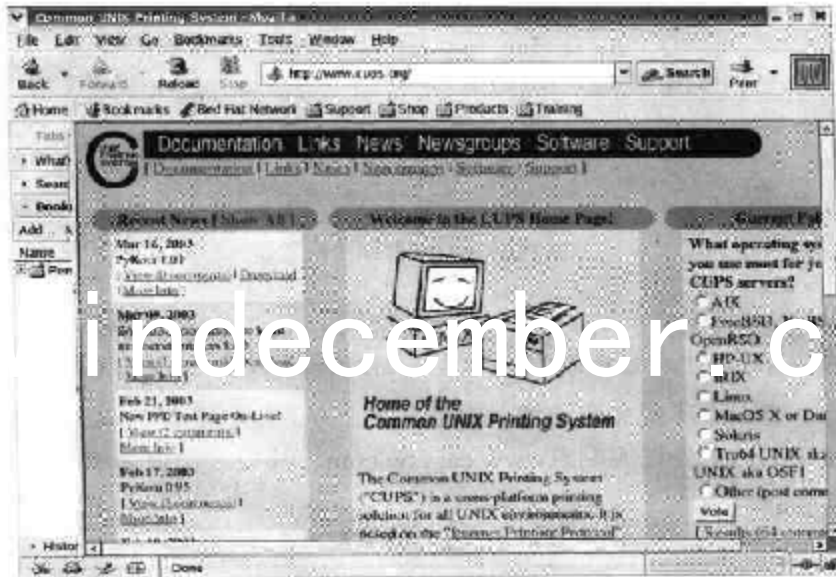


图25.2 CUPS主页

因此,通常最好从红帽子FTP服务器上下载CUPS的最新版本。第10章曾介绍过,获得最新的红帽子定制CUPS软件有两个基本路径:从Rawhide目录下载,或用up2date实用程序更新。

管理打印机

这时单击Printers或Manage Printers链接,CUPS配置工具打开当前配置的打印机清单。单击Add Printer。即使以根用户身份登录,CUPS也会提示输入管理账号,如图25.3。

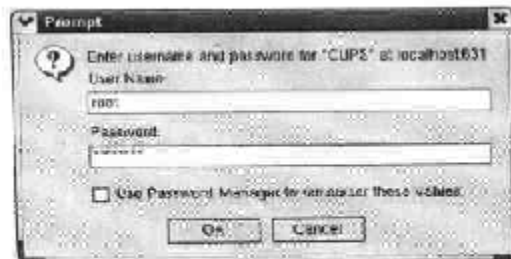


图25.3 授权访问

输入相应用户名（通常是根）和口令之后，进入图25.4所示的增加新打印机界面。

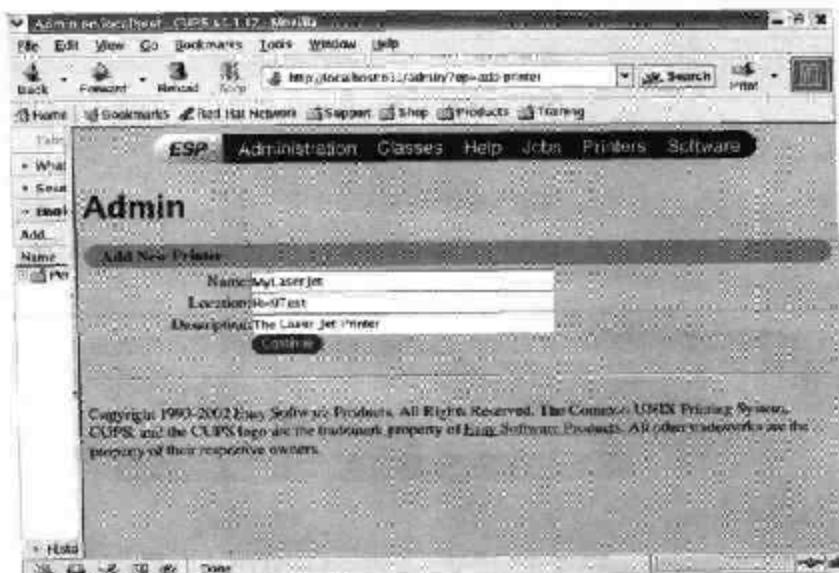


图25.4 添加新打印机界面

在这个界面中，要输入打印机名称、地址与描述，如表25.5。

表25.5 增加新打印机

项目	描述
Name	打印机的基本名，如MyLaserJet与HPLaserJet
Location	打印机相关的主机名或域名，如RH8 ₁ Test或 HPLaser.mommabears.com
Description	所选描述名，可以包括打印机的物理地址

输入之后，单击Continue按钮移到下一步。

指定打印设备

从图25.5可以看出，打印设备有多种。CUPS可以管理连接在不同物理端口和打印服务器的打印机，表25.6列出了其中一些选项。

表25.6 CUPS打印设备类型

打印设备	描述
AppSocket/HP JetDirect	连接惠普JetDirect打印服务器的打印机
Internet Printing Protocol (http)	如果将CUPS设置成在端口80通信，则可以将打印机地址设置为 <code>http://printername</code>
Internet Printing Protocol (ipp)	通常，CUPS使用IPP端口631，对应于URI <code>ipp://printername</code>
LPD/LPR Host Or Printer	通过LPD打印服务器管理的打印机

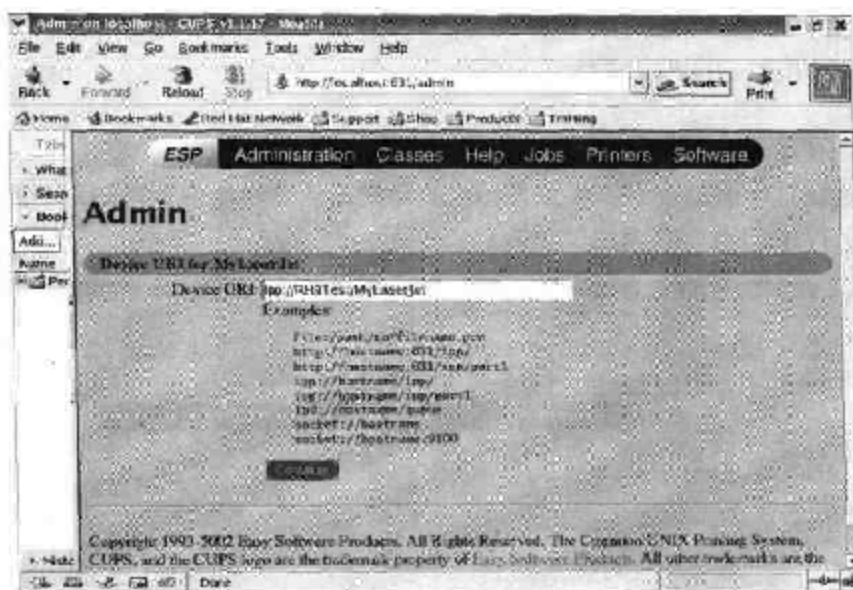


图25.6 设置打印机URI

选择打印机型

选择打印机型很简单，就是告诉CUPS打印机要用哪个打印过滤器。本节要选择打印机品牌，如图25.7。如果没有看到打印机的品牌，则可能是PostScript打印机。也许你的打印机不需要过滤器，换句话说，它可以处理“原始”输出。这里也可以使用Raw和PostScript选项。

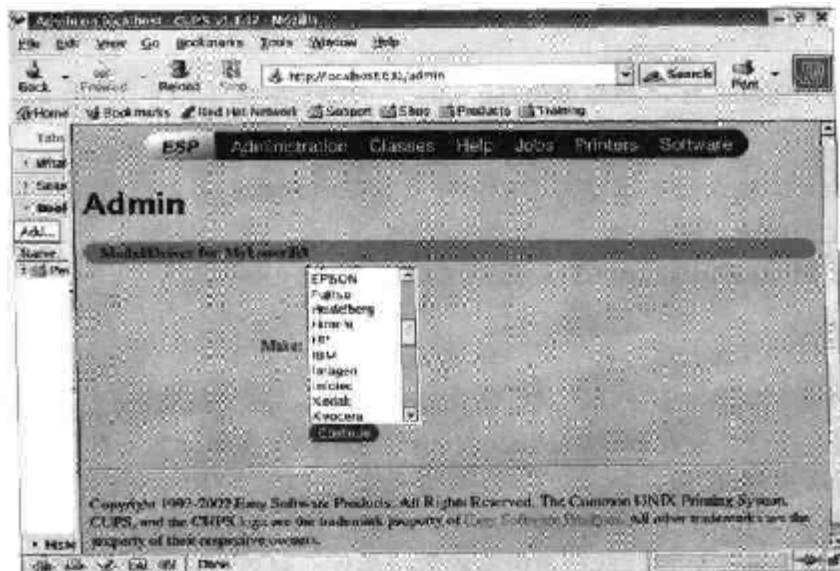


图25.7 选择打印机型

如果只看到少量打印机型和驱动器，则可能是红帽子公司更希望通过redhat-config-printer进行配置。有大量打印驱动器，放在foomatic-* RPM包中。其他Linux发行版本在cups-

drivers-* RPM包中包括了其他打印驱动器。这个RPM也在Red Hat 8.0中提供。选择了打印机型，然后单击Continue按钮移到下一步。

选择打印驱动程序

现在要选择打印驱动程序。根据打印机的品牌，选项可能很多，如果图25.8中看到打印机有多个驱动程序，则可以采用试错方法。

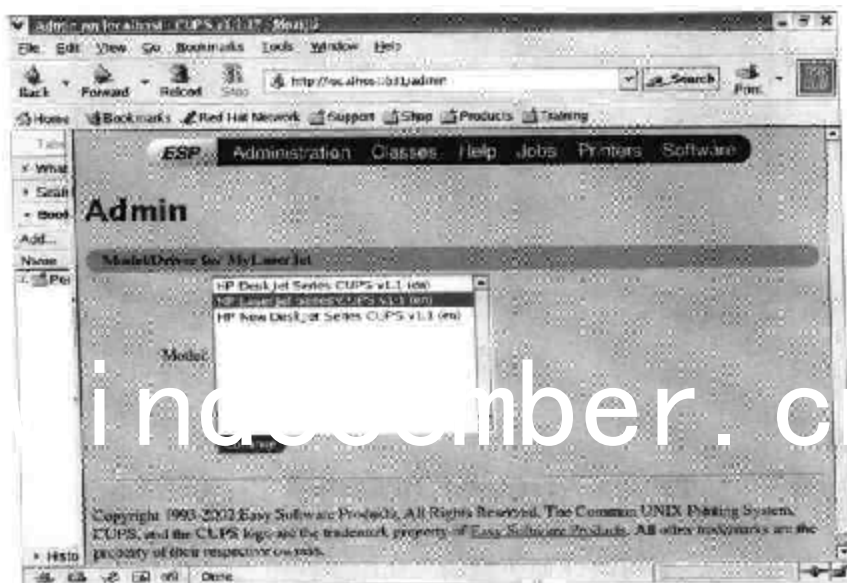


图25.8 选择打印驱动器

选择打印驱动程序，然后单击Continue，可以看到如下消息：

Printer MyLaserJet has been added successfully.

设置的打印机名成为浏览器中的链接（显示下划线）。可以单击这个链接，检查新配置的CUPS打印机的当前状态。

现在移到<http://localhost:631>，返回主CUPS菜单。

管理作业

检查当前打印作业队列很简单。单击Jobs或Manage Jobs链接，可以看到当前打印作业的队列清单。这些作业存放在/var/spool/cups目录下的文件中。如果有等待的作业，则会以图25.9所示的格式显示。

从图中可以看出，很容易保持或取消等待的作业。任何保持的作业放在/var/spool/cups中，其他作业先进行处理。然后可以在需要时将作业释放到队列中。单击相关ID可以显示每个作业的细节。

一个重要的CUPS特性是已完成作业的记录。单击Show Completed Jobs按钮可以检查已完成作业的记录，类似于图25.10。可以用这个特性监视打印机活动，看看是否有已完成的打印作业。

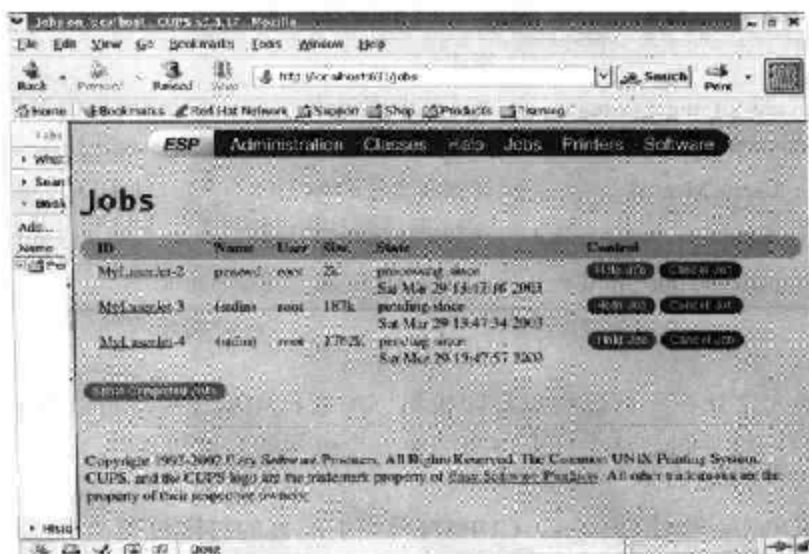


图25.9 等待的作业

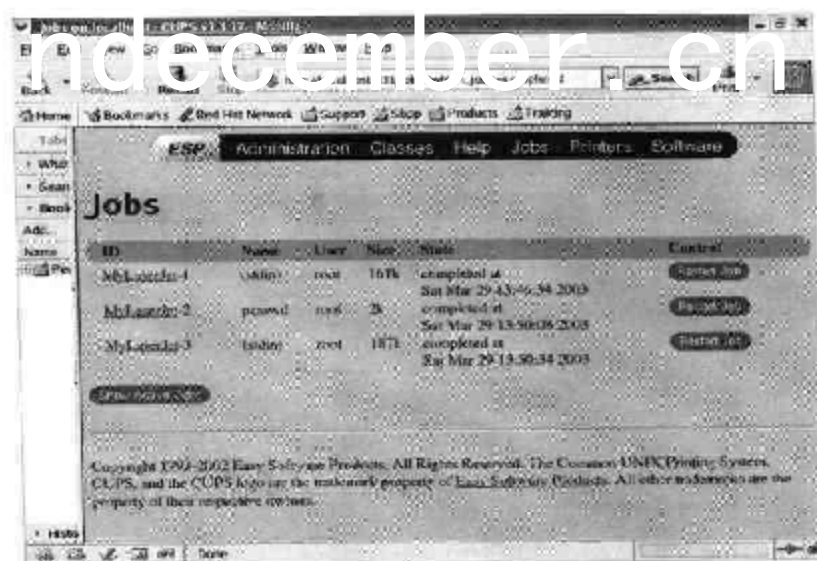


图25.10 CUPS已完成作业的记录

提示：如果从CUPS配置打印机打印时遇到问题，则可能是不小心切换成LPD了。

访问联机帮助

CUPS联机帮助很丰富。只要单击Help或On-Line Help链接即可打开本地计算机上cups-* RPM包安装的CUPS文档。简单地说，它们包括表25.7所示的文档。其他手册是CUPS开发人员使用的。

现在转移到<http://localhost:631>，返回主CUPS菜单。

表25.7 CUPS联机帮助

文档	描述
An overview of the Common UNIX Printing System	描述CUPS的基本结构、如何使用IPP 1.1及其与LPD命令的兼容性
Software Users Manual	详细描述用正确CUPS命令定制打印的方法
Software Administrators Manual	详细描述CUPS安装和/etc/cups配置文件的语言
CUPS Implementation of IPP	比较CUPS的功能与IPP的要求

管理打印机类

CUPS的强大之处在于可以组织打印机组。配置打印机之后，可以将其组成CUPS类。向一个类发送打印作业时，这个作业由类中第一个可用的打印机处理。用户不再需要等待可用打印机。

在CUPS菜单中，单击Classes。CUPS打开当前配置的打印机类清单。单击Add Class打开增加新类屏幕，如图25.11。这里新类名为HPLasers，不同于现有打印机名。Location与Description字段与增加新CUPS打印机时相同，前者对应于打印服务器相关的主机名或域名，后者描述新的打印机类。

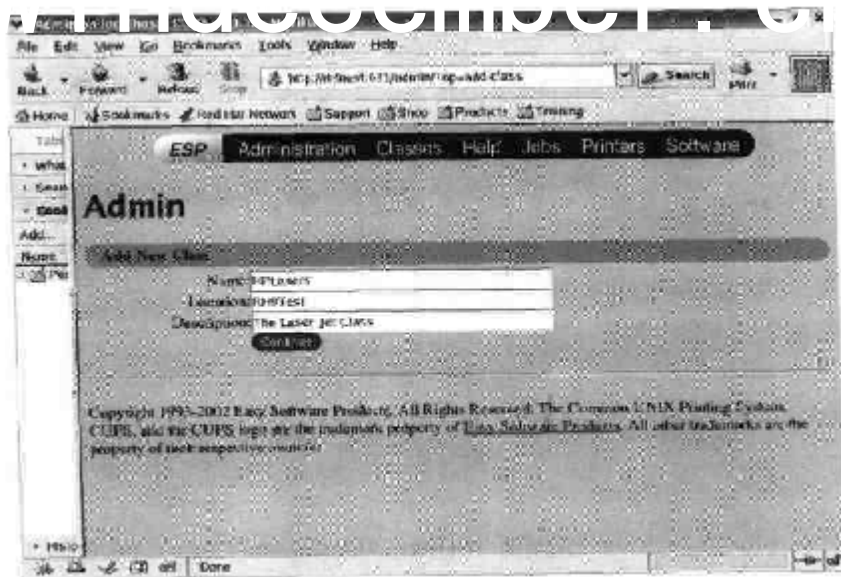


图25.11 增加新类界面

单击Continue进入Members For PrintClassName界面。这个界面中列出所有配置的CUPS打印机，包括已经分配给另一个打印机类的打印机。要将图15.12所示的打印机加进新的HPLasers类，加亮显示这些打印机，然后单击Continue。CUPS显示一个消息，表示HPLasers类已经成功添加。现在可以用HPLasers打印，CUPS会让类中第一个可用的打印机处理打印作业。

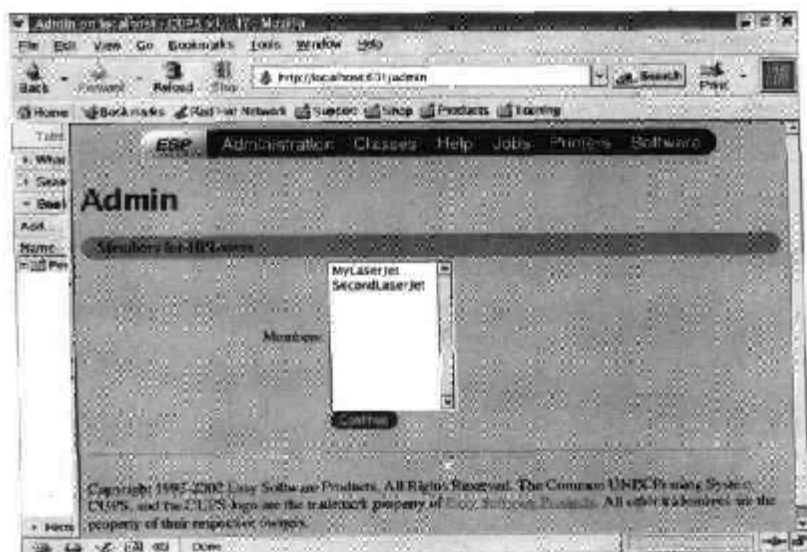


图15.12 Members For PrintClassName界面

再次单击 **Classes**，可以看到配置的打印机类。图25.13显示了生成的类，具有成员 **MyLaserJet** 与 **SecondLaserJet**。

现在转移到 <http://localhost:631>，返回主CUPS菜单。

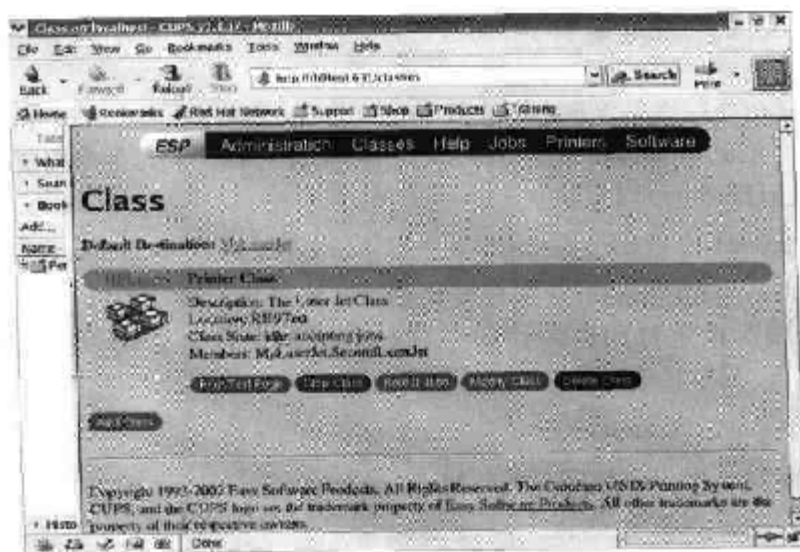


图25.13 配置的打印机类

管理任务

单击 **Administration** 或 **Do Administration Tasks** 时，打开一个菜单，可以管理打印机类、打印作业和打印机。如图25.14所示，这是个集成的CUPS管理菜单。

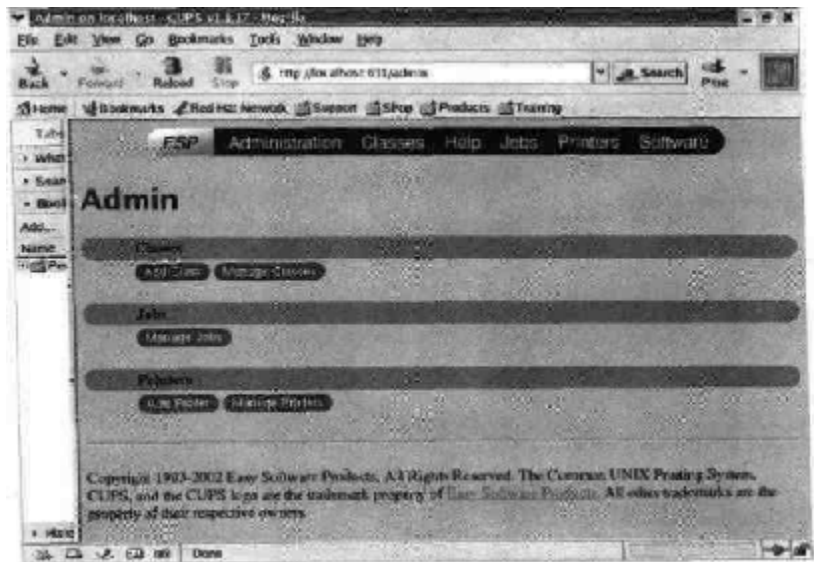


图25.14 CUPS管理菜单

lpadmin命令

专业Linux管理员通常从命令行界面进行管理，但许多人已经开始信任CUPS Web配置器。许多人不相信GUI界面增加的一层，因为多一层就多一个出错的可能。毫不奇怪，仍然有很多人用lpadmin命令从命令行界面进行管理，但由于打印机品牌和机型很多，使这个命令很不方便。

但可以从命令行进行管理。一个关键的功能是设置打印机的用户配额，帮助跟踪使用情况。例如，可以用lpadmin命令对特定打印机设置配额。下列命令指定所有用户在打印机MyLaserJet上只限于每天十页：

```
# lpadmin -p MyLaserJet -o job-quota-period=86400 -o job-page-limit=10
```

也可以用-o job-k-limit开关限制发送到打印机的数据量（KB）。

可以限制对指定打印机的访问。例如，下列命令只让用户ez与tblair访问打印机MyLaserJet：

```
# lpadmin -p MyLaserJet -u allow:ez,tblair
```

这个命令禁止用户mj访问打印机MyLaserJet：

```
# lpadmin -p MyLaserJet -u deny:mj
```

lpadmin命令影响/etc/cups/printers.conf中的数据。

lpstat命令

lpstat命令可以检查打印机与类的状态，用起来非常简单：-c class选项列出指定类的成员，-v printer选项列出指定打印机的设备或地址。

配置文件

CUPS配置文件存放在/etc/cups目录中。如果你熟悉第30章介绍的Apache Web服务器，则很容易理解CUPS。

它们的语言也相似。记住，CUPS用URI列出打印机，如ipp://RH9/MyLaserJet。我们知道，URL列出http://www.sybex.com之类的地址。表25.8列出了标准配置文件，下节详细介绍/etc/cups/cupsd.conf。

表25.8 CUPS配置文件（在/etc/cups目录中）

文件	描述
classes.conf	指定不同打印机组，用CUPS Web工具生成打印机类时，其细节写入这个文件
client.conf	指向默认CUPS服务器，可以指定加密要求
cupsd.conf	主CUPS配置文件
mime.convs	列出不同文件格式的过滤器，如文档与图形
mime.types	列出CUPS打印机可处理的文件类型
printers.conf	CUPS Web工具改变的配置文件，细节写入这个文件
pstoraster.convs	包含Ghostscript文件的转换过滤器，GNU用这个方法处理PostScript打印机

/etc/cups/cupsd.conf

尽管可以用Web工具设置CUPS打印机和类，但如果要管理一组打印机，则要知道主CUPS配置文件/etc/cups/cupsd.conf。本节详细介绍这个文件的默认版本，稍后将会介绍，其中许多变量被标识为说明语句，可以激活打印机网络。本节列出的变量与默认/etc/cups/cupsd.conf配置文件中的顺序不完全一致，例如，与日志文件相关的变量在一段中。

cupsd.conf还有其他变量，更多信息见CUPS GUI配置程序联机帮助部分提供的CUPS软件管理员手册。

说明：记住，#是说明代码，要将其删除以激活命令。有时，显示为说明的命令是默认命令。

服务器变量

ServerName变量很简单，列出CUPS打印服务器计算机的显示名。默认情况下，它设置为本地计算机的主机名：

```
#ServerName myhost.domain.com
```

这个名称应与/etc/cups/client.conf中CUPS客户计算机的ServerName变量相符。ServerAdmin变量实际上设置为CUPS服务器的网管的电子邮件地址：

```
#ServerAdmin root@your.domain.com
```

标准目录

cupsd.conf中列出了几个文件，如果用相对路径列出，则相对于ServerRoot目录，默认设置为/etc/cups:

```
#ServerRoot /etc/cups
```

默认情况下，CUPS RPM包在/usr/share/cups目录中存放了标准打印数据，包括类别、字体、字符集、帮助文档，等等。可以改变下列变量，从而改变CUPS寻找这个目录的地址:

```
#DataDir /usr/share/cups
```

发送打印作业时，其处理成假脱机存放的文件。通常，文件保留在假脱机目录中，直到打印机实际处理这个打印作业。标准目录用RequestRoot变量指定，默认设置为/var/spool/cups:

```
# RequestRoot /var/spool/cups
```

CUPS还要一个所有用户可以写入的临时目录。处理打印作业时，可能在这个目录中存储过滤器。默认为/var/tmp，但Red Hat Linux在/var/spool/cups/tmp目录中配置如下:

```
#TempDir /var/spool/cups/tmp
```

如果生成自己的临时目录作为根目录，则可以用下列命令设置相应权限:

```
# chmod a+t /tmpdir
```

为了使结果直观化，可以看看ls -l /var/spool/cups命令的输出:

```
drwx-----T  2 lp  sys   4096 Mar 3 12:48 tmp
```

日志文件变量

第13章曾介绍过，大多数日志文件存放在/var/log目录中。CUPS日志文件也不例外，存放在/var/log/cups目录中。标准日志文件行如下:

```
#AccessLog /var/log/cups/access_log
#ErrorLog /var/log/cups/error_log
#PageLog /var/log/cups/page_log
```

这些变量设置为默认值。当然，可以将这些日志文件改为指向所选目录。这些日志收集表25.9所列的数据。

表25.9 CUPS日志文件

日志文件	描述
access_log	列出通过CUPS Web管理工具访问的HTTP文件
error_log	除了错误消息，标准日志格式中还包括警告、信息与调试消息
page_log	记录发送到打印机的每一天

第13章介绍了每周如何轮换日志文件。MaxLogSize变量在日志文件到达指定长度时强制轮换日志文件。如果不设置这个变量，则默认为1MB；如果设置为0，则日志不轮换，除非另一个作业指定轮换日志文件，如/etc/cron.daily目录中列出的作业:

```
MaxLogSize 0
```

第13章已介绍了日志如何根据/etc/syslog.conf配置文件中的设置收集数据。表25.10列出了CUPS级。默认情况下，LogLevel设置为info：

```
LogLevel info
```

表25.10 CUPS日志级

日志级	描述
emerg	使CUPS无法工作的条件
alert	要立即解决的项目
crit	可能使CUPS无法工作的关键错误
error	一般错误
warn	警报消息
notice	临时错误
info	所有请求
debug	基本调试信息
debug2	所有调试信息

安全打印输出

可以设置每个打印页的页头。如果网络打印输出有一定安全要求，则可以激活下列命令之一：

```
#Classification classified
#Classification confidential
#Classification secret
#Classification topsecret
#Classification unclassified
```

默认情况下没有Classification。但如果有，则要采用ClassifyOverride变量。如果将这个变量设置为on，则其允许用户变量特定打印作业的分类，默认为off如下：

```
#ClassifyOverride Off
```

CUPS Web配置工具使用的标准字体由DefaultCharset变量设置，常见选项为iso-8859-1与windows-1251，但不适用于指定DefaultLanguage变量时以及CUPS客户机设置为不同DefaultCharset时：

```
#DefaultCharset utf-8
```

DefaultLanguage指定连接CUPS Web浏览器工具时所用的语言，默认为英语(en)，也可以用德语(de)、西班牙语(es)、语法(fr)和意大利语(it)：

```
#DefaultLanguage en
```

和Apache一样，DocumentRoot变量指定不同HTML页面的基础目录。这里HTML页面与CUPS Web浏览器工具相关联，默认设置为/usr/share/doc/cups-versionnumber目录：

```
#DocumentRoot /usr/share/doc/cups-versionnumber
```

Linux通常用Ghostscript实现PostScript文件。将这种文件发送到打印机时，需要FontPath变量当前指定的字体，默认设置如下：

```
#FontPath /usr/share/cups/fonts
```

打印作业管理

与打印作业管理相关的基本变量有四个。例如，可以将CUPS打印服务器配置成记录过去的作业或假脱机文件。PreserveJobHistory变量默认设置为Yes，记录过去的作业：

```
#PreserveJobHistory Yes
```

可以记录作业假脱机文件历史。如果将这个变量设置为Yes，则可以重新打印过去的作业，直到将其清除。但是，PreserveJobFiles变量默认设置no：

```
#PreserveJobFiles No
```

由于硬盘空间是有限的，MaxJobs变量设置要保留的打印作业个数，默认为500：

```
#MaxJobs 500
```

自然，MaxCopies变量设置拷贝极限：

```
#MaxCopies 100
```

通常，最好按前面介绍的lpac命令分配额，根据CUPS打印机使用情况。打印作业通常不消除，因此系统中会保留打印机使用情况的相关数据。

相反，如果没有设置配额，则不需要跟踪每个用户运行的打印作业数。

然后可以激活AutoPurgeJobs变量，自动从系统中删除打印作业：

```
#AutoPurgeJobs No
```

可以用下列简单命令在/etc/printcap之类的标准文件中配置可用的打印机清单：

```
#Printcap /etc/printcap
```

通常，/etc/printcap基于为BSD开发的LPD系统。但是，Solaris操作系统也提供了类似的格式。尽管默认为BSD式系统，但也可以用下列命令激活：

```
#PrintcapFormat BSD
```

```
#PrintcapFormat Solaris
```

说明：不必考虑PrintcapGUI变量，它只用于SGI IRIX操作系统的打印机控制。

有些打印作业需要程序提供帮助，这些程序通常存放成/usr/lib/cups中的可执行格式，由ServerBin变量指定：

```
#ServerBin /usr/lib/cups
```

大多数打印机配置成在“光栅”方式中一点一点地打印图形，但晒图机和其他特殊打印过滤器可以使用光栅图形处理缓存变量RIPCache。默认情况下，缓存为8MB，可以设置为KB或GB值，如100k或1g。

```
#RIPCache 8m
```

说明：这里RIP与TCP/IP的RIP（路由信息协议）毫无关系。

如果打印作业占用了太多服务器的功能，则可以设置FilterLimit，这个变量通常设置为0，表示无限制：

```
#FilterLimit 0
```

使用的值可以通过试错取得，准则如下：如果要用普通打印机打印，则应将这个值设置为200；如果有几个普通打印机，则可以设置为更大的值。如果这个值低于200，则会把CUPS限制在一次处理一个作业。

加密支持

有时要加密网络通信。可以将CUPS配置成读取加密打印请求。SSL证书和密钥用下列变量定义：

```
#ServerCertificate /etc/cups/ssl/server.crt
#ServerKey /etc/cups/ssl/server.key
```

这些证书要在网络上定期刷新，用RootCert-Duration变量指定（秒数）：

```
#RootCertDuration 300
```

CUPS用户

CUPS由根用户启动，而CUPS作业通常由其他权限更小的用户运行。从不同计算机访问CUPS时，CUPS指定不同用户名remroot，它是RemoteRoot变量指定的：

```
#RemoteRoot remroot
```

标准CUPS用户为lp，标准组为sys，由User与Group变量定义。可以用RunAsUser Yes命令覆盖这些值：

```
#User lp
#Group sys
```

基本网络设置

CUPS是对TCP/IP网络开发的。配置CUPS时，可以将其设置为监听特定计算机或IP地址的特定端口。例如，下列命令将CUPS设置为监听端口631，来自计算机linux.mommabears.com的请求，来自192.168.22.0网络的请求：

```
Port 631
Listen linux.mommabears.com
Listen 192.168.22.0
```

如果要监听特定主机名，则要将HostNameLookups变量设置为on。甚至可以将这些设置组合起来。例如，下列命令将CUPS设置为端口80上监听网络10.11.12.0的请求：

```
Listen 10.11.12.0:80
```

说明：在Apache 2.0.x中，Listen指令取代Port指令。详见第30章。

通常，要遵照cupsd.conf配置文件中的IP地址。查找DNS服务器中的域名很费时间，会减慢CUPS打印服务器的速度。如果需要，可以将Red Hat Linux cupsd.conf变量设置为让

CUPS寻找与域名相关的IP地址。自然，默认为off，但下列说明行放在默认的Red Hat Linux cupsd.conf文件中：

```
# HostNameLookups On
```

CUPS通常保持与Web浏览器的打开连接，这是KeepAlive On变量所指定的。但如果通过Netscape 2.x之类的旧式Web浏览器管理CUPS，则这个变量不起作用。这时要设置CUPS等待Web工具提供数据的时间。这是用KeepAliveTimeout设置定义的，其在指定时间（秒数）内保持打开连接：

```
#KeepAlive On
#KeepAliveTimeout 60
```

用户限制

在网络上设置打印服务器时，任何用户可能任何时间请求访问。MaxClients变量限制连接CUPS打印服务器的用户数，默认极限为100人：

```
#MaxClients 100
```

可以多次登录一个主机计算机，默认情况下，登录的次数为MaxClients值的十分之一。

还可以控制通过CUPS打印服务器发送的作业长度。可能要把很大的作业发送到其他服务器。可以用MaxRequestSize变量设置字节或MB数，但默认用下列命令避免受限：

```
#MaxRequestSize 0
```

相关变量包括MaxJobsPerPrinter与MaxJobsPerUser。如果要在CUPS打印机或用户中设置作业极限，则这些变量很容易理解。

有时，用户想发送打印作业，但程序不能满足。标准Timeout变量设置为关闭CUPS连接的时间。默认为300秒：

```
#Timeout 300
```

网络浏览

CUPS中的浏览参数确定网络上的其他计算机（或其他网络）能否看到你用CUPS服务器配置的打印机。默认情况下，Browsing为on，其他参数确定其他计算机如何去访问CUPS打印机。

CUPS浏览可以配置两个协议：CUPS与SLPv2。前者广播打印机信息，后者是SLP（服务位置协议）的第二版，它使其他计算机可以找到可用的服务。

这两个协议都可以配置成在网络上收集与分配共享打印机的信息。默认为CUPS，如果要使用SLPv2，则网络要访问至少一个SLPv2目录代理。尽管默认为CUPS协议，但也可以用下列命令配置某个协议或两个协议：

```
#BrowseProtocols cups
#BrowseProtocols slp
#BrowseProtocols all
```

CUPS服务器广播共享打印机信息时，需要一个广播地址，通常是网络的广播IP地址，由BrowseAddress指定。如果网络包括拨号连接，则可以将BrowseAddress设置为@LOCAL；

如果只要浏览连接eth2网卡的网络，则可设置为@IF (eth2)。可以根据需要使用多个BrowseAddress命令。下面是几个例子：

```
#BrowseAddress 192.168.99.255
#BrowseAddress 10.255.255.255
#BrowseAddress @IF(eth1)
```

如果打印机名一目了然（如hplaser@joescomp），则不必指定打印机的完整地址。CUPS假设你在这方面有一些技巧，因此将BrowseShortNames变量设置为Yes。如果你所在的大公司中有大量打印机，并且需要使用每台打印机的大量数据，则应将其设置为No，如下：

```
#BrowseShortNames Yes
```

增加或共享新CUPS打印机时，CUPS要更新可用打印机的清单。这是由BrowseInterval变量控制的，其默认设置为30秒：

```
#BrowseInterval 30
```

也可以将BrowseInterval设置为0，表示新CUPS打印机上的信息不自动发送到其他计算机。但是，可以将另一CUPS服务器配置成寻找打印机浏览表。例如，下列命令从地址192.168.0.222端口631的CUPS服务器取得打印机的列表：

```
#BrowsePort 192.168.0.222:631
```

无论如何，不要把BrowseTimeout设置为比BrowseInterval小的值，否则会在网络其他部分共享打印机之前它会被从表中删除。BrowseTimeout默认为300秒：

```
#BrowseTimeout 300
```

如果要向其他网络提供访问，则可以使用BrowseRelay变量。下面的例子将共享CUPS打印机表发送给其他网络上的计算机。第一个地址或接口应在本地网络上。如果使用IP地址，则第二个地址可以是其他网络的广播地址。

CUPS广播的默认端口是Internet打印协议（IPP）的默认TCP/IP端口：631。为了增加系统安全性，可以指定不同的端口，但要保证网络上所有其他计算机都使用BrowsePort变量指定端口上的打印机：

```
#BrowsePort 631
```

浏览安全性

可以限制可以浏览CUPS打印机表的计算机。默认情况下，BrowseAllow接受来自所有地址的数据，BrowseDeny不拒绝对任何计算机的访问。可以用几种方式指定网络的IP地址、网址或域名。下面是些有效命令的例子：

```
# BrowseAllow 10.12.0.0/24
# BrowseAllow 10.12.0.0/255.255.0.0
# BrowseAllow all
# BrowseDeny *.example.com
# BrowseDeny none
# BrowseDeny @IF(eth1)
```

但Allow与Deny哪个在先呢？这是由BrowseOrder变量确定的，如果将其设置如下：

```
#BrowseOrder allow,deny
```

则计算机可以看到共享打印机表，除非在BrowseDeny命令中列出。相反，下列命令导致只能在BrowseAllow命令列出的计算机上访问：

```
#BrowseOrder deny,allow
```

说明：自然，如果要指定域或主机名，则要将HostNameLookups设置为On。

系统安全性

cupsd.conf的安全性 with Apache 配置文件非常相似。尽管默认CUPS用户由SystemGroup变量定义为sys：

```
#SystemGroup sys
```

但可以配置<Location />容器，控制访问IP地址、类、作业、加密，等等。标准红帽子配置文件只允许从本地计算机访问CUPS服务器：

```
<Location />
Order Deny,Allow
Deny from All
Allow From 127.0.0.1
</Location>
```

可以按普通或CIDR符号指定其他IP地址。如果将HostNameLookups设置为m（不提倡），则甚至可以使用主机名或域名。如下所示，可以按类（第一个例子限制AnyPrinter类访问）或按打印机（第二个例子限制HPLaserJet打印机访问）限制访问：

```
<Location /AnyPrinter>
Order Deny,Allow
Deny from All
Allow From 127.0.0.1
</Location>

<Location /AnyPrinter/HPLaserJet>
Order Deny,Allow
Deny from All
Allow From 127.0.0.1
</Location>
```

其他容器可以控制管理操作，见表25.11。

表25.11 位置容器选项

容器	描述
<Location />	与所有CUPS打印操作相关联
<Location /admin>	与CUPS管理操作相关，可以限制对CUPS的管理访问
<Location /classes>	限制所有配置的CUPS打印机类

(续表)

容器	描述
<Location /classes/classname>	限制名为classname的CUPS打印机类
<Location /jobs>	限制打印作业管理
<Location /printers>	限制管理所有打印机的管理访问
<Location /printers/printname>	限制管理名为printname的打印机的管理访问

不要忘了在容器末尾使用</Location>命令。除了Order、Deny与Allow之外，还有其他命令可以加进<Location />容器中，见表25.12。

表25.12 位置指令命令/定义

命令	描述
Allow	用于允许访问指定打印机或类的计算机或接口
Anonymous	表示不需要用户名和口令，通常是默认
AuthClass	指定所要的验证，选项包括Anonymous、User、System与Group
AuthGroupName	设置与Group AuthClass相关联的组名
AuthType	定义新的用户名和口令类型，选项包括None、Basic（使用/etc/passwd、Digest和Basic Digest使用/etc/cups/passwd.md5
Deny	用于不允许访问指定打印机或类的计算机或接口
Encryption	指定用户名和口令是否要加密，选项包括Never、IfRequested、Required与Always
Limit	指定允许的CUPS请求命令
LimitExcept	指定不允许的CUPS请求命令
Order	指定CUPS按什么顺序读取Deny与Allow命令
Require	限制组、用户或所有具有valid-user的用户访问

打印机类

不一定要对每个CUPS打印机配置一个类。可以对同名的不同打印机设置ImplicitClasses，如HPLaserJet。ImplicitClasses的打印作业发送到具有第一个可用队列的打印机。ImplicitClasses默认为on：

```
#ImplicitClasses On
```

可以将ImplicitAnyClasses设置为on，从而将ImplicitClasses设置为AnyPrinter。其默认为off：

```
#ImplicitAnyClasses Off
```

如果使用ImplicitClasses，则用户不需要知道类中的各个打印机。如果ImplicitClasses为on，则HideImplicitMembers变量默认为on。

打印机管理

配置CUPS之后, 可以用CUPS GUI工具管理当前的打印作业。还可以将cups-lpd服务设置成允许使用大多数标准的LPD命令, 包括lpr、lpq与lprm。这些命令将在本章稍后介绍。最后, 可以通过/var/log/cups目录中的CUPS日志文件监视状态、错误和可疑访问企图。

作业管理

管理活动的CUPS打印作业很简单。图25.15所示的CUPS作业屏幕显示了两个不同的打印作业。如果要先打印作业MyLaserJet-8, 则可以单击MyLaserJet-7的Hold Job按钮。CUPS显示一个消息“Job7 has been held from printing”, 表示作业7保持, 并自动启动MyLaserJet-8作业。

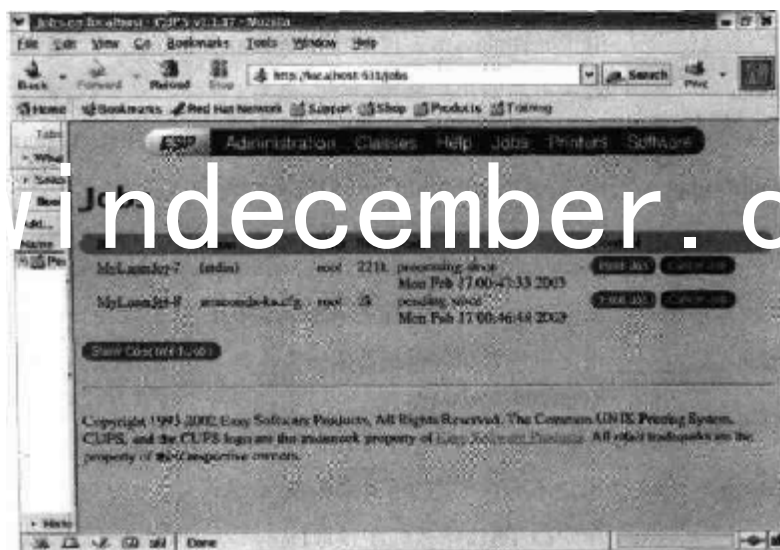


图25.15 管理CUPS打印作业

作业MyLaserJet-7在打印队列中保持, 直到返回Jobs菜单并单击Release Job按钮。

激活LPD命令

要对CUPS服务器激活LPD命令, 就要激活/etc/xinetd.d目录中的cups-lpd服务。可以用chkconfig service cups-lpd on命令激活这个服务。第23章介绍了管理xinetd服务的更多信息。

可能要对最初为LPD接口设计的某些应用程序激活cups-lpd服务。

CUPS日志文件

CUPS日志文件已经在本章前面简要介绍过, 它通常存放在/var/log/cups目录中。access_log文件列出了访问CUPS服务器的计算机及访问日期与时间。图25.16的例子只列出了默认本地计算机localhost的访问。

error_log文件如图25.17, 它不仅列出标准错误, 还列出CUPS服务器的基本活动, 包括上节保持的打印作业(在第一行)。

```
localhost - root [29/Mar/2003:13:57:21 -0500] "POST /admin/ HTTP/1.1" 200 842
localhost - root [29/Mar/2003:13:57:18 -0500] "POST /admin HTTP/1.1" 200 1780
localhost - - [29/Mar/2003:13:57:24 -0500] "POST / HTTP/1.1" 200 220
localhost - - [29/Mar/2003:13:57:25 -0500] "GET /classes/HPLasers HTTP/1.1" 200
0
localhost - - [29/Mar/2003:13:57:25 -0500] "POST / HTTP/1.1" 200 77
localhost - - [29/Mar/2003:13:57:28 -0500] "POST / HTTP/1.1" 200 125
localhost - - [29/Mar/2003:13:57:28 -0500] "POST / HTTP/1.1" 200 125
localhost - - [29/Mar/2003:13:57:25 -0500] "GET /classes/HPLasers HTTP/1.1" 200
8170
localhost - - [29/Mar/2003:13:57:29 -0500] "GET /images/classes.gif HTTP/1.1" 20
0 581
localhost - - [29/Mar/2003:13:57:29 -0500] "GET /images/stop-class.gif HTTP/1.1"
200 245
localhost - - [29/Mar/2003:13:57:29 -0500] "GET /images/delete-class.gif HTTP/1.
1" 200 259
localhost - - [29/Mar/2003:13:57:29 -0500] "GET /images/modify-class.gif HTTP/1.
1" 200 267
localhost - - [29/Mar/2003:13:57:29 -0500] "POST / HTTP/1.1" 200 220
localhost - - [29/Mar/2003:13:57:31 -0500] "GET /classes HTTP/1.1" 200 0
localhost - - [29/Mar/2003:13:57:31 -0500] "POST / HTTP/1.1" 200 77
localhost - - [29/Mar/2003:13:57:32 -0500] "POST / HTTP/1.1" 200 77
localhost - - [29/Mar/2003:13:57:31 -0500] "GET /classes HTTP/1.1" 200 3010
```

图25.16 CUPS access_log文件

```
[29/Mar/2003:13:54:11 -0500] Started "/usr/lib/cups/cgi-bin/jobs.cgi" (pid=240
9)
E [29/Mar/2003:13:54:11 -0500] Failed to delete job: job not owned by user
I [29/Mar/2003:13:54:14 -0500] Started "/usr/lib/cups/cgi-bin/jobs.cgi" (pid=241
0)
I [29/Mar/2003:13:54:28 -0500] Started "/usr/lib/cups/cgi-bin/printers.cgi" (pid
=2411)
I [29/Mar/2003:13:54:33 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
12)
I [29/Mar/2003:13:55:07 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
15)
I [29/Mar/2003:13:55:15 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
16)
I [29/Mar/2003:13:55:20 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
17)
I [29/Mar/2003:13:55:23 -0500] Started "/usr/lib/cups/cgi-bin/admin.cgi" (pid=24
18)
I [29/Mar/2003:13:55:25 -0500] Setting SecondLaserJet device-uri to "parallel:/d
ev/lp0" (was "").
I [29/Mar/2003:13:55:25 -0500] Setting SecondLaserJet printer-is-accepting-jobs
to 1 (was 0.)
•
```

图25.17 error_log文件

最后，page_log文件列出发送到队列的任何作业，包括已经取消的。图25.18显示了这个文件的例子。

使用LPD（行打印监控程序）

Red Hat Linux的默认打印服务器是CUPS。由于CUPS是在Red Hat Linux 9中首次成为默认，因此许多人仍然倾向于使用行打印监控程序（LPD）。尽管LPD能很好地为Linux服务，但它没有CUPS的打印机组或类的功能。而且CUPS允许使用IPP，这是大多数操作系统中打印服务器的新标准。


```

HPLaser:\
:ml#0:\
:mx#0:\
:sd=/var/spool/lpd/HPLaser:\
:af=/var/spool/lpd/HPLaser/HPLaser.acct:\
:sh:\
:lp=/dev/lp0:\
:lpd_bounce=true:\
:if=/usr/share/printconf/util/nf_wrapper:

printer:\
:ml#0:\
:mx#0:\
:sd=/var/spool/lpd/printer:\
:af=/var/spool/lpd/printer/printer.acct:\
:sh:\
:lp=/dev/lp0:\
:lpd_bounce=true:\
:if=/usr/share/printconf/util/nf_wrapper:

printer1:\
:ml#0:\
:mx#0:\

```

图25.19 LPD配置文件 (/etc/printcap)

表25.12 /etc/printcap 缩进代码

代码	描述
:	在一个/etc/printcap命令中分隔代码行
\	将两行连在一起，取消新行效果
af	与账号过滤器 (af) 相关
if	对特定打印机使用输入过滤器 (if)
lp	表示与打印机相关的行打印 (lp) 设备
lpd_bounce	设置为真值时通过过滤器发送打印作业
ml	检查不可打印字符，设置为非零值时，阻止打印大多数二进制文件
mx	指定最大文件长度，设置为0时没有极限
sd	表示假脱机目录
sh	取消头
pl	指定页长 (行数)
pw	指定页宽 (字符数)

还有另外两个主要的LPD配置文件。这些配置文件的默认版本适用于大多数情形。大多数情况下，可以在/etc/printcap中或使用的应用程序中进行所需的改变。由于这些文件很少被修改，因此我们只是介绍其用途。/etc/lpd.conf文件指定打印机的默认设置，/etc/lpd.perms文件设置LPD假脱机程序的权限。

说明：如果使用CUPS，则/etc/printcap中有个已配置打印机和打印机类的简单清单。

打印机管理

LPD中有四个基本命令：行打印机请求 (Line Printer Request, lpr)、行打印机查询 (Line Printer Query, lpq)、行打印机删除 (Line Printer Remove, lprm) 和行打印机控制 (Line Printer Control, lpc)，这些命令也称为lp命令。

说明：如果使用CUPS，并在/etc/xinetd.d中激活了cups-lpd服务，则这些命令的用法不尽相同，但结果是相似的。

lpr

让Linux用cat命令读取文件内容时，shell将结果发送到标准输出，通常可以在屏幕上看到结果。相反，使用lpr时，shell将结果发送到本地计算机上的假脱机文件，然后发送到打印服务器计算机，最后发送到打印机上。lpr命令效果上是个客户机。产生假脱机文件时，lpd服务器在本地或远程服务器上处理这个结果。

因此，运行lpr file之类的命令时，shell将结果发送到/etc/printcap中配置的默认打印机。也可以将打印作业发送到不同打印机。例如，如果/etc/printcap中配置了colorprinter，则下列命令将打印作业发送到这台打印机：

```
# lpr -Pcolorprinter file1
```

说明：使用lpr命令指定打印机时，-p与打印机名之间没有空格。

表25.14列出了lpr命令的其他形式。

表25.14 lpr命令

命令	结果
lpr -h file1	打印没有作业控制页的file1，通常包含用户账号和源计算机的主机名。作业控制页也称为奔发页
lpr -Pother file1	用/etc/printcap文件中定义的打印机other打印file1
lpr -s file1	生成file1的符号链，避免生成假脱机文件在lpr的BSD版本中使用大于1MB的大文件时有用。Red Hat Linux 9中使用LPRng程序，因此不需要这个命令

lpq

lpq命令提供当前打印队列，有三个基本选项，见表25.15。这个命令还有一列作业号，可能是lprm命令所需要的。

表25.15 lpq命令

命令	结果
lpq	返回默认打印机的当前打印队列，默认打印机在/etc/printcap文件中定义
lpq -P printer	返回指定打印机的当前打印队列，使用/etc/printcap文件中定义的名称

lprm

如果打印作业还在打印机内存中，则可以用lprm命令删除当前在队列中的打印作业。利用lprm命令可以有三种方法删除打印作业：按打印作业号、按用户或按打印机。表25.16显示了lprm命令的例子。

表25.16 lprm命令例子

命令	结果
<code>lprm 188</code>	删除lpq命令输出中定义的打印作业188
<code>lprm -P hp2 mj</code>	从/etc/printcap文件中的打印机hp2删除用户mj的打印作业

lpc

`lpc`命令可以控制每台打印机的几个特征。如表25.17所示，这个命令可以检查打印机状态、删除活动打印作业和将打印作业改向到不同打印机。

表25.17 lpc命令例子

命令	结果
<code>lpc -P canon1 status</code>	显示打印机canon1的状态。换句话说，输出显示能否将打印作业发送到队列、队列中的作业号、打印机是否接收作业和与打印机的通信状态
<code>lpc disable</code>	禁止对默认打印机将作业发送（假脱机）到打印队列，与 <code>lpc enable</code> 相反
<code>lpc start</code>	从打印队列删除所有传输
<code>lpc stop</code>	停止打印机与打印队列之间的通信

红帽子打印机工具

由于与/etc/cups/cupsd.conf及/etc/printcap相关的命令非常难懂，因此更常见的方法是用图形工具配置CUPS或LPD打印机。红帽子打印机工具基于`redhat-config-printer`（和`redhat-config-printer-gui`），可以通过同名RPM包取得。可以从文本或GUI命令行控制台运行这个命令。尽管外观不同（如图25.20和图25.21），但信息是相同的。

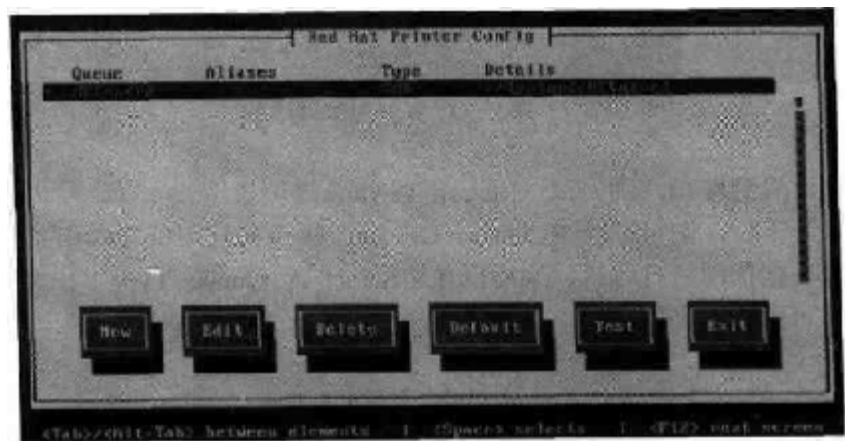


图25.20 redhat-config-printer命令行版

用redhat-config-printer设置新打印机很简单。下列步骤基于redhat-config-printer GUI版，在打印机配置窗口中启动：

- 1. 单击New，出现Add A New Print Queue对话框时，单击Forward按钮继续。
- 2. 在Queue Name对话框中，输入打印机名称和描述，如图25.22。完成之后，单击Forward按钮继续。



图25.21 redhat-config printer GUI版

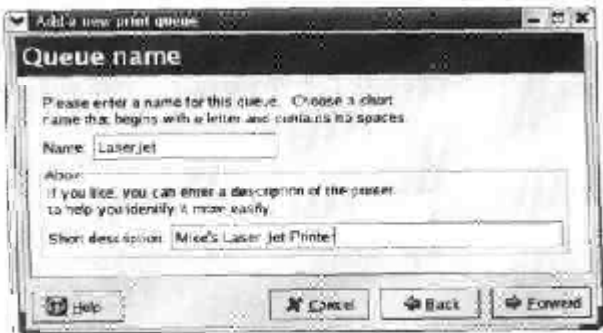


图25.22 增加新打印队列

- 3. 在Queue Type对话框中，可以看到可用的打印机端口，如图25.23。例如，/dev/lp0对应于第一个端口。如果配置本地打印机，则应该选择可用的打印机端口，然后单击Forward按钮继续。如果不符合要求，则可以试用下列方法：



图25.23 队列类型对话框

- 如果没看到端口，则先试试Rescan Devices选项。
- 如果还不行，则可以单击Custom Device，输入与打印机端口相关联的设备。
- 如果要选择网络打印机，则可以单击Select A Queue Type下拉文本框。表25.18列出了可能的选项。

表25.18 网络队列类型

类型	描述
Networked CUPS (IPP)	对远程CUPS服务器上的打印机，要求服务器主机或域名和IPP路径
Networked UNIX (LPD)	对远程LPD服务器上的打印机，要求服务器主机或域名和远程队列名

(续表)

类型	描述
Networked Windows (SMB)	对远程Microsoft Windows 打印服务器上的打印机, 自动探测共享打印机
Networked Novell (NCP)	对远程Novell打印服务器上的打印机, 要求服务器主机或域名和队列名, 以及授权用户名与口令
Networked JetDirect	对直接连接网络的远程JetDirect打印服务器上的打印机, 要求JetDirect打印机名

4. 在**Printer Model**对话框中, 选择打印机品牌和厂家。按下列准则选择最适合的驱动器, 然后单击**Forward**按钮继续:

- 有些打印机使用**PostScript**打印驱动器, 处理原始打印数据的打印机可以使用原始打印队列驱动器, 一般性驱动器适用于文本和各种点阵打印机。
- 要选择特定机型, 单击**Generic (Click To Select Manufacturer)**文本框, 出现一系列制造商名单, 如图25.24所示。进行选择之后, 可以选择与打印机最接近的打印机型。

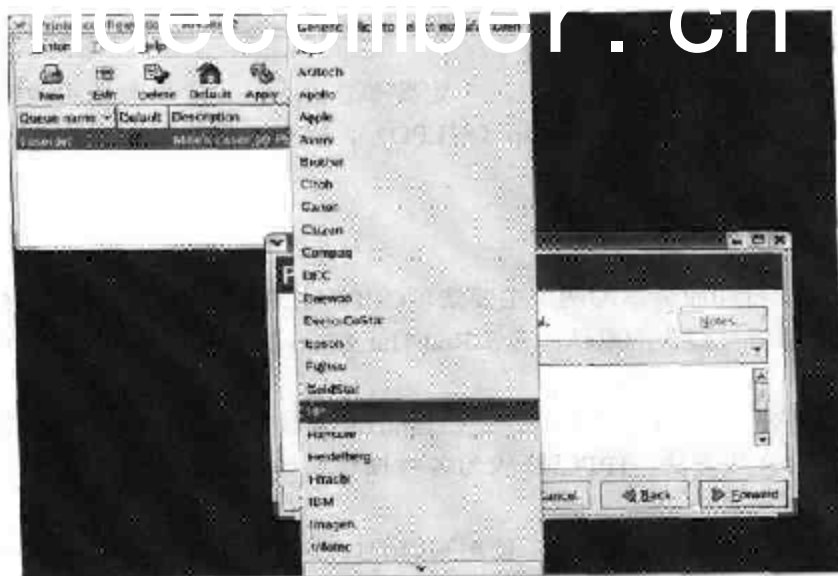


图25.24 选择打印机厂家

5. 出现**完成并生成新打印队列**对话框, 其中包括选择的汇总, 如图25.25。如果对所作选择感到满意, 则单击**Apply**。

6. 这时可以打印测试页。最好打印测试页, 如果连接打印机, 只要单击**Yes**。

回到**Printer Configuration**对话框, 可以看到新打印机的项目。可以编辑设置, 只要加亮打印机并单击**Edit**按钮, 打开所配置打印机的编辑**Print Queue**对话框, 这个对话框有五个标签, 见表25.19。

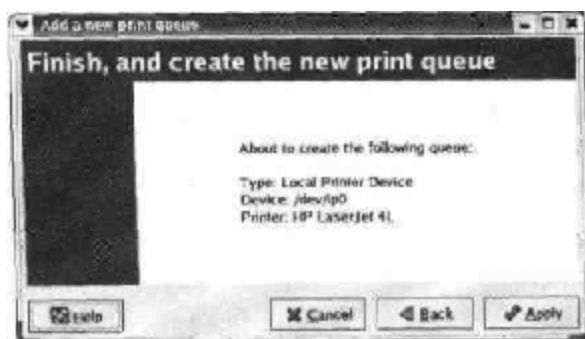


图25.25 打印配置汇总

表25.19 编辑打印机设置

标签	描述
Queue Name	可以指定打印队列名
Queue Type	可以取得设备, 包括网络打印机
Queue Options	可以配置标题页、边界、过滤等基本设置
Printer Driver	可以改变驱动器
Printer Options	可以指定更多驱动器设置

离开redhat-config-printer之前, 一定要单击Apply。这个操作将改变写入/etc/cups/cupsd.conf (对CUPS) 或/etc/printcap (对LPD), 然后重新启动相应的打印监控程序。

小结

本章介绍了打印服务器的两个主要选项CUPS与LPD, 前者是新Red Hat Linux默认的打印服务器, 后者是过去的默认, 今后Red Hat Linux版本中会将其删除, 因此一定要学习CUPS。

CUPS就是公用UNIX打印系统, 提供Linux和其他UNIX式操作系统使用的Internet打印协议 (IPP) 的公共方法。IPP已经成为各种操作系统的标准打印服务器, 因此最好转用CUPS。

CUPS包括图形化浏览器工具, 使用端口631。利用CUPS工具, 可以配置打印机、不同打印机的类和打印作业。打印设备与驱动程序可以支持各种不同连接与协议。甚至可以将一组打印机配置成一个类, 打印作业会自动发送到这个类中第一台可用的打印机。

CUPS配置文件存放在/etc/cups目录中。主CUPS配置文件cupsd.conf很长, 但其基本格式与Apache配置文件相同。配置文件中有大量设置, 可以控制作业长度、日志、安全性, 等等。

配置打印机和打印类之后, 很容易用CUPS Web配置工具管理打印机和打印作业。例如, 在Jobs段中, 可以保持一个打印作业, 让更高优先级的打印作业通过。也可以使用redhat-config-printer, 这取决于redhat-switch-printer中监控程序的设置。也可以用lpstat与lpadmin命

令检查当前打印机状态。如果激活cups-lpd监控程序，则还可以使用几个基本LPD命令。

LPD（行打印监控程序）基于LPRng-* RPM包。要配置打印机，可以直接编辑/etc/printcap.local，也可以用redhat-config-printer工具直接将打印机命令写入/etc/printcap。可以用几个基本命令管理打印机和队列，包括lpr、lpq、lprm与lpc。

第26章将介绍邮件服务器与客户机，并重点介绍网络中如何配置sendmail。

第26章 邮件服务

本章介绍任何连接网络的计算机都有的一个重要应用：电子邮件。可以通过不同的服务器发送与接收电子邮件，每个服务器与一个或几个协议相关联。尽管电子邮件客户机的配置比较简单，但电子邮件服务器则具有丰富而复杂的选项。

电子邮件有几个基本TCP/IP协议，其中接收电子邮件的两个最常用协议是邮局协议（POP）和Internet消息访问协议（IMAP），而从网络中发送电子邮件的最常用协议是简单邮件传输协议（SMTP）。

Internet上最常用的SMTP电子邮件服务器是sendmail。尽管基本sendmail配置文件很复杂，但由于Red Hat Linux包括了一个宏文件，所以很容易根据需要进行配置。可以编辑这个文件，然后用宏处理器生成sendmail的定制配置文件。这个配置文件还可以满足安全需求，设置不能验证的完全限定域名和不想发邮件的域。

入站邮件有两个基本服务器，基于IMAP4与POP3协议。可以生成自己的入站邮件服务器，也可以通过设置电子邮件客户机，使用外部邮件提供者的入站邮件服务器。Red Hat Linux在一个RPM包中提供了这些服务器的普通版和安全版。

大多数计算机用户至少熟悉一个电子邮件客户机，其原理很简单。它们取得电子邮件数据，将其格式化为很容易阅读和答复的形式。Linux中有文本和图形电子邮件客户机。本章介绍下列主题：

- 介绍一般电子邮件服务
- 配置sendmail
- 使用入站邮件服务器
- 配置邮件客户机

介绍一般电子邮件服务

邮件服务有三种：消息传输主体（MTA）、邮件发送主体（MDA）和邮件用户主体（MUA）。

消息传输主体是一个通过网络发送电子邮件的服务器。Linux使用sendmail之类消息传输主体，其在Internet之类TCP/IP网络上用SMTP协议发送电子邮件。

邮件发送主体是一个邮件处理器，从Internet中取得消息并将其存放在服务器或池中——如pine、Mozilla Mail、KMail与Evolution之类的邮件阅读器（即邮件用户主体）——可以读取。最常用的邮件发送主体是procmail，尽管procmail-* RPM包默认安装，但它能无缝地用于正确配置的sendmail（和其他出站邮件服务器）包。

邮件用户主体是个应用程序，帮助这些服务器发送和接收电子邮件。大多数用户至少熟悉一种邮件用户主体，如上面列出的以及Lotus Notes、Netscape与pine。准备和发送电子邮件消息时，就是用邮件用户主体将消息发送到sendmail之类的消息传输主体。

接收电子邮件的两个主要协议是POP3与IMAP4。配置这些协议的邮件服务器在邮件发送主体处理中只需一步。

说明：要配置POP3或IMAP4，只要启用/etc/xinetd.d目录中的相应配置文件（pop3s和imap4）。详见第23章介绍。

关键协议

从一个用户向另一个用户发送电子邮件时，涉及几个TCP/IP协议。我们介绍其中三个：SMTP、POP3与IMAP4。

Linux管理员可能要在某个时候设置电子邮件服务器。尽管sendmail是最重要的SMTP服务器，但也还有其他几个服务器，如Exim、Postfix与Qmail。

作为Linux管理员，你可以帮助用户配置电子邮件客户机。一般来说，需要知道网络上或ISP的任何人站邮件服务器名，包括第24章在DNS服务器中生成的邮件交换器（MX）记录名。但是，本章主要介绍外走邮件。

旧式邮件服务器用UNIX-to-UNIX复制协议（UUCP），直接在计算机之间发送消息。如果消息要到达不同网络，则要指定路径中的每台计算机。毫无疑问，随着Internet的扩展，这个做法行不通。

其他邮件服务器

本章余下部分主要介绍sendmail，但也还有其他易于配置的邮件服务器。每个系统的包（除了商业化sendmail版本Sendmail）都可以从www.rpmfind.net之类站点取得。

商业化Sendmail 与Red Hat Linux所带的版本不同，商业化Sendmail版本是为企业设计的。换句话说，它可以为几千个用户服务，甚至可以为移动客户机配置。更多信息见www.sendmail.com。

Exim 这个MTA是在英国剑桥开发的，它采用GPL许可证。尽管它基于旧的Smail邮件传输主体，但可以帮助验证用户地址和拒绝电子邮件，从而减少向系统用户发送的垃圾邮件。更多信息www.exim.org。

Postfix 这个MTA是sendmail的替换，也许已经在Red Hat Linux系统中安装。它是VMailer与IBM Secure Mailer系统的后续版本。第19章曾介绍过，可以用redhat-switchmail实用程序在这些服务器之间切换。更多信息见www.postfix.org。

Qmail 这个MTA是sendmail的另一个替换。据www.qmail.org称，这个MAT在大量Internet站点中使用。开发者D. J. Bernstein为第一个在该系统中找到安全漏洞的人提供了奖金（cr.yp.to/qmail/guarantee.html）。

Smail 这个MTA据说比sendmail更容易配置。它还支持消息阻止。此外，它可以阻止伪装消息以信任站点的面貌进入。尽管这个邮件传输主体没有正式Web站点，但其开发人员的站点为www.planix.com。

配置sendmail

和大多数复杂的Linux服务一样，sendmail组件可以从几个RPM包安装，有许多关键配置文件，包括sendmail.cf配置文件和sendmail.mc宏。

在最新sendmail版本中，配置文件已经分成两个部分：sendmail接收电子邮件时，使用sendmail.cf；而sendmail发送电子邮件时，使用submit.cf。

设置和运行sendmail之后，可以修改各种配置文件，提高安全性。

说明：这里不准备全面介绍sendmail，否则可以为这个服务编写上千页的书，例如“Linux Sendmail Administration”一书，作者为Craig Hunt（Sybex出版，2001年，其中文译本《Linux Sendmail 管理指南》由电子工业出版社美迪亚公司2001年出版）。

包

使用sendmail配置所要的惟一RPM包是sendmail-* RPM包，其默认安装。表26.1列出了可用的sendmail包。第10章曾介绍过，可以用rpm -q packagename命令检查其是否安装，安装之后可以用rpm -ql packagename命令检查相关文件。

表26.1 sendmail RPM包

包	功能
sendmail-*	sendmail MTA软件
sendmail-cf-*	生成各种sendmail配置文件的工具与模板
sendmail-devel-*	sendmail开发库
sendmail-doc-*	版本说明、常见问题和其他sendmail文档

基本配置文件

sendmail中不仅有基本配置文件sendmail.cf、宏文件、sendmail.mc。和许多其他监控程序一样，sendmail在/etc/sysconfig中有控制文件，可以通过/etc/aliases将其设置成将邮件转发给不同用户，/etc/mail中还存放了许多其他配置文件。

基本/etc/sysconfig/sendmail

/etc/sysconfig/sendmail文件很简单：

```
DAEMON=yes
QUEUE=1h
```

其中DAEMON=yes项将sendmail设置成监听TCP/IP端口25的消息，与SMTP相关联。QUEUE=1h项让sendmail每小时试发送队列中的邮件。

sendmail别名

etc/aliases文件非常简单，指定实际接收邮件的用户。例如，如果要向ftp@localhost之类的服务器发邮件，则可以通过下列项目将这个邮件改向到root@localhost：

```
ftp:      root
```

也可以从前者改向到当前员工:

```
byeltsin: vputin
```

sendmail /etc/mail配置文件

/etc/mail中有几个配置文件, 可以配置sendmail或设置数据库以规定sendmail的工作方法。如果要启用这些配置文件, 则通常要在sendmail.mc宏文件中有项目。如果有.db文件, 则大多数情况下可以用makemap命令将access之类的文本文件转换成access.db。

access与access.db 配置域或电子邮件地址。来自这些地方的电子邮件可以删除(DISCARD)、拒绝并发出错误消息(REJECT)或发送到指定地址(RELAY)。为了减少不要的电子邮件, 可以删除或拒绝特定域或电子邮件地址发来的电子邮件。/etc/mail/access文件是一个例子。

domaintable与domaintable.db 映射两个不同域。这些文件可以在转换域名之后以及别人仍然向旧的电子邮件地址发送电子邮件时使用。如果只是将域名dictatorsrus.com变成democracyisus.com, 则可以在domaintable文件中增加下列项目:

```
dictatorsrus.com    democracyisus.com
```

helpfile 对sendmail提示下的命令提供帮助。可以用telnet localhost 25命令打开sendmail提示。

local-host-names 包含sendmail服务器的别名或其他主机名。只要在这个文件的另一行中输入sendmail服务器计算机的其他名称。

mailertable与mailertable.db 可以对特定地址指定异常电子邮件服务器类型, 很少使用。

Makefile 可以编译不同选项, 可代替sendmail宏处理器。

sendmail.cf与sendmail.mc 可以配置sendmail, sendmail.cf是配置文件, sendmail.mc是配置文件的宏文件, 可以处理成配置文件。本章稍后将详细介绍这些文件的更多信息。

statistics 包含sendmail使用的统计信息。用mailstats命令读这个文件。

submit.cf与submit.mc 可以将sendmail使用限制在特定组内。默认submit.mc文件中的语法与sendmail.mc中的相同。本章稍后将详细介绍这个文件的更多信息。

trusted-users 列出以其他用户身份发送电子邮件的用户, 很少使用, 你愿意向别人提供这个权利吗?

virtualusertable与virtualusertable.db 支持邮件转发, 类似于外部用户的/etc/aliases文件。

了解sendmail.mc

/etc/mail/sendmail.cf文件很可怕, 它长达2000多行。相反, /etc/mail/sendmail.mc文件只有70行左右, 很容易阅读和理解。按照需要配置这个文件之后, 可以用合适的make命令或m4宏处理器生成需要的sendmail.cf定制文件。看看这个文件, 我在需要时增加了一些说明。也许你可能不需要修改这个文件中的大部分内容, 因此我的说明很简单。由于sendmail是个

复杂的课题，可以参阅“Linux Sendmail Administration”一书，作者Craig Hunt（Sybex出版，2001）。

说明：括号中的引号在sendmail.mc文件中比较特别，以反引号开始（```），以单引号（`'`）结尾。反引号在美式键盘的Tab键上方。

`divert (-1)` 命令是开始sendmail.mc文件的标准方式，如果与`divert (0)` 匹配时，则这两个命令间的所有行都作为说明行，忽略不计。

```
divert(-1)dnl
```

以dnl开头的行为说明行。这些特定说明包括一种处理sendmail.mc文件的方法，但仍然可以用`m4 sendmail.mc > sendmail.cf`命令重新生成/etc/mail/sendmail.cf文件。

```
dnl #
dnl # This is the sendmail macro config file for m4. If you make changes to
dnl # /etc/mail/sendmail.mc, you will need to regenerate the
dnl # /etc/mail/sendmail.cf file by confirming that the sendmail-cf package is
dnl # installed and then performing a
dnl #
dnl #     make -C /etc/mail
dnl #
```

下列include命令将cf.m4命令作为宏处理原型。默认情况下，它要求安装sendmail-cf-* RPM包：

```
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
```

VERSIONID是与每个sendmail配置文件相关联的标识符：

```
VERSIONID(`setup for Red Hat Linux ')dnl
```

自然，任何OSTYPE命令指定操作系统，这里是Linux：

```
OSTYPE(`linux')dnl
```

下列define命令协调sendmail服务器与出站电子邮件服务器，可能在网络以外。如果要激活这个命令，删除define前面的dnl并将smtp.your.provider换成ISP的出站（SMTP）电子邮件服务器地址：

```
dnl #
dnl # Uncomment and edit the following line if your outgoing mail needs to
dnl # be sent out through an external mail server:
dnl #
dnl define(`SMART_HOST',`smtp.your.provider')
dnl #
```

一般来说，下列命令不需要改变，详见“Linux Sendmail Administration”一书。

```
define(`confDEF_USER_ID',`8:12')dnl
define(`confTRUSTED_USER',`smmsp')dnl
dnl define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT',`lm')dnl
define(`confTRY_NULL_MX_LIST',true)dnl
```



```
define(`confDONT_PROBE_INTERFACES',true)dnl
define(`PROCMail_MAILER_PATH',`/usr/bin/procmail')dnl
define(`ALIAS_FILE',`/etc/aliases')dnl
dnl define(`STATUS_FILE',`/etc/mail/statistics')dnl
define(`UUCP_MAILER_MAX',`2000000')dnl
define(`confUSERDB_SPEC',`/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS',`authwarnings,novrfy,noexpn,restrictqrun')dnl
```

下面两个以define(`confAUTH_OPTIONS'开头的命令是互相排斥的，TLS是传输层安全，它是SSL（安全套接层）协议的正式版本。

```
define(`confAUTH_OPTIONS',`A')dnl
dnl #
dnl # The following allows relaying if the user authenticates, and disallows
dnl # plaintext authentication (PLAIN/LOGIN) on non-TLS links
dnl #
dnl define(`confAUTH_OPTIONS',`A p')dnl
dnl #
dnl # PLAIN is the preferred plaintext authentication method and used by
dnl # Mozilla Mail and Evolution, though Outlook Express and other MUAs do
dnl # use LOGIN. Other mechanisms should be used if the connection is not
dnl # guaranteed secure.
dnl #
```

如果要防止普通文本方式登录sendmail服务器，可以将这两个命令做如下修改：

```
dnl define(`confAUTH_OPTIONS',`A')dnl
define(`confAUTH_OPTIONS',`A p')dnl
```

下面继续看默认的sendmail.mc文件。下面两个命令与授权方法有关：

```
dnl TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confAUTH_MECHANISMS',`EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN
➡ PLAIN')dnl
```

下列命令可以在sendmail所在系统中使用SSL证书。关于SSL证书的更多信息，见第30章，该章对Apache生成的证书也在这里适用。

```
dnl #
dnl # Rudimentary information on creating certificates for sendmail TLS:
dnl #      make -C /usr/share/ssl/certs usage
dnl #
dnl define(`confCACERT_PATH',`/usr/share/ssl/certs')
dnl define(`confCACERT',`/usr/share/ssl/certs/ca-bundle.crt')
dnl define(`confSERVER_CERT',`/usr/share/ssl/certs/sendmail.pem')
dnl define(`confSERVER_KEY',`/usr/share/ssl/certs/sendmail.pem')
dnl #
```

下列define命令集成了LDAP（轻量级目录辅助协议），提供详细的用户信息，因此可以替换下列/etc/aliases与/etc/mail/virtusertable.db文件。sendmail与LDAP的集成是个复杂课题，关于此方面的讨论已经超出本书范围。

```

dnl # This allows sendmail to use a keyfile that is shared with OpenLDAP's
dnl # slapd, which requires the file to be readable by group ldap
dnl #
dnl define(`confDONT_BLAKE_SENDMAIL',`groupreadablekeyfile')dnl
dnl #

```

下列命令指定找不到目的地时电子邮件相关的操作:

```

dnl define(`confTO_QUEUEWARN',`4h')dnl
dnl define(`confTO_QUEUERETURN',`5d')dnl
dnl define(`confQUEUE_LA',`12')dnl
dnl define(`confREFUSE_LA',`18')dnl
define(`confTO_IDENT',`0')dnl
dnl FEATURE(delay_checks)dnl
FEATURE(`no_default_msa',`dnl')dnl

```

这个FEATURE命令设置默认的sendmail shell——smrsh。mailertable.db与不同域名相关联:

```

FEATURE(`smrsh',`/usr/sbin/smrsh')dnl
FEATURE(`mailertable',`hash -o/etc/mail/mailertable.db')dnl
FEATURE(`virtuallertable',`hash -o/etc/mail/virtuallertable.db')dnl
FEATURE(`redirect')dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
dnl #
dnl # The -t option will retry delivery if e.g. the user runs over his quota.
dnl #
FEATURE(local_procmail,`,`,`procmail -t -Y -a $h -d $u')dnl
FEATURE(`access_db',`hash -T<TMPF> -o/etc/mail/access.db')dnl
FEATURE(`blacklist_recipients')dnl

```

如果根用户想登录, 则EXPOSED_USER命令要求输出完整的电子邮件地址:

```

EXPOSED_USER(`root')dnl
dnl #
dnl # The following causes sendmail to only listen on the IPv4 loopback address
dnl # 127.0.0.1 and not on any other network devices. Remove the loopback
dnl # address restriction to accept email from the internet or intranet.
dnl #

```

默认情况下, sendmail只对本地计算机监听和处理电子邮件。如果要想让sendmail服务器为网络上的其他计算机服务, 则要在命令前面加上dnl, 并将其从下列命令中删除:

```

DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 587 for
dnl # mail from MUAs that authenticate. Roaming users who can't reach their
dnl # preferred sendmail daemon due to port 25 being blocked or redirected find
dnl # this useful.
dnl #

```

如果激活下列DAEMON_OPTIONS命令, 则sendmail监听发送用户名与口令的用户的电子邮件, 即其电子邮件管理器经过验证。这个过程通过TCP/IP端口587工作:

```
dnl DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
dnl #
dnl # The following causes sendmail to additionally listen to port 465, but
dnl # starting immediately in TLS mode upon connecting. Port 25 or 587 followed
dnl # by STARTTLS is preferred, but roaming clients using Outlook Express can't
dnl # do STARTTLS on ports other than 25. Mozilla Mail can ONLY use STARTTLS
dnl # and doesn't support the deprecated smtps; Evolution <1.1.1 uses smtps
dnl # when SSL is enabled-- STARTTLS support is available in version 1.1.1.
dnl #
dnl # For this to work your OpenSSL certificates must be configured.
dnl #
```

如果要求与sendmail服务器的安全连接, 则可以激活这个命令, 其要求使用TLS。但是, 正如说明中所述, 如果用户使用Microsoft Outlook Express或Evolution 1.1.1以下, 则不能激活这个命令。

```
dnl DAEMON_OPTIONS(`Port=smtps, Name=MSMTA, M=s')dnl
dnl #
dnl # The following causes sendmail to additionally listen on the IPv6 loopback
dnl # device. Remove the loopback address restriction listen to the network.
dnl #
dnl # NOTE: binding both IPv4 and IPv6 daemon to the same port requires
dnl #       a kernel patch
dnl #
```

如果网络配置成使用IPv6 (见第20章介绍), 则要激活下面这个命令。IPv6的这个命令与前面只接受本地计算机邮件的默认命令等价:

```
dnl DAEMON_OPTIONS(`port=smtp,Addr=::1, Name=MTA-v6, Family=inet6')dnl
dnl #
dnl # We strongly recommend not accepting unresolvable domains if you want to
dnl # protect yourself from spam. However, the laptop and users on computers
dnl # that do not have 24x7 DNS do need this.
dnl #
```

这个FEATURE命令表示sendmail不进行电子邮件的DNS逆向查找。除非具有DNS服务器的可靠访问权并且能够接受更多的通信流, 否则不要修改这个命令。

```
FEATURE(`accept_unresolvable_domains')dnl
dnl #
```

这个FEATURE命令可以对DNS数据库中指定的邮件服务器使用MX记录。关于DNS的更多信息, 见第24章。

```
dnl FEATURE(`relay_based_on_MX')dnl
dnl #
```

```
dn1 # Also accept email sent to "localhost.localdomain" as local email.
dn1 #
```

LOCAL_DOMAIN命令指定本地计算机别名，`/etc/hosts`中的默认别名为**localhost.localdomain**。

```
LOCAL_DOMAIN('localhost.localdomain')dn1
dn1 #
dn1 # The following example makes mail from this host and any additional
dn1 # specified domains appear to be sent from mydomain.com
dn1 #
```

MASQUERADE_AS命令改变**sendmail**连接到出站电子邮件的标签。如果要激活这个命令，则将**mydomain.com**改成所要的标签，通常用于指定子域的电子邮件。例如，如果在**mommabears.com**网络上，则可以将**MASQUERADE_AS**设置为**linux.mommabears.com**。

```
dn1 MASQUERADE_AS('mydomain.com')dn1
dn1 #
dn1 # masquerade not just the headers, but the envelope as well
dn1 #
dn1 FEATURE(masquerade_entire_domain)dn1
dn1 #
dn1 # masquerade not just @mydomainalias.com, but @*.mydomainalias.com as well
dn1 #
dn1 FEATURE(masquerade_entire_domain)dn1
dn1 #
```

MASQUERADE_DOMAIN命令可以让**sendmail**以相同的方式处理来自其他域的电子邮件地址。例如，激活下列命令时，将来自这些子域（**localhost**、**localhost.localdomain**、**mydomainalias.com**与**mydomain.lan**）的电子邮件设置成前面用**MASQUERADE_AS**命令指定的域。

```
dn1 MASQUERADE_DOMAIN(localhost)dn1
dn1 MASQUERADE_DOMAIN(localhost.localdomain)dn1
dn1 MASQUERADE_DOMAIN(mydomainalias.com)dn1
dn1 MASQUERADE_DOMAIN(mydomain.lan)dn1
```

下列**MAILER**命令指定实际发送电子邮件的服务器类型。

```
MAILER(smtp)dn1
MAILER(procmail)dn1
```

修改sendmail.mc

开始修改之前，最好先备份**/etc/mail**目录中的**sendmail.cf**与**sendmail.mc**文件。

默认**sendmail.mc**配置文件中有两行需要改变。首先，这一行限制**sendmail**服务器只向指定的地址发送电子邮件，**127.0.0.1**是本地计算机的回环地址：

```
DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
```

如果具有可靠的DNS访问和高速的Internet访问, 则可以将下一行标作为说明语句。它防止sendmail检查与入站电子邮件地址相关的域。可以在此行前面加上dnl将其标为说明语句, 重新启动sendmail服务时, sendmail自动开始检查域:

```
FEATURE('accept-unresolvable_domains')dnl
```

了解submit.mc

submit.mc宏文件用于生成submit.cf, 这是出站电子邮件的sendmail配置文件, 可以和sendmail.mc一样处理, 但这个文件更简单。一般来说, 不需要对这个文件作任何改变, 但最好知道这个文件, 以了解需要配置哪些其他文件。

这些开始命令实际上与sendmail.mc文件中的开始命令相同, 可以见本章前面介绍:

```
divert(-1)dnl
divert(0)dnl
include(`/usr/share/sendmail-cf/m4/cf.m4')
VERSIONID('linux setup for Red Hat Linux')dnl
```

confCF_Version命令只是增加版本名。

```
define(`confCF_VERSION', `Submit')dnl
```

这个命令增加邮件系统类型。类似于sendmail.mc中的OSTYPE('linux')dnl命令。

```
define(`__OSTYPE__', `')dnl dirty hack to keep proto.m4 from complaining
```

DECNET是一种旧式大型机和微型机中很常见的网络类型。

```
define(`_USE_DECNET_SYNTAX_', `1')dnl support DECnet
```

confTIME_ZONE变量增加时间标志。

```
define(`confTIME_ZONE', `USE_TZ')dnl
```

这个设置避免通过任何NIS表寻找用户与口令, 其它用户与口令源为/etc/passwd。

```
define(`confDONT_INIT_GROUPS', `True')dnl
```

这个命令设置进程标识符(PID)文件。

```
define(`confPID_FILE', `/var/run/sm-client.pid')dnl
```

confDIRECT_SUBMISSION_MODIFIERS变量假设使用标准“规范”主机名。

```
dnl define(`confDIRECT_SUBMISSION_MODIFIERS', `C')
```

use_ct_file FEATURE读取/etc/mail/trusted-users中的标准用户。

```
FEATURE('use_ct_file')dnl
```

```
dnl
```

```
dnl If you use IPv6 only, change [127.0.0.1] to [IPv6:::1]
```

这个命令指定本地计算机(127.0.0.1)上的消息提交程序(msp)。

```
FEATURE('msp', `[127.0.0.1]')dnl
```

大多数情况下, 不需要对这个文件作任何改变。需要改变时, 记住先要进行备份。如果安装了sendmail-doc-* RPM包, 则可以从/usr/share/doc/sendmail目录的README.cf文件中

得到关于这个文件的更多信息。

处理与重新激活sendmail

如果不设置备份，则现在可以备份当前的sendmail.cf配置文件。进行所要的改变之后，要用m4宏处理器或make -C /etc/mail命令生成新的sendmail.cf文件，然后用下列命令重新启动sendmail监控程序：

```
# m4 /etc/mail/submit.mc > /etc/mail/submit.cf
# service sendmail restart
```

这些命令要求先安装sendmail-cf-* RPM。

使用入站电子邮件服务器

两个基本入站电子邮件服务器非常常用。这些服务器对应于两个主要的入站电子邮件协议POP3与IMAP4。在Red Hat Linux中，这两个服务器都由imap-* RPM包提供，并已经安装成xinetd服务（见第23章）。

不需要生成自己的电子邮件服务器。可以将自己的客户设置成使用mail.com与yahoo.com之类的提供者电子邮件。如果想生成自己的电子邮件服务器，则要安装imap-* RPM包。记住用service servername on命令激活其xinetd配置，然后运行service xinetd reload命令，保证xinetd重新读取相应的配置文件。

如果局域网上有DNS服务器，则还可以用相应/var/named数据库文件中的MX项目进行配置。关于DNS的细节见第24章。

POP3协议在Internet上仍然很普及。从电子邮件客户机连接时，POP3服务器会自动下载电子邮件。对大多数客户机，可以在服务器上保持电子邮件的原备份。

而IMAP4协议更灵活。如果使用IMAP4服务器，则可以在服务器中用文件夹管理电子邮件。可以搜索不同消息中的关键字，也可以下载所要的消息。这在拥有多台计算机的用户想把电子邮件放在中央数据库中时非常有用。

POP3电子邮件服务器

激活POP3服务器之后，要生成账号。任何要使用POP3服务器的人都要在系统中有个账号。但是，这些用户不需要主目录。

第9章曾介绍过，useradd username命令自动对新用户生成主目录。但是，如果直接编辑/etc/passwd而增加新用户，则不会生成主目录。然后可以用passwd username命令指定新口令。

生成账号之后，要让用户将配置为电子邮件服务器的计算机的FQDN和用户名加进其电子邮件客户机中。本章稍后会详细介绍如何在电子邮件客户机中进行这些操作。

IMAP4电子邮件服务器

激活IMAP4服务器之后，也要生成账号（像POP3服务器中一样）。如果有人要用IMAP4服务器，则要在系统中有个账号。与POP3服务器不同的是，IMAP4服务器的用户必须在系

统中有主目录。

第9章曾介绍过，`useradd username`命令自动对新用户生成主目录。然后可以用`passwd username`命令指定新口令。

和POP3服务器中一样，生成账号之后，要让用户将配置为电子邮件服务器计算机的FQDN和用户名加进其电子邮件客户机中。

配置邮件客户机

大多数人使用图形邮件客户机，如Evolution与Netscape。但是，基于文本的邮件客户机仍然在Linux与UNIX世界中很普及。熟练的Linux管理员喜欢用命令行界面，因此也喜欢用基于文本的邮件客户机。尽管图形邮件客户机很漂亮，但大量用户的图形邮件客户机需要占用邮件服务器的功能。

可能还要帮助用户配置他们自己的邮件客户机，这个过程很简单。

基于文本的客户机

基于文本的邮件客户机在默认情况下可以用mail程序发送和接收电子邮件。不熟悉计算机的人可能喜欢图形邮件客户机，但是许多用户仍然使用基于文本的邮件客户机，特别是在大学和科研机构中。也许两个最常用的基于文本的邮件客户机是pine与elm。尽管红帽子公司计划在今后版本中将它们删除，但pine（Program for Internet News and E-mail）是最友好的基于文本的邮件客户机，因此，我准备在此介绍它。

你的Red Hat Linux中可能没有安装pine客户机，但很容易从pine-* RPM包安装。可以用pine命令方便地启动这个邮件客户机，但是，红帽子公司已经让pine过时，即新版Red Hat Linux中可能改用不同的邮件客户机。图形邮件客户机将在下节介绍。另一个基于文本的邮件客户机是mutt。

首次运行pine时，可以看到一个前言，然后是图26.1所示的主菜单。检查屏幕中间的命令（？、C、I、L、A、S与Q）和屏幕下方的命令选项（？、P、R、O、>、N与K）。



图26.1 pine主菜单

说明: pine命令菜单是Linux中少有的不考虑大小写的情形之一, 例如, P与p是一样的。

可以看出, 可以输入C开始一个邮件消息, 输入I浏览当前消息, 输入L列出当前文件夹, 等等。但第一步要设置pine让其具有阅读电子邮件的功能。输入S命令打开Setup屏幕, 然后输入C开始基本配置, 如图26.2。



图26.2 pine配置信息

pine设置部分包括大量的配置选项, 但只要设置三个选项即可开始接收电子邮件。下列步骤假设电子邮件地址为abcd@example.com, 入站电子邮件服务器为mail.example.com。根据需要进行替换。

- 将personal-name设置成要让电子邮件接收者看到的姓名。
- 将与电子邮件地址相关的域名加到user-domain中。例如, 如果电子邮件地址为abcd@example.com, 则要将example.com加进user-domain字段。
- 设置inbox-path。本例中, 如果mail.example.com是POP3服务器, 则输入{mail.example.com/pop3/user=abcd}INBOX; 如果是IMAP4服务器, 则输入{mail.example.com/user=abcd}。

提示: 有些电子邮件服务器具有特殊要求。例如, 有些域要求完整的电子邮件地址(如abcd@example.com)和inbox-path中的用户名, 还要求入站邮件服务器user-domain使用不同的域名。如果有不明白之处, 可以向电子邮件提供者了解。

如果使用外部SMTP服务器, 如与ISP相关联的SMTP服务器, 则还可以在这里输入。多次按Page Down键, 可以看到pine的大量选项。

说明: 在4.x版本之前, pine无法处理POP3电子邮件。

进行改变之后, 输入E退出设置界面。假设对改变表示满意, 则可以在提示下输入Y确认, 回到图26.1所示的主菜单。在主菜单中输入L, 加亮收件箱并按Enter键。首次这样做时, 程序会提示输入电子邮件口令。

然后, pine进入电子邮件服务器, 取得最新信息, 并在图26.3所示的消息索引中显示(我

盖住了电子邮件的标识)。这里一切都很直观,可以使用屏幕下方的命令选项。要阅读消息,加亮这个消息并按Enter键。



图26.3 pine消息索引

生成新消息也很简单。回到图26.1所示的主菜单,然后输入C开始编写新消息。如果使用过电子邮件,则很容易理解图26.4所示的格式。屏幕下方的命令是控制符,例如,写完消息之后,Ctrl+X命令发送消息(先要按Y确认)。如果已经配置了SMTP服务器或使用sendmail服务,则pine会自动发送消息。



图26.4 生成pine电子邮件

图形客户机

Linux中有三个图形邮件客户机: Evolution、Mozilla Mail与KMail。本书第四部分介绍了这些图形客户机的基本操作。本节介绍这些图形客户机的配置窗口。

对任何电子邮件客户机，配置要求是相同的。和pine文本客户机一样，至少要有表26.2所示的信息。

表26.2 电子邮件客户机所需数据

数据	描述
Name	要让其他用户看到的姓名
Domain Name	电子邮件地址中@后面的信息
Inbox Server	入站邮件服务器的完全限定域名，有时也称“Host”或“Server Name”
Username	邮件服务器上的用户名或登录，通常是电子邮件地址中@前面的信息

配置Evolution

第18章简要介绍了Evolution。使用Evolution时，在喜欢的GUI中打开，然后从菜单栏中单击Tools►Settings打开Evolution Settings窗口，如图26.5。

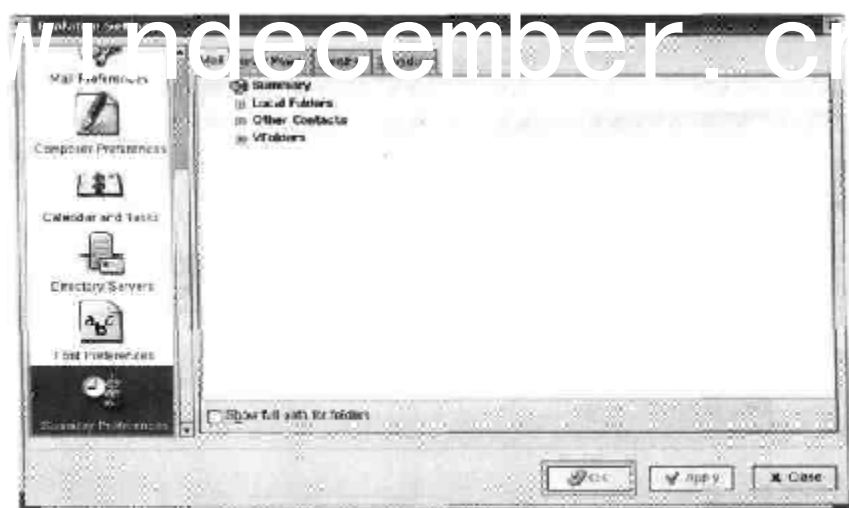


图26.5 Evolution Settings窗口

在左窗格中，向上滚动，直到能够单击Mail Accounts图标，然后单击Add生成新账号或加亮显示现有账号并单击Edit，打开Evolution Account Editor。在Identity标签中输入基本账号信息，然后单击图26.6所示的Receiving Mail标签。必要时选择Server Type，在Host文本框中输入入站邮件服务器，并在Username文本框中输入服务器上的用户名。

配置KMail

如果使用第17章介绍的KMail，则可以在喜欢的GUI中打开，然后从菜单栏中单击Settings►Configure KMail打开Configure窗口（如图26.7），单击左窗格中的Network，然后单击Receiving标签。单击Add按钮生成新账号并选择账号类型（local、POP3、IMAP或Maildir），也可以加亮显示现有账号并单击Modify。

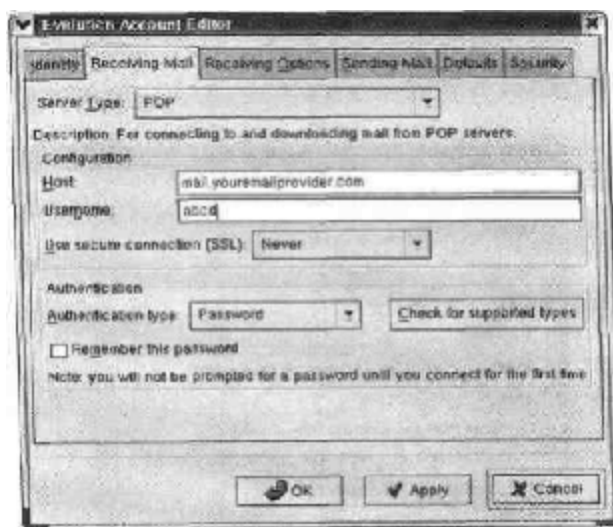


图26.6 配置Evolution邮件账号

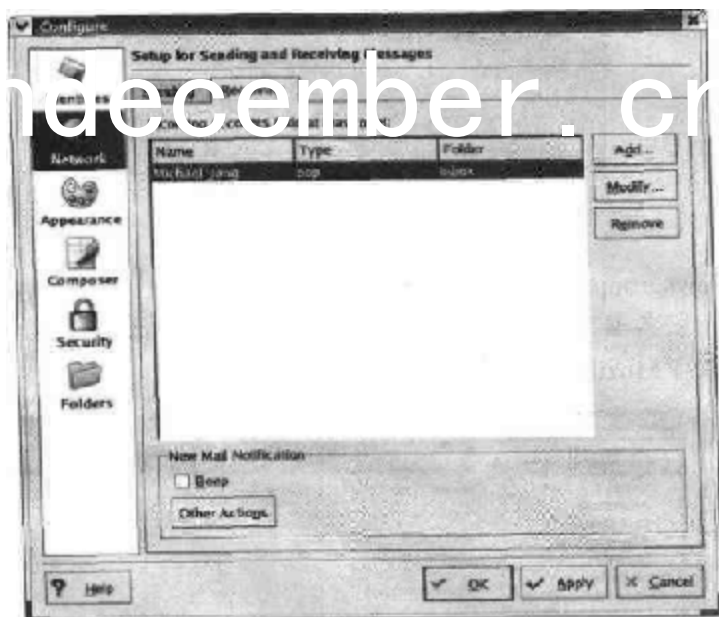


图26.7 配置KMail

这就打开Add Account - KMail或Modify Account - KMail窗口。这两个窗口只有标题不同。图26.8显示了一个例子。输入收件人收到电子邮件时看到的姓名，并在必要时指定一个口令。然后必要时选择Server Type，在Host文本框中输入网站邮件服务器，并在Username文本框中输入服务器上的用户名。

配置Mozilla Mail

如果使用Mozilla Mail，则可以看到它与Netscape 6.x邮件客户机有着惊人的相似。这是可能的，因为Netscape已经使用GPL许可证（见说明）。在喜欢的GUI中打开Mozilla

Mail, 从菜单栏中单击Edit►Mail & Newsgroups Account Settings打开Mail & Newsgroups Account Settings窗口。如果还没有生成电子邮件账号, 则要先完成Mozilla Mail Account Wizard步骤。

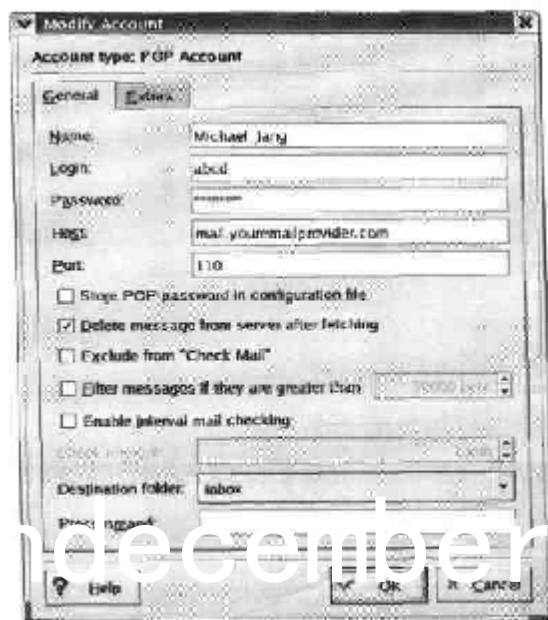


图26.8 配置KMail电子邮件账号

在Mail & Newsgroups Account Settings窗口中, 加亮显示账号名, 并在此输入标识信息。然后加亮显示服务器设置, 如图26.9, 可以看到Server Name文本框中显示的人站电子邮件服务器名。关于Mozilla Mail的更多信息见第16章。

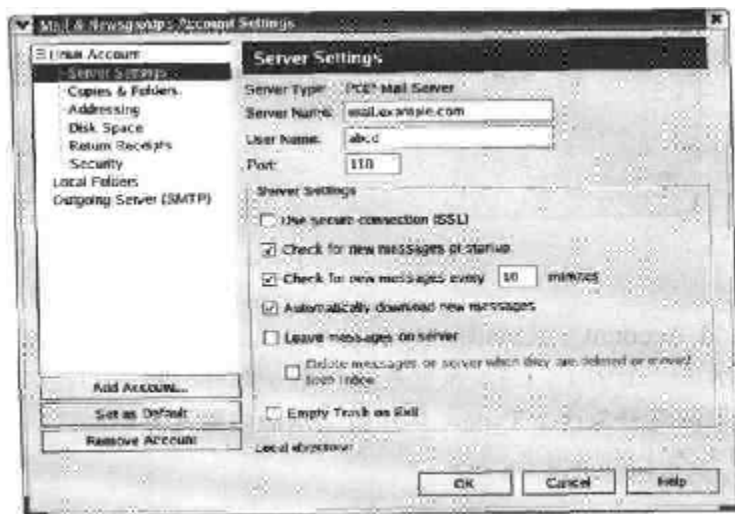


图26.9 加亮显示服务器设置

说明: 并不是每个开放源代码自由软件基金会社区成员都喜欢Netscape许可证, 原因见www.gnu.org/philosophy/netcape-npl.html。

小结

有的服务器发送电子邮件，有的服务器接收电子邮件。现代版本使用一些基本TCP/IP协议：SMTP、POP3与IMAP4。要通过这些协议发送和接收电子邮件，可以选择下列三种邮件服务：MTA、MDA与MUA。sendmail之类的MTA通过网络发送电子邮件。procmail之类的MDA从Internet取得消息并将其存放在池中，有时放在入站电子邮件服务器中；MUA是个电子邮件客户机，如pine、Kmail、Mozilla Mail与Evolution。

sendmail是目前Internet上最常用的出站电子邮件服务器。由于编辑sendmail.cf配置文件很难，因此红帽子公司提供了宏文件sendmail.mc，使得理解和编辑更容易。很容易用m4宏处理器转换成sendmail.cf。还有其他重要的sendmail配置文件（包括/etc/sysconfig/sendmail与/etc/aliases）和/etc/mail目录中的其他文件。有了新的sendmail.cf文件之后，可以用service sendmail restart命令让sendmail监控程序重新读取这个文件。

符合POP3与IMAP4协议的电子邮件服务器有两个基本选项。每个服务器都有安全版本，都是xinetd服务，可以从imap-* RPM包安装。安装并激活这些服务之后，用户需要电子邮件服务器的完全限定域名和用户名。如果是IMAP4服务器，则还要有电子邮件文件的主目录。

文本和图形电子邮件客户机都在使用。pine是一个十分有用而高配置的可配置的文本客户机。图形电子邮件客户机有多种，包括Evolution、Mozilla Mail与KMail。

下一章将介绍各种FTP客户机和服务器。FTP客户机很灵活，甚至可以用FTP命令连接和升级RPM包，可以在Red Hat Linux计算机上安装匿名、标准和安全的FTP服务器。

.

.

.

第七部分 Linux文件共享服务

第27章 FTP客户机和服务器

文件传输协议（FTP）是最古老的TCP/IP协议栈成员之一，但至今仍然广泛使用。顾名思义，FTP针对文件传输进行优化。尽管也可以通过其他协议（如HTTP）或加密服务（如SFTP）下载文件，但FTP速度更快。我在红帽子公司发布新版Linux发行版本时用FTP下载光盘文件，同样是利用DSL连接，同一传输媒介上的FTP下载速度是HTTP下载速度的两倍。

和其他服务一样，有FTP客户机和FTP服务器。FTP客户机有许多相关的命令，甚至可以通过正确的ftp命令直接更新RPM包。当然，FTP客户机也有使用GUI界面的。

Linux有许多FTP服务器，本章介绍其中两种：超安全FTP（vsFTP）和华盛顿大学的圣路易斯WU-FTP。这两种服务器都可以配置成支持匿名用户。vsFTP是目前默认的，WU-FTP是Red Hat Linux 8.0以前默认的FTP服务器，但Red Hat Linux 9中没有包括这个FTP服务器。尽管这两个服务器都不是真正安全的，但它们都有自己的配置文件，可以控制允许访问的用户和计算机。两者都能够保护系统中的其他文件和目录。本章介绍下列主题：

- 使用FTP客户机
- 配置安全FTP服务器
- 生成匿名FTP服务器
- 用实名配置WU-FTP

使用FTP客户机

FTP服务已经有很长的历史，其命令在bash之类的shell以前就有了。要学会使用FTP客户机，因为关键的Red Hat RPM包都是在FTP服务器上更新的。和其他Linux客户机一样，gFTP（GNOME FTP）之类的图形FTP客户机只是文本控制台中所用命令的“前端”。

下面几节介绍从FTP客户机到红帽子公司的主FTP站点ftp.redhat.com的连接。这个站点通常很忙，特别是在美国的上班时间。红帽子公司列出了大量的FTP镜像站点（www.redhat.com/download/mirror.html），包括ftp.redhat.com中一样的更新文件。如果无法访问红帽子公司的主FTP站点，可以试着访问这些镜像站点。

基本命令

如图27.1所示，FTP客户机有大量命令。这里只介绍几个最重要的命令，即使很少用到的FTP命令，也可以用man ftp命令打开FTP手册进行查询。可以从ftp>提示下输入help command，打开一个命令的简单描述。

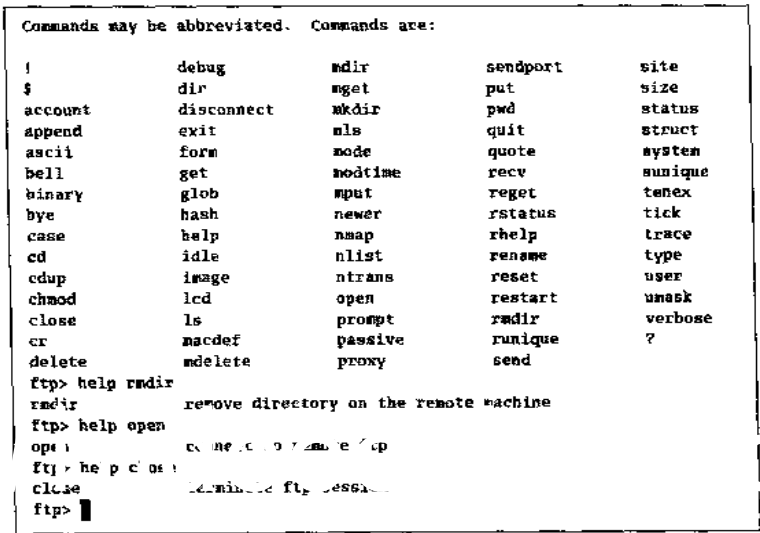


图27.1 FTP客户机命令

表27.1列出了几个重要FTP命令。注意这些命令与bash shell中一些命令的相似之处。

表27.1 基本FTP客户机命令

命令	描述
!command	在本地计算机的本地目录中运行shell命令
ascii	将文件传输方式设置为ASCII方式，适合文本文件
binary	将文件传输方式设置为二进制方式，适合可执行文件和压缩文件
bye	从当前FTP会话退出，是exit的同义词
cd	改变目录，类似于这个命令的Linux版本
dir	等于ls -l shell命令
get ftpfile localfile	将ftpfile从FTP服务器复制到本地计算机上的localfile，mget可以使用通配符，也称为全局化
ls	见dir
put localfile ftpfile	将本地计算机上的localfile复制到FTP服务器上的ftpfile，mput可以使用通配符，也称为全局化
pwd	列出FTP服务器上的当前工作目录，如果安全配置FTP，则FTP服务器上看到的根目录是FTP文件的主目录，通常是/var/ftp
user	可以输入用户名，提示输入口令

连接ftp.redhat.com

下面看看命令行FTP客户机的用法。假设Linux计算机已经连接了Internet，运行ftp ftp.redhat.com命令。红帽子FTP主站点只允许匿名连接。尽管图27.2所示的命令好像需要口令，但其实并不需要特殊口令。习惯上，匿名连接FTP服务器时，可以在提示输入口令时输入你的电子邮件地址。

```
[root@RH9Desk root]# ftp ftp.redhat.com
Trying 66.77.185.6...
Connected to ftp.redhat.com (66.77.185.6).
220 Red Hat FTP server ready. All transfers are logged.
Name (ftp.redhat.com:root): anonymous
331 Please specify the password.
Password:
230 Login successful. Have fun.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

图27.2 连接FTP服务器

说明：可以在自己的网络上建立FTP连接。按本章稍后“生成匿名FTP服务器”一节介绍的方法生成一个匿名的FTP服务器。一旦服务配置完成，就可以用ftp localhost命令从本地计算机连接。

在ftp>提示下，输入所需的命令。试使用上节介绍的一些命令。可以看到，put之类的命令无法工作，匿名用户不能写入标准红帽子FTP服务器。

说明：默认情况下，根用户不能访问任何FTP服务器。如果以根用户身份通过FTP登录，则即使输入的口令正确，也会被拒绝。

例如，导航到i386 Rawhide RPM所在的目录。到本书编写时，它们位于/pub/redhat/linux/rawhide/i386/RedHat/RPMS目录中，这里列出了长长的RPM包清单。

说明：尽管其他CPU也有RPM包，但最常见的是i386 Rawhide RPM包。尽管i386 RPM包没有针对其他Intel CPU优化，但也能使用。第10章详细介绍了这个主题。

Rawhide是最新RPM包的红帽子存储区。如果你不喜欢up2date（见第10章介绍），则可以直接更新RPM包。从当前的Rawhide数据库中下载包，可以用图27.3所示的命令。然后可以随意安装或更新这些包。

也可以不用这些过程。第10章曾介绍过，可以用一次性rpm命令直接连接所选FTP服务器，安装最新RPM包。

GUI FTP客户机

当然，还有图形FTP客户机。一个常见的图形FTP客户机是gFTP，可以在GUI中用命令行界面输入gftp启动，打开gFTP客户机，如图27.4。

说明：可以从gFTP包中的普通虚拟控制台运行gftp命令，打开一个与ftp相似的文本方式FTP客户机。

gFTP客户机使用起来很方便，在Bookmarks菜单中预先定义了一些常用站点。但是，选择Bookmarks>RedHat Sites>RH Rawhide时打开的站点不一定是更新的。然而用这种方式建立FTP连接时非常方便。例如，可以试试Bookmarks>RedHat Sites>RH Main。如果红帽子FTP主站点服务器没有过载，则可以打开图27.5所示的红帽子FTP主站点目录。

```
ftp> cd RPMS
250 CWD command successful.
ftp> ls z*
227 Entering Passive Mode (10,252,113,155,11,207).
125 Data connection already open; Transfer starting.
-rwxrwxrwx 1 owner group 1011615 Feb 25 13:42 zebra-0.93b-1.i386.rpm
-rwxrwxrwx 1 owner group 113724 Feb 24 0:40 zip-2.3-16.i386.rpm
-rwxrwxrwx 1 owner group 15425 Feb 24 0:40 zisofs-tools-1.0.4-2.i386.rpm
-rwxrwxrwx 1 owner group 33793 Feb 24 13:47 zlib-1.1.4-8.i386.rpm
-rwxrwxrwx 1 owner group 70750 Feb 24 13:47 zlib-devel-1.1.4-8.i386.rpm
-rwxrwxrwx 1 owner group 1407003 Feb 24 0:41 zsh-4.0.6-5.i386.rpm
226 Transfer complete.
ftp> mget zip*
mget zip-2.3-16.i386.rpm? y
227 Entering Passive Mode (10,252,113,155,11,209).
125 Data connection already open; Transfer starting.
WARNING: 385 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
113724 bytes received in 2.02 secs (55 Kbytes/sec)
ftp> bye
221
[root@RH9Desk root]#
```

图27.3 下载i386 Rawhide RPM包

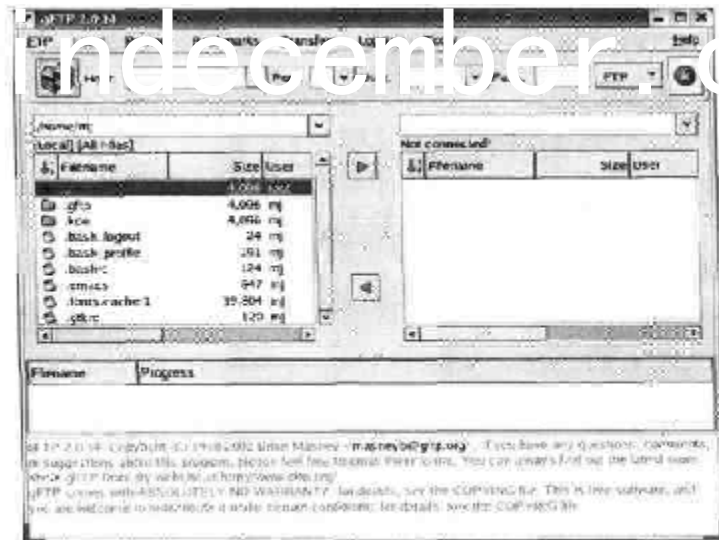


图27.4 gFTP客户机

试比较图27.4与图27.5的差别。选择gFTP书签时，它要求在几个文本框中填入项目（见表27.2）。

表27.2 连接gFTP客户机的项目

项目	作用
Host	FTP服务器的完全限定域名
Port	连接的TCP/IP端口，默认为21
User	连接的用户名，匿名FTP服务器常用anonymous
Pass	与用户名相关联的口令，习惯上建议输入电子邮件地址

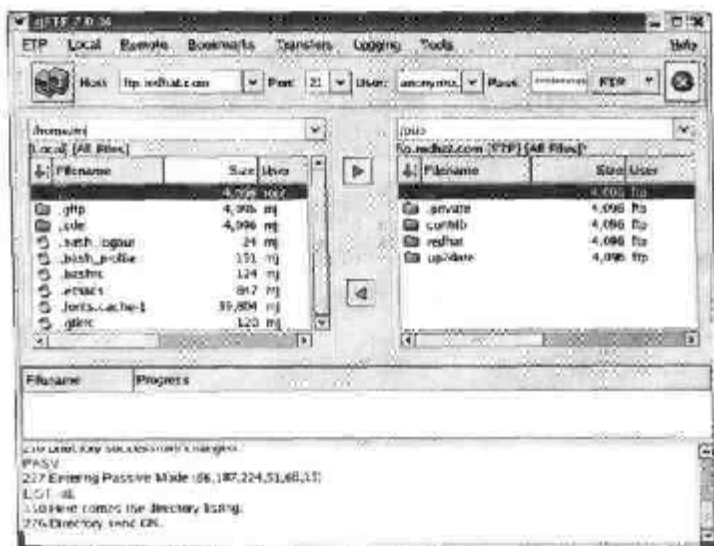


图27.5 红帽子FTP主站点目录

可能还要进入FTP服务器的主目录。要访问所要目录，双击这个目录。记住，双点号(../)表示上一层目录。找到要复制的文件或文件夹之后，加亮选择，然后单击箭头按钮。

可以看看gFTP窗口下方传输的命令与消息。

配置安全FTP服务器

普通FTP服务器的一大缺点是不安全。可以按第23章介绍的方法配置安全FTP服务器，但加密会大大影响性能，而且sftp命令通常不标准。

一个办法是使用超安全FTP服务器——vsFTP。红帽子公司已经把它作为Red Hat Linux 9中的默认和惟一的FTP服务器。旧版Red Hat Linux的默认FTP服务器WU-FTP也放在这里一并介绍，以供熟悉旧版Red Hat的读者参考。

尽管vsFTP并不将通信加密，但可以避免一些WU-FTP中常见的安全问题。许多站点用其作为标准FTP服务器，包括红帽子FTP主站点。它可以配置匿名或实名。事实上，这个服务器的主页（<http://vsftpd.beasts.org>）认为它比WU-FTP速度更快。

vsFTP与WU-FTP有许多相同特性。如果可能，下面几节介绍配置文件时会与WU-FTP进行对照。

基本安全特性

与vsFTP相关联的命令通常用最低权限进行配置，从而减少黑客用这些命令取得系统根权限的风险。

配置文件

vsFTP包的/etc目录中有几个配置文件。其中两个配置文件——vsftpd.ftusers与vsftpd.user_list实际上禁止优先用户访问。这个清单很简单，包括一系列用户名单，如root、bin与

adm。主配置文件是/etc/vsftpd/vsftpd.conf。下面一行一行地分析默认配置文件，其中包括几个选项。更多细节可以通过`man vsftpd.conf`命令访问。

我在此放上整个文件及我的注释，帮助读者理解每个命令：

```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are very paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
#
# Allow anonymous FTP?
anonymous_enable=YES
```

第一个注释以#开头，是个说明语句。注意第一个说明语句是错的，它反映的是vsftpd.conf文件的旧地址。默认情况下，vsFTP允许用上述命令匿名访问。用户可以以用户名anonymous或ftp匿名登录。

```
# Uncomment this to allow local users to log in.
local_enable=YES
```

默认红帽子配置变量local enable使FTP服务器中具有普通账号的用户可以以实名登录。

这些用户能够访问FTP服务器上的所有目录（包括根目录`/`）。可能要求write_enable命令标为说明语句，否则登录用户对系统具有写入访问权限，这会非常危险。还可以配置所有非优先用户的访问权限，见下面介绍的nopriv_user变量。

为了减少问题，可以增加chroot_local_user=YES命令，使用户无法访问FTP服务器上的根目录`/`。但是，如果用户能够上传主目录，则可以上传可执行文件，从而破坏服务器的安全性。

默认红帽子配置文件允许实名用户删除主目录中的文件，但不允许匿名用户删除文件。

```
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
```

如果没有这个umask命令（见第6章介绍），则上传的文件读取和写入权限限于文件拥有者。利用这个命令，所有用户至少有上传文件的读取权限。

```
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
```

有时要让匿名用户上传到FTP服务器。尽管让用户上传到/var文件系统的分区有一定风险，但可以限制这个风险，将/var装载到不同分区中，见第7章介绍。稍后介绍匿名服务器时将会介绍，要对接收上传的目录设置相应权限，如/var/ftp/pub。注意默认vsftpd.conf配置文件中关闭这个设置。

```
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
```

也可以让匿名用户生成具有写入权限的新目录。注意命令前面将这个设置关闭的说明标志（#），还要增加`anon_other_write_enable=YES`语句，让用户实际可以将文件写入新目录中。

```
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
```

默认情况下，用户可以看到不同目录中`.message`文件的消息。用户转入这个目录时，显示相关`.message`文件的消息（也可以用`message_file=filename`命令指定不同文件名）。

```
# Activate logging of uploads/downloads.
xferlog_enable=YES
```

通常，上传与下载的记录存放在`/var/log/vsftpd.log`中。可以用`xferlog_file=filename`命令指定不同文件。

```
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
```

有些FTP客户机可能要求上述命令。端口20是`/etc/services`中显示的一个TCP/IP端口。

```
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
```

上传文件的用户不一定要拥有这个文件。例如，下列命令与`vsftpd.conf`文件中看到的稍有不同，可以将任何上传文件的拥有者改成mj：

```
chown_uploads=YES
chown_username=mj
```

然后看看标准日志文件地址：

```
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
```

通常，**vsFTP**日志文件存放在`/var/log/vsftpd.log`中，可以改成其他地址。

```
# If you want, you can have your log file in standard ftpd xferlog format
xferlog_std_format=YES
```

这个命令可以用标准格式登记FTP服务器的上传与下载，**WU-FTP**中就使用这个命令。可以在命令前面加上#号将其关闭。编写这个文件，然后建立从FTP连接的传输，然后阅读`/var/log/vsftpd.log`文件中的结果。非标准**vsFTP**日志格式更有描述性。

```
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
```

vsFTP服务器规定用户登录时可以待机多长时间，默认为300秒。上述命令激活时将这个时间改成10分钟。

```
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
```

有时文件传输过程中可能发生错误。如果发生错误，则FTP客户机会试图重新连接。但有时不如重新启动连接。默认时间为300秒，上述命令激活时将这个时间改成2分钟。

```
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
```

启用上述命令可以设置特殊的非优先用户ftpsecure，这时一定要在/etc/passwd中使用户退出。

设置特殊的FTP用户

可以把ftpsecure设置成“guest”式用户。配置之后，所有连接FTP服务器的用户都得到ftpsecure用户名。如果不想让用户直接登录你的计算机，则可以改变/etc/passwd中的相关项目，将/sbin/nologin设置为默认shell：

```
ftpsecure:x:601:601 :/home/ftpsecure:/sbin/nologin
```

下列命令可以让功能更强的FTP客户机取消下载而不死机：

```
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
```

但是，本章前面介绍的普通命令行FTP客户机不需要这个设置。

```
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that turning on ascii_download_enable enables malicious remote parties
# to consume your I/O resources, by issuing the command "SIZE /big/file" in
# ASCII mode.
# These ASCII options are split into upload and download because you may wish
# to enable ASCII uploads (to prevent uploaded scripts etc. from breaking),
# without the DoS risk of SIZE and ASCII downloads. ASCII mangling should be
# on the client anyway..
#ascii_upload_enable=YES
#ascii_download_enable=YES
```

如果要在ASCII方式中传输文件，则可以启用上面一个或两个“ascii”命令，这通常不需要，即使文本文件也是这样，除非要保留一定类型的格式。

```
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
```

可以在用户登录之前对其配置上述ftpd_banner消息。例如，可以将消息改成如下，只让匿名登录：

```
# ftp_banner=Welcome. Type ftp at the prompt for an anonymous login.
```

有时黑客会对FTP服务器进行其他攻击，如第22章介绍的“ping到死机”。

```
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
```

如果启用上面两个命令，则可以在`/etc/vsftpd.banned_emails`中建立一列不让访问的匿名口令，拒绝黑客用自动化工具访问，避免FTP服务器被ping到死机。

```
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
```

如果激活`chroot_list_enable=YES`，则可以配置一组用户，其主目录为`/etc/vsftpd.chroot_list`中的主目录（/）。如果能配置`chroot_local_user=YES`，则`/etc/vsftpd.chroot_list`中清单的效果正好相反。

```
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
```

如果激活上述命令，则FTP客户机可以在任何目录上运行`ls -R`命令，使用户可以看到子目录内容。但这是默认关闭的，多次登录FTP服务器的用户可能因为在所有会话中运行`ls -R`命令而产生大量负载。

```
pam_service_name=vsftpd
```

`pam_service_name`列出与vsFTP相关联的PAM（可插入验证模块）文件。关于PAM的更多信息，见第22章。

```
userlist_enable=YES
```

这个命令使vsFTP检查`/etc/vsftpd.user_list`文件中禁止的用户名。

```
#enable for standalone mode
listen=YES
```

这样就使vsFTP可以作为单独的监控程序运行，用`/etc/rc.d/init.d`目录中的`vsftpd`脚本支持。否则可以将vsFTP作为`xinetd`脚本运行，见第23章介绍。

生成匿名FTP服务器

生成匿名FTP服务器并不困难。但是，保护这个服务器涉及到许多细节。正确配置服务

器之后，用户无法超越基础FTP目录/var/ftp，当然无法访问根目录（/）。默认的红帽子FTP配置基于vsFTP服务器。

本节介绍如何生成基本的匿名FTP服务器，适用于vsFTP或WU-FTP服务器。可以用本章稍后介绍的许多设置进一步定制配置。

配置vsFTP

安装适当的包之后，需要激活服务。假设使用vsFTP，则要运行service vsftpd start命令。记住用适当的chkconfig命令（见第13章）保证在下次启动Linux时激活vsFTP。

前面曾介绍过，vsFTP配置文件vsftpd.conf默认允许匿名访问。

vsFTP配置文件中支持匿名服务器的最关键命令已经在本章第一部分介绍，见/etc/vsftpd/vsftpd中的anonymous_enable命令。下面介绍WU-FTP的配置文件。

配置WU-FTP

如果安装WU-FTP服务器，则要处理几个/etc/ftp*配置文件，见下面几节的介绍。下一节“用实名配置WU-FTP”介绍每个配置文件的细节。

说明：Red Hat Linux中不再包括WU-FTP，但可以从FTP站点ftp.wu-ftp.org或SneakEasy RPM库站点www.rpmsf.com下载。

匿名目录

可以在WU-FTP上设置基本的匿名FTP连接。要有anonftp-* RPM包以便在/var/ftp中安装几个子目录，存放FTP用户在这个目录及其子目录中导航时所需的文件与命令。表27.3列出了这些子目录。

表27.3 匿名目录

目录	描述
/var/ftp/bin	可执行shell命令，可用的命令有限
/var/ftp/etc	配置文件，默认包括passwd与group的缩写版本
/var/ftp/lib	程序库
/var/ftp/pub	用户文件，可以配置上传权限

WU-FTP是个xinetd服务，适用第23章介绍的技术。保证/etc/xinetd.d/wu-ftp中没有关闭这个服务，并且/etc/hosts.deny（以及可能激活的任何iptables防火墙）中没有阻止这个服务。

限制访问

很容易限制匿名用户对FTP服务器的访问。首先打开/etc/ftpaccess配置文件。默认情况下，这个配置文件包含下列项目：

```
# User classes . . .
class    all    real,guest,anonymous    *
```


这个FTP访问类可以让所有地址的实名、匿名和客户用户访问。而下列语句则限制192.168.0.0/24网络的匿名用户访问：

```
class    all    anonymous    192.168.0.0/24
```

匿名FTP的安全性

有几个默认措施保护WU-FTP服务器生成的匿名FTP站点。本节介绍这些措施。

限制访问

默认情况下，所有登录定向到/var/ftp目录。可以在/etc/ftpaccess中对所要用户激活下列语句，从而改变这个功能：

```
# realuser user1,user2
```

如果删除说明标志（#），并将user1与user2改成系统中的实际用户，则FTP服务器在这些用户登录时将其发送到主目录，他们可以访问根目录（/）之类的高层目录。

如果要让所有用户访问FTP服务器中从/var/ftp目录开始的位置，则可以将/etc/ftpaccess中这一行语句标为说明语句。

chroot监禁

保护FTP服务器中其他目录的概念是chroot监禁。根据定义，没有比根目录（/）更高层的目录。chroot /abc/def命令可以将有效的根目录改成/abc/def。

在匿名FTP服务器中，/abc/def目录像个根目录（/）。匿名FTP服务器的配置对登录服务器的所有用户采用chroot /var/ftp命令。如果匿名用户要运行cd /var与cd /etc之类的命令，则行不通，因为更高层目录已经用chroot监禁保护起来。

命令限制

还可以限制危险命令。默认情况下，/etc/ftpaccess限制下列四个命令的使用。还可以限制更多命令。例如，如果授权用户可以执行一个命令，则可以将其加进这个表中，防止匿名用户使用：

```
chmod      no    guest,anonymous
delete     no    anonymous
overwrite  no    anonymous
rename     no    anonymous
```

用实名配置WU-FTP

本节和上节的信息基于WU-FTP服务器包，需要从上述第三方站点装入。我们已经介绍了如何启用匿名用户访问。本节介绍与WU-FTP相关的配置文件和如何将其用于系统中的普通用户。

配置文件

很多配置文件都与WU-FTP包有关，且都在/etc目录中，它们是：ftpaccess、ftpconversions、ftpgroups、ftphosts和ftpusers。

这些文件中，ftpusers已经过时，ftpgroups很少使用，这些文件的功能已经加进ftpaccess中。本节详细介绍其他配置文件。

WU-FTP文档的/usr/share/doc/wu-ftp-d-versionnumber/examples目录中也提供了这些配置文件的例子。

/etc/ftpaccess

本章前面已经介绍了默认/etc/ftpaccess文件的几个特性。下面要一行一行地介绍这个文件。开头几行承担/etc/ftpusers的功能：

```
deny-uid %-99 %65534-
deny-gid %-99 %65534-
allow-uid ftp
allow-uid ftp
```

这些行拒绝所有用户号与组号在99以下和65534以上的用户访问。如果检查/etc/passwd与/etc/group文件，则可以看到这些ID号与管理账号相关联。可以用一个简单的改变限制除ftp以外的所有用户的访问：

```
deny-uid *
deny-gid *
allow-uid ftp
allow-uid ftp
```

下列语句设置chroot监禁。所有用户都归类为客户用户，限于主目录中。例如，用户程序登录时，这个消息被发送到/home/mj目录：

```
guestuser *
```

我们已经在上一节介绍过下一行，用户程序不能导航到/home根目录(/)，除非激活下列语句：

```
# realuser user1,user2
```

记住，散列标志（#）使Linux忽略后面的信息。如果删除散列标志（#），则user1与user2取得FTP服务器上的完全用户权限。下列行可以限制realuser清单中的用户。例如，如果上一行为realuser *，则可以将ftpchroot组加进/etc/group中。ftpchroot组的成员无法导航到相应的主目录以上：

```
# guestgroup ftpchroot
```

说明：第9章介绍了/etc/passwd与/etc/group之类的用户与组配置文件的管理。

前面曾介绍过，前几行允许实名、匿名和客户用户登录。后几行（如果激活）限制实名用户从192.168.0.0/24网络登录访问。匿名访问是不允许的，用户必须输入口令。一个明显的缺点是实名用户口令要以明文形式在局域网上传送：

```
class all real,guest,anonymous *
# class all real 192.168.0.0/24
```

如果将上述`guestuser` *行标为说明语句, 则可以将实名换成`guest`:

```
class all guest 192.168.0.0/24
```

如果你是服务器的管理员, 则要换上电子邮件地址:

```
email root@localhost
```

下列命令限制试图登录的次数。这里, 五次登录这个FTP服务器失败后将关闭连接:

```
loginfails 5
```

在Linux与UNIX世界中, `README*`文件常用于说明或对特定目录中包含的包提供更多信息。下列语句在用户登录和转入`README*`文件所在的目录时返回一个**Please read the file README**消息:

```
readme README* login
readme README* cwd=*
```

FTP服务器的管理员可能要向用户发送其他消息。下列语句可以在打开目录的`welcome.msg`文件中增加欢迎信息。也可以编辑`message`文件, 向通过`cd`命令转入这些目录的用户发送其他消息:

```
message /welcome.msg login
message .message cwd=*
```

图27.6显示了在`/var/ftp`目录中增加`README*`文件和在各种消息文件中增加信息时发生的情形。

```
Connected to RH9Test (10.252.113.63).
220 RH9Test FTP Server (Version wu-2.6.2-8) ready.
Name (RH9Test:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-This is a test message welcoming users to a new FTP server
230-
230-You can add the rules or requests of your choice to the welcome.msg.
230-
230-Using this file makes sense for an Anonymous FTP server; otherwise, you'd have to add welcome messages to each user's home directory.
230-
230-Please read the file README
230- it was last modified on Sat Apr 5 15:34:29 2003 - 0 days ago
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd etc/
250-This is a test message warning about the embedded /var/ftp/etc directory
250-
250-Please be careful about anything you might add to this directory.
250-
250 CWD command successful.
ftp> █
```

图27.6 FTP登录消息

可以在FTP服务器中以压缩格式存储软件包。下列命令使访问这些包的用户能够将其自动解压或解包, 这是通过`/etc/ftpconversions`中的命令完成的, 见稍后的“`/etc/ftpconversions`”

一节介绍:

```
compress    yes    all
tar         yes    all
```

上节已经介绍过下列命令。如果保留**guestuser**行,对/etc/ftpaccess行稍做修改(黑体部分),则可以阻止所有用户使用这些命令。

```
chmod       no    guest,anonymous
delete      no    guest,anonymous
overwrite   no    guest,anonymous
rename      no    guest,anonymous
```

FTP服务器登录通常存放在/var/log/messages中,但服务器上来回传输的文件记录在/var/log/xferlog中。

```
log transfers anonymous,guest,real inbound,outbound
```

如果运行**ftput**命令,则其生成一个临时/etc/shutmsg文件。这个命令在FTP服务器即将关闭时拒绝其他登录:

```
shutdown /etc/shutmsg
```

匿名用户可以输入电子邮件地址作为口令。这时可以在var/log/messages中看到其口令。下列命令向连接FTP服务器而没有按正确格式输入电子邮件地址的用户发一个警告。根据配置,用户即使没有输入有效的电子邮件地址,仍然可以登录。

```
passwd-check rfc822 warn
```

/etc/ftpaccess限制

如果在Internet上运行FTP服务器,则要限制同时连接服务器的用户数。这样可以控制用户下载文件的速度。一个简单方法是在/etc/ftpaccess中使用Linux命令。例如,下列命令防止同时登录FTP服务器的用户超过二十人。warning.msg文件在登录FTP服务器的用户达到二十人时向新用户发出如下消息:

```
limit      all      20      Any      warning.msg
```

也许要在上班时间(上午八时到下午五时)限制用户访问,因为这时服务器可能正在进行其他工作:

```
limit      all      20      Wk0800-1700      warning.msg
```

这个命令中的时间语法基于UUCP远程主机描述文件。要寻找这个文件,最简单的方法是用搜索引擎搜索l.sys。

提示: 我喜欢到新闻组中搜索常见Linux问题的答案。记住,全世界的用户与开发人员在不断开发Linux,他们经常通过新闻组和其他许多论坛讨论Linux问题。通过groups.google.com很容易到新闻组中进行搜索。

也可以限制用户可以从FTP服务器下载的数据量。例如,下列命令将下载的数据量限制在100MB:

```
byte-limit out 100000000 all
```



```
ftpshtut +15 "The FTP Server will close in 15 minutes"
ftpshtut 1530 "The FTP server will stop at 3:30 PM"
```

可以将其设置成cron脚本，见第13章介绍。这样就可以有规律地关闭FTP服务器。表27.4列出了其他的FTP服务器命令。

表27.4 FTP服务器命令

命令	描述
ftpwho	列出连接的用户和所在IP地址
ftpcount	列出连接数
ftpshtut	可以现在或在指定时间关闭FTP服务器
ftprestart	停止与重新启动FTP服务器

匿名上传

默认情况下，匿名用户不能在/var/ftp目录中写入任何文件。有时可能要在/var/ftp/pub之类的目录中让用户提供文件。

要允许上传，就要修改/etc/ftpaccess文件和相应目录的权限。例如，下列语句允许上传到/var/ftp/letter目录

```
upload /var/ftp /letter yes cindy ywow 0660
```

在FTP服务器中，这些文件属于用户cindy、组ywow，权限为660，允许用户cindy和组ywow的成员读取和写入上传的文件。

上传目录中也要有正确的权限，为了在目录中写入文件，你至少要有写入和执行的权限。这里chmod 733 /var/ftp/letter命令可以满足这些基本要求。当然，如果要想让服务器上的普通用户读取这个目录中的文件，则可以用chmod 733/var/ftp/letter之类的命令提供更低的权限。关于权限的更多信息，见第6章。

小结

FTP（文件传输协议）至今仍然广泛使用。FTP是针对文件共享进行优化的。文件下载速度和过去一样重要。例如，我们要把下载650MB+红帽子安装光碟文件的时间减到最少。

FTP客户机有文本和图形两种方式。尽管gFTP之类的图形客户机很漂亮，但实际上只是命令行FTP客户机的前端。ftp>命令提示下可以使用大量命令。FTP客户机也很容易连接红帽子FTP站点，下载最新RPM包。gFTP之类的图形客户机的一个优点是方便，例如，它提供了预先配置的书签，可以连接常见的FTP服务器。

默认红帽子FTP服务器是超安全FTP，即vsFTP。开发人员认为它比WU-FTP更有效，这是旧版红帽子默认的FTP服务器。尽管vsFTP仍然以明文形式传输数据，可能危及口令，但避免了WU-FTP中根用户账号被攻击的风险。vsFTP通过命令非优先状态实现这个功能。关键配置文件是/etc/vsftpd.conf，在这个文件中可以配置匿名访问、消息、日志、上传，等等。

我们经常要配置匿名FTP服务器。为此还要有anonftp-* RPM包，在/var/ftp目录中配置

匿名目录。其适用于vsFTP和WU-FTP。匿名用户不能到这个目录以上，这个功能称为chroot监禁。vsFTP可以配置匿名访问。在WU-FTP中，很容易限制匿名访问和/etc/ftpaccess中的关键命令。

也可以根据FTP服务器/etc/passwd文件中的用户账号用实名用户设置WU-FTP。/etc目录中的关键配置文件包括ftpaccess、ftpconversions与ftphosts。只要正确改变，还可以配置用户与时间权限以及FTP服务器上的匿名上传。可以用几个命令管理WU-FTP服务器，包括ftpwho、ftpcount、ftpshut与ftprestart。

下一章介绍Linux与UNIX计算机网络上的服务。NFS（网络文件系统）对计算机间的文件共享进行优化，NIS（网络信息系统）可以用一个数据库配置网络上的登录和其他信息文件。

第28章 Linux共享服务：NFS与NIS

NFS与NIS是Linux与UNIX计算机网络上的两个常见的共享服务。NFS（网络文件系统）对计算机间的文件共享进行优化，NIS（网络信息系统）可以用一个数据库配置网络上的登录和其他信息文件。

装载NFS目录时，可能无法将这个目录与自己计算机上的目录相区别。例如，可以对服务器上的所有用户配置主目录，通过NFS共享。然后将局域网上的客户计算机配置成在引导过程中装载/home。NFS看上去比较复杂，因为它最多使用六个监控程序，但其基本配置文件和命令都很简单。如果你不太熟悉NFS，则可以使用redhat-config-nfs图形工具。本章会介绍如何理解与管理NFS中常见的风险。

每个Linux计算机通常都有自己的基本用户配置文件，如/etc/passwd与/etc/group。在许多局域网中，更简单的方法是所有用户配置相同的用户名和口令。如果没有NIS，则要求所有用户在这台计算机上有账号，每个账号具有相同UID和GID号，这是个非常麻烦的过程。NIS可以配置一个用户和口令数据库，以及其他几个配置文件。本章介绍下列主题：

- 配置NFS服务器
- 使用NFS客户机
- 配置NIS服务器
- 使用NIS客户机

配置NFS服务器

NFS（网络文件系统）是Linux的基础。事实上，与/etc/passwd与/etc/profile所在的同一个setup-* RPM包中就有一个基本NFS配置文件。但是，管理NFS时还要注意几个不同的监控程序。

从NFS服务器设置导出比较容易。基本上，只要对每个共享目录在/etc/exports中增加一行，并与网络共享，就可以了。但要特别注意语法，正确的命令能够保护通过NFS共享的目录。

NFS的一个关键是RPC（远程过程调用），可以在远程装载目录中无缝地运行命令。所有的NFS监控程序都使用RPC。

NFS的GUI配置工具redhat-config-nfs可以配置简单的共享目录。记住，这个GUI配置工具只是本章介绍的NFS配置的前端。

NFS包

也许你已经安装了NFS所要的包。其中一些包是顺利运行Linux系统的基础包。表28.1列出了与NFS相关RPM包。第10章曾介绍过，可以运行rpm -qi packagename命令，进一步了解每个包。

表28.1 与NFS相关的RPM包

包	功能
setup-*	共享NFS目录在/etc/exports中定义
initscripts-*	包括引导过程中装载网络目录的基本脚本
nfs-utils-*	包括基本的NFS命令与监控程序
portmap-*	支持安全NFS远程过程调用（RPC）的连接
quota-*	网络上共享的目录配额，包括rpc.rquotad，这个包不是必需的

基本监控程序

要顺利运行NFS，至少需要五个Linux服务，它们各有不同功能，有的装载，有的保证远程命令指向正确的位置。这些服务通过/etc/rc.d/init.d目录中的nfs、nfslock与portmap脚本启动。下面简要介绍每个监控程序：

基本NFS 自然，有个NFS服务器监控程序——rpc.nfsd，它通过/etc/rc.d/init.d目录中的nfs脚本启动。NFS监控程序还启动装载监控程序（rpc.mountd）并导出共享目录。可以停止或重新启动NFS服务，从而实现配置的改变。

RPC装载 可以用mount命令连接本地目录（如从软盘）或网络目录（如Samba服务器），但还需要一个装载NFS目录的监控程序——rpc.mountd。

端口映射器 portmap监控程序只是定向RPC通信流，但它对NFS服务至关重要。如果不运行portmap，则NFS客户机无法找到从NFS服务器共享的目录。

重新启动与statd 有时NFS服务器会断开连接。你可能计划重新启动，也可能是服务器崩溃了。rpc.statd监控程序和rpc.lockd一起在服务器重新启动之后帮助客户机恢复NFS连接。

锁定 通过共享NFS目录打开文件时，增加一个锁。锁使用户无法用不同改变覆盖同一个文件。锁通过nfslock脚本用rpc.lockd监控程序运行。

设置导出

共享NFS目录在/etc/exports中列出。例如，假设NFS服务器中有一个光驱，要与局域网其他计算机共享。通常，光碟装载到/mnt/cdrom目录。还要共享/tmp目录，帮助共享特殊包。格式很简单：

```
sharedirectory hosts(specs)
```

换句话说，/etc/exports中要指定要共享的目录、要共享的计算机和所要的限制。下面举几个例子：

```
/mnt/cdrom *.example.com(ro,sync) big.example.com(rw,sync)
/tmp *(rw,insecure,sync,no_wdelay,anonuid=600)
```

sharedirectory一目了然，可以用几种方式指定要共享的计算机，可以使用IP地址，但NFS不能识别CIDR语法。表28.2列出了几个例子。

最后，还要指定是否限制和如何限制共享目录的访问。是否共享成只读文件系统？是否共享共享目录中的所有子目录？是否让特定计算机上的根用户具有这个目录的根访问权？尽管本节列出的选项比较古怪，但可以在/etc/exports中指定这类参数，见表28.3。

表28.2 在/etc/exports中指定主机

例子	说明
*.example.com	example.com域中的所有计算机
newcomp	计算机newcomp
10.11.12.13/255.255.255.0	具有指定IP地址和子网掩码的网络

从Red Hat Linux 8.0开始，任何共享目录都要指定sync与async。换句话说，要指定文件永久写入（如写入磁盘）之前，共享NFS目录是否响应命令。

表28.3 /etc/exports共享目录指定

指定	效果
ro	如果目录装载为ro，则用户只能进行只读访问（这是默认）
rw	如果目录装载为rw，则用户可以进行读写访问
sync	所有数据在请求时写入共享
async	NFS在写入数据前可以响应请求
secure	NFS请求（默认）通过1024以下端口经TCP/IP端口发送，默认中，高级安全防护将阻止这些端口
insecure	NFS请求通过1024以上的端口发送
wdelay	如果多台计算机要写入共享NFS目录，则成组写入（默认）
no_wdelay	如果多台计算机要写入共享NFS目录，则数据立即写入。设置为async时，不需要这个设置
hide	NFS默认共享目录（如/home/mj）而不共享其子目录（如/home/mj/.kde）
no_hide	共享NFS目录时自动共享其子目录
subtree_check	导出/usr/sbin之类子目录时，强制NFS服务器检查高层目录（如/usr）的权限（默认）
no_subtree_check	导出/home/mj之类子目录时，不检查高层目录（如/home）的权限
insecure_locks	对旧版NFS客户机，不检查用户是否有请求文件的读访问权，同no_auth_nlm
secure_locks	对旧版NFS客户机，检查用户是否有请求文件的读访问权（默认），同auth_nlm
all_squash	导出文件的UID与GID映射用户anonymous，适用于公用目录
no_all_squash	保留导出文件的UID与GID（默认）
root_squash	根用户的所有请求映射或转换成如同来自用户anonymous的一样（默认）
no_root_squash	根用户具有根目录的完全管理访问权
anonuid=xyz	指定NFS服务器/etc/passwd文件中匿名用户的UID
anongid=xyz	指定NFS服务器/etc/group文件中匿名组的GID

介绍了/etc/exports文件的内容之后，回到前面的例子，现在应该更容易理解了：

```
/mnt/cdrom *.example.com(ro,sync) big.example.com(rw,sync)
/tmp *(rw,insecure,sync,no_wdelay,all_squash,anonuid=600)
```

第一行与example.com域中的所有计算机共享/mnt/cdrom目录。这个目录是只读的，除非从big.example.com计算机建立连接（自然，这要求光碟是可写的）。

下一行与所有计算机共享/tmp目录。连接这个共享的计算机可以读取或写入（rw）/tmp目录。请求可以通过1024以上的TCP/IP端口发送（insecure）。请求写入/tmp之后才能进行任何其他操作（sync）。数据立即写入磁盘，即使其他共享这个目录的计算机也要写入文件（no_wdelay）。装载这个目录时，所有用户得到NFS服务器/etc/passwd文件中与UID 600相关的权限。

保护NFS

共享NFS目录可以在两个层次配置安全性：通过/etc/exports设置和通过防火墙设置。我们只介绍了/etc/exports。如果要阻止外部网络访问NFS共享目录，则可以用相应的iptables命令或/etc/hosts.allow或/etc/hosts.deny中相应的命令。

有时可能要让用户通过防火墙访问NFS共享目录。尽管最好不要通过Internet提供NFS连接，但在企业或组织内部局域网之间允许NFS连接还是比较安全的。

考虑NFS安全和防火墙时，要考虑端口111和2049。从/etc/services中可以看出，端口111与portmap监控程序有关，而端口2049是NFS的信道。

NFS与iptables防火墙

第22章介绍了iptables基础。第3章和第19章曾介绍过，Red Hat Linux防火墙工具lokket与redhat-config-securitylevel可以配置标准的中、高级防火墙。默认高级安全防火墙阻止所有网络通信流，只允许DNS服务器响应。自然，NFS通信所需的两个TCP/IP端口也被阻止。

默认中级安全防火墙如图28.1，阻止从0到1023的所有端口上的所有通信，包括标准portmap端口111，并显式拒绝NFS端口2049移动的数据。

```
Chain INPUT (policy ACCEPT)
target prot opt source destination
RH-Lokkit-0-50-INPUT all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)
target prot opt source destination
RH-Lokkit-0-50-INPUT all -- anywhere anywhere

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

Chain RH-Lokkit-0-50-INPUT (2 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere
REJECT tcp -- anywhere anywhere tcp dpts:0:1023 flags:
SYN,RST,ACK/SYN reject-with icmp-port-unreachable tcp dpt:nfs flags:SYN,
REJECT tcp -- anywhere anywhere
RST,ACK/SYN reject-with icmp-port-unreachable udp dpts:0:1023 reject
REJECT udp -- anywhere anywhere
-with icmp-port-unreachable
REJECT udp -- anywhere anywhere udp dpt:nfs reject-wit
h icmp-port-unreachable
REJECT tcp -- anywhere anywhere tcp dpts:x11:6009 flag
s:SYN,RST,ACK/SYN reject-with icmp-port-unreachable
REJECT tcp -- anywhere anywhere tcp dpt:xfs flags:SYN,
RST,ACK/SYN reject-with icmp-port-unreachable
[root@RH9Test root]#
```

图28.1 标准级安全防火墙

说明：关于iptables防火墙格式的更多信息，见第22章。

首先，删除拒绝NFS数据的规则。如图28.1所示，这些规则在RH-Lokkit-0-50-INPUT防火墙序列中为第三和第五条规则。因此要运行下列命令：

```
# iptables -D RH-Lokkit-0-50-INPUT 5
# iptables -D RH-Lokkit-0-50-INPUT 3
```

然后要保证防火墙接受通过端口111的输入。第22章曾介绍过，可以增加带-I开关的规则。例如，下列命令接受端口111的TCP与UDP输入，作为防火墙中第二和第三条命令：

```
# iptables -I RH-Lokkit-0-50-INPUT 2 -p tcp -m tcp --dport 111 -j ACCEPT
# iptables -I RH-Lokkit-0-50-INPUT 3 -p udp -m udp --dport 111 -j ACCEPT
```

对所作改变表示满意之后，保存防火墙，以便下次启动Linux时使用，命令如下：

```
# iptables-save > /etc/sysconfig/iptables
```

现在就可以通过防火墙设置NFS连接了。

说明：第22章曾介绍过，也可以用service iptables save命令将新的防火墙规则保存到/etc/sysconfig/iptables中。

NFS与TCP/IP防火墙

第23章介绍了与xinetd服务相关的另一种Linux防火墙。/etc/hosts.deny中的命令出错时，可能阻止portmap、rpc.mountd、rquotad、statd和lockd服务。例如，/etc/hosts.deny中最简单的防火墙阻止一切通信流：

```
ALL:ALL
```

前面曾介绍过，xinetd先读取/etc/hosts.allow，因此可以用一个简单命令让portmap通过这个防火墙。例如，可以在/etc/hosts.allow中增加下列命令，让某个网络的IP地址（如192.168.0.0）的portmap通过它：

```
portmap: 192.168.0.0/255.255.255.0
```

其他与NFS相关的服务可以使用相同方法。记住，/etc/hosts.allow与/etc/hosts.deny文件中不允许192.168.0.0/24之类的CIDR语法。

启动NFS

配置导出后，可能也已经定制了防火墙。最后，可以启动NFS，导出准备共享的目录。

用rpcinfo -p命令启动。如果NFS正确运行，则至少可以看到portmap、nfs与mountd的项目，如图28.2所示。

如果没有看到，则说明NFS没有准备好，要启动这些监控程序。可以用service nfs start命令启动rpc.mountd与nfs监控程序，也可以用service portmap start命令启动portmap监控程序。

启动服务之后，可以用相应exportfs命令导出共享目录。表28.4列出了一些选项。

```
[root@RH9Test root]# rpcinfo -p
      program vers proto  port
100000  2      tcp    111  portmapper
100000  2      udp    111  portmapper
100024  1      udp    1024 status
100024  1      tcp    1024 status
991002  2      tcp    1025 sgi_fam
100011  1      udp    947  rquotad
100011  2      udp    947  rquotad
100011  1      tcp    950  rquotad
100011  2      tcp    950  rquotad
100003  2      udp    2049 nfs
100003  3      udp    2049 nfs
100021  1      udp    1026 nlockmgr
100021  3      udp    1026 nlockmgr
100021  4      udp    1026 nlockmgr
100005  1      udp    1027 mountd
100005  1      tcp    2068 mountd
100005  2      udp    1027 mountd
100005  2      tcp    2068 mountd
100005  3      udp    1027 mountd
100005  3      tcp    2068 mountd
[root@RH9Test root]#
```

图28.2 检查NFS监控程序

表28.4 exports命令

命令	功能
exportfs -a	从/etc/exports导出所有共享目录
exportfs -r	改变/etc/exports之后取得共享目录清单
exportfs -u	不导出所有目录
exportfs -v	显示当前的共享目录

现在就可以从NFS客户机连接共享目录了。但还有一件事要做：保证下次启动Linux时启动正确的服务。第13章曾介绍过，可以用适当的chkconfig命令完成这个功能。下列命令检查启动nfs与portmap监控程序的运行级：

```
# chkconfig --list nfs
# chkconfig --list portmap
```

如果需要，下列命令可以保证这些监控程序在相应运行级启动。启动nfs监控程序时，也启动rpc.mountd监控程序和rpc.rquotad监控程序（如有）：

```
# chkconfig --level 235 portmap on
# chkconfig --level 235 nfs on
```

用redhat-config-nf配置

也可以在GUI中用redhat-config-nf配置NFS服务器。要启动redhat-config-nf，运行这个命令，或在GNOME（或KDE）中选择Main Menu（K Menu）►System Settings►Server Settings►NFS Server，打开NFS服务器配置菜单，如图28.3。

要开始配置过程，单击Add按钮打开Add NFS Share窗口，如图28.4。我们将介绍如何用redhat-config-nf配置前面介绍的目录。我们仿真/etc/exports中的下列命令：

```
/mnt/cdrom *.example.com(ro,sync) big.example.com(rw,sync)
/tmp *(rw,insecure,sync,no_wdelay,all_squash,anonuid=600)
```

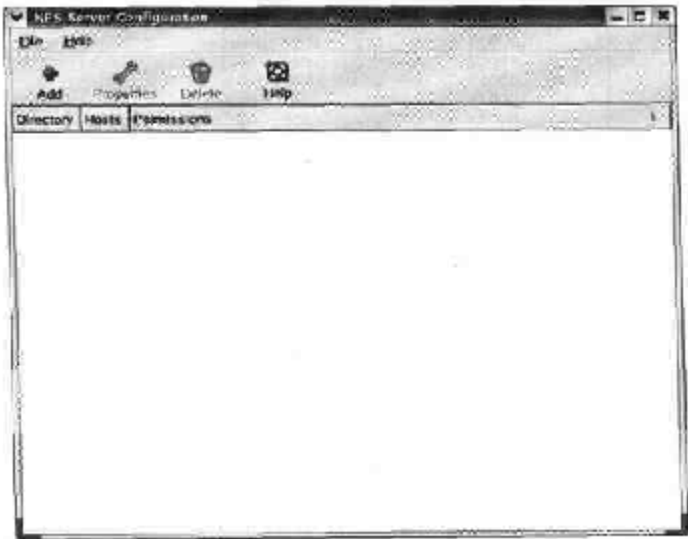


图28.3 NFS服务器配置菜单

如图28.4所示，我们建立了/mnt/cdrom目录的共享，*.example.com域中的计算机具有只读权限。我们可以对big.example.com之类特定的计算机建立/mnt/cdrom和/tmp的另一个共享，使其具有读写权限。

选择General Options标签，如图28.5。可以设置表28.5所示的选项。默认情况下，只激活Sync Write Operations On Request。表28.5列出了每个选项和相应的命令。

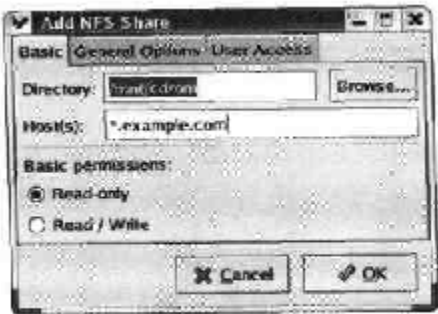


图28.4 Add NFS Share窗口

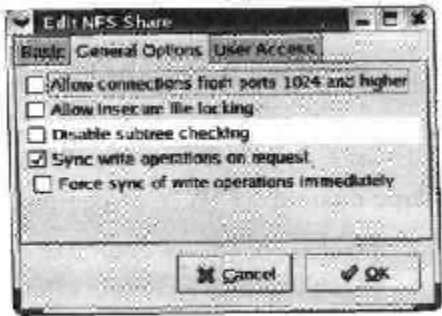


图28.5 General Options标签

表28.5 Add NFS Share窗口的一般选项及相应的NFS/etc/exports命令

选项	命令
Allow Connections From Ports 1024 And Higher	insecure
Allow Insecure File Locking	insecure_locks
Disable Subtree Checking	no_subtree_check
Sync Write Operations On Request	sync
Force Sync Of Write Operations Immediately	no_wdelay

选择User Access标签，如图28.6。表28.6列出了每个选项和相应的命令。

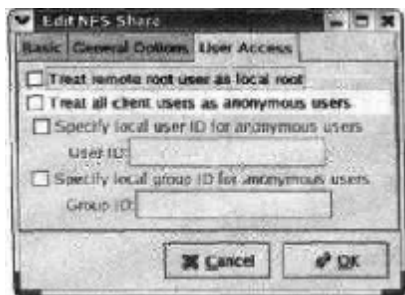


图28.6 User Access标签

表28.6 Add NFS Share窗口的用户访问选项及相应的NFS/etc/exports命令

选项	命令
Treat Remote Root User As Local Root	no_root_squash
Treat All Client Users As Anonymous Users	all_squash
Specify Local User ID For Anonymous Users UID	anonuid= <i>userid</i>
Specify Local Group ID For Anonymous Users Group ID	anongid= <i>groupid</i>

注意这个标签中前两个命令是相互排斥的，换句话说，如果将所有NFS客户机都配置成匿名用户，则不能把远程用户作为根用户。

Specify Local User ID与Specify Local Group ID选项没有用相应NFS命令配置，它们没有意义，因此不需要激活，除非要设置特定用户或组ID。关于用户或组ID的详细信息，见第9章。

得到的/etc/exports文件与原先稍有不同，前面指定的计算机与网络的只读和读写设置需要放在不同行中：

```
/mnt/cdrom *.example.com(ro,sync)
/mnt/cdrom big.example.com(rw,sync)
/tmp *(rw,insecure,sync,no_wdelay,all_squash,anonuid=600)
```

记住，不能单纯用redhat-config-nfs配置NFS。例如，还要保证防火墙不会阻止NFS站点，见本章前面介绍。还要保证下次启动Linux时，nfs与portmap监控程序在相应运行级启动。

使用NFS客户机

NFS客户机不仅需要知道可用的共享目录，还需要知道如何正确装载这些目录和如何将这目录配置成在计算机上下次启动Linux时自动装载。

列出共享目录

只要有服务器的主机名或IP地址，就很容易从NFS服务器中列出共享目录。下列命令给出计算机RHL9上的当前共享目录清单：

```
# showmount -e RHL9
Export list for RHL9:
/home/gb RHL9*
/tmp      *.example.com
```

提示：也可以在NFS服务器中使用showmount -e命令，保证其实际通过/etc/exports导出要共享的目录。

这个命令列出两个共享目录和可以连接每个目录的计算机。如果清单不准确，或这个命令无法工作，则可以采取下列步骤：

检查服务器上的监控程序 nfs、portmap与mountd监控程序是否运行？

检查服务器和客户机上的防火墙 是否有iptables命令阻止端口111和2049？/etc/hosts.deny中的某些NFS服务是否被阻止了？

验证导出了/etc/exports中的目录 在NFS服务器中，运行showmount -e命令。记住，如果修改了这个文件，则要在服务器上运行exportfs -a命令，刷新导出列表。

如果所有其他办法都失败，则可以按第21章介绍的方法进行网络查错。尽管也有测试网络连接的命令，但最常见的网络问题是物理连接。

装载共享NFS目录

假设服务器上的一切顺利，则可以再试试showmount -e NFSserver命令。看到导出表之后，可以将其中一个目录装载到Linux计算机上。下面的例子从RHL9计算机的/tmp目录装载到本地计算机的/tmp目录：

```
# mount -t nfs RH81:/tmp /tmp
```

即在本地/tmp目录中装载一个NFS（-t nfs）文件系统，它是RHL9上的本地/tmp目录。但如果NFS服务器上遇到故障或网络连接遇到故障，则会有风险。假设连接“被挂起”了，则会把控制台锁住。计算机将会一直重试连接，即使NFS服务器可能已经消失。这样，可以用下列带选项（-O）的命令：

```
# mount -t nfs -o soft,intr,timeo=50 RH81:/tmp /tmp
```

其增加NFS服务器可以中断的软装载选项，超时值（timeo）为50个十分之一秒（即5秒）。第7章曾介绍过，这个命令可以简化，可以在/etc/fstab中输入装载信息：

```
RHL9:/tmp    /tmp    nfs    soft,intr,timeo=50  0 0
```

然后只要用下列命令即可装载共享/tmp目录：

```
# mount /tmp
```

配置NIS服务器

NIS（网络信息服务）是个分布式数据库服务，用一组配置文件控制局域网上的多台计

算机。

所有Linux计算机带有相同的基本配置文件。配置文件的NIS数据库可能比不同计算机使用同一文件的不同版本更容易维护。

例如，每次用户到不同计算机上时，应能够输入相同的用户名和口令。一个方法是将/etc/passwd与/etc/group文件复制到局域网上的每一台计算机。也可以在NIS服务器上配置中央数据库，NIS中，这些数据库称为映射。

也许你的局域网很大，又不想生成DNS服务器。虽然可以把/etc/hosts文件复制到局域网上的每一台计算机，但在局域网上增加计算机时就非常麻烦。将/etc/hosts存放在中央NIS服务器映射中是一个更好的选择。

说明：尽管生成DNS服务器并不困难，但需要运行另一个服务。许多管理员希望尽量减少服务。一种方法是避免在局域网上使用DNS，而通过利用NIS共享的/etc/hosts，只在Internet上利用ISP的DNS服务器。

Red Hat Linux 9带有支持普通NIS 2.2服务器所需的包。本章介绍nisplus的两个引用，其基于NIS 3.x服务器（据说有缺陷）。

下面几节检查所要的RPM包、定义NIS域、定义要共享的内容、启动NIS服务器并产生需要的数据映射。

说明：NIS的优点是安全。如果NIS服务器，则立于防火墙后面的局域网中。NIS服务器与客户机之间不能有防火墙。尽管防火墙中可能通过几种办法保护局域网上的NIS，但太过麻烦。只要搜索NIS和“安全性”之类术语就可以找到几十个Web站点与消息，其中有关于各种安全问题的详细介绍。

NIS包

NIS有四个基本RPM包，见表28.7。注意这里也包括NFS使用的portmap-*包。第10章曾介绍过，可以用rpm-qi packagename命令了解每个包的细节。

表28.1 NIS包

包	功能
portmap-*	支持安全NIS远程过程调用（RPC）连接
ypbind-*	NIS客户机包，将客户机与服务器相关联
ypserv-*	NIS服务器包
yp-tools-*	包括基本NIS命令

定义NIS域

NIS客户机与服务器组织成域，但NIS域与计算机名中的域（如linux.mommabears.com）无关，也与Microsoft网络中的域无关。

首先，计算机可能已经有个NIS域名。为了找到NIS域名，可以运行domainname命令。如果其返回“（none）”，则计算机还没有指定NIS域名。

指定NIS域名很简单。例如，下列命令定义本地计算机上的域名为nistest:

```
# domainname nistest
```

还要在/etc/sysconfig/network中增加相应的项目，使下次启动Linux时它为已知。这样还要增加下列语句：

```
NISDOMAIN=nistest
```

定义共享文件

安装了所要的RPM包并设置好NIS域名之后，下一步要配置NIS服务器。首先要配置/var/yp目录中的Makefile文件，这是个丰富的文件，实际上，可以设置参数，下方的脚本处理选择加入NIS数据库映射中的文件，使其在NIS域上共享。本节介绍的变量基于默认Makefile，且只限于这个文件。

可以将NIS配置成查找不在NIS数据库中的计算机。如果启用这个命令（通过删除#），则其可以查找DNS服务器中的更多信息：

```
#B=-b
```

在大型局域网中，可能还有备份的NIS服务器。如果这样，则要将true改成false，使NIS寻找/var/yp/ypservers中的从服务器名：

```
NOPUSH=true
```

默认情况下，普通用户ID（用户ID和组ID在500以上），ID号较小的包括管理用户。下列命令从相应NIS数据库映射中排除低ID号：

```
MINUID=500
```

```
MINGID=500
```

提示：如果要保留一些“纯本地”用户，则可以设置较高的ID号。例如，如果将MINUID与MINGID设置为505，则NIS域中所有计算机上的前五个用户是本地的。

如果以根用户身份连接NIS域中的NIS服务器，则下列命令将根用户ID映射为没有什么权限的特殊用户nobody：

```
NFSNOBODYUID=65534
```

```
NFSNOBODYGID=65534
```

第9章曾介绍过，口令通常放在/etc/shadow与/etc/gshadow中。如果你的Linux系统是这样配置的，则以下命令将口令加进NIS映射数据库中：

```
MERGE_PASSWD=true
```

```
MERGE_GROUP=true
```

下列源目录应当是标准的，除非改变/etc/passwd之类的基本文件的地址，否则不会改变这些设置：

```
YPSRCDIR = /etc
```

```
YPPWDDIR = /etc
```

```
YPBINDDIR = /usr/lib/yp
```

```
YPSBINDDIR = /usr/sbin
```

```
YPDIR = /var/yp
```

```
YPMAPDIR = ${YPDIR}/${DOMAIN}
```

下列许多设置是标准的。例如，GROUP与YPPWDDIR相关联，是个/etc目录。从这个表中第一行，组配置文件为/etc directory，是个标准地址。如果改变其中任何配置文件的地址，则要相应地修改下列行：

```
GROUP      = ${YPPWDDIR}/group
PASSWD     = ${YPPWDDIR}/passwd
SHADOW     = ${YPPWDDIR}/shadow
GSHADOW   = ${YPPWDDIR}/gshadow
ADJUNCT    = ${YPPWDDIR}/passwd.adjunct
#ALIASES   = ${YPSRCDIR}/aliases # could be in /etc/mail
ALIASES    = /etc/aliases
ETHERS     = ${YPSRCDIR}/ethers
BOOTPARAMS = ${YPSRCDIR}/bootparams
HOSTS      = ${YPSRCDIR}/hosts
NETWORKS   = ${YPSRCDIR}/networks
PRINTCAP   = ${YPSRCDIR}/printcap
PROTOCOLS  = ${YPSRCDIR}/protocols
PUBLICKEYS = ${YPSRCDIR}/publickey
RPC        = ${YPSRCDIR}/rpc
SERVICES   = ${YPSRCDIR}/services
NETGROUP   = ${YPSRCDIR}/netgroup
NETID      = ${YPSRCDIR}/netid
AMD_HOME   = ${YPSRCDIR}/amd.home
AUTO_MASTER= ${YPSRCDIR}/auto.master
AUTO_HOME  = ${YPSRCDIR}/auto.home
AUTO_LOCAL = ${YPSRCDIR}/auto.local
TIMEZONE   = ${YPSRCDIR}/timezone
LOCALE     = ${YPSRCDIR}/locale
NETMASKS   = ${YPSRCDIR}/netmasks
YPSERVERS  = ${YPDIR}/ypservers
```

然后可以选择通过NIS服务器共享的文件。下列清单来自默认的配置文件的，可以增加或减少文件，只需将其放进说明区（带#的区）或从说明区取出：

```
all: passwd group hosts rpc services netid protocols mail \
    # netgrp shadow publickey networks ethers bootparams \
    # printcap amd.home auto.master auto.home auto.local \
    # passwd.adjunct timezone locale netmasks
```

其余的Makefile文件处理这些设置。由于这本书不是编程书，因此我不准备进一步介绍配置，本文件中的默认脚本对大多数用户足够用了。

生成数据库映射

配置/var/yp/Makefile之后，下一步要启动NIS服务器。由于它是个标准Linux服务，因此只需发出下列命令：

```
# service ypserv start
```

说明：ypserv监控程序要求事先定义NIS域名。前面曾介绍过，可以用domainname yourNISdomain命令定义NIS域名。

现在可以把Makefile处理成数据库映射。/usr/lib/yp/ypinit -m命令把Makefile处理到/var/yp/domainname子目录中，其中domainname是NIS域名。可以看到，/usr/lib/yp目录不在PATH中（见第8章），因此要用完全目录路径运行ypinit命令。

说明：一定要保证下次启动Linux时启动NIS服务。chkconfig --level 345 ypserv on命令可以保证在运行级3、4、5中自动启动NIS服务。

运行这个命令时，程序提示输入要加进NIS域的计算机名。这个例子中RHL9是NIS服务器计算机名，也可能计算机名为linux.example.com。增加的计算机放进/var/yp/ypservers中，即可以将其配置成从服务器。

```
# /usr/lib/yp/ypinit -m
```

这时，要构造运行NIS服务器的主机表。NIS服务器的主机表中有个RHL9。可以继续增加其他主机名，一行一个。完成之后，输入Ctrl-D：

```
next host to add: RHL9
```

```
next host to add:
```

将计算机加进NIS域后，要确认这个表。如果输入n，则提示重新输入这个表，否则ypinit命令开始处理Makefile，并出现图28.7所示的消息。

```
The current list of NIS servers looks like this:

RHL9
RHL9laptop

Is this correct? [y/n: y] y
We need a few minutes to build the databases...
Building /var/yp/nistest/ypservers...
Running /var/yp/Makefile...
gnake[1]: Entering directory `/var/yp/nistest'
Updating passwd.byname...
Updating passwd.byuid...
Updating group.byname...
Updating group.bygid...
Updating hosts.byname...
Updating hosts.byaddr...
Updating rpc.byname...
Updating rpc.bynumber...
Updating services.byname...
Updating services.byservicename...
Updating netid.byname...
Updating protocols.bynumber...
Updating protocols.byname...
Updating mail.aliases...
gnake[1]: Leaving directory `/var/yp/nistest'

RHL9 has been set up as a NIS master server.

Now you can run ypinit -s RHL9 on all slave server.
[root@RHL9 root]#
```

图28.7 处理NIS数据库

提示：如果遇到以failed to send 'clear' to local ypserv开头的错误消息，则可能是忘了启动NIS服务器的ypserv监控程序。

更新数据库映射

如果要更新数据库映射，则可以返回/var/yp目录，然后运行make命令。第12章曾介绍过，可以对内核、大多数包和NIS数据库这样处理Linux Makefile。

NIS从服务器

在大型网络中，NIS服务器最好有个备份。NIS从服务器中包括网络上其他计算机保持运行所需的信息。要建立NIS从服务器，就要在NIS主、从计算机上做一些工作。

配置NIS主服务器

在NIS主服务器中，保证已经把两台计算机加进了NIS域中的NIS计算机清单/var/yp/ypservers里，这应当在运行/usr/lib/yp/ypinit -m命令之前完成。

还要修改主NIS服务器/var/yp/Makefile文件中的行，显示NOPUSH=false，使主NIS服务器可以通过yppush命令将数据库复制到从NIS服务器中。

还要启动NIS映射传输服务器监控程序——ypxfrd。自然，这可以在Linux运行时用service ypxfrd start命令完成，为了保证下次启动Linux时它能启动，使用下列命令：

```
# chkconfig --level 345 ypxfrd on
```

配置NIS从服务器

准备好NIS主服务器之后，需要在NIS服务器上检查几个东西。首先，NIS从服务器也应为两个服务器的客户机。更多信息见下节介绍的NIS客户机部分。

保证从NIS计算机关联到NIS主服务器。只要在从计算机上指定了NIS域名，则ypbind命令可以自动完成这个工作。ypserv监控程序应该运行，可以用service ypserv status命令检查。根据需要启动这些监控程序。准备好以后，执行下列命令（将NIS主服务器的主机名换成RHL9）：

```
# /usr/lib/yp/ypinit -s RHL9
```

如果这个命令取得成功，则可以看到长长的消息序列，每个消息都从NIS主服务器向NIS从服务器传输一个配置文件。例如：

```
Transferring passwd.byname...
Trying ypxfrd ... success
```

如果需要查错，则应检查这里（和ypbind -debug命令中）的一些消息。除了检查网络之外，还要重新检查NIS主服务器的配置过程。另外，检查主NIS上是否设置了NOPUSH=false以满足NIS从服务器。保证本地NIS从计算机上启动了相应服务。

说明：默认情况下，NIS不使用DNS服务器，因此至少要在从NIS计算机/etc/hosts文件中具有NIS主服务器信息。

使用NFS客户机

将计算机配置成NIS客户机很简单，只要编辑/etc/yp.conf文件并运行ypbind命令即可。如果要将计算机设置成永久的NIS客户机，则记住运行chkconfig --level 345 ypbind on命令，保证其在相应运行级中启动。

有几个以yp开头的命令，可以帮助测试连接。为了保证NIS客户机实际使用某些数据库映射文件，需要配置/etc/nsswitch.conf文件。

yp.conf中的NIS客户机配置

配置NIS客户机很简单，在文本编辑器中打开/etc/yp.conf时，可以看到三个基本命令：

```
domain NISDOMAIN server HOSTNAME
domain NISDOMAIN broadcast
ypserver HOSTNAME
```

这里的项目很简单。可以将NISDOMAIN换成NIS域名，将HOSTNAME换成NIS服务器所在的计算机名。如果还有从服务器，则需增加下列命令：

```
domain NISDOMAIN server NISSLAVERHOSTNAME
```

其中NISSLAVEHOSTNAME是NIS从服务器的主机名。现在就可以用service ypbind start命令启动NIS客户机。

提示：如果ypbind无法与NIS服务器通信，则要检查NIS服务器上的防火墙，也许是这个防火墙阻止了NIS通信。一般来说，运行NIS的局域网，只在网络之外用防火墙保护。

NIS客户机命令

NIS客户机可以使用几个命令，它们都以yp开头，它们使你可以在远程NIS服务器数据库中设置口令、测试连接、从NIS服务器数据库读取文件，等等。下面几节将介绍这些命令。

ypcat

ypcat命令从NIS服务器数据库读取文件。和普通cat命令一样，它将文件中的信息进行滚动。但是，NIS客户机中看到的内容可能与服务器上的实际文件稍有不同。例如，下列命令只列出UID >= 500的用户的/etc/passwd信息（除非改变/var/yp/Makefile中的MINUID与MINGID变量）：

```
# ypcat passwd
```

ypchfn

ypchfn命令改变NIS服务器数据库映射中的个人信息。和chfn命令一样，它通常适用于当前用户。如果你使用根账号，则可以用chfn username命令改变所选用户的个人信息。

第23章曾介绍过，可以将用户姓名、电话号码之类的个人信息存放在/etc/passwd中该用户项目的第五个字段。

这样，下列命令提示改变RHL9 NIS服务器中用户mj的个人信息，并提供一系列提示，帮助修改用户mj的个人信息：

```
# ypchfn mj
Changing NIS account information for mj on RHL9.
Please enter root password:

Changing full name for mj on RHL9.
To accept the default, simply press return. To enter an empty field, type the word
"none".
Name [Michael Jang]:
```

ypchsh

ypchsh username命令改变NIS服务器/etc/passwd文件中特定用户的默认shell，类似于**ypchfn**。这个命令提示输入NIS服务器的根口令，然后提示改变shell。

ypmatch

ypmatch username password命令很容易从NIS数据库文件中搜索NIS主服务器的/etc/passwd文件中的局域网用户数据库。

yppasswd

yppasswd username命令可以改变NIS服务器中的用户口令。用户要用新口令登录任何NIS客户机计算机。和**ypchfn**与**ypchsh**命令一样，要先输入NIS服务器根口令，再输入所要用户的新口令。

yppush

如果最近改变了主服务器上的NIS数据库，则**yppush**命令强制主服务器将修改的数据库映射拷贝发送到/var/yp/ypservers文件中列出的任何NIS从服务器。

配置/etc/nsswitch.conf

如果网络上有NIS服务器，则要保证NIS客户机上的/etc/nsswitch.conf文件从NIS服务器中寻找任何相关的配置文件。还可以将NIS客户机指向其他源，如本地配置文件。

例如，如果没有NIS服务器，则/etc/nsswitch.conf很简单，仅包含如下命令：

```
passwd: files
shadow: files
group: files
hosts: files dns
```

每个命令指定一个搜索顺序。例如，**hosts**行指定先搜索本地文件（/etc/hosts）之后再搜索DNS服务器（匹配/etc/host.conf中的配置）。但是，如果有NIS服务器，则应将其放在清单中。例如，下列语句先查找正确关联的NIS服务器数据库：

```
passwd: nis files
shadow: nis files
group: nisfiles
```

nis项目对应于标准NIS服务器。如果运行NIS 3.x, 则要将这个项目换成nisplus。

如果要使用中央NIS服务器数据库/etc/hosts, 则可以在/etc/host.conf中增加相应的项目。例如, 下列语句让计算机先搜索NIS /etc/hosts数据库, 然后搜索本地/etc/hosts, 最后搜索/etc/resolv.conf中的任何DNS服务器:

```
order nis,hosts,bind
```

小结

如果在Linux与UNIX计算机之间共享文件, 则标准服务为NFS(网络文件系统)。运行NFS时要启动几个/etc/rc.d/init.d脚本, 包括nfs、nfslock与portmap。NFS目录通过/etc/exports共享, 并用exportfs命令发表。NFS通信可以通过iptables防火墙用TCP/IP端口111与2049或/etc/hosts.allow与/etc/hosts.deny中的TCP包装规则阻止。

通过NFS共享目录之后, 可以从NFS客户机计算机装载。showmount -e NFSserver命令列出共享目录。可以和任何其他本地或远程目录一起挂载NFS服务器。一定要使/etc/fstab中配置的装载不会在无法访问NFS服务器时“被挂起”。

NFS在Linux与UNIX计算机之间共享目录, 而NIS(网络信息服务)则在Linux与UNIX计算机之间共享配置文件。例如, 可以用NIS生成一个用户名与口令数据库, 只需将服务器上的/etc/passwd与/etc/groups文件转换成一个共享数据库。要在/var/yp/Makefile中定义NIS域名和共享文件。准备好Makefile之后, 可以用ypinit命令将其转换成数据库, 这个改变可以用/var/yp目录中的make命令处理。从服务器可以用ypinit进行配置, 用yppush进行刷新。

配置NFS客户机比较简单, 只要将其ypbind到相应服务器, 也可以使用authconfig命令。一旦连接之后, NFS客户机命令可以查找可用的数据库。最后, 正确配置/etc/nsswitch.conf, 将NFS客户机指定到NIS服务器上的相应数据库。

下一章介绍Samba, 可以和Linux、UNIX以及Microsoft Windows计算机共享文件与目录。

第29章 利用Samba

利用Samba可以把Linux计算机放进Microsoft网络中。本章介绍如何将Samba配置成Linux计算机网络中的客户机和服务器。

使用各种Microsoft操作系统的计算机之间可以通过SMB（服务器消息块）协议相互通信。Microsoft操作系统在TCP/IP网络上共享文件和打印机时，使用公用Internet文件系统（CIFS）。Linux计算机可以用Samba与SMB和CIFS通信。

Samba是个异构服务。一旦配置Samba之后，就看不到它与其他Microsoft计算机的任何差别了。和第25章介绍的CUPS一样，Samba也有自己的Web配置实用程序——SWAT。

可以用Samba包将Linux计算机配置成客户机和服务器，然后连接或共享目录和打印机。作为Samba客户机，还可以在终端方式中，像个文本FTP连接一样，连接共享Microsoft目录。

主要的Samba配置文件是/etc/samba/smb.conf。许多Linux管理员直接在文本编辑器中配置这个文件，我们将介绍如何用这个方法从Linux计算机中共享目录。很容易测试和查错smb.conf中所作的改变。

Linux提供了两个GUI配置工具：SWAT（Samba Web管理工具）是特性完整的浏览器工具，可以由TCP/IP端口901提供；redhat-config-samba工具更简单，但可以配置Samba服务器和共享目录的基本设置。本章介绍下列主题：

- 沟通Linux与Microsoft Windows
- 配置Samba客户机
- 了解Samba配置文件
- Samba Web管理工具（SWAT）
- redhat-config-samba工具

沟通Linux与Microsoft Windows

Samba是个异构服务，可以沟通Linux与Microsoft Windows，即可以在这些操作系统中无差异地通信。事实上，可以将Samba配置成像Microsoft Windows网络的任何其他成员一样共享目录。

Microsoft网络功能

Samba的一个优点是可将Linux与UNIX计算机配置成在Microsoft Windows网络中按不同的方式工作。配置完成后，Microsoft用户不知道他们的对方是一台Linux计算机。利用Samba可以将Linux计算机配置成下列计算机类型：

- Microsoft Windows工作组成员
- Microsoft Windows域成员
- Microsoft Windows成员服务器

- Microsoft主域控制器（PDC）

NetBIOS与NetBEUI 2.2.7（Red Hat Linux 9所带的版本）不允许将Linux配置成备份域控制器（BDC）。但是，也可以实现这个功能，详见Samba BDC HOWTO，位于www.samba.org站点。Samba开发人员正在Samba 3.0中显式增加备份域控制器支持。

Samba最初基于Microsoft的LAN Manager系统，客户机使用TCP/IP网络上的NetBIOS名称——NBT（NetBIOS over TCP/IP），而不需要Microsoft的另一网络系统NetBEUI。关于NetBIOS与NetBEUI的细节，见第20章。

许可证

别看到这个标题就头痛。Samba采用公用许可证（GPL），和不同UNIX式操作系统一起免费提供，包括Red Hat Linux 9。

Samba可以将Linux计算机设置成Microsoft网络的一部分，可以减少网络中要购买的Microsoft操作系统的数量。到本书编写时，使用Samba不需要支付任何Microsoft许可证费用。

说明：据说Microsoft公司正准备采取法律手段阻止免费Samba连接其网络。但我认为许多公司会反对这种做法。据我所见，只要这些公司能够支持Samba工作，这种法律活动就可以拖上好几年，到时候也许会出现其他技术。

定义

本章包含几个Samba专用的或与Microsoft网络密切相关的术语，现介绍如下。

主域控制器（PDC） 具有用户名和口令中央数据库的计算机，通常还包含Microsoft Windows登录配置文件的中央数据库。

备份域控制器（BDC） 这台计算机从主域控制器中取得信息，主域控制器和备份域控制器是Windows NT中的概念。

浏览表 网络上的共享资源表。

浏览主机 负责维护网络中浏览表的计算机。

域 至少有用用户名和口令的中央数据库网络，这个概念与互联网域名大不相同。

成员服务器 Microsoft Windows网络中共享目录或打印机，且不是主域控制器和备份域控制器的任何计算机。

对等实体 局域网上的一组计算机，每台都可以作为服务器，通常与工作组相关联。

服务器 共享目录或打印机的计算机。

共享 网络上共享的任何目录或打印机。

工作组 没有专用服务器的局域网。每台计算机负责自己的用户名和口令，每台计算机通常与局域网其他部分共享目录或打印机。

说明：本章网络上的“Microsoft服务器”可以指任何共享目录或打印机的Microsoft操作系统。它也可以指Linux计算机上的Samba服务器。

包

Linux中的Samba有五个基本包。要将计算机配置成Microsoft客户机，只需使用samba-client-*与samba-common-*。其他包可以帮助你Microsoft网络中将计算机配置成服务器。

表29.1列出了这些包。

表29.1 Samba RPM包

包	描述
samba-*	基本Samba服务器包，包括匹配Linux和Microsoft用户名或口令的命令
samba-client-*	这个包可以将Linux计算机设置成读取共享Microsoft目录和在共享的Microsoft打印机打印
samba-common-*	这个包中的文件可以支持Linux作为Samba客户机或Samba服务器
samba-swat-*	这个GUI工具可以修改主Samba配置文件，特别是smb.conf。如果不需要微调控制，则可以改用redhat-config-samba
redhat-config-samba-*	可以替代samba-swat，它更简单，但不够成熟，支持的配置控制更少

配置Samba客户机

利用samba-client-*与samba-common-* RPM包可以看到Microsoft Windows计算机中共享的目录和打印机。可以用两种基本方法连接共享目录：在本地Microsoft目录中装载共享Microsoft目录或像连接FTP服务器一样，在终端方式中连接共享目录。此外，还要知道如何连接与Microsoft计算机相联的共享打印机。

共享Samba目录

从Microsoft Windows服务器连接共享目录很简单。如图29.1所示，只要用smbclient命令和服务器名称或IP地址。这个命令有点奇怪，注意smbclient命令中的反斜杠。

这个目录中有几个有趣的共享。如果在Microsoft服务器中设置相应的权限，则可以像装载NFS目录一样装载任何共享目录，二者之间的差别很小。例如，下列命令可以在本地目录/root/downloads中装载计算机laptop2上共享的Downloads目录。然后Linux请求一个口令：

```
# mount '//laptop2/downloads' /root/downloads
Password:
```

装载命令实际上是mount.smbfs命令的“前端”，其来自samba-client RPM包。也可以替换smbclient命令。

说明：严格地说，要用-t smbfs开关指定mount的Samba文件类型，但因为mount是mount.smbfs命令的“前端”，因此不需要这样。

由于没有用户名，因此这个mount命令只适用于Microsoft工作组型的共享目录。换句话说，这要求Windows 95/98/ME计算机上的共享目录（或用户Everyone可以访问的共享目录），并且要有与共享目录相关联的口令（如有）（Microsoft Windows NT/2000/XP计算机也可以按这种方式配置）。

```
[root@RH9Test root]# smbclient -L \\laptop2
added interface ip=10.252.113.63 bcast=10.252.113.255 nmask=255.255.255.0
Password:
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

      Sharename      Type      Comment
      -----
      IPC$           IPC       Remote IPC
      D$             Disk      Default share
      SharedDocs     Disk
      print$         Disk      Printer Drivers
      ftproot        Disk
      Downloads      Disk
      HPLaserJ       Printer   Comment Test
      Temp           Disk
      RedHat         Disk
      OEDboot        Disk
      ADMIN$         Disk      Remote Admin
      C$             Disk      Default share
      Proposals      Disk
      mls            Disk
      RedHatOld      Disk

      Server          Comment
      -----
      Workgroup       Master

[root@RH9Test root]#
```

图2.11 从Microsoft Windows服务器控制共享

但是，大多数网络的限制更加严格。在Microsoft Windows服务器中，可以限制特定用户或组的访问。这时要有具有该目录相应权限的用户名和口令。**-o**选项可以在指定共享时指定用户名、口令，等等。我喜欢只在命令行指定用户名，以免在终端中以明文形式输入口令。Linux会提示输入口令。

```
# mount -o username=michael '//laptop2/downloads' /root/downloads
Password:
```

说明：甚至可以提供不同的访问水平，例如，可以对guest用户配置只读访问，对优先用户提供完全访问。Windows服务器的指定更加复杂，表29.2列出了一些Samba mount选项。

表29.2 Samba mount -o选项

选项	描述
username=winuser	可以对Microsoft服务器上的授权用户指定Microsoft用户名
password=winpass	可以指定与Microsoft优先用户相关的Microsoft口令，如果只输入用户名，则会自动提示输入口令
credentials=file	从可以保护的指定文件中读取用户名和口令（如/etc/shadow），可以自动从/etc/fstab之类的文件装载。其语法如下： username=winuser password=winpass
uid=linuser	可以设置拥有装载文件系统中文件的Linux用户，可以是用户ID号或用户名
workgroup=winwork	可以指定带共享目录的工作组

说明：这些命令假设DNS服务器或/etc/hosts文件中列出Microsoft Windows计算机名。可以将计算机名换成IP地址。

Samba终端模式

利用Microsoft Windows计算机和共享名，可以直接连接共享目录，就像连接FTP服务器一样。建立连接之后，可以上传和下载文件。例如，图29.2所示的命令连接我在本书中使用的目录。注意cd命令中用双引号，导航到双字的Windows XP目录。

```
[root@RH9Test root]# smbclient //laptop2/ml3 -U michael
added interface ip=10.252.113.63 bcast=10.252.113.255 nmask=255.255.255.0
Password:
Domain=[WORKGROUP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> cd "Other Stuff"
smb: \Other Stuff\> dir
.
..
4179CoverCopy.doc          D      0 Wed Apr  2 19:05:15 2003
4179CoverCopy_mj.doc       A      24064 Tue Mar 11 09:57:36 2003
4179CoverCopy_mja.doc      A      26624 Tue Mar 11 10:15:36 2003
4179CoverCopy_mja.doc      A      28672 Tue Mar 11 13:57:48 2003
4179EP1.doc                A      52224 Mon Mar 31 16:09:49 2003
4179EP4.doc                A      51712 Mon Mar 31 16:09:08 2003

      45778 blocks of size 524288. 28963 blocks available
smb: \Other Stuff\> help
?      remove      archive      lowercase      cancel
cd      chmod      chown      cat      dir
du      exec      set      help      history
lcd      link      lowercase      ls      mask
md      mget      mkdir      more      mput
newer      open      print      printmode      prompt
put      pwd      q      queue      quit
rd      recurse      rename      rm      rmdir
setmode      symlink      tar      tarmode      translate
!
smb: \Other Stuff\> 
```

图29.2 直接Samba连接

另外，注意可用的命令表。其中许多命令与第27章介绍的相似，事实上，Samba实现了该章介绍的chroot监禁。

连接打印机

Linux中很容易配置从Microsoft Windows计算机上共享打印机。如果能够使用Linux网络的浏览功能，则可以在Queue Type屏幕中用redhat-config-printer向导选择打印机，如第25章所示。

但这不一定可行。Microsoft浏览功能可能无法及时找到打印机，也可能没有将打印机设置成可浏览。为此可以配置标准本地打印机，再在后面修改设置。例如，图29.3显示了如何配置标准本地打印机。

很容易将其改成指向远程打印机，为此只要单击Queue Type下拉框。从得到的清单中选择Networked Windows (SMB) 打印机。

图29.4演示了连接Samba打印机所需的格式，表29.3列出了其中每个项目。

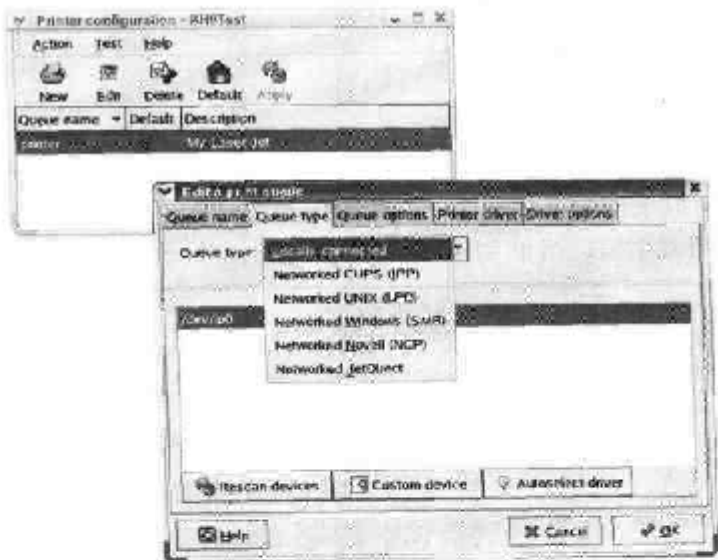


图29.3 用redhat-config-printer配置标准本地计算机



图29.4 配置Samba打印队列

表29.3 连接Samba打印机所需信息

字段	描述
Share	“//服务器名/打印机名”格式的共享名
Server Name Or IP Address	共享打印机的计算机名或IP地址
Workgroup	Windows工作组名，仅当Windows服务器在工作组中时输入
User	授权用户的Microsoft用户名
Password	与用户相关的Microsoft口令

了解Samba配置文件

有三个默认的Samba配置文件，它们都在/etc/samba目录中。其中两个（lmhosts与

smbusers) 很简单。第三个文件smb.conf是主Samba配置文件, 将在本节详细介绍。

说明: 这个目录中还有secrets.tdb文件, 通常包括Microsoft Windows网络中使用的安全标准符(SID)。

如果你按本书的方法做, 则建议把这些文件备份到另一目录中。这样, 如果改变得太乱, 就可以恢复这些文件, 而不必重新安装相关的包。

smb.conf文件包括大量有用的说明语句, 可以帮你了解Samba的配置。如果只想学习Samba, 则备份smb.conf有三个好处:

- 原smb.conf中的说明语句可以帮你进一步了解Samba。
- SWAT和redhat-config-samba之类的工具在把改变写入smb.conf时可能会删除一些说明语句。
- SWAT和redhat-config-samba之类的工具可能会删除smb.conf文件中的默认设置, 如workgroup=WORKGROUP。

Samba监控程序

有两个基本的Samba监控程序: smbd与nmbd。改变任何配置文件之后, 至少要重载Samba。编辑主Samba配置文件/etc/samba/smb.conf时, 需要用service smb reload命令让Samba读取改变。但是, 如果进行大的改变, 则需要重新启动这两个监控程序。用下列命令重新启动smbd监控程序, 即可以重新启动smbd与nmbd:

```
# service smb restart
```

其他Samba配置文件

/etc/samba目录中的其他Samba配置文件有lmhosts与smbusers。前面曾介绍过, 它们是非常简单的文件。可以在Samba配置过程中增加其他文件。

lmhosts

与/etc/hosts相似, lmhosts文件是IP地址与NetBIOS名称的数据库。NetBIOS名称是Microsoft Windows计算机名, 通常只限于15个字母或数字字符。默认lmhosts文件只有一行, Microsoft Windows操作系统还可以用lmhosts名称指向本地计算机:

```
127.0.0.1 localhost
```

smbusers

smbusers文件是Linux与Microsoft Windows用户名的数据库。默认情况下, 它包括两行:

```
root = administrator admin
nobody = guest pcguest smbguest
```

换句话说, Linux根用户映射Microsoft账号administrator, Linux的nobody用户映射Microsoft账号guest, pcguest与smbguest。

可以用smbadduser命令在这个文件中增加用户。例如, 假设Linux用户jp和Microsoft Windows用户Jean-Paul在网络上, 则图29.5所示命令可以让Linux用户jp访问局域网中Microsoft Windows用户Jean-Paul的文件。

```
[root@RH9Test root]# smbadduser jp:Jean-Paul
Adding: jp to /etc/samba/smbpasswd
Added user jp.
Adding: {jp = Jean-Paul} to /etc/samba/smbusers
-----
ENTER password for jp
New SMB password:
Retype new SMB password:
Password changed for user jp.
Password changed for user jp.
[root@RH9Test root]#
```

图29.5 增加Samba用户

图29.5所示命令在/etc/samba/smbusers中增加下列简单内容:

```
jp = Jean-Paul
```

要使用这个数据库, 首先要激活smb.conf中的下列行:

```
; username map = /etc/samba/smbusers
```

在Samba配置中, 散列号(#)和分号(;)后面都是说明语句。要激活这一行, 在文本编辑器中打开/etc/samba/smb.conf, 并从该行前面删除分号。smb.conf中还有另外几行也包括分号。本章稍后部分介绍删除各个分号以激活和立命令时的效果。

增加Samba用户之后, Linux在/etc/samba目录中增加smbpasswd文件, 包括用加密格式增加Microsoft Windows口令。

主Samba文件: smb.conf

默认Samba配置文件/etc/samba/smb.conf中有一组说明语句, 提供了丰富的信息源。但是, 如果你不熟悉Samba服务, 则不容易理解这些说明语句。在处理之前, 先把这个文件备份到另一目录中。

说明: 如果已经配置了Samba, 则可能没有带说明语句的原smb.conf文件。要取得另一拷贝, 可以备份并删除/etc/samba目录中的当前配置文件, 然后用rpm -Uvh --force samba-common-*命令重新安装samba-common-*包。完成之后一定要记住恢复原先的Samba配置文件。

smb.conf文件中包括连接所要的Microsoft Windows网络的全局设置, 还有要与局域网中其他计算机共享的任何目录与打印机的共享定义。不同设置组可以让你在不同的局域网中工作, 这些局域网可以配置成Microsoft工作组模式、成员服务器模式或主与备份域控制器模式。

下面几节依次对/etc/samba/smb.conf中的标准设置模式进行简单分析。本章稍后要用SWAT和redhat-config-samba工具配置smb.conf。

下节从Red Hat samba-* RPM包中开始分析smb.conf文件。这个smb.conf版本的许多设置与Samba默认设置不同。

Samba全局设置

smb.conf文件中有大量全局变量。如果不用某个变量, 则Samba假设该变量采用默认值。利用不同的全局变量可以完成下列功能:

- 限制可以访问的服务器的IP地址
- 在Samba浏览表中设置打印机
- 配置guest账号与日志文件
- 将Samba配置成匹配网络上的主导Windows安全方式
- 利用多口令设置
- 将Linux用户名映射为Windows用户名
- 对不同计算机定制配置文件
- 用PAM（可插验证模块）限制Samba验证，见第22章介绍
- 将Samba配置成使用不同长度的数据块和通过不同的接口发送数据
- 设置浏览表，向可能基于网络上的不同主计算机广告共享信息
- 使Samba符合Microsoft网络上的登录参数
- 在Linux计算机上存储配置文件
- 将Samba配置成使用WINS与DNS

Linux是大小写相关的，而Windows是大小写无关，Samba可以克服这个差别。

基本网络类型

第一个全局变量描述要加入的网络类型。它名为workgroup，但可以将其设置成Microsoft网络的工作组名或域名。例如，如果网络的域名为bignet，则可在smb.conf中用下列行替换：

```
workgroup=BIGNET
```

Samba还可以包括计算机的描述，图29.6反映了计算机RH9test的下列命令：

```
server string = Mike's Samba Server
```



图29.6 共享Samba服务器的Microsoft Windows视图

IP地址限制

可以通过第22章介绍的iptables命令限制对Samba的访问。可以用hosts allow命令进一步限制访问。例如，下列命令限制对本地计算机和10.122.33.0网络的访问：

```
hosts allow = 10.122.33. 127.  
hosts allow = 10.122.33.0/255.255.255.0 127.
```

Samba与打印机

默认情况下, 打印机放在共享的可浏览项目列表中。下列命令通过Samba在标准CUPS系统装入一系列打印机:

```
printcap name = /etc/printcap
load printers = yes
printing = cups
```

说明: Samba中有一些参数看起来是拼写错误的, 但都可以使用。例如, browsable与browseable可以通用, writable与writeable也可以通用。

如果使用LPD (见第25章), 则要替换下列值:

```
printcap name = /etc/printcap
load printers = yes
printing = lprng
```

客户账号

Samba可以生成标准guest账号。例如, 可能需要对门厅里的人设置工作站, 只让他们访问广告, 而不让他们访问其他内容。如果激活下列标准, 则要保证pcguest是Linux系统中的实名用户:

```
; guest account = pcguest
```

日志文件

下列选项对连接Samba服务器的每台计算机配置不同的日志文件。例如, 如果有个Windows计算机havel, 则下列语句表示可以在指定目录的havel.log文件中找到调试信息。max log size为0表示这些日志文件的长度没有限制, 其他限制的单位为KB。

```
log file = /var/log/samba/%m.log
max log size = 0
```

说明: smb.conf中以%开头的任何表达式都可能改变。例如, %m表示客户计算机名, 因此其改变依赖于客户机。

安全模式

Microsoft Windows网络中有几个基本安全模式。一般来说, 选择的方法取决于共享目录的条件和共享网络的类型。表29.4描述了这些安全模式选项:

```
security = share
security = user
security = server
security = domain
```

口令设置

Samba中有几种口令设置方法。如果为Microsoft Windows用户名和口令配置中央服务器, 则可以在这里指定。主域控制器还可以放在支持Samba的Linux计算机上。

表29.4 Samba安全模式

安全模式	描述
share	共享目录只要用口令即可访问的系统，最常见的是没有任何专用服务的对等实体计算机工作组
user	共享目录通过用户名和口令限制的系统，常用于对等实体工作组网络上的服务器级计算机，如Windows 2000、Windows XP与Linux
server	用户名和口令优先选择集中式数据库的系统，如果找不到这种数据库，则返回到security = user
domain	连接Windows域的系统，要求/etc/samba中有smbuser与smbpasswd数据库文件

如果设置security = share或security = domain，则还应指定网络的口令服务器。例如，如果已知主域控制器和备份域控制器名称为ntserv1与ntserv2，则可以插入下列命令：

```
password server = ntserv1 ntserv2
```

如果不知道主与备份域控制器名称，则可以通过下列命令将Samba服务器设置成搜索主域控制器：

```
password server = *
```

一些Microsoft Windows操作系统不能很好地处理混合大小写字母的口令。激活这个命令时，需试验八字符口令与用户名的所有大小写字母组合：

```
; password level = 8
; username level = 8
```

自然，Samba配置成以标准Samba口令文件发送加密口令。记住，这个口令文件包括用smbadduser命令增加的Microsoft Windows用户名和口令。但是，并不是所有Microsoft Windows计算机都能够处理加密口令。

```
encrypt passwords = yes
smb passwd file = /etc/samba/smbpasswd
```

如果不用这些命令，则Samba逆转成默认，以明文形式在网络上发送口令。这在Windows 95第一版和早期Microsoft操作系统中仍然必要。

如果用SSL（安全套接层）库配置Samba，则可以激活下列命令。

```
; ssl CA certFile = /usr/share/ssl/certs/ca-bundle.crt
```

如果用户在Microsoft Windows计算机上改变口令，则下列命令同步相应的Linux口令：

```
unix password sync = Yes
passwd program = /usr/bin/passwd %u
passwd chat = *New*password* %n\n *Retype*new*password* %n\n *passwd:
➤ *all*authentication*tokens*updated*successfully*
```

最后，可以用PAM（可插入验证模块）帮助保护口令（见第22章），PAM命令将覆盖password program变量：

```
pam password change = yes
```

隔几行还有一个PAM命令。如果设置明文口令，则下列命令用PAM控制对系统的访问：

```
obey pam restrictions = yes
```

映射Linux与Windows用户

前面曾介绍过，可以用不同的用户名匹配Linux与Windows用户。使用smbadduser命令时，结果存放在/etc/samba/smbusers目录下的数据库中，也可以直接编辑这个文件。如果要使用这个数据库，则需激活下列命令：

```
; username map = /etc/samba/smbusers
```

计算机定制Samba

可以在远程计算机上配置Samba服务器。如果激活下列命令，则每台计算机会寻找特定的配置文件。例如，如果Microsoft Windows计算机名为Chirac，则%m变量使其在连接时寻找/etc/samba/smb.conf.Chirac配置文件。

```
; include = /etc/samba/smb.conf.%m
```

性能管理

熟悉Samba之后，可以优化网络性能，需要进行的工作取决于网络与通信流的大小。下列命令中，TCP_NODELAY通常能使Samba性能加倍，SO_RCVBUF与SO_SNDBUF变量是进出Samba的数据缓冲区。最优设置随Samba服务器中负荷的不同而不同。如果要试验，可以一次调整1KB（如SO_RCVBUF=7168或SO_RCVBUF=9216）：

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
```

网络接口

服务器可以配置多个网络接口卡。可以将Samba访问限制在一个网卡上，也可以将Samba服务器设置用于特定的远程网络。例如，下列语句设置Samba使用网卡eth1和网址172.168.33.0：

```
interfaces eth1 172.168.33.0/24
```

浏览

在Microsoft Windows网络中，浏览就是计算机显示可用的共享目录与打印机。一台计算机是浏览主计算机，其他计算机将共享信息发送到这台计算机。

甚至可以将Samba服务器设置成将共享发送到远程网络。如果不知道网络中主浏览器的IP地址，则可以使用广播地址。例如，下列命令在局域网与192.168.1.0网络之间同步浏览表：

```
remote browse sync = 192.168.1.255
```

这个命令只是将Samba服务器的浏览信息发送到这个网络（也可以指定浏览主计算机）上。

```
remote announce = 192.168.1.255
```

Microsoft网络中的一台计算机保存浏览表，通过“选举”确定这台计算机，Samba服务器也可以被“选举”为维护浏览表的计算机。但是，下列命令将Samba服务器排除在选举之外：

```
; local master = no
```

如果要让Samba服务器参与浏览“选举”，则可以使用下列命令。这时，Samba通常会在“选举”中战胜除域控制器和Microsoft Windows NT服务器外的其他计算机：

```
; os level = 33
```

如果不想别的计算机有任何机会，则可以将Samba设置为域中的主浏览器：

```
; domain master = yes
```

如果Samba服务器的工作量不足，则可以将其设置为优选主浏览器，如下：

```
; preferred master = yes
```

登录管理

如果网络中有Linux计算机和Microsoft Windows计算机，则可以激活下列命令，将Samba设置为这个网络的主域控制器，控制用户名与口令数据库：

```
; domain logons = yes
```

说明：这要求用户级安全和netlogon目录，见这个文件的其他部分。

Microsoft网络可以按用户或按计算机配置登录，一个登录脚本配置一种，这些脚本可以存放在Samba服务器中。%m对应于每台机器（计算机），%U对应于每个用户：

```
; logon script = %m.bat
; logon script = %U.bat
```

利用中央配置文件，用户登录时可以向网络中的任何Microsoft计算机上提供一致的外观。可以将配置文件存放在Samba服务器的登录路径中。%L表示服务器名，而%U表示用户名：

```
; logon path = \\%L\Profiles\%U
```

WINS与DNS

Windows Internet名称服务（WINS）与DNS相似，但它是一个NetBIOS名称与IP地址的数据库。如果Samba无法在/etc/hosts中找到所需计算机名，则WINS与DNS提供了两个其他的数据库。

下列命令在本地Samba服务器中设置WINS：

```
; wins support = yes
```

也可以查找特定的IP地址的不同WINS服务器（这里的地址是任意的，应换成相应的地址）。这里Samba服务器成为WINS客户机：

```
; wins server = 192.168.0.22
```

如果Microsoft网络中还有旧式计算机，则可能需要激活这个命令，使所有计算机都能访问WINS数据库：

```
; wins proxy = yes
```

如果计算机不在WINS数据库中，则可以激活这个命令，将DNS服务器设置为替换数据库：

```
; dns proxy = yes
```

大小写管理

Linux是大小写相关操作系统，而Microsoft是大小写无关操作系统。通常，Samba保留所传输文件的大小写。可以强制让一切保持小写，下列命令影响长文件名和采用Microsoft 8.3文件名格式的文件名（如abcdefgh.123）：

```
; preserve case = no
; short preserve case = no
```

相反，也可以用下列命令将所有文件名设置为默认大写：

```
; default case = upper
```

如果所有用户在网络中所有计算机上都采用大小写相关文件名，则可以用下列命令使Samba服务器大小写相关：

```
; case sensitive = yes
```

记住：Microsoft Windows是大小写无关操作系统，在大小写相关性时，不同文件名的任何大小写错误都可能造成问题。

说明：将Samba配置成主域控制器是个丰富而复杂的课题，更多信息见新的Samba HOWTO文档，位于us1.samba.org/samba/docs/Samba-HOWTO-Collection.html页面。

默认全局设置

表29.5列出了smb.conf默认的全局设置。记住，如果使用默认参数，则不必在smb.conf中列出。SWAT与redhat-config-samba之类的工具会在更新smb.conf时删除默认的全局设置。

表29.5 smb.conf默认全局设置

变量	默认
case sensitive	no
default case	lower
dns proxy	yes
domain logons	no
encrypt passwords	no
guest account	nobody
hosts allow	所有主机都可以访问
include	无默认
interfaces	除127.0.0.1以外的所有活动接口（只要能这个地址发送广播消息）
load printers	yes
local master	yes
log file	无默认
logon path	\\%N\\%U\\profile，其中%N为NIS服务器名，%U为用户名

(续表)

变量	默认
logon script	无默认
max log size	5000 (KB)
obey pam restrictions	no
pam password change	no
passwd chat	*new*password* %n\n *new*password* %n\n* changed
passwd program	/bin/passwd
passwd server	无默认
password level	0
preferred master	auto
preserve case	yes
printcap name	/etc/printcap
printing	无默认
remote announce	无默认
remote browse sync	无默认
security	user
server string	Samba %v,其中%v = 版本号
show print caps	yes
smb password file	无默认
socket options	TCP_NODELAY
ssl CA certFile	/usr/local/ssl/certs/trustedCAs.pem
unix password sync	no
username level	0
username map	无默认
wins proxy	no
wins server	不支持
wins support	no
workgroup	WORKGROUP

配置共享

下面要分析packaged smb.conf配置文件中的目录共享方式。标准的smb.conf文件中有七个共享目录的例子，介绍这些例子之后，就不难了解如何配置共享目录了。

[homes]共享

只要在smb.conf中使用下列标准命令，在Linux计算机中有账号的Microsoft Windows用户就可以读取和写入主目录：

```
[homes]
comment = Home Directories
browseable = no
writeable = yes
valid users = %S
create mode = 0664
directory mode = 0775
```

表29.6介绍了这些命令。

表29.6 典型的Samba主目录共享命令

命令	描述
[homes]	smb.conf中的标准“特殊”段
comment = Home Directories	这个命令描述Windows Network Neighborhood, My Network Places或smbclient -L %hostname的共享
browseable = no	通常这个命令使共享目录不在Network Neighborhood或My Network Places中显示, 不适用于拥有主目录的用户
writable = yes	这个命令使用户可以写入这个目录, 也可以用 read only=no
valid users = %S	%S是服务名, 这里与user相关联
create mode = 0644	这个命令对新文件设置rw-r--r--权限, 不覆盖Windows NT/2000/XP计算机的权限设置。也称为生成掩码
directory mode = 0775	这个命令对新目录设置rwxr-xr-x权限, 不覆盖Windows NT/2000/XP计算机的权限设置。也称为目录掩码

要从Microsoft Windows计算机访问其目录, 用户只需在Connect To Computernam窗口中输入Linux用户名和口令, 如图29.7。



图29.7 连接共享的Samba主目录

[tmp]共享

可以将/tmp目录设置为网络上用户共享文件的共享位置。下列命令使任何用户都能访问这个目录:


```
[tmp]
comment = Temporary file space
path = /tmp
read only = no
public = yes
```

这些命令很简单，在Network Neighborhood或My Network Places的/tmp视图中加进了说明，任何有效用户都可以写入这个目录。`public = yes`命令是新增的，是`guest ok = yes`的同义词。换句话说，连口令都不需要，就可访问此目录。

[public]共享

不一定要与所有人共享目录。和第9章介绍的用户专用组模式相似，可以设置所有人可读但只有staff组成员可写的目录，如下：

```
[public]
comment = Public Stuff
path = /home/samba
public = yes
writable = yes
printable = no
write list = @staff
```

设置这个特定共享之前，要先保证有个/home/samba目录，且/etc/groups中有staff组。

另一个[public]共享

另一个[public]共享可以用于更公开的情形，下列命令配置的目录使所有用户可以读取和写入该目录下的所有文件。但是，`only guest = yes`命令使任何连接这个目录的用户只有guest用户的权限。当然，要保证path目录（这里是/usr/somewhere/else/public）实际存在。

```
[public]
path = /usr/somewhere/else/public
public = yes
only guest = yes
writable = yes
printable = no
```

两人共享

另一种共享配置是仅有两人（这个例子中我们假设是Mary与Fred）共享。尽管它不是公共共享，但稍后将会看到，默认**browseable = yes**。换句话说，其他用户可看到Mary与Fred的共享，但不能访问其共享目录，除非其具有下列之一的用户名和口令：

```
[myshare]
comment = Mary's and Fred's stuff
path = /usr/somewhere/shared
valid users = mary fred
public = no
```

```
writable = yes
printable = no
create mask = 0765
```

记住，上述项目要放在Samba服务器中，这个例子中，此服务器包括/usr/somewhere/shared目录和用户mary与fred。

专用目录

除了各个用户的主目录之外，还可以配置专用目录。例如，下列命令为Linux用户fred配置专用目录/usr/somewhere/private。由于public = no，因此客户用户不能访问这个目录：

```
[fredsdir]
comment = Fred's Service
path = /usr/somewhere/private
valid users = fred
public = no
writable = yes
printable = no
```

计算机的共享目录

可以配置特定计算机的共享目录，这对同一计算机上的不同用户非常有用。例如，工厂中不同班次的人可以在计算机上留言：

```
[pchome]
comment = PC Directories
path = /usr/local/pc/%m
public = no
writable = yes
```

必须生成path所列的目录。记住，%m表示计算机名。例如，如果要连接计算机factory1，则上述path命令表示要生成/usr/local/pc/factory1目录。

共享打印机

如果配置了CUPS打印机，则要配置基本共享。尽管标准smb.conf文件推荐BSD打印系统，但下列命令也适用CUPS打印机：

```
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
guest ok = no
writable = no
printable = yes
```

如果要共享一台LPD打印机，则标准smb.conf文件中的另一预配置共享可以供用户（这里是fred）专用：

```
[fredsprn]
comment = Fred's Printer
valid users = fred
path = /home/fred
printer = fred's_printer
public = no
writable = no
printable = yes
```

writable = no指定的限制不影响打印假脱机目录，计算机仍然可以发送打印假脱机文件请求到打印服务器中。

配置登录目录

在Microsoft网络上用Samba将Linux计算机配置成域控制器（PDC或BDC）时，要配置每个用户的登录和配置文件路径。和前面一样，要事先建立相应的目录。

下列命令根据**path**指定的目录在Microsoft Windows域中配置登录：

```
[netlogon]
comment = Network Logon Service
path = /usr/local/samba/lib/netlogon
guest ok = yes
writable = no
share modes = no
```

这个目录要指定**share modes = no**，否则黑客可能知道如何去访问每个用户的登录信息。

下列命令可以对登录Samba服务器的用户配置本地配置文件，就像对Samba服务器一样：

```
[Profiles]
path = /usr/local/samba/profiles
browseable = no
guest ok = yes
```

默认全局设置

表29.7列出了目录与打印机的默认全局设置。记住，如果使用默认参数，则不必在**smb.conf**中列出。SWAT与redhat-config-samba之类的工具会在更新**smb.conf**时删除默认的共享设置。

表29.7 smb.conf默认全局设置

变量	默认
browseable	yes
comment	无默认
create mode	a.k.a. create mask = 0744
directory mode	a.k.a. directory mask = 0755
guest ok	no

(续表)

变量	默认
path	无默认
printable	no
public	a.k.a. guest ok = no
read only	yes
writable	no (真值默认为read only = yes)
write list	无默认
valid users	无默认 (任何标准用户都可以登录)

Samba查错检查表

Samba配置文件可能很大，特别是smb.conf。一个小小的错误就可能使服务产生异常。多一个防火墙之类的简单问题也可能需要花上几个小时去修改配置。

查错时，首先要检查smb.conf文件的语法。特别注意说明语句，很可能是不小心删除了分号、散列号之类的说明语句标志。然后要检查本地Samba服务器的浏览表。如果本地浏览表没错，则要检查网络。几个有效smb.conf设置可能造成问题。

测试smb.conf

配置smb.conf之后，很容易测试。testparm命令是Samba配置文件的语法检查器。如果不指定地址，则testparm自动检查/etc/samba目录中的smb.conf文件。

重新启动或重新装入smb监控程序之前，要运行testparm命令。如果编辑时出了小错则它会指出smb.conf问题的来源，从而节省大量时间。

检查本地Samba浏览表

重新启动Samba之后，可以用smbclient命令检查要共享的项目表。如果在Samba服务器中可以看到正确的表，则网络上Microsoft Windows计算机中也应能看到本图的表，否则说明有网络或防火墙的相关问题。例如，下列命令检查计算机RH9test中的浏览表，mj是这台计算机上的用户：

```
# smbclient -L \\RH9test -U mj
```

程序提示输入mj的口令，然后可以看到计算机RH9test中的浏览表。图29.8的例子中，还可以看到工作组WORKGROUP与MYGROUP的成员。

说明：记住，Samba用户名在/etc/samba/smbusers文件中，前面我们已经用smbadduser命令将其加进了这个文件中。

检查网络

第21章曾介绍过，大多数网络问题都是物理问题。也许是电线松了，也许是集成器没电或类似的其他问题。第21章介绍的几个命令（如ping与netstat）可以检查网络状态。

我们经常遇到的一个问题是防火墙。如果Samba服务器上有防火墙，则它可能阻止服务器与客户机的通信。如果Samba服务器看不到客户机，则无法登录共享Samba目录或打印机。

```
[root@RH9Desk root]# smbclient -L \\RH9Test -U mj
added interface ip=10.252.113.211 bcast=10.252.113.255 nmask=255.255.255.0
Password:
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 2.2.7a]

      Sharename      Type      Comment
      -----
      mao             Disk      Mao's Home Directory
      var             Disk      Logs and More
      IPC$            IPC       IPC Service (the samba server)
      ADMIN$          Disk      IPC Service (the samba server)
      MyLaserJet       Printer
      HPLasers         Printer
      printer          Printer
      SecondLaserJe    Printer
      mj              Disk      Home Directories

      Server          Comment
      -----
      LAPTOP2          LaptopWin
      RH9DESK          samba server
      RH9SERVER
      RH9TEST          the samba server

      Workgroup        Master
      -----
      MYGROUP          RH9DESK
      WORKGROUP        RH9TEST
[root@RH9Desk root]#
```

图29.8 本地lan服务器的浏览表

其他Samba问题

我还遇到过其他Samba问题，其中大部分与smb.conf配置文件中的错误有关。有些错误是有效选项，它们能够通过testparm语法检查，但不能在局域网中正确表示你的Samba服务器。有时可以从相应的日志文件中找到线索。前面曾介绍过，每个Samba客户机都有一个默认的日志文件。例如，图29.9列出了smb.conf计算机上的连接。

```
[2002/12/09 13 25 42. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\redhatbeta, pid=12182
[2002/12/09 13 36 13. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\redhat, pid=12188
[2002/12/09 15 38 45. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\redhatbeta, pid=3738
[2002/12/09 15 41 05. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\redhat, pid=3801
[2002/12/09 19 26 34. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\redhatbeta, pid=2017
[2002/12/10 09 18 42. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\redhatbeta, pid=2003
[2002/12/10 11 15 38. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\downloads, pid=3469
[2002/12/10 11 16 54. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\downloads, pid=3526
[2002/12/10 11 18 44. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\downloads, pid=3535
[2002/12/10 11 23 42. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\downloads, pid=3543
[2002/12/11 14 19 40. 0] client/smbmount c send_fs_socket(383)
mount smbfs entering daemon mode for service \\laptop2\redhatbeta, pid=2301
-
-
-
"smbmount log" 22L, 15520
```

图29.9 smb.conf计算机上的连接

smb.conf文件中的常见错误分成下面几类:

错误的工作组 默认smb.conf文件中的Samba workgroup是MYGROUP, 不同于workgroup的默认值WORKGROUP。如果将包含的计算机设置为一个域而没有对这个变量输入正确的域名, 则可能遇到问题。

browsable = no 设置browsable = no时, 用户通常无法在Windows Network Neighborhood或My Network Places中看到共享目录和打印机。

共享配置不对 从前面几节可以看到, 共享有多种方式, 可以与用户、客户、组或每个人共享。如果共享配置不对, 则用户无法得到所要的目录或打印机。

writable = no Samba的共享目录默认为只读。如果不另外指定, 则用户无法写入相应的共享目录。

防火墙配置不对 Red Hat Linux标准防火墙会阻止Samba通信。如果有hosts allow变量, 则不在表中的计算机无法访问Samba服务器。

Samba Web管理工具 (SWAT)

当前Samba包中有个综合的 GUI配置实用程序Samba Web管理工具 (SWAT)。前面曾介绍过, 它放在samba-swat * RPM包中。运行 SWAT之前, 首先要用下列命令激活相应的xinetd监控程序:

```
# chkconfig swat on
```

SWAT有几个菜单, 见下面几节的介绍。简而言之, 在每个菜单中进行所要的配置之后, 单击Commit Changes按钮将这个改变保存到文件中。

完成改变之后, 要重新启动smbd与nmbd监控程序, 可以通过SWAT Service菜单, 也可以利用service smb restart命令。

Home菜单

要启动SWAT, 打开所选浏览器并导航到localhost:901。即使以根用户身份登录, SWAT也会提示输入有效的用户名和密码。输入有效的用户名和密码信息之后, SWAT打开Home菜单, 如图29.10。

可以看出, Home菜单包含其他Home菜单的链接, 后面几节将一一介绍。Home菜单还可以访问几个Samba文档的选项, 有些是与特定命令或文件相应的手册页面。文档清单末尾是Samba HOWTOs, 以及第一版“Using Samba”的电子书格式。

Samba配置向导

SWAT的Samba配置向导提供了解决Samba服务器三个基本设置的方法。单击Wizard链接并向下滚动, 直到出现图29.11所示的选项。

下面看看其中的每个选项:

Server Type 可以选择Microsoft网络上的三种服务器之一: Stand Alone、Domain Member或Domain Controller (PDC或BDC)。如果连接Microsoft对等实体工作组, 则只能选择Stand Alone服务器。

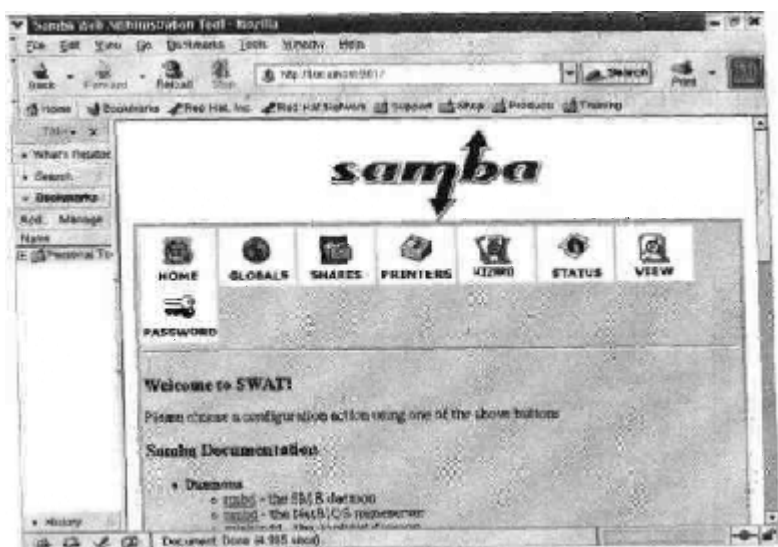


图29.10 Home菜单

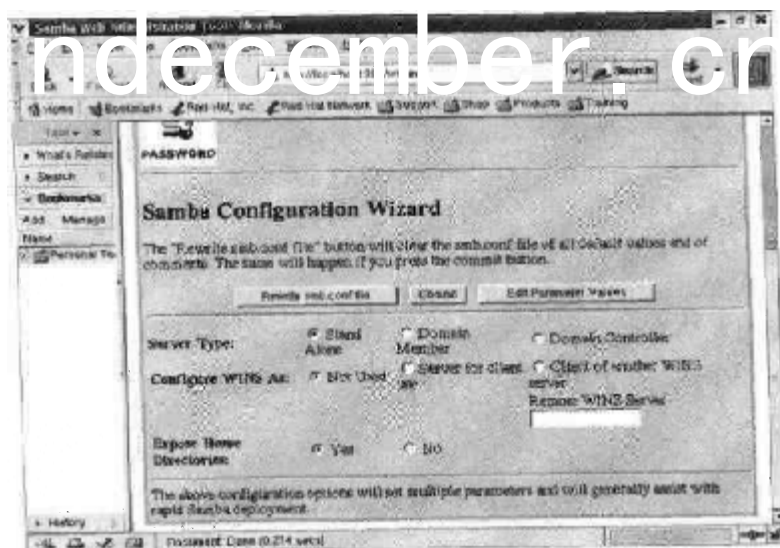


图29.11 Samba配置向导

Configure WINS As 可以指定WINS在网络上的角色，有三个选择：可以将Samba服务器配置成WINS服务器，也可以将其配置成不同Samba服务器的客户机（如果已知其IP地址），甚至还可以避免在网络中使用WINS。这些与wins server以及wins support变量相关。

Expose Home Directories 允许用户看到与Linux用户名相关联的目录，这个选项与本章前面介绍的[homes]共享相关。

进行选择之后，单击Commit按钮。这个配置向导可能与你想像的有些不同，因为还要进行许多工作才能启动Samba服务器。单击菜单顶部的Globals链接，转入下节工作。

Samba菜单

通过Samba菜单可以配置smb.conf文件的[global]设置。单击Globals链接可以看到图29.12所示的菜单。

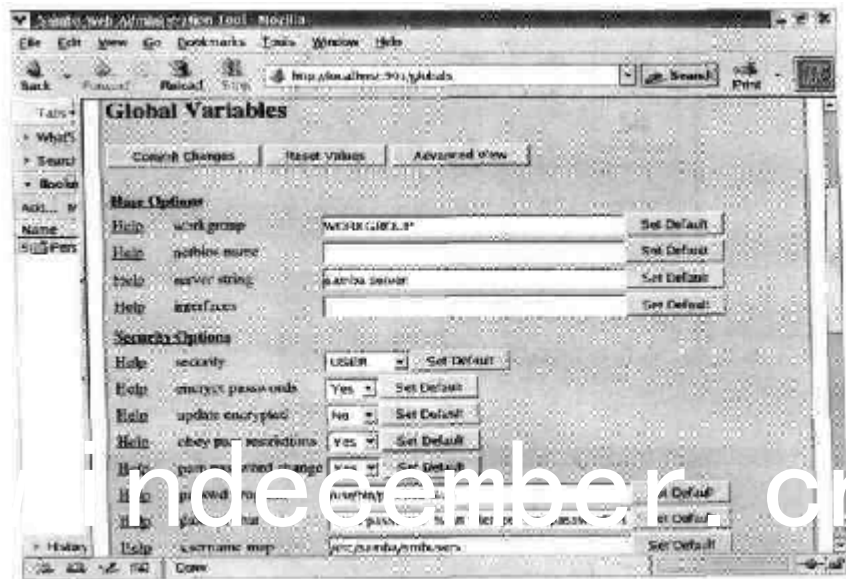


图29.12 SWAT全局变量

可以看到，每个变量都有相关的Help选项。单击Help选项可以打开smb.conf手册页，并在新的浏览器窗口中显示所要变量的内容。

在这个菜单和另外几个菜单中，可以访问下面三个按钮：Commit Changes、Reset Values与Advanced View。在单个设置中，还可以看到Set Default按钮。表29.8总结了这些按钮的功能。

表29.8 基本SWAT选项按钮

按钮	描述
Commit Changes	将所作改变写入smb.conf
Reset Values	在菜单中恢复当前的smb.conf值
Advanced View	提供其他设置
Set Default	激活与变量相关的默认设置

如果你读了本章前面的“Samba全局变量”一节，则可能对其中几个设置比较熟悉。尽管这里不准备重复介绍每个变量，但了解变量的组织方式有助于我们了解全局变量的工作。表29.9列出了全局变量的类别，其中有些类别只在单击global按钮之后才能看到。

表29.9 全局变量类别

类别	描述
Base	指定Samba服务器的基本选项
Security	可以配置允许连接的口令、用户账号与计算机
Logging	可以定制信息登记方式与位置
Protocol	定制与不同Windows协议的交互
Tuning	可以优化Samba服务器的性能
Printing	设置基本打印协议，标准Linux选项为cups与lprm
Filename Handing	可以设置计算机之间如何传输短文件名和普通文件名
Domain	如果将这台计算机配置成域控制器（PDC或BDC），则这时可以设置管理组与客户组
Logon	如果将这台计算机配置成登录控制器，则这时可以配置登录与脚本文件的位置
Browse	对共享目录与打印机的Microsoft浏览表配置这台计算机的优先级
Win S	设置使用NTFS与DFS服务器的基本选项
Locking	锁住文件，防止多个用户同时写入同一文件
MSDfs	允许使用Microsoft分布文件系统树
Winbind	用/etc/nsswitch.conf文件解析计算机主机名

完成改变之后，一定要单击Commit Changes按钮，将其保存到smb.conf中。然后单击菜单顶部的Shares链接，转入下节工作。

提示：每个SWAT变量都有相关的Help选项。单击Help选项可以打开一个新的浏览器窗口，其中显示了所要变量部分的内容。

Shares菜单

SWAT Shares菜单中可以配置现有共享或生成新共享。图29.13显示了最初的Shares菜单，要先选择共享，然后才能定制Shares菜单。

现有共享从smb.conf文件中列出的名称取得，包smb.conf文件中的典型共享包括[homes]与[tmp]。选择现有共享，然后单击Choose Share。

也可以配置新共享目录。在Create Share文本框中输入所选名称，然后单击Create Share打开完整的Shares菜单，如图29.14。

图中显示了与[homes]共享目录相关的共享参数。我们已经在本章前面介绍过所有这些共享参数。还可以单击Advanced View按钮显示更多配置选项。

完成改变之后，一定要单击Commit Changes按钮，将其保存到smb.conf中。然后单击菜单顶部的Printers链接。

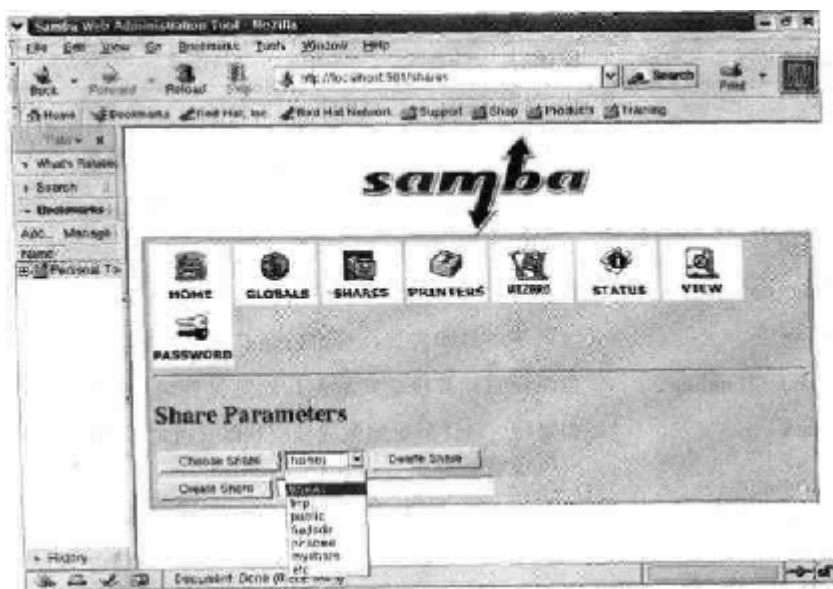


图29.13 SWAT Shares菜单

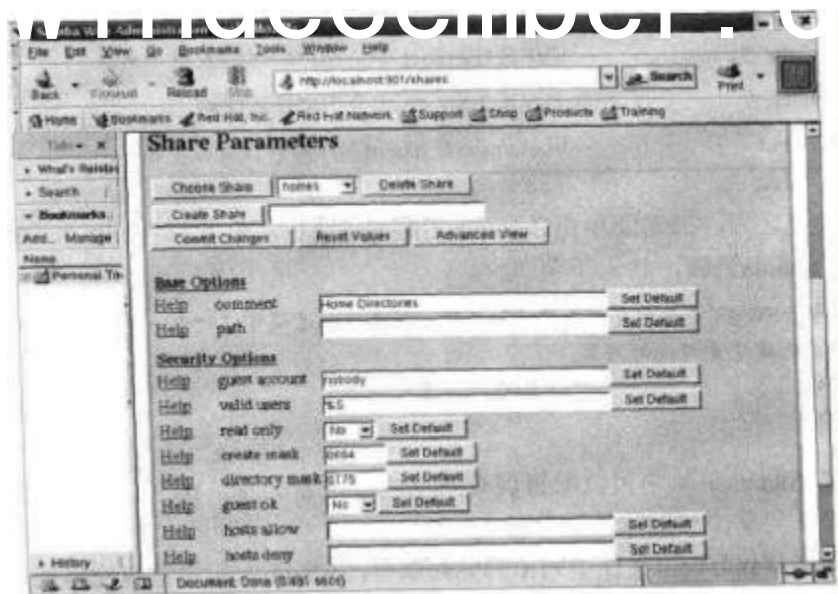


图29.14 配置共享参数

Printers菜单

SWAT Printers菜单和Shares菜单相似。可以用它配置现有打印机，也可以生成新打印机。进行选择之后，单击Choose Printer或Create Printer链接。Choose Printer下拉文本框中的各个选项来自于/etc/printcap文件。记住，CUPS与LPD都在这个文件中列出了打印机。进行选择之后，可以定制不同的打印机参数，如图29.15。

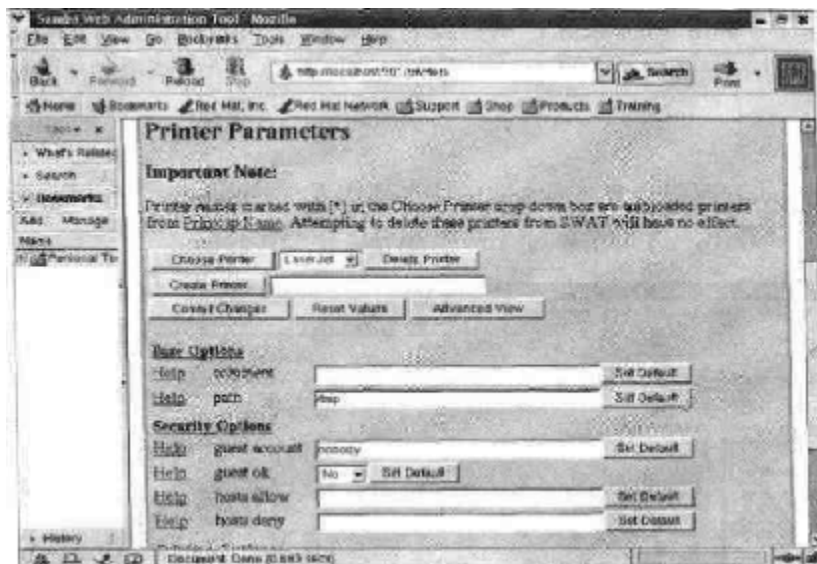


图29.15 SWAT打印机参数

完成设置之后，单击 **Commit Change** 按钮，将其保存到 `smb.conf` 中。然后单击菜单顶部的 **View** 链接。

View菜单

通过 **SWAT View** 可以检查 `smb.conf` 配置文件。注意所有说明语句和原 `smb.conf` 文件中的大多数设置已经删除。因为如果变量设置成默认值，则其不在正常视图中显示，如图29.16。

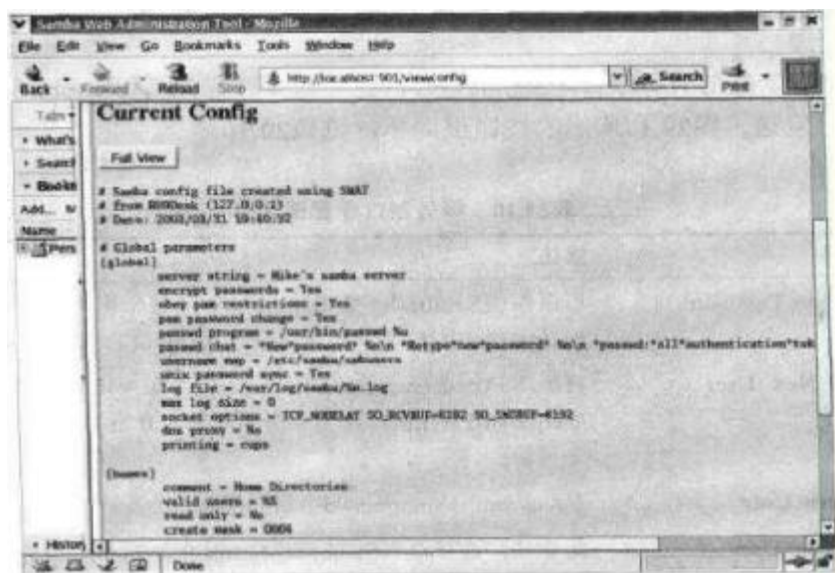


图29.16 保存的smb.conf文件

但是，如果单击Full View按钮，则可以看到完整的smb.conf文件，其中有所有的可用变量。然后可以单击Normal View按钮返回当前文件。这时，单击菜单顶部的Password链接。

Password菜单

SWAT Password可以管理本地Samba服务器中存储的Samba口令和远程计算机上的口令。从图29.17可以看出，这个菜单分为两个部分。

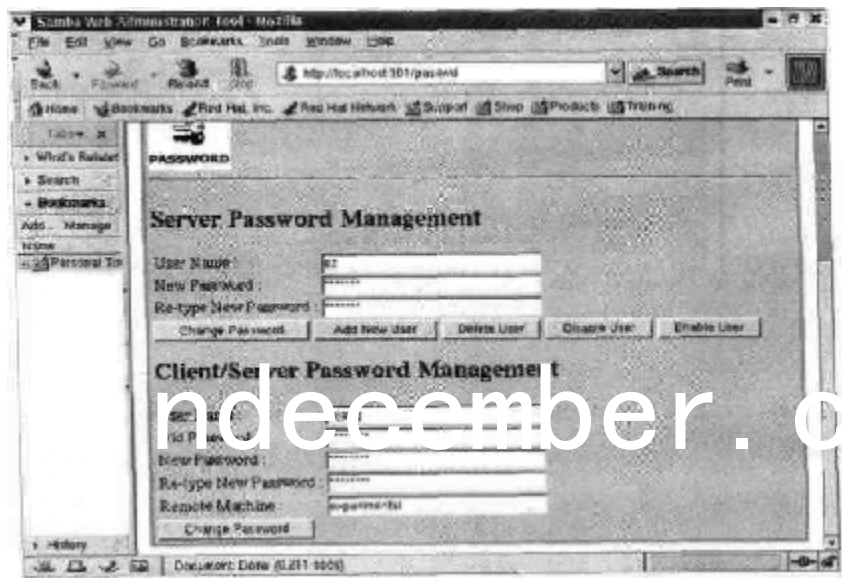


图29.17 口令管理

服务器口令管理

服务器口令管理部分可以管理Samba口令，这些口令在连接远程Samba或Microsoft Windows服务器时发送。图29.17所示的按钮很简单，见表29.10。

表29.10 服务器口令管理功能

功能	描述
Change Password	可以改变Samba用户的Samba口令，每个用户应当已经在/etc/passwd中存在
Add New User	将新用户加进/etc/samba/smbpasswd，每个用户应当已经在/etc/passwd中存在。这个命令不如前面介绍的smbadduser命令灵活
Delete User	从/etc/samba/smbpasswd中删除用户
Disable User	防止用户连接远程Samba或Microsoft Windows服务器
Enable User	允许用户连接远程Samba或Microsoft Windows服务器

客户机/服务器口令管理

这一部分可以改变远程Samba或Microsoft Windows服务器上的口令。在图29.17的例子中，我改变了运行Microsoft Windows 2000的计算机experimental上用户mjang的口令。

如果Samba无法在/etc/hosts、DNS或WINS中找到计算机名，则这个方法行不通。如果用户名在远程计算机上不存在，则这个方法也行不通。然后单击菜单顶部的Status链接。

Server Status菜单

用户从其他计算机连接Samba计算机之后，要检查服务器状态。例如，图29.18显示的Samba服务器从其他计算机连接，这些计算机为rh9server与laptop2，各自具有专用的IP地址。

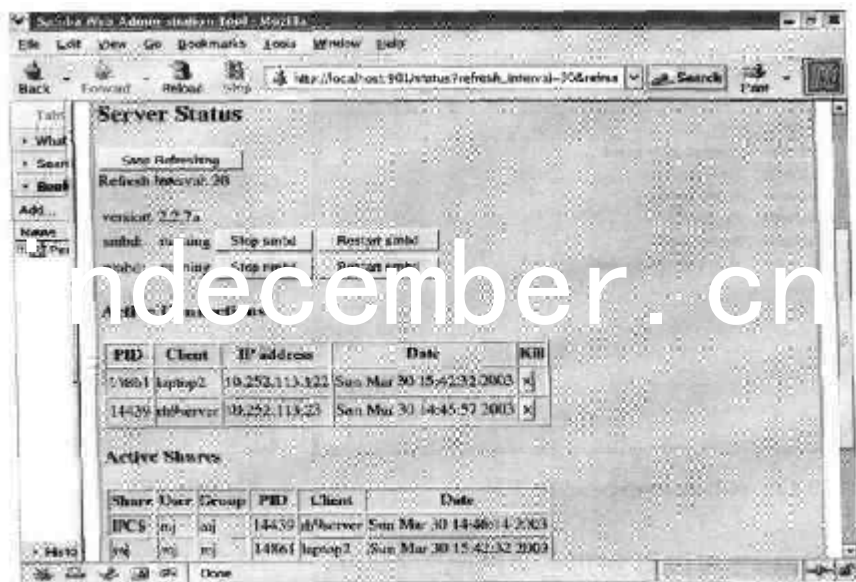


图29.18 Server Status菜单

这时SWAT是个活动的管理工具。在屏幕顶端，可以看到每个连接的状态每30秒刷新一次。可以停止或重启smbd与nmbd监控程序。在Active Connections中，可以浏览不同计算机的连接状态。要切断远程用户连接，单击Kill列出的相应按钮。

改变smb.conf文件时，要重新装入或重新启动smbd监控程序。重新启动smbd监控程序时还要重新启动nmbd监控程序。

redhat-config-samba工具

SWAT工具太复杂，还有一种更简单更灵活的方式可以将计算机配置成Samba服务器，即使用redhat-config-samba工具。在需要时安装redhat-config-samba RPM包，然后运行同名程序。可以看到图29.19所示的工具。

这个工具从当前的smb.conf文件读取初始设置，图29.19所示的设置反映了包smb.conf文件中的一些共享目录。

说明: redhat-config-samba工具相当新, 其特性还在不断改变, 使用时要小心。而SWAT工具更成熟, 至少是我比较喜欢的工具。

下面几节介绍配置基本的服务器设置、管理Samba用户和生成新共享。

服务器设置

在redhat-config-samba中单击Preferences►Server Settings打开服务器设置对话框, 如图29.20。可以看出, 基本服务器设置很简单, 选项与前面几节相似。由于Workgroup文本框是空的, 因此workgroup变量设置为默认值WORKGROUP, 服务器说明为“Mike's Samba Server”。

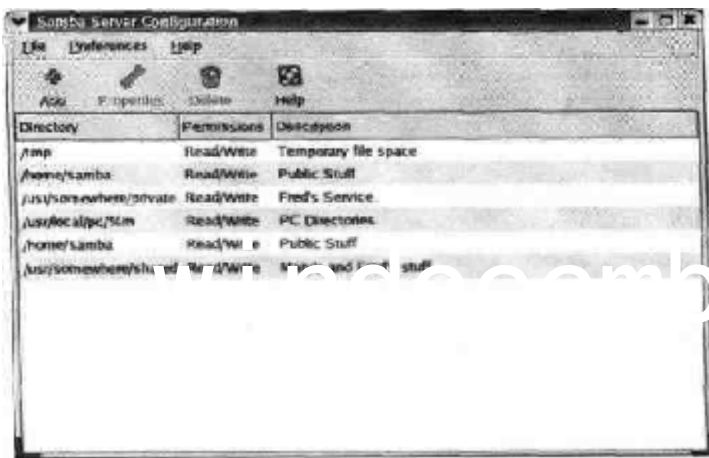


图29.19 redhat-config-samba工具



图29.20 服务器设置对话框Basic标签

单击Security标签可以看到几个关键的安全变量。记住, 可以选择SHARE、USER、SERVER或DOMAIN验证方式。如果选择SERVER或DOMAIN, 则需指定验证服务器名。大多数当前Windows服务器都使用加密口令。Guest Account账号可以在/etc/passwd中指定, 如guest与ftp。图29.21显示了这些选项。

用户管理

可以在redhat-config-samba中管理用户。在这个工具中单击Preferences►Samba Users进入Samba用户对话框, 如图29.22。

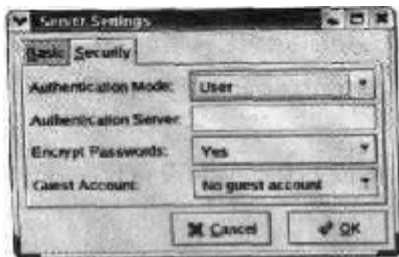


图29.21 Server Setting中的Security标签

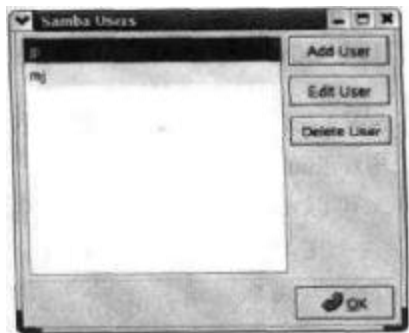


图29.22 管理Samba用户

这里的选项很简单，可以从/etc/samba/smbusers数据库中增加、编辑或删除用户。单击Add User可以打开Create New Samba User对话框。如果能记住本章前面介绍的smbadduser命令，则可以看到它与图29.23所示文本框中所需的信息是一致的。

生成新共享

可以用redhat-config-samba增加新的目录共享。在这个工具中单击Add按钮打开Create Samba Share对话框，图29.24显示了几个选项。

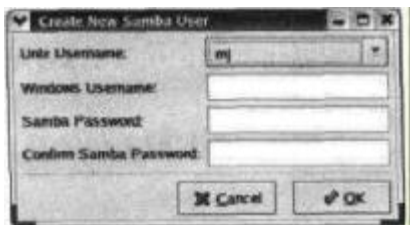


图29.23 Create New Samba User对话框

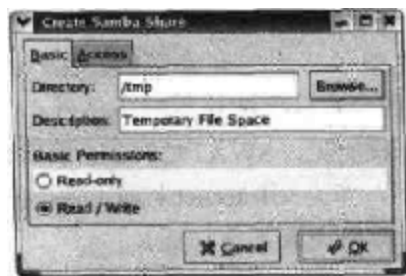


图29.24 Create Samba Share对话框

这些选项很简单，但与前面对应的变量有对应关系，因此我们在图2.11总结了Create Samba Share的基本选择。

表29.11 生成新共享的基本选择

选项	描述
Directory	指定要共享的目录
Browse	调用Select Directory对话框，帮助寻找共享的目录
Description	对应于smb.confcomment
Read-Only	删除不允许写入这个目录的用户
Read/Write	删除允许写入这个目录的用户

在Access标签中，可以从加入/etc/samba/smbusers文件的用户访问中指定用户或访问所有用户。

小结

Samba是个异构服务，可以沟通Linux与Microsoft之间的差别。一旦配置Samba之后，Linux计算机就像工作组或域中的Microsoft成员服务器一样。甚至可以将Samba配置成Microsoft主域控制器。

可以将Microsoft配置成Linux客户机。利用正确的包，甚至可以用mount命令从另一Linux服务器或其他Microsoft Windows服务器中连接共享目录。甚至可以在终端方式中连接共享目录，类似于FTP连接。

Linux配置文件位于/etc/samba，关键文件是smb.conf。samba-* RPMs包中原有的smb.conf

文件包括一些说明语句，有助于进一步学习。

`smb.conf`文件中的全局设置可以确定服务器如何连接Microsoft网络。可以配置安全性、打印机列表、日志文件、定制登录目录、浏览优先级，等等。还有共享设置，可以配置不同目录与打印机。可以按用户限制共享，确定文件如何访问与写入，等等。配置`smb.conf`之后，可以用`testparm`命令检查其语法。

SWAT是配置`smb.conf`的Web浏览器工具。它们在`xinetd`监控程序中激活`swat`服务。这个工具是高度可定制的，具有Home、Globals、Shares、Printers、View、Password与Server Status menus菜单。

红帽子公司开发了SWAT的简单替换工具`redhat-config-samba`。由于`redhat-config-samba`相当乱，因此使用时应格外小心。尽管它有助于配置基本共享，但没有SWAT的灵活性。据我所见，SWAT是Samba最佳的GUI工具。

下一章介绍Internet上最重要的Web服务器Apache，介绍如何将其配置成为局域网提供Web页面和完成其他功能。

第30章 Web服务

Linux的发展与万维网的发展密切相关。第1章曾介绍过，Linux是由志愿者社区开发的软件。Apache是目前使用最广泛的Web服务器，也是由志愿者社区开发的软件。因此，毫不奇怪的是，Linux和Apache的成功都与万维网的成功密切相关。

1995年，最著名的Web服务器是伊利诺斯大学国家超级计算机应用中心（NCSA）的HTTP监控程序。这个Web服务器的开发者离开NCSA中心之后，全世界的Web管理员纷纷开始通过补包更新和维护这个程序，从而形成了“贴满补丁”的服务器，因此把这个Web服务器软件称为Apache。

由于Apache和Linux的开发非常相似，因此它们的命运联系在一起。但是，Apache也用于其它UNIX式操作系统和Microsoft Windows。据Netcraft统计（www.netcraft.com/survey），Apache是1996年初以来Internet上最普及的Web服务器。

本章介绍Red Hat Linux 9所带的Apache版本V 2.0.40。Apache项目Web站点httpd.apache.org中会提供最新版本，红帽子公司的高级Web服务器产品中提供的Stronghold企业Web服务器，也是以Apache为基础的。

此外，本章还将介绍红帽子公司的Content Accelerator，原名为Tux，是基于内核的Web服务器，用于快速提供静态信息（如图形），可以配置成和Apache一起使用。本章介绍下列主题：

- 探索Web服务器选项
- 了解Apache基础
- 配置Apache
- 配置Red Hat GUI Apache实用程序
- 集成Red Hat Content Accelerator

探索Web服务器选项

Apache不是惟一可用的Web服务器，也可以购买一些专用的Web服务器。表30.1简要列出了几个重要Web服务器。据Netcraft统计（www.netcraft.com/survey），Internet上超过1%的Web站点都在使用如下四个Web服务器：Apache、Microsoft公司的Internet Information Server、Zeus和Sun系统公司的Sun One。

表30.1 Web服务器

名称	描述
AOLServer	美国在线公司使用，是个开放源代码Web服务器，更多信息见 www.aolserver.com
Apache	Internet上最普及的Web服务器，更多信息见 httpd.apache.org

(续表)

名称	描述
Boa	高性能开放源代码Web服务器，与其他Web服务器不同的是，它用一个进程运行大多数连接。更多信息见 www.boa.org
Caudium	模块化、开放源代码Web服务器，和Boa相似，它用一个进程运行大多数标准连接。更多信息见 www.caudium.net
Jigsaw	W3C开发的Web服务器，更多信息见 www.w3.org/Jigsaw 。W3C的所有软件都遵循开放源代码许可证
Red Hat Content Accelerator	基于内核的高性能Web服务器，原名为TUX。更多信息见 www.redhat.com/docs/manuals/tux
Resin	基于Java服务器页面（JSP）的服务器，更多信息见 www.caucho.com/resin 。这是专属服务器，需要付费购买
Roxin	采用GPL许可证的安全Web服务器。更多信息见 www.roxin.com
Servetec	用Java语言编写的应用程序Web服务器。更多信息见 www.servetec.com
Stronghold	基于Apache的安全Web服务器，由红帽子公司所有，是红帽子高级服务器的部分。更多信息见 www.redhat.com/software/stronghold
Sun One	Sun系统公司的Web服务器，原名为iPlanet，现在放在Sun One系统应用程序服务器中。更多信息见 www.sun.com/software
WN	小型安全Web服务器，使用GPL许可证。更多信息见 hopf.math.nyu.edu
Zeus	商业化高性能Web服务器。更多信息见 www.zeus.co.uk

了解Apache基础

Apache是个Web服务器，换句话说，这个服务在Linux之类的操作系统中运行，响应请求。用户在浏览器中输入所要Web页面的地址时，计算机通过DNS服务器寻找所要的Web服务器的IP地址，一旦建立连接之后，浏览器请求Web页面，通常在TCP/IP端口80。Apache响应这种请求，将Web页面发送给请求计算机。

如果当前运行基于Apache1.3.x的Web服务器，则要进行一些决策。Red Hat Linux 9带有Apache V2.0.40，如果安装这些Apache包，则可能要进行几个配置的改变。升级Apache服务器之前，要先了解新系统并用新系统测试Web站点。

Apache 2.0

红帽子公司在Red Hat Linux8.0中首次加进了Apache V2.0.x，但Apache 1.3.x仍然很普及，许多熟悉Apache的人不一定熟悉2.0.x中的改变，这些改变包括：

- 虚拟主机特性，可以用同一IP地址配置完全不同的Web站点。
- 目录已经改变。Perl、PHP（PHP超文本处理器）、Python、SQL（结构化查询语言）

和SSL（安全套接层）在/etc/httpd/conf.d目录中有自己的配置文件。

- 变量已经改变。例如，本章稍后将介绍如何用Listen变量改变与Apache相关的TCP/IP端口。
- 包更加模块化，我们将在下节介绍与Apache相关的各个包。
- 线程高效使用。线程可以共享数据。在Apache2.0中，线程通常基于进程，使服务器不会崩溃。MPM（多处理模块）支持这方面的定制，从而对主机操作系统优化Apache。
- 可以使用IPv6地址。尽管Apache 1.3.x中有个补包可以使用IPv6地址，但我们不再提供。

尽管其中一些特性已经由Apache 1.3.x向下移植（这也是这个老Apache服务器还会普及的原因之一），但这些特性是针对Apache 2.0开发的。

包

Apache的模块化服务器，Web上第5章已经介绍过，惟一需要的Apache RPM包是httpd-*，但还可以安装许多其他Apache包，见表30.2。

表30.2 Apache包

包名	描述
httpd	安装主Apache服务器
httpd-manual	包括完整Apache手册
hwcrypto	可以和Linux硬件加密加速器接口
mod_auth_pgsq1	可以限制访问PostgreSQL数字
mod_auth_mysql	可以限制访问MySQL数字
mod_python	在Apache中增加Python语言解释器
mod_perl	在Apache中增加Perl语言解释器
mod_ssl	在Apache中增加SSL安全性
php	对动态脚本安装PHP（PHP指PHP超文本处理器）
php-imap	对Apache提供IMAP邮件服务器支持
php-ldap	对Apache允许LDAP支持
php-mysql	对MySQL数据库实现PHP支持
php-odbc	对ODBC（开放数据库连接）数据库实现PHP对支持
php-pgsq1	对PostgreSQL数据库实现PHP支持
squid	安装代理服务器
tux	增加基于内核的Web服务器
webalizer	包括Web服务器的日志分析程序

配置Apache

安装所要的Apache包之后，服务器就可以向本地计算机提供Web页面。只要启动httpd服务并将Web浏览器指向localhost地址即可。

但是，如果不能从其他计算机上调用Web服务器的Web页面，则这个Web服务器作用不大。本章要分析主要Apache配置文件httpd.conf的细节。

这些设置基于HTTP（超文本传输协议）v 1.1标准规范，这里只是简要介绍Apache 2.0，更多信息见“Linux Apache Web Server Administrator”（第二版，Sybex公司，2002年版）。

提示：如果安装httpd-manual-* RPM包，则可以在/var/www/manual目录得到完整的HTML格式的Apache手册。

启动Apache

安装需要的Apache包之后，很容易启动Apache。和本章介绍的其他服务一样，只要从etc/rc.d/init.d目录中启动相应脚本即可。这里可以使用下列命令：

```
# service httpd start
```

如果仍然使用默认Apache配置文件，则可以看到下列消息：

```
Starting httpd: httpd: Could not determine the server's fully qualified domain
name, using 127.0.0.1 for ServerName
```

现在可以将所选Web浏览器指向localhost地址，即回环IP地址，第20章将其定义为127.0.0.1。图30.1显示了Mozilla Web浏览器中的结果。

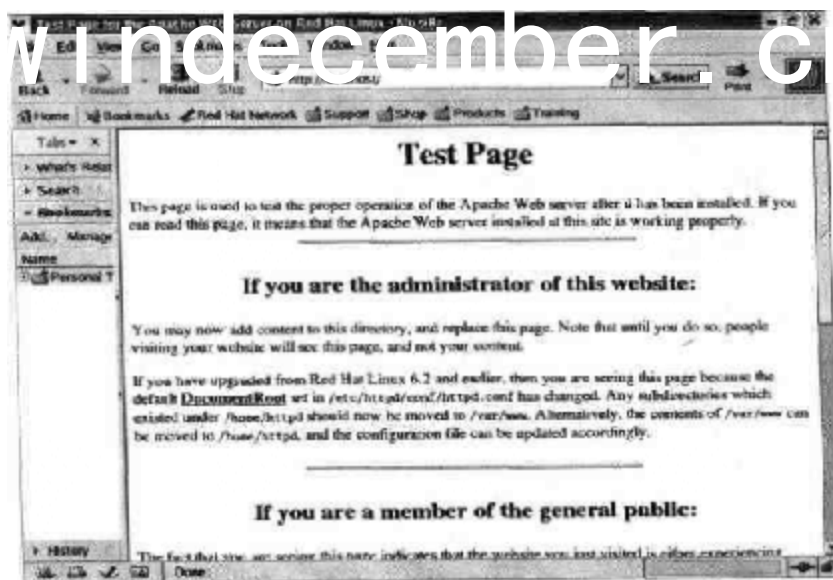


图30.1 Apache安装完毕

还要用chkconfig之类的命令（见第13章介绍）保证下次在相应运行级启动Linux时启动Apache。例如，下列命令在2、3、5运行级启动Linux时启动Apache：

```
# chkconfig --level 235 httpd on
```

现在可以开始定制Apache配置。

定制Apache

主Apache配置文件httpd.conf位于/etc/httpd/conf目录中，它分为三部分。在全局环境段中，可以配置这个Web服务器的基本设置。在主服务器配置段中，可以设置服务器中任何Web

站点的基本默认。虚拟主机段可以在Apache服务器上设置几个不同的Web站点，即使只有一个IP地址。

说明：Apache最初有三个不同的配置文件access.conf、srm.conf与httpd.conf，它们位于同一目录中。尽管新版Apache 1.3.x在httpd.conf中增加了access.conf与srm.conf中的信息，但服务器至少还需要空白的access.conf与srm.conf文件。但Apache 2.0.x中不再需要这些多余的配置文件。

Apache配置文件中的命令称为指令。下面几节分析Red Hat Linux 9安装的默认Apache httpd.conf中的指令。你可以自己阅读这个文件，其中还有许多其他重要的注释。

前面带#号的命令在默认Apache配置文件中标识说明语句。如果首次学习Apache，则不妨试试这些命令。在计算机上设置一些Web站点文件，使用DocumentRoot指令指定的目录，默认为/var/www/html。试激活其中一些命令，重新启动httpd监控程序，并看看发生的改变，也许你会对结果大吃一惊。

全局环境段

我们要介绍默认Apache配置文件中全局环境段的每个指令。全局环境段的变量适用于这个服务器上要配置的所有虚拟主机。有些变量是基本参数，有些涉及不同的客户机、端口设置、其他配置文件的指针和模块地址。

注意 如果一个指令设置为0，则通常表示该指令不设置界限。例如，如果将Timeout设置为0，则客户机浏览器的连接可以永久打开。

基本全局环境段参数

下列指令向Web站点用户提供软件的基本信息。下列命令告诉用户，Web服务器是UNIX这类系统中的Apache，但也可以使用其他命令，见表30.3：

```
ServerTokens OS
```

表30.3 ServerTokens指令选项

指令	描述
ServerTokens Prod	指定Web服务器为Apache
ServerTokens Min	指定Apache及其版本号
ServerTokens OS	指定Apache及其版本号与操作系统类型
ServerTokens Full	指定Apache及其版本号与操作系统类型和编译模块

ServerRoot指令指定配置、错误和日志文件所在的目录：

```
ServerRoot "/etc/httpd"
```

如果运行ls -l /etc/httpd，则可以看到某些目录实际地址的链接。例如，/etc/httpd/logs链接/var/log/httpd目录。

Apache的不同连接包括父子进程。ScoreBoardFile参数帮助这些进程相互通信，否则要通过活动内存才能相互通信。

```
#ScoreBoardFile run/httpd.scoreboard
```

提示：我通常避免激活ScoreBoardFile参数，它只在某些体系结构中需要，不包括Red Hat Linux 9。

注意run是个相对子目录，完整的目录名基于ServerRoot指令，即/etc/httpd/run。

PidFile指令指定Apache记录进程标准符（PID）的文件：

```
PidFile run/httpd.pid
```

如果计算机无法在网络上通信，则要一个**Timeout**值，避免Apache死机。**Timeout**指令指定停止值（秒数）：

```
Timeout 300
```

通常，每个连接允许传递多个请求。下列命令禁止这种行为：

```
KeepAlive Off
```

如果打开**KeepAlive**指令，则可以用**MaxKeepAliveRequests**指令控制每个连接的请求数：

```
MaxKeepAliveRequests 100
```

在Apache与某个Web浏览器之间建立连接后，**KeepAliveTimeout**指令指定等待下一个客户请求的秒数：

```
KeepAliveTimeout 15
```

详细客户机参数

Apache中有几个MPM（多处理模块）。这些多处理模块可以分成三大类：

- **Prefork MPM**适合基于进程的Web服务器，适合Apache模块不需要单独线程时，这与Apache 1.3.x中的行为相似。
- **Worker MPM**支持两种类型的模块，但不能在使用Apache 1.3模块时使用，因为线程可能造成问题。
- **Per-child MPM**支持客户机需要不同用户ID的Web站点。

说明：多处理模块很灵活，mpm_winnt和mpm_netware分别是针对Windows NT与Novell Netware网络的特定模块。

每个多处理模块类别中可以指定几个常用指令。

启动Apache时，**StartServers**指令对需要Web页面的用户设置可用的子服务器进程数：

```
StartServers 8
```

启动Apache之后，可以接受其他客户的请求。如果未用服务器进程数在**MinSpareServers**指令指定的值以下，则自动启动其他httpd进程：

```
MinSpareServers 5
```

通信流减少时，**MaxSpareServers**指令指定可以闲置的最大httpd进程数：

```
MaxSpareServers 20
```

可以用**MaxClients**指令控制向Web服务器请求信息的客户数：

```
MaxClients 150
```

还可以用**MaxRequestsPerChild**指令控制每个客户的信息请求数：

```
MaxRequestsPerChild 1000
```

Apache 2.0服务器可以对每个请求启动新线程。**MinSpareThreads**指令与**MinSpareServers**相似,使Apache可以处理峰值时期的其他请求:

```
MinSpareThreads 25
```

请求数减少时,Apache监视空闲线程数,此数超过**MaxSpareThreads**时则删除一些线程:

```
MaxSpareThreads 75
```

每个子进程可以生成多个线程,以处理每个用户对Web站点的请求。**ThreadsPerChild**指令在每个子进程启动时生成:

```
ThreadsPerChild 25
```

可以用**MaxRequestsPerChild**指令限制每个子进程允许的线程数(默认httpd.conf文件中没有限制):

```
MaxRequestsPerChild 0
```

还可以用**MaxThreadsPerChild**指令限制每个子进程允许的线程数:

```
MaxThreadsPerChild 20
```

端口设置

可以将Apache设置成只监听来自某个IP地址或TCP/IP端口的请求。默认httpd.conf文件中包括下列指令:

```
#Listen 12.34.56.7
Listen 80
```

如果有多个网卡,则可以将Apache限制在某些网络。例如,下列指令只监听IP地址192.168.13.64上TCP/IP端口为80的网卡:

```
Listen 192.168.13.64:80
```

说明: Listen指令覆盖Apache v 1.3.x中的BindAddress与Port指令。

其他配置文件的指针

前面曾介绍过,Apache 2.0.x服务器还有其他配置文件。默认情况下,它们放在/etc/httpd/conf.d目录中。通常,文件地址由**ServerRoot**指令(设置为/etc/httpd)和**Include**指令确定:

```
Include conf.d/*.conf
```

模块地址

需要Apache中的模块时,应装入httpd.conf配置文件中。通常,模块按下列格式列出:

```
LoadModule module_type location
```

例如,下列指令从**ServerRoot**模块子目录/etc/httpd/modules装入模块access_module。其链接Apache模块的实际目录/usr/lib/httpd/modules。

```
LoadModule access_module modules/mod_access.so
```

默认httpd.conf文件中列出了一些个模块,表30.4提供了简要介绍。模块的顺序与其在文件中出现的顺序相同。

表30.4 标准Apache模块

模块	描述
access_module	支持基于标准符的访问控制，如计算机名或IP地址
auth_module	可以用文本文件验证（用户名和口令）
auth_anon_module	让用户匿名访问需要验证的区
auth_dbm_module	支持DBM（数据库管理）文件验证
auth_digest_module	用MD5摘要设置验证
include_module	包括动态Web页面的SSI（服务器方包括）数据
log_config_module	对服务器请求设置日志
env_module	可以控制传入CGI（公共网关接口）脚本与SSI页面的环境
mime_magic_module	将Apache设置成从内容的前几个字节定义文件类型
cern_meta_module	按照W3C标准支持Web页面的其他元信息
expires_module	让Apache设置页面有效期，支持Web浏览器的刷新请求
headers_module	可以控制HTTP请求并响应信息头
usertrack_module	支持用cookies跟踪用户
unique_id_module	设置每个请求的惟一标识符
setenvif_module	允许Apache根据请求特征（如Web浏览器类型）设置环境变量
mime_module	将文件扩展名（如.txt）与特定应用程序相关联
dav_module	支持Web分布式写作与脚本功能
status_module	提供服务性能与功能信息
autoindex_module	可以列表Web目录中的文件
asis_module	发送文件而不增加信息头
info_module	支持用户访问服务器的配置信息
dav_fs_module	支持dav_module
vhost_alias_module	可以动态配置虚拟主机
negotiation_module	将Apache设置为匹配内容（如语言、Web浏览器设置等）
dir_module	支持浏览Apache目录中的文件
imap_module	配置imagemap指令（与电子邮件无关）
actions_module	可以运行CGS脚本
speling_module	允许请求文档名中的小错（可笑的是，这个模块名拼写不对）
userdir_module	支持对用户特定目录的访问
alias_module	设置改向URL
rewrite_module	支持改向URL
proxy_module	设置Apache代理服务器
proxy_ftp_module	允许FTP数据的代理服务器支持
proxy_http_module	允许HTTP数据的代理服务器支持
proxy_connect_module	用于代理服务器的连接请求
cgi_module	配置运行CGI脚本
cgid_module	支持外部监控程序运行CGI脚本

一个更有趣的模块是info_module，在下节末尾可以看到，它支持localhost/server-info中浏览器的Apache服务器的详细配置图。

主服务器配置

配置虚拟主机之前，先要看看httpd.conf配置文件的下一部分，包括Apach的默认指令。尽管可以对其中许多指令进行不同的设置，但需要知道这个部分的默认值。我们依次分析httpd.conf文件中这个部分的基本设置。

说明：这一段很长，如果你习惯于一次读一整段，则可能要先歇一会儿。

系统用户

根据User与Group指令指定，Apach监控程序httpd在这里和/etc/passwd与/etc/group中指定特定的用户名与组名：

```
User apache
Group apache
```

管理联系

对Apach生成的Web页面，有一列管理联系名单，由ServerAdmin指令指定：

```
ServerAdmin root@localhost
```

Web服务器名

如果有个Web服务器的Web管理站点，则可能要用ServerName指令设置，如果没有DNS服务器中的完全限定域名，则可以使用IP地址：

```
#ServerName new.host.name:80
```

如果激活这个指令，则通常用每个虚拟主机中设置的名称覆盖它。

规范名

技术上，每个URL（如http://www.Sybex.com/）都在尾部有个斜杠。但我老会把它忘掉。如果没有下列指令，则导航到www.Sybex.com时会到达ServerName指令指定的地址。标准httpd.conf文件中有个UseCanonicalName指令，可以自动增加尾部的斜杠：

```
UseCanonicalName Off
```

文档根

Web服务器的根目录由DocumentRoot指令指定：

```
DocumentRoot "/var/www/html"
```

Web目录权限

然后要看看用户在服务器的Web站点上可以访问的目录中是否有默认缺陷。它是用<Directory />容器设置的，定义与DocumentRoot相关的权限：

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>
```

Options指令确定到哪里可以找这个目录中的文件，可以按表30.5所示设置为几个不同的规则。AllowOverride指令可以从.htaccess文件中找允许访问某个文件的用户或计算机名列表，而AllowOverride None设置不检查.htaccess文件。

表30.5 Options指令值

值	描述
All	支持除MultiViews以外的所有设置
ExecCGI	可以运行CGI脚本
FollowSymLinks	让请求跟随符号键文件或目录
Includes	可以使用SSI（服务器方包括）
IncludesNOEXEC	支持SSI而不支持CGI
Indexes	如果没有index.html类型的文件，则将Apache设置成返回该目录中的文件清单。这个文件的选项在DirectoryIndex指令中指定
MultiViews	支持内容协商，如不同语言的Web页面之间的内容协商
SymLinkIfOwnerMatch	目录文件与目录属于同一用户时支持跟随符号键

.htaccess文件

.htaccess文件是分布式配置文件，可以配置Web站点上的各个目录，是对特定目录实现限制性访问的常见方法。

.htaccess文件在大多数情况下不需要，可以在主Apache配置文件httpd.conf中配置各个目录的访问。在主Apache配置文件的默认版本中，寻找<Directory>容器，注意不同目录的限制各不相同。

但是，如果服务器中有大量Web站点，如许多ISP相关的个人Web页面，则可以用.htaccess文件让各个用户控制主目录中Web页面的访问。可以设置读取.htaccess文件的标准模式，见“用户目录权限”一节介绍。

如果要实现分布式配置文件，则可以设法保护。找到httpd.conf中的AccessFileName指令，指定.htaccess以外的隐藏文件名。见本章稍后的“访问控制”一节。

特定目录权限

下面要看看httpd.conf中/var/www/html目录的默认权限，由下列容器指定：

```
<Directory "/var/www/html">
```

下列Options指令可以通过符号键支持改向，在没有index.html类型文件时列出当前目录中的文件（例子见图30.2）：

```
Options Indexes FollowSymLinks
```

上节曾介绍过，AllowOverride指令指定.htaccess文件中的指令类型，下列指令不检查.htaccess文件：

```
AllowOverride None
```

最后，还有访问控制指令。下列命令按顺序在这个目录寻找Allow与Deny指令：

```
Order allow,deny
Allow from all
```

根目录权限

现在在httpd.conf文件中对访问Web站点顶层目录（也称为DocumentRoot）用户增加几个指令：

```
<LocationMatch "^/$">
    Options -Indexes
    ErrorDocument 403 /error/noindex.html
</LocationMatch>
```

<LocationMatch "^/\$">容器看上去有点奇怪，这个特定指令对根目录（/）采用其中的命令Options与ErrorDocument。

Options -Indexes指令禁止列出文件，这是Indexes设置前面的-指定的。如果没有index.html页面，则ErrorDocument指令向用户返回指定的错误Web页面。这个地址基于ServerRoot指令，因此，noindex.html位于/etc/httpd/error目录中。

奇怪的是，noindex.html文件是个测试页。它在启动Apache而没有与实际Web站点相关的页面时显示，如图30.1。

用户目录权限

可以在用户主目录中设置Web页面，它们默认用下列命令关闭：

```
UserDir disable
```

可以将其换成下列命令：

```
UserDir public_html
```

假设用户ez在/home/ez/public_html目录中有一组Web页面文件，假设Web站点为www.example.abc，则要设置相应的权限如下：

```
# chmod 711 /home/ez
# chmod 755 /home/ez/public_html
# chmod 744 /home/ez/public_html/*
```

将浏览器指向www.example.abc/~ez时，可以看到/home/ez/public_html目录中存储的任何index.html Web页面。

还可以进一步控制用户主目录中文件与Web页面的访问。下列命令来自默认的httpd.conf文件：

```
#<Directory /home/*/public_html>
#   AllowOverride FileInfo AuthConfig Limit
#   Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
#   <Limit GET POST OPTIONS>
#       Order allow,deny
#       Allow from all
```

```
#      </Limit>
#      <LimitExcept GET POST OPTIONS>
#          Order deny,allow
#          Deny from all
#      </LimitExcept>
#</Directory>
```

如果激活这些命令，则Apache允许浏览public_html子目录中的文件，见稍后的“目录列表”一节介绍。

前面曾介绍过，AllowOverride指令与Apache从各个.htaccess文件读取的访问信息相联系。表30.6显示了与这个指令相关的不同参数。所有描述所指的命令都可以在.htaccess文件中对各个目录使用。

表30.6 AllowOverride指令参数

参数	描述
AuthConfig	支持使用授权指令
FileInfo	可以配置不同文档类型
Indexes	可以配置目录索引
Limit	支持访问控制限制，即拒绝或允许

表30.5介绍的Options指令支持内容协商、文件索引、跟随符号键和SSI而不支持CGI。

Limit指令对从用户主目录发送（POST）与接收（GET）文件的用户设置选项，LimitExcept指令拒绝使用所有其他的访问命令。

目录索引

用户在Web站点上导航时，实际上是查找目录。DirectoryIndex指令告诉Apache要发给Web站点用户的页面类型：

```
DirectoryIndex index.html index.html.var
```

index.html文档是许多Web站点使用的标准主页文件，index.html.var是一种设置动态主页的方法。可以在/var/www/error目录中看到.var文件的例子。在某个文本编辑器中打开这些文件，可以看到标准的错误消息。

访问控制

前面的.htaccess文件中曾介绍过，可以对各个目录配置访问控制文件。默认情况下，这是隐藏文件.htaccess，但也可以用AccessFileName指令设置不同文件名。

```
AccessFileName .htaccess
```

下列files指令保证用户浏览Web站点时看不到任何以.ht打头的文件：

```
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>
```

MIME类型

MIME（多用途Internet邮件扩展）标准最初是为在电子邮件中发送二进制文件而建立的，它也适用于Web页面。例如，可以将浏览器配置成在导航到.htaccess中的PDF文件时打开一个PDF阅读器。MIME类型与文件扩展名之间的标准转换由TypesConfig指令列出：

```
TypesConfig /etc/mime.types
```

许多文件没有.pdf、.doc之类的扩展名。可以设置DefaultType指令指定浏览器中的显示选项。如果使用文本文件，则也可以使用下列标准：

```
DefaultType text/plain
```

如果大多数文件都采用二进制格式，则可能要向用户发送几十页毫无意义的信息，除非将这个指令改成如下：

```
DefaultType application/octet-stream
```

如果扩展名没有提供线索，则可以使用MIMEMagicFile指令，其使用表30.4定义的mod_mime_magic模块：

```
<IfModule mod_mime_magic.c>
#  MIMEMagicFile /usr/share/magic/mime
MIMEMagicFile conf/magic
</IfModule>
```

记住，conf/magic之类的相对路径基于ServerRoot指令。换句话说，这一段指向/etc/httpd/conf/magic目录中的MIMEMagicFile文件。

在httpd.conf文件末尾，还有一个相关指令。AddType指令可以覆盖/etc/mime.types中TypesConfig定义的配置：

```
AddType application/x-tar .tgz
```

日志数据

Apache日志可能很大。如果运行大型的商业化Web站点，则每天的日志数据可能超过几百MB。选择的日志数据很容易使系统过载。

```
HostnameLookups Off
```

通常，HostnameLookups设置为Off，否则Apache会寻找每个请求用户的完全限定域名。一般不要这么做，除非有可靠的DNS服务器访问，而且网络能够处理这么大的信息量。

可以设置不同日志文件的地址。ErrorLog指令设置error_log文件地址。指定ServerRoot值时，下列日志文件位于/etc/httpd/logs目录中：

```
ErrorLog logs/error_log
```

可以控制发送到ErrorLog文件的消息类型，LogLevel指令的取值debug、info、notice、warn、error、crit、alert、emerg与标准的错误日志文件/etc/syslog.conf相似，见第13章。

```
LogLevel warn
```

日志信息按特定格式发送到error_log文件中，可用下列LogFormat指令定义：

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
```

每一行采用四种不同格式之一指定一组数据：**combined**、**common**、**referer**与**agent**。

表30.7列出了与**LogFormat**相关的变量，还有大量其他变量，可以从/var/www/manual/mod目录的mod_log_config.html文件中找到。其他请求字段符合www联盟的标准，见www.w3.org/Protocols/HTTP/HTREQ-Headers.html。

表30.7 LogFormat指令变量

变量	描述
%a	远程IP地址
%b	发送的字节（不包括HTTP头）
%h	远程主机
%l	远程登录名
%r	客户机请求的第一行
%s	请求并行的
%t	时间
%u	远程用户
referer	指定用户单击链接的页面（Apache中这个变量的拼写有错）
user-agent	指定客户机程序，如Mozilla

还可以用**CustomLog**变量设置另外几种日志的地址。可以在一个虚拟主机中进行设置，使服务器中各个Web站点的拥有者能得到自己的日志文件：

```
# CustomLog logs/access_log common
CustomLog logs/access_log combined
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent
#CustomLog logs/access_log combined
```

这些行指定日志文件地址。根据默认的**ServerRoot**，这里是/etc/httpd/logs，发送到每个日志文件的实际信息基于引用的**LogFormat**。例如，活动**CustomLog**指令引用组合格式，如下所示：

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
```

服务器签名Web页面

根据**ServerSignature**指令，httpd.conf文件可以在动态生成的Web页面中增加一个元素。其通常设置如下：

```
ServerSignature On
```

ServerSignature为On时，可以在动态生成的Web页面底部看到如下的消息：

```
Apache/2.0.40 Server at localhost Port 80
```

如果将On换成Email, 则会得到从计算机名(这里是localhost)到ServerAdmin指令定义的服务器管理员之间的超级链接。

别名

可以用Alias指令设置URL中的目录与计算机上的目录之间的链接。例如, 默认httpd.conf文件中第一个Alias指令从一个URL链接/icons/子目录:

```
Alias /icons/ "/var/www/icons/"
```

到Web服务器上的/var/www/icons/目录。这里这可以指定与/var/www/icons/相关的权限。

```
<Directory "/var/www/icons">
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

这些权限使用户可以读取目录内容, 除非有index.html之类的DirectoryIndex文件和通过MultiViews支持不同语言之类的内容协商

如果安装了httpd-manual * RPM包, 要在Web站点中包括Apache手册, 则可能将下列默认Alias指令:

```
Alias /manual "/var/www/manual"
```

改为

```
Alias /etc/httpd/manual "/var/www/manual"
```

这里假设ServerRoot指令设置成/etc/httpd。下列语句设置指令目录的权限, 包括Web分布式写作与版本(WebDAV)数据库:

```
<Directory "/var/www/manual">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

<IfModule mod_dav_fs.c>
    # Location of the WebDAV lock database.
    DAVLockDB /var/lib/dav/lockdb
</IfModule>
```

脚本

httpd.conf中的脚本指向通过Web服务器运行的程序。Apache通过ScriptAli指令在默认httpd.conf文件中启动, 这是针对脚本的特殊Alias:

```
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
```

有些脚本要求访问CGI监控程序，这是由Scriptsock指令定义的：

```
<IfModule mod_cgid.c>
    Scriptsock    run/httpd.cgid
</IfModule>
```

这里可以定义与Web站点相关的脚本的权限：

```
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
```

注意这些权限不允许使用.htaccess文件，但支持所有用户执行脚本。

如果改变Web站点名称，则要改向用户。例如，下列默认Redirect指令让导航到/bears目录的用户改向到www.mommabears.com：

```
# Redirect permanent /bears http://www.mommabears.com
```

目录列表

有时要显示一个目录中的文件。例如，图30.2显示了/home/mike/public_html目录中的文件，基于前面“用户目录权限”一节指定的UserDir指令。

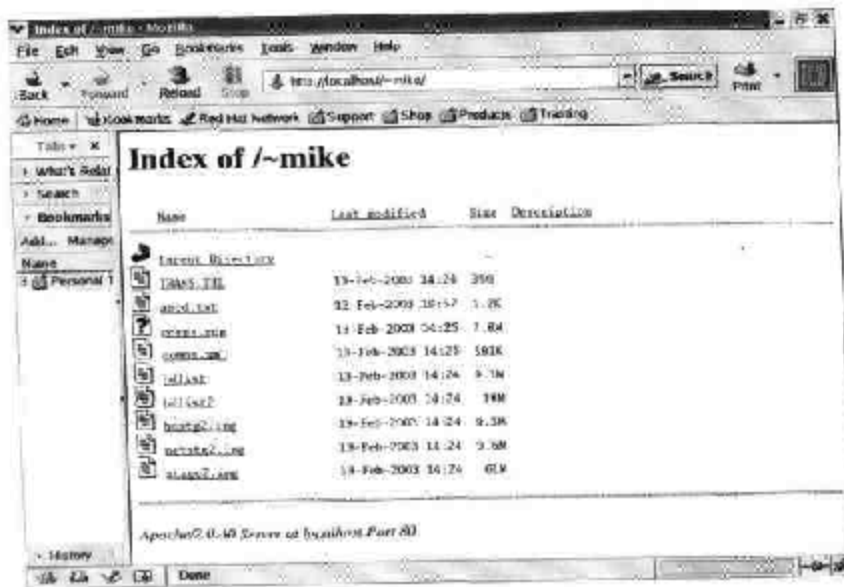


图30.2 浏览主目录文件

IndexOptions指令确定客户机在Web浏览器中是如何显示索引文件的。例如，默认IndexOptions指令如下：

```
IndexOptions FancyIndexing VersionSort NameWidth=*
```

配置三个项目：**FancyIndexing**表示图标和文件的大小，**VersionSort**表示按特定顺序排序RPM

版本之类的数字，**NameWidth**表示目录中文件名所需的宽度。

目标

不同文件类型和扩展名有一列图标，这些图标在文件清单中列出，只要按上节的方法设置**IndexOptions FancyIndexing**即可。有三个基本**AddIcon***指令：

```
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
```

AddIconByEncoding指令适用于压缩二进制文件，四种不同类型文件使用如下的**AddIconBy-Encoding**指令：

```
AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*
```

最后，还有一系列**AddIcon**指令，将特定图标与不同的文件扩展名相联系：

```
AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/largefile.gif
AddIcon /icons/unknown.gif .wrl .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
AddIcon /icons/a.gif .ps .ai .eps
AddIcon /icons/layout.gif .html .shtml .htm .pdf
AddIcon /icons/text.gif .txt
AddIcon /icons/c.gif .c
AddIcon /icons/p.gif .pl .py
AddIcon /icons/f.gif .for
AddIcon /icons/dvi.gif .dvi
AddIcon /icons/uuencoded.gif .uu
AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
AddIcon /icons/tex.gif .tex
AddIcon /icons/bomb.gif core
AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^
```

这些**AddIcon**指令很简单。例如，如果Apache看到扩展名为.exe的文件，则会增加/icons/binary.gif图标作为这个文件的标志。但这个清单并不完整，还有**DefaultIcon**指令，用于未知扩展名的文件：

```
DefaultIcon /icons/unknown.gif
```

如果你喜欢，也可以激活下列**AddDescription**指令，让用户得到特定扩展名文件的更多信息：

```
#AddDescription "GZIP compressed document" .gz
#AddDescription "tar archive" .tar
#AddDescription "GZIP compressed tar archive" .tgz
```

可以对不同的HTML文件建立目录。例如，HeaderName指令指定文件清单前面要列出的文件，ReadmeName指令指定文件清单后面要列出的文件。

```
ReadmeName README.html
HeaderName HEADER.html
```

IndexIgnore指令将Apache设置为避免列出任何目录表中的指定文件。注意默认值包括HEADER.html与README.html文件。

```
IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
```

解压缩

有些浏览器可以读取和自动解压缩Web站点目录中的某些文件。只要用AddEncoding指令指定与某个文件扩展名相关的编辑方式即可：

```
AddEncoding x-compress Z
AddEncoding x-gzip gz tgz
```

语言

多语种Web站点包括多种语言的Web页面。DefaultLanguage指令定义与没有标志的所有Web页面相关的语言。下列非活动指令指定德语：

```
# DefaultLanguage nl
```

可以用AddLanguage指令将Web页面设置为不同语言。例如，index.html.cz是与捷克语相关的Web页面：

```
AddLanguage cz .cz
```

表30.8列出了其他语言代码。

表30.8 语言代码

代码	语言	代码	语言
ca	加泰罗尼亚语	kr	朝鲜语
cz	捷克语	ltz	卢森堡语
da	丹麦语	nl	荷兰语
de	德语	nn	挪威尼诺斯克语
en	英语	no	挪威语
el	现代希腊语	pl	波兰语
es	西班牙语	pt	葡萄牙语
et	爱沙尼亚语	pt-br	巴西葡萄牙语
fr	法语	ru	俄语
he	希伯来语	sv	瑞典语
hr	匈牙利语	tw	中文简体
it	意大利语	zh-tw	中文繁体
ja	日语		

目前，Apache的开发者正在把所有中文AddLanguage的代码改成zh。

Web浏览器要向Web服务器指定优选语言，但如果没有用，则可以用LanguagePriority指定的优选语言：

LanguagePriority en da nl et fr de el it ja kr no pl pt pt-br ltz ca es sv tw
它和ForceLanguagePriority指令一起使用。根据默认httpd.conf文件的定义，它用LanguagePriority指令表选择客户端Web浏览器能接受的语言。如果没有能接受的语言的页面，则使用LanguagePriority表中第一个项目（这里是英语）。

许多语言要求提供正确的字符集。大多数语言字符组织成不同的ISO字符集。默认为ISO-8859-1，适用于英语和其他类似语言。它用下列指令强制为Apache的默认Web站点：

```
AddDefaultCharset ISO-8859-1
```

还有另外几个字符集，可用下列AddCharset指令定义。关于这些字符集的更多信息，见www.iana.org/assignments/character-sets。

```
AddCharset ISO-8859-1 .iso8859-1 .latin1
AddCharset ISO-8859-2 .iso8859-2 .latin2 .cen
AddCharset ISO-8859-3 .iso8859-3 .latin3
AddCharset ISO-8859-4 .iso8859-4 .latin4
AddCharset ISO-8859-5 .iso8859-5 .latin5 .cyrl .iso-cyrl
AddCharset ISO-8859-6 .iso8859-6 .latin6 .arab
AddCharset ISO-8859-7 .iso8859-7 .latin7 .grk
AddCharset ISO-8859-8 .iso8859-8 .latin8 .heb
AddCharset ISO-8859-9 .iso8859-9 .latin9 .trk
AddCharset ISO-2022-JP .iso2022-jp .jis
AddCharset ISO-2022-KR .iso2022-kr .kis
AddCharset ISO-2022-CN .iso2022-cn .cis
AddCharset Big5 .Big5 .big5
# For Russian, more than one charset is used (depends on client, mostly):
AddCharset WINDOWS-1251 .cp-1251 .win-1251
AddCharset CP866 .cp866
AddCharset KOI8-r .koi8-r .koi8-ru
AddCharset KOI8-ru .koi8-uk .ua
AddCharset ISO-10646-UCS-2 .ucs2
AddCharset ISO-10646-UCS-4 .ucs4
AddCharset UTF-8 .utf8
AddCharset GB2312 .gb2312 .gb
AddCharset utf-7 .utf7
AddCharset utf-8 .utf8
AddCharset big5 .big5 .b5
AddCharset EUC-TW .euc-tw
AddCharset EUC-JP .euc-jp
AddCharset EUC-KR .euc-kr
AddCharset shift_jis .sjis
```

映射处理器

可以将文件扩展名映射为特定的处理器。例如，下列标为说明的命令行用AddHandler指令对扩展名为.cgi的文件激活CGI脚本处理，假设subject目录已经设置了Options ExecCGI指令：

```
#AddHandler cgi-script .cgi
```

下列标为说明的指令保证不处理已经有HTTP头的文件：

```
#AddHandler send-as-is asis
```

要激活标为说明的指令，用文本编辑器删除httpd.conf文件中的#号。

这个指令处理图形映射文件：

```
AddHandler imap-file map
```

最后，这个指令支持.var文件，寻找Web浏览器客户机指定的语言：

```
AddHandler type-map var
```

部分过程包括输出过滤。例如，下列AddOutputFilter指令寻找带.shtml扩展名的Web页面中的SSI（服务器方包括）。

错误消息

在Web服务器上遇到错误时，可以得到与特定Web页面相关的消息。图30.3显示的错误消息与HTML 404错误码相关，也称为file not found错误。



图30.3 HTML 404错误码

默认错误目录为/var/www/error。下列Alias指令将错误目录与这些文件相联系：

```
Alias /error/ "/var/www/error/"
```

下列模块对/var/www/error/目录中的Web页面提供内容协商和SSI：

```
<IfModule mod_negotiation.c>
<IfModule mod_include.c>
```

下列/var/www/error/目录权限依次设置英语、西班牙语、德语和法语的错误消息。可以从本章前面“目录索引”一节看到更多的指令。

```
<Directory "/var/www/error">
    AllowOverride None
    Options IncludesNoExec
    AddOutputFilter Includes html
    AddHandler type-map var
    Order allow,deny
    Allow from all
    LanguagePriority en es de fr
    ForceLanguagePriority Prefer Fallback
</Directory>
```

这些指令与HTML错误码一起使用。用户看到的页面取决于下列ErrorDocument指令定义的错误码和Web页面：

```
ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
ErrorDocument 408 /error/HTTP_REQUEST_TIMEOUT.html.var
ErrorDocument 410 /error/HTTP_GONE.html.var
ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
ErrorDocument 415 /error/HTTP_SERVICE_UNAVAILABLE.html.var
ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var
```

浏览器定制

Web浏览器请求Web页面时，告诉Apache它是何种Web浏览器。BrowserMatch指令可以定制不同Web浏览器的响应：

```
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
```

前两个命令对老式Web浏览器产生特殊响应：Mozilla/2对应于Netscape 2.x，MSIE 4.0b2对应于Microsoft Internet Explorer 4.x。这些Web浏览器不符合当前的HTTP 1.1标准。后面三个命令强制指定Web浏览器提供HTTP 1.0级的响应。

Microsoft Web Folders中存在特殊问题，它不能正确处理WebDAV数据库。这个问题用下列BrowserMatch指令解决：

```
BrowserMatch "Microsoft Data Access Internet PublishingProvider"
➡ redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
```

服务器报告

可以用各种服务器报告发送Apache服务器中状态与配置信息的报告。例如，下列命令段激活时，可以提供Apache当前状态的报告：

```
#<Location /server-status>
#   SetHandler server-status
#   Order deny,allow
#   Deny from all
#   Allow from .your-domain.com
#</Location>
```

需要用下列命令激活它，否则Deny from all命令会阻止发往http://servername/server-status地址的所有通信流，这里，我的局域网在192.168.13.0/24网络上：

```
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from 192.168.13.0/24
</Location>
```

可以通过图30.4所示另一Web浏览器在局域网的另一台计算机上看到结果。

正确激活下列命令时，可以得到Apache配置的类似报告：

```
#<Location /server-info>
#   SetHandler server-info
#   Order deny,allow
#   Deny from all
#   Allow from .your-domain.com
#</Location>
```

这些命令从默认httpd.conf文件定向，记住要像上一段一样设置Allow from your_network_address。这时可以远程看到结果，如图30.5。

代理服务器

Apache有自己的代理服务器。可以将Apache设置成在本地网络上缓存并提供请求的Web页面。基本命令如下，我将其稍作改变，将代理服务器用于网址为192.168.13.0/24的局域网：

```
#<IfModule mod_proxy.c>
#ProxyRequests On
#
#<Proxy *>
#    Order deny,allow
#    Deny from all
#    Allow from 192.168.13.0/24
#</Proxy>
```

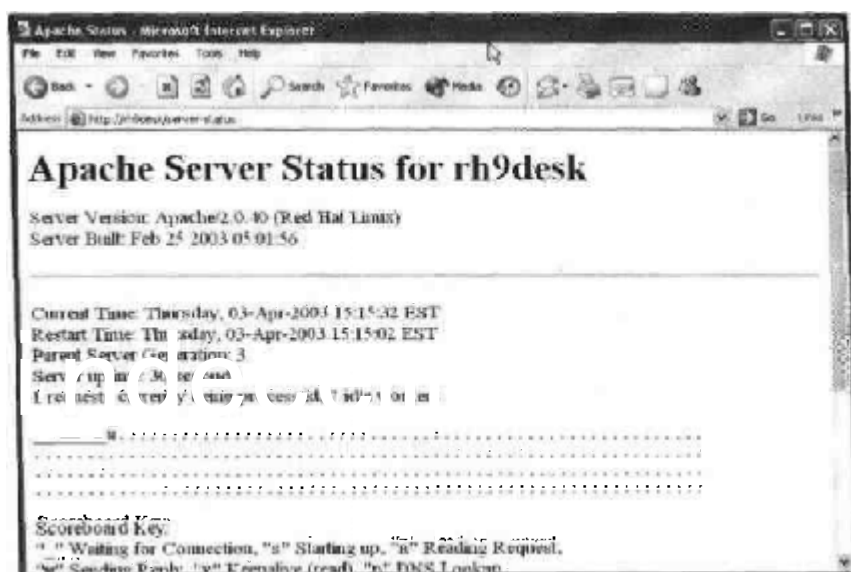


图30.4 远程检查服务器状态



图30-5 远程检查服务器配置

如果有多个代理服务器，则要激活下列ProxyVia指令，可以用HTTP 1.1搜索代理服务链：

```
#ProxyVia On
```

如果不配置缓冲区，则代理服务器没什么用。表30.9列出了与缓冲区相关的一系列特殊指令。如果设置代理服务器，则可能要改变其中一些设置。例如，可能要让CacheSize大于5KB：

```
#CacheRoot "/etc/httpd/proxy"
#CacheSize 5
#CacheGcInterval 4
#CacheMaxExpire 24
#CacheLastModifiedFactor 0.1
#CacheDefaultExpire 1
#NoCache a-domain.com another-domain.edu joes.garage-sale.com
```

表30.9 Apache缓冲区相关指令

指令	说明
CacheMaxExpire	设置缓存的最长时间（秒数）
CacheGcInterval	配置从缓冲区清除旧数据的时间间隔（小时）
CacheLastModifiedFactor	设置缓冲区中文件的有效期。如果没有与Web页面相关的有效期和时间，则Apache相对于上次改变页面的时间进行设置
CacheMaxExpire	选择缓存文档的最长时间（秒数）
CacheRoot	配置代理服务器缓存的默认目录
CacheSize	设置缓冲区长度（KB）

虚拟主机

Apache 2.0.x的一大优势是它能够在—个IP地址上设置多个Web站点，这个特性称为虚拟主机。

旧版Apache只支持基于IP的虚拟主机，要求通过Apache服务器配置的每个Web站点使用不同的IP地址。而Apache 2.0.x支持基于名称的虚拟主机。

按照这个模式，DNS服务器将多个域名（如www.mommabears.com与www.sybex.com）映射同一IP地址（如10.111.123.45）。可以将httpd.conf设置成识别不同域名和提供相应的Web站点。

说明：不能总是使用基于名称的模式。如果需要Web站点的安全（SSL）部分，则不能用基于名称的模式，如电子商务站点。旧式客户机也会遇到这类问题，如Netscape 2.0与Internet Explorer 4.0浏览器。这些浏览器无法处理与当前HTTP 1.1标准相关的大量信息。

下列代码显示了如何配置两个虚拟主机www.sybex.com与www.mommabears.com：

```
NameVirtualHost *
```


这个NameVirtualHost指令监听本地计算机上所有IP地址的请求。也可以将本节的*换成实际的IP地址：

```
<VirtualHost *>
    ServerAdmin webmaster@sybex.com
    DocumentRoot /www/site1/sybex.com
    ServerName sybex.com
    ErrorLog logs/sybex.com-error_log
    CustomLog logs/sybex.com-access_log common
</VirtualHost>
```

www.sybex.com <Virtual Host *>容器中的指令覆盖了前面在httpd.conf文件中建立的任何设置。可以增加所要指令，定制每个虚拟主机：

```
<VirtualHost *>
    ServerAdmin webmaster@mommabears.com
    DocumentRoot /www/site2/mommabears.com
    ServerName mommabears.com
    ErrorLog logs/mommabears.com-error_log
    CustomLog logs/mommabears.com-access_log common
</VirtualHost>
```

可以看出，mommabears.com Web站点的设置也差不多，别忘了相对目录依赖于ServerRoot指令。

定制Apache模块

/etc/httpd/conf.d目录中有几个ServerRoot模块特定的配置文件，可以通过前面“包”一节介绍的模块RPM包安装。它们按照主httpd.conf文件中的Include conf.d/*.conf指令指定，放在基于Apache的配置中。表30.10列出了这些ServerRoot模块的配置文件。

表30.10 ServerRoot模块的配置文件

文件	描述
auth_mysql.conf	支持访问MySQL数据库，这个文件的默认版本包括各种验证命令
auth_pgsql.conf	支持访问PostgreSQL数据库，这个文件的默认版本包括各种验证命令
perl.conf	集成Perl解释器，支持使用Perl命令和脚本
php.conf	集成PHP脚本语言解释器
python.conf	集成Python脚本语言解释器，支持使用Python命令和脚本
ssl.conf	增加SSL（安全套接层）支持，默认使用TCP/IP端口，包括几个证书与加密方法的指令

Apache查错

如果无法连接Apache Web服务器中配置的Web站点，则可以检查如下几个地方。首先要检查网络。任何网络中最常见的问题是物理问题，例如电缆和接头。然后用ping之类的命令检查连接，详见第21章。

检查基本操作

保证网络正常之后，下一步看看Apache是否运行。用下列命令启动：

```
# service httpd status
```

应该出现如下消息：

```
httpd (pid 3464 3463 3462 3461 3460 3459 3458) is running
```

表示有几个Apache (httpd) 监控程序正在运行，个数取决于StartServers之类的httpd.conf指令。如果遇到问题，则会出现三个常见的消息：

```
httpd is stopped
```

解决这个问题很简单。试使用`service httpd start`命令。更新运行`service httpd status`命令，可能看到如下消息：

```
httpd is dead but pid file exists
```

本例中，Apache无法启动，部分原因是/var/run目录中的httpd.pid文件有问题。可能是发生电源故障（假设没有不间断的电源）之后Linux没有删除httpd.pid文件。试删除httpd.pid文件，然后运行`service httpd start`命令。更新运行`service httpd status`命令，可能看到如下消息：

```
httpd dead but subsys locked
```

这告诉我们出现了另外的一些问题，此时需要检查日志文件。

检查日志文件

Apache日志文件的默认地址在httpd.conf中定义为/etc/httpd/logs，但这个目录链接更标准的日志文件地址/var/log/httpd。记住，可以用虚拟主机容器中的CustomLog指令将日志文件放到不同的地址。

从这个目录中的日志文件寻找线索，本书不准备介绍这里出现的不同错误，但许多日志项目是一目了然的。

检查语法

Apache Web服务器有自己的语法检查器。下列命令检查主配置文件httpd.conf中的语法。如果遇到问题，则下列命令：

```
# httpd -t
```

可以标识问题所在的行，如拼写错误的指令。下列命令在调试方式中启动Apache，可以找出其他问题：

```
# httpd -X
```

检查防火墙

有时消息根本无法到达Web服务器，可能是忘了在防火墙中让消息通过标准HTTP端口80。运行`iptables -L`命令，列出当前的防火墙规则。第22章详细介绍了这个命令。

第3章、第4章和第19章介绍不同防火墙实用程序时曾介绍过，可以将防火墙设置成自动允许数据通过HTTP端口。记住，如果还提供安全Web页面，则要打开相关端口。对于HTTPS，端口为443。`httpd.conf`中定义了标准的TCP/IP端口号。

配置Red Hat GUI Apache实用程序

红帽子公司开发了配置Apache的GUI工具，可以用`redhat-config-httpd` command命令启动。首次打开这个GUI工具时，可以看到Apache配置窗口，如图30.6。



图30.6 红帽子GUI Apache实用程序

可以看出，这个实用程序有四个标签，见下面几节介绍。完成改变前单击OK按钮，这些改变将写入`httpd.conf`文件中，覆盖前面用文本编辑器完成的任何改变。

说明：到本书编写时，`redhat-config-httpd`还在开发之中。使用这个实用程序之前，我首先备份了当前`httpd.conf`文件。作出改变之后，我先用`httpd -t`命令测试`httpd.conf`的语法。我在文本编辑器中打开`httpd.conf`文件，分析发生的改变。然后，使用`redhat-config-httpd`工具是进一步学习Apache配置的好办法。

设置主Apache参数

Apache的基本设置很简单，可以在Apache配置窗口Main标签里配置三个指令：

- **Server Name**文本框对应于`ServerName`指令，设置Apache服务器的主站点名。要使用这个实用程序，就要在这个文本框中输入服务器名或地址。如果配置虚拟主机，则不要在这个文本框中输入这些域名。最好输入服务器的IP地址，避免连接网络的DNS服务器上不必要的通信流。
- **Webmaster Email Address**文本框对应于`ServerAdmin`指令，自动生成的Web页面列出的默认电子邮件地址。图30.6显示了默认设置`root@localhost`。

- Available Addresses框设置Apache监控请求的TCP/IP端口，使用Listen指令。端口80是标准HTTP TCP/IP端口，Apache通常监听Internet上所有地址的请求，命令为Allow from all。

可以限制允许访问你的Web站点的计算机范围。加亮显示Addresses On Port 80并单击Edit按钮，打开地址编辑窗口，如图30.7。

例如，图30.7显示限制计算机上IP地址为192.168.13.64的网络适配器访问。其将httpd.conf文件中的Listen指令变为如下：

```
Listen 192.168.13.64:80
```

如果要配置其他服务，如安全Web页面（HTTPS），则单击Add按钮打开Add New Address窗口，与图30.7大致相同。然后可以输入所要网卡的IP地址和与HTTPS相关联的TCP/IP端口443。完成所要的改变之后，单击Virtual Hosts标签。

配置虚拟主机

然后可以在Apache中配置虚拟主机。如果还没有启动redhat-config-httpd实用程序，则要启动redhat-config-httpd实用程序并单击Virtual Hosts标签，默认视图如图30.8。



图30.7 限制允许访问Web站点的计算机

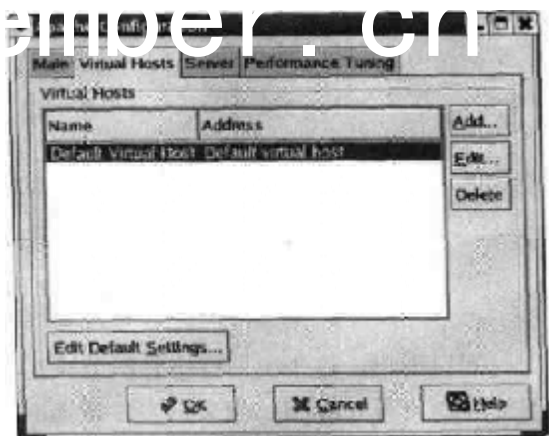


图30.8 配置虚拟主机

Default Virtual Host设置与默认Edit或httpd.conf文件相关联。如果要了解更多默认设置，可以单击Edit Default Settings并分析属性窗口。但我们主要关心对实际Web站点生成虚拟主机，因此单击Add按钮打开Virtual Host Properties窗口，如图30.9。

可以看出，Virtual Host Properties窗口有六个部分：General Options、Site Configuration、SSL、Logging、Environment Variables与Directories。

General Options

每个虚拟主机都有General Options，如图30.9。在这个图中，我们对Web站点mywebsite.abc填入了一些基本的参数。

前面曾介绍过，可以在一个IP地址上用基于IP的虚拟主机设置建立多个虚拟主机。而基于名称的虚拟主机则通过Apache服务器配置的每个Web站点需要一个IP地址。

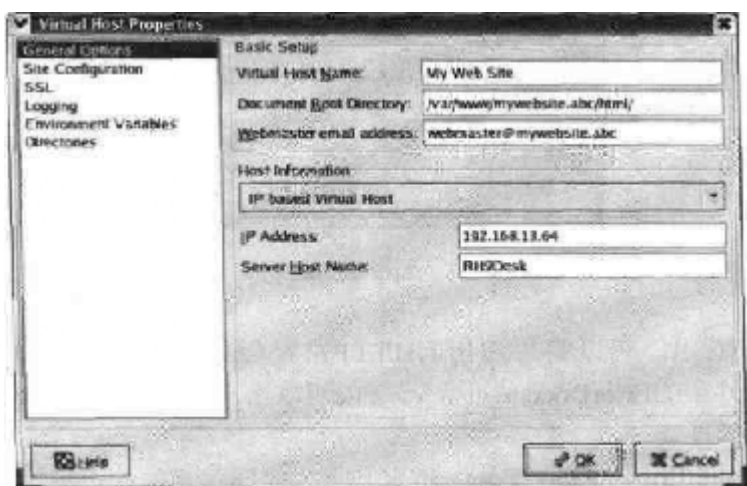


图30.9 配置虚拟主机属性窗口

Site Configuration

然后选择窗口左边的Site Configuration选项打开一系列目录页和错误文件的设置，如图30.10。

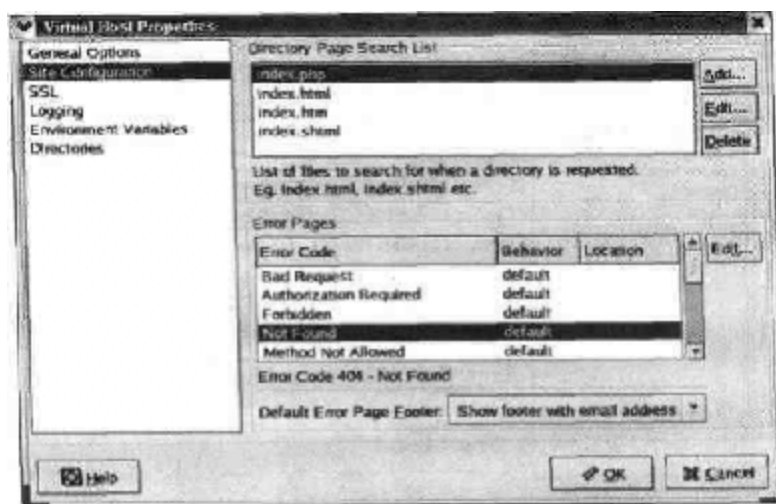


图30.10 站点设置

用户寻找你的Web站点时，进入与DocumentRoot指令相关联的目录，如图30.9所示，这里是/var/www/mywebsite.abc/html目录。其寻找Directory Page Search列表框中的下列文件名之一：index.php、index.html、index.htm和index.shtml。

窗口底部的错误页显示Apache对各种HTTP错误的响应。例如，加亮显示的错误“file not found”与HTTP错误码404相关。默认行为指向ApacheConf.py文件中的ErrorDocument指令。如果需要特殊错误页，则可以对特定虚拟主机生成特殊的ErrorDocument指令。为此，加亮显示所选错误码并单击Edit按钮，打开ApacheConf.py窗口，如图30.11。



图30.11 ApacheConf.py窗口

从图中可以看出，可以将用户指向HTTP错误码404相关的三个方向：默认为指向ApacheConf.py文件中的ErrorDocument指令，File可以指定所选的Web页面，URL可以设置指向联机错误消息的地址。

最后，Default Error Page Footer指定与每个错误页相关的页脚信息。标准页脚基于/var/www/error/include目录中的bottom.html文件。可以不显示页脚，也可以带或不带电子邮件地址。

SSL

然后选择窗口左边的SSL选项卡并打开一系列与安全套接层相关的选项（如图30.12）。安装mod_ssl-* RPM时，得到/etc/httpd/conf目录中的一系列保密钥，如图30.12所示。

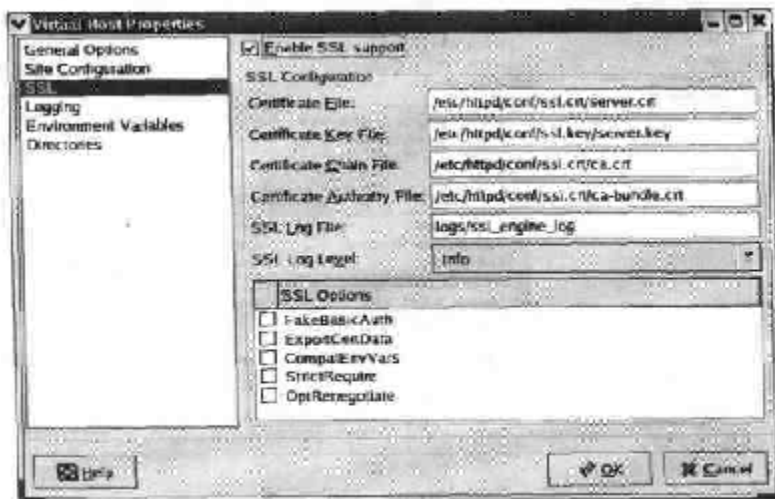


图30.12 安全套接层相关的选项

如果真要运行安全Web服务器，则要从VeriSign (www.verisign.com)与Thawte (www.thawte.com)之类的证书机构(CA)取得一组真实的证书数据。我们在“生成安全密钥”中简要介绍了设置安全服务器的一般方法，但其细节太复杂，超出了本书范围，详见<http://httpd.apache.org>、www.apache-ssl.org和“Linux Apache Web Server Administration”（第二版，Sybex公司，2002年出版）。

这里所作的改变将写入/etc/httpd/conf.d目录中的ssl.conf文件。

生成安全密钥

这里简要介绍对Apache设置安全服务器的一般方法。假设安装了相应RPM包，则步骤如下：

1. 用下列命令删除基本服务器密钥：

```
# rm /etc/httpd/conf/ssl.key/server.key
# rm /etc/httpd/conf/ssl.crt/server.crt
```

2. 转移到/usr/share/ssl/certs目录：

```
# cd /usr/share/ssl/certs
```

3. 然后生成安全密钥：

```
# make genkey
```

程序两次提示输入特殊口令，这个口令是大小写相关的，保存的密钥保护Web服务器上的信息。

4. 然后可以用下列命令建立向证书机构（CA）的请求：

```
# make genkey
```

程序提示输入口令和服务管理信息。完成之后，这个命令生成下列命令，可以在向证书机构（CA）的请求中发送：

```
/etc/httpd/conf/ssl.csr/server.csr
```

5. 证书机构（CA）响应一个文件，可以保存为/etc/httpd/conf/ssl.crt目录中的server.crt文件。

可以在第4步运行make testcert命令，建立用于测试的非正式证书。

下次启动Apache时，它提示输入口令。如果输入不正确，则Apache无法启动。

Logging

然后选择窗口左边的Logging选项打开一系列与日志和日志文件相关的选项，如图30.13。

图中显示了默认的日志文件，路径相对于ServerRoot指令，通常是normally/etc/httpd。自然，可能要在与虚拟主机相关联的特殊目录中指定日志文件，如mywebsite.abc/logs/access_log。

可以在Custom Log String文本框中指定要放进这个日志文件的信息。这里的信息与本章前面介绍的LogFormat指令相关联。

Log Level下拉列表中的选项与前面Log Level指令中的选项匹配：Emergency、Alert、Critical、Error、Warn、Notice、Info和Debug。

可能要保证Reverse DNS Lookup设置为No Reverse Lookup。除非与DNS服务器有可靠的快速连接，否则寻找与IP地址相关联的完全限定域名会影响Web服务器的性能。

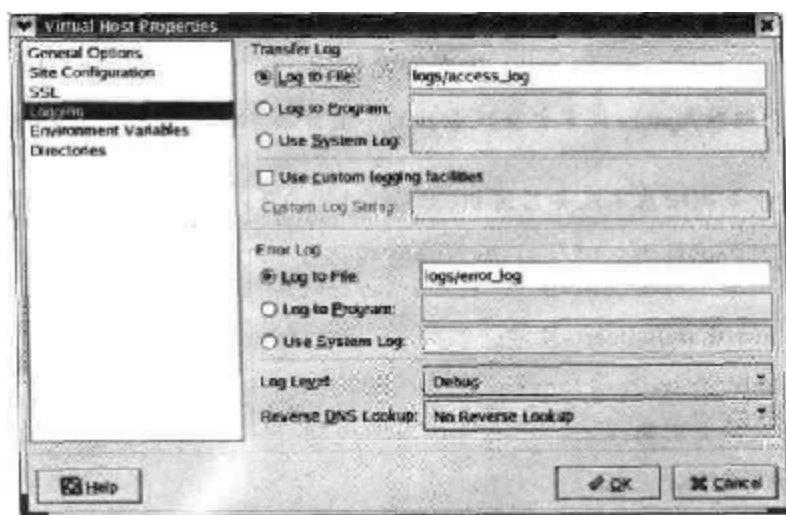


图30.13 虚拟主机日志

Environment Variables

然后选择窗口左边的 **Environment Variables** 选项打开一些设置，可以设置与CGI或SSI脚本相关联的环境变量，如图30.14。

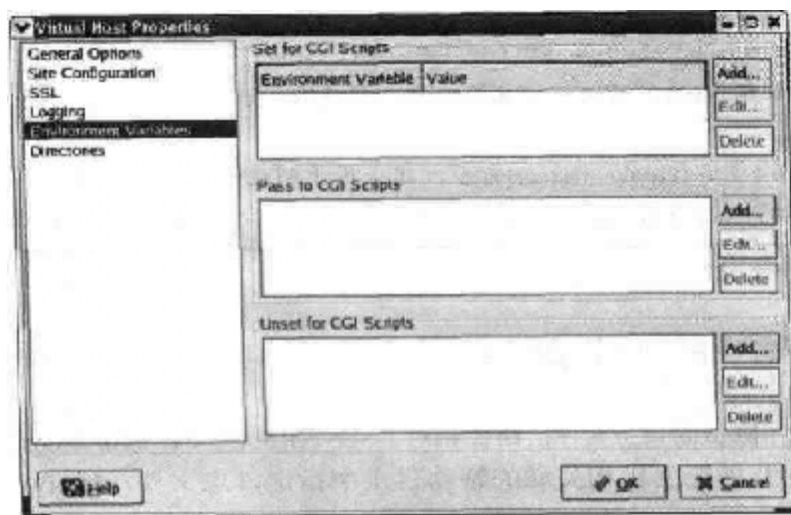


图30.14 环境变量

原理上与shell中的普通环境变量相同，但这里的设置只与CGI或SSI脚本相关。

Directory Options

最后选择窗口左边的 **Directories** 选项打开一组设置，可以设置不同目录的选项指令，如图30.15。



图30.15 目录选项

图30.15显示了默认目录的选项ExecCGI、FollowSymLinks、Includes、IncludesNOEXEC、Indexes与SymLinuxIfOwnerMatch（见表30.5）。要编辑默认设置，单击窗口右上角的Edit按钮。

还可以指定其他目录的选项。单击Add按钮打开目录选项窗口，如图30.16。表30.11列出了目录选项窗口的选项。

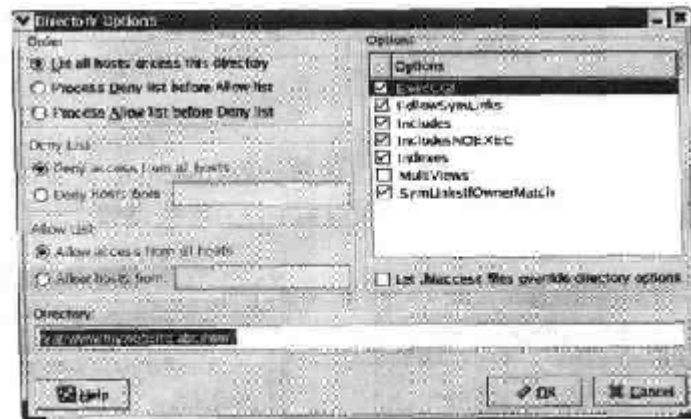


图30.16 目录选项窗口

表30.11 目录选项窗口的选项

选择	描述
Order	设置指令顺序，选项包括Allow from all Order deny, allow或Order allow, deny
Deny List	如果不允许所有主机，则可以按域名或IP地址向一些或所有主机拒绝对这个目录的访问
Allow List	如果不允许所有主机，则可以按域名或IP地址向一些或所有主机允许对这个目录的访问

(续表)

选择	描述
Directory	指定Options指令适用的目录
Options	与Options指令相关联设置
.htaccess	如果激活这个设置，则AllowOverride指令加进这个目录中

配置服务器

每个Apache服务器都有一些基本设置。回到Apache配置窗口并单击Server标签，出现30.17所示的信息，表30.12总结了这些设置。

表30.12 Apache配置服务器设置

设置	说明
Lock File	Apache启动时打开的文件
PID File	Apache启动时打开的另一文件，包括与打开httpd进程程序相关联的PID
Core Dump Directory	当核心转储发生时，用于调试。要让与Apache服务器相关联的用户写入，通常是apache
User	与Apache服务器相关联的用户名
Group	与Apache服务器相关联的组名

性能调整

每个Apache服务器都有几个基本的性能设置。在Apache配置窗口中，单击Performance Tuning标签，出现图30.18所示的信息，表30.13总结了这些设置。

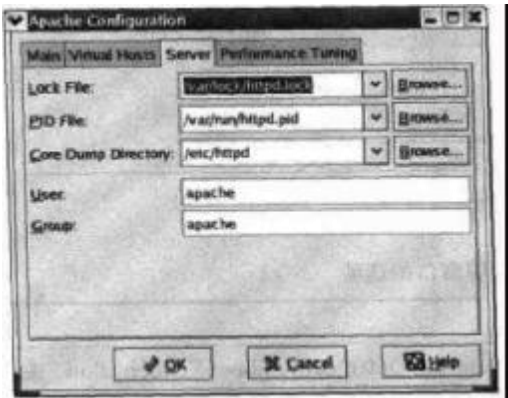


图30.17 Apache配置服务器设置

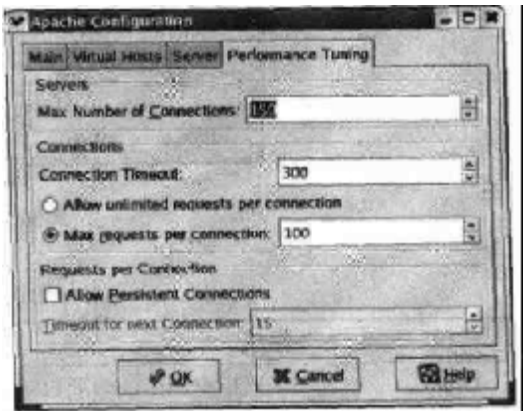


图30.18 Apache性能调整设置

表30.13 Apache性能调整设置

设置	说明
Max Number Of Connections	对应于可以同时连接Web服务器的最大客户数，设置MaxClients指令
Connection Timeout	设置Web服务器等待客户浏览器进一步通信的时间（秒数），设置TimeOut指令
Requests Per Connection	限制每个连接浏览器请求的项目数，设置MaxRequestsPerChild指令
Allow Persistent Connections	保持打开浏览器连接，独立于超时，选择时设置KeepAlive指令为真
Timeout For Next Connection	KeepAlive为真时设置Apache等待客户机下一个请求的时间，设置KeepAliveTimeout指令

集成Red Hat Content Accelerator

Red Hat Content Accelerator是另一种Web服务器。原名为TUX，可以迅速管理静态Web内容。因为它的位置直接内嵌在Linux内核中。尽管这个工具也可以管理动态Web页面，但红帽子公司建议用Red Hat Content Accelerator管理静态Web内容，用Apache管理动态Web页面。

这个工具还在开发中，因为TUX与Apache一起使用时要求它们装入同一台计算机，这对大型Web站点不太方便，因为其通常要求多个服务器，这些服务器可能在不同的地点工作。由于Red Hat Content Accelerator的包名还是TUX，因此本节互换使用这两个术语。

说明：TUX表示线程化Linux Web服务器，顺便说一句，它也是Linux吉祥物企鹅的名字。

安装与启动TUX

通常，Red Hat Content Accelerator (TUX) 与Apache不能同时运行，因此，要看看计算机上能否使用TUX，就要在停止Apache之后用下列步骤安装并启动TUX：

1. 在计算机上安装tux-* RPM包。
2. 在默认DOCROOT目录/var/www/html中建立index.html文件，本练习修改并复制/var/www/error/noindex.html，可以从图30.1看出。
3. 用service httpd stop命令停止Apache服务器。
4. 用service tux start命令启动TUX服务器。
5. 将所选浏览器中移到localhost。

结果如图30.19所示。

图中可以看到TUX从/var/www/html目录提供index.html页面。因此，Linux中的TUX已经在工作。下面几节简要介绍其工作机制。

说明：红帽子公司建议在另一RAID分区配置与TUX相关的DOCROOT，对应于Apache中的DocumentRoot指令。RAID分区配置的细节见第14章介绍。

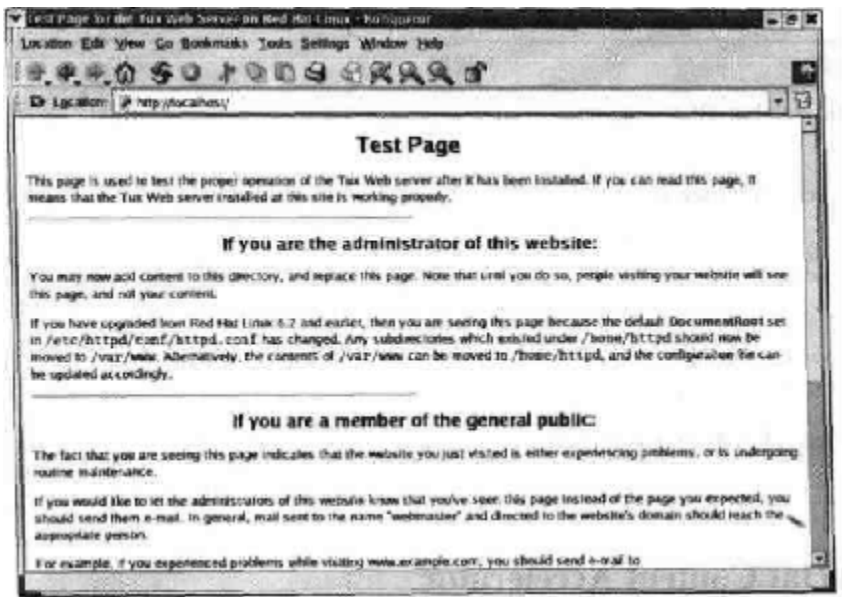


图30.19 TUX在工作

配置Red Hat Content Accelerator

由于Rad Hat Content Accelerator的配置在内核中，因此默认设置不在标准配置文件中，而位于/etc/sysconfig/tux中。这个文件中有一些参数，见表30.14。

TUX还有一系列日志文件，位于文件/var/log/tux中。但是，这些日志文件压缩成二进制格式。要阅读这些日志文件，就要用tux2w3c命令。图30.20显示了一个结果：网络中有两个连接，一个来自本地计算机127.0.0.1，一个来自IP地址为10.252.113.122的计算机。

表30.14 TUX配置参数

参数	描述
TUXTHREADS	定义允许的内核线程数，但不要超过计算机上的CPU个数
DOCROOT	设置请求Web服务器的顶层目录，对应于DocumentRoot指令。浏览器可以在这个目录中找到index.html之类的主页文件。标准位置为/var/www/html
LOGFILE	指定TUX日志文件地址，通常为/var/log/tux
DAEMON_UID	指定与TUX相关的用户ID，默认为nobody
DAEMON_GID	指定与TUX相关的组ID，默认为nobody
CGIROOT	必要时定义CGI脚本的目录
MAX_KEEPALIVE_TIMEOUT	设置遇到网络故障时的连接超时值
TUXMODULES	定义动态TUX数据模块
MODULEPATH	设置Content Accelerator应用程序的接口模块目录

```
[root@RH9Desk root]# tux2w3c /var/log/tux
127.0.0.1 - - [03/Apr/2003:16:08:08 -0500] "GET / HTTP/1.0" 200 2898 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:48 -0500] "GET / HTTP/1.1" 200 2898 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:48 -0500] "GET /icons/apache_pb.gif HTTP/1.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:48 -0500] "GET /icons/powered_by.gif HTTP/1.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:55 -0500] "GET / HTTP/1.1" 304 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:55 -0500] "GET /icons/apache_pb.gif HTTP/1.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:55 -0500] "GET /icons/powered_by.gif HTTP/1.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:55 -0500] "GET / HTTP/1.1" 304 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:56 -0500] "GET /icons/apache_pb.gif HTTP/1.1" 404 0 "-" ""
10.252.113.122 - - [03/Apr/2003:16:09:56 -0500] "GET /icons/powered_by.gif HTTP/1.1" 404 0 "-" ""
[root@RH9Desk root]#
```

图30.20

组合TUX与Apache

可以让TUX与Apache同时运行，只要它们监听不同的TCP/IP端口。Apache httpd.conf文件中所需的改变很简单，只涉及两个指令。

Listen 指令告诉Apache要监听输入的计算机与端口，通常设置或监听标准HTTP端口，命令为Listen 80。如果在同一计算机上使用TUX，则要用这个命令让其本地监听：

```
Listen 127.0.0.1:8080
```

TUX用TUX内核设置目录/proc/sys/net/tux中的clientport设置寻找帮助，这个文件中的值已经设置为端口8080。

假设使用Apache虚拟主机，则要通过NameVirtualHost指令指定与Web服务器相关联的IP地址：

```
NameVirtualHost 192.168.13.64:80
```

对应于标准的TUX服务器端口，位于/proc/net/tux/0/listen/0文件中。这个文件中这个值应设置如下：

```
http://0.0.0.0:80
```

监听TCP/IP端口80上所有IP地址的请求。

进行这些改变之后，就可以让TUX与Apache同时运行。如果按前面介绍的命令停止了Apache，则可以用下列命令启动Apache：

```
service httpd start
```

小结

Linux是为网络建立的，在这个Internet时代，Linux操作系统可以在Web服务器上使用。可以在Linux中建立几种不同的Web服务器，包括Apache、TUX、AOLServer、BOA、Zeus等。

Apache是Internet最普及的Web服务器。Apache 2.0.x可以在同一Web服务器上用同一IP地址建立多个虚拟主机。

Apache的主配置文件httpd.conf很长，但并不复杂。我们对其中三个部分进行了分析：全局环境控制整个服务器的操作，主服务器参数是默认值，而虚拟主机部分可以配置硬件能够处理的多个Web站点。

红帽子公司建议用Rad Hat Content Accelerator管理静态Web内容。Content Accelerator原名TUX，速度很快，因为它直接内驻在Linux内核中。这两个Web服务很容易集成在一起。红帽子公司建议用TUX作为主Web服务器，Apache提供动态内容。

本书主体部分就到此结束了，但本书还有一个附录，介绍一些基本的Linux命令。

另外，Sybex公司Web站点还有五个附加章。Web上的第1章介绍主要Linux证书项目，Linux证书项目很多，CompTIA公司的Linux+考试针对初级Linux用户，只要六个月经验；SAIR与LPI考试针对中高级系统管理员，要两年以上经验。Web上的第3章介绍红帽子上机证书，是计算机产业中最难和最实用的考试之一。Web上的第2章列出Web上的联机资源，Web上的第4章介绍了GNU/Linux通用许可证（GPL），而Web上的第5章按组列出Red Hat Linux包，可以帮助配置Kickstart安装。这些内容可以到www.sybex.com站点搜索Mastering Red Hat Linux 9找到。

附录 Linux命令手册

本附录列出许多可以在命令行界面输入的命令。

大多数Linux命令已经有参考手册，如果要查，只要去查询即可。操作也很简单，使用ls这类的命令，你只要输入`man ls`即可打开这个命令的Linux参考手册。

但是，参考手册的格式是新Linux用户所不习惯的。Linux专家可能认为学习Linux参考手册的妙处对学习Linux有帮助，但参考手册读起来并不容易。本附录按功能列出几组重要目录，这些组与本书的大部分大致对应。

一个附录显然无法提供完整的清单，这方面的好书之一是Bryan Pfaffenberger的“Linux Command Instant Reference”。

例如，第一部分“安装Red Hat Linux”中有几个重要命令，可以帮助组织分区、生成引导盘和设置网络安装。本附录按本书不同部分的章节组织，以便你能找到所要的命令。

此外，还有一些Web上第1章与第2章中的命令是别的地方没有详细介绍的。本附录介绍了完成下列工作所需的命令：

- 安装Red Hat Linux
- Linux基础
- 基本Linux管理
- 管理X窗口
- Linux联网基础
- Linux网络服务
- Linux文件共享服务
- 其他命令

安装Red Hat Linux

安装Red Hat Linux的命令行命令很简单。由于Red Hat Linux通过图形界面安装，因此不需要太多文本命令。我们知道，可以不用任何文本命令安装Red Hat Linux，但如果需要文本命令，则其可能对安装至关重要。

安装命令分为四类：组织分区、生成引导盘，设置网络安装以及设置Kickstart安装。

准备硬盘

可以用第3章介绍的Disk Druid配置硬盘分区，但Disk Druid不能像fips一样分解现有分区，不能在完成Linux安装之后访问Disk Druid，而且它没有像fdisk一样的分区控制程度。另外，虽然parted很危险（立即发生改变），但它可以缩放分区。

划分分区

Linux的分区划分程序是fips, 这个工具只能在MS-DOS命令行界面中运行。第2章曾介绍过, 如果使用XP之前的Microsoft Windows操作系统, 则可以在MS-DOS方式中重新启动Microsoft Windows, 否则需要MS-DOS引导盘或Microsoft Windows 98之类的启动盘。

运行fips时, 步骤如下:

1. 将fips.exe复制到可引导软盘。
2. 在MS-DOS方式中重新启动计算机, 可以使用MS-DOS或Microsoft Windows 98启动盘。
3. 从DOS提示下运行fips.exe命令。最好从不同的物理盘中运行, 如软盘或红帽子安装光碟中。
4. fips命令读取硬盘上的分区, 选择出现的分区表中要划分的分区。
5. 指定要划分分区的柱面。
6. 检查并确认新分区表的改变。

生成新分区

划分的分区还需要赋值和格式化。为此可以在Red Hat Linux安装过程中使用Disk Druid, 也可以在Linux中随时使用fdisk。如果有多个硬盘, 需要指定硬盘设备。其用法如下:

```
# fdisk [-l] [-s partition] [device]
```

下面举几个例子:

fdisk -l 列出所有硬盘上的分区。

fdisk -s /dev/sda1 返回第一个SCSI硬盘中第一个分区长度。

fdisk /dev/hda 在第一个IDE硬盘上启动fdisk实用程序。

出现fdisk提示之后, 可以运行表A.1所示的命令。

表A.1 fdisk提示下的命令

命令	结果
a	设置或清除可引导标志, 至少要把前两个硬盘之一的一个主分区设置为可引导分区
b	编辑标签 (如果有BSD (伯克利标准发行版本) 分区)
c	切换DOS兼容性标志, 如果读分区时遇到问题, 则可以将其关掉, 但有时会在分区边界上造成问题
d	删除分区, 在实际删除分区之前, 要选择分区号
l	列出已知的分区类型, 共有100多种分区类型
m	显示可用的fdisk命令
n	配置新分区
p	列出当前分区表
q	退出fdisk而不保存改变
t	可以改变分区系统ID, 还要有分区号和基于已知分区类型的分区类型ID (可以用l命令找到)
u	在扇区与柱面之间切换显示的分区长度
v	验证当前分区表
w	写入改变并退出fdisk。执行这个命令之后才能将改变写入分区表

生成或缩放分区

parted命令是更灵活的GNU工具，但也更危险，与退出**fdisk**相似，但它还有更多功能。其语法很简单，下列命令打开第二个IDE硬盘进行编辑。如果不指定硬盘，则**parted**默认打开第一个硬盘：

```
# parted /dev/hdb
```

值得重述的是，这个命令很危险，一旦运行某个选项之后，就可能删除整个分区或整个硬盘的所有数据。此外，尽管可以用**parted**命令将硬盘分区格式化，但只能格式化为**ext2**格式。到本书编写时，还不能格式化为**ext3**格式。

出现**parted**提示时，可以运行表A.2的命令。

表A.2 parted提示下的命令

命令	结果
check <i>number</i>	对指定分区 <i>number</i> 进行文件系统检查。可以用 print 命令打开分区号清单
cp <i>device</i> <i>fr-number</i> <i>to-number</i>	将指定设备（如/dev/sda）上的文件系统从一个分区（ <i>fr-number</i> ）复制到另一分区（ <i>to-number</i> ）。到本书编写时，还不能复制选项
help	打印命令清单
mklabel <i>label</i>	用 bsd 、 loop 、 mac 与 msdos 之类的标量类型覆盖整个硬盘。这是个危险命令
mkfs <i>number</i> <i>format</i>	格式化指定分区，目前还不能格式化为 ext3
mkpart <i>type</i> <i>format</i> <i>start</i> <i>end</i>	生成指定格式的新分区， type 为主分区、逻辑分区或扩展分区， start 与 end 的单位为MB。到本书编写时，还不能使用格式选项
move <i>number</i> <i>start</i> <i>end</i>	将指定分区移到硬盘上的新位置， start 与 end 的单位为MB
print	显示当前分区列表
quit	退出 parted
resize <i>number</i> <i>start</i> <i>end</i>	缩放指定分区， start 与 end 的单位为MB
rm <i>number</i>	删除指定分区
select <i>device</i>	让 parted 指向不同的设备，如/dev/sda

准备引导盘

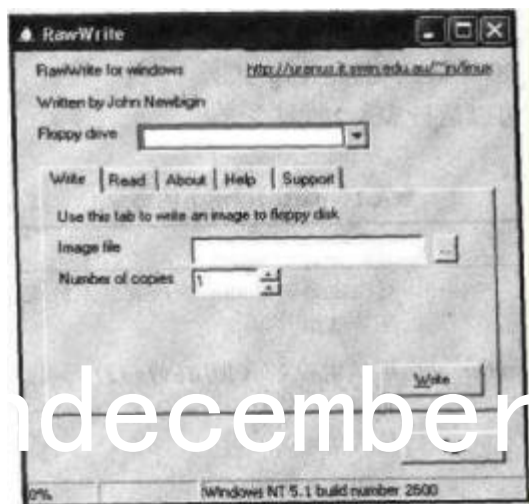
可以通过三个基本命令将Red Hat Linux映象文件的内容复制到软盘上。其中两个用于Linux系统，另外一个用于Microsoft操作系统。

在Microsoft操作系统中生成引导盘

rawrite命令可以将boot.img之类的映象文件内容复制到软盘上。标准方法是进入MS-DOS方式并运行**rawrite**命令。假设**rawrite**在D盘的dosutils子目录中，则**rawrite**命令会提示如下：

```
D:\> \dosutils\rawrite
Enter disk image source file name: d:\images\boot.img
Enter target diskette drive: a
Please insert a formatted diskette into drive A: and press -ENTER-:
```

另外，第一张Red Hat Linux安装光碟中的\dosutils\rawritewin\rawritewin.exe命令提供了具有同样功能的GUI，如图A.1所示的是RawWrite窗口。



图A.1 RawWrite窗口

在Linux中，可以用dd命令将boot.img之类的映象文件内容复制到软盘上。例如，下列命令将boot.img中的文件复制到系统中第一个软盘设备：

```
# dd if=/mnt/cdrom/images/bootdisk.img of=/dev/fd0
```

但是，Linux了解映象文件格式，因此可以用下列命令直接读取到软盘设备：

```
# cat /mnt/cdrom/images/bootdisk.img > /dev/fd0
```

设置网络服务器

可以用Red Hat Linux安装文件和包设置FTP、NFS与HTTP网络服务器，详细过程见第4章介绍。无论哪种情况，都要将文件从所有Red Hat Linux安装光碟复制到/mnt/source之类的共享目录中。一旦装载Red Hat Linux安装光碟后，可用下列命令复制文件：

```
# cp -ar /mnt/cdrom/RedHat /mnt/source
```

设置Kickstart安装

设置Kickstart安装的细节见第5章。总之，已经有一个Kickstart文件，安装Red Hat Linux的相关设置保存在/root目录的anaconda-ks.cfg文件中。可以根据另一台计算机上的需要修改这个文件，记住要激活分区命令，其默认标为说明语句。

设置Kickstart安装的最简单方法是把ks.cfg之类需要的文件复制到引导软盘中。在Red Hat Linux安装提示下输入下列命令：

```
boot: linux ks=floppy
```

Linux基础

第6章、第7章和第8章的几个基本命令是Linux中导航的基础。有些命令可以管理文件和目录，寻找不同文件或操纵文件，有些是帮助管理分区的关键命令。由于vi文本编辑器是救援盘上惟一可用的编辑器，因此一定要了解vi命令。

本节的格式有所不同，因为这些命令已经在相关章节详细介绍过。

导航

表A.3列出了基本导航命令。用这些命令可以在Linux命令行界面中漫游。关于这些命令的细节，见第6章。

表A.3 导航命令

命令	描述
cd name	改变目录，目录名可以是绝对格式（如/etc/xinetd.d）或相对格式（如usr/source）
dir	按特别方式列出当前目录中的文件，是ls的特殊版本，有些Linux发行版本设置alias dir=ls -l
ls	列出当前目录中的文件，有许多变换形式
pwd	列出当前的工作目录

管理文件和目录

表A.4列出了管理文件和目录的基本命令。管理文件和目录是命令行界面的另一个重要技巧。关于这些命令的更多信息，见第6章。

表A.4 文件管理命令

命令	描述
cp file1 file2	复制文件，利用相应的变换形式，这个命令可以复制目录的及其子目录内容
file filename	确定文件类型，选项包括文本、图形数据、gzip压缩文件、cpio档案、邮件文本，等等
ln file1 file2	链接两个不同文件，硬链接生成相同文件的完全拷贝，软链接生成指针
mkdir name	生成新目录，名称可以用绝对或相对路径格式，利用正确的变换形式，甚至可以用一个命令建立多层子目录

(续表)

命令	描述
<code>mv file1 file2</code>	删除与复制文件
<code>rm filename</code>	删除文件, 利用正确的变换形式, 甚至可以用一个命令删除多层子目录。这个命令很危险, 特别是对根用户
<code>rmdir dirname</code>	删除目录, 利用正确的变换形式, 甚至可以用一个命令删除多层子目录。默认情况下, 目录应为空
<code>touch filename</code>	用filename生成空白文件
<code>umask abcd</code>	对用户新建的文件设置默认权限

搜索不同文件

表A.5列出了搜索不同文件的命令。可以通过搜索不同的文件来管理Linux操作系统。关于这些命令的更多信息, 见第6章。

表A.5 文件读取命令

命令	描述
<code>cat filename</code>	读取文件内容, 也将一个或几个文本文件滚动到屏幕上。这个命令也可以将映象文件(如红帽子安装bootdisk.img)内容改向(>)到软盘设备上
<code>head filename</code>	将文件的前几行发送到屏幕上, 默认为10行
<code>less filename</code>	在文本型阅读器中打开文件, 可以一次一屏地向上或向下滚动。可以使用vi搜索命令
<code>more filename</code>	在文本型阅读器中打开文件, 可以一次一屏地滚动。可以使用vi搜索命令

操纵文件

表A.6列出了操纵文件的基本命令。你需要检查文件内容, 以便在Linux操作系统中操纵文件。关于这些命令的更多信息, 见第6章。

表A.6 操纵文件的命令

命令	描述
<code>find / -name file -print</code>	从根目录(/)开始搜索文件地址, 可以使用通配符或从其他目录开始
<code>grep string file</code>	搜索指定文件中的文本字符串。可以用通配符搜索一系列文件
<code>locate file</code>	从slocate数据库搜索指定文件的地址。可以用通配符, 例如 <code>locate abc</code> 命令还寻找文件abcd的地址。slocate数据库在每晚默认的cron作业中刷新
<code>wc file</code>	显示文本文件中的行数、字数和字符数

管理分区

还有管理分区的命令，其中有些与分区配置方式有关（如**fdisk**、**fips**、**parted**），见本附录前面介绍。表A.7列出的分区管理命令，见第7章详细介绍。

表A.7 分区管理命令

命令	描述
df	报告当前硬盘上的分区
du	指定每个文件的文件空间使用情况，包括子目录中的分区
dumpe2fs device	列出与设置相关的所有信息（如/dev/sdb2）
e2label device label	如果只指定设备（如/dev/hda1），则这个命令返回当前标签，否则其指定新标签，对应于/etc/fstab中的项目
fsck device	检查和修复Linux文件系统，要指定与卸载分区相关的设备。这个命令通常探测文件系统和使用正确格式，否则可以用 fsck.minix device 、 fsck.ext2 device 或 e2fsck device 之类的命令。后两个命令适用于ext2和ext3格式
mount filesystem device	在/dev/hda2分区和设备上装载/home之类的文件系统
tune2fs device	将分区从ext2转换为ext3
umount filesystem	卸载/home之类的文件系统

vi编辑器

第6章曾介绍过，vi有三种方式：命令方式、插入方式和执行方式。可用命令的细节见“Linux Instant Command Reference”一书。

命令方式

vi命令方式可以操纵文件中的现有文本。表A.8列出了一些命令方式命令。这些命令影响光标当前位置的文本。

表A.8 命令方式命令

命令	功能
cc	删除当前行并转入插入方式，以便输入替换内容
cw	删除当前单词并转入插入方式，以便输入替换内容
dd	删除当前行
dw	删除当前单词
D	删除光标当前位置到行末的内容
p	将寄存器（缓冲区当前内容）复制到光标当前位置后面
:reg	显示寄存器内容
u	取消上次改变
U	恢复当前行
nY	将几行复制到寄存器中，见p命令

插入方式

vi中有几种方法可以开始插入方式。进入插入方式之后，可以输入所要的文本。有些vi命令方式命令（如cw）也自动启动插入方式。表A.9列出了一些插入方式命令。这些命令基于光标当前位置。

表A.9 插入方式命令

命令	功能
a	在光标当前位置后面插入新文本
A	在当前行末尾插入新文本
Esc	返回命令方式
i	在光标当前位置插入新文本
I	在行开头插入新文本
o	在当前行后面开始新行
O	在当前行前面开始新行

执行方式

可以在vi编辑器内运行shell命令，只要用:!shell命令启动命令即可。两个特殊的执行方式命令可以写入和退出文件（见表A.10）。可以组合这些命令，如:wq写入文件并退出vi编辑器。

表A.10 执行方式命令

命令	功能
!:command	运行指定的shell命令，从启动vi编辑器的目录开始
q	退出文件。如果进行了改变，则可以用q!命令退出vi编辑器而不保存改变
w	写入当前文件

基本Linux管理

第9章到第14章介绍了基本的Linux管理命令。这些命令可以管理Linux系统，有些可以管理用户与组，有些可以使用RPM与tarball中的包。有些包要先编译才能安装。

有些重要的管理命令可以帮你完成引导过程并建立作业，如半夜完成的备份。

用户与组管理

用户与组管理命令见表A.11，有些可以生成用户与组，有些可以配置隐蔽口令组。关于这些命令的更多信息，见第9章。

修改用户与组访问

可以用配额限制用户与组的访问。配额限制文件数或文件大小。可以用用户专用组模式在特定目录中组织组访问。表A.12列出用户与组访问命令。关于这些命令的更多信息，见第9章。

表A.11 用户与组管理命令

命令	功能
<code>chage option user</code>	根据选项，设置用户口令或账号的寿命
<code>grpconv</code>	将/etc/group中的口令转换并存放在/etc/gshadow中
<code>grpunconv</code>	与上述过程相反，将口令恢复到/etc/group中
<code>newusers file</code>	从file的清单中增加新用户
<code>pwconv</code>	将/etc/passwd中的口令转换并存放在/etc/shadow中
<code>pwunconv</code>	与上述过程相反，将口令恢复到/etc/group中
<code>useradd name</code>	增加新用户name
<code>userdel name</code>	删除用户name，如果还要删除该用户的主目录，用-r选项

表A.12 用户与组访问命令

命令	功能
<code>edquota user</code>	打开用户的配额配置文件
<code>grpquota group</code>	打开组的配额配置文件
<code>quotacheck</code>	生成基础配额配置文件，通常用-avum选项运行
<code>quoton f les st ...</code>	对特定文件设置配额，如/home

包管理

Red Hat Linux可以从RPM或tarballs安装包。可以用相应的rpm命令安装RPM包，详见第10章介绍。Tarballs则有一些麻烦，首先要解压缩和解包。这个过程例子见第12章，其中使用了Linux内核。

一般来说，RPM包安装好之后，就可以使用。可能要用chkconfig之类的命令激活，但所有组件都已经各就各位了。

但是，仅仅将tarball解压缩和解包还不够。例如，如果从互联网上下载newprogram.tar.gz包，则可以用下列命令解压缩和解包：

```
# tar xzvf newprogram.tar.gz
```

这个命令在某个目录中设置一系列文件（如newprogram）。这个目录中通常有个README文件，其中包含安装指令。有时是个可以马上使用的脚本，如install.pl。也许还要编辑设置，然后编译程序。

要编译程序，首先要导航到程序目录。有时只要编辑相应的配置文件，并移到正确的目录下，然后运行make命令即可。但有时情形会更加复杂，可能要对内核使用make mrproper、make modules与make modules_install之类的命令，见第12章介绍。

引导过程命令

表A.13列出了管理引导过程的命令。这些命令很难分类。有些用于检查引导消息，有些则在引导过程中使用。关于这些命令的更多信息，见第11章。

表A.13 引导过程命令

命令	描述
dmesg	检查引导消息，通常存放在内核环缓冲区，也可以检查/var/log/messages末尾的引导消息
grub-install	将GRUB安装成引导装入器，可以将系统从LILO之类的另一引导装入器中转过来
init runlevel	指定新的运行级，可以测试新配置或进入单用户方式进行查错
initdefault	在/etc/inittab中指定默认运行级
kudzu	启动Red Hat Linux硬件配置实用程序，通常在安装或删除硬件时自动运行
mkbootdisk version	根据/boot目录中指定的内核版本生成定制引导盘

管理命令

表A.14列出了一些重要的管理命令，它们可以帮助你方便地管理系统。例如，cron与at监控程序可以在不打扰用户活动的基础上进行计划操作，如午夜。关于这些命令的更多信息，见第13章。

表A.14 管理命令

命令	描述
at file time	执行作业或程序的一次性命令，与atq、atrm和batch密切相关
atq	查询当前的at作业表
atrm job	从队列中删除作业的命令
batch file	指定at作业，通常在CPU需求低于CPU能力80%时运行
crontab	打开文件，可以配置要定期运行的作业
kill PID	停止指定PID的进程
logrotate	cron作业，定期轮换日志文件，默认在/etc/cron.daily目录中
nice -n number command	启动低优先级的另一命令
ps	列出运行进程，x选项列出所有用户的进程，还有许多其他选项
renice PID	提高指定PID的进程优先级
tmpwatch	cron作业，定期删除/tmp与/var/tmp文件，默认在/etc/cron.daily目录中
top	这个实用程序动态显示需要CPU资源最多的进程
who	列出登录用户

备份命令

另一些重要命令（如表A.15）与系统数据备份有关。有些可以直接备份与恢复数据，另一些可以设置RAID阵列，提供数据冗余度。关于这些命令的更多信息，见第14章。

表A.15 备份命令

命令	描述
<code>cdrecord options file</code>	复制文件（通常是.iso文件）到相应光驱上的可写光碟中
<code>dump type device directory</code>	用某种类型的备份将一个目录备份到指定设备
<code>dvdrecord options file</code>	复制文件（通常是.iso文件）到相应光驱上的可写DVD中
<code>cpio</code>	从清单（如find命令清单）中取得输入并将其复制到标准输出，可以定向到backedup.cpio之类的文件
<code>mkisofs options new.iso directory</code>	根据选项在指定的目录中生成new.iso文件
<code>mkraid</code>	根据/etc/raidtab中定义的条件生成RAID设备
<code>restore</code>	从dump命令生成的备份恢复
<code>tar</code>	从一组文件建档到一个磁带档案文件

X窗口管理

由于本附录是Linux命令手册，因此本节只介绍可以从命令行界面调用的工具。但本节的许多工具都与CNCM和KDE密切相关。有几个重要工具可以帮助配置GUI，以及GNOME与KDE桌面环境。红帽子还有一系列GUI工具，可以管理Linux的各个部分。

X窗口配置

X窗口配置有两个基本工具：`xf86config`与`redhat-config-xfree86`，都可以从普通命令行界面调用。这两个工具可以编辑主X窗口配置文件`Linux`，也可以直接在vi之类的文本编辑器中编辑这个文件。关于这些命令的更多信息，见第15章。

xf86config

Red Hat Linux 9中不包括`xf86config`，但这是个标准工具，可以从www.xfree86.org站点下载XFree86服务器的另一个版本。运行`xf86config`时，可以配置几个不同组件，见表A.16。但不需要所有的信息。

表A.16 xf86config信息

数据	选项	要求/默认
Mouse（鼠标）	九种不同协议	Microsoft协议
Third Button（第三键）	中间键（对三键Logitech鼠标或有可单击滚动球的鼠标而言）	无
Simulate Middle Button （模拟中间键）	Emulate3Buttons（同时单击左右键可以在GUI中模拟中间键命令）	无
Mouse Device（鼠标设备）	设备名	/dev/mouse
Keyboard（键盘）	25个选项	一般101键PC （选项1）

(续表)

数据	选项	要求/默认
National Layout (国家布局)	按国家	必须选择, 最标准的为美式英语
Variant Name (变体名)	生成自己的标签	默认标签= us
XKB Options (XKB选项)	如需要特殊键, 输入y	无
Monitor Horizontal Sync (显示器水平同步)	可以选择或输入特殊同步速率	31.5MHz
Monitor Vertical Refresh (显示器垂直同步)	可以选择或输入特殊同步速率	50~70kHz
Identifier (标识符)	显示器标签	"My Monitor"
Video Card Database (显卡数据库)	对预配置卡输入y	No
Video Card Memory (显卡内存)	单位为KB	256KB
Identifier (标识符)	显卡标签	"My Video Card"
Color Depth (颜色深度)	1到24位	配置为8、16或24位

redhat-config-xfree86

redhat-config-xfree86的好处之一是可以从命令行界面调用, 它的功能与旧的XF86Setup工具相似, 可以探测系统并打开基本的GUI配置菜单。使用redhat-config-xfree86时不必选择那么多选项, 而xf86config中则还要选择输入设备(鼠标与键盘)。根据所要的显卡与显示器情况, 可以配置几个项目, 见表A.17。

表A.17 redhat-config-xfree86信息

数据	选项
分辨率 (Resolution)	640×480到1920×1440
颜色深度 (Color Depth)	8位 (256色), 15位或16位 (几千色) 和24位 (几百万色)
显示器类型 (Monitor Type)	可以按机型和版本配置, 也有一般性选项, 还可以设置水平同步与垂直刷新率, 有时允许探测
DPI	单击Set DPI按钮, 可以输入显示器高度与宽度
显卡 (Video Card)	可以按机型和版本配置。可以设置内存, 有些卡可以探测。可以选择不同驱动器。如果探测到卡, 则可以增加特殊选项, 也可以对XF86Config增加其他选项 有时, 还可以启用三维加速功能, 但Linux的三维支持通常比显卡厂家的硬件版本落后

GUI管理工具

Linux还提供了其他的GUI管理工具，许多都在redhat-config-*系列中，且只能在安装了相应RPM包时使用。表A.18所列的大多数工具都在第15章与第19章有详细介绍。大多数要求事先有GNOME与KDE之类的GUI。但是，也可以用表中所示的工具名从GUI的终端窗口启动。

表A.18 GUI管理工具

工具	描述
etherreal	网络通信流分析器，见第22章
gfloppy	格式化3.5寸盘或5.25寸盘的工具
hwbrowser	读取计算机上已探测到的硬件的工具
nautilus	GNOME文件管理器
redhat-config-bind	DNS服务器配置工具，与redhat-config-bind-gui密切相关
redhat-config-date	日期/时区配置器，可以和NTP服务器同步（两个命令启动同一工具）
redhat-config-timed	
redhat-config-httpd	通过/etc/httpd/conf/httpd.conf配置Apache Web服务器的工具
redhat-config-keyboard	基本键盘配置器
redhat-config-kickstart	配置Kickstart文件的工具，见第5章介绍
redhat-config-language	可以从所安装语言中选择默认的语言
redhat-config-mouse	对鼠标或指示设备配置Linux的工具。如果有串行鼠标，则可以设置端口，它是mouseconfig的GUI版本
redhat-config-network	配置现有网络设备/etc/hosts、/etc/resolv.conf的工具，不同配置可以有不同的配置文件，如停靠端口。其文本版本为redhat-config-network-tui
redhat-config-network-druid	配置新网卡的工具，包括电话modems，也称为Internet配置向导
redhat-config-nfs	NFS服务器配置工具
redhat-config-packages	基本RPM包管理工具，可以按组或各个RPM安装与删除包。是gnorpm的后续产品
redhat-config-printer	打印机配置工具，相当于printconf，更多信息见第25章。与redhat-config-printer-gui密切相关，文本版本为redhat-config-printer-tui
redhat-config-proc	内核调整器，将改变写入/etc/sysctl.conf，在/proc文件中使用
redhat-config-rootpassword	改变根口令的工具
redhat-config-samba	在Samba服务器上配置共享目录的语言
redhat-config-securitylevel	iptables防火墙配置器，是lokkit的GUI版本
redhat-config-services	chkconfig的图形前端，控制不同运行级的活动服务

(续表)

工具	描述
redhat-config-soundcard	探测并列出可探测声卡的工具。如果需要定制设置, 可以使用sndconfig或直接编辑/etc/modules.conf
redhat-config-users	用户与组管理工具, 是编辑/etc中主要用户与组文件passwd、group、shadow、gshadow的前端
redhat-config-xfree86	前面已经介绍, 是Xconfigurator的后续产品
redhat-logviewer	从/var/log中打开日志文件的工具
switchdesk	可以在可用GUI之间切换的工具, 通常在GNOME、KDE与twm之间切换

基本Linux网络

下一类要介绍的命令可以在Linux计算机上配置与控制网络。有些命令提供网卡的基本信息, 有些则可以指定网络到哪里查找域、网络设置和其他类似信息。

网络查错命令和用ip地址防止入侵保护系统的命令也属于这一类。关于这些命令的更多信息, 见第2.1章与第2.2章。

网卡命令

设置网卡的两个关键命令是ifconfig与arp, 其相关命令可以激活和冻结所选网卡。表A.19列出了这些网卡命令。

表A.19 网卡命令

命令	描述
arp	控制硬件与IP地址数据库
ifconfig	返回活动网卡, 可以指定IP地址、网络掩码、硬件地址等TCP/IP信息, 也可以指定网卡的特殊IRQ和I/O端[]
ifdown device	冻结网络设备的命令
ifdown-*	这个命令启动/etc/sysconfig/network-scripts中的脚本, 冻结特定设备
ifup device	激活网络设备
ifup-*	这个命令启动/etc/sysconfig/network-scripts中的脚本, 激活特定设备

网络域管理

有些命令可以标识不同网络类型上的Linux计算机。单独运行hostname之类的命令时, shell返回当前域名。也可以用这个命令指定新名, 如hostname newname。表A.20列出了网络域管理命令。

表A.20 网络域管理命令

命令	描述
domainname	列出或指定当前计算机的NIS域名，永久改变应放在/etc/sysconfig/network中，格式为NISDOMAIN=domainname
hostname	列出或指定当前计算机的主机名，永久改变应放在/etc/sysconfig/network中，格式为HOSTNAME=hostname
nisdomainname	见domainname
ypdomainname	见domainname

网络查错命令

Linux提供了三个基本的网络查错命令netstat、ping与traceroute。关于这些命令的更多信息，见第22章。

netstat命令显示当前网络连接信息，表A.21列出了一些netstat命令选项。

表A.21 netstat命令

命令	结果
netstat	列出不同端口打开的所有TCP网络连接
netstat -a	列出所有网络端口的活动
netstat -c	和netstat -a相似，但这个命令每秒运行，并将结果连续发送到屏幕
netstat -e	提供每个连接的其他信息
netstat -l	将清单限制在监听请求的Telnet与Apache (httpd) 之类的服务
netstat -n	指定良好的IP地址，适用于找不到主机名时，如逆向DNS域有问题时
netstat -p	包括每个打开端口上进程的名称与PID

ping命令发送一个数据分组，测试与指定主机计算机的连接。第21章介绍了标准ping查错命令。这个命令的其他选项见表A.22。

表A.22 ping命令

命令	结果
ping hostname	测试计算机与hostname之间的连接
ping -c n hostname	将连接测试限于几个分组，不必按Ctrl+C键停止测试
ping -i n hostname	在ping之间等待n秒，默认为1秒
ping -n hostname	在输出中使用IP地址，用于找不到DNS服务器时
ping -s data	在ping中发送data字节分组，是一些“ping到死机”的命令源

说明：本书不支持使用“ping到死机”命令，除非用其测试系统能否抵抗这个攻击。第22章介绍的iptables命令可以停止“ping到死机”命令。

traceroute命令可以隔离大网络中的问题。经过路由器时，它会监听ICMP的“time exceeded”消息，并将其返回你的计算机。这样，它可以跟踪消息路径。如果跟踪Internet上的消息，则默认的30步可能不够，下列命令可以跟踪40步的消息：

```
# traceroute -m 40 www.example.com
```

如果Internet响应速度很慢，则可以延长ICMP消息返回计算机的时间。例如，下列命令表示最多等待10秒：

```
# traceroute -w 10 www.example.com
```

iptables与防火墙

iptables命令很复杂，第22章提供了基本解释。iptables命令采用特定格式，如：

```
# iptables -t table option pattern -j target
```

表A.23介绍了其中的每个项目。

表A.23 iptables命令格式

项目	描述
-t table	这个项目指定表格类型，选项有filter与nat，默认为filter
option	可以在iptables链中增加规则（-A）、删除规则（-D）或插入规则。三个标准链是 INPUT、OUTPUT与FORWARD。可以生成自己的链。例如，许多防火墙的iptables建立在BLOCKED-5 INPUT链
pattern	可以将iptables设置成在每个分组中查找模式，模式可以匹配IP地址、TCP/IP端口号和协议类型
-j target	如果有模式匹配，则告诉iptables要干什么，目标选项为ACCEPT、DROP、REJECT与LOG

Linux网络服务

可以在Linux计算机上激活许多基本网络服务，其中几个由xinetd监控程序控制。许多管理员建立自己的DNS服务器，避免在网络的每台计算机上维护/etc/hosts。有些设置自己的DHCP服务器，避免在网络的每台计算机上维护IP地址信息。还有一些命令可以设置和配置打印机，以及配置sendmail服务器。

本节只介绍命令行界面中可以运行的命令，而不介绍GUI工具。关于这些命令的更多信息，见第23章到第26章。

xinetd服务的命令

前面曾介绍过，许多服务都是通过扩展Internet服务监控程序xinetd控制的，包括远程Shell与Telnet。这个监控程序监听请求并在需要时启动网络服务。

可以用几个不同的命令从客户端启动远程Shell，见表A.24。

telnet命令的变体非常丰富，且许多涉及很特殊的情形。由于telnet提供了简单的远程登录界面，因此不需要太多变形。表A.25列出了几个telnet命令选项。

表A.24 远程Shell命令

命令	描述
<code>rlogin hostname</code>	用远程Shell服务器登录远程计算机，使用当前用户名
<code>rlogin -l username hostname</code>	用不同用户名登录远程计算机
<code>rsh hostname</code>	用远程Shell服务器登录远程计算机，使用当前用户名
<code>rsh -l username hostname</code>	用不同用户名登录远程计算机
<code>rexec hostname command</code>	登录远程计算机并执行命令

表A.25 telnet命令

命令	描述
<code>telnet hostname</code>	在hostname上打开控制台登录界面
<code>telnet -a hostname</code>	发送当前USER，作为telnet登录过程的用户名
<code>telnet -f hostname</code>	支持在Telnet服务器上使用Kerberos
<code>telnet -l username hostname</code>	以username身份登录到hostname计算机

DNS与DHCP

DNS与DHCP服务与客户端有许多相关命令。第24章介绍这些系统的配置，介绍主配置文件`/etc/named.conf`和`/etc/dhcpd.conf`中的命令。表A.26介绍了一些基本DNS与DHCP命令。

表A.26 DNS与DHCP命令

命令	描述
<code>named</code>	DNS服务器监控程序
<code>dhcpd</code>	DHCP服务器监控程序
<code>dhclient</code>	DHCP客户端监控程序，也可以作为刷新IP地址数据的命令。在旧版红帽子发行版本中，这个命令称为 <code>dhcpcd</code> 或 <code>pump</code>

打印机命令

有几个基本命令与CUPS和LPD打印系统相关，其中有些在两个系统都适用。例如，利用`xinetd`中的`cups-lpd`服务，可以将LPD命令自动转换成CUPS命令。表A.27列出了基本打印机命令。

表A.27 基本打印机命令

命令	描述
<code>lpr file</code>	打印file，这是基本LPD打印机命令
<code>lpc</code>	管理LPD打印队列和活动打印机
<code>lpq</code>	检查打印假脱机，可以用-P开关指定打印机
<code>lprm job</code>	删除指定作业号的打印作业
<code>cupsaddsmb</code>	可以通过Samba共享CUPS打印机

(续表)

命令	描述
cupsconfig	在Lynx文本浏览器中打开CUPS配置实用程序
cups-lpd	启动CUPS LPD xinetd, 使CUPS可以读取LPD命令
filter	增加新的CUPS过滤器
lp file	用CUPS打印file
lppasswd	控制CUPS配置的访问
lpoptions	设置CUPS打印机选项以及默认
lpstatus	打印CUPS状态(队列)信息

邮件管理命令

Linux提供了管理sendmail邮件服务器的命令, 其中最重要的是m4宏处理器, 它处理sendmail配置文件。其他命令可以管理别名、数据库, 等等。表A.28列出了这些命令。关于sendmail的更多信息见第26章。

表A.28 邮件维护命令

命令	描述
m4	将sendmail宏文件/etc/mail/sendmail.mc处理成适合sendmail配置文件的格式, 通常是/etc/mail/sendmail.cf
mailq	向打印机发送排队邮件消息头汇总, sendmail -bp可完成相同的工作
makemap	从/etc/mail配置文件生成sendmail数据库映射
mailstats	返回邮件统计信息: 消息数, 总长度, 等等
newaliases	改变/etc/aliases时, 这个命令更新sendmail数据库
praliases	显示数据库的当前别名
rmail	读取UUCP邮件
smrsh	进入sendmail shell

Linux文件共享服务

可以用多种方法在Linux中共享文件。一般来说, 先配置服务器, 然后通过一个目录共享文件。四种主要的Linux共享服务器是FTP、NFS、Samba与Apache。如果启用NIS, 则它也共享配置文件。尽管每个服务都有图形化配置工具, 但都可以从命令行界面设置, 而且分别包括客户机和服务器的普通文本命令。关于这些服务的详细信息, 见第27章到第30章。

FTP服务器

基本FTP命令见第27章介绍。本节总结相关的命令与配置文件。尽管Red Hat Linux 9安装光碟只包括vsFTP, 但WU-FTP是个常用选项, 它也提供RPM格式。vsFTP服务器是推荐的服务器, 因为Red Hat Linux在自己的FTP服务器中使用这个服务器。

vsFTP命令与配置文件

vsFTP包有一组配置文件，比WU-FTP之类的其他服务器简单，惟一需要的命令是vsftpd监控程序。VsFTP服务器现已成为/etc/rc.d/init.d目录中的普通服务，而不再是xinetd服务。如果两个服务器都安装，则一次只能激活一个。表A.29显示了vsFTP配置文件。

表A.29 vsFTP配置文件

文件	描述
/etc/vsftpd.conf	主配置文件
/etc/vsftpd.ftpusers	不允许登录的用户表，应包括根用户和news、bin与mail之类的服务级用户
/etc/vsftpd.user_list	允许或拒绝的用户名单，取决于/etc/vsftpd.conf中的userlist_deny变量

WU-FTP命令与配置文件

vsFTP和一个主要替代产品是WU-FTP，可以从开发小组主页www.wu-ftp.org或资源中心www.hardfield.com/wu-ftp/下载。表A.30的命令可以管理WU-FTP服务器。记住，WU-FTP是个xinetd服务，要通过/etc/xinet.d中的wu_ftp文件激活。也可以用chkconfig命令激活这个服务。

表A.30 WU-FTP命令

命令	描述
ckconfig	检查配置文件的完整性
ftpcount	列出连接数
ftpwho	列出连接用户和源IP地址
ftprestart	停止并重新启动FTP服务器
ftpsht	可以立即或在指定时间关闭FTP服务器
in.ftpd	启动FTP服务器监控程序
in.wuftp	启动WU-FTP服务器
privatepw	从/etc/ftpgroups中增加或删除FTP组，这些组对应于/etc/group中的真实组

WU-FTP服务器还有一组配置文件，如表A.31。第27章曾介绍过，其中有些文件的功能已经放到了/etc/ftpaccess中。

FTP客户机

FTP客户机有多种，都是FTP文本客户机的前端。FTP客户机命令是变化的，第27章介绍了其中最重要的命令。表A.32是个完整的清单，但只是基本清单，没有列出选项。要取得更多信息，可以在ftp>提示下输入help command。

表A.31 WU-FTP配置文件

文件	函数
/etc/ftpaccess	打开基本WU-FTP配置文件
/etc/ftpconversions	列出FTP上传与下载期间自动运行的命令
/etc/ftpgroups	定义指定口令的特殊组, 通过privatepw命令定义
/etc/ftphosts	允许或拒绝访问特定用户账号
/etc/ftpusers	允许或拒绝访问特定用户

表A.32 FTP客户机命令

命令	描述
!	转义到shell, !ls -l命令可以得到当前本地目录中的完整文件清单
\$	执行一个宏
append	将一个文件添加到另一文件末尾, 如append local remote命令将本地文件添加到远程文件末尾
ascii	将文件传输方式设置为ASCII
bell	在文件传输之类的命令完成时发一声响
binar	将文件传输方式设置为二进制
bye	退出当前FTP会话
cd	改变目录
cdup	向上移一层目录
close	关闭连接而不退出FTP
delete	删除远程目录中的指定文件
dir	等于ls -l
exit	关闭连接并退出FTP
get	从FTP服务器复制文件
hash	切换散列标志的使用, 以便监视文件传输的进程
lcd	改变本地计算机上的工作目录
ls	等于bash shell中的ls -l
mdelete	删除多个文件
mdir	取得远程目录中的内容并将其输出到本地文件
mget	从FTP服务器复制多个文件
mkdir	在FTP服务器上生成多个文件
mput	向FTP服务器发送多个文件
newer	如果远程文件较新, 则使用get命令
open	在FTP提示下连接远程FTP服务器
put	将文件复制到FTP服务器

(续表)

命令	描述
pwd	列出FTP服务器上的工作目录
quit	退出FTP shell
rename	重命名FTP服务器上的文件
rmdir	删除远程目录
status	检查连接状态
system	显示基本系统类型, 通常为UNIX
user	以用户身份登录

NFS命令

NFS（网络文件系统）用于Linux与UNIX计算机之间共享目录。第28章介绍了其基本配置过程，表A.33总结了一些重要的NFS命令。

表A.33 NFS命令

命令	描述
exportfs	根据/etc/exports导出和维护可用NFS目录表
nfsstat	返回共享NFS目录信息，这个命令的输出可以查出连接问题
nhfsstone	测试NFS服务器负载
rpc.mountd	启动NFS装载监控程序，这个服务实际检查装载请求与/etc/exports中允许的项目
nhfsrun	测试程序，在服务器需求处于一定范围时运行nhfsstone
showmount	显示NFS服务器中可用的目录

NIS命令

NIS（网络信息系统）可以对Linux与UNIX计算机局域网中的/etc/passwd之类的关键配置文件建立一个数据库。第28章介绍了基本配置过程，表A.34总结了一些重要的NIS命令。许多关键NIS命令都在/usr/lib/yp目录中。如果使用NIS，则可以用PATH=\$PATH:/usr/lib/yp命令将这个目录加进PATH中。

表A.34 NIS命令

命令	描述
create_printcap	将/etc/printcap之类的LPD文件处理成NIS数据库映射，不处理CUPS打印机配置文件
makedbm	生成NIS数据库文件
match_printcap	处理/etc/lpd.conf中的printcap_path，不处理CUPS打印机配置文件

(续表)

命令	描述
mknetid	对关键配置文件生成NIS数据库映射: /etc/passwd、/etc/group与/etc/hosts
pwupdate	对普通口令与隐蔽口令生成NIS数据库映射
revnetgroup	生成逆向NIS netgroup数据
ypcat	从NIS服务器数据库读取文件
ypchfn	在NIS数据库中改变用户的个人信息
ypchsh	在NIS数据库中改变用户的默认shell
ypinit	在主或从NIS服务器上建立数据库
ypmatch	在NIS数据库中搜索用户
yppasswd	在NIS数据库中改变口令
yppush	将NIS主数据库复制到NIS从数据库
ypxfr	从NIS从数据库中复制NIS数据库

Samba命令

Samba可以将Linux配置成连接Microsoft Windows计算机和共享目录。Linux与UNIX计算机也可以用Samba相互共享目录。

第29章曾介绍过, 可以用SWAT实用程序配置Samba。SWAT是个丰富的工具, 但和其他GUI工具一样, 它也只是一组命令的前端。Samba命令很多, 有些与服务器相关, 有些常用于Samba客户端。

Samba服务器命令

配置Samba服务器时, 就是用与Microsoft Windows兼容的格式共享目录和打印机。表A.35列出了重要的Samba服务器命令。

表A.35 Samba服务器命令

命令	描述
make_unicodemap	指定从DOS或UNIX文本向16位Unicode的转换
mk smbpasswd.sh	启动一个脚本, 直接编辑SMB口令文件/etc/samba/smbpasswd
smbadduser	在Linux用户与Microsoft Windows用户之间建立数据库项目, 提示输入口令, 并将结果放进/etc/smbusers和/etc/smbpasswd
smbcontrol	可以向SMB服务器发送消息, 如调试、选举和ping消息
smbpasswd	改变用户的Samba口令, 适用于本地或远程Samba服务器
smbstatus	显示本地SMB服务器的连接状态
testparm	检查smb.conf语法
testprns	检查提供的打印机的Samba共享名
winbindd	对Microsoft Windows服务器名启动名称服务监控程序

Samba客户机命令

配置Samba客户机时，要用Linux或UNIX计算机上的命令连接共享Samba或Microsoft Windows目录。表A.36列出了重要的Samba客户机命令。

表A.36 Samba客户机命令

命令	描述
mount.smb	可以用mount命令作为前端，连接共享Samba目录
nmblookup	搜索与NetBIOS名称相关联的IP地址
rpcclient	允许连接Microsoft Windows服务器上的远程过程调用（RPC）
Smbcacs	允许浏览和设置Microsoft Windows服务器上的访问控制表
smbclient	可以用FTP接口直接连接Samba服务器
smbmount	装载Samba文件系统，可以用mount命令作为前端
smbprint	将打印作业发送到Samba服务器上的共享打印机
smbumount	卸载共享Samba目录

Apache命令

Apache是Internet上最常用的Web服务器，也是Red Hat Linux的默认Web服务器。第30章曾介绍过，配置Apache的标准方式是编辑/etc/httpd.conf/httpd.conf配置文件。可以用命令确定使用的Apache配置，表A.37列出了一些重要的Apache命令。

表A.37 Apache命令

命令	描述
ab	测试Apache服务器性能的工具
apachectl	Apache服务器的控制脚本
htdbm	新Apache 2.0中管理授权用户/口令数据库的工具
htdigest	对用户与口令生成验证数据库的工具
htpasswd	可以对Web服务器设置各个用户与口令的工具
httpd	Apache监控程序，httpd -t测试httpd.conf配置文件的语法
logresolve	对Apache日志文件进行逆向名称查找，以便知道连接服务器的域或计算机
rotatelog	自动转换Apache日志文件，否则用cron控制的标准logrotate作业时要停止Apache服务器

其他命令

Web上第1章介绍了与基本Linux证书相关的命令。表A.38详细介绍这些命令。

表A.38 其他命令

命令	描述
dhcpcd	对Red Hat Linux 7.2启动DHCP客户机（现已过时）
ifport	将10baseT（Ethernet）与100baseT（Fast Ethernet）之类的网络类型与网络接口相关联，只适用于相当于一般网络驱动器的有限组
ifuser	确定通过特定网络设备与主机或IP地址的连接，常用于脚本
innnd	启动Internet网络新闻监控程序，可以用这个监控程序配置新闻组。关键配置文件在/etc/news目录中，包括inn.conf。还有配置文件语法检查器/usr/lib/news/bin/inncheck
ncpmount	装载共享Novell目录，要求ipxutils-*与ncpfs-* RPM包
pump	对Red Hat Linux 7.1启动DHCP客户机（现已过时）
route	列出路由表，如route -n命令列出本地计算机的路由表。将不同的IP地址与网络设备和IP网关地址相关联
slattach	将网络设备（如eth0）与串口（如/dev/ttyS0）相关联，对PPP或SLIP连接准备设备
stunnel	在Internet上的公共网和IP地址集和之间的直接连接中增加SSL加密，是实现虚拟专用网的方法之一
su	超级用户命令，普通用户要取得根用户权限时（结果有根口令）可以用这个命令以根用户身份登录。su -c 'command'只要一个命令
sudo	超级用户do命令，授权用户见/etc/sudoers。默认情况下，一旦指定根口令，就有五分钟授权
talkd	启动talk监控程序，在talk-server-* RPM包中，可以帮助一个用户启动与另一用户的会话
whois	查询Internet注册表数据库。例如，Sybex公司web站点的管理信息可以通过whois Sybex.com命令取得

小结

本附录总结了命令行界面的一些重要命令，主要来自本书介绍的基本命令，但还不是Linux的全部命令。

表A.38 其他命令

命令	描述
dhcpcd	对Red Hat Linux 7.2启动DHCP客户机（现已过时）
ifport	将10baseT（Ethernet）与100baseT（Fast Ethernet）之类的网络类型与网络接口相关联，只适用于相当于一般网络驱动器的有限组
ifuser	确定通过特定网络设备与主机或IP地址的连接，常用于脚本
innnd	启动Internet网络新闻监控程序，可以用这个监控程序配置新闻组。关键配置文件在/etc/news目录中，包括inn.conf。还有配置文件语法检查器/usr/lib/news/bin/inncheck
ncpmount	装载共享Novell目录，要求ipxutils-*与ncpfs-* RPM包
pump	对Red Hat Linux 7.1启动DHCP客户机（现已过时）
route	列出路由表，如route -n命令列出本地计算机的路由表。将不同的IP地址与网络设备和IP网关地址相关联
slattach	将网络设备（如eth0）与串口（如/dev/ttyS0）相关联，对PPP或SLIP连接准备设备
stunnel	在Internet上的公共SSL和IP连接集和之间的直接连接中增加SSL加密，是实现虚拟专用网的方法之一
su	超级用户命令，普通用户要取得根用户权限时（结果有根口令）可以用这个命令以根用户身份登录。su -c 'command'只要一个命令
sudo	超级用户do命令，授权用户见/etc/sudoers。默认情况下，一旦指定根口令，就有五分钟授权
talkd	启动talk监控程序，在talk-server-* RPM包中，可以帮助一个用户启动与另一用户的会话
whois	查询Internet注册表数据库。例如，Sybex公司web站点的管理信息可以通过whois Sybex.com命令取得

小结

本附录总结了命令行界面的一些重要命令，主要来自本书介绍的基本命令，但还不是Linux的全部命令。