

FreeBSD 使用手册

The FreeBSD Documentation Project

FreeBSD 中文计划

FreeBSD 使用手册

由The FreeBSD Documentation Project, FreeBSD 中文计划

出版方1999年2月

出版方2005年12月

版权 © 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006 The FreeBSD Documentation Project

版权 © 2003, 2004, 2005, 2006 FreeBSD 中文计划

欢迎使用FreeBSD！本手册适用于安装**FreeBSD 5.4-RELEASE** 和**FreeBSD 6.0-RELEASE** 以及它们的日常使用。这个手册目前由很多人**持续地** 维护。其中的内容需要不断的添加和更新。如果您有兴趣参加这个项目，请发邮件到FreeBSD 文档计划邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-doc>)。此文档最新的英文原始版本可以从FreeBSD Web站点 (<http://www.FreeBSD.org/>) 上获得(这本手册的较早期版本可以在<http://docs.FreeBSD.org/doc/> 找到)，最新中文译本可从FreeBSD 中文计划Web站点 (<http://www.freebsd.org.cn/>)获得。其他的各种格式和压缩的文档可以从FreeBSD的FTP服务器 (<ftp://ftp.FreeBSD.org/pub/FreeBSD/doc/>)或下列其中的一个镜像站点下载获得。如果您更希望得到一份印刷版本的手册，可以从FreeBSD Mall (<http://www.FreeBSDmall.com/>) 购买。您还可以搜索手册 (<http://www.FreeBSD.org/search/index.html>)。

重要: 本文中许可证的非官方中文翻译仅供参考，不作为判定任何责任的依据。如与英文原文有出入，则以英文原文为准。

在满足下列许可条件的前提下，允许再分发或以源代码(SGML DocBook) 或“编译” (SGML, HTML, PDF, PostScript, RTF 等) 的经过修改或未修改的形式：

1. 再分发源代码(SGML DocBook) 必须不加修改的保留上述版权告示、本条件清单和下述弃权书作为该文件的最先若干行。
2. 再分发编译的形式(转换为其它DTD、PDF、PostScript、RTF 或其它形式)，必须将上述版权告示、本条件清单和下述弃权书复制到与分发品一同提供的文件，以及其它材料中。

重要: 本文档由FREEBSD DOCUMENTATION PROJECT “按现状条件” 提供，并在此明示不提供任何明示或暗示的保障，包括但不限于对商业适销性、对特定目的的适用性的暗示保障。任何情况下，FREEBSD DOCUMENTATION PROJECT 均不对任何直接、间接、偶然、特殊、惩罚性的，或必然的损失(包括但不限于替代商品或服务的采购、使用、数据或利益的损失或营业中断) 负责，无论是如何导致的并以任何有责任逻辑的，无论是否是在本文档使用以外以任何方式产生的契约、严格责任或是民事侵权行为(包括疏忽或其它)中的，即使已被告知发生该损失的可能性。

Redistribution and use in source (SGML DocBook) and 'compiled' forms (SGML, HTML, PDF, PostScript, RTF and so forth) with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code (SGML DocBook) must retain the above copyright notice, this list of conditions and the following disclaimer as the first lines of this file unmodified.

2. Redistributions in compiled form (transformed to other DTDs, converted to PDF, PostScript, RTF and other formats) must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

重要: THIS DOCUMENTATION IS PROVIDED BY THE FREEBSD DOCUMENTATION PROJECT "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD DOCUMENTATION PROJECT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

重要: 从FreeBSD和FreeBSD中文化项目官方网站获取的本文档PostScript®和PDF格式文件中内嵌的中文字体，由文鼎科技开发股份有限公司按《文鼎公众授权书》授权提供。

文鼎公众授权书

版权所有(C) 1999 文鼎科技开发股份有限公司

台湾110台北市永吉路168号11楼

除以下规定外，保留所有权利。

任何人均可以复制及分发本授权书原始文件的复本，但禁止修改之。

前言

绝大多数软件的授权书是用来剥夺您共享和修改软件的自由。相反，如果您将我们所授与您的一切权利授与您的接受者，并且确保他们能得到本软件的修改物，文鼎公众授权书特别许可并鼓励您使用本软件。

法律性条款

0. 定义

本授权书中，「字型」是指「文鼎PL细上海宋」、「文鼎PL中楷」（BIG-5码）和「文鼎PL简报宋」、「文鼎PL简中楷」（GB码）等TrueType字型，以及经修改而产生的该等字型的衍生物，包括修改字型样式、更动编码顺序、转换格式、变更字型名称，或者在glyph table中增减一些文字。

「PL」是指「Public License」（公众授权）。

「版权人」是指在字型版权声明中被称为版权所有者之人。

「您」是指被授权者或复制、再散布、修改字型的人。

「自由使用」是指您在所接受的相同条件下，有复制、修改字型及散布字型复制品的自由，而非指价格。如果您愿意，可以对此项服务收取费用。

1. 复制及分发

如果在所有复制品维持本授权书文件（ARPHICPL.TXT）不变，您可以在任何媒体无限制复制及分发本字型之复制品。

2. 修改

如果满足以下条件，您可以用任何方式修改本字型的复制品，包括修改字型样式、更换编码顺序、转换格式、变更字型名称，或者在glyph table中增减一些文字，并且依据上述第一条的规定复制及分发该修改物。

a)您必须在每个修改过的文件中插入明显的声明，表示您如何及何时修改了该文件。

b)您必须允许所有第三方在本授权书条款下，得以「自由使用」该修改物的全部，例如通过提供指定地点的复制路径，或在通常作为软件交换的媒体上发布该修改物。

c)如果修改过的字型在执行时以交谈方式读取命令，您必须使它在开始进入一般的交谈使用方式时打印或显示声明，包括适当的版权声明、无担保声明（或者其他您提供担保的声明），以及使用者可以依据这些条件再分发本字型的声明，并且告知使用者如何看到本授权书的副本。

这些要求适用于整个修改过的作品。如果作品的可辨识部分并非衍生自本字型，且可以合理地认其为独立而个别的产品，则当您将它当作个别产品分发时，本授权书及其条款将不适用于该部分。因此，仅将非基于本字型之其他作品和本字型一起放入贮存或分发媒体的同一卷上，并不会使该其他作品纳入本授权书的适用范围。

3. 解除条件

除非依照本授权书的规定，否则您不能复制、修改、再授权或分发本字型。任何用其他方式复制、修改、再授权或分发本字型的意图，将使本授权书所授与您的权利自动失效。不过，从您那依据本授权书取得复制品和权利的人，只要他们完全遵行条款，其权利将维持有效。

4. 同意

因您未签订本授权书，所以没必要遵行它。然而，没有任何其他文件授与您复制、修改、再授权或分发本字型之权利，如果您不同意本授权书，这些行为是法律所禁止的。因此一旦复制、修改、再授权或分发本字型，就表示您接受本授权书及其一切条款和条件。

5. 自动取得授权

每当您再散布本字型时，收受者便自动从原始授权者处取得依据这些条款和条件复制、分发或修改本字型的授权。您不可对在此所授与收受者之权利实行强加其他限制，您也没有使第三方遵行本授权书的义务。

6. 抵触

若因法院判决、违反专利宣称或任何其他原因（不限于专利纠纷）的结果，使强加于您的条件（不论是法院命令、协议或其他）和授权书的条件有所冲突时，也不能让您违背授权书的条件。如果您不能同时满足本授权书所定的义务及其他相关义务来分发时，那麽您根本不可分发本字型。例如，如果专利授权不许所有直接或间接从您那里取得复制品者，在免授权费的情况下再分发本字型时，唯一能同时满足双方要求的方法是避免分发本字型。

如果本条款之任何部分在特定情况下无效或无法实施，条款的其他部分将继续适用，并作为整体适用于其他情况。

7. 无担保

由于本字型是免费授权，在法律允许的范围内，本字型将不附带任何担保。除非另有书面说明，版权人或其他提供本字型者「同样」不提供任何种类的担保，不论是明示还是暗示，包括但不限于销售性和适于特定目的的暗示担保。有关本字型品质和执行的一切危险均由您承担。如果本字型出现瑕疵，您应承担一切所需服务、修复和改正的费用。

8. 损害赔偿请求权的放弃

除非法律规定或以书面形式同意，在任何情况下，任何版权人或以上被允许得以复制、修改或再分发本字型者，均不对您因使用或不能使用本字型（包括但不限于替代商品或服务的采购；使用、数据或利益之损失；或者营业妨碍）所引致的任何直接、间接、必然、偶然、特殊或惩罚性损失负责，即使版权人或其他人已知该损失的可能性时亦不例外。

FreeBSD 是FreeBSD基金会的注册商标

3Com 和HomeConnect 是3Com Corporation 的注册商标。

3ware 和Escalade 是3ware Inc 的注册商标。

ARM 是ARM Limited. 的注册商标。

Adaptec 是Adaptec, Inc. 的注册商标。

Adobe, Acrobat, Acrobat Reader, 以及PostScript 是Adobe Systems Incorporated 在美国和/或其他国家的商标或注册商标。

Apple, FireWire, Mac, Macintosh, Mac OS, Quicktime, 以及TrueType 是Apple Computer, Inc. 在美国以及其他国家的注册商标。

Corel 和WordPerfect 是Corel Corporation 和/或其子公司在加拿大、美国和/或其他国家的注册商标。

Sound Blaster 是Creative Technology Ltd. 在美国和/或其他国家的注册商标。

CVSup 是John D. Polstra 的注册商标。

Heidelberg, Helvetica, Palatino, 和Times Roman 是Heidelberger Druckmaschinen AG 在美国以及其他国家的商标或注册商标。

IBM, AIX, EtherJet, Netfinity, OS/2, PowerPC, PS/2, S/390, 和ThinkPad 是国际商用机器公司在美国和其他国家的注册商标或商标。

IEEE, POSIX, 和802 是Institute of Electrical and Electronics Engineers, Inc. 在美国的注册商标。

Intel, Celeron, EtherExpress, i386, i486, Itanium, Pentium, 和Xeon 是Intel Corporation 及其分支机构在美国和其他国家的商标或注册商标。

Intuit 和Quicken 是Intuit Inc., 或其子公司在美国和其他国家的商标或注册商标。

Linux 是Linus Torvalds 的注册商标。

LSI Logic, AcceleRAID, eXtremeRAID, MegaRAID 和Mylex 是LSI Logic Corp 的商标或注册商标。

M-Systems 和DiskOnChip 是M-Systems Flash Disk Pioneers, Ltd. 的商标或注册商标。

Macromedia, Flash, 以及Shockwave Macromedia, Inc. 在美国和/或其他国家的商标或注册商标。

Microsoft, IntelliMouse, MS-DOS, Outlook, Windows, Windows Media, 和Windows NT 是Microsoft Corporation 在美国和/或其他国家的商标或注册商标。

Netscape 以及Netscape Navigator 是Netscape Communications Corporation 在美国和其他国家的注册商标。

GateD 和NextHop 是NextHop 在美国和其他国家的商标或注册商标。

Motif, OSF/1, 和UNIX 是The Open Group 在美国和其他国家的注册商标; IT DialTone 和The Open Group 是其商标。

Oracle 是Oracle Corporation 的注册商标。

PowerQuest 和PartitionMagic 是PowerQuest Corporation 在美国和/或其他国家的注册商标。

RealNetworks, RealPlayer, 和RealAudio 是RealNetworks, Inc. 的注册商标。

Red Hat, RPM, 是Red Hat, Inc. 在美国和其他国家的注册商标。

SAP, R/3, 和mySAP 是SAP AG 在德国以及许多其他国家的商标或注册商标。

Sun, Sun Microsystems, Java, Java Virtual Machine, JavaServer Pages, JDK, JSP, JVM, Netra, Solaris, StarOffice, Sun Blade, Sun Enterprise, Sun Fire, SunOS, 和Ultra 是Sun Microsystems, Inc. 在美国和其他国家的商标或注册商标。

Symantec 和Ghost 是Symantec Corporation 在美国和其他国家的注册商标。

MATLAB 是The MathWorks, Inc. 的注册商标。

SpeedTouch 是Thomson 的商标。

U.S. Robotics 和Sportster 是U.S. Robotics Corporation 的注册商标。

VMware 是VMware, Inc. 的商标

Waterloo Maple 和Maple 是Waterloo Maple Inc 的商标或注册商标

Mathematica 是Wolfram Research, Inc 的注册商标。

XFree86 是The XFree86 Project, Inc 的商标。.

Ogg Vorbis 和Xiph.Org 是Xiph.Org 的商标。

许多制造商和经销商使用一些称为商标的图案或文字设计来彰显自己的产品。本文档中出现的, 为FreeBSD Project 所知晓的商标, 后面将以'™' 或'®' 符号来标注。

目录

前言	xiv
I. 起步	xx
1 介绍	1
1.1 概述	1
1.2 欢迎来到FreeBSD 的世界!	1
1.3 关于FreeBSD 项目	3
2 安装FreeBSD	8
2.1 概述	8
2.2 安装前的准备工作	8
2.3 开始安装	14
2.4 介绍Sysinstall	22
2.5 分配磁盘空间	27
2.6 选择要安装的软件包	37
2.7 选择您要使用的安装介质	39
2.8 安装确认	41
2.9 安装后的配置	42
2.10 支持的硬件	80
2.11 常见问题	81
2.12 高级安装指南	83
2.13 准备您自己的安装介质	84
3 UNIX 基础	89
3.1 概述	89
3.2 虚拟控制台和终端	89
3.3 权限	92
3.4 目录架构	94
3.5 磁盘组织	95
3.6 文件系统的挂接和卸下	101
3.7 进程	104
3.8 守护进程, 信号和杀死进程	105
3.9 Shells	107
3.10 文本编辑器	108
3.11 设备和设备节点	109
3.12 二进制文件格式	109
3.13 取得更多的资讯	111
4 安装应用程序: Packages 和Ports	113
4.1 概述	113
4.2 软件安装预览	113
4.3 寻找您要的应用程序	114
4.4 使用Packages系统	115
4.5 使用Ports Collection	118
4.6 安装之后的待办事宜	124
4.7 如何处理坏掉的Ports	125
5 X Window 系统	127
5.1 概述	127
5.2 理解X	127

5.3 安装X11	129
5.4 配置X11	131
5.5 在X11 中使用字体	134
5.6 X 显示管理器	137
5.7 桌面环境	140
II. 常见的任务	145
6 桌面应用	146
6.1 概述	146
6.2 浏览器	146
6.3 办公、图象处理	149
6.4 文档查看器	151
6.5 财务	153
6.6 总结	154
7 多媒体	156
7.1 概述	156
7.2 安装声卡	156
7.3 MP3音频	160
7.4 视频回放	163
7.5 安装电视卡	170
7.6 图象扫描仪	171
8 配置FreeBSD的内核	176
8.1 概述	176
8.2 为什么需要建立定制的内核?	176
8.3 建立并安装一个定制的内核	176
8.4 配置文件	179
8.5 创建设备节点	191
8.6 如果出现问题怎么办	192
9 打印	194
9.1 概述	194
9.2 介绍	194
9.3 基本设置	195
9.4 高级设置	207
9.5 使用打印机	232
9.6 替换标准打印池	239
9.7 疑难问题	240
10 Linux二进制兼容模式	243
10.1 概述	243
10.2 安装	243
10.3 安装Mathematica®	246
10.4 安装Maple™	248
10.5 安装MATLAB®	250
10.6 安装Oracle®	252
10.7 安装SAP® R/3®	255
10.8 高级主题	274

III. 系统管理	276
11 设置和调整	277
11.1 概述	277
11.2 初步配置	277
11.3 核心配置	278
11.4 应用程序配置	279
11.5 启动服务	279
11.6 配置cron	281
11.7 在FreeBSD 5.X 和更新版本中使用rc	283
11.8 设置网卡	284
11.9 虚拟主机	288
11.10 配置文件	289
11.11 用sysctl 进行调整	293
11.12 调整磁盘	293
11.13 调整内核限制	296
11.14 添加交换空间	299
11.15 电源和资源管理	300
11.16 使用和调试FreeBSD ACPI	301
12 FreeBSD 引导过程	308
12.1 概述	308
12.2 引导问题	308
12.3 引导管理器和各引导阶段	309
12.4 内核在引导时的交互	312
12.5 Device Hints	313
12.6 Init: 进程控制及初始化	314
12.7 shutdown 队列	315
13 用户和基本的帐户管理	316
13.1 概述	316
13.2 介绍	316
13.3 超级用户帐户	317
13.4 系统帐户	317
13.5 用户帐户	318
13.6 修改帐户	318
13.7 限制用户使用系统资源	323
13.8 组	325
14 安全	327
14.1 概述	327
14.2 介绍	327
14.3 确保FreeBSD 的安全	329
14.4 DES, MD5, 以及Crypt	334
14.5 一次性口令	335
14.6 TCP Wrappers	340
14.7 KerberosIV	342
14.8 Kerberos5	349
14.9 OpenSSL	356
14.10 IPsec 上的VPN	358
14.11 OpenSSH	368
14.12 文件系统访问控制表	373

14.13	监视第三方安全问题	374
14.14	FreeBSD 安全公告	375
14.15	进程记帐	377
15	集权式访问控制	379
15.1	概要	379
15.2	本章出现的重要术语	380
15.3	关于MAC 的说明	380
15.4	理解MAC 标签	381
15.5	模块配置	386
15.6	MAC bsdextended 模块	386
15.7	MAC ifoff 模块	387
15.8	MAC portacl 模块	388
15.9	包含标签功能的MAC 策略	389
15.10	MAC partition (分区) 模块	390
15.11	MAC Multi-Level 安全模块	391
15.12	MAC Biba 模块	392
15.13	MAC LOMAC 模块	393
15.14	通过使用MAC 来实现安全的环境	394
15.15	另一个例子: 使用MAC 来约束Web 服务器	399
15.16	MAC 框架的故障排除	400
16	安全事件审计	402
16.1	概述	402
16.2	您需要了解的一些关键术语	402
16.3	安装审计支持	403
16.4	对审计进行配置	403
16.5	管理事件审计	405
17	存储	407
17.1	概述	407
17.2	设备命名	407
17.3	添加磁盘	408
17.4	RAID	410
17.5	USB 存储设备	414
17.6	创建和使用光学介质(CD)	416
17.7	创建和使用光学介质(DVD)	421
17.8	创建和使用软盘	425
17.9	用磁带机备份	427
17.10	用软盘备份	429
17.11	备份策略	430
17.12	备份程序	431
17.13	网络、内存和File-Backed 文件系统	437
17.14	文件系统快照	440
17.15	文件系统配额	441
17.16	加密磁盘分区	444
17.17	对交换区进行加密	449
18	GEOM: 模块化磁盘变换框架	452
18.1	概述	452
18.2	GEOM 介绍	452
18.3	RAID0 - 条带	452

18.4 RAID1 - 镜像	454
19 Vinum 卷管理程序	457
19.1 概述	457
19.2 磁盘容量太小	457
19.3 访问瓶颈	457
19.4 数据的完整性	459
19.5 Vinum 目标	460
19.6 一些例子	461
19.7 对象命名	467
19.8 配置Vinum	469
19.9 使用Vinum 作为根文件系统	470
20 本地化—I18N/L10N使用和设置	476
20.1 概述	476
20.2 基础知识	476
20.3 使用本地化语言	477
20.4 编译I18N程序	482
20.5 本地化FreeBSD	482
21 最前沿	486
21.1 概述	486
21.2 FreeBSD-CURRENT 和FreeBSD-STABLE 的对比	486
21.3 同步您的源码	489
21.4 重新编译 “world”	490
21.5 跟踪多台机器	502
IV. 网络通讯.....	504
22 串口通讯	505
22.1 概述	505
22.2 介绍	505
22.3 终端	510
22.4 拨入服务	513
22.5 拨出设备	520
22.6 设置串行控制台	523
23 PPP 和SLIP	531
23.1 概述	531
23.2 使用用户级PPP.....	531
23.3 使用内核级PPP.....	542
23.4 PPP 连接故障排除.....	549
23.5 使用基于以太网的PPP(PPPoE).....	552
23.6 Using PPP over ATM (PPPoA).....	554
23.7 使用SLIP	556
24 电子邮件	566
24.1 概述	566
24.2 使用电子邮件	566
24.3 sendmail 配置	568
24.4 改变您的邮件传输代理程序	570
24.5 疑难解答	573
24.6 高级主题	576
24.7 SMTP 与UUCP	578

24.8	只发送邮件的配置	579
24.9	拨号连接时使用邮件传送	580
24.10	SMTP 验证	581
24.11	邮件用户代理	582
24.12	使用fetchmail	589
24.13	使用procmail	590
25	网络服务器	592
25.1	概要	592
25.2	inetd “超级服务器”	592
25.3	网络文件系统 (NFS)	596
25.4	网络信息服务(NIS/YP)	600
25.5	网络自动配置(DHCP)	615
25.6	域名系统(DNS)	619
25.7	BIND9 和FreeBSD	630
25.8	Apache HTTP 服务器	632
25.9	文件传输协议(FTP)	636
25.10	为Microsoft® Windows 客户机提供文件和打印服务(Samba)	637
25.11	通过NTP 进行时钟同步	639
26	防火墙	642
26.1	入门	642
26.2	防火墙的概念	642
26.3	防火墙软件包	642
26.4	OpenBSD Packet Filter (PF) 和ALTQ	643
26.5	IPFILTER (IPF) 防火墙	645
26.6	IPFW	663
27	高级网络	679
27.1	概述	679
27.2	网关和路由	679
27.3	无线网络	685
27.4	蓝牙	691
27.5	桥接	698
27.6	无盘操作	700
27.7	ISDN	707
27.8	网络地址转换	711
27.9	并口电缆IP (PLIP)	714
27.10	IPv6	715
27.11	异步传输模式(ATM)	720
V.	附录	722
A.	获取FreeBSD	723
A.1	CDROM 和DVD 发行商	723
A.2	FTP 站点	726
A.3	匿名CVS	736
A.4	使用CTM	738
A.5	使用CVSup	741
A.6	使用Portsnap	763
A.7	CVS 标签	765
A.8	AFS 站点	769

A.9 rsync 站点.....	770
B. 参考文献	772
B.1 关于FreeBSD 的专业书籍与杂志	772
B.2 用户指南.....	773
B.3 管理员指南.....	773
B.4 开发指南.....	774
B.5 操作系统原理.....	774
B.6 信息安全方面的参考文献.....	775
B.7 硬件参考.....	775
B.8 UNIX 历史.....	776
B.9 各种期刊.....	776
C. Internet上的资源.....	778
C.1 邮件列表.....	778
C.2 Usenet新闻组.....	792
C.3 World Wide Web服务器.....	793
C.4 Email地址	801
C.5 Shell账号	801
D. PGP公钥.....	802
D.1 官员	802
D.2 核心团队成員	802
D.3 开发者	803
索引	843
Colophon.....	855

表格清单

2-1. 硬件设备清单	8
2-2. 为第一个硬盘分区	32
2-3. 为其它磁盘分区	33
2-4. 可能的安全等级	49
2-5. FreeBSD 4.X ISO 映像文件名和含意	84
2-6. FreeBSD 5.X ISO 映像文件名和含意	84
3-1. 磁盘设备的代码	100
17-1. 物理磁盘命名规则	407
19-1. Vinum Plex组织图	461
22-1. DB-25 to DB-25 Null-Modem Cable	506
22-2. DB-9 到DB-9 Null-Modem 电缆.....	506
22-3. DB-9 到DB-25 Null-Modem 电缆.....	507
22-4. 信号名称	514
27-1. 用于网络连接的并口电缆接线方式	714
27-2. 保留的IPv6 地址.....	716

前言

Intended Audience

作为FreeBSD的新用户，您将会在本手册第一部分找到FreeBSD的安装方法，同时逐渐引入概念和习俗来加强UNIX®基础。阅读这部分只需要您有探索的精神和接受新概念的能力。

读完这些之后，手册中很漫长的第二部分是FreeBSD中系统管理员感兴趣的所有主题的全面参考。在阅读这些章节的内容时所需要的背景知识都注释在每一章节的大纲里面，如果需要，可在阅读前进行预习。

要获得附加的信息来源列表，请查阅附录B。

相对于第二版的改动

您目前看到的这本手册的第三版是FreeBSD文档计划的成员历时两年完成的顶峰之作。第三版包含了如下的主要变动：

- 第11章，配置和优化，进行了扩充并增加了关于ACPI电源和资源管理，cron系统实用程序，以及更多的内核优化选项的相关内容。
- 第14章，安全一章增加了虚拟专用网(VPNs)，文件访问控制表(ACLs)，以及安全公告的内容。
- 第15章，强制访问控制(MAC)是这一版新增的章节。它解释了什么是MAC，以及这一机制如何使您的FreeBSD系统更安全。
- 第17章，存储，在原有基础上增加了USB存储设备，文件系统快照，文件系统容限，基于文件及网络的文件系统，以及与加密磁盘分区有关的内容。
- 第19章，Vinum，是这一版中的新章节。描述了如何使用这种提供了设备无关的逻辑磁盘、软件RAID-0, RAID-1和RAID-5的卷管理系统Vinum。
- 在第23章，PPP和SLIP一章中增加了排除故障的说明。
- 第24章，电子邮件一章中增加了关于如何使用其它的邮件传输代理、SMTP认证，UUCP, fetchmail, procmail, 以及其它进阶内容。
- 第25章，网络服务，是新版中全新的一章。这一章包括了如何架设Apache HTTP服务器，FTPd，以及用于支持Microsoft Windows客户的Samba。一些段落来自原先的第27章，进阶网络应用一章。
- 第27章，进阶网络应用一章增加了关于在FreeBSD中使用蓝牙设备，安装无线网络，以及使用异步传输模式(ATM)网络的内容。
- 增加了一份词汇表，用以说明整本书中出现的术语。
- 对于全书中图表进行了进一步的美化工作。

相对于第一版的改变

本手册的第二版是FreeBSD文档计划的成员历时两年完成的顶峰之作。第二版包含了如下的主要变动：

- 添加了完整的索引。
- 用图形替换了以前所有用ASCII插图。

- 每个章节添加了标准大纲，列出了该章所包含的信息和读者所应该了解的知识。
- 内容逻辑地分成三个部分：“起步”，“系统管理”和“附录”。
- 第2章(“安装FreeBSD”)新版本中使用了抓屏图片，使新用户更容易的领会正文。
- 第3章(“UNIX 基础”)扩充了进程、守护进程和信号的附加信息。
- 第4章(“安装应用程序”)扩充了二进制包管理的附加信息。
- 第5章(“X Window 系统”)新版本中着重介绍使用现代桌面技术例如XFree86TM 4.x 上的**KDE**和**GNOME**
- 第12章(“FreeBSD 启动过程”)对第一版内容进行扩充。
- 第17章(“存储”)由第一版中两个单独的章节“磁盘”和“备份”合并而成。我们认为这两部分作为一个整体比较容易理解。同时RAID (包括硬件和软件RAID) 部分也被添加进来。
- 第22章(“串口通信”)对第一版进行完善，并为FreeBSD 4.x/5.x 做了更新。
- 第23章(“PPP 和SLIP”)全部更新。
- 许多新的内容被添加到第27章(“高级网络”)。
- 第24章(“电子邮件”)增加了关于配置**sendmail** 的信息。
- 第10章(“Linux® 兼容性”)增加了关于安装**Oracle®** 和**SAP® R/3®** 的信息。
- 第二版中也涵盖了下列主题:
 - 配置和调整(第11章)。
 - 多媒体(第7章)

本手册的组织

这本手册分成了三个逻辑清晰的部分。第一部分**起步** 涵盖了FreeBSD 的安装和基本使用方法。读者可根据自己的情况按顺序或者跳过一些熟悉的主题来阅读。第二部分**常用操作** 涵盖了FreeBSD 常用的功能，这部分可以不按顺序阅读。每个部分由一个简明的大纲开始，这个大纲描述本章节涵盖的内容和读者应该已经知道的知识。这主要是让读者可以更好的选择感兴趣的章节阅读。第三部分**系统管理** 涵盖了FreeBSD 高级用户所感兴趣的广泛的话题。第四部分**网络通讯** 包括了网络和服务的话题，而第五部分则是资源信息的附录。

第1章，介绍

向新用户介绍FreeBSD。它描述了FreeBSD 计划的历史、目标和开发模式。

第2章，安装

本章将会带领用户完成安装过程。一些高级安装主题，例如如何通过串行控制台安装，也涵盖在内。

第3章，UNIX 基础

本章涵盖了FreeBSD 操作系统基础命令和功能。如果熟悉Linux 或者其他类UNIX 操作系统，则可以跳过这章。

第4章，安装应用程序

本章涵盖如何用FreeBSD的“Ports Collection”和标准二进制软件包来安装第三方软件。

第5章，X Window 系统

本章概要地描述了X Window System系统并详细地介绍了如何在FreeBSD上使用它。此外他也描述了常用的桌面环境，例如**KDE**和**GNOME**。

第6章，桌面应用

列出了一些常用的桌面应用程序，比如web浏览器和办公套件，描述了在FreeBSD上如何安装它们。

第7章，多媒体

展示了如何为您的系统设置声卡和视频回放支持。也描述了一些简单的音频和视频应用程序。

第8章，配置FreeBSD内核

解释了为什么需要配置一个新内核并提供了配置、编译、安装自定义内核的详细说明。

第9章，打印

描绘了FreeBSD上打印机管理，包括横幅页、打印统计，还有初始的设置。

第10章，Linux 二进制兼容

描述了FreeBSD的Linux兼容特性。也提供了许多流行的Linux应用程序的详细安装说明，比如**Oracle**、**SAP R/3**，还有**Mathematica®**。

第11章，配置和调整

本章描述了管理员调整FreeBSD系统以优化性能时可能用到的一些参数。也描述了FreeBSD中的各种配置文件以及它们所在的位置。

第12章，启动过程

本章描述FreeBSD的启动过程并且解释了如何用配置选项来控制这个过程。

第13章，用户和基本帐号管理

本章描述了如何创建和操作用户帐号，同样也论述了设置用户资源限制和其他帐号管理任务的方法。

第14章，安全

描述了保证FreeBSD系统安全可以使用的许多工具，这包括Kerberos，IPsec以及OpenSSH。

第15章，强制访问控制

解释了何谓强制访问控制(MAC)以及如何利用这一机制来加强FreeBSD系统的安全。

第17章，存储

本章描述了怎样用FreeBSD来管理存储介质和文件系统，包括物理磁盘、RAID阵列、光学和磁带媒体、后备存储磁盘以及网络文件系统。

第18章，GEOM

介绍了FreeBSD中的GEOM框架是什么，以及如何配置它所支持的各级RAID。

第19章, Vinum

本章描述了怎样使用逻辑卷管理器Vinum。它提供了设备无关的逻辑磁盘和软件RAID-0、RAID-1以及RAID-5。

第20章, 本地化

本章描述了如何在FreeBSD上使用非英语语言。它涵盖了系统和应用程序级的本地化。

第21章, 最前沿

介绍了FreeBSD-STABLE、FreeBSD-CURRENT以及FreeBSD发行版本之间的差异。描述了一般用户如何紧跟开发过程并从中受益。

第22章, 串行通信

本章解释了如何连接终端和调制解调器到FreeBSD系统, 包括拨入和拨出连接。

第23章, PPP和SLIP

本章描述了如何用FreeBSD通过使用PPP, SLIP或者基于以太网的PPP(PPPoE)来连接远程系统。

第24章, 电子邮件

本章解释了一个email服务器的不同组成部分并且简单讨论了关于最流行的mail服务器软件sendmail的配置。

第25章, 网络服务

提供了详细的指引和示范配置文件以说明如何将一台FreeBSD机器作为网络文件系统服务器, 域名服务器, 网络信息服务器或时间同步服务器来使用的方法。

第26章, 防火墙

解释了基于软件的防火墙的原理, 并提供了关于配置FreeBSD上的几种防火墙的详细说明。

第27章, 高级网络应用

描述了许多关于网络的主题, 包括如何在您的局域网中共享Internet连接, 高级路由话题, 无线网络, 蓝牙, ATM, IPv6以及许多高级话题。

附录A, 获取FreeBSD

列出了获得FreeBSD安装CDROM或DVDROM的不同资源, 也提供了允许您自由下载FreeBSD的不同Internet站点。

附录B, 参考书目

由于本手册触及到了很多不同的主题, 因而可能引发您想要获取更多详细的讲解。参考书目列出了很多写作这本书时参考的好书。

附录C, Internet上的资源

讲述了很多对FreeBSD用户有用的能够提出问题并进行技术交流的关于FreeBSD的论坛。

附录D, PGP秘钥

列出了一些FreeBSD开发者的PGP签名。

本书中使用的一些约定

为了使本书保持一致性和易读性特做了以下约定：

排版约定

斜体

斜体 字用来表示文件名、URLs、强调文字和术语的主流用法。

等宽

等宽 字体用来表示错误信息、命令、环境变量、port 的名字、主机名、用户名、组名、设备名、变量名，以及代码片断。

粗体

粗体 字用来表示应用程序、命令和关键字。

用户输入

按键用**粗体**来突出于其他文本。组合键意味着字用‘+’连接时，同时的按下它们，例如：

Ctrl+Alt+Del

表示您应该同时按下**Ctrl**，**Alt** 和**Del** 键。

按顺序依次键入的关键字通常是用逗号隔开，例如：

Ctrl+X, Ctrl+S

这意味着用户应该同时按**Ctrl** 和**X**，然后同时按**Ctrl** 和**S**。

示例

以E:\> 开头的例子代表一个MS-DOS® 命令。除非另有说明，这些命令都可以在一个现代的Microsoft® Windows® “命令行” 窗口环境被执行。

E:\> **tools\fdimage floppies\kern.flp A:**

以# 开头的例子代表必须以FreeBSD 超级用户身份执行的命令。您可以用root 身份登录来输入这些命令，或者以普通账号登录然后用su(1) 来获得超级用户权限。

dd if=kern.flp of=/dev/fd0

以% 开头的例子代表命令应该被普通账号执行。除非另有说明，C-shell 语法来设置环境变量和其他shell 命令。

% **top**

致谢

您所看到的这本书是全球几百人努力的结果。无论他们只是纠正一些错误或提交完整的章节，所有的贡献都是非常有用的。

一些公司通过提供资金让作者专注于文档开发、提供出版资金等等方式来支持文档开发。其中，BSDi (后并入Wind River Systems (<http://www.windriver.com>)) 资助FreeBSD 文档计划成员来专职改善这本书直到2000年三月第一个印刷版(ISBN 1-57176-241-8) 的出版。Wind River Systems 同时资助其他作者来对输出结构做很多改进和给文章添加一些附加章节。这项工作结束于2001年11月印刷第二版(ISBN 1-57176-303-1)。在2003-2004两年中，FreeBSD Mall (<http://www.freebsdmail.com>)，向为改进这本手册以使其第三版印刷版本能够出版的志愿者支付了报酬。

I. 起步

手册的以下章节主要是针对刚开始使用FreeBSD 的用户及管理员:

- FreeBSD 入门。
- 安装过程向导。
- 教您UNIX 基本知识和基本原理。
- 展示如何在FreeBSD 上安装大量的第三方应用。
- 介绍使用X, UNIX 窗口系统, 以及为一些生产环境配置桌面环境的细节。

我们尝试用最少的页数来保持前言的索引, 以至于可以用最少翻页次数将该手册从头至尾读过。

第1章

介绍

Restructured, reorganized, and parts rewritten by Jim Mock.

1.1 概述

非常感谢您对FreeBSD 感兴趣！下面的章节覆盖了FreeBSD 项目的各个方面，比如它的历史、目标、开发模式，等等。

阅读完这章，您将了解：

- FreeBSD 与其它计算机操作系统的关系。
- FreeBSD 项目的历史。
- FreeBSD 项目的目标。
- FreeBSD 开放源代码开发模式的基础。
- 当然还有：“FreeBSD” 这个名称的由来。

1.2 欢迎来到FreeBSD 的世界！

FreeBSD 是一个支持Intel (x86 和Itanium®), AMD64, Alpha™, Sun UltraSPARC® 计算机的基于4.4BSD-Lite 的操作系统。到其他体系结构的移植也在进行中。您也可以阅读FreeBSD 的历史，或者最新的发行版本。如果您有意捐助(代码，硬件，不记名捐款)，请看为FreeBSD 提供帮助 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/contributing/index.html)这篇文章。

1.2.1 FreeBSD 能做些什么？

FreeBSD有许多非凡的特性。其中一些是：

- **抢占式多任务**与动态优先级调整确保在应用程序和用户之间平滑公正的分享计算机资源，即使工作在最大的负载之下。
- **多用户设备** 使得许多用户能够同时使用同一FreeBSD 系统做各种事情。比如，像打印机和磁带驱动器这样的系统外设可以完全的在系统或者网络上的所有用户之间共享，可以对用户或者用户组进行个别的资源限制，以保护临界系统资源不被滥用。
- 符合业界标准的强大**TCP/IP 网络** 支持，例如SLIP, PPP, NFS, DHCP, 还有NIS。这意味着您的FreeBSD 主机可以很容易地和其他系统互联，也可以作为企业的服务器，提供重要的功能，比如NFS(远程文件访问)以及email 服务，或将您的组织接入Internet 并提供WWW, FTP, 路由和防火墙(安全)服务。
- **内存保护**确保应用程序(或者用户)不会相互干扰。一个应用程序崩溃不会以任何方式影响其他程序。
- FreeBSD 是一个**32 位**操作系统(在Alpha, Itanium, AMD64, 和UltraSPARC 上是**64 位**)，并且从开始就是如此设计的。

- 业界标准的**X Window 系统 (X11R6)**为便宜的常见VGA 显示卡和监视器提供了一个图形化的用户界面(GUI), 并且完全开放代码。
- 和许多Linux, SCO, SVR4, BSDI 和NetBSD 程序的**二进制代码兼容性**
- 数以千计的**ready-to-run** 应用程序可以从FreeBSD **ports** 和**packages collection** 中找到。您可以顺利的从这里找到, 何用搜索网络?
- 可以在Internet 上找到成千上万其它**easy-to-port** 的应用程序。FreeBSD 和大多数流行的商业UNIX 代码级兼容, 因此大多数应用程序不需要或者只要很少的改动就可以编译。
- 页式请求**虚拟内存**和“集成的VM/buffer 缓存”设计有效的满足了应用程序巨大的内存需求并依然保持其他用户的交互式响应。
- **SMP** 提供对多处理器的支持。
- **C, C++, Fortran,** 和**Perl** 开发工具的完整扩充。许多附加的用于高级研究和开发的程序语言也可以在ports 和packages collection 中找到。
- 完整的系统**源代码**意味着您对您环境的最大程度的控制。当您拥有了一个真正的开放系统时, 为什么还要受困于私有的解决方案, 任商业公司摆布呢?
- 丰富的**在线文档**。
- **不仅如此!**

FreeBSD 基于加州大学伯克利分校计算机系统研究组(CSRG)发布的4.4BSD-Lite, 继承了BSD 系统开发的优良传统。除了CSRG 优秀的工作之外, FreeBSD 项目花费了非常多的时间来优化调整系统, 使其在真实负载情况下拥有最好的性能和可靠性。像许多商业巨人努力地增加PC 操作系统的特性、提升性能并改善其可靠性一样, FreeBSD **现在** 就已经可以提供了!

FreeBSD 可以提供的应用事实上仅局限于您的想象力。从软件开发到工厂自动化, 从存货控制到遥远的人造卫星天线方位控制, 如果商业的UNIX 产品可以做到, 那么就非常有可能您也可以**用FreeBSD** 来做! FreeBSD 也极大地受益于全世界的研究中心和大学开发的数以千计的高质量的应用程序, 这些程序通常只需要很少的花费甚至免费。商业应用程序也是可用的, 并且每天都有大量的出现。

因为FreeBSD 自身的源代码是完全公开的, 所以对于特定的应用程序或项目, 可以对系统进行最大限度的定制。这对于大多数主流的商业生产商的操作系统来说几乎是不可能的。以下是当前人们应用FreeBSD 的某些程序的例子:

- **Internet 服务:** FreeBSD 内建的强大的TCP/IP 网络使它得以成为各种Internet 服务的理想平台, 比如:
 - FTP 服务器
 - World Wide Web 服务器(标准的或者安全的[SSL])
 - 防火墙和NAT(“IP 伪装”) 网关
 - 电子邮件服务器
 - USENET 新闻组和电子布告栏系统
 - 还有许多...

使用FreeBSD, 您可以容易的从便宜的386 类PC 起步, 并随着您的企业成长, 一路升级到带有RAID 存储的四路Xeon 服务器。

- **教育:** 您是一名计算机科学或者相关工程领域的学生吗? 学习操作系统, 计算机体系结构和网络没有比在FreeBSD 可提供的体验下动手实践更好的办法了。许多可自由使用的CAD、数学和图形设计包也使它对于那些主要兴趣是在计算机上完成**其他**工作的人非常有帮助。

- **研究：**有完整的系统源代码，FreeBSD 对于操作系统研究以及其他计算机科学分支都是一个极好的平台。FreeBSD 可自由获得的本性，同样可以使处在不同地方的开发团队在开放的论坛上讨论问题、交流想法与合作开发成为可能，且不必担心特别的版权协定或者限制。
- **网络：**需要一个新的路由器？一台域名服务器(DNS)？一个隔离您的内部网络的防火墙？FreeBSD 可以容易的把丢弃在角落不用的386 或者486 PC 变成一台完善的带包过滤能力的高级路由器。
- **X Window 工作站：**FreeBSD 是廉价X 终端的一种绝佳解决方案，您可以选择使用免费的X11 服务器，或由Xi Graphics (<http://www.xig.com>) 提供的非常优秀的商业服务器。与X 终端不同，如果需要的话FreeBSD 能够在本地直接运行程序，因而减少了中央服务器的负担。FreeBSD 甚至能够在“无盘”环境下启动，这使得终端更为便宜和易于管理。
- **软件开发：**基本的FreeBSD 系统带有包括著名的GNU C/C++ 编译器和调试工具在内的一整套开发工具。

FreeBSD 可以通过CDROM、DVD，以及匿名FTP 以源代码和二进制方式获得。请查看附录A 了解获取FreeBSD 的更多细节。

1.2.2 谁在使用FreeBSD？

FreeBSD 用来支持Internet 上一些最大的站点，包括：

- Yahoo! (<http://www.yahoo.com/>)
- Apache (<http://www.apache.org/>)
- Blue Mountain Arts (<http://www.bluemountain.com/>)
- Pair Networks (<http://www.pair.com/>)
- Sony Japan (<http://www.sony.co.jp/>)
- Netcraft (<http://www.netcraft.com/>)
- Weathernews (<http://www.wni.com/>)
- Supervalu (<http://www.supervalu.com/>)
- TELEHOUSE America (<http://www.telehouse.com/>)
- Sophos Anti-Virus (<http://www.sophos.com/>)
- JMA Wired (<http://www.jmawired.com/>)

等等许多。

1.3 关于FreeBSD 项目

下面的章节提供了项目的一些背景信息，包括简要的历史、项目目标、以及项目开发模式。

1.3.1 FreeBSD 的简要历史

Contributed by Jordan Hubbard.

FreeBSD 项目起源于1993 年早期，部分作为“Unofficial 386BSD Patchkit” 的副产物，patchkit 的最后3 个协调维护人是：Nate Williams, Rod Grimes 和我。

我们最初的目标是做出一份386BSD的测试版以修正一些Patchkit机制无法解决的错误(bug)。很多人可能还记得早期的项目名称叫做“386BSD 0.5”或者“386BSD Interim”就是这个原因。

386BSD是Bill Jolitz的操作系统，一直到忍受了激烈的将近一年的忽视。由于Patchkit的急剧膨胀，使得很难每天都能够消化吸收，我们一致同意应该做些事情并决定通过提供这个临时的“cleanup”版本来帮助Bill。然而，Bill却在事先没有指出这个项目应该如何开展下去的情况下，突然决定退出这个项目，最终这个计划只好被迫停止。

没过多久，我们认为在没有Bill的支持下，项目仍有保留的价值，因此，我们采用了David Greenman的意见，给其命名为“FreeBSD”。在和当时的几个用户商量后，我们提出了最初的目标，而这件事明朗化后，这个项目就走上了正轨，甚至可能成为现实。为了增加FreeBSD的发行渠道，我抱着试试看的心态，联系了光盘商Walnut Creek CDROM，以便那些上网不方便的用户得到FreeBSD。Walnut Creek CDROM不仅支持发行FreeBSD光盘版的想法，还为这个计划提供了所需的计算机和高速网络接入。在那时，没有Walnut Creek CDROM对一个完全未知的项目的空前信任，FreeBSD不太可能像它今天这样，影响如此深远，发展如此快速。

第一个CDROM(以及在整个互连网范围内发行的)发行版本是FreeBSD 1.0，于1993年10月发布。这个版本基于U.C. Berkeley的4.3BSD-Lite(“Net/2”)磁带，也有许多组件是386BSD和自由软件基金会提供的。对于第一次发行，这算是相当成功了。在1994年5月，我们发布了更加成功的FreeBSD 1.1版。

然而此后不久，发生了一些意外的情况。Novell和U.C. Berkeley决定就Berkeley Net/2磁带的归属权问题打的那场马拉松式的官司达成和解。判决的结果是，U.C. Berkeley承认Net/2很大一部分代码是“侵占来的”且这些代码归Novell公司所拥有。这些代码是Novell不久前从AT&T买来的。Berkeley得到了来自Novell的“祝福”：4.4BSD-Lite发行后，将不认为是侵权，且要求现存的Net/2的用户更换新版。这也包括FreeBSD，我们的项目被要求在1994年6月底停止发行基于Net/2的产品。在此协议允许的的时间内，本项目被允许发行最后一版，也就是FreeBSD 1.1.5.1。

于是FreeBSD开始艰苦的从全新的而且不完整的4.4BSD-Lite中重新整合自己。“Lite”版本是不完整的，因为Berkeley的CSRG已经删除了大量的构建可启动运行的系统所需要的代码(因为各种各样的版权问题)，事实上4.4的Intel port是非常不完整的。直到1994年11月项目才完成这个转换，这个时候才把FreeBSD 2.0通过网络和CDROM(在12月)发布出来。尽管系统很多地方还很粗糙，这个版本还是取得了重大的成功，接下来在1995年6月发布了更强大和容易安装的FreeBSD 2.0.5版本。

我们于1996年8月发布了FreeBSD 2.1.5版本，它在ISP和商业团体中非常流行。随后，2.1-STABLE分支的另一个版本应运而生，它就是FreeBSD 2.1.7.1，在1997年2月发布并停止了2.1-STABLE的主流开发。现在，它处于维护状态，仅仅提供安全性的增强和其他严重的错误修补的维护(RELENG_2_1_0)。

FreeBSD 2.2版作为RELENG_2_2分支，于1996年11月从开发主线(“-CURRENT”)分出来。它的第一个完整版(2.2.1)于1997年4月发布出来。97年夏秋之间，顺着2.2分支的更进一步的版本在开发。其最后一版(2.2.8)于1998年11月发布出来。第一个官方的3.0版本出现在1998年10月，意味着2.2分支结束的开始。

1999年1月20日又出现了新的分支，就是4.0-CURRENT和3.X-STABLE分支。从3.X-STABLE起，3.1在1999年2月15日发行，3.2在1999年5月15日，3.3在1999年9月16日，3.4在1999年12月20日，3.5在2000年6月24日，接下来几天后发布了很少的修补升级至3.5.1，加入了对Kerberos安全性方面的修补。这是3.X分支最后一个发行版本。

随后在March 13, 2000出现了一个新的分支，也就是4.X-STABLE。这之后发布了许多的发行版本：4.0-RELEASE于2000年3月发布，而最后的5.4-RELEASE则在May 2005发布。

期待已久的5.0-RELEASE于2003年1月19日正式发布。这是将近三年的开发的巅峰之作，同时也标志了FreeBSD在先进的多处理器和应用程序线程支持的巨大成就，并引入了对于UltraSPARC和ia64平台的支持。之后于2003年6月发布了5.1。最后一个-CURRENT分支的5.X版本是5.2.1-RELEASE，它在2004年2月正式发布。

RELENG_5 于2004 年8 月正式创建，其后是5.3-RELEASE，它是5-STABLE 分支的标志性发行版。最新的6.0-RELEASE 是在Nov 2005 发布的，RELENG_5 分支还将有后续的发行版。

目前，中长期的开发项目继续在6.X-CURRENT (trunk) 分支中进行，而6.X 的CDROM (当然，也包括网络) 快照版本可以在 快照服务器 (<ftp://current.FreeBSD.org/pub/FreeBSD/snapshots/>) 找到。

1.3.2 FreeBSD 项目目标

Contributed by Jordan Hubbard.

FreeBSD 项目的目标是无附加条件地提供能够用于任何目的的软件。我们中的许多人对代码(以及项目本身) 都有非常大的投入，因此当然不介意偶尔有一些资金上的补偿，但我们并没打算坚决地要求得到这类资助。我们认为我们的首要“使命” 是为任何人提供代码，不管他们打算用这些代码做什么，因为这样代码将能够被更广泛地使用，从而最大限度地发挥其价值。我认为这是自由软件最基本的，同时也是为我们所倡导的一个目标。

我们源代码树中，以GNU 公共许可证(GPL) 或者GNU 函数库公共许可证(LGPL) 发布的那些代码带有少许的附加限制，还好只是强制性的要求开放代码而不是别的。由于使用GPL 的软件在商业用途上会增加若干复杂性，因此，如果可以选择的话，我们更偏好使用限制相对更宽松的BSD 版权来发布软件。

1.3.3 FreeBSD 开发模式

撰写者Satoshi Asami.

FreeBSD 的开发是一个非常开放且有伸缩性的过程，就像从我们的 贡献者列表 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/contributors/article.html)里看到的，它是完全由来自全世界的数以百计的贡献者发展起来的。FreeBSD 的开发基础结构允许数以百计的开发者通过互联网协同工作。我们也经常关注着那些对我们的计划感兴趣的新开发者和新的创意，那些有兴趣更进一步参与项目的人只需要在FreeBSD 技术讨论邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-hackers>) 联系我们。FreeBSD 公告邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-announce>) 对那些希望了解我们工作所涉及到的哪些领域的人也是有用的。

无论是独立地工作或者封闭式的团队工作，了解FreeBSD计划和它的开发过程都是有益的：

CVS 代码库

FreeBSD 的中央源代码树是由CVS (<http://ximbiot.com/cvs/wiki/>) (并行版本控制系统)来维护的。CVS 是一个与FreeBSD 捆绑的可自由获得的源代码控制工具。主CVS 代码库 (<http://www.FreeBSD.org/cgi/cvsweb.cgi>)放置在美国加利福尼亚州圣克拉拉的一台机器上，它被复制到全世界的大量镜像站上。CVS 中包括了-CURRENT 和-STABLE 树，它同样可以很容易地复制到您的机器上。请查阅 同步您的源代码树这一章节来了解更多信息。

committer 列表

committer 是那些对CVS 树有写权限的人，他们被授权修改FreeBSD 的源代码(术语“committer” 来自于cvs(1) 的commit 命令，这个命令用来把新的修改提交给CVS 代码库)。提交修正的最好方法是使用send-pr(1) 命令。如果您发现在系统中出现了一些问题的话，您也可以通过邮件将它们发送至FreeBSD committer 的邮件列表。

FreeBSD 核心团队

如果把FreeBSD项目看作一个公司，那么**FreeBSD 核心团队**就相当于董事会。核心团队的主要任务是提出总体上的发展计划，然后确定一个正确的方向。邀请那些富有献身精神和可靠的开发者加入到**committer**队伍中来也是核心团队的工作之一，这些新的成员将作为新核心团队成员和其他人一起继续前进。当前的核心团队是2004年7月从**committer**中选举产生的。选举每两年一次。

一些核心团队的成员还负责特定的责任范围，也就是说他们必须尽力确保某个子系统能工作正常。FreeBSD开发者的完整列表和他们的责任范围，请参见**贡献者列表** (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/contributors/article.html)

注意：核心团队的大部分成员加入FreeBSD开发的时候都是志愿的，并没有从项目中获得任何财政上的资助，所以“承诺”不应该被理解为“支持保证”。前面所述“董事会”的类推并不十分准确，或许更好的说法是，他们是一群愿意放弃他们的生活，投身于FreeBSD项目而非选择其个人更好的生活的人！

外围贡献者

事实上，最大的开发团队正是为我们提供反馈和错误修补的用户自己。FreeBSD的非集中式的开发者保持联系的主要方式就是预订FreeBSD技术讨论邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-hackers>)，很多事情在那里讨论。查看附录C了解众多FreeBSD邮件列表的更多信息。

FreeBSD 贡献者列表 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/contributors/article.html) 很长并在不断增长，为什么不加入它来为FreeBSD做贡献呢？

提供代码不是为这个计划做贡献的唯一方式；有一个更完整的需要做的事情的列表，可以参见FreeBSD项目网站 (<http://www.FreeBSD.org/index.html>)。

总的来说，我们的开发模式好像是一组没有拘束的同心圆。这种集中式的开发模式，主要是考虑到用户的方便，同时让他们能很容易地维护同一份软件，而不会把潜在的贡献者排除在外！我们的目标是提供一个包含有大量具有一致性应用程序的稳定的操作系统，以利于用户的安装和使用，——这种模式在完成目标的过程中工作得非常有效。

我们对于那些想要加入，成为FreeBSD开发者的期待是：具有如同当前其他人一样的投入，来确保持续的成功！

1.3.4 最新的FreeBSD 发行版本

FreeBSD是一个免费使用且带有完整源代码的基于4.4BSD-Lite的系统，它广泛运行于Intel i386TM、i486TM、Pentium®、Pentium Pro、Celeron®、Pentium II、Pentium III、Pentium 4(或者兼容系统)、XeonTM、DEC Alpha和Sun UltraSPARC的计算机系统上。它主要以加州大学伯克利分校的CSRG研究小组的软件为基础，并加入了NetBSD、OpenBSD、386BSD以及来自自由软件基金会的一些东西。

自从94年末我们的FreeBSD 2.0发行以来，FreeBSD的性能，可定制性，稳定性都有了令人瞩目的提高。最大的变化是通过整合虚拟内存/文件系统的高速缓存改进的虚拟内存系统，它不仅提升了性能，而且减少了FreeBSD对内存的需要，使得5 MB内存成为可接受的最小配置。其他的改进包括完整的NIS客户端和服务端的支持，事务式TCP协议支持，按需拨号的PPP，集成的DHCP支持，改进的SCSI子系统，ISDN的支持，ATM，FDDI，快速Gigabit以太网(1000 Mbit)支持，提升了最新的Adaptec控制器的支持和修补了很多的错误。

除了最基本的系统软件，FreeBSD 还提供了一个拥有成千上万广受欢迎的程序组成的软件的Ports Collection。到本书付印时，已有超过13,300 个ports (ports 包括从http(WWW) 服务器到游戏、程序设计语言、编辑器以及您能想到的几乎所有的东西)。完整的Ports Collection 大约需要440 MB 的存储空间。所有的只提供对原始代码的“修正”。这使得我们能够容易地更新软件，而且减少了老旧的1.0 Ports Collection 对硬盘空间的浪费。要编译一个port，您只要切换到您想要安装的程序的目录，输入make install，然后让系统去做剩下的事情。您要编译的每一个程序完整的原始代码可以从CDROM 或本地FTP 获得，所以您只需要编译您想要软件的足够的磁盘空间。几乎大多数的软件都提供了事先编译好的“package” 以方便安装，对于那些不希望从源代码编译他们自己的ports 的人只要使用一个简单的命令(pkg_add)就可以安装。有关package 和ports 的更多信息可以在第4 章中找到。

您可以在最近的FreeBSD 主机的/usr/share/doc 目录下找到许多有用的文件来帮助您安装及使用FreeBSD。您也可以用一个HTML 浏览器来查阅本地安装的手册，使用下面的URL：

FreeBSD 使用手册

`/usr/share/doc/handbook/index.html`

FreeBSD FAQ

`/usr/share/doc/faq/index.html`

您也可以查看在<http://www.FreeBSD.org/> 的主站上的副本。

第2章

安装FreeBSD

结构、组织重整, 部分重写Jim Mock. sysinstall 操作流程、屏幕抓图以及一般性文件Randy Pratt.

2.1 概述

FreeBSD 提供了一个以文字为主, 简单好用的安装程序, 叫做**sysinstall**。这是FreeBSD 默认使用的安装程序; 厂商如果想, 也可以提供适合自己需要的安装程序。本章说明如何使用**sysinstall** 来安装FreeBSD。

学习完本章之后, 您将会知道:

- 如何制作FreeBSD 安装磁盘
- FreeBSD如何参照及分割您的硬盘
- 如何启动**sysinstall**.
- 在执行**sysinstall** 时您将要回答的问题、问题代表什么意义, 以及该如何回答它们。

在阅读本章之前, 您应该:

- 阅读您要安装的FreeBSD 版本所附的硬件支持列表以确定您的硬件有没有被支持。

注意: 一般来说, 此安装说明是针对i386 (“PC 兼容机”) 体系结构的电脑。如果有其它体系结构(如Alpha)的安装说明, 我们将一并列出。虽然本文档经常保持更新, 但有可能与您安装版本上所带的说明文档有些许出入。在这里建议您使用本说明文章作为一般性的安装指导参考手册。

2.2 安装前的准备工作

2.2.1 列出您电脑的硬件清单

在安装FreeBSD 之前, 您应该试着将您电脑中的硬件清单列出来。FreeBSD 安装程序会将这些硬件(磁盘、网卡、光驱等等)以及型号及制造厂商列出来。FreeBSD 也会尝试为这些设备找出最适当的IRQ 及IO 端口的设定。但是因为PC 的硬件种类实在太复杂, 这个步骤不一定总是能成功。这时, 您就可能需要手动更改有问题的设备的设定值。

如果您已经安装了其它的操作系统, 如Windows 或Linux, 那么您可以先由这些系统所提供的工具来查看您的设备设定值是怎么分配的。如果您真的没办法确定某些接口卡用什么设定值, 那么您可以检查看看, 说不定它的设定已经标示在卡上。常用的IRQ 号码为3、5 以及7; IO 端口的值通常以16 进制位表示, 例如Ox330。

我们建议您在安装FreeBSD 之前把这些信息打印或记录下来, 做成表格的样子也许会比较有帮助, 例如:

表2-1. 硬件设备清单

设备名	IRQ	IO 端口号	备注
第一块硬盘	N/A	N/A	40 GB, Seagate 制造, 第一个IDE 接口主设备
CDROM	N/A	N/A	第一个IDE 接口从设备
第二块硬盘	N/A	N/A	20 GB, IBM 制造, 第二个IDE 接口主设备
第一个IDE 控制器	14	0x1f0	
网卡	N/A	N/A	Intel® 10/100
Modem	N/A	N/A	3Com® 56K faxmodem, 位于COM1 口
...			

2.2.2 备份您的数据

如果您的电脑上面存有重要的数据资料, 那么在安装FreeBSD 前请确定您已经将这些资料备份了, 并且先测试这些备份文档是否有问题。FreeBSD 安装程序在要写入任何资料到您的硬盘前都会先提醒您确认, 一旦您确定要写入, 那么以后就没有反悔的机会。

2.2.3 决定要将FreeBSD 安装到哪里

如果您想让FreeBSD 使用整个硬盘, 那么请直接跳到下一节。

但是, 如果您想让FreeBSD 跟您已有的系统并存, 那么您必须对您数据存在硬盘的分布方式有深入的了解以及其所造成的影响。

2.2.3.1 i386™ 体系结构的硬盘分配方式

一个PC 硬盘可以被细分为许多分散的区域。这些区域叫做分区(*partitions*)。由于设计的原因, 每个硬盘仅支持四个分区; 这些分区叫做主分区(*Primary partion*)。为了突破这个限制以便能使用更多的分区, 就有了新的分区类型, 叫做 扩展分区(*Extended partition*)。一个硬盘可以拥有一个扩展分区。在扩展分区里可以建立许多个所谓的逻辑分区(*Logical partitions*)。

每个分区都有其独立的分区号(*partition ID*), 用以区分每个分区的数据类型。FreeBSD 分区的分区号为165。

一般而言, 每种操作系统都会有自己独特的方式来区别分区。例如DOS 及其之后的Windows, 会分配给每个主分区及逻辑分区一个驱动器字符, 从C: 开始。

FreeBSD 必须安装在主分区。FreeBSD 可以在这个分区上面存放系统数据或是您建立的任何文件。然而, 如果您有多个硬盘, 您也可以在这些硬盘上(全部或部分)建立FreeBSD 分区。在您安装FreeBSD 的时候, 必须要有一个分区可以给FreeBSD 使用。这个分区可以是尚未规划的分区或是已经划好, 但是里面的数据您都不想保存的分区。

如果您已经用完了您硬盘上的所有分区, 那么您必须使用其它操作系统所提供的工具(如DOS 或Windows 下的fdisk)来腾出一个分区给FreeBSD 使用。

如果您的某个分区有多余的空间, 您可以使用它。但是使用前您需要先整理一下这些分区。

FreeBSD 最小安装需要约100 MB 的空间, 但是这仅是非常基本的安装, 几乎没有剩下多少空间可以建立您自己的文件。一个较理想的最小安装是250 MB, 不含图形界面; 或是350 MB 以上, 包含图形界面。如果您还需要安装其它的第三方厂商的套件, 那么将需要更多的硬盘空间。

您可以使用商业软件，例如**PartitionMagic®(硬盘分区魔术师)**来建立给FreeBSD使用的空间。FreeBSD光盘的tools目录包含两个免费的工具也可以完成这个工作：**FIPS**以及**PResizer**，它们的文档可以在同一目录中找到。**FIPS**、**PResizer**，和**PartitionMagic**能够改变FAT16以及FAT32分区的大小——它们可以在MS-DOS以及Windows ME系统中使用。这些工具的说明文件可以在同一个目录下面找到**PartitionMagic**是目前已知的唯一能改变NTFS分区大小的应用软件。

警告：不当的使用这些工具可能会删掉您硬盘上的数据资料！在使用这些工具前确定您有最近的、没问题的备份数据。

例2-1. 使用已存在的分区

假设您只有一个4GB的硬盘，而且已经装了Windows然后您将这个硬盘分成两个分区C：跟D：，每个分区大小为2GB。在C：分区上存放有1GB的数据、D：分区上存放0.5GB的数据。

这意味着您的盘上有两个分区，一个驱动器符号是一个分区(如c：、d：)。您可以把所有存放在D：分区上的数据拷贝到C：分区,这样就空出了一个分区(d:)给FreeBSD使用。

例2-2. 缩减已现在的分区

假设您只有一个4GB的硬盘，而且已经装了Windows。您在安装Windows的时候把4GB都给了C：分区，并且已经使用了1.5GB的空间。您想将剩余空间中的2GB给FreeBSD使用。

为了安装FreeBSD，您必须从下面两种方式中选择一种：

1. 备份Windows的数据资料，然后重新安装Windows，并给Windows分配2GB的空间。
2. 使用上面提及的**PartitionMagic**来整理或切割您的分区。

2.2.3.2 Alpha 体系结构的硬盘分配方式

在Alpha上，您必须使用一整颗硬盘给FreeBSD，没有办法在同一个硬盘上跟其它操作系统共存。根据不同的Alpha机器，您的硬盘可以是SCSI或IDE硬盘，只要您的机器可以从这些硬盘开机就可以。

按照Digital/Compaq使用手册书写的惯例，所有SRM输入的部分都用大写表示。注意，SRM大小写有别。

要想得知您硬盘的名称以及型号，可以在SRM console提示符下使用 **SHOW DEVICE** 命令：

```
>>>SHOW DEVICE
dka0.0.0.4.0          DKA0          TOSHIBA CD-ROM XM-57  3476
dkc0.0.0.1009.0       DKC0          RZ1BB-BS  0658
dkc100.1.0.1009.0     DKC100        SEAGATE ST34501W  0015
dva0.0.0.0.1          DVA0
ewa0.0.0.3.0          EWA0          00-00-F8-75-6D-01
pkc0.7.0.1009.0       PKC0          SCSI Bus ID 7  5.27
pqa0.0.0.4.0          PQA0          PCI EIDE
```

pqb0.0.1.4.0

PQB0

PCI EIDE

此范例使用Digital Personal Workstation 433au 并且显示出此机器联接有三个硬盘。第一个是CDROM, 叫做DKA0; 另外两个是两个硬盘, 分别叫做DKC0 及DKC100。

硬盘名称中有DKx 字样的是SCSI 硬盘。例如DKA100 表示是一个SCSI 设备, 其SCSI ID 为1, 位于第一个SCSI 接口(A)。DKC300 表示一个SCSI 硬盘, SCSI ID 为3, 位于第三个SCSI 接口(C)。设备名称PKx 表示SCSI 控制卡。由以上SHOW DEVICE 指令的输出结果看来, SCSI 光盘也被视为是SCSI 硬盘的一种。

IDE 硬盘的名称类似DQx, 而PQx 则表示相对应的硬盘控制器。

2.2.4 收集您的网络配置相关资料

如果您想通过网络(FTP 或是NFS)安装FreeBSD, 那么您就必须知道您的网络配置信息。在安装FreeBSD 的过程中将会提示您输入这些资料, 以顺利完成安装过程。

2.2.4.1 使用以太网或电缆/DSL Modem

如果您通过局域网或是要通过网卡使用电缆/DSL 上网, 那么您必须准备下面的信息:

1. IP 地址。
2. 默认网关IP 地址。
3. 主机名称。
4. DNS 服务器的IP 地址。
5. 子网掩码。

如果您不知道这些信息, 您可以询问系统管理员或是您的网络服务提供者。他们可能会说这些信息会由DHCP 自动分配; 如果这样的话, 请记住这一点就可以了。

2.2.4.2 使用Modem 连接

如果您由ISP 提供的拨号服务上网, 您仍然可以通过它安装FreeBSD, 只是会需要很长的时间。

您必须知道:

1. 拨号到ISP 的电话号码。
2. 您的modem 是连接到哪个COM 端口。
3. 您拨号到ISP 所用的账号和密码。

2.2.5 检查FreeBSD 发行勘误

虽然我们尽力确保每个FreeBSD 发行版本的稳定性, 但偶尔也会有一些错误进入发行版。极少数情况下, 这些问题甚至可能会影响安装。当发现和修正问题之后, 它们会列在FreeBSD 网站中的FreeBSD 发行勘误 (<http://www.FreeBSD.org/releases/6.0R/errata.html>) 中。在您安装之前, 应该首先看一看这份勘误表, 以了解可能存在的问题。

虽然我们尽力使得每个FreeBSD 释出版本都很稳定，但是过程中仍然不免有时会发现错误。在很罕见的情形下，这些错误会影响到安装过程。当我们发现这些错误并且修正后，会将它们列在FreeBSD 网站的FreeBSD Errata(勘误表) (<http://www.freebsd.org/releases/6.0R/errata.html>)中, 在您安装FreeBSD前应该先看看勘误表中有没有什么问题会影响到您的安装。

关于所有释出版本的信息，包括勘误表，可以在FreeBSD 网站 (<http://www.FreeBSD.org/index.html>)的发行版信息 (<http://www.FreeBSD.org/releases/index.html>) 一节中找到。

2.2.6 准备安装介质

FreeBSD 可以通过下面任何一种安装介质进行安装:

安装介质

- CDROM 或DVD
- 在同一计算机上的DOS 分区
- SCSI 或QIC 磁带
- 软盘

网络

- 通过防火墙的一个FTP 站点，或使用HTTP 代理。
- NFS 服务器
- 一个指定的并行或串行接口

如果您购买了FreeBSD 的CD 或DVD，那么您可以直接进入下一节第2.2.7 节。

如果您还没有FreeBSD 的安装文件，您应该回到第2.13 节 一节，它介绍了如何准备所需要的安装介质。之后，您就可以回到这一节，并从第2.2.7 节 继续。

2.2.7 准备引导介质

FreeBSD 的安装过程开始于将您的电脑开机进入FreeBSD 安装环境——并非在其它的操作系统上运行一个程序。计算机通常使用安装在硬盘上的操作系统进行引导，也可以配置成使用一张“bootable(可引导)”的软盘进行启动。大多数现代计算机都可以从光驱进行引导系统。

提示: 如果您有FreeBSD 的安装光盘或DVD(或者是您购买的，或者是您自己准备的。)并且您的计算机可以从光驱进行启动(通常在BIOS 中会有“Boot Order” 或类似的选项可以设置)，那么您就可以跳过此小节。因为FreeBSD 光盘及DVD 光盘都是可以引导的，用它们开机您不用做什么特别的准备。

一般来说，要建立安装盘(软盘)请依照下列步骤:

1. 获取开机软盘映像文件

开机软盘映像文件可以在您的安装介质的floppies/ 目录下找到，另外您也可以从下述网站的floppies 目录下载: <ftp://ftp.FreeBSD.org/pub/FreeBSD/releases/<架构名>/<版本>-RELEASE/floppies/>。将<架构名> 和<版本> 替换为您使用的计算机体系结构和希望安装的版本

号。例如，用于安装i386上的FreeBSD 6.0-RELEASE的文件的地址，应该是ftp://ftp.FreeBSD.org/pub/FreeBSD/releases/i386/6.0-RELEASE/floppies/。

软盘映像文件的扩展名是.flp。在floppies/目录中包括了许多不同的映像文件，随您安装的FreeBSD版本，某些时候也随硬件的不同，您需要使用的映像文件可能会有所不同。如果您正在安装的是FreeBSD 4.X则通常只需要两张软盘的映像，即kern.flp和mfsroot.flp。如果您正在安装的是FreeBSD 5.X则您通常会需要三张软盘，即boot.flp、kern1.flp，以及kern2.flp。请查阅同一目录下的README.TXT文件以了解关于这些映像文件的最新信息。

注意：在安装FreeBSD 5.3之前的5.X系统时，某些设备可能会需要另一张软盘来加载它们的驱动。这些驱动在drivers.flp映像中提供。

重要：您的FTP程序必须使用**二进制模式**来下载这些映像文件。有些浏览器只会用**text** (或**ASCII**) 模式来传输数据，用这些浏览器下载的映像文件做成的软盘将无法正常开机。

2. 准备软盘

您必须为您下载的每一个映像文件准备一张软盘。并且请避免使用到坏掉的软盘。最简单的方式就是您先将这些软盘格式化，不要相信所谓的已格式化的软盘。在Windows下的格式化程序不会告诉您出现多少坏块，它只是简单的标记它们为“bad”并且忽略它们。根据建议您应该使用全新的软盘来存放安装程序。

重要：如果您在安装FreeBSD的过程中造成当机、冻结或是其它怪异现象，第一个要怀疑的就是引导软盘。请用其它的软盘制作映像文件再试试看。

3. 将映像文件写入软盘中

.flp文件并非一般的文件，您不能直接将它们复制到软盘上。事实上它是一张包含完整磁盘内容的映像文件。这表示您**不能**简单的使用DOS的copy命令将文件写到软盘上，而必须使用特别的工具程序将映像文件直接写到软盘中。

如果您使用MS-DOS或Windows操作系统来制作引导盘，那么您可以使用我们提供的fdimage程序来将映像文件写到软盘中。

如果您使用的是光盘，假设光盘的驱动器符号为E:，那么请执行下面的命令：

```
E:\> tools\fdimage floppies\kern.flp A:
```

重复上述命令以完成每个.flp文件的写入，每换一个映像文件都必须更换软盘；制作好的软盘请注明是使用哪个映像文件做的。如果您的映像文件存放在不同的地方，请自行修改上面的指令指向您存放.flp文件的地方。要是您没有FreeBSD光盘，您可以到FreeBSD的FTP站点tools目录(ftp://ftp.FreeBSD.org/pub/FreeBSD/tools/)中下载。

如果您在UNIX系统上制作软盘(例如其它FreeBSD机器)，您可以使用dd(1)命令来将映像文件写到软盘中。如果您用FreeBSD,可以执行下面的命令：

```
# dd if=kern.flp of=/dev/fd0
```

在FreeBSD中，/dev/fd0指的是第一个软驱(即A:驱动器)；/dev/fd1是B:驱动器,依此类推。其它的UNIX系统可能会用不同的名称，这时您就要查阅该系统的说明文件。

您现在可以安装FreeBSD了

2.3 开始安装

重要: 默认情况下, 安装过程并不会改变任何您硬盘中的数据, 除非您看到下面的讯息:

Last Chance: Are you SURE you want continue the installation?

If you're running this on a disk with data you wish to save then WE STRONGLY ENCOURAGE YOU TO MAKE PROPER BACKUPS before proceeding!

We can take no responsibility for lost disk contents!

在看到这最后的警告讯息前您都可以随时离开安装程序而不会变更您的硬盘。如果您发现有任何设定错误, 这时您可以直接将电源关掉而不会造成任何伤害。

2.3.1 开机启动

2.3.1.1 引导i386系统

1. 从电脑尚未开机开始说起
2. 将电脑电源打开。刚开始的时候它应该会显示进入系统设置菜单或BIOS 要按哪个键, 常见的是**F2**、**F10**、**Del** 或**Alt+S**。不论是要按哪个键, 请按它进入BIOS 设置画面。有时您的计算机可能会显示一个图形画面, 典型的做法是按**Esc** 将关掉这个图形画面, 以使您能够看到必要的设置信息。
3. 找到设置开机顺序的选项, 它的标记为“Boot Order” 通常会列出一些设备让您选择, 例如: **Floppy**、**CDROM**、**First Hard Disk** 等等。

如果您要用软盘安装, 请确定选到floppy disk; 如果您要用光盘安装, 请选择CDROM。为了避免疑惑, 请参考您的主板说明手册。

储存设定并离开, 系统应该会重新启动。

4. 如果您用软盘安装, 请将在第2.2.7 节 一节中制作好的第一张引导盘, 里面包含kern.flp 文件的那张盘, 放入软盘驱动器中。

如果您是从光盘安装, 那么开机后请将FreeBSD 光盘放入光驱中。

如果您开机后如往常一样并没有从软盘或光盘引导, 请检查:

1. 是不是软盘或光盘太晚放入而错失开机引导时间。如果是, 请将它们放入后重新开机。
 2. BIOS 设定不对, 请重新检查BIOS 的设定。
 3. 您的BIOS 不支持从这些安装介质引导。
5. FreeBSD 即将启动。如果您是从光盘引导, 您会见到类似下面的画面:

```
Verifying DMI Pool Data .....
Boot from ATAPI CD-ROM :
1. FD 2.88MB System Type-(00)
```

```
Uncompressing ... done
```

```
BTX loader 1.00 BTX version is 1.01
Console: internal video/keyboard
BIOS drive A: is disk0
BIOS drive B: is disk1
BIOS drive C: is disk2
BIOS drive D: is disk3
BIOS 639kB/261120kB available memory
```

```
FreeBSD/i386 bootstrap loader, Revision 0.8
```

```
/kernel text=0x277391 data=0x3268c+0x332a8 |
```

```
|
Hit [Enter] to boot immediately, or any other key for command prompt.
Booting [kernel] in 9 seconds... _
```

如果您是从软盘引导，会看到类似下面的画面：

```
Verifying DMI Pool Data .....
```

```
BTX loader 1.00 BTX version is 1.01
Console: internal video/keyboard
BIOS drive A: is disk0
BIOS drive C: is disk1
BIOS 639kB/261120kB available memory
```

```
FreeBSD/i386 bootstrap loader, Revision 0.8
```

```
/kernel text=0x277391 data=0x3268c+0x332a8 |
```

```
Please insert MFS root floppy and press enter:
```

请根据提示将kern.flp软盘取出，并插入mfsroot.flp这张盘，然后按**Enter**。FreeBSD 5.3和更高版本提供了另外一组软盘，在前一节中已经介绍过了。您只需从第一张软盘启动，然后再需要时根据提示插入其他软盘。

6. 不论是从软盘或光盘引导，您都会看到下面这段信息：

```
Hit [Enter] to boot immediately, or any other key for command prompt.
Booting [kernel] in 9 seconds... _
```

您可以等待十秒，或按**Enter**（对于FreeBSD 4.X则接下来将是进入内核配置菜单）。

2.3.1.2 引导Alpha系统

1. 从电脑尚未打开电源开始。
2. 找开电脑电源并等待屏幕上出现开机提示信息。
3. 如您需要准备安装软盘，请参考第2.2.7节。将用kern.flp做的引导盘放入软驱中然后输入下列命令（请视实际情况修改命令中的软驱盘符）：

```
>>>BOOT DVA0 -FLAGS " -FILE "
```

如果您要从光盘引导，请将光盘放入光驱中然后输入下列命令开始安装(请视情况修改命令中的光驱盘符):

```
>>>BOOT DKA0 -FLAGS " -FILE "
```

4. 然后FreeBSD 就会启动。如果您从软盘引导，到某个阶段您会看到下面的信息:

```
Please insert MFS root floppy and press enter:
```

按照屏幕指示，将kern.flp 软盘取出，换上mfsroot.flp 然后按Enter键。

5. 不论从软盘或光盘引导，您都会看到下面这段信息:

```
Hit [Enter] to boot immediately, or any other key for command prompt.
Booting [kernel] in 9 seconds... _
```

您可以等待10 秒或是按Enter 跳过。之后就会进入内核设定菜单。

2.3.2 配置内核

注意: 从FreeBSD 5.0 开始，改用了新的device.hints(5) 方式来进行配置，而淘汰了先前的userconfig 。关于这一机制的进一步介绍，请参考device.hints(5) 或阅读第12.5 节

内核是操作系统最核心的部分。它负责很多工作，包括存取系统上所有设备，如硬盘、网卡、声卡等等。每一个FreeBSD 核心支持的设备都有其相对应的驱动程序。这些驱动程序的名称由两个或三个字母级成，譬如：sa 表示SCSI 存取驱动程序；sio 表示串口I/O 驱动程序(管理COM 端口)。

当内核启动的时候，每个驱动程序会检查系统中是否有它所支持的设备。如果找到的话，这些驱动程序就会配置这些设备的状态以代核心使用。

上述设备的检查我们称做*device probing*(设备探测)。但是很不幸地，这样做并不是完全安全的。因为有些硬件驱动程序没有办法想到共存，有时找到这个设备却让另一个设备处在不稳定的状态。这是PC 设计上的限制。

许多早期的称作ISA 的设备——(相对于PCI 设备而言)。ISA 设备的规格需要将硬件的某些数据写死在设备上，最具代表性的就是中断号(IRQ)以及IO 端口号。这些设定值通常是通过改变设备上的jumpers(跳线)，或是使用由厂商提供的DOS 工具程序来改变。

这通常是问题的所在，因为这没办法让两个设备共同分享一个IRQ 或是IO 端口地址。

新的设备都按照PCI 规格设计，这些设备就没有上述限制；它们会参考BIOS 中的设定然后动态分配IRQ 及IO 端口地址。

如果您的系统中有任何ISA 设备，那么在设置FreeBSD 驱动程序的时候您就必须指定这些设备的IRQ 及IO 地址。这也是我们在第2.2.1 节一节中希望您先准备一份设备清单的用意。

仍然很不幸地，预设给某些设备使用的IRQ 会跟内存地址互相冲突。这是因为有些ISA 设备出厂的设定值就会跟其它的设备冲突。撇开这个不谈，FreeBSD 驱动程序通常都会根据各制造商设备的出厂设定值来设定，这也是为什么许多设备可以在FreeBSD 顺利驱动的原因。

在跑FreeBSD 的时候根本不会有上冲突的问题，因为当两个设备互相冲突的时候，其中一个设备将被停用(不论您用的是哪种操作系统)。

通常在第一次安装FreeBSD 的时候才会有问题，因为内核希望尽是多包含一些驱动程序，这样才能支持许多不同设备的配置。这意味着在找到的这些设备中有可能设定值会互相冲突。FreeBSD 在探测系统设

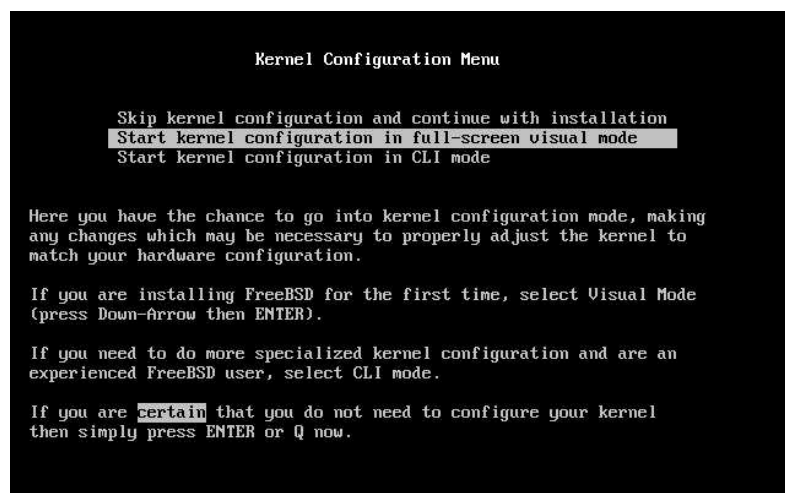
备的时候会按照一的顺序，如果您的某个设备在较后面探测到，但是跟前面找到的设备设定冲突，那么在安装FreeBSD的时候，这个设备不一定能正确雇用。

因为如此，当您在安装FreeBSD前，可以先看看在系统内核中包含了哪些驱动程序，如果您没有某些设备，则可以将它们的驱动程序删除或是在稍后您也可以确认您有的设备的设定值有没有问题。

这听起来好像很复杂，但不全然如此。

图2-1显示的是内核能设置的第一个配置菜单。我们推荐您选择Start kernel configuration in full-screen visual mode选项，因为这对新手来说比较容易。

图2-1. 内核配置菜单



内核配置画面(图图2-2) 被分成四个部分:

1. 在“active(可用)”区域的展开式选择菜单分为四个群，例如Storage(储存设备)、Network(网络设备)。每个设备会显示一个对应的说明、由二或三个字母组成的驱动程序名称以及驱动程序所使用的IRQ和内存地址。另外，如果可用的驱动程序跟另一个可用的驱动程序有冲突，它们的驱动程序名称之后会显示CONF字样。同时栏目标题也会显示在可用的设备中总共有几个设备有冲突。
2. 在Inactive(停用)区域的驱动程序仍然保留在内核中，但当内核启动的时候并不会探测这些设备。这个区域的分组方式跟可用区一样。
3. 第三区(信息显示区)显示的是目前所选择设备的细节项目设置，包括IRQ及IO端口地址。
4. 第四区告诉您这个画面的操作按键。

图2-2. 配置内核可视化视觉接口

Active Drivers		? conflicts	Dev	IRQ	Port
Storage :	(Collapsed)				
Network :	(Collapsed)				
Communications :	(Collapsed)				
Input :	(Collapsed)				
Multimedia :					
Miscellaneous :	(Collapsed)				
Inactive Drivers			Dev		
Storage :					
Network :					
Communications :	(Collapsed)				
Input :					
Multimedia :					
Miscellaneous :	(Collapsed)				
[Enter] Expand device list		[X] Expand all lists			
[TAB] Change fields		[Q] Save and Exit			[?] Help

在这个阶段，您总是会看到有冲突的设备被列出。请不要担心，因为这是正常的；前面提到在安装的时候所有的设备都会被启用，而其中的某些设备就会跟其它的设备产生冲突。

现在您必须逐一检查这些设备驱动程序，然后解决冲突的问题。

解决驱动程序冲突

- 1. 按下X 键可以将所选择区域的驱动程序完全展开以方便您检阅。您可以使用方向键在可用设备区前后移动。

图2-3 显示按下X 键后的结果。

图2-3. 展开驱动程序清单

Active Drivers		? conflicts	Dev	IRQ	Port
Storage :					
AdvanSys SCSI narrow controller			adu0		
Adaptec 154x SCSI controller			aha0		
Adaptec 152x SCSI and compatible sound cards			aic0		
ATA/ATAPI compatible disk controller			ata0	14	0x1f0
ATA/ATAPI compatible disk controller			ata1	15	0x170
Buslogic SCSI controller			bt0		
Floppy disk controller			fdc0	6	0x3f0
Inactive Drivers			Dev		
Storage :					
Network :					
Communications :	(Collapsed)				
Input :					
Multimedia :					
Miscellaneous :	(Collapsed)				
[Enter] Collapse device list		[C] Collapse all lists			
[TAB] Change fields		[Q] Save and Exit			[?] Help

- 2. 停用任何您没有的设备的驱动程序。要停用一个设备，用方向键移动将该设备反白然后按下Del 键，则此设备驱动程序就会被移到Inactive Drivers(停用设备区) 列表。

如果您不小心将一个设备停用，那么请按**Tab** 切换到Inactive Drivers 区, 选择被停用的设备，然后按下**Enter** 键将它移回可用设备区。

警告: 请不要移除sc0。这个驱动程序是控制屏幕用的，除非您是通过串行线进行安装，否则请不要移除它。

警告: 如果您用的是USB 键盘才可以停用atkbd0 用一般的键盘请保留此atkbd0 设备驱动程序。

- 如果现在显示没有冲突，那么您可以跳过这一步骤。否则，剩下的冲突还是必须解决。如果在信息显示区没有看到“allowed conflict(允许冲突)”，那么您必须改变这边显示的IRQ 及内存地址，或必须变更设备上面的IRQ 及内存地址。

要改变设备驱动程序的IRQ 及IO 端口地址，选择要变更的驱动程序然后按**Enter** 键。之后等光标移到第三区(信息显示区)时候您就可以理发这些设置。您应该输入之前做硬件清单列表的时候所记录的IRQ 及IO 端口地址。要完成更改请按**Q** 键并回到可用设备区。

如果您不确定该设定什么值，那么可以试试看-1。有些FreeBSD 驱动程序在搜寻设备的时候可以安全找出设备的正确设定值；所以这里设置-1 就是告诉这些驱动程序自行去尝试找出合适的设置。

如果要直接在设备硬件上改变设定值，设定的方法每种设备都不大相同。有些设备您必须将它从电脑中拆下来然后调整路线或是DIP开关；其它的可能厂商会提供DOS 工具软盘，里面有程序可以更改这些设定。不论是哪一种方式，您都应该参考设备所附的使用手册。很明显地，改变这些设定值必须重新开机后才会生效，所以您必须重新进入FreeBSD 安装程序。

- 当所有的冲突都解决了以后，您会看到类似图2-4 的画面。

图2-4. 没有冲突的设备驱动程序状态画面

Active Drivers		Dev	IRQ	Port
Storage :				
ATA/ATAPI compatible disk controller		ata0	14	0x1f0
ATA/ATAPI compatible disk controller		ata1	15	0x170
Floppy disk controller		fdc0	6	0x3f0
Network :				
NE1000,NE2000,3C503,WD/SMC80xx Ethernet adapters		ed0	10	0x280
Communications :				
Parallel Port chipset		ppc0	7	
Inactive Drivers		Dev		
Storage :		(Collapsed)		
Network :		(Collapsed)		
Communications :		(Collapsed)		
Input :				
Multimedia :				
Miscellaneous :		(Collapsed)		
Port address :		0x1f0		
IRQ number :		14		
Flags :		0x0		
[Enter] Edit device parameters		[DEL] Disable device		
[TAB] Change fields		[Q] Save and Exit		[?] Help

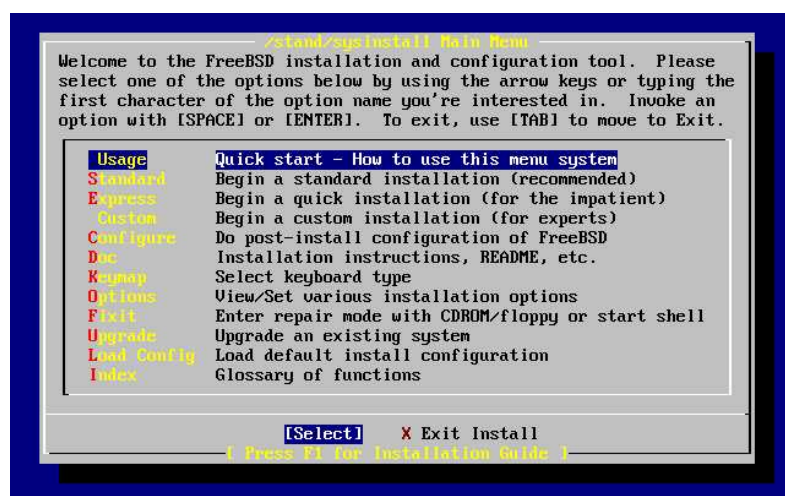
如您所见，可用设备列表变得干净多了，只列出您系统中有的设备。

现在您可以储存所做的改变，然后进到下一个安装步骤。按**Q** 键离开设备配置界面，您会看到下面的信息：

Save these parameters before exiting? ([Y]es/[N]o/[C]ancel)

回答`Y` 保存配置到内存(安装完成后将后保存到磁盘)然后开始探测设备。在设备探测完毕后, `sysinstall` 就会启动并且显示它的主界面。(图2-5)。

图2-5. Sysinstall 主界面



2.3.3 查看设备探测的结果

前面屏幕显示的最后几百行字会存在缓冲区中以便您查阅。

要浏览缓冲区, 您可以按下**Scroll Lock** 键, 这会开启画面的卷动功能。然后您就可以使用方向键或**PageUp**、**PageDown** 键来上下翻阅。再按一次**Scroll Lock** 键将停止画面卷动。

在您浏览的时候会看到类似图2-6的画面。真正的结果依照您的电脑装置而有所不同。

图2-6. 典型的设备探测结果

```

avail memory = 253050880 (247120K bytes)
Preloaded elf kernel "kernel" at 0xc0817000.
Preloaded mfs_root "/mfsroot" at 0xc0817084.
md0: Preloaded image </mfsroot> 4423680 bytes at 0xc03ddcd4

md1: Malloc disk
Using $PIR table, 4 entries at 0xc00fde60
npx0: <math processor> on motherboard
npx0: INT 16 interface
pcib0: <Host to PCI bridge> on motherboard
pci0: <PCI bus> on pcib0
pcib1: <VIA 82C598MVP (Apollo MVP3) PCI-PCI (AGP) bridge> at device 1.0 on pci0
pci1: <PCI bus> on pcib1
pci1: <Matrox MGA G200 AGP graphics accelerator> at 0.0 irq 11
isab0: <VIA 82C586 PCI-ISA bridge> at device 7.0 on pci0
isa0: <ISA bus> on isab0
atapci0: <VIA 82C586 ATA33 controller> port 0xe000-0xe00f at device 7.1 on pci0
ata0: at 0x1f0 irq 14 on atapci0
  
```

```

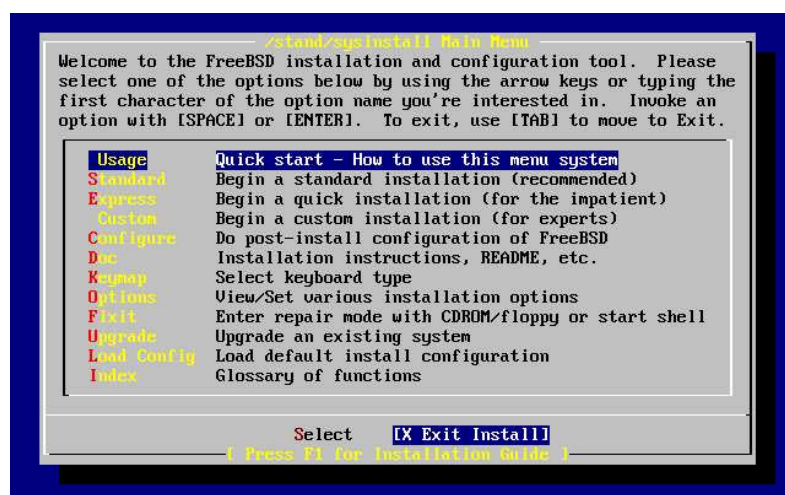
ata1: at 0x170 irq 15 on atapci0
uhci0: <VIA 83C572 USB controller> port 0xe400-0xe41f irq 10 at device 7.2 on pci
0
usb0: <VIA 83572 USB controller> on uhci0
usb0: USB revision 1.0
uhub0: VIA UHCI root hub, class 9/0, rev 1.00/1.00, addr1
uhub0: 2 ports with 2 removable, self powered
pci0: <unknown card> (vendor=0x1106, dev=0x3040) at 7.3
dc0: <ADMtek AN985 10/100BaseTX> port 0xe800-0xe8ff mem 0xdb000000-0xeb0003ff ir
q 11 at device 8.0 on pci0
dc0: Ethernet address: 00:04:5a:74:6b:b5
miibus0: <MII bus> on dc0
ukphy0: <Generic IEEE 802.3u media interface> on miibus0
ukphy0: 10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, auto
ed0: <NE2000 PCI Ethernet (RealTek 8029)> port 0xec00-0xec1f irq 9 at device 10.
0 on pci0
ed0 address 52:54:05:de:73:1b, type NE2000 (16 bit)
isa0: too many dependant configs (8)
isa0: unexpected small tag 14
orm0: <Option ROM> at iomem 0xc0000-0xc7fff on isa0
fdc0: <NEC 72065B or clone> at port 0x3f0-0x3f5,0x3f7 irq 6 drq2 on isa0
fdc0: FIFO enabled, 8 bytes threshold
fd0: <1440-KB 3.5" drive> on fdc0 drive 0
atkbd0: <Keyboard controller (i8042)> at port 0x60,0x64 on isa0
atkbd0: <AT Keyboard> flags 0x1 irq1 on atkbd0
kbd0 at atkbd0
psm0: <PS/2 Mouse> irq 12 on atkbd0
psm0: model Generic PS/@ mouse, device ID 0
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff on isa0
sc0: <System console> at flags 0x100 on isa0
sc0: VGA <16 virtual consoles, flags=0x300>
sio0 at port 0x3f8-0x3ff irq 4 flags 0x10 on isa0
sio0: type 16550A
sio1 at port 0x2f8-0x2ff irq 3 on isa0
sio1: type 16550A
ppc0: <Parallel port> at port 0x378-0x37f irq 7 on isa0
pppc0: SMC-like chipset (ECP/EPP/PS2/NIBBLE) in COMPATIBLE mode
ppc0: FIFO with 16/16/15 bytes threshold
plip0: <PLIP network interface> on ppbus0
ad0: 8063MB <IBM-DHEA-38451> [16383/16/63] at ata0-master UDMA33
acd0: CD-RW <LITE-ON LTR-1210B> at ata1-slave PI04
Mounting root from ufs:/dev/md0c
/stand/sysinstall running as init on vty0

```

仔细检查探测结果以确定FreeBSD 找到所有您期望出现的设备。如果设备没有被探测到，那么就不会列出。如果此设备需要配置IRQ 以及IO 端口地址，请检查输入是否正确。

如果您需要改变某些设备的设置，您可以很容易地退出sysinstall 程序，然后从头重新来过。这也有助于您熟悉这些过程。

图2-7. 选择离开Sysinstall



在主界面使用方向键选择Exit Install 您会看到如下的信息:

```

User Confirmation Requested
Are you sure you wish to exit? The system will reboot
(be sure to remove any floppies from the drives).

[ Yes ]      No
  
```

如果CDROM 还留在光驱里，而且选择了[Yes]，则安装程序将重新启动。

如果您是从软盘启动，那么重新开机前您必须将mfsroot.flp 软盘取出再换上kern.flp 软盘。

2.4 介绍Sysinstall

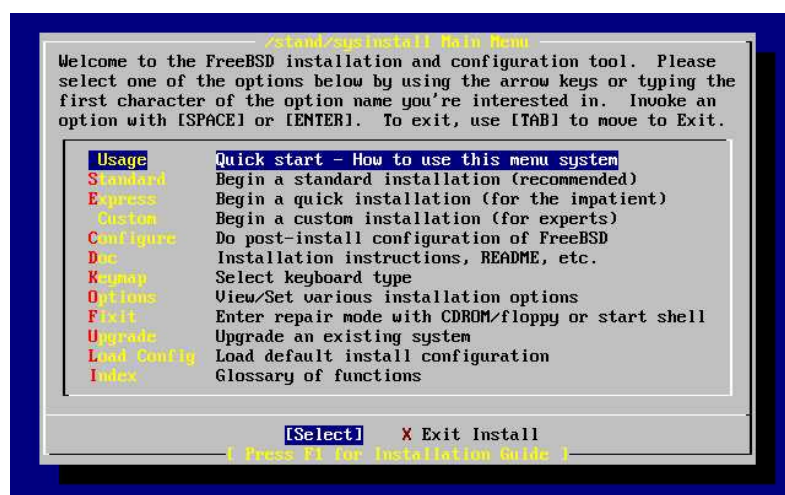
sysinstall 是FreeBSD 项目所提供的安装程序。它以console(控制台)为主，分为向个菜单及画面让您配置及控制安装过程。

sysinstall 菜单画面由方向键、**Enter**、**Space**、以及其它按键所控制。在主画面的Usage 菜单有这些按键的说明。

要查看这些说明，请将光标移到Usage 项目，然后[Select] 按键被选择，图2-8，然后按下**Enter** 键。

安装画面的使用说明会显示出来，阅读完毕请按**Enter** 键回到主画面。

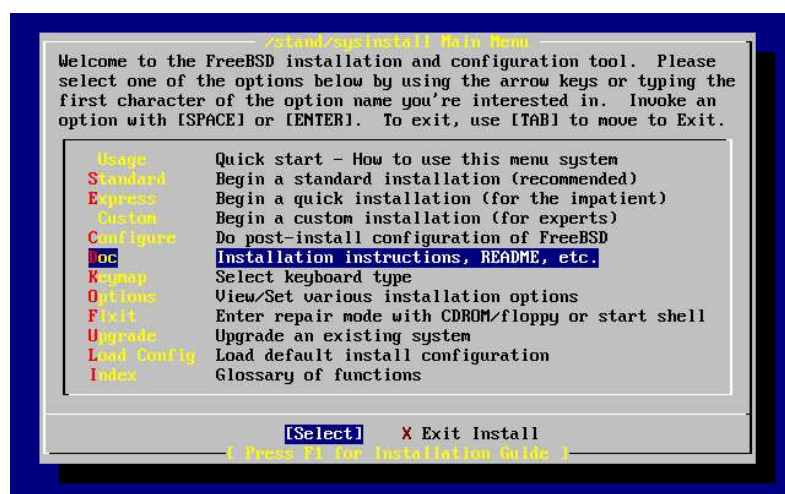
图2-8. 选取Sysinstall 主菜单的Usage 项目



2.4.1 选择Documentation(说明文件) 菜单

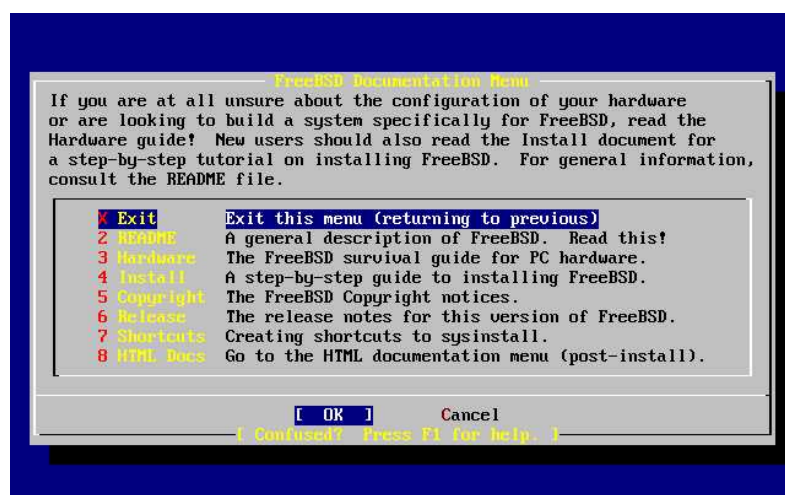
用方向键从主菜单选择Doc 条目然后按Enter键。

图2-9. 选择说明文件菜单



这将会进入说明文件菜单。

图2-10. Sysinstall 说明文件菜单



阅读这些说明文件很重要。

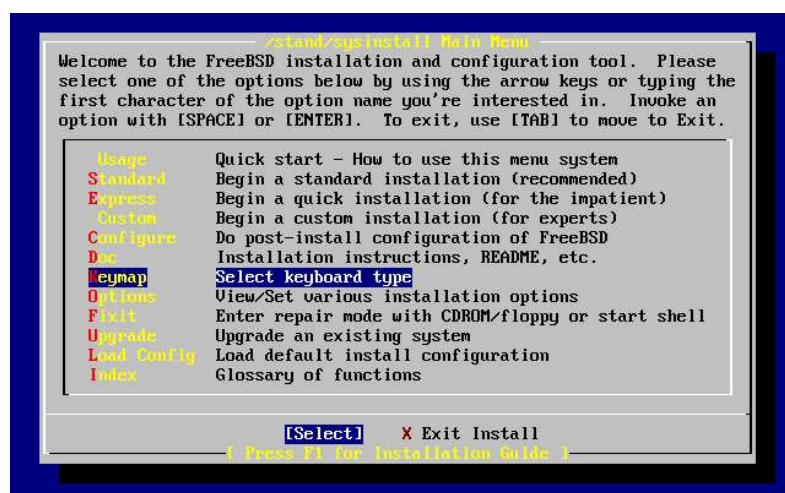
要阅读一篇文章，请用方向键选取要阅读的文章然后按**Enter** 键。阅读中再按一下**Enter** 就会回到说明文件画面。

若要回到主菜单，用方向键选择Exit 然后按下**Enter** 键。

2.4.2 选择键盘对应(Keymap)菜单

如果要改变键盘按键的对应方式，请在主菜单选取Keymap 然后按**Enter** 键。一般情况下不改变引项，除非您使用了非标准键盘或非美国键盘。

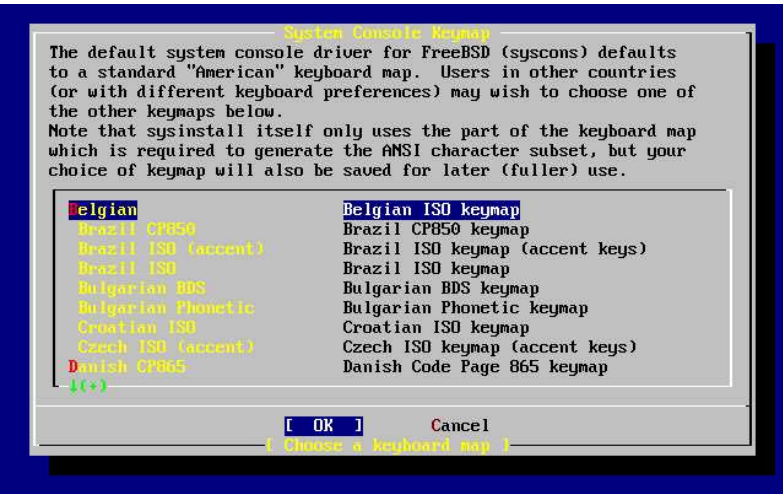
图2-11. Sysinstall 主菜单



您可以使用上下键移动到您想使用的键盘对应方式，然后按下**Space** 键以选取它；再按**Space** 键可以取消选取。当您完成后，请选择[OK] 然后按**Enter** 键。

这一屏幕只显示出部分列表。选择[Cancel] 按Tab 键将使用默认的键盘对应，并返回到主菜单

图2-12. Sysinstall 键盘对应菜单



2.4.3 安装选项设置画面

选择Options 然后按Enter 键。

图2-13. Sysinstall 主菜单

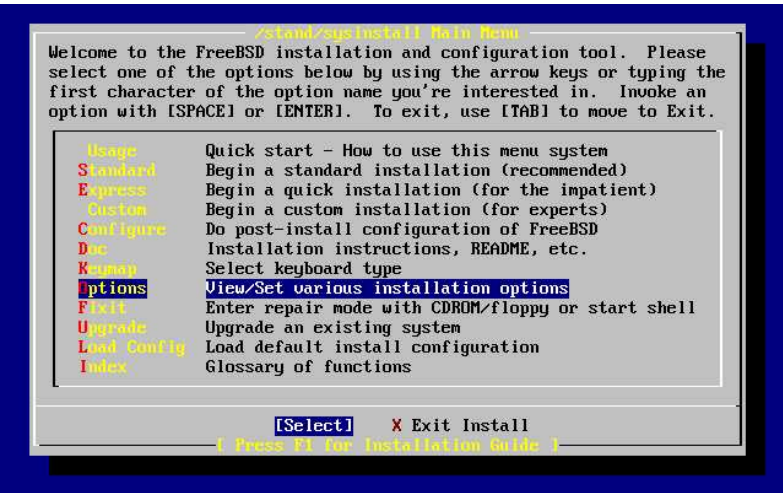
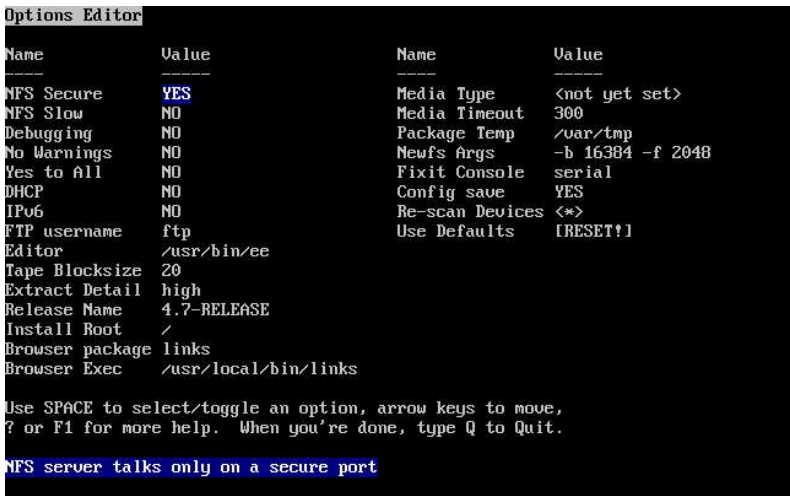


图2-14. Sysinstall 选项设置



预设值通常可以适用于大部分的使用者，您并不需要改变它们。版本名称要根据安装的版本进行变化。

目前选择项目的描述会在屏幕下方以蓝底白字显示。注意其中有一个项目是Use Defaults(使用默认值)您可以由此项将所有的设定还原为预设值。

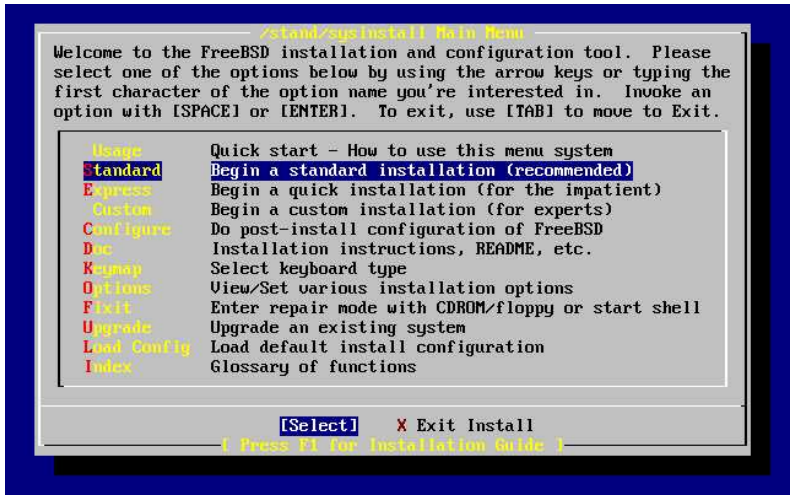
可以按下**F1**来阅读各选项的说明。

按**Q**键可以回到主画面。

2.4.4 开始进行标准安装

Standard(标准) 安装适用于那些UNIX 或FreeBSD 的初级使用者。用方向键选择Standard 然后按Enter 键可开始进入标准安装。

图2-15. 开始进行标准安装



2.5 分配磁盘空间

您的第一个工作就是要分配FreeBSD用的硬盘空间以便**sysinstall**先做好一些准备。为了完成这个工作，您必须先对FreeBSD如何找到磁盘信息做一个了解。

2.5.1 BIOS 磁盘编号

当您在系统上安装配置FreeBSD之前，有一个重要的事情一定要注意，尤其是当您有多个硬盘的时候。

在pc架构，当您跑像MS-DOS或Microsoft Windows这种跟BIOS相关的操作系统的时候，BIOS有能力改变正常的磁盘顺序，然后这些操作系统会跟着BIOS做改变。这让使用者不一定非要有所谓的“**primary master**”硬盘开机。许多人发现最简单而便宜备份系统的方式就是再去买一块一模一样的硬盘，然后定期将数据从第一块硬盘复制到第二个硬盘，使用**Ghost®**或**XCOPY**。所以，当第一个硬盘死了，或者是被病毒破坏，或者有坏轨道，他们可以调整BIOS中的开机顺序而直接用第二块硬盘开机。这跟将机壳拆开，把第二块硬盘跟第一块硬盘对调(要调**jumper**)有同样的效果，差别就是不用拆壳；因此，对有这方面需求的人而言，直接在BIOS中设定非常方便。

比较昂贵，配有SCSI控制卡的系统通常可以延伸BIOS的功能来让SCSI设备(可达七个)达到类似改变顺序的功能。

习惯于使用这种方式的使用者可能会感到惊讶，因为在FreeBSD中并非如此。FreeBSD不会参考BIOS，而且也不知道所谓的“BIOS逻辑磁盘对应”。是怎么回事。这会让人感觉很疑惑，明明就是一样的硬盘而且资料也完全从另一块复制过来的，结果却没办法像以前那样用。

当使用FreeBSD以前，请将BIOS中的硬盘开机顺序调回正常的顺序，并且以后不要再改变。如果一定要交换硬盘顺序，那请用硬件的方式，打开机壳并调整调线。

范例：Bill 和Fred 的安装历险

Bill 替Fred 把旧的Wintel 的机器装上了FreeBSD。他装了一台SCSI 硬盘，ID 是0，然后把FreeBSD 装在上面。

Fred 开始使用他新的FreeBSD 系统；但是过了几天，他发现这旧的SCSI 硬盘发生了许多小问题。之后，他就跟Bill 说起这件事。

又过了几天，Bill 决定是该解决问题的时候了，所以他从后面房间的硬盘“收藏”中找出了一模一样的硬盘，并且经过表面测试后显示这块硬盘没有问题。因此，Bill 将它的ID 调成4，然后安装到Fred 的机器，并且将资料从磁盘0 复制到磁盘4。现在新硬盘装好了，而且看起来好像一切正常；所以，Bill 认为现在应该可以开始用它了。Bill 于是到SCSI BIOS 中设定SCSI ID 4 为开机盘，用磁盘4 重新开机后，一切跑得很顺利。

继续用了几天后，Bill 跟Fred 决定要来玩点新的：该将FreeBSD 升级了。Bill 将ID 0 的硬盘移除(因为有问题)并且又从收藏区中拿了一块一样的硬盘来。然后他用Fred 神奇的网络FTP 磁盘将新版的FreeBSD 安装在这块硬盘上；安装过程没什么问题发生。

Fred 用了这新版本几天后，觉得它很适合用在工程部门…是时候将以前放在旧系统的工作资料复制过来了。因此，Fred 将ID4 的SCSI 硬盘(里面有放着旧系统中复制过来的最新资料)mount 起来，结果竟然发现在ID4 的硬盘上，他以前的所有资料都不见了！

资料跑到哪里去了呢？

当初Bill 将ID0 硬盘的资料复制到ID4 的时候，ID4 即成为一个“新的副本”。而当他调SCSI BIOS 设定ID4 为开机盘，想让系统从ID4 开机，这其实只是他自己笨，因为大部分的系统可以直接调BIOS 而改变开机顺序，但是FreeBSD 却会把开机顺序还原成正常的模式，因此，Fred 的FreeBSD 还是从原来那块ID0 的硬盘开机的。所有的资料都还在那块硬盘上，而不是在想象之中的ID4 硬盘。

幸运的是，在我们发现这件事的时候那些资料都还在，我们将这些资料从最早的那块ID0 硬盘取出来并交还给Fred，而Bill 也由此了解到计算机计数是从0 开始的。

虽然我们这里的例子使用SCSI 硬盘，但是相同的概念也可以套用在IDE 硬盘上。

2.5.2 使用FDisk 创建分区

注意：如果不再做改变，数据将会写进硬盘。如果您犯了一个错误想重新开始，请选择**sysinstall** 安装程序的退出按钮(exit)。或按**U** 键来Undo 操作。如果您的操作没有结果，您总可以重新启动您的计算机来达到您的目的。

当您在**sysinstall** 主菜单选择使用标准安装后，您会看到下面的信息：

Message

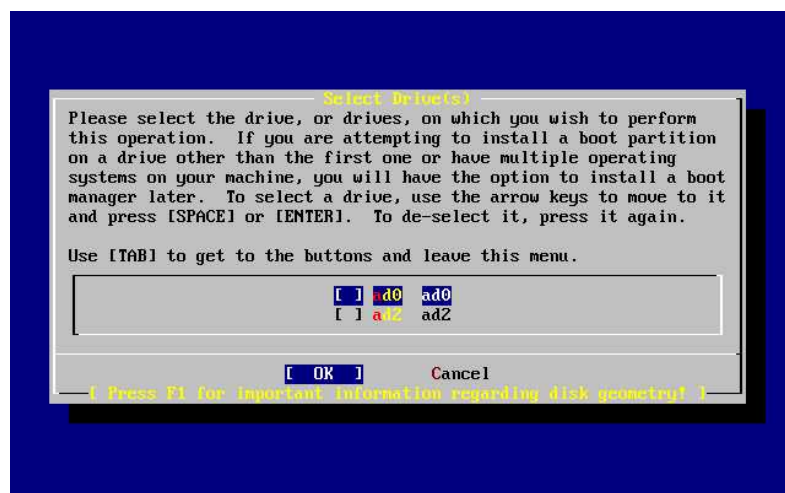
In the next menu, you will need to set up a DOS-style ("fdisk") partitioning scheme for your hard disk. If you simply wish to devote all disk space to FreeBSD (overwriting anything else that might be on the disk(s) selected) then use the (A)ll command to select the default partitioning scheme followed by a (Q)uit. If you wish to allocate only free space to FreeBSD, move to a partition marked "unused" and use the (C)reate command.

[OK]

[Press enter or space]

如屏幕指示，按**Enter** 键，然后您就会看到一个列表列出所有在探测设备的时候找到的硬盘。图2-16 范例显示的是有找到两个IDE 硬盘的情形，这两个硬盘分别为ad0 和ad2。

图2-16. 选择要分区的硬盘



您可能正在奇怪，为什么ad1 没有列出来？为什么遗失了呢？

试想，如果您有两个IDE 硬盘，一个是在第一个Primary master，一个是Secondary master，这样会发生什么事呢？如果FreeBSD 依照找到的顺序来为他们命名，如ad0 和ad1 那么就不会有什么问题。

但是，现在问题来了。如果您现在想在primary slave 加装第三个硬盘，那么这个硬盘的名称就会是ad1，之前的ad1 就会变成ad2。这会造成什么问题呢？因为设备的名称（如ad1s1a）是用来寻找文件系统的，因此您可能会发现，突然，您有些文件系统从此无法正确地显示出来，必须修改FreeBSD 配置文件（译注：/etc/fstab）才可以正确显示。

为了解决这些问题，在配置内核的时候可以叫FreeBSD 直接用IDE 设备所在的位置来命名，而不是要据的到的顺序。使用这种方式的话，在secondary master 的IDE 设备就永远是 ad2，即使您的系统中没有ad0 或ad1 也不受影响。

此为FreeBSD 内核的默认值，这也是为什么上面的画面只显示ad0 和ad2的原因。画面上这台机器的两颗硬盘是装在primary 及secondary 的master 上面；并没有任何一个硬盘安装在slave 插槽上。

您应该选择您想安装FreeBSD 的硬盘，然后按下[OK]。之后FDisk 就会开始，您会看到类似图2-17的画面。

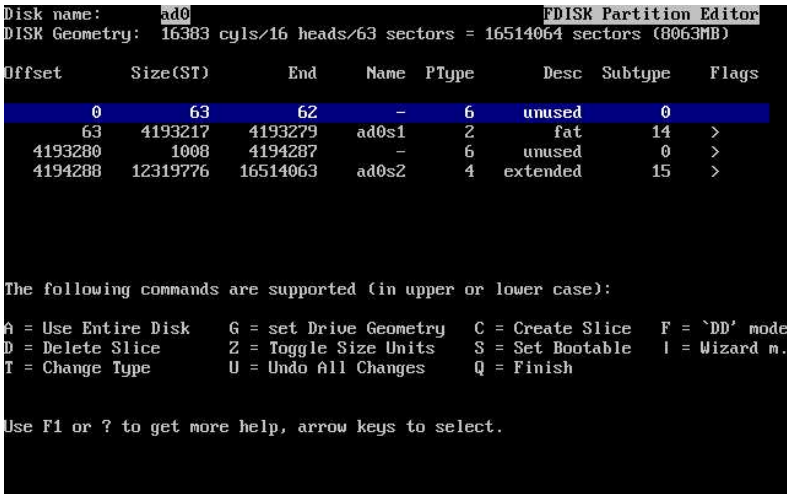
FDisk 的显示画面分为三个部分。

第一部分是画面上最上面两行，显示的是目前所选择的硬盘的信息。包含它的FreeBSD 名称、硬盘分布以及硬盘的总容量。

第二部分显示的是目前选择的硬盘上有哪些分区，每个分区的开始及结束位置、所占容量、FreeBSD 名称、它们的描述以及类别（sub-type）。此范例显示有两个分区、一个大的FAT 分区，（很可能是MS-DOS 或Windows 的C:）、以及一个扩展分区（在MS-DOS 或Windows 里面还可以包含逻辑分区）。

第三个部分显示**FDisk** 中可用的命令。

图2-17. 典型的尚未编辑前的Fdisk 分区表



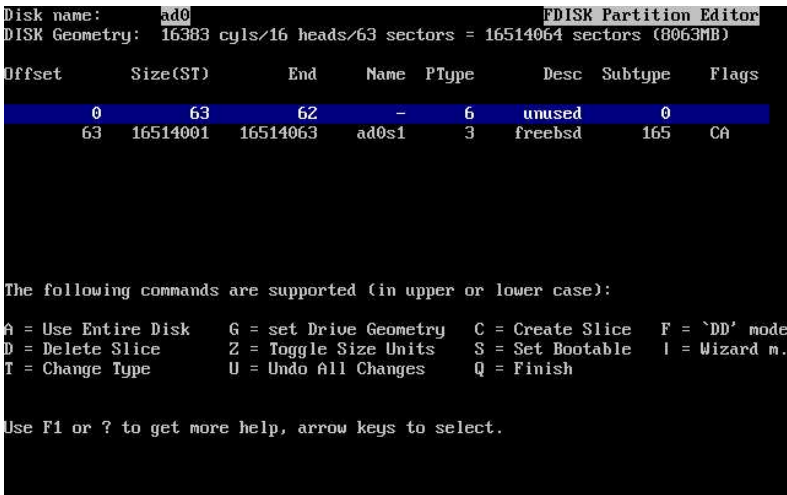
接下来要做的事跟您要怎么给您的硬盘分区有关。

如果您要让FreeBSD 使用整个硬盘（稍后您确认要**sysinstall** 继续安装后会删除所有这个硬盘上的资料），那么您就可以按**A** 键（Use Entire Disk）目前已有的分区都会被删除，取而代之的是一个小的，标示为**unused** 的分区，以及一个大的FreeBSD 分区。之后，请用方向键将光标移到这个FreeBSD 分区，然后按**S** 以将此分区标记为启动分区。您会看到类似图2-18 的画面。注意，在**Flags** 栏中的**A** 记号表示此分区是**激活** 的，因而启动将从此分区进行。

要删除现有的分区以便为FreeBSD 腾出空间，您可以将光标移动到要删除的分区后按**D** 键。然后就可按**C** 键，并在弹出的对话框中输入将要创建的分区的大小。输入合适的大小后按**Enter** 键。一般而言，这个对话框中的初始值是可以分配给该分区的最大值。它可能是最大的邻接分区或未分配的整个硬盘大小。

如果您已经建立好给FreeBSD 的分区（使用像**PartitionMagic** 类似的工具），那么您可以按下**C** 键来建立一个新的分区。同样的，会有对话框询问您要建立的分区的大小。

图2-18. Fdisk 分区使用整个硬盘



完成后，按**Q**键。您的变更会存在**sysinstall**中，但是还不会真正写入您的硬盘。

2.5.3 安装多重引导

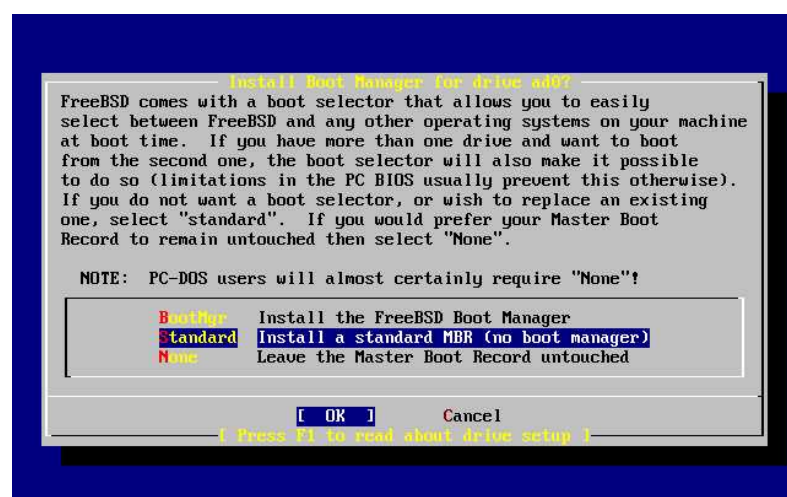
在这步骤您可以选择要不要安装一个多重引导管理器。一般而言，如果碰到下列的情形，您应该选择要安装多重引导管理程序。

- 您有一个以上的硬盘，并且FreeBSD并不是安装在第一个硬盘上。
- 您可以在一个硬盘上，除了FreeBSD，您还有安装其它的操作系统；然后您想要选择在开机的时候要进入哪个系统。

如果您在这台机器上只安装一个FreeBSD操作系统，并且安装在第一个硬盘，那么选择**Standard**安装就可以了。如果您已经使用了一个第三方的多重引导程序，那么请选择**None**。

选择好配置后请按**Enter**。

图2-19. Sysinstall 多重引导管理程序



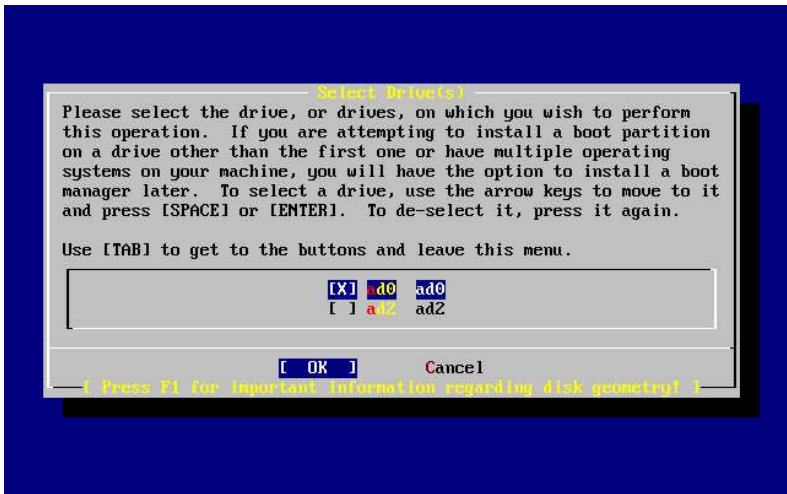
按下**F1**键所显示的在线说明中有讨论一些操作系统共存可能发生的问题。

2.5.4 在其它硬盘上创建分区

如果您的系统上有一个以上的硬盘，在选择完多重引导管理程序后会再回到选择硬盘的画面。如果您要将FreeBSD安装在多个硬盘上，那么您可以在这里选择其它的硬盘，然后重复使用**FDisk**来建立分区。

重要: 如果您想让FreeBSD来管理其它的硬盘，那么两个硬盘都必须安装FreeBSD的多重引导管理程序。

图2-20. 离开选择硬盘画面



Tab 键可以在您最后选择的硬盘、[OK] 以及[Cancel] 之间进行切换。
用Tab 键将光标移动到[OK]然后按Enter 键继续安装过程。

2.5.5 使用Disklabel 创建分区

您现在必须在刚刚建立好的slice 中规划一些label。请注意，每个label 的代号是a 到h，另外，习惯上b、c 和d 是有特殊用途的，不应该随意变动。

某些应用程序可以利用一些特殊的分区而达到较好的效果，尤其是分区分散在不同的硬盘的时候。但是，现在您是第一次安装FreeBSD，所以不需要去烦恼如何分割您的硬盘。最重要的是，装好FreeBSD然后学习如何使用它。当您对FreeBSD 有相当程序的熟悉后，您可以随时重新安装FreeBSD，然后改变您分区的方式。

下面的范例中有四个分区——一个是磁盘交换分区，别外三个是文件系统。

表2-2. 为第一个硬盘分区

分区	文件系统	大小	描述
a	/	100 MB	这是一个根文件系统（root filesystem）。任何其它的文件系统都会挂在根目录（译注：用根目录比较亲切）下面。100 MB 对于要目录来说是合理的大小，因为您往后并不会在这里存放太多的数据；在安装FreeBSD后会用掉约40 MB 的根目录空间。剩下的空间是用来存放临时文件用的，同时，您也应该预留一些空间，因为以后的FreeBSD版本可能会需要较多的/（根目录）空间。

分区	文件系统	大小	描述
b	N/A	2-3 x RAM	此分区为系统磁盘交换分区（swap space）。选择正确的交换空间大小可是一门学问。一般来说，交换空间的大小应该是您系统上内存（RAM）大小的2到3倍。交换空间至少要有64 MB 因此，如果您的电脑上的RAM比32 MB 小，请将交换空间大小设为64 MB。 如果您有一个以上的硬盘，您可以在每个硬盘上都配置交换分区。FreeBSD 会利用每个硬盘上的交换空间，这样做能够提高swap 的性能。如果是这种情形，先算出您总共需要的交换空间大小（如128 MB），然后除以您拥有的硬盘数目（如2块），算出的结果就是每个硬盘上要配置的交换空间的大小。在这个例子中，每个硬盘的交换空间为64 MB
e	/var	50 MB	/var 目录会存放不同长度的文件、日志以及其它管理用途的文件。大部分这些文件都是FreeBSD每天在运行的时候会读取或是写入的。当这些文件放在另外的文件系统（译注：即/var）可以避免影响到其它目录下面类似的文件存取机制。
f	/usr	剩下的硬盘空间	您所有的其它的文件通常都会存在/usr 目录以及其子目录下。

如果您要将FreeBSD安装在一个以上的硬盘，那么您必须在您配置的其它分区上再建立分区。最简单的方式就是在每个硬盘上建立两个分区，一个是交换分区，一个是文件系统分区。

表2-3. 为其它磁盘分区

分区	文件系统	大小	描述
b	N/A	见描述	之前提过，交换分区是可以跨硬盘的。但是，即使a 分区没有使用，习惯上还是会把交换分区放在b 分区上。
e	/diskn	剩下的硬盘空间	剩下的空间是一个在的分区，最简单的做法是将之规划为a分区而不是e分区。然而，习惯上a分区是保留给根目录(/) 用的。您不一定要遵守这个习惯，但是sysinstall 会，所以照着它做会使您的安装比较清爽、干净。您可以将这些文件系统挂在任何地方，本范例建议将它们挂在/diskn 目录，n 依据每个硬盘而有所不同，但是，您喜欢的话也可将它们挂在别的地方。

分区的配置完成后，您可以用sysinstall. 来建立它们了。您会看到下面的信息：

```
Message
Now, you need to create BSD partitions inside of the fdisk
partition(s) just created. If you have a reasonable amount of disk
space (200MB or more) and don't have any special requirements, simply
use the (A)uto command to allocate space automatically. If you have
more specific needs or just don't care for the layout chosen by
```

(A)uto, press F1 for more information on manual layout.

[OK]
[Press enter or space]

按下**Enter** 键开始FreeBSD分区表编辑器，称做**Disklabel**。

图2-21 显示您第一次执行**Disklabel**的画面。画面分为三个区域。

前几行显示的是您正在编辑的硬盘以及您正在建立的slice位于哪个分区上。（在这里，**Disklabel** 使用的是分区名称 而不是slice 名）。此画面也会显示slice还有多少空间可以使用；亦即，有多余的空间，但是尚未指派分区。

画面中间区域显示已建立的分区，每个分区的文件系统名称、所占的大小以及一些关于建立这些文件系统的参数选项。

下方的第三区显示在**Disklabel**中可用的按键。

图2-21. Sysinstall Disklabel 编辑器



Disklabel 您可以自动配置分区以及给它们预设的大小。您可以按**A**键使用此功能。您会看到类似图2-22的画面。根据您硬盘的大小，自动分配所配置的大小不一定合适。但是没有关系，您并不一定要使用预设的大小。

注意: 从FreeBSD 4.5开始，自动配置会给/tmp 目录一个独立分区，而不是附属在/ 之下。这样可以避免将一些临时文件放到根目录中（译注：可能会用完根目录空间）。

图2-22. Sysinstall Disklabel 编辑器-使用自动配置

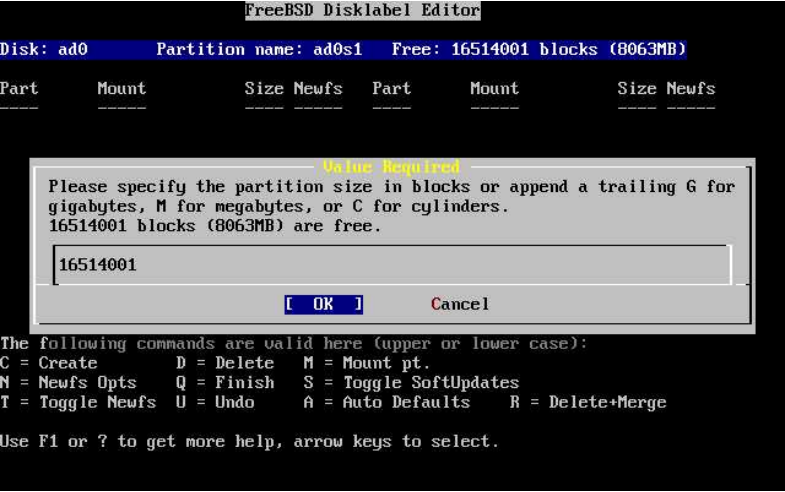


如果您不想使用默认的分​​区布局，则需要用方向键移动光标并选中第一个分区，然后按**D**来删除它。重复这一过程直到删除了所有推荐的分区。

要建立第一个分区(a, 作为/ ——根文件系统)，请确认您已经在屏幕顶部选中了正确的slice，然后按**C**。接下来将出现一个对话框，要求您输入新分区的尺寸(如图2-23所示)。您可以输入以块为单位的尺寸，或以M表示MB、G结尾表示GB，或者C表示柱面数的方式来表达尺寸。

注意: 从FreeBSD 5.X 开始，用户可以：使用Custom Newfs (**Z**) 选项来选择UFS2 (在FreeBSD 5.1 和更高版本中的默认值)。用Auto Defaults 来创建，然后用Custom Newfs 选项，或在创建文件系统时指定 -o 2。如果您使用了Custom Newfs选项，不要忘记增加 -u 来启用SoftUpdates！

图2-23. 根目录使用空间



显示在对话框中的默认大小是使用整个分区，您可以用**Backspace**键删除这些数字然后按照上述方式输入您想要的大小，如**64M**（图2-24），然后按[OK]。

图2-24. 编辑要分区大小



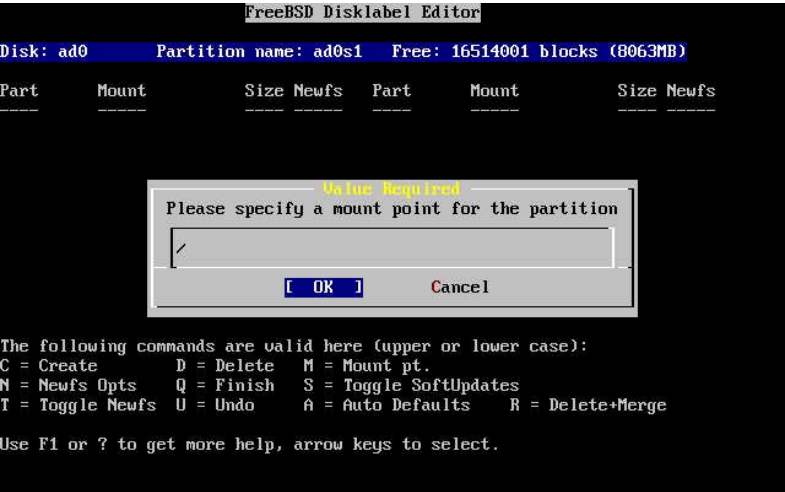
输入完大小后接着部您要建立的分区是文件系统还是交换空间，如图2-25所示。第一个分区是文件系统，所以确认选择FS后按**Enter**键。

图2-25. 选择根分区类型



最后，因为您要建立的是一个文件系统，所以必须告诉**Disklabel** 这个文件系统要挂接在什么地方，如图2-26所示。根文件系统的挂接点**/**，所以请输入**/**，然后按**Enter**键。

图2-26. 选择根挂载点



刚刚制作好的分区会显示在画面上。您应该重复上述的动作以建立其它的分区。当建立交换空间的时候，系统不会问您要将它挂载在哪里，因为交换空间是不用挂在系统上的。当您在建立最后一个分区 /usr 的时候，您可以直接使用默认的大小，即所有此分区剩余的空间。

您最终的FreeBSD DiskLabel 编辑器画面会类似图2-27, 实际数字按您的选择而有所不同。按下 **Q** 键完成分区的建立。

图2-27. Sysinstall Disklabel 编辑器



2.6 选择要安装的软件包

2.6.1 选择要安装的软件包

安装哪些软件包在很大程度上取决于系统将被用来做什么，以及有多少可用的磁盘空间。内建的选项包括了运行所需要的最小系统，到把所有软件包全都装上的常用配置。UNIX 或FreeBSD 新手通常直接选择一个设定好的软件包就可以了，而有经验的使用者则可以考虑自己订制安装哪些软件包。

按下**F1**可以看到有关软件包的更多选项信息，以及它们都包含了哪些软件，之后，可以按**Enter**回到软件包选择画面。

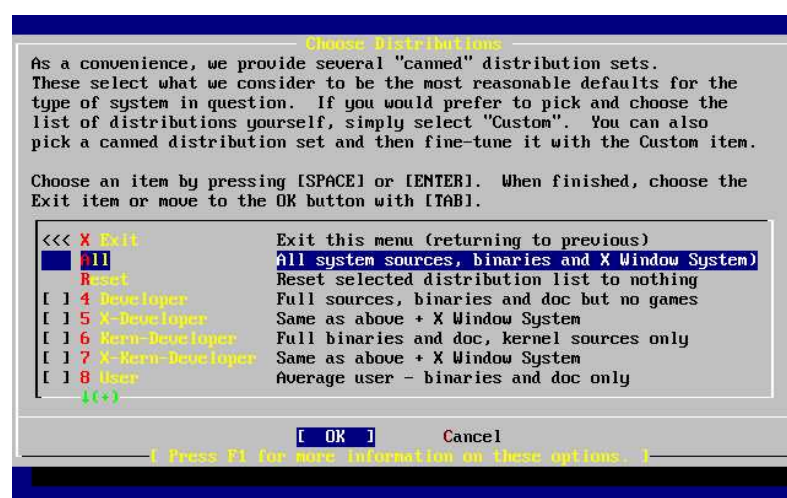
如果您想要使用图形界面，则必须选择软件包名称开头是x的那些软件包。对于X服务器的配置，以及选择默认的桌面管理器这样的工作必须在FreeBSD 安装完成之后才能作。关于配置X服务器的更多资料可以在第5章找到。

默认的X11版本取决于您所安装的FreeBSD版本。对于FreeBSD 5.3以前的版本，安装的将是**XFree86 4.X**。对于FreeBSD 5.3和以后的版本，默认的则是**Xorg**。

如果需要定制内核，您还需要选择包含源代码的那个选项。要了解为什么应该编译和构建新的内核，请参见第8章。

显然，包含所有组件的系统是最万能的。如果磁盘空间足够，用光标键选择图2-28中的**All**并按**Enter**。如果担心磁盘空间不够的话，则选择最合适的选项。不要担心选择的是否是最合适的，因为其他软件包可以在安装完毕后再加入进来。

图2-28. 选择软件包



2.6.2 安装ports软件包

当选择完您想要安装的部分后，接着会询问您要不要安装FreeBSD Ports 软件包；Ports软件包可以让您简单方便地安装软件包。Ports本身并不包含编辑软件所需要的程序源代码，而是一个包含自动下载、编辑以及安装的文档集合。第4章一章讨论如何使用Ports。

安装程序并不会检查您是否有足够的硬盘空间来放ports,所以,如果要安装ports软件所,请先确定您有足够的硬盘空间。FreeBSD 6.0版本FreeBSD Ports Collection 大约占用440 MB 大小的硬盘空间。您要为这些版本设置大一点的值来安装它们。

User Confirmation Requested

Would you like to install the FreeBSD Ports Collection?

This will give you ready access to over 13,300 ported software packages, at a cost of around 440 MB of disk space when "clean" and possibly much more than that if a lot of the distribution tarballs are loaded (unless you have the extra CDs from a FreeBSD CD/DVD distribution available and can mount it on /cdrom, in which case this is far less of a problem).

The Ports Collection is a very valuable resource and well worth having on your /usr partition, so it is advisable to say Yes to this option.

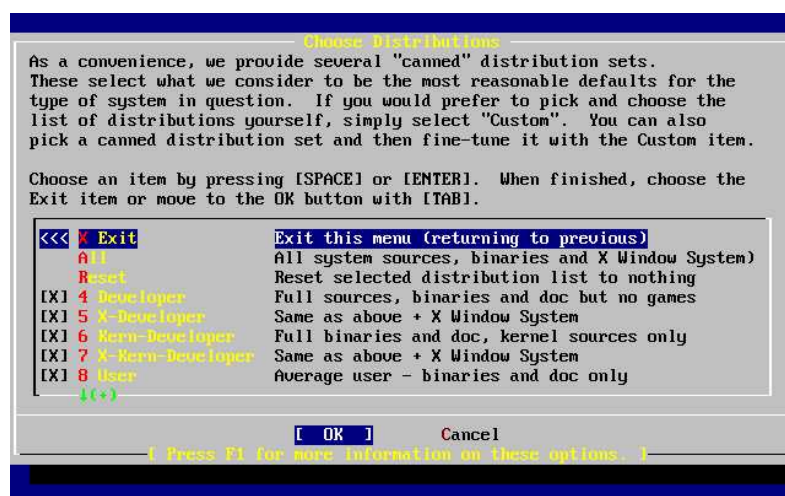
For more information on the Ports Collection & the latest ports, visit:

<http://www.FreeBSD.org/ports>

[Yes] No

选择[Yes] 将会安装Ports Collection, 而选择[No] 则将跳过它。选好后按**Enter** 继续。此后, 选择安装的软件包的屏幕将再次出现。

图2-29. 确认您要安装的软件包



如果对您选择感到满意, 请选择Exit 退出, 确保[OK] 被高亮显示, 然后按**Enter** 继续。

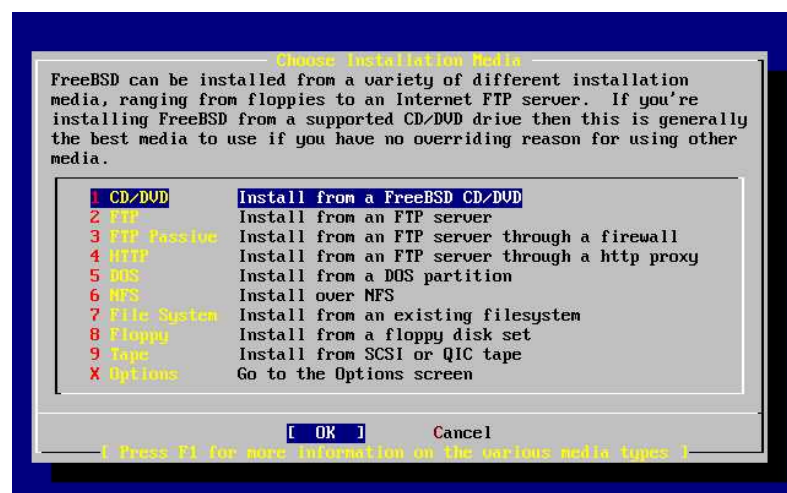
2.7 选择您要使用的安装介质

如果要从CDROM 或DVD安装，使用方向键将光标移到Install from a FreeBSD CD/DVD。确认[OK] 被选取，然后按Enter 开始安装程序。

如果要使用其它的方式安装，请选择适当的安装介质然后按照屏幕指示进行安装。

按F1 可以显示安装介质的在线说明。按一下Enter 可返回选择安装介质画面。

图2-30. 选择安装介质



FTP安装模式: 使用FTP安装，有三种方式：主动式（active）FTP、被动式（passive）FTP 或是透过HTTP代理服务器。

主动式FTP: 从FTP服务器安装

这个选项将会使所有的FTP传输使用“Active”模式。这将无法通过防火墙，但是可以使用在那些比较早期，不支持被动模式的FTP站。如果您的连接在使用被动（默认值）模式卡住了，请换主动模式看看！

被动模式FTP: 通过防火墙从FTP服务器安装

此选项会让sysinstall 使用“Passive”模式来安装。这使得使用者可以穿过不允许用非固定TCP PORTS连入的防火墙。

FTP 透过HTTP 代理服务器: 透过HTTP代理服务器，由FTP服务器安装

此选项会让sysinstall 通过HTTP协议（像浏览器一样）连到proxy服务器。proxy服务器会解释送出的请求，然后通知FTP服务器。因为通过HTTP协议，所以可以穿过防火墙。要用这种方式，您必须指定proxy服务器的地址。

对于一个FTP 代理服务器而言，通常在使用者登入名称中加入您要登入的服务器的用户名，加在“@”符号后面。然后代理服务器就会“假装”成一个真的服务器。例如，假设您要从ftp.FreeBSD.org 安装，通过FTP 代理服务器foo.example.com，使用1024端口。

在这种情况下，您可以到options 菜单，将FTP username 设为ftp@ftp.FreeBSD.org，密码设为您的电子邮件地址。安装介质部分，指定FTP (或是被动式FTP，如果代理服务器支持的话) 以及URL为ftp://foo.example.com:1234/pub/FreeBSD。

因为ftp.FreeBSD.org的/pub/FreeBSD 目录会被抓取到foo.example.com之下，您就可以从这台 机器(会从ftp.FreeBSD.org 抓取文件) 安装。

2.8 安装确认

到此为止，可以开始进行安装了，这也是您避免更动到您的硬盘的最后机会。

```

User Confirmation Requested
Last Chance! Are you SURE you want to continue the installation?

If you're running this on a disk with data you wish to save then WE
STRONGLY ENCOURAGE YOU TO MAKE PROPER BACKUPS before proceeding!

We can take no responsibility for lost disk contents!

```

```
[ Yes ]    No
```

选择[Yes] 然后按下**Enter** 确认安装

安装所需的时间会根据您所选择的软件、安装介质以及您电脑的速度而有所不同。在安装的过程中会有一些信息来显示目前的进度。

当您看到下面的信息表示已经安装完成了：

```

Message

Congratulations! You now have FreeBSD installed on your system.

We will now move on to the final configuration questions.
For any option you do not wish to configure, simply select No.

If you wish to re-enter this utility after the system is up, you may
do so by typing: /stand/sysinstall .

```

```
[ OK ]
```

```
[ Press enter to continue ]
```

按下**Enter** 以进行安装后的配置。

选择[No] 然后按**Enter** 会取消安装，不会对您的系统造成更动。您会看到下面的信息：

```

Message

Installation complete with some errors. You may wish to scroll
through the debugging messages on VTY1 with the scroll-lock feature.
You can also choose "No" at the next prompt and go back into the
installation menus to retry whichever operations have failed.

```

[OK]

产生这个信息是因为什么东西也没有安装，按下**Enter**后会离开安装程序回到主安装界面。从主安装界面可以退出安装程序。

2.9 安装后的配置

安装成功后，就可以进行进一步的配置了。引导新安装的FreeBSD系统之后，使用sysinstall (/stand/sysinstall 如果您使用的是FreeBSD 5.2 之前的版本)，并选择Configure。

2.9.1 配置网卡

如果您之前配置用PPP通过FTP安装，那么这个画面将不会出现；正像所说的那样，您可以稍后再做配置。

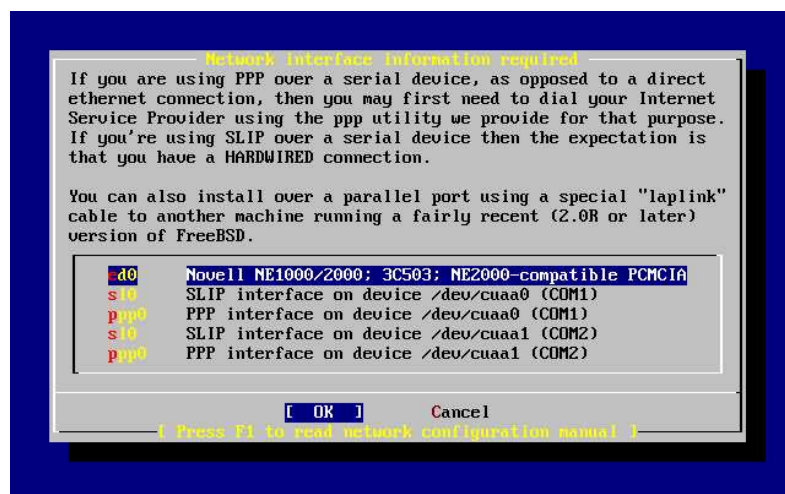
如果想更多的了解网卡或将FreeBSD配置为网关或路由器，请参考Advanced Networking 的相关文章。

```
User Confirmation Requested
Would you like to configure any Ethernet or SLIP/PPP network devices?
```

[Yes] No

如果要配置网卡，请选择[Yes]然后按**Enter**。否则请选择[No]继续。

图2-31. 选择网卡设备



用方向键选择您要配置的网卡接口，然后按**Enter**。

```
User Confirmation Requested
Do you want to try IPv6 configuration of the interface?
```

Yes [No]

目录私人区域网络IP协议IPv4已经足够，所以选择[No]然后按**Enter**。

如果想试试新的IP通信协议IPv6，使用RA服务，请选择[Yes] 然后按**Enter**。寻找RA服务器将会花费几秒的时间。

```
User Confirmation Requested
Do you want to try DHCP configuration of the interface?
```

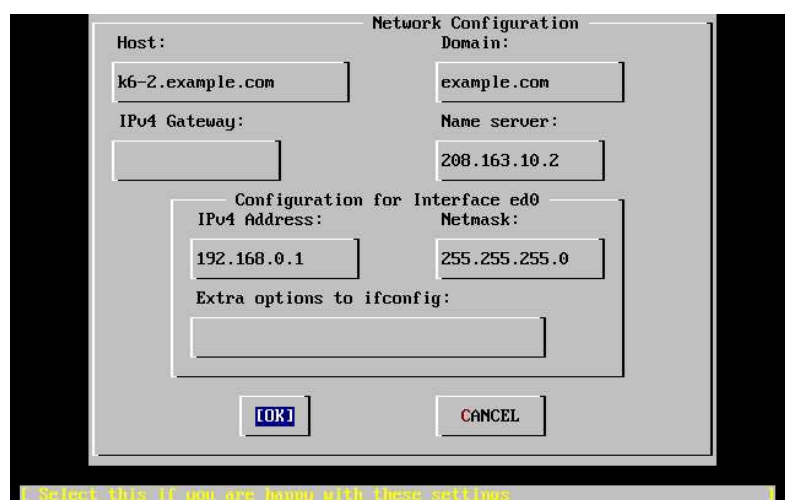
```
Yes    [ No ]
```

如果您不需要DHCP (Dynamic Host Configuration Protocol 动态主机配置协议)，选择[No] 然后按**Enter**。

选择[Yes] 会执行**dhclient**，如果成功，它会自动将网络配置信息填上。更多的信息请参考第25.5节。

下面的网络配置显示了怎样把以太网设备配置成区域网络网关的角色。

图2-32. 配置ed0接口



使用**Tab**键可以在各个栏目之间进行切换，请输入适当的信息：

Host（机器名称）

完整的机器名称，例如本例中的k6-2.example.com。

Domain（域名）

您机器所在的域名称，如本例的example.com

IPv4 Gateway（IPv4网关）

输入将数据包传送到远端网络的机器IP地址。只有当机器是网络上的一个接点时才要输入。如果这台机器要作为您局域网的网关，**请将此处设为空白**。IPv4网关，也被称作默认网关或默认路由器。

域名服务器

本地网络中的域名服务器的IP地址。本例中假设机器所在的网络中没有域名服务器，所以填入的是ISP提供的域名服务器地址（208.163.10.2。）

IPv4 地址

本机所使用的IP地址。本例为192.168.0.1。

子网掩码

本范例中的IP地址属于一个C类地址（192.168.0.0 - 192.168.255.255）。默认的子网掩码为（255.255.255.0）。

ifconfig 额外参数设定

任何ifconfig命令跟网卡接口有关的参数。本范例中没有。

使用**Tab** 键选择[OK]然后按**Enter**键。

```
User Confirmation Requested
Would you like to Bring Up the ed0 interface right now?
```

```
[ Yes ]    No
```

选择[Yes] 然后按**Enter** 将会将机器的网卡转为启用状态。机器下次启动的时候即可使用。

2.9.2 配置网关

```
User Confirmation Requested
Do you want this machine to function as a network gateway?
```

```
[ Yes ]    No
```

如果这台机器要作为本地网络和其它机器之间传送数据包的网关，请选择[Yes] 然后按**Enter**。如果这台机器只是网络上的普通节点，请选择[No] 并按**Enter** 继续。

2.9.3 配置网络服务

```
User Confirmation Requested
Do you want to configure inetd and the network services that it provides?
```

```
Yes    [ No ]
```

如果选择[No]，许多网络服务，如**telnetd** 将不会启用。这表示远端用户将无法**telnet** 进入这台机器。本机器上的用户还是可以**telnet**到远端机器的。

这些服务可以在安装完成后修改/etc/inetd.conf 配置文件来启用它们。请参阅第25.2.1 节 以获得更多的信息。

如果您想现在就配置这些网络服务，请选择[Yes]，然后会看到下面的信息：

```
User Confirmation Requested
The Internet Super Server (inetd) allows a number of simple Internet
services to be enabled, including finger, ftp and telnetd.  Enabling
these services may increase risk of security problems by increasing
the exposure of your system.
```

With this in mind, do you wish to enable inetd?

[Yes] No

选择[Yes]继续。

User Confirmation Requested

inetd(8) relies on its configuration file, /etc/inetd.conf, to determine which of its Internet services will be available. The default FreeBSD inetd.conf(5) leaves all services disabled by default, so they must be specifically enabled in the configuration file before they will function, even once inetd(8) is enabled. Note that services for IPv6 must be separately enabled from IPv4 services.

Select [Yes] now to invoke an editor on /etc/inetd.conf, or [No] to use the current settings.

[Yes] No

选择[Yes]将允许您添加网络服务(或将相应网络服务每行开头的# 除掉即可。)

图2-33. 编辑inetd.conf配置文件

```

^I (escape) menu ^Y search prompt ^K delete line ^P prev li ^G prev page
^O ascii code ^X search ^L undelete line ^N next li ^U next page
^U end of file ^A begin of line ^W delete word ^B back 1 char
^T begin of file ^E end of line ^R restore word ^F forward 1 char
^C command ^D delete char ^J undelete char ^Z next word
L: 1 C: 1 =====
Sep 22 23:42:04 k6-2 login: ROOT LOGIN (root) ON ttyv121:13:33 obrien Exp $
#
# Internet server configuration database
#
# Define *both* IPv4 and IPv6 entries for dual-stack support.
# To disable a service, comment it out by prefixing the line with '#'.
# To enable a service, remove the '#' at the beginning of the line.
#
#ftp stream tcp nowait root /usr/libexec/lukemftpd ftpd -l -r
#ftp stream tcp nowait root /usr/libexec/ftpd ftpd -l
#ftp stream tcp6 nowait root /usr/libexec/ftpd ftpd -l
#telnet stream tcp nowait root /usr/libexec/telnetd telnetd
#telnet stream tcp6 nowait root /usr/libexec/telnetd telnetd
#shell stream tcp nowait root /usr/libexec/rshd rshd
#shell stream tcp6 nowait root /usr/libexec/rshd rshd
#login stream tcp nowait root /usr/libexec/rlogind rlogind
#login stream tcp6 nowait root /usr/libexec/rlogind rlogind
#finger stream tcp nowait/3/10 nobody /usr/libexec/fingerd fingerd -s
file "/etc/inetd.conf", 119 lines

```

在加入您想启用的服务后，按下**Esc**键会出现一个对话框可以让您离开以及保存修改。

2.9.4 匿名FTP

User Confirmation Requested

Do you want to have anonymous FTP access to this machine?

Yes [No]

2.9.4.1 不允许匿名FTP访问

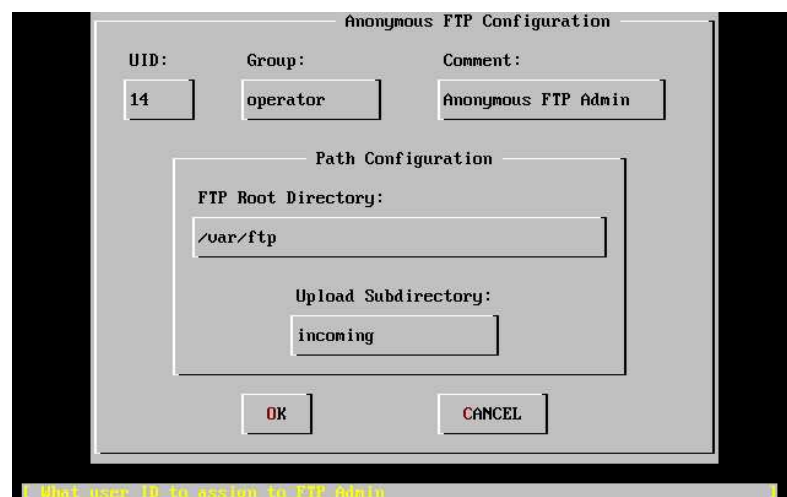
选择默认的[No] 并按下 **Enter** 键将仍然可以让在这台机器上有账号的用户访问FTP。

2.9.4.2 允许匿名FTP访问

如果您选择允许匿名FTP 存取，那么网络中任何人都可以使用FTP来访问您的机器。在启用匿名访问之前应该考虑网络的安全问题。如果要知道更多有关网络安全的信息，请参阅第14 章。

要启用FTP匿名访问，用方向键选择[Yes] 然后按**Enter**键。您会看到下面（或类似）的画面：

图2-34. 默认的匿名FTP 配置



按**F1** 键可以查看在线帮助文档：

This screen allows you to configure the anonymous FTP user.

The following configuration values are editable:

UID: The user ID you wish to assign to the anonymous FTP user.
All files uploaded will be owned by this ID.

Group: Which group you wish the anonymous FTP user to be in.

Comment: String describing this user in /etc/passwd

FTP Root Directory:

Where files available for anonymous FTP will be kept.

Upload subdirectory:

Where files uploaded by anonymous FTP users will go.

默认的FTP根目录将放在/var目录下。如果您的/var目录空间不足以应付您的FTP需求，您可以将FTP的根目录改为/usr目录下的/usr/ftp目录。

当您的一切配置都满意后，请按**Enter**键继续。

```
User Confirmation Requested
Create a welcome message file for anonymous FTP users?
```

```
[ Yes ]    No
```

如果您选择[Yes]并按下**Enter**键，系统会自动打开文本编辑器让您编辑FTP的欢迎信息。

图2-35. 编辑FTP欢迎信息

```
^[(escape) menu ^y search prompt ^k delete line ^p prev line ^g prev page
^o ascii code ^x search ^l undelete line ^n next line ^u next page
^u end of file ^a begin of line ^w delete word ^b back char ^z next word
^t begin of file ^e end of line ^r restore word ^f forward char
^c command ^d delete char ^j undelete char ESC-Enter: exit
=====
Your welcome message here.
=====
file "/var/ftp/etc/ftpmotd", 1 lines, read only
```

此文本编辑器叫做ee。按照指示修改信息文本或是稍后再用您喜爱的文本编辑器来修改。请记住画面下方显示的文件位置。

按**Esc**将弹出一个默认为a) leave editor的对话框。按**Enter**退出并继续。再次按**Enter**将保存修改。

2.9.5 配置网络文件系统

网络文件系统(NFS)可以让您可以在网络上共享您的文件。一台机器可以配置成NFS服务器、客户端或两者并存。请参考第25.3节以获得更多的信息。

2.9.5.1 NFS 服务器

```
User Confirmation Requested
Do you want to configure this machine as an NFS server?
```

```
Yes    [ No ]
```

如果您不想安装网络文件系统，请选择[No]然后按**Enter**键。

如果您选择[Yes]将会出现一个对话框提醒您必须先建立一个exports文件。

Message

Operating as an NFS server means that you must first configure an /etc/exports file to indicate which hosts are allowed certain kinds of access to your local filesystems.

Press [Enter] now to invoke an editor on /etc/exports

[OK]

按**Enter** 键继续。系统会启动文本编辑器让您编辑exports 文件。

图2-36. 编辑exports文件

```

^i (escape) menu ^y search prompt ^k delete line ^p prev line ^g prev page
^o ascii code ^x search ^l undelete line ^n next line ^v next page
^u end of file ^a begin of line ^w delete word ^b back char ^z next word
^t begin of file ^e end of line ^r restore word ^f forward char
^c command ^d delete char ^j undelete char ESC-Enter: exit
=====
#The following examples export /usr to 3 machines named after ducks,
#/home and all directories under it to machines named after dead rock stars
#and, finally, /a to 2 privileged machines allowed to write on it as root.
#/usr      huey louie dewie
#/home     -alldirs  janice jimmy frank
#/a        -maproot=0 bill albert
#
# You should replace these lines with your actual exported filesystems.

file "/etc/exports", 9 lines

```

按照指示加入真实输出的文件目录或是稍后用您喜爱的编辑器自行编辑。请记住画面下方显示的文件名称及位置。

按下**Esc** 键会出现一具对话框，默认选项是a) leave editor。按下**Enter** 离开并继续。

2.9.5.2 NFS 客户端

NFS 客户端允许您的机器访问NFS服务器。

User Confirmation Requested

Do you want to configure this machine as an NFS client?

Yes [No]

按照您的需要，选择[Yes] 或[No] 然后按**Enter**。

2.9.6 安全配置

“安全配置” 中包含了一些可以通过启用或停用某些程序来达到某些程序的安全性配置。安全配置越严格，则默认启动的程序就越少。基本的原则是：除非必要，否则不要执行一些可有可无的程序。

请注意，安全文件的配置都是默认值，在安装完成后您可以随时通过编辑/etc/rc.conf配置文件来改变这些配置。如果想得到更多的信息请参阅rc.conf(5) 手册。

下表说明每一种安全等级的意义。每列所代表的是安全等级，每行所代表的是程序或功能是启用还是停用。

表2-4. 可能的安全等级

	极/高度安全	中度安全
sendmail(8)	否	是
sshd(8)	否	是
portmap(8)	否	不一定 ^a
NFS server	否	是
securelevel(8)	是 ^b	否

表注: a. 如果之前安装时配置机器为NFS客户端或服务器，则会启用些项目。 b. 如果打算将安全级配置securelevel 设置

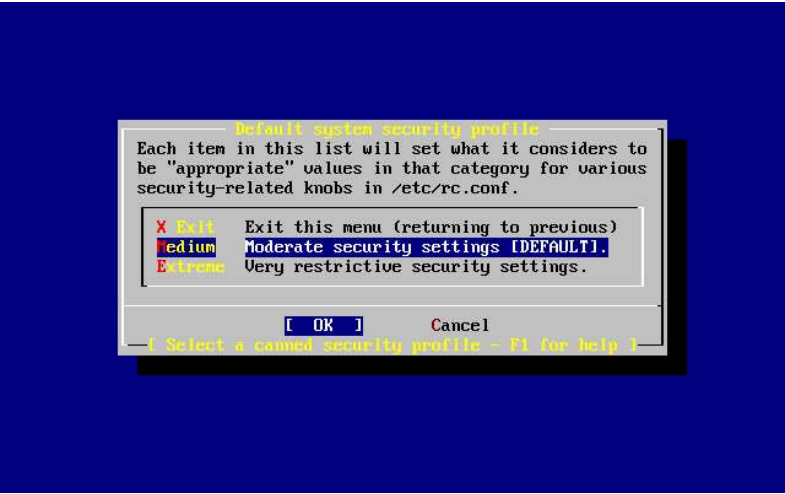
```

User Confirmation Requested
Do you want to select a default security profile for this host (select
No for "medium" security)?

[ Yes ]    No
```

选择[No] 并按**Enter** 会将安全等级高为中度安全。
选择[Yes] 并按**Enter**将允许您选择不同程序的安全等级。

图2-37. 选择安全等级



按**F1** 显示在线帮助；按**Enter** 键可以回到选择画面。
如果您没有什么特殊的等级需求，请用方向键选择中度，确定选择了[OK] 然后按**Enter**。
依据您选择的安全等级，会显示相对应的确认信息。

```

Message

Moderate security settings have been selected.
```

Sendmail and SSHd have been enabled, securelevels are disabled, and NFS server setting have been left intact. PLEASE NOTE that this still does not save you from having to properly secure your system in other ways or exercise due diligence in your administration, this simply picks a standard set of out-of-box defaults to start with.

To change any of these settings later, edit /etc/rc.conf

[OK]

Message

Extreme security settings have been selected.

Sendmail, SSHd, and NFS services have been disabled, and securelevels have been enabled. PLEASE NOTE that this still does not save you from having to properly secure your system in other ways or exercise due diligence in your administration, this simply picks a more secure set of out-of-box defaults to start with.

To change any of these settings later, edit /etc/rc.conf

[OK]

按下**Enter** 继续安装后面的配置。

警告: 安全等级并非万能药！即使您选择极度安全，您还是必须时常阅读第C.1节邮件列表中有关安全的部分、使用有效的密码以及平常就注意安全问题。这里只是稍为配置一下常用的安全等级而已。

2.9.7 配置系统终端

系统提供了几个选项可以让您配置终端的表现方式。

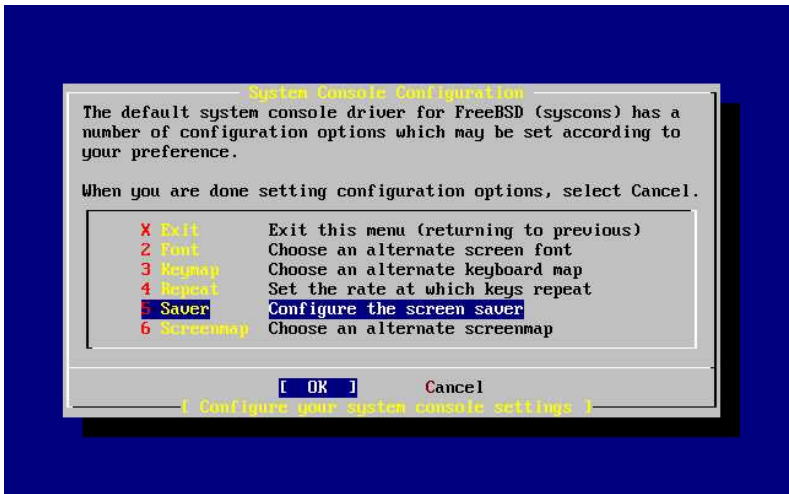
User Confirmation Requested

Would you like to customize your system console settings?

[Yes] No

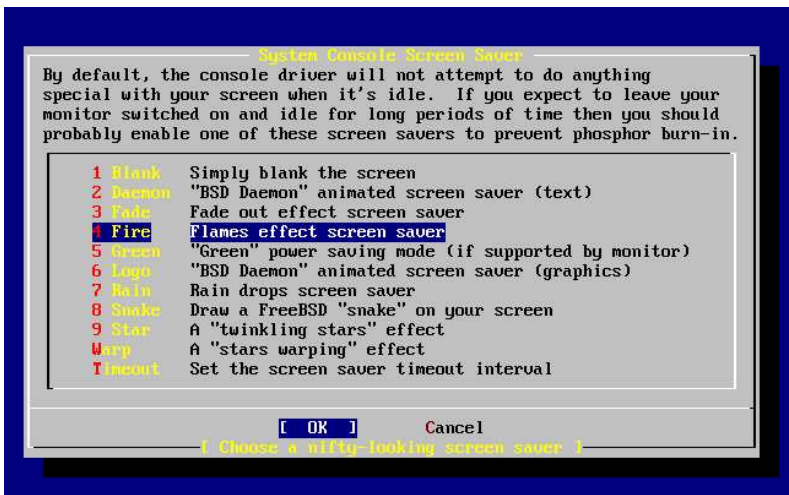
要查阅及配置这些选项，请选择[Yes] 并按**Enter**。

图2-38. 系统终端配置选项



最常用的选项就是屏幕保护程序了。使用方向键将光标移动到Saver 然后按**Enter**。

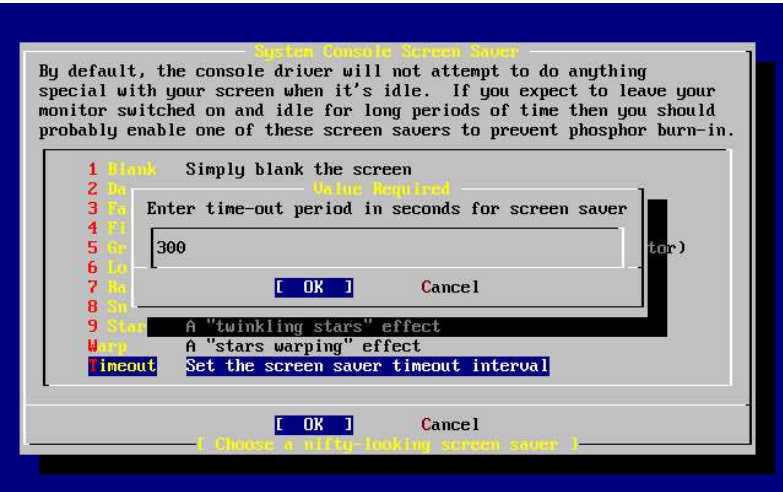
图2-39. 屏幕保护程序选项



选择您想使用的屏幕保护程序，然后按**Enter**。之后回到系统终端配置画面。

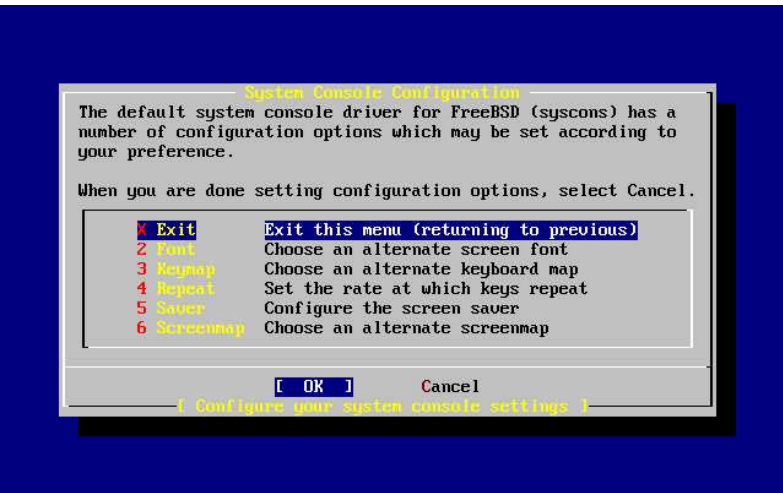
默认开启屏幕保护程序的时间是300秒。如果要更改此时间，请再次选择Saver。然后选择Timeout 并按**Enter**键。系统会弹出一个对话框如下：

图2-40. 屏幕保护时间设置



您可以直接改变这个值，然后选[OK]并按**Enter** 键回到系统终端配置画面。

图2-41. 退出系统终端配置



选择Exit 然后按下**Enter** 键会回到安装后的配置画面。

2.9.8 配置时区

配置您机器的时区可以让系统自动校正任何区域时间的变更并且在执行一些跟时区相关的程序时不会出错。

例子中假设此台机器位于美国东部的时区。请参考您所在的地理位置来配置。

User Confirmation Requested
Would you like to set this machine's time zone now?

[Yes] No

选择[Yes] 并按下**Enter**键以配置时区。

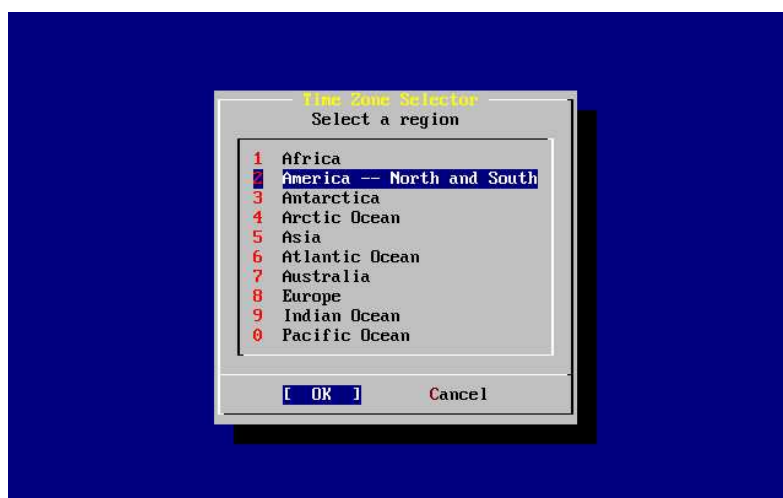
User Confirmation Requested

Is this machine's CMOS clock set to UTC? If it is set to local time or you don't know, please choose NO here!

Yes [No]

这里按照您机器时间的配置，选择[Yes] 或[No] 然后按**Enter**。

图2-42. 选择您所处的地理区域



请选择适当的区域然后按**Enter**。

图2-43. 选择您所在的国家



选择您所在的国家然后按**Enter**。

图2-44. 选择您所在的时区



选择您所在的时区然后按**Enter**。

```
Confirmation
Does the abbreviation 'EDT' look reasonable?

[ Yes ]   No
```

检查一下时区的缩写是否正确，如果没错，请按**Enter** 返回系统安装后的配置画面。

2.9.9 Linux 兼容性

```
User Confirmation Requested
Would you like to enable Linux binary compatibility?

[ Yes ]   No
```

选择[Yes] 并按下**Enter** 键，将允许您在FreeBSD中执行Linux的软件。安装程序会安装一些为了跟Linux 兼容的软件包。

如果您是通过FTP安装，那么您必须连到网络上。有时候FTP站并不会包含所有的安装软件包（例如Linux兼容软件包）；不过，稍后您还可以再安装这个项目。

2.9.10 配置鼠标

此选项可以让您在终端上使用三键鼠标剪贴文字。如果您用的鼠标是两个按钮，请参考手册moused(8)；以取得有关模拟三键鼠标的信息。范例中使用的鼠标不是USB接口。（例如ps/2或com接口的鼠标）：

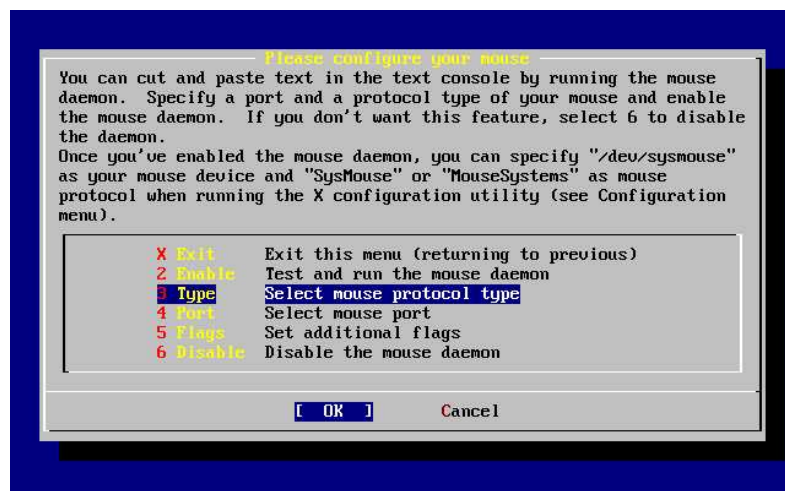
```
User Confirmation Requested
```

Does this system have a non-USB mouse attached to it?

[Yes] No

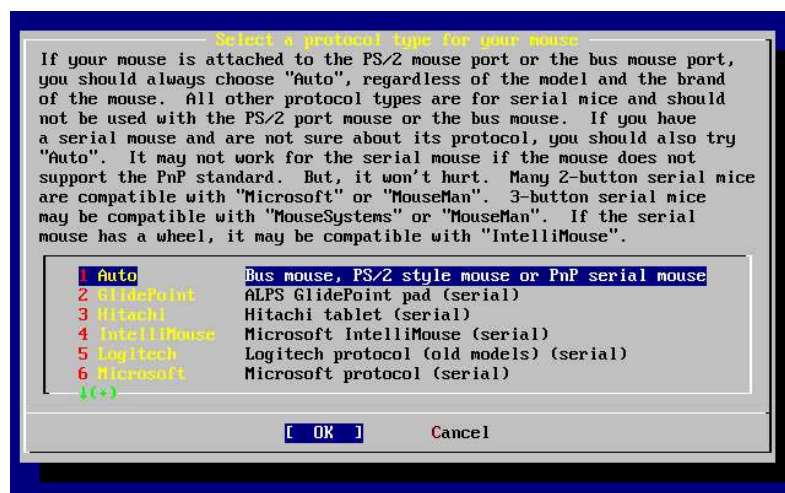
如果您使用的不是USB鼠标，请选择[Yes]；否则请选择[No]。然后按**Enter**。

图2-45. 选择鼠标类型



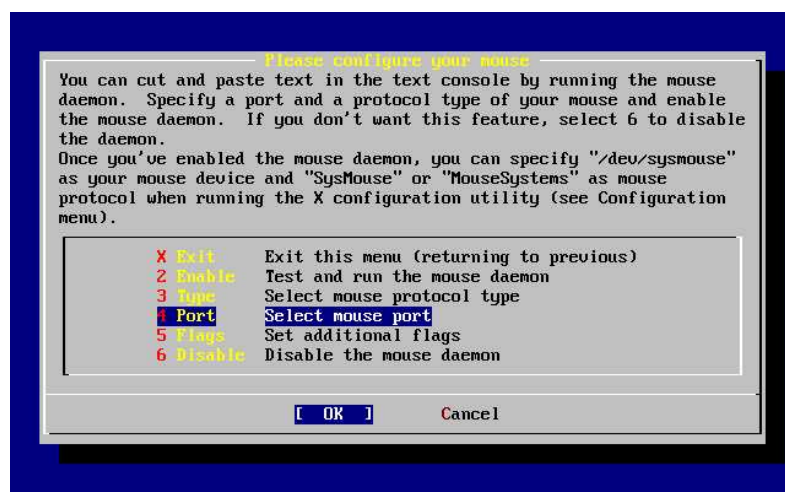
使用方向键选择Type 然后按**Enter**。

图2-46. 设置鼠标协议



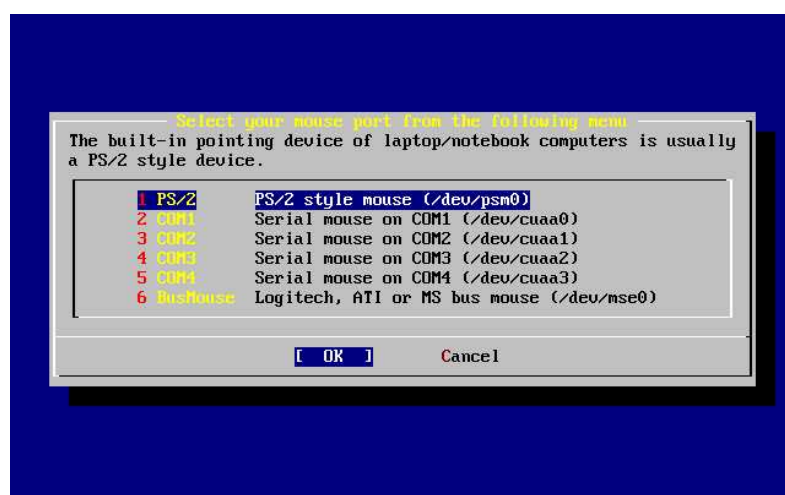
在这个例子中使用的类型是ps/2鼠标，所以可以使用默认的Auto（自动）。您可以用方向键选择合适的项目，确定选择了[OK] 后按**Enter** 键离开此画面。

图2-47. 配置鼠标端口



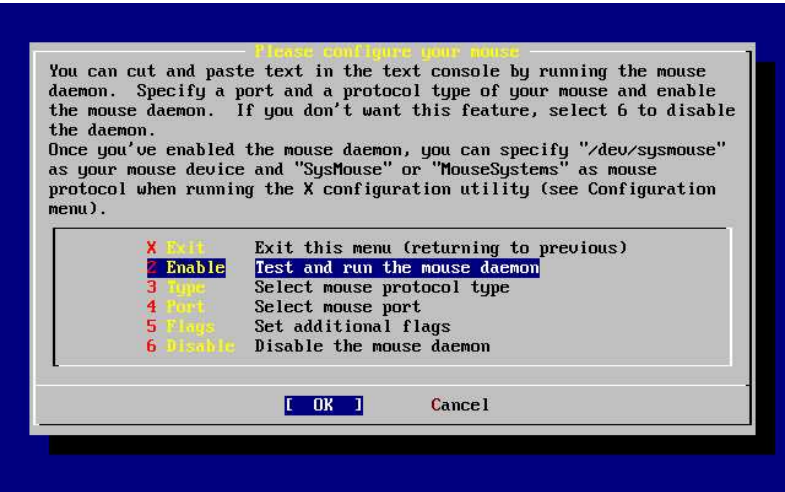
选择Port 然后按Enter。

图2-48. 配置鼠标端口



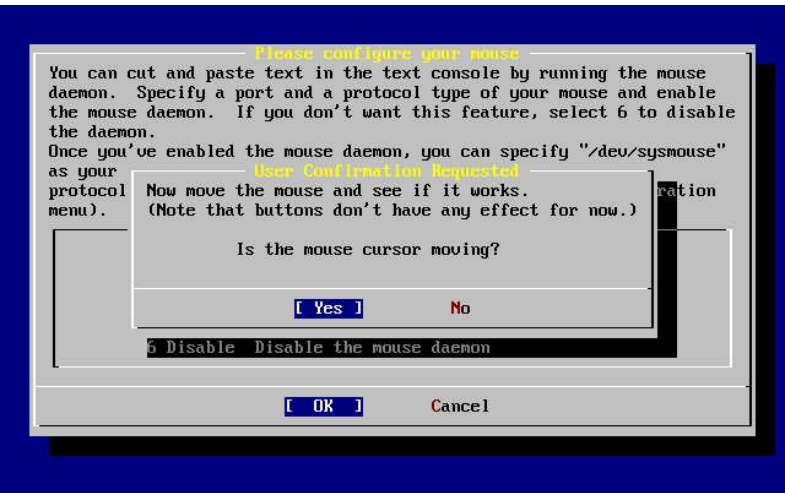
假设这台机器用的是ps/2鼠标，您可以采用默认的PS/2 选项。请选择适当的项目然后按Enter。

图2-49. 启动鼠标服务进程



选择Enable然后按Enter 来启动和测试鼠标。

图2-50. 测试鼠标功能



鼠标指针可以在屏幕上移动，指明鼠标服务已经正常启用。那么请选择[Yes] 按Enter键。否则鼠标没有配置成功——选择[No] 并尝试不同的配置选项。

选择Exit 并按Enter 退回到系统安装完成后的配置画面。

2.9.11 配置其他网络服务

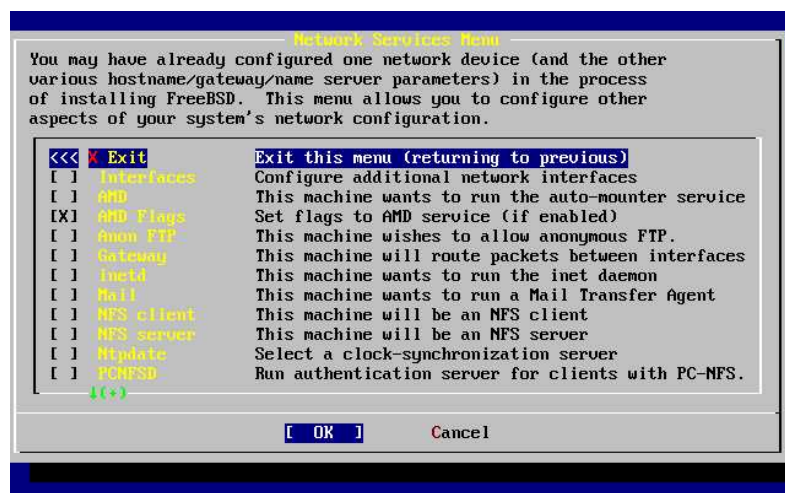
Contributed by Tom Rhodes.

配置网络服务总是让那些新手敬畏，因为他们缺乏在这个领域应有的基础知识。网络，包括因特网有许多关于现代操作系统包括FreeBSD;的评论文章。这些文章对于理解FreeBSD拥有的广泛的网络性能是非常有帮助的。在安装这些服务的过程中也能让用户理解它们可用的各种服务。

网络服务是一些可以使在网络的任何人来访问您提供的服务的程序。有许多努力想使这些程序不会有任何的“伤害”。不幸的是，这些程序并不是十全十美的，黑客可能会掌握程序中的一些漏洞来进行攻击。只启用一些您熟悉的和需要的服务十分重要。如果您存在一些疑虑或没有启用这些服务的必要那么最好不要使用这些服务。您可以事后通过运行`sysinstall` 程序或使用`/etc/rc.conf` 配置文件来启用它们。

选择“Networking”选项将下显示一个类似下面的菜单：

图2-51. 网络配置之上层配置



第一个选项，Interfaces，已经在前面第2.9.1节中讨论过，因此这里可以略过。

选择AMD选项，添加BSD对自动挂载程序的支持。这个程序和NFS协议一起使用不需要经过特别的设置就可以自动挂载远程文件系统。

下一行是AMD Flags的参数选项。当您选择后，会弹出一个子菜单来让您选择AMD的参数。菜单中包含一系列的选项：

```
-a /.amd_mnt -l syslog /host /etc/amd.map /net /etc/amd.map
```

-a选项用来设置默认的挂载位置，这里使用的是`/.amd_mnt`目录。-l指定默认的日志文件；但是，当`syslogd`被指定用来接收所有的日志时，那么它们会被送到系统日志程序。`/host`被用来挂载远程主机输出的一个文件系统，例子中`/net`目录被用来挂载从IP输出的一个文件系统。`/etc/amd.map`文件定义了AMD的默认输出选项。

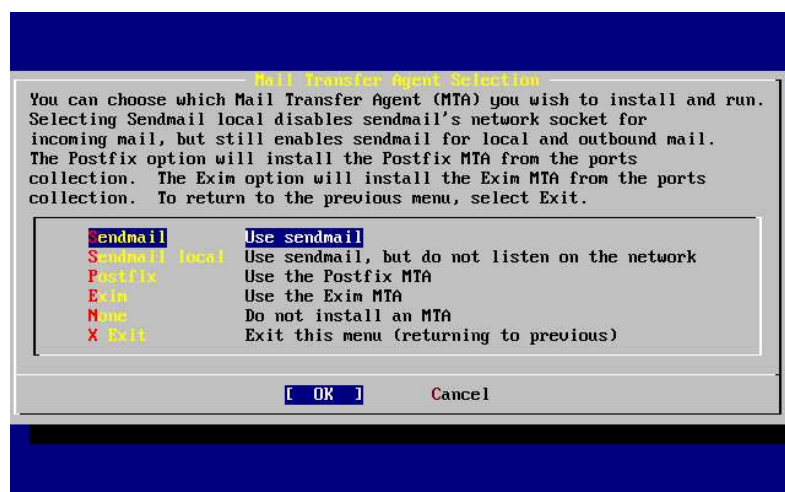
Anon FTP允许匿名FTP访问。选中这个选项，可以使这台机器成为一台匿名FTP服务器。要注意启用这个选项的安全风险。其它的菜单将说明一些安全问题和更深入的配置。

Gateway配置菜单可以使本机器成为一台以前我们提到过的网关。如果您在安装过程中偶尔选中了它，也可以在这里选中这个选项来取消。

Inetd选项用来配置或完全禁止我们在上面讨论的inetd(8)守护程序。

Mail可以用来配置系统默认的MTA或邮件传输代理。选择这个选项将了出现下面的菜单：

图2-52. 选择默认的MTA



这里给您提供了一个安装默认MTA 的机会。MTA 用来投递本系统上用户邮件到因特网去。

选择Sendmail 将会安装FreeBSD默认的流行的的**sendmail** 服务程序。Sendmail local 选项用来设置**sendmail** 默认的MTA，也可以禁止它从Internet接收邮件的能力。还有其它的一些选项如：Postfix 和Exim 都类似于Sendmail的角色。它们两者也可以投递邮件；有些用户更喜欢选择使用Sendmail、MTA二者之一。

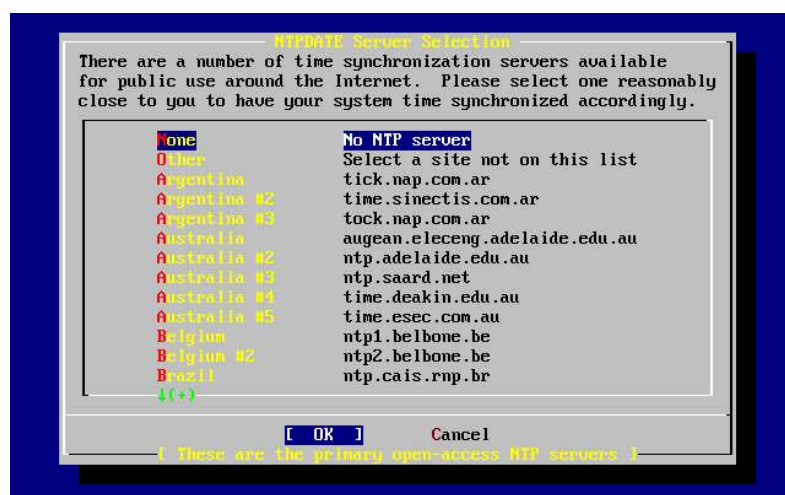
选择MTA或不选择它之后，网络配置菜单的下一个选项是NFS client 客房端程序。

NFS client 客房端可以使系统通过NFS 与服务器进行通信。NFS 服务器通过NFS 协议可以使其它在网络上的机器来访问自己的文件系统。如果这台机器要作为一台独立的服务器，这个选项可以保留不选。下面可能还有更多的配置，关于客户端和服务器的配置请参阅第25.3 节 一节。

接下来的NFS 服务器选项，可以允许您把系统设备成为一台NFS 服务器。这需要更多的信息来启动远程过程调用（RPC）服务。RPC用来连接调用两台机器上的程序。

下一项是Ntpdate 选项，处理时间同步。当选择它后，会出现一个像下面所似的菜单：

图2-53. Ntpdate 配置

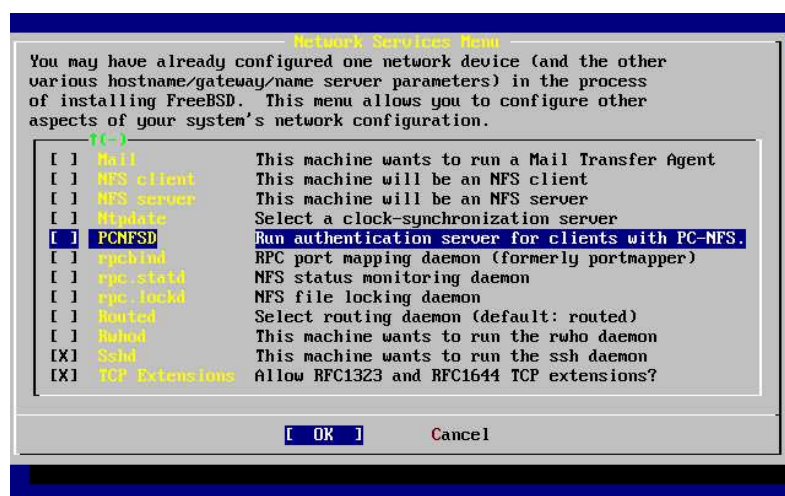


从这个菜单选择一个离您最近的服务器。在您连接这台服务器时，除去连接时的反应时间，时间同步最精确的服务器。

下一个选项是PCNFSD。这个选项将安装第三方软件包net/pcnfsd。它可以用来为无法自行提供NFS认证服务的操作系统，如微软的MS-DOS 提供服务。

滚屏到下一页看一下其它选项:

图2-54. 网络配置之下层配置



rpcbind(8)、rpc.statd(8)和rpc.lockd(8)这三个程序是用来提供远程过程调用(RPC)服务的。rpcbind 程序管理NFS 服务器和客户端的通信，这是NFS 正确工作的必要前提。rpc.statd 程序可以和其它主机上rpc.statd 程序交互，以提供的状态监控。这些状态报告默认情况下会保存到/var/db/statd.status 文件中。最后的一项是rpc.lockd 选项，如果启用，则将提供文件上锁服务。通常将它和rpc.statd 联用，以监视哪些主机会请求对文件执行上锁操作，以及这种操作的频繁程度。尽管后两项功能对于调试非常有用，但它们并不是NFS 服务器和客户端正常运行所必需的。

下一个项目是**Routed**，这是一个路由程序。**routed(8)** 程序管理网络路由表，发现多播路由，并且支持在网络上与它物理相连的主机来拷贝它的路由表的请求。它被广泛的应用在本地网络中并扮演网关的角色。当选择它后，一个子菜单会来询问您这个程序的默认位置。默认的位置已经被定义过，您可以选择**Enter** 键，您也可以按下其它的键。这时会出来另一个菜单来询问您传递给**routed**程序的参数。默认的是**-q** 参数。

接下来是**Rwhod** 选项，选中它会启用**rwhod(8)** 程序在系统初时化的时候。**rwhod**程序通过网络周期性的广播系统信息或以“客户”的身份来收集这些信息。更多的信息可以查看**ruptime(1)** 和**rwho(1)** 手册页。

倒数第二个选项是**sshd(8)** 程序。它可以通过使用**OpenSSH**来提供安全的shell服务，我们推荐通过使用它来使用**telnet** 和**FTP** 服务。**sshd**服务通过使用加密技术来创建从一台机器到另一台机器的安全连接。

最后有一个**TCP** 扩展选项。这可以用来扩展在**RFC 1323** 和**RFC 1644** 里定义的**TCP** 功能。当许多主机以高速连接本机时，可能会引起某些连接被丢弃。我们不推荐使用这个选项，但是当使用独立的主机时可以从它上面得到一些好处。

现在您已经配置完成了网络服务，您可以滚动屏幕到顶部选择**Exit** 项，退出进入下一个配置部分。

2.9.12 配置X Server

注意: 从FreeBSD 5.3-RELEASE 开始，X 服务的配置机制从**sysinstall** 中删掉了。您必须在安装完FreeBSD 之后再配置X 服务。关于安装和配置X 服务的进一步细节可以在第5 章 找到。如果您不是在安装5.3-RELEASE 之前的FreeBSD 版本的话，则可以跳过这一节。

要使用诸如**KDE**、**GNOME**，以及其他一些图形界面，则需要配置X 服务器。

注意: 为了以非root用户运行**XFree86** 您必须安装**x11/wrapper** 软件。在FreeBSD 4.7及以上版本是默认安装的，但以前的版本要手工安装到系统中。

要知道您的显卡是否被支持，请参考**XFree86** (<http://www.xfree86.org/>) 网站。

```

User Confirmation Requested
Would you like to configure your X server at this time?

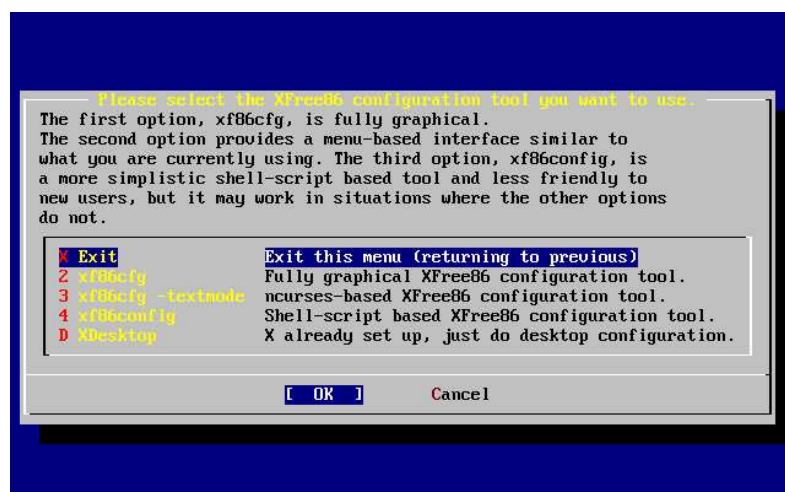
[ Yes ]   No

```

警告: 您需要了解监视器和显卡信息的制造规格。如果配置有误，可能会造成设备损毁。如果您一时没有这样的信息，请选择[No]，之后再通过**sysinstall** (对于FreeBSD 5.2 以前的版本来说，是**/stand/sysinstall**)，选择**Configure** 然后是**XFree86** 来配置。如果设置不当，X 服务器将导致系统停止响应。通常，建议您在安装完成之后再配置X 服务程序。

如果您有显卡和显示器的信息，请选择[Yes] 并按**Enter** 来配置X-server。

图2-55. 选择配置方法菜单



您可以通过许多方法来配置X server。在认真读了所有的说明后，请使用方向键来选择一种配置方式，并按**Enter**。键确认。

xf86cfg 和 **xf86cfg -textmode** 配置方法可能会使屏幕黑屏一会过一会即会启动。要有耐心。

下面将介绍**xf86config** 配置工具。根据系统硬件的不同，下面的信息可能会适当的发生变动：

Message

You have configured and been running the mouse daemon.
Choose "/dev/sysmouse" as the mouse port and "SysMouse" or
"MouseSystems" as the mouse protocol in the X configuration utility.

[OK]

[Press enter to continue]

这个信息指明，前面配置的鼠标驱动程序被检测到。按**Enter** 键继续。

启动**xf86config** 后会显示一个简单的说明：

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.

按**Enter**将启动鼠标配置。请按照指示选择“Mouse Systems”作为鼠标协议，`/dev/sysmouse`作为鼠标端口。下面的例子向您说明的是使用一个PS/2鼠标：

First specify a mouse protocol type. Choose one from the following list:

1. Microsoft compatible (2-button protocol)
2. Mouse Systems (3-button protocol) & FreeBSD moused 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 varieties 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: 2

You have selected a Mouse Systems protocol mouse. If your mouse is normally in Microsoft-compatible mode, enabling the ClearDTR and ClearRTS options may cause it to switch to Mouse Systems mode when the server starts.

Please answer the following question with either 'y' or 'n'.
Do you want to enable ClearDTR and ClearRTS? n

You have selected a three-button mouse protocol. It is recommended that you do not enable Emulate3Buttons, unless the third button doesn't work.

Please answer the following question with either 'y' or 'n'.
Do you want to enable Emulate3Buttons? y

Now give the full device name that the mouse is connected to, for example `/dev/tty00`. Just pressing enter will use the default, `/dev/mouse`.
On FreeBSD, the default is `/dev/sysmouse`.

Mouse device: `/dev/sysmouse`

下一个要配置的项目是键盘。在例子中使用的键盘一般是101-key。您可以选择不同的键盘类型或直接按**Enter**键来使用默认配置。

Please select one of the following keyboard types that is the better description of your keyboard. If nothing really matches, choose 1 (Generic 101-key PC)

- 1 Generic 101-key PC
- 2 Generic 102-key (Intl) PC
- 3 Generic 104-key PC
- 4 Generic 105-key (Intl) PC
- 5 Dell 101-key PC
- 6 Everex STEPhote
- 7 Keytronic FlexPro
- 8 Microsoft Natural
- 9 Northgate OmniKey 101
- 10 Winbook Model XP5
- 11 Japanese 106-key
- 12 PC-98xx Series
- 13 Brazilian ABNT2
- 14 HP Internet
- 15 Logitech iTouch
- 16 Logitech Cordless Desktop Pro
- 17 Logitech Internet Keyboard
- 18 Logitech Internet Navigator Keyboard
- 19 Compaq Internet
- 20 Microsoft Natural Pro
- 21 Genius Comfy KB-16M
- 22 IBM Rapid Access
- 23 IBM Rapid Access II
- 24 Chicony Internet Keyboard
- 25 Dell Internet Keyboard

Enter a number to choose the keyboard.

1

Please select the layout corresponding to your keyboard

- 1 U.S. English
- 2 U.S. English w/ ISO9995-3
- 3 U.S. English w/ deadkeys
- 4 Albanian
- 5 Arabic
- 6 Armenian
- 7 Azerbaidjani
- 8 Belarusian
- 9 Belgian
- 10 Bengali
- 11 Brazilian
- 12 Bulgarian
- 13 Burmese
- 14 Canadian
- 15 Croatian
- 16 Czech
- 17 Czech (qwerty)
- 18 Danish

Enter a number to choose the country.
Press enter for the next page

1

Please enter a variant name for 'us' layout. Or just press enter
for default variant

us

Please answer the following question with either 'y' or 'n'.
Do you want to select additional XKB options (group switcher,
group indicator, etc.)? n

接下来，我们要配置显示器。不要超过您显示器的刷新频率，这样可以会损坏您的显示器。如果您有疑问，请参考其它信息后再做配置。

Now we want to set the specifications of the monitor. The two critical
parameters are the vertical refresh rate, which is the rate at which the
whole screen is refreshed, and most importantly the horizontal sync rate,
which is the rate at which scanlines are displayed.

The valid range for horizontal sync and vertical sync should be documented
in the manual of your monitor. If in doubt, check the monitor database
/usr/X11R6/lib/X11/doc/Monitors to see if your monitor is there.

Press enter to continue, or ctrl-c to abort.

You must indicate the horizontal sync range of your monitor. You can either
select one of the predefined ranges below that correspond to industry-
standard monitor types, or give a specific range.

It is VERY IMPORTANT that you do not specify a monitor type with a horizontal
sync range that is beyond the capabilities of your monitor. If in doubt,
choose a conservative setting.

- hsync in kHz; monitor type with characteristic modes
- 1 31.5; Standard VGA, 640x480 @ 60 Hz
 - 2 31.5 - 35.1; Super VGA, 800x600 @ 56 Hz
 - 3 31.5, 35.5; 8514 Compatible, 1024x768 @ 87 Hz interlaced (no 800x600)
 - 4 31.5, 35.15, 35.5; Super VGA, 1024x768 @ 87 Hz interlaced, 800x600 @ 56 Hz
 - 5 31.5 - 37.9; Extended Super VGA, 800x600 @ 60 Hz, 640x480 @ 72 Hz
 - 6 31.5 - 48.5; Non-Interlaced SVGA, 1024x768 @ 60 Hz, 800x600 @ 72 Hz
 - 7 31.5 - 57.0; High Frequency SVGA, 1024x768 @ 70 Hz
 - 8 31.5 - 64.3; Monitor that can do 1280x1024 @ 60 Hz
 - 9 31.5 - 79.0; Monitor that can do 1280x1024 @ 74 Hz
 - 10 31.5 - 82.0; Monitor that can do 1280x1024 @ 76 Hz
 - 11 Enter your own horizontal sync range

Enter your choice (1-11): 6

You must indicate the vertical sync range of your monitor. You can either select one of the predefined ranges below that correspond to industry-standard monitor types, or give a specific range. For interlaced modes, the number that counts is the high one (e.g. 87 Hz rather than 43 Hz).

- 1 50-70
- 2 50-90
- 3 50-100
- 4 40-150
- 5 Enter your own vertical sync range

Enter your choice: 2

You must now enter a few identification/description strings, namely an identifier, a vendor name, and a model name. Just pressing enter will fill in default names.

The strings are free-form, spaces are allowed.

Enter an identifier for your monitor definition: Hitachi

下一个配置是从显卡的驱动列表里选择一个显卡驱动程序。如果忽略当前列表中的选项，请直接按**Enter**，下一屏将会出现在屏幕上，会显示下面的信息：

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 Ramdacs 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? y

288	Matrox Millennium G200 8MB	mgag200
289	Matrox Millennium G200 SD 16MB	mgag200
290	Matrox Millennium G200 SD 4MB	mgag200
291	Matrox Millennium G200 SD 8MB	mgag200
292	Matrox Millennium G400	mgag400

293	Matrox Millennium II 16MB	mga2164w
294	Matrox Millennium II 4MB	mga2164w
295	Matrox Millennium II 8MB	mga2164w
296	Matrox Mystique	mga1064sg
297	Matrox Mystique G200 16MB	mgag200
298	Matrox Mystique G200 4MB	mgag200
299	Matrox Mystique G200 8MB	mgag200
300	Matrox Productiva G100 4MB	mgag100
301	Matrox Productiva G100 8MB	mgag100
302	MediaGX	mediagx
303	MediaVision Proaxcel 128	ET6000
304	Mirage Z-128	ET6000
305	Miro CRYSTAL VRX	Verite 1000

Enter a number to choose the corresponding card definition.
Press enter for the next page, q to continue configuration.

288

Your selected card definition:

Identifier: Matrox Millennium G200 8MB
Chipset: mgag200
Driver: mga
Do NOT probe clocks or use any Clocks line.

Press enter to continue, or ctrl-c to abort.

Now you must give information about your video card. This will be used for the "Device" section of your video card in XF86Config.

You must indicate how much video memory you have. It is probably a good idea to use the same approximate amount as that detected by the server you intend to use. If you encounter problems that are due to the used server not supporting the amount memory you have (e.g. ATI Mach64 is limited to 1024K with the SVGA server), specify the maximum amount supported by the server.

How much video memory do you have on your video card:

- 1 256K
- 2 512K
- 3 1024K
- 4 2048K
- 5 4096K
- 6 Other

Enter your choice: 6

Amount of video memory in Kbytes: 8192

You must now enter a few identification/description strings, namely an identifier, a vendor name, and a model name. Just pressing enter will fill in default names (possibly from a card definition).

Your card definition is Matrox Millennium G200 8MB.

The strings are free-form, spaces are allowed.

Enter an identifier for your video card definition:

接下来，设置显卡的分辨率。典型的使用范围是640x480, 800x600, 和1024x768，这些显卡的功能特性、分辨率的大小以眼睛的舒适为准。当选择颜色深度时，可以选择您显卡支持最大模式。

For each depth, a list of modes (resolutions) is defined. The default resolution that the server will start-up with will be the first listed mode that can be supported by the monitor and card.

Currently it is set to:

```
"640x480" "800x600" "1024x768" "1280x1024" for 8-bit
"640x480" "800x600" "1024x768" "1280x1024" for 16-bit
"640x480" "800x600" "1024x768" "1280x1024" 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: 2

Select modes from the following list:

- 1 "640x400"
- 2 "640x480"
- 3 "800x600"
- 4 "1024x768"
- 5 "1280x1024"
- 6 "320x200"
- 7 "320x240"
- 8 "400x300"
- 9 "1152x864"
- a "1600x1200"
- b "1800x1400"
- c "512x384"

Please type the digits corresponding to the modes that you want to select. For example, 432 selects "1024x768" "800x600" "640x480", with a default mode of 1024x768.

Which modes? 432

You can have a virtual screen (desktop), which is screen area that is larger

than the physical screen and which is panned by moving the mouse to the edge of the screen. If you don't want virtual desktop at a certain resolution, you cannot have modes listed that are larger. Each color depth can have a differently-sized virtual screen

Please answer the following question with either 'y' or 'n'.
Do you want a virtual screen that is larger than the physical screen? n

For each depth, a list of modes (resolutions) is defined. The default resolution that the server will start-up with will be the first listed mode that can be supported by the monitor and card.
Currently it is set to:

"640x480" "800x600" "1024x768" "1280x1024" for 8-bit
"1024x768" "800x600" "640x480" for 16-bit
"640x480" "800x600" "1024x768" "1280x1024" 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: 4

Please specify which color depth you want to use by default:

- 1 1 bit (monochrome)
- 2 4 bits (16 colors)
- 3 8 bits (256 colors)
- 4 16 bits (65536 colors)
- 5 24 bits (16 million colors)

Enter a number to choose the default depth.

4

最后，要保存您的配置，确定输入/etc/X11/XF86Config 作为保存位置。

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? y

如果您配置失败，您也可以尝试着按[Yes] 来重新再试一次，会显示下面的信息：

User Confirmation Requested

The XFree86 configuration process seems to have failed. Would you like to try again?

[Yes] No

如果配置**XFree86**时遇上困难, 请选择[No] 并按**Enter**键继续进行安装。安装完成后可以使用**xf86cfg -textmode** 或**xf86config** 命令行配置程序来以root 用户的身份进行配置。配置**XFree86** 的另外一种方法描述在第5 章。如果您选择不配置**XFree86** 那么下一个菜单将让您选择要安装的软件包。

默认情况下可以使用组合键**Ctrl+Alt+Backspace**, 在发生错误或在硬件损坏前退出设置屏幕。

默认的显示模式可以使用X 系统下的**Ctrl+Alt++** 或**Ctrl+Alt+-**来改变。

一旦有了可以运行的**XFree86**, 就可以使用**xvidtune** 来调整显示的高度和宽度以及显示器的中心位置。

一些不适当的配置可能会损坏您的设备。如果在使用它们前存在疑虑, 请不要安装它们。可以使用监视器的控制工具来调整X 窗口的显示。与文本显示模式不同它更容易损坏设备。

在调整这些参数前, 请阅读**xvidtune(1)** 手册。

下面是一个配置**XFree86** 的成功例子, 它选择了使用默认的桌面。

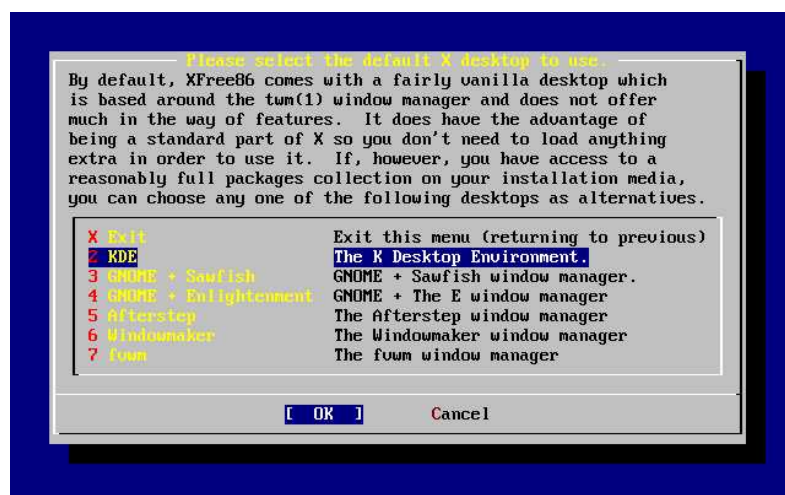
2.9.13 选择默认的桌面

注意: 从FreeBSD 5.3-RELEASE 开始, X 桌面的选择机制已经从**sysinstall** 中删掉了。您只能在安装好FreeBSD 之后再配置它。关于安装和配置X 桌面的更多细节可以在第5 章 找到。如果不是在安装FreeBSD 5.3-RELEASE 之前的版本, 则可以跳过这一节。

有许多窗口管理器可以使用。它们从基本的桌面环境到全部的桌面应用, 是一个大型的软件集。一些人可能只希望使用一些占用磁盘空间少, 内存低的窗口管理器; 而另外一些人则更倾向于使用有便多特性的桌面环境。选择使用那种桌面的最好的方法就是尝试着试用一些不同的桌面环境。这些桌面都可以在安装完成后通过ports收集或包管理器来进行安装。

您可以选择一个流行的桌面配置成为默认的桌面, 可以使您在安装完成后立刻启动它。

图2-56. 选择默认桌面



使用箭头选择一个桌面，然后键入**Enter**键。选择的桌面将被安装。

2.9.14 安装软件包

这些软件包已经被预编译成二进制程序了，安装软件有一个很简单的方法。

前面已经介绍了如何安装一个软件包的例子。如果需要的话，在安装结束之后，仍然可以使用sysinstall (对于FreeBSD 5.2 之前的版本是/stand/sysinstall) 来安装其他软件包。

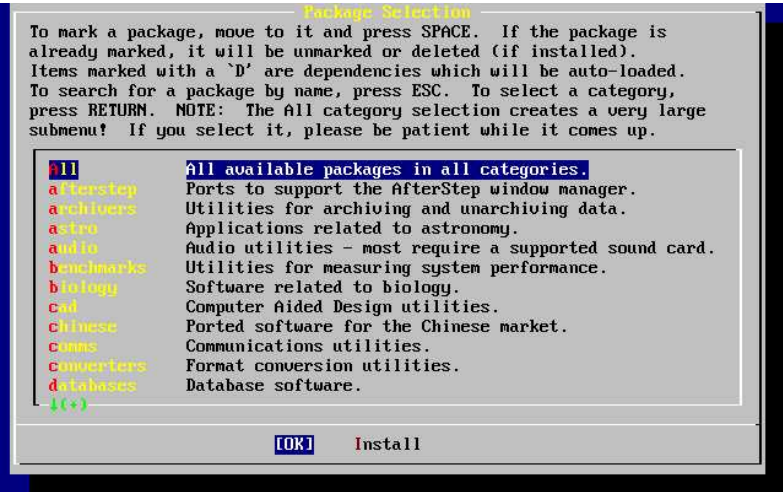
User Confirmation Requested

The FreeBSD package collection is a collection of hundreds of ready-to-run applications, from text editors to games to WEB servers and more. Would you like to browse the collection now?

[Yes] No

选择[Yes] 按**Enter** 将会显示软件包选择屏幕。

图2-57. 选择软件所的种类

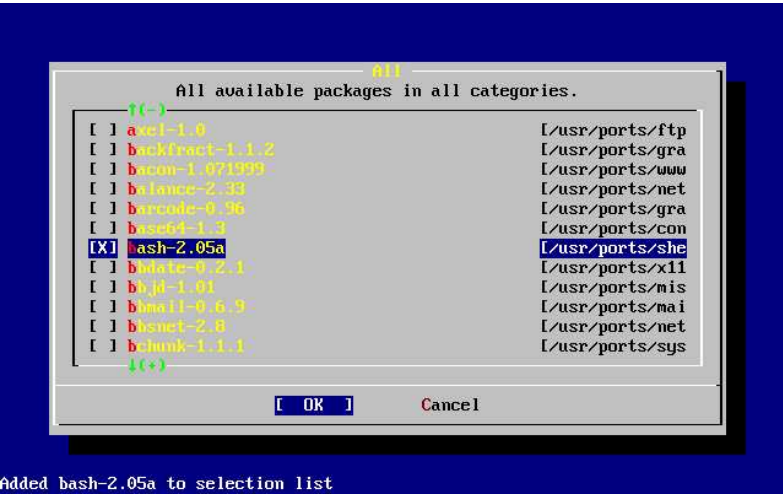


在任何时候只有安装介质上有的软件包才能被安装进系统。

如果选择**All** 那么所有的软件包将会被显示， 您也可以选择一个特殊的分类。使用箭头进行选择， 然后键入**Enter**。

一个菜单将会显示这个分类中可用的所有软件包。

图2-58. 选择软件包



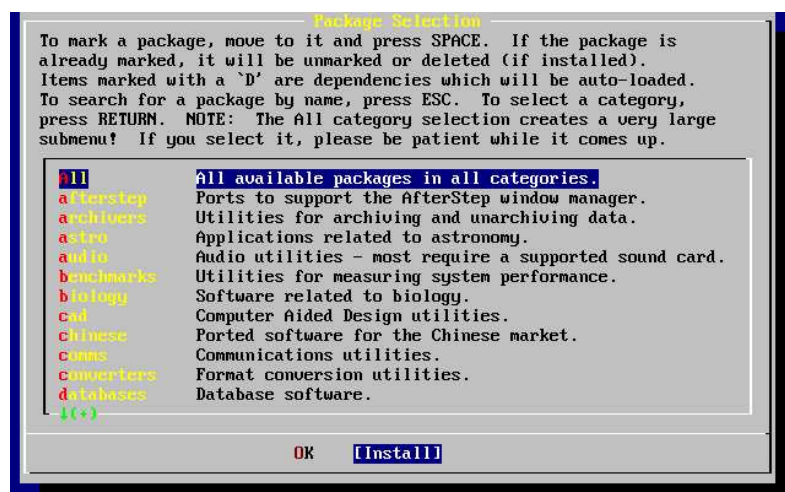
bash shell 被选中了。通过在加亮的软件上键入**Space** 键， 来选择您想要的软件所。每个选择的软件包的简短描述都会显示在屏幕左下角。

按**Tab** 键选择[OK]或[Cancel]。

当您完成了安装标记之后， 键入**Tab** 键选择[OK] 然后键入**Enter** 返回软件包选择菜单。

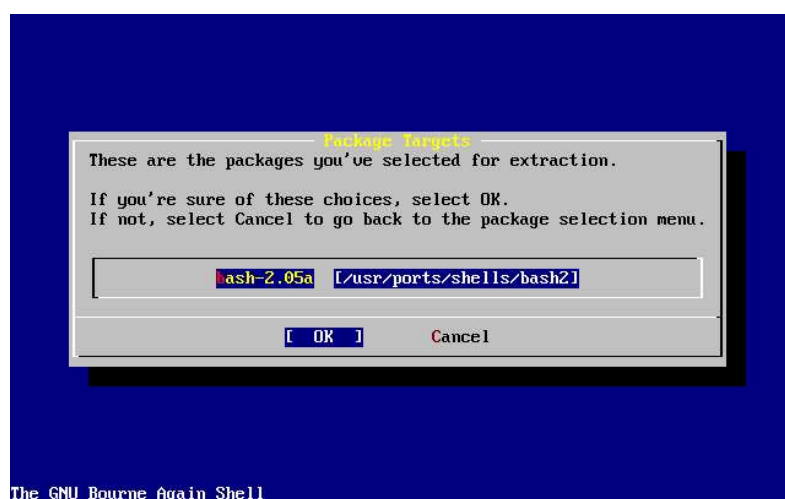
左右箭头键也可以用来选择[OK]和[Cancel]。用这种方法也可以用[OK] 然后按**Enter** 来返回软件包选择菜单。

图2-59. 安装软件包



使用**Tab** 和箭头键来选择[Install] 然后键入**Enter**。您接着需要确定您要安装的软件包。

图2-60. 确认安装的软件包



选择[OK] 然后键入**Enter** 键将开始软件的安装，安装信息将会不断地出现。如果有一些错误信息，请作好记录。

安装完成之后，继续最后的配置。如果您不想安装任何软件包并退回到最终配置屏幕，请选择Install。

2.9.15 添加用户/组

您至少要在安装过程中添加一个用户，以便于您能不用root 来登录使用系统。根分区通常比较小，用root 来运行应用程序可能会快一点。但这样会有一些危险：

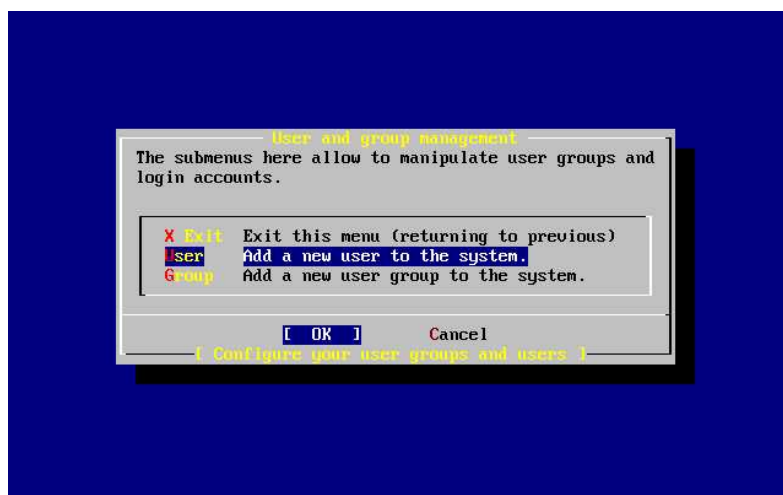
User Confirmation Requested

Would you like to add any initial user accounts to the system? Adding at least one account for yourself at this stage is suggested since working as the "root" user is dangerous (it is easy to do things which adversely affect the entire system).

[Yes] No

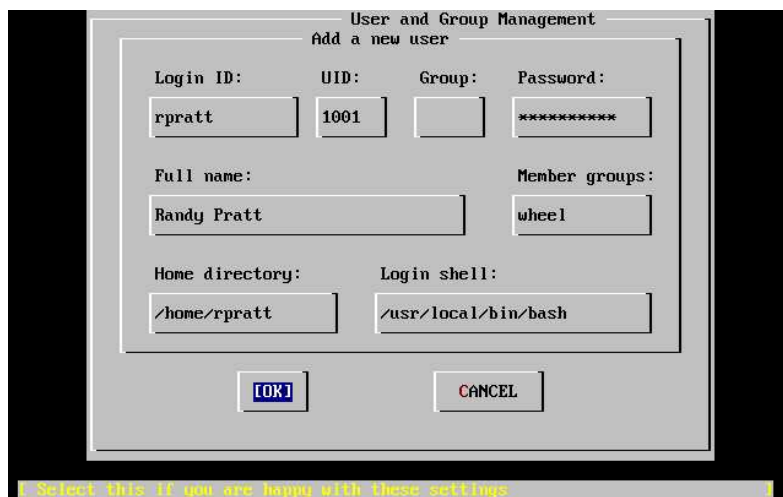
选择[Yes] 然后键入**Enter** 继续添加用户。

图2-61. 选择用户



用箭头键来选择User 然后按**Enter**。

图2-62. 添加用户信息



下面的描述信息会出现在屏幕的下方，可以使用**Tab** 键来切换不同的项目，以便输入相关信息：

Login ID

新用户的登录名（强制性必须写）

UID

这个用户的ID编号（如果不写，系统自动添加）

Group

这个用户的登录组名（如果不写，系统自动添加）

Password

这个用户的密码（键入这个需要很仔细！）

Full name

用户的全名（解释、备注）

Member groups

这个用户所在的组

Home directory

用户的主目录（如果不写，系统自动添加）

Login shell

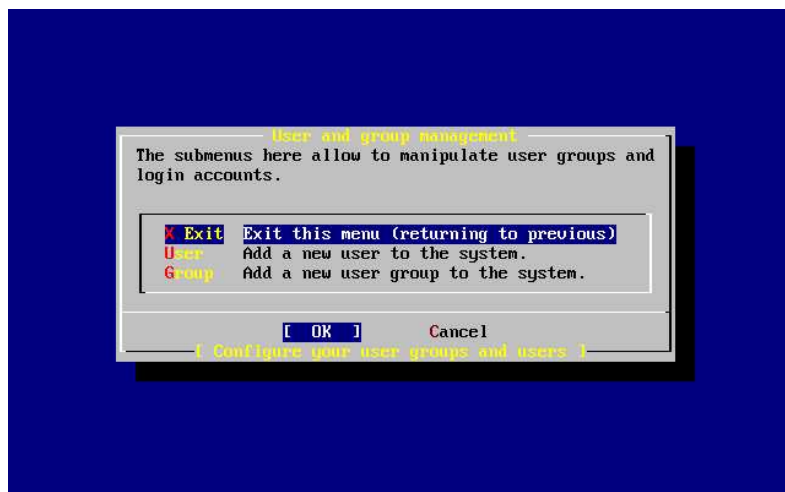
用户登录的shell（默认是/bin/sh）。

登录的shell可以在/bin/sh到/usr/local/bin/bash中修改。**bash shell**是先前默认安装的shell。不要使用一个不存在的或您不能登录的shell。最通用的shell是使用BSD-world的C shell，可以通过指定/bin/tcsh来修改。

用户也可以被添加到wheel组中成了一个超级用户，从而拥有root权限。

当您感觉满意时，键入[OK]键，用户和组管理菜单将会重新出现。

图2-63. 退出用户和组管理



如果有其他的需要，此时还可以添加其他的组。此外，还可以通过`sysinstall` (在FreeBSD 5.2 以前的版本中是`/stand/sysinstall`) 在安装完成之后添加它们。

当您完成添加用户的时候，选择**Exit** 然后键入**Enter** 继续下面的安装。

2.9.16 设置root 密码

```

      Message
Now you must set the system manager's password.
This is the password you'll use to log in as "root".

```

```
[ OK ]
```

```
[ Press enter to continue ]
```

键入**Enter** 来设置root 密码。

密码必须正确地输入两次。毋庸讳言，您需要选择一个不容易忘记的口令。请注意您输入的口令不会回显，也不会显示星号。

```

Changing local password for root.
New password :
Retype new password :

```

密码成功键入后，安装将继续。

2.9.17 退出安装

如果您需要设置其他的网络设备，或者需要完成其他的配置，可以在此时或者事后通过`sysinstall` (对于FreeBSD 5.2 之前的版本是`/stand/sysinstall`) 来进行配置。

```

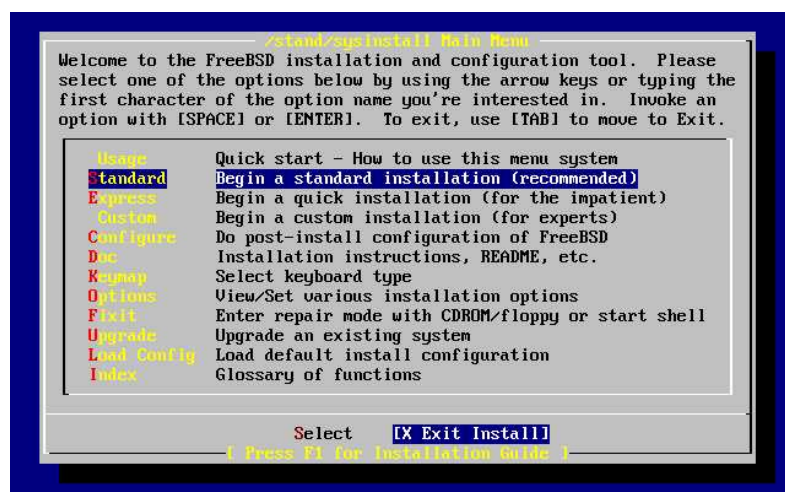
      User Confirmation Requested
Visit the general configuration menu for a chance to set any last
options?

```

```
Yes    [ No ]
```

选择**[No]** 然后键入**Enter** 返回到主安装菜单。

图2-64. 退出安装



选择[X Exit Install] 然后键入**Enter**。您可能需要确认是否真的退出安装:

```

User Confirmation Requested
Are you sure you wish to exit? The system will reboot (be sure to
remove any floppies from the drives).

```

```
[ Yes ] No
```

选择[Yes] 取出软盘。CDROM驱动器将被锁定，直到机器重新启动。CDROM然后就可以从驱动器中取出来了。

在系统重新启动的时候可能会见到出错信息。

2.9.18 FreeBSD的启动

2.9.18.1 FreeBSD 在i386上启动

如果启动正常，您将看到在屏幕上有很多信息滚动，最后您会看到登录命令行。您可以通过键入**Scroll-Lock**和使用**PgUp**与**PgDn**来查看信息，再键入**Scroll-Lock**回到命令行。

记录信息可能不会显示（缓冲区的限制）。您可以通过键入**dmesg**来查看。

使用您在安装过程中设置的用户名/密码来登录。（例子中使用**rpratt**）。除非必须的时候请不要用**root**用户登录。

典型的启动信息：（忽略版本信息）

```

Copyright (c) 1992-2002 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

```

```

Timecounter "i8254" frequency 1193182 Hz
CPU: AMD-K6(tm) 3D processor (300.68-MHz 586-class CPU)
Origin = "AuthenticAMD" Id = 0x580 Stepping = 0

```

```

Features=0x8001bf<FPU,VME,DE,PSE,TSC,MSR,MCE,CX8,MMX>
AMD Features=0x80000800<SYSCALL,3DNow!>
real memory = 268435456 (262144K bytes)
config> di sn0
config> di lnc0
config> di le0
config> di ie0
config> di fe0
config> di cs0
config> di bt0
config> di aic0
config> di aha0
config> di adv0
config> q
avail memory = 256311296 (250304K bytes)
Preloaded elf kernel "kernel" at 0xc0491000.
Preloaded userconfig_script "/boot/kernel.conf" at 0xc049109c.
md0: Malloc disk
Using $PIR table, 4 entries at 0xc00fde60
npx0: <math processor> on motherboard
npx0: INT 16 interface
pcib0: <Host to PCI bridge> on motherboard
pci0: <PCI bus> on pcib0
pcib1: <VIA 82C598MVP (Apollo MVP3) PCI-PCI (AGP) bridge> at device 1.0 on pci0
pci1: <PCI bus> on pcib1
pci1: <Matrox MGA G200 AGP graphics accelerator> at 0.0 irq 11
isab0: <VIA 82C586 PCI-ISA bridge> at device 7.0 on pci0
isa0: <ISA bus> on isab0
atapci0: <VIA 82C586 ATA33 controller> port 0xe000-0xe00f at device 7.1 on pci0
ata0: at 0x1f0 irq 14 on atapci0
ata1: at 0x170 irq 15 on atapci0
uhci0: <VIA 83C572 USB controller> port 0xe400-0xe41f irq 10 at device 7.2 on pci0
usb0: <VIA 83C572 USB controller> on uhci0
usb0: USB revision 1.0
uhub0: VIA UHCI root hub, class 9/0, rev 1.00/1.00, addr 1
uhub0: 2 ports with 2 removable, self powered
chip1: <VIA 82C586B ACPI interface> at device 7.3 on pci0
ed0: <NE2000 PCI Ethernet (RealTek 8029)> port 0xe800-0xe81f irq 9 at
device 10.0 on pci0
ed0: address 52:54:05:de:73:1b, type NE2000 (16 bit)
isa0: too many dependant configs (8)
isa0: unexpected small tag 14
fdc0: <NEC 72065B or clone> at port 0x3f0-0x3f5,0x3f7 irq 6 drq 2 on isa0
fdc0: FIFO enabled, 8 bytes threshold
fd0: <1440-KB 3.5" drive> on fdc0 drive 0
atkbd0: <keyboard controller (i8042)> at port 0x60-0x64 on isa0
atkbd0: <AT Keyboard> flags 0x1 irq 1 on atkbd0
kbd0 at atkbd0
psm0: <PS/2 Mouse> irq 12 on atkbd0
psm0: model Generic PS/2 mouse, device ID 0
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff on isa0
sc0: <System console> at flags 0x1 on isa0
sc0: VGA <16 virtual consoles, flags=0x300>

```

```

sio0 at port 0x3f8-0x3ff irq 4 flags 0x10 on isa0
sio0: type 16550A
sio1 at port 0x2f8-0x2ff irq 3 on isa0
sio1: type 16550A
ppc0: <Parallel port> at port 0x378-0x37f irq 7 on isa0
ppc0: SMC-like chipset (ECP/EPP/PS2/NIBBLE) in COMPATIBLE mode
ppc0: FIFO with 16/16/15 bytes threshold
ppbus0: IEEE1284 device found /NIBBLE
Probing for PnP devices on ppbus0:
plip0: <PLIP network interface> on ppbus0
lpt0: <Printer> on ppbus0
lpt0: Interrupt-driven port
ppi0: <Parallel I/O> on ppbus0
ad0: 8063MB <IBM-DHEA-38451> [16383/16/63] at ata0-master using UDMA33
ad2: 8063MB <IBM-DHEA-38451> [16383/16/63] at ata1-master using UDMA33
acd0: CDR0M <DELTA OTC-H101/ST3 F/W by OIPD> at ata0-slave using PIO4
Mounting root from ufs:/dev/ad0s1a
swapon: adding /dev/ad0s1b as swap device
Automatic boot in progress...
/dev/ad0s1a: FILESYSTEM CLEAN; SKIPPING CHECKS
/dev/ad0s1a: clean, 48752 free (552 frags, 6025 blocks, 0.9% fragmentation)
/dev/ad0s1f: FILESYSTEM CLEAN; SKIPPING CHECKS
/dev/ad0s1f: clean, 128997 free (21 frags, 16122 blocks, 0.0% fragmentation)
/dev/ad0s1g: FILESYSTEM CLEAN; SKIPPING CHECKS
/dev/ad0s1g: clean, 3036299 free (43175 frags, 374073 blocks, 1.3% fragmentation)
/dev/ad0s1e: filesystem CLEAN; SKIPPING CHECKS
/dev/ad0s1e: clean, 128193 free (17 frags, 16022 blocks, 0.0% fragmentation)
Doing initial network setup: hostname.
ed0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 192.168.0.1 netmask 0xfffff00 broadcast 192.168.0.255
    inet6 fe80::5054::5ff::fede:731b%ed0 prefixlen 64 tentative scopeid 0x1
    ether 52:54:05:de:73:1b
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x8
    inet6 ::1 prefixlen 128
    inet 127.0.0.1 netmask 0xff000000
Additional routing options: IP gateway=YES TCP keepalive=YES
routing daemons:.
additional daemons: syslogd.
Doing additional network setup:.
Starting final network daemons: creating ssh RSA host key
Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
cd:76:89:16:69:0e:d0:6e:f8:66:d0:07:26:3c:7e:2d root@k6-2.example.com
creating ssh DSA host key
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
f9:a1:a9:47:c4:ad:f9:8d:52:b8:b8:ff:8c:ad:2d:e6 root@k6-2.example.com.
setting ELF ldconfig path: /usr/lib /usr/lib/compat /usr/X11R6/lib

```

```

/usr/local/lib
a.out ldconfig path: /usr/lib/aout /usr/lib/compat/aout /usr/X11R6/lib/aout
starting standard daemons: inetd cron sshd usbd sendmail.
Initial rc.i386 initialization:.
rc.i386 configuring syscons: blank_time screensaver moused.
Additional ABI support: linux.
Local package initialization:.
Additional TCP options:.

```

```
FreeBSD/i386 (k6-2.example.com) (ttyv0)
```

```
login: rpratt
Password:
```

生成RSA 和DSA密钥在比较慢的机器上可能要花很长时间。这只是一个新安装后的首次启动，以后的启动会变得更快一点。

如果已经完成X 服务器的配置，且指定了默认的桌面窗口管理器，就可以在命令行键入**startx** 来启动它了。

2.9.18.2 FreeBSD 在Alpha机器上启动

一旦安装完成，您就可以键入下面的命令来启动FreeBSD:

```
>>>BOOT DKC0
```

这是从指定的固定硬件进行引导。如果要使FreeBSD 下次能够自动启动，使用下面的命令:

```

>>> SET BOOT_OSFLAGS A
>>> SET BOOT_FILE "
>>> SET BOOTDEF_DEV DKC0
>>> SET AUTO_ACTION BOOT

```

启动信息跟启动i386机器时差不多。(但不完全一样)

2.9.19 FreeBSD 关机

正确的关闭操作系统是很重要的。不要仅仅关闭电源。首先，您需要成为一个超级用户，通过键入**su** 命令来实现。然后输入**root** 密码。这需要用户是**wheel** 组的一名成员。然后，以**root**键入**shutdown -h now**命令。

```

The operating system has halted.
Please press any key to reboot.

```

当**shutdown**命令发出后，屏幕上出现“Please press any key to reboot” 信息时，您就可以安全的关闭计算机了。如果按下任意一个键，计算机将重新启动。

您也能够使用**Ctrl+Alt+Del** 组合键来重新启动计算机，但是不推荐使用这个操作。

2.10 支持的硬件

FreeBSD当前可以广泛运行在ISA、VLB、EISA、PCI总线的PC上，包括Inter,AMD,Cyrix或NexGen“x86”系列的机器，还有一些Compaq Alpha的机器。支持普通的IDE或ESDI驱动配置，各种SCSI控制器，PCMCIA卡，USB设备，网卡和其它网络串口设备。FreeBSD也支持IBM微通道（MCA）的总线结构。

每个发行版都会提供一个FreeBSD支持的硬件列表。您可以在名字叫做HARDWARE.TXT的文件中找到。它可以在CDROM或FTP发行组件或sysinstall的文档菜单中找到。对于特定的架构，都有相应的硬件支持列表。也可以在FreeBSD的网站Release Information (<http://www.FreeBSD.org/releases/index.html>) 找到更多的信息。

2.11 常见问题

下面将介绍一些在安装过程中常见的问题，像如何报告发生的问题，如何双重启动FreeBSD和MS-DOS。

2.11.1 当您遇到错误时，应该怎么做？

由于pc结构的限制，不可能100%的不出现问题，但是有些问题是您可以自己解决的。

先检查您的硬件，确保您的硬件被支持。

如果您的硬件能够被扶持，但还是会出问题，那就重新启动计算机。当出现内核配置信息的时候，重新配置一下硬件信息。因为绝大多数硬件的IRQ，IO地址，DMA通道都有它们的生产商预先进行默认配置。如果您的硬件已经重新装配了，就需要使用配置编辑器告诉FreeBSD到哪里去找相关信息。

如果某个设备配置好后，发现又有个设备出现错误。碰到这种情况，就当卸掉这个设备的驱动程序。

注意：有些安装问题可以借助更新硬件的程序来解决，特别是主板的BIOS。大部分的主板制造商都会提供网站给用户下载新的BIOS以及提供如何更新的说明。

也有许多制造商强烈建议，除非必要否则不要轻易更新BIOS。因为更新的过程可能会发生问题，进而损害BIOS芯片。

警告：不要禁用安装过程中您会用到的驱动程序，例如显示sc0。如果安装程序在修改了某些配置之后安装程序行为吊诡或失败，您可能修改或删除了某些不应删除的组件。如果遇到这种情况，应重新启动以便尝试其他设置。

在配置模式下，您可以：

- 列出在内核中安装的设备驱动程序。
- 禁用不适合您机器的设备驱动程序。
- 通过驱动程序改变IRQ，DRQ和IO端口地址。

调整内核与您的硬件设置一致之后，键入Q，以新的设置重新启动计算机。当FreeBSD安装完成之后，在配置模式下做的更改会一直存在，不需要在每次启动计算机时再重新设置。即使如此，有可能您会想建立一个定制内核使您的系统效率达到最好，可以看看以下的链接custom kernel。

2.11.2 处理MS-DOS® 分区存在的问题

许多FreeBSD的用户会在运行了Microsoft的PC上安装FreeBSD。以下是一些关于在这种系统中安装FreeBSD常会出现的问题。FreeBSD中有一个叫**FIPS**的应用程序。此工具程序可以在安装光盘的tools目录下找到，或者，也可以从FreeBSD的镜像站点下载。

FIPS允许您将现有的MS-DOS分区一分为二，保留原原有的分区，而将新系统安装到空出来的分区上。首先要整理MS-DOS分区的碎片，您可以用Windows的**Disk Defragmenter** (进入资源管理器，右键单击硬盘，并选择整理碎片) 或**Norton Disk Tools**来完成这项工作。接下来就可以运行**FIPS**，它会提示您接下来所需要进行的操作。接下来就可以重新启动并将FreeBSD安装到新空出来的分区中了。安装所需的磁盘空间，可以从Distributions菜单给出的值来进行估计。

有一个由PowerQuest公司生产的非常有用的工具。从<http://www.powerquest.com> (<http://www.powerquest.com/>)网站上可以得到**PartitionMagic**。这个工具的功能比**FIPS**要强大。如果您经常要添加或删除操作系统，强烈建议您使用它。当然，它很贵。如果您只是想安装FreeBSD的话，**FIPS**就足够了。

2.11.3 使用MS-DOS 和Windows® 文件系统

现在FreeBSD还不支持经过**Double Space™**应用程序压缩过的文件系统。因此其它的文件系统在被FreeBSD访问其数据之前必须先解压缩。它可以通过运行位于Start> Programs > System Tools menu中的**Compression Agent**程序来实现。

FreeBSD可以支持基于MS-DOS的文件系统。这要求您使用带参数的mount_msdos(8)命令(在FreeBSD 5.X版本，相应的命令为mount_msdosfs(8)) 最常使用的是：

```
# mount_msdos /dev/ad0s1 /mnt
```

在此例子中，MS-DOS文件系统位于主硬盘的第一个分区。您的情况可能与引不同，查看命令dmesg和mount的输出。它们应该可以让您得到足够的分区信息。

注意：MS-DOS的扩展分区会被映射在FreeBSD分区的末尾。换句话说，分区号要大于FreeBSD正在使用的分区号。例如，第一个MS-DOS分区可能位于/dev/ad0s1，FreeBSD分区可能位于/dev/ad0s2，跟着是MS-DOS的扩展分区位于/dev/ad0s3。这可能会使您感觉迷茫。

NTFS分区也可以通过类似mount_ntfs(8)命令挂接在FreeBSD上。

2.11.4 Alpha 用户的问题与解答

这节主要回答一些在Alpha系统上安装FreeBSD时经常问到的问题。

1. 我可以从ARC 或Alpha BIOS 控制台启动吗？

不行。FreeBSD，像Compaq Tru64 和VMS，只能从SRM控制台启动。

2. 求救，我没有空间了！我需要删除每一样东西吗？

不，这个时候不行。

3. 我可以挂上Compaq Tru64 或VMS 的文件系统吗？

不，这个时候不行。

2.12 高级安装指南

Contributed by Valentino Vaschetto.

这节主要描述在一些特殊情况下如何安装FreeBSD。

2.12.1 在一个没有显示器或键盘的系统上安装FreeBSD

这种类型的安装叫做“headless install（无关安装）”，因您正要安装FreeBSD的机器不是没带显示器，就是没有显卡。您可能会问那怎么安装？可以使用一个串行控制台。串行控制台基本上是使用另外一台机器来充当主显示设备和键盘。要这样做，只要执行下面的步骤：创建安装软件，请看第2.2.7 节一节说明。

按下面的步骤，修改这些软盘用来引导进入一个串行控制台：

1. 通过启动软盘来引导进入一个串行控制台

如果您想用软盘，FreeBSD将进入它通常的安装模式。我们要把FreeBSD 引导进入串行控制台，需要这样做，您必须使用mount(8)命令在FreeBSD系统上挂一kern.flp的那个软盘。

```
# mount /dev/fd0 /mnt
```

现在您已经挂上了软盘，需要进入/mnt 目录：

```
# cd /mnt
```

这儿是您必须设置软盘引导进入串行控制台的地方。您必须制作一个包含/boot/loader -h这行的叫做boot.config 的文件。所有这些是为了给引导程序一个标记以引导进入串行控制台。

```
# echo "/boot/loader -h" > boot.config
```

现在您已经正确配置好了软盘，您必须使用umount(8) 命令卸下软盘。

```
# cd /
```

```
# umount /mnt
```

现在您可以从软盘驱动器中取出软盘了。

2. 连接您的Null-modem 线

您现在需要一根null modem线来连接两台机器。只要连接两台机器的串口。普通的串行线是不行的，您需要使用一根null modem的线，因为它在一些十字交叉口有金属线。

3. 开始启动安装

现在开始启动安装。把kern.flp 的那张软盘插入软盘驱动器，然后开启电源。

4. 连接您的无头机器

现在您已经通过cu(1)连接到了那台机器。

```
# cu -l /dev/cuaa0
```

就这样！您已经能够通过您的cu session对话来控制那台“无头”机器了。它将要求您把mfsroot.flp的那张软盘插入驱动器，然后它将提示选择使用哪种终端。只要选择FreeBSD的彩色控制台，然后继续您的安装。

2.13 准备您自己的安装介质

注意: 为了避免重复 “FreeBSD disc” 在这里指FreeBSD CDROM or DVD 那即意味着您要购买或自己制做。

有好几个原因需要您创建自己的FreeBSD安装介质。这可能是物理介质，如磁带，使用sysinstall程序找到的安装文件，FTP站点或MS-DOS分区。

例如:

- 您有许多机器连接到本地网络，使用一个FreeBSD光盘。您要使用FreeBSD来创建一个本地FTP站点，然后使用这个FTP站点来代替连接到Internet。
- 您有一张FreeBSD 光盘，FreeBSD 不支持您的CD/DVD 驱动器，但MS-DOS/Windows 支持。您要复制安装文件到一个DOS分区，然后使用这些文件进行安装。
- 您要安装的计算机没有CD/DVD驱动器和网卡，但您可以连接一个 “Laplink-style” 串口或并口线缆到那台计算机。
- 您要通过一个磁带机来安装FreeBSD.

2.13.1 创建一张安装光盘

FreeBSD的每个发行版本都提供两张CDROM映像(“ISO images”)。如果您有刻录机，这些映像文件可以被(“burned”)成FreeBSD的安装光盘。如果没有刻录机，而上网带宽却很便宜，它也是一种很好的安装方式。

1. 下载正确的ISO 映像文件

每个版本的ISO映像文件都可以从ftp://ftp.FreeBSD.org/pub/FreeBSD/ISO-IMAGES-架构名/版本或最近的镜像站点下载。选择合适的架构和版本。

目录中包含下面一些映像文件:

表2-5. FreeBSD 4.x ISO 映像文件名和含意

文件名	包含内容
版本-RELEASE-架构名-miniinst.iso	安装FreeBSD 所需的全部文件。
版本-RELEASE-架构名-disc1.iso	安装FreeBSD 所需的全部文件，以及这张光盘能装下的、尽可能多的第三方软件包。
版本-RELEASE-架构名-disc2.iso	一份用于与sysinstall 中的 “Repair” (修复) 机制联用的 “现场文件系统”。一份FreeBSD CVS 目录的副本，以及这张光盘能装下的、尽可能多的第三方软件包。

表2-6. FreeBSD 5.x ISO 映像文件名和含意

文件名	包含内容
版本-RELEASE-架构-bootonly.iso	引导FreeBSD 内核并启动安装界面所需的全部数据。安装文件可以从FTP 或其他安装源获得。
版本-RELEASE-架构名-miniinst.iso	安装FreeBSD 所需的全部文件。
版本-RELEASE-架构名-disc1.iso	安装FreeBSD 所需的全部文件，以及一份用于与sysinstall 中的“Repair” (修复) 机制联用的“现场文件系统”。
版本-RELEASE-架构名-disc2.iso	FreeBSD 文档以及这张光盘能装下的、尽可能多的第三方软件包。

您必须 下载miniinst ISO 镜像或第一张光盘的镜像之一。不需要两个都下载，因为第一张光盘包括了miniinst ISO 的全部内容。

注意: miniinst ISO 镜像只有在5.4-RELEASE 之前的版本才提供。

如果访问Internet 的价格便宜，建议使用miniinst ISO。这样您可以安装FreeBSD，并从网上通过ports/packages 系统(参见第4 章) 根据需要下载和安装第三方软件包。

如果您正打算安装FreeBSD 4.x 版本，并同时选择一些第三方软件包，则可以下载第一张光盘的镜像文件。

其它的映像盘也是很有用的，但不是必须的，尤其是在您有高速的网络连接时。

2. 刻录CDs

您必须把这些映像文件刻录成光盘。如果您在其它的FreeBSD系统上完成此项工作，请看第17.6 节 得到更多的信息，（特别是第17.6.3 节 和第17.6.4 节）

如果您在其它的系统平台上执行，您需要相应的刻录软件。映像文件使用的是标准的ISO格式，必须被您的刻录软件所支持。

注意: 如果有兴趣制作一张定制的FreeBSD 版本，请参考Release Engineering Article (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/releeng)。

2.13.2 为FreeBSD 安装盘建立局域网FTP 站点

FreeBSD 光盘的布局和FTP 站点相同。这样，建立局域网FTP 站点来用于网络上的其它计算机安装FreeBSD，就十分的容易。

1. 在要作为FTP站点的那台FreeBSD机器上，确定FreeBSD磁盘放入光驱中并将它挂在/cdrom目录中。

```
# mount /cdrom
```

2. 在/etc/passwd文件中建立一个可匿名访问FTP 服务器的账号。您可以利用vipw(8) 命令编辑/etc/passwd 文件，加入下面这一行叙述：

```
ftp:*:99:99::0:0:FTP:/cdrom:/nonexistent
```

3. 确定在/etc/inetd.conf配置文件中开启了FTP服务。

任何本地网络中的机器在安装FreeBSD选择安装介质时就可以选择透过FTP站点，然后选取“Other”后输入 **ftp://本地FTP服务器** 即可以透过本地的FTP站点来安装FreeBSD。

注意: 如果用作FTP客户端的引导介质(通常是软盘)与本地局域网的FTP站点上的版本不一致，**sysinstall** 会不允许您完成安装。如果您使用的版本差距不很大，并且希望绕过这一判断，则应进入**Options** 菜单，并将安装包的名字改为**any**。

警告: 此方式最好使用在有防火墙保护的内部网络。如果要将此FTP服务公开给外面的网际网络（非本地用户），您的电脑必须承担被侵入或其它的风险。我们强烈建议您要有完善的安全机制才这样做。

2.13.3 创建安装软盘

如果您从软盘安装（我们不推荐那样做），或者是由于不支持硬件或者更简单的理由是因为您坚持要使用软盘安装。您必须准备几张软盘。

至少这些软盘必须是1.44 MB 或1.2 MB 的，用来容纳所有在**bin** (命令) 目录下的文件。如果您在DOS操作系统下准备就**MUST**使用MS-DOS下的**FORMAT** 命令来格式化软盘。如果您使用的是Windows 操作系统，在资源管理器中就可以完成这个工作(用右键单击**A:** 驱动器，并选择“**Format**”)。

不要 指望厂家的预先格式化！最好还是亲自进行格式化。过去用户报告的很多问题都是由于不正确地使用格式化设备所造成的，所以我们需要在这里着重提一下。

如果您在另外一台FreeBSD的机器上做了启动盘的话，进行格式化是一个不错的主意。虽然您不需要把每张盘都做成DOS文件系统。您也可以使用**disklabel** 和**newfs** 命令来创建一个UFS文件系统，具体操作按下面的顺序进行：

```
# fdformat -f 1440 fd0.1440
# disklabel -w -r fd0.1440 floppy3
# newfs -t 2 -u 18 -l 1 -i 65536 /dev/fd0
```

注意: 如果使用5.25"软盘的话，需要使用**fd0.1200** 和**floppy5** 来格式化1.2 MB 的磁盘空间。

然后您就可以像其它的文件系统一样挂上和写入这些磁盘。

格式化这些磁盘后，您必须拷贝文件到磁盘中。这些发行文件被分割成刚好可存进五张1.44 MB 软盘。检查您所有的磁盘，找出所有可能适合的文件。直到您找到所有需要的配置并且将它们以这种方式安置。第一个配置都应该有一个子目录在磁盘上，例如：**a:\bin\bin.aa**, **a:\bin\bin.ab**, 等等。

一旦您进入选择安装介质的屏幕，选择**Floppy** 将会看到后面的提示符。

2.13.4 从MS-DOS 分区安装

如果从MS-DOS 分区安装，您需要将发布文件复制到该分区根目录下的**freebsd** 目录中。例如：**c:\freebsd**。您必须复制一部分CDROM 或FTP 上的目录结构，因此，如果您从光盘进行复制，建议使用DOS 的xcopy 命令。下面是准备进行FreeBSD 最小系统安装的例子：

```
C:\> md c:\freebsd
C:\> xcopy e:\bin c:\freebsd\bin\ /s
C:\> xcopy e:\manpages c:\freebsd\manpages\ /s
```

假设**C:** 盘是您的空闲空间，**E:** 盘是您挂接的CDROM。

如果您没有光盘驱动器，您可以从以下网站下载发行包。ftp.FreeBSD.org ([ftp://ftp.FreeBSD.org/pub/FreeBSD/releases/i386/6.0-RELEASE/](http://ftp.FreeBSD.org/pub/FreeBSD/releases/i386/6.0-RELEASE/))。每一个发行包都在一个目录中，例如**base** 发行包可以在6.0/base/ ([ftp://ftp.FreeBSD.org/pub/FreeBSD/releases/i386/6.0-RELEASE/base/](http://ftp.FreeBSD.org/pub/FreeBSD/releases/i386/6.0-RELEASE/base/)) 目录中找到。

注意：在4.X 和其它老版本的FreeBSD the “base” 发行包被叫做 “bin” 。如果您使用这些版本的话，请调整上例中的命令和URLS。

对很多发行包来说，如果您希望从MS-DOS分区安装的话（您有足够的空间），安装**c:\freebsd** —— 下的每个文件——这个**BIN** 发行包只是最低限度的要求。

2.13.5 创建一个安装磁带

从磁带安装也许是最简单的方式，比在线使用FTP 安装或使用CDROM 还快。安装的程序假设是简单地被压缩在磁带上。在您到所有配置文件后，简单的解开它们，用下面的命令：

```
# cd /freebsd/distdir
# tar cvf /dev/rwt0 dist1 ... dist2
```

在您安装的时候，您要确定留有足够的空间给临时目录（允许您选择）来容纳磁带安装时**全部** 的内容。由于不是随机访问磁带的，所以这种安装方法需要很多临时空间。

注意：开始安装时，在从软盘启动之前，磁带机必须已经放在驱动设备中。否则，安装过程中可能会找不到它。

2.13.6 通过网络安装

有三种类型的网络安装方法。串口（SLIP或PPP），并口（PLIP），以太网（标准的以太网控制器，包括PCMCIA）。

SLIP 支持是相当原始的，并且被限制在主要对hard-wired 的连接，就像一台膝上型计算机与另一台计算机间的串行线。现在的SLIP的安装还没有提供拨号功能，这个连接应该是hard-wired；用PPP工具提供的这种便利性应该首先尽可能被用于SLIP 设备。

如果您使用一个MODEM，那您就只有PPP这一种选择了。在您安装的过程中，要确定您能很容易地获得完整且快速的关于您服务提供商的信息。

如果您使用PAP或CHAP方式连接到您的ISP，（换句话说，如果您不使用脚本在Windows中连接到您的ISP），那么您需要在`ppp`提示符下输入`dial`命令。否则，当PPP连接者只提供一种最简单的终端模拟器，您必须知道如何使用针对MODEM的“AT commands”拨号到您的ISP。想知道更深入的信息可以参考用户级PPP那节handbook and FAQ (http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/faq/ppp.html)。如果您有一些问题，可以使用`set log local ...`命令将日志显示在屏幕上。

您也可以通过并口电缆连接到另外一台FreeBSD（2.0或以后的版本）机器上进行安装，您可以考虑使用“laplink”并口电缆进行安装。通过并口安装要比通过串口（最高50 kbytes/sec）安装快得多。

最后，通过网络安装最快的方法是利用以太网技术！FreeBSD支持绝大多数普通的以太网卡。每个FreeBSD发行版都在硬件注释中提供支持的网卡的列表和需要的设置。如果您要使用PCMCIA接口的以太网，在启动计算机之前，确信已经把它插好了。目前，FreeBSD还不支持PCMCIA的热插拔。

通过网络安装，您可能需要知道IP地址，地址掩码，还有机器的名字。如果您通过PPP进行安装，就不需要静态的IP地址，IP地址会由ISP给您自动指派。您的系统管理员会告诉您通过网络安装的细节。如果您通过主机名而不是IP地址来访问其它主机，需要有一个域名服务器或一个网关地址（如果您使用PPP进行安装，那它就您的ISP的IP地址）。如果您要通过一个HTTP的代理服务器进行FTP安装，需要一个代理服务地址。如果您不知道这些，在安装之前可以询问您的系统管理员或您的ISP服务商。

2.13.6.1 通过NFS安装之前

NFS安装方式是非常方便的。只需要简单地将FreeBSD文件拷贝到一台服务器上，然后在安装时选择NFS介质。

如果这个服务器要“特权端口”才能支持（如SUN的工作站），您需要在安装前在Options菜单中设置NFS Secure。

如果您的一台网卡比较糟糕，速度很慢，则应考虑NFS Slow的选项。

为了达到NFS安装的目的，这个服务器必须支持subdir加载。例如，如果您的FreeBSD 6.0 目录存在：`ziggy:/usr/archive/stuff/FreeBSD`，然后ziggy将必须允许直接挂上`/usr/archive/stuff/FreeBSD`，而不仅仅是`/usr`或`/usr/archive/stuff`。

在FreeBSD的`/etc/exports`配置文件中，是由`-alldirs`选项来控制的。其它NFS服务器也许有不同的方式。如果您从服务器得到`permission denied`这个信息，可能是因为没有正确的启用它。

第3章

UNIX 基础

Rewritten by Chris Shumway.

3.1 概述

下列章节的命令和功能适用于FreeBSD操作系统。同时这里许多内容和一些类-UNIX 操作系统相关。假如您已经熟悉这些内容可跳过不阅读。假如您是FreeBSD新手，那您应该认真详细地从头到尾读一遍这些章节。

读取这些内容，您将了解：

- 怎样在FreeBSD使用“虚拟控制台”。
- 在UNIX 中文件权限如何运作，以及理解FreeBSD 中的文件标志。
- FreeBSD 默认文件系统的架构。
- FreeBSD磁盘架构。
- 怎样挂接或卸下文件系统。
- 什么是进程、守护进程、信号。
- 什么是shell，应当怎样去改变登录进入的默认环境。
- 怎样使用基本的文本编辑器。
- 什么是设备，什么是设备节点。
- FreeBSD 下，使用的是何种可执行文件格式。
- 怎样使用man 手册并取得更多资讯。

3.2 虚拟控制台和终端

FreeBSD能多方面应用，其中之一它能在字符终端输入命令。您可以在这方面容易地使用FreeBSD这个有强大适应性和功能的UNIX 系统，这部份介绍“多终端”和“多控制台”，和您在FreeBSD 应怎样使用它们。

3.2.1 控制台

假如您没有设置到FreeBSD 在启动期间给出图形登录，那么系统将在引导和启动脚本正确运行完成后，给您一个登录的提示。您会看到类似这样的界面：

```
Additional ABI support:.  
Local package initialization:.  
Additional TCP options:.
```

```
Fri Sep 20 13:01:06 EEST 2002
```

```
FreeBSD/i386 (pc3.example.org) (ttyv0)
```

```
login:
```

这些信息可能和您的系统稍微有点不同，但不会有很大差别。最后两行是我们感兴趣的，理解这一行：

```
FreeBSD/i386 (pc3.example.org) (ttyv0)
```

这一行是您刚才启动的系统信息其中一块，您所看到的是一个“FreeBSD”控制台，运行在一个Intel或兼容的x86体系架构上面¹。这个结构名称(每一种UNIX结构都有自己的名称)叫pc3.example.org，就是现在这个系统控制台——这个ttyv0终端的样子。

在最后，最后一行一直保持这样：

```
login:
```

这里，您将可以输入用户名“username”并登录到FreeBSD系统中。接下来的一节，将介绍如何登录系统。

3.2.2 进入FreeBSD

FreeBSD是一个多用户和多重处理的系统，这个介绍换句话说就是一个系统可容纳许多不同的用户，谁都可以同时在单一结构下运行大量的程序。

每一个多用户系统都必须在某方面去区别“user”，在FreeBSD里(以及类-UNIX操作系统)，完成这方面工作是有必要的，每位使用者在运行程之前都必须“登录”，每位用户都有他的用户名(“username”)和密码(“password”)。FreeBSD会在用户进入之前作出两次询问。

当FreeBSD引导并运行完启动脚本之后，²，它会给出一个提示，并要求输入有效的用户名：

```
login:
```

举个例子更容易理解，我们假设您的用户名叫john。在提示符下输入john并单击**Enter**，此时您应该看到这个提示“password”：

```
login: john
Password:
```

现在输入john的密码，和单击**Enter**。这个密码是没有回显的！您在这时不必担心，它出于安全考虑才这样做的。

假如您输入的密码是正确的，您应该尽快进入FreeBSD并为练习可用的命令作好准备。

您应该看见MOTD 或者出现一个命令提示符(#、\$ 或% 字符)，这表明您已成功登录进入FreeBSD。

3.2.3 多个控制台

在一个控制台运行UNIX命令虽说很好，但FreeBSD具有一次运行多个程序的能力。仅使用一个控制台只会浪费FreeBSD同时运行多任务的能力。而“虚拟控制台”在这方面发挥强大的功能。

FreeBSD能配置出给您不同需求的虚拟控制台，在键盘上您用一组键就能从各个虚拟控制台之间切换。各个控制台有自己的传输通道，当您从各个控制台切换时FreeBSD会切换到合适的键盘传输通道和显示器传输通道。

FreeBSD 各个控制台之间可利用特殊组键切换并保留原有控制台³，您可这样做：**Alt-F1**，**Alt-F2**，一直到**Alt-F8**在FreeBSD里切换到其中一个虚拟控制台。

同样地，您正在从其中某个控制台切换到另一个控制台的时候，FreeBSD 会保存正在使用和恢复将要使用屏幕传输通道。这种结果形成一种“错觉”，您拥有许多“虚拟”屏幕和键盘可以输入很多的命令。这些程序需要在一个虚拟控制台不能停止运行而又不需要观察它，它继续运行而您可以切换到其他的虚拟控制台。

3.2.4 /etc/ttys文件

FreeBSD 虚拟控制台的默认配置为8个，但并不是硬性设置，您可以很容易设置虚拟控制台的个数增多或减少。虚拟控制台的编号和设置在/etc/ttys 文件里。

您可以使用/etc/ttys 文件在FreeBSD 下配置虚拟控制台。文件里每一未加注释的行都能设置一个终端或虚拟控制台(当行里含有# 这个字符时不能使用)。FreeBSD 默认配置是配置出9个虚拟控制台而只能启动8个，以下这些行是ttyv 一起启动：

#	name	getty	type	status	comments
#	tttyv0	"/usr/libexec/getty Pc"	cons25	on	secure
#	Virtual terminals				
	tttyv1	"/usr/libexec/getty Pc"	cons25	on	secure
	tttyv2	"/usr/libexec/getty Pc"	cons25	on	secure
	tttyv3	"/usr/libexec/getty Pc"	cons25	on	secure
	tttyv4	"/usr/libexec/getty Pc"	cons25	on	secure
	tttyv5	"/usr/libexec/getty Pc"	cons25	on	secure
	tttyv6	"/usr/libexec/getty Pc"	cons25	on	secure
	tttyv7	"/usr/libexec/getty Pc"	cons25	on	secure
	tttyv8	"/usr/X11R6/bin/xdm -nodaemon"	xterm	off	secure

您能在这文件详细设置每行的参数，加载虚拟控制台启动所需要的物件。请参考ttys(5) 联机手册。

3.2.5 单用户模式的控制台

关于“单用户模式”详细介绍在第12.6.2 节 这里可以找到。当您运行单用户模式时只能使用一个控制台，没有多个虚拟控制台可使用。单用户模式的控制台也可以在/etc/ttys 文件设置，可在这行找到要启动的控制台：

#	name	getty	type	status	comments
#	# If console is marked "insecure", then init will ask for the root password				
#	# when going to single-user mode.				
	console	none	unknown	off	secure

注意：这个console 已经注释掉，您可编辑这行把secure 改为insecure。这样，当用单用户进入FreeBSD 时，它仍然要求提供root 用户的密码。

在把这个选项改为insecure 的时候一定要小心，如果您忘记了root 用户的密码，进入单用户会有点麻烦。尽管仍然能进入单用户模式，但如果您不熟悉它就会非常令人头疼。

3.3 权限

FreeBSD, 是BSD UNIX 的延续, 并基于几个关键的UNIX 观念。从一开始就多处提到FreeBSD 是一个多用户的操作系统, 它能分别处理几个同时工作的用户所分配的毫无关联任务。并负责为每位用户的硬件设备、外设、内存和CPU 处理时间作出合理安排。

因为系统有能力支持多用户, 在每一方面系统都会作出谁能读、写和执行的资源权力限制。这点权限以三个八位元的方式储存着, 一个是表示文件所有者, 一个是表示文件所属群组, 一个是表示其他人。这些数字以下列方式表示:

数值	权限	目录列表
0	不能读, 不能写, 不能执行	---
1	不能读, 不能写, 可执行	--x
2	不能读, 可写, 不能执行	-w-
3	不能读, 可写, 可执行	-wx
4	可读, 不能写, 不能执行	r--
5	可读, 不能写, 可执行	r-x
6	可读, 可写, 不能执行	rw-
7	可读, 可写, 可执行	rwX

使用命令的-l (ls(1)) 参数可以显示出文件的所属者、所属组和其他人等属性。请看以下的例子:

```
% ls -l
total 530
-rw-r--r--  1 root  wheel    512 Sep  5 12:31 myfile
-rw-r--r--  1 root  wheel    512 Sep  5 12:31 otherfile
-rw-r--r--  1 root  wheel   7680 Sep  5 12:31 email.txt
...
```

使用ls -l 在每行的开始出现了:

```
-rw-r--r--
```

从左边起的第一个字, 告诉我们这个文件是一怎样的文件: 普通文件? 目录? 特殊设备? socket? 或是设备文件? 在这个例子, - 表示一个普通文件。接下来三个字是rw- 是文件拥有者的权限。再接下来的三个字是r-- 是文件所属群组的权限。最後三个字是r-- 是其他人的权限。以这一个文件为例, 他的权限设定是拥有者可以读写这个文件、群组可以读取、其他使用者也能读取这个文件。根据上面的表格, 用数字表示这个文件其三部分的权限应该是644。

这样很好, 但系统怎样对设备进行权限控制的? 事实上FreeBSD 将大部份设备(的每一个设备)当作一个文件看待, 用程序能打开、读取、写入数据就如其他的文件一样。而设备文件放在/dev 目录。

目录也视为一种文件, 也有读取、写入、执行的权限。但目录的执行权限意义并不与普通文件相同, 实际上执行权限是进入权限。当一个目录是被标示可以执行的时候, 那表示它可以被进入, 利用“cd” (变化目录位置)可以进入。这意味着访问这些目录必须是谁才有权力(当然目录下的文件也受到访问限制)。

详细方面, 想读取一个目录的列表就必须设为可读权限, 同时想删除一个已知的文件, 就必须把目录下这个文件设为可写和 执行权限。

还有更多权限设定, 但是他们大多用在特殊状况下如一个setuid的执行文件和粘贴性目录, 如果想要得知有关文件权限和如何设定的更多资讯, 请看手册chmod(1)。

3.3.1 权限的符号化表示

Contributed by Tom Rhodes.

权限符号，某些时候就是指符号表达式，使用八进制的字符给目录或文件分配权限。权限符号的使用语法是(谁) (作用) (权限)。看看下列数值的在那些地方所起什么样的作用：

选项	字母	介绍
(谁)	u	用户
(谁)	g	所属群体
(谁)	o	其他人
(谁)	a	所有人(“全部”)
(作用)	+	增加权限
(作用)	-	减少权限
(作用)	=	确定权限
(权限)	r	可读
(权限)	w	可写
(权限)	x	执行
(权限)	t	粘贴位
(权限)	s	设置UID 或GID

这些数值chmod(1)以习惯标定的。举个例子，用以下命令阻止其他人访问`FILE`文件：

```
% chmod go= FILE
```

倘若对一个文件作太多的变化设置可用逗号分开，在下面的例子里，可以去掉`FILE`文件的群体和“全部”可写权限，但所有人都可以有执行权限：

```
% chmod go-w,a+x FILE
```

3.3.2 FreeBSD 文件标志

Contributed by Tom Rhodes.

在前面所介绍的文件权限的基础之上，FreeBSD 还支持使用“文件标志”。这些标志为文件提供了进一步的安全控制机制，但这些控制并不适用于目录。

这些文件标志提供了针对文件的进一步控制，帮助确保即使是`root` 用户也无法删除或修改文件。

文件标志可以通过使用chflags(1) 工具来修改，其用户界面很简单。例如，要在文件`file1` 上应用系统禁删标志，应使用下述命令：

```
# chflags sunlink file1
```

要禁用系统禁删标志，只需在前述命令中的`sunlink` 标志前加“no”。例如：

```
# chflags nosunlink file1
```

要显示文件上的标志，应使用ls(1) 的-l 参数：

```
# ls -lo file1
```

删除应类似于：

```
-rw-r--r-- 1 trhodes trhodes sunlnk 0 Mar 1 05:54 file1
```

许多标志只可以由root 用户来增加，而另一些，则可以由文件的所有者来增加。建议管理员仔细阅读chflags(1) 和chflags(2) 联机手册，以对其加深理解。

3.4 目录架构

目录层次是理解一个系统的重要基础，最重要的莫过于它的根目录“/”，这个目录在启动时就挂上，它包含了启动时所需的基本系统。这个根目录同样包含了想要挂接的每一个文件系统。

挂接点(mount point) 是新增的文件系统在接入现有系统时的起点位置。在第3.5 节 对此进行了详细的阐述。标准的挂接点包括/usr、/var、/tmp、/mnt，以及/cdrom。这些目录通常会在/etc/fstab 文件中提及。/etc/fstab 是一张包含系统中各个文件系统及挂接点的表。在/etc/fstab 中的绝大多数文件系统都会在启动时由rc(8) 脚本自动挂接，除非特别指定了noauto 选项。更多细节请参考第3.6.1 节。

您可以通过hier(7) 来了解完整的文件系统层次说明。现在，让我们先来看一看绝大多数的常见的目录以供参考。

目录	介绍
/	文件系统的根目录。
/bin/	在单个用户和多用户环境下的基本工具目录。
/boot/	在操作系统在启动加载期间所用的程序和配置。
/boot/defaults/	默认每步引导启动的配置文件，请查阅loader.conf(5)。
/dev/	设备接点，请查阅intro(4)。
/etc/	系统启动的配置和脚本。
/etc/defaults/	系统默认的启动配置和脚本，请参考rc(8)。
/etc/mail/	关系到邮件系统运作的配置，请参考sendmail(8)。
/etc/namedb/	named 配置文件，请参考named(8)。
/etc/periodic/	每天、每星期和每月周期性地运行的脚本，请通过cron(8)查阅periodic(8)。
/etc/ppp/	ppp配置文件，请查阅ppp(8)。
/mnt/	由管理员习惯使用挂接点的临时空目录。
/proc/	运行中的文件系统，请参阅procfs(5) 和mount_procfs(8)。
/rescue/	用于紧急恢复的一组静态联编的程序；参见rescue(8)。
/root/	root用户的Home(主)目录。
/sbin/	在单个用户和多用户环境下的存放系统程序和管理所需的基本实用目录。

目录

`/stand/``/tmp/``/usr/``/usr/bin/``/usr/include/``/usr/lib/``/usr/libdata/``/usr/libexec/``/usr/local/``/usr/obj/``/usr/ports``/usr/sbin/``/usr/share/``/usr/src/``/usr/X11R6/``/var/``/var/log/``/var/mail/``/var/spool/``/var/tmp/``/var/yp`

介绍

独立的程序环境。

临时文件。`/tmp` 目录中的内容，一般不会对系统重新启动之后保留。通常会将基于内存的文件系统挂在 `/tmp` 上。这一工作可以用一系列 `tmpmfs` 相关的 `rc.conf(5)` 变量来自动完成。(或者，也可以在 `/etc/fstab` 增加对应项；参见 `mdmfs(8)`，或者，如果是 `FreeBSD 4.X`，`mfs(8)`)。

存放大多数用户的应用软件。

存放实用命令，程序设计工具，和应用软件。

存放标准 C include 文件。

存放库文件。

存放各种实用工具的数据文件。

存放系统实用或后台程序(从另外的程序启动执行)。

存放本地执行文件，库文件等等，同时也是 `FreeBSD ports` 安装的默认安装目录。`/usr/local` 在 `/usr` 总体布置请查阅 `man.hier.7`。 `man` 目录例外，它们直接放在 `/usr/local` 而不是 `/usr/local/share` 下，而 `ports` 说明文档在 `share/doc/port`。

通过联编 `/usr/src` 得到的目标文件。

存放 `FreeBSD` 的 `Ports Collection` (可选)。

存放系统后台程序和系统工具(由用户执行)。

存放架构独立的文件。

存放 `BSD` 或者本地源码文件。

存放 `X11R6` 可执行文件、库文件、配置文件等的目录(可选)。

多用途日志、临时或短期存放的，以及打印假脱机系统文件。有时会将基于内存的文件系统挂在 `/var` 上。这一工作可以通过在 `rc.conf(5)` 中设置一系列 `varmfs` 变量(或在 `/etc/fstab` 中加入一行配置；参见 `mdmfs(8)`，或者，如果您用 `FreeBSD 4.X` 则是 `mfs(8)`) 来完成。

存放各种的系统记录文件。

存放用户 `mailbox`(一种邮件存放格式)文件。

各种打印机和邮件系统 `spooling`(回环)的目录。

临时文件。这些文件在系统重新启动时通常会保留，除非 `/var` 是一个内存中的文件系统。

NIS 映射。

3.5 磁盘组织

`FreeBSD` 查找文件的最小单位是文件名。而文件名区分大小写，这就意味着 `readme.txt`

和README.TXT 是两个不相同的文件。FreeBSD 不凭文件扩展名(.txt) 去识别这个文件是程序、文档，或是其他格式的数据。

各种文件存放在目录里。一个目录可以含有许许多多的文件，允许含有其他的目录，同样允许您添加不同层次的目录在里面。可以轻松地组织您的数据。

可以通过文件或目录名来指定文件和目录，在目录名后面加上一个斜线，/，如果需要的话。如果您有一个名为foo 的目录，它包含另一个目录bar，后者包括一个叫readme.txt 的文件，则全名，或者说到文件的路径就是foo/bar/readme.txt。

在文件系统里目录和文件的作用是存储数据。每一个文件系统都正确含有一个顶级目录根目录，这个根目录包含其他目录。

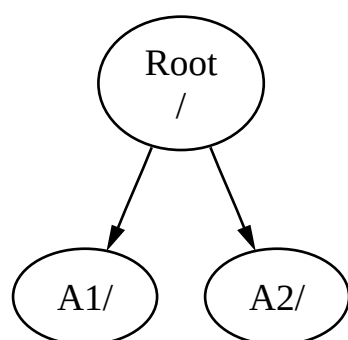
您也许在其他的一些操作系统碰到类似这里的情况，当然也有不同的情况。举些例子，MS-DOS 是用\ 分隔文件名或目录名，而Mac OS® 则使用:。

FreeBSD在路径方面不使用驱动器名符号或驱动器名称，在FreeBSD里您不能这样使用：c:/foo/bar/readme.txt。

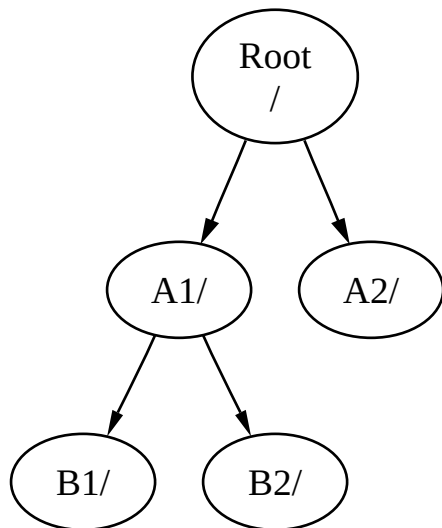
为了代替(驱动器名符号)，一个文件系统会指定根文件系统，根文件系统的根目录是/。其他每一个文件系统挂在根文件系统下。无论有多少磁盘在FreeBSD 系统里，每个磁盘都会以目录的方式加上。

假设您有三个文件系统，名为A、B 和C。每个文件系统有一个根目录，而各自含有两个其他的目录，名为A1, A2 (B1, B2 和C1, C2)。

看看A 这个根文件系统。假如您用ls 命令来查看这个目录您会见到两个子目录: A1 和A2。这个目录树是这个样子:

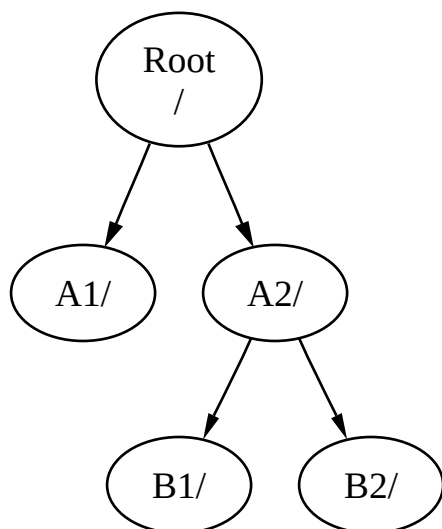


一个文件系统必须挂到另一个文件系统的某一目录，所以现在假设把B 文件系统挂到A1目录，那B 根目录因此代替了A1，而显示出B 目录(的内容):



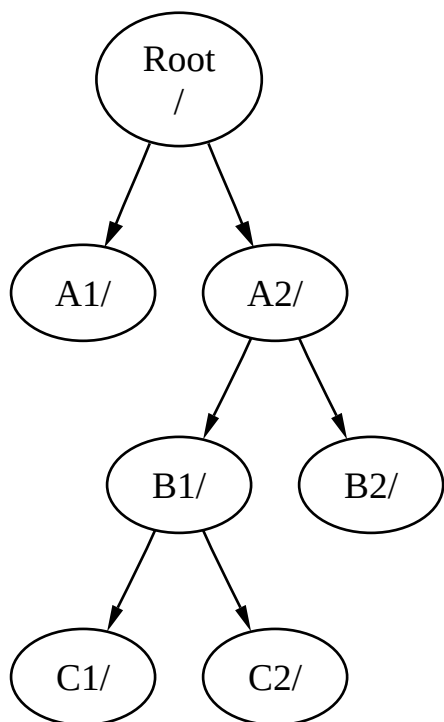
无论B1 或B2 目录在那里而延伸出来的路径必须为/A1/B1 或/A1/B2。而在/A1 里原有的文件会临时隐藏。想这些文件再出现把B 从A 挂接释放。

把B 挂接在A2 那图表的样子就是这样子:

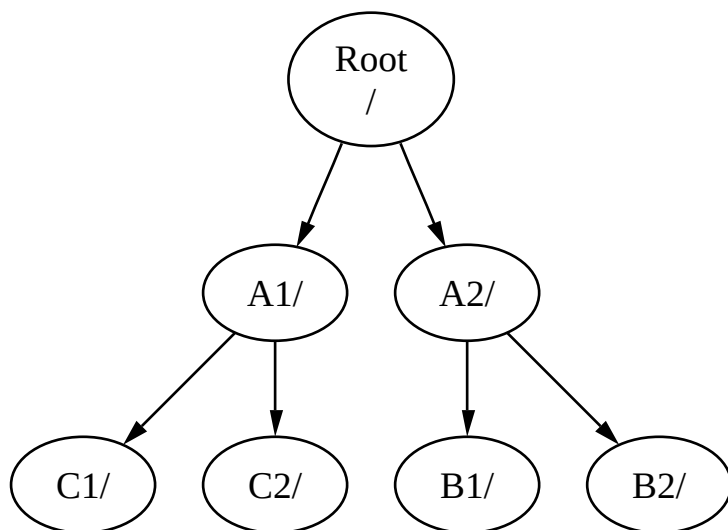


这个路径分别是/A2/B1 和/A2/B2。

文件系统能把顶部挂接上另一个文件系统上。继续这个例子，把C 文件系统挂接在B 文件系统里的B1 目录，排列如下:



或者把C 文件系统挂接在A 文件系统里的A1目录:



假如您熟悉MS-DOS 并知道join 命令，尽管不相同，其实是相似的。

这方面不是普通知识而且涉及到您所关心的，当您安装FreeBSD并在以后添加新磁盘时，您必须知道该如何新建文件系统和挂接上。

(FreeBSD系统)它有一个主要的根文件系统，不需要另外新建立，但当需要手工处理时，这是一个有用的知识。

多样性文件系统的益处

- 不同的文件系统可用不同的挂接参数。举些例子，仔细想一下，根文件系统能用只读的方式挂接上，防止不经意删除或编辑到一个危险的文件。把各用户能写入的文件系统分开，像/home这样，由另外的文件系统分别用nosuid参数挂接，这个参数防止suid/guid在执行这个文件系统中的文件时生效，从而缓解了一些安全问题。
- FreeBSD 对一个文件系统的文件布局自动优化，并依赖文件系统的使用习惯。所以一个文件系统应有一个针对大量小型文件频繁写入的优化，另外大型文件系统的优化也应落实。
- FreeBSD 的文件系统能够在断电时尽可能避免损失。然而，在关键点时的电源失效仍然可能会破坏文件系统的结构。将您的文件系统分成多个有助于分散风险，并方便备份和恢复。

统一文件系统的益处

- 文件系统是固定大小的。当安装FreeBSD时新建一个文件系统并设定一个大小，您会在稍后发觉到必须去建一个大的分区。如果配置不当，则需要备份、重新创建文件系统，然后再恢复数据。

重要: FreeBSD 4.4 或更高的版本提供了growfs(8)命令。这使得能够实时地调整文件系统的大小，因而不受其限制。

文件系统是和分区一一对应的。这里的分区和常用的术语分区(例如，MS-DOS分区)的意思并不一样，这是由于FreeBSD的UNIX传统造成的。每一个分区使用一个从a到h的字母来表示。每个分区只能包含一个文件系统，这意味着文件系统通常可以由它们在文件系统目录结构中的挂接点，或对应的分区字母来表示。

FreeBSD的交换分区也需要使用磁盘空间。交换分区是给FreeBSD作虚拟内存使用的，这样能令您的计算机有更多的内存可使用，当FreeBSD在运行而内存不够的时候，它会把其他一些可转移的数据转移到交换分区，空出内存的位置以供使用。

某些partitions的用途是确定的。

分区	约定
a	通常指定为根文件系统
b	通常指定为交换分区
c	通常它和所在的slice大小相同。c分区上工作时必定会影响到整个slice(举个例子，坏块扫描器)。您通常不愿意在这个partition建立文件系统。
d	分区d曾经有特殊的含义，虽然(对我们来说)早已远离而去。但直到今天，一些工具在分区d上运行会发生古怪事情，所以sysinstall通常不建立分区d。

每一个包含了文件系统的分区被保存在FreeBSD称为slice的部分上。Slice是一个FreeBSD术语，通常被叫做分区，再次强调，这是由于FreeBSD的UNIX背景。Slices有其编号，从1到4。

Slice编号在设备名后面，并有一个s前缀，从1开始。因此“da0s1”是第一个SCSI驱动器的第一个slice。每个磁盘上只能有四个物理的slices，但您可以在物理slice中使用适当的类型来创建逻辑slice。这些扩展slice编号从5开始，因此“ad0s5”是第一个IDE磁盘中的第一个扩展slice。文件系统所使用的设备应该占满slice。

Slices，“专项指定”物理驱动器，和其他驱动器都包含partitions，那几个的partitions都是用字母从a到h来标定的，而这些字母都在驱动器名字之后，所以“da0a”是指首个da设备的a partition，而那个就

是“专项指定”。“ad1s3e”是指IDE磁盘第三个slice的第五个partition。

最终，每个磁盘都被系统识别。一个磁盘名字是用磁盘类型代码和编号来标识的，它不像slices，磁盘的编号是由0开始的。对应代码请看这里所列出的表3-1。

当提供一个partition名字给FreeBSD时，slice 和磁盘所必须有这个partition，还应当提供所partition所涉及到的slice和磁盘的名字。可这样列出：磁盘名称,s,slice 编号,和partition标定字母。例子请看例3-1。

例3-2 这里显示了一个磁盘的布局，有更清楚的帮助。

在安装FreeBSD时，您首先要配置好磁盘slices，然后在FreeBSD使用的slice上建立partitions。并在每个partition上建立一个文件系统(或交换分区)，和指定文件系统的挂接位置。

表3-1. 磁盘设备的代码

代码	说明
ad	ATAPI (IDE) 磁盘
da	SCSI 直接存取磁盘
acd	ATAPI (IDE) 光驱
cd	SCSI 光驱
fd	软驱

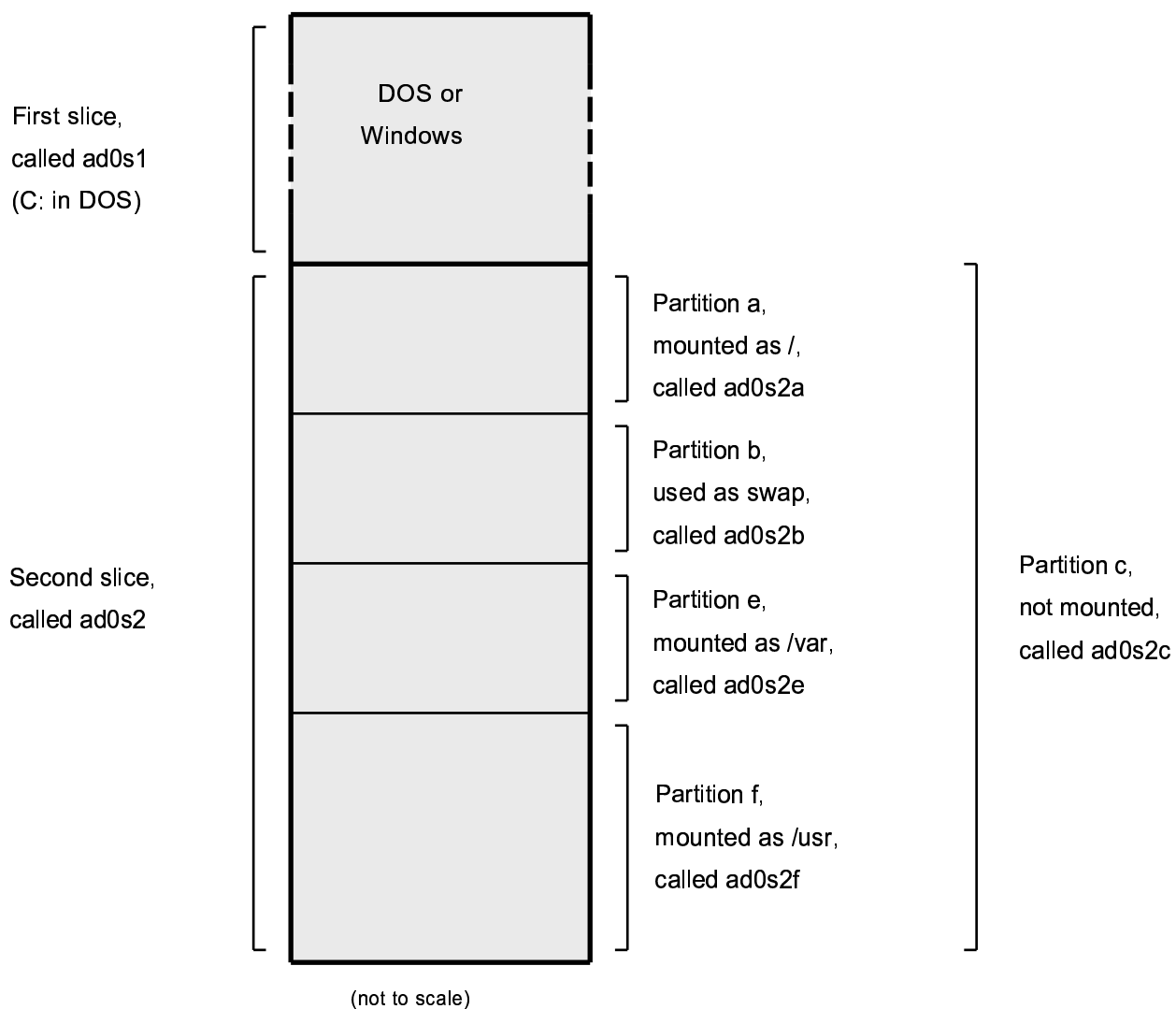
例3-1. 样例磁盘, Slice, 和Partition 它们的命名

命名	说明
ad0s1a	在首个IDE磁盘(ad0)上的第一个slice (s1)里的第一个partition (a)。
da1s2e	在第二个SCSI磁盘(da1)上的第二个slice(s2)里的第五个partition(e)。

例3-2. 一个磁盘的布局

从在系统里的首个IDE磁盘图表可以显示出FreeBSD的见解。假设磁盘大小为4 GB，它里面包含了两个2 GB大小的slices (但在MS-DOS叫partitions)。首个slice是一个MS-DOS磁盘叫C:，而第二个slice是FreeBSD配置好的slice。FreeBSD配置好的slice有三个partitions和另一个交换分区。

这三个partitions各自控制一个文件系。partitiona用于根文件系统，partitione用于/var目录层，partitionf用于/usr目录层。



3.6 文件系统的挂接和卸下

这种文件系统就像一棵树那样用`/`确立根部，是比较理想的文件系统。而`/dev`、`/usr`和其他目录就是根目录的分枝，另外这些目录可以再分枝，例如`/usr/local`。

应该考虑给某些目录一些空间从而分散文件系统。`/var`之下包含目录`log/`，目录`spool/`，和不同类型的临时文件，很可能把它塞满。把什么都塞进根文件系统不是一个好主意，好的做法是应该把`/var`从`/`分离出去。

另一个要考虑的是，给物理设备或虚拟磁盘这些自带空间的文件系统确定目录结构树。例如网络文件系统 或光驱的挂接。

3.6.1 fstab 文件

在引导过程 期间，自动挂上 `/etc/fstab` 所列出的文件系统。(除非他们注明为 `noauto` 选项)。

`/etc/fstab` 文件包含的各行的列表格式如下：

```
device          /mount-point fstype      options      dumpfreq      passno
```

device

设备名称(设备必须存在)，说明在第17.2 节。

mount-point

目录(目录必须存在)，用在那个挂接上的文件系统上。

fstype

文件系统类型，请通过 `mount(8)` 查阅。默认的FreeBSD文件系统类型是 `ufs`。

options

设为可读写文件系统的 `rw` 选项，或设为只读文件系统的 `ro` 选项，或其他一些选项，可随意选一个。一个常用的选项 `noauto` 用在不需在引导过程期间挂接的文件系统。其他的选项在 `mount(8)` 手册里列出。

dumpfreq

`dump(8)` 使用这项去决定那个文件系统必须移贮。假如缺少这项，默认的数值为0。

passno

这一项决定文件系统的检查顺序，文件系统想跳过检查应将 `passno` 设为0。根文件系统(那个是在每方面开始之前必须检查的) 应该将它的 `passno` 设为1，其他文件系统的 `passno` 必须把数值设到大于1。假如多个文件系统的 `passno` 的值相同，那么 `fsck(8)` 在允许的情况下将尝试并行地去检查文件系统。

Consult the `fstab(5)` manual page for more information on the format of the `/etc/fstab` file and the options it contains.

3.6.2 mount 命令

这个 `mount(8)` 命令是挂接文件系统的基本运用。

使用最多的基本格式：

```
# mount device mountpoint
```

它的选项非常多，而 `mount(8)` 手册同样提及，但常用的都在这里：

挂接的各种选项

-a

挂接/etc/fstab里所有列出的文件系统。除非标记为“noauto”或作了排除在外的-t 类型标记，或者在这之前已挂上。

-d

除了实际上系统调用以外，可以完成任何事情，这个选项是和-v参数一起连在一块使用，可以决定mount(8)所做的事情。

-f

强制去挂接一个未知的文件系统(会有危险)，或当把一个文件系统挂接状态由可读写降为只读时，强制撤消可写通道。

-r

以只读方式挂接文件系统。这和在指定了-o 选项配合ro (对于FreeBSD 5.2 之前的版本来说，则是rdonly) 参数的效果是一样的。

-t fstype

根据给出的文件系统类型挂接文件系统，假如给于-a选项，仅挂接这个类型的文件系统。

“ufs” 是默认的文件系统类型。

-u

在文件系统上修改挂接选项。

-v

版本模式。

-w

以可读写方式挂接文件系统。

The -o 选项采用一个逗号分开以下多个选项:

nodev

拒绝把文件系统识别为特别的设备。这是一个有用的安全选项。

noexec

不允许文件系统上的二进制程序执行。这也是一个有用的安全选项。

nosuid

不允许文件系统上的setuid 或setgid 标记生效。这也是一个有用的安全选项。

3.6.3 umount 命令

umount(8) 命令同样采用一个参数、一个挂接点、一个设备名。或采用-a选项，又或采用-A选项。

所有格式都可采用 **-f** 去强行卸下，或采用 **-v** 用那适当的版本。但警告，采用 **-f** 并不是一个好主意，强行卸下文件系统可能损坏计算机或破坏文件系统上的数据。

-a 和 **-A** 会卸下所有已挂接的文件系，可能通过 **-t** 后面列出的文件系统进行修改，但无论如何，**-A** 都不会尝试去卸下根文件系统。

3.7 进程

FreeBSD 是一个多任务操作系统。这就意味着好像一次可以运行一个以上的程序。每个占用一定时间运行的程序就叫 *process*。每个程序启动运行时至少有一个新进程，并在所有运行的时候保持有一个系统进程的编号，而一直由系统对它监管。

每个进程用来标识的一个编号就叫 *进程ID*，或叫 *PID*。而且，就像文件那样，每个进程也有所属用户和所属群体。所属用户和所属群体使用在这方面：确定这个进程可以打开那些文件和那些设备，从而在初期使用文件的权限。多数的进程都同样有一个父进程，而进程是依靠父进程来启动的。例如，假如您把命令输入到 *shell* 里那 *shell* 是一个进程，而您运行的各个命令同样是进程，那么，*shell* 就是您各个运行进程的父进程。而这方面有一个例外的进程就叫 *init(8)*。*init* 始终是首个进程，所以他的 *PID* 始终是 1，而 *init* 在 FreeBSD 启动时由内核自动启动。

在系统上，有两个命令对进程观察非常有用：*ps(1)* 和 *top(1)*。这个 *ps* 命令作用是观察当前运行进程的状态，显示他们的 *PID*，使用了多少内存，它们启动的命令行。而 *top* 命令则是显示所有运行进程，并在以秒计的短小时内更新数据。您能交互式的观察您计算机的工作。

默认情况下，*ps* 仅显示出您自己所运行的命令。例如：

```
% ps
  PID  TT  STAT      TIME COMMAND
  298   p0  Ss      0:01.10 tcsh
  7078  p0   S      2:40.88 xemacs mdoc.xsl (xemacs-21.1.14)
 37393  p0   I      0:03.11 xemacs freebsd.dsl (xemacs-21.1.14)
 48630  p0   S      2:50.89 /usr/local/lib/netscape-linux/navigator-linux-4.77.bi
 48730  p0  IW      0:00.00 (dns helper) (navigator-linux-)
 72210  p0  R+      0:00.00 ps
   390  p1  Is      0:01.14 tcsh
  7059  p2  Is+     1:36.18 /usr/local/bin/mutt -y
  6688  p3  IWs     0:00.00 tcsh
 10735  p4  IWs     0:00.00 tcsh
 20256  p5  IWs     0:00.00 tcsh
   262  v0  IWs     0:00.00 -tcsh (tcsh)
   270  v0  IW+     0:00.00 /bin/sh /usr/X11R6/bin/startx -- -bpp 16
   280  v0  IW+     0:00.00 xinit /home/nik/.xinitrc -- -bpp 16
   284  v0  IW      0:00.00 /bin/sh /home/nik/.xinitrc
   285  v0   S      0:38.45 /usr/X11R6/bin/sawfish
```

在这个例子里您可看到，从 *ps(1)* 输出的每一列是有规律的。*PID* 就是进程ID，这个较早前已讨论过了。*PID* 号的分配由 1 一直上升直到 99999，当您运行到超过限制时，这些编号会回转分配。*TT* 这一列显示了程序运行所在的终端，目前可以安全地忽略。*STAT* 显示程序的状态，也可以安全地被忽略。*TIME* 是程序在 CPU 处理时间——运行的时间量，并不是指您程序启动到现在的所用的时间。许多程序碰巧遇到某方面在他们之前要花费大量 CPU 处理时间时，他们就必须等候。Finally, *COMMAND* is the command line that was used to run the program.

`ps(1)`支持使用各种选项去改变显示出来的内容，最有一个就是`auxww`。`a`选项显示出所有运行进程的内容，而不仅仅是您的进程。`u`选项显示出进程所归属的用户名字以及内存使用，`x`选项显示出后台进程。而`ww`选项表示为`ps(1)`把整个命令行全部显示完，而不是由于命令行过长就把它从屏幕上截去。

下面和从`top(1)`输出是类似的，一个示例式对话就象这样子：

```
% top
last pid: 72257; load averages: 0.13, 0.09, 0.03 up 0+13:38:33 22:39:10
47 processes: 1 running, 46 sleeping
CPU states: 12.6% user, 0.0% nice, 7.8% system, 0.0% interrupt, 79.7% idle
Mem: 36M Active, 5256K Inact, 13M Wired, 6312K Cache, 15M Buf, 408K Free
Swap: 256M Total, 38M Used, 217M Free, 15% Inuse

  PID USERNAME PRI NICE  SIZE  RES STATE   TIME  WCPU   CPU COMMAND
72257 nik      28  0 1960K 1044K RUN    0:00 14.86% 1.42% top
 7078 nik       2  0 15280K 10960K select 2:54 0.88% 0.88% xemacs-21.1.14
  281 nik       2  0 18636K 7112K select 5:36 0.73% 0.73% XF86_SVGA
  296 nik       2  0 3240K 1644K select 0:12 0.05% 0.05% xterm
48630 nik       2  0 29816K 9148K select 3:18 0.00% 0.00% navigator-linu
  175 root       2  0 924K 252K select 1:41 0.00% 0.00% syslogd
 7059 nik       2  0 7260K 4644K poll  1:38 0.00% 0.00% mutt
...
```

这个输出分成两部份。前面部份(起始前五行)显示了:运行于最后进程的PID、系统负载均衡(那个是指系统繁忙时的调节方式)、系统正常运行时间(指从启动算起所用的时间)和当前时间。前面部份另外的图表涉及:多少进程在运行(这个情况是47)，多少内存和多少交换分区在使用，和在不同CPU状态里系统消耗多少时间。

在那下面一连串的纵列和从`ps(1)`输出的的内存是相似的。如以前`ps(1)`一样，您能见到:PID、用户名、CPU处理时间合计、运行的命令。`top(1)`默认是显示您的进程所用内存空间的合计。内存空间这里分成两列，一列为总体大小，另一列是必须请求驻留大小是多少内存——总体大小。而驻留大小实际上是瞬间使用的多少。在以上那个例子，您会看到那Netscape®总计需要30 MB内存，但实际只用了9 MB。

`top(1)`每两秒自动刷新一次，您可以用`s`改变刷新的秒数。

3.8 守护进程，信号和杀死进程

当您运行一个编辑器时它是很容易控制的，告诉它去加载文件它就加载。您之所以能这样做，是因为编辑器提供这样便利去这样做，和因为有编辑器去附上的终端。一些程序在运行中不需要连续的用户输入，一有机会就从终端里分离到后台去。例如，一个web系统整天都在作web请求的响应，他不需要您输入任何东西就能完成，这个类别的另一个例子就是把email的传送。

我们把那些程序叫守护进程。守护神是希腊神话中的一些人物，非正非邪，他们是些守护小精灵，大体上为人类作出贡献。许多类似web服务或mail服务的系统对于今天仍有用途，这就是为什么在那么长的时间里，BSD的吉祥物保持为一双鞋加一把钢叉的守护神模样。

守护进程的程序命名通常在最后加一个“d”。**BIND**是伯克利互联网域名服务(而实际执行的程序名称则是named)，**Apache web**系统的程序就叫httpd，在行式打印机上的打印守护进程就是lpd。这只是一种惯例，不是标准或硬性规定。例如，为**Sendmail**而应用的主要mail守护进程就叫sendmail，却不叫maild，这和您推测的一样。

有时可能会需要与守护进程进行通讯。而信号则是其中的一种通讯机制。可以发送信号给守护进程(或相关的另一些进程)来与它进行通信，不同的信号都有自己的数字编号——其中一些有特殊的含义，其它的

则可以被应用程序自己进行解释，而一般来说，应用程序的文档会告诉哪些信号会被如何处理。您只能给所属于您的进程发信号，假如您给其他人的进程发信号，进程就会用kill(1)或kill(2)权限进行拒绝。当然，root用户会例外，它能把各种信号发送给每个进程。

在某些情况下，FreeBSD也会向应用软件发送信号。假如一个应用软件含有恶意写入并试图去访问内存，那是不可想象的，FreeBSD会向那个进程发送段式违规信号(SIGSEGV)。假如一个应用软件使用alarm(3)系统去进行周期性调用闹钟功能，每当达到时间时，FreeBSD会向应用软件发送闹钟信号(SIGALRM)。

有两个信号可以停止进程：SIGTERM和SIGKILL。SIGTERM比较友好，进程能捕捉这个信号，根据您的需要来关闭程序。在关闭程序之前，您可以结束打开的记录文件和完成正在做的任务。在某些情况下，假如进程正在进行作业而且不能中断，那么进程可以忽略这个SIGTERM信号。

对于SIGKILL信号，进程是不能忽略的。这是一个“我不管您在做什么，立刻停止”的信号。假如您发送SIGKILL信号给进程，FreeBSD就将进程停止在那里。⁴

您可能会去使用SIGHUP、SIGUSR1和SIGUSR2信号。这都是些通用的信号，各种应用程序都可以应用在各方面的信号发送。

假如您改变了web系统的配置文件——并想web系统去重读它的配置，您可以停止然后再启动httpd。但这样做web系统会导致一个短暂的中断周期，那样是不受欢迎的。几乎所有的守护进程在编写时，都会指定对SIGHUP信号进行响应从而重读配置文件。所以，最好的方法，就不是杀死并重启httpd，而是发一个SIGHUP信号给它。因为在这方面没有一个标准，不同的守护进程有不同的用法，所以不了解时应读一下守护进程的文档。

发送信号可用kill(1)命令，请参考kill(1)所列出的例子。

发送一个信号给进程

这个例子显示了怎样去发一个信号给inetd(8)。inetd配置文件是/etc/inetd.conf，如果想inetd去重读文件系统的话，可以给它发一个SIGHUP信号。

1. 寻找您要发送信号的进程ID，可以用ps(1)加grep(1)来完成。grep(1)命令被用在搜索输出方面，搜索您指定的字符串。这命令是由普通用户来执行的，而inetd(8)是root用户运行的，所以必须给ps(1)带上ax选项。

```
% ps -ax | grep inetd
198  ??  IWs    0:00.00 inetd -ww
```

得出inetd(8) PID号是198。有时grep inetd命令也出现在输出中，这是因为在这方面ps(1)也是寻找列表中运行进程。

2. 使用kill(1)去发送信号。因为inetd(8)是由root启动的，您必须使用su(1)去变为root用户。

```
% su
Password:
# /bin/kill -s HUP 198
```

和大多数UNIX命令一样，kill(1)如果完成了任务，就不会给出任何消息。假如您发送信号给一个不属于您的进程，您会看到kill: PID: Operation not permitted。假如输错了PID号，把信号发送到其他进程，那是坏事。或者您侥幸，把信号发送到不存在的进程，您会看见kill: PID: No such process。

为什么使用/bin/kill? 许多shell提供了内建kill命令，这样，shell就能直接发送信号，而不是运行/bin/kill。这点非常有用，但不同shell有不同的语法来指定发送信号的名字，与其试图把它们学完倒不如简单地直接使用/bin/kill ...。

发送其他的信号也很相似，只要在命令行替换TERM或KILL就行了。

重要：在系统上随意杀死进程是个坏主意，特别是init(8)，它的进程ID是1，它非常特殊。可以运行/bin/kill -s KILL 1 命令来让系统迅速关机。当您按下Return键之前，一定要详细检查您运行kill(1)时所指定的参数。

3.9 Shells

在FreeBSD里，每日有一大堆工作是在命令行的界面完成的,那就叫做shell。一个shell的主要功能就是从输入是取得命令然后去执行他。许多的shell同样能帮我们完成内建的每日功能，例如:文件管理、文件寻找、命令行编辑、宏指令和环境变量。FreeBSD内含了一些shell，例如:sh、Bourne Shell、tcsh和改良过的C-shell。另外也有些shell也可在FreeBSD的Ports得到，例如:zsh和bash。

您想使用那一种shell取决于您的喜好，假如您是C程序设计师，您可能选择一个C-like shell例如tcsh。假如您是从Linux过来的或是一个命令行的新手，您可能会试一下bash。这一点告诉我们每一个shell都有各自的特性，可能适用于您的工作环境，也可能不适用于您的工作环境。

每个shell都有一个共通点就是文件名补全。输入命令或文件名的前几个字，然后按Tab键，就能靠shell的自动补全功能得出命令或文件名。这里有一个例子，假设您有两个文件叫foobar 和foo.bar，而您想删除foo.bar，可这样在键盘上输入rm fo[Tab].[Tab]。

那么shell就会输出rm foo[BEEP].bar。

这个[BEEP]是这控制台铃声，那个是告诉我们它不能完成文件名补全，因为有多多个文件名符合。foobar 和foo.bar 都是以fo开头，它只可以补全到foo。输入.并再按一次Tab，shell才把其余的文件名全部显示出来。

另一个特点就是shell利用环境变量运行。环境变量是贮存在shell环境空间上相对应的键和可变值，这个空间能够补程序从shell里读出，而且包含了许多程序的配置。这个一个常用环境变量列和其含义的列表：

变量	说明
USER	当前登录进入的用户名。
PATH	搜索程序路径，以两点的冒号分隔开。
DISPLAY	假如有这个变量的话，就是X11显示器的网络名称。
SHELL	当前所用的shell。
TERM	用户终端的名字，通常用在确定终端的能力。
TERMCAP	各种终端功能所用终端分离编码的基本数据项目。
OSTYPE	操作系统类型，默认是FreeBSD。
MACHTYPE	是指系统上运行的CPU体系结构。
EDITOR	用户首选的文本编辑器。
PAGER	用户首选的文本页面调度程序。
MANPATH	搜索联机手册路径，以两点的冒号分隔开。

不同的shell设置环境变量也不相同。举个例子，在如tcsh 和csh这样的C-Style shell，您必须使

用`setenv`去设置环境变量。而在如`sh`和`bash`这样的Bourne shell，您必须使用`export`去设置当前环境变量。再举个例子，要去设置或改变`EDITOR`环境变量，在`csh`或`tcsh`下将`EDITOR`设为`/usr/local/bin/emacs`：

```
% setenv EDITOR /usr/local/bin/emacs
```

而在Bourne shell下，则是：

```
% export EDITOR="/usr/local/bin/emacs"
```

您也可以在命令行上加一个`$`字符在变量之前从而取得环境变量。举个例子，用`echo $TERM`就会显示出`$TERM`的设定值，其实就是shell取得`$TERM`并传给`echo`来显示的。

shell里有许多特别的字符代表着特别的资料，我们把叫做meta-characters。最常用的就是`*`字符，它可代表文件名的任何字符。这些特别字符应用到文件名全域方面。假如，输入`echo *`和输入`ls`的效果是相同的，其实就是shell取得了全部符合`*`的文件名，并传给`echo`在命令行下显示出来。

为了防止shell去分析这些特别字符，我们可在它之前加一个`\`字符去说明它只是普通字符。`echo $TERM`就会显示出您的终端情况，而`echo \$TERM`就会显示出`$TERM`这几个字。

3.9.1 改变您用的Shell

改变您的Shell的最简单方法是使用`chsh`命令。执行`chsh`将根据您设定的`EDITOR`环境变量进入到那个编辑器，假如没有设定，就会进入`vi`编辑器。请改变“Shell:”这行对应值。

您可使用`chsh`的`-s`选项，这样就能设置您的shell却又不用编辑器。假如您想把shell改为`bash`可用下面的技巧。

```
% chsh -s /usr/local/bin/bash
```

注意：您使用的shells必须在`/etc/shells`文件里列出。假如您从ports里装一个shell，那就不用做这步了。假如您手工装一个shell，那就要手工添加进去。

举个例子，假如您手工把`bash`装到`/usr/local/bin`里，您还要进行这一步：

```
# echo "/usr/local/bin/bash" >> /etc/shells
```

然后运行`chsh`。

3.10 文本编辑器

FreeBSD 的很多配置都可以通过编辑文本文件来完成。因此，最好能熟悉某种文本编辑器。FreeBSD 基本系统中提供了一些，您也可以从Ports Collection 安装其它编辑器。

最容易学的而又简单的编辑器是`ee`编辑器，是个标准的简易编辑器。要启动`ee`，首先就要在命令行输入`ee filename`，`filename`是一个要编辑的文件名。例如，要编辑`/etc/rc.conf`就要输入`ee /etc/rc.conf`，在`ee`的控制内，编辑器所有功能的操作方法都显示在最上方。这个`^`字符代表键盘上的`Ctrl`键，所以`^e`就是`Ctrl+e`组合键。假如想离开`ee`，按`Esc`键，就可选择离开编辑器。当您修改了内容的时候，编辑器会提示您保存。

FreeBSD本身也带许可多有强大功能的文本编辑器，例如**vi**。还有其他在FreeBSD Ports里几种，像**emacs** 和**vim**。这些编辑器有着强大的功能，但同时学习起来比较复杂。不管怎样，假如您从事文字编辑方面的工作，学习如**vim** 或**emacs** 这些有强大功能的编辑器用法，在长时间工作里会帮您节省不少的时间。

3.11 设备和设备节点

在一个系统里，硬件描述通常用法就是一个设备对应一个术语，包括磁盘、打印机、显卡和键盘。当FreeBSD启动过程中，大多数的设备都能探测到并显示出来，您也可以查阅`/var/run/dmesg.boot`，引导时所有信息都在里面。

例如，`acd0` 就是首个IDE 光盘设备，而`kbd0` 则代表键盘。

在UNIX操作系统里，大多数设备存在的特殊访问文件就是叫做设备节点，他们都定位在`/dev`目录里。

3.11.1 建立设备节点

当增加一个新设备或附加设备需要寻求支持时，您也许需要在新设备上建立单个或多个的设备节点。

3.11.1.1 MAKEDEV 脚本

当系统缺少DEVFS (涉及的是FreeBSD 5.0之前的版本)，建立设备节点可以使用MAKEDEV(8)，就如下面显示的那样：

```
# cd /dev
# sh MAKEDEV ad1
```

这个是一个例子，在安装第二个IDE设备时去建立设备节点。

3.11.1.2 DEVFS (DEvIce 文件系统)

这个设备文件系统，或叫DEVFS，为内核的设备命名在整体文件系统命名里提供通道，并不是建立或更改设备节点，DEVFS只是为您的特别文件系统进行维护。

更多的资料请查devfs(5) 手册。

DEVFS在FreeBSD 5.0或更高的版本里是默认使用。

3.12 二进制文件格式

要理解为什么FreeBSD 使用elf(5) 格式，您必须首先了解一些UNIX 系统中的三种“主要”可执行文件格式的有关知识：

- a.out(5)

是最古老和“经典的” UNIX 目标文件格式，这种格式在其文件的开始处有一个短小而又紧凑的首部，该首部带有一个魔幻数字，用来标识具体的格式(更多详情参见a.out(5))。这种格式包含3个要装载入内存的段：`.text`，`.data`，和`.bss`，以及一个符号表和一个字符串表。

- COFF

SVR3目标文件格式。其文件头现在包括一个区段表(section table)，因此除了.text，.data，和.bss区段以外，您还可以包含其它的区段。

- elf(5)

COFF 的后继，其特点是可以有多个区段，并可以使用32位或64位的值。它有一个主要的缺点：ELF 在其设计时假设每个系统体系结构只有一种ABI。这种假设事实上相当错误，甚至在商业化的SYSV世界中都是错误的(它们至少有三种ABI: SVR4, Solaris, SCO)。

FreeBSD试图在某种程度上解决这个问题，它提供一个工具，可以对一个已知的ELF可执行文件标识它所遵从的ABI的信息。更多这方面的知识可以参见手册页brandelf(1)

FreeBSD从“经典”阵营中来，因此使用了a.out(5)格式，众多BSD版本的发行(直到3.X分支的开始)也证明了这种格式的有效性。虽然在那以前的某段时间，在FreeBSD系统上创建和运行ELF格式的二进制可执行文件(和内核)也是可能的，但FreeBSD一开始并不积极“进步”到使用ELF作为其缺省的格式。为什么？噢，当Linux阵营完成了转换到ELF格式的痛苦历程后，却发现并不足以由此而放弃a.out可执行文件格式，因为正是由于它们不灵活的，基于跳转表的共享库机制，使得销售商和开发者们构建共享库非常困难。直到已有的ELF工具提供了一种解决共享库问题的办法，并被普遍认为是“前进方向”以后，迁徙的代价在FreeBSD界才被接受，并由此完成了迁徙。FreeBSD的共享库机制其基础更类似于Sun SunOS™的共享库机制，并且正因为此，其易用性很好。

那么，为什么会有这么多不同的格式呢？

回溯到蒙昧和黑暗过去，那时只有简单的硬件。这种简单的硬件支撑了一个简单和小型的系统。在这样的简单系统上(PDP-11)a.out格式足以胜任表达二进制文件的任务。当人们将UNIX从这种简单的系统中移植出来的时候，a.out格式被保留了下来，因为对于早期将UNIX移植到Motorola 68k，VAXen等系统来说，它还是足够可用的。

然后，一些聪明的硬件工程师认为，如果可以让软件完成一些简单的聪明操作，那么他们就可以在硬件设计中减少若干门电路，并可以让CPU核心运行得更快。当a.out格式用于这种新型的硬件系统时(现在我们叫它RISC)，显得并不合适。因此，人们设计了许多新的格式以便在这样的硬件系统上能获得比简单的a.out格式更优越的性能。诸如COFF，ECOFF，还有其它一些晦涩难懂的格式正是在这个阶段被发明出来的，人们也研究了这些格式的局限性，慢慢地最终落实到ELF格式。

同时，程序的大小变得越来越大，磁盘空间(以及物理内存)相对来说却仍然较小，因此共享库的概念便产生了。VM系统也变得越来越复杂了。当所有这些进步都建立在a.out格式的基础上的时候，它的可用性随着每个新特性的产生就受到了严重考验。并且，人们还希望可以在运行时动态装载某些东西，或者在初始化代码运行以后可以丢弃部分程序代码，以便节约主存储器和交换区。编程语言也变得越来越复杂，人们希望可以在main()函数执行之前自动执行某些代码。为了实现所有这些功能，人们对a.out格式作了很多改动(hack)，他们在某个阶段里基本也是可行的。随着时间的推移，a.out格式不得不增加大量的代码和复杂度来满足这些需求。虽然ELF格式解决了许多这样的问题，但是从一个可用的系统迁移到另一个系统却是痛苦的。因此直到继续保留a.out格式的代价比迁移到ELF格式的代价还大的时候，人们才会最终转换到ELF格式。

然而，随着时间的推移，FreeBSD系统本身的编译工具(特别是汇编器和装载器)赖以派生的编译工具，其发展却形成了两个平行的分支。FreeBSD这个分支增加了共享库，并修改了一些错误。而原先编写了这些工具的GNU人则重写了这些工具，并对交叉编译提供了更简化的支持，还随意插入了不同格式的支持，等等。虽然很多人希望创建针对FreeBSD的交叉编译器，但他们却并未如愿以偿，因为FreeBSD的as和ld的源代码更为老旧，所以无法完成这个任务。新的GNU工具链(binutils)则确实支持交叉编译，ELF格式，共享库，C++扩展，等等。并且，由于很多供应商都发布ELF格式的二进制文件，因而让FreeBSD能够运行它们将是一个很好的事情。

ELF格式比a.out格式开销要大些，同时也允许基础系统有更好的扩展性。ELF格式的有关工具有着更好的维护，并且提供交叉编译支持，这对许多人来说是很重要的。ELF格式可能会稍微慢一些，但很难测量出来。另外，在这两者之间，有许多细节也是不同的，比如它们映射页面的方式，处理初始化代码的方式，等等。所有这些都不太重要，但这也确实是不同之处。在将来的适当时候，GENERIC内核将不再支持a.out格式，并且，当不再需要运行遗留的a.out格式程序时，内核也将不再提供对其的支持。

3.13 取得更多的资讯

3.13.1 联机手册

最详细的使用说明文档莫过于FreeBSD里的联机手册了。几乎每一个程序都会附上一份简短说明，以介绍这个程序的的基本功能以及参数的用法。我们能通过man命令来阅读这些说明，而使用man命令却是简单的事情：

```
% man command
```

command就是您要了解的命令名称。举个例子，想了解ls命令就输入：

```
% man ls
```

这些在线手册分下列章节：

1. 用户命令。
2. 系统调用以及错误代码。
3. C库文件里的函数说明。
4. 设备驱动程序。
5. 文件格式。
6. 游戏以及其他娱乐。
7. 各种资讯。
8. 系统维护以及命令。
9. 内核开发情况。

在某些情况下，同样的主题也会出现在在线手册的不同章节。举个例子，系统里有chmod这个用户命令，而又有个chmod()系统调用。在这种情形下，您应当向man命令指定需要的内容：

```
% man 1 chmod
```

这样就会显示出手册里的用户chmod命令。传统上，我们在写入文档时把特定详细参考内容在在线手册括号里注明。所以chmod(1)是指chmod用户命令，而chmod(2)是指系统调用。

如果您已经知道命令的名字，只是不知道要怎样使用的话，那就比较好办。但您连名字都不知到呢？这个时候您就可以利用man的搜寻功能，它会在手册的介绍部份找寻您要搜寻的关键字，它的选项是-k：

```
% man -k mail
```

当您使用这个命令的时候，`man`会把介绍里含有“mail”关键字的命令列出来，实际上这和`apropos`命令的功能是相同的。

有时您会看到`/usr/bin`下有许多命令但不知他们的用途，您只需这样做：

```
% cd /usr/bin
% man -f *
```

或者这样做

```
% cd /usr/bin
% whatis *
```

两个命令是一样的。

3.13.2 GNU Info 文件

FreeBSD许多应用软件以及实用工具来自Free软件基金会(FSF)。作为手册的扩充，这些程序提供了一种更具有活力的超文档说明`info`，您可用`info`命令来阅读他们。假如您装上`emacs`，也能利用`emacs`的`info`模式来阅读。

使用`info(1)` 这个命令只需简单地输入：

```
% info
```

想得到简单介绍，请按`h`。想快速得到的命令说明，请按`?`。

备注

1. 现在理解一下`i386`的含义。请注意即使您的FreeBSD不是运行在一个Intel 386 CPU，都会定为`i386`。他不是指您的处理器，而处理器的“体系结构”已经显示过去了。
2. 启动脚本这些程序在FreeBSD在启动过程中运行。它们的主要功能为其他每方面的运行作好准备，和运行您的配置所用到的相关环境。
3. 关于FreeBSD的控制台和键盘设备这些详细资料或使用技巧可在手册里找到：`syscons(4)`、`atkbd(4)`、`vidcontrol(1)`和`kbdcontrol(1)`。我们不在这里详细介绍，但是爱好者总会在手册里找到详细的答案。
4. 有点不正确——少数的东西是不能中断的。例如，假如进程试图读取网络上另一计算机上的文件，而那个的计算机会因为某些原因拿走了这个文件，那这个进程从上述情况来看是“不能中断”。最终这个进程会超时，典型的两分钟。一出现超时进程将被杀死。

第4章

安装应用程序: *Packages* 和*Ports*

4.1 概述

FreeBSD 将许多系统工具捆绑作为基本系统的一部分。然而，要完成实际的工作，可能还需要安装更多的第三方应用。FreeBSD 提供了两种补充的技术，用以在您的系统中安装第三方软件：FreeBSD Ports 套件(用于从源代码安装)，以及packages (用以从预编译的二进制版本安装)。这两种方法都可以用于从本地介质，或从网上直接安装您喜欢的应用程序的最新版本。

读完本章，您将了解到：

- 如何安装第三方的二进制软件包。
- 如何使用ports 套件从源代码构建第三方软件。
- 如何删除先前安装的软件包。
- 如何改动Ports Collection里面的一些参数，定制软件使用。
- 如何找到您需要的软件包。
- 如何升级您的应用软件。

4.2 软件安装预览

如果您以前使用过UNIX 系统，那典型的第三方软件安装的步骤是像下面描述的：

1. 下载这个软件，软件的发行版可能是源代码格式，或是一个二进制包。
2. 解开软件(其中代表性的是用compress(1), gzip(1), 或bzip2(1) 压缩过的tar包)。
3. 阅读相关文档，了解如何安装。(多半一个文件名是INSTALL或README，或在doc/ 目录下的一些文档)
4. 如果软件是以源代码形式发布的，那就需要编译它。可能需要编辑一个Makefile文件, 或运行configure脚本，和其他的一些工作。
5. 测试和安装软件。

如果一切顺利的话，就这么简单。如果您在安装一个软件包时发生一些错误，您可能需要编辑一下它的代码，以使它能正常工作。

您可以继续使用“传统的”方式安装软件。然而，FreeBSD 提供了两种技术：packages 和ports。就在写这篇文章的时候，已经有超过13,300 个第三方的应用程序可以使用了。

对于任意一个应用程序包，是一个可以下载的FreeBSD package文件。这个FreeBSD package包含了编译好的副本，还有一些配置文件或文档。一个下载的包文件可以用FreeBSD 的包管理命令来操作，例如pkg_add(1), pkg_delete(1), pkg_info(1) 等等。可以使用一个简单的命令安装一个新的应用程序。

一个FreeBSD的port是一个可以自动从源代码编译成应用程序的文件集合。

记住,如果您自己来编译的话,需要执行很多步的操作(解压,补丁,编译,安装)。这些整理port的文件集合包含了系统需要完成这个工作的必需信息。您可以运行一些简单的命令,那些源代码就可以自动地下载,解开,打补丁,编译,直至安装完成。

实际上,ports系统也能做出被pkg_add的程序包和不久就要讲到的其他包管理命令来安装的软件包。

Packages和ports是互相依赖的。假设您想安装一个依赖于已经安装的特定库的应用程序。应用程序和那个库都已经应用于FreeBSD ports和packages。如果您使用命令或ports系统来添加应用程序,两个都必须注意库是否被安装,如果没有,它会自动先安装库。

这里给出的两种技术是很相似的,您可能会奇怪为什么FreeBSD会弄出这两种技术。其实,packages和ports都有它们自己的长处,使用哪一种完全取决于您自己的喜好。

Package的优点

- 一个压缩的package通常要比一个压缩的包含源代码的应用程序小得多。
- package不需要进行额外的编译。对于大型应用程序如Mozilla, KDE或GNOME来说这显得尤为重要,特别是在您的系统资源比较差的情况下。
- package不需要您知道如何在FreeBSD上编译软件的详细过程。

Ports 的优点

- package在编译时通常使用比较保守的选项,这是为了保证它们能够运行在大多数的系统上。通过从port安装,您可以细微调整编译选项来产生适合于处理器的代码(针对于Pentium IV或AMD的Athlon CPU)。
- 一些软件包已经把与它们相关的能做和不能做的事情的选项都编译进去了。例如,Apache可能就配置了很多的选项。从port中安装时,您不一定要接受默认的选项,可以自己来设置。

在一些例子中,一个软件有不同的配置存在多个package。例如,Ghostscript存在ghostscript package和ghostscript-nox11 package两个配置package,这取决于您是否安装了X11服务器。这样的调整对package是可能的,但如果一个应用程序有超过一个或两个不同的编译时间选项时,就不行了。

- 一些软件的许可条件禁止采用二进制形式发行。它们必须带上源代码。
- 一些人不信任二进制发行形式。至少有了源代码,(理论上)可以亲自阅读它,寻找潜在的问题。
- 如果您要自己对软件打补丁,您就需要有源代码。
- 一些人喜欢整天围着源代码转,所以他们喜欢亲自阅读源代码,修改源代码等等。

保持更新ports,订阅邮件列表FreeBSD ports 邮件列表(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ports>)和递交错误报告FreeBSD ports bugs 邮件列表(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ports-bugs>)。

警告: 安装任何应用程序之前,应首先检查<http://vuxml.freebsd.org/>上是否有关于您所安装的应用程序的安全问题报告。

您也可以安装security/portaudit,它能够自动地检查已经安装的应用程序的漏洞;此外,在您安装程序之前它也会首先检查是否存在已知的漏洞。另外,您也可以使用portaudit -F -a这个命令在安装某个软件包之后作出检查。

这章的其余部分将介绍如何使用packages和ports来安装和管理第三方软件。

4.3 寻找您要的应用程序

在您安装任何应用程序之前，需要知道您需要什么，那个应用程序叫什么。

FreeBSD中可用的应用程序正在不断地增长着。幸运的是，有许多方法可以找到您所需要的程序：

- FreeBSD站点上有一个可以搜索到的当前所有可用的应用程序列表，在<http://www.FreeBSD.org/ports/> (<http://www.FreeBSD.org/ports/index.html>)。它分很多种类，您既可以通过程序的名称来搜索，也可以在分类中列出所有可用的应用程序(如果您知道名字)，也可以在分类中列出所有可用的应用程序。
- Dan Langille 维护着网站FreshPorts，在<http://www.FreshPorts.org/>。FreshPort时刻“追踪”着在ports中应用程序的变化。当有任何程序被升级时，他们就会发email提醒您。
- 如果您不知道您想要的应用程序的名字，可以通过(<http://www.freshmeat.net/>) 网站来查找，如果找到了应用程序，您可以回FreeBSD的主站去看一下这个应用程序是否已经被port进去了。
- 如果您知道一个port的准确名字，但需要知道在哪个类别里面能找到它，您可以使用whereis(1) 这个命令。简单地输入whereis file, file 就是您想安装的程序名字。如果系统找到了它，您将被告知它在它在哪里，例如：

```
# whereis lsof
lsof: /usr/ports/sysutils/lsof
```

结果告诉我们这个命令lsof (一个系统配置程序)可以在/usr/ports/sysutils/lsof目录中找到。

- 还有另外的一个寻找您需要的port的方法--是用ports collecton 内嵌的搜索机制。要使用这个搜索, 您需要先到/usr/ports目录下面。在那个目录里面，运行make search name=program-name, program-name 就是您想寻找的程序名字。举个例子，如果您想找lsof：

```
# cd /usr/ports
# make search name=lsof
Port:    lsof-4.56.4
Path:    /usr/ports/sysutils/lsof
Info:    Lists information about open files (similar to fstat(1))
Maint:   obrien@FreeBSD.org
Index:   sysutils
B-deps:
R-deps:
```

在输出的内容里面您要特别注意包含“Path:”的这行将告诉您在哪里可以找到这个port。如果要安装此port，那其他输出的信息不是必须的，但是还是显示输出了。

为了更深入的搜索，您还可以用make search key=string, string就是您想搜索的部分内容。它将搜索port的名字、注释，描述和从属关系，如果您不知道您想搜索的程序名字，可以利用它搜索一些关键主题来找到您需要的。

上面说的这些方法，搜索的关键字没有大小写区分的。搜索“LSOF”的结果将和搜索“lsof”的结果一样。

4.4 使用Packages系统

Contributed by Chern Lee.

4.4.1 一个package的安装

您可以用`pkg_add(1)`这个命令从本地文件或网络上的服务器来安装一个FreeBSD 软件包。

例4-1. 在本地手动下载一个package,并安装它

```
# ftp -a ftp2.FreeBSD.org
Connected to ftp2.FreeBSD.org.
220 ftp2.FreeBSD.org FTP server (Version 6.00LS) ready.
331 Guest login ok, send your email address as password.
230-
230-      This machine is in Vienna, VA, USA, hosted by Verio.
230-      Questions? E-mail freebsd@vienna.verio.net.
230-
230-
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /pub/FreeBSD/ports/packages/sysutils/
250 CWD command successful.
ftp> get lsof-4.56.4.tgz
local: lsof-4.56.4.tgz remote: lsof-4.56.4.tgz
200 PORT command successful.
150 Opening BINARY mode data connection for 'lsof-4.56.4.tgz' (92375 bytes).
100% |*****| 92375      00:00 ETA
226 Transfer complete.
92375 bytes received in 5.60 seconds (16.11 KB/s)
ftp> exit
# pkg_add lsof-4.56.4.tgz
```

如果您没有本地package的安装盘(如FreeBSD CD-ROM), 可以执行`pkg_add(1)`命令并加上`-r`选项。这将迫使程序自动决定目标文件的正确格式和版本, 然后自动从一个FTP 站点寻找和安装package。

```
# pkg_add -r lsof
```

上面的例子将下载正确的package, 而不需要用户的干预就可以安装。如果您想指定FreeBSD package 的镜像站点, 替换主站点, 您必须新设置`PACKAGESITE`这个环境变量, 覆盖原来的设置。`pkg_add(1)`使用`fetch(3)`下载文件, 可以使用多种环境变量, 包含`FTP_PASSIVE_MODE`、`FTP_PROXY`, 和`FTP_PASSWORD`。如果您使用FTP/HTTP 代理或在防火墙后面, 您可能需要设置这些环境变量。详细的列表请参考`fetch(3)`。上述例子中用`lsof`替代了`lsof-4.56.4`。当使用远程安装Package 的时候软件名字不需要包含版本号。`pkg_add(1)`将自动的找到这个软件最新的版本。

注意: 如果您使用FreeBSD-CURRENT 或FreeBSD-STABLE版本的FreeBSD, `pkg_add(1)`将下载您的应用软件的最新版本。如果您使用-RELEASE 版本的FreeBSD, 它将会获得与您的版本相应的软件包版本。您可以通过修改环境变量`PACKAGESITE`来改变这一行为。例如, 如果您运行FreeBSD 5.4-RELEASE 系统, 默认情况下`pkg_add(1)`将尝试从`ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-5.4-release/Latest/` 下载预编译的

软件包。如果您希望强制`pkg_add(1)`下载FreeBSD 5-STABLE 的软件包，则可以将`PACKAGESITE` 设置为`ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-5-stable/Latest/`。

软件包采用`.tgz` 和`.tbz` 两种格式。您可以在`ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/packages/` 下面或从FreeBSD 的发行光盘找到，它在每一个4CD 的FreeBSD 发行版的`/packages`目录中。软件包的设计规划与`/usr/ports` 树一致。每个分类都有自己的目录，所有的软件包可以在目录`All`中找到。

软件包系统的目录结构与`ports`的设计规划一致；它们共同构成了整个`package/port`。

4.4.2 软件包的管理

`pkg_info(1)` 是用于列出已安装的所有软件包列表和描述的程序。

```
# pkg_info
cvsup-16.1          A general network file distribution system optimized for CV
docbook-1.2        Meta-port for the different versions of the DocBook DTD
...
```

`pkg_version(1)`是一个用来统计所有安装的软件包版本的工具。它可以用来比较本地`package` 的版本与`ports` 目录中的当前版本是否一致。

```
# pkg_version
cvsup                =
docbook              =
...
```

在第二列的符号指出了安装版本的相关时间和本地`ports`目录树中可用的版本。

符号	含义
=	在本地 <code>ports</code> 树中与已安装的软件包版本相匹配。
<	已安装的版本要比在 <code>ports</code> 树中的版本旧。
>	已安装的版本要比在 <code>ports</code> 树中的版本新(本地的 <code>port</code> 树可能没有更新)。
?	已安装的软件包无法在 <code>ports</code> 索引中找到。(可能发生这种事情，举个例子，您早先安装的一个 <code>port</code> 从 <code>port</code> 树中移出或改名了)
*	软件包有很多版本。

4.4.3 删除一个软件包

要删除先前安装的软件`package`，只要使用`pkg_delete(1)` 工具。

```
# pkg_delete xchat-1.7.1
```

4.4.4 其它

所有已安装的package 信息都保存在 `/var/db/pkg` 目录下。安装文件的列表和每个package 的内容和描述都能在这个目录的相关文件中找到。

4.5 使用 Ports Collection

下面的几个小节中，给出了关于如何使用 Ports 套件来在您的系统中安装或卸载程序的介绍。关于可用的make targets 以及环境变量的介绍，可以在ports(7) 中找到。

4.5.1 获得 Ports Collection

在您能使用ports 之前，您必须先获得Ports Collection ——本质上是 `/usr/ports` 目录下的一堆Makefile、补丁和描述文件。

在您安装FreeBSD 系统的时候，`sysinstall` 会询问您是否需要安装Ports Collection。如果您选择no，那您可以用下面的指令来安装Ports Collection：

CVSup 方法

保持您本地Ports 套件最新的一种快捷的方法，是使用CVSup 来进行更新。如果您希望了解更多关于CVSup 的细节，请参见使用CVSup。

1. 安装net/cvsup-without-gui 软件包：

```
# pkg_add -r cvsup-without-gui
```

请参见如何安装CVSup (第A.5.2 节) 以了解更多细节。

2. 运行cvsup:

```
# cvsup -L 2 -h cvsup.FreeBSD.org /usr/share/examples/cvsup/ports-supfile
```

将 `cvsup.FreeBSD.org` 改为离您较近的CVSup 服务器。请参见CVSup 镜像 (第A.5.7 节) 中的镜像站点完整列表。

注意：有时可能希望使用自己的ports-supfile，比如说，不想每次都通过命令行来指定所使用的CVSup 服务器。

1. 这种情况下，需要以root 身份将 `/usr/share/examples/cvsup/ports-supfile` 复制到新的位置，例如 `/root` 或您的主目录。
2. 编辑ports-supfile。
3. 把 `CHANGE_THIS.FreeBSD.org` 修改成离您较近的CVSup 服务器。可以参考CVSup 镜像 (第A.5.7 节) 中的镜像站点完整列表。
4. 接下来按如下的方式运行cvsup:

```
# cvsup -L 2 /root/ports-supfile
```

3. 此后运行cvsup(1) 命令将下载最近所进行的改动，并将它们应用到您的Ports Collection 上，不过这一过程并不重新联编您系统上的ports。

Portsnap 方式

portsnap(8) 是另一种用于发布 Ports 套件的方法。它最早从 FreeBSD 6.0 开始引入。在较早的系统中, 您可以通过 sysutils/portsnap port 来安装它:

```
# pkg_add -r portsnap
```

请参见使用 Portsnap 以了解关于全部 Portsnap 功能的详细描述。

1. 如果没有的话, 建立一个空的 /usr/ports 目录。

```
# mkdir /usr/ports
```

2. 下载压缩的 Ports 套件快照到 /var/db/portsnap。您可以根据需要在这之后关闭 Internet 连接。

```
# portsnap fetch
```

3. 假如您是首次运行 Portsnap, 则需要将快照释放到 /usr/ports:

```
# portsnap extract
```

如果您已经有装好的 /usr/ports 而您只想更新, 则应执行下面的命令:

```
# portsnap update
```

Sysinstall 方式

这种方法需要使用 sysinstall 从安装介质上安装 Ports 套件。注意, 安装的将是发布发行版时的旧版 Ports 套件。如果您能访问 Internet, 应使用前面介绍的方法之一。

1. 以 root 身份运行 sysinstall (对 FreeBSD 5.2 之前的版本, 应执行 /stand/sysinstall):

```
# sysinstall
```

2. 用光标向下选择 Configure, 并按 Enter。
3. 向下并选择 Distributions, 按 Enter。
4. 选择 ports, 并按 Space。
5. 选择 Exit, 并按 Enter。
6. 选择所希望的安装介质, 例如 CDROM、FTP, 等等。
7. 选择 Exit 并按 Enter。
8. 按 X 退出 sysinstall。

4.5.2 安装 Ports

当提到 Ports Collection 时, 第一个要说明的就是何谓 “skeleton”。简单地说, port skeleton 是让一个程序在 FreeBSD 上简洁地编译并安装的所需文件的最小组合。每个 port skeleton 包含:

- 一个 Makefile。Makefile 包括好几个部分, 指出应用程序是如何编译以及将被安装在系统的哪些地方。
- 一个 distinfo 文件。这个文件包括这些信息: 这些文件用来对下载后的文件校验和进行检查, 使用 md5(1) 来确保在下载过程中文件没有被破坏。

- 一个 **files** 目录。这个目录包括在 FreeBSD 系统上编译和安装程序需要用到的补丁。这些补丁基本上都是一些小文件，指出特定文件作了哪些修正。它们都是纯文本的格式，基本上是这样的“删除第10行”或“将第26行改为这样...”，补丁文件也被称作“diffs”，他们由 `diff(1)` 程序生成。

这个目录也包含了在编译 port 时要用到的其它文件。

- 一个 **pkg-descr** 文件。这是一个提供更多细节，有软件的多行描述。
- 一个 **pkg-plist** 文件。这是即将被安装的所有文件的列表。它告诉 ports 系统在卸载时需要删除哪些文件。

一些 ports 还有些其它的文件，例如 **pkg-message**。ports 系统在一些特殊情况下会用到这些文件。如果您想知道这些文件更多的细节以及 ports 的概要，请参阅 *FreeBSD Porter's Handbook* (http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/porters-handbook/index.html)。

port 里面包含着如何编译源代码的指令，但不包含真正的源代码。您可以在网上或 CD-ROM 上获得源代码。源代码可能被开发者发布成任何格式。一般来说应该是一个被 `tar` 和 `gzip` 过的文件，或者是被一些其他的工具压缩或未压缩的文件。ports 中这个程序源代码标示文件叫“distfile”，安装 FreeBSD port 的方法还不止这两种。

注意：您必须使用 `root` 用户登录后安装 ports。

警告：在安装任何 port 之前，应该首先确保已经更新到了最新的 Ports Collection，并检查 <http://vuxml.freebsd.org/> 中是否有与那个 port 有关的安全问题。

在安装应用程序之前，可以使用 **portaudit** 来自动地检查是否存在已知的安全问题。这个工具同样可以在 Ports Collection (`security/portaudit`) 中找到。在安装新的 port 之前，可以考虑先运行一下 `portaudit -F` 来抓取最新的漏洞数据库。在每天的周期性系统安全检察时，数据库会被自动更新，并且会在这之后实施安全审计。欲了解进一步的情况，请参阅 `portaudit(1)` 和 `periodic(8)`。

Ports 套件假定您有可用的 Internet 连接。如果您没有，则需要将 distfile 手工放到 `/usr/ports/distfiles` 中。

要开始操作，首先进入要安装 port 的目录：

```
# cd /usr/ports/sysutils/lsof
```

一旦进入了 `lsof` 的目录，您将会看到这个 port 的结构。下一步就是 `make`，或说“联编”这个 port。只需在命令行简单地输入 `make` 命令就可轻松完成这一工作。做好之后，您可以看到下面的信息：

```
# make
>> lsof_4.57D.freebsd.tar.gz doesn't seem to exist in /usr/ports/distfiles/.
>> Attempting to fetch from ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/.
==> Extracting for lsof-4.57
...
[extraction output snipped]
...
>> Checksum OK for lsof_4.57D.freebsd.tar.gz.
==> Patching for lsof-4.57
==> Applying FreeBSD patches for lsof-4.57
==> Configuring for lsof-4.57
...
```



```
[configure output snipped]
...
==> Building for lsof-4.57
...
[compilation output snipped]
...
#
```

注意，一旦编译完成，您就会回到命令行。下一步安装port，要安装它只需要在make 命令后跟上一个单词install即可：

```
# make install
==> Installing for lsof-4.57
...
[installation output snipped]
...
==> Generating temporary packing list
==> Compressing manual pages for lsof-4.57
==> Registering installation for lsof-4.57
==> SECURITY NOTE:
      This port has installed the following binaries which execute with
      increased privileges.
#
```

一旦您返回到提示符，您就可以运行您刚刚安装的程序了。因为lsof 是一个赋予特殊权限的程序，因此显示了一个安全警告。在编译和安装ports 的时候，您应该留意任何出现的警告。

删除工作目录是个好主意，这个目录中包含了全部在编译过程中用到的临时文件。这些文件不仅会占用宝贵的磁盘空间，而且可能会给升级新版本的port 时带来麻烦。

```
# make clean
==> Cleaning for lsof-4.57
#
```

注意：使用make install clean 可以代替make、make install 和make clean 这三个分开的步骤。

注意：一些shell 会缓存环境变量PATH 中指定的目录里的可执行文件，以加速查找它们的速度。如果您使用的是这类shell，在安装port 之后可能需要执行rehash 命令，然后才能运行新安装的那些命令。这个命令可以在类似tcsh 的shell 中使用。对于类似sh 的shell，对应的命令是hash -r。请参见您的shell 的文档以了解进一步的情况。

某些第三方DVD-ROM 产品，如FreeBSD Mall (<http://www.freebsdmail.com/>) 的FreeBSD Toolkit 中包含了distfiles。这些文件可以与Ports 套件配合使用。将DVD-ROM 挂接到/cdrom。如果您使用不同的挂接点，则应设置make 变量CD_MOUNTPTS。如果盘上有需要的distfiles，则会自动使用。

注意：请注意，少数ports 并不允许通过CD-ROM 发行。这可能是由于下载之前需要填写注册表格，或者不允许再次发布，或者有一些其它原因。如果您希望安装在CD-ROM 上没有的port，就需要在线操作了。

ports 系统使用`fetch(1)`去下载文件，它有很多可以设置的环境变量，其中包括`FTP_PASSIVE_MODE`、`FTP_PROXY`，和`FTP_PASSWORD`。如果您在防火墙之后，或使用FTP/HTTP代理，您可能需要设置它们。完整的说明请看`fetch(3)`。

当使用者不是所有时间都能连接上网络，则可以利用`make fetch`。您只要在顶层目录(`/usr/ports`)下运行这个命令，所有需要的文件都将被下载。这个命令也同样可以在下级类别目录中使用，例如：`/usr/ports/net`。注意，如果一个port有一些依赖的库或其他port，它将不下载这些依赖的port的distfile文件，如果您想获取所有依赖的port的所有distfile，请用`fetch-recursive`命令代替`fetch`命令。

注意：您可以在一个类别或在顶级目录编译所有的port，或者使用上述提到的`make fetch`命令。这样是非常危险的，因为有一些port不能并存。或者有另一种可能，一些port会安装两个不同的文件，但是却是相同的文件名。

在一些罕见的例子中，用户可能需要在除了`MASTER_SITES`以外的一个站点(本地已经下载下来的文件)去获得一个文件包。您可以用以下命令不使用`MASTER_SITES`：

```
# cd /usr/ports/directory
# make MASTER_SITE_OVERRIDE= \
ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/ fetch
```

在这个例子中，我们把`MASTER_SITES`这个选项改为了`ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/`。

注意：一些port允许(或甚至要求)您指定编译选项来启用/禁用应用程序中非必需的功能，一些安全选项，以及其他可以定制的内容。具有代表性的包括`www/mozilla`、`security/gpgme`、以及`mail/sylpheed-claws`。如果存在这样的选项，通常会在编译时给出提示。

4.5.2.1 改变默认的Ports 目录

有时，使用不同的工作临时目录和目标目录可能很有用(甚至是必要的)。可以用`WRKDIRPREFIX`和`PREFIX`这两个变量来改变默认的目录。例如：

```
# make WRKDIRPREFIX=/usr/home/example/ports install
```

将把编译`/usr/home/example/ports`中的port并把所有的文件安装到`/usr/local`。

```
# make PREFIX=/usr/home/example/local install
```

将在`/usr/ports`编译它并安装到`/usr/home/example/local`。

当然，

```
# make WRKDIRPREFIX=./ports PREFIX=./local install
```

将包含两种设置(没有办法在这一页把它写完，但您应该已经知道怎么回事了)。

另外，这些变量也可以作为环境变量来设置。请参考您的shell的联机手册上关于如何设置环境变量的说明。

4.5.2.2 处理 imake

一些 port 使用 imake (这是 X Window 系统的一部分) 不能正常地配合 PREFIX, 它们会坚持把文件安装到 /usr/X11R6 下面。类似地, 一些 Perl port 会忽略 PREFIX 并把文件安装到 Perl 的目录中。让这些 port 尊重 PREFIX 是困难甚至是不可能的事情。

4.5.3 卸载已经安装的 Ports

现在您已经了解了如何安装 ports, 并希望进一步了解如何卸载, 特别是在安装了某个之后发现不合适的 port 时。我们将卸载前面例子(假如您没有注意的话, 是 lsof) 中安装的 port。Ports 可以同 packages 以完全相同的方式(在 Packages 一节 中进行了介绍) 卸载, 方法是使用 pkg_delete(1) 命令:

```
# pkg_delete lsof-4.57
```

4.5.4 升级 Ports

首先, 使用 pkg_version(1) 命令来列出 Ports Collection 中提供了更新版本的那些 port:

```
# pkg_version -v
```

注意: 一旦您更新了 Ports Collection, 在开始升级之前, 应该首先检查一下 /usr/ports/UPDATING 文件。它描述了在升级时可能遇到的问题, 以及因应的步骤。

4.5.4.1 使用 Portupgrade 来更新 Ports

portupgrade 工具是设计来简化升级已安装的 port 的操作的。它通过 sysutils/portupgrade port 来提供。您可以像其它 port 那样, 使用 make install clean 命令来安装它:

```
# cd /usr/ports/sysutils/portupgrade
# make install clean
```

使用 pkgdb -F 命令来扫描已安装的 port 的列表, 并修正其所报告的不一致。在每次升级之前, 有规律地执行它是个好主意。

运行 portupgrade -a 时, **portupgrade** 将开始并升级系统中所安装的所有过时的 ports。如果您希望在每个升级操作时得到确认, 应指定 -i 参数。

```
# portupgrade -ai
```

如果您只希望升级某个特定的应用程序, 而非全部可用的 port, 应使用 portupgrade pkgname。如果 **portupgrade** 应首先升级指定应用程序的话, 则应指定 -R 参数。

```
# portupgrade -R firefox
```

要使用预编译的 package 而不是 ports 来进行安装, 需要指定 -P。如果指定了这个选项, **portupgrade** 会搜索 PKG_PATH 中指定的本地目录, 如果没有找到, 则从远程站点下载。如果本地没有找到, 而且远程站点也没有成功地下载预编译包, 则 **portupgrade** 将使用 ports。要禁止使用 port, 可以指定 -PP。

```
# portupgrade -PR gnome2
```

如果只想下载distfiles (或者, 如果指定了 -P 的话, 是packages) 而不想构建或安装任何东西, 可以使用 -F。要了解更多细节, 请参考portupgrade(1)。

4.5.4.2 使用Portmanager 来升级Ports

Portmanager 是另一个用以简化已安装port 升级操作的工具。它可以通过sysutils/portmanager port 安装:

```
# cd /usr/ports/sysutils/portmanager
# make install clean
```

可以通过这个简单的命令来升级所有已安装的port:

```
# portmanager -u
```

如果希望**Portmanager** 在进行每步操作之前都给出提示, 应使用 -ui 参数。**Portmanager** 也可以用来在系统中安装新的ports。与通常的make install clean 命令不同, 它会在联编和安装您所选择的port 之前升级所有依赖包。

```
# portmanager x11/gnome2
```

如果关于所选port 的依赖有任何问题, 可以用**Portmanager** 来以正确的顺序重新构建它们。完成之后, 有问题的port 也将被重新构建。

```
# portmanager graphics/gimp -f
```

要了解更多信息, 请参见**Portmanager** 联机手册。

4.5.5 Ports 和磁盘空间

使用Ports 套件会最终用完磁盘空间。在通过ports 联编和安装软件之后, 您应记得清理临时的work 目录, 其方法是使用make clean 命令。您可以使用下面的命令来清理整个Ports 套件:

```
# portsclean -C
```

随着时间的推移, 您可能会在distfiles 目录中积累下大量源代码文件。您可以手工删除这些文件, 也可以使用下面的命令来删除所有port 都不引用的文件:

```
# portsclean -D
```

注意: 这个portsclean 工具是portupgrade 套件的一部分。

不要忘记删除那些已经安装, 但已不再使用的ports。用于自动完成这种工作的一个好工具是sysutils/pkg_cutleaves port。

4.6 安装之后的待办事宜

通常, 您通过port安装完一个软件后, 可以阅读它带的一些文档(如果它包含文档的话), 或需要编辑它的配置文件, 来确保这个软件的运行, 或在机器启动的时候启动(如果它是一个服务的话), 等等。

对于不同的软件有着不同的配置步骤。不管怎样, 如果您装好了一个软件, 但是不知道下一步怎么办的时候, 这些小技巧可能可以帮助您:

- 使用`pkg_info(1)`命令, 它能找到安装了哪些文件, 以及装在哪里。举个例子, 如果您安装了FooPackage version 1.0.0, 那么这个命令

```
# pkg_info -L foopackage-1.0.0 | less
```

将显示这个软件包安装的所有文件, 您要特别注意在`man/`目录里面的文件, 它们可能是手册, `etc/`目录里面的配置文件, 以及`doc/`目录下面更多的文档。

如果您不确定已经安装好的软件版本, 您可以使用这样的命令

```
# pkg_info | grep -i foopackage
```

它将会找到所有已安装的软件包名字中包含`foopackage`的软件包。对于其他的查找, 您只需要在命令行中替换`foopackage`。

- 一旦一些软件手册已被您确认安装, 您可以使用`man(1)`查看它。同样的, 如果有的话, 您还可以完整的查看一边配置文件的示例, 以及任何额外的文档。
- 如果应用软件有网站, 您还可以从网站上找到文档, 常见问题的解答, 或其他更多。如果您不知道它们的网站地址, 请使用下面的命令

```
# pkg_info foopackage-1.0.0
```

一个`www:`行, 如果它存在, 它将提供一个这个应用程序的网站URL。

- Ports 如果需要在服务器启动时运行(就像互联网服务器), 它通常会把一个脚本的样例放入`/usr/local/etc/rc.d`目录。为了保证正确性, 您可以查看这个脚本, 并编辑或更改这个脚本的名字。详情请看启动服务。

4.7 如何处理坏掉的Ports

如果您发现某个port无法正常工作, 有几件事值得尝试, 包括:

1. 在问题报告数据库 (<http://www.FreeBSD.org/support.html#gnats>) 中查找是否有尚未提交的修正。如果有, 可以使用所提议的修正。
2. 要求port的监护人(maintainer)提供帮助。输入`make maintainer`或阅读Makefile 查找监护人的电子邮件地址。请记得把port的名字和版本写在邮件里(Makefile 中的`$FreeBSD:`这一行) 并把错误输出的头几行发给maintainer。

注意: 某些ports 并没由个人维护, 而是写了一个邮件列表

(http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/mailling-list-faq/article.html)。许多, 但并非所有port, 使用类似`<freebsd-listname@FreeBSD.org>` 这样的地址。请在提出问题时考虑这一点。

特别地, 由`<freebsd-ports@FreeBSD.org>` 监护的port, 实际上并没有人维护。订阅这个邮件列表的人们会感谢您提供的修正和支持。我们一直都需要更多志愿者!

如果您没有得到回应，则可以使用`send-pr(1)`来提交问题报告(请参见如何撰写FreeBSD问题报告(http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/problem-reports/article.html))。

3. 修正它！Porter 手册 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/porters-handbook/index.html) 中提供了关于“Ports”基础设施的详细信息，通过了解这些内容，您就能修正偶然坏掉的port，或甚至提交自己的port了！
4. 从较近的FTP站点下载一个编译好的安装包。“中央的”package collection 在`ftp.FreeBSD.org`的packages目录中 (<ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/packages/>)，但在此之前一定记得先看看本地镜像 (<http://mirrorlist.FreeBSD.org/>) 上是否已经有了！通常情况下这些安装包都可以直接使用，而且应该比自行编译快一些。安装过程本身可以通过`pkg_add(1)`来完成。

第5章

X Window 系统

Updated for X.Org's X11 server by Ken Tom 和 Marc Fonvieille.

5.1 概述

FreeBSD 使用X11 来为用户提供功能强大的图形用户界面。X11 是一种开放源代码的X Window 系统实现，它包括**Xorg** 和**XFree86**。FreeBSD 在包括FreeBSD 4.11-RELEASE 和FreeBSD 5.2.1-RELEASE 在内的版本之前，都默认安装**XFree86**，一种由XFree86 Project, Inc. 发布的X11 服务。从FreeBSD 5.3-RELEASE 开始，默认并且为官方支持的X11 变成了**Xorg**，它是由X.Org 基金会开发的X11 服务。

本章将介绍X11 的安装和配置，并着重强调**Xorg**。

欲了解X11 所支持的显示卡等硬件，请访问Xorg (<http://www.x.org/>) 或XFree86 (<http://www.XFree86.org/>) 的网站。

在阅读完这一章后，您将会了解：

- X 视窗系统的不同组件，它们是如何协同工作的。
- 如何安装和配置X11。
- 如何安装和使用不同的窗口管理器。
- 如何在X11 中使用TrueType® 字体。
- 如何为您的系统设置图形登陆(XDM)。

在阅读这一章之前，您应该：

- 知道如何安装额外的第三方应用程序(第4 章)。

注意：这一章介绍了**Xorg** 和**XFree86** 两种X11 服务的安装和配置。绝大多数时候，配置文件、命令句法是完全一样的。当存在差异时，**Xorg** 和**XFree86** 的写法都会有所体现。

5.2 理解X

对于那些熟悉其他图形环境，比如Microsoft Windows 或者Mac OS 的用户来说，第一次使用X 可能会感觉很惊讶。

尽管您不需要了解各种X 组件的所有细节和它们是如何互相影响的；然而，了解一些基本的知识可以让您很好地利用X 的强大功能。

5.2.1 为什么要使用X?

X 不是第一个为UNIX 而开发的视窗系统，但它是最流行的。X 的原始开发团队在开发X 之前就已经在另外一个视窗系统上工作了。那个系统的名字叫做“W” (就是“Window”)。X 只是罗马字母中W 后面的一个。

X 可以被叫做“X”，“X Window 系统”，“X11”，等等。把X11 称做“X Windows” 可能会冒犯某些人；查看X(7) 可以了解更多的信息。

5.2.2 X 客户机/服务器模型

X 一开始就是针对网络而设计的，所以采用了“client-server” 模型。在X 模型中，“X server” 运行在有键盘，显示器，鼠标的计算机上。服务器用来管理显示信息，处理来自键盘和鼠标的输入等。每一个X 应用程序(比如XTerm, 或者Netscape) 就是一个“client”。一个client 给服务器发送信息，如“Please draw a window at these coordinates”，然后服务器就返回处理信息，如“The user just clicked on the OK button”。

如果您在只有一台计算机的家里或小型办公环境中使用FreeBSD，您就需要在同一台计算机上运行X server和X client。然而，如果您有很多运行FreeBSD 的机器，您可以在您的桌面计算机上运行X server，而在比较高档的服务器上运行X 应用程序。在这样的环境中，X server 和X client 之间的通信就可以通过网络来进行。

这迷惑了一些人，因为X 的术语和他们料想的有些不同。他们以为“X server” 是运行在功能强大的大型机上的，而“X client” 是运行在他们桌面上的计算机上的。

记住，X server 是有键盘和显示器的那台计算机，而X client 是那些显示窗口的程序。

并不需要client 和server 都运行在同一种操作系统上，或甚至运行在同一种类型的计算机上。在Microsoft Windows 或者Apple 公司的Mac OS 上运行一个X server 也是可以的，在它们上面也有很多免费和商业化的应用程序。

从FreeBSD 5.3-RELEASE 开始，随FreeBSD 一同安装的X 服务改成了Xorg，它的授权同FreeBSD 的授权类似，可以免费使用。此外，也有一些针对FreeBSD 的商业X 服务器。

5.2.3 窗口管理器

X 的设计哲学很像UNIX 的设计哲学，“tools, not policy”。这就意味着X 不会试图去规定任务应该如何去完成，而是，只给用户提供一些工具，至于决定如何使用这些工具为用户自己的事情。

这套哲学扩展了X，它不会规定窗口在屏幕上应该是什么样子，要如何移动鼠标，什么键应该用来切换窗体(比如，Alt+Tab按键，在Microsoft Windows 环境中的作用)，每个窗口的工具条应该看起来像什么，他们是否应该有关闭按钮等等。

实际上，X 行使了一种叫做“窗口管理器”的应用程序的职责。有很多这样的程序可用：AfterStep, Blackbox, ctwm, Enlightenment, fvwm, Sawfish, twm, Window Maker，等等。每一个窗口管理器都提供了不同的界面和观感；其中一些还支持“虚拟桌面”；有一些允许您可以定制一些键来管理您的桌面；一些有“开始”按钮，或者其他类似的设计；一些是“可定制主题的(themeable)”，通过安装新的主题，可以完全改变外观。这些以及很多其他的窗口管理器，都可以在Ports Collection 的x11-wm 分类目录里找到。

另外，KDE 和GNOME 桌面环境都有他们自己的窗口管理器与桌面集成。

每个窗口管理器也有不同的配置机制；有些需要手工来写配置文件，而另外一些则可以使用GUI 工具来完成大部分的配置任务，至少(Sawfish) 有一个用Lisp 语言来写的配置文件。

焦点策略: 窗口管理器的另一个特性是鼠标的“focus policy”。每个窗口系统都需要有一个选择窗口的方法来接受键盘的输入信息，以及当前哪个窗口处于可用状态。

您通常比较熟悉的是一个叫做“click-to-focus”的焦点策略。这是Microsoft Windows 使用的典型焦点策略，也就是您在一个窗口上点击一下鼠标，这个窗口就处于当前可用的状态。

X 不支持一些特殊的焦点策略。而是，窗口管理器控制着在什么时候哪个窗口拥有焦点。不同的窗口管理器支持不同的焦点方案。它们都支持点击即获得焦点，而且它们中的大多数都支持好几种方案。

最流行的焦点策略：

focus-follows-mouse

鼠标指示器下面的窗口就是获得焦点的窗口。这可以不是位于其他所有窗口顶部的窗口。您可以通过将鼠标移到另一个窗口就可以来改变焦点，您不需要在它上面点击。

sloppy-focus

这种方式是对focus-follows-mouse 策略的一个小小扩展。对于focus-follows-mouse，如果您把鼠标移到了根窗口（或桌面背景）上，则所有的其它窗口都会失去焦点，而相关的全部键盘输入也会丢失。对于sloppy-focus，只有当指针在键入一个新窗口时，窗口焦点才会发生变化，当退出当前窗口时是不会变化的。

click-to-focus

当前窗口由鼠标点击来选择。窗口被“突出显示”，出现在所有其他窗口的前面。即使指针被移向了另一个窗口，所有的键盘输入仍会被这个窗口接收。

许多窗口管理器支持其他的策略，与这些相比又有些变化。您可以看具体窗口管理器的文档。

5.2.4 窗口部件

提供工具而非策略的X 方法使得在每个应用程序屏幕上看到的窗口部件得到了大大的扩展。

“Widget”只是针对用户接口中所有列举项目的一个术语，它可以用某种方法来点击或操作；如按钮，复选框，单选按钮，图标，列表框等等。Microsoft Windows 把这些叫做“控件”。

Microsoft Windows 和苹果公司的Mac OS 都有一个严格的窗口部件策略。应用程序开发者被建议确保他们的应用程序共享一个普通的所见即所得的用户界面。对于X，它并不要求一个特殊的图形风格或一套相结合的窗口部件集。

这样的结果是您不能期望X 应用程序只拥有一个普通的所见即所得的界面。有很多的流行的窗口部件集设置，包括来自于MIT 的Athena，**Motif®** (模仿Microsoft Windows 的窗口风格，所有部件都具有斜边和3种灰色度)，**OpenLook**，和其他一些窗口部件集。

如今，绝大多数比较新的X 应用程序将使用一组新式的窗口设计，包括**KDE**所使用的Qt，以及**GNOME**所使用的GTK+。在这样一种窗口系统下，UNIX 桌面的一些所见即所得特性作了一些收敛，以使初学者感到更容易一些。

5.3 安装X11

Xorg 或**XFree86** 都可以在FreeBSD 上安装。从FreeBSD 5.3-RELEASE 开始，**Xorg** 成为了FreeBSD 上的默认X11 实现。**Xorg** 是由X.Org 基金会发行的开放源代码X Window 系统实现中的X 服务。**Xorg** 基

于**XFree86 4.4RC2**和**X11R6.6**的代码。X.Org 基金会在2004年4月发行了**X11R6.7**，并在2005年2月发布了**X11R6.8.2**，后者是可以从目前的FreeBSD Ports Collection 中获得的版本。

如果需要从Ports Collection 编译和安装**Xorg**：

```
# cd /usr/ports/x11/xorg
# make install clean
```

注意：要完整地编译**Xorg**则需要至少4 GB 的剩余磁盘空间。

如果想从Ports Collection 中编译和安装**XFree86**：

```
# cd /usr/ports/x11/XFree86-4
# make install clean
```

另外**X11**也可以直接从package 来安装。我们提供了可以与**pkg_add(1)**工具配合使用的**X11**安装包。如果从远程下载并安装时，**pkg_add(1)**请不要指定版本号。**pkg_add(1)**会自动地下载最新版本的安装包。

想要从package 安装**Xorg**，简单地输入下面的命令：

```
# pkg_add -r xorg
```

XFree86 4.X也可以用类似的办法安装：

```
# pkg_add -r XFree86
```

注意：上面的例子介绍了如何安装完整的**X11**软件包，包括服务器端，客户端，字体等等。此外，也有一些单独的**X11**的ports 和packages.

这一章余下的部分将会讲解如何配置**X11**，以及如何设置一个高效的桌面环境。

5.3.1 从XFree86™ 转移到Xorg

任何port 都一样，您应该检查/usr/ports/UPDATING 文件看看有哪些改变。这个文件中包含了把您的系统从**XFree86**转换到**Xorg**的说明。

在尝试任何转换之前请使用**CVSup**来更新您的ports tree。在转换您的**X11**安装前您还需要安装sysutils/portupgrade。

在/etc/make.conf 中您需要添加变量**X_WINDOW_SYSTEM=xorg**。这样做确保您的系统知道正在使用哪种**X11**。旧的**XFREE86_VERSION**变量已经过时并被**X_WINDOW_SYSTEM**变量所取代。

然后，使用下面的命令：

```
# pkg_delete -f /var/db/pkg/imate-4* /var/db/pkg/XFree86-*
# cd /usr/ports/x11/xorg
# make install clean
# pkgdb -F
```

pkgdb(1)命令是**portupgrade**软件的一部分，会更新各种软件包的依赖关系。

注意: 要联编完整的**Xorg**，请确保至少有4 GB 的剩余磁盘空间。

5.4 配置X11

Contributed by Christopher Shumway.

5.4.1 开始之前

在配置X11 之前，您需要了解所安装的系统的下列信息：

- 显示器规格
- 显示卡的芯片类型
- 显示卡的显存容量

显示器的规格被X11 用来决定显示的分辨率和刷新率。这些规格通常可以从显示器所带的文档中，以及制造商的网站找到。需要知道两个数字范围：垂直刷新率和水平刷新率。

显示卡的芯片类型将决定X11 使用什么模块来驱动图形硬件。绝大多数的硬件都能被自动检测，但是了解它在自动检测出错的时候还是很有用处的。

显示卡的显存大小决定了系统支持的分辨率和颜色深度。了解这些限制非常重要。

5.4.2 配置X11

配置X11 需要几步。第一步是以超级用户的身份建立初始的配置文件：

```
# Xorg -configure
```

在使用**XFree86** 的情况下键入：

```
# XFree86 -configure
```

这会在/root 中生成一个叫做xorg.conf.new 的配置文件(无论您使用su(1) 或直接登录，都会改变默认的\$HOME 目录变量)。对于**XFree86** 来说，配置文件的名字是XF86Config.new。X11 程序将尝试探测系统中的图形硬件并写包含检测到的硬件的配置文件，以便加载正确的驱动程序。

下一步是测试现存的配置文件，以确认**Xorg** 能够同系统上的图形设备正常工作。要完成这个任务，只需：

```
# Xorg -config xorg.conf.new
```

XFree86 用户应：

```
# XFree86 -xf86config XF86Config.new
```

如果用户看到一个黑灰的格子和一个X 形的鼠标指针，那么配置就是成功的。要退出测试，只要同时键入**Ctrl+Alt+Backspace**。

注意: 如果鼠标工作不正常, 则需要先配置它。参见FreeBSD 安装一张中的第2.9.10 节。

接下来是调整xorg.conf.new (或XF86Config.new, 如果运行XFree86 的话) 配置文件并作测试。用文本编辑器如emacs(1) 或ee(1) 打开这个文件。要做的第一件事是为当前系统的显示器设置刷新率。这些值包括垂直和水平的同步频率。把它们加到xorg.conf.new 的"Monitor" 小节中:

```
Section "Monitor"
    Identifier      "Monitor0"
    VendorName      "Monitor Vendor"
    ModelName       "Monitor Model"
    HorizSync       30-107
    VertRefresh     48-120
EndSection
```

HorizSync 和VertRefresh 在配置文件中可能没有。如果是这样的话, 就需要添加它们, 并在HorizSync 以及VertRefresh 后面设置合适的数值。在上面的例子中, 给出了相应的显示其的参数。

X 能够利用显示器所支持的DPMS (能源之星) 功能。xset(1) 程序可以控制超时时间, 并强制待机、挂起或关机。如果希望启用显示器的DPMS 功能, 则需要把下面的设置添加到monitor 节中:

```
Option      "DPMS"
```

关闭xorg.conf.new (或XF86Config.new) 之前还应该选择默认的分辨率和色深。这是在"Screen" 小节中定义的:

```
Section "Screen"
    Identifier "Screen0"
    Device     "Card0"
    Monitor    "Monitor0"
    DefaultDepth 24
    SubSection "Display"
        Viewport   0 0
        Depth      24
        Modes       "1024x768"
    EndSubSection
EndSection
```

DefaultDepth 关键字描述了要运行的默认色深。这可以通过Xorg(1) (或XFree86(1)) 的-depth 命令行开关来替代配置文件中的设置。Modes 关键字描述了给定颜色深度下屏幕的分辨率。需要说明的是, 目标系统的图形硬件只支持由VESA 定义的标准模式。前面的例子中, 默认色深是使用24位色。在采用这个色深时, 允许的分辨率是1024x768。

最后就是将配置文件存盘, 并使用前面介绍的测试模式测试一下。

注意: 在发现并解决问题的过程中可以帮助您的工具之一就是X11 的日志文件, 包含了与X11 服务器相关的每个设备的信息。Xorg 日志的文件名是/var/log/Xorg.0.log 这样的格式(XFree86 日志文件名是XFree86.0.log 这样的格式)。日志的准确的名字可以从Xorg.0.log 到Xorg.8.log 等等。

如果一切准备妥当，就可以把配置文件放到公共的目录中了。您可以在Xorg(1) (或XFree86(1)) 里面找到具体位置。这个位置通常是/etc/X11/xorg.conf 或/usr/X11R6/etc/X11/xorg.conf (对于XFree86 它应该是/etc/X11/XF86Config 或/usr/X11R6/etc/X11/XF86Config)。

```
# cp xorg.conf.new /etc/X11/xorg.conf
```

For XFree86:

```
# cp XF86Config.new /etc/X11/XF86Config
```

现在已经完成了X11 的配置全过程。为了使用startx(1) 来启动XFree86 4.X 需要安装x11/wrapper port。Xorg 已经包含了wrapper 代码，因此并不需要安装wrapper port。X11 服务器也可以用xdm(1) 来启动。

注意: 有一个图形配置工具，xorgcfg(1) (对于XFree86 来说，是xf86cfg(1))，随X11 软件包一同安装。它可以通过选择合适的驱动和设置交互式地定义配置。这个程序可以从控制台通过命令xorgcfg -textmode 来直接启动。与了解详情，请参考xorgcfg(1) 和xf86cfg(1) 的联机手册。

另外还有一个叫做xorgconfig(1) 的文本界面配置工具(对于XFree86 是xf86config(1))，这是一个控制台工具因此对用户显得不太友好，不过当其他工具无法工作时，它仍然可能可以使用。

5.4.3 高级配置主题

5.4.3.1 配置Intel® i810 显示芯片组

配置Intel i810芯片组的显卡需要有针对X11 的能够用来驱动显卡的agpgart AGP程序接口。自从发行版本4.8-RELEASE 和5.0-RELEASE 发行以来agp(4) 驱动程序就包含在GENERIC 内核配置里面了。在以前的发行版里，您必须要在您的内核配置文件里添加下面的一行：

```
device agp
```

然后重新编译一个新的内核。或者，您可以在启动的时候使用loader(8) 自动加载agp.ko 内核模块。简单的添加下面这行到/boot/loader.conf 文件里：

```
agp_load="YES"
```

接下来，如果您正在运行FreeBSD 4.X 或者更早的版本，需要创建一个设备节点作为程序接口。要创建AGP 设备节点，在/dev 下运行MAKEDEV(8)：

```
# cd /dev # sh MAKEDEV agpgart
```

注意: FreeBSD 5.X 和以后的版本会使用devfs(5) 来半透明的分配设备节点，因此MAKEDEV(8) 这一步是不必要的。

这也适用于其他的图形卡硬件配置。注意如果系统没有将agp(4) 驱动程序编译进内核，尝试用kldload(8) 加载模块是无效的。这个驱动程序必须编译进内核或者使用/boot/loader.conf 在启动时加载进入内核。

如果您正在使用**XFree86 4.1.0** (或者以后的版本) 并且出现了像**fbPictureInit** 这样未解决的符号提示, 试着在X11 配置文件里的**Driver "i810"** 一行后面加入下面这行:

```
Option "NoDDC"
```

5.5 在X11 中使用字体

Contributed by Murray Stokely.

5.5.1 Type1 字体

X11 使用的默认字体不是很理想。大型的字体显得参差不齐, 看起来很不专业, 并且, 在**Netscape** 中, 小字体简直无法看清。有好几种免费、高质量的字体可以很方便地用在X11 中。例如, **URW**字体集合(**x11-fonts/urwfonts**) 就包括了高质量的标准**type1** 字体(**Times Roman®**, **Helvetica®**, **Palatino®** 和其他一些).在**Freefont** 集合中(**x11-fonts/freefonts**) 也包括更多的字体, 但它们中的绝大部分使用在图形软件中, 如**Gimp**, 在屏幕字体中使用并不完美。另外, 只要花很少的功夫, 可以将**XFree86** 配置成能使用**TrueType** 字体: 请参见后面的**TrueType** 字体一节。

要安装上面的**Type1**字体, 您只需要运行下面的命令:

```
# cd /usr/ports/x11-fonts/urwfonts
# make install clean
```

freefont 或其他的字库和上面所说的大体类似。为了让X 服务器能够检测到这些字体, 需要在X 服务器的配置文件/etc/X11/ (**Xorg** 是**xorg.conf** 而**XFree86** 则是**XF86Config**) 中增加下面的配置:

```
FontPath "/usr/X11R6/lib/X11/fonts/URW/"
```

或者, 也可以在命令行运行:

```
% xset fp+ /usr/X11R6/lib/X11/fonts/URW
% xset fp rehash
```

这样会起作用, 但是当X 会话结束后就会丢失, 除非它被添加到启动文件(**~/.xinitrc** 中, 针对一个寻常的**startx** 会话, 或者当您通过一个类似**XDM** 的图形登陆管理器登陆时添加到**~/.xsession** 中)。第三种方法是使用新的**/usr/X11R6/etc/fonts/local.conf** 文件: 查看**anti-aliasing** 章节。

5.5.2 TrueType® 字体

XFree86 4.X 和**Xorg** 都已经内建了对**TrueType** 字体的支持。有两个不同的模块能够启用这个功能。在这个例子中使用**freetype** 这个模块, 因为它与其他的字体描绘后端是兼容的。要启用**freetype** 模块, 只需要将下面这行添加到/etc/X11/XF86Config 文件的"Module" 部分。

```
Load "freetype"
```

对于**XFree86 3.3.X**, 需要额外的**TrueType** 字体服务器。**Xfstt** 通常被用于这个目的。要安装**Xfstt**, 只要简单的安装**port x11-servers/Xfstt**。

现在, 为TrueType 字体创建一个目录(比如, `/usr/X11R6/lib/X11/fonts/TrueType`) 然后把所有的TrueType 字体拷贝到这个目录。记住您不能直接从Macintosh® 计算机中提取TrueType 字体; 能被X11 使用的必须是UNIX/MS-DOS/Windows 格式的。一旦您已经拷贝了这些文件到这个目录, 使用**ttmkfdir** 来创建一个**fonts.dir** 文件, 以便让X字体引擎知道您已经安装了这些新文件。**ttmkfdir** 可以在FreeBSD Ports Collection `x11-fonts/ttmkfdir` 中找到。

```
# cd /usr/X11R6/lib/X11/fonts/TrueType
# ttmkfdir > fonts.dir
```

现在把TrueType 字体目录添加到字体路径中。这和上面Type1 字体的步骤是一样的, 那就是, 使用

```
% xset fp+ /usr/X11R6/lib/X11/fonts/TrueType
% xset fp rehash
```

或者把FontPath 这行加到**xorg.conf** (或**XF86Config**) 文件中。

就是这样。现在**Netscape**, **Gimp**, **StarOffice**TM 和其他所有的X 应用程序应该可以认出安装的TrueType 字体。一些很小的字体(如在Web 页面上高分辨率显示的文本) 和一些很大的字体(在**StarOffice** 下) 现在看起来已经很好了。

5.5.3 Anti-Aliased 字体

Updated by Joe Marcus Clarke.

X11 从**XFree86** 4.0.2 开始支持字体的反走样。但是, 字体配置在**XFree86** 4.3.0 之前是非常繁琐的。从**XFree86** 4.3.0 开始, 对于所有支持Xft 的应用程序, 所有放到**X11 /usr/X11R6/lib/X11/fonts/** 和**~/.fonts/** 中的字体都自动地被加入反走样支持。并不是所有的应用程序都支持Xft, 但已经有相当多的程序提供Xft 支持了。支持Xft 的应用程序包括Qt 2.3 以及更高版本(用以开发**KDE** 桌面的工具包)、**GTK+** 2.0 和更高版本(用于开发**GNOME** 桌面的工具包), 以及**Mozilla** 1.2 和更高版本。

要控制哪些字体是anti-aliased, 或者配置anti-aliased 特性, 创建(或者编辑, 如果文件已经存在的话)文件**/usr/X11R6/etc/fonts/local.conf**。Xft 字体系统的几个高级特性都可以使用这个文件来调节; 这一部分只描述几种最简单的情况。要了解更多的细节, 请查看**fonts-conf(5)**。

这个文件一定是XML 格式的。注意确保所有的标签都完全的关闭掉。这个文件以一个很普通的XML 头开始, 后跟一个DOCTYPE 定义, 接下来是**<fontconfig>** 标签:

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

像前面所做的那样, 在**/usr/X11R6/lib/X11/fonts/** 和**~/.fonts/** 目录下的所有字体已经可以被支持Xft 的应用程序使用了。如果您想添加这两个目录以外的其他路径, 简单的添加下面这行到**/usr/X11R6/etc/fonts/local.conf**文件中:

```
<dir>/path/to/my/fonts</dir>
```

添加了新的字体, 尤其是添加了新的字体目录后, 您应该运行下面的命令重建字体缓存:

```
# fc-cache -f
```

Anti-aliasing 会让字体边缘有些模糊，这样增加了非常小的文本的可读性，并从大文本字体中删除“锯齿”。但如果使用普通的文本，则可能引起眼疲劳。要禁止14磅以下字体的反走样，需要增加如下配置：

```
<match target="font">
  <test name="size" compare="less">
    <double>14</double>
  </test>
  <edit name="antialias" mode="assign">
    <bool>>false</bool>
  </edit>
</match>
<match target="font">
  <test name="pixelsize" compare="less" qual="any">
    <double>14</double>
  </test>
  <edit mode="assign" name="antialias">
    <bool>>false</bool>
  </edit>
</match>
```

用anti-aliasing 来间隔一些等宽字体也是不适当的。这似乎是KDE 的一个问题。要修复这个问题需要确保每个字体之间的间距保持在100。加入下面这些行：

```
<match target="pattern" name="family">
  <test qual="any" name="family">
    <string>fixed</string>
  </test>
  <edit name="family" mode="assign">
    <string>mono</string>
  </edit>
</match>
<match target="pattern" name="family">
  <test qual="any" name="family">
    <string>console</string>
  </test>
  <edit name="family" mode="assign">
    <string>mono</string>
  </edit>
</match>
```

(这里把其他普通的修复的字体作为"mono")，然后加入：

```
<match target="pattern" name="family">
  <test qual="any" name="family">
    <string>mono</string>
  </test>
  <edit name="spacing" mode="assign">
    <int>100</int>
  </edit>
</match>
```


某些字体，比如Helvetica，当anti-aliased的时候可能存在问题。通常的表现字体本身似乎被垂直的切成两半。糟糕的时候，还可能导致应用程序比如Mozilla崩溃。为了避免这样的现象，考虑添加下面几行到local.conf文件里面：

```
<match target="pattern" name="family">
  <test qual="any" name="family">
    <string>Helvetica</string>
  </test>
  <edit name="family" mode="assign">
    <string>sans-serif</string>
  </edit>
</match>
```

一旦您完成对local.conf文件的编辑，确保您使用了</fontconfig>标签来结束文件。不这样做将会导致您的更改被忽略。

X11 默认的字库当使用反走样时会比较难看。更好的字库可以在x11-fonts/bitstream-vera port 中找到。这个port 会创建一个/usr/X11R6/etc/fonts/local.conf 文件，如果这个文件不存在的话。反之，port 将创建/usr/X11R6/etc/fonts/local.conf-vera 文件。将其内容合并到/usr/X11R6/etc/fonts/local.conf 中，则Bitstream 字体将自动地代替默认的X11 Serif, Sans Serif, 以及单倍距字体。

最后，用户可以通过他们个人的.fonts.conf 文件来添加自己的设定。要完成此项工作，用户只需简单地创建~/.fonts.conf 并添加相关配置。此文件也必须是XML 格式的。

最后：对于LCD屏幕，可能希望使用子像素的取样。简单而言，这是通过分别控制(水平方向分开的)红、绿、蓝像素，来改善水平分辨率；这样做的效果一般会非常明显。要启用它，只需在local.conf 文件的某个地方加入：

```
<match target="font">
  <test qual="all" name="rgba">
    <const>unknown</const>
  </test>
  <edit name="rgba" mode="assign">
    <const>rgb</const>
  </edit>
</match>
```

注意：依赖于显示器的种类，rgb 可能需要被更改为bgr, vrgb 或vbgr：实验一下看看那个更好。

Anti-aliasing 在您下次启动系统时就能用了。然而，注意您的程序必须知道如何使用它。现在，Qt 工具包做到了，所以整个KDE 环境能够使用anti-aliased 字体(查看KDE 上的第5.7.3.2 节 了解细节)。通过“Font” capplet (参见第5.7.1.3 节 以了解进一步的细节)，GTK+ 和GNOME 也可以使用anti-aliasing。默认情况下，Mozilla 1.2 以及更高版本都会自动的使用anti-aliasing。要禁用它，使用-DWITHOUT_XFT 选项重新编译Mozilla。

5.6 X 显示管理器

Contributed by Seth Kingsley.

5.6.1 概要

X 显示管理器(**XDM**) 是一个X视窗系统用于进行登陆会话管理的可选项。这个可以应用于多种情况下, 包括小 “X Terminals”, 桌面, 大网络显示服务器。既然X 视窗系统不受网络和协议的限制, 那对于通过网络连接起来的运行X 客户端和服务端的不同机器, 就会有许多的可配置项。**XDM** 提供了一个选择要连接到哪个显示服务器的图形接口, 只要键入如登陆用户名和密码这样的验证信息。

您也可以把**XDM** 想象成与**getty(8)** 工具一样(see 第22.3.2 节 for details)。为用户提供了同样功能。它可以完成系统的登陆任务, 然后为用户运行一个会话管理器(通常是一个X 视窗管理器)。接下来**XDM** 就等待这个程序退出, 发出信号用户已经登陆完成, 应当退出屏幕。这时, **XDM** 就可以为下一个登陆用户显示登陆和可选择屏幕。

5.6.2 使用XDM

XDM 精灵程序在`/usr/X11R6/bin/xdm` 中。您可以在任何时候用**root** 来运行这个程序, 在本地机器上, 它将启动管理X的画面。如果要**XDM** 每次机器一启动就开始运行, 一个简单的办法是在`/etc/ttys` 中加入一个记录。有关这个文件的更多的格式和使用方法, 可以看看第22.3.2.1 节。在默认的`/etc/ttys` 文件中用于运行**XDM** 守护程序的一行是这样的:

```
ttyv8    "/usr/X11R6/bin/xdm -nodaemon"  xterm    off secure
```

默认情况下, 这个记录是关闭的, 要启用它, 您需要把第5部分的**off** 改为**on** 然后按照第22.3.2.2 节的指导重新启动**init(8)**。第一部分, 这个程序将管理的终端名称是**ttyv8**。这意味着**XDM** 将运行在第9个虚拟终端上。

5.6.3 配置XDM

XDM 的配置目录是在`/usr/X11R6/lib/X11/xdm`中。在这个目录中, 您会看到几个用来改变**XDM** 行为和外观的文件。您会找到这些文件:

文件	描述
<code>Xaccess</code>	客户端授权规则。
<code>Xresources</code>	默认的X资源值。
<code>Xservers</code>	远程和本地显示管理列表。
<code>Xsession</code>	用于登陆的默认的会话脚本。
<code>Xsetup_*</code>	登陆之前用于加载应用程序的脚本。
<code>xdm-config</code>	运行在这台机器上的所有显示的全局配置。
<code>xdm-errors</code>	服务器程序产生的错误。
<code>xdm-pid</code>	当前运行的 XDM 的进程ID。

当**XDM** 运行时, 在这个目录中有几个脚本和程序可以用来设置桌面。这些文件中的每一个的用法都将被简要地描述。这些文件的更详细的语法和用法在**xdm(1)** 中将有详细描述。

默认的配置是一个矩形的登陆窗口，上面有机器的名称，“Login:”和“Password:”。如果您想设计您自己个性化的**XDM**屏幕，这是一个很好的起点。

5.6.3.1 Xaccess

用以连接由**XDM**所控制的显示设备的协议，叫做X显示管理器连接协议(**XDMCP**)。这个文件是一组用以控制来自远程计算机的**XDMCP**连接的规则。除非您修改**xdm-config**使其接受远程连接，否则其内容将被忽略。默认情况下，它不允许来自任何客户端的连接。

5.6.3.2 Xresources

这是一个默认的用来显示选项和登陆屏幕的应用程序文件。这就是您能够定制登陆程序的外观的地方。这个格式与X11文档中描述的默认应用程序文件是一样的。

5.6.3.3 Xservers

这是一个选择者应当提供的作为可选的远程显示列表。

5.6.3.4 Xsession

这是一个用户登陆后针对**XDM**的默认会话脚本。通常，在`~/.xsession`中每个用户将有一个可定制的会话脚本。

5.6.3.5 Xsetup_*

在显示选择者或登陆接口之前，这些将被自动运行。这是一个每个显示都要用到的脚本，叫做**Xsetup_**，后面会跟一个本地显示的数字(比如**Xsetup_0**)。典型的，这些脚本将在后台(如**xconsole**)运行一个或两个程序。

5.6.3.6 xdm-config

此文件以应用程序默认值的形式，提供了在安装时所使用的普适的显示设置。

5.6.3.7 xdm-errors

这个文件包含了**XDM**正设法运行的X服务器的输出。如果**XDM**正设法运行的显示由于某种原因被挂起，那这是一个寻找错误信息的好地方。这些信息会在每一个会话的基础上被写到用户的`~/.xsession-errors`文件中。

5.6.4 运行一个网络显示服务器

对于其他客户端来说，为了连接到显示服务器，您将必须编辑访问控制规则，然后启用连接侦听。默认的这些被设置成比较保守的值。要让**XDM**能侦听连接，先要在**xdm-config**文件中注释掉一行：

```
! SECURITY: do not listen for XDMCP or Chooser requests ! Comment out this line if you want to ma
```

```
DisplayManager.requestPort: 0
```

然后重新启动**XDM**。记住默认应用程序文件的注释以“!”字母开始,不是“#”。您需要设置严格的访问控制。看看在**Xaccess**文件中的实例记录,可以参考**xdm(1)**的联机手册。

5.6.5 替换XDM

有几个替换默认**XDM**程序的方案。它们是,上一节已经描述过的**kdm**(与**KDE**捆绑在一起)。**kdm**提供了许多视觉上的改进和局部的修饰,同样能让用户在启动时能选择他们喜欢的窗口管理器。

5.7 桌面环境

Contributed by Valentino Vaschetto.

这节描述了FreeBSD上用于X的不同桌面环境。“桌面环境”可能仅仅是一个简单的窗口管理器,也可能是一个像**KDE**或者**GNOME**这样的完整桌面应用程序套件。

5.7.1 GNOME

5.7.1.1 有关GNOME

GNOME是一个用户界面友好的桌面环境,能够使用户很容易地使用和配置他们的计算机。**GNOME**包括一个面板(用来启动应用程序和显示状态),一个桌面(存放数据和应用程序的地方),一套标准的桌面工具和应用程序,和一套与其他人相互协同工作的协议集。其他操作系统的用户在使用**GNOME**提供的强大的图形驱动环境时会觉得很好。更多的关于FreeBSD上**GNOME**的信息可以在FreeBSD GNOME Project (<http://www.FreeBSD.org/gnome>)的网站上找到。此外,这个网站也提供了相当详尽的关于安装、配置和管理**GNOME**的常见问题解答(FAQ)。

5.7.1.2 安装GNOME

安装**GNOME**的最简单的方法是第2.9.13节第2章描述的在FreeBSD安装过程中通过“Desktop Configuration”菜单来进行。它们也可以很容易地从一个package或Ports Collection安装:

要从网络安装**GNOME**,只要键入:

```
# pkg_add -r gnome2
```

从源代码编译**GNOME**,可以使用ports树:

```
# cd /usr/ports/x11/gnome2
# make install clean
```

一旦装好了**GNOME**,就必须告诉X server启动**GNOME**而不是默认的窗口管理器。

最简单的启动**GNOME**的方法是使用**GDM**, **GNOME**显示管理器。随**GNOME**桌面一同安装的**GDM**(但默认是禁用的),可以通过在/etc/rc.conf中加入**gdm_enable="YES"**来启用。这样在重新启动的时候, **GNOME**就会在登录时自动启动——除此之外不需要进一步设置了。

GNOME 也可以通过适当地配置名为 `.xinitrc` 的文件来启动。如果已经有了自定义的 `.xinitrc`，将启动当前窗口管理器的那一行改为启动 `/usr/X11R6/bin/gnome-session` 就可以了。如果还没有，那么只需简单地：

```
% echo "/usr/X11R6/bin/gnome-session" > ~/.xinitrc
```

接下来输入 `startx`，**GNOME** 桌面环境就启动了。

注意：如果之前使用了一些旧式的显示管理器，例如 **XDM**，则这样做是没用的。此时应建立一个可执行的 `.xsession` 文件，其中包含同样的命令。要完成这项工作，需要用 `/usr/X11R6/bin/gnome-session` 取代现有的窗口管理器：

```
% echo "#!/bin/sh" > ~/.xsession
% echo "/usr/X11R6/bin/gnome-session" >> ~/.xsession
% chmod +x ~/.xsession
```

还有一种做法，是配置显示管理器，以便在登录时提示您选择窗口管理器；在 **KDE** 细节 环节中介绍了关于如何为 **kdm**，**KDE** 的显示管理器进行这样的配置。

5.7.1.3 在GNOME上使用Anti-aliased字体

X11 通过“**RENDER**”扩展来支持 **anti-aliasing**。GTK+ 2.0 以及更高的版本(被 **GNOME** 使用的工具包)可以使用这个功能。配置 **anti-aliasing** 在第 5.5.3 节描述。所以，使用最近的软件，**anti-aliasing** 可以应用在 **GNOME** 桌面环境中。只需要依次选择应用程序→桌面首选项→字体，然后选上最佳形状，最佳对比度，或者像素圆滑(LCD)。对于 GTK+ 应用程序，它们不是 **GNOME** 桌面的一部分，在启动程序前需要设置环境变量 `GDK_USE_XFT` 的值为 1。

5.7.2 KDE

5.7.2.1 有关KDE

KDE 是一个容易使用的现代桌面环境。**KDE** 有很多很好的特性：

- 一个美丽的现代的桌面。
- 一个集合了完美网络环境的桌面。
- 一个集成的允许您方便、高效地帮助您使用 **KDE** 桌面和它的应用程序的帮助系统。
- 所有的 **KDE** 应用程序具有一致的所见即所得界面。
- 标准的菜单和工具栏，键盘布局，颜色配置等。
- 国际化：**KDE** 可以使用超过 40 种语言。
- 集中的一致化的桌面驱动配置。
- 许多有用的 **KDE** 应用程序。

KDE 中有一个基于 **KDE** 的“**KParts**”技术的办公套件，它提供了电子表格、幻灯片、日程管理，以及新闻组阅读器等软件。**KDE** 还附带了一个叫做 **Konqueror** 的 web 浏览器，是为其他运行于 UNIX 系统上

的web浏览器的强大竞争对手。关于**KDE**的更多详情可以在**KDE**网站 (<http://www.kde.org/>) 上找到。要了解FreeBSD 专属的**KDE** 信息和资源, 请参考FreeBSD-KDE 团队 (<http://freebsd.kde.org/>) 的网站。

5.7.2.2 安装KDE

与**GNOME** 或其他桌面环境一样, 安装**KDE** 的最容易的方法是通过第2.9.13 节 第2 章所描绘的FreeBSD 安装过程的“Desktop Configuration” 菜单来安装。另外, 它也可以很容易地从**packages**或**Ports Collection**安装:

要从网络安装**KDE** 只需要:

```
# pkg_add -r kde
```

`pkg_add(1)` 就会自动的下载最新版本的应用程序。

要从源代码编译**KDE**, 可以使用**ports** 树:

```
# cd /usr/ports/x11/kde3 # make install clean
```

KDE 安装完成后, **X server**必须被告知启动这个应用程序以代替默认的窗口管理器。这可以通过编辑**.xinitrc** 文件来完成:

```
% echo "exec startkde" > ~/.xinitrc
```

现在, 无论您什么时候用**startx**进入**X** 视窗系统, **KDE** 就将成为您的桌面环境。

如果使用一个像**XDM**这样的显示管理器, 那配置文件可能有点不同。需要编辑一个**.xsession** 文件, 有关**kdm** 的用法会在这章的后面介绍。

5.7.3 有关KDE 的更多细节

现在**KDE** 已经被安装在系统中了。通过帮助页面或点击多个菜单可以发现很多东西。**Windows** 或**Mac®** 用户会有回到家的感觉。

有关**KDE** 的最好的参考资料是它的在线文档。**KDE** 拥有它自己的web 浏览器**Konqueror**, 还有很多其他的应用程序和丰富文档。这节的余下部分将讨论一些很难用走马观花的方法来学习的技术项目。

5.7.3.1 KDE 显示管理器

一个多用户系统的系统管理员可能希望给用户提供一个图形化的登陆界面, 像前面描述的一样, 可以使用**xdm**。然而, **KDE** 提供了另一种选择, **kdm**, 它看起来很吸引人, 还包含很多登陆选项。特别的, 用户可以很容易地(通过一个菜单) 选择登陆后使用哪个桌面环境(**KDE**, **GNOME**或其他)。

首先, 以**root** 用户身份运行**KDE** 控制面板, **kcontrol**。通常情况下, 以**root** 身份运行**X** 环境是很不安全的。您应当以普通用户来使用窗口管理器, 打开一个终端窗口(例如**xterm** 或者**KDE** 的**konsole**), 用**su** 来切换到**root**(这个用户必须首先在**/etc/group** 的**wheel** 组里), 然后再键入**kcontrol**。

点击左边标记系统的图标, 然后选择登陆管理器。在右面, 有几个配置选项, **KDE** 手册会解释的更加详细一些。点击右边的会话。点击新类型来添加几个窗口管理器或桌面环境。这些只是标签, 所以它们用**KDE**或**GNOME**要比用**startkde**或者**gnome-session**来得好。也可以是**failsafe**。

也可以用同样方法定制其他菜单，它们主要是起修饰和自我解释用的。完成之后，键入**Apply**按钮，退出控制中心。

要确信**kdm**理解标签(**KDE**，**GNOME**等)的意思，需要编辑一些**xm**用的文件。

注意: 在**KDE 2.2**中，这有些变化：**kdm**现在使用它自己的配置文件。请看看**KDE 2.2**的文档。

在一个终端窗口，作为**root**用户，要编辑**/usr/X11R6/lib/X11/xm/Xsession**文件，中间有一部分是这样的：

```
case $# in
1)
    case $1 in
    failsafe)
        exec xterm -geometry 80x24-0-0
        ;;
    esac
esac
```

需要在这部分加几行。假定使用的标签是“**KDE**”和“**GNOME**”，就像下面这样：

```
case $# in
1)
    case $1 in
    kde)
        exec /usr/local/bin/startkde
        ;;
    GNOME)
        exec /usr/X11R6/bin/gnome-session
        ;;
    failsafe)
        exec xterm -geometry 80x24-0-0
        ;;
    esac
esac
```

为了加上**KDE** 的登陆桌面背景，需要在**/usr/X11R6/lib/X11/xm/Xsetup_0**中加入下面这行：

```
/usr/local/bin/krootimage
```

现在，确信**kdm**在**/etc/ttys**中列出来了，并且将被启动。要这样做，只要跟着先前有关**XDM**用法，用**/usr/X11R6/bin/xm** 程序的用法替换**/usr/local/bin/kdm**的用法就可以了。

5.7.3.2 Anti-aliased 字体

X11 通过它的“**RENDER**”扩展来支持anti-aliasing，从2.3版本开始，**Qt** (被**KDE**使用的工具包)也支持这个扩展。在有关anti-aliasing **X11**字体的第5.5.3 节节描述到了如何配置这些。所以，对于现在的软件，anti-aliasing也可以用在**KDE**桌面上。只需要到**KDE** 菜单，到**Preferences**→**Look and Feel**→**Fonts**，然后点击**Use Anti-Aliasing for Fonts and Icons**。对于一个不是**KDE**的一部分的**Qt**应用程序，环境变量**QT_XFT**需要在启动程序前被设置成**true**。

5.7.4 XFce

5.7.4.1 有关XFce

XFce是以被**GNOME**使用的GTK+ 工具包为基础的桌面环境，但是更加轻巧，适合于那些需要一个易于使用和配置并且简单而高效的桌面的人。看起来，它非常像使用在商业UNIX系统上的**CDE**环境。**XFce**的主要特性有下面这些：

- 一个简单，易于使用的桌面。
- 完全通过鼠标的拖动和按键来控制等。
- 与**CDE**相似的主面板，菜单，applets和应用launchers。
- 集成的窗口管理器，文件管理器，声音管理器，**GNOME**应用模块，和其他一些。
- 可配置界面的主题。(因为它使用GTK+)
- 快速，轻便，高效：对于比较老的/旧的机器或带有很少内存的机器仍然很理想。

更多有关**XFce**的信息可以参考**XFce** 网站 (<http://www.xfce.org/>)。

5.7.4.2 安装XFce

有一个二进制的**XFce** 软件包存在(在写作的时候)。要安装的话，执行下面的命令：

```
# pkg_add -r xfce4
```

另外，要从源代码建立，使用Ports Collection：

```
# cd /usr/ports/x11-wm/xfce4
# make install clean
```

现在，要告诉X服务器在下次X启动时执行**XFce**。只要执行下面的命令：

```
% echo "/usr/X11R6/bin/startxfce4" > ~/.xinitrc
```

接下来就是启动X，**XFce**将成为您的桌面。与以前一样，如果使用像**XDM** 这样的显示管理器，需要创建一个.xsession文件，就像有关**GNOME** 的那节描述的，使用/usr/X11R6/bin/startxfce4 命令，或者，配置显示管理器允许在启动时选择一个桌面，就像有关**kdm**的那节描述的。

II. 常见的任务

前面已经介绍了必要的基础知识，手册的这一部分将讨论FreeBSD的一些最常用的功能。这些章节包括：

- 向您介绍流行和实用的桌面应用程序：浏览器、产品工具、文档察看程序，等等。
- 向您介绍一系列可以在FreeBSD上使用多媒体工具。
- 介绍构建定制的FreeBSD内核以启用附加功能的方法。
- 详细介绍包括桌面和网络打印机在内的打印系统设置。
- 向您展示如何在FreeBSD上运行Linux应用程序。

某些章节希望您首先阅读过其他部分，在这些章的开头部分也会给出类似的提示。

第6章

桌面应用

Contributed by Christophe Juniet.

6.1 概述

FreeBSD 可以运行种类繁多的桌面应用程序，这包括像浏览器和字处理这样的软件。绝大多数这样的程序都可以通过package来安装，或者从Ports Collection自动地构建。许多新用户希望能够在它们的系统中找到这样的应用程序。这一章将向您展示如何轻松地使用package或者Ports Collection中安装这样的软件。

需要注意的是从ports安装意味着要编译源码。根据编译的ports和电脑速度的不同，这可能需要花费相当长的时间。若是您觉得编译源码太过耗时的话，绝大多数ports也有预编译的版本可供安装。

因为FreeBSD提供的二进制兼容Linux的特性，许多原本为Linux开发的程序都可以直接用在您的桌面。在安装任何的Linux应用程序之前，强烈的推荐您阅读第10章。当您在寻找特定的ports时，可以使用whereis(1)。一般来说，许多利用Linux二进制兼容特性的ports都以“linux-”开头。在下面的介绍中，都假设安装Linux应用程序前已经开启了Linux二进制兼容功能。

本章涵盖以下种类应用程序：

- 浏览器(例如Mozilla、Opera、Firefox、Konqueror)
- 办公、图象处理(例如KOffice、AbiWord、GIMP、OpenOffice.org)
- 文档查看(例如Acrobat Reader®、gv、Xpdf、GQview)
- 财务(例如GnuCash、Gnumeric、Abacus)

阅读这章之前，您应该：

- 知道如何安装额外的第三方软件(第4章)。
- 知道如何安装Linux软件(第10章)。

想要获得更多的有关多媒体环境的信息，请阅读第7章。如果您想要建立和使用电子邮件，请参考第24章。

6.2 浏览器

FreeBSD并没有预先安装特定的浏览器。然而，在ports的目录www(<http://www.FreeBSD.org/ports/www.html>)有许多浏览器可以安装。如果您没有时间一一编译它们(有些时候这可能需要花费相当长的时间)大部分都有package可用。

KDE和GNOME已经提供HTML浏览器。请参考第5.7节得到更多完整的有关设定这些桌面环境的信息。

如果您要找小型的浏览器，可以试试看www/dillo、www/links或www/w3m。

这一节涉及如下程序：

程序名称	资源需求	安装时间	主要依赖
Mozilla	多	大量时间和空间	Gtk+
Opera	少	轻松	同时有可用的FreeBSD和Linux版本。Linux版本需要使用Linux二进制兼容模块和linux-openmotif。
Firefox	中等	长	Gtk+
Konqueror	中等	长	需要KDE库

6.2.1 Mozilla

Mozilla 是一个完全移植到FreeBSD上的现代化的、稳定的浏览器。它拥有非常合乎标准的HTML支持，它也能处理邮件和阅读新闻组。假如您打算做一个自己的主页的话，它甚至提供一个HTML编辑器。**Netscape** 的使用者可能觉得它和**Communicator** 非常相似，两者有些部分实际上是相通的。

在CPU速度低于233MHz或者内存少于64MB的老式电脑上，**Mozilla** 会占用相当多资源而难以使用。您也许可以试试**Opera** 浏览器，本章稍后将会介绍它。

也许基于某种原因，您不能或者不想编译**Mozilla**，FreeBSD GNOME 团队已经为您制作好了package。只需要通过网络安装它：

```
# pkg_add -r mozilla
```

如果没package可用，而您又有足够的时间和磁盘空间，您可以获取**Mozilla** 的源码来编译并安装它到您的系统上。执行以下指令既可：

```
# cd /usr/ports/www/mozilla
# make install clean
```

Mozilla 需要root权限执行chrom注册来确定正确的初始化。另外，如果您想要一些额外的插件比如象mouse gestures，您也必须以root权限执行**Mozilla** 以便正确的安装。

一旦您完成了**Mozilla** 安装，您就再也不需要root权限了。您可以用如下方式执行**Mozilla**：

```
% mozilla
```

也可以用如下方式直接运行电子邮件和新闻阅读器：

```
% mozilla -mail
```

6.2.2 Mozilla 与Java™ 插件

Contributed by Tom Rhodes.

安装**Mozilla** 很简单，但不幸的是安装包含第三方插件，如Java™ 和Macromedia® Flash™ 支持的**Mozilla** 却是一件消耗时间和磁盘空间的事。

首先需要做的事情时下载将要同**Mozilla** 联用的文件。让浏览器进入<http://www.sun.com/software/java2/download.html> 并建立一个他们网站上的账户。记得保存此处使用的用户名和口令，以备今后使用。下载jdk-1_5_0-bin-scs1.zip (JDK 5.0 SCSL 预编译部分) 和jdk-1_5_0-src-scs1.zip (JDK 5.0 SCSL 源代码部分) 文件，并将它们放到/usr/ports/distfiles，

因为port 不能自动下载这些文件。这是由于授权方面的限制。此外，也应该从http://javashoplm.sun.com/ECom/docs/Welcome.jsp?StoreId=22&PartDetailId=j2sdk-1.4.2_08-oth-JPR&SiteId=JSC&TransactionId=noreg 顺便下载“java 环境”，其文件名是j2sdk-1_4_2_08-linux-i586.bin。与前面类似，这个文件也必须放到/usr/ports/distfiles。接着，从<http://www.eyesbeyond.com/freebsd/java/jdk15.html> 下载一份“java 补丁包”并将其放到/usr/ports/distfiles。最后，用标准的make install clean 来安装java/jdk15 port。

启动**Mozilla** 并从Help (帮助) 菜单中选择About Plug-ins (关于插件) 这个选项。现在**Java** 插件应该会出现在列表里面了。

6.2.3 Mozilla 与Macromedia® Flash™ 插件

Macromedia Flash 插件并没有直接提供其FreeBSD 版本。不过，我们有一个软件层(wrapper) 可以用来运行Linux 版本的插件。这个wrapper 也支持Adobe® Acrobat®、RealPlayer 和很多其他插件。

应安装www/linuxpluginwrapper port，这个port 需要依赖一个很大的port，emulators/linux_base。请按照port 在安装过程中所给出的提示对您的/etc/libmap.conf 进行正确的配置！示范的配置可以在/usr/local/share/examples/linuxpluginwrapper/ 目录找到。

安装www/mozilla port，如果还没有安装**Mozilla** 的话。

现在只要如下启动**Mozilla**：

```
% mozilla &
```

然后从Help 菜单选取About Plug-ins 选项，就能够看到目前可用的插件列表了。

注意：linuxpluginwrapper 只能在i386 架构上运行。

6.2.4 Opera

Opera 是一个功能齐全，并符合标准的浏览器。它还提供了内建的邮件和新闻阅读器、IRC 客户端，RSS/Atom feed 阅读器以及更多功能。除此之外，**Opera** 是一个比较轻量的浏览器，其速度很快。它提供了两种不同的版本：“native” FreeBSD 版本，以及通过Linux 模拟运行的版本。

要使用**Opera** 的FreeBSD 版本来浏览网页，安装以下的package：

```
# pkg_add -r opera
```

有些FTP 站点没有所有版本的package，您也可以通过Ports Collection 来安装：

```
# cd /usr/ports/www/opera # make install clean
```

要安装Linux 版本的**Opera**，将上面例子中的opera 替换为linux-opera。Linux 版本在某些情况下非常有用，象是使用只有Linux 版本的插件，例如**Adobe Acrobat Reader**。不然的话在其它方面，FreeBSD 和Linux 版本是完全一样的。

6.2.5 Firefox

Firefox 是基于**Mozilla** 代码基础的下一代浏览器。**Mozilla** 是一个完整的应用程序套件，包括比如浏览器、邮件客户端、聊天客户端等等。**Firefox** 只是一个浏览器，所以更小、更快。

安装软件包键入：

```
# pkg_add -r firefox
```

如果您更喜欢从源代码编译，也可以使用Ports Collection：

```
# cd /usr/ports/www/firefox
# make install clean
```

6.2.6 Konqueror

Konqueror 是**KDE** 的一部分，不过也可以通过安装x11/kdebase3 在非**KDE** 环境下使用。**Konqueror** 不止是一个浏览器，也是一个文件管理器和多媒体播放器。

Konqueror 也带有丰富的插件，可以在misc/konq-plugins 下面找到。

Konqueror 也支持**Flash**，可以在<http://freebsd.kde.org/howto.php> 找到一个How To。

6.3 办公、图象处理

当需要进行办公或者进行图象处理时，新用户通常都会找一些好用的办公套件或者字处理软件。目前有一些桌面环境比如象**KDE** 已经提供了办公套件。**FreeBSD** 提供所有的要求，桌面环境也不例外。

这节涉及如下程序：

软件名称	资源需求	安装时间	主要依赖
KOffice	少	多	KDE
AbiWord	少	少	Gtk+ 或 GNOME
The Gimp	少	长	Gtk+
OpenOffice.org	多	长	JDK™ 1.4 、 Mozilla

6.3.1 KOffice

KDE 社区提供了一套办公套件，它能用在桌面环境。它包含四个标准的组件，这些组件可以在其它办公套件中找到。**KWord** 是字处理程序、**KSpread** 是电子表格程序、**KPresenter** 是演示文档制作管理程序、**Kontour**是矢量绘图软件。

安装最新的**KOffice** 之前，先确定您是否安装了最新版的**KDE**。

使用package 来安装**KOffice**，安装细节如下：

```
# pkg_add -r koffice
```

如果没有可用的package，您可以使用Ports Collection 安装。安装**KDE3** 的**KOffice** 版本，如下：

```
# cd /usr/ports/editors/koffice-kde3
# make install clean
```

6.3.2 AbiWord

AbiWord 是一个免费的字处理程序，它看起来和**Microsoft Word** 的感觉很相似。它适合用来打印文件、信函、报告、备忘录等等，它非常快且包含许多特性，并且非常容易使用。

AbiWord 可以导入或输出很多文件格式，包括一些象**Microsoft.doc** 格式的文件。

AbiWord 也有package 的安装方式。您可以用以下方法安装：

```
# pkg_add -r abiword
```

如果没有可用的package，它也可以从Ports Collection 编译。ports collection 应该是最新的。它的安装方式如下：

```
# cd /usr/ports/editors/abiword
# make install clean
```

6.3.3 GIMP

对图象的编辑或者加工，**GIMP** 是一个非常精通图象处理的软件。它可以被用来当作简单的绘图程序或者一个专业的照片处理套件。它支持大量的插件和具有脚本界面的特性。**GIMP** 可以读写众多的文件格式，支持扫描仪和手写板。

您可以用下列命令安装：

```
# pkg_add -r gimp
```

如果您在FTP 站点没有找到这个package，您也可以使用Ports Collection 的方法安装。ports 的graphics (<http://www.FreeBSD.org/ports/graphics.html>) 目录也包含有**Gimp 手册**。以下是安装它们的方法：

```
# cd /usr/ports/graphics/gimp
# make install clean
# cd /usr/ports/graphics/gimp-manual-pdf
# make install clean
```

注意：Ports 中的graphics (<http://www.FreeBSD.org/ports/graphics.html>) 目录也有开发中的**GIMP** 版本graphics/gimp-devel。HTML 版本的**Gimp 手册** 可以在graphics/gimp-manual-html 找到。

6.3.4 OpenOffice.org

OpenOffice.org 包括一套完整的办公套件：一个字处理程序、一个电子表格程序、一个演示文档管理程序和一个绘图程序。它和其它的办公套件的特征非常相似，它可以导入输出不同的流行的文件格式。它包括一些不同的语言界面、拼写检查和字典。

OpenOffice.org 的字处理程序使用XML 文件格式使它增加了可移植性和灵活性。电子表格程序支持宏语言和使用外来的数据库界面。**OpenOffice.org** 已经可以平稳的运行在Windows、SolarisTM、Linux、FreeBSD 和Mac OS X 等各种操作系统下。更多的有关**OpenOffice.org** 的信息您可以在OpenOffice.org 网页 (<http://www.openoffice.org/>)找到。对于特定的FreeBSD 版本的信息, 您可以在直接在FreeBSD OpenOffice 移植团队 (<http://porting.openoffice.org/freebsd/>)的页面下载。

安装**OpenOffice.org** 方法如下:

```
# pkg_add -r openoffice
```

注意: 如果您正在使用FreeBSD 的-RELEASE 版本, 一般来说这样做是没问题的。如果不是这样, 您可能需要看一看FreeBSD **OpenOffice.org** 移植小组的网站, 并使用pkg_add(1) 从那里下载并安装合适的软件包。最新的发布版本和开发版本都可以在那里找到。

装好package 之后, 您只需输入下面的命令就能运行**OpenOffice.org** 了:

```
% openoffice.org
```

注意: 在第一次运行时, 将询问您一些问题, 并在您的主目录中建立一个.openoffice.org2 目录。

如果没有可用的**OpenOffice.org** package, 您仍旧可以选择编译port。然而, 您必须记住它的要求以及大量的磁盘空间和相当长的时间编译。

```
# cd /usr/ports/editors/openoffice.org-2.0
# make install clean
```

注意: 如果希望联编一套进行过本地化的版本, 将前述命令行改为:

```
# make LOCALIZED_LANG=your_language install clean
```

您需要将*your_language* 改为正确的ISO-代码。所支持的语言代码可以在files/Makefile.localized 文件中找到, 这个文件位于port 的目录。

一旦完成上述操作, 就可以通过下面的命令来运行**OpenOffice.org** 了:

```
% openoffice.org
```

6.4 文档查看器

一些新的文档格式近来得到流行。它们所需要的标准查看器可能不一定在系统内。在本节我们将了解如何安装它们。

这节涵盖如下应用程序:

软件名称	资源需求	安装时间	主要依赖
Acrobat Reader	少	少	Linux二进制兼容
gv	少	少	Xaw3d
Xpdf	少	少	FreeType
GQview	少	少	Gtk+ 或GNOME

6.4.1 Acrobat Reader®

现在许多文档都用PDF 格式，根据“轻便小巧文档格式”的定义。一个被建议使用的查看器是**Acrobat Reader**，由Adobe 所发行的Linux 版本。因为FreeBSD 能够运行Linux 二进制文件，所以它也可以用FreeBSD 中。

要从Ports collection 安装**Acrobat Reader 7**，只需：

```
# cd /usr/ports/print/acroread7
# make install clean
```

由于授权的限制，我们不提供预编译的版本。

6.4.2 gv

gv 是PostScript® 和PDF 文件格式查看器。它源自**ghostview** 因为使用**Xaw3d** 函数库让它看起来更美观。它很快而且界面很干净。**gv** 有很多特性比如象纸张大小、刻度或者抗锯齿。大部分操作都可以用键盘或鼠标完成。

安装**gv** package，如下：

```
# pkg_add -r gv
```

如果您无法获取预编译的包，则可以使用Ports collection：

```
# cd /usr/ports/print/gv # make install clean
```

6.4.3 Xpdf

如果您想要一个小型的FreeBSD PDF 查看器，**Xpdf** 是一个小巧并且高效的查看器。它只需要很少的资源而且非常稳定。它使用标准的X 字体并且不需要**Motif** 或者其它的X 工具包。

安装**Xpdf** package，使用如下命令：

```
# pkg_add -r xpdf
```

如果package 不可用或者您宁愿使用Ports Collection，如下：

```
# cd /usr/ports/graphics/xpdf
# make install clean
```

一旦安装完成，您就可以启动**Xpdf** 并且使用鼠标右键来使用菜单。

6.4.4 GQview

GQview 是一个图片管理器。您可以单击鼠标来观看一个文件、开启一个外部编辑器、使用预览和更多的功能。它也有幻灯片播放模式和一些基本的文件操作。您可以管理采集的图片并且很容易找到重复的。**GQview** 可以全屏幕观看并且支持国际化。

如果您想要安装**GQview** package，如下：

```
# pkg_add -r gqview
```

如果您没有可用的package 或者您宁愿使用Ports Collection，如下：

```
# cd /usr/ports/graphics/gqview
# make install clean
```

6.5 财务

假如，基于任何的理由，您想要在FreeBSD Desktop 管理您个人的财政，有一些强大并且易于使用的软件可以被您选择安装。它们中的一些与流行的文件格式兼容象**Quicken®** 或**Excel** 文件。

本节涵盖如下软件：

软件名称	资源需求	安装时间	主要依赖
GnuCash	少	长	GNOME
Gnumeric	少	长	GNOME
Abacus	少	少	Tcl/Tk

6.5.1 GnuCash

GnuCash 是**GNOME** 的一部分，**GNOME** 致力于为最终用户提供用户友好且功能强大的软件。使用**GnuCash**，您可以关注您的收入和开支、您的银行帐户，或者您的股票。它的界面特性看起来非常的专业。

GnuCash 提供一个智能化的注册、帐户分级系统、很多键盘快捷方式和自动完成方式。它能分开一个单个的处理到几个详细的部分。**GnuCash** 能导入和合并**Quicken** QIF 文件格式。它也支持大部分的国际日期和流行的格式。

安装**GnuCash** 到您的系统，如下：

```
# pkg_add -r gnucash
```

如果package 不可用，您可以使用Ports Collection 安装：

```
# cd /usr/ports/finance/gnucash
# make install clean
```

6.5.2 Gnumeric

Gnumeric 是一个电子表格程序，**GNOME** 桌面环境的一部分。它以通过元素格式和许多片断的自动填

充系统来方便的自动“猜测”用户输入而著称。它能导入一些流行的文件格式，比如象**Excel**、**Lotus 1-2-3**或**Quattro Pro**。**Gnumeric** 凭借**math/guppi** 支持图表。它有大量的嵌入函数和允许所有通常比如象、数字、货币、日期、时间等等的一些单元格式。

安装**Gnumeric** package，如下：

```
# pkg_add -r gnumeric
```

如果package 不可用，您可以使用Ports Collection 安装：

```
# cd /usr/ports/math/gnumeric
# make install clean
```

6.5.3 Abacus

Abacus 是一个小巧易用的电子表格程序。它包含许多嵌入函数在一些领域如统计学、财务和数学方面很有帮助。它能导入和输出**Excel** 文件格式。**Abacus** 可以产生PostScript 输出。

安装**Abacus** package，如下：

```
# pkg_add -r abacus
```

如果package 不可用，您可以使用Ports Collection 安装：

```
# cd /usr/ports/deskutils/abacus
# make install clean
```

6.6 总结

当FreeBSD 因为它的效能和稳定而在ISP 之间流行时，它也可以完全应用在桌面环境。拥有数以千计的packages (<http://www.FreeBSD.org/where.html>) 或者ports (<http://www.FreeBSD.org/ports/index.html>)，您可以为您的需要建立完美的桌面环境。

一旦您完成了您的桌面环境的安装，您可能想要进一步了解misc/instant-workstation。“meta-port” 允许您为一个工作站建立一个定制的ports 设置。您可以编辑/usr/ports/misc/instant-workstation/Makefile 定制它。接着是缺省添加和删除ports 的语法，和使用通常的步骤建立它。最后，您将能建立一个适合您自己桌面的大的package 并在您的其它的工作站上安装它！

下面是本章涉及到的所有的软件的快速回顾：

软件名称	Package 名称	Ports 名称
Mozilla	mozilla	www/mozilla
Opera	opera	www/opera
Firefox	firefox	www/firefox
KOffice	koffice-kde3	editors/koffice-kde3
AbiWord	abiword	editors/abiword
The GIMP	gimp	graphics/gimp

软件名称	Package 名称	Ports 名称
OpenOffice.org	openoffice	editors/openoffice-1.1
Acrobat Reader	acroread	print/acroread7
gv	gv	print/gv
Xpdf	xpdf	graphics/xpdf
GQview	gqview	graphics/gqview
GnuCash	gnucash	finance/gnucash
Gnumeric	gnumeric	math/gnumeric
Abacus	abacus	deskutils/abacus

第7章

多媒体

编辑: Ross Lippert. 中文翻译: 张雪平.

7.1 概述

FreeBSD 广泛地支持各种声卡，让您可以从容地享受来自您的计算机的高保真输出。这包括了录制和播放MPEG Audio Layer 3 (MP3)、WAV、以及Ogg Vorbis 等许多种格式声音的能力。FreeBSD 同时也包括了许多的应用程序，让您可以录音、增加声音效果以及控制附加的MIDI设备。

要是乐于动手，FreeBSD 也能支持播放一般的视频文件和DVD。对各种视频媒体进行编码、转换和播放的应用程序比起处理声音的应用程序略少一些。例如，在撰写这章时，FreeBSD Ports Collection 中还没有类似audio/sox 那样好的重编码工具能够用来在不同的格式之间转换。不过，这个领域的软件研发进展是很快的。

本章将介绍配置声卡的必要步骤。X11 的安装和配置(第5 章) 里已经考虑到了您显卡的问题，但要想有更好的播放效果，仍需要调整一些东西。

读了本章后，您将知道：

- 如何配置系统识别声卡。
- 运用样本程序去测试声卡工作的方法。
- 如何排除声卡安装中的问题。
- 如何播放和编码MP3以及其它格式的音频。
- X 服务器如何支持视频。
- 哪些好的视频播放/压缩 “ports” 。
- 如何播放DVD、.mpg 以及.avi 文件。
- 如何从CD和DVD中提取文件。
- 怎样配置电视卡。
- 如何配置图像扫描仪。

在读本章这前，您应该：

- 知道如何配置、安装一个新的内核(第8 章)

警告: 用mount(8) 命令去装载CD光盘，至少会产生一个错误，更糟的情况下会产生**kernel panic**。这种媒体所用的编码与通常的ISO文件系统是不同的。

7.2 安装声卡

贡献者Moses Moore. Enhanced for FreeBSD 5.X by Marc Fonvieille.

7.2.1 配置系统

在开始之前，您应该清楚声卡类型、所用的芯片以及它是PCI 还是ISA 卡。FreeBSD 支持种类繁多的PCI 和ISA 卡。检查Hardware Notes (<http://www.FreeBSD.org/releases/6.0R/hardware.html>) 中支持的音频设备列表看看是否支持您的声卡。这份文档也只论及支持您的声卡的驱动程序。

要使用声卡，就应装载正确的驱动程序。完成的方式有两种：最简单的是使用命令kldload(8) 来装载一个内核模块，在命令行输入

```
# kldload snd_emu10k1
```

或者在文件/boot/loader.conf 里加入一行，内容如下

```
snd_emu10k1_load="YES"
```

上边实例用于Creative SoundBlaster® Live! 声卡。其它可装载的模块列在文件/boot/defaults/loader.conf里边。如果不知道应该使用哪个驱动，您可以尝试加载snd_driver module:

```
# kldload snd_driver
```

这是个meta 驱动，一次加载了最常见的设备驱动。这会提高搜索正确驱动的速度。也可以通过/boot/loader.conf 工具来加载所有的声卡驱动。

如果希望在加载了snd_driver meta 驱动之后了解到底选择了哪种声卡，可以通过使用cat /dev/sndstat 来查询/dev/sndstat 文件。

注意: 在FreeBSD 4.X 下，要加载所有的声卡驱动，您必须加载snd 模块而不是snd_driver 模块。

另外，您也可以把支持您声卡的代码静态地编译到内核里去。下一节就采用这种方式支持硬件给出提示。关于重新编译内核，请参考第8 章。

7.2.1.1 定制内核使其支持声卡

要做的第一件事情就是添加通用音频驱动sound(4) 到内核中，您需要添加下面这行到内核配置文件中：

```
device sound
```

在FreeBSD 4.X 下，使用下面这行：

```
device pcm
```

接下来就是加入对我们所用声卡的支持了。首先需要确定我们的声卡需要使用哪一个驱动。您可以参考硬件兼容列表 (<http://www.FreeBSD.org/releases/6.0R/hardware.html>) 所列出的音频设备，以确定您声卡的驱动。例如，Creative SoundBlaster Live! 声卡由snd_emu10k1(4) 驱动来支持。要添加它，需要在内核编译配置文件中加入下面一行：

```
device snd_emu10k1
```

一定要阅读驱动的联机手册了解如何使用它们。关于内核配置文件中声卡驱动的写法,也可以在`/usr/src/sys/conf/NOTES`文件(对于FreeBSD 4.X, 则是`/usr/src/sys/i386/conf/LINT`)。

非即插即用的ISA卡可能需要您为内核提供一些关于声卡配置的信息(IRQ、I/O 端口, 等等)。这项工作可以通过`/boot/device.hints`文件来完成。系统启动时, loader(8) 将读取这个文件, 并将其中的配置传给内核。例如, 旧式的Creative SoundBlaster 16 ISA 非即插即用卡需要使用`snd_sbc(4)` 驱动并配合`snd_sb16(4)`。您可以在内核编译配置文件中增加如下配置:

```
device snd_sbc
device snd_sb16
```

还有下面这些到`/boot/device.hints`中:

```
hint.sbc.0.at="isa"
hint.sbc.0.port="0x220"
hint.sbc.0.irq="5"
hint.sbc.0.drq="1"
hint.sbc.0.flags="0x15"
```

这样, 声卡使用0x220 I/O 端口和IRQ 5。

`/boot/device.hints` 文件的写法会在声卡驱动的联机手册中描述。在FreeBSD 4.X 上, 这些设定直接写进内核配置文件中。对于我们的ISA 卡这种情况, 我们只要使用这行:

```
device sbc0 at isa? port 0x220 irq 5 drq 1 flags 0x15
```

上面所展示的是默认的配置。有时候, 您可能需要更改IRQ 或其他配置, 以适应声卡的实际情况。查看`snd_sbc(4)` 联机手册了解更多信息。

注意: 在FreeBSD 4.X 下, 一些主板内建声卡设备的系统需要在内核配置文件中配置下面的选项:

```
options PNPBIOS
```

7.2.2 测试声卡

用修改过的内核重起, 或者加载了需要的模块之后, 声卡将会出现在您的系统消息缓存中(`dmesg(8)`), 就像这样:

```
pcm0: <Intel ICH3 (82801CA)> port 0xdc80-0xdcbf,0xd800-0xd8ff irq 5 at device 31.5 on pci0
pcm0: [GIANT-LOCKED]
pcm0: <Cirrus Logic CS4205 AC97 Codec>
```

声卡的状态可以通过`/dev/sndstat` 文件来查询:

```
# cat /dev/sndstat
FreeBSD Audio Driver (newpcm)
Installed devices:
pcm0: <Intel ICH3 (82801CA)> at io 0xd800, 0xdc80 irq 5 bufisz 16384
```

```
kld snd_ich (1p/2r/0v channels duplex default)
```

您系统的输出可能与此不同。如果没有看到`pcm`设备，回顾并检查一下前面做的。重新检查您的内核配置文件并保证选择了正确的设备。常见问题列在第7.2.2.1节一节。

如果一切正常，您现在应该拥有一个多功能声卡了。如果您的CD-ROM 或者DVD-ROM 驱动器适当的与声卡相关联，您可以把CD 放入驱动器并用`cdcontrol(1)`来播放：

```
% cdcontrol -f /dev/acd0 play 1
```

许多应用程序，比如`audio/workman` 可以提供一个友好的界面。您可能想要安装一个应用程序比如`audio/mpg123` 来听MP3 音频文件。一个快速的测试声卡正在发送数据到`/dev/dsp` 的方式，像这样做：

```
% cat filename > /dev/dsp
```

这里`filename` 可以是任意文件。这行命令会产生一些噪音，证明声卡果真在工作。

注意：FreeBSD 4.X 用户需要创建声卡设备节点才能使用。如果在消息缓存中展示出来的卡是`pcm0`，您必须以`root` 来运行下面这两行：

```
# cd /dev
# sh MAKEDEV snd0
```

如果检测的声卡返回`pcm1`，做上面展示的同样的步骤，只是要用`snd1` 来取代`snd0`。

`MAKEDEV` 会创建一组设备节点让相关联应用程序的不同声音使用。

声卡混音级别可以通过`mixer(8)` 命令更改。更多细节可以在`mixer(8)` 联机手册中找到。

7.2.2.1 常见问题

错误信息	解决方法
unsupported subdevice XX	一个或多个设备节点没有正确地建立。重复上面的步骤。
sb_dspwr(XX) timed out	I/O端口没有设置正确。
bad irq XX	IRQ设置不正确。确信设定的IRQ和声卡的IRQ是一样的。
xxx: gus pcm not attached, out of memory	没有足够的内存空间供设置使用。
xxx: can't open /dev/dsp!	使用命令 <code>fstat grep dsp</code> 进行检查是否有其它的程序打开了设备。值得注意的是 <code>esound</code> 和 <code>KDE</code> 提供的声卡支持经常是造成麻烦的祸根。

7.2.3 利用多个声源

贡献者Munish Chopra.

同时有多个声源的声音在播放，这是完全可能的，例如当`esound` 或者`artsd` 不支持与其它程序共享音频设备时。

FreeBSD可以通过**虚拟声道(Virtual Sound Channels)**来达到，具体设置用工具sysctl(8)来完成。虚拟的声道可以能过在内核里混合声音来混合声卡里播放的声道。

使用两条sysctl命令来设置虚拟声道的数目。如果您是root用户，执行下面的操作：

```
# sysctl hw.snd.pcm0.vchans=4
# sysctl hw.snd.maxautovchans=4
```

上面的实例设定了4个虚拟声道，这也是实际上所使用的数目。hw.snd.pcm0.vchans是pcm0的虚拟声道数，一当链接上一个设备它就可配置了。hw.snd.maxautovchans是分配给新的音频设备的虚拟声道数，此时这个设备要用kldload(8)来链接。因为pcm模块可以独立装载许多硬件驱动程序，因此hw.snd.maxautovchans也就可以存储分配给以后链接到的设备的虚拟声道数。

注意：您不能在使用某个设备的时候改变其虚拟通道数。首先需要关闭所有使用该设备的程序，如音乐播放器或声音服务。

如果不使用devfs(5)，就必须把应用程序指向/dev/dsp0.x，这里x为0到3，因为在上面的例子中hw.snd.pcm.0.vchans被设为了4。在使用devfs(5)的系统里，上边那些会自动分配给用户。

7.2.4 如何设置混音器通道值

这一节的作者是Josef El-Rayes.

注意：只有FreeBSD 5.3-RELEASE 和更新的版本中才支持这一功能。

不同的混音通道的默认音量是硬编码进pcm(4)驱动程序的。同时，也有很多应用或服务程序提供了允许用户直接设置并记住这些值的功能。不过这并不是一个很好的解决方案，您可能希望在驱动一级有一个可以设置的默认值。这可以通过在/boot/device.hints定义适当的值来实现。例如：

```
hint.pcm.0.vol="100"
```

这将在pcm(4)模块加载时，将通道音量设置为默认的100。

7.3 MP3音频

贡献者Chern Lee.

MP3 (MPEG Layer 3 Audio)达到过CD音质的效果，FreeBSD工作站没理由会缺少这样的好东东。

7.3.1 MP3播放器

目前为止，最为流行的X11 MP3播放器是XMMS (X多媒体系统)。Winamp的肤面可以直接用于XMMS，因为它的GUI几乎和Nullsoft的Winamp完全一样。另外，XMMS也提供了内建的插件支持。

XMMS可以通过multimedia/xmms port或package来安装。

XMMS 的界面很直观，它提供了播放列表、图形化均衡器等等。如果您熟悉**Winamp**，就会感觉**XMMS** 很容易使用。

audio/mpg123 port 提供了一个命令行界面的MP3 播放器。

mpg123 可以在执行时通过命令行指定声音设备和要播放的MP3 文件，如下所示：

```
# mpg123 -a /dev/dsp1.0 Foobar-GreatestHits.mp3
High Performance MPEG 1.0/2.0/2.5 Audio Player for Layer 1, 2 and 3.
Version 0.59r (1999/Jun/15). Written and copyrights by Michael Hipp.
Uses code from various people. See 'README' for more!
THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTY! USE AT YOUR OWN RISK!
```

```
Playing MPEG stream from Foobar-GreatestHits.mp3 ...
MPEG 1.0 layer III, 128 kbit/s, 44100 Hz joint-stereo
```

/dev/dsp1.0 应该换成您的系统上的dsp 设备。

7.3.2 抓取CD音轨

在对CD或CD音轨编码成MP3之前，CD上的音频数据应先抓到硬盘里。这个可以通过复制原始的CDDA(CD数字音频)数据成为波形(WAV)文件。

工具**cdda2wav** 是**sysutils/cdrtools** 套件的一部份，可用来从CD中获取音频及其相关信息。

把CD放到光驱里，下面的命令可以完成(作为root用户)把整张CD 分割成单个(每个音轨)的WAV文件：**/para>**

```
# cdda2wav -D 0,1,0 -B
```

cdda2wav 支持ATAPI (IDE)光驱。从IDE光驱中抓取音轨，需要用设备名称代替SCSI的单元号。例如，想从IDE 光驱中抓取第7道音轨：

```
# cdda2wav -D /dev/acd0a -t 7
```

参数**-D 0,1,0** 表示SCSI 设备**0,1,0**，与命令**cdrecord -scanbus**的输出相对应。

抓取单轨，要使用选项**-t**，如下所示：

```
# cdda2wav -D 0,1,0 -t 7
```

这个实例用于抓取第七个音轨。要抓取一定范围的音轨，如从1到7：

```
# cdda2wav -D 0,1,0 -t 1+7
```

利用**dd(1)**也可以从ATAPI光驱中抓取音轨，从第17.6.5 节可以了解更多。

7.3.3 MP3 编码

现今，可选的MP3编码器是**lame**。**Lame**可以从ports树里的audio/lame处找到。

利用抓取的WAV文件，下边的命令就可以把audio01.wav转换成audio01.mp3:

```
# lame -h -b 128 \
--tt "Foo Song Title" \
--ta "FooBar Artist" \
--tl "FooBar Album" \
--ty "2001" \
--tc "Ripped and encoded by Foo" \
--tg "Genre" \
audio01.wav audio01.mp3
```

128 kbits 是标准的MP3位率(bitrate)。许多人可能喜欢更高的品质例如160 或192。更高的位率，会使MP3 占用更多的磁盘空间--但音质会更高。选项-h 控制“高品质但低速度(higher quality but a little slower)”模式的开关。选项-t 表示把ID3 标签--通常包含了歌曲的信息，植入到MP3文件里。其它的编码选项可以查询lame 的联机手册。

7.3.4 MP3 解码

要把MP3歌曲刻录成音乐CD，就需要把它转换成非压缩的波形(WAV)格式。**XMMS** 和**mpg123** 都支持把MP3输出成非压缩格式文件。

在**XMMS**中输出到磁盘:

1. 启动**XMMS**。
2. 在窗口里右击鼠标，弹出**XMMS**菜单。
3. 在选项(Options)里选择设定(Preference)。
4. 改变输出插件成“写磁盘插件(Disk Writer Plugin)”。
5. 按配置(Configure)。
6. 输入或选择一个目录用于存放解压的文件。
7. 象平常一样，把MP3文件装入到**XMMS**里边，把音量调节到100%并且关掉EQ设定。
8. 按一下播放(Play)——**XMMS** 如同在播放mp3一样，只是听不到声音。实际上是在播放mp3到一个文件里。
9. 要想再听MP3歌曲，记得把默认的输出插件设回原来的值。

用**mpg123**进行标准输出:

1. 执行 `mpg123 -s audio01.mp3 > audio01.pcm`

XMMS输出的文件是波形(WAV)格式，而**mpg123** 则把MP3转换成无压缩的PCM 音频数据。两种格式都支持用**cdrecord** 刻录成音乐CD。使用**burncd(8)** 您就必须使用无压缩的PCM。如果选择波形格式，就要注意在每道开始时的一小点杂音，这段声音是波形文件的头部份。可以使用工具**SoX** 来轻松去除。**SoX** 可从audio/sox port 或包(package)中安装得到:

```
% sox -t wav -r 44100 -s -w -c 2 track.wav track.raw
```

阅读第17.6节 这部份可以了解到更多在FreeBSD 里刻盘的信息。

7.4 视频回放

贡献者Ross Lippert.

视频回放是个很新并且迅速发展中的应用领域。一定要有耐心，因为不是所有的事情都象处音频那么顺利。

在开始之前，您要了解显卡的类型以及它所用的芯片的类型。尽管**Xorg** 和**XFree86** 支持大量的显卡，但能达到好的回放效果的却寥寥无几。在X11运行时，您可以使用命令xdpyinfo(1) 获得使用您的显卡的X服务器所支持的扩展列表。

为了评估各种播放器和设置，您需要有一小段用作测试的MPEG文件。由于一些DVD播放器会默认地在/dev/dvd 里去找DVD文件，因此，您会发样建立符号链接到恰当的设备会很有用：

```
# ln -sf /dev/acd0c /dev/dvd
# ln -sf /dev/racd0c /dev/rdvd
```

在使用了FreeBSD 5.X 的devfs(5) 里，有一个略微不同的推荐链接集：

```
# ln -sf /dev/acd0 /dev/dvd
# ln -sf /dev/acd0 /dev/rdvd
```

注意：由于devfs(5)本身的原因，像这样手工建立的链接在重启后将不会存在。想要无论什么时候您启动系统都能自动建立符号链接，那就把下边这行加到/etc/devfs.conf 里边：

```
link acd0 dvd
link acd0 rdvd
```

另外，DVD解密要求调用专用的DVD-ROM函数，要求把许可定到DVD设备里。

前面讨论的一些ports 要正确地联编有赖于下列内核的选项设置。在试图联编之前，把这一选项增加到内核配置文件中，联编新的内核，并重启系统：

```
options CPU_ENABLE_SSE
```

注意：在FreeBSD 4.X 上，内核配置文件中还应加入options USER_LDT。这一选项在FreeBSD 5.X 和更新版本中不再提供。

为了增强用于共享内存的X11接口，推荐增加一些sysctl(8) 参数的值：

```
kern.ipc.shmmax=67108864
kern.ipc.shmall=32768
```

7.4.1 测定视频的性能

在X11下有几种可以显示图像的方式。到底哪个能工作很大程度上依赖于硬件。首先，下边描述的每一种方法在不同的硬件上都会有不同的品质。其次，在X11里的图像显示近来引起普遍的关注，随着**Xorg**或**XFree86**的每一个版本，都会有很大的突破。

常见图像接口列表：

1. X11: 一般性的使用共享内存的X11输出。
2. XVideo: 一种X11接口扩展，支持任何X11图像的可拖拉。
3. SDL: 简单直接媒体层。
4. DGA: 直接图片存取。
5. SVGAlib: 低层次掌控图片层。

7.4.1.1 XVideo

Xorg 和**XFree86 4.X** 有种扩展叫做**XVideo** (或称Xvideo, Xv, xv)，它可以通过一个特殊的加速器直接把图像显示在可拖拉的对象里。即使在低端的计算机(例如我的PIII 400 Mhz膝上电脑)，这个扩展也提供了很好的播放质量。

要了解这一扩展是否在正常工作，使用xvinfo 命令：

% **xvinfo**

如果显示结果如下，那您的显卡就支持XVideo：

```
X-Video Extension version 2.2
screen #0
Adaptor #0: "Savage Streams Engine"
  number of ports: 1
  port base: 43
  operations supported: PutImage
  supported visuals:
    depth 16, visualID 0x22
    depth 16, visualID 0x23
  number of attributes: 5
    "XV_COLORKEY" (range 0 to 16777215)
      client settable attribute
      client gettable attribute (current value is 2110)
    "XV_BRIGHTNESS" (range -128 to 127)
      client settable attribute
      client gettable attribute (current value is 0)
    "XV_CONTRAST" (range 0 to 255)
      client settable attribute
      client gettable attribute (current value is 128)
    "XV_SATURATION" (range 0 to 255)
      client settable attribute
      client gettable attribute (current value is 128)
    "XV_HUE" (range -180 to 180)
      client settable attribute
      client gettable attribute (current value is 0)
```

```

maximum XvImage size: 1024 x 1024
Number of image formats: 7
  id: 0x32595559 (YUY2)
    guid: 59555932-0000-0010-8000-00aa00389b71
    bits per pixel: 16
    number of planes: 1
    type: YUV (packed)
  id: 0x32315659 (YV12)
    guid: 59563132-0000-0010-8000-00aa00389b71
    bits per pixel: 12
    number of planes: 3
    type: YUV (planar)
  id: 0x30323449 (I420)
    guid: 49343230-0000-0010-8000-00aa00389b71
    bits per pixel: 12
    number of planes: 3
    type: YUV (planar)
  id: 0x36315652 (RV16)
    guid: 52563135-0000-0000-0000-000000000000
    bits per pixel: 16
    number of planes: 1
    type: RGB (packed)
    depth: 0
    red, green, blue masks: 0x1f, 0x3e0, 0x7c00
  id: 0x35315652 (RV15)
    guid: 52563136-0000-0000-0000-000000000000
    bits per pixel: 16
    number of planes: 1
    type: RGB (packed)
    depth: 0
    red, green, blue masks: 0x1f, 0x7e0, 0xf800
  id: 0x31313259 (Y211)
    guid: 59323131-0000-0010-8000-00aa00389b71
    bits per pixel: 6
    number of planes: 3
    type: YUV (packed)
  id: 0x0
    guid: 00000000-0000-0000-0000-000000000000
    bits per pixel: 0
    number of planes: 0
    type: RGB (packed)
    depth: 1
    red, green, blue masks: 0x0, 0x0, 0x0

```

同时注意：列出来的格式(YUV2, YUV12, 等等) 并不总是随着XVdieo的每一次执行而存在。没有它们可能或迷惑有些人。

如果结果看起来是这样:

```

X-Video Extension version 2.2
screen #0
no adaptors present

```

那么您的显卡可以就不支持XVideo功能。

如果您的卡不支持XVideo, 则只是说明您的显示器在满足刷新图像的计算要求上存在更大的困难。尽管显卡和处理器很重要, 您仍然会有个不错的显示效果。此外, 您也可以参考我们提供的文献, 在第7.4.3节中有所介绍。

7.4.1.2 简单直接媒体层

简单直接媒体层(SDL), 原意是做为Microsoft Windows、BeOS 以及UNIX 之间的端口层, 允许跨平台应用发展, 更高效地利用声卡和图形卡。SDL 层可以在低层访问硬件, 有时这样做就比X11 接口层更为高效。

关于SDL, 可以参考`devel/sdl12`。

7.4.1.3 直接图形存取

直接图形存取(Direct Graphics Access) 是一种X11 扩展, 通过它, 应用程序能够绕过X 服务, 并直接修改画面缓存(framebuffer)。由于它依赖一种底层的内存映射来实现其功能, 因此使用它的程序必须以root 身份来执行。

DGA 扩展可以通过`dga(1)` 来完成测试和性能测量。运行`dga` 时, 它将随按键改变现实的颜色。按`q` 退出这个程序。

7.4.2 Ports 和包(Packages) 对视频的解决

这部份主要讨论在FreeBSD Ports 集中提供的可用于视频回放的软件。视频回放在软件发展中是个很活跃的领域, 并且各种不同程序的功能可能与这里的描述不尽相同。

首先要弄清楚的重要一点是在FreeBSD 上使用的视频程序其发展与在Linux 里使用的是一样的。大部份程序都还处在 β 阶段。使用FreeBSD 的包可能面对的问题:

1. 一个应用程序不能播放其它程序制作的文件。
2. 一个应用程序不能播放其自己制作的文件。
3. 不同机上的同样的程序, 各自重新建立(rebuild)了一次, 播放同一个文件结果也会有不同。
4. 一个看起来没什么的过滤器, 如图像尺寸的调整, 也有可能因为一个调整例程的问题变得很不象样。
5. 应用程序频繁地留下垃圾(dumps core)。
6. 没有随port 一起安装的文档可以在网上或者port 的work 目录中找到。

这些程序中许多也体现了“Linux主义”。即, 有些问题来自于(程序)使用的标准库存在于Linux的发行版中, 或者有些是Linux 内核的功能, 而该程序的作者事先所假定的是Linux内核。这些问题并不总是被port 编护人员注意到或处理过, 这也就可能导致如下问题:

1. 使用`proc/cpuinfo`去检测处理器的特性。
2. 滥用线程可能导致一个程序悬挂完成, 而不是完全中止。
3. 软件还不属于FreeBSD Ports集, 而又与其它程序经常地一起使用。

现在, 这些程序的开发人员也已同port 的维护人员进行了联合, 以减少制作port时出错。

7.4.2.1 MPlayer

MPlayer 是近来开发的同时也正迅速发展着的一个视频播放器。**MPlayer** 团队的目标是在Linux 和其它UNIX 系统中的速度和机动性能。在团队的创始人实在受不了当时可用的播放器的性能时，这个计划就开始了。有人也许会说图形接口已经成为新型设计的牺牲品。但是一旦您习惯了命令行选项和按键控制方式，它就能表现得很好。

7.4.2.1.1 创建MPlayer

MPlayer 可以从multimedia/mplayer 找到。**MPlayer** 在联编过程中会进行许多硬件检测，而得到的可执行文件因此将无法移植到其他系统中使用。因此，从ports 完成联编而不是安装预编译的包就很重要。另外，在make 命令行还可以指定许多选项，在Makefile 中有所描述，接下来我们开始联编：

```
# cd /usr/ports/multimedia/mplayer
# make
N - O - T - E

Take a careful look into the Makefile in order
to learn how to tune mplayer towards you personal preferences!
For example,
make WITH_GTK1
builds MPlayer with GTK1-GUI support.
If you want to use the GUI, you can either install
/usr/ports/multimedia/mplayer-skins
or download official skin collections from
http://www.mplayerhq.hu/homepage/dload.html
```

默认的port 选项对于绝大多数用户来说是够用了。不过，如果您需要XviD 编解码器，则必须指定WITH_XVID 这个命令行选项。默认的DVD 设备也可以用WITH_DVD_DEVICE 选项来定义，其默认值是/dev/acd0。

撰写这一章的时候，**MPlayer** port 的联编过程包括了HTML 文档和两个可执行文件，mplayer 和mencoder，后者是一个视频再编码工具。

MPlayer 的HTML 文档提供了丰富的内容。如果读者发现本章中缺少关于视频硬件的一些信息，则**MPlayer** 的文档将是十分详尽的补充。如果您正在找关于UNIX 中的视频支持的资料，您绝对应该花一些时间来阅读**MPlayer** 的文档。

7.4.2.1.2 使用MPlayer

任何**MPlayer** 用户必须在主目录下建立一个叫.mplayer 的子目录。输入下边的内容来建立这个必须的子目录：

```
% cd /usr/ports/multimedia/mplayer
% make install-user
```

在mplayer的手册里列出了它的命令选项。HTML文档里有更为详细的信息。这部份里，我们只是描述了很少的常见应用。

要播放一个文件，如testfile.avi，可以通过各种视频接口当中的某一个去设置-vo 选项：

```
% mplayer -vo xv testfile.avi
```

```
% mplayer -vo sdl testfile.avi
% mplayer -vo x11 testfile.avi
# mplayer -vo dga testfile.avi
# mplayer -vo 'sdl:dga' testfile.avi
```

所有这些选项都是值得一试的，因为它们的性能依赖很多因素，并且都与硬件密切相关。

要播放DVD，需要把testfile.avi改为dvd://N -dvd-device DEVICE。这里N是要播放的节目编号，而DEVICE则是DVD-ROM的设备节点。例如，要播放/dev/dvd的第三个节目：

```
# mplayer -vo xv dvd:///3 -dvd-device /dev/dvd
```

注意：可以在编译MPlayer时，通过WITH_DVD_DEVICE来指定默认的DVD设备。系统内定的默认设备是/dev/acd0。更多细节，请参考port的Makefile。

要停止、暂停、前进等等，可以参考设定的按键---这些可以通过mplayer -h得到或查看手册。

另外，回放的重要选项是：用于全屏模式的-fs -zoom和起辅助完成作用的-framedrop。

为了让mplayer的命令行不是太长，使用者可以通过建立一个文件.mplayer/config来设定如下默认选项：

```
vo=xv
fs=yes
zoom=yes
```

最后，mplayer可以把DVD题目(title)抓取成为.vob文件。为了从DVD中导出第二个题目，请输入：

```
# mplayer -dumpstream -dumpfile out.vob dvd:///2 -dvd-device /dev/dvd
```

输出文件out.vob将是MPEG并且可以被这部份描述的其它“包”利用。

7.4.2.1.3 mencoder

在使用mencoder之前，首先熟悉其HTML文档中所介绍的选项是一个不错的主意。它提供了联机手册，但如果没有HTML文档则帮助不大。有无数种方法来提高视频品质、降低比特率、修改格式，而这些技巧可能会影响性能。下面是几个例子，第一个是简单地复制：

```
% mencoder input.avi -oac copy -ovc copy -o output.avi
```

不正确的命令选项组合可能使生成的文件不能被mplayer播放。因此，如果您只是想抓取文件，一定在mplayer里使用“-dumpfile”。

转换input.avi成为带有MPEG3音频编码(要求audio/lame)的MPEG4编码：

```
% mencoder input.avi -oac mp3lame -lameopts br=192 \
-oac lavc -lavcopts vcodec=mpeg4:vhq -o output.avi
```

这样就产生了可被mplayer和xine播放的输出。

`input.avi` 可以换成 `dvd://1 -dvd-device /dev/dvd` 并以 `root` 的身份来执行，以重新对DVD 节目进行编码。由于您第一次做这样的工作时很可能对结果不太满意，建议您首先把节目复制成文件，然后对它进行操作。

7.4.2.2 xine视频播放器

xine 视频播放器是一个关注范围很广的项目，它不仅看准多合一的视频解决，而且出品了一个可再用的基本库和一个可扩展插件的可执行模块。发行有“包”和port版本-- `multimedia/xine`。

xine 播放器仍然很粗糙，但这很显然与好开头无关。实际上 **xine** 即需要一个快速的带有快速显卡的CPU，也支持XVideo的扩展。图形界面(GUI)可以使用，但很勉强。

到写这章时，还没有可用于播放CSS编码的DVD文件的输入模块随同**xine**一起发行。第三方的建造(builds)里内建有这样的模块，但都不属于FreeBSD Ports 集。

与**MPlayer**相比，**xine** 为用户考虑得更多，但同时，对用户来说也少了很多有条理的控制方式。**xine** 播放器在XVideo接口上做得不错。

默认情况下，播放器**xine**启动的时会使用图形界面。那么就可以使用菜单打开指定的文件：

```
% xine
```

另外，没有图形界面也可以使用如下命令立即打开播放文件：

```
% xine -g -p mymovie.avi
```

7.4.2.3 使用transcode

transcode 这个软件并不是播放器，而是一系列用于对视频和音频文件进行重新编码的工具。通过使用**transcode**，就可以拥有使用带stdin/stdout 接口的命令行工具来合并视频文件，以及修复损坏文件的能力。

在联编multimedia/transcode port 时可以指定大量选项，我们建议使用下面的命令行来构建**transcode**：

```
# make WITH_OPTIMIZED_CFLAGS=yes WITH_LIBA52=yes WITH_LAME=yes WITH_OGG=yes \
WITH_MJPEG=yes -DWITH_XVID=yes
```

对于多数用户而言，前述配置已经足够了。

为了说明**transcode** 的功能，下面的例子展示了如何将DivX 转换为PAL MPEG-1 文件(PAL VCD)：

```
% transcode -i input.avi -V --export_prof vcd-pal -o output_vcd
% mplex -f 1 -o output_vcd.mpg output_vcd.m1v output_vcd.mpa
```

生成的MPEG 文件，`output_vcd.mpg`，可以通过**MPlayer** 来播放。您甚至可以直接将这个文件烧录到CD-R 介质上来创建Video CD，如果希望这样做的话，需要安装multimedia/vcdimager 和sysutils/cdrdao 这两个程序。

transcode 提供了联机手册，但您仍应参考transcode wiki (<http://www.transcoding.org/cgi-bin/transcode>) 以了解更多信息和例子。

7.4.3 进一步了解

FreeBSD里不同的视频软件包正迅速发展。很可能在不久的将来，这里所谈到的问题都将得到解决。同时，有些人想超越FreeBSD的声/像(A/V)能力，那他们就不得不从一些FAQ和指南里学知识，并使用一些不同的应用程序。这里就给这些读者指出一些补充信息。

MPlayer 文档 (<http://www.mplayerhq.hu/DOCS/>)是很技术性的。这些文档可以给那些希望获得关于UNIX视频高级技术的人们提供参考。MPlayer邮件列表很不喜欢没耐心阅读文档的人，如果您发现什么问题想报告给他们，请首先RTFM。

xine HOWTO (http://dvd.sourceforge.net/xine-howto/en_GB/html/howto.html)里边有一章是关于提高性能的，对所有的播放器都很适应。

最后是一些很有前途的程序，读者可以试一下：

- Avifile (<http://avifile.sourceforge.net/>)，它就是multimedia/avifile port。
- Ogle (<http://www.dtek.chalmers.se/groups/dvd/>) 它就是multimedia/ogle port。
- Xtheater (<http://xtheater.sourceforge.net/>)
- multimedia/dvdauthor，一个制作DVD节目的源码开放包。

7.5 安装电视卡

原创: Josef El-Rayes. 改编: Marc Fonvieille.

7.5.1 介绍

电视卡可以让您在您的计算机里观看到无线或有线电视。许多卡是通过RCA或S-video输入接收复合视频，而且有些卡还带有调频广播接收器。

FreeBSD 通过bktr(4)驱动程序，提供了对基于PCI的电视卡的支持，要求这些卡使用的是Brooktree Bt848/849/878/879 或Conexant CN-878/Fusion 878a视频采集芯片。您还要确保这个板上带的有被支持的调谐器，参考bktr(4)手册查看所支持的调谐器列表。

7.5.2 增加驱动程序

要使用您的卡，您就要装载bktr(4)驱动程序。这个可以通过往/boot/loader.conf里边添加下边一行来实现。象这样：

```
bktr_load="YES"
```

另外，您也可以静态地这个支持编译到内核里去，要是这样的话，就把下边几行加到内核配置里去：

```
device bktr
device iicbus
device iicbb
device smbus
```

这些附加的设备驱动程序是必须的，因为卡的各组成部分是能过一根I2C总线相互连接在一起的。然后建立安装新的内核。

一旦这个支持被加到了您的系统里，您须要重启系统。在启动过程中，您的电视卡应该显示为up(启动)，象这样：

```
bktr0: <BrookTree 848A> mem 0xd7000000-0xd7000fff irq 10 at device 10.0 on pci0
iicbb0: <I2C bit-banging driver> on bti2c0
iicbus0: <Philips I2C bus> on iicbb0 master-only
iicbus1: <Philips I2C bus> on iicbb0 master-only
smbus0: <System Management Bus> on bti2c0
bktr0: Pinnacle/Miro TV, Philips SECAM tuner.
```

当然，这些信息可能因您的硬件不同而有所区别。但是您应该能检查那个调制器是否被正确检测到了，可能要忽略一些检测到的同sysctl(8) MIB（管理系统库）和内核配置文件选项一起的参数。例如，如果您想强制使用Philips(飞利浦) SECAM制式的调谐器，您就应把下列行加到内核配置文件里：

```
options OVERRIDE_TUNER=6
```

或者，您直接使用sysctl(8)：

```
# sysctl hw.bt848.tuner=6
```

查看bktr(4)手册和/usr/src/sys/conf/NOTES文件了解更多详细关于可用选项的资料。（如果您在FreeBSD 4.X下，就使用/usr/src/sys/i386/conf/LINT代替/usr/src/sys/conf/NOTES。）

7.5.3 有用的应用程序

要使用您的电视卡，您需要安装下列应用程序之一：

- multimedia/fxvtv提供“窗口电视(TV-in-a-window)”功能和图像/声音/图像采集功能。
- multimedia/xawtv也是一款电视应用程序，功能同fxtv一样。
- misc/alevt解码和显示Videotext/Teletext。
- audio/xmradio，一款用于一些电视卡的调频电台调谐器的程序。
- audio/wmtune，一款用于电台调谐器的便捷的桌面程序。

更多的程序在FreeBSD Ports Collection(Ports 集)里。

7.5.4 问题解决

如果您的电视卡遇到了什么问题，您应该首先检查一下您的视频采集芯片和调谐器是不是真正的被bktr(4)驱动程序支持，并且是不是使用了正确的配置选项。想得到更多支持和关于您的电视卡的各种问题，您可以接触和使用freebsd-multimedia (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-multimedia>) 邮件列表的压缩包。

7.6 图象扫描仪

撰写人 Marc Fonvieille.

7.6.1 介绍

像任何其他现代操作系统一样，FreeBSD 可以使用图像扫描仪。对扫描仪的标准访问是通过 FreeBSD Ports Collection 中的 **SANE** (Scanner Access Now Easy) API 提供的。**SANE** 也会使用一些 FreeBSD 设备驱动来访问扫描仪硬件。

FreeBSD 支持 SCSI 和 USB 扫描仪。在做任何配置之前请确保您的扫描仪被 **SANE** 支持。**SANE** 有一个支持的设备 (<http://sane-project.org/sane-supported-devices.html>) 列表，可以为您提供有关扫描仪的支持情况和状态的信息。`uscaner(4)` 手册页也提供了一个支持的 USB 扫描仪列表。

7.6.2 内核配置

上面提到 SCSI 和 USB 接口都是支持的。取决于您的扫描仪接口，需要不同的设备驱动程序。

7.6.2.1 USB 接口

默认的 **GENERIC** 内核包含了支持 USB 扫描仪需要的设备驱动。如果您决定使用一个定制的内核，确保下面在您的内核配置文件中存在下面这些行：

```
device usb
device uhci
device ohci
device uscaner
```

取决于您主板上的 USB 芯片，您只需要 `device uhci` 或者 `device ohci` 中的一种，但是两个都在内核配置文件中是没有害处的。

如果您不想重新编译内核而且您的内核也不是 **GENERIC** 的，您可以用 `kldload(8)` 命令直接加载 `uscaner(4)` 设备驱动模块：

```
# kldload uscaner
```

要在每次系统启动的时候加载这个模块，添加下面这行到 `/boot/loader.conf` 中：

```
uscaner_load="YES"
```

在用正确的内核重新启动后，或者在加载了需要的模块之后，插上您的 USB 扫描仪。扫描仪会出现在您的系统消息缓存 (`dmesg(8)`) 中，就像这样：

```
uscaner0: EPSON EPSON Scanner, rev 1.10/3.02, addr 2
```

这表明我们的扫描仪正在使用 `/dev/uscaner0` 设备节点。

注意：在 FreeBSD 4.X 上，USB 进程 (`usbd(8)`) 必须运行来检测 USB 设备。要启用它，添加 `usbd_enable="YES"` 到您的 `/etc/rc.conf` 文件中并重新启动。

7.6.2.2 SCSI 接口

如果您的扫描仪是SCSI接口的，重要的是要知道您使用哪种SCSI控制器。取决于所使用的SCSI芯片，您需要调整内核配置文件。GENERIC的内核支持最常用的SCSI控制器。确保阅读NOTES文件(在FreeBSD 4.x下面是LINT)并在您的内核配置文件中添加正确的行。除了SCSI适配器驱动之外，您还需要在内核配置文件中添加如下行：

```
device scbus
device pass
```

一旦完全编译好您的内核，您就可以在启动时的系统消息缓冲中看到这些设备：

```
pass2 at aic0 bus 0 target 2 lun 0
pass2: <AGFA SNAPSCAN 600 1.10> Fixed Scanner SCSI-2 device
pass2: 3.300MB/s transfers
```

如果您的扫描仪没有在系统启动的时候加电，很可能还需要强制手动检测一下，用camcontrol(8)命令执行一次SCSI总线扫描：

```
# camcontrol rescan all
Re-scan of bus 0 was successful
Re-scan of bus 1 was successful
Re-scan of bus 2 was successful
Re-scan of bus 3 was successful
```

然后扫描仪就会出现在SCSI设备列表里：

```
# camcontrol devlist
<IBM DDRS-34560 S97B>          at scbus0 target 5 lun 0 (pass0,da0)
<IBM DDRS-34560 S97B>          at scbus0 target 6 lun 0 (pass1,da1)
<AGFA SNAPSCAN 600 1.10>      at scbus1 target 2 lun 0 (pass3)
<PHILIPS CDD3610 CD-R/RW 1.00> at scbus2 target 0 lun 0 (pass2,cd0)
```

有关SCSI设备的更多细节，可以查看scsi(4)和camcontrol(8)手册页。

7.6.3 SANE 配置

SANE系统分为两部分：后端(graphics/sane-backends)和前端(graphics/sane-frontends)。后端部分提供到扫描仪自身的访问。SANE的支持设备(<http://sane-project.org/sane-supported-devices.html>)列表详细说明了哪一个后端可以支持您的图象扫描仪。如果您想使用您的设备，就必须为您的扫描仪选定正确的后端。前端部分提供图形化的扫描界面(xscanimage)。

要做的第一件事就是安装graphics/sane-backends port 或者package。然后，使用sane-find-scanner命令来检查SANE系统做的扫描仪检测：

```
# sane-find-scanner -q
found SCSI scanner "AGFA SNAPSCAN 600 1.10" at /dev/pass3
```

输出显示了扫描仪的接口类型和扫描仪连接到系统上的设备节点。生产厂家和产品型号可能没有显示，不过不重要。

注意: 一些USB 扫描仪需要您加载固件，后端的手册页中有这方面的解释。您也应该阅读sane-find-scanner(1)和sane(7)手册页。

现在我们需要检查扫描仪是否可以被扫描前端识别。默认情况下，**SANE** 后端自带一个叫做scanimage(1)的命令行工具。这个命令允许您列出设备以及从命令行执行图片扫描。-L 选项用来列出扫描仪设备：

```
# scanimage -L
device 'snapscan:/dev/pass3' is a AGFA SNAPSCAN 600 flatbed scanner
```

如果没有输出任何信息，或提示没有识别到扫描仪，则说明scanimage(1)无法识别它。如果发生这种情况，您就需要修改扫描仪支持后端的配置文件，并定义所使用的扫描设备。/usr/local/etc/sane.d/ 目录中包含了所有的后端配置文件。这类识别问题经常会在某些USB 扫描仪上发生。

例如，对于在第7.6.2.1 节中所使用的USB 扫描仪，sane-find-scanner 会给出下面的信息：

```
# sane-find-scanner -q
found USB scanner (UNKNOWN vendor and product) at device /dev/usb/lp0
```

扫描仪被正确的探测到了，它使用USB 接口，连接在/dev/usb/lp0 设备节点上。我们现在可以检查看看扫描仪是否被正确的识别：

```
# scanimage -L

No scanners were identified. If you were expecting something different,
check that the scanner is plugged in, turned on and detected by the
sane-find-scanner tool (if appropriate). Please read the documentation
which came with this software (README, FAQ, manpages).
```

既然扫描仪没有被识别，我们就需要编辑/usr/local/etc/sane.d/epson.conf 文件。所用的扫描仪型号是EPSON Perfection® 1650，这样我们知道扫描仪应使用epson 后端。确保阅读后端配置文件中的帮助注释。改动非常简单：注释掉导致您的扫描仪使用错误接口的所有行(在我们这种情况下，我们将注释掉从scsi 开始的所有行，因为我们的扫描仪使用USB 接口)，然后在文件的结尾添加指定的接口和所用的设备节点。这种情况下，我们添加下面这行：

```
usb /dev/usb/lp0
```

请确保阅读后端配置文件提供的注释以及后端手册页了解更多细节，并使用正确的语法。我们现在可以检验扫描仪是否被识别到了：

```
# scanimage -L
device 'epson:/dev/usb/lp0' is a Epson GT-8200 flatbed scanner
```

我们的USB 扫描仪被识别到了。如果商标和型号不匹配也不重要。相关的关键一条是'epson:/dev/usb/lp0' 字段，这个给了我们正确地后端名称和正确的设备节点。

一旦scanimage -L 命令可以看到扫描仪，配置就完成了。设备现在准备好等待扫描了。

scanimage(1) 允许我们从命令行执行图片扫描，相比之下使用图形用户界面来执行图片扫描会更好。**SANE** 提供了一个简单但实用的图形界面：**xscanimage** (graphics/sane-frontends)。

Xsane (graphics/xsane)是另一个流行的图形扫描前端。这个前端提供了一些高级特性，比如多样的扫描模式(photocopy, fax, 等。), 色彩校正, 批量扫描, 等等。这两个程序都可以作为**GIMP**的插件使用。

7.6.4 授予其他用户扫描权限

前面所有的操作都是用root 权限来完成的。You may however, need 然而您可能需要让其他的用户也可以访问扫描仪。用户需要有扫描仪所用的设备节点的读和写权限。比如, 我们的USB 扫描仪使用设备节点/dev/usb/lp/lp0, 这个节点属于operator 组。将用户joe 添加到operator 组会允许他使用扫描仪:

```
# pw groupmod operator -m joe
```

要了解更多细节, 请阅读pw(8) 联机手册。此外, 还需要为/dev/usb/lp/lp0 设备节点设置正确的写入权限(0660 或0664), 因为默认情况下, operator 组只能读这个设备节点。这项工作可以通过在/etc/devfs.rules 文件中添加如下设置来自东完成:

```
[system=5]
add path usb/lp/lp0 mode 660
```

随后您还需要在/etc/rc.conf 中添加下面的内容并重新启动:

```
devfs_system_ruleset="system"
```

关于这些配置的进一步细节请参考联机手册devfs(8)。对于FreeBSD 4.X, 默认情况下operator 组已经拥有对/dev/usb/lp/lp0 的读和写权限。

注意: 当然, 考虑安全的原因, 在您将用户添加到任何组, 尤其是operator 组时, 都应三思而后行。

第8章

配置FreeBSD的内核

Updated and restructured by Jim Mock. Originally contributed by Jake Hamby.

8.1 概述

内核是FreeBSD操作系统的核心。它负责管理内存、执行安全控制、网络、磁盘访问等等。尽管FreeBSD可以动态修改的现在已经越来越多，但有时您还是需要重新配置和编译您的内核。

读完这章，您将了解：

- 为什么需要建立定制的内核。
- 如何编写内核配置文件，或修改已存在的配置文件。
- 如何使用内核配置文件创建和联编新的内核。
- 如何安装新内核。
- 如何在/dev中创建设备节点。
- 如何出现问题怎么办。

这一章给出的命令应该以root身份执行，否则可能会不成功。

8.2 为什么需要建立定制的内核？

过去，FreeBSD采用称作“单片式”的内核。这句话的意思是说内核是一个大的程序，支持固定的设备，如果您希望改变内核的行为则必须编译一个新的，并重新启动计算机来引导它。

今天，FreeBSD已经迅速地转移到了一个新的模型，其重要特征是内核功能可以由能够根据需要动态加载和卸载的模块来提供。这是的内核能够迅速地适应硬件的调整(例如笔记本电脑的PCMICA)，或为内核增加在最初编译它时所不具备的新的功能。这一模式成为模块化内核。

尽管如此，一些功能仍然需要静态地连编进内核。一些情况是因为这些功能于内核的结合十分紧密，而不可能将它们做成可以动态加载的。另一种情况是因为没有人有时间来编写实现那个功能的可以动态加载的内核模块。

建造定制的内核是几乎每一个BSD用户所必须经历的一关。尽管这项工作可能比较耗时，但它能够为使用FreeBSD系统带来很多好处。与必须支持大量各式硬件的GENERIC内核不同，定制的内核可以只包含对于您的PC硬件的支持。这有很多好处，例如：

- 更快地启动。因为内核只需要检测您系统上的硬件，启动时所花费的时间将大大缩短。
- 使用更少的内存。定制的内核通常会比GENERIC内核使用更少的内存，由于内核必须时刻处于物理内存中，因此这就显得更加重要。基于这样的原因，对于内存较小的系统来说，定制内核将发挥更大的作用。
- 支持更多的硬件。定制的内核允许您增加类似声卡这样的GENERIC内核没有提供内建支持的硬件。

8.3 建立并安装一个定制的内核

首先对内核构建目录做一个快速的浏览。这里所提到的所有目录都在`/usr/src/sys`目录中；也可以通过`/sys`来访问它。这里的众多子目录包含了内核的不同部分，但对我们所要完成的任务最重要的目录是`arch/conf`，您将在这里编辑定制的内核配置；以及`compile`，编译过程中的文件将放置在这里。`arch`表示`i386`、`alpha`、`amd64`、`ia64`、`powerpc`、`sparc64`，或`pc98`（在日本比较流行的另一种PC硬件开发分支）。在特定硬件架构目录中的文件只和特定的硬件有关；而其余代码则是与机器无关的，则所有已经或将要移植并运行FreeBSD的平台上都共享这些代码。文件目录是按照逻辑组织的，所支持的硬件设备、文件系统，以及可选的组件通常都在它们自己的目录中。5.X版之前的FreeBSD只支持`i386`、`alpha`和`pc98`这三种硬件架构。

这一章提供的例子假定您使用`i386`架构的计算机。如果您的情况不是这样，只需对目录名作相应的调整即可。

注意：如果您的系统中没有`/usr/src/sys`这样一个目录，则说明没有安装内核源代码。安装它最简单的方法是通过以`root`身份运行`sysinstall`（对于FreeBSD 5.2之前的版本，则是`/stand/sysinstall`），选择`Configure`，然后`Distributions`，然后`src`，`sys`。如果您不喜欢`sysinstall`并且可以使用“官方的”FreeBSD CDROM，则也可以通过命令行来安装：

```
# mount /cdrom
# mkdir -p /usr/src/sys
# ln -s /usr/src/sys /sys
# cat /cdrom/src/sys.[a-d]* | tar -xvzf -
```

接下来，进入`arch/conf`目录下面，复制`GENERIC`配置文件，并给这个文件起一个容易辨认的名称，它就是您的内核名称。例如：

```
# cd /usr/src/sys/i386/conf
# cp GENERIC MYKERNEL
```

通常，这个名称是大写的，如果您正维护着多台不同硬件的FreeBSD机器，以您机器的域名来命名是非常好的主意。我们把它命名为`MYKERNEL`就是这个原因。

提示：将您的内核配置文件直接保存在`/usr/src`可能不是一个好主意。如果您遇到问题，删掉`/usr/src`并重新开始很可能是一个诱人的选择。一旦开始做这件事，您可能几秒钟之后才会意识到您同时会删除定制的内核配置文件。另外，也不要直接编辑`GENERIC`，因为下次您更新代码时它会被覆盖，而您的修改也就随之丢失了。

您也可以考虑把内核配置文件放到别的地方，然后再到`i386`目录中创建一个指向它的符号链接。

例如：

```
# cd /usr/src/sys/i386/conf
# mkdir /root/kernels
# cp GENERIC /root/kernels/MYKERNEL
# ln -s /root/kernels/MYKERNEL
```

注意：必须以`root`身份执行这些和接下来命令，否则就会得到`permission denied`的错误提示。

现在就可以用您喜欢的文本编辑器来编辑MYKERNEL了。如果您刚刚开始使用FreeBSD，唯一可用的编辑器很可能是vi，它的使用比较复杂，限于篇幅，这里不予介绍，您可以在参考书目一章中找到很多相关书籍。不过，FreeBSD也提供了一个更好用的编辑器，它叫做ee，对于新手来说，这很可能是一个不错的选择。您可以修改配置文件中的注释以反映您的配置，或其他与GENERIC不同的地方。

如果您在SunOS或者其他BSD系统下定制过内核，那这个文件中的绝大部分将对您非常熟悉。如果您使用的是诸如DOS这样的系统，那GENERIC配置文件看起来就非常困难，所以在下面的配置文件章节将慢慢地、仔细地进行介绍。

注意：如果您和FreeBSD project进行了代码同步，则一定要在进行任何更新之前查看/usr/src/UPDATING。这个文件中描述了更新过的代码中出现的重大问题或需要注意的地方。/usr/src/UPDATING总是和您的FreeBSD源代码对应，因此能够提供比手册更具时效性的新内容。

现在应该编译内核的源代码了。一共有两种方法来完成这项工作，使用哪一种取决于您为什么要重新编译内核，以及所运行的FreeBSD版本。

- 如果您只安装内核源代码，使用方法1。
- 如果您正运行FreeBSD 4.0以前的版本，而且您不是准备使用make buildworld来升级到FreeBSD 4.0或更高版本的话，则应使用方法1。
- 如果您在没有升级源代码的情况下编译一个新内核（也许您只想为内核添加一个新的选项，如IPFIREWALL），可以使用任何一种方法。
- 如果您打算把重新构建内核作为make buildworld过程的一部分来进行，则应使用方法2。

如果从上次成功地完成buildworld-installworld以来您还没有升级过代码(也就是没有运行CVSup、CTM，或使用anoncvs)，则可以放心使用config、make depend、make、make install。

方法1. 用“传统”方法建立一个内核

1. 运行config(8)来产生内核源代码。

```
# /usr/sbin/config MYKERNEL
```

2. 进入编译内核的目录。config(8)将在像上面一样显示执行它所在的目录的名字。

```
# cd ../compile/MYKERNEL
```

对于FreeBSD 5.0以及更早的版本，使用下面的形式：

```
# cd ../../compile/MYKERNEL
```

3. 编译内核。

```
# make depend
```

```
# make
```

4. 安装新内核。

```
# make install
```

方法2. 用“新的”方法建立一个内核

1. 切换到/usr/src目录。

```
# cd /usr/src
```

2. 编译内核。

```
# make buildkernel KERNCONF=MYKERNEL
```

3. 安装新内核。

```
# make installkernel KERNCONF=MYKERNEL
```

注意: 使用这种方法构建内核，需要完整的源代码。如果您只安装了内核的源代码，就只能使用前面所介绍的传统方法了。

提示: 默认情况下，在联编您所定制的内核时，**全部** 内核模块也会同时参与构建。如果您希望更快地升级内核，或者只希望联编您所需要的模块，则应在联编之前编辑/etc/make.conf:

```
MODULES_OVERRIDE = linux acpi sound/sound sound/driver/ds1 ntfs
```

这个变量的内容是所希望构建的模块列表。如果希望了解更多与构建内核有关的变量，请参见make.conf(5) 联机手册。

新内核将会被复制到/boot/kernel 目录中成为/boot/kernel/kernel 而旧的则被移到/boot/kernel.old/kernel。现在关闭系统，然后用新的内核启动计算机。如果出现问题，后面的一些故障排除方法 将帮您摆脱困境。如果您的内核无法启动，请参考那一节。

注意: 在FreeBSD 4.X 以及更早的版本中，内核被安装到/kernel 而模块则放到/modules，旧的内核则被备份到/kernel.old。其他与启动过程相关的文件，如loader(8) 以及配置则放在/boot。第三方或定制的模块也可以放在/modules，不过应该注意保持模块和内核的同步时很重要的，否则会导致不稳定和错误。

注意: 如果添加了新设备(例如声卡) 并在运行FreeBSD 4.X 或更早的版本，则可能好需要在/dev 目录中添加它们的设备节点之后才能使用。欲了解详情，请参考本章稍后的制作设备节点 一节。

8.4 配置文件

Updated for FreeBSD 5.X by Joel Dahl.

配置文件的格式是非常简单的。每一行都包括一个关键词，以及一个或多个参数。实际上，绝大多数行都只包括一个参数。在# 之后的内容会被认为是注释而忽略掉。接下来几节，将以GENERIC 中的顺序介绍所有关键字。如果需要与平台有关的选项和设备的详细列表，请参考与GENERIC 在同一个目录中的那个NOTES，而平台无关的选项，则可以在/usr/src/sys/conf/NOTES 找到。

注意: NOTES 在FreeBSD 4.X 中并不存在。作为替代，请参考LINT 文件来获得关于GENERIC 中的选项和设备详细介绍。LINT 在4.X 中完成了两项使命：为构建定制内核提供可选的选项，以及提供尽可能多的调整为非默认值的选项。这么做背后的原因是这种配置文件能够帮助(并且仍然能) 测试新代码以及现有代码的修改是否会造成与内核其他部分的冲突。然而，内核配置的架构在5.X 中经历了巨大的变化；其中的一个例子是设备驱动选项被移到

了hints 中，从而可以随时修改并在启动时动态加载，而LINT 不能再包含这些hints 了。由于这个以及许多其他原因，决定将LINT 改名为NOTES，而保留它的主要是为了前面所说的第一个原因：给出可用的选项，为用户提供方便。

在FreeBSD 5.X 和以后的版本中您仍然可以通过下面的命令生成LINT 文件：

```
# cd /usr/src/sys/i386/conf && make LINT
```

下面是一个GENERIC 内核配置文件的例子，它包括了一些需要解释的注释。这个例子应该和您复制的/usr/src/sys/i386/conf/GENERIC 非常接近。

```
machine i386
```

这是机器的架构，他只能是alpha, amd64, i386, ia64, pc98, powerpc, 或sparc64 中的一种。

```
cpu          I486_CPU
cpu          I586_CPU
cpu          I686_CPU
```

上面的选项指定了您系统中所使用的CPU 类型。您可以使用多个CPU 类型(例如，您不确定是应该指定I586_CPU 或I686_CPU)。然而对于定制的内核，最好能够只指定您使用的那种CPU。如果您对于自己使用的CPU 类型没有把握，可以通过查看/var/run/dmesg.boot 中的启动信息来了解。

在FreeBSD的内核里面仍然支持I386_CPU，但是在-STABLE和-CURRENT里面缺省已经被禁用了。这就意味着安装FreeBSD在386-class的cpu，一般有下面几种情况：

- 安装一个老的FreeBSD release并且按照第8.3 节从源码重建系统。
- 在一个新的机器上构建用户和内核程序，然后用已经编译好的/usr/obj下的文件安装到386的机器上(详细情况看第21.5 节)。
- 定制您自己的FreeBSD 发行版本，其中的安装光盘包含I386_CPU 支持。

第一种情况可能是最容易的，但您需要大量的磁盘空间，而386-级别拥有这种配置的计算机可能很难找到。

```
ident          GENERIC
```

这是内核的名字。您应该取一个自己的名字，例如取名叫MYKERNEL，如果您一直在按照前面的说明做的话。您放在ident 后面的字符串在启动内核时会显示出来，因此如果希望能够容易区分常用的内核和刚刚定制的内核，就应该采取不同的名字(例如，您想定制一个试验性的内核)。

```
#To statically compile in device wiring instead of /boot/device.hints
#hints          "GENERIC.hints"          # Default places to look for devices.
```

在FreeBSD 5.X和更新的版本里面，device.hints(5)被用来配置设备驱动选项。在启动的时候loader(8)将会检查缺省位置/boot/devicehints。使用hints选项您就可以把这些hints静态编译进内核。这样就没有必要在/boot下创建devicehints。

```
#makeoptions    DEBUG=-g          # Build kernel with gdb(1) debug symbols
```

一般的FreeBSD 构建过程并不包括调试信息，在构建内核时，绝大多数符号会在最终的内核连接之后剔除出去，以节省安装时所需的空間。如果您打算测试-CURRENT 分支的内核，或开发您自己的FreeBSD

内核功能，则可能会需要去掉这一行的注释。这将启用 `-g` 选项，它会在 `gcc(1)` 中打开调试信息。如果您使用“传统”方法来构建内核，也可以通过 `config(8)` 的 `-g` 选项来达到同样的目的(参见第8.3节 了解进一步的信息)。

```
options          SCHED_4BSD          # 4BSD scheduler
```

这是FreeBSD的传统调度器。取决于您系统的工作负荷，使用新的ULE调度器通常可以获得更好的性能。它是专门为FreeBSD在SMP上运行而设计的调度器，但在UP系统上也能工作得很好。如果您想试验这个功能，则应把配置文件中的 `SCHED_4BSD` 改为 `SCHED_ULE`。

```
options          INET                # InterNETworking
```

网络支持，即使您不打算连网，也请保留它，大部分的程序至少需要回环网络（就是和本机进行网络连接），所以强烈要求保留它。

```
options          INET6               # IPv6 communications protocols
```

这将打开IPv6连接协议。

```
options          FFS                 # Berkeley Fast Filesystem
```

这是最基本的硬盘文件系统，如果打算从本地硬盘启动，请保留它。

```
options          SOFTUPDATES         # Enable FFS Soft Updates support
```

这个选项会启用内核中的Soft Updates支持，它会显著地提高磁盘的写入速度。尽管这项功能是由内核直接提供的，但仍然需要在每个磁盘上启用它。请检查 `mount(8)` 的输出，以了解您系统中的磁盘上是否已经启用了Soft Updates。如果没有看到 `soft-updates` 选项，则需要使用 `tunefs(8)` (对于暨存系统) 或 `newfs(8)` (对于新系统) 命令来激活它。

```
options          UFS_ACL             # Support for access control lists
```

这个选项只能在FreeBSD 5.X和更高版本中使用，它将启用内核中的访问控制表的支持。这依赖于扩展属性以及UFS2，以及在第14.12节中所介绍的那些特性。ACL默认是启用的，并且如果已经在文件系统上使用了这一特性，就不应再关掉它，因为这会去掉文件的访问控制表，并以不可预期的方式改变受保护的文件的访问方式。

```
options          UFS_DIRHASH         # Improve performance on big directories
```

通过使用额外的内存，这个选项可以加速在大目录上的磁盘操作。您应该在大型服务器和频繁使用的工作站上打开这个选项，而在磁盘操作不是很重要的小型系统上关闭它，比如防火墙。

```
options          MD_ROOT             # MD is a potential root device
```

这个选项将打开以基于内存的虚拟磁盘作为根设备的支持。

```
options          NFSCLIENT          # Network Filesystem Client
```

```
options          NFSSERVER           # Network Filesystem Server
```

```
options          NFS_ROOT            # NFS usable as /, requires NFSCLIENT
```

网络文件系统。如果您不打算通过TCP/IP挂接UNIX文件服务器的分区，就可以注释掉它。

```
options          MSDOSFS             # MSDOS Filesystem
```

MS-DOS 文件系统。只要您不打算在启动时挂接由DOS 格式化的硬盘分区，就可以把它注释掉。如前面所介绍的那样，在您第一次挂接DOS 分区时，内核会自动加载需要的模块。此外，`emulators/mtools` 软件提供了一个很方便的功能，通过它您可以直接访问DOS 软盘而无需挂接或卸下它们(而且也完全不需要MSDOSFS)。

```
options          CD9660          # ISO 9660 Filesystem
```

用于CDROM 的ISO 9660 文件系统。如果没有CDROM 驱动器或很少挂接光盘数据(因为在首次使用数据CD 时会自动加载)，就可以把它注释掉。音乐CD 并不需要这个选项。

```
options          PROCFS          # Process filesystem
```

进程文件系统。这是一个挂接在`/proc` 的一个“伪装的”文件系统，允许类似`ps(1)` 这样的程序给出正在运行的进程的更多信息。在FreeBSD 5.X 和更高版本中，绝大多数情况下都不再需要PROCFS，因为绝大多数调试和监视工具都已经进行了修改，不再需要PROCFS：与FreeBSD 4.X 不同，新安装的FreeBSD 5.X 默认情况下并不挂接它。此外，6.X-CURRENT 内核在使用PROCFS 时还必须加入PSEUDofs 的支持：

```
options          PSEUDofs        # Pseudo-filesystem framework
```

PSEUDofs 在FreeBSD 4.X 上不可用。

```
options          GEOM_GPT        # GUID Partition Tables.
```

这个选项提供了在一个磁盘上使用大量的分区的能力。

```
options          COMPAT_43       # Compatible with BSD 4.3 [KEEP THIS!]
```

使系统兼容4.3BSD。不要去掉这一行，不然有些程序将无法正常运行。

```
options          COMPAT_FREEBSD4 # Compatible with FreeBSD4
```

为了支持在旧版本的FreeBSD下编译的程序，该选项在FreeBSD 5.X i386和Alpha systems下需要打开。最好在所有的i386和Alpha systems下打开这个选项，因为可能要运行老应用程序。在5.X才开始支持的平台，比如ia64和Sparc64®，就不需要这个选项。

```
options          SCSI_DELAY=15000 # Delay (in ms) before probing SCSI
```

这将让内核在探测每个SCSI 设备之前等待15 秒。如果您只有IDE 硬盘驱动器，则可以不管它，反之您可能会想降低这个数值，可能减少到5 秒，以加速启动过程。当然，如果您这么做之后FreeBSD 在识别您的SCSI 设备时遇到问题，则您还需要再把它改回去。

```
options          KTRACE          # ktrace(1) support
```

这个选项打开内核进程跟踪，在调试时很有用。

```
options          SYSVSHM         # SYSV-style shared memory
```

提供System V共享内存(SHM)的支持，最常用到SHM的应该是X Window的XSHM延伸，不少绘图相关程序会自动使用SHM来提供额外的速度。如果您要使用X Window，您最好加入这个选项。

```
options          SYSVMSG         # SYSV-style message queues
```

支持System V 消息。这只会在内核中增加数百字节的空间占用。

```
options          SYSVSEM          # SYSV-style semaphores
```

支持System V 信号量，不常用到，但只在kernel中占用几百个字节的空间。

注意: `ipcs(1)` 命令的 `-p` 选项可以显示出任何用到这些System V 机制的进程。

```
options          _KPOSIX_PRIORITY_SCHEDULING # POSIX P1003_1B real-time extensions
```

在1993年POSIX®添加的实时扩展。在Ports Collection 中某些应用程序会用到这些（比如StarOffice）。

```
options          KBD_INSTALL_CDEV # install a CDEV entry in /dev
```

这个选项与键盘有关。它在/dev 中安装一个CDEV 项。

```
options          AHC_REG_PRETTY_PRINT      # Print register bitfields in debug
                                                    # output. Adds ~128k to driver.
```

```
options          AHD_REG_PRETTY_PRINT      # Print register bitfields in debug
                                                    # output. Adds ~215k to driver.
```

这个选项主要用于帮助调试，它能够给出更容易阅读的寄存器数值。

```
options          ADAPTIVE_GIANT           # Giant mutex is adaptive.
```

内核全局锁(Giant)是一种互斥机制(休眠互斥体)的名字，它用于保护许多内核资源。现在，这已经成为了一种无法接受的性能瓶颈，它已经被越来越多地使用保护单个资源的锁代替。ADAPTIVE_GIANT 选项将使得内核全局锁作为一种自适应自旋锁。这意味着，当有线程希望锁住内核全局锁互斥体，但互斥体已经被另一个CPU 上的线程锁住的时候，它将继续运行，直到那个线程释放锁为止。一般情况下，另一个线程将进入休眠状态并等待下一次调度。如果您不确定是否应该这样做的话，一般应该打开它。

```
device          apic                  # I/O APIC
```

apic 设备将启用使用I/O APIC 作为中断发送设备的能力。apic 设备可以被UP 和SMP 内核使用，但SMP 内核必须使用它。要支持多处理器，还需要加上options SMP。

```
device          isa
```

所有为FreeBSD 所支持的PC 都需要这个设置，即使没有ISA 插槽也是一样。如果您使用IBM PS/2 (微通道架构) 的计算机，FreeBSD 目前只能提供有限的支持。要了解关于MCA 支持的详情，请参考/usr/src/sys/i386/conf/NOTES。

```
device          eisa
```

如果您的主机板上有EISA总线，加入这个设置。使用这个选项可以自动扫描并设置所有连接在EISA总线上的设备。

```
device          pci
```

如果您的主板有PCI总线，就加入这个选项。使用这个选项可以自动扫描PCI卡，并在PCI到ISA之间建立通路。

```
# Floppy drives
```

```
device      fdc
```

这是软驱控制器。

```
# ATA and ATAPI devices
```

```
device      ata
```

这个驱动器支持所有ATA和ATAPI设备。您只要在内核中加入`device ata`选项，就可以让内核支持现代计算机上的所有PCI ATA/ATAPI设备。

```
device      atadisk          # ATA disk drives
```

这个是ATAPI 磁盘驱动器所必须的。

```
device      ataraid          # ATA RAID drives
```

这个选项需要`device ata`，它用于ATA RAID 驱动。

```
device      atapicd          # ATAPI CDRom drives
```

这个是ATAPI CDRom驱动器所必须的。

```
device      atapifd          # ATAPI floppy drives
```

这个是ATAPI 磁盘驱动器所必须的。

```
device      atapist          # ATAPI tape drives
```

这个是ATAPI 磁带机驱动器所必须的。

```
options     ATA_STATIC_ID    # Static device numbering
```

这指定对控制器使用其静态的编号；如果没有这个选项，则会动态地分配设备的编号。

```
# SCSI Controllers
```

```
device      ahb              # EISA AHA1742 family
device      ahc              # AHA2940 and onboard AIC7xxx devices
device      ahd              # AHA39320/29320 and onboard AIC79xx devices
device      amd              # AMD 53C974 (Teckram DC-390(T))
device      isp              # Qlogic family
device      mpt              # LSI-Logic MPT-Fusion
#device      ncr              # NCR/Symbios Logic
device      sym              # NCR/Symbios Logic (newer chipsets)
device      trm              # Tekram DC395U/UW/F DC315U adapters
```

```
device      adv              # Advansys SCSI adapters
device      adw              # Advansys wide SCSI adapters
device      aha              # Adaptec 154x SCSI adapters
device      aic              # Adaptec 15[012]x SCSI adapters, AIC-6[23]60.
device      bt               # Buslogic/Mylex MultiMaster SCSI adapters
```

```
device      ncv              # NCR 53C500
device      nsp              # Workbit Ninja SCSI-3
device      stg              # TMC 18C30/18C50
```


SCSI控制器。可以注释掉您系统中没有的设备。如果您只有IDE设备，您可以把这些一起删掉。

```
# SCSI peripherals
device      scbus      # SCSI bus (required for SCSI)
device      ch          # SCSI media changers
device      da          # Direct Access (disks)
device      sa          # Sequential Access (tape etc)
device      cd          # CD
device      pass        # Passthrough device (direct SCSI access)
device      ses          # SCSI Environmental Services (and SAF-TE)
```

SSCSI外围设备。也可以像上面一样操作。

注意: 目前系统提供的USB umass(4) 以及少量其它驱动使用了SCSI 子系统，尽管它们并不是真的SCSI 设备。因此，如果在内核配置使用了这类驱动程序，请务必不要删除SCSI 支持。

```
# RAID controllers interfaced to the SCSI subsystem
device      amr          # AMI MegaRAID
device      arcmsr       # Areca SATA II RAID
device      asr          # DPT SmartRAID V, VI and Adaptec SCSI RAID
device      ciss         # Compaq Smart RAID 5*
device      dpt          # DPT Smartcache III, IV - See NOTES for options
device      hptmv        # Highpoint RocketRAID 182x
device      iir          # Intel Integrated RAID
device      ips          # IBM (Adaptec) ServeRAID
device      mly          # Mylex AcceleRAID/extremeRAID
device      twa          # 3ware 9000 series PATA/SATA RAID

# RAID controllers
device      aac          # Adaptec FSA RAID
device      aacp         # SCSI passthrough for aac (requires CAM)
device      ida          # Compaq Smart RAID
device      mlx          # Mylex DAC960 family
device      pst          # Promise Supertrak SX6000
device      twe          # 3ware ATA RAID
```

支持RAID控制器。如果您没有这些，可以把它们注释掉或是删掉。

```
# atkbdc0 controls both the keyboard and the PS/2 mouse
device      atkbdc       # AT keyboard controller
```

键盘控制器 (atkbdc) 提供AT键盘输入以及PS/2指针设备的I/O服务。键盘驱动程序 (atkbd) 与PS/2鼠标驱动程序 (psm) 需要这个控制器，所以不要删除它。

```
device      atkbd        # AT keyboard
```

atkbd驱动程序，与atkbdc控制器一起使用，提供连接到AT键盘控制器的AT 84键盘与AT加强型键盘的访问服务。

```
device      psm          # PS/2 mouse
```

如果您的鼠标连接到PS/2鼠标端口，就使用这个设备驱动程序。

```
device          vga          # VGA video card driver
```

显卡驱动。

```
# splash screen/screen saver
```

```
device          splash      # Splash screen and screen saver support
```

启动时出现了splash画面！屏幕保护程序也需要它。在FreeBSD 4.X 中，应写作pseudo-device splash。

```
# syscons is the default console driver, resembling an SCO console
```

```
device          sc
```

sc 是默认的控制台驱动程序，类似SCO控制台。由于绝大部分全屏幕程序都通过类似termcap这样的终端数据库函数库访问控制台，因此无论您使用这个或与VT220兼容的vt都没有什么关系。如果您在运行这种控制台时使用全屏幕程序时发生问题，请在登录之后将TERM变量设置为scoansi。

```
# Enable this for the pcvt (VT220 compatible) console driver
```

```
#device          vt
```

```
#options          XSERVER          # support for X server on a vt console
```

```
#options          FAT_CURSOR      # start with block cursor
```

这是一个兼容VT220的控制台驱动，它同时能够向下兼容VT100/102。在同sc硬件不兼容的一些笔记本上它能够运行的很好。当然，登录系统时请把TERM变量设置为vt100或vt220。此驱动在连接网络上大量不同的机器时也被证明非常有用，因为此时termcap或terminfo通常没有可用的sc设备——而vt100则几乎每种平台都支持。

```
device          agp
```

如果您的机器使用AGP卡，请把上面一行加入配置。这将启用AGP，以及某些卡上的AGP GART支持。

```
# Floating point support - do not disable.
```

```
device          npx
```

npx是FreeBSD中浮点运算单元的接口，用于支持硬件的浮点运算协处理器，以及软件仿真程序。这个设置不是可有可无的。

```
# 电源管理支持 (参见 NOTES 了解更多选项)
```

```
#device          apm
```

高级电源管理支持。对笔记本有用，不过在FreeBSD 5.X和更高版本中的GENERIC里默认禁用。

```
# 增加 i8254 的 挂起/恢复 支持。
```

```
device          pmtimer
```

用于电源管理事件，例如APM和ACPI的时钟设备驱动。

```
# PCCARD (PCMCIA) support
```

```
# PCMCIA and cardbus bridge support
```

```
device          cbb          # cardbus (yenta) bridge
```

```
device          pccard        # PC Card (16-bit) bus
```

```
device          cardbus       # CardBus (32-bit) bus
```

PCMCIA支持。如果您使用膝上型计算机，您需要这个。

```
# Serial (COM) ports
device          sio          # 8250, 16[45]50 based serial ports
```

这些串口在MS-DOS/Windows 的世界中称为COM 口。

注意: 如果使用内置式的调制解调器，并占用COM4 而您另有一个串口在COM2，则必须把调制解调器的IRQ 改为2 (由于晦涩的技术原因，IRQ2 = IRQ 9) 才能够在FreeBSD 中访问它。如果有多口的串口卡，请参考sio(4) 以了解需要在/boot/device.hints 中进行的设置。某些显卡(特别是基于S3 芯片的卡) 使用形如0x*2e8 的IO 地址，而许多廉价的串口卡不能够正确地对16-位IO 地址空间进行解码，因此它们会产生冲突，并造成COM4 实际上无法使用。

每一个串口都需要有一个唯一的IRQ (除非您使用支持中断分享的串口卡)，因此默认的COM3 和COM4 IRQ 是不能使用的。

```
# Parallel port
device          ppc
```

ISA-bus并行接口。

```
device          ppbus        # Parallel port bus (required)
```

提供并行总线的支持。

```
device          lpt          # Printer
```

提供并口打印机的支持。

注意: 要使用并口打印机，就必须同时加入上面三行设置。

```
device          plip          # TCP/IP over parallel
```

这是针对并行网络接口的驱动器。

```
device          ppi          # Parallel port interface device
```

普通用途的I/O (“geek port”) + IEEE1284 I/O.

```
#device          vpo          # Requires scbus and da
```

这是针对Iomega Zip驱动器的。它要求scbus和da的支持。最好的执行效果是工作在EPP 1.9模式。

```
#device          puc
```

如果您有由puc(4) 支持的“哑” 串行或并行PCI 卡，则应去掉这一行的注释。

```
# PCI Ethernet NICs.
device          de            # DEC/Intel DC21x4x ( “Tulip” )
device          em            # Intel PRO/1000 adapter Gigabit Ethernet Card
device          ixgb          # Intel PRO/10GbE Ethernet Card
```

```
device      txp      # 3Com 3cR990 ( "Typhoon" )
device      vx       # 3Com 3c590, 3c595 ( "Vortex" )
```

多种PCI网卡驱动器。注释或删除您系统中没有的设备。

```
# PCI Ethernet NICs that use the common MII bus controller code.
# NOTE: Be sure to keep the 'device miibus' line in order to use these NICs!
device      miibus   # MII bus support
```

MII总线支持对于一些PCI 10/100 Ethernet NIC来说是必需的。

```
device      bfe      # Broadcom BCM440x 10/100 Ethernet
device      bge      # Broadcom BCM570xx Gigabit Ethernet
device      dc       # DEC/Intel 21143 and various workalikes
device      fxp      # Intel EtherExpress PRO/100B (82557, 82558)
device      lge      # Level 1 LXT1001 gigabit ethernet
device      nge      # NatSemi DP83820 gigabit ethernet
device      pcn      # AMD Am79C97x PCI 10/100 (precedence over 'lnc')
device      re       # RealTek 8139C+/8169/8169S/8110S
device      rl       # RealTek 8129/8139
device      sf       # Adaptec AIC-6915 ( "Starfire" )
device      sis      # Silicon Integrated Systems SiS 900/SiS 7016
device      sk       # SysKonnect SK-984x & SK-982x gigabit Ethernet
device      ste      # Sundance ST201 (D-Link DFE-550TX)
device      ti       # Alteon Networks Tigon I/II gigabit Ethernet
device      tl       # Texas Instruments ThunderLAN
device      tx       # SMC EtherPower II (83c170 "EPIC" )
device      vge      # VIA VT612x gigabit ethernet
device      vr       # VIA Rhine, Rhine II
device      wb       # Winbond W89C840F
device      xl       # 3Com 3c90x ( "Boomerang" , "Cyclone" )
```

使用MII总线控制器代码的驱动器。

```
# ISA Ethernet NICs. pccard NICs included.
device      cs       # Crystal Semiconductor CS89x0 NIC
# 'device ed' requires 'device miibus'
device      ed       # NE[12]000, SMC Ultra, 3c503, DS8390 cards
device      ex       # Intel EtherExpress Pro/10 and Pro/10+
device      ep       # Etherlink III based cards
device      fe       # Fujitsu MB8696x based cards
device      ie       # EtherExpress 8/16, 3C507, StarLAN 10 etc.
device      lnc      # NE2100, NE32-VL Lance Ethernet cards
device      sn       # SMC's 9000 series of Ethernet chips
device      xe       # Xircom pccard Ethernet
```

```
# ISA devices that use the old ISA shims
#device      le
```

ISA 以太网卡驱动。参见/usr/src/sys/i386/conf/NOTES 以了解关于哪个驱动程序能够驱动您的网卡的细节。

```
# Wireless NIC cards
device      wlan     # 802.11 support
```

```

device      an          # Aironet 4500/4800 802.11 wireless NICs.
device      awi         # BayStack 660 and others
device      wi          # WaveLAN/Intersil/Symbol 802.11 wireless NICs.
#device     wl          # Older non 802.11 Wavelan wireless NIC.

```

用以支持多种无线网卡。

```

# Pseudo devices
device      loop        # Network loopback

```

这是TCP/IP的通用回环设备。如果您telnet或FTP到localhost(也就是127.0.0.1)则将通过这个设备回到本机。这个设备是必需的。在FreeBSD 4.X中, 则应使用pseudo-device loop。

```

device      mem          # Memory and kernel memory devices

```

The system memory devices.

```

device      io           # I/O device

```

This option allows a process to gain I/O privileges. This is useful in order to write userland programs that can handle hardware directly. This is required to run the X Window system.

```

device      random       # Entropy device

```

Cryptographically secure random number generator.

```

device      ether        # Ethernet support

```

ether 只有在使用以太网卡时才需要。它包含了通用的以太网协议代码。在FreeBSD 4.X中应写作pseudo-device ether。

```

device      sl           # Kernel SLIP

```

sl 用以提供SLIP支持。目前它几乎已经完全被PPP取代了, 因为后者更容易配置, 而且更适合调制解调器之间的连接, 并提供了更强大的功能。在FreeBSD 4.X中, 这一行应写作pseudo-device sl。

```

device      ppp          # Kernel PPP

```

这一选项用以提供内核级的PPP支持, 用于拨号连接。也有以用户模式运行的PPP实现, 使用tun并提供包括按需拨号在内的更为灵活的功能。在FreeBSD 4.X中应写作pseudo-device ppp。

```

device      tun          # Packet tunnel.

```

它会被用户模式的PPP软件用到。参考本书的PPP以了解更多的细节。在FreeBSD 4.X中则应使用pseudo-device tun。

```

device      pty          # Pseudo-ttys (telnet etc)

```

这是一个“pseudo-terminal”或模拟登入端口。它用来接收连入的telnet以及rlogin会话、xterm, 以及一些其它程序如Emacs等。

注意: 在FreeBSD 4.X中, 您应该使用pseudo-device pty number。pty后面的number用于指定要创建的pty数量。如果您需要多于默认的同时16个xterm窗口或远程登录会话, 则应相应的提高这个值, 其上限是256。

```
device    md                # Memory "disks"
```

Memory disk pseudo-devices. With FreeBSD 4.X use the line pseudo-device md.

```
device    gif                # IPv6 and IPv4 tunneling
```

它实现了在IPv4上的IPv6隧道、IPv6上的IPv4隧道、IPv4上的IPv4隧道、以及IPv6上的IPv6隧道。从FreeBSD 4.4开始gif设备具有了“自动克隆”能力，因此只需指定pseudo-device gif。更早版本的FreeBSD 4.X需要手工指定一个数字，例如pseudo-device gif 4。

```
device    faith              # IPv6-to-IPv4 relaying (translation)
```

这个伪设备能捕捉发给它的数据包，并把它们转发给IPv4/IPv6翻译服务程序。在FreeBSD 4.X中，应写作pseudo-device faith 1。

```
# The 'bpf' device enables the Berkeley Packet Filter.
# Be aware of the administrative consequences of enabling this!
# Note that 'bpf' is required for DHCP.
device    bpf                # Berkeley packet filter
```

这是Berkeley包过滤器。这个伪设备允许网络接口被置于混杂模式，从而，截获广播网(例如，以太网)上的每一个数据包。截获的数据报可以保存到磁盘上，也可以使用tcpdump(1)程序来分析。在FreeBSD 4.X中，应写作pseudo-device bpf。

注意：bpf(4)设备也被用于dhclient(8)来获取默认路由器(网关)的IP地址。如果使用DHCP，就不要注释掉这行。

```
# USB support
device    uhci                # UHCI PCI->USB interface
device    ohci                # OHCI PCI->USB interface
#device    ehci                # EHCI PCI->USB interface (USB 2.0)
device    usb                 # USB Bus (required)
#device    udbp                # USB Double Bulk Pipe devices
device    ugen                # Generic
device    uhid                # "Human Interface Devices"
device    ukbd                # Keyboard
device    ulpt                # Printer
device    umass               # Disks/Mass storage - Requires scbus and da
device    ums                 # Mouse
device    urio                # Diamond Rio 500 MP3 player
device    uscanner            # Scanners
# USB Ethernet, requires mii
device    aue                 # ADMtek USB Ethernet
device    axe                 # ASIX Electronics USB Ethernet
device    cdce                # Generic USB over Ethernet
device    cue                 # CATC USB Ethernet
device    kue                 # Kawasaki LSI USB Ethernet
device    rue                 # RealTek RTL8150 USB Ethernet
```

支持各类USB设备。

```
# FireWire support
device      firewire      # FireWire bus code
device      sbp            # SCSI over FireWire (Requires scbus and da)
device      fwe           # Ethernet over FireWire (non-standard!)
```

支持各类火线设备。

要了解FreeBSD 所支持的设备的其他情况，请参考/usr/src/sys/i386/conf/NOTES。

8.4.1 大内存支持(PAE)

大内存配置的机器需要超过 4 GB的虚拟地址。因为4GB的限制，Intel在Pentium及后续的CPUs上增加了36位物理地址的支持。

Intel Pentium Pro和后续的CPUs允许内存地址扩展到64GB.(PAE) FreeBSD通过PAE选项来支持这个能力。在FreeBSD 4.X系列里面，4.9-RELEASE开始支持，FreeBSD 5.X系列里面，从5.1-RELEASE开始支持。in the 4.X series of FreeBSD beginning with 4.9-RELEASE and in the 5.X series of FreeBSD beginning with 5.1-RELEASE。因为Intel架构的限制，高于或低于4GB都没有什么区别，内存分配到大于4GB仅仅是增加了可利用的内存池。

为了让内核支持PAE，只要增加下面这一行到配置文件：

```
options      PAE
```

注意：PAE在FreeBSD里面现在只能支持Intel IA-32处理器。同时，还应该注意，FreeBSD的PAE支持没有经过广泛的测试，和其他稳定的特性相比只能当作是beta版。

PAE在FreeBSD下有如下的一些限制：

- 进程不能接触大于4GB的VM空间。
- KLD 模块不能加载到一个打开了PAE支持的内核里面，这是因为内核模块和内核的建立框架不一样。
- 没有使用bus_dma(9)界面的设备驱动程序在打开了PAE支持的内核里面会导致数据腐化（corruption）。因为这个原因，FreeBSD 5.X的PAE内核配置文件把所有在打开了PAE的内核上不能工作的驱动程序排除在外。
- 一些系统打开了探测系统内存资源使用能力的功能，因为打开了PAE支持，这些功能可能会被覆盖掉。其中一个例子就是内核参数kern.maxvnodes，它是控制内核能使用的最大vnodes数目的，建议重新调整它及其他类似参数到合适的值。
- 为了避免KVA的消耗，很有必要增加系统的内核虚拟地址，或者减少很耗系统资源的内核选项的总量（看上面）。KVA_PAGES选项可以用来增加KVA空间。

为了稳定和高性能，建议查看tuning(7)手册页。pae(4)手册页包含FreeBSD's PAE支持的最新信息。

8.5 创建设备节点

如果您在运行FreeBSD 5.0 或更高版本，则可以略过这节。新版本使用devfs(5) 来分配设备节点，这一过程对用户是透明的。

内核中的几乎每个设备在`/dev`目录中都有对应的“节点”项。这些节点看上去像是普通的文件，但事实上却是程序在使用对应的设备时，与内核联系的入口。`Shell`脚本`/dev/MAKEDEV`在首次安装操作系统时会创建几乎所有能够支持的设备节点。然而，它并不会创建所有的节点，因此当您增加了某些设备的支持时，就需要检查这个目录中是否有对应的项了，如果没有，就应该添加它们。这有一个简单的例子：

假定在内核中加入了IDE CD-ROM的支持。可以这样加入：

```
device acd0
```

这意味着您应当在`/dev`目录下找一些以`acd0`为起点的入口，通常后面有一个字母，像是以`c`，或者`r`开头，表示这是一个“raw”设备。如果那些文件不在那儿，就必须改变到`/dev`目录然后键入：

```
# sh MAKEDEV acd0
```

这些脚本完成后，您要在`/dev`目录下确认有`acd0c`和`racd0c`等几个入口，这表示程序已经正确执行。

以下是加入声卡节点的例子：

```
# sh MAKEDEV snd0
```

注意：当创建完诸如声卡这样的设备节点时，如果其他人有权访问您的机器，可能有必要在`/etc/fstab`文件中添加这些节点来保护系统安全。更多的信息参考`fstab(5)`

依上述的简单程序，建立任何不在`GENERIC`里的硬件设备节点

注意：所有的SCSI控制器都使用一样的设备节点，所以您无须重新建立节点。另外，网卡与SLIP/PPP虚拟设备并没有任何设备节点，所以您不必担心怎么建立节点。

8.6 如果出现问题怎么办

在定制一个内核时，可能会出现五种问题。它们是：

config失败：

如果`config(8)`在给出您的内核描述时失败，则可能在某些地方引入了一处小的错误。幸运的是，`config(8)`会显示出它遇到问题的行号，这样您就能够迅速地定位错误。例如，如果您看到：

```
config: line 17: syntax error
```

可以通过与`GENERIC`或其他参考资料对比，来确定这里的关键词是否拼写正确。

make失败：

如果`make`命令失败，它通常表示内核描述中发生了`config(8)`无法找出的错误。同样地，仔细检查您的配置，如果仍然不能解决问题，发一封邮件到FreeBSD一般问题邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-questions>) 并附上您的内核配置，则问题应该很快就能解决。

安装新内核失败:

如果内核编译得很顺利, 但安装失败(即`make install` 或 `make installkernel` 命令失败), 第一件事是检查您的系统是否是以1 或更高的安全级运行的(参见`init(8)`)。内核安装过程将尝试去掉原有内核的`immutable` (不可改) 标志, 并在新的内核上设置它。由于安全级1 或更高的安全级会阻止修改系统中任何文件的这个标志, 因此安装内核需要0 或者更低的安全级。

不过这只对FreeBSD 4.X 以及更早的版本有效。FreeBSD 5.X 以及之后的版本并不会给内核设置不可改标志, 因此安装失败可能说明发生了更深层次的问题。

内核无法启动:

如果您的内核无法启动, 或不识别您的设备, 千万别慌! 非常幸运的是, FreeBSD 有一个很好的机制帮助您从不兼容的内核恢复。在FreeBSD 启动加载器那里简单地选择一下要启动的内核就可以了。当系统在引导菜单的10 秒倒计时时进入它。按下了**Enter** 之外的任意键, `unload` 然后输入 `boot /boot/kernel.old/kernel`, 或者其他任何一个可以正确引导的内核即可。当重新配置内核时, 保持一个已经证明能够正常启动的内核永远是一个好习惯。

当使用好的内核启动之后您可以检查配置文件并重新尝试编译它。比较有用的资源是 `/var/log/messages` 文件, 它会记录每次成功启动所产生的所有内核消息。此外, `dmesg(8)` 命令也会显示这次启动时产生的内核消息。

注意: 如果在编译内核时遇到麻烦, 请务必保留一个GENERIC 或已知可用的其他内核, 并命名为别的名字以免在下次启动时被覆盖。不要依赖`kernel.old` 因为在安装新内核时, `kernel.old` 会被上次安装的那个可能不正常的内核覆盖掉。另外, 尽快把可用的内核挪到 `/boot/kernel` 否则类似`ps(1)` 这样的命令可能无法正常工作。为了完成这一点, 需要修改目录的名字:

```
# mv /boot/kernel /boot/kernel.bad
# mv /boot/kernel.good /boot/kernel
```

对于FreeBSD 5.X 之前的版本, 正确的“解除” `make` 所实施的保护的命令(为了把另一个内核永久性地挪回来) 是:

```
# chflags noschg /kernel
```

如果您发现您不能这样做, 您的系统的安全级别可能大于0了。在`/etc/rc.conf`里面编辑`kern_securelevel`并把它设置为-1然后重启。当您很满意这个内核的时候, 您可以再把设置改回去。

另外, 如果您要“锁住”内核或其他文件, 以致它不能被移动或修改, 可以用下面的命令:

```
# chflags schg /kernel
```

内核工作, 但是ps(1)根本不工作:

如果您安装了一个与系统中内建工具版本不同的内核, 例如在4.x 系统上安装了5.x 的内核, 许多用于检查系统状态的工具如`ps(1)` 和`vmstat(8)` 都将无法正常使用。您应该重新编译一个和内核版本一致的系统。这也是为什么一般不鼓励使用与系统其他部分版本不同的内核的一个主要原因。

第9章

打印

Contributed by Sean Kelly. Restructured and updated by Jim Mock.

9.1 概述

FreeBSD 可以支持众多种类的打印机，从最古老的针式打印机到最新的激光打印机以及它们之间所有类型的打印机。您可以使运行的应用程序产生高质量的打印输出。

FreeBSD 也可以被设置成一个网络上的打印服务器。它可以从包括FreeBSD、Windows 及Mac OS 在内的多种其他主机上接收打印任务。FreeBSD 将保证任务在某时被打印，并且可以把哪台机器，哪位用户打印的最多记录在统计表中，生成“横幅”页，显示哪份打印输出的是哪位用户的等等。

在读完这章后，您将知道：

- 怎样配置FreeBSD打印池。
- 怎样安装打印过滤器来对特殊的打印任务做特殊的处理，包括把传来的文档转换成打印机能理解的格式。
- 怎样在打印输出上开启报头或者横幅页功能。
- 怎样打印到连接在其他计算机上的打印机。
- 怎样打印到直接连接在网络上的打印机。
- 怎样控制打印机的限制，包括限制打印任务的大小和阻止某些用户打印。
- 怎样记录打印机统计表和使用情况。
- 怎样解决打印故障。

在读这章之前，您应该：

- 知道怎样配置并安装新内核(第8 章)。

9.2 介绍

为了在FreeBSD 中使用打印机，您需要将伯克利行式打印机打印池系统即**LPD** 打印池系统设置好。它是FreeBSD的标准打印控制系统。这章介绍**LPD** 打印池系统，经常简称**LPD**，并且将指导您贯穿它的配置。

如果您已经熟悉了**LPD**或者其他打印池系统，您可以跳到设置打印池系统这部分。

LPD完全控制一台主机的打印机。它负责许多的事情：

- 它控制本地和连接在网络上其他主机上的打印机的访问。
- 它允许用户提交要打印的文件；这些通常被认为是**任务**。
- 它为每个打印机维护一个**队列**来防止多个用户在同一时刻访问一台打印机。

- 它可以打印**报头**(也叫做**banner**或者 **burst**页使用户可以轻松的从一堆打印输出中找到它们打印的任务。
- 它来设置连接在串口上的打印机的通讯参数。
- 它能通过网络将任务发送到另外一台主机的**LPD**打印池中。
- 它可以根据不同种类的打印机语言和打印机的性能运行特殊的过滤器来格式化任务。
- 它记录打印机的使用情况。

通过配置文件(/etc/printcap)和提供的特殊过滤程序，您可以使**LPD**系统在众多种类的打印机硬件上完成上面全部的或者一些子集的功能。

9.2.1 为什么要用打印池

如果您是系统唯一的用户，您可能会奇怪为什么要在您不需要访问控制，报头页或者打印机使用统计时为打印池费心。它可以设置成允许直接访问打印机，但您还是应该使用打印池，因为：

- **LPD**在后台打印任务；您不用被迫等待数据被完全拷贝到打印机的时间。
- **LPD**可以方便的通过过滤器给任务加上日期/时间的页眉或者把一种特殊的文件格式(比如**TEX DVI**文件)转换成一种打印机可以理解的格式。您不必去手动做这些步骤。
- 许多提供打印功能的免费和商业程序想要和您系统上的打印池通讯。通过设置打印池系统，您将更轻松的支持其他以后要添加的或者现有的软件。

9.3 基本设置

要想在**LPD**打印池系统上使用打印机，您需要设置打印机硬件和**LPD**软件。这个文档描述了这两级设置：

- 参见简单打印机设置来了解怎样连接一个打印机，告诉**LPD**怎样与它通讯，并且打印纯文本到打印机。
- 参见高级打印机设置 来了解怎样打印多种特殊格式的文件，怎样打印报头页，怎样通过网络打印，怎样控制打印机的访问权限，并且学会为打印作业记帐统计。

9.3.1 简单打印机设置

这部分讲解怎样配置打印机硬件和**LPD**使之与打印机配合。讲解的基础知识有：

- 硬件设置部分将讲解怎样把一台打印机连接到您计算机的一个端口上。
- 软件设置部分将讲解怎样配置**LPD**打印池的配置文件(/etc/printcap)。

如果您正在设置一台通过网络协议接收数据来打印而不是通过串行或者并口的打印机，参见使用网络数据流界面的打印机。

尽管这部分叫“简单打印机设置”，但还是相当复杂的。使打印机配合和**LPD**打印池在计算机上正常运转是最难的部分。一旦您的打印机可以正常工作后，那些高级选项，比如报文页和记帐，是相当简单的。

9.3.1.1 硬件设置

这部分讲述了打印机连接到计算机的多种途径。主要讨论了多种接口和连接线，还有允许FreeBSD与打印机通讯所需的内核配置。

如果您已经连接好了您的打印机而且已经用它在另外一个操作系统下成功的打印，您或许可以跳到这个部分软件设置。

9.3.1.1.1 端口和连接电缆

现在所出售的在PC上使用的打印机通常至少有以下三种接口中的一个：

- **串行接口**，也叫**RS-232**或者**COM**口，使用您计算机上的串口来发送数据到打印机。串行接口在计算机上已经非常普遍，而且电缆也非常容易买到且容易制作。串行接口有时需要特殊的电缆，而且可能需要您去配置稍微有点儿复杂的通讯选项。大多数PC的串口的最高传输速度只有115200 bps，这使得打印很大的图像需要的时间很长。
- **并口**使用计算机上的并口来发送数据到打印机。并口在计算机上也已经非常普遍，而且速度高于RS-232串口。电缆非常容易买到，但很难手工制作。并口通常没有通讯选项，这使得配置它相当简单。

并口按打印机上的接头来命名也叫做“Centronics”接口。

- **USB**接口，即通用串行总线，可以达到比并口和串口高很多的速度。其电缆既简单又便宜。USB用来打印比串口和并口更有优势，但UNIX系统不能很好的支持它。避免这个问题的方法就是购买一台像大多数打印机一样的既有USB接口又有并口的打印机。

一般来说并口只提供单向通讯(计算机到打印机)，而串口和USB则可以提供双向通讯。新的并口(EPP和ECP)及打印机在使用了IEEE-1284标准的电缆之后，可以在FreeBSD下双向通讯。

与打印机通过并口双向通讯通常由这两种方法中的一种来完成。第一个方法是使用为FreeBSD编写的可以通过打印机使用的语言与打印机通讯的驱动程序。这通常用在喷墨打印机上，且可以用来报告剩余墨水多少和其他状态信息。第二种方法使用在支持PostScript的打印机上。

PostScript任务事实上由程序发送给打印机；但它并不进行打印而是直接将结果返回给计算机。PostScript也采取双向通讯来将打印中的问题报告给计算机，比如PostScript程序中的错误或者打印机卡纸。这些信息对于用户来说也许是非常有价值的。此外，最好的在支持PostScript的打印机上记帐的方法需要双向通讯：询问打印机打印总页数(打印机从出厂一共打印过多少页)，然后发送用户的任务，之后再次查询总打印页数。将打印前后得到的两个值相减就可以得到该用户要付多少纸钱。

9.3.1.1.2 并口

用并口连接打印机需要用Centronics电缆把打印机与计算机连接起来。具体说明指导在打印机的说明书上应该有，或者干脆两个上面都有。

记住您用的计算机上的哪个并口。第一个并口在FreeBSD上叫/dev/ppc0；第二个叫/dev/ppc1，依此类推。打印机设备也用同样的方法命名：/dev/lpt0是接在第一个并口上的打印机，依此类推。

9.3.1.1.3 串口

用串口连接打印机需要用合适的串口电缆把打印机与计算机连接起来。具体说明指导应该在打印机的说明书上有，或者同样干脆两个上面都有。

如果您不确定什么样儿的电缆才是“合适的串口电缆”，您可以尝试以下几种不同的电缆：

- **调制解调器** 电缆每一端的每一根引脚都直接连接到另一端相应的引脚上。这种电缆也叫做“DTE-to-DCE”电缆。
- **非调制解调器** 电缆上每一端的有些引脚是与另一端相应引脚直接连接的,而有一些则是交叉连接的(比如,发送数据引脚连接到接收数据引脚),还有一些引脚直接在电缆连接头儿内短接。这种电缆也叫做“DTE-to-DTE”电缆。
- 一些特殊的打印机需要的**串行打印机** 电缆,是一种和非调制解调器电缆类似的电缆,只是一些信号还是送到了另一端,而不是直接在连接头儿内短路。

当然,您还得为打印机设置通讯参数。一般是通过打印机面板上的按钮或者DIP 开关进行设置。在计算机和打印机上都选择它们所支持的最高波特(每秒多少比特,有时也叫**波特率**)的传输速率。选择7或者8个数据位;选择不校验,偶校验或者奇校验;选择1个或2个停止位。还要选择流量控制协议:无,XON/XOFF(也叫做“in-band”或“软件”)流量控制。记住您的软件配置中的参数也要设成上面的数值。

9.3.1.2 软件设置

这部分描述了要使用FreeBSD系统中的**LPD** 打印池进行打印所需的软件设置。

包括这几个步骤:

1. 在需要的时候配置内核来允许您连接打印机的端口;配置内核 部分会告诉您需要做什么。
2. 如果您使用并口,则需要设置一下并口的通讯模式;设置并口通讯模式 部分会告诉您具体的细节。
3. 测试操作系统是否能够发送数据到打印机。检测打印机联机状况 部分会告诉您要怎样做。
4. 为**LPD** 设置与打印机匹配的参数则通过修改/etc/printcap 这个文件来完成。这章后面的部分将讲解如何来完成设置。

9.3.1.2.1 配置内核

操作系统的内核为了使某些特殊设备工作需要重新编译。打印机所用的串口、并口就属于那些特殊设备。因此,可能需要添加对串口或并口的支持,如果内核并没有配置它们的话。

要想知道您现在使用的内核是否支持串口,输入:

```
# grep sioN /var/run/dmesg.boot
```

其中N 是串口的编号,从0开始。如果您看到类似下面的输出:

```
sio2 at port 0x3e8-0x3ef irq 5 on isa
sio2: type 16550A
```

则说明您现在使用的内核支持串口。

要想知道您现在使用的内核是否支持并口,输入:

```
# grep ppcN /var/run/dmesg.boot
```

其中N 是并口的编号,同样从0开始。如果得到类似下面的输出:

```
ppc0: <Parallel port> at port 0x378-0x37f irq 7 on isa0
```

```
ppc0: SMC-like chipset (ECP/EPP/PS2/NIBBLE) in COMPATIBLE mode
ppc0: FIFO with 16/16/8 bytes threshold
```

那么您现在使用的内核支持并口。

您可能必须为了使操作系统支持您打印机需要的串口或并口而重新配置内核。

要增加对串口的支持，参见内核配置这部分。要增加对并口的支持，除了参见上面提到的那部分之外，还要参见下面的部分。

9.3.1.3 在/dev 中为端口添加设备节点

注意: FreeBSD 5.0 支持devfs 这种在需要的时候自动添加设备节点的文件系统。如果您正在使用的FreeBSD 开启了devfs 文件系统，那么您可以安全的跳过这部分。

尽管内核可能已经支持通过串口或者并口通讯，但您还是需要一个软件接口来使您系统上的程序通过它发送和接收数据。这也是/dev 目录中那些设备节点的作用。

要在/dev 中为端口添加一个设备节点：

1. 使用su(1) 命令切换到root 帐号。在出现提示的时候输入root 帐号的密码。
2. 将当前目录改变到/dev 目录：

```
# cd /dev
```

3. 输入：

```
# ./MAKEDEV port
```

其中`port` 替换成您需要添加端口的节点名。当打印机连接在第一个并口上时，替换成`lpt0`，连接在第二个并口上时，替换成`lpt1`，依此类推；当打印机连接在第一个串口上时，替换成`ttyd0`，连接在第二个串口上时，替换成`ttyd1`，依此类推。

4. 输入：

```
# ls -l port
```

来检查设备节点是否正常建立。

9.3.1.3.1 设置并口的通讯模式

在使用并口时，您可以选择让FreeBSD 用中断方式还是轮询方式来与打印机通讯。在FreeBSD 4.X and 5.X 上，通用的打印机驱动(lpt(4)) 使用ppbus(4) 系统，它由ppc(4) 驱动来控制端口芯片。

- **中断** 方式是GENERIC 核心的默认方式。在这种方式下，操作系统占用一条中断请求线来检测什么时候打印机做好接收数据的准备。
- **轮询** 方式是操作系统反复不断的询问打印机是否做好接收数据的准备。当它返回准备好时，核心开始发送下面要发送的数据。

中断方式速度通常会快一些，但却占用了一条宝贵的中断请求线。一些新出的HP 打印机不能正常的工作在中断模式下，是由于一些定时问题(还没正确的理解) 造成的。这些打印机需要使用轮询方式。您应该

使用任何一种方式，只要它能正常工作就行。一些打印机虽然在两种模式下都可以工作，但在中断模式下会慢的要命。

您可以用以下两种方法设定通讯模式：通过配置内核或者使用lptcontrol(8)这个程序。

要通过配置内核的方法设置通讯模式：

1. 修改内核配置文件。找到一个叫ppc0的记录。如果您想要设置的是第二个并口，那么用ppc1代替。使用第三个并口的时候用ppc2代替，依此类推。

- 如果您想要使用中断方式，在FreeBSD 4.X下的方法是指定一个irq：

```
device ppc0 at isa? irq N
```

其中N是计算机并口的中断编号。

在FreeBSD 5.X下，修改下面这一行：

```
hint.ppc.0.irq="N"
```

它在/boot/device.hints这个文件中，其中N用正确的中断编号代替。同时，核心配置文件也必须包括ppc(4)的驱动：

```
device ppc
```

- 如果您想要使用轮询方式，则不用指定irq：

在FreeBSD 4.X下，在内核配置文件中使下面这行：

```
device ppc0 at isa?
```

在FreeBSD 5.X下，只需要把/boot/device.hints这个文件中的下面这行删除掉：

```
hint.ppc.0.irq="N"
```

在FreeBSD 5.X下，有时上面的方法并不能使并口工作在轮询方式。大多数情况是由于acpi(4)驱动造成的，它可以自动侦测到设备并将其挂载到系统上，但也因此，它控制着打印机端口的访问模式。您得检查acpi(4)的配置来解决这个问题。

2. 保存文件。然后配置，建立，并安装刚配置的内核，最后重新启动。参见内核配置 这章来获得更多细节。

使用 lptcontrol(8) 设置通讯模式：

1. 输入：

```
# lptcontrol -i -d /dev/lptN
```

将lptN设置成中断方式。

2. 输入：

```
# lptcontrol -p -d /dev/lptN
```

将lptN设置成轮询方式。

您可以把这些命令加入到/etc/rc.local这个文件中，这样每次启动系统时都会设置成您想要的方式。参见lptcontrol(8)来获得更多信息。

9.3.1.3.2 检测打印机的通讯

在设置打印池系统之前，您应该确保您的计算机可以把数据发送到打印机上。分别独立调试打印机的通讯和打印池系统会更简单。

我们为了测试打印机，将发送一些文本给它。一个叫`lptest(1)`的程序能胜任这项工作，它可以让打印机立即打印出程序发给它的字符：它在每行打出可以打印的96个ASCII字符。

当我们使用的是一台PostScript (或者以其他语言为基础的) 打印机，那么需要更仔细的检测。一段小小的PostScript 程序足以完成检测的任务，比如下面这段程序：

```
%!PS
100 100 moveto 300 300 lineto stroke
310 310 moveto /Helvetica findfont 12 scalefont setfont
(Is this thing working?) show
showpage
```

可以把上面这段PostScript 代码写进一个文件里，并且像下面部分的例子里那样使用。

注意：上面的小程序是基于PostScript 写成的，而不是惠普的PCL。尽管PCL拥有强大的功能，比如您可以在打印纯文本的同时夹带着特殊的命令。PostScript 不能直接打印纯文本，所以这类打印机语言是我们要特殊照顾的对象。

9.3.1.3.2.1 检测并口打印机

这部分内容将指导您怎样检测FreeBSD是否可以与一台已经连接在并口上的打印机通讯。

要测试并口上的打印机：

1. 用`su(1)` 命令转换到root 用户。
2. 发送数据到打印机。
 - 如果打印机可以直接打印纯文本，可以用`lptest(1)`。输入：

```
# lptest > /dev/lptN
```

其中`N` 是并口的编号，从0开始。

- 如果打印机支持PostScript 或者其他打印机语言，可以发送一段小程序到打印机。输入：

```
# cat > /dev/lptN
```

然后，一行一行的**输入** 输入这段程序。因为在按下换行 或者回车 之后，这一行就不能再修改了。当您输入完这段程序之后，按`CONTROL+D`，或者其他表示文件结束的键。

另外一种办法，您可以把这段程序写在一个文件里并输入：

```
# cat file > /dev/lptN
```

其中`file` 是包含这您要发给打印机程序的文件名。

之后，您应该看到打印出了一些东西。如果打印出的东西看起来并不正确，请不要着急；我们将在后面指导您怎样解决这类问题。

9.3.1.3.2.2 检测串行打印机

这部分将告诉您如何检测FreeBSD是否可以与连接在串口上的打印机通讯。

要测试一个连接在串口上的打印机：

1. 通过su(1) 命令转换成root 用户。
2. 修改/etc/remote 这个文件。增加下面这些内容：

```
printer:dv=/dev/port:br#bps-rate:pa=parity
```

其中`port` 是串口的设备节点(`ttyd0`, `ttyd1`, 等等。), `bps-rate` 是与打印机通讯时使用的波特, `parity` 是通讯时打印机要求的校验方法(either even, odd, none, or zero)。

这儿有一个串口打印机的例子, 它连接在第三个串口上, 速度为19200 波特, 不进行校验:

```
printer:dv=/dev/ttyd2:br#19200:pa=none
```

3. 用tip(1) 连接打印机。输入：

```
# tip printer
```

如果没能成功, 则要再次修改/etc/remote 这个文件, 并且试试用/dev/cuaaw 代替/dev/ttydw。

4. 发送数据到打印机。

- 如果打印机可以直接打印纯文本, 则用lpctest(1) 。输入：

```
% $lpctest
```

- 如果打印机支持PostScript 或者其他打印机语言, 则发送一段小程序到打印机。一行一行的输入程序, 必须非常仔细 因为像退格或者其他编辑键也许对打印机来说有它的意义。您同样也需要按一个特殊的文件结束键, 让打印机知道它已经接收了整个程序。对于PostScript 打印机, 按CONTROL+D。

或者, 您同样也可以把程序存储在一个文件里并输入：

```
% >file
```

其中`file` 是包含要发送程序的文件名。在tip(1) 发送这个文件之后, 按代表文件结束的键。

您应该看到打印出了一些东西。如果它们看起来并不正确也不要着急; 我们将在以后的部分中解决它。

9.3.1.4 开启打印池：文件/etc/printcap

目前, 您的打印机应该已经连好了线, 系统内核也为与打印机联机而重新配置好(如果需要的话), 而且您也已经可以发送一些简单的数据到打印机。现在, 我们要配置LPD 来使其控制您的打印机。

配置LPD 要修改/etc/printcap 这个文件。LPD 打印池系统在每次打印池被使用的时候都会读取这个文件, 所以对对这个文件的修改会立即生效。

printcap(5) 这个文件的格式很简单。您可以用您最喜欢的文本编辑器来修改/etc/printcap 这个文件。这种格式和其他的像/usr/share/misc/termcap 和/etc/remote 这类文件是一样的。要得到完整的关于这种格式的信息, 参见cgetent(3) 。

简单的打印池配置包括下面的几步：

1. 为打印机起一个名字(和一些方便的别名),然后把它们写进文件`/etc/printcap`;参见Naming the Printer 这章来得到更多的关于起名的帮助。
2. 关掉报头页(它默认是打开的),通过增加`sh`项目;参见Suppressing Header Pages 部分来得到更多信息。
3. 建立一个打印池缓冲的目录,并且通过`sd`项目指定它的位置;参见Making the Spooling Directory 部分来得到更多信息。
4. 在`/dev`下设置打印机设备节点,并且在写在`/etc/printcap`文件中`lp`项目里;参见识别打印机设备 这部分得到更多信息。还有,如果打印机连接在串口上,设置通讯参数要写在`ms#`项目中。这些参数在配置打印池通讯参数 这部分已经讨论过。
5. 安装纯文本过滤器;参见安装文本过滤器 这章来得到细节。
6. 用`lpr(1)`命令来测试设置。想得到更多信息可以参见测试 and 疑难问题解答 部分。

注意: 基于打印机语言的打印机,比如PostScript打印机,不能直接打印纯文本。简单的设置方法在上面提到并且下面的部分也要讨论,假如您正在安装这样一台只能打印它明白的文件的打印机。

用户总是希望他们能在任何一个安装在他们系统的打印机上打印纯文本。使用LPD接口的程序也通常这样希望。如果您正在安装这样一台打印机,并且想要它能打印基于它支持的打印机语言的任务并且还可以打印纯文本的任务,那么强烈建议您在上面提到的简单设置的步骤上增加一步:安装一个自动纯文本到PostScript(或者其他打印机语言)的转化程序。参见在PostScript打印机上打印纯文本 将得到更多有关信息。

9.3.1.4.1 命名打印机

第一步(简单)就是给打印机起一个名字。您是按功能起名字还是干脆起个古怪的名字都没有关系,因为您可以给打印机设置许多的别名。

在`/etc/printcap`里至少有一个打印机必须指定,别名是`lp`。这是默认的打印机名。如果用户既没有PRINTER环境变量,也没有在任何LPD命令的命令行中指定打印机名,则`lp`将是默认要使用的打印机。

还有,我们通常把最后一个别名设置成能完全描述打印机的名字,包括厂家和型号。

一旦您选好了名字或者一些别名,把它们放进文件`/etc/printcap`里。打印机的名字应该从最左边的一列写起。用竖杠来隔开每个别名,并且在最后一个别名后面加上一个冒号。

在下面的例子中,我们从一个基本的`/etc/printcap`开始,它只定义了两台打印机(一台Diablo 630 行式打印机和一台Panasonic KX-P4455 PostScript 激光打印机):

```
#
# /etc/printcap for host rose
#
rattan|line|diablo|lp|Diablo 630 Line Printer:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:
```

在这个例子中,第一台打印机被命名为`rattan`并且设置了`line`, `diablo`, `lp`, 和`Diablo 630 Line Printer`这几个别名。因为它被设置了`lp`这个别名,所以它是默认打印机。第二台被命名为`bamboo`,并且设置了`ps`, `PS`, `S`, `panasonic`, 和`Panasonic KX-P4455 PostScript v51.4`这几个别名。

9.3.1.4.2 不打印报头页

LPD 打印池系统默认会为每个任务打印**报头页**。报头页包含了发送这个任务的用户，发送这个任务的主机，任务的名字，并用大字母打出。但不幸的是，所有这些额外的文本会妨碍在简单设置打印机时的除错，所以我们将先不打印报头页。

要暂停打印报头页，为打印机的记录增加sh 标记，在/etc/printcap 文件中。这儿有一个/etc/printcap 文件中使用的例子：

```
#
# /etc/printcap for host rose - no header pages anywhere
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
    :sh:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
    :sh:
```

注意我们的正确格式：第一行从最左边一列开始，而后的每一行用TAB 缩进一次。一行写不下需要换行时，在换行前打一个反斜杠。

9.3.1.4.3 建立打印池目录

下一步设置就是要建立一个**打印池目录**，一个在任务被打印完之前存放任务的目录，也有很多其他的打印池系统所用到的文件存在里面。

由于打印池目录的变量本质，通常把这些目录安排在/var/spool 下。您也没有必要去备份打印池目录里的内容。重新建立它们只要简单的使用mkdir(1) 命令。

通常，我们习惯将目录名起成和打印机一样的名字，像下面这样：

```
# mkdir /var/spool/printer-name
```

然而，如果您有很多网络打印机，您可能想要把这些打印池目录放在一个单独的您专门为使用**LPD** 打印而准备的目录里。我们将用我们的两台打印机作为例子rattan 和bamboo：

```
# mkdir /var/spool/lpd
# mkdir /var/spool/lpd/rattan
# mkdir /var/spool/lpd/bamboo
```

注意：如果您在关心用户任务的保密性，您可能想保护相应的打印池目录，使它们不能被公开访问。打印池目录应该被daemon 用户拥有，用户daemon 和daemon 组拥有读写和搜索的权限，并且其他用户没有。我们将用我们的两台打印机作为例子：

```
# chown daemon:daemon /var/spool/lpd/rattan
# chown daemon:daemon /var/spool/lpd/bamboo
# chmod 770 /var/spool/lpd/rattan
# chmod 770 /var/spool/lpd/bamboo
```

最后，您需要通过/etc/printcap 文件告诉**LPD** 这些目录。您可以用sd 标记来指定打印池目录的路径：

```
#
# /etc/printcap for host rose - added spooling directories
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
      :sh:sd=/var/spool/lpd/rattan:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
      :sh:sd=/var/spool/lpd/bamboo:
```

注意打印机的名字要从第1列开始，其他记录每行都要用TAB键缩进一次，写不开需要换行在最后加上反斜杠。

如果您没用sd标记指定打印池目录，打印池系统会将/var/spool/lpd目录作为默认目录。

9.3.1.4.4 识别打印机设备

在为端口在/dev目录下增加设备节点章节中，我们确定了使用/dev目录中的哪个节点来让FreeBSD与打印机通讯。现在，我们来告诉LPD这个信息。当打印池系统有任务需要打印，它将为过滤程序（负责传送数据到打印机）打开指定的设备。

用lp标记在/etc/printcap里列出/dev下的设备节点。

在我们的例子中，假设打印机rattan在第一个并口上，打印机bamboo在第六个串口上；下面是要对/etc/printcap文件里增加的内容：

```
#
# /etc/printcap for host rose - identified what devices to use
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
      :sh:sd=/var/spool/lpd/rattan:\
      :lp=/dev/lpt0:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
      :sh:sd=/var/spool/lpd/bamboo:\
      :lp=/dev/ttyd5:
```

如果您没在您的/etc/printcap文件中用lp标记指定设备节点，LPD将默认使用/dev/lp。/dev/lp目前在FreeBSD中不存在。

如果您正在安装的打印机是连接在并口上的，请跳到安装文本过滤器 这章。如果不是的话，还是最好按下面介绍的步骤做。

9.3.1.4.5 配置打印池通讯参数

对于连在串口上的打印机，LPD可以为发送数据到打印机的过滤程序设置好波特率，校验，和其他串口通讯参数。这是有利的，因为：

- 它可以让您只需简单的修改/etc/printcap就能尝试不同的通讯参数；您并不需要去重新编译过滤器程序。
- 它使得打印池系统可以在多台有不同串口通讯设置的打印机上使用相同的过滤器程序。

下面这个/etc/printcap中用lp标记来控制列出设备的串口通讯参数：

br#bps-rate

设置设备的通讯速度为**bps-rate**，这里**bps-rate**可以为50, 75, 110, 134, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 比特每秒。

ms#stty-mode

设置已打开的中端设备的选项。**stty(1)** 将详细讲述可用的选项。

当**LPD** 打开用**lp** 指定的设备时，它会将设备的特性设置成在**ms#** 标记后指定的那样。特别是**parenb**, **parodd**, **cs5**, **cs6**, **cs7**, **cs8**, **cstopb**, **crtscs**, 和**ixon** 这些模式，它们在**stty(1)** 手册中有详细说明。

我们举个例子来添加我们连在第6个串口上的打印机。我们将设波特为38400。至于模式，我们将用**-parenb** 设置成不校验，用**cs8** 设置成8位字符，用**cllocal** 设置成不要调制解调器控制，用**crtscs** 设置成硬件流量控制：

```
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
      :sh:sd=/var/spool/lpd/bamboo:\
      :lp=/dev/ttyd5:ms#-parenb cs8 cllocal crtscs:
```

9.3.1.4.6 安装文本过滤器

我们现在准备告诉**LPD** 使用什么文本过滤器给打印机发送任务。**文本过滤器**，也叫**输入过滤器**，是一个在**LPD** 有一个任务要发给打印机时运行的程序。当**LPD** 为打印机运行文本过滤器时，它设置过滤器的标准输入为要发给打印机的任务，而标准输出为用**lp** 标记指定的打印机。过滤器先从标准输入读取任务，为打印机进行一些转换，并将结果写到标准输出，这些结果将被打印。想得到更多关于文本过滤器的信息，见过滤器 这节。

对于简单的打印机设置，文本过滤器可以仅仅是一段执行**/bin/cat** 的shell 脚本来发送任务到打印机。**FreeBSD** 还提供了一个叫做**lpf** 的过滤器，它可以处理退格和下划线来使那些可能不能很好处理这类字符流的打印机正常工作。而且，当然，您可以用任何其他的您想用的过滤程序。**lpf** 过滤器在**lpf: 一个文本过滤器** 这节将有详细描述。

首先，我们来写一段叫做**/usr/local/libexec/if-simple** 的简单shell 脚本作为文本过滤器。用您熟悉的文本编辑器将下面的内容放进这个文件：

```
#!/bin/sh
#
# if-simple - Simple text input filter for lpd
# Installed in /usr/local/libexec/if-simple
#
# Simply copies stdin to stdout. Ignores all filter arguments.

/bin/cat && exit 0
exit 2
```

使这个文件可以被执行：

```
# chmod 555 /usr/local/libexec/if-simple
```

然后用**if** 标记在**/etc/printcap** 里告诉**LPD** 使用这个脚本。我们将仍然为一直作为例子的这两台打印机在**/etc/printcap** 里增加这个标记：

```
#
# /etc/printcap for host rose - added text filter
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
    :sh:sd=/var/spool/lpd/rattan:\ :lp=/dev/lpt0:\
    :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
    :sh:sd=/var/spool/lpd/bamboo:\
    :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:\
    :if=/usr/local/libexec/if-simple:
```

注意: if-simple 脚本的副本可以在 /usr/share/examples/printing 目录中找到。

9.3.1.4.7 开启LPD

lpd(8) 在 /etc/rc 中被运行, 它是否被运行由 lpd_enable 这个变量控制。这个变量默认是 NO。如果您还没有修改, 那么增加这行:

```
lpd_enable="YES"
```

到 /etc/rc.conf 文件当中, 然后既可以重启您的机器, 也可以直接运行 lpd(8)。

```
# lpd
```

9.3.1.4.8 测试

现在已经基本完成了 LPD 的基本设置。但不幸的是, 还不是庆祝的时候, 因为我们还需要测试设置并且修正所有的问题。要测试设置, 尝试打印一些东西。要用 LPD 系统打印, 您可以使用 lpr(1) 命令, 它可以提交一个任务来打印。

您可以联合使用 lpr(1) 和 the lptest(1) 程序, 在检查打印机通讯 这节介绍怎样生成一些测试文本。

要测试简单 LPD 设置:

输入:

```
# lptest 20 5 | lpr -Pprinter-name
```

其中 *printer-name* 是在 /etc/printcap 中指定的打印机的一个名字(或者一个别名)。要测试默认打印机, 输入 lpr(1) 不带任何 -P 选项。同样, 如果您正在测试一台使用 PostScript 的打印机, 发送一个 PostScript 程序到打印机而不是使用 lptest(1)。您可以把程序放在一个文件里, 然后输入: `lpr file`。

对于一台 PostScript 打印机, 您应该得到那段程序的结果。而如果您使用的 lptest(1), 则您得到的结果应该看起来像下面这样:

```
!"#$%&'()*+,-./01234
"#$$$%&'()*+,-./012345
#$$$%&'()*+,-./0123456
$$$%&'()*+,-./01234567
```

```
%&'()*+,-./012345678
```

要更进一步的测试打印机，尝试下载一些大的程序(为基于特定语言的打印机) 或者运行 `lpctest(1)` 并使用不同的参数。比如，`lpctest 80 60` 将生成60行每行80个字符。

如果打印机不能工作，参考故障排除 这节。

9.4 高级设置

这部分将描述用来打印特别格式文件，页眉，通过网络打印，以及对打印机使用限制和记帐。

9.4.1 过滤器

尽管**LPD** 处理网络协议，任务排队，访问控制，和打印的其他方面，但大部分实际工作还是由**过滤器**。过滤器是一种与打印机通讯并且处理设备依赖和特殊需要的程序。在简单打印机设置这节里，我们安装了一个纯文本过滤器——一个应该可以用在大多数打印机上的极简单的过滤器(安装文本过滤器)。

然而，为了进行格式转换，打印记帐，适应特殊的打印机，等等，您需要明白过滤器是怎样工作的。在根本上过滤器负责处理这些方面。但坏消息是大多数时候您必须自己提供过滤器。好消息是很多过滤器通常都已经有了；当没有的时候，它们通常也是很好写的。

FreeBSD 也提供了一个过滤器，`/usr/libexec/lpr/lpf`，可以让大多数可以打印纯文本的打印机工作。(它处理文件里的退格和跳格，并且进行记帐，但这基本就是它所有能做的了。) 这里还有几个过滤器和过滤器组件在FreeBSD Ports Collection 里。

这是在这节里您将找到的内容：

- 过滤器是怎样工作的，设法给出一个过滤器在打印过程中的大致角色。您应该阅读这节来理解在**LPD** 使用过滤器时“表面上看不到”的事情。这个知识能够帮您预期并调试您在为每个打印机安装越来越多的过滤器时可能遇到的问题。
- **LPD** 默认每个打印机都能打印纯文本。这就出现一个问题在PostScript (或者基于其他语言的打印机) 以及所有无法直接打印纯文本的打印机。让PostScript 打印机适应纯文本任务 这节将告诉您要解决这个问题应该做些什么。如果您使用一台PostScript 打印机，那么您应该阅读这个小节。
- PostScript 对于许多程序来说都是一个非常受欢迎的输出格式。一些人甚至直接写PostScript 代码。但不幸的是，PostScript 打印机非常昂贵。模拟PostScript 在非PostScript 打印机上 这节将告诉您怎样进一步修改打印机的文本过滤器，使得一台**非PostScript** 打印机接受并打印PostScript 数据。如果您没有PostScript 打印机，那么您应该阅读这个小节。
- 转换过滤器 这节讲述了一个自动把指定格式文件，比如图像或排版数据，转换成您打印机可以理解的格式。在阅读了这节之后，您应该可以设置好您的打印机使得用户可以输入 `lpr -t` 来打印带有不同宏定义库的文本，或者用 `lpr -d` 来打印**T_EX** DVI 数据，用 `lpr -v` 来打印光栅图像数据，等等。我推荐您阅读这节。
- 输出过滤器 这节讲述了这个不是经常使用的**LPD** 的功能——输出过滤器。除非您要打印页眉(见页眉 这节)，您或许可以完全跳过这节。

- **lpf**: 一个文本过滤器 描述了 **lpf**，一个FreeBSD 自带的相当完整而又简单的文本过滤器，可以使用在行式打印机(和那些担当行式打印机功能的激光打印机) 上。如果您需要一个快速的方法来让打印机统计打印纯文本的工作量，或者您有一台遇到退格字符就冒烟的打印机，您应该考虑 **lpf**。

注意: 您可以在 `/usr/share/examples/printing` 目录中找到下面将提到的那些脚本的副本。

9.4.1.1 过滤器是怎样工作的

前面说过，过滤器是一个被**LPD** 启动，用来处理与打印机通讯过程中设备依赖的部分的可执行程序。

当**LPD** 想要打印一个任务中的文件，它启动一个过滤器程序。它把要打印的文件设置成过滤器的标准输入，标准输出设置成打印机，并且把错误信息定向到错误日志文件(在**lf** 标识里指定，默认在 `/etc/printcap`，或者 `/dev/console` 文件里)。

过滤器被**LPD** 启动，并且过滤器的参数依赖于 `/etc/printcap` 文件中所列出的和用户为任务用 **lpr(1)** 命令所指定的。例如，如果用户输入 **lpr -t**，**LPD** 会启动 **troff** 过滤器，即在目标打印机的 **tf** 标签里所列出的过滤器。如果用户想要打印纯文本，它将会启动 **if ***** 过滤器(这是通常的情况：参见输出过滤器 来得到细节)。

在 `/etc/printcap` 文件中，您可以指定三种过滤器：

- **The 文本过滤器**，在**LPD** 文档中也叫做 **输入过滤器**，处理常规的文本打印。可以把它想象成默认过滤器。**LPD** 默认每台打印机都可以打印纯文本，而文本过滤器的任务就是来搞定退格、跳格，或者其他在某种打印机上容易错误的特殊字符。如果您所在的环境对打印机的使用情况进行记帐，那么文本过滤器必须也对打印进行统计，统计通常是通过对打印的行数进行计数然后与打印机所支持的每页的行数做比较后得出的。文本过滤器的启动命令为：

```
filter-name [-c] -wwidth -llength -iindent -n login -h host acct-file
```

where

-c

当任务用 **lpr -l** 这个命令提交时出现

width

这里取您在 `/etc/printcap` 文件中指定的 **pw** (页宽) 标签的值，默认为132。

length

这里取您的 **pl** (页长) 标签的值，默认为66

indent

这里是来自 **lpr -i** 命令的总缩进量，默认为0

login

这里是正在打印文件的用户名

host

这里是提交打印任务的主机名

acct-file

这里是来自`af`变量中指定的用于记帐的文件名。

- **转换过滤器** 将一个特定的文件格式转换成另一种打印机能够理解并且将内容打印出来的格式。例如，`ditroff` 格式的排版数据就是无法直接打印的，但您可以安装一个转换过滤器来将`ditroff` 文件转换成一种打印机可以理解并打印的形式。参考 转换过滤器 这一节来了解更多细节。如果您需要对打印进行记帐，那么转换过滤器也必须完成记帐工作。转换过滤器的启动命令为：

```
filter-name -xpixel-width -ypixel-height -n login -h host acct-file
```

pixel-width 的值来自`px` 标签(默认为0)，*pixel-height* 的值来自`py` 标签(默认为0)。

- **输出过滤器** 仅在没有文本过滤器时，或者报头页被打开时使用。就我的经验而言，输出过滤器是很少用到的。在 输出过滤器 这节中会介绍它们。启动输出过滤器的命令行只有两个参数：

```
filter-name -wwidth -llength
```

`-w` 和 `-l` 参数的意义和文本过滤器中的一样。

过滤器也应该在 **退出** 时给出下面的几种退出状态：

exit 0

过滤器已经成功的打印了文件。

exit 1

过滤器打印失败了，但想要**LPD**来试着再打印一次。如果过滤器返回了这个状态，**LPD**将重新启动一个过滤器。

exit 2

过滤器打印失败并且不想要**LPD**重试。**LPD**将放弃这个文件。

文本过滤器随FreeBSD一起发布，文件名为`/usr/libexec/lpr/lpf`，它利用页宽和页长参数来决定何时发送送纸指令和为打印记帐的方法。它使用登陆名，主机名，和记帐文件参数来生成记帐记录。

如果您想购买过滤器，要注意它是否是LPD-兼容的。如果是，则它们必须支持上面提到的那些参数。如果您打算编写普通的过滤器程序，则同样需要让它们支持上面那些参数和退出状态码。

9.4.1.2 在PostScript® 打印机上打印纯文本任务

如果您是您的计算机和PostScript (或者其他语言的) 打印机的唯一用户，而且您不打算发送纯文本到打印机且不打算使用程序里那些会发送纯文本到打印机的功能的话，那么您完全不需要再关心这节的内容。

但是，如果PostScript 和纯文本的任务都需要发送到打印机，那么就需要对打印机进行设置了。要完成工作，我们需要一个文本过滤器来检测到达的任务是纯文本的还是PostScript 格式的。所有PostScript 的任务必须以%! (对于其他打印机语言，参见打印机的文档) 开头。如果任务的头两个字符是这两个，就代表这是PostScript 格式的，并且可以直接略过任务剩余的部分。如果任务开头的两个字符不是这两个，那么过滤器将把文本转换成PostScript 并打印结果。

我们怎样去做？

如果你有一台串行打印机，一个好办法就是安装 `lprps`。 `lprps` 是一个可以与打印机进行双向通信 `PostScript` 打印机过滤器。它用打印机传来的详细信息来更新打印机的状态文件，所以用户和管理员可以准确的看到打印机处在什么样的状态(比如缺墨 或者卡纸)。但更重要的是，它包含了一个叫做 `psif` 的程序，它可以检测接收到的文件是否是纯文本的，并且将使用 `textps` 命令(也是由 `lprps` 提供的程序)转换文本到 `PostScript`。然后它会用 `lprps` 将任务发送到打印机。

`lprps` 可以在 `FreeBSD Ports Collection` (详见 `The Ports Collection`) 中找到。您当然可以自己获取，构建并安装它。在安装之后 `lprps`，只需指定 `psif` 这个程序的路径，这也是包含在 `lprps` 中的一个程序。如果您已经用 `ports` 安装好了 `lprps`，将下面的内容添加到 `/etc/printcap` 文件中 `PostScript` 打印机的记录部分中：

```
:if=/usr/local/libexec/psif:
```

同时还需要指定 `rw` 标签来告诉 `LPD` 使用读-写模式打开打印机。

如果您有一台并行的 `PostScript` 打印机(因此不能与打印机进行 `lprps` 需要的双向通信)，可以使用下面这段 `shell` 脚本来充当文本过滤器：

```
#!/bin/sh
#
#  psif - Print PostScript or plain text on a PostScript printer
#  Script version; NOT the version that comes with lprps
#  Installed in /usr/local/libexec/psif
#

IFS="" read -r first_line
first_two_chars='expr "$first_line" : \'(..\)'

if [ "$first_two_chars" = "%!" ]; then
    #
    #  PostScript job, print it.
    #
    echo "$first_line" && cat && printf "\004" && exit 0
    exit 2
else
    #
    #  Plain text, convert it, then print it.
    #
    ( echo "$first_line"; cat ) | /usr/local/bin/textps && printf "\004" && exit 0
    exit 2
fi
```

在上面的脚本中， `textps` 命令是一个独立安装的程序用来将纯文本转换成 `PostScript`。您可以使用任何您喜欢的文本到 `PostScript` 转换程序。 `FreeBSD Ports Collection` (详见 `Ports Collection`) 中包含了一个功能非常完整的文本到 `PostScript` 的转换程序，它叫做 `a2ps`。

9.4.1.3 模拟 `PostScript` 在非 `PostScript` 打印机上

`PostScript` 高质量排版和打印的 **de facto** 标准。而 `PostScript` 也是一个 昂贵的标准。幸好， `Aladdin` 开发了一个和 `PostScript` 类似的叫做 **Ghostscript** 的程序可以用在 `FreeBSD` 上。 `Ghostscript` 可以读取大多数 `PostScript` 的文件并处理其中的页面交给多种设备，包括许多品牌的非 `PostScript` 打印机。通过安

装Ghostscript 并使用一个特殊的文本过滤器，则可以使一台非PostScript 打印机用起来就像真的PostScript 打印机一样。

Ghostscript 也包括在FreeBSD Ports Collection 中，如果您想要从这里安装。您同样可以很容易地获取，构建，并安装它。

要模拟PostScript，文本过滤器要检测是否要打印一个PostScript 文件。如果不是，那么过滤器将直接将文件发送到打印机；否则，它会用Ghostscript 先将文件转换成打印机可以理解的格式。

这里有一个例子：下面的脚本是一个针对Hewlett Packard DeskJet 500 打印机的文本过滤器。对于其他打印机，替换gs (Ghostscript) 命令中的-sDEVICE 参数就可以了。(输入gs -h 来获得当前安装的Ghostscript 所支持的设备列表。)

```
#!/bin/sh
#
# ifhp - Print Ghostscript-simulated PostScript on a DeskJet 500
# Installed in /usr/local/libexec/ifhp

#
# Treat LF as CR+LF (to avoid the "staircase effect" on HP/PCL
# printers):
#
printf "\033&k2G" || exit 2

#
# Read first two characters of the file
#
IFS="" read -r first_line
first_two_chars='expr "$first_line" : \'(..\)'

if [ "$first_two_chars" = "%" ]; then
    #
    # It is PostScript; use Ghostscript to scan-convert and print it.
    #
    /usr/local/bin/gs -dSAFER -dNOPAUSE -q -sDEVICE=djet500 \
        -sOutputFile=- - && exit 0
else
    #
    # Plain text or HP/PCL, so just print it directly; print a form feed
    # at the end to eject the last page.
    #
    echo "$first_line" && cat && printf "\033&l0H" &&
exit 0
fi

exit 2
```

最后，需要告知LPD 所使用的过滤器，通过if 标签完成：

```
:if=/usr/local/libexec/ifhp:
```

您可以输入lpr plain.text 和lpr whatever.ps，它们都应该可以成功打印。

9.4.1.4 转换过滤器

在完成了打印机简单设置 这节中所描述的内容之后，头一件事恐怕就是为你喜爱的格式的文件安装转换过滤器了(除了纯ASCII 文本)。

9.4.1.4.1 为什么安装转换过滤器?

转换过滤器使打印众多格式的文件变得很容易。比如，假设我们大量使用 $\text{\TeX}$ 排版系统，并且有一台PostScript 打印机。每次从 $\text{\TeX}$ 生成一个DVI 文件，我们都不能直接打印它直到我们将DVI 文件转换成PostScript。转换的命令应该是下面的样子：

```
% dvips seaweed-analysis.dvi
% lpr seaweed-analysis.ps
```

通过安装DVI 文件的转换过滤器，我们可以跳过每次手动转换这一步，而让**LPD** 来完成这个步骤。现在，每次要打印DVI 文件，我们只需要一步就可以打印它：

```
% lpr -d seaweed-analysis.dvi
```

我们要**LPD** 转换DVI 文件是通过指定**-d** 选项完成的。格式和转换选项 这一节列出了所有的转换选项。

对于每种想要打印机支持的转换，首先要安装 **转换过滤器** 然后在`/etc/printcap` 中指定它的路径。在简单打印设置中，转换过滤器类似于文本过滤器(详见 安装文本过滤器) 不同的是它不是用来打印纯文本，而是将一个文件转换成打印机能够理解的格式。

9.4.1.4.2 我应该安装哪个转换过滤器?

您应该安装您希望使用的转换过滤器。如果要打印很多DVI 数据，就需要DVI 转换过滤器；如果有大量的troff 数据，就应该安装troff 过滤器。

下面的表格总结了可以与**LPD** 配合工作的过滤器，以及它们在`/etc/printcap` 文件中的变量名，还有如何在**lpr** 命令中调用它们：

文件类型	在 <code>/etc/printcap</code> 文件中的变量名	在 lpr 命令中调用使用的参数
cifplot	cf	-c
DVI	df	-d
plot	gf	-g
ditroff	nf	-n
FORTTRAN text	rf	-f
troff	tf	-t
raster	vf	-v
plain text	if	none, -p, or -l

在例子中，**lpr -d**就是指打印机需要在`/etc/printcap`文件中df变量所指的过滤器。

不管别人怎么说，像FORTTRAN 的文本和plot 这些格式已经基本不用了。所以在您的机器上，就可以安装其他的过滤器来替换这些参数原有的意义。例如，假设想要能直接打印Printerleaf 文件(由Interleaf desktop publishing 程序生成)，而且不打算打印plot 文件，就可以安装一个Printerleaf 转换过滤器并且用gf 变量指定它。然后就可以告诉您的用户使用**lpr -g** 就可以“打印Printerleaf 文件。”

9.4.1.4.3 安装转换过滤器

以为安装的转换过滤器不是FreeBSD基本系统的一部分，所以它们可能是在`/usr/local`目录下。通常目录`/usr/local/libexec`是保存它们的地方，因为它们通常是通过**LPD**运行的；普通用户没有并不需要直接运行它们。

要启用一个转换过滤器，只需要在`/etc/printcap`文件中为目标打印机中合适的变量赋上过滤器所在的路径。

在接下来的例子当中，我们将为一台叫做**bamboo**的打印机添加一个转换过滤器。下面是这个例子的`/etc/printcap`文件，其中使用新变量**df**来为打印机**bamboo**设置转换过滤器。

```
#
# /etc/printcap for host rose - added df filter for bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
    :sh:sd=/var/spool/lpd/rattan:\
    :lp=/dev/lpt0:\
    :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
    :sh:sd=/var/spool/lpd/bamboo:\
    :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:\
    :if=/usr/local/libexec/psif:\
    :df=/usr/local/libexec/psdf:
```

这里的DVI过滤器是一段shell脚本，名字叫做`/usr/local/libexec/psdf`。下面是它的代码：

```
#!/bin/sh
#
# psdf - DVI to PostScript printer filter
# Installed in /usr/local/libexec/psdf
#
# Invoked by lpd when user runs lpr -d
#
exec /usr/local/bin/dvips -f | /usr/local/libexec/lprps "$@"
```

这段脚本以过滤器模式运行**dvips** (参数**-f**) 并从标准输入读取要打印的任务。然后运行**PostScript** 文本过滤器**lprps** (详见在**PostScript** 打印机上打印纯文本任务 这一节)，并且带着**LPD** 传给脚本的全部参数。**lprps** 将利用这些参数来为打印进行记帐。

9.4.1.4.4 更多转换过滤器应用实例

因为安装转换过滤器的步骤并不是固定的，所以这里会多给出一些例子。在以后的安装配置过程中可以以这些例子为参考。甚至如果合适的话，可以完全照搬过去。

这段例子中的脚本是一个Hewlett Packard LaserJet III-Si 打印机的光栅格式数据(实际上也就是**GIF** 文件)：

```
#!/bin/sh
#
# hpvf - Convert GIF files into HP/PCL, then print
# Installed in /usr/local/libexec/hpvf
```

```
PATH=/usr/X11R6/bin:$PATH; export PATH
giftopnm | ppmtopgm | pgmtopbm | pbmtolj -resolution 300 \
    && exit 0 \
    || exit 2
```

它的工作原理就是将GIF文件转换成portable anymap，再转换成portable graymap，然后再转换成portable bitmap，最后再转换成LaserJet/PCL-兼容的数据。

下面是为打印机配置上上述过滤器的/etc/printcap文件：

```
#
# /etc/printcap for host orchid
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
    :lp=/dev/lpt0:sh:sd=/var/spool/lpd/teak:mx#0:\
    :if=/usr/local/libexec/hpif:\
    :vf=/usr/local/libexec/hpvf:
```

下面的脚本是一个在名叫bamboo的这台PostScript打印机上打印用groff排版软件生成的troff数据的打印过滤器：

```
#!/bin/sh
#
# pstf - Convert groff's troff data into PS, then print.
# Installed in /usr/local/libexec/pstf
#
exec grops | /usr/local/libexec/lprps "$@"
```

上面这段脚本还是用lprps来与打印机进行通讯。如果打印机是接在并口上的，那么就应该使用下面的这段脚本：

```
#!/bin/sh
#
# pstf - Convert groff's troff data into PS, then print.
# Installed in /usr/local/libexec/pstf
#
exec grops
```

这里是我们要启用过滤器需要在/etc/printcap里增加的内容：

```
:tf=/usr/local/libexec/pstf:
```

下面的例子也许会让许多FORTRAN老手羞愧。它是一个FORTRAN-文本的过滤器，能在任意一台可以打印纯文本的打印机上使用。我们将为打印机teak安装这个过滤器：

```
#!/bin/sh
#
# hprf - FORTRAN text filter for LaserJet 3si:
# Installed in /usr/local/libexec/hprf
#

printf "\033&k2G" && fpr && printf "\033&l0H" &&
exit 0
exit 2
```

然后我们要在`/etc/printcap`中为打印机能够teak启用这个过滤器添加下面的内容:

```
:rf=/usr/local/libexec/hprf:
```

最后,再给出一个有些复杂的例子。我们将给以前介绍过的teak这台激光打印机添加一个DVI过滤器。首先,最容易的部分:更新`/etc/printcap`加入DVI过滤器的路径:

```
:df=/usr/local/libexec/hpdf:
```

现在,该困难的部分了:编写过滤器。为了实现过滤器,我们需要一个DVI-到-LaserJet/PCL转换程序。FreeBSD Ports Collection (详见Ports Collection 这一节)中有一个包: `dvi2xx` 是这个包的名称。安装这个包就会得到我们需要的程序, `dvilj2p`, 它可以将DVI数据转换成LaserJet IIP, LaserJet III, 和LaserJet 2000兼容的数据。

`dvilj2p`使得过滤器hpdf变得十分复杂,因为`dvilj2p`不能读取标准输入。它需要从文件中读取数据。更糟糕的是,这个文件的名字必须以`.dvi`结尾。所以使用`/dev/fd/0`作为标准输入是有问题的。我们可以通过连接(符号连接)来解决这个问题。连接一个临时的文件名(一个以`.dvi`结尾的文件名)到`/dev/fd/0`,从而强制`dvilj2p`从标准输入读取。

现在迎面而来的是另外一个问题,我们不能使用`/tmp`存放临时连接。符号连接是被用户和组`bin`拥有的。而过滤器则是以`daemon`用户运行的。并且`/tmp`目录设置了`sticky`位。所以过滤器只能建立符号连接,但它不能在用完之后清除掉这些连接。因为它们属于不同的用户。

所以过滤器将在当前工作目录下建立符号连接,即打印池目录(用变量`sd`在`/etc/printcap`中指定)。这是一个非常好的让过滤器完成它工作的地方,特别还是因为(有时)这个目录比起`/tmp`来有更多的可用磁盘空间。

最后,给出过滤器的代码:

```
#!/bin/sh
#
# hpdf - Print DVI data on HP/PCL printer
# Installed in /usr/local/libexec/hpdf

PATH=/usr/local/bin:$PATH; export PATH

#
# Define a function to clean up our temporary files. These exist
# in the current directory, which will be the spooling directory
# for the printer.
#
cleanup() {
    rm -f hpdf$$dvi
}

#
# Define a function to handle fatal errors: print the given message
# and exit 2. Exiting with 2 tells LPD to do not try to reprint the
# job.
#
fatal() {
    echo "$@" 1>&2
    cleanup
    exit 2
}
```

```

}

#
# If user removes the job, LPD will send SIGINT, so trap SIGINT
# (and a few other signals) to clean up after ourselves.
#
trap cleanup 1 2 15

#
# Make sure we are not colliding with any existing files.
#
cleanup

#
# Link the DVI input file to standard input (the file to print).
#
ln -s /dev/fd/0 hpdf$$dvi || fatal "Cannot symlink /dev/fd/0"

#
# Make LF = CR+LF
#
printf "\033&k2G" || fatal "Cannot initialize printer"

#
# Convert and print. Return value from dvi2p does not seem to be
# reliable, so we ignore it.
#
dvi2p -M1 -q -e- dhpdp$$dvi

#
# Clean up and exit
#
cleanup
exit 0

```

9.4.1.4.5 自动转换：一种替代转换过滤器的方法

以上这些转换过滤器基本上建成了您的打印环境，但也有不足就是必须由用户来指定(在`lpr(1)`命令行中) 要使用哪一个过滤器。如果您的用户不是对计算机很在行，那么选用过滤器将是一件麻烦的事情。更糟的是，当过滤器设定的不正确时，过滤器被用在了不它对应类型的文件上，打印机也许会喷出上百张纸。

比只安装转换过滤器更好的方法，就是让文本过滤器(因为它是默认的过滤器) 来检测要打印文件的类型，然后自动运行正确的转换过滤器。像`file`这样的工具可以给我们一定的帮助。当然，要区分开有些文件的类型还是有困难的——而且，当然，您可以仅为它们提供转换过滤器。

FreeBSD Ports Collection 包含了一个可以自动进行转换的文本过滤器，名字叫做`apsfilter`。它可以检测出纯文本，PostScript，和DVI格式的文件，并且运行相应的转换过滤器，然后打印。

9.4.1.5 输出过滤器

LPD 打印池系统还支持一种我们还没有讨论过的过滤器：输出过滤器。输出过滤器只是用来打印纯文本的，类似于文本过滤器，但简化了许多地方。如果您正在使用输出过滤器而不是文本过滤器，那么：

- **LPD** 为整个任务启动一个输出过滤器，而不是为任务中的每个文件都启动一次。
- **LPD** 不会提供任务中文件开始和结束的信息给输出过滤器。
- **LPD** 不会提供用户名或者主机名给过滤器，所以它是无法做打印记帐的。事实上它只有两个参数：

过滤器-名字 -w宽度 -l长度

宽度来自于pw变量，而length来自于pl变量，这些值都是实际问题中给打印机设置的。

不要让输出过滤器的简化所耽误。如果想要输出过滤器完成让任务中的每个文件都重新开始一页打印是不可能。请使用文本过滤器(也叫输入过滤器)；详见安装文本过滤器。此外，实际上，输出过滤器更复杂，它要检查发给它的字节流中是否有特殊的标志字符，并且给自己发送信号来代替**LPD**的。

可是，如果打算要报头页或者需要发送控制字符或者其他的初始化字符串来完成打印报头页，那么输出过滤器则是必需的。(但是它也是无用的 如果打算对打印的用户计费，因为**LPD**不会给输出过滤器任何用户或者主机的信息。)

在一台单个的打印机上，**LPD**同时允许输出过滤器、文本过滤器和其他的过滤器。在某些情况下，**LPD**将仅会启动输出过滤器来打印报头页(详见报头页)。然后**LPD**会要求输出过滤器自己停止运行，它发送给过滤器两个字节：ASCII 031跟着一个ASCII 001。当输出过滤器看见这两个字节(031,001)，它应该通过发送SIGSTOP信号来停止自己的运行。当**LPD**已经运行好了其他的过滤器，它会通过给输出过滤器发送SIGCONT信号来让输出过滤器重新运行。

如果仅有一个输出过滤器而没有文本过滤器，并且**LPD**正在处理一个纯文本任务，**LPD**会使用输出过滤器来完成这个任务。像以前运行一样，输出过滤器会按顺序打印任务中的文件，而不会插入送纸或其他进纸的命令，但这也也许并不是您想要的结果。在大多数情况下，您还是需要一个文本过滤器。

lpf这个我们前面介绍过的文本过滤器程序，也可以用来做输出过滤器。如果需要使用快速且混乱的输出过滤器，但又不想写字节检测和信号发送代码，那么试试lpf。lpf也可以包含在一个shell脚本中来处理任何打印机可能需要的初始化代码。

9.4.1.6 lpf：一个文本过滤器

/usr/libexec/lpr/lpf这个程序包含在FreeBSD的二进制程序中，它是一个文本过滤器(输入过滤器)。它可以缩排输出(用lpr -i命令提交的任务)，可以打印控制字符禁止断页用lpr -l提交的任务)，可以调整任务中退格和制表符打印的位置，还可以对打印进行记帐。它同样可以像输出过滤器一样工作。

lpf适用于很多打印环境。尽管它本身没有向打印机发送初始化代码的功能，但写一个shell脚本来完成所需的初始化并执行lpf是很容易的。

为了让lpf可以正确的进行打印记帐，那么需要/etc/printcap中的pw和pl变量都填入正确的值。它用这些值来测定一页能打印多少文本，并计算出任务有多少页。想得到更多关于打印记帐的信息，请参见对打印机使用进行记帐。

9.4.2 报头页

如果您有**很多**用户，他们正在使用各式各样的打印机，那么您允许要考虑一下把**报头页**当作一个必要的麻烦了。

报头页，也叫**banner** 或者**burst** 页，可以用来辨别打印出的文件是谁打印的。它们通常用大号的粗体字母打印出来，也可能用装饰线围绕四周，所以在一堆打印出的文件中，突出的显示了这个文件属于哪个用户的哪个任务。这可以让用户快速的找到他们的任务。而报头页一个明显的缺点就是，在每个任务中都要有一张或者几张纸作为报头页印出来，可是它们的有用的地方只发挥几分钟的作用，最后它们会被放进回收站或者扔进垃圾堆。(注意报头页只是一个任务一个，而不是任务中的每个文件都有一个，所以可能对纸张还不算很浪费。)

LPD 系统可以自动为您的打印提供报头页，**如果** 您的打印机可以直接打印纯文本。如果您的打印机是一台PostScript 打印机，您将需要一个外部的程序来生成报头页；详见在PostScript 打印机上打印报头页。

9.4.2.1 打开报头页

在简单打印设置 这节，我们通过在/etc/printcap 文件中指定sh (“禁止报头页”) 来把报头页功能关掉了。要重新为打印机开启报头页功能，只需要删除掉sh。

听起来很容易，不是么？

是的。您可能不得不让输出过滤器来给打印机发送初始化字符串。下面是一个用在Hewlett Packard PCL-兼容打印机上的输出过滤器的例子：

```
#!/bin/sh
#
# hpof - Output filter for Hewlett Packard PCL-compatible printers
# Installed in /usr/local/libexec/hpof

printf "\033&k2G" || exit 2
exec /usr/libexec/lpr/lpf
```

用of 变量指定输出过滤器的路径。参见输出过滤器 这一节来得到更多信息。

下面是一个为我们以前介绍的叫做teak 的打印机配置的/etc/printcap 文件；在配置当中我们开启了报头页并且加入了上述的打印过滤器：

```
#
# /etc/printcap for host orchid
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
    :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:\
    :if=/usr/local/libexec/hpif:\
    :vf=/usr/local/libexec/hpvf:\
    :of=/usr/local/libexec/hpof:
```

现在，当用户再发任务给打印机teak 的时候，每个任务都会有一个报头页。如果用户想要花时间来寻找他们自己打印的文件，那么他们可以通过lpr -h 命令来提交任务；参考报头页选项 这一节来得到更多关于lpr(1) 的选项。

注意: **LPD** 在报头页之后发出一个换纸字符。如果您的打印机使用一个不同的字符或者字符串当作退纸指令，在/etc/printcap 中用ff 变量指定即可。

9.4.2.2 控制报头页

通过启用报头页，**LPD** 将生成出一个**长报头**，一整页的大字母，标着用户，主机和任务名。下面是一个例子(kelly 打印了用主机rose 打印了一个叫做outline 的任务):

```

k          ll      ll
k          l       l
k          l       l
k  k      eeee    l       l   y   y
k  k      e  e    l       l   y   y
k  k      eeeee   l       l   y   y
kk k      e       l       l   y   y
k  k      e  e    l       l   y  yy
k  k      eeee    ll      ll   yyy y
                        y
                        y  y
                        yyyy

                        ll
                        l       i
                        t       l
                        t       l
o o o o  u  u  t t t t  l       ii  n n n  eeee
o  o  u  u  t         l       i  nn  n  e  e
o  o  u  u  t         l       i  n  n  eeeee
o  o  u  u  t         l       i  n  n  e
o  o  u  uu  t  t     l       i  n  n  e  e
o o o o  u u u u  t t  ll      iii  n  n  eeee

r r r r  o o o o  s s s s  eeee
r r  r  o  o  s  s  e  e
r      o  o  s s  eeeee
r      o  o  s s  e
r      o  o  s  s  e  e
r      o o o o  s s s s  eeee

```

```

Job:  outline
Date: Sun Sep 17 11:04:58 1995

```

LPD 会附加一个换页符在这段文本之后，所以任务会在新的一页上开始(除非设置了 **sf** (禁止换纸) 在 `/etc/printcap` 文件里目标打印机的记录中)。

如果您喜欢，**LPD** 可以生成一个**短报头**；指定 **sb** (短 banner) 在文件 `/etc/printcap` 中。报头页就会看起来像下面这样：

```
rose:kelly Job: outline Date: Sun Sep 17 11:07:51 1995
```

同样是默认的，**LPD** 也是先打印报头页，然后才是任务。要想反过来，在 `/etc/printcap` 中指定 **hl** (最后报头)。

9.4.2.3 为带报头页的任务记帐

使用**LPD** 内置的报头页会在进行打印记帐的时候产生一种特殊情况：报头页肯定是**免费** 的。

为什么？

因为输出过滤器是仅有的一个在打印报头页时能进行记帐的外部程序，但却没有提供给它任何**用户或者主机** 的信息或者记帐文件，所以它无法知道谁应该为打印机的使用付费。如果仅仅是“增加一页”给文本过滤器或者其他过滤器(它们有用户和主机的信息)是不够的，因为用户可以用 `lpr -h` 命令跳过报头页。他还是需要为自己并没有打印的报头页付钱。基本上，`lpr -h` 是明知用户的首选，但也不能强制让别人使用它。

让每个过滤器生成自己的报头页(因此可以为它们计费)是**仍然不够的**。如果用户想要用 `lpr -h` 命令禁止报头页，它们将仍然印出报头页并且为它们付费。因为**LPD** 不会把 **-h** 这个参数传给任何过滤器。

这样，您该怎么办呢？

您可以：

- 认可**LPD** 的这个问题，并且免费提供报头页打印。
- 安装一个替代**LPD** 的软件，比如**LPRng**。参考替换标准的打印池软件 来得到更多关于可以替代**LPD** 的软件的信息。
- 写一个**聪明的** 输出过滤器。通常，输出过滤器不应该去完成除了初始化打印机或者进行一些简单字符转换以外的任何事情。它适合完成报头页和纯文本任务(当没有文本(输入)过滤器时)。但是，如果有文本过滤器为纯文本任务服务，那么**LPD** 将仅为打印报头页启动输出过滤器。而且，这个输出过滤器可以理解报头页里**LPD** 生成的信息，然后决定哪位用户和主机应该为报头页付费。这种方法仅有的问题是输出过滤器仍然不知道应该使用什么记帐文件(**af** 变量的内容并没有被传递过来)，但是如果您有一个众所周知的记帐文件，就可以直接把文件名写进输出过滤器。为了简化解释报头的步骤，我们定义 **sh** (短报头) 变量在 `/etc/printcap` 文件中。但这些还是太麻烦了，而且用户也更喜欢让他们免费打印报头页的慷慨的系统管理员。

9.4.2.4 在PostScript 打印机上打印报头页

像上面描述的那样，**LPD** 可以生成一个纯文本的报头页来适应多种打印机。当然，PostScript 不能直接打印纯文本，所以**LPD** 没什么用——或者说大多数时候是这样。

一个显而易见的方法来得到报头页就是让每个转换过滤器和文本过滤器都来生成报头页。这些过滤器应该用用户名和主机的参数来生成一个相对应的报头页。这种方法的缺点就是用户总是打印出报头页，无论他们是否用 `lpr -h` 命令来提交的任务。

让我们来深入深入的研究一下这个方法。下面的脚本输入三个参数(用户登陆名, 主机名, 和任务名)然后生成一个简单的PostScript 报头页:

```
#!/bin/sh
#
# make-ps-header - make a PostScript header page on stdout
# Installed in /usr/local/libexec/make-ps-header
#
#
# These are PostScript units (72 to the inch). Modify for A4 or
# whatever size paper you are using:
#
page_width=612
page_height=792
border=72
#
# Check arguments
#
if [ $# -ne 3 ]; then
    echo "Usage: 'basename $0' <user> <host> <job>" 1>&2
    exit 1
fi
#
# Save these, mostly for readability in the PostScript, below.
#
user=$1
host=$2
job=$3
date='date'
#
# Send the PostScript code to stdout.
#
exec cat <<EOF
%!PS
%
% Make sure we do not interfere with user's job that will follow
%
save
%
% Make a thick, unpleasant border around the edge of the paper.
%
$border $border moveto
$page_width $border 2 mul sub 0 rlineto
0 $page_height $border 2 mul sub rlineto
currentscreen 3 -1 roll pop 100 3 1 roll setscreen
$border 2 mul $page_width sub 0 rlineto closepath
0.8 setgray 10 setlinewidth stroke 0 setgray
```

```
%
% Display user's login name, nice and large and prominent
%
/Helvetica-Bold findfont 64 scalefont setfont
$page_width ($user) stringwidth pop sub 2 div $page_height 200 sub moveto
($user) show

%
% Now show the boring particulars
%
/Helvetica findfont 14 scalefont setfont
/y 200 def
[ (Job:) (Host:) (Date:) ] {
  200 y moveto show /y y 18 sub def }
forall

/Helvetica-Bold findfont 14 scalefont setfont
/y 200 def
[ ($job) ($host) ($date) ] {
  270 y moveto show /y y 18 sub def
} forall

%
% That is it
%
restore
showpage
EOF
```

现在，每个转换过滤器和文本过滤器都能调用这段脚本来生成报头页，然后打印用户的任务。下面是我们早些时候在这个文档中提到的DVI转换过滤器，被修改之后来生成一个报头页：

```
#!/bin/sh
#
# psdf - DVI to PostScript printer filter
# Installed in /usr/local/libexec/psdf
#
# Invoked by lpd when user runs lpr -d
#

orig_args="$@"

fail() {
  echo "$@" 1>&2
  exit 2
}

while getopts "x:y:n:h:" option; do
  case $option in
    x|y) ;; # Ignore
    n)   login=$OPTARG ;;
    h)   host=$OPTARG ;;
```

```

        *)      echo "LPD started 'basename $0' wrong." 1>&2
                exit 2
                ;;
    esac
done

[ "$login" ] || fail "No login name"
[ "$host" ] || fail "No host name"

( /usr/local/libexec/make-ps-header $login $host "DVI File"
  /usr/local/bin/dvips -f ) | eval /usr/local/libexec/lprps $orig_args

```

过滤器是怎样解释参数列表来决定用户名和主机名的。解释的方法对于其他转换过滤器来说也是一样的。尽管文本过滤器需要输入的参数有些小的不同, (参见过滤器是怎样工作的)。

像我们以前提到的那样, 上面的配置, 尽管相当简单, 关掉了“禁止报头页”的选项(-h 选项) 在 `lpr` 中。如果用户想要保护树木(或者是几便士, 如果你对打印报头页收费的话), 它还不能完成这件事情, 因为每个过滤器都要为每个任务打印一个报头页。

要允许用户对于每个任务都可以关闭报头页, 您需要使用在为报头页记帐 这节中介绍的那种技巧: 写一个输出过滤器来解释LPD- 生成的报头页并且生成一个PostScript 的版本。如果用户用 `lpr -h` 命令提交任务, 那么LPD 将不会生成报头页, 并且输出过滤器也不会生成报头页。否则, 输出过滤器将从LPD 读取文本, 然后发送适当的报头页的PostScript 编码给打印机。

如果您有的是一台连在串口上的PostScript 打印机, 您可以使用 `lprps` 里的一个输出过滤器, `psuf`, 它可以完成上述任务。但注意 `psuf` 不对报头页计费。

9.4.3 网络打印

FreeBSD 支持网络打印: 发送任务给远程打印机。网络打印通常指两种不同的方式:

- 访问一台连接在远程主机上的打印机。在一台主机上安装一台常规的串行或并行打印机。然后, 设置LPD 来通过网络访问其他主机上的打印机。具体见安装在远程主机上的打印机 这节。
- 访问一台直接连接在网络上的打印机。打印机另有一个网络接口(或者替代常规的串口或者并口)。这样的打印机可能像下面这样工作:
 - 它或许可以理解LPD 的协议, 并且甚至可以接收远程主机发来的任务排进队列。这样, 它就像一个普通的主机运行着LPD 一样。做在安装在远程主机上的打印机 里介绍的步骤, 可以设置好这样的打印机。
 - 它或许支持网络数据流。这样, 把打印机“接”在一台网络上的主机上, 由这台主机负责安排任务并发送任务到打印机。参见带网络数据流接口的打印机 这节来得到更多安装这类打印机的建议。

9.4.3.1 安装在远程主机上的打印机

LPD 打印池系统内建了对给其他也运行着LPD (或者是与LPD 兼容的) 的主机发送任务的功能。这个功能使您可以在一台主机上安装打印机, 并让它可以在其他主机上访问。这个功能同样适用在那些有网络接口并且可以理解LPD 协议的打印机上。

要开启这种远程打印的功能，首先在一台主机上安装打印机，就是**打印主机**，可以使用在简单打印机设置 这节中简单设置的方法。高级的设置可以参考高级打印机设置 这节中你需要的部分。一定要测试一下打印机，看看它是不是所有您开启的**LPD** 的功能都正常工作。同样确定**本地主机** 允许使用**远程主机** 上的**LPD** 服务(参见限制远程打印机任务)。

如果您正在使用一台带网络接口并与**LPD** 兼容的打印机，那么我们那下面讨论中的**打印主机** 就是打印机本身，而**打印机名** 就是您为打印机配置的名字。参考随打印机和/或者打印机-网络接口供给的文档。

提示: 如果您正使用惠普的Laserjet，则打印机名text 将自动地为您完成LF 到CRLF 的转换，因而也就不需要hpif 脚本了。

然后，在另外一台你想要访问打印机的主机上的/etc/printcap 文件中加入它们的记录，像下面这样：

1. 可以随意给这个记录起名字。简单起见，您可以给打印主机使用相同的名字或者别名。
2. 保留lp 变量为空，(:lp=:)。
3. 建立一个打印池目录并且用sd 变量指明它的位置。**LPD** 将把任务存储在这里在它们被送到打印主机之前。
4. 在rm 变量中放入打印主机的名字。
5. 在rp 中放入打印主机上打印机的名字。

就是这样。不需要列出转换过滤器，页面大小，或者其他的一些东西在/etc/printcap 文件中。

这有一个例子。主机rose 有两台打印机，bamboo 和rattan。我们要让主机orchid 的用户可以使用这两台打印机。下面是/etc/printcap 文件，用在主机orchid(详见开启报头页) 上的。文件中已经有了打印机teak 的记录；我们在主机rose 上增加了两台打印机：

```
#
# /etc/printcap for host orchid - added (remote) printers on rose
#

#
# teak is local; it is connected directly to orchid:
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
    :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:\
    :if=/usr/local/libexec/ifhp:\
    :vf=/usr/local/libexec/vfhp:\
    :of=/usr/local/libexec/ofhp:

#
# rattan is connected to rose; send jobs for rattan to rose:
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
    :lp=:rm=rose:rp=rattan:sd=/var/spool/lpd/rattan:

#
# bamboo is connected to rose as well:
#
```



```
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
      :lp=:rm=rose:rp=bamboo:sd=/var/spool/lpd/bamboo:
```

然后, 我们只需要在主机orchid上建立一个打印池目录:

```
# mkdir -p /var/spool/lpd/rattan /var/spool/lpd/bamboo
# chmod 770 /var/spool/lpd/rattan /var/spool/lpd/bamboo
# chown daemon:daemon /var/spool/lpd/rattan /var/spool/lpd/bamboo
```

现在, 主机orchid上的用户可以打印到rattan和bamboo了。如果, 比如, 一个用户在主机orchid上输入了

```
% lpr -P bamboo -d sushi-review.dvi
```

LPD 系统在主机orchid上会复制这个任务到打印池目录/var/spool/lpd/bamboo并且记下这是一个DVI任务。当主机rose上的打印机bamboo的打印池目录有空间的时, 这两个**LPDs**系统将会传输这个文件到主机rose上。文件将排在主机rose的队列中知道最终被打印出来。它将被从DVI转换成PostScript(因为bamboo是一台PostScript打印机)在主机rose。

9.4.3.2 带有网络数据流接口的打印机

通常, 当您为打印机购买了一块网卡, 可以得到两个版本: 一个是模拟打印池(贵一些的版本), 或者一个只发送数据给打印机就像在使用串口或者并口一样(便宜一些的版本)。这节讲述如何使用这个便宜一些的版本。要得到贵一些版本的更多信息, 参见前面章节安装在远程主机上的打印机。

/etc/printcap文件的格式让您指定使用哪个串口或并口, 并且还要指定(如果您正在使用串口), 使用多快的波特, 是否使用流量控制, 为制表符延迟, 转换换行, 等等。但是没有一种方法指定一个连接到一台正在监听TCP/IP的或者其他网络接口的打印机。

要发送数据到网络打印机, 需要开发一个通讯程序, 它可以被文本或者转换过滤器调用。下面是一些例子: 脚本netprint将标准输入的所有数据发送到一个连在网络上的打印机。我们将打印机的名字作为第一个参数, 端口号跟在后面作为第二个参数, 传给netprint。注意它只支持单向通讯(FreeBSD到打印机); 很多网络打印机支持双向通讯, 并且这是您可能利用到的(得到打印机状态, 进行打印记帐, 等等的时候)。

```
#!/usr/bin/perl
#
# netprint - Text filter for printer attached to network
# Installed in /usr/local/libexec/netprint
#
$#ARGV eq 1 || die "Usage: $0 <printer-hostname> <port-number>";

$printer_host = $ARGV[0];
$printer_port = $ARGV[1];

require 'sys/socket.ph';

($ignore, $ignore, $protocol) = getprotobyname('tcp');
($ignore, $ignore, $ignore, $ignore, $address)
    = gethostbyname($printer_host);

$sockaddr = pack('S n a4 x8', &AF_INET, $printer_port, $address);
```

```
socket(PRINTER, &PF_INET, &SOCK_STREAM, $protocol)
|| die "Can't create TCP/IP stream socket: $!";
connect(PRINTER, $sockaddr) || die "Can't contact $printer_host: $!";
while (<STDIN>) { print PRINTER; }
exit 0;
```

然后我们就可以在多种过滤器里使用这个脚本了。加入我们有一台Diablo 750-N 行式打印机联在网络上。打印机在5100 端口上接收要打印的数据。打印机的主机名是scrivener。这里是为这个打印机写的文本过滤器：

```
#!/bin/sh
#
# diablo-if-net - Text filter for Diablo printer 'scrivener' listening
# on port 5100. Installed in /usr/local/libexec/diablo-if-net
#
exec /usr/libexec/lpr/lpf "$@" | /usr/local/libexec/netprint scrivener 5100
```

9.4.4 限制使用打印机

这节将讲述关于限制打印机使用的问题。**LPD** 系统让您控制谁可以访问打印机，无论本地或是远程的，是否他们可以打印多份拷贝，任务可以有多大，和打印机能有多大的队列。

9.4.4.1 限制多份拷贝

LPD 系统使用户要打印文件的多份拷贝变得容易。用户可以用 `lpr -#5` (举例) 来提交打印任务，则会将任务中每个文件都打印五份拷贝。这是不是一件很棒的事情呢。

如果您感觉多份拷贝会对打印机造成不必要的磨损和损耗，您可以屏蔽掉 `lpr(1)` 的 `-#` 选项，通过增加 `sc` 变量在 `/etc/printcap` 文件里。当用户用 `-#` 选项提交任务时，他们将看到：

```
lpr: multiple copies are not allowed
```

注意当为一台远程打印机设置的时候(参见安装在远程主机上的打印机) 这一节，您同时还需要增加 `sc` 变量在远程主机的 `/etc/printcap` 文件中，否则用户将还是可以在其他主机上提交多份拷贝的任务。

下面是一个例子。这个是 `/etc/printcap` 文件在主机 `rose` 上。打印机 `rattan` 非常轻闲，所以我们将允许多份拷贝，但是激光打印机 `bamboo` 则有些忙，所以我们禁止多份拷贝，通过增加 `sc` 变量：

```
#
# /etc/printcap for host rose - restrict multiple copies on bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
    :sh:sd=/var/spool/lpd/rattan:\
    :lp=/dev/lpt0:\
    :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
    :sh:sd=/var/spool/lpd/bamboo:sc:\
    :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:\
    :if=/usr/local/libexec/psif:\
```

```
:df=/usr/local/libexec/psdf:
```

现在, 我们还需要增机sc 变量在主机orchid 的/etc/printcap 文件中(顺便我们也禁止打印机teak 多份打印):

```
#
# /etc/printcap for host orchid - no multiple copies for local
# printer teak or remote printer bamboo
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
    :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:sc:\
    :if=/usr/local/libexec/ifhp:\
    :vf=/usr/local/libexec/vfhp:\
    :of=/usr/local/libexec/ofhp:

rattan|line|diablo|lp|Diablo 630 Line Printer:\
    :lp=:rm=rose:rp=rattan:sd=/var/spool/lpd/rattan:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
    :lp=:rm=rose:rp=bamboo:sd=/var/spool/lpd/bamboo:sc:
```

通过使用sc 变量, 我们阻止了lpr -# 命令的使用, 但仍然没有禁止用户多次运行lpr(1), 或者多次提交任务中同样的文件, 像下面这样:

```
% lpr forsale.sign forsale.sign forsale.sign forsale.sign forsale.sign
```

这里有很多种方法可以阻止这种行为(包括忽略它), 并且是免费的。

9.4.4.2 限制对打印机的访问

您可以控制谁可以打印到哪台打印机通过UNIX 的组机制和文件/etc/printcap 中的rg 变量。只要把可以访问打印机的用户放进适当的组中, 然后在rg 变量中写上组的名字。

非这组的用户(包括root)将会得到这样的问候: lpr: Not a member of the restricted group 如果他们试图打印到被限制的打印机。

像使用sc (禁止多份拷贝) 变量一样, 您需要指定rg 在远程同样对打印机有访问限制的主机上, 如果您感觉合适的话(参考安装在远程主机上的打印机 这一节)。

比如, 我们将让任何人都可以访问打印机rattan, 但只有在artists 组中的人可以使用打印机bamboo。这里是类似的主机rose 上的/etc/printcap 文件:

```
#
# /etc/printcap for host rose - restricted group for bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
    :sh:sd=/var/spool/lpd/rattan:\
    :lp=/dev/lpt0:\
    :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
    :sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:\
    :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:\
    :if=/usr/local/libexec/psif:\
```

```
:df=/usr/local/libexec/psdf:
```

Let us leave the other example `/etc/printcap` file (for the host `orchid`) alone. Of course, anyone on `orchid` can print to `bamboo`. It might be the case that we only allow certain logins on `orchid` anyway, and want them to have access to the printer. Or not.

注意: 这里每台仅能有一个限制的组。

9.4.4.3 控制提交的任务大小

如果您有很多用户访问打印机，可能需要对用户可以提交的文件尺寸设置一个上限。毕竟，文件系统中打印池目录的空间是有限的，您需要保证这里有空间来存放其他用户的任务。

LPD 允许限制任务中文件的最大字节数，通过使用 `mx` 变量。单位为 `BUFSIZ` 块，每块 1024 字节。如果在这个变量中放入 0 值，将没有文件大小的限制；然而，就算没有指定 `mx` 变量，那么默认值 1000 块将被使用。

注意: 这个限制是对于任务中文件的，而不是任务总共的大小。

LPD 不会拒绝比限制大小大的文件。但它是将限制大小以内的部分排入队列，并且打印出来的只有这些。剩下的部分将被丢弃。这个行为是否正确还需讨论。

让我们来为例子打印机 `rattan` 和 `bamboo` 增加限制。由于那些艺术家的 `PostScript` 文件可能会很大，我们将限制大小为 5 兆字节。我们将不对纯文本行式打印机做限制：

```
#
# /etc/printcap for host rose
#

#
# No limit on job size:
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
    :sh:mx#0:sd=/var/spool/lpd/rattan:\
    :lp=/dev/lpt0:\
    :if=/usr/local/libexec/if-simple:

#
# Limit of five megabytes:
#
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
    :sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:mx#5000:\
    :lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:\
    :if=/usr/local/libexec/psif:\
    :df=/usr/local/libexec/psdf:
```

同样，限制只对本地用户起作用。如果远程设置了限制，远程用户将不会受到这些限制。您也需要指定`mx`变量在远程主机的`/etc/printcap`文件中。参见安装在远程主机上的打印机这一节来得到更多有关远程打印的信息。

这里还有一种限制远程任务大小的方法；参见限制远程打印机任务。

9.4.4.4 限制远程打印机任务

LPD 打印池系统提供了多种方法来限制从远程主机提交的任务：

主机限制

您可以控制本地**LPD**接收哪台远程主机发来的请求，通过`/etc/hosts.equiv`文件和`/etc/hosts.lpd`文件。**LPD**查看是否到来的任务请求来自被这两个文件中列出的主机。如果没有，**LPD**会拒绝这个请求。

这些文件的格式非常简单：每行一个主机名。注意`/etc/hosts.equiv`文件也被`ruserok(3)`协议使用，并影响着`rsh(1)` and `rcp(1)`等程序，所以要小心。

举个例子，下面是`/etc/hosts.lpd`文件在主机`rose`上：

```
orchid
violet
madrigal.fishbaum.de
```

意思是主机`rose`将接收来自`orchid`，`violet`，和`madrigal.fishbaum.de`的请求。如果任何其他的主机试图访问主机`rose`的**LPD**，任务将被拒绝。

大小限制

您可以控制打印池目录需要保留多少空间。建立一个叫做`minfree`的文件在打印池目录下为本地打印机。在这个文件中插入一个数字来代表多少磁盘块数(512字节)的剩余空间来接收远程任务。

这让您可以保证远程用户不会填满您的文件系统。您也可以用它来给本地用户一个优先：他们可以在磁盘剩余空间低于`minfree`文件中的指定值后仍然可以提交任务。

比如，让我们增加一个`minfree`文件为打印机`bamboo`。我们检查`/etc/printcap`文件来找到这个打印机的打印池目录；这里是打印机`bamboo`的记录：

```
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
:sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:mx#5000:\
:lp=/dev/ttyd5:ms#-parenb cs8 clocal crtscts:rw:mx#5000:\
:if=/usr/local/libexec/psif:\
:df=/usr/local/libexec/psdf:
```

打印池目录在`sd`变量中给出。我们设置3兆字节(6144磁盘块)为文件系统上必须存在的总共剩余空间，让**LPD**可以接受远程任务：

```
# echo 6144 > /var/spool/lpd/bamboo/minfree
```

用户限制

您可以控制哪些远程用户可以打印到本地打印机，通过指定`rs`变量在`/etc/printcap`文件中。当`rs`出现在一个本地打印机的记录中时，**LPD**将接收来自远程主机并在本地有同样登陆名的用户提交的任务。否则，**LPD**会拒绝这个任务。

这个功能在一个(比如)有许多部门共享一个网络的环境中特别有用,并且有些用户可以越过部门的边界。通过为他们在您的系统上建立帐号,他们可以他们自己的部门的系统里使用您的打印机。如果只允许他们您的打印机,而不是您的计算机资源,您可以给他们“象征”帐户,不带主目录并且设置一个没用的shell,比如`/usr/bin/false`。

9.4.5 对打印机使用记帐

当然,您需要对打印付费。为什么不?纸张和墨水都需要花钱的。并且这里还有维护的费用——打印机是由很多部件组装成的,并且零件会坏掉。您可以检查您的打印机,使用形式,和维护费用来得出每页(或者每尺,每米,或者每什么)的费用。现在,您怎样启动打印记帐呢?

好了,坏消息是**LPD**打印池系统在这个部分没有提供很多帮助。记帐是一个对使用的打印机的种类,打印的格式,和您的在对打印机的使用计费的需求依赖性很高的。

要实现记帐,您必须更改打印机的文本过滤器(对纯文本任务计费)和转换过滤器(对其他格式的文件计费),要统计页数或者查询打印了多少页的话。您不可以通过使用简单的输出过滤器来逃脱计费,因为它不能进行记帐。参见过滤器 这节。

通常,有两种方法来进行记帐:

- **定期记帐** 是更常用的方法,可能因为它更简单。无论合适何人打印一个任务,过滤器都将记录用户名,主机名,和打印的页数到一个记帐文件。每个月,学期,年,或者任何您想设定的时间段,收集这些不同打印机上的记帐文件,按用户对打印的页数进行结算,并对使用进行付费。然后删掉所有记录文件,开始一个新的计费周期。
- **实时记帐** 不太常用,可能因为它比较难。这种方法让过滤器对用户的打印进行实时的记帐。像磁盘配额,记帐是实时的。您可以组织用户打印当他们的帐户超额的时候,并且可能提供一种方法让用户检查并调整他们的“打印配额。”但这个方法需要一些数据库代码来跟踪用户和他们的配额。

LPD打印池系统对两种方法都支持且很简单:所以您需要提供过滤器(大多数时候),还要提供记帐代码。但这好的方面是:您可以有非常灵活的记帐方法。比如,您可以选择使用阶段记帐还是实时记帐。您可以选择记录哪些信息:用户名,主机名,任务类型,打印页数,使用了多少平方尺的纸,任务打印了多长时间,等等。您可以通过修改过滤器来存储这些信息。

9.4.5.1 快速并且混乱的打印记帐

FreeBSD 包含两个可以让您立刻可以建立起简单的阶段记帐的程序。它们是文本过滤器**lpf**,在**lpf**: 一个文本过滤器 这节中描述,和**pac(8)**,一个收集并统计打印机记帐文件中记录的程序。

像在前面章节提到的过滤器一样(过滤器),**LPD**启动文本或者转换过滤器并在过滤器命令行里带上记帐文件的名字。过滤器可以使用这个参数知道该往哪写记帐记录。这个文件的名字来自于**af**变量在**/etc/printcap**文件里,并且如果没有指定绝对路径,则默认是相对于打印池目录的。

LPD启动**lpf**带着页宽和页长的参数(通过**pw**和**pl**变量)。**lpf**使用这些参数来判定将使用多少张纸。在文件发送到打印机之后,它就会在记帐文件中写入记录。记录像下面这个样子:

```
2.00 rose:andy
3.00 rose:kelly
3.00 orchid:mary
5.00 orchid:mary
2.00 orchid:zhang
```

您应该让每个打印机都使用一个独立的记帐文件，像 **lpf** 就没有内建文件锁逻辑，这样两个 **lpf** 可能会发生彼此记录混合的情况，如果它们同时要在同一个文件写入内容的时候。一个最简单的保证每个打印机都使用一个独立的记帐文件的方法就是将 **af=acct** 写在 **/etc/printcap** 文件中。然后，每个打印机的记帐文件都会在这台打印机的打印池目录中，文件的名字叫做 **acct**。

当您准备对用户的打印进行收费时，运行 **pac(8)** 程序。只要转换到要收集信息的这台打印机的打印池目录，然后输入 **pac**。您将会得到一个美元计费的摘要像下面这样：

Login	pages/feet	runs	price
orchid:kelly	5.00	1	\$ 0.10
orchid:mary	31.00	3	\$ 0.62
orchid:zhang	9.00	1	\$ 0.18
rose:andy	2.00	1	\$ 0.04
rose:kelly	177.00	104	\$ 3.54
rose:mary	87.00	32	\$ 1.74
rose:root	26.00	12	\$ 0.52
total	337.00	154	\$ 6.74

这些时 **pac(8)** 需要的参数：

-P 打印机

哪台打印机要结帐。这个选项仅在用 **af** 变量在 **/etc/printcap** 文件中指定了绝对路径的情况下起作用。

-c

以金额来排序输出来代替以用户名字字母排序。

-m

忽略记帐文件中的主机名。带上这个选项，用户 **smith** 在主机 **alpha** 上与同样的用户 **smith** 在主机 **gamma** 上一样。不带这个选项的话，他们则是不同的用户。

-p 单价

使用 **price** 作为每页或每尺美元的单价来替代 **pc** 变量指定的单价在 **/etc/printcap** 文件中，或者两分(默认)。**price** 可以用一个浮点数来指定。

-r

反向排序。

-s

建立一个记帐摘要文件，并且截短记帐文件。

名字...

只打印指定名字用户的记帐信息。

在 **pac(8)** 默认产生的摘要中，可以看到在不同主机上的每个用户打印了多少页。如果在您这里，主机不考虑(因为用户可以使用任何主机)，运行 **pac -m**，来得到下面的摘要：

Login	pages/feet	runs	price
-------	------------	------	-------

andy	2.00	1	\$ 0.04
kelly	182.00	105	\$ 3.64
mary	118.00	35	\$ 2.36
root	26.00	12	\$ 0.52
zhang	9.00	1	\$ 0.18
total	337.00	154	\$ 6.74

要以美元计算应付钱数，`pac(8)` 指定 `pc` 变量在 `/etc/printcap` 文件中(默认是200，或者2分每页). 这个参数的单位是百分之一分，在这个变量中指定每页或者每尺的价格。您可以覆盖这个值当运行 `pac(8)` 带着参数 `-p` 的时候。参数 `-p` 的单位是美元，而不是百分之一分。例如，

```
# pac -p1.50
```

设定每页的价格是1美元5美分。您可以通过这个选项来达到目标利润。

最终，运行 `pac -s` 将存储这些信息在一个记帐文件里，文件名和打印机帐户的名字相同，但是带着 `_sum` 的后缀。然后截短记帐文件。当您再次运行 `pac(8)` 的时候，它再次读取记帐文件来得到初始的总计，然后在记帐文件中增加信息。

9.4.5.2 怎样对打印的页数进行计数？

为了进行远程的精确记帐，需要判断一个任务将会消耗多少张纸。这是打印记帐问题的关键。

对于纯文本任务，这个问题不是太难解决：对任务中的行数进行计数然后与打印机支持的每页行数进行比较。别忘了也对添印的行，或者很长的逻辑上的一行但在打印机上会折成两行的这类进行记帐。

文本过滤器 `lpf` (在 `lpf`: 一个文本过滤器 这节中介绍) 会在记帐时考虑这些问题。如果正在编写一个可以进行记帐的文本过滤器，您可能需要查看 `lpf` 的源代码。

怎样处理其他格式的文件？

好，对于 `DVI`- 到-`LaserJet` 或者 `DVI`- 到-`PostScript` 转换，可以让您的过滤器输出诊断信息，关于 `dvilj` 或者 `dvips` 命令，并且看到多少页被转换了。您也许可以对于其他类型的文件和转换程序进行类似操作。

但是这些方法的弱点就是事实上打印机并不是打印了所有的页。比如，卡纸，缺墨，或者炸掉了——但用户还是要为没有打印的部分付钱。

您该怎样做？

只有一条肯定 的方法来进行精确 的记帐。购买一台可以告诉您它使用了多少纸的打印机，并且将它连接到串口或者网络上。几乎所有 `PostScript` 打印机都支持这个小功能。其他制造厂或其他型号也可以有这个功能(比如 `Imagen` 激光网络打印机)。为这些打印机更改过滤器使它在打印完每个任务之后接收纸张用量，并仅 基于这个值进行记帐。不需要计算行数，也不需要容易出错的文件检查。

当然，您也总是可以大方的使打印免费。

9.5 使用打印机

这节将讲述如何使用在 `FreeBSD` 下设置好的打印机。下面是一个用户级命令的总览：

`lpr(1)`

打印任务

`lpq(1)`

检查打印队列

`lprm(1)`

从打印机的队列中移除任务

还有一个管理命令，`lpc(8)`，在管理打印机一节中有所介绍，它可以用于控制打印机及其队列。

`lpr(1)`, `lprm(1)`, and `lpq(1)` 这三个命令都接受 `-P printer-name` 选项来指定对哪个打印机/队列进行操作，在 `/etc/printcap` 文件中列出的打印机。这允许您提交，删除，并检查任务在多个打印机上。如果您不使用 `-P` 选项，那么这些命令会使用在环境变量 `PRINTER` 中指定的打印机。最终，如果您也没有 `PRINTER` 这个环境变量，这些命令的默认值是叫做 `lp` 的这台打印机。

从此以后，术语**默认打印机**就是指 `PRINTER` 环境变量中指定的这台，或者叫做 `lp` 的这一台当没有环境变量 `PRINTER` 的时候。

9.5.1 打印任务

要打印文件，输入：

```
% lpr filename ...
```

这个命令会打印所有列出的文件到默认打印机。如果没有列出文件，`lpr(1)` 会从标准输入读取打印数据。比如，这个命令打印一些重要的系统文件：

```
% lpr /etc/host.conf /etc/hosts.equiv
```

要选择一个指定的打印机，输入：

```
% lpr -P printer-name filename ...
```

这个例子打印一个当前目录的长长的列表到叫做 `rattan` 的这台打印机：

```
% ls -l | lpr -P rattan
```

因为没有为 `lpr(1)` 命令列出文件，`lpr` 从标准输入读入数据，在这里是 `ls -l` 命令的输出。

`lpr(1)` 命令同样可以接受多种控制格式的选项，应用文件转换，生成多份拷贝，等等。要得到更多信息，参考打印选项 这节。

9.5.2 检查任务

当使用 `lpr(1)` 进行打印时，您希望打印的所有数据被放在一起打包成了一个“打印任务”，它被发送到 **LPD** 打印池系统。每台打印机都有一个任务队列，并且您的任务在队列中等待其他用户的其他任务打印。打印机按照先来先印的规则打印这些任务。

要显示默认打印机的队列，输入 `lpq(1)`。要指定打印机，使用 `-P` 选项。例如，命令

```
% lpq -P bamboo
```

会显示打印机bamboo的队列。下面是命令lpq输出的一个例子：

```
bamboo is ready and printing
Rank  Owner   Job  Files                                Total Size
active kelly    9    /etc/host.conf, /etc/hosts.equiv  88 bytes
2nd    kelly    10    (standard input)                 1635 bytes
3rd    mary     11    ...                               78519 bytes
```

这里显示了队列中有三个任务在bamboo中。第一个任务，用户kelly提交的，标识“任务编号”9。每个要打印的任务都会获得一个不同的任务编号。大多时候可以忽略这个任务编号，但在您需要取消任务时会用到这个号码；参考移除任务 这节得到更多信息。

编号为9的任务包含了两个文件；在lpr(1)命令行中指定的多个文件被看作是一个单个的任务。它是当前激活的任务(注意这个词激活在“Rank”这列下面)，意思是打印机当前正在打印那个任务。第二个任务包含了标准输入传给lpr(1)命令的数据。第三个任务来自用户mary；，它是一个比较大的任务。她要打印的文件的路径名太长了，所以lpq(1)命令只显示了三个点。

lpq(1)输出的头一行也很有用：它告诉我们打印机正在做什么(或者至少是LPD认为打印机应该正在做的)。

lpq(1)命令同样支持-l选项来生成一个详细的长列表。下面是一个lpq -l命令的例子：

```
waiting for bamboo to become ready (offline ?)
kelly: 1st  [job 009rose]
          /etc/host.conf                73 bytes
          /etc/hosts.equiv              15 bytes

kelly: 2nd  [job 010rose]
          (standard input)              1635 bytes

mary: 3rd   [job 011rose]
          /home/orchid/mary/research/venus/alpha-regio/mapping 78519 bytes
```

9.5.3 移除任务

如果您对一个打印任务改变了主意，可以用lprm(1)将任务从队列中删除。通常，您甚至可以用lprm(1)命令来移除一个当前激活的任务，但是任务的一部分或者所有还是可能打印出来。

要从默认打印机中移除一个任务，首先使用lpq(1)找到任务编号。然后输入：

```
% lprm job-number
```

要从指定打印机中删除任务，增加-P选项。下面的命令会删除编号为10的任务从bamboo这台打印机：

```
% lprm -P bamboo 10
```

lprm(1)命令有一些快捷方式：

```
lprm -
```

删除所有属于您的任务(默认打印机的)。

`lprm user`

删除所有属于用户`user`的任务(默认打印机的)。超级用户可以删除用户的任务；您只可以删除自己的任务。

`lprm`

命令行中不带任务编号，任务名，或者-选项，`lprm(1)`会删除默认打印机上当前激活的任务，如果它属于你。超级用户可以删除任务激活的任务。

使用参数`-P`和上面的快捷方式来指定打印机替代默认打印机。例如，下面的命令会删除当前用户在打印机`rattan`队列中的所有任务：

```
% lprm -P rattan -
```

注意：如果您正工作在一个网络环境中，`lprm(1)`将只允许在提交任务的主机上删除任务，甚至是同一台打印机也可以在其他主机上使用时。下面的命令证明了这个：

```
% lpr -P rattan myfile
% rlogin orchid
% lpq -P rattan
Rank  Owner  Job  Files          Total Size
active seeyan  12  ...      49123 bytes
2nd   kelly   13  myfile      12 bytes
% lprm -P rattan 13
rose: Permission denied
% logout
% lprm -P rattan 13
dfA013rose dequeued
cfA013rose dequeued
```

9.5.4 超越纯文本：打印选项

`lpr(1)`支持许多控制文本格式的选项，转换图形和其他格式文件，生成多份拷贝，处理任务，等等。这一节将描述这些选项。

9.5.4.1 格式与转换选项

下面的`lpr(1)`参数控制任务中文件的格式。使用这些参数，如果任务不含纯文本，或者您想让纯文本通过`pr(1)`格式化。

例如，下面的命令打印一个DVI文件(来自`TEX`排版系统)文件名为`fish-report.dvi`到打印`bamboo`：

```
% lpr -P bamboo -d fish-report.dvi
```

这些选项应用到任务中的每个文件，所以您不能混合(说)DVI和`ditroff`文件在同一个任务中。替代的方法是，用独立的任务提交这些文件，使用不同的转换选项给不同的任务。

注意：所有这些选项除了`-p`和`-T`都需要转换过滤器安装给目标打印机。例如，`-d`选项需要DVI转换过滤器。参考转换过滤器 这节得到更多细节。

-c

打印cifplot 文件。

-d

打印DVI 文件。

-f

打印FORTRAN 文本文件。

-g

打印plot 数据。

-i *number*

缩进*number* 列；如果没有指定*number*，则缩进8 列。这个选项仅可以工作在某些过滤器上。

注意：不要在选项-i 和数字之间加入空格。

-l

打印文字数据，包括控制字符。

-n

打印ditroff (无设备依赖troff) 数据。

-p

打印之前用pr(1) 格式化纯文本。参考pr(1) 得到更多信息。

-T *title*

使用*title* 在pr(1) 上来替代文件名。这个选项仅在使用-p 选项时起作用。

-t

打印troff 数据。

-v

打印raster 数据。

下面是一个例子：这个命令打印了一个很好的ls(1) 手册页面到默认打印机：

```
% zcat /usr/share/man/man1/ls.1.gz | troff -t -man | lpr -t
```

zcat(1) 命令解压缩ls(1) 的手册并且将内容传给troff(1) 命令，它将格式化这些内容并且生成GNU troff 输出给lpr(1)，它提交任务到L^{PD} 打印池。因为使用了-t 选项为lpr(1)，打印池将会转换GNU troff 输出到默认打印机可以理解的格式当任务被打印时。

9.5.4.2 任务处理选项

下面的`lpr(1)`选项告诉**LPD**对任务特殊处理:

`-# copies`

生成`copies`个副本给任务中的每个文件，替代每个文件一份拷贝。管理员可以禁止这个选项来减少打印机的浪费和鼓励复印机的使用。参考限制多份拷贝。

这个例子打印三份拷贝的文件`parser.c`跟着三份拷贝的文件`parser.h`到默认打印机:

```
% lpr -#3 parser.c parser.h
```

`-m`

打印完成后发信。使用这个选项，**LPD**系统将会发送邮件到您的帐户，当它完成了处理您的任务后。在信中，它将会告诉您任务是否成功完成或者出现了错误，并且(通常)指明是什么错误。

`-s`

不要复制文件到打印池目录，要使用符号连接。

如果您正在打印一个很大的任务，您可能需要这个选项。它节省打印池目录的空间(您的任务可能使打印池目录所在的文件系统剩余空间超出)。它同样也节省了时间，因为**LPD**将不会拷贝任务的每个字节到打印池目录。

这也有一个缺点：因为**LPD**将直接指向源文件，您不能修改或者删除它们直到它们被打印出来。

注意: 如果您打印到一台远程打印机，**LPD**将最终将文件从本地主机拷贝到远程主机上，所以选项`-s`只能节省本地打印池目录的空间，而不是远程的。虽然如此，但它还是很有用。

`-t`

移除任务中的文件在它们被复制到打印池目录之后，或者在用`-s`选项打印它们之后。谨慎使用这个选项！

9.5.4.3 报头页选项

这些`lpr(1)`的选项调整了通常出现在任务报头页上的文本。如果报头页被跳过了在目标打印机上，这些选项将不会起作用。参考报头页 得到更多关于设置报头页的信息。

`-C text`

替换报头页上的主机名为`text`。主机名通常都是提交任务的主机名称。

`-J text`

替换报头页上的任务名为`text`。任务名通常是任务中头一个文件的名称，或者`stdin`如果您正在打印标准输入。

-h

不打印任何报头页。

注意: 在某些地点, 这个选项可能无效, 与报头页的产生方法有关。参考报头页 得到详细信息。

9.5.5 管理打印机

作为一个打印机的管理者, 您必须要安装, 设置, 并且测试它们。使用lpc(8) 命令, 您可以与打印机以更多的方式交流。用lpc(8), 您可以

- 启动或停止打印机
- 启用或禁止它们的队列
- 重新安排每个队列中的任务。

首先, 一个关于术语的解释: 如果一个打印机被**停止**了, 它将不会打印它队列中的任何东西。但用户还是可以提交任务, 它们会在队列中等待直到打印机被**启动** 或者队列被清空。

如果一个队列被**禁止**, 没有用户(除了root) 可以提交任务到打印机。一个**启用** 的队列允许任务被提交。一个打印机可以被**启动** 但它的队列被禁止, 在这种情况下打印机将打印队列中的任务知道队列为空。

通常, 您必须有root 权限来使用lpc(8) 命令。普通用户可以使用lpc(8) 命令来获得打印机状态并且重启一台挂了的打印机。

这里是一个关于lpc(8) 命令的摘要。大部分命令带着一个*printer-name* 参数来知道要对哪台打印机操作。您可以用all 填在*printer-name* 的位置来代表所有在/etc/printcap 文件中列出的打印机。

abort *printer-name*

取消当前任务并停止打印机。用户仍然可以提交任务, 如果队列还是启用的。

clean *printer-name*

从打印机的打印池目录移除旧的文件。有时, 组成任务的文件没有被LPD 正确的删除, 特别是在打印中出现错误或者管理活动比较多时候。这个命令查找不属于打印池目录的文件并删除它们。

disable *printer-name*

禁止新任务入队。如果打印机正在工作, 它将会继续打印队列中剩余的任务。超级用户(root) 总是可以提交任务, 甚至提交到一个禁止的队列。

这个命令在测试一台新打印机或者安装过滤器时非常有用: 禁止队列并提交以root 提交任务。其他用户将不能提交任务直到您完成了测试并用命令enable 重新启用了队列的时候。

down *printer-name message*

打印机下线。等于disable 命令后跟一个stop 命令。*message* 将作为打印机状态, 当用户使用lpq(1) 或者lpc status 命令查看打印机队列状态的时候显示出来。

enable printer-name

为打印机开启队列。用户可以提交任务到打印机但是在打印机启动之前不会打印出任何东西。

help command-name

打印关于**command-name** 命令的帮助。不带**command-name**，则打印可用命令的摘要。

restart printer-name

启动打印机。普通用户可以使用这个命令，当一些特别的环境导致**LPD** 锁死时，但他们不能启用一台使用**stop** 或者**down** 命令停用的打印机。**restart** 命令等同于**abort** 后跟着一个**start**。

start printer-name

启用打印机。打印机将开始打印队列中的任务。

stop printer-name

停止打印机。打印机将完成当前任务并且将不再打印队列中的任务任务。尽管打印机被停用，但用户仍然可以提交任务到一个开启的队列。

topq printer-name job-or-username

重新以**printer-name** 安排队列，通过将列出的**job** 编号或者指定的所属**username** 的任务放在队列的最前面。对于这个命令，您不可以使用**all** 当作**printer-name**。

up printer-name

打印机上线；相对于**down** 命令。等同于**start** 后跟着一个**enable** 命令。

lpc(8) 的命令行接受上面的命令。如果您不输入任何命令，**lpc(8)** 则进入一个交互模式，在这里您可以输入命令直到输入**exit**，**quit**，或者文件结束符。

9.6 替换标准打印池

如果您已经通读过了这个手册，那么到现在您应该已经了解了关于FreeBSD 包含的打印池系统**LPD** 的一切。您可能发现了它很多的缺点，它们很自然的让您提出这样的问题：“这里还有什么打印池系统吗(并且可以工作在FreeBSD 上)？”

LPRng

LPRng，它的意思是“LPR：下一代”，是一个完全重写的PLP。Patrick Powell 和Justin Mason (PLP 维护的主要负责人) 合作完成了**LPRng**。**LPRng** 的主站是<http://www.lprng.org/>。

CUPS

CUPS，通用UNIX 打印系统，提供了一个轻便的打印层给UNIX-基础的操作系统。它是由Easy Software Products 开发的，并且成为了UNIX 供应商和用户的标准打印解决方案。

CUPS 使用Internet 打印协议(IPP) 作为管理打印任务和队列的基础。行式打印机守护程序(LPD) 服务器消息块(SMB)，和AppSocket (a.k.a. JetDirect) 协议的部分功能也被支持。**CUPS** 增加了基于浏览网络打印机和PostScript 打印机描述(PPD) 的打印选项来支持UNIX 下的真实打印。

CUPS 的主站是<http://www.cups.org/>。

9.7 疑难问题

在使用lpctest(1) 进行简单的测试之后，您可能得到了下面的结果，而不是正确的结果：

过了一会儿，它工作了；或者，它没有退出一整张纸。

打印机进行了打印，但在这之前它呆了一段而且什么都没做。事实上，您可能需要按一下打印机上的打印剩余或者送纸按钮来让结果出现。

如果这是问题所在，打印机可能在等待在打印之前任务是否还有更多的数据。要修正这个问题，您可以让文本过滤器发送一个送纸字符(或者其他需要的) 到打印机。这通常足够让打印机立即打印出内部缓存内剩余的文本。它同样可以用来确保每个任务的结尾都占用一整张纸，这样下一个任务才不会在前一个任务最后一张纸的中间开始。

接下来的shell 脚本/usr/local/libexec/if-simple 的脚本打印了一个送纸符在它发送任务到打印机之后：

```
#!/bin/sh
#
# if-simple - Simple text input filter for lpd
# Installed in /usr/local/libexec/if-simple
#
# Simply copies stdin to stdout. Ignores all filter arguments.
# Writes a form feed character (\f) after printing job.

/bin/cat && printf "\f" && exit 0
exit 2
```

它的输出产生了“楼梯效果。”

您可能在纸上得到下面这些：

```
! "$%&'()*+,-./01234
      "$%&'()*+,-./012345
                "$%&'()*+,-./0123456
```

您也成为了**楼梯效果**的受害者，这是由对新行的标志字符的解释不一致造成的。UNIX 风格的操作系统使用一个单个字符：ASCII 码10，即换行(LF)。MS-DOS，OS/2®，和其他的系统使用一对儿字符，ASCII 码10 和 ASCII 码13 (回车CR)。许多打印机使用MS-DOS 的习惯来代表新行。

当您在FreeBSD 上打印时，您的文本仅用了换行字符。打印机，打印机看到换行字符后，走一行纸，但还光标位置还是在这张纸上要打印的下一个字符处。这就是回车的作用：将下一个要打印的字符的位置移到纸张的左边缘。

这里是FreeBSD 想要打印机做的：

打印机收到CR	打印机打印CR
打印机收到LF	打印机打印CR + LF

下面有几种完成这个的办法：

- 使用打印机的配置开关或者控制面板来更改它对这些字符的解释。查看打印机的手册来找到怎样更改。

注意：如果您引导您的系统到其他除了FreeBSD 之外的操作系统，您可能不得不**重新配置** 打印机使用这个操作系统对CR 和LF 字符的解释。您可能更喜欢下面这另一种解决方案。

- 让FreeBSD 的串口驱动自动转换LF 到CR+LF。当然，这仅仅 工作在串口打印机上。要开启这个功能，定义ms# 变量并设置onlcr 模式在/etc/printcap 文件中相应打印机处。
- 发送一个转义码 到打印机来让它临时对LF 字符做不同的处理。参考您的打印机手册来了解您的打印机支持哪些转义码。当您找到合适的转义码，修改文本过滤器让其先发送这个转义码，然后再发送打印任务。

这里是一个为懂得Hewlett-Packard PCL 转义码的打印机编写的文本过滤器。这个过滤器使得打印机将LF 作为一个LF 和一个CR 来对待；然后它发送任务；最后发送一个送纸符弹出任务的最后一张纸。它应该可以在几乎所有Hewlett Packard 打印机上工作。

```
#!/bin/sh
#
# hpif - Simple text input filter for lpd for HP-PCL based printers
# Installed in /usr/local/libexec/hpif
#
# Simply copies stdin to stdout. Ignores all filter arguments.
# Tells printer to treat LF as CR+LF. Ejects the page when done.

printf "\033&k2G" && cat && printf "\033&l0H" && exit 0
exit 2
```

下面是一个/etc/printcap 文件的例子在叫做orchid的主机上。它只有一台打印机连接在第一个并口上，一台Hewlett Packard LaserJet 3Si 名字叫做teak。它使用上面那段脚本作为文本过滤器：

```
#
# /etc/printcap for host orchid
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
    :lp=/dev/lpt0:sh:sd=/var/spool/lpd/teak:mx#0:\
    :if=/usr/local/libexec/hpif:
```

行行覆盖。

打印机从来不进纸换行。所有的文本都打印在头一行文本的上面。

这个问题是“相反”于楼梯效果，像上面描述的那样，并且更少见。一些地方，LF 这个FreeBSD 用来结束一行的字符被作为CR 这个将打印位置返回到纸的左边的字符对待。而没有向下走纸一行。

使用打印机的配置开关或者控制面板来强制对LF 和CR 进行下面的转换：

打印机收到	打印机打印
CR	CR
LF	CR + LF

打印丢掉字符。

当打印时，每行里打印机都丢掉一些字符没有打。这个问题可能随着打印的进行越发严重，丢掉越来越多的字符。

这个问题是由打印机跟不上计算机通过串口发送数据的速度造成的(这个问题应该不会发生在并口打印机上)。有两种方法能克服这个问题:

- 如果打印机支持XON/XOFF 流量控制, 那就让FreeBSD 使用它, 通过加入ixon 模式在ms# 变量里。
- 如果打印机支持载波流量控制, 指定crtscts 模式在ms# 变量里。并且要确定连接打印机和计算机的线是支持载波流量控制的。

它打印出垃圾。

打印机打印出的东西看起来是一些随机的字符, 而不是想要打印的东西。

这通常意味着另一种串口打印机通讯参数设置不正确的错误。复查br 变量中设定的波特, 和ms# 中的校验设置; 确定打印机也在使用和/etc/printcap 文件中相同的设置。

没有反应。

如果没有反应, 问题就可能出在FreeBSD 而不是硬件上了。增加日志文件(lf) 变量到/etc/printcap 文件里出现问题的打印机的记录处。比如, 下面是打印机rattan 的记录, 使用了lf 变量:

```
rattan|line|diablo|lp|Diablo 630 Line Printer:\
:sh:sd=/var/spool/lpd/rattan:\
:lp=/dev/lpt0:\
:if=/usr/local/libexec/if-simple:\
:lf=/var/log/rattan.log
```

然后, 再次打印。检查日志文件(在我们的例子当中, 是/var/log/rattan.log 这个文件) 来看是否有错误信息出现。根据出现的信息, 试着来修正问题。

如果您没有指定lf 变量, **LPD** 会使用/dev/console 作为默认值。

第10章

Linux 二进制兼容模式

Restructured and parts updated by Jim Mock. Originally contributed by Brian N. Handy 和 Rich Murphey.

10.1 概述

FreeBSD 提供了与其他几种类UNIX 操作系统，包括Linux，的兼容性。现在您可能会问，为什么FreeBSD 需要能够运行Linux 的可执行文件？答案很简单。许多公司和开发人员只为Linux 开发程序，因为这是目前计算机世界“最热门”的技术。这使得我们FreeBSD 用户不得不去劝说这些公司和开发人员提供他们应用程序可以直接在FreeBSD 上运行的版本。问题是，许多这样的公司并不真的知道到底提供了FreeBSD 版本之后能带来多少用户，因此许多仍然只开发Linux 的版本。这时FreeBSD 用户能做什么呢？答案就是使用FreeBSD 所提供的Linux 二进制兼容性。

简而言之，这种兼容性能够让FreeBSD 用户不加修改地直接运行大约90% 的Linux 应用程序。这包括类似StarOffice，Linux 版本的Netscape，Adobe Acrobat，RealPlayer®，VMware™，Oracle，WordPerfect®，Doom，Quake，等等。此外，也有人说，某些情况下，在FreeBSD 上面运行的Linux 程序的性能，甚至好于直接在Linux 上面运行。

然而，仍然有一些只有Linux 才有的操作系统特性在FreeBSD 上并不被支持。如果Linux 程序过分地使用只能在i386 上使用的特性，例如启用虚拟8086 模式，则也有可能无法在FreeBSD 上运行。

读完这章，您将了解到：

- 如何在您的系统中启用Linux兼容模式。
- 如何安装额外的Linux共享库。
- 如何在FreeBSD上安装Linux应用程序。
- 在FreeBSD上，Linux兼容模式的执行细节。

阅读这章之前，您应该知道：

- 如何安装第三方软件（第4 章）。

10.2 安装

默认情况下，并不开启Linux 二进制兼容支持。启用这一功能最简单的方法是载入linux KLD 模块(“Kernel Loadable object”)。以root 的身份，键入下列命令即可：

```
# kldload linux
```

如果希望Linux 兼容支持在系统初始化过程中自动启用，则应在/etc/rc.conf 中增加：

```
linux_enable="YES"
```

kldstat(8)可以用来检查KLD模块是否加载：

```
% kldstat
Id Refs Address      Size      Name
  1    2 0xc0100000 16bdb8    kernel
  7    1 0xc24db000 d000      linux.ko
```

如果您不想或者无法将Linux KLD加载，您就需要在内核中静态链接进Linux二进制兼容模式。您必须在您的内核配置文件里面加入`options COMPAT_LINUX`，然后按照第8章重新编译内核。

10.2.1 安装Linux运行时库

有两种方法来安装Linux运行时库，要么使用linux_base port，要么手动安装。

10.2.1.1 通过使用linux_base Port 来安装

这是最容易的安装方法，只需要像安装其他port一样从Ports Collection (/usr/ports/)来安装：

```
# cd /usr/ports/emulators/linux_base
# make install distclean
```

您现在应当是工作在Linux兼容模式下了。一些程序可能会提示系统库的版本不正确。通常，这不是问题。

注意：有多个版本的emulators/linux_base port，针对不同的版本的Linux。您应该选择最接近Linux应用程序需要的那个版本来安装。

10.2.1.2 手动安装

如果您没有安装Ports Collection，您也可以通过手动来安装Linux运行时库。您将需要这些程序依赖的Linux共享库，而且您需要创建一个“shadow root”目录`/compat/linux`，任何要被Linux程序打开的共享库都首先在这个目录里面查找。所以，如果一个Linux程序加载了，例如，`/lib/libc.so`，FreeBSD会首先尝试打开`/compat/linux/lib/libc.so`，如果不存在，它将尝试打开`/lib/libc.so`。共享库应该安装在`/compat/linux/lib`而不是Linux `ld.so`报告的其他路径。

通常，您需要寻找Linux程序依赖的共享库。此后，你的系统上就会有一组Linux共享库，这组共享库足以用来运行新安装的Linux二进制程序。

10.2.1.3 如何安装额外的共享库

如果您安装了linux_base port，但是您的应用程序仍会报告丢失共享库的信息？您如何知道Linux程序需要哪个共享库？基本上，有两种可能性（接下来的指令需要root权限）：

如果您有可以访问的Linux系统，看看应用程序需要什么共享库，把它们拷贝到您的FreeBSD系统。看下面的例子：

我们假设您通过FTP得到Linux程序**Doom**，并把它放在您能访问的Linux系统上。然后您可以通过`ldd linuxdoom`来检查需要哪些共享库，就像这样：

```
% ldd linuxdoom
libXt.so.3 (DLL Jump 3.1) => /usr/X11/lib/libXt.so.3.1.0
```

```
libX11.so.3 (DLL Jump 3.1) => /usr/X11/lib/libX11.so.3.1.0
libc.so.4 (DLL Jump 4.5pl26) => /lib/libc.so.4.6.29
```

您需要得到上面输出的右列的所有文件，并把它们拷贝到`/compat/linux`，第一列的名字用符号连接指向它们。这样您的FreeBSD系统上就有了这些文件：

```
/compat/linux/usr/X11/lib/libXt.so.3.1.0
/compat/linux/usr/X11/lib/libXt.so.3 -> libXt.so.3.1.0
/compat/linux/usr/X11/lib/libX11.so.3.1.0
/compat/linux/usr/X11/lib/libX11.so.3 -> libX11.so.3.1.0
/compat/linux/lib/libc.so.4.6.29
/compat/linux/lib/libc.so.4 -> libc.so.4.6.29
```

注意：如果您已经有了一个与`ldd`输出的第一列的主修订号相匹配的Linux共享库，您将不需要把右列命名的文件拷贝到您的系统，您已经完成了工作。如果有一个新的版本，那无论如何都要拷贝一个共享库。您可以删掉旧的，您只要做一个符号连接到新的版本。所以，如果有这些库在您的系统上：

```
/compat/linux/lib/libc.so.4.6.27
/compat/linux/lib/libc.so.4 -> libc.so.4.6.27
```

如果您根据`ldd`输出的发现需要一个更新版本的库：

```
libc.so.4 (DLL Jump 4.5pl26) -> libc.so.4.6.29
```

如果结尾的数字只有一到两个版本过期，那也不要担心拷贝`/lib/libc.so.4.6.29`，因为程序在稍微旧一些的版本上也能很好地工作。然而，如果喜欢的话，您可以替换`libc.so`，变成这样：

```
/compat/linux/lib/libc.so.4.6.29
/compat/linux/lib/libc.so.4 -> libc.so.4.6.29
```

注意：符号链接机制仅仅是Linux程序需要的。FreeBSD的运行时连接器会自己寻找匹配的主修订号，您不需要为此担心。

10.2.2 安装Linux ELF程序

ELF格式的程序需要一步额外的步骤“标记”。如果您尝试运行没有标记的ELF程序，您会得到像下面这样的错误信息：

```
% ./my-linux-elf-binary
ELF binary type not known
Abort
```

为了帮助FreeBSD内核分辨FreeBSD ELF程序和Linux程序，要使用`brandelf(1)`工具：

```
% brandelf -t Linux my-linux-elf-binary
```

GNU工具现在会自动把适当的标记信息放到ELF程序中，您以后遇到这个问题的机会越来越少。

10.2.3 配置主机名解析器

如果DNS不能正常工作或是您得到下列信息:

```
resolv+: "bind" is an invalid keyword resolv+:
"hosts" is an invalid keyword
```

您就需要配置`/compat/linux/etc/host.conf`文件, 此文件包含:

```
order hosts, bind
multi on
```

`order`这一行指出`/etc/hosts`先被搜索紧接着搜索DNS。如果`/compat/linux/etc/host.conf`没有被安装, Linux程序会读取FreeBSD的`/etc/host.conf`然后提示不兼容的FreeBSD语法。如果您没有使用`/etc/resolv.conf`文件设置DNS, 应该删除`bind`。

10.3 安装Mathematica®

Updated for Mathematica 5.X by Boris Hollas.

这份文档介绍了如何在FreeBSD 系统中安装Linux 版本的**Mathematica 5.X**。

Linux 版本的**Mathematica** 或**Mathematica for Students** 可以直接从Wolfram 的<http://www.wolfram.com/>订购。

10.3.1 运行Mathematica 安装程序

首先您应告诉FreeBSD **Mathematica** 的Linux 可执行文件需要使用Linux ABI。达到这一目的最简单的办法, 是将未加标志的可执行文件的默认ELF 标记为Linux, 输入下面的命令:

```
# sysctl kern.fallback_elf_brand=3
```

这回让FreeBSD 假定所有未加标志的ELF 可执行文件, 都应使用Linux ABI, 这样就可以直接从CDROM 执行安装程序了。

接下来, 需要将MathInstaller 复制到硬盘上:

```
# mount /cdrom
# cp /cdrom/Unix/Installers/Linux/MathInstaller /localdir/
```

在这个文件的第一行中, 将`/bin/sh` 改为`/compat/linux/bin/sh`。这样就能确保安装程序是使用Linux 版本的`sh(1)` 来运行的。接下来, 使用文本编辑器或下面的脚本, 把所有的Linux) 替换为FreeBSD)。由于**Mathematica** 安装程序会调用`uname -s` 来检测操作系统, 这样做能够让它视FreeBSD 为一种类-Linux 操作系统。现在执行MathInstaller 就能安装**Mathematica** 了。

10.3.2 修改Mathematica 执行文件

在安装**Mathematica** 的过程中所创建的脚本, 必须首先进行适当的修改才能使用。如果您选择将`/usr/local/bin` 作为**Mathematica** 可执行文件的安装路径, 则可以在这个目录中找到一些到名

为math、mathematica、Mathematica，以及MathKernel的文件的符号连接。您可以使用文本编辑器，或者下面的shell脚本来将这些文件中的Linux) 改为FreeBSD):

```
#!/bin/sh
cd /usr/local/bin
for i in math mathematica Mathematica MathKernel
do sed 's/Linux)/FreeBSD)/g' $i > $i.tmp
sed 's/\\bin\\sh\\/compat\\/linux\\/bin\\/sh/g' $i.tmp > $i
rm $i.tmp
chmod a+x $i
done
```

10.3.3 获得您的Mathematica 密码

在首次启动**Mathematica**时，您将被问及一个密码。如果您还未从Wolfram获得密码，则安装目录中的mathinfo可以帮助您获得“machine ID”(计算机ID)。这个计算机ID取决于您第一块以太网的MAC地址，以确保您不在多台机器上运行**Mathematica**。

在通过电子邮件、电话或传真向Wolfram注册时，您需要向他们提供“machine ID”，随后它们会给您一个与之对应的由一组数字组成的密码。

10.3.4 通过网络来运行Mathematica

Mathematica使用一些特殊的字体来显示字符，与现在使用的标准字体不一样(integrals, sums, Greek letters,等等)。X协议要求将这些字体安装在本地。这意味着您需要从**Mathematica**的CDROM里面拷贝这些字体并安装到本地。这些字体一般在CDROM的/cdrom/Unix/Files/SystemFiles/Fonts里面，或本地硬盘的/usr/local/mathematica/SystemFiles/Fonts。实际的字体在Type1和X子目录。有很多种方法来使用它们。

第一种方法是把字体拷贝到一个已存在的目录/usr/X11R6/lib/X11/fonts。这需要编辑fonts.dir文件。添加字体名字进去，并改变第一行的字体数目。另外，您也需要在拷贝字体的目录下执行mkfontdir(1)。

第二种方法是拷贝目录到/usr/X11R6/lib/X11/fonts:

```
# cd /usr/X11R6/lib/X11/fonts
# mkdir X
# mkdir MathType1
# cd /cdrom/Unix/Files/SystemFiles/Fonts
# cp X/* /usr/X11R6/lib/X11/fonts/X
# cp Type1/* /usr/X11R6/lib/X11/fonts/MathType1
# cd /usr/X11R6/lib/X11/fonts/X
# mkfontdir
# cd ../MathType1
# mkfontdir
```

现在，添加新的字体目录到您的字体目录:

```
# xset fp+ /usr/X11R6/lib/X11/fonts/X
# xset fp+ /usr/X11R6/lib/X11/fonts/MathType1
# xset fp rehash
```

如果您正使用**Xorg** 服务器，则可以通过修改**xorg.conf** 文件来自动加载它们。

注意：对于**XFree86** 服务器，配置文件的名字是**XF86Config**。

如果您没有一个叫**/usr/X11R6/lib/X11/fonts/Type1**的目录，您可以把**MathType1**改成**Type1**。

10.4 安装MapleTM

Contributed by Aaron Kaplan. Thanks to Robert Getschmann.

MapleTM是一个类似于**Mathematica**的商业数学软件。您可以从<http://www.maplesoft.com/>买到这个软件并注册得到一个使用许可。要在**FreeBSD**上安装这个软件，请按照下面的步骤：

1. 从软件的发行包执行**INSTALL** shell脚本。当进入安装程序的提示符时，选择“RedHat”选项。典型的安装目录是**/usr/local/maple**。
2. 如果您不这样做，可以从Maple Waterloo Software (<http://register.maplesoft.com/>)为**Maple**订购一个许可。然后拷贝到**/usr/local/maple/license/license.dat**。
3. 通过运行**Maple**中的**INSTALL_LIC**安装shell脚本来安装**FLEXlm**许可管理器。指定许可服务器为您的机器名。
4. 像下面这样Patch您的**/usr/local/maple/bin/maple.system.type**文件：

```
----- snip -----
*** maple.system.type.orig      Sun Jul  8 16:35:33 2001
--- maple.system.type    Sun Jul  8 16:35:51 2001
*****
*** 72,77 ***
--- 72,78 ----
        # the IBM RS/6000 AIX case
        MAPLE_BIN="bin.IBM_RISC_UNIX"
        ;;
+   "FreeBSD"|\
    "Linux")
        # the Linux/x86 case
        # We have two Linux implementations, one for Red Hat and
----- snip end of patch -----
```

请注意**"FreeBSD"|**后面没有空格。

这个补丁指示**Maple**把“FreeBSD”识别为一种Linux系统。**bin/maple** shell脚本调用**bin/maple.system.type**脚本执行**uname -a**来查找操作系统名，根据操作系统名，就知道该使用哪个程序。

5. 启动许可服务器。

下面的脚本，安装成**/usr/local/etc/rc.d/lmgrd.sh**，是很方便的启动**lmgrd**的方法：

```
----- snip -----

#! /bin/sh
```



```
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin
PATH=${PATH}:/usr/local/maple/bin:/usr/local/maple/FLEXlm/UNIX/LINUX
export PATH
```

```
LICENSE_FILE=/usr/local/maple/license/license.dat
LOG=/var/log/lmgrd.log
```

```
case "$1" in
start)
lmgrd -c ${LICENSE_FILE} 2>> ${LOG} 1>&2
echo -n " lmgrd"
;;
stop)
lmgrd -c ${LICENSE_FILE} -x lmdown 2>> ${LOG} 1>&2
;;
*)
echo "Usage: 'basename $0' {start|stop}" 1>&2
exit 64
;;
esac
```

```
exit 0
----- snip -----
```

6. 开始测试Maple:

```
% cd /usr/local/maple/bin
% ./xmaple
```

您应该成功启动起来了。记得写信告诉Maplesoft您想要一个本地FreeBSD版本！

10.4.1 一些缺陷

- **FLEXlm**许可管理器可能是一个使用比较困难的工具。关于它的额外的文档可以在<http://www.globetrotter.com/>找到。
- **lmgrd**对许可文件非常挑剔，有一点问题就会core dump。正确的许可文件看起来像下面这样：

```
# =====
# License File for UNIX Installations ("Pointer File")
# =====
SERVER chillig ANY
#USE_SERVER
VENDOR maplelmg

FEATURE Maple maplelmg 2000.0831 permanent 1 XXXXXXXXXXXX \
    PLATFORMS=i86_r ISSUER="Waterloo Maple Inc." \
    ISSUED=11-may-2000 NOTICE=" Technische Universitat Wien" \
    SN=XXXXXXXXXX
```

注意：序列号被'X'代替了。chillig是主机名。

只要不修改“FEATURE”行，编辑后一般都能工作。

10.5 安装MATLAB®

Contributed by Dan Pelleg.

这一节描述在一个FreeBSD上安装Linux版本的**MATLAB® version 6.5**。它工作的很好，除了**Java Virtual Machine™**例外（参考第10.5.3节）。

Linux版本的**MATLAB**可以从MathWorks<http://www.mathworks.com>订购。请确定您也得到了许可文件或安装说明。等您成功后，让他们知道您想要一个本地FreeBSD版本。

10.5.1 安装MATLAB

请按照下面的步骤安装**MATLAB**：

1. 以root身份插入安装CD并挂载上。推荐使用安装脚本，为了启动安装脚本，键入：

```
# /compat/linux/bin/sh /cdrom/install
```

提示：安装程序是图形的。如果您得到不能打开显示的错误，可以键入`setenv HOME ~USER`，`USER`是您su(1)成的用户。

2. 当问**MATLAB**的根目录时，键入：`/compat/linux/usr/local/matlab`。

提示：为了下面的安装过程更方便，在Shell提示符下键入`set MATLAB=/compat/linux/usr/local/matlab`

3. 根据获得**MATLAB**许可时的指示来编辑许可文件。

提示：您可以用您喜欢的编辑器提前准备这个文件，并在安装程序要您编辑它之前拷贝到**\$MATLAB/license.dat**

4. 完成安装过程

到这里，您的**MATLAB**安装已经完成了。接下来的步骤是让它和您的FreeBSD系统“胶合”在一起。

10.5.2 许可管理器的启动

1. 为许可管理器建立符号链接的脚本：

```
# ln -s $MATLAB/etc/lmboot /usr/local/etc/lmboot_TMW
# ln -s $MATLAB/etc/lmdown /usr/local/etc/lmdown_TMW
```

2. 建立启动文件`/usr/local/etc/rc.d/flexlm.sh`。下面的例子是一个\$MATLAB/etc/rc.lm.glnx86的修改版本。变化的是文件的位置，和模拟Linux下许可管理器的启动。

```
#!/bin/sh
case "$1" in
  start)
    if [ -f /usr/local/etc/lmboot_TMW ]; then
      /compat/linux/bin/sh /usr/local/etc/lmboot_TMW -u username && echo 'MATLAB_lmgrd'
    fi
    ;;
  stop)
    if [ -f /usr/local/etc/lmdown_TMW ]; then
      /compat/linux/bin/sh /usr/local/etc/lmdown_TMW > /dev/null 2>&1
    fi
    ;;
  *)
    echo "Usage: $0 {start|stop}"
    exit 1
    ;;
esac

exit 0
```

重要: 必须使脚本文件可执行:

```
# chmod +x /usr/local/etc/rc.d/flexlm.sh
```

您也必须替换`username`为机器上的一个用户（不要是`root`）。

3. 用命令启动许可管理器:

```
# /usr/local/etc/rc.d/flexlm.sh start
```

10.5.3 链接Java运行时环境

改变Java运行时环境（JRE），链接到一个可以工作的版本:

```
# cd $MATLAB/sys/java/jre/glnx86/
# unlink jre; ln -s ./jre1.1.8 ./jre
```

10.5.4 创建MATLAB启动脚本

1. 把下面的启动脚本放到`/usr/local/bin/matlab`:

```
#!/bin/sh
/compat/linux/bin/sh /compat/linux/usr/local/matlab/bin/matlab "$@"
```

2. 然后输入命令`chmod +x /usr/local/bin/matlab`。

提示: 依赖于您的emulators/linux_base版本, 您在运行这个脚本时可能会出错, 为了避免错误, 编辑/compat/linux/usr/local/matlab/bin/matlab, 把这行:

```
if [ 'expr "$lscmd" : '.*->.*'' -ne 0 ]; then
```

(在13.0.1版本是在第410行) 改成:

```
if test -L $newbase; then
```

10.5.5 Creating a MATLAB Shutdown Script

The following is needed to solve a problem with MATLAB not exiting correctly.

1. Create a file \$MATLAB/toolbox/local/finish.m, and in it put the single line:

```
! $MATLAB/bin/finish.sh
```

注意: The \$MATLAB is literal.

提示: In the same directory, you will find the files finishsav.m and finishdlg.m, which let you save your workspace before quitting. If you use either of them, insert the line above immediately after the save command.

2. Create a file \$MATLAB/bin/finish.sh, which will contain the following:

```
#!/usr/compat/linux/bin/sh
(sleep 5; killall -1 matlab_helper) &
exit 0
```

3. Make the file executable:

```
# chmod +x $MATLAB/bin/finish.sh
```

10.5.6 使用MATLAB

现在您已经可以键入matlab 并开始使用它了。

10.6 安装Oracle®

Contributed by Marcel Moolenaar.

10.6.1 前言

这节描述在FreeBSD上安装Linux版的Oracle 8.0.5和Oracle 8.0.5.1 Enterprise Edition。

10.6.2 安装Linux环境

确信您已经从Ports Collection 安装了emulators/linux_base 和devel/linux_devtools。如果在使用这些port时遇到困难，您可能就不得不从package，或使用较早版本的Ports Collection 来安装。

如果要运行智能代理，您还需要安装Red Hat Tcl 软件包：tcl-8.0.3-20.i386.rpm。用于安装官方的RPM (archivers/rpm) 软件包的命令是：

```
# rpm -i --ignoreos --root /compat/linux --dbpath /var/lib/rpm package
```

包的安装通常不会出错。

10.6.3 创建Oracle环境

安装Oracle之前，您需要设置正确的环境。这节只描述了在FreeBSD下安装Linux版本Oracle需要特别注意的地方。不像在Oracle安装指南中所描述的那样。

10.6.3.1 调整内核

正如Oracle安装指南描述的那样，您需要设置共享内存的最大值。不要在FreeBSD下使用SHMMAX，SHMMAX 只是用来计算SHMMAXPGS和PGSIZE的。因此要使用SHMMAXPGS。所有其他要使用的选项可以参考指南，例如：

```
options SHMMAXPGS=10000
options SHMMNI=100
options SHMSEG=10
options SEMMNS=200
options SEMMNI=70
options SEMMSL=61
```

设置这些选项来适应Oracle的使用。

当然，确信您的内核配置文件中有下列这些选项：

```
options SYSVSHM #SysV shared memory
options SYSVSEM #SysV semaphores
options SYSVMSG #SysV interprocess communication
```

10.6.3.2 Oracle帐号

创建一个oracle帐号，正如您创建其他帐号一样。oracle 帐号特殊的地方是您需要给它一个Linux shell。添加/compat/linux/bin/bash到/etc/shells，然后设置oracle帐号的shell为/compat/linux/bin/bash。

10.6.3.3 环境

除了普通的Oracle变量外，比如ORACLE_HOME和ORACLE_SID，您还必须设置下面的环境变量：

变量	值
LD_LIBRARY_PATH	\$ORACLE_HOME/lib

变量	值
CLASSPATH	\$ORACLE_HOME/jdbc/lib/classes111.zip
PATH	/compat/linux/bin /compat/linux/sbin /compat/linux/usr/bin /compat/linux/usr/sbin /bin /sbin /usr/bin /usr/sbin /usr/local/bin \$ORACLE_HOME/bin

建议在.profile里面设置所有的环境变量。一个完整的例子是:

```
ORACLE_BASE=/oracle; export ORACLE_BASE
ORACLE_HOME=/oracle; export ORACLE_HOME
LD_LIBRARY_PATH=$ORACLE_HOME/lib
export LD_LIBRARY_PATH
ORACLE_SID=ORCL; export ORACLE_SID
ORACLE_TERM=386x; export ORACLE_TERM
CLASSPATH=$ORACLE_HOME/jdbc/lib/classes111.zip
export CLASSPATH
PATH=/compat/linux/bin:/compat/linux/sbin:/compat/linux/usr/bin
PATH=$PATH:/compat/linux/usr/sbin:/bin:/sbin:/usr/bin:/usr/sbin
PATH=$PATH:/usr/local/bin:$ORACLE_HOME/bin
export PATH
```

10.6.4 安装Oracle

由于Linux 模拟器的一处小小的差异,您必须在/var/tmp 中创建一个名为.oracle 的目录才能够启动安装程序。需要把它设置为属于oracle 用户。接下来,您就可以毫无问题地安装Oracle 了。如果您遇到问题,请首先检查Oracle 软件包和/或配置文件!安装完Oracle 之后,使用下面两节中所说的补丁。

一个比较常见的问题是TCP 协议适配器安装不正确。其结果是将无法进行任何的TCP 侦听。下面的操作将帮助解决此问题:

```
# cd $ORACLE_HOME/network/lib
# make -f ins_network.mk ntcontab.o
# cd $ORACLE_HOME/lib
# ar r libnetwork.a ntcontab.o
# cd $ORACLE_HOME/network/lib
# make -f ins_network.mk install
```

不要忘了再运行一下root.sh!

10.6.4.1 修补root.sh

从CD安装Oracle时,一些工作需要root下执行,这些工作都被记录在一个叫root.sh的脚本里面。这个脚本被写在oraInst目录。为了使用root.sh来正确定位chown或在Linux本地shell下执行脚本,应该对它进行修补。

```
*** oraInst/root.sh.orig Tue Oct 6 21:57:33 1998
--- oraInst/root.sh Mon Dec 28 15:58:53 1998
*****
*** 31,37 ****
# This is the default value for CHOWN
```

```
# It will redefined later in this script for those ports
# which have it conditionally defined in ss_install.h
! CHOWN=/bin/chown
#
# Define variables to be used in this script
--- 31,37 ----
# This is the default value for CHOWN
# It will redefined later in this script for those ports
# which have it conditionally defined in ss_install.h
! CHOWN=/usr/sbin/chown
#
# Define variables to be used in this script
```

当您不从CD安装**Oracle**时，您可以从源代码来修补root.sh。它叫做rthd.sh，定位在源代码树的orainst目录。

10.6.4.2 修补gencIntsh

gencIntsh脚本用来创建一个简单的共享客户端库。在建立demos时被使用。完成补丁后就注释掉了下面的PATH变量：

```
*** bin/gencIntsh.orig Wed Sep 30 07:37:19 1998
-- bin/gencIntsh Tue Dec 22 15:36:49 1998
*****
*** 32,38 ****
#
# Explicit path to ensure that we're using the correct commands
#PATH=/usr/bin:/usr/ccs/bin export PATH
! PATH=/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin export PATH
#
# each product MUST provide a $PRODUCT/admin/shrept.lst
--- 32,38 ----
#
# Explicit path to ensure that we're using the correct commands
#PATH=/usr/bin:/usr/ccs/bin export PATH
! #PATH=/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin export PATH
#
# each product MUST provide a $PRODUCT/admin/shrept.lst
```

10.6.5 运行Oracle

如果您已经按上面的指示去操作，您应该可以像在Linux下运行**Oracle**了。

10.7 安装SAP® R/3®

Contributed by Holger Kipp. Original version converted to SGML by Valentino Vaschetto.

在FreeBSD上安装的SAP系统不会被SAP支持团队——所支持他们只支持某些特定的平台。

10.7.1 前言

这篇文章描述了在FreeBSD系统上安装一个带有**Oracle Database** for Linux的**SAP R/3 System**，包括FreeBSD的安装和**Oracle**的安装。下面将描述两个不同的配置：

- 在FreeBSD 4.3-STABLE上安装带有**Oracle 8.0.5**的**SAP R/3 4.6B (IDES)**。
- 在FreeBSD 4.5-STABLE上安装带有**Oracle 8.1.7**的**SAP R/3 4.6C**。

虽然这篇文章深入地描述了许多重要的安装步骤，但它不能取代**Oracle**和**SAP R/3**的安装指南。

请参考**SAP R/3 Linux edition**自带的文档和**Oracle**的特殊问题。

10.7.2 软件

下面的CD-ROMs被用作**SAP**的安装：

10.7.2.1 SAP R/3 4.6B, Oracle 8.0.5

名称	号码	描述
KERNEL	51009113	SAP Kernel Oracle / Installation / AIX, Linux, Solaris
RDBMS	51007558	Oracle / RDBMS 8.0.5.X / Linux
EXPORT1	51010208	IDES / DB-Export / Disc 1 of 6
EXPORT2	51010209	IDES / DB-Export / Disc 2 of 6
EXPORT3	51010210	IDES / DB-Export / Disc 3 of 6
EXPORT4	51010211	IDES / DB-Export / Disc 4 of 6
EXPORT5	51010212	IDES / DB-Export / Disc 5 of 6
EXPORT6	51010213	IDES / DB-Export / Disc 6 of 6

此外，我们使用**Oracle 8 Server**（Linux版本的8.0.5预览版，Linux内核是2.0.33）和FreeBSD 4.3-STABLE。

10.7.2.2 SAP R/3 4.6C SR2, Oracle 8.1.7

名称	号码	描述
KERNEL	51014004	SAP Kernel Oracle / SAP Kernel Version 4.6D / DEC, Linux
RDBMS	51012930	Oracle 8.1.7/ RDBMS / Linux

名称	号码	描述
EXPORT1	51013953	Release 4.6C SR2 / Export / Disc 1 of 4
EXPORT1	51013953	Release 4.6C SR2 / Export / Disc 2 of 4
EXPORT1	51013953	Release 4.6C SR2 / Export / Disc 3 of 4
EXPORT1	51013953	Release 4.6C SR2 / Export / Disc 4 of 4
LANG1	51013954	Release 4.6C SR2 / Language / DE, EN, FR / Disc 1 of 3

依赖于您要安装的语言，可能需要额外的语言CDs。这儿我们只使用DE和EN，所以只需要第一张语言CD。还要注意的是所有EXPORT CDs的号码是一样的。其他3张语言CDs的号码也一样（这和4.6B IDES release CD的号码不同）。

10.7.3 SAP Notes

安装使用SAP R/3之前，请先看看下面的注释：

10.7.3.1 SAP R/3 4.6B, Oracle 8.0.5

号码	标题
0171356	SAP Software on Linux: Essential Comments
0201147	INST: 4.6C R/3 Inst. on UNIX - Oracle
0373203	Update / Migration Oracle 8.0.5 --> 8.0.6/8.1.6 LINUX
0072984	Release of Digital UNIX 4.0B for Oracle
0130581	R3SETUP step DIPGNTAB terminates
0144978	Your system has not been installed correctly
0162266	Questions and tips for R3SETUP on Windows NT / W2K

10.7.3.2 SAP R/3 4.6C, Oracle 8.1.7

号码	标题
0015023	Initializing table TCPDB (RSXP0004) (EBCDIC)
0045619	R/3 with several languages or typefaces
0171356	SAP Software on Linux: Essential Comments
0195603	RedHat 6.1 Enterprise version: Known problems
0212876	The new archiving tool SAPCAR
0300900	Linux: Released DELL Hardware
0377187	RedHat 6.2: important remarks

号码	标题
0387074	INST: R/3 4.6C SR2 Installation on UNIX
0387077	INST: R/3 4.6C SR2 Inst. on UNIX - Oracle
0387078	SAP Software on UNIX: OS Dependencies 4.6C SR2

10.7.4 硬件要求

下面的设备配置对SAP R/3 System来说已经足够了。如果用于生产用途，就需要更强的配置：

组件	4.6B	4.6C
处理器	2 x 800MHz Pentium III	2 x 800MHz Pentium III
内存	1GB ECC	2GB ECC
Hard Disk Space	50-60GB (IDES)	50-60GB (IDES)

用于生产使用，就需要使用带大缓存的Xeon处理器，和高速大容量磁盘（SCSI, RAID hardware controller），以及USV 和ECC-RAM内存。配置IDES System前需要大量的硬盘空间，因为安装时将创建27 GB的数据库文件。这些空间用于系统和数据的初始化也是足够的。

10.7.4.1 SAP R/3 4.6B, Oracle 8.0.5

对于这个安装，我的硬件配置如下：带2个800 MHz Pentium III处理器的主板，Adaptec® 29160 Ultra160 SCSI适配器（能够访问40/80 GB DLT磁带机和CDROM），Mylex® AcceleRAID™（2个通道，firmware 6.00-1-00 with 32 MB RAM）。Mylex RAID controller被挂上2个17 GB（mirrored）硬盘和4个36 GB硬盘(RAID level 5)。

10.7.4.2 SAP R/3 4.6C, Oracle 8.1.7

对于这个安装，配置是Dell™ PowerEdge™ 2500，带2个1000 MHz Pentium III处理器的主板（256 kB Cache），2 GB PC133 ECC SDRAM，PERC/3 DC PCI RAID Controller with 128 MB，和一个EIDE DVD-ROM驱动器。RAID controller被挂上2个18 GB硬盘（mirrored）和4个36 GB硬盘（RAID level 5）。

10.7.5 安装FreeBSD

首先需要安装FreeBSD。有很多方法来完成这个工作(FreeBSD 4.3 通过FTP 安装，而FreeBSD 4.5 则是从RELEASE CD 安装的)。要了解进一步的情况请参考第2.13 节。

10.7.5.1 磁盘划分

为了简单，对SAP R/3 46B和SAP R/3 46C SR2的安装使用相同的磁盘划分。只是设备名换了，因为是安装在不同的硬件上(/dev/da 和/dev/amr，所以如果是使用AMI MegaRAID®，我们能看到/dev/amr0s1a代替了/dev/da0s1a)：

文件系统	尺寸(1k-blocks)	尺寸(GB)	挂载点
------	---------------	--------	-----

文件系统	尺寸(1k-blocks)	尺寸(GB)	挂载点
/dev/da0s1a	1.016.303	1	/
/dev/da0s1b		6	swap
/dev/da0s1e	2.032.623	2	/var
/dev/da0s1f	8.205.339	8	/usr
/dev/da1s1e	45.734.361	45	/compat/linux/oracle
/dev/da1s1f	2.032.623	2	/compat/linux/sapmnt
/dev/da1s1g	2.032.623	2	/compat/linux/usr/sap

预先用Mylex 或PERC/3 RAID 软件配置和初始化这两个逻辑驱动器。改变BIOS的引导顺序来启动软件。

请注意这里的磁盘划分和SAP推荐的是不一样的，SAP建议把Oracle子目录（及其他子目录）分离开来，我决定只简单的创建几个子目录。

10.7.5.2 make world和建立新内核

下载最新的-STABLE源代码，配置完内核配置文件后重建系统和新内核。这儿当然要包括SAP R/3和Oracle需要的内核参数。

10.7.6 安装Linux环境

10.7.6.1 安装Linux基本系统

首先linux_base port需要安装（以root身份）：

```
# cd /usr/ports/emulators/linux_base
# make install distclean
```

10.7.6.2 安装Linux开发环境

如果您想根据第10.6 节在FreeBSD上安装Oracle：

```
# cd /usr/ports/devel/linux_devtools
# make install distclean
```

Linux开发环境只是安装给SAP R/3 46B IDES的，如果Oracle DB不是在这个FreeBSD系统上重新链接，它就不需要了。

10.7.6.3 安装必需的RPMs

为了启动R3SETUP程序，PAM支持是必需的。第一次安装SAP到FreeBSD 4.3-STABLE时我们先安装了PAM的所有依赖包再安装PAM包，它可以工作。对于SAP R/3 4.6C SR2我们直接安装PAM RPM也可以工作，所以依赖包不是必需的：

```
# rpm -i --ignoreos --nodeps --root /compat/linux --dbpath /var/lib/rpm \
```

pam-0.68-7.i386.rpm

要让**Oracle 8.0.5**运行智能代理，我们需要安装RedHat Tcl包tcl-8.0.5-30.i386.rpm（否则重新链接**Oracle**不能工作）。重新链接**Oracle**时还有其他要注意的地方，但那是**Oracle Linux**的问题，不是FreeBSD的问题。

10.7.6.4 其它一些注意的地方

添加linprocfs 到/etc/fstab 是个好主意。要了解进一步的细节，请参考linprocfs(5) 联机手册。另一个是设置kern.fallback_elf_brand=3，这可以通过/etc/sysctl.conf 文件来完成。

10.7.7 创建SAP R/3环境

10.7.7.1 创建必需的文件系统和挂载点

对简单的安装，创建下面的文件系统就够了：

mount point	size in GB
/compat/linux/oracle	45 GB
/compat/linux/sapmnt	2 GB
/compat/linux/usr/sap	2 GB

创建一些链接也是必要的，否则**SAP**安装程序在检查创建的链接时会报错：

```
# ln -s /compat/linux/oracle /oracle
# ln -s /compat/linux/sapmnt /sapmnt
# ln -s /compat/linux/usr/sap /usr/sap
```

安装时可能出现的错误（对于**PRD**系统和**SAP R/3 4.6C SR2** 的安装）：

```
INFO 2002-03-19 16:45:36 R3LINKS_IND_IND SyLinkCreate:200
Checking existence of symbolic link /usr/sap/PRD/SYS/exe/dbg to
/sapmnt/PRD/exe. Creating if it does not exist...

WARNING 2002-03-19 16:45:36 R3LINKS_IND_IND SyLinkCreate:400
Link /usr/sap/PRD/SYS/exe/dbg exists but it points to file
/compat/linux/sapmnt/PRD/exe instead of /sapmnt/PRD/exe. The
program cannot go on as long as this link exists at this
location. Move the link to another location.

ERROR 2002-03-19 16:45:36 R3LINKS_IND_IND Ins_SetupLinks:0
can not setup link '/usr/sap/PRD/SYS/exe/dbg' with content
'/sapmnt/PRD/exe'
```

10.7.7.2 创建用户和目录

SAP R/3需要两个用户和3个组。用户名依赖于包含3个字母的**SAP**系统ID（SID）。一些SIDs 被**SAP**保留（例如**SAP**和**NIX**）。完成的列表参考**SAP**文档。对于**IDES**的安装，我们使用**IDS**，对于**4.6C SR2**安装，使用**PRD**。这样我们定义了下面的几个组：

组ID	组名	描述
100	dba	Data Base Administrator
101	sapsys	SAP System
102	oper	Data Base Operator

对于默认的**Oracle**安装，只有**dba**组被使用。和**oper**组一样，我们也可以使用**dba**组（更详细的信息参考**Oracle**和**SAP**文档）。

我们也需要下面的用户

用户ID	用户名	普通名称	组	附加组	描述
1000	idsadm/prdadm	<i>sidadm</i>	sapsys	oper	SAP Administrator
1002	oraid/oraprd	<i>orasid</i>	dba	oper	Oracle Administrator

使用adduser(8)添加用户要求 “SAP Administrator” 有下面的记录（请注意shell和home目录）：

```
Name: sidadm
Password: *****
Fullname: SAP Administrator SID
Uid: 1000
Gid: 101 (sapsys)
Class:
Groups: sapsys dba
HOME: /home/sidadm
Shell: bash (/compat/linux/bin/bash)
```

对于 “Oracle Administrator”：

```
Name: orasid
Password: *****
Fullname: Oracle Administrator SID
Uid: 1002
Gid: 100 (dba)
Class:
Groups: dba
HOME: /oracle/sid
Shell: bash (/compat/linux/bin/bash)
```

在您使用组**dba**和**oper**的情况下您也应该包括**oper**。

10.7.7.3 创建目录

这些目录通常建立在不同的文件系统上。这完全依赖于您的需求。我们选择把它们建立在同一个目录:

首先我们将设置一些目录的所有者和权限（以root身份设置）:

```
# chmod 775 /oracle
# chmod 777 /sapmnt
# chown root:dba /oracle
# chown sidadm:sapsys /compat/linux/usr/sap
# chmod 775 /compat/linux/usr/sap
```

然后我们以orasid身份创建目录，这些目录将成为/oracle/SID的子目录:

```
# su - orasid
# cd /oracle/SID
# mkdir mirrlogA mirrlogB origlogA origlogB
# mkdir sapdata1 sapdata2 sapdata3 sapdata4 sapdata5 sapdata6
# mkdir saparch sapreorg
# exit
```

对于Oracle 8.1.7的安装，需要一些额外的目录:

```
# su - orasid
# cd /oracle
# mkdir 805_32
# mkdir client stage
# mkdir client/80x_32
# mkdir stage/817_32
# cd /oracle/SID
# mkdir 817_32
```

注意: 目录client/80x_32必须是这个名字，不要用其他数字或字母来替换x。

第三步我们要以sidadm身份创建目录:

```
# su - sidadm
# cd /usr/sap
# mkdir SID
# mkdir trans
# exit
```

10.7.7.4 /etc/services中的条目

SAP R/3在/etc/services里面需要一些条目，这些不会在安装过程中被正确设置，请添加下面的条目:

```
sapdp00    3200/tcp # SAP Dispatcher.      3200 + Instance-Number
sapgw00    3300/tcp # SAP Gateway.        3300 + Instance-Number
sapsp00    3400/tcp #                      3400 + Instance-Number
```

```
sapms00 3500/tcp # 3500 + Instance-Number
sapmsSID 3600/tcp # SAP Message Server. 3600 + Instance-Number
sapgw00s 4800/tcp # SAP Secure Gateway 4800 + Instance-Number
```

10.7.7.5 必要的本地化

SAP至少要求两个本地化设置，它不是RedHat的默认安装。**SAP**提供从他们的FTP服务器下载必需的RPMs（只有您是OSS的客户才能访问）。看注解0171356查找您需要的RPMs列表。

也可以只创建适当的链接（例如从**de_DE**到**en_US**），但是我们不推荐在生产系统上这样做（尽管它让**IDES system**工作的没有一点问题）。下面的本地化设置是必需的：

```
de_DE.ISO-8859-1
en_US.ISO-8859-1
```

像这样创建链接

```
# cd /compat/linux/usr/share/locale
# ln -s de_DE de_DE.ISO-8859-1
# ln -s en_US en_US.ISO-8859-1
```

如果他们不出现，在安装时可能会有问题。如果忽略这些问题（通过设置**CENTRDB.R3S**文件里面的**STATUS**为**OK**），不费一番周折，您就别想登陆进**SAP**系统。

10.7.7.6 内核调整

SAP R/3需要许多资源。我因此添加了下面的参数在我的内核配置文件中：

```
# Set these for memory pigs (SAP and Oracle):
options MAXDSIZ="(1024*1024*1024)"
options DFLDSIZ="(1024*1024*1024)"
# System V options needed.
options SYSVSHM #SYSV-style shared memory
options SHMMAXPGS=262144 #max amount of shared mem. pages
#options SHMMAXPGS=393216 #use this for the 46C inst.parameters
options SHMMNI=256 #max number of shared memory ident if.
options SHMSEG=100 #max shared mem.segs per process
options SYSVMSG #SYSV-style message queues
options MSGSEG=32767 #max num. of mes.segments in system
options MSGSSZ=32 #size of msg-seg. MUST be power of 2
options MSGMNB=65535 #max char. per message queue
options MSGTQL=2046 #max amountof msgs in system
options SYSVSEM #SYSV-style semaphores
options SEMMNU=256 #number of semaphore UNDO structures
options SEMMNS=1024 #number of semaphores in system
options SEMMNI=520 #number of semaphore identifiers
options SEMUME=100 #number of UNDO keys
```

这篇文档中指定的最小值是来自**SAP**。没有针对Linux的描述，看看**HP-UX**的相关介绍了解更多信息。安装**4.6C SR2**需要更多的内存，共享内存比**SAP**和**Oracle**需要的还多，所以尽量为共享内存选一个大值。

注意: FreeBSD 4.5在i386上缺省应该设置MAXDSIZ和DFLDSIZ到1 GB。否则，奇怪的错误像ORA-27102: out of memory和Linux Error: 12: Cannot allocate memory会出现。

10.7.8 安装SAP R/3

10.7.8.1 准备SAP CDROMs

在安装过程中，有许多CDROM要被挂上和卸下。建议您有多个CDROM驱动器，您可以把它们都挂上。我决定拷贝CDROM的内容到相应的目录：

```
/oracle/SID/sapreorg/cd-name
```

对于4.6B/IDES的安装，*cd-name*是KERNEL，RDBMS，EXPORT1，EXPORT2，EXPORT3，EXPORT4，EXPORT5 和EXPORT6中的一个，对于4.6C SR2的安装，是KERNEL，RDBMS，DISK1，DISK2，DISK3，DISK4和LANG中的一个。所有挂载上的CDs里面的文件名都应该是大写，否则要用-g选项来挂载。所以使用下面的命令：

```
# mount_cd9660 -g /dev/cd0a /mnt
# cp -R /mnt/* /oracle/SID/sapreorg/cd-name
# umount /mnt
```

10.7.8.2 运行安装脚本

首先您需要准备一个install目录：

```
# cd /oracle/SID/sapreorg
# mkdir install
# cd install
```

然后运行安装脚本，他会拷贝所有相关的文件到install目录：

```
# /oracle/SID/sapreorg/KERNEL/UNIX/INSTT00L.SH
```

由于这是一个完全定制化的SAP R/3演示系统的IDES安装（4.6B），我们有6个而不仅仅是3个EXPORT CDs。基于这点，安装模板CENTRDB.R3S是用来安装一个标准的中央环境（R/3和数据库），而不是IDES中央环境，所以从EXPORT1目录拷贝相应的CENTRDB.R3S，否则R3SETUP只要求3个EXPORT CDs。

新的SAP 4.6C SR2发行版带有4张EXPORT CDs。控制安装步骤的参数文件是CENTRAL.R3S。和早期发行版不同，它没有分开的中央环境的安装模板。

安装完后，使用hostname命令得到SAP需要的主机名，不需要完整的域名。所以为orasisd和sidadm 直接设置主机名，或设置别名alias hostname='hostname -s'。可以在.profile和.login里面为这两个用户设置。

10.7.8.3 启动R3SETUP 4.6B

确定LD_LIBRARY_PATH设置正确：


```
# export LD_LIBRARY_PATH=/oracle/IDS/lib:/sapmnt/IDS/exe:/oracle/805_32/lib
```

从安装目录以root身份启动R3SETUP:

```
# cd /oracle/IDS/sapreorg/install
# ./R3SETUP -f CENTRDB.R3S
```

这个脚本会问一些问题（括号里面是缺省值，后面是实际输入）：

问题	缺省值	输入
Enter SAP System ID	[C11]	IDS Enter
Enter SAP Instance Number	[00]	Enter
Enter SAPMOUNT Directory	[/sapmnt]	Enter
Enter name of SAP central host	[troubadix.domain.de]	Enter
Enter name of SAP db host	[troubadix]	Enter
Select character set	[1] (WE8DEC)	Enter
Enter Oracle server version (1) Oracle 8.0.5, (2) Oracle 8.0.6, (3) Oracle 8.1.5, (4) Oracle 8.1.6		1 Enter
Extract Oracle Client archive	[1] (Yes, extract)	Enter
Enter path to KERNEL CD	[/sapcd]	/oracle/IDS/sapreorg/KERNEL
Enter path to RDBMS CD	[/sapcd]	/oracle/IDS/sapreorg/RDBMS
Enter path to EXPORT1 CD	[/sapcd]	/oracle/IDS/sapreorg/EXPORT1
Directory to copy EXPORT1 CD	[/oracle/IDS/sapreorg/CD4_DIR]	Enter
Enter path to EXPORT2 CD	[/sapcd]	/oracle/IDS/sapreorg/EXPORT2
Directory to copy EXPORT2 CD	[/oracle/IDS/sapreorg/CD5_DIR]	Enter
Enter path to EXPORT3 CD	[/sapcd]	/oracle/IDS/sapreorg/EXPORT3
Directory to copy EXPORT3 CD	[/oracle/IDS/sapreorg/CD6_DIR]	Enter
Enter path to EXPORT4 CD	[/sapcd]	/oracle/IDS/sapreorg/EXPORT4
Directory to copy EXPORT4 CD	[/oracle/IDS/sapreorg/CD7_DIR]	Enter
Enter path to EXPORT5 CD	[/sapcd]	/oracle/IDS/sapreorg/EXPORT5
Directory to copy EXPORT5 CD	[/oracle/IDS/sapreorg/CD8_DIR]	Enter
Enter path to EXPORT6 CD	[/sapcd]	/oracle/IDS/sapreorg/EXPORT6
Directory to copy EXPORT6 CD	[/oracle/IDS/sapreorg/CD9_DIR]	Enter
Enter amount of RAM for SAP + DB		850 Enter (in Megabytes)
Service Entry Message Server	[3600]	Enter
Enter Group-ID of sapsys	[101]	Enter
Enter Group-ID of oper	[102]	Enter
Enter Group-ID of dba	[100]	Enter
Enter User-ID of <i>sidadm</i>	[1000]	Enter
Enter User-ID of <i>orasid</i>	[1002]	Enter
Number of parallel procs	[2]	Enter

如果没有把CD拷贝到不同的位置，那么SAP安装程序就不能找到需要的CD（通过CD上

的LABEL.ASC来辨别），它会要求您挂上CD，或键入加载路径。

CENTRDB.R3S不可能是自由出错的，它再次请求EXPORT4 CD，但是正确的值是6_LOCATION，然后7_LOCATION 等，所以您可以键入正确的值。

处理下面提到的问题，一样东西都要直接通过Oracle数据库软件安装的地方。

10.7.8.4 Start R3SETUP 4.6C SR2

确定LD_LIBRARY_PATH设置正确。这和带Oracle 8.0.5的4.6B的安装是不同的:

```
# export LD_LIBRARY_PATH=/sapmnt/PRD/exe:/oracle/PRD/817_32/lib
```

以root身份从安装目录启动R3SETUP：

```
# cd /oracle/PRD/sapreorg/install
# ./R3SETUP -f CENTRAL.R3S
```

这个脚本会问一些问题（括号里面是缺省值，后面是实际输入）：

问题	缺省值	输入
Enter SAP System ID	[C11]	PRDEnter
Enter SAP Instance Number	[00]	Enter
Enter SAPMOUNT Directory	[/sapmnt]	Enter
Enter name of SAP central host	[majestix]	Enter
Enter Database System ID	[PRD]	PRDEnter
Enter name of SAP db host	[majestix]	Enter
Select character set	[1] (WE8DEC)	Enter
Enter Oracle server version (2) Oracle 8.1.7		2Enter
Extract Oracle Client archive	[1] (Yes, extract)	Enter
Enter path to KERNEL CD	[/sapcd]	/oracle/PRD/sapreorg/KERNEL
Enter amount of RAM for SAP + DB	2044	1800Enter (in Megabytes)
Service Entry Message Server	[3600]	Enter
Enter Group-ID of sapsys	[100]	Enter
Enter Group-ID of oper	[101]	Enter
Enter Group-ID of dba	[102]	Enter
Enter User-ID of oraprd	[1002]	Enter
Enter User-ID of prdadm	[1000]	Enter
LDAP support		3Enter (no support)
Installation step completed	[1] (continue)	Enter
Choose installation service	[1] (DB inst,file)	Enter

到目前为止，安装阶段只在创建用户时给出了一个错误OSUSERDBSID_IND_ORA（创建用户orasid）和OSUSERSIDADM_IND_ORA（创建用户sidadm）。

处理下面提到的问题，一样东西都要直接通过Oracle数据库软件安装的地方。

10.7.9 安装Oracle 8.0.5

请看相应的SAP注释和Oracle的关于Linux的Readme 以及**Oracle DB**可能出现的问题。不是所有的问题都和不兼容库有关。

关于**Oracle**更多的安装信息，请参考安装Oracle。

10.7.9.1 用orainst安装Oracle 8.0.5

如果**Oracle 8.0.5**要被使用，一些其他的库需要被成功地重新链接，因为**Oracle 8.0.5**是与一个老的glibc连接的（Redhat 6.0），但RedHat 6.1已经使用了一个新的glibc。所以您必须安装下面额外的软件包来保证链接正常：

```
compat-libs-5.2-2.i386.rpm
compat-glibc-5.2-2.0.7.2.i386.rpm
compat-egcs-5.2-1.0.3a.1.i386.rpm
compat-egcs-c++-5.2-1.0.3a.1.i386.rpm
compat-binutils-5.2-2.9.1.0.23.1.i386.rpm
```

更多的信息，看相应的SAP注释和Oracle的Readme。如果这不是选项，您可以使用最初的程序，或使用与最初的Redhat系统重链接的程序。

要编译智能代理，必须安装RedHat Tcl包。如果您不能得到tcl-8.0.3-20.i386.rpm，一个更新的tcl-8.0.5-30.i386.rpm也可以用。

除了重新链接，安装是直截了当的：

```
# su - oraids
# export TERM=xterm
# export ORACLE_TERM=xterm
# export ORACLE_HOME=/oracle/IDS
# cd $ORACLE_HOME/orainst_sap
# ./orainst
```

用Enter来确认所有的屏幕直到安装完成，除了您必须取消**Oracle On-Line Text Viewer**选项，因为当前Linux下不可用。**Oracle**会要求用i386-glibc20-linux-gcc重新链接来代替gcc，egcs或者i386-redhat-linux-gcc。

由于时间紧迫，我决定使用**Oracle 8.0.5 PreProduction**版本。

10.7.9.2 安装Oracle 8.0.5 Pre-production Release for Linux (Kernel 2.0.33)

个安装很容易。挂上CD，启动安装程序。它就会要求Oraclehome目录的定位，然后拷贝那儿所有的程序。我不删除先前安装的RDBMS。

然后，**Oracle**数据库就可以毫无问题地运行了。

10.7.10 安装Oracle 8.1.7 Linux压缩包

拷贝oracle81732.tgz到您要安装的目录，然后解压到/oracle/SID/817_32/。

10.7.11 继续SAP R/3安装

首先检查用户idsamd (sidadm)和oraids(orasid)的环境变量。他们现在都有使用主机名的.profile, .login 和.cshrc文件。在这个例子中，系统的主机名是没有限制的名称，您必须在所有三个文件中改变hostname为hostname -s。

10.7.11.1 加载数据库

然后，可以重新启动或继续R3SETUP。R3SETUP就使用R3load 创建表空间加载数据（对46B IDES，从EXPORT1到EXPORT6，对46C从DISK1到DISK4）。

数据加载完后（可能需要一些时间），需要创建一些口令。对于测试安装，可以使用缺省口令：

问题	输入
Enter Password for sapr3	sapEnter
Confirm Password for sapr3	sapEnter
Enter Password for sys	change_on_installEnter
Confirm Password for sys	change_on_installEnter
Enter Password for system	managerEnter
Confirm Password for system	managerEnter

到目前为止，我们只在安装4.6B的过程中dipgntab出现了几个问题。

10.7.11.2 监听

像下面这样用orasid用户启动Oracle:

```
% umask 0; lsnrctl start
```

另外您可能得到ORA-12546错误，因为sockets没有正确的权限。看SAP注释072984。

10.7.11.3 更新MNLS表

如果您打算倒入non-Latin-1 languages到SAP系统，您必须更新表的多语言支持。这在SAP OSS注释15023和45619有描述。否则，您可以在安装SAP的时候忽略这个问题。

注意: 如果您不需要MNLS，还是需要检查表TCPDB和初始化工作是否做了。更多信息参考SAP注释0015023和0045619。

10.7.12 快速安装步骤

10.7.12.1 需要SAP R/3许可密钥

您不得不要SAP R/3许可密钥。这是必需的，因为临时许可只能用4个星期。首先得到硬件的密匙。以用idsadm登入，然后调用saplicense:

```
# /sapmnt/IDS/exe/saplicense -get
```

不带参数调用saplicense会给出一系列选项。要安装上面的许可密钥，可以这样：

```
# /sapmnt/IDS/exe/saplicense -install
```

您要输入下面的值：

```
SAP SYSTEM ID    = SID, 3 chars
CUSTOMER KEY     = hardware key, 11 chars
INSTALLATION NO = installation, 10 digits
EXPIRATION DATE  = yyyymmdd, usually "99991231"
LICENSE KEY      = license key, 24 chars
```

10.7.12.2 创建用户

在客户机000中创建一个用户（有些工作需用客户机000来完成，但与用户sap*和ddic有些不同）。作为一个用户名，我通常选择wartung（或英语中的service）。配置文件需要sap_new和sap_all。对于额外的安全的默认用户口令应当被改变（这包括用户sap*和ddic）。

10.7.12.3 配置传送系统，配置，操作模式等

在客户端000，用户不同于ddic和sap*，做下面的工作：

任务	处理
Configure Transport System, e.g. as Stand-Alone Transport Domain Entity	STMS
Create / Edit Profile for System	RZ10
Maintain Operation Modes and Instances	RZ04

些和所有其他的快速安装步骤在SAP安装指南里面有描述。

10.7.12.4 编辑initsid.sap (initIDS.sap)

文件/oracle/IDS/dbs/initIDS.sap 包含了SAP备份配置。这儿是使用的磁带机的大小，压缩的类型。要使用sapdba / brbackup来得到这些。我们可以改变下面的值：

```
compress = hardware
archive_function = copy_delete_save
cpio_flags = "-ov --format=newc --block-size=128 --quiet"
cpio_in_flags = "-iuv --block-size=128 --quiet"
tape_size = 38000M
tape_address = /dev/nsa0
tape_address_rew = /dev/sa0
```

解释

compress: 我使用的磁带机是HP DLT1，它支持硬件压缩。

archive_function: 这个定义了保存Oracle文件日志的默认行为：新的日志文件被保存到磁带上，保存的日志文件会被再次保存然后再删除。如果您需要恢复数据库，而其中一个磁带机已经损坏了，这可以防止出现麻烦。

cpio_flags: 缺省使用-B来设置块大小为5120 Bytes。对于DLT-Tapes，HP建议至少32 K，所以我们使用--block-size=128 设置64 K。--format=newc是必需的，因为我的inode数目超过了65535。最后一个选项--quiet是必需的，否则brbackup会在用cpio来输出的时候报错。

cpio_in_flags: 这个标志从磁带机加载回数据。格式是自动验证的。

tape_size: 通常给出了磁带机的存储容量。出于安全原因，这个值要比实际的值要小一些。

tape_address: 被cpio使用的非rewindable的设备。

tape_address_rew: 被cpio使用的非rewindable的设备。

10.7.12.5 安装后的配置

下面的SAP参数应该在安装以后调整（例子是IDES 46B, 1 GB内存）：

名称	值
ztta/roll_extension	250000000
abap/heap_area_dia	300000000
abap/heap_area_nondia	400000000
em/initial_size_MB	256
em/blocksize_kB	1024
ipc/shm_psize_40	70000000

SAP注释0013026:

名称	值
ztta/dynpro_area	2500000

SAP注释0157246:

Name	Value
rdisp/ROLL_MAXFS	16000
rdisp/PG_MAXFS	30000

注意: 根据上面的参数，在使用1 GB内存的系统上，可以像下面这样找到内存消耗:

Mem: 547M Active, 305M Inact, 109M Wired, 40M Cache, 112M Buf, 3492K Free

10.7.13 安装过程出现的问题

10.7.13.1 修复一个问题后重起R3SETUP

如果出现问题R3SETUP会停止。如果您找到相关的日志文件并修复了问题。您需要再次重起R3SETUP，对于R3SETUP报的最后一个错误可以使用REPEAT选项。

要重起R3SETUP，只要使用相应的R3S文件重起：

```
# ./R3SETUP -f CENTRDB.R3S
```

for 4.6B, or with

```
# ./R3SETUP -f CENTRAL.R3S
```

对4.6C，不管有没有错误都使用CENTRAL.R3S或DATABASE.R3S。

注意：在某些阶段，R3SETUP假设database和SAP进程都启动了。但是如果发生错误使得database没有启动，您就必须手动启动database和SAP。修复错误后，还需要再次重起R3SETUP。

也不要忘记再次重起Oracle监听。

10.7.13.2 OSUSERSIDADM_IND_ORA during R3SETUP

如果在这阶段R3SETUP报错,编辑R3SETUP使用的模板文件（CENTRDB.R3S (4.6B)或者CENTRAL.R3S或者DATABASER3S (4.6C)）。定位到[OSUSERSIDADM_IND_ORA]或者搜索STATUS=ERROR条目然后像下面这样编辑它：

```
HOME=/home/sidadm (was empty)
STATUS=OK (had status ERROR)
```

然后重起R3SETUP。

10.7.13.3 OSUSERDBSID_IND_ORA during R3SETUP

R3SETUP也可能在这个阶段报错。修正方法和上面的OSUSERSIDADM_IND_ORA一样。编辑下面的值：

```
STATUS=OK
```

重起R3SETUP。

10.7.13.4 Oracle安装找不到oraview.vrf文件

开始安装之前没有取消**Oracle On-Line Text Viewer** 既然这个选项当前没有用于Linux，这在安装时是需要标记的，在**Oracle**安装中取消它，然后重新安装。

10.7.13.5 TEXTENV_INVALID during R3SETUP, RFC or SAPgui Start

如果这个错误还出现，正确的本地化可能已经丢了。SAP注释0171356列出了必须的RPMs（比如saplocales-1.0-3, saposcheck-1.0-1 for RedHat 6.1）。在这个例子中，您忽略了所有相关的错误，STATUS从ERROR到OK然后重起R3SETUP。SAP系统不会被正确地配置，您就不能用一个SAPgui连接到系统。设法使用一个旧的Linux sapgui连接会得到下面的信息：

```
Sat May 5 14:23:14 2001
*** ERROR => no valid userarea given [trmsgso. 0401]
Sat May 5 14:23:22 2001
*** ERROR => ERROR NR 24 occurred [trmsgsi. 0410]
*** ERROR => Error when generating text environment. [trmsgsi. 0435]
*** ERROR => function failed [trmsgsi. 0447]
*** ERROR => no socket operation allowed [trxio.c 3363]
Speicherzugriffsfehler
```

这个问题归咎于SAP R/3不能正确地本地化，也不能自己正确地配置。要能够连接到SAP，需要在DEFAULT.PFL（看注释0043288）文件中添加下面的记录：

```
abap/set_etct_env_at_new_mode = 0
install/collate/active = 0
rscp/TCP0B = TCP0B
```

重起SAP系统。现在，您可以连接到系统，即使您指定的国家语言不能正常工作。设置完国家后，这些记录会从DEFAULT.PFL文件删除。然后重新启动SAP系统。

10.7.13.6 ORA-00001

这个错误只会在FreeBSD 4.5上安装Oracle 8.1.7的时候出现。因为Oracledatabase不能自己正确初始化。在系统上保留semaphores和shared memory。然后再次启动数据库会出现ORA-00001错误。

用ipcs -a找到再用ipcrm去掉。

10.7.13.7 ORA-00445（后台进程PMON没有启动）

这个错误发生在Oracle 8.1.7上。如果没有用prdadm用户启动startsap脚本（例如startsap_majestix_00）会报这个错误。

一种可能的解决方法是用oraprd用户使用svrmgrl：

```
% svrmgrl
SVRMGR> connect internal;
SVRMGR> startup;
SVRMGR> exit
```

10.7.13.8 ORA-12546（用正确的权限启动监听）

以oraids用户启动Oracle监听：

```
# umask 0; lsnrctl start
```


如果您得到ORA-12546错误，没有权限连接到sockets。请看SAP注释0072984。

10.7.13.9 ORA-27102 (Out of Memory)

这个错误发生在使用MAXDSIZ和DFLDSIZ大于1 GB（1024x1024x1024）。我们一般得到错误Linux Error 12: Cannot allocate memory。

10.7.13.10 [DIPGNTAB_IND_IND] during R3SETUP

基本上，参见SAP注释0130581 (R3SETUP 步骤中的DIPGNTAB 终止)。在IDES-专用安装的时候，因为某些原因安装过程没有使用正确的SAP 系统名“IDS”，而是用空串""代替。这会导致一些访问目录的小问题，因为路径是动态使用SID来创建的(这里是IDS)。所以用下面的方法代替：

```
/usr/sap/IDS/SYS/...
/usr/sap/IDS/DVMGS00
```

下面的路径被使用

```
/usr/sap//SYS/...
/usr/sap/D00
```

为了继续安装，我们创建了一个附加的目录：

```
# pwd
/compat/linux/usr/sap
# ls -l
total 4
drwxr-xr-x 3 idsadm sapsys 512 May 5 11:20 D00
drwxr-x--x 5 idsadm sapsys 512 May 5 11:35 IDS
lrwxr-xr-x 1 root sapsys 7 May 5 11:35 SYS -> IDS/SYS
drwxrwxr-x 2 idsadm sapsys 512 May 5 13:00 tmp
drwxrwxr-x 11 idsadm sapsys 512 May 4 14:20 trans
```

我们也发现在SAP注释（0029227和0008401）里面描述了这个行为。我们没有在SAP 4.6C安装里面遭遇这些问题。

10.7.13.11 [RFCRSWBOINI_IND_IND] during R3SETUP

安装SAP 4.6C时，这个错误是前面发生过的一个错误的结果。所以，您不得不查看相应的日志文件并修复错误。

如果查看完日志文件后这个错误确实存在（看SAP注释），您可以设置STATUS从ERROR到OK（CENTRDB.R3S文件里面）然后重起R3SETUP。安装完后，您必须从事务SE38执行RSWBOINS。关于RFCRSWBOINI和RFCRADDBDIF的更多信息查看SAP注释0162266。

10.7.13.12 [RFCRADDBDIF_IND_IND] during R3SETUP

通过查看日志文件确定这个错误，它不是由于前面的问题导致的。

如果您确定已经应用了SAP注释0162266，就只要设置STATUS从ERROR到OK（CENTRDB.R3S文件里面）。然后重起R3SETUP。安装完后，您必须从事务SE38执行RADDDBIF。

10.7.13.13 sigaction sig31: File size limit exceeded

这个错误在启动SAP进程disp+work时出现。如果用startsap脚本启动SAP，就会启动子进程，并由它启动后面所有的其他SAP进程。所以脚本本身不会注意到有错误发生。

为了检查SAP进程是否正确启动，可以用`ps ax | grep SID`查看进程的状态。您会得到所有Oracle和SAP进程列表。如果看起来有些进程没有启动，或者您不能正确连接到SAP系统。查看相应的日志文件，可以在`/usr/sap/SID/DVEBMGSnr/work/`下找到，一般查看`dev_ms`和`dev_disp`文件。

如果Oracle和SAP的共享内存总量超过了内核配置文件定义的大小就会出现signal 31错误，并且不能解析大的内存地址：

```
# larger value for 46C production systems:
options SHMMAXPGS=393216
# smaller value sufficient for 46B:
#options SHMMAXPGS=262144
```

10.7.13.14 启动saposcol失败

使用saposcol (version 4.6D)会出现一些问题。SAP系统使用saposcol收集系统性能数据。这个程序不是必需的。所以这些问题可以看作是小问题。老版本（4.6B）可以工作，但是不能收集所有的性能数据（很多调用只返回0，像CPU使用率）。

10.8 高级主题

如果您对Linux兼容模式是如何工作的感到好奇，这节正是您所需要的。下面的绝大部分内容是由Terry Lambert<tlambert@primenet.com>（Message ID: <199906020108.SAA07001@usr09.primenet.com>）发表在邮件列表FreeBSD 闲聊邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-chat>)上的内容组成的。

10.8.1 它是如何工作的？

FreeBSD有一个“可执行类加载器”。它主要是嵌入了execve(2)系统调用。

碰巧的是FreeBSD有一个引导器（loader）的列表，而不是一个简单的返回一个符号#1的引导器！

从历史上讲，只有UNIX平台的引导器会检查魔术（magic）数（通常是文件的前4个或8个字节）是否是二进制的，如果是，就调用二进制引导程序。

如果它不是二进制类型的execve(2)调用就会返回一个错误，shell就试图用shell命令执行它。

缺省是使用“当前设定的shell”。

随后，进行了一些hack，sh(1)开始检查前两个字符，如果它们是:\n，那它就调用csh(1)（我们相信是SCO最先做这个hack的）。

FreeBSD现在所做的是用一个普通的#!引导器仔细检查引导器的列表，然后由解释程序一个接一个地解释，返回给/bin/sh。

为了支持Linux ABI，FreeBSD就把魔术数看作为一个二进制ELF程序。（这样一来，它就使得在FreeBSD，Solaris，Linux和其他任何操作系统之间只要使用ELF格式就都可以顺利运行）。

ELF引导器会寻找一个专门的标记，它是在ELF映像中的一个注释部分，但在SVR4/Solaris的ELF中没有。

为了执行Linux程序，它们必须被打上Linux类型的标记；使用brandelf(1)：

```
# brandelf -t Linux file
```

做完之后，ELF引导器就会看到文件上的Linux的标记。

当ELF引导器看到Linux的标记，引导器就会在proc结构中替换一个指示器。所有的系统调用就会通过这个指示器来索引（在一个传统的UNIX系统中，这就是sysent[]结构队列，包含系统调用）。此外，为了解决由于信号杂乱所造成的陷阱向量的问题，会造成线程的剧增，需要切断其他（或较小的）由Linux内核模块产生的修正。

Linux系统调用向量包含一个sysent[]记录的列表，它的地址位于内核模块之中。

当一个系统调用被Linux程序调用时，有缺陷的代码会把系统调用功能的指示器从proc结构中解除，然后获得Linux，而不是FreeBSD，系统调用入口点。

另外，Linux模式动态地reroots查找；这和启动文件系统的union选项是等效的（即时不是unionfs文件系统）。首先会试图在/compat/linux/original-path目录查找文件，如果失败了，就会在/original-path目录下查找。这使得需要其它程序的程序可以运行（例如，Linux工具链都可以在Linux ABI的支持下工作）。也就是说Linux程序可以加载和执行FreeBSD程序，如果当前没有相应的Linux程序，那您可以在/compat/linux目录树中放置一个uname(1)，来确保Linux程序不提示它们不能运行在Linux上。

在FreeBSD内核中有一个Linux内核；由内核提供的能够提供所有服务的各种潜在功能在FreeBSD系统调用表记录和Linux系统调用表记录之间是一样的：文件系统操作，虚拟内存操作，信号发送，System V IPC，...等等。唯一的不同是FreeBSD会得到FreeBSD的胶合功能，而Linux程序会得到Linux的胶合功能（大部分老的操作系统只有它们自己的胶合函数，函数地址在静态全局变量sysent[]结构数据里面，而不是动态的初始化到进程的proc结构）。

哪一个是FreeBSD自己的ABI呢？这无关紧要。基本上，唯一的不同是FreeBSD的胶合功能是被静态连接到内核，而Linux的胶合功能可能是被静态连接到内核，也可能它们通过一个内核模块来访问。

有一个真正的模拟器吗？没有，它只不过是一个ABI执行机制，不是一个模拟器。

为什么有时它被叫做“Linux模拟器”？只是为了更容易地卖出FreeBSD罢了！实际上，历史上从来没有描述这样一种执行机制的名字，FreeBSD并不是真正地运行Linux程序，如果您不编译进代码，或加载一个模块。就需要有一个名字来描述这样一种加载功能--因此就想出了“Linux模拟器”这样一个名字。

III. 系统管理

FreeBSD 手册中其余章节的内容都是关于系统管理。每一章节都从描述开始，由浅入深。

这些章节被设计成很多相对完整的部分，如果您需要了解某部分内容，直接阅读这部分内容即可，无需按照顺序，也不用在您使用FreeBSD 的时候需要先读一遍。

第11章

设置和调整

原作: Chern Lee. 这份文档基于一份教程, 其作者是Mike Smith. 此外, 也参考了tuning(7), 其作者是Matt Dillon.

11.1 概述

使用FreeBSD的一个重要问题是系统配置。正确地配置系统能充分地减少以后维护和升级系统所需的工作量。本章将解释一些FreeBSD的配置过程, 包括一些可以调整的FreeBSD系统的一些参数。

读完本章, 您将了解:

- 如何有效地利用文件系统和交换分区。
- rc.conf的基本设置以及/usr/local/etc/rc.d启动体系。
- 如何设置和测试网卡。
- 如何在您的网络设备上配置虚拟主机。
- 如何使用/etc下的各配置文件。
- 如何通过sysctl变量来对FreeBSD系统进行调优。
- 怎样调整磁盘性能和修改内核限制。

在阅读本章之前, 您应该了解:

- 了解UNIX和FreeBSD的基础知识(第3章)。
- 熟悉内核配置编译的基础知识(第8章)。

11.2 初步配置

11.2.1 分区规划

11.2.1.1 基本分区

当使用disklabel(8)或者sysinstall(8)来分割您的文件系统的时候, 要记住硬盘驱动器外磁道传输数据要比从内磁道传输数据快。因此应该将小的和经常访问的文件系统放在驱动器靠外的位置, 一些大的分区比如/usr应该放在比较靠里的位置。以类似这样的顺序建立分区是一个不错的主意: root, swap, /var, /usr。

/var的大小能反映您的机器使用情况。它用来存储邮件, 日志文件和打印队列缓存, 特别是邮箱和日志文件可能会达到无法预料的大小, 这主要取决于在您的系统上有多少用户和您的日志文件可以保存多长时间。一般大多数用户不需要一个G以上的空间, 但要记住/var/tmp应该足够大来以便存储一些packages。

`/usr` 分区存储很多用来系统运行所需要的文件例如ports(7) (建议这样做) 和源代码(可选的)。安装的时候这两项都是可选的。这个分区至少要保留两个G 的可用空间。

当选择分区大小的时候，记住保留一些空间。用完了一个分区的空间而在另一个分区上还有很多，可能会导致出现一些错误。

注意：一些用户会发现sysinstall(8) 的Auto-defaults 自动分区有时会分配给/var 和/ 较小的分区空间。分区应该精确一些并且大一些。

11.2.1.2 交换分区

一般来讲，交换分区应该大约是系统内存(RAM) 的两倍。例如，如果机器有128M 内存，交换文件应该是256M。较小内存的系统可以通过多一点地交换分区来提升性能。不建议小于256 兆的交换分区，并且扩充您的内存应该被考虑一下。当交换分区最少是主内存的两倍的时候，内核的VM (虚拟内存) 页面调度算法可以将性能调整到最好。如果您给机器添加更多内存，配置太小的交换分区会导致VM 页面扫描的代码效率低下。

在使用多块SCSI磁盘(或者不同控制器上的IDE磁盘)的大系统上，建议在每个驱动器上建立交换分区(直到四个驱动器)。交换分区应该大约一样大小。内核可以使用任意大小，但内部数据结构则是最大交换分区的4 倍。保持交换分区同样的大小，可以允许内核最佳地调度交换空间来访问磁盘。即使不太使用，分配大的交换分区也是好的，在被迫重启之前它可以让您更容易的从一个失败的程序中恢复过来。

11.2.1.3 为什么要分区？

一些用户认为一个单独的大分区将会很好，但是有很多原因会证明为什么这是个坏主意。首先，每个分区有不同的分区特性，因此分开可以让文件系统调整它们。例如，根系统和/usr 一般只是读取，写入很少。很多读写频繁的被放在/var 和/var/tmp中。

适当的划分一个系统，用比较小的分区方法，那些以写为主的分区将不会比以读为主的分区付出更高的代价。将以写为主的分区放在靠近磁盘的边缘，例如放在实际的大硬盘的前面代替放在分区表的后面，将会提高您需要的分区的I/O 性能。现在可能也需要在比较大的分区上有很好的I/O 性能，把他们移动到磁盘外围不会带来多大的性能提升，反而把/var 移到外面会有很好的效果。最后涉及到安全问题。一个主要是只读的小的、整洁的根分区可以提高从一个严重的系统崩溃中恢复过来的机会。

11.3 核心配置

系统的配置信息主要位于/etc/rc.conf。这个文件包含了配置信息很大的一部分，主要在系统启动的时候来配置系统，这个名字直接说明了这点；它也是rc* 文件的配置信息。

系统管理员应该在rc.conf 文件中建立记录来覆盖/etc/defaults/rc.conf 中的默认设置。这个默认文件不应该被逐字的拷贝到/etc 它包含的是默认值而不是一个例子。所有特定的改变应该在rc.conf 中。

为了降低管理成本，有很多策略可以应用在成群的应用程序中来从系统指定的配置中分离site-wide 配置。建议的方法是将site-wide 配置放在另一个文件中，例如/etc/rc.conf.site，并且把它包含进然后把这个文件包括进只包含系统指定信息的/etc/rc.conf。

由于rc.conf 可以被sh(1) 阅读，所以达到这个目的很简单，例如：

- rc.conf:

```
. /etc/rc.conf.site
hostname="node15.example.com"
network_interfaces="fxp0 lo0"
ifconfig_fxp0="inet 10.1.1.1"
```
- rc.conf.site:

```
defaultrouter="10.1.1.254"
saver="daemon"
blanktime="100"
```

rc.conf.site 文件会被分发给每一个使用rsync 或相似程序的系统，同时rc.conf 文件仍然保持独立。

使用sysinstall(8) 或者make world 来升级系统不会覆盖rc.conf 文件，所以系统配置信息不会丢失。

11.4 应用程序配置

典型的，被安装的应用程序有他自己的配置文件、语法等等。从基本系统中分开他们是很重要的以至于他们可以容易的被package 管理工具定位和管理

一般来说，这些文件被安装在/usr/local/etc。这个例子中，一个应用程序有很多配置文件并且创建了一个子目录来存放他们。

通常，当一个port 或者package 被安装的时候，配置文件示例也同样被安装了。它们通常用.default 的后缀来标识。如果不存在这个应用程序的配置文件，它们会通过拷贝.default 文件来创建。

例如，看一下这个目下的内容/usr/local/etc/apache:

```
-rw-r--r--  1 root  wheel   2184 May 20   1998 access.conf
-rw-r--r--  1 root  wheel   2184 May 20   1998 access.conf.default
-rw-r--r--  1 root  wheel   9555 May 20   1998 httpd.conf
-rw-r--r--  1 root  wheel   9555 May 20   1998 httpd.conf.default
-rw-r--r--  1 root  wheel  12205 May 20   1998 magic
-rw-r--r--  1 root  wheel  12205 May 20   1998 magic.default
-rw-r--r--  1 root  wheel   2700 May 20   1998 mime.types
-rw-r--r--  1 root  wheel   2700 May 20   1998 mime.types.default
-rw-r--r--  1 root  wheel   7980 May 20   1998 srm.conf
-rw-r--r--  1 root  wheel   7933 May 20   1998 srm.conf.default
```

文件大小显示了只有srm.conf 改变了。以后Apache 的升级就不会改变这个文件。

11.5 启动服务

Contributed by Tom Rhodes.

许多用户会选择使用Ports Collection 来在FreeBSD 上安装第三方软件。很多情况下这可能需要进行一些配置以便让这些软件能够在系统初始化的过程中启动。服务，例如mail/postfix 或www/apache13 就是这些需要在系统初始化时启动的软件包中的两个典型代表。这一节解释了启动第三方软件所需要的步骤。

FreeBSD 包含的大多数服务，例如cron(8)，就是通过系统启动脚本启动的。这些脚本也许会有些不同，这取决于FreeBSD 版本。但是不管怎样，需要考虑的一个重要方面是他们的启动配置文件要能被基本启动脚本识别捕获。

在rc.d 出现之前，应用程序会把一个简单的启动脚本放到/usr/local/etc/rc.d 目录中，这个目录中的脚本会被系统初始化脚本读取。

尽管很多人已经花费了相当多的时间来把旧的配置方式融入到新系统中，仍然有许多第三方软件需要把脚本放到上面提到的目录中。是否使用rc.d 会对这些脚本的执行带来一些变化。在FreeBSD 5.1 之前采用的是旧式的配置，当然，绝大多数情况下，新式的脚本也会工作的很好。

每个脚本都应该遵守FreeBSD 版本所需求的一些规定：每个脚本必须在文件名最后添加一个.sh 的扩展名，并且这个脚本能被系统执行。后者可以通过chmod 命令把权限设置为755来实现。它还应该能接受start 选项来启动程序并且接受stop 选项来结束程序。

一个简单的脚本看起来可能会像这样：

```
#!/bin/sh
echo -n ' utility'

case "$1" in
start)
    /usr/local/bin/utility
    ;;
stop)
    kill -9 'cat /var/run/utility.pid'
    ;;
*)
    echo "Usage: 'basename $0' {start|stop}" >&2
    exit 64
    ;;
esac

exit 0
```

这个脚本提供了stop 和start 两个选项，用以操作utility。

可以用如下方法来启动：

```
# /usr/local/etc/rc.d/utility.sh start
```

现在不是所有第三方软件都需要在rc.conf 中进行如此的配置，不过几乎每天都有新的port 被修改来采用这种配置方法。您应在安装的最后阶段查看所显示的信息，以了解某个具体的应用是否需要这样的配置。某些第三方软件会提供启动脚本，以便与rc.d 配合使用；这些内容将在下一节介绍。

11.5.1 扩展应用程序配置

现在FreeBSD 提供了rc.d，这使得对应用程序的启动进行配置变得更加方便，并提供了更多的其他功能。例如，使用在rc.d 一节中所介绍的关键字，应用程序就可以设置在某些其他服务，例如DNS 之后启动；除此之外，还可以通过rc.conf 来指定一些额外的启动参数，而不再需要将它们硬编码到启动脚本中。基本的启动脚本如下所示：

```
#!/bin/sh
#
```



```

# PROVIDE: utility
# REQUIRE: DAEMON
# KEYWORD: shutdown

#
# DO NOT CHANGE THESE DEFAULT VALUES HERE
# SET THEM IN THE /etc/rc.conf FILE
#
utility_enable=${utility_enable-"NO"}
utility_flags=${utility_flags-""}
utility_pidfile=${utility_pidfile-"/var/run/utility.pid"}

. /etc/rc.subr

name="utility"
rcvar='set_rcvar'
command="/usr/local/sbin/utility"

load_rc_config $name

pidfile="${utility_pidfile}"

start_cmd="echo \"Starting ${name}.\"; /usr/bin/nice -5 ${command} ${utility_flags} ${command_arg}"

run_rc_command "$1"

```

这个脚本将保证**utility**能够在**daemon**服务之后启动。它同时也提供了设置和跟踪PID，也就是进程ID文件的方法。

可以在**/etc/rc.conf**中加入：

```
utility_enable="YES"
```

这个新方法也使得命令行参数、包含**/etc/rc.subr**中所提供的功能，兼容**rcorder(8)**工具并提供更简单的通过**rc.conf**文件来配置的方法。

11.5.2 用服务来启动服务

其他服务，例如POP3服务器，IMAP，等等，也可以通过**inetd(8)**来启动。这一过程包括从**Ports Collection**安装相应的应用程序，并把配置加入到**/etc/inetd.conf**文件，或去掉当前配置中的某些注释。如何使用和配置**inetd**在**inetd**一节中进行了更为深入的阐述。

一些情况下，通过**cron(8)**来启动系统服务也是一种可行的选择。这种方法有很多好处，因为**cron**会以**crontab**的文件属主身份执行那些进程。这使得普通用户也能够执行他们的应用。

cron工具提供了一个独有的功能，以**@reboot**来指定时间。这样的设置将在**cron(8)**启动时运行，通常这也是系统初始化的时候。

11.6 配置cron

Contributed by Tom Rhodes.

FreeBSD 最有用的软件包(utilities)中的一个cron(8)。cron 软件在后台运行并且经常检查/etc/crontab 文件。cron 软件也检查/var/cron/tabs 目录，搜索新的crontab 文件。这些crontab 文件存储一些cron 在特定时间执行任务的信息。

cron 程序使用两种不同类型的配置文件，即系统crontab 和用户crontabs。两种格式的唯一区别是第六个字段。在系统crontab 中，第六个字段是用于执行命令的用户名。这给予了系统crontab 以任意用户身份执行命令的能力。在用户crontab 中，第六个字段是要执行的命令，所有的命令都会以这个用户自己的身份执行；这是一项重要的安全功能。

注意：同其他用户一样，root 用户也可以有自己的crontab。它不同于/etc/crontab (也就是系统crontab)。由于有系统crontab 的存在，通常并不需要给root 建立单独的用户crontab。

让我们来看一下/etc/crontab 文件：

```
# /etc/crontab - root's crontab for FreeBSD
#
# $FreeBSD: src/etc/crontab,v 1.32 2002/11/22 16:13:39 tom Exp $
# ❶
#
SHELL=/bin/sh
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin ❷
HOME=/var/log
#
#
#minute hour mday month wday who command ❸
#
#
*/5 * * * * root /usr/libexec/atrun ❹
```

- ❶ 像大多数FreeBSD 配置文件一样，# 字符是注释。作为什么和为什么要执行，可以加一个注释来描述以便将来提醒您。注释不能跟命令一样在同一行上否则他们会被看成命令的一部分。注释应该另起一行。空行将会被忽略。
- ❷ 首先应该定义环境变量。等号(=) 字符用来定义任何环境变量，像这个例子用到了SHELL，PATH 和HOME 变量。如果shell 行被忽略掉，cron 将会用默认值sh。如果PATH 变量被忽略，那么就没有默认值并且需要指定文件绝对位置。如果HOME 被忽略，cron 将用执行者的home 目录。
- ❸ 这一行定义了七个字段。它们是minute、hour、mday、month、wday、who 和command。它们差不多已经说明了各自的用处。Minute 是命令要运行时的分钟，Hour 跟minute 差不多，只是用小时来表示。Mday 是每个月的天。Month 跟hour 还有minute 都差不多，用月份来表示。wday 字段表示星期几。所有这些字段的值必须是数字并且用24小时制来表示。“who” 字段是特别的，并且只在/etc/crontab 文件中存在。这个字段指定了命令应该以哪个用户的身份来运行。当一个用户添加了他(她)的crontab 文件的时候，他们就会没有这个字段选项。最后，是command 字段。这是最后的一个字段，所以自然就是它指定要运行的程序。

- ④ 最后一行定义了上面所说的值。注意这里我们有一个*/5列表，紧跟着是一些*字符。*字符代表“开始到最后”，也可以被解释成**每次**。所以，根据这行，显然表明了无论在何时每隔5分钟以root身份来运行atrun命令。查看atrun(8)手册页以获得atrun的更多信息。

命令可以有任意多个传递给它们的标志。无论怎样，扩展到多行的命令应该用反斜线(“\”)来续行。

这是每个crontab文件的基本设置，虽然它们有一个不同。第六行我们指定的用户名只存在于系统/etc/crontab文件。这个字段在普通用户的crontab文件中应该被忽略。

11.6.1 安装Crontab

重要: 绝对不要用这种方法来编辑/安装系统crontab。您需要做的只是使用自己喜欢的编辑器：cron程序会注意到文件发生了变化，并立即开始使用新的版本。参见这个FAQ项目

(http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/faq/admin.html#ROOT-NOT-FOUND-CRON-ERRORS)以了解进一步的情况。

要安装刚写好的用户crontab，首先使用最习惯的编辑器来创建一个符合要求格式的文件，然后用crontab程序来完成。最常见的用法是：

```
% crontab crontab-file
```

In this example, crontab-file is the filename of a crontab that was previously created.

还有一个选项用来列出安装的crontab文件：只要传递-l选项给crontab然后看一下输出。

用户想不用模板(已经存在的文件)而直接安装他的crontab文件，用crontab -e选项也是可以的。它将会启动一个编辑器并且创建一个新文件，当这个文件被保存的时候，它会自动的用crontab来安装这个文件。

如果您稍后想要彻底删除自己的用户crontab可以使用crontab的-r选项。

11.7 在FreeBSD 5.X 和更新版本中使用rc

Contributed by Tom Rhodes.

在2002年，FreeBSD整合了来自NetBSD的rc.d系统，并通过它来完成系统的初始化工作。用户要注意在/etc/rc.d目录下的文件。这里面的许多文件是用来管理基础服务的，它们可以通过start、stop，以及restart选项来控制。举例来说，sshd(8)可以通过下面的命令来重启：

```
# /etc/rc.d/sshd restart
```

对其它服务的操作与此类似。当然，这些服务通常是在启动时根据rc.conf(5)自动启动的。例如，要配置使系统启动时启动网络地址转换服务，可以简单地通过在/etc/rc.conf中加入如下设置来完成：

```
natd_enable="YES"
```

如果natd_enable="NO"行已经存在，只要简单的把NO改成YES即可。rc脚本在下次重新启动的时候会启动所需要的服务，像下面所描述的那样。

由于rc.d 系统在系统启动/关闭时首先启动/停止服务，如果设置了适当的/etc/rc.conf 变量，标准的start、stop 和restart 选项将会执行他们的动作。例如sshd restart 命令只在/etc/rc.conf 中的sshd_enable 设置成YES 的时候工作。不管是否在/etc/rc.conf 中设置了，要start、stop 或者restart 一个服务，命令前可以加上一个“force”前缀。例如要不顾当前/etc/rc.conf 的设置重新启动sshd，执行下面的命令：

```
# /etc/rc.d/sshd forcerestart
```

用选项rcvar 可以简单来的检查/etc/rc.conf 中用适当的rc.d 脚本启动的服务是否被启用。从而管理员可以运行这样的程序来检查sshd 是否真的在/etc/rc.conf 中被启动了：

```
# /etc/rc.d/sshd rcvar
# sshd
$sshd_enable=YES
```

注意：第二行(# sshd) 是从sshd 命令中输出的，而不是root 控制台。

为了确定一个服务是否真的在运行，可以用status 选项。例如验证sshd 是否真的启动了：

```
# /etc/rc.d/sshd status
sshd is running as pid 433.
```

有些时候也可以reload 服务。这一操作实际上是向服务发送一个信号，来强制其重新加载配置。多数情况下，发给服务的会是SIGHUP 信号。并非所有服务都支持这一功能。

rc.d 系统不仅用于网络服务，它也为系统初始化中的多数过程提供支持。比如bgfsck 文件，当它被执行时，将会给出下述信息：

```
Starting background file system checks in 60 seconds.
```

这个文件用做后台文件系统检查，系统初始化的时候完成。

很多系统服务依赖其他服务提供的相应功能。例如，NIS 和其他基于RPC 的服务启动可能在rpcbind 服务启动之前失败。要解决这个问题，依赖关系信息和其他头信息当作注释被包含在每个启动脚本文件的前面。程序在系统初始化时分析这些注释以决定调用其他系统服务来满足依赖关系。下面的字句可能会包含在每个启动脚本文件的前面：

- PROVIDE: Specifies the services this file provides.
- REQUIRE: Lists services which are required for this service. This file will run **after** the specified services.
- BEFORE: Lists services which depend on this service. This file will run **before** the specified services.

通过这种方法，系统管理员可以容易的控制系统而不用像其他一些UNIX 操作系统一样要用“runlevels”来控制。

更多关于rc.d 系统的信息，可以在rc(8) 和rc.subr(8) 联机手册中找到。

11.8 设置网卡

Contributed by Marc Fonvieille.

现在我们不可想象一个计算机没有网络连接的情况。添加和配置一块网卡是任何FreeBSD 系统管理员的一项基本任务。

11.8.1 查找正确的驱动程序

在开始之前，您应该知道您的网卡类型，它用的芯片和它是PCI 还是ISA 网卡。FreeBSD 支持很多种PCI 和ISA 网卡。可以查看您的版本硬件兼容性列表以确定您的网卡被支持。

确认系统能够支持您的网卡之后，您还需要为它选择合适的驱动程序。`/usr/src/sys/conf/NOTES` 和 `/usr/src/sys/arch/conf/NOTES` 将为您提供所支持的一些网卡和芯片组的信息。如果您怀疑驱动程序是否使所要找的那一个，请参考驱动程序的联机手册。联机手册将提供关于所支持的硬件更详细的信息，甚至还包括可能发生的问题。

注意: NOTES 在FreeBSD 4.X 上并不存在。您需要查看LINT 来了解关于网卡的信息。参见第8.4 节 以了解关于NOTES 和LINT 的进一步信息。

如果您有一个普通的网卡，大多数时候您不需要为驱动浪费精力。常用的网卡在GENERIC 内核中已经支持了，所以您的网卡在启动时就会显示出来，像是：

```
dc0: <82c169 PNIC 10/100BaseTX> port 0xa000-0xa0ff mem 0xd3800000-0xd38000ff irq 15 at device 11.0 on pci0
dc0: Ethernet address: 00:a0:cc:da:da:da
miibus0: <MII bus> on dc0
ukphy0: <Generic IEEE 802.3u media interface> on miibus0
ukphy0: 10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, auto
dc1: <82c169 PNIC 10/100BaseTX> port 0x9800-0x98ff mem 0xd3000000-0xd30000ff irq 11 at device 12.0 on pci0
dc1: Ethernet address: 00:a0:cc:da:da:db
miibus1: <MII bus> on dc1
ukphy1: <Generic IEEE 802.3u media interface> on miibus1
ukphy1: 10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, auto
```

在这个例子中，我们看到有两块使用dc(4) 驱动的网卡在系统中。

如果您的网卡没有出现在GENERIC 中，则需要手工加载合适的驱动程序。要完成这项工作可以使用下面两种方法之一：

- 最简单的办法是用`kldload(8)` 加载网卡对应的内核模块。并不是所有的网卡都能够通过这种方法提供支持；比较明显的例子是ISA 网卡。
- 另外，您也可以将网卡的支持静态联编进内核。察看`/usr/src/sys/conf/NOTES`，`/usr/src/sys/arch/conf/NOTES` 以及驱动程序的联机手册以了解需要在您的内核配置文件中加一些什么。要了解关于重新编译内核的进一步细节，请参见第8 章。如果您的卡在引导时可以被内核(GENERIC) 识别，您应该不需要编译新的内核。

11.8.2 配置网卡

现在正确的网卡驱动程序已经装载，那么就应该配置它了。跟其他配置一样，网卡可以在安装时用 `sysinstall` 来配置。

要显示您系统上的网络接口的配置，输入下列命令：

```
% ifconfig
dc0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 192.168.1.3 netmask 0xfffffff00 broadcast 192.168.1.255
    ether 00:a0:cc:da:da:da
    media: Ethernet autoselect (100baseTX <full-duplex>)
    status: active
dc1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 10.0.0.1 netmask 0xfffffff00 broadcast 10.0.0.255
    ether 00:a0:cc:da:da:db
    media: Ethernet 10baseT/UTP
    status: no carrier
lp0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet 127.0.0.1 netmask 0xff000000
tun0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
```

注意：老版本的FreeBSD可能需要在`ifconfig(8)`后面接`-a`选项，需要了解更多的`ifconfig(8)`语法请查阅使用手册。注意所有关于IPv6 (`inet6` 等等) 的记录在这个例子里都被忽略了。

在这个例子中，显示出了下列设备：

- `dc0`: The first Ethernet interface
- `dc1`: The second Ethernet interface
- `lp0`: The parallel port interface
- `lo0`: The loopback device
- `tun0`: The tunnel device used by **ppp**

FreeBSD 使用内核引导时检测到的网卡驱动顺序来命名网卡。例如 `sis2` 是系统中使用 `sis(4)` 驱动的第三块网卡。

在这个例子中，`dc0` 设备启用了。主要表现在：

1. `UP` 表示这块网卡已经配置完成准备工作。
2. 这块网卡有一个Internet (`inet`) 地址(这个例子中是`192.168.1.3`)。
3. 它有一个有效的子网掩码(`netmask`; `0xfffffff00` 等同于`255.255.255.0`)。
4. 它有一个有效的广播地址(这个例子中是`192.168.1.255`)。
5. 网卡的MAC (`ether`) 地址是`00:a0:cc:da:da:da`
6. 物理传输媒介模式处于自动选择状态(`media: Ethernet autoselect (100baseTX <full-duplex>)`)。我们看到`dc1` 被配置成运行在`10baseT/UTP` 模式下。要了解驱动媒介类型的更多信息，请查阅它们的使用手册。

7. 连接状态(status)是active, 也就是说连接信号被检测到了。对于dc1, 我们看到status: no carrier。这通常是网线没有插好。

如果ifconfig(8) 的输出显示了类似于:

```
dc0: flags=8843<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
    ether 00:a0:cc:da:da:da
```

的信息, 那么就是还没有配置网卡。

要配置网卡, 您需要root 权限。网卡配置可以通过使用ifconfig(8) 命令行方式来完成, 但是这样每次启动都要做一遍。放置网卡配置信息的文件是/etc/rc.conf。

用您自己喜欢的编辑器打开/etc/rc.conf。并且您需要为每一块系统中存在的网卡添加一行, 在我们的例子中, 添加如下几行:

```
ifconfig_dc0="inet 192.168.1.3 netmask 255.255.255.0"
ifconfig_dc1="inet 10.0.0.1 netmask 255.255.255.0 media 10baseT/UTP"
```

用自己正确的设备名和地址来替换例子中的dc0, dc1 等内容。您应该应该查阅网卡驱动和ifconfig(8) 的手册页来了解各选项, 也要查看一下rc.conf(5) 帮助页来了解/etc/rc.conf 的语法。

如果在安装的时候配置了网络, 关于网卡的一些行可能已经存在了。所以在添加新行前仔细检查一下/etc/rc.conf。

您可能也需要编辑/etc/hosts 来添加局域网中不同的机器名称和IP 地址, 如果它们不存在, 查看hosts(5) 帮助和/usr/share/examples/etc/hosts 以获得更多信息。

11.8.3 测试和调试

对/etc/rc.conf 做了必要的修改之后应该重启系统以应用对接口的修改, 并且确认系统重启后没有任何配置错误。

系统重启后就应该测试网络接口了。

11.8.3.1 测试以太网卡

为了确认网卡被正确的配置了, 在这里我们要做两件事情。首先, ping 自己的网络接口, 接着ping 局域网内的其他机器。

首先测试本地接口:

```
% ping -c5 192.168.1.3
PING 192.168.1.3 (192.168.1.3): 56 data bytes
64 bytes from 192.168.1.3: icmp_seq=0 ttl=64 time=0.082 ms
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.074 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.076 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.108 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.076 ms

--- 192.168.1.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.074/0.083/0.108/0.013 ms
```

现在我们应该ping 局域网内的其他机器:

```
% ping -c5 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=0.726 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.766 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.700 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.747 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.704 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.700/0.729/0.766/0.025 ms
```

您如果您设置了/etc/hosts 文件，也可以用机器名来替换192.168.1.2。

11.8.3.2 调试

调试硬件和软件配置一直是一件头痛的事情，从最简单的开始可以减轻一些痛苦。例如网线是否插好了？是否配置好了网络服务？防火墙配置正确吗？是否使用了被支持的网卡？在发送错误报告之前您应该查看一下硬件说明，升级FreeBSD 到最新的STABLE 版本，看一下邮件列表或者在Internet 上搜索一下。

如果网卡工作了，但性能低下，应该好好阅读一下tuning(7) 联机手册。您也可以检查一下网络配置，不正确的设置会导致慢速的网络连接。

一些用户可能会在一些网卡上经历一到两次device timeouts，这通常是正常现象。如果经常这样甚至引起麻烦，则应确定一下它跟其他设备没有冲突。仔细检查网线连接，或者换一块网卡。

有时用户会看到少量watchdog timeout 错误。这种情况要做的第一件事就是检查线缆连接。一些网卡需要支持总线控制的PCI 插槽。在一些老的主板上，只有一个PCI 插槽支持(一般是slot 0)。检查网卡和主板说明书来确定是不是这个问题。

No route to host 通常发生在如果系统不能发送一个路由到目的主机的包的时候。这在没有指定默认路由或者网线没有插上时会发生。检查netstat -rn 的输出并确认有一个有效的路由能到达相应的主机。如果没有，请查阅第27 章。

ping: sendto: Permission denied 错误信息经常由防火墙的配置错误引起。如果ipfw 在内核中启用了但是没有定义规则，那么默认的规则就是拒绝所有通讯，甚至ping 请求！查阅第26 章 以了解更多信息。

有时网卡性能低下或者低于平均水平，这种情况最好把传输媒介模式从autoselect 改变为正确的传输介质模式。这通常对大多数硬件有用，但可能不会解决所有人的问题。接着，检查所有网络设置，并且阅读tuning(7) 手册页。

11.9 虚拟主机

FreeBSD 的一个很普通的用途是虚拟主机站点，一个服务器虚拟成很多服务器一样提供网络服务。这通过在一个接口上绑定多个网络地址来实现。

一个特定的网络接口有一个“真实”的地址，也可能有一些“别名”地址。这些别名通常用/etc/rc.conf 中的记录来添加。

一个fxp0 的别名记录类似于:

```
ifconfig_fxp0_alias0="inet xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx"
```

记住别名记录必须从alias0 开始并且按顺序递增(例如_alias1、_alias2)。配置程序将会停止在第一个缺少的数字的地方。

计算别名的子网掩码是很重要的, 幸运的是它很简单。对于一个接口来说, 必须有一个描述子网掩码的地址。任何在这个网段下的地址必须有一个全是1 的子网掩码(通常表示为255.255.255.255 或0xffffffff)。

举例来说, 假设使用fxp0 连接到两个网络, 分别是10.1.1.0, 其子网掩码为255.255.255.0, 以及202.0.75.16, 其子网掩码为255.255.255.240。我们希望能从10.1.1.1到10.1.1.5 以及从202.0.75.17 到202.0.75.20 的地址能够互相访问。如前所述, 只有两个网段中的第一个地址(本例中, 10.0.1.1 和202.0.75.17) 应使用真实的子网掩码; 其余的(10.1.1.2 到10.1.1.5 以及202.0.75.18 到202.0.75.20) 则必须配置为使用255.255.255.255 作为子网掩码。

下面是根据上述描述所进行的/etc/rc.conf 配置:

```
ifconfig_fxp0="inet 10.1.1.1 netmask 255.255.255.0"
ifconfig_fxp0_alias0="inet 10.1.1.2 netmask 255.255.255.255"
ifconfig_fxp0_alias1="inet 10.1.1.3 netmask 255.255.255.255"
ifconfig_fxp0_alias2="inet 10.1.1.4 netmask 255.255.255.255"
ifconfig_fxp0_alias3="inet 10.1.1.5 netmask 255.255.255.255"
ifconfig_fxp0_alias4="inet 202.0.75.17 netmask 255.255.255.240"
ifconfig_fxp0_alias5="inet 202.0.75.18 netmask 255.255.255.255"
ifconfig_fxp0_alias6="inet 202.0.75.19 netmask 255.255.255.255"
ifconfig_fxp0_alias7="inet 202.0.75.20 netmask 255.255.255.255"
```

11.10 配置文件

11.10.1 /etc 布局

在配置信息中有很多的目录, 这些包括:

/etc	一般的系统配置信息。这儿的数据是与特定系统相关的。
/etc/defaults	系统配置文件的默认版本。
/etc/mail	额外的sendmail(8) 配置信息, 其他MTA 配置文件。
/etc/ppp	用于用户级和内核级ppp 程序的配置。
/etc/namedb	named(8) 数据的默认位置。通常named.conf 和区域文件存放在这里。
/usr/local/etc	被安装的应用程序配置文件。可以参考每个应用程序的子目录。
/usr/local/etc/rc.d	被安装程序的启动/停止脚本。
/var/db	特定系统自动产生的数据库文件, 像package 数据库, 位置数据库等等。

11.10.2 主机名

11.10.2.1 /etc/resolv.conf

/etc/resolv.conf 指示了FreeBSD 如何访问域名系统(DNS)。

resolv.conf 中最常见的记录是:

nameserver	按顺序要查询的名字服务器的IP 地址，最多三个。
search	搜索机器名的列表。这通常由本地机器名的域决定。
domain	本地域名。

一个典型的resolv.conf 文件:

```
search example.com
nameserver 147.11.1.11
nameserver 147.11.100.30
```

注意: 只能使用一个search 和domain 选项。

如果您在使用DHCP，dhclient(8) 经常使用从DHCP 服务器接受来的信息重写resolv.conf。

11.10.2.2 /etc/hosts

/etc/hosts 是Internet 早期使用的一个简单文本数据库。它结合DNS 和NIS 提供名字到IP 地址的映射。通过局域网连接的机器可以用这个简单的命名方案来替代设置一个named(8) 服务器。另外，/etc/hosts 也可以提供一个Internet 名称的本地纪录以减轻需要从外部查询带来的负担。

```
# $FreeBSD$
#
# Host Database
# This file should contain the addresses and aliases
# for local hosts that share this file.
# In the presence of the domain name service or NIS, this file may
# not be consulted at all; see /etc/nsswitch.conf for the resolution order.
#
#
::1                localhost localhost.my.domain myname.my.domain
127.0.0.1          localhost localhost.my.domain myname.my.domain

#
# Imaginary network.
#10.0.0.2          myname.my.domain myname
#10.0.0.3          myfriend.my.domain myfriend
#
# According to RFC 1918, you can use the following IP networks for
# private nets which will never be connected to the Internet:
#
#      10.0.0.0      -      10.255.255.255
```

```
#      172.16.0.0      -   172.31.255.255
#      192.168.0.0     -   192.168.255.255
#
# In case you want to be able to connect to the Internet, you need
# real official assigned numbers. PLEASE PLEASE PLEASE do not try
# to invent your own network numbers but instead get one from your
# network provider (if any) or from the Internet Registry (ftp to
# rs.internic.net, directory '/templates').
#
```

/etc/hosts 用简单的格式:

```
[Internet address] [official hostname] [alias1] [alias2] ...
```

例如:

```
10.0.0.1 myRealHostname.example.com myRealHostname foobar1 foobar2
```

参考hosts(5) 以获得更多信息。

11.10.3 日志文件配置

11.10.3.1 syslog.conf

syslog.conf 是syslogd(8) 程序的配置文件。它指出了的syslog 哪种信息类型被存储在特定的日志文件中。

```
# $FreeBSD$
#
#      Spaces ARE valid field separators in this file. However,
#      other *nix-like systems still insist on using tabs as field
#      separators. If you are sharing this file between systems, you
#      may want to use only tabs as field separators here.
#      Consult the syslog.conf(5) manual page.
*.err;kern.debug;auth.notice;mail.crit      /dev/console
*.notice;kern.debug;lpr.info;mail.crit;news.err /var/log/messages
security.*                                    /var/log/security
mail.info                                     /var/log/maillog
lpr.info                                      /var/log/lpd-errs
cron.*                                       /var/log/cron
*.err                                         root
*.notice;news.err                           root
*.alert                                      root
*.emerg                                      *
# uncomment this to log all writes to /dev/console to /var/log/console.log
#console.info                               /var/log/console.log
# uncomment this to enable logging of all log messages to /var/log/all.log
#*. *                                        /var/log/all.log
# uncomment this to enable logging to a remote log host named loghost
#*. *                                        @loghost
# uncomment these if you're running inn
```

```

# news.crit                /var/log/news/news.crit
# news.err                 /var/log/news/news.err
# news.notice              /var/log/news/news.notice
!startslip
*.*                        /var/log/slip.log
!ppp
*.*                        /var/log/ppp.log

```

参考syslog.conf(5)手册页以获得更多信息

11.10.3.2 newsyslog.conf

newsyslog.conf 是一个通常用cron(8) 计划运行的newsyslog(8) 程序的配置文件。newsyslog(8) 指出了什么时候日志文件需要打包或者重新整理。比如logfile 被移动到logfile.0, logfile.0 被移动到logfile.1 等等。另外, 日志文件可以用gzip(1) 来压缩, 它们是这样的命名格式: logfile.0.gz, logfile.1.gz 等等。

newsyslog.conf 指出了哪个日志文件要被管理, 要保留多少和它们什么时候被创建。日志文件可以在它们达到一定大小或者在特定的日期被重新整理。

```

# configuration file for newsyslog
# $FreeBSD$
#
# filename          [owner:group]    mode count size when [ZB] [/pid_file] [sig_num]
/var/log/cron                600  3    100  *    Z
/var/log/amd.log             644  7    100  *    Z
/var/log/kerberos.log        644  7    100  *    Z
/var/log/lpd-errs            644  7    100  *    Z
/var/log/maillog             644  7    *    @T00  Z
/var/log/sendmail.st         644 10    *    168  B
/var/log/messages            644  5    100  *    Z
/var/log/all.log             600  7    *    @T00  Z
/var/log/slip.log            600  3    100  *    Z
/var/log/ppp.log             600  3    100  *    Z
/var/log/security            600 10    100  *    Z
/var/log/wtmp                644  3    *    @01T05 B
/var/log/daily.log           640  7    *    @T00  Z
/var/log/weekly.log          640  5    1    $W6D0 Z
/var/log/monthly.log         640 12    *    $M1D0 Z
/var/log/console.log         640  5    100  *    Z

```

参考newsyslog(8)手册页以获得更多信息。

11.10.4 sysctl.conf

sysctl.conf 看起来很像rc.conf。它用variable=value 的形式来设定值。指定的值在系统进入多用户模式之后被设定。并不是所有的变量都可以在这个模式下设定。

一个简单的例子举明了在sysctl.conf 中关闭了重要的退出信号的日志并且让Linux 程序知道他们其实运行在FreeBSD 下面:

```
kern.logsigexit=0      # Do not log fatal signal exits (e.g. sig 11)
compat.linux.osname=FreeBSD
compat.linux.osrelease=4.3-STABLE
```

11.11 用sysctl 进行调整

sysctl(8) 是一个允许您改变正在运行中的FreeBSD 系统的接口。它包含一些TCP/IP 堆栈和虚拟内存系统的高级选项，这可以让有经验的管理员提高引人注目的系统性能。用sysctl(8) 可以读取设置超过五百个系统变量。

基于这点，sysctl(8) 提供两个功能：读取和修改系统设置。

查看所有可读变量：

```
% sysctl -a
```

读一个指定的变量，例如kern.maxproc：

```
% sysctl kern.maxproc
kern.maxproc: 1044
```

要设置一个指定的变量，直接用`variable=value` 这样的语法：

```
# sysctl kern.maxfiles=5000
kern.maxfiles: 2088 -> 5000
```

sysctl 变量的设置通常是字符串、数字或者布尔型。(布尔型用1 来表示‘yes’，用0 来表示‘no’)。

If you want to set automatically some variables each time the machine boots, add them to the /etc/sysctl.conf file. For more information see the sysctl.conf(5) manual page and the 第11.10.4 节。

11.11.1 只读的sysctl(8)

Contributed by Tom Rhodes.

有时可能会需要修改某些只读的sysctl(8) 的值。尽管有时不得不这样做，但只有通过(重新)启动才能达到这样的目的。

例如一些膝上型电脑的cardbus(4) 设备不会探测内存范围，并且产生看似于这样的错误：

```
cbb0: Could not map register memory
device_probe_and_attach: cbb0 attach returned 12
```

像上面的错误通常需要修改一些只读的sysctl(8) 默认设置。要实现这点，用户可以在本地的/boot/loader.conf.local 里面放一个sysctl(8) “OIDs”。那些设置定位在/boot/defaults/loader.conf 文件中。

修复上面的问题用户需要在刚才所说的文件中设置hw.pci.allow_unsupported_io_range=1。现在在cardbus(4) 就会正常的工作了。

11.12 调整磁盘

11.12.1 Sysctl 变量

11.12.1.1 vfs.vmiodirenable

`vfs.vmiodirenable` sysctl 变量可以设置成0(关)或者1(开); 默认是1。这个变量控制目录是否被系统缓存。大多数目录是小的, 在系统中只使用单个片断(典型的是1K)并且在缓存中使用的更小(典型的是512字节)。当这个变量设置为关闭(0)时, 缓存器仅仅缓存固定数量的目录, 即使您有很大的内存。而将其开启(设置为1)时, 则允许缓存器用VM 页面缓存来缓存这些目录, 让所有可用内存来缓存目录。不利的是最小的用来缓存目录的核心内存是大于512 字节的物理页面大小(通常是4k)。我们建议如果您在运行任何操作大量文件的程序时保持这个选项打开的默认值。这些服务包括web 缓存, 大容量邮件系统和新闻系统。尽管可能会浪费一些内存, 但打开这个选项通常不会降低性能。但还是应该检验一下。

11.12.1.2 vfs.write_behind

`vfs.write_behind` sysctl 变量默认是1 (打开)。它告诉文件系统簇被收集满的时候把内容写进介质, 典型的是在写入大的连续的文件时。主要的想法是, 如果可能对I/O 性能会产生负面影响时, 应尽量避免让缓冲缓存被未同步缓冲区充满。然而它可能降低处理速度并且在某些情况下您可能想要关闭它。

11.12.1.3 vfs.hirunningspace

`vfs.hirunningspace` sysctl 变量决定了在任何场合多少写I/O 被排进队列以给系统的磁盘控制器。默认值一般是足够的, 但是对有很多磁盘的机器来说您可能需要把它设置成4M 或5M。注意这个设置成很高的值(超过缓存器的写极限)会导致坏的性能。不要盲目的把它设置太高! 高的数值会导致同时发生的读操作的迟延。

sysctl 中还有许多与buffer cache 和VM页面cache 有关的值, 一般不推荐修改它们。从FreeBSD 4.3 开始, 虚拟内存系统已经能够很好地进行自动调整了。

11.12.1.4 vm.swap_idle_enabled

`vm.swap_idle_enabled` sysctl 变量在有很多用户进入、离开系统和有很多空闲进程的大的多用户系统中很有用。这些系统注重在空闲的内存中间产生连续压力的处理。通过`vm.swap_idle_threshold1`和`vm.swap_idle_threshold2`打开这个特性并且调整交换滞后(在空闲时)允许您降低内存页中空闲进程的优先权, 从而比正常的出页(pageout)算法更快。这给出页守护进程带来了帮助。除非您需要否则不要把这个选项打开, 因为您所权衡的是更快地进入内存, 因而它会吃掉更多的交换和磁盘带宽。在小的系统上它会有决定性的效果, 但是在大的系统上它已经做了合适的页面调度这个选项允许VM 系统容易的让全部的进程进出内存。

11.12.1.5 hw.ata.wc

FreeBSD 4.3 中默认将IDE 的写缓存关掉了。这会降低到IDE 磁盘用于写入操作的带宽, 但我们认为这有助于避免硬盘厂商所引入的, 可能引致严重的数据不一致问题。这类问题实际上是由于IDE 硬盘就写操作完成这件事的不诚实导致的。当启用了IDE 写入缓存时, IDE 硬盘驱动器不但不会按顺序将数据写到盘上, 而且当磁盘承受重载时, 它甚至会自作主张地对推迟某些块的实际写操作。这样一来, 在系统发生崩溃或掉电时, 就会导致严重的文件系统损坏。基于这些考虑, 我们将FreeBSD 的默认配置改成了更为安全

的禁用IDE 写入缓存。然而不幸的是，这样做导致了性能的大幅降低，因此在后来的发行版中这个配置又改为默认启用了。您可以通过观察`hw.ata.wc sysctl` 变量，来确认您的系统中所采用的默认值。如果IDE 缓存被禁用，您可以通过将内核变量设置为1 来启用它。这一操作必须在启动时通过boot loader 来完成。在内核启动之后尝试这么做是没有任何作用的。

要了解更多的信息，请查阅`ata(4)`。

11.12.1.6 SCSI_DELAY (kern.cam.scsi_delay)

SCSI_DELAY 内核配置会缩短系统启动时间。默认值在系统启动过程中有15 秒的迟延时间，这是一个足够多且可靠的值。把它减少到5 通常也能工作(特别是现代的驱动器)。新一些的FreeBSD (5.0 或更高版本) 应该用启动时刻可调整`kern.cam.scsi_delay`。这个可调整的和内核配置选项接受的值是毫秒 不是 秒。

11.12.2 Soft Updates

`tunefs(8)` 程序能够用来很好的调整文件系统。这个程序有很多不同的选项，但是现在只介绍Soft Updates 的打开和关闭，这样做：

```
# tunefs -n enable /filesystem
# tunefs -n disable /filesystem
```

在文件系统被挂载之后不能用`tunefs(8)` 来修改。打开Soft Updates 的最佳时机是在单用户模式下任何分区被被挂载前。

注意：像FreeBSD 4.5，在文件系统创建时也可以打开Soft Updates，通过`newfs(8)` 的`-u` 选项。

Soft Updates 彻底的改善了数据描述(meta-data)的性能，主要是文件创建和删除，通过内存缓存。我们建议您在所有的文件系统上使用Soft Updates。应该知道Soft Updates 的两点：首先，Soft Updates 保证了崩溃后的文件系统完整性，但是很可能有几秒钟(甚至一分钟！) 之前的数据没有写到物理磁盘。如果您的系统崩溃了您可能会丢失很多工作。第二，SoftUpdates 推迟文件系统块的释放时间。如果在文件系统(例如根文件系统)快满了的情况下对系统进行大规模的升级比如`make installworld`，可能会引起磁盘空间不足从而造成升级失败。

11.12.2.1 Soft Updates 的详细资料

有两种传统的方法来把文件系统的元数据(meta-data) 写入磁盘。(Meta-data更新是更新类似inodes 或者目录这些没有内容的数据)

从前，默认方法是同步更新这些元数据(meta-data)。如果一个目录改变了，系统在真正写到磁盘之前一直等待。文件数据缓存(文件内容)在这之后以非同步形式写入。这么做有利的一点是操作安全。如果更新时发生错误，元数据(meta-data) 一直处于完整状态。文件要不就被完整的创建要不根本就不创建。如果崩溃时找不到文件的数据块，`fsck(8)` 可以找到并且依靠把文件大小设置为0 来修复文件系统。另外，这么做既清楚又简单。缺点是元数据(meta-data)更新很慢。例如`rm -r` 命令，从而改变目录下的所有文件，但是每个目录的改变(删除一个文件)都要同步写入磁盘。这包含它自己更新目录，inode 表和可能对文件分散的块的更新。同样问题出现大的文件操作上(比如`tar -x`)。

第二种方法是非同步元数据更新。这是Linux/ext2fs 和*BSD ufs 的`mount -o async` 默认的方法。所有元数据更新也是通过缓存。也就是它们会混合在文件内容数据更新中。这个方法的优点是不需要等待每个

元数据更新都写到磁盘上，所以所有引起元数据更新大的操作比同步方式更快。同样，这个方法也是清楚且简单的，所以代码中的漏洞风险很小。缺点是不能保证文件系统的状态一致性。如果更新大量元数据时失败(例如掉电或者按了重启按钮)，文件系统会处在不可预知的状态。系统再启动时没有机会检查文件系统的状态；inode 表更新的时候可能文件的数据块已经写入磁盘了但是相关联的目录没有，却不能用 `fsck` 命令来清理(因为磁盘上没有所需要的信息)。如果文件系统修复后损坏了，唯一的选择是使用 `newfs(8)` 并且从备份中恢复它。

这个问题通常的解决办法是使用 **dirty region logging** 或者 **journaling** 尽管它不是一贯的被使用并且有时候应用到其他的事务纪录中更好。这种方法元数据更新依然同步写入，但是只写到磁盘的一个小区域。过后他们将会被移动到正确的位置。因为纪录区很小，磁盘上接近的区域磁头不需要移动很长的距离，所以这些比写同步快一些。另外这个方法的复杂性有限，所以出现错误的机会也很少。缺点是元数据要写两次(一次写到纪录区域，一次写到正确的区域)。正常情况下，悲观的性能可能会发生。从另一方面来讲，崩溃的时候所有未发生的元数据操作可以很快的在系统启动之后从记录中恢复过来。

Kirk McKusick，伯克利FFS 的开发者，用Soft Updates 解决了这个问题：元数据更新保存在内存中并且按照排列的顺序写入到磁盘(“有序的元数据更新”)。这样的结果是，在繁重的元数据操作中，如果先前的更新还在内存中没有别写进磁盘，后来的更新就会捕捉到。所以所有的目录操作在写进磁盘的时候首先在内存中执行(数据块按照它们的位置来排列，所以它们不会在元数据前被写入)。如果系统崩溃了这将导致一个固定的“日志回朔”：所有不知如何写入磁盘的操作都像没有发生过一样。文件系统的一致性保持在30到60秒之前。它保证了所有正在使用的资源被标记例如块和inodes。崩溃之后，唯一的资源分配错误是一个实际是“空闲”的资源的资源被标记为“使用”。`fsck(8)` 可以认出这种情况并且释放不再使用的资源。它对于忽略崩溃后用 `mount -f` 强制挂上的文件系统的错误状态是安全的。为了释放可能没有使用的资源，`fsck(8)` 需要在过后的时间运行。一个主意是用**后台fsck**：系统启动的时候只有一个文件系统的**快照**被记录下来。`fsck` 可以在过后运行。所有文件系统可以在“有错误”的时候被挂接，所以系统可以在多用户模式下启动。接着，后台 `fsck` 可以在所有文件系统需要的时候启动来释放可能没有使用的资源。(尽管这样，不用Soft Updates 的文件系统依然需要通常的 `fsck`。)

它的优点是元数据操作几乎跟非同步一样快(也就是比需要两次元数据写操作的**logging** 更快)。缺点是代码的复杂性(意味着对于丢失用户敏感数据有更多的风险)和高的内存使用量。另外它有些特点需要知道。崩溃之后，文件系统状态会“落后”一些。同步的方法用 `fsck` 后在一些地方可能产生一些零字节的文件，这些文件在用Soft Updates 文件系统之后不会存在，因为元数据和文件内容根本没有写进磁盘(可能发生在运行 `rm` 之后)。这可能在文件系统上安装大量数据时候引发问题，没有足够的剩余空间来两次存储所有文件。

11.13 调整内核限制

11.13.1 文件/进程限制

11.13.1.1 kern.maxfiles

`kern.maxfiles` 可以根据系统的需要适当增减。这个变量用于指定在系统中允许的文件描述符的最大数量。当文件描述符表满的时候，`file: table is full` 会在系统消息缓冲区中反复出现，您可以使用 `dmesg` 命令来观察这一现象。

每个打开的文件、套接字和管道，都会占用一个文件描述符。在大型生产服务器上，可能会轻易地用掉数千个文件描述符，具体用量取决于服务的类型和并行启动的服务数量。

`kern.maxfile` 的默认值，是由您内核配置文件中的 `maxusers` 选项决定的。`kern.maxfiles` 这个数值，会与 `maxusers` 成比例增减。当编译定制的内核时，按照您系统的用途来修改这个值是个好主意。这个数字同时还决定内核的许多预设的限制值。有时，尽管并不会真的有256个用户同时连接一台生产服务器，但对于高负载的web服务器而言，却可能需要与之类似的资源。

从FreeBSD 4.5开始，如果您明确地将 `maxusers` 设置为0，则系统会自动地根据硬件配置来确定这个值。¹。在FreeBSD 5.X和更高版本中，`maxusers` 如果不指定的话，就会取默认值0。如果您正使用的是FreeBSD 4.5之前的版本，或者希望自行管理 `maxusers`，则应配置一个不低于4的值，特别是使用X Window System 或编译软件的时候。这样做的原因是，`maxusers` 所决定的一个最为重要的表的尺寸会影响最大进程数，这个数值将是 $20 + 16 * \text{maxusers}$ 。因此如果将 `maxusers` 设置为1，您就只能同时运行36个进程，这还包括了18个左右的系统引导时启动的进程，以及15个左右的，在您启动X Window System 时所引发的进程。即使是简单的任务，如阅读联机手册，也需要启动多至九个的进程，用以过滤、解压缩，并显示它。将 `maxusers` 设为64将允许您同时执行最多1044个进程，这几乎足以满足任何需要了。不过，如果您看启动其它程序，或运行用以支持大量用户的服务(例如 `ftp.FreeBSD.org`) 时，看到令人担忧的 `proc table full` 错误，就应该提高这一数值，并重新联编内核。

注意: `maxusers` 并不能限制能够登录到您机器上的用户的实际数量。它只是简单地将一系列内核数据表设置为合理的尺寸，使其与您系统上可能同时登录的用户的最大数量相适应。**确实** 能够限制同时进行的远程登录，以及X终端窗口数量的关键字是 `pseudo-device pty 16`。从FreeBSD 5.X开始，您不再需要担心这个数字，因为 `pty(4)` 驱动具备了“自动克隆”的能力；只需在配置文件中配置 `device pty` 就可以了。

11.13.1.2 kern.ipc.somaxconn

`kern.ipc.somaxconn sysctl` 变量限制了接收新TCP连接侦听队列的大小。对于一个经常处理新连接的高负载web服务环境来说，默认的128太小了。大多数环境这个值建议增加到1024或者更多。服务进程会自己限制侦听队列的大小(例如 `sendmail(8)` 或者 **Apache**)，常常在它们的配置文件中有设置队列大小的选项。大的侦听队列对防止拒绝服务DoS攻击也会有所帮助。

11.13.2 网络限制

`NMBCLUSTERS` 内核配置选项指出了系统可用的网络Mbuf的数量。一个高流量的服务器使用一个小数目的网络缓存会影响FreeBSD的性能。每个cluster可能需要2K内存，所以一个1024的值需要在内核中给网络缓存保留2M内存。可以用简单的方法计算出来需要多少网络缓存。如果您有一个同时发生1000个以上连接的web服务器，并且每个连接用掉16K接收和发送缓存，就需要大概32M网络缓存来确保web服务器的工作。一个好的简单计算方法是乘以2，所以 $2 \times 32\text{Mb} / 2\text{Kb} = 64\text{MB} / 2\text{kb} = 32768$ 。我们建议在有大量内存的机器上把这个值设置在4096到32768之间。没有必要把它设置成任意太高的值，它会在启动时引起崩溃。`netstat(1)` 的 `-m` 选项可以用来观察网络cluster使用情况。

`kern.ipc.nmbclusters` 可以用来在启动时刻调节这个。仅仅在旧版本的FreeBSD需要使用 `NMBCLUSTERS config(8)` 选项。

经常使用 `sendfile(2)` 系统调用的繁忙的服务器，有必要通过 `NSFBUFS` 内核选项或者在 `/boot/loader.conf` (查看 `loader(8)` 以获得更多细节) 中设置它的值来调节 `sendfile(2)` 缓存数量。这个参数需要调节的普通原因是在进程中看到 `sfbufa` 状态。`sysctl kern.ipc.nsfbufs` 变量在内核配置变量中是只读的。这个参数是由 `kern.maxusers` 决定的，然而它可能有必因此而调整。

重要: 即使一个套接字被标记成非阻塞, 在这个非阻塞的套接字上呼叫`sendfile(2)` 可能导致`sendfile(2)` 呼叫阻塞直到有足够的`struct sf_buf` 可用。

11.13.2.1 net.inet.ip.portrange.*

`net.inet.ip.portrange.*` `sysctl` 变量自动的控制绑定在TCP 和UDP 套接字上的端口范围。这里有三个范围: 一个低端范围, 一个默认范围和一个高端范围。大多数网络程序分别使用由`net.inet.ip.portrange.first` 和`net.inet.ip.portrange.last` 控制的从1024 到5000 的默认范围。端口范围用作对外连接, 并且某些情况可能用完系统的端口, 这经常发生在运行一个高负荷web 代理服务器的时候。这个端口范围不是用来限制主要的例如web 服务器进入连接或者有固定端口例如邮件传递对外连接的。有时您可能用完了端口, 那就建议适当的增加`net.inet.ip.portrange.last`。10000、20000 或者30000 可能是适当的值。更改端口范围的时候也要考虑到防火墙。一些防火墙会阻止端口的大部分范围(通常是低范围的端口)并且用高端口进行对外连接(——)。基于这个问题建议不要把`net.inet.ip.portrange.first` 设的太小。

11.13.2.2 TCP 带宽延迟(Bandwidth Delay Product)

限制TCP 带宽延迟积和NetBSD 的TCP/Vegas 类似。它可以通过将`sysctl` 变量`net.inet.tcp.inflight.enable` 设置成1 来启用。系统将尝试计算每一个连接的带宽延迟积, 并将排队的数据量限制在恰好能保持最优吞吐量的水平上。

这一特性在您的服务器同时向使用普通调制解调器, 千兆以太网, 乃至更高速度的光与网络连接(或其他带宽延迟积很大的连接) 的时候尤为重要, 特别是当您同时使用滑动窗缩放, 或使用了大的发送窗口的时候。如果启用了这个选项, 您还应该把`net.inet.tcp.inflight.debug` 设置为0 (禁用调试), 对于生产环境而言, 将`net.inet.tcp.inflight.min` 设置成至少6144 会很有好处。然而, 需要注意的是, 这个值设置过大事实上相当于禁用了连接带宽延迟积限制功能。这个限制特性减少了在路由和交换包队列的堵塞数据数量, 也减少了在本地主机接口队列阻塞的数据的数量。在少数的等候队列中、交互式连接, 尤其是通过慢速的调制解调器, 也能用低的往返时间操作。但是, 注意这只影响到数据发送(上载/服务端)。对数据接收(下载)没有效果。

调整`net.inet.tcp.inflight.stab` 是不推荐的。这个参数的默认值是20, 表示把2 个最大包加入到带宽延迟积窗口的计算中。额外的窗口似的算法更为稳定, 并改善对于多变网络环境的相应能力, 但也会导致慢速连接下的ping 时间增长(尽管还是会比没有使用inflight 算法低许多)。对于这些情形, 您可能会希望把这个参数减少到15, 10, 或5; 并可能因此而不得不减少`net.inet.tcp.inflight.min` (比如说, 3500) 来得到希望的效果。减少这些参数的值, 只应作为最后不得已时的手段来使用。

注意: 对于4.X 和更早的FreeBSD 版本, `inflight` `sysctl` 变量直接隶属于`net.inet.tcp`。它们的名字是(按字母顺序): `net.inet.tcp.inflight_debug`, `net.inet.tcp.inflight_enable`, `net.inet.tcp.inflight_max`, `net.inet.tcp.inflight_min`。

11.13.3 虚拟内存

11.13.3.1 kern.maxvnodes

`vnode` 是对文件或目录的一种内部表达。因此, 增加可以被操作系统利用的`vnode` 数量将降低磁盘

的I/O。一般而言，这是由操作系统自行完成的，也不需要加以修改。但在某些时候磁盘I/O会成为瓶颈，而系统的vnode不足，则这一配置应被增加。此时需要考虑是非活跃和空闲内存的数量。

要查看当前在用的vnode数量：

```
# sysctl vfs.numvnodes
vfs.numvnodes: 91349
```

要查看最大可用的vnode数量：

```
# sysctl kern.maxvnodes
kern.maxvnodes: 100000
```

如果当前的vnode用量接近最大值，则将kern.maxvnodes值增大1,000可能是个好主意。您应继续查看vfs.numvnodes的数值，如果它再次攀升到接近最大值的程度，仍需继续提高kern.maxvnodes。在top(1)中显示的内存用量应有显著变化，更多内存会处于活跃(active)状态。

11.14 添加交换空间

不管您计划的如何好，有时候系统并不像您所期待的那样运行。如果您发现需要更多的交换空间，添加它很简单。有三种方法增加交换空间：添加一块新的硬盘驱动器、通过NFS使用交换空间和在一个现有的分区上创建一个交换文件。

要了解关于如何加密交换区，相关配置，以及为什么要这样做，请参阅手册的第17.17节。

11.14.1 在新的硬盘驱动器上使用交换空间

这是添加交换空间最好的方法，当然为了达到这个目的需要添加一块硬盘。毕竟您总是可以使用另一块磁盘。如果能这么做，重新阅读一下手册中关于交换空间的第11.2节来了解如何最优地安排交换空间。

11.14.2 通过NFS交换

通过NFS来交换只在您没有本地硬盘交换的时候被建议。在FreeBSD 4.X以前的版本中使用NFS交换速度很慢并且效率低下。4.0-RELEASE和更新的版本中他的速度和效率还是可以接受的。即使使用新版本的FreeBSD，NFS交换也会被可用的网络带宽限制并且增加NFS服务器的负担。

11.14.3 交换文件

您可以创建一个指定大小的文件用来当作交换文件。在我们的例子中我们将会使用叫做/usr/swap0的64MB大小的文件。当然您也可以使用任何您所希望的名字。

例11-1. 在FreeBSD 4.X上创建一个交换文件

1. 确认您的内核配置包含了vnode驱动。它不包含在最近版本的GENERIC。
pseudo-device vn 1 #Vnode driver (turns a file into a device)

2. 创建一个vn-device 设备:

```
# cd /dev
# sh MAKEDEV vn0
```

3. 创建一个交换文件(/usr/swap0):

```
# dd if=/dev/zero of=/usr/swap0 bs=1024k count=64
```

4. 赋予它(/usr/swap0)一个适当的权限:

```
# chmod 0600 /usr/swap0
```

5. 在/etc/rc.conf 中启用交换文件:

```
swapfile="/usr/swap0" # Set to name of swapfile if aux swapfile desired.
```

6. 通过重新启动机器或下面的命令使交换文件立刻生效:

```
# vnconfig -e /dev/vn0b /usr/swap0 swap
```

例11-2. 在FreeBSD 5.X 上创建一个交换文件:

1. 确认您的内核配置包含虚拟磁盘(Memory disk)驱动(md(4))。它在GENERIC 内核中是默认的。

```
device md # Memory "disks"
```

2. 创建一个交换文件(/usr/swap0):

```
# dd if=/dev/zero of=/usr/swap0 bs=1024k count=64
```

3. 赋予它(/usr/swap0)一个适当的权限:

```
# chmod 0600 /usr/swap0
```

4. 在/etc/rc.conf 中启用交换文件:

```
swapfile="/usr/swap0" # Set to name of swapfile if aux swapfile desired.
```

5. 通过重新启动机器或下面的命令使交换文件立刻生效:

```
# mdconfig -a -t vnode -f /usr/swap0 -u 0 && swapon /dev/md0
```

11.15 电源和资源管理

Written by Hiten Pandya 和 Tom Rhodes.

以有效的方式利用硬件资源是非常重要的。在提出ACPI 之前, 管理电源使用和系统散热对操作系统是很困难的。硬件被嵌入的BIOS 接口管理, 例如可插拔BIOS (PNPBIOS)或者高级电源管理(APM) 等等。电源和资源管理是现代操作系统的关键组成部分。例如您可能当系统温度过高的时候让您的操作系统能监视到(并且可能提醒您)。

在FreeBSD 使用手册的这一章节, 我们将提供ACPI 全面的信息。参考资料会在末尾。ACPI 在FreeBSD 5.X 及以下的操作系统中作为一个默认的内核模块被支持。对于FreeBSD 4.9, ACPI 可以通过在内核配置文件中添加device acpica 并且重新编译内核来启用。

11.15.1 什么是ACPI?

高级配置和电源接口(ACPI)是一个业界标准的硬件资源和电源管理接口(因此而得名)。它是**操作系统控制的配置和电源管理(Operating System-directed configuration and Power Management)**,也就是说,它给操作系统(OS)提供了更多的控制和弹性。现代操作系统“延伸”了当前即插即用接口(像是FreeBSD4.X中使用的APM)的限制,在ACPI的介绍之前。ACPI是APM(高级电源管理)的直接继承者。

11.15.2 高级电源管理(APM) 的缺点

高级电源管理(APM)是一种基于系统目前的活动控制其电源使用的机制。APM BIOS 由(系统的) 制造商提供,并且是硬件平台专属的。在OS中的APM驱动作为中介来访问**APM 软件接口**,从而实现对电源使用的管理。

APM有四个主要的问题。首先,电源管理是通过(制造商专属的) BIOS实现的,而OS则完全不了解其细节。例如,用户在APM BIOS中设置了硬盘驱动器的空闲等待数值,当超过这一空闲时间的限制时,它(BIOS)将会减慢硬盘驱动器的速度,而不会征求OS的同意。第二,APM逻辑是嵌入BIOS的,因此它是在OS的控制之外运转的。这意味着用户只能通过通过刷新他们ROM中的APM BIOS才能够解决某些问题;而这是一个很危险的操作,因为它可能使系统进入一个无法恢复的状态。第三,APM是一种制造商专属的技术,也就是说有很多第三方的(重复的工作)以及bugs,如果在一个制造商的BIOS中有,也未必会在其他的产品中解决。最后但绝不是最小的问题,APM BIOS没有为实现复杂的电源策略提供足够的余地,也无法实现能够非常适合具体机器的策略。

即插即用BIOS (PNPBIOS)在很多时候都是不可靠的。PNPBIOS是16-位的技术,因此OS不得不使用16-位模拟才能够与PNPBIOS的方法“接口”。

FreeBSD APM驱动在apm(4)手册页中有描述。

11.15.3 配置ACPI

acpi.ko驱动默认的在启动时通过loader(8)被加载并且**不应该**被编译进内核。原因是这个模块跟系统很容易的工作在一起,比方说不用为了acpi.ko而重新编译内核。这对更简单的测试来说很有利。另一个原因是系统启动后再启动ACPI不是很有用,并且在一些情况下会失败。拿不准的话只要全部禁止ACPI即可。这个驱动不应该而且不能被卸载,因为系统通过它跟各种各样的硬件打交道。ACPI可以通过acpicnf(8)来禁止。实际上通过ACPI的交互可以通过acpicnf(8)来完成。简单的说,如果任何关于ACPI的信息在dmesg(8)的输出中,那么它很可能已经运行了。

注意: ACPI和APM不能共存并且应该份开始用。后来装载的如果注意到另一个在运行将会终止执行。

最简单的表现形式是,ACPI可以通过acpicnf(8)的-s标志和一个1-5的选项来使系统进入休眠状态。5选项将会像下面动作一样让系统软关机:

```
# halt -p
```

其他选项也是可行的。查看acpicnf(8)手册页以获得更多信息。

11.16 使用和调试FreeBSD ACPI

撰写人: Nate Lawson. 协力: Peter Schultz 和Tom Rhodes.

ACPI 是一种全新的发现设备、管理电源使用, 提供过去由BIOS 管理的访问不同硬件的标准化方法。让ACPI 在各种系统上都能正确使用的工作一直在进行, 但许多主板的ACPI 机器语言(AML) 字节代码中的bug, FreeBSD 的内核中资系统设计的不完善, 以及Intel ACPI-CA 解释器中的bug 仍然不时会出现。

这份文档期望能够帮助您协助FreeBSD ACPI 的维护人员来找到您所观察到的问题的根源, 并通过调试找到其解决方法。感谢您阅读这份文档, 我们也希望能够解决您的系统上的问题。

11.16.1 提交调试信息

注意: 在提交问题之前, 请确认您已经在运行最新的BIOS 版本, 此外, 也包括嵌入式控制器的固件版本。

如果您希望提交一个问题, 请确保将下述信息发到 freebsd-acpi@FreeBSD.org (<mailto:freebsd-acpi@FreeBSD.org>):

- 问题行为的描述, 包括系统类型、型号, 以及任何触发问题的相关信息。另外, 请注意尽可能准确地描述这一问题是否对您陌生的。
- 在 “boot -v” 之后得到的dmesg(8) 输出, 以及任何在重现bug 时出现的错误信息。
- 在禁用了ACPI 之后的 “boot -v” 的dmesg(8) 输出, 如果您发现禁用ACPI 能够帮助消除问题。
- 来自sysctl hw.acpi的输出。这也是找到您的系统所提供的功能的一种好办法。
- 能够得到您的ACPI Source Language (ASL) 的URL。不要 把ASL 直接发到邮件列表中, 因为它们可能非常大。为了得到ASL 您可以运行这个命令:

```
# acpidump -t -d > name-system.asl
```

(把name 改为您的登录名, 并把system 改为您的硬件制造商及其型号。例如: njl-FooCo6000.asl)

许多开发者也会订阅FreeBSD-CURRENT 邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-current>) 但还是请发到freebsd-acpi (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-acpi>) 这样它会被更多人看到。请耐心等待, 因为我们都有全职的其他工作。如果您的bug 不是显而易见的, 我们可能会要求您通过send-pr(1) 来提交一个PR。在输入PR 时, 请将同样的信息包含进去。这将帮助我们追踪和解决问题。不要在给freebsd-acpi (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-acpi>) 写信之前发送PR 因为我们把它当作已知文体的备忘录而不是报告机制。您的问题很可能已经被其他人报告过了。

11.16.2 背景

ACPI 存在于采用ia32 (x86)、ia64 (安腾)、以及amd64 (AMD) 架构的所有现代计算机上。完整的标准具有大量的各式功能, 包括CPU 性能管理、电源控制、温度监控、电池系统、嵌入式控制器以及总线枚举。绝大多数系统实现比完整标准的功能要少一些。例如, 桌面系统通常只实现总线枚举部分, 而笔记本则通常支持降温和电源管理功能。笔记本通常还提供休眠和唤醒支持, 并提供与此适应的复杂功能。

符合ACPI的系统中有许多组件。BIOS和芯片组制造商提供一些固定的表(例如, FADT)在存储器中, 以提供类似APIC映射(用于SMP)、配置寄存器、以及简单的配置值等等。另外, 一个字节代码(bytecode)表(系统区别描述表 DSDT)则提供了通过树状命名空间来指定设备及其功能的方法。

ACPI驱动必须要处理固定表, 实现字节码解释器, 并修改驱动程序和内核, 以接受来自ACPI子系统的信息。对于FreeBSD, Intel提供了一个解释器(ACPI-CA), 它在Linux和NetBSD也可以使用。ACPI-CA源代码可以在src/sys/contrib/dev/acpica找到。用于在FreeBSD中允许ACPI-CA正确运转的代码则在src/sys/dev/acpica/Osd。最后, 用于实现ACPI设备的驱动可以在src/sys/dev/acpica找到。

11.16.3 常见问题

要让ACPI正常工作, 它的每一部分都必须工作正常。下面是一些常见的问题, 按照出新的频繁程度排序, 并给出了一些绕过或修正它们的方法。

11.16.3.1 鼠标问题

某些时候, 唤醒操作会导致鼠标不再正常工作。已知的绕过这一问题的方法, 是在/boot/loader.conf文件中添加hint.psm.0.flags="0x3000"设置。如果这样做不能解决问题, 请考虑按前面介绍的方法提交问题报告。

11.16.3.2 休眠/唤醒

ACPI提供了三种休眠到RAM (STR) 的状态, S1-S3, 以及一个休眠到磁盘的状态(STD), 称作S4。S5是“软关机”同时也是系统接好电源但没有开机时的正常状态。S4实际上可以用两种不同的方法来实现。S4BIOS是一种由BIOS辅助的挂起到磁盘方法, 而S4OS则是完全由操作系统实现的。

可以使用sysctl hw.acpi来查看与休眠有关的项目。这里是我的Thinkpad上得到的结果。

```
hw.acpi.supported_sleep_state: S3 S4 S5
hw.acpi.s4bios: 0
```

这表示我可以使acpicnf -s来测试S3, S4OS, 以及S5。如果s4bios是一(1), 则可以使用S4BIOS来代替S4 OS。

当测试休眠/唤醒时, 从S1开始, 如果它被支持的话。这个状态是最可能正常工作的状态, 因为它不需要太多的驱动支持。没有人实现S2但如果您有它的支持, 则应该和S1类似。下一件值得尝试的是S3。这是最深的STR状态, 并需要一系列驱动的支持才能够正常地重新初始化您的硬件。如果您在唤醒系统时遇到问题, 请不要吝惜发邮件给freebsd-acpi (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-acpi>) 邮件列表, 尽管不要指望问题一定会很快解决, 因为有许多驱动程序/硬件需要进行更多的测试和改进。

为了帮助隔离问题, 请在内核中删去尽可能多的驱动。如果这样做能够解决问题, 请尝试逐个加载驱动直到问题再次出现。通常预编译的驱动程序如nvidia.ko、X11显示驱动, 以及USB的问题最多, 而以太网卡的驱动则通常工作的很好。如果您能够通过加载和卸载驱动使系统正常工作, 您可以通过将适当的命令放到/etc/rc.suspend和/etc/rc.resume来将这个过程的自动化。在这两个文件中有一个注释掉的卸载和加载驱动程序的例子供您参考。另外您还可以将hw.acpi.reset_video设置为零(0), 如果您的显示在唤醒之后显得很混乱。此外您还可以尝试更长或更短的hw.acpi.sleep_delay值看看是否有所助益。

另一件值得一试的事情是使用一个比较新的包含ACPI支持的Linux发行版来试试看他们的休眠/唤醒功能是否在同样的硬件上能够正常工作。如果在Linux下正常, 则很可能是FreeBSD驱动程序的问题, 而隔离问题并找到存在问题的驱动有助于解决它。需要注意的是ACPI的维护人员通常并不维护其他驱动(例如声音、ATA, 等等) 因此如果最终发现是驱动的问题最好还是发到freebsd-current

(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-current>) 邮件列表并发给驱动程序的维护者。如果您喜欢冒险, 则可以加一些`printf(3)`到有问题的驱动中, 以找到它的恢复功能发生问题的位置。

最后, 试试看禁用ACPI 并代之以启用APM。如果休眠/唤醒能够在APM 下正常工作, 使用APM 可能会更好, 特别是对于较老的硬件(2000年以前)。硬件制造商需要一些时间来让老硬件的ACPI 工作正常, 而ACPI 的问题十之八九是BIOS 中的毛病引发的。

11.16.3.3 系统停止响应(暂时或永久性地)

绝大多数系统停止响应是由于未能及时响应中断或发生了中断风暴导致的。芯片组有很多问题最终会溯源到BIOS 如何在引导系统之前配置中断, APIC (MADT) 表的正确性, 以及系统控制中断(SCI) 如何路由。

通过察看`vmstat -i`的输出中包括`acpi0`的那一行可以区分中断风暴和未能及时响应中断。如果每秒计数器增长的速度多于一两个, 则您是遇到了中断风暴。如果系统停止了响应, 您可以尝试停止内核并进入DDB (在控制台上按`CTRL+ALT+ESC`) 并输入`show interrupts`。

处理中断问题的救命稻草是尝试禁用APIC 支持, 这是通过在`loader.conf` 中加入`hint.apic.0.disabled="1"` 完成的。

11.16.3.4 崩溃

崩溃对于ACPI 是比较罕见的情况, 如果发现, 将会非常重视并很快修复。您要做的第一件事是设法隔离出能够重现崩溃(如果可能的话) 的操作并获取一份调用堆栈。请启用`options DDB` 并设置串行控制台(参见第22.6.5.3 节) 或配置一个`dump(8)` 分区。您将在DDB 中通过`tr` 得到调用堆栈。如果您只能用手抄的方法记录它, 一定要记下头五(5) 行和最后五(5) 行。

然后, 尝试通过在启动时禁用ACPI 来隔离故障。如果这样做能够正常工作, 请通过设置`debug.acpi.disable` 的那组数值来隔离具体是哪个ACPI 子系统的问题。请参见`acpi(4)` 联机手册中给出的那些例子。

11.16.3.5 系统在休眠或关机之后又启动了

首先请尝试在`loader.conf(5)` 中设置`hw.acpi.disable_on_poweroff= "0"`。这将让ACPI 不再在关机过程中禁用一些事件。基于同样的原因, 一些系统需要把这个值设置为“1” (这是默认值)。这通常能够修复在休眠或关机时立即再次启动的问题。

11.16.3.6 其他问题

如果您有ACPI 的其他问题(同docking station 协同工作、无法检测设备, 等等), 请把描述发给邮件列表; 不过, 这些问题也有可能和ACPI 中尚未完成的部分有关, 它们可能需要时间才能被实现。请保持耐心, 并准备测试我们可能会发给您的补丁。

11.16.4 ASL、acpidump, 以及IASL

最常见的问题是BIOS 制造商提供的不正确(甚至完全错误的!) 字节代码。这通常会以类似下面这样的内核消息显示在控制台上:


```
ACPI-1287: *** Error: Method execution failed [\\_SB_.PCI0.LPC0.FIGD._STA] \\
(Node 0xc3f6d160), AE_NOT_FOUND
```

许多时候，您可以通过将BIOS升级到最新版本来解决此类问题。绝大多数控制台消息是无害的，但如果您有其他问题例如电池工作不正常，则从AML开始查找问题将是一条捷径。字节代码，或常说的AML，是从一种叫做ASL的语言写成的源代码进行编译得到的结果。AML一般存放在DSDT表中。要得到您系统的ASL，需要使用acpidump(8)。需要同时指定-t(显示固定标的内容)和-d(将AML反编译成ASL)两个选项。请参见如何提交调试信息一节了解如何使用它。

最方便的初步检查是尝试重新编译ASL来看看是否有错误。通常可以忽略这一过程中产生的警告，但错误一般就都是bug，它们通常就是导致ACPI无法正常工作的原因。要重新编译您的ASL，可以使用下面的命令：

```
# iasl your.asl
```

11.16.5 修复ASL

我们的长期目标是让每一个人都能够在不需要任何用户干预的情况下使用ACPI。然而，目前我们仍然在开发绕过BIOS制造商常见错误的方法。Microsoft解释器(acpi.sys和acpiec.sys)并不会严格地检查是否遵守了标准，因此许多只在Windows中测试ACPI的BIOS制造商很可能永远不会修正他们的ASL。我们希望不断地找出并用文档说明Microsoft的解释器到底允许那些不标准的行为，并在FreeBSD进行对应的修改使它能够正常工作而不需要用户修正ASL。作为一项临时缓解问题的方法，并帮助我们确认其行为，您可以手工修正ASL。如果这样能够解决问题，请把新旧ASL的diff(1)发给我们，这样我们就有可能绕过ACPI-CA中的错误行为，从而不再需要您来手工修正。

下面是一些常见的错误信息，它们的原因，以及如何修正。

11.16.5.1 _OS dependencies (_OS 依赖)

某些AML假定世界是由不同版本的Windows组成的。您可以让FreeBSD声称自己是任意OS来看一看是否能够修正问题。比较简单的办法是设置hw.acpi.osname="Windows 2001"到/boot/loader.conf中，或使用您在ASL中找到的其他字符串。

11.16.5.2 Missing Return statements (缺少返回语句)

一些方法可能没按照标准要求的那样显式地返回值。尽管ACPI-CA无法处理它，但FreeBSD提供了一个绕过它并允许其暗含地返回值的方法。您也可以增加一个显式的Return语句，如果您知道那里需要返回一个值的话。要强制iasl编译ASL，需要使用-f标志。

11.16.5.3 替换默认的AML

在定制your.asl之后，您可以通过下面的命令编译它：

```
# iasl your.asl
```

可以使用-f标志来强制创建AML，即使在编译过程中发生了错误。请注意某些错误(例如，缺少Return语句)会自动被解释器忽略掉。

DSDT.aml 是 `iasl` 命令的默认输出文件名。可以加载它来取代您 BIOS 中存在问题的副本(它仍然存在于闪存中), 其方法是按下面的说明编辑 `/boot/loader.conf`:

```
acpi_dsdt_load="YES"
acpi_dsdt_name="/boot/DSDT.aml"
```

一定要把您的 `DSDT.aml` 复制到 `/boot` 目录中。

11.16.6 从ACPI 中获取调试输出信息

ACPI 驱动程序提供了非常灵活的调试机制。这允许您指定一组子系统, 以及所需要的详细信息。需要调试的子系统可以按“layers(层)”来指定, 并分为ACPI-CA 组件(`ACPI_ALL_COMPONENTS`)和ACPI 硬件支持(`ACPI_ALL_DRIVERS`)。调试输出的详细程度可以通过“level(详细度)”来指定, 其范围是 `ACPI_LV_ERROR` (只报告错误)到 `ACPI_LV_VERBOSE` (显示所有)。“level”是一个位掩码因此可以一次设置多个选项, 中间用空格分开。实际使用中您应该考虑使用串行控制台来记录输出, 如果它太长以至于冲掉了控制台消息缓冲的话。不同的层和输出详细度的完整列表可以在 `acpi(4)` 联机手册中找到。

调试输出默认并不开启。要起用它, 您需要在内核设置中添加 `options ACPI_DEBUG`, 如果您的内核中编入了ACPI 的话。您还可以在 `/etc/make.conf` 中加入 `ACPI_DEBUG=1` 来在全局起用它。如果它只是模块, 您可以用下面的方法来重新编译 `acpi.ko`:

```
# cd /sys/modules/acpi/acpi
&& make clean &&
make ACPI_DEBUG=1
```

安装 `acpi.ko` 到 `/boot/kernel` 并添加 `your` 并把所需的详细度和层在 `loader.conf` 中指定。这个例子将启用所有ACPI-CA 组件以及所有ACPI 硬件驱动(CPU、LID, 等等)的消息。只输出错误信息, 也就是最低的详细度。

```
debug.acpi.layer="ACPI_ALL_COMPONENTS ACPI_ALL_DRIVERS"
debug.acpi.level="ACPI_LV_ERROR"
```

如果您需要的信息是由某个特定的事件触发的(比如说, 休眠之后的唤醒), 您可以不修改 `loader.conf` 而转而使用 `sysctl` 来在启动和为那个事件准备系统之后再指定层和详细度。这些 `sysctl` 的名字和 `loader.conf` 中的一致。

11.16.7 参考文献

关于ACPI 的更多信息可以从下面这些地方找到:

- The FreeBSD ACPI 邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-acpi>)
- ACPI 邮件列表存档 <http://lists.freebsd.org/pipermail/freebsd-acpi/>
- 旧的ACPI 邮件列表存档 <http://home.jp.FreeBSD.org/mail-list/acpi-jp/>
- The ACPI 2.0 标准 <http://acpi.info/spec.htm>
- FreeBSD 手册页: `acpi(4)`, `acpi_thermal(4)`, `acpidump(8)`, `iasl(8)`, `acpidb(8)`

- DSDT 调试资源 (http://www.cpqlinux.com/acpi-howto.html#fix_broken_dsdt). (使用Compaq 作为例子但通常情况下都很有用。)

备注

1. 自动调整算法会将`maxusers` 设置为与主存的数量一样，或者取其下限32 或上限384。

第12章

FreeBSD 引导过程

12.1 概述

启动电脑以及加载操作系统的过程被称为“引导过程”，或者简称为“引导”。FreeBSD 的引导过程给用户自定义启动提供了很大的伸缩性，您可以选择启动不同的操作系统，或者是同一系统的不同版本及内核。

本章将详细介绍您能在FreeBSD 引导过程中设置的配置选项。这包括了引导内核、探测设备并启动init(8) 等等之前所发生的所有事情。这些事项一般发生在文本由白变灰时。

读完这章您将会知道：

- FreeBSD 引导系统里的各项组件，以及它们之间的交互方式。
- 在FreeBSD 引导时给各组件配置选项以控制引导过程。
- device.hints(5)的基本知识。

只适用于x86: 本章只描述了运行于Intel x86 体系之上的FreeBSD 的引导过程。

12.2 引导问题

启动电脑及启动和引导操作系统构成了一个有趣的两难境地。按照定义在操作系统被启动之前计算机是无法完成任何任务的，包括运行磁盘上的程序。如果计算机在没有操作系统的情况下不能运行来自于磁盘上的程序而操作系统又是放在磁盘上的，那操作系统是如何启动的呢？

在*Munchausen男爵历险记(The Adventures of Baron Munchausen)* 这本书中有一个和这个过程类似的故事，一个人掉到了下水管道里，然后靠着拉自己的靴襻(bootstrap) 克服重重困难爬了出来。在早期文献中，多以术语*bootstrap* 来指代操作系统的加载机制，如今它逐渐被简写为“booting”。

在x86 硬件体系中，基本输入/输出系统(BIOS) 负责加载操作系统，为了做到这一点，BIOS 在磁盘上寻找主引导记录(MBR)，而MBR 必须在放置的磁盘的特定位置。BIOS 有足够的能力来读入和运行MBR，且假使地认为MBR 能完成加载操作系统的剩余任务，MBR可能需要BIOS的帮助。

在MBR中的代码通常被提为**引导管理器**，尤其是与用户交互的那类。这一类引导器通常有更多代码位于磁盘第一**轨道**或在操作系统的文件系统中。(引导管理器有时也被称为**boot loader**，但是FreeBSD对后面的引导阶段才使用这个术语。) 流行的引导管理器包括**boot0**(亦称**Boot Easy**，标准的FreeBSD 引导管理器)、**Grub**、**GAG**，以及**LILO**。(只有**boot0**能装得进MBR。)

如果您只安装了一个操作系统，那么一个标准的MBR 就足够了。这个MBR 先在磁盘上搜索可引导的(亦称“活动的”)分区，然后运行分区上的代码以加载操作系统的其它部分。MBR由fdisk(8)安装，是一个缺省的MBR。相关文件为/boot/mbr。

如果您在磁盘上安装了多个操作系统那么您可以安装一个不同的引导管理器，它能显示一张操作系统的列表，您能从中选择启动哪个。这样的两种引导器将在下一小节中讨论。

启动系统的剩余部分被分为三个阶段。第一阶段由MBR执行,它只是使计算机进入特定的状态然后执行第二阶段。第二阶段稍微干得多一些。第三阶段完成加载操作系统的任务。工作被分为三个阶段是因为PC标准对第一第二阶段执行的程序的大小有所限制。把这些任务连在一起使得FreeBSD可以提供更大伸缩性的加载器(loader)。

然后内核启动,它开始探测设备并初始化它们。一旦内核引导进程完成任务,内核将控制权交给用户进程init(8),它确认磁盘是否处于可用状态。init(8)然后开始用户级资源配置:加载文件系统启动网卡,及粗略地启动所有FreeBSD系统加载时经常运行的进程。

12.3 引导管理器和各引导阶段

12.3.1 The Boot Manager

在MBR或引导管理器中的代码有时被提为引导过程的**阶段0**。这一小节前面提到引导器中的两种: **boot0**和**LILO**。

boot0引导管理器: 由FreeBSD的安装程序以及boot0cfg(8)所安装的MBR,默认基于/boot/boot0。(程序boot0非常简单,由于在MBR中的程序只能有446字节长,分区表和MBR末端的0x55AA标识也要挤占一些空间。)如果你已经安装boot0并且有多个操作系统在你的硬盘上,那么如果你安装了FreeBSD MBR而且安装了多个操作系统,则会在系统启动时看到类似下面的提示:

例12-1. boot0 截屏

```
F1 DOS
F2 FreeBSD
F3 Linux
F4 ??
F5 Drive 1
```

Default: F2

目前已经知道一些其它操作系统,特别是Windows,会以自己的MBR覆盖现有MBR。如果发生了这种事情,或者您想用FreeBSD的MBR覆盖现有的MBR,您可以使用以下的命令:

```
# fdisk -B -b /boot/boot0 device
```

device 是要写入MBR的设备名,比如ad0代表第一个IDE磁盘,ad2代表第二个IDE控制器上的第一个IDE磁盘,da0代表第一个SCSI磁盘,等等。抑或,如果你需要一个自行配置的MBR,请使用boot0cfg(8)。

The LILO Boot Manager: 要想安装这个引导管理器并也用来引导FreeBSD,首先启动Linux,并将以下选项加入到已有的配置文件/etc/lilo.conf:

```
other=/dev/hdXY
table=/dev/hdX
loader=/boot/chain.b
label=FreeBSD
```

在上面的内容里,使用Linux的标示符指定了FreeBSD的主分区和驱动器,将X替换为Linux驱动器字母,将Y替换为Linux主分区号。如果您使用的是SCSI驱动器,您需要将/dev/hd改成/dev/sd,这里再次

使用了`xy`的语法。如果您安装的两个系统在同一驱动器上，`loader=/boot/chain.b`选项可以去掉。现在您可以执行`/sbin/lilo -v`使修改生效；应检查屏幕上的消息确认修改。

12.3.2 第一阶段，`/boot/boot1`，和第二阶段，`/boot/boot2`

概念上，第一，第二阶段同属于一个程序，处于磁盘的相同区域。但由于空间限制，它们被分为两部分。可是您总是会一起安装它们。它们由安装器或**`disklabel`**(见下文)复制自被组合而成的`/boot/boot`。

它们位于文件系统外，引导分区的第一轨道，从第一扇区开始。在这里`boot0`，或者任何其它引导管理器，期望找到一个程序运行，继续引导进程。所使用的扇区数可由`/boot/boot`的大小确定。

`boot1`非常简单，因为它再多也只能有512字节，只能识别储存着分区信息的**`disklabel`**，及寻找执行**`boot2`**。

`boot2`稍微有点加强，能够理解FreeBSD的文件系统以便于寻找里面的文件，能提供选择内核和加载器的简单界面。

因为**`loader`**有着更强的功能，提供了一套易于使用的引导配置，`boot2`一般都执行**`loader`**，但以前它的任务是直接运行内核。

例12-2. `boot2` 的屏幕输出

```
>> FreeBSD/i386 B00T
Default: 0:ad(0,a)/boot/loader
boot:
```

如果您要更改已安装的**`boot1`**和**`boot2`**，请使用命令**`disklabel(8)`**。

```
# disklabel -B diskslice
```

`diskslice`是用于引导的磁盘和分区，比如**`ad0s1`**代表第一个IDE磁盘上的第一个分区。

dangerously dedicated: 如果您在**`disklabel(8)`**命令中只使用了磁盘名，比如**`ad0`**，就会破坏磁盘上的所有分区。这当然不是您所希望的，所以在按下**回车**之前一定要对命令进行多次确认。

12.3.3 第三阶段，`/boot/loader`

加载器(**`loader`**)是三个阶段中的最后阶段，且是放置在文件系统之中的，一般是文件**`/boot/loader`**。

`loader`被作为一种友好的配置方式，使用了一组内建且易用的命令集。这些命令由一个强大的多的解释器支持构建，其本身带有复杂得多的命令集。

12.3.3.1 **`Loader`** 程序流程

初始时，**`loader`**会探测控制台和磁盘，识别是从哪块盘引导的。它会根据这些信息设置变量，启动解释器以接受通过脚本或交互方式传来的用户命令。

`loader`然后会读取并运行**`/boot/loader.rc`**，默认地读取**`/boot/defaults/loader.conf`**以设置可靠的默认变量，读取**`/boot/loader.conf`**对这些变量作本地修改。**`loader.rc`**依据这些变量进行动作，加载任何被选择的模块和内核。

最后，默认地，`loader` 会停留10秒等待按键，若没有发生中断，就开始引导内核。如果被中断，用户会得到一个命令行提示符，在这里用户得更改变量、卸载所有模块、加载模块、最后引导或重新引导。

12.3.3.2 Loader 内建的命令

这些是最常用的`loader`命令。对所有可用命令的解释请参见`loader(8)`。

`autobootseconds`

在给定的时间内如果没有中断发生就引导内核。它显示一个倒数计时，默认的时间范围是10秒。

`boot [-options] [kernelname]`

立即按照给定的选项(如果有的话)和内核名(如果是内核的)引导内核。

`boot-conf`

基于变量对各种模块进行自动配置(和引导内核时发生的一样)。您只须记住要先使用`unload`命令，然后修改一些变量，比如`kernel`。

`help [topic]`

显示从文件`/boot/loader.help`读取的帮助信息。如果给定的主题是`index`，那么列出来的是所有可用的主题。

`include filename ...`

通过给定的文件名处理文件。文件被读入，然后被一行一行地解释。任何错误都会立即中止`include`命令。

`load [-t type] filename`

加载内核、内核模块，或者是给定类型的文件(通过给定的文件名)。任何在文件名后面的参数都会被传给文件。

`ls [-l] [path]`

显示给定路径或者是根目录(如果路径没有指定)下面的文件列表。如果指定了`-l`选项，文件大小也会显示。

`lsdev [-v]`

列出所有可以加载模块的设备。如果指定了`-v`选项，会显示出更多的细节。

`lsmod [-v]`

显示已被加载的模块。如果指明了`-v`选项，会显示更多的细节。

`more filename`

显示指定的文件，每隔`LINES`停顿一次。

`reboot`

立即重启系统。

```
set variable
set variable=value
```

设置loader的环境变量。

```
unload
```

移除所有已被加载的模块。

12.3.3.3 Loader 示例

这里有一些实际中loader用法的示例

- 只是简单的引导默认内核，不同的是进入单用户模式：

```
boot -s
```

- 卸载默认内核和模块，然后加载旧的(或者其它)的内核：

```
unload
load kernel.old
```

您可以使用被称为通用内核的kernel.GENERIC，或者您以前安装的内核kernel.old(当您升级或配置了您自己的内核等时候)。

注意：使用以下命令加载常用的模块和另一个内核：

```
unload
set kernel="kernel.old"
boot-conf
```

- 加载内核配置脚本：

```
load -t userconfig_script /boot/kernel.conf
```

12.4 内核在引导时的交互

一旦内核被loader (一般情况下) 或者boot2 (越过loader) 加载，它将检查引导标志，如果有的话，就会进行必要的动作调整。

12.4.1 内核引导标志

这里是一些常用的引导标志：

```
-a
```

在内核初始化时，询问作为根加载的设备。

```
-C
```

从CDROM 引导。

-C

运行UserConfig (引导时的内核配置器)

-S

引导进入单用户模式

-V

在内核引导过程中显示更多的信息

注意: 还有更多的引导标志, 阅读boot(8) 以获取有关它们的信息。

12.5 Device Hints

Contributed by Tom Rhodes.

注意: 这是FreeBSD 5.0 及其以后版本的组件, 不存在于早前的版本中。

在初始化系统启动时, loader(8) 会读取device.hints(5) 文件。这个文件以变量的形式储存着内核引导信息, 有时被称为“device hints”。设备驱动程序用“device hints”对设备进行配置。

Device hints 也可以在 第三阶段的boot loader 的命令行提示符中指定。变量可以用set 命令添加, unset 命令删除, show 命令查看。在文件/boot/device.hints 设置的变量亦可以在这里被覆盖。键入boot loader 中的变量不是永久性的, 在下次启动时就会被忘记。

一旦系统引导成功, kenv(1) 命令可以用来清楚所有的变量。

文件/boot/device.hints 的语法是一行一个变量, 使用“#”作为注释标记。每行是按照如下方式组织的:

```
hint.driver.unit.keyword="value"
```

第三阶段boot loader 的语法是:

```
set hint.driver.unit.keyword=value
```

driver 是设备驱动程序名, unit 是设备驱动程序单位名, keyword 是hint 关键字。关键字可以由以下选项组成:

- at: 指明设备所绑定的总线
- port: 指明所使用I/O 的起始地址。
- irq: 指明所使用的中断请求号。
- drq: 指明DMA channel 号。
- maddr: 指明设备占用的物理内存地址。

- **flags**: 给设备设置各种标志位。
- **disabled**: 如果设成1, 设备被禁用。

设备驱动程序能够接受更多的**hints**, 推荐您参看它们的联机手册。参看**device.hints(5)**、**kenv(1)**、**loader.conf(5)**和**loader(8)** 联机手册以获取更多的信息。

12.6 Init: 进程控制及初始化

一旦内核完成引导, 它就把控制权交给了用户进程**init(8)**, 它放置在**/sbin/init**, 或者**init_path** 变量指定的程序路径中。这个变量是在**loader** 里面设置的。

12.6.1 自动重启队列

自动重启队列保证了可用的文件系统是稳定的。如果不是, 且**fsck(8)** 不能修复这些错误, **init(8)** 会进入单用户模式 以便系统管理员直接解决问题。

12.6.2 单用户模式

此模式可以通过 自动重启队列或者通过带有**-s** 选项的用户引导或通过在**loader** 里设置**boot_single** 变量等多种方式来达到。

也可以在多用户模式下调动无**reboot(-r)**选项和**halt(-h)** 选项的**shutdown(8)** 命令来进入单用户模式。

如果系统控制台 在文件**/etc/ttys** 中被设置为不安全(**insecure**), 在初始化单用户模式前会出现要求输入**root** 密码的命令行提示符。

例12-3. 在**/etc/ttys** 文件中的不安全控制台

```
# name  getty                                type    status      comments
#
# If console is marked "insecure", then init will ask for the root password # when going to single
console none                                unknown off insecure
```

注意: 把控制台设置成不安全(**insecure**) 使只知道**root** 密码的人才能进入单用户模式, 因为您认为控制台在物理上是不安全的。因此如果您考虑到安全性, 请选择不安全(**insecure**), 而非安全(**secure**)。

12.6.3 多用户模式

如果**init(8)** 发现您的文件系统一切正常, 又或者用户在单用户模式完成了工作, 系统就会进入多用户模式, 开始系统的资源配置。

12.6.3.1 资源配置(rc)

资源配置分别从文件**/etc/defaults/rc.conf**、**/etc/rc.conf** 中读取默认配置和细节配置, 然后加载在文件**/etc/fstab** 中提及的文件系统、启动网络服务、启动各种系统守护进程, 最后启动本地安装包的启动脚本。

rc(8) 联机手册是关于资源配置的很好的参考。

12.7 shutdown 队列

由命令shutdown(8)的控制，init(8)会试着运行/etc/rc.shutdown脚本，给所有进程发送TERM信号，然后给不按时停止的进程发送KILL信号。

在支持电源管理的体系上关闭FreeBSD系统的电源，只要简单的使用命令shutdown -p now立即关闭电源。使用命令shutdown -r now重启FreeBSD。要执行shutdown(8)您必须是root用户或operator组的成员。也可以使用halt(8)和reboot(8)命令来关闭系统，请参看它们的联机手册以获得更多的信息。

注意：电源管理需要支持，在FreeBSD 5.X中要求内核支持acpi(4)或以模块加载，在FreeBSD 4.X中需要apm(4)的支持。

第13章

用户和基本的帐户管理

Contributed by Neil Blakey-Milner.

13.1 概述

FreeBSD允许多个用户同时使用计算机. 当然,这些用户中不是很多人同时坐在同一台计算机前.¹,而是其他用户可以通过网络来使用同一台计算机以完成他们的工作.要使用系统,每个人都应该有一个帐户.

读完这章,您将了解到:

- 在一个FreeBSD系统上不同用户帐户之间的区别.
- 如何添加用户帐户.
- 如何删除用户帐户.
- 如何改变帐户细节,如用户的全名,或首选的shell.
- 如何在每个帐户基础上设置限制,来控制像内存, CPU时钟这样的资源.
- 如何使用组来使帐户管理更容易.

在阅读这章之前,您应当了解:

- 了解UNIX和FreeBSD的基础知识(第3章).

13.2 介绍

所有访问系统的用户都是通过帐户完成的,所以用户和帐户管理是FreeBSD系统不可或缺的重要部分.

每个FreeBSD系统的帐户都有一些和它相对应的信息去验证它.

用户名

用户名在login: 提示符的后面键入. 用户名对于一台计算机来讲是唯一的; 您不可以使用两个相同的用户名来登录. 有很多用来创建正确用户名的规则, 具体请参考passwd(5); 您使用的用户名通常需要8个或更少的小写字母.

口令

每个帐户都有一个口令与它对应. 口令可以是空的, 这样不需要口令就可以访问系统. 这通常不是一个好主意; 每个帐户都应该有口令.

用户ID (UID)

UID是系统用来识别用户的数字, 传统上它的范围是0到65536之间², 用以唯一地标识用户. FreeBSD在内部使用UID来识别用户——在工作以前. 任何允许您指定一个用户名的FreeBSD 命令都会把它转换成UID. 这意味着您可以用不同的用户名使用多个帐户, 但它们的UID是一样的. FreeBSD 会把这些帐户认定是同一个用户.

组ID (GID)

GID是用来识别用户所在的组的，传统上范围在0到65536之间²的数字。组是一种基于用户GID而不是它们的UID的用来控制用户访问资源的机制。这可以减少一些配置文件的大小。一个用户也可以属于多个组。

登录类

登录类是对组机制的扩展,当把系统分配给不同用户时,它提供了额外的灵活性.

口令的定期更改

默认情况下, **FreeBSD** 并不强制用户去改变他们的口令。您可以以用户为单位强制要求一些或所有的用户定期改变他们的口令。

帐户的到期时间

默认情况下**FreeBSD** 不会自动完成帐户过期操作。如果您正在创建帐户, 您应该知道一个帐户的有效使用期限。例如, 在学校里您会为每个学生建立一个帐户, 您可以指定它们何时过期。帐户过期后, 虽然帐户的目录和文件仍然存在, 但帐户已经不能继续使用了。

用户的全名

用户名可以唯一地识别**FreeBSD**的帐户, 但它不会反映用户的全名。这些信息可能与帐户是相关的。

主目录

主目录是用户用来启动的目录的完全路径。一个通常的规则是把所有用户的主目录都放在 `/home/username` 下, 或者 `/usr/home/username` 下。用户将把他们的个人文件放在自己的主目录下, 他们可以在那里创建任何目录。

用户shell

Shell提供了用户用来操作系统的默认环境。有很多不同的shell, 有经验的用户会根据他们的经验来选择自己喜好的shell。

有三种类型的帐户: 超级用户, 系统用户, 以及普通用户。超级用户帐户通常叫做**root**, 可以没有限制地管理系统。系统用户运行服务。最后, 普通用户给那些登录系统以及阅读邮件的人使用。

13.3 超级用户帐户

超级用户帐户, 通常叫做**root**, 可以重新配置和管理系统, 在收发邮件, 系统检查或编程这样的日常工作中, 尽量不要使用**root**权限。

这是因为不象普通用户帐户, 超级用户能够无限制地操作系统, 超级用户帐户的滥用可能会引起无法想象的灾难。普通的用户帐户不会由于出错而破坏系统, 所以要尽可能的使用普通帐户, 除非您需要额外的特权。

在使用超级用户命令时要再三检查, 因为一个额外的空格或缺少某个字符的命令都可能会引起数据丢失。

所以, 在阅读完这章后您第一件要做的事就是, 在平时使用的时候, 创建一个没有特权的用户帐户。无论您使用的是单用户还是多用户系统这样的申请都是相同的。在这章的后面, 我们将讨论如何创建一个额外的帐户和如何在普通用户和超级用户之间进行切换。

13.4 系统帐户

系统用户是那些要使用诸如DNS、邮件、web等服务的用户。使用帐户的原因就是安全；如果所有的用户都由超级用户来运行，那它们就可以不受约束地做任何事情。

典型的系统帐户包括daemon、operator、bind (供域名服务使用)、news，以及www。

nobody 是普通的没有特权的系统用户。然而，大多数与用户联系很密切的服务是使用nobody的，记的这点非常重要，这样可能使用户变的非常有特权。

13.5 用户帐户

用户帐户是让真实的用户访问系统的主要方式，这些帐户把用户和环境隔离，能阻止用户损坏系统和其他用户，在不影响其他用户的情况之下定制自己的环境。

任何人访问您的系统必须要有他们自己唯一的帐户。这可以让您找到谁做了什么事，并且阻止人们破坏其他用户的设置和阅读其他人的邮件等等。

每个用户能够设置他们自己的环境，以利于他们通过改变shell，编辑器，键盘绑定和语言等适应并且更好的使用这个系统。

13.6 修改帐户

在UNIX 的处理用户帐户的环境中有很多不同的命令可用. 最普通的命令如下，接下来是详细使用它们的例子。

命令	摘要
adduser(8)	在命令行添加新用户.
rmuser(8)	在命令行删除用户.
chpass(1)	一个灵活的用于修改用户数据库信息的工具.
passwd(1)	一个用于修改用户口令的简单的命令行工具.
pw(8)	一个强大灵活修改用户帐户的工具.

13.6.1 添加用户

adduser(8) 是一个简单的添加新用户的命令. 它为用户创建passwd 和group 文件。它也为新用户创建一个主目录，它拷贝一个默认的配置文件(“dotfiles”)从/usr/share/skel 这个目录，然后给新用户发送一封带欢迎信息的邮件。

在FreeBSD 5.0版本，adduser(8)命令从Perl脚本改写为shell脚本，起包装pw(8)的作用，所以它的用法在FreeBSD 4.X 上和FreeBSD 5.X 上略有不同。

建立初始化配置文件, 使用adduser -s -config_create.³ 接下来，我们配置adduser(8) 的默认设置，并建立第一个普通用户帐户，因为将root 用于日常使用会带来很多潜在问题。

例13-1. 配置adduser 和添加一个新用户，在FreeBSD 4.X版本

```
# adduser -v Use option "--silent" if you don't want to see all warnings and questions.
Check /etc/shells
```

```

Check /etc/master.passwd
Check /etc/group
Enter your default shell: csh date no sh tcsh zsh [sh]: zsh Your default shell is: zsh -> /usr/lo
Copy dotfiles from: /usr/share/skel no [/usr/share/skel]:
Send message from file: /etc/adduser.message no
[/etc/adduser.message]: no Do not send message Use passwords (y/n) [y]: y

Write your changes to /etc/adduser.conf? (y/n) [n]: y

Ok, let's go.
Don't worry about mistakes. I will give you the chance later to correct any input.
Enter username [a-z0-9_-]: jru Enter full name []: J. Random User Enter shell csh date no sh tcsh z
Enter home directory (full path) [/home/jru]:
Uid [1001]:
Enter login class: default []:
Login group jru [jru]:
Login group is "jru". Invite jru into other groups: guest no
[no]: wheel
Enter password []:
Enter password again []:

Name:   jru
Password: ****
Fullname: J. Random User
Uid:    1001
Gid:    1001 (jru)
Class:
Groups:  jru wheel
HOME:    /home/jru
Shell:   /usr/local/bin/zsh
OK? (y/n) [y]: y
Added user "jru"
Copy files from /usr/share/skel to /home/jru Add another user? (y/n) [y]: n Goodbye!
#

```

总体而言，我们把默认的shell设置成**zsh**（一个可以在Ports Collection找到的shell），关闭欢迎邮件。然后保存配置，接着创建一个名为**jru**的帐户，并且确信**jru**在**wheel**组里（这样它就能够通过**su(1)**转变为**root**。）

注意：输入的口令不会被回显，也不会显示星号。请确保不要误输口令。

注意：从现在起，使用**adduser(8)**不再需要改变默认设置。如果您要求改变默认设置，先退出程序，然后使用**-s**选项。

例13-2. 添加一个新用户在FreeBSD 5.X版本

```
# adduser
Username: jru
Full name: J. Random User Uid (Leave empty for default):
Login group [jru]:
Login group is jru. Invite jru into other groups? []: wheel Login class [default]:
Shell (sh csh tcsh zsh nologin) [sh]: zsh Home directory [/home/jru]:
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username   : jru
Password   : ****
Full Name  : J. Random User
Uid        : 1001
Class      :
Groups     : jru wheel
Home       : /home/jru
Shell      : /usr/local/bin/zsh
Locked     : no
OK? (yes/no): yes
adduser: INFO: Successfully added (jru) to the user database.
Add another user? (yes/no): no Goodbye!
#
```

13.6.2 删除用户

您可以使用`rmuser(8)`从系统中完全删除一个用户。`rmuser(8)`执行如下步骤:

1. 删除用户的`crontab(1)`记录(如果有的话).
2. 删除属于用户的`at(1)`工作.
3. 杀掉属于用户的所有进程.
4. 删除本地口令文件中的用户.
5. 删除用户的主目录(如果他有自己的主目录).
6. 删除来自`/var/mail`属于用户的邮件.
7. 删除所有诸如`/tmp`的临时文件存储区中的文件.
8. 最后, 删除`/etc/group`中所有属于组的该用户名.

注意: 如果一个组变成空, 而组名和用户名一样, 组将被删除. `adduser(8)`命令建立每个用户唯一的组.

`rmuser(8)`不能用来删除超级用户的帐户, 因为那样做是对系统极大的破坏.

默认情况下, 使用交互模式, 这样能够让您清楚的知道您在做什么.

例13-3. 删除用户 交互模式下的帐户删除

```
# rmuser jru Matching password entry:
jru:*:1001:1001::0:0:J. Random User:/home/jru:/usr/local/bin/zsh Is this the entry you wish to re
Updating group file: trusted (removing group jru -- personal group is empty) done.
Removing user's incoming mail file /var/mail/jru: done.
Removing files belonging to jru from /tmp: done.
Removing files belonging to jru from /var/tmp: done.
Removing files belonging to jru from /var/tmp/vi.recover: done.
#
```

13.6.3 chpass

chpass(1) 可以改变用户的口令, shells, 和包括个人信息在内的数据库信息.

只有系统管理员, 即超级用户, 才可以用chpass(1) 改变其他用户口令和信息。

除了可选择的用户名, 不需要任何选项, chpass(1) 将显示一个包含用户信息的编辑器. 可以试图改变用户在数据库中的信息.

注意: 在FreeBSD 5.X版本, 编辑退出后,您应该索要您的口令,如果您不是超级用户的话.

例13-4. 以超级用户交互执行chpass 命令

```
#Changing user database information for jru.
Login: jru
Password: *
Uid [#]: 1001
Gid [# or name]: 1001
Change [month day year]:
Expire [month day year]:
Class:
Home directory: /home/jru
Shell: /usr/local/bin/zsh
Full Name: J. Random User
Office Location:
Office Phone:
Home Phone:
Other information:
```

普通用户只能改变他们自己很少的一部分信息.

例13-5. 以普通用户交互执行chpass 命令

```
#Changing user database information for jru.
Shell: /usr/local/bin/zsh
Full Name: J. Random User
Office Location:
Office Phone:
Home Phone:
Other information:
```

注意: chfn(1) 和chsh(1) 只是到chpass(1) 的符号连接。类似地, ypchpass(1), ypchfn(1) 以及ypchsh(1) 也是这样。NIS 是自动支持的, 不一定要在命令前指定yp。如果这让您有点不太明白, 不必担心, NIS 将在第25 章 介绍。

13.6.4 passwd命令

passwd(1) 是改变您自己作为一个普通用户口令或者作为超级用户口令常用的方法。

注意: 用户改变口令前必须键入原来的口令, 防止用户离开终端时非授权的用户进入改变合法用户的口令。

例13-6. 改变您的口令

```
% passwd Changing local password for jru.
Old password:
New password:
Retype new password:
passwd: updating the database...
passwd: done
```

例13-7. 改变其他用户的口令同超级用户的一样

```
# passwd jru Changing local password for jru.
New password:
Retype new password:
passwd: updating the database...
passwd: done
```

注意: 就象chpass(1)一样, yppasswd(1) 只是一个到passwd(1)的连接, 所以NIS用任何一个命令都可以正常工作。

13.6.5 pw命令

`pw(8)` 是一个用来创建、删除、修改、显示用户和组的命令行工具。它还有系统用户和组文件编辑器的功能。`pw(8)` 有一个非常强大的命令行选项设置，但新用户可能会觉得它比这里讲的其它命令要复杂很多。

13.7 限制用户使用系统资源

如果您有一些用户，并想要对他们所使用的系统资源加以限制，FreeBSD 提供了一些系统管理员限制用户访问系统资源的方法。这些限制通常被分为两种：磁盘配额，以及其它资源限制。

磁盘配额限制用户对磁盘的使用，而且它还提供一种快速检查用户使用磁盘数量而不需要时刻计算的方法。配额将在第17.15节讨论。

其它资源限制包括CPU、内存以及用户可能会使用的其它资源。这些是通过对登录进行分类完成的，下面将做讨论。

登录的类由`/etc/login.conf` 文件定义。比较精确的描述超出了本章的范围，但`login.conf(5)` 联机手册会有比较详细的描述。可以说每个用户都分配到一个登录类(默认是`default`)，每个登录类都有一套和它相对应的功能。登录功能是 `名字=值` 这样的一对值，其中 `名字` 是一个众所周知的标识符，`值` 是一个根据名字经过处理得到的任意字符串。设置登录类和功能相当简单，在`login.conf(5)` 联机手册会有比较详细的描述。

注意：系统并不直接读取`/etc/login.conf` 中的配置，而是采用数据库文件`/etc/login.conf.db` 以提供更快的查找能力。要从`/etc/login.conf` 文件生成`/etc/login.conf.db`，应使用下面的命令：

```
# cap_mkdb /etc/login.conf
```

资源限制与普通登录限制是有区别的。首先，对于每种限制，有软限制(比较常见)和硬限制之分。一个软限制可能被用户调整过，但不会超过硬限制。越往后可能越低，但不会升高。其次，绝大多数资源限制会分配特定用户的每个进程，而不是该用户的全部进程。注意，这些区别是资源限制的特殊操作所规定的，不是登录功能框架的完成(也就是说，他们实际上不是一个登录功能的特例)。

不再罗嗦了，下面是绝大多数资源限制的例子(您可以在`login.conf(5)` 找到其它与登录功能相关的内容)。

coredumpsize

很明显，由程序产生的核心文件大小的限制在磁盘使用上是属于其它限制的(例如，文件大小，磁盘配额)。不过，由于用户自己无法产生核心文件，而且通常并不删除它们，设置这个可以尽量避免由于一个大型应用程序的崩溃所造成的大量磁盘空间的浪费。(例如，**emacs**) 崩溃。

cputime

这是一个用户程序所能消耗掉的最大CPU时钟数量。一些不理想的进程会被内核杀掉。

注意：这是一个有关CPU消耗的**时钟** 限制，不是`top(1)` 和`ps(1)` 命令时屏幕上显示的CPU消耗的百分比。在写此说明时，后者的限制是是不太可能和没有价值的：编译器——编译一个可能是合法的工作——可以在某一时刻轻易的用掉100%的CPU。

filesize

这是用户可以处理一个文件的最大值。不象磁盘配额，这个限制是对单个文件强制执行的，不是用户自己的所有文件。

maxproc

这是一个用户可以运行的最大进程数。这包括前台和后台进程。很明显，这不可能比系统指定 `kern.maxproc sysctl(8)` 的限制要大。同时也要注意，设置的过小会妨碍用户的处理能力：可能需要多次登录或执行多个管道。一些任务，例如编译一些大的程序，也可能产生很多进程(例如，`make(1)`，`cc(1)` 以及其它一些预处理程序)。

memorylocked

这是一个进程允许锁到主存中的最大内存容量(参见 `mlock(2)`)。大型程序，例如像 `amd(8)` 在遇到问题时，它们得到的巨大交换量无法传递给系统进行处理。

memoryuse

这是在给定时间内一个进程可能消耗的最大内存数量。它包括核心内存和交换内存。在限制内存消耗方面，这不是一个完全的限制，但它是一个好的开始。

openfiles

这是一个进程可以打开的最大文件数。在 `FreeBSD` 中，文件可以被表现为套接字和 `IPC` 通道；注意不要把个数设置的太小。系统级的限制是由 `kern.maxfiles` 定义的，详情参见 `sysctl(8)`。

sbsize

这是网络内存数量的限制，这主要是针对通过创建许多套接字的老式 `DoS` 攻击的，但也可以用来限制网络通信。

stacksize

这是一个进程堆栈可能达到的最大值。它不能单独的限制一个程序可能使用的内存数量；所以，需要与其它的限制手段配合使用。

在设置资源限制时，有一些其他的事需要注意。下面是一些通常的技巧、建议和注意事项。

- 系统启动的进程 `/etc/rc` 会被指派给守护程序的登录类。

- 虽然/etc/login.conf 文件是一个对绝大多数限制做合理配置的资源文件，但只有您也就是系统管理员，才知道什么最适合您的系统。设置的太高可能会因为过于开放而导致系统被滥用，而设置过低，则可能降低效率。
- 使用X Window 的用户可能要比其他用户使用更多的资源。因为X11本身就使用很多资源，而且它鼓励用户同时运行更多的程序。
- 务必注意，许多限制措施是针对单个进程来实施的，它们并不限制某一用户所能用到的总量。例如，将openfiles 设置为50 表示以该用户身份运行的进程最多只能打开50 个文件。因而，用户实际可以打开的文件总数就应该是maxproc 和openfiles 值的乘积。对内存用量的限额与此类似。

有关资源限制,登录类的更深入信息可以查看相关联机手册: cap_mkdb(1), getrlimit(2), login.conf(5).

13.8 组

组简单的讲就是一个用户列表. 组通过组名和GID (组ID) 来识别。在FreeBSD (以及绝大多数其他UNIX 系统) 中，内核用以决定一个进程是能够完成一项动作的两个因素是它所属的用户ID 和组ID。与用户ID 不同，每个进程都有一个和它相关联的组的列表。您可能听说过用户或进程的“组ID”；大多数情况下，这表示列表中的第一个组。

与组ID对应的组名在/etc/group中。这是一个由冒号来界定的文本文件。第一部分是组名，第二部分是加密后的口令，第三部分是组ID，第四部分是以逗号相隔的成员列表。它可以用手工方式进行编辑(当然，如果您能保证不出语法错误的话！)。对于更完整的语法描述，参见group(5) 联机手册。

如果不想手工编辑/etc/group，也可以使用pw(8) 添加和编辑组。例如，要添加一个叫teamtwo 的组，确定它存在：

例13-8. 使用pw(8)添加一个组

```
# pw groupadd teamtwo # pw groupshow teamtwo teamtwo:*:1100:
```

上面的数字1100 是组teamtwo 的组ID。目前，teamtwo 还没有成员，因此也就没有多大用处。接下来，把jru 加入到teamtwo 组。

例13-9. 使用pw(8) 在组中添加用户

```
# pw groupmod teamtwo -M jru # pw groupshow teamtwo teamtwo:*:1100:jru
```

-M 所需的参数是一个用逗号分隔的组中用户成员的列表。前面我们已经知道，口令文件中，每个用户已经指定了一个所属组。之后用户被自动地添加到组列表里；当我们使用groupshow 命令时pw(8) 用户列表不被显示出来。但当通过id(1) 或者类似工具查看时，就会看到用户列表。换言之，pw(8) 命令只能读取/etc/group 文件；它从不尝试从/etc/passwd 文件读取更多信息。

例13-10. 使用id(1)来决定组成员

```
% id jru
uid=1001(jru) gid=1001(jru) groups=1001(jru), 1100(teamtwo)
```

正如您所看到的，jru 是组jru 和组teamtwo的成员。

有关pw(8)的更多信息，请参看其它联机手册。更多的关于/etc/group 文件格式的信息，请参考group(5) 联机手册。

备注

1. Well, 除非您连接多个终端设备,这种情况我们在第22 章讨论.
2. 可以使用的UID/GID 的最大值是4294967295, 但这可能会给采用上述假定的软件造成严重的问题。
3. 选项-sadduser(8) 是。当我们想要改变默认设置可以使用-v选项

第14章

安全

这一章的许多内容来自security(7) 联机手册，其作者是Matthew Dillon.

14.1 概述

这一章将对系统安全的基本概念进行介绍，除此之外，还将介绍一些好的习惯，以及FreeBSD下的一些更深入的话题。这章的许多内容对于一般的系统和Internet安全也适用。如今，Internet已经不再像以前那样是一个人人都愿意与您作好邻居的“友善”的地方。让系统更加安全，将保护您的数据、智力财产、时间，以及其他很多东西不至于被入侵者或心存恶意的人所窃取。

FreeBSD提供了一系列工具和机制来保证您系统和网络的完整和安全。

FreeBSD提供了大量的工具和机制来确保您的系统和网络的安全。

读完这章，您将了解：

- 基本的FreeBSD系统安全概念。
- FreeBSD中众多可用的密码学设施，例如DES和MD5。
- 如何设置一次性口令验证机制。
- 如何配置TCP Wrappers以便与inetd配合使用。
- 如何在FreeBSD 5.0以前的版本上设置KerberosIV。
- 如何在FreeBSD 5.0或更高版本上设置Kerberos5。
- 如何配置IPsec并在FreeBSD/Windows机器之间建构VPN。
- 如何配置并使用OpenSSH，以及FreeBSD的SSH执行方式。
- 系统ACL的概念，以及如何使用它们。
- 如何使用Portaudit工具来审核从Ports Collection安装的第三方软件包的安全性。
- 如何从FreeBSD的安全公告中获得有用信息并采取相应措施。
- 对于进程记帐功能的感性认识，并了解如何在FreeBSD中启用它。

在开始阅读这章之前，您需要：

- 理解基本的FreeBSD和Internet概念。

其他安全方面的话题，则贯穿本书的始终。例如，强制性访问控制(MAC)在第15章中进行了介绍，而Internet防火墙则在第26章中进行了讨论。

14.2 介绍

安全是系统管理员自始至终的基本要求。由于所有的BSD UNIX多用户系统都提供了与生俱来的安全性，因此建立和维护额外的安全机制，确保用户的“诚实”可能也就是最需要系统管理员考虑的艰巨的工作了。机器的安全性取决于您设置的安全设施，而许多安全方面的考虑，则会与人们使用计算机时的便利

性相矛盾。一般来说，UNIX 系统能够胜任数目众多进程并发地处理各类任务，这其中的许多进程是以服务身份运行的——这意味着，外部实体能够与它们互联并产生会话交互。如今的桌面系统，已经能够达到许多昔日的小型机甚至主机的性能，而随着这些计算机的联网和在更大范围内完成互联，安全也成为了一个日益严峻的课题。

最好能够通过像“洋葱”那样的分层方式来实现安全。简而言之，方便的话，应该建立尽可能多的安全层次，并小心地监视针对系统的各类入侵。当然，不应过分地构建安全机制，因为这样做可能会干扰甚至阻碍入侵检测，而后者正是安全机制中最为重要的一环。例如，在所有操作系统的可执行文件上都设置schg 标志(参见chflags(1))往往收效甚微，因为这样做，尽管短时间内能够保护这些文件，但也阻止了闯入者进行那些易于检测的修改，这意味着您设置的安全机制可能根本就无法监测到攻击者。

系统的安全也应能够应付各种形式的攻击，这也包括那些使系统崩溃，或阻止其正常运转，但并不试图窃取root 帐号(“破译root”)的攻击形式。安全问题大体可分为以下几类：

1. 拒绝服务攻击。
2. 窃取其他用户的帐户。
3. 通过可访问服务窃取root帐户。
4. 通过用户帐户窃取root帐户。
5. 建立后门。

拒绝式服务攻击是侵占机器所需资源的一种行为。通常，DoS 攻击采用暴力(brute-force)手段通过压倒性的流量来破坏服务器和网络栈，以使机器崩溃或无法使用。某些DoS 攻击则利用在网络栈中的错误，仅用一个简单的信息包就可以让机器崩溃，这类情况通常只能通过给内核打补丁来修复。在一些不利的条件下，对服务器的攻击能够被修复，只要适当地修改一下系统的选项来限制系统对服务器的负荷。顽强的网络攻击是很难对付的。例如，一个欺骗性信息包的攻击，无法阻止入侵者切断您的系统与Internet的连接。它不会使您的机器死掉，但它会把Internet连接占满。

窃取用户帐户要比D.o.S.攻击更加普遍。许多系统管理员仍然在他们的服务器上运行着基本的telnetd, rlogind, rshd 和ftpd 服务。这些服务在默认情况下不会以加密连接来操作。结果是如果您的系统有中等规模大小的用户群，在通过远程登录的方式登录到您系统的用户中，一些人的口令会被人窃取。仔细的系统管理员会从那些成功登录系统的远程访问日志中寻找可疑的源地址。

通常必须假定，如果一个入侵者已经访问到了一个用户的帐户，那么它就可能使自己成为root。然而，事实是在一个安全和维护做得很好的系统中，访问用户的帐户不一定会让入侵者成为root。这个差别是很重要的，因为没有成为root 则入侵者通常是无法隐藏它的轨迹的，而且，如果走运的话，除了让用户文件乱掉和系统崩溃之外，它不能做什么别的事情。窃取用户帐户是很普遍的事情，因为用户往往不会对系统管理员的警告采取措施。

系统管理员必须牢牢记住，可能有许多潜在的方法会使他们机器上的root 用户受到威胁。入侵者可能知道root 的口令，而如果在以root 权限运行的服务器上找到一个缺陷(bug)，就可以通过网络连接到那台服务器上达到目的；另外，一旦入侵者已经侵入了一个用户的帐户，可以在自己的机器上运行一个suid-root 程序来发现服务器的漏洞，从而让他侵入到服务器并获取root。攻击者找到了入侵一台机器上root 的途径之后，他们就不再需要安装后门了。许多root 漏洞被发现并修正之后，入侵者会想尽办法去删除日志来消除自己的访问痕迹，所以他们会安装后门。后门能给入侵者提供一个简单的方法来重新获取访问系统的root 权限，但它也会给聪明的系统管理员一个检测入侵的简便方法。让入侵者无法安装后门事实上对您的系统安全是有害的，因为这样并不会修复那些侵入系统的入侵者所发现的新漏洞。

安全的管理方法应当使用像“洋葱皮”一样多层次的方法来实现，这些措施可以按下面的方式进行分类：

1. 确保root 和维护人员帐户的安全。
2. 确保root – 以root用户权限运行的服务器和suid/sgid可执行程序的安全。
3. 确保用户帐户的安全。
4. 确保口令文件的安全。
5. 确保内核中核心组件、直接访问设备和文件系统的安全。
6. 快速检测系统中发生的不适当的变化。
7. 做个偏执狂。

这一章的下一节将比较深入地讲述上面提到的每一个条目。

14.3 确保FreeBSD 的安全

命令与协议: 在这份文档中，我们使用**粗体**来表示应用程序，并使用单倍距 字体来表示命令。这样的排版区分能够有效地区分类似ssh 这样的概念，因为它既可以表示命令，又可以表示协议。

接下来的几节中，将介绍在这一章中前一节 中所介绍的那些加强FreeBSD 系统安全性的手段。

14.3.1 确保root 和维护人员帐户的安全

首先，如果您没有确保root 帐户的安全，就没必要先劳神确保用户帐户的安全了。绝大多数系统都会指派一个口令给root 帐户。我们的第一个假定是，口令**总是**不安全的。这并不意味着您要把口令删掉。口令通常对访问机器的控制台来说是必须的。也就是说，您应该避免允许在控制台以外的地方使用口令，甚至包括使用su(1) 命令的情形。例如，确信您的pty 终端在/etc/ttys 文件中被指定为insecure (不安全)，这将使直接通过telnet 或rlogin 登录root 会不被接受。如果使用如sshd 这样的其他登录服务，也要确认直接登录root 是关闭的。您可以通过编辑/etc/ssh/sshd_config 文件来做到这一点，确信PermitRootLogin 被设置成NO。考虑到每一种访问方法——如FTP这样的服务，以免因为它们而导致安全性的损失。直接登录root 只有通过系统控制台才被允许。

当然，作为一个系统管理员，您应当获得root 身份，因此，我们开了一些后门来允许自己进入。但这些后门只有在经过了额外的口令确认之后才能使用。一种让root 可访问的方法是增加适当的用户帐户到wheel 组(在/etc/group 中)。wheel 组中的用户成员可以使用su 命令来成为root。绝对不应该通过在口令项中进行设置来赋予维护人员天然的wheel 组成员身份。维护人员应被放置在staff 组中，然后通过/etc/group 文件加入到wheel 组。事实上，只有那些需要以root 身份进行操作的用户才需要放进wheel 组中。当然，也可以通过某种其它的验证手段，例如Kerberos，可以通过root 帐户中的.k5login 文件来允许执行ksu(1) 成为root，而不必把它们放进wheel 组。这可能是一种更好的解决方案，因为wheel 机制仍然可能导致入侵者获得root，如果他拿到了口令文件，并能够进入职员帐户。尽管有wheel 比什么都强一些，但它并不是一种绝对安全的办法。

一种间接地提高员工帐号，乃至root 权限安全性的方法，便是采用其他的登录访问方式，并使用“星号” 替代员工加密的口令。使用vipw(8) 命令，可以把每一个加密的口令替换成一个“*” 符。这将更新/etc/master.passwd 文件，以及用户名/口令数据库，以禁用口令登录。

如下面的员工帐号

```
foobar:R9DT/Fa1/LV9U:1000:1000::0:0:Foo Bar:/home/foobar:/usr/local/bin/tcsh
```

应被改为:

```
foobar:*:1000:1000::0:0:Foo Bar:/home/foobar:/usr/local/bin/tcsh
```

这一更改将阻止一般的登录, 因为加密的口令永远不会与“*”匹配。一旦这么做之后, 任何员工都必须使用其他的方式来完成登录, 例如, 使用`kerberos(1)`或者通过`ssh(1)`利用公钥/密钥对的方式来完成登录。当使用`Kerberos`这样的工具时, 通常必须加强运行`Kerberos`的服务器, 以及桌面工作站的安全性。当使用公钥/密钥对以`ssh`登录时, 通常必须加固用户开始登录的那台机器的安全(通常这是他们的工作站)。在这之上还可以增加一层安全性, 即在使用`ssh-keygen(1)`生成它的时候, 使用口令来保护它们。如果能够用“星号”替换掉所有员工的口令, 那么, 这也就保证了他们只能通过您设置的的安全的方法来登录。这将迫使所有的员工使用安全的、经过加密的连接来完成他们的会话, 而这将使得入侵者通过监听网络通讯, 从某些不相关的、不太安全的机器上窃取口令成为不可能。

另一种间接的安全机制则是, 从严格受限的机器向限制更宽松的机器上登录。例如, 如果您的服务器运行了所有的服务, 那么, 工作站应该什么都不运行。为了让工作站尽可能地安全, 应该避免运行任何没有必要的服务, 甚至不运行任何服务。另外, 也应该考虑使用带口令保护功能的屏幕保护程序。毋庸置疑, 如果攻击者能够物理地接触您的工作站, 那么他就有能力破坏任何安全设施, 这确实是我们需要考虑的一个问题, 但同样地, 真正能够物理接触您的工作站或服务器并实施攻击的人在现实生活中并不常见, 绝大多数攻击来自于网络, 而攻击者往往无法物理地接触服务器或工作站。

使用类似`Kerberos`这样的工具, 也为我们提供了使用一个工具来禁用某个用户, 或修改他们的口令, 并在所有机器上立即生效的方法。如果员工的帐号被窃取, 能够在所有的其他机器上生效的口令变更将很有意义。如果口令分散地保存在多个机器上, 一次修改`N`台机器上的口令很可能是一件痛苦的事情。此外, `Kerberos`还能够提供更多的限制, 除了`Kerberos`令牌有很好的过期机制之外, 它还能够强制用户在某个特定的期限内修改口令(比如说, 每月一次)。

14.3.2 确保以root用户权限运行的服务器和suid/sgid可执行程序的安全

谨慎的管理员只运行他们需要的服务, 不多, 不少。要当心第三方的服务程序很可能有更多的问题。例如, 运行旧版的`imapd`或`popper`无异于将`root`令牌拱手送给全世界的攻击者。永远不要运行那些您没有仔细检查过的服务程序, 另外也要知道, 许多服务程序并不需要以`root`的身份运行。例如, `ntalk`、`comsat`, 以及`finger`这些服务, 都能够以一种被称作沙盒的特殊用户的身份运行。除非您已经解决掉了许多麻烦的问题, 否则沙盒就不是完美的, 但洋葱式安全规则仍然成立: 如果有人设法攻破了在沙盒中运行的程序, 那么在做更多坏事之前, 他们还必须想办法攻破沙盒本身的限制。攻击者需要攻破的层次越多, 他们成功的可能性就越小。过去, 破解`root`的漏洞几乎在所有以`root`身份运行的服务上都发现过, 包括那些基本的系统服务。如果您的机器只打算向外界提供`sshd`登录, 而用户不会使用`telnetd`或`rshd`甚至`rlogind`登录, 就应该毫不犹豫地关闭它们!

FreeBSD 现在默认在沙盒中运行`ntalkd`, `comsat`, 以及`finger`。此外, `named(8)`也可以这样运行。`/etc/defaults/rc.conf`中包括了如何如此运行`named`的方法, 只是这些内容被注释掉了。如何升级或安装系统将决定这些沙盒所使用的特殊用户是否被自动安装。谨慎的系统管理员将根据需要研究并实现沙盒。

此外, 还有一些服务通常并不在沙盒中运行: `sendmail`, `popper`, `imapd`, `ftpd`, 以及一些其他的。当然, 它们有一些替代品, 但安装那些服务可能需要做更多额外的工作。可能必须以`root`身份运行这些程序, 并通过其他机制来检测入侵。

系统中另一个比较大的`root`漏洞是安装在其中的`suid-root`和`sgid`的可执行文件。绝大多数这类程序, 例如`rlogin`, 被存放于`/bin`, `/sbin`, `/usr/bin`, 或`/usr/sbin`中。尽管并没有100%的安全保证, 但系统默认的`suid`和`sgid`可执行文件通常是相对安全的。当然, 偶尔也会发现一些存在于这些可执行文件中的`root`漏洞。1998年, `xlib`中发现了一处`root`漏洞, 这使得`xterm`(通常是做了`suid`的)变得可以入侵。做的安全

些，总比出现问题后再后悔要强。因此，谨慎的管理员通常会限制suid可执行文件，并保证只有员工帐号能够执行它们，或只开放给特定的用户组，甚至彻底干掉(chmod 000)任何suid可执行文件，以至于没有人能够执行它们。没有显示设备的服务器通常不会需要xterm可执行文件。sgid可执行文件通常同样地危险。一旦入侵者攻克了sgid-kmem，那么他就能读取/dev/kmem并进而读取经过加密的口令文件，从而窃取任何包含口令的帐号。另外，攻破了kmem的入侵者能够监视通过pty传送的按键序列，即使用户使用的是安全的登录方式。攻破了tty组的用户则能够向几乎所有用户的tty写入数据。如果用户正在运行一个终端程序，或包含了键盘模拟功能的终端仿真程序，那么，入侵者能够以那个用户的身份执行任何命令。

14.3.3 确保用户帐户的安全

用户帐号的安全通常是最难保证的。虽然您可以为您的员工设置严苛的登录限制，并用“星号”替换掉他们的口令，但您可能无法对普通的用户这么做。如果有足够的决策权，那么在保证用户帐号安全的斗争中或许会处于优势，但如果不是这样，您能做的只是警惕地监控这些帐号的异动。让用户使用ssh或Kerberos可能会有更多的问题，因为需要更多的管理和技术支持，尽管如此，与使用加密的口令文件相比，这仍不失为一个好办法。

14.3.4 确保口令文件的安全

尽可能使用*替换掉口令是保证口令文件安全唯一的解决方法，如果能够用ssh或Kerberos的话。即使只有root用户能够读取加密过的口令文件(/etc/spwd.db)，入侵者仍然可能设法读到它的内容，即使他暂时还无法写入这个文件。

您的安全脚本应该经常检查并报告口令文件的异动(参见后面的检查文件完整性一节)。

14.3.5 确保内核中内核设备、直接访问设备和文件系统的安全

如果攻击者已经拿到了root那么他就有能力作任何事情，当然，有一些事情是他们比较喜欢干的。例如，绝大多数现代的内核都包括一个内建的听包设备。在FreeBSD中，这个设备被称作bpf。攻击者通常会尝试在攻克的系统上运行它。如果您不需要bpf设备提供的功能，那么，就不要把它编入内核。

但即使已经关掉了bpf设备，您仍然需要担心/dev/mem和/dev/kmem。就事论事地说，攻击者仍然能够通过直接访问的方式写入磁盘设备。同样地，还有一个被称作模块加载器，kldload(8)的机制，也会包含潜在的危险。尝试入侵企业网络的入侵者会尝试在正在运行的内核上安装他自己的bpf设备，或其他听包设备。为了防止这些问题，需要抬高内核安全级，至少调整到1。可以通过对kern.securelevel执行sysctl来完成这个任务。一旦把安全级调整到1，对于直接访问设备的写入操作将被拒绝，而特殊的chflags标记，如schg，将被强制执行。一定要在重要的启动执行文件、目录和脚本文件上设置schg标记——在安全级生效之前的所有文件。这可能做得有些过火，并将导致在较高安全级上运行时升级系统变得困难。此外，运行于较高安全级上，而没有正确设置schg标记的系统仍然是存在弱点的。另一种方法是把/和/usr以只读方式挂接。此外，请注意过于严苛的安全设置将使得入侵检测同样无法进行。

14.3.6 检查文件完整性: 可执行文件，配置文件和其他文件

当实施严格的限制时，往往会在使用的方便性上付出代价。例如，使用chflags来把schg标记应用到/和/usr中的绝大多数文件上可能会起到反作用，因为尽管它能够保护那些文件，但同样关掉了一个很好的监测机制。层次化安全的最后一层可能是最重要的——检测。安全的其他部分可能相对来讲意义并不大(或者，更糟糕的事情是，那些措施会给您安全的假象)，假如您无法检测潜在的入侵事件。层次化安

全最重要的功能是减缓入侵者，而不是彻底不让他们入侵，这能够让检测起到作用，并更好地捕捉入侵行为。

检测入侵的一种好办法是查找那些被修改、删除或添加的文件。检测文件修改的最佳方法是与某个(通常是中央的)受限访问的系统上的文件进行比对。在一台严格限制访问的系统上撰写您的安全脚本通常不能够被入侵者察觉，因此，这非常重要。为了最大限度地发挥这一策略的优势，通常会使用只读的NFS，或者设置ssh 密钥对以便为其他机器提供访问。除了网络交互之外，NFS可能是一种很难被察觉的方法——它允许您监控每一台客户机上的文件系统，而这种监控几乎是无法察觉的。如果一台严格受限的服务器和客户机是通过交换机连接的，那么NFS将是一种非常好的方式。不过，如果那台监控服务器和客户机之间通过集线器(Hub)，或经过许多层的路由来连接，则这种方式就很不安全了，此时，应考虑使用ssh，即使这可以在审计记录中查到。

一旦为这个受限的机器赋予了至少读取它应监控的客户系统的权限，就应该为实际的监控撰写脚本。以NFS 挂接为例，可以用类似find(1) 和md5(1) 这样的命令为基础来完成我们所需的工作。最好能够每天对被控机的所有执行文件计算一遍md5，同时，还应以更高的频率测试那些/etc 和/usr/local/etc 中的控制文件。一旦发现了不匹配的情形，监控机应立即通知系统管理员。好的安全脚本也应该检查在系统分区，如/ 和/usr 中是否有新增或删除的可执行文件，以及不适宜的suid 。

如果打算使用ssh 来代替NFS，那么撰写安全脚本将变得困难许多。本质上，需要在脚本中使用scp 在客户端复制文件，另一方面，用于检查的执行文件(例如find) 也需要使用scp 传到客户端，因为ssh 客户程序很可能已经被攻陷。总之，在一条不够安全的链路上ssh 可能是必须的，但也必须应付它所带来的难题。

安全脚本还应该检查用户以及职员成员的权限设置文件：.rhosts、.shosts、.ssh/authorized_keys 等等。... 这些文件可能并非通过MD5 来进行检查。

如果您的用户磁盘空间很大，检查这种分区上面的文件可能非常耗时。这种情况下，采用标志来禁止使用suid 可执行文件和设备在这些文件系统上出现将是一个好主意。您可能会想看看nodev 和nosuid 这两个选项(参见mount(8))。尽管如此，这些扫描仍然应该至少每周进行一次，这样做的意义并不是检测有效的攻击，而是检查攻击企图。

进程记帐(参见accton(8)) 是一种相对成本较低的，可以帮助您在被入侵后评估损失的机制。对于找出入侵者是如何进入系统的这件事情来说，它会非常的有所助益，特别是当入侵者什么文件都没有修改的情况下。

最后，安全脚本应该处理日志文件，而日志文件本身应该通过尽可能安全的方法生成——远程syslog 可能非常有用。入侵者会试图掩盖他们的踪迹，而日志文件对于希望了解入侵发生时间的系统管理员来说则显得尤为重要。保持日志文件的永久性记录的一种方法是在串口上运行系统控制台，并持续不断地在一台安全的机器上收集这些信息。

14.3.7 偏执

带点偏执不会带来伤害。作为一种惯例，系统管理员在不影响使用的便利的前提下可以启用任何安全特性，此外，在经过深思熟虑之后，也可以增加一些**确实会** 让使用变得不那么方便的安全特性。更重要的是，有安全意识的管理员应该学会混合不同的安全策略——如果您逐字逐句地按照这份文档来配置您的机器，那无异于向那些同样能得到这份文档的攻击者透露了更多的信息。

14.3.8 拒绝服务攻击

这一节将介绍拒绝服务攻击。DoS 攻击通常是基于数据包的攻击，尽管几乎没有任何办法来阻止大量的伪造数据包耗尽网络资源，但通常可以通过一些手段来限制这类攻击的损害，使它们无法击垮服务器。

1. 限制服务进程fork.
2. 限制springboard 攻击(ICMP 响应攻击, ping 广播, 等等)。
3. 内核路由缓存

对于通过复制进程(fork)来进行服务的服务器的一种很常见的攻击是想办法耗尽其进程、文件描述符或者内存,直到机器彻底死掉。**inetd** (参见**inetd(8)**)提供了许多选项来限制这类攻击。需要注意的是,尽管能够阻止一台机器彻底垮掉,但通常无法防止服务本身被击垮。请仔细阅读**inetd**的联机手册,特别是它的-c、-C以及-R这三个选项。伪造IP攻击能够绕过**inetd**的-C选项,因此,这些选项需要配合使用。某些独立的服务器也有类似的限制参数。

例如,**Sendmail**就提供了自己的-OMaxDaemonChildren选项,它通常比sendmail的负载限制选项更为有效,因为服务器负载的计算有滞后性。您可以在启动**sendmail**时指定一个MaxDaemonChildren参数,把它设的足够高以便承载您所需要的负荷,当然,不要高到足以让运行**sendmail**的机器死掉。此外,以队列模式(-ODeliveryMode=queued)并把服务程序(sendmail -bd)和队列执行程序分别执行(sendmail -q15m)也是一个好主意。如果您希望保证队列的实时性,可以考虑使用更短的间隔,例如-q1m,但同时也需要指定一个合理的子进程数,也就是通过MaxDaemonChildren选项以免那个 sendmail 造成重叠的故障。

Syslogd可以被直接地攻击,因此,强烈建议只要可行,就在启动它的时候加上-s参数,其他情况下,则至少应该加上-a。

对于基于连接的服务,例如**TCP Wrapper**的reverse-identd,都应该格外的小心,因为它们都可能直接遭受攻击。一般情况下,基于安全考虑,不应使用**TCP Wrapper**所提供的reverse-ident这样的功能。

此外,将内部服务保护起来,阻止来自其他主机的访问也十分重要,这些工作可以通过设置边界路由器来完成。主要的想法,是阻止来自您的LAN以外的访问,这有助于避免root受到攻击。尽可能配置排他式的防火墙,例如,“用防火墙阻止所有的网络流量除了端口A、B、C、D,以及M-Z”。通过采用这种方法,您可以很容易地将低端口的访问阻止在外,而又不难配置使防火墙放过那些明确需要开放的服务,例如**named** (如果您的机器准备作为域的主要解析服务器),**ntalkd**, **sendmail**,以及其他可以从Internet访问的服务。如果您尝试以其他方式配置防火墙——采用比较宽松的策略,那么您将很有可能忘记“关掉”一两个服务,或者在增加了一些服务之后忘记更新防火墙策略。尽管如此,仍然可以考虑允许让数据进入编号较高的那一部分端口,这将保证那些需要这样特性的服务能够正常工作,而又不影响低端口服务的安全性。此外,还应注意到FreeBSD允许您来控制动态绑定的端口的范围,即一系列net.inet.ip.portrange变量,通过sysctl来完成设置。(sysctl -a | fgrep portrange)。这使得您完成较复杂的防火墙策略变得易如反掌。例如,您可能希望普通的高段端口的起止范围是4000到5000,而更高范围则是49152到65535,随后在防火墙中阻止低于4000的所有端口(当然,除了那些特地为Internet访问而开设的端口)。

另一种常被称作springboard的攻击也是非常常见的DoS攻击——它通过使服务器产生其无法处理的响应来达到目的。最常见的攻击就是**ICMP ping 广播攻击**。攻击者通过伪造ping包,将其源IP设置为希望攻击的机器的IP。如果您的边界路由器没有进行禁止ping广播地址的设置,则您的网络将最终陷于响应伪造的ping之中,特别是当攻击者同时使用了多个不同的网络时。广播攻击能够产生超过120兆位的瞬时流量。另一种常见的针对ICMP错误报告系统的springboard攻击,通过建立可以生成ICMP出错响应的包,攻击者能够攻击服务器的网络下行资源,并导致其上行资源耗尽。这种类型的攻击也可以通过耗尽mbuf来使得被攻击的服务器崩溃,特别是当这些服务器无法足够快地完成ICPM响应的时候。在FreeBSD 4.X内核中有一个叫做ICMP_BANDLIM的编译选项来限制这类攻击,使其变得不再那么有效,而较新的内核则可以通过sysctl变量net.inet.icmp.icmplim来调整。最后一类主要的springboard是针对某些**inetd**的内部服务,例如udp echo服务进行的。攻击者简单地伪造一个来自服务器A的echo口的UDP包,然后将这个包发到B的echo口。于是,两台服务器将不停地将包弹给对方。攻击者能够将两台服务器的这种服务都耗竭,并且通过这种方式,只需要很少的包就可以让LAN超载。类似的问题对**chargen**口也是存在的。好的系统管理员应该关闭这些**inetd**的测试服务。

伪造的包攻击也可以用来使内核的路由缓存过载。请参考net.inet.ip.rtexpire, rtminexpire, 以

及`rtmaxcache sysctl`参数。伪造的包可以用随机的源IP攻击，使得内核在路由表中产生一个临时的缓存项，它可以通过`netstat -rna | fgrep w3`看到。这些路由通常需要1600秒才会过期。如果内核发现路由表变得太大，它会动态地降低`rtexpire`但以`rtminexpire`为限。这引发了两个问题：

1. 在访问量不大的服务器上，内核对于突然袭击的反应不够快。
2. `rtminexpire`的值没有低到让内核在此类攻击时活下去的程度。

如果您的服务器通过T3或更快的线路接入Internet，那么通过`sysctl(8)`来手动地降低`rtexpire`和`rtminexpire`就非常必要。当然，绝不要把它们设置为零(除非您想让机器崩溃)将这两个参数设置为2通常已经足以抵御这类攻击了。

14.3.9 Kerberos 和SSH 的访问问题

如果您打算使用，那么Kerberos和ssh都有一些需要解决的问题。Kerberos V是一个很棒的验证协议，但使用了它的`telnet`和`rlogin`应用程序有一些bug，使得它们不适合处理二进制流。而且，除非使用了`-x`选项，否则默认情况下Kerberos并不加密会话。`ssh`在默认时加密所有的会话内容。

除了默认转发加密密钥，ssh在所有的其他方面都做得很好。这意味着如果您持有供您访问系统其他部分密钥的工作站作了很好的安全防护，而您连到了一台不安全的机器上，则您的密钥可能被别人获得。尽管实际的密钥并没有被泄漏，但由于ssh会在您登录的过程中启用一个转发端口，如果攻击者拿到那台不安全的机器上的root那么他将能够利用那个端口来使用您的密钥，从而访问您能够访问的那些机器。

我们建议您在ssh时配合Kerberos来完成工作人员的登录过程。ssh在编译时可以加入Kerberos支持。在减少了潜在地暴露ssh密钥的机会的同时，它还能够通过Kerberos来保护口令。ssh密钥只有在做过安全防护的机器上执行自动操作时才应使用(这是Kerberos不适合的情形)。此外，我们还建议您要么在ssh配置中关闭密钥转发，要么在`authorized_keys`中增加`from=IP/DOMAIN`选项，来限制这些密钥能够登录的来源机器。

14.4 DES，MD5，以及Crypt

部分重写、更新来自Bill Swingle.

UNIX系统上的每个用户都有一个与其帐户关联的口令。很显然，密码只需要被这个用户和操作系统知道。为了保证口令的私密性，采用了一种称为“单向散列”的方法来处理口令，简单地说，很容易从口令推算出散列值，反之却很难。其实，刚才那句话可能并不十分确切：因为操作系统本身并不真的知道您的口令。它只知道口令经过加密的形式。获取口令对应“明文”的唯一办法是采用暴力在口令可能的区间内穷举。

不幸的是，当UNIX刚刚出现时，安全地加密口令的唯一方法基于DES，数据加密标准(the Data Encryption Standard)。于是这给那些非美国居民带来了问题，因为DES的源代码在当时不能被出口到美国以外的地方，FreeBSD必须找到符合美国法律，但又要与其他那些使用DES的UNIX版本兼容的办法。

解决方案是把加密函数库分割为两个，于是美国的用户可以安装并使用DES函数库，而国际用户则使用另外一套库提供的一种可以出口的加密算法。这就是FreeBSD为什么使用MD5作为它的默认加密算法的原因。MD5据信要比DES更安全，因此，安装DES更多地是出于兼容目的。

14.4.1 识别您采用的加密算法

在FreeBSD 4.4之前, `libcrypt.a` 曾经是一个指向相应加密算法的符号连接。FreeBSD 4.4开始, 把`libcrypt.a` 变成了一个可以配置的密码验证散列库。现在这个库支持DES, MD5和Blowfish散列函数。默认情况下, FreeBSD 使用MD5来加密口令。

可以很容易地识别FreeBSD使用哪种加密方法。检查`/etc/master.passwd`文件中的加密密码是一种方法。用MD5散列加密的密码通常要比用DES散列得到的长一些, 并且以`$1$`字符开始。以`$2a$`开始的口令是通过Blowfish散列函数加密的。DES密码字符没有任何可以用于鉴别的特征, 但他们要比MD5短, 并且以不包括`$`在内的64个可显示字符来表示, 因此相对比较短的、没有以美元符号开头的字符串很可能是一个DES口令。

新口令所使用的密码格式是由`/etc/login.conf`中的`passwd_format`来控制的, 可供选择的算法包括`des`, `md5`和`blf`。请参考`login.conf(5)`联机帮助以获得更进一步的详情。

14.5 一次性口令

UNIX系统上的每个用户都有一个与其帐户关联的口令。很显然, 为了保证口令的私密性, 使用了一种容易加密, 却很难解密的被称作“单向散列”的方法来处理口令。换言之, 我们刚刚说的那句话并不十分确切: 操作系统本身并不真的知道您的口令。它只知道口令经过加密的形式。获取口令对应“明文”的唯一办法是采用暴力在口令可能的区间内穷举。

S/Key是基于单向hash功能的一次性密码管理方式。为了考虑兼容性而使用了MD4散列, 而其他系统则使用了MD5和DES-MAC。S/Key从1.1.5版之后就一直是FreeBSD基本系统的一部分, 包含这一特性的操作系统也日益增多。S/Key是Bell Communications Research, Inc.的注册商标。

从FreeBSD 5.0版开始, S/Key被功能相同的OPIE (One-time Passwords In Everything)取代了。OPIE默认使用MD5散列。

下面将介绍三种不同的口令。第一种是您常用的UNIX风格或Kerberos口令; 我们在后面的章节中将称其为“UNIX口令”。第二种是使用S/Key的`key`程序或OPIE的`opiekey(1)`程序生成, 并为`keyinit`或`opiepasswd(1)`以及登录提示所接受的一次性口令, 我们称其为“一次性口令”。最后一类口令是您输入给`key/opiekey`程序(有些时候是`keyinit/opiepasswd`程序)用以产生一次性口令的秘密口令, 我们称其为“秘密口令”或通俗地简称为“口令”。

秘密口令和您的UNIX口令毫无关系, 尽管可以设置为相同的, 但不推荐这么做。S/Key和OPIE秘密口令并不像旧式的UNIX口令那样只能限于8位以内¹。您想要用多长的口令都可以。有六、七个词的短句是很常见的选择。在绝大多数时候, S/Key或OPIE系统和UNIX口令系统完全相互独立地工作。

除了口令之外, 对于S/Key和OPIE还有两组至关重要的数据。其一被称作“种子”或“key”, 它包括两个字符和五个数字。另一个被称作“迭代轮数”, 这是一个1到100之间的数字。S/Key通过将种子加到秘密口令后面, 并执行迭代轮数那么多次的MD4/MD5散列运算来得到结果, 并将结果表示为6个短的英文单词。这6个英文单词就是您的一次性口令。验证系统(主要是PAM)会记录上次使用的一次性口令, 如果用户提供的口令的散列值与上次一致, 则可以通过身份验证。由于使用了单向的散列函数, 因此即使截获了上次使用的口令, 也没有办法恢复出下次将要使用的口令; 每次成功登录都将导致迭代轮数递减, 这样用户和登录程序将保持同步。每当迭代轮数减少到1时, 都必须重新初始化S/Key和OPIE。

接下来将讨论和每个系统有关的三个程序。`key`和`opiekey`程序能够接收带迭代计数, 种子和秘密口令, 并生成一个一次性口令, 或一张包含连续的一组一次性口令的表格。`keyinit`和`opiepasswd`程序分别用于初始化S/Key和OPIE, 并修改口令、迭代次数、种子和一次性口令。`keyinfo`和`opieinfo`程序可以用

于检查相应的验证数据文件(/etc/skeykeys 或/etc/opedkeys)并显示执行命令的用户当前的迭代轮数和种子。

我们将介绍四种不同的操作。在安全的连接上通过keyinit 或opedpasswd 来第一次设置一次性口令,或修改口令及种子。第二类操作是在不安全的连接上使用keyinit 或opedpasswd 辅以在安全连接上执行的key 或opedkey 来完成同样的工作。第三类操作是在不安全的连接上使用key/opedkey 来登录。最后一类操作是采用key 或opedkey 来生成大批的密码,以便抄下来或打印出来,在没有安全连接的地方使用。

14.5.1 安全连接的初始化

第一次初始化S/Key,修改口令或种子需要在安全的连接(例如,在那台机器的控制台上或者通过ssh)登录来完成。以自己的身份登录并执行不带参数的keyinit 命令:

```
% keyinit
Adding unfurl:
Reminder - Only use this method if you are directly connected.
If you are using telnet or rlogin exit with no password and use keyinit -s.
Enter secret password:
Again secret password:

ID unfurl s/key is 99 to17757
DEFY CLUB PRO NASH LACE SOFT
```

对于OPIE,则使用opedpasswd:

```
% opedpasswd -c
[grimreaper] ~ $ opedpasswd -f -c
Adding unfurl:
Only use this method from the console; NEVER from remote. If you are using
telnet, xterm, or a dial-in, type ^C now or exit with no password.
Then run opedpasswd without the -c parameter.
Using MD5 to compute responses.
Enter new secret pass phrase:
Again new secret pass phrase:
ID unfurl OTP key is 499 to4268
MOS MALL GOAT ARM AVID COED
```

在Enter new secret pass phrase: 或Enter secret password: 提示之后,应输入一个密码或口令字。请注意,这并不是您用于登录的口令,它用于生成一次性的登录密钥。“ID”这一行给出了所需的参数:您的登录名,迭代轮数,以及种子。登录系统时,它能够记住这些参数并呈现给您,因此无需记忆它们。最后一行给出了与您的秘密口令对应的、用于登录的一个一次性口令;如果您立即重新登录,则它将是您需要使用的那个口令。

14.5.2 不安全连接初始化

如果您需要通过一个不安全的连接来初始化,则应首先在安全连接上执行过一次key 或opedkey;这可以在Macintosh 的桌面附件,或是在可信的机器的shell 上面完成。此外还需要指定一个迭代轮数(100 也许是一个较好的选择)也可以选择一个自己的种子,或让计算机随机生成一个。在不安全的连接上(当然是连到您希望初始化的机器上),使用keyinit -s 命令:

```
% keyinit -s
```



```
Updating unfurl:
Old key: to17758
Reminder you need the 6 English words from the key command.
Enter sequence count from 1 to 9999: 100
Enter new key [default to17759]:
s/key 100 to 17759
s/key access password:
s/key access password:CURE MIKE BANE HIM RACY GORE
```

对于OPIE, 则需要使用opiepasswd:

```
% opiepasswd
```

```
Updating unfurl:
You need the response from an OTP generator.
Old secret pass phrase:
    otp-md5 498 to4268 ext
    Response: GAME GAG WELT OUT DOWN CHAT
New secret pass phrase:
    otp-md5 499 to4269
    Response: LINE PAP MILK NELL BUOY TROY
```

```
ID mark OTP key is 499 gr4269
LINE PAP MILK NELL BUOY TROY
```

为了接受默认的种子(keyinit 程序令人困惑地将其称作key), 按下**Return**。在输入访问口令之前, 到一个有安全连接或S/Key 桌面附件的机器上, 并给它同样的参数:

```
% key 100 to17759
Reminder - Do not use this program while logged in via telnet or rlogin.
Enter secret password: <secret password>
CURE MIKE BANE HIM RACY GORE
```

对于OPIE:

```
% opiekey 498 to4268
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
GAME GAG WELT OUT DOWN CHAT
```

现在回到不安全的连接, 并将生成的一次性口令粘贴到相应的应用程序中。

14.5.3 生成一个一次性密码

一旦初始化过S/Key 或OPIE, 当您登录时将看到类似这样的提示:

```
% telnet example.com
Trying 10.0.0.1...
Connected to example.com
Escape character is '^['.
```

```
FreeBSD/i386 (example.com) (ttya)
```

```
login: <username>
s/key 97 fw13894
Password:
```

对于OPIE 则是:

```
% telnet example.com
Trying 10.0.0.1...
Connected to example.com
Escape character is '^['.
```

```
FreeBSD/i386 (example.com) (ttya)
```

```
login: <username>
otp-md5 498 gr4269 ext
Password:
```

另外, S/Key 和OPIE 提示有一个很有用的特性(这里没有表现出来): 如果您在口令提示处按下**Return**(回车) 系统将回显刚键入的口令, 您可以藉此看到自己所键入的内容。如果试图手工键入一个一次性密码, 这会非常有用。

此时您需要生成一个一次性密码来回答这一提示。这项工作必须在一个可信的系统上执行**key** 或**opiekey** 来完成。(也可以找到DOS、Windows 以及Mac OS 等操作系统上运行的版本)。这个程序需要将迭代轮数和种子提供给它。您可以从登录提示那里复制和粘贴它们。

在可信的系统上:

```
% key 97 fw13894
Reminder - Do not use this program while logged in via telnet or rlogin.
Enter secret password:
WELD LIP ACTS ENDS ME HAAG
```

对于OPIE:

```
% opiekey 498 to4268
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
GAME GAG WELT OUT DOWN CHAT
```

现在使用刚刚生成的一次性口令登录:

```
login: <username>
s/key 97 fw13894
Password: <return to enable echo>
s/key 97 fw13894
Password [echo on]: WELD LIP ACTS ENDS ME HAAG
Last login: Tue Mar 21 11:56:41 from 10.0.0.2 ...
```

14.5.4 产生多个一次性口令

有时，会需要到不能访问可信的机器或安全连接的地方。这种情形下，可以使用`key`和`opiekey`命令来一次生成许多一次性口令。例如：

```
% key -n 5 30 zz99999
Reminder - Do not use this program while logged in via telnet or rlogin.
Enter secret password: <secret password>
26: SODA RUDE LEA LIND BUDD SILT
27: JILT SPY DUTY GLOW COWL ROT
28: THEM OW COLA RUNT BONG SCOT
29: COT MASH BARR BRIM NAN FLAG
30: CAN KNEE CAST NAME FOLK BILK
```

对于OPIE：

```
% opiekey -n 5 30 zz99999
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase: <secret password>
26: JOAN BORE FOSS DES NAY QUIT
27: LATE BIAS SLAY FOLK MUCH TRIG
28: SALT TIN ANTI LOON NEAL USE
29: RIO ODIN GO BYE FURY TIC
30: GREW JIVE SAN GIRD BOIL PHI
```

`-n 5` 按顺序请求5个口令，`30` 则指定了最后一个迭代轮数应该是多少。注意这些口令将按与使用顺序相反的顺序来显示。如果您比较偏执，可以手工写下这些结果；一般来说把它粘贴到`lpr`就可以了。注意，每一行都显示迭代轮数及其对应的一次性的密码；一些人建议用完一个就划掉一个。

14.5.5 限制使用UNIX® 口令

S/Key 可以对UNIX 口令的使用实施基于主机名、用户名、终端端口或登录会话的IP 地址的各种限制。这些限制可以在配置文件`/etc/skey.access`中找到。`skey.access(5)`联机帮助提供了关于文件格式的详细资料，并给出了更详细的使用这一配置文件时在安全方面需要注意的事项。

如果没有`/etc/skey.access`这个文件(在FreeBSD 4.X 系统上这是默认的)，那么所有的用户都可以使用UNIX 口令。然而如果它存在，所有的用户将被要求使用S/Key，除非明确地在`skey.access`中配置允许这样做。无论如何，UNIX 在控制台上总是可用的。

下面是一个示例的`skey.access`配置文件，它展示了最常用的三类配置语句：

```
permit internet 192.168.0.0 255.255.0.0
permit user fnord
permit port ttyd0
```

第一行(`permit internet`)允许来自IP 源地址(需要注意这是可能被伪造的)与指定的掩码值进行逻辑与之后，与给定值匹配的用户使用UNIX 口令。这不应被认为是一种安全机制，它只是为那些使用不安全网络的获得许可的用户提供了用S/Key 进行身份验证的手段。

第二行(`permit user`)允许指定的用户，在本例中是`fnord`，在任何时候使用UNIX 口令。一般说来，只应为无法使用`key`程序，例如那些使用哑终端，或无法学会如何使用它的用户启用这样的功能。

第三行(`permit port`)允许通过指定终端线的用户使用UNIX 口令；这可以被用于拨号用户。

OPIE 可以像S/Key 一样对UNIX 口令的使用进行基于IP 的登录限制。对应的文件是`/etc/opieaccess`，在FreeBSD 5.0 和更高版本的系统中，默认情况下它就已经存在了。请参阅`opieaccess(5)` 以了解关于这个文件进一步的情况，以及安全方面需要进行的一些考虑。

下面是一个示范的`opieaccess` 文件：

```
permit 192.168.0.0 255.255.0.0
```

这行允许指定IP 地址的用户(再次强调这种地址容易被伪造) 在任何时候使用UNIX 口令登录。

如果`opieaccess` 中没有匹配的规则，则将默认拒绝任何非OPIE 登录。

14.6 TCP Wrappers

作者: *Tom Rhodes*.

每一个熟悉`inetd(8)` 都应该听说过TCP Wrappers，但几乎没有人对它在网络环境中的作用有全面的理解。几乎每个人都会安装防火墙来处理网络连接，然而虽然防火墙有非常广泛的用途，它却不是万能的，例如它无法处理类似向连接发起者发送一些文本这样的任务。而TCP 软件能够完成它以及更多的其他事情。接下来的几段中将讨论许多TCP Wrappers 提供的功能，并且，还给出了一些配置实例。

TCP Wrappers 软件扩展了`inetd` 为受其控制的服务程序实施控制的能力。通过使用这种方法，它能够提供日志支持、返回消息给联入的连接、使得服务程序只接受内部连接，等等。尽管防火墙也能够完成其中的某些功能，但这不仅增加了一层额外的保护，也提供了防火墙无法提供的功能。

然而，由TCP Wrappers 提供一些额外的安全功能，不应被视为好的防火墙的替代品。TCP Wrappers 应结合防火墙或其他安全加强设施一并使用，为系统多提供一层安全防护。

由于这些配置是对于`inetd` 的扩展，因此，读者应首先阅读配置`inetd` 这节。

注意：尽管由`inetd(8)` 运行的程序并不是真正的“服务程序”，但传统上也把它们称为服务程序。下面仍将使用这一术语。

14.6.1 初始配置

在FreeBSD 中使用TCP Wrappers 的唯一要求是确保`inetd` 在从`rc.conf` 中启动时包含了`-ww` 选项；这是默认的设置。当然，还需要对`/etc/hosts.allow` 进行适当的配置，但`syslogd(8)` 在配置不当时会在系统日志中记录相关消息。

注意：与其它的TCP Wrappers 实现不同，使用`hosts.deny` 在这里被认为是不推荐和过时的做法。所有的配置选项应放到`/etc/hosts.allow` 中。

在最简单的配置中，服务程序的连接策略是根据`/etc/hosts.allow` 允许或阻止。FreeBSD 中的默认配置是允许一切发到由`inetd` 所启动的服务的连接请求。在基本配置之后将讨论更复杂的情况。

基本配置的形式通常是服务：地址：动作。这里服务 是从`inetd` 启动的服务程序的名字。而地址 可以是任何有效的主机名、一个IP 或由方括号([]) 括起来的IPv6 地址。动作字段可以使`allow` 或`deny`，分别用于允

许和禁止相应的访问。在配置时您需要注意所有的配置都是按照第一个匹配的规则运转的，这表示配置文件将按照顺序查找匹配规则，而一旦找到匹配，则搜索也就停止了。

另外也有许多其他选项，这些将在后面介绍。简单的配置行从上面这些描述之中可以很容易得出。例如，允许POP3 连接通过mail/qpopper 服务，应把下面的行添加到hosts.allow:

```
# This line is required for POP3 connections:
qpopper : ALL : allow
```

增加这样之后，需要重新启动inetd。可以通过使用kill(1) 命令来完成这项工作，或使用/etc/rc.d/inetd 的restart parameter 参数。

14.6.2 高级配置

TCP Wrappers 也有一些高级的配置选项；它们能够用来对如何处理连接实施更多的控制。一些时候，返回一个说明到特定的主机或请求服务的连接可能是更好的办法。其他情况下，记录日志或者发送邮件给管理员可能更为适合。另外，一些服务可能只希望为本机提供。这些需求都可以通过使用通配符，扩展字符以及外部命令来实现。接下来的两节将介绍这些。

14.6.2.1 外部命令

假设由于发生了某种状况，而导致连接应该被拒绝掉，而将其原因发送给发起连接的人。如何完成这样的任务呢？这样的动作可以通过使用twist 选项来实现。当发起了连接请求时，twist 将调用一个命令或脚本。在hosts.allow 文件中已经给出了一个例子：

```
# The rest of the daemons are protected.
ALL : ALL \
      : severity auth.info \
      : twist /bin/echo "You are not welcome to use %d from %h."
```

这个例子将把消息 “You are not allowed to use daemon from hostname.” 返回给访问先前没有配置过允许访问的服务客户。对于希望把消息反馈给连接发起者，然后立即切断这样的需求来说，这样的配置非常有用。请注意所有反馈信息必须 被引号" 包围；这一规则是没有例外的。

警告: 如果攻击者向服务程序发送大量的连接请求，则可能发动一次成功的拒绝服务攻击。

另一种可能是针对这种情况使用spawn。类似twist，spawn 也暗含拒绝连接，并可以用来执行外部命令或服务。与twist 不同的是，spawn 不会向连接发起者发送回应。考虑下面的配置：

```
# We do not allow connections from example.com:
ALL : .example.com \
      : spawn (/bin/echo %a from %h attempted to access %d >> \
      /var/log/connections.log) \
      : deny
```

这将拒绝来自*.example.com 域的所有连接；同时还将记录主机名，IP 地址，以及对方所尝试连接的服务名字到/var/log/connections.log 文件中。

除了前面已经介绍过的转义字符，例如%a 之外，还有一些其它的转义符。参考hosts_access(5) 联机手册可以获得完整的列表。

14.6.2.2 通配符选项

前面的例子都使用了ALL。其它选项能够将功能扩展到更远。例如，ALL 可以被用来匹配每一个服务、域，或IP 地址。另一些可用的通配符包括PARANOID，它可以用来匹配任何来自可能被伪造的IP 地址的主机。换言之，paranoid 可以被用来定义来自IP 与其主机名不符的客户。下面的例子将给您更多的感性认识：

```
# Block possibly spoofed requests to sendmail:
sendmail : PARANOID : deny
```

在这个例子中，所有连接sendmail 的IP 地址与其主机名不符的主机都将被拒绝。

小心: 如果服务器和客户机有一方的DNS 配置不正确，使用PARANOID 可能会严重地削弱服务。在设置之前，管理员应该谨慎地考虑。

要了解关于通配符和他们的功能，请参考hosts_access(5) 联机手册。

为了使设置能够生效，应该首先把hosts.allow 的第一行配置注释掉。这节的开始部分已经说明了这一点。

14.7 KerberosIV

撰写者Mark Murray. 初稿Mark Dapoz.

Kerberos 是一个网络附加系统/协议，它使得用户能够通过一个安全服务器的服务来验证身份。象远程登录，远程复制，系统间的相互文件复制和其他完成高风险任务的服务将被变得相当安全和可控制。

下面将具体介绍如何配置随FreeBSD 发行的Kerberos。不过，您还是应该阅读相应的联机手册以获得完整的说明。

14.7.1 安装KerberosIV

Kerberos 是FreeBSD 的一项可选组件。安装该软件最简单的办法就是在使用sysinstall 安装FreeBSD 时选择krb4 或krb5。这样将会安装“eBones” (KerberosIV) 或“Heimdal” (Kerberos5) 的Kerberos 实现。采用实现的原因是它们在美国/加拿大以外的地区开发，因此这些国家之外的人使用，而不必受美国的加密代码出口管制的限制。

此外，您可以从security/krb5 得到Kerberos 的MIT 实现。

14.7.2 创建最初的数据库

这项工作只需要在Kerberos 服务器上完成。首先确认没有旧的Kerberos 数据库存在。您应该进入到/etc/kerberosIV 目录中并检查下述文件是否已经存在：

```
# cd /etc/kerberosIV
# ls
README krb.conf          krb.realms
```

如果您发现了除此之外的其它文件(例如principal.* 或master_key) 已经存在, 请使用kdb_destroy 命令来销毁旧的数据库, 或者, 如果Kerberos 没有在运行, 简单地删除掉那些多余的文件。

现在必须编辑krb.conf 和krb.realms 文件来定义您的Kerberos 领域。在本例中, 这个领域将是EXAMPLE.COM 而其服务器是grunt.example.com。我们编辑或创建如下的krb.conf 文件:

```
# cat krb.conf
EXAMPLE.COM
EXAMPLE.COM grunt.example.com admin server
CS.BERKELEY.EDU okeeffe.berkeley.edu
ATHENA.MIT.EDU kerberos.mit.edu
ATHENA.MIT.EDU kerberos-1.mit.edu
ATHENA.MIT.EDU kerberos-2.mit.edu
ATHENA.MIT.EDU kerberos-3.mit.edu
LCS.MIT.EDU kerberos.lcs.mit.edu
TELECOM.MIT.EDU bitsy.mit.edu
ARC.NASA.GOV trident.arc.nasa.gov
```

在这个例子中, 除此之外的其它领域并不是必需的。把他们在这里一并展示是为了演示如何让机器了解多个领域的存在。简单起见, 在实际的配置中可以省略它们。

第一行命名了这个系统工作的领域。其它行包含了领域/主机的记录。每行的第一项是一个领域, 其后是在这个领域中充当“密钥分发中心”的主机名。其后的admin server 表示该主机同时还提供管理数据库服务。进一步的详细说明请参考Kerberos 联机手册。

现在应该添加grunt.example.com 到EXAMPLE.COM 领域, 同时追加一项以便将出现在EXAMPLE.COM 领域中.example.com 域的所有主机也加入进来。krb.realms 这个文件需要按照下面的方法修改:

```
# cat krb.realms
grunt.example.com EXAMPLE.COM
.example.com EXAMPLE.COM
.berkeley.edu CS.BERKELEY.EDU
.MIT.EDU ATHENA.MIT.EDU
.mit.edu ATHENA.MIT.EDU
```

再次强调, 其它领域并不是必需的。在这里只是要展示如何使用多个领域。可以删掉它们以简化配置。

第一行将指定的系统置于所指名字的领域内。这一行的其它部分则指明了特定子域内的主机应该默认属于哪个领域。

接下来我们就可以创建数据库了。只有在Kerberos 服务器上(或密钥分发中心上)才需要它。可以通过kdb_init 命令来完成这一步:

```
# kdb_init
Realm name [default ATHENA.MIT.EDU ]: EXAMPLE.COM
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
```

Enter Kerberos master key:

现在我们应该保存密钥, 这样本机上运行的其他服务就能够了解这一变化。用kstash 命令来完成这一步:

```
# kstash
```

```
Enter Kerberos master key:
```

```
Current Kerberos master key version is 1.
```

```
Master key entered. BEWARE!
```

这一操作将把主口令保存到/etc/kerberosIV/master_key。

14.7.3 让一切运转起来

有两个主要的东西需要被添加到要用Kerberos 来确保安全的每一个系统上。它们的名字是kpasswd和rcmd。这些程序允许另外系统改变Kerberos 的密码，在不同的系统上可能有不同的名字。

服务程序kpasswd 和rcmd 使得其他系统能够修改Kerberos 口令，以及执行类似rcp(1), rlogin(1) 和rsh(1) 这样的命令。

我们添加下面这些记录：

```
# kdb_edit
Opening database...

Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered. BEWARE!
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: passwd
Instance: grunt

<Not found>, Create [y] ? y

Principal: passwd, Instance: grunt, kdc_key_ver: 1
New Password: <---- enter RANDOM here
Verifying password

New Password: <---- enter RANDOM here

Random password [y] ? y

Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name: rcmd
Instance: grunt

<Not found>, Create [y] ?
```



```
Principal: rcmd, Instance: grunt, kdc_key_ver: 1
New Password: <---- enter RANDOM here
Verifying password

New Password:          <---- enter RANDOM here

Random password [y] ?

Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name:        <---- null entry here will cause an exit
```

14.7.4 创建服务器文件

现在需要分析在每台机器上定义的服务的所有情况。为了做到这一点，可以使用`ext_srvtab`命令。这将创建一个文件，它需要被通过安全的途径复制或移动到每一个Kerberos客户端的`/etc/kerberosIV`目录中。在每一台服务器上都必须存在这个文件，它对Kerberos的运行至关重要。

```
# ext_srvtab grunt
Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered. BEWARE!
Generating 'grunt-new-srvtab'....
```

现在，这个命令只产生一个临时文件，必须被重命名为`srvtab`以便所有的服务可以识别它。用`mv(1)`命令把它挪到原系统的这个位置：

```
# mv grunt-new-srvtab srvtab
```

如果文件是针对客户系统的，而且网络可能会不安全，则应把`client-new-srvtab`复制到可移动的介质上，并通过物理上安全的方式拿走。将其改名为`srvtab`并放到客户机的`/etc/kerberosIV`目录中，并赋予mode 600：

```
# mv grumble-new-srvtab srvtab
# chmod 600 srvtab
```

14.7.5 复制数据库

现在添加一些用户记录到数据库。首先为用户jane创建其对应的项。使用`kdb_edit`命令来完成此项工作：

```
# kdb_edit
Opening database...

Enter Kerberos master key:
```

```

Current Kerberos master key version is 1.

Master key entered.  BEWARE!
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: jane
Instance:

<Not found>, Create [y] ? y

Principal: jane, Instance: , kdc_key_ver: 1
New Password:          <---- enter a secure password here
Verifying password

New Password:          <---- re-enter the password here
Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name:      <---- null entry here will cause an exit

```

14.7.6 测试全部相关信息

首先必须启动Kerberos的服务程序。这里需要指出，如果您正确地修改了/etc/rc.conf 则系统在启动时会自动完成这个工作。只有在Kerberos服务器上才需要这么做。Kerberos 客户程序将自动地从/etc/kerberosIV 目录中的文件获取所需要的信息。

```

# kerberos &
Kerberos server starting
Sleep forever on error
Log file is /var/log/kerberos.log
Current Kerberos master key version is 1.

Master key entered.  BEWARE!

Current Kerberos master key version is 1
Local realm: EXAMPLE.COM
# kadmin -n &
KADM Server KADM0.0A initializing
Please do not use 'kill -9' to kill this job, use a
regular kill instead

Current Kerberos master key version is 1.

Master key entered.  BEWARE!

```

接下来应使用kinit 命令来获取与我们刚刚创建的ID jane 对应的ticket:

```
% kinit jane
```

```
MIT Project Athena (grunt.example.com)
Kerberos Initialization for "jane"
Password:
```

尝试使用`klist` 列出句柄以了解是否真的拥有它们:

```
% klist
Ticket file:      /tmp/tkt245
Principal:        jane@EXAMPLE.COM

    Issued            Expires            Principal
Apr 30 11:23:22  Apr 30 19:23:22  krbtgt.EXAMPLE.COM@EXAMPLE.COM
```

现在可以试试看用`passwd(1)` 来修改口令, 以验证`kpasswd` 服务程序是否能够从Kerberos 数据库中获得需要的授权:

```
% passwd
realm EXAMPLE.COM
Old password for jane:
New Password for jane:
Verifying password
New Password for jane:
Password changed.
```

14.7.7 授予su 特权

Kerberos 使我们能够给予每一个 需要使用root 特权的用户使用他们自己单独的 `su(1)` 口令。现在我们追加一个被授予`su(1)` 到root 权限的ID。这件事是由与root 相关联的一个principal 实例来控制的。使用`kdb_edit` 可以在Kerberos 数据库中建立一个`jane.root` 条目:

```
# kdb_edit
Opening database...

Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered.  BEWARE!
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: jane
Instance: root

<Not found>, Create [y] ? y

Principal: jane, Instance: root, kdc_key_ver: 1
New Password:          <---- enter a SECURE password here
Verifying password

New Password:          <---- re-enter the password here
```

```
Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ? 12 <--- Keep this short!
Attributes [ 0 ] ?
Edit O.K.
Principal name: <---- null entry here will cause an exit
```

现在试试看获得相应的句柄，以确认它已经正常工作了：

```
# kinit jane.root
MIT Project Athena (grunt.example.com)
Kerberos Initialization for "jane.root"
Password:
```

接下来我们需要把用户添加到root的.klogin 文件里：

```
# cat /root/.klogin
jane.root@EXAMPLE.COM
```

试试看su(1)：

```
% su
Password:
```

然后看看我们拥有哪些句柄：

```
# klist
Ticket file: /tmp/tkt_root_245
Principal: jane.root@EXAMPLE.COM

Issued                Expires                Principal
May  2 20:43:12    May  3 04:43:12    krbtgt.EXAMPLE.COM@EXAMPLE.COM
```

14.7.8 使用其它命令

在前文给出的例子中，我们创建了一个称为jane的用户，以及一个root实例。此处的用户名和它的principal相同，这是Kerberos默认的；一个形如<username>.root的<principal>.<instance>将允许<username>使用su(1)成为root，只要所需的那些条目在root home目录中的.klogin中存在的话：

```
# cat /root/.klogin
jane.root@EXAMPLE.COM
```

类似地，如果用户的home目录中有这样的设置：

```
% cat ~/.klogin
jane@EXAMPLE.COM
jack@EXAMPLE.COM
```

则表明在EXAMPLE.COM领域的经过身份验证的jane或者jack(通过kinit，详情见前文)能够使用jane的身份或系统(grunt)中的文件，无论通过rlogin(1), rsh(1)或是rcp(1)。

举例来说，jane现在通过Kerberos登入了其它系统：

```
% kinit
MIT Project Athena (grunt.example.com)
Password:
% rlogin grunt
Last login: Mon May  1 21:14:47 from grumble
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
    The Regents of the University of California.  All rights reserved.

FreeBSD BUILT-19950429 (GR386) #0: Sat Apr 29 17:50:09 SAT 1995
```

或者，当jack登录到jane在同一台机器上的账号(jane按照前面所介绍的那样配置了.klogin文件，而负责Kerberos的管理员，则为jack的principal配置了一个空的instance):

```
% kinit
% rlogin grunt -l jane
MIT Project Athena (grunt.example.com)
Password:
Last login: Mon May  1 21:16:55 from grumble
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
    The Regents of the University of California.  All rights reserved.

FreeBSD BUILT-19950429 (GR386) #0: Sat Apr 29 17:50:09 SAT 1995
```

14.8 Kerberos5

撰写者Tillman Hodgson. 原文来自Mark Murray.

在FreeBSD-5.1之后的每一个FreeBSD版本都只包含**Kerberos5**支持了，因而，**Kerberos5**是它们所包含的唯一的Kerberos版本，其配置在绝大多数方面和**KerberosIV**非常类似。下述信息只适用于FreeBSD-5.0之后版本中的**Kerberos5**。希望使用**KerberosIV**的用户可以安装security/krb4 port。

Kerberos是一组附加的网络系统/协议，用以让用户通过一台安全服务器提供的服务来验证身份。包括远程登录、远程复制、在系统间安全地复制文件，以及其它高危险性的操作，由于其存在而显著地提高了安全型并且更加可控。

Kerberos可以理解作为一种身份验证代理系统。它也被描述为一种以受信第三方为主导的身份验证系统。**Kerberos**只提供一种功能——在网络上安全地完成用户的身份验证。它并不提供授权功能(也就是说用户能够做什么操作)或审计功能(记录用户作了什么操作)。一旦客户和服务器都使用了**Kerberos**来证明各自的身份之后，他们还可以加密全部的通讯以保证业务数据的私密性和完整性。

因此，强烈建议将**Kerberos**同其它提供授权和审计服务的安全手段联用。

接下来的说明可以用来指导如何安装FreeBSD所附带的**Kerberos**。不过，您仍然需要参考相应的联机手册以获得完整的描述。

为了展示**Kerberos**的安装过程，我们约定：

- DNS域(“zone”)为example.org。
- **Kerberos**领域是EXAMPLE.ORG。

注意: 在安装**Kerberos**时请使用实际的域名即使您只是想在内部网上用一用。这可以避免DNS问题并保证了同其它**Kerberos**之间的互操作性。

14.8.1 历史

Kerberos 最早由MIT 作为解决网络安全问题的一个方案提出。**Kerberos** 协议采用了强加密，因此客户能够在不安全的网络上向服务器(以及相反地) 验证自己的身份。

Kerberos 是网络验证协议名字，同时也是用以表达实现了它的程序的形容词。(例如**Kerberos telnet**)。目前最新的协议版本是5，在RFC 1510 中有所描述。

该协议有许多免费的实现，这些实现涵盖了许多种不同的操作系统。最初研制**Kerberos** 的麻省理工学院(MIT) 也仍然在继续开发他们的**Kerberos** 软件包。在US 它被作为一种加密产品使用，因而历史上曾经受到US 出口管制。MIT **Kerberos** 可以通过port (security/krb5) 来安装和使用。Heimdal **Kerberos** 是另一种第5 版实现，并且明确地在US 之外的地区开发，以避免出口管制(因此在许多非商业的类UNIX 系统中非常常用。Heimdal **Kerberos** 软件包可以通过port (security/heimdal) 安装，最新的FreeBSD 的最小安装也会包含它。

为使尽可能多的读者从中受益，这份说明以FreeBSD 附带的Heimdal 软件包为准。

14.8.2 配置Heimdal KDC

密钥分发中心(KDC) 是**Kerberos** 提供的集中式验证服务——它是签发**Kerberos tickets** 的那台计算机。KDC 在**Kerberos** 领域中的其它机器看来是“受信的”，因此必须格外注意其安全性。

需要说明**Kerberos** 服务器只需要非常少的计算资源，尽管如此，基于安全理由仍然推荐使用独占的机器来扮演KDC 的角色。

要开始配置KDC，首先请确认您的/etc/rc.conf 文件包含了作为一个KDC 所需的设置(您可能需要适当地调整路径以适应自己系统的情况):

```
kerberos5_server_enable="YES"
kadmind5_server_enable="YES"
kerberos_stash="YES"
```

注意: kerberos_stash 只能在FreeBSD 4.X 上使用。

接下来需要修改**Kerberos** 的配置文件，/etc/krb5.conf:

```
[libdefaults]
    default_realm = EXAMPLE.ORG
[realms]
    EXAMPLE.ORG = {
        kdc = kerberos.example.org
        admin_server = kerberos.example.org
    }
[domain_realm]
    .example.org = EXAMPLE.ORG
```

请注意这个/etc/krb5.conf 文件假定您的KDC 有一个完整的主机名，即kerberos.example.org。如果您的KDC 主机名与它不同，则应添加一条CNAME (别名) 项到zone 中去。

注意: 对于有正确地配置过的BIND DNS 服务器的大型网络, 上述例子可以精简为:

```
[libdefaults]
    default_realm = EXAMPLE.ORG
```

将下面的内容加入到example.org zone 数据文件中:

```
_kerberos._udp      IN  SRV      01 00 88 kerberos.example.org.
_kerberos._tcp      IN  SRV      01 00 88 kerberos.example.org.
_kpasswd._udp       IN  SRV      01 00 464 kerberos.example.org.
_kerberos-adm._tcp  IN  SRV      01 00 749 kerberos.example.org.
_kerberos           IN  TXT       EXAMPLE.ORG
```

注意: 要让客户机能够找到Kerberos 服务, 就必须 首先配置完整或最小配置的/etc/krb5.conf 并且 正确地配置DNS 服务器。

接下来需要创建Kerberos 数据库。这个数据库包括了使用主密码加密的所有实体的密钥。您并不需要记住这个密码, 它会保存在一个文件(/var/heimdal/m-key)中。要创建主密钥, 需要执行kstash 并输入一个口令。

主密钥一旦建立, 您就可以用kadmin 程序的-l 参数(表示“local”)来初始化数据库了。这个选项让kadmin 直接地修改数据库文件而不是通过kadmind 的网络服务。这解决了在数据库创建之前连接它的鸡生蛋的问题。进入kadmin 提示符之后, 用init 命令来创建领域的初始数据库。

最后, 仍然在kadmin 中, 使用add 命令来创建第一个principal。暂时使用全部的默认设置, 随后可以在任何时候使用modify 命令来修改这些设置。另外, 也可以用? 命令来了解可用的选项。

典型的数据库创建过程如下:

```
# kstash
Master key: xxxxxxxx
Verifying password - Master key: xxxxxxxx

# kadmin -l
kadmin> init EXAMPLE.ORG
Realm max ticket life [unlimited]:
kadmin> add tillman
Max ticket life [unlimited]:
Max renewable life [unlimited]:
Attributes []:
Password: xxxxxxxx
Verifying password - Password: xxxxxxxx
```

现在是启动KDC 服务的时候了。运行/etc/rc.d/kerberos start 以及/etc/rc.d/kadmind start 来启动这些服务。尽管此时还没有任何正在运行的Kerberos 服务, 但您仍然可以通过获取并列出您刚刚创建的那个principal (用户) 的ticket 来验证KDC 确实在正常工作, 使用KDC 本身的功能:

```
% k5init tillman
tillman@EXAMPLE.ORG's Password:

% k5list
```

```
Credentials cache: FILE:/tmp/krb5cc_500
Principal: tillman@EXAMPLE.ORG
```

```
Issued          Expires          Principal
Aug 27 15:37:58 Aug 28 01:37:58 krbtgt/EXAMPLE.ORG@EXAMPLE.ORG
```

14.8.3 为Kerberos 启用Heimdal 服务

首先我们需要一份**Kerberos** 配置文件/etc/krb5.conf 的副本。只需简单地用安全的方式(使用类似scp(1) 的网络工具, 或通过软盘) 复制KDC 上的版本, 并覆盖掉客户机上的对应文件就可以了。

接下来需要一个/etc/krb5.keytab 文件。这是提供**Kerberos** 服务的服务器和工作站的一个主要区别——服务器必须有keytab 文件。这个文件包括了服务器的主机密钥, 这使得KDC 得以验证它们的身份。此文件必须以安全的方式传到服务器上, 因为如果密钥被公之于众, 则安全也就毁于一旦。也就是说, 通过明文的通道, 例如FTP 是非常糟糕的想法。

一般来说, 您会希望使用kadmin 程序来把keytab 传到服务器上。由于也需要使用kadmin 来为主机建立principal (KDC 一端的krb5.keytab), 因此这并不复杂。

注意您必须已经获得了一个ticket 而且这个ticket 必须许可使用kadmind.acl 中的kadmin 接口。请参考Heimdal info 中的“Remote administration(远程管理)”一节(info heimdal) 以了解如何设计访问控制表。如果不希望启用远程的kadmin 操作, 则可以简单地采用安全的方式连接KDC (通过本机控制台, ssh(1) 或**Kerberos** telnet(1)) 并使用kadmin -l 在本地执行管理操作。

安装了/etc/krb5.conf 文件之后, 您就可以使用**Kerberos** 上的kadmin 了。add --random-key 命令可以用于添加主机principal, 而ext 命令则允许导出服务器的主机principal 到它的keytab 中。例如:

```
# kadmin
kadmin> add --random-key host/myserver.example.org
Max ticket life [unlimited]:
Max renewable life [unlimited]:
Attributes []:
kadmin> ext host/myserver.example.org
kadmin> exit
```

注意ext 命令(这是“extract” 的简写) 默认会把导出的密钥放到/etc/krb5.keytab 中。

如果您由于没有在KDC 上运行kadmind (例如基于安全理由) 因而无法远程地使用kadmin 您可以直接在KDC 上添加主机principal (host/myserver.EXAMPLE.ORG) 随后将其导出到一个临时文件中(以免覆盖KDC 上的/etc/krb5.keytab), 方法是使用下面的命令:

```
# kadmin
kadmin> ext --keytab=/tmp/example.keytab host/myserver.example.org
kadmin> exit
```

随后需要把keytab 复制到服务器上(例如使用scp 或软盘)。一定要指定一个不同于默认的keytab 名字以免覆盖KDC 上的keytab。

到现在您的服务器已经可以同KDC 通讯了(因为已经配置了krb5.conf 文件), 而且它还能够证明自己的身份(由于配置了krb5.keytab 文件)。现在可以启用一些**Kerberos** 服务。在这个例子中, 我们将在/etc/inetd.conf 中添加下面的行来启用telnet 服务, 随后用/etc/rc.d/inetd restart 重启inetd(8) 服务来使设置生效:


```
telnet stream tcp nowait root /usr/libexec/telnetd telnetd -a user
```

关键的部分是 `-a` (表示验证) 类型设置为用户(user)。请参考telnetd(8) 联机手册以了解细节。

14.8.4 使用Heimdal 来启用客户端Kerberos

设置客户机是非常简单的。在正确配置了 **Kerberos** 的网络中, 只需要将位于 `/etc/krb5.conf` 的配置文件进行一下设置就可以了。这一步骤可以简单地通过安全的方式将文件从KDC 复制到客户机上来完成。

尝试在客户机上执行 `kinit`、`klist`, 以及 `kdestroy` 来测试获取、显示并删除刚刚为principal 建立的ticket 是否能够正常进行, 如果能, 则用其它的 **Kerberos** 应用程序来连接启用了 **Kerberos** 的服务。如果应用程序不能正常工作而获取ticket 正常, 则通常是服务本身, 而非客户机或KDC 有问题。

在测试类似telnet 的应用程序时, 应考虑使用抓包程序(例如tcpdump(1)) 来确认您的口令没有以明文方式传输。尝试使用telnet 的 `-x` 参数, 它将加密整个数据流(类似ssh)。

核心的 **Kerberos** 客户端应用(按照传统命名, 包括了 `kinit`、`klist`、`kdestroy`, 以及 `kpasswd`) 已经随基本的FreeBSD 安装到了系统上。请注意5.0 之前的FreeBSD 版本将它们改名为 `k5init`、`k5list`、`k5destroy`、`k5passwd`, 以及 `k5stash` (尽管这些命令通常只会用到一次)。

许多非核心的 **Kerberos** 客户应用程序也是默认安装的。在Heimdal 的“最小” 安装理念下, telnet 是唯一一个采用了 **Kerberos** 的服务。

Heimdal port 则提供了一些默认不安装的客户应用程序, 例如启用了 **Kerberos** 版本的 `ftp`、`rsh`、`rcp`、`rlogin` 以及一些更不常用的程序。MIT port 也包括了一整套 **Kerberos** 客户应用程序。

14.8.5 用户配置文件: .k5login 和.k5users

在某个领域中的用户往往都有自己的 **Kerberos** principal (例如 `tillman@EXAMPLE.ORG`) 并映射到本机用户帐户(例如本机上名为 `tillman` 的帐户)。客户端应用程序, 如telnet 通常并不需要用户名或principal。

不过, 有时您可能会需要赋予某些没有匹配 **Kerberos** principal 的人使用本地用户帐户的权限。例如 `tillman@EXAMPLE.ORG` 可能需要访问本地的 `webdevelopers` 用户帐号。其它principal 可能也会需要访问这个本地帐号。

用户home 目录中的 `.k5login` 和 `.k5users` 这两个文件可以配合 `.hosts` 和 `.rhosts` 来有效地解决这个问题。例如, 如果 `.k5login` 中有如下内容:

```
tillman@example.org
jdoe@example.org
```

并放到了本地用户 `webdevelopers` 的home 目录中, 则列出的两个principals 都可以使用那个帐号, 而无须共享口令。

建议您在开始实施之前首先阅读这些命令的联机帮助。特别地, `ksu` 的联机手册包括了 `.k5users` 的相关内容。

14.8.6 Kerberos 提示、技巧和故障排除

- 当使用Heimdal 或MIT **Kerberos** ports 时, 需要确认PATH 环境变量把 **Kerberos** 客户应用列在系统自带的版本之前。

- 同一领域内的所有计算机的时间设置是否同步？如果不是的话，则身份验证可能会失败。第25.11节描述了如何使用NTP来同步时钟。
- MIT和Heimdal能够很好地互操作。一个例外是kadmin，因为这个协议没有被标准化。
- 如果您改变了主机名，您还需要修改您的host/ principal并更新keytab。这一规律也适用于类似Apache的www/mod_auth_kerb所使用的www/ principal这样的特殊keytab项。
- 您的领域中的每一台主机必须在DNS(或至少在/etc/hosts中)可以解析(同时包括正向和反向)。CNAME能够正常使用，但必须有正确的对应A和PTR记录。此时给出的错误信息可能很让人困惑：Kerberos5 refuses authentication because Read req failed: Key table entry not found。
- 某些作为客户使用您的KDC的操作系统可能没有将ksu设置为setuid root的权限。这意味着ksu将不能够正常工作，从安全角度说这是一个不错的主意，但可能令人烦恼。这类问题并不是KDC的错误。
- 使用MIT Kerberos时，如果希望允许一个principal拥有超过默认的十小时有效期的ticket则必须使用kadmin中的modify_principal来修改principal本身以及krbtgt的maxlife(最大有效期)。此后，principal可以使用kinit的-l参数来请求一个有更长有效期的ticket。
-

注意：如果在KDC上运行了听包程序，并在工作站上执行kinit，您可能会注意到TGT是在kinit一开始执行的时候就发出了的——甚至在您输入口令之前！关于这个现象的解释是Kerberos服务器可以无限制地收发TGT (Ticket Granting Ticket) 给任何未经授权的请求；但是，每一个TGT都是使用用户的口令派生出来的密钥进行加密的。因此，当用户输入口令时它并不会发送给KDC，而是直接用于解密kinit所拿到的TGT。如果解密过程得到了一个包含合法的时间戳的有效ticket，则说明用户的Kerberos凭据有效。这些凭据包含了一个会话密钥用以在随后建立Kerberos服务器的加密通讯，传递由服务器自己的私钥加密的实际的ticket-granting ticket。这个第二层加密对于用户来说是看不到的，但它使得Kerberos服务器能够验证每一个TGT的真实性。

- 如果需要有效期更长的ticket(例如一周)而且您使用OpenSSH连接保存您的ticket的机器，请确认sshd_config中的Kerberos TicketCleanup被设置为no 否则在注销时会自动删除所有的ticket。
- 切记主机的principals的ticket有效期一定要比用户的长。如果您的用户principal的有效期是一周，而所连接的主机的有效期是九个小时，则缓存的主机principal将先行过期，结果是ticket缓存无法正常工作。
- 当配置krb5.dict文件来防止使用特定的简单口令(kadmind的联机手册中简要介绍了它)，请切记只有指定了口令策略的principals才会使用它们。krb5.dict文件的格式很简单：每个串占一行。创建一个到/usr/share/dict/words的符号连接会很有用。

14.8.7 与MIT port 的区别

MIT和Heimdal主要的区别在于kadmin程序使用不同(尽管等价)的命令和协议。如果您的KDC是MIT的，则其影响是不能使用Heimdal的kadmin程序来远程管理KDC(或相反)。

完成同样工作的命令可能会有些许的不同。推荐按照MIT Kerberos的网站(<http://web.mit.edu/Kerberos/www/>)上的说明来操作。请小心关于路径的问题，MIT port会默认安装到/usr/local/，您因此可能会执行“普通的”系统应用程序而非MIT，如果您的PATH环境变量把系统目录放在前面的话。

注意: 如果使用FreeBSD提供的MIT security/krb5 port, 一定要仔细阅读port所安装的/usr/local/share/doc/krb5/README.FreeBSD, 如果您想知道为什么通过telnetd和klogind登录时会出现一些诡异的现象的话。最重要地, “incorrect permissions on cache file(缓存文件权限不正确)”行为需要使用login.krb5来进行验证, 才能够正确地修改转发凭据的属主。

14.8.8 缓解Kerberos的限制

14.8.8.1 Kerberos 是一种all-or-nothing 方式

在网络上启用的每个服务都必须进行修改以便让其能够配合**Kerberos**工作(否则就只能使用其它方法来保护它们不受网络攻击的侵害), 如果不是这样, 则用户的凭据就有可能被窃取并再次使用。一个例子是对所有的远程shell(例如通过rsh和telnet)启用了**Kerberos**但没有将使用明文验证的POP3邮件服务器Kerberos化。

14.8.8.2 Kerberos 是为单用户工作站设计的

在多用户环境中**Kerberos**的安全性会被削弱。这是因为它把ticket保存到/tmp目录中, 而这个目录可以被任何用户读取。如果有用户与其它人同时共享一台计算机(也就是multi-user), 则这个用户的ticket就可能被其它用户窃取(复制)。

可以通过使用-c 文件名这样的命令行选项, 或者(推荐的)改变KRB5CCNAME环境变量来避免这个问题, 但很少有人这么做。原则上, 将ticket保存到用户的home目录并简单地设置权限就能够缓解这个问题。

14.8.8.3 KDC 会成为单点崩溃故障点

根据设计, KDC必须是安全的, 因为主密码数据库保存在它上面。决不应该在KDC上面运行其它服务, 而且还应确保它的物理安全。由于**Kerberos**使用同一个密钥(传说中的那个“主”密钥)来加密所有的密码, 而将这个文件保存在KDC, 因此其安全尤为重要。

不过, 主密钥的泄露并没有想象中的那么可怕。主密钥只用来加密**Kerberos**数据库以及产生随机数发生器的种子。只要KDC是安全的, 即使攻击者拿到了主密钥也做不了什么。

另外, 如果KDC不可用(例如由于拒绝服务攻击或网络故障)则网络服务将由于验证服务无法进行而不能使用, 从而导致更大范围的拒绝服务攻击。通过部署多个KDC(一个主服务器, 配合一个或多个从服务器)并采用经过仔细设计和实现的备用验证方式可以避免这种问题(PAM是一个不错的选择)。

14.8.8.4 Kerberos 的不足

Kerberos允许用户、主机和服务之间进行相互认证。但它并没有提供机制来向用户、主机或服务验证KDC。这意味着种过木马的程序, 例如kinit有可能记录用户所有的用户名和密码。尽管如此, 可以用类似security/tripwire这样的文件系统完整性检查工具来避免此类情况的发生。

14.8.9 相关资源和其它资料

- The **Kerberos** FAQ (<http://www.faqs.org/faqs/Kerberos-faq/general/preamble.html>)
- Designing an Authentication System: a Dialog in Four Scenes (<http://web.mit.edu/Kerberos/www/dialogue.html>)
- RFC 1510, The **Kerberos** Network Authentication Service (V5) (<http://www.ietf.org/rfc/rfc1510.txt?number=1510>)
- MIT **Kerberos** home page (<http://web.mit.edu/Kerberos/www/>)
- Heimdal **Kerberos** home page (<http://www.pdc.kth.se/heimdal/>)

14.9 OpenSSL

作者Tom Rhodes.

许多用户可能并没有注意到FreeBSD所附带的**OpenSSL**工具包的功能。**OpenSSL**提供了建立在普通的通讯层基础上的加密传输层；这些功能为许多网络应用和服务程序所广泛使用。

对**OpenSSL**的一些常见用法包括加密邮件客户的身份验证过程，基于Web的交易如信用卡等等。许多ports如www/apache13-ssl，以及mail/sylpheed-claws等等都提供了编译进**OpenSSL**支持的方法。

注意：绝大多数情况下Ports Collection会试图使用security/openssl除非明确地将WITH_OPENSSL_BASE make变量设置为“yes”。

FreeBSD中附带的**OpenSSL**版本能够支持安全套接字层v2/v3 (SSLv2/SSLv3) 和安全传输层v1 (TLSv1) 三种网络协议，并可作为通用的密码学函数库使用。

注意：尽管**OpenSSL**支持IDEA算法，但由于美国专利，它在默认情况下是不编译的。如果想使用它，请查阅相应的授权，如果认为授权可以接受，则可以在make.conf中设置MAKE_IDEA。

为应用软件提供证书是**OpenSSL**最为常用的功能之一。证书是一种能够确保公司或个人有效身份不被伪造的凭据。如果证书没有被众多“权威发证机构”，或CA中的某一个确认，则会产生一个警告。权威发证机构通常是一家公司，例如VeriSign (<http://www.verisign.com>)，它能够通过签署来证明个人或公司证书的有效性。这个过程是需要付费的，当然，这不是使用证书的必要条件；然而，这样做会让那些比较偏执的用户感到轻松。

14.9.1 生成证书

为了生成证书，需要使用下面的命令：

```
# openssl req -new -nodes -out req.pem -keyout cert.pem
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'cert.pem'
-----
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
Country Name (2 letter code) [AU]:us
State or Province Name (full name) [Some-State]:PA
Locality Name (eg, city) []:Pittsburgh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:Systems Administrator
Common Name (eg, YOUR name) []:localhost.example.org
Email Address []:trhodes@FreeBSD.org
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:SOME PASSWORD
An optional company name []:Another Name
```

请注意，在“Common Name”提示后面我们输入的是一个域名。这个提示要求输入服务器的名字，这个名字今后将用于完成验证过程；如果在这里输入域名以外的内容，那么证书也就失去其意义了。您还可以指定一些其他的选项，比如证书的有效期，以及使用的加密算法等等。这些选项的完整列表，可以在`openssl(1)`联机手册中找到。

在您执行前述命令的目录中将生成两个文件。证书申请，即`req.pem`，可以发给一家发证机构，它将验证您输入的凭据的真实性，并对申请进行签名，再把证书返还给您。第二个文件的名称将是`cert.pem`，它包含了证书的私钥，应被全力保护；如果它落入别人手中，则可以被用来伪造您(或您的服务器)。

如果不需要来自CA的签名，也可以创建自行签名的证书。首先，需要生成RSA密钥：

```
# openssl dsaparam -rand -genkey -out myRSA.key 1024
```

接下来，生成CA密钥：

```
# openssl gendsa -des3 -out myca.key myRSA.key
```

然后用这个密钥来创建证书：

```
# openssl req -new -x509 -days 365 -key myca.key -out new.crt
```

上述步骤将在当前目录中生成两个新文件：一个是权威发证机构的签名文件，`myca.key`；另一个是证书本身，`new.crt`。这些文件应该放到同一个目录中，一般而言，推荐放到`/etc`，并且只允许`root`读取。建议把权限设置为0700，这可以通过`chmod`工具来完成。

14.9.2 使用证书的一个例子

那么有了这些文件可以做些什么呢？一个比较典型的用法是用来加密Sendmail MTA的通讯连接。这可以解决用户通过本地MTA发送邮件时使用明文进行身份验证的问题。

注意：这个用法可能并不完美，因为某些MUA会由于没有在本机安装证书而向用户发出警告。请参考那些软件的说明了解关于安装证书的信息。

下面的设置应添加到本地的.mc 文件

```
dn1 SSL Options
define('confCACERT_PATH','/etc/certs')dn1
define('confCACERT','/etc/certs/new.crt')dn1
define('confSERVER_CERT','/etc/certs/new.crt')dn1
define('confSERVER_KEY','/etc/certs/myca.key')dn1
define('confTLS_SRV_OPTIONS','V')dn1
```

这里，/etc/certs/ 是准备用来在本地保存证书和密钥的位置。最后，需要重新生成本地的.cf 文件。这一工作可以简单地通过在/etc/mail 目录中执行make install 来完成。接下来，可以使用make restart 来重新启动Sendmail 服务程序。

如果一切正常的话，在/var/log/maillog 中就不会出现错误提示，Sendmail 也应该出现在进程列表中。

做一个简单的测试，使用telnet(1) 来连接邮件服务器：

```
# telnet example.com 25
Trying 192.0.34.166...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP Sendmail 8.12.10/8.12.10; Tue, 31 Aug 2004 03:41:22 -0400 (EDT)
ehlo example.com
250-example.com Hello example.com [192.0.34.166], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH LOGIN PLAIN
250-STARTTLS
250-DELIVERBY
250 HELP
quit
221 2.0.0 example.com closing connection
Connection closed by foreign host.
```

如果输出中出现了“STARTTLS” 则说明一切正常。

14.10 IPsec 上的VPN

撰写者Nik Clayton.

使用FreeBSD 网关在两个被Internet 分开的网络之间架设VPN。

14.10.1 理解IPsec

撰写者Hiten M. Pandya.

这一节将指导您完成架设IPsec，并在一个包含了FreeBSD和Microsoft Windows 2000/XP机器的网络中使用它来进行安全的通讯的全过程。为了配置IPsec，您应当熟悉如何编译一个定制的内核的一些概念(参见第8章)。

IPsec 是一种建立在Internet协议(IP)层之上的协议。它能够让两个或更多主机以安全的方式来通讯(并因此而得名)。FreeBSD IPsec “网络协议栈” 基于KAME (<http://www.kame.net/>) 的实现，它支持两种协议族，IPv4 和IPv6。

注意: FreeBSD 5.X 包括了采用“硬件加速的” IPsec 协议栈，也称作“Fast IPsec”，它来自OpenBSD。它能够通过crypto(4)子系统来利用加密硬件(只要可能)优化IPsec的性能。这个子系统是新的，暂时还不支持KAME版本的IPsec的全部功能。此外，为了启用硬件加速的IPsec，必须把下面的选项加入到内核配置中：

```
options    FAST_IPSEC    # new IPsec (cannot define w/ IPSEC)
```

需要注意的是，目前还不能“Fast IPsec”子系统完全替代KAME的IPsec实现。请参见联机手册fast_ipsec(4)以了解进一步的详情。

IPsec 包括了两个子协议：

- **Encapsulated Security Payload (ESP)**, 保护IP包数据不被第三方介入，通过使用对称加密算法(例如Blowfish、3DES)。
- **Authentication Header (AH)**, 保护IP包头不被第三方介入和伪造，通过计算校验和以及对IP包头的字段进行安全散列来实现。随后是一个包含了散列值的附加头，以便能够验证包。

ESP和AH可以根据环境的不同，分别或者一同使用。

IPsec既可以用来直接加密主机之间的网络通讯(也就是**传输模式**)；也可以用来在两个子网之间建造“虚拟隧道”用于两个网络之间的安全通讯(也就是**隧道模式**)。后一种更多的被称之为**虚拟专用网(VPN)**。ipsec(4)联机手册提供了关于FreeBSD中IPsec子系统的详细信息。

要把IPsec支持放进内核，应该在配置文件中加入下面的选项：

```
options    IPSEC          #IP security
options    IPSEC_ESP      #IP security (crypto; define w/ IPSEC)
```

如果需要IPsec的调试支持，还应增加：

```
options    IPSEC_DEBUG    #debug for IP security
```

14.10.2 问题

由于对如何建立VPN并不存在标准，因此VPN可以采用许多种不同的技术来实现，每种技术都有其长处和弱点。这篇文章讲展现一个具体的应用情景，并为它设计了适合的VPN。

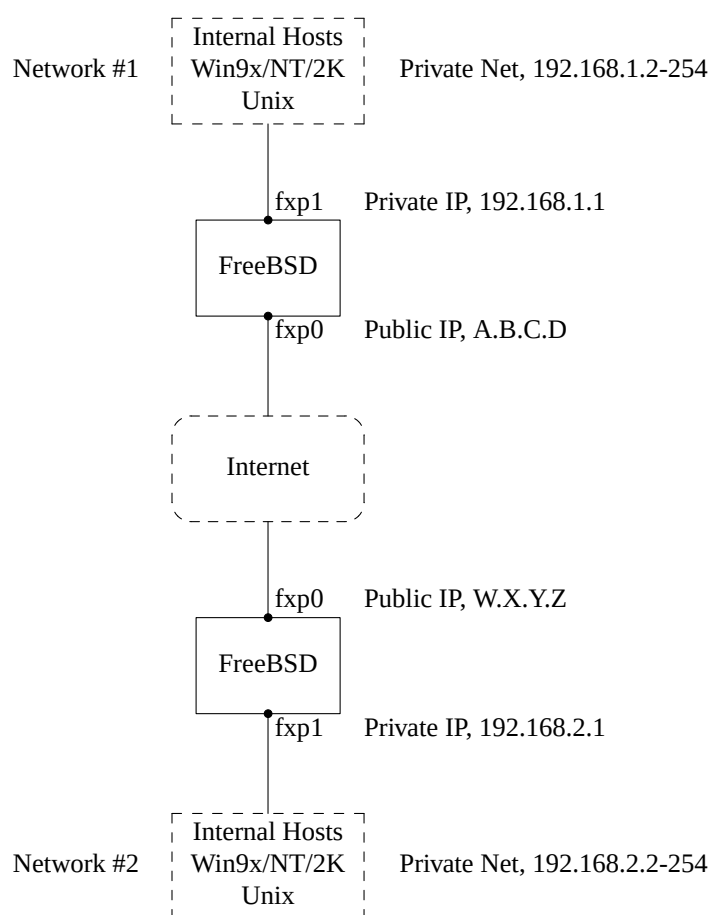
14.10.3 情景：两个网络都接入了Internet，希望像一个网络那样工作

现有条件如下：

- 至少有两个不同的站点
- 每个站点都使用内部的IP
- 两个站点都通过运行FreeBSD 的网关接入Internet。
- 每个网络上的网关至少有一个公网的IP 地址。
- 网络的内部地址可以是公网或私有的IP 地址，这并不是问题。如果需要，还可以在网关上运行NAT。
- 两个网络上的IP 地址不冲突。虽然理论上可以通过VPN 和NAT 连用来使这种情况能够正常工作，但那毫无疑问将是管理的噩梦。

如果您发现您正打算连接两个内网使用同一私有IP 地址范围的网络(例如它们都使用192.168.1.x)，则其中的一个必须修改网络地址。

网络的拓扑结构如下：



请注意两个公网IP 地址。在这篇文章的其余部分我将用这些字母来表示它们。在文章中看到这些字母的时候，请把它们换成自己的公网IP 地址。另外，在内部，两个网关都是使用的.1 的IP地址，而两个网络使用了不同的私有IP 地址(相应地，192.168.1.x 和192.168.2.x)。所有私有网络上的机器都被配置为使用.1 这台机器作为它们的网关。

我们希望，从网络的观点看，每一个网络上的机器都应该能够像在直接连接到同一路由器上一样看到对方网络上的机器-- 尽管可能比路由器略慢一些，并且有时会有丢包的现象。

这意味着(举例来说)，主机192.168.1.20 应该能够运行

```
ping 192.168.2.34
```

并且这能够透明地工作。Windows 机器应该能够看到其他网络上的机器，浏览文件共享，等等，就像在本地网络上一样。

而且这些事情必须是安全的，也就是说两个网络之间的通讯必须加密。

在两个网络之间建立VPN 可以分为几步。这些步骤包括：

1. 在两个网络之间，通过Internet 建立一个“虚拟的”网络连接。使用类似ping(8) 这样的工作来验证它是否正常工作。
2. 在两个网络之间应用安全策略以保证它们之间的通讯被透明地加密盒解密。可以使用tcpdump(1) 或类似的工具来验证这一点。
3. 在FreeBSD 网关上配置其他软件，让Windows 机器能够通过VPN 看到另一个网络中的机器。

14.10.3.1 步骤1：建立并测试“虚拟的”网络连接

假设您目前已经登录到了网络#1 的网关机上(其公网IP 地址是A.B.C.D，私网IP 地址是192.168.1.1)，则您可以执行ping 192.168.2.1，这是公网IP 为W.X.Y.Z 的私网地址。需要做什么实现上述功能呢？

1. 作为网关的机器需要知道如何能够到达192.168.2.1。换言之，它需要一条通往192.168.2.1 的路由。
2. 私网IP 地址，例如192.168.x 这样的地址是不应在Internet 上面大量出现的。于此相反，发送到192.168.2.1 的数据包将会封装到另外的包中。这样的包对外展现的应该是来自A.B.C.D，并被发到W.X.Y.Z 去。这个过程称为封装。
3. 一旦包到达了W.X.Y.Z 就需要对其“拆封”，并传递给192.168.2.1。

可以把上述过程理解为在两个网络间建立了一个“隧道”。两个“隧道口”是IP 地址A.B.C.D 和W.X.Y.Z，而隧道必须被告知哪些私有地址可以自由地在其中通过。隧道被用来在公共的Internet 上传递私有的IP 数据。

在FreeBSD 上，隧道可以通过一般的网络接口，或gif 来建立。您也许已经猜到了，每一台网关机的gif 接口需要配置四个IP 地址；两个是公网IP 地址，另两个则是私网IP 地址。

对于gif 设备的支持必须在两台网关机上编译进FreeBSD 内核。可以通过添加下面的设置来达到目的：

```
device gif
```

到两边的内核配置文件中，并重新编译、安装和启动它们。

配置隧道可以分为两步来完成。首先隧道必须被告知外部的(或公网的) IP 地址，可以通过gifconfig(8) 来完成这步。私网IP 地址则必须使用ifconfig(8) 来配置。

注意：在FreeBSD 5.X 中，gifconfig(8) 的功能已经并入ifconfig(8)。

在网络#1 的网关机上可以通过下面的两个命令来配置隧道。

```
gifconfig gif0 A.B.C.D W.X.Y.Z
ifconfig gif0 inet 192.168.1.1 192.168.2.1 netmask 0xffffffff
```

在另一边也需要做类似的设置，只是IP 地址的顺序是反过来的。

```
gifconfig gif0 W.X.Y.Z A.B.C.D
ifconfig gif0 inet 192.168.2.1 192.168.1.1 netmask 0xffffffff
```

随后执行：

```
gifconfig gif0
```

可以查看当前的配置情况。例如，在网络#1 的网关上您应该能够看到：

```
# gifconfig gif0
gif0: flags=8011<UP,POINTTOPOINT,MULTICAST> mtu 1280
inet 192.168.1.1 --> 192.168.2.1 netmask 0xffffffff
physical address inet A.B.C.D --> W.X.Y.Z
```

如您所见，虽然到已经在物理地址A.B.C.D 和W.X.Y.Z 之间建立起来，而允许通过隧道的地址则是192.168.1.1 到192.168.2.1 这个范围。

这同时会在两边机器的路由表中加入一项，可以通过netstat -rn 来观察。来自网络#1的网关机的输出如下。

```
# netstat -rn
Routing tables

Internet:
Destination      Gateway          Flags    Refs      Use    Netif  Expire
...
192.168.2.1      192.168.1.1    UH        0         0      gif0
...
```

正如“Flags” 的值所显示的那样，这是一个主机路由，这意味着每一个网关都知道如何到达另一端的网关，但它们现在还不知道如何到达对方的网络。我们接下来立刻解决这个问题。

您很可能在两台机器上都在运行防火墙。这需要作一些变动，以便适应VPN 的需要。一般来说会希望两个网络相互传递数据包，或者通过防火墙来隔离两边的危险。

如果您将防火墙配置为允许两边的网络传输通过，则测试工作会简单不少。随后您可以随时将限制变得更严格一些。假如您在网关上使用ipfw(8) 则下面的命令

```
ipfw add 1 allow ip from any to any via gif0
```

将允许两端点的VPN 数据通过，而不影响其他防火墙策略。很显然，您需要在两个网关上都执行上述命令。

现在已经可以让两台机器相互ping 了。在192.168.1.1 您应该能够正常执行

```
ping 192.168.2.1
```

并得到回应。对于另一台网关来说也是一样。

然而，到目前为止仍然还无法连上另一网络上的内部主机。原因是路由-- 尽管网关机知道如何到达对方那里，但它们都不知道如何到达对方后面的网络。

要解决这个问题，就必须在两边都添加一条静态路由。可以在第一台网关上执行：

```
route add 192.168.2.0 192.168.2.1 netmask 0xffffffff00
```

这相当于是说“为了到达192.168.2.0子网的机器，需要把包发给192.168.2.1”。您需要在另一个网关上也执行类似的命令，但使用192.168.1.x的地址。

来自一个网络上的IP访问现在能够抵达对面的网络了。

在两个网络之间建立VPN的过程已经完成了三分之二，它现在已经是“虚拟的”“网络”，然而它还不够专用。您可以使用ping(8)和tcpdump(1)来进行测试，并记录两边收发的数据包

```
tcpdump dst host 192.168.2.1
```

接下来登录到本机的另一个会话

```
ping 192.168.2.1
```

您将在输出中发现

```
16:10:24.018080 192.168.1.1 > 192.168.2.1: icmp: echo request
16:10:24.018109 192.168.1.1 > 192.168.2.1: icmp: echo reply
16:10:25.018814 192.168.1.1 > 192.168.2.1: icmp: echo request
16:10:25.018847 192.168.1.1 > 192.168.2.1: icmp: echo reply
16:10:26.028896 192.168.1.1 > 192.168.2.1: icmp: echo request
16:10:26.029112 192.168.1.1 > 192.168.2.1: icmp: echo reply
```

如您所见，ICMP消息在收发的过程中都没有加密。如果使用了-s参数来运行tcpdump(1)，甚至可以得到包中的更多信息以及其中的数据。

很明显这是不能接受的。下一节将讨论如何让两个网络之间的连接更安全，这件事是通过对通讯实施加密来完成的。

小结：

- 在两边的内核中配置“device gif”。
- 编辑网关#1上的/etc/rc.conf并将下面的行添加进去(根据需要改IP)。

```
gifconfig_gif0="A.B.C.D W.X.Y.Z"
ifconfig_gif0="inet 192.168.1.1 192.168.2.1 netmask 0xffffffff"
static_routes="vpn"
route_vpn="192.168.2.0 192.168.2.1 netmask 0xffffffff00"
```

- 在两台机器上编辑防火墙脚本(/etc/rc.firewall，或类似的名字)在其中加入
ipfw add 1 allow ip from any to any via gif0
- 在网络#2的网关机上也对/etc/rc.conf做同样的修改，注意把IP地址倒过来。

14.10.3.2 步骤2: 对连接实施安全加固

为了加密连接通讯将用到IPsec。IPsec提供了一种机制,使得两台主机协商一个加密密钥,并使用它加密之间的通讯。

在配置时有两个地方需要考虑。

1. 必须有能够让两台主机协商所采用的加密方式的机制。一旦双方确认了这机制,则称他们之间建立了“安全关联”。
2. 必须采用某种机制来指定哪些通讯需要加密。很明显地,通常并不需要所有的发出数据都被加密--一般只需要加密在VPN上传输的那些数据。这类决定哪些数据被加密的规则被称为“安全策略”。

安全关联和安全策略都是由内核来维护的,并可以通过用户态的程序来修改。在能够这样做之前,首先需要配置内核来让它支持IPsec和安全载荷封装(ESP)协议。配置下面的内核选项

```
options IPSEC
options IPSEC_ESP
```

然后重新编译、安装最后重新启动新的内核。在继续进行设置之前,您需要在两台网关上都进行同样的设置。

在建立安全关联时有两种选择。一种方法是完全手工地在两台主机之间选择加密算法、密钥等等,另一种方法是使用实现了Internet密钥交换协议(IKE)的服务程序来帮您完成这些任务。

我们推荐后者。不说别的,它配置起来要容易得多。

用setkey(8)可以编辑和显示安全策略。打个比方, setkey 之于内核的安全策略表,就相当于route(8)之于内核中的路由表。setkey 还可以显示当前的安全关联,这一点和netstat -r 类似。

在FreeBSD上可供选择的用于管理安全关联的服务程序有很多。这篇文章将介绍其中的一种, racoon —— 它可以从FreeBSD的Ports collection中的security/ipsec-tools安装。

racoon 软件,必须在两台网关机上都运行。需要配置VPN另一端的IP,以及一个密钥(这个密钥可以任意选择,但两个网关上的密钥必须一致)。

两端的服务程序将相互通讯,并确认它们各自的身份(使用刚刚配置的密钥)然后服务程序将生成一个新的密钥,并用它来加密VPN上的数据通讯。它们定期地改变密钥,因此即使供给者破解了一个密钥(虽然这在理论上并不十分可行)他也得不到什么--破解密钥的时候,已经产生一组新的密钥了。

racoon 的配置文件是存放在\${PREFIX}/etc/racoon 目录中的。在那里应该能够找到一个配置文件,不需要修改太多的设置。racoon 配置的另一部分,也就是需要修改的内容,是“预先配置的共享密钥”。

默认的racoon 配置应该可以在\${PREFIX}/etc/racoon/psk.txt 这个文件中找到。需要强调的是,这个密钥并非用于加密VPN连接的密钥,他们只是密钥管理服务程序用以信任对方的一种凭据。

psk.txt 包含了需要打交道的每一个远程站点。在本例中一共有两个站点,每一个psk.txt 都只有一行(因为每个VPN接入点都只和一个端点连接)。

在网关机#1上应该是:

```
W.X.Y.Z          secret
```

这包括了远程站点的公网IP地址,空格,以及提供秘密的字符串。很明显不应使用“secret”作为实际的密钥--通常的口令选择策略在这里也适用。

在网关#2上对应的配置是

A.B.C.D secret

也就是说，对面端的公网IP 地址，以及同样的密钥。psk.txt 的权限必须是0600 (也就是说，只有root 能够读写) 否则racoon 将不能运行。

两边的机器上都必须执行racoon。另外，还需要增加一些防火墙规则来允许IKE 通讯通过，它是通过UDP 在ISAKMP (Internet 安全关联密钥管理协议) 端口上运行的协议。再次强调，这个规则应该在规则集尽可能早的位置出现。

```
ipfw add 1 allow udp from A.B.C.D to W.X.Y.Z isakmp
ipfw add 1 allow udp from W.X.Y.Z to A.B.C.D isakmp
```

一旦racoon 开始运行，就可以开始测试让网关进行相互的ping 了。此时连接还没有进行加密，但racoon 将在两个主机之间建立安全关联-- 这可能需要一段时间，对您来说，具体的现象则是在ping 命令开始响应之前会有短暂的延迟。

一旦安全关联建立之后，就可以使用setkey(8)；来查看它了。在两边的网关上执行

setkey -D

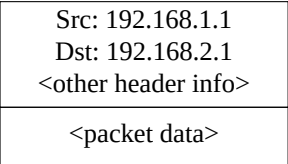
就可以看到安全关联的相关信息了。

现在只完成了一半的工作。另一半是设置安全策略。

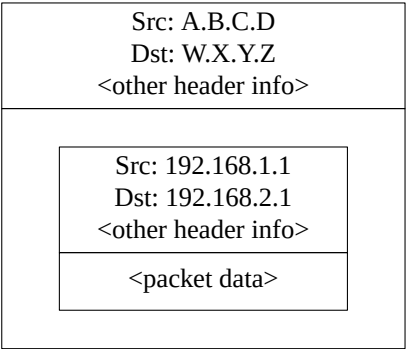
想要完成一个有判断力的安全策略，首先要看我们已经完成的步骤。接下来的讨论针对连接的两端。

您所发出的每一个IP 包都包括一个包头，其内容是和这个包有关的描述性数据。包头包括了包的来源和目的的IP 地址。正如我们所了解的那样，私有IP 地址，例如192.168.x.y 这样的地址范围，不应该出现在Internet 的公网上。于此相反，他们必须首先封装到别的包中。包的来源或目的如果是私有IP 地址，则必须替换成公网IP 地址。

因此如果发出的包类似下面这样：



随后它将被封装进另一个包中，像下面这样：



封装过程是在gif 设备上完成的。如上图所示，包现在有了外部的实际IP 地址，而原始的包则被封装到里面作为数据。这个包将通过Internet 传递。

很明显地，我们希望VPN之间的通讯是加密的。用于言来描述大致是：

“如果包从A.B.C.D发出且其目的地是W.X.Y.Z，则通过必要的安全关联进行加密。”

“如果包来自W.X.Y.Z且其目的地是A.B.C.D，则通过必要的安全关联进行解密。”

这已经很接近了，但还不够正确。如果这么做的话，所有来自和发到W.X.Y.Z的包，无论是否属于VPN通讯都会被加密。这可能并不是您所希望的，因此正确的安全策略应该是

“如果包从A.B.C.D发出，且封装了其他的包，其目的地是W.X.Y.Z，则通过必要的安全关联进行加密。”

“如果包来自W.X.Y.Z，且封装了其他的包，其目的地是A.B.C.D，则通过必要的安全关联进行解密。”

一个很小，但却必要的改动。

安全策略也是通过setkey(8)设置的。setkey(8)提供了一种用于配置策略的语言。可以直接在stdin上输入策略，或通过-f选项来指定一个包含配置命令的文件。

网关#1上的配置(其IP地址是A.B.C.D)强制将所有到W.X.Y.Z的通讯进行加密的配置是：

```
spdadd A.B.C.D/32 W.X.Y.Z/32 ipencap -P out ipsec esp/tunnel/A.B.C.D-W.X.Y.Z/require;
```

把这些命令放到一个文件(例如/etc/ipsec.conf)然后执行

```
# setkey -f /etc/ipsec.conf
```

spdadd会告诉setkey(8)我们希望把规则加入到安全策略数据库中。命令的其它部分指定了什么样的包能够匹配这规则。A.B.C.D/32和W.X.Y.Z/32是用于指定规则能够匹配的网络或主机的IP地址和掩码。本例中，希望应用到两个主机之间的通讯上。ipencap则告诉内核这规则只应被用于封装其他包的那些数据包。-P out表示策略是针对发出的包的，而ipsec则表示需要对数据包进行加密。

第二行指定了如何加密。esp是即将使用的协议，而tunnel则表示包应该进一步封装进一个IPsec包里面。反复使用A.B.C.D和W.X.Y.Z用来选择所用的安全关联而最后的require则强制所有匹配这规则的包都被加密。

上面的规则只匹配了发出的包。接下来需要配置类似的匹配进入包的规则。

```
spdadd W.X.Y.Z/32 A.B.C.D/32 ipencap -P in ipsec esp/tunnel/W.X.Y.Z-A.B.C.D/require;
```

请注意本例中in代替了out并且IP地址的顺序也相反。

在另一个网关上(其公网IP地址是W.X.Y.Z)也需要类似的规则。

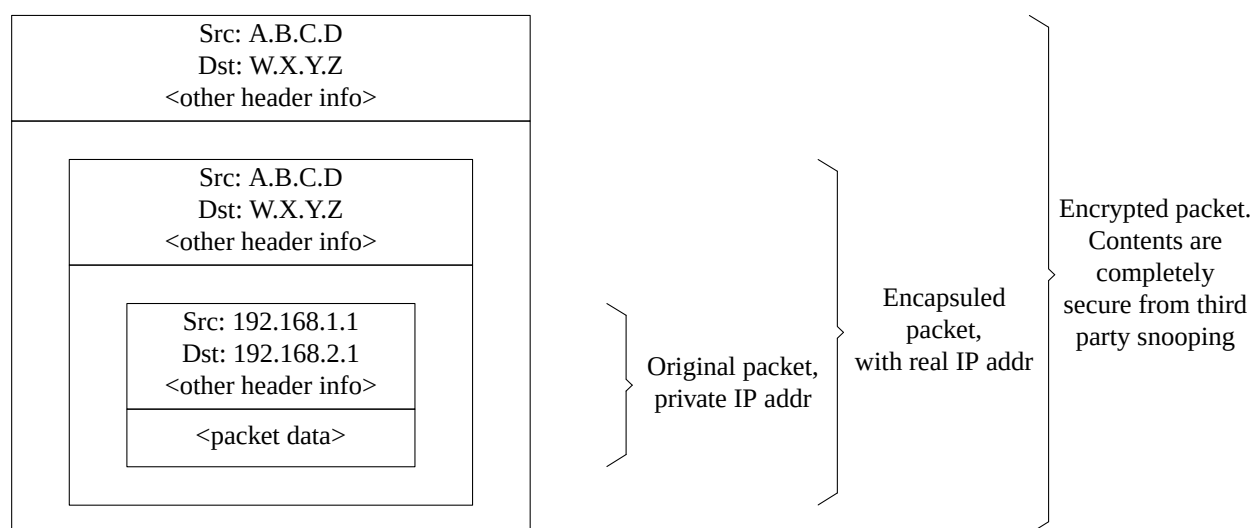
```
spdadd W.X.Y.Z/32 A.B.C.D/32 ipencap -P out ipsec esp/tunnel/W.X.Y.Z-A.B.C.D/require;
spdadd A.B.C.D/32 W.X.Y.Z/32 ipencap -P in ipsec esp/tunnel/A.B.C.D-W.X.Y.Z/require;
```

最后是添加允许ESP和IPENCAP包进出的防火墙规则。这些规则需要在两边分别设置。

```
ipfw add 1 allow esp from A.B.C.D to W.X.Y.Z
ipfw add 1 allow esp from W.X.Y.Z to A.B.C.D
ipfw add 1 allow ipencap from A.B.C.D to W.X.Y.Z
ipfw add 1 allow ipencap from W.X.Y.Z to A.B.C.D
```

由于规则的对称性，因此可以在两台网关上使用同样的规则。

发出的包如下图所示:



当VPN数据被远端接到时,它将首先被解密(使用racoon协商得到的安全关联)。然后它们将进入gif接口,并在那里展开第二层,直到只剩下最里层的包,并将其转发到内网上。

可以通过与之前同样的ping(8)命令来测试安全性。首先登录到A.B.C.D网关上并执行:

```
tcpdump dst host 192.168.2.1
```

在同一主机上登录另一会话,执行

```
ping 192.168.2.1
```

此时的输出应该是:

```
xxx tcpdump output
```

如您看到的, tcpdump(1)给出的将是ESP包。假如您想查看它们的内容可以使用-s option选项,您将(显然地)看到一些乱码,因为传输过程实施了加密。

祝贺您。您已经完成了两个远程站点之间的VPN的架设工作。

小结

- 将两边的内核配置加入:

```
options IPSEC
options IPSEC_ESP
```

- 安装security/ipsec-tools。编辑两台网关上的\${PREFIX}/etc/racoon/psk.txt并添加远程主机的IP和共享的密钥。文件的权限应该是0600。
- 将下面的设置加入两台主机的/etc/rc.conf中:

```
ipsec_enable="YES"
ipsec_file="/etc/ipsec.conf"
```

- 在两个网关上都建立/etc/ipsec.conf并添加必要的spdadd。在网关#1上是:

```
spdadd A.B.C.D/32 W.X.Y.Z/32 ipencap -P out ipsec
    esp/tunnel/A.B.C.D-W.X.Y.Z/require;
spdadd W.X.Y.Z/32 A.B.C.D/32 ipencap -P in ipsec
    esp/tunnel/W.X.Y.Z-A.B.C.D/require;
```

在网关#2 上则是:

```
spdadd W.X.Y.Z/32 A.B.C.D/32 ipencap -P out ipsec
    esp/tunnel/W.X.Y.Z-A.B.C.D/require;
spdadd A.B.C.D/32 W.X.Y.Z/32 ipencap -P in ipsec
    esp/tunnel/A.B.C.D-W.X.Y.Z/require;
```

- 添加防火墙规则以允许IKE, ESP, 和IPENCAP 通讯能够到达各自的主机:

```
ipfw add 1 allow udp from A.B.C.D to W.X.Y.Z isakmp
ipfw add 1 allow udp from W.X.Y.Z to A.B.C.D isakmp
ipfw add 1 allow esp from A.B.C.D to W.X.Y.Z
ipfw add 1 allow esp from W.X.Y.Z to A.B.C.D
ipfw add 1 allow ipencap from A.B.C.D to W.X.Y.Z
ipfw add 1 allow ipencap from W.X.Y.Z to A.B.C.D
```

前面的两步应该足以让VPN 运转起来了。两个网络上的机器都应该能通过IP 来访问对方，而所有的通讯都被自动地进行加密。

14.11 OpenSSH

原著Chern Lee.

OpenSSH 是一组用于安全地访问远程计算机的连接工具。它可以作为rlogin、rsh rcp 以及telnet 的直接替代品使用。更进一步，其他任何TCP/IP 连接都可以通过SSH 安全地进行隧道/转发。**OpenSSH** 对所有的传输进行加密，从而有效地阻止了窃听、连接劫持，以及其他网络级的攻击。

OpenSSH 由OpenBSD project 维护，它基于SSH v1.2.12 并包含了最新的错误修复和更新。它同时兼容SSH 协议的1 和2 两个版本。从FreeBSD 4.0 开始，**OpenSSH** 成为了基本系统的一部分。

14.11.1 使用OpenSSH 的好处

通常，当使用telnet(1) 或rlogin(1) 时，数据是以明码的形式发送的，并没有加密。在客户机和服务器之间的网络上运行的听包程序可以在会话中偷窃到传输的用户名/密码和数据。**OpenSSH** 提供了多种的身份验证和加密方法来防止这种情况的发生。

14.11.2 启用sshd

在FreeBSD 4.X 上，sshd 服务是默认启用的。在FreeBSD 5.X 和更高版本上，sshd 的启用是作为FreeBSD 安装中Standard 安装过程中的一步来进行的。要查看sshd 是否已被启用，请检查rc.conf 文件中的:

```
sshd_enable="YES"
```


这表示在下次系统启动时加载**OpenSSH** 的服务程序sshd(8)。此外，也可以手动使用rc(8)脚本/etc/rc.d/sshd 来启动**OpenSSH**：

```
/etc/rc.d/sshd start
```

14.11.3 SSH 客户

ssh(1) 的工作方式和rlogin(1) 非常类似。

```
# ssh user@example.com
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host 'example.com' added to the list of known hosts.
user@example.com's password: *****
```

登录过程和使用rlogin 或telnet 建立的会话非常类似。在连接时，SSH 会利用一个密钥指纹系统来验证服务器的真实性。只有在第一次连接时，用户会被要求输入yes。之后的连接将会验证预先保存下来的密钥指纹。如果保存的指纹与登录时接收到的不符，则将会给出警告。指纹保存在~/.ssh/known_hosts 中，对于SSH v2 指纹，则是~/.ssh/known_hosts2。

默认情况下，较新版本的**OpenSSH** 只接受SSH v2 连接。如果能用版本2 则客户程序会自动使用，否则它会返回使用版本1 的模式。此外，也可以通过命令行参数-1 或-2 来相应地强制使用版本1 或2。保持客户端的版本1 能力是为了考虑较早版本的兼容性。

14.11.4 安全复制

scp(1) 命令和rcp(1); 的用法类似，它用于将文件复制到远程的机器上，或复制过来，区别它是安全的。

```
# scp user@example.com:/COPYRIGHT COPYRIGHT
user@example.com's password: *****
COPYRIGHT          100% |*****| 4735
00:00
#
```

由于先前的例子中已经保存了指纹，使用scp(1) 时会自动地加以验证。

scp(1) 使用的参数同cp(1) 类似。第一个参数是一个或一组文件，然后是复制的目标。由于文件是通过SSH 在网上传递的，因此某些文件的名称需要写成用户名@主机名:<远程文件路径>。

14.11.5 配置

针对**OpenSSH** 服务程序和客户端的系统级配置文件在/etc/ssh 目录中。

ssh_config 用于配置客户端的设定，而sshd_config 则用于配置服务器端。

另外sshd_program(默认是/usr/sbin/sshd)，以及sshd_flags 这两个rc.conf 选项提供了更多的配置选择。

14.11.6 ssh-keygen

用于取代口令的一种方法是使用ssh-keygen(1)来生成DSA或RSA密钥对用于验证用户的身份:

```
% ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_dsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_dsa.
Your public key has been saved in /home/user/.ssh/id_dsa.pub.
The key fingerprint is:
bb:48:db:f2:93:57:80:b6:aa:bc:f5:d5:ba:8f:79:17 user@host.example.com
```

ssh-keygen(1)会生成一个包含公私钥对用于验证身份。私钥将保存到`~/.ssh/id_dsa`或`~/.ssh/id_rsa`,而公钥则被存放到`~/.ssh/id_dsa.pub`或`~/.ssh/id_rsa.pub`,文件名取决于您选择的DSA和RSA密钥类型。公钥必须被存放到远程机器上的`~/.ssh/authorized_keys`才能够使系统正确运转。类似地,第1版的RSA公钥应存放到`~/.ssh/authorized_keys`。

这将允许从远程连接时以基于SSH密钥的验证来代替口令验证。

如果在ssh-keygen(1)中使用了通行字,则每次使用私钥时都需要输入它。ssh-agent(1)能够缓解多次输入长通行字的压力,并将在接下来的第14.11.7节予以详述。

警告: 选项和配置文件可能随OpenSSH的版本不同而不同;为了避免出现问题,您应参考ssh-keygen(1)联机手册。

14.11.7 ssh-agent 和ssh-add

ssh-agent(1)和ssh-add(1)这两个工具,提供了一种将SSH秘钥加载到内存中以便使用,而不必每次都输入通行字的方法。

ssh-agent(1)工具能够使用加载到其中的私钥来处理验证过程。ssh-agent(1)应被用于启动另一个应用程序。最基本的用法是,使用它来启动shell,而高级一些的用法则是用它来启动窗口管理器。

要在shell中使用ssh-agent(1),首先应把shell作为参数来启动它。随后,应通过ssh-add(1)并输入通行字,来向它提供身份验证信息。一旦这些步骤都做完了,用户就应该能够ssh(1)到任何一个安装了对应公钥的机器了。例如:

```
% ssh-agent csh
% ssh-add
Enter passphrase for /home/user/.ssh/id_dsa:
Identity added: /home/user/.ssh/id_dsa (/home/user/.ssh/id_dsa)
%
```

要在X11中使用ssh-agent(1),调用ssh-agent(1)的过程应置于`~/.xinitrc`之中。这将把ssh-agent(1)服务提供给所有在X11中运行的程序。下面是一个`~/.xinitrc`文件的实例:

```
exec ssh-agent startxfce4
```

这将启动ssh-agent(1)，而后者将在每次X11启动时运行XFCE。作完这些之后就可以重启X11以便使修改生效。随后您就可以运行ssh-add(1)来加载全部SSH密钥了。

14.11.8 SSH 隧道

OpenSSH能够创建隧道以使用加密的会话来封装其他协议。

下面的命令告诉ssh(1)为telnet创建一个隧道：

```
% ssh -2 -N -f -L 5023:localhost:23 user@foo.example.com
%
```

上述ssh命令使用了下面这些选项：

-2

强制ssh使用第2版的协议(如果需要和较老的SSH一同工作请不要使用这个选项)。

-N

表示不使用命令行，或者说只使用隧道。如果省略，ssh将同时初始化会话。

-f

强制ssh在后台执行。

-L

表示产生一条本地端口:远程主机:远程端口形式的隧道。

user@foo.example.com

远程SSH服务器。

SSH隧道通过监听localhost上面指定端口来完成工作。它将把本机主机/端口上接收到的连接通过SSH连接转发到远程主机/端口。

本例中，位于localhost的5023端口被用于转发localhost的连接到达远程主机的23端口。由于23是telnet使用的，因此它将通过SSH隧道完成telnet会话。

这可以用来封装任意不安全的TCP协议，例如SMTP、POP3、FTP等等。

例14-1. 使用SSH为SMTP创建安全隧道

```
% ssh -2 -N -f -L 5025:localhost:25 user@mailserver.example.com
user@mailserver.example.com's password: *****
% telnet localhost 5025
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mailserver.example.com ESMTP
```

这可以与ssh-keygen(1)以及额外的用户帐号配合来建立一个更透明的SSH隧道环境。密钥可以被用在需要输入口令的地方，而且可以为不同的用户配置不同的隧道。

14.11.8.1 实用的SSH 通道例子

14.11.8.1.1 加强POP3 服务的安全

工作时，有一个允许外来连接的SSH 服务器。同一个办公网络中有一个邮件服务器提供POP3 服务。这个网络，或从您家到办公室的网络可能不，或不完全可信。基于这样的原因，您需要以安全的方式来察看邮件。解决方法是创建一个到办公室SSH 服务器的连接，并通过这个连接来访问POP3 服务：

```
% ssh -2 -N -f -L 2110:mail.example.com:110 user@ssh-server.example.com
user@ssh-server.example.com's password: *****
```

当这个通道连上时，您可以把POP3 请求发到localhost 端口2110。这个连接将通过通道安全地转发到mail.example.com。

14.11.8.1.2 绕过严厉的防火墙

一些大脑长包的网络管理员会使用一些极端的防火墙策略，不仅过滤进入的连接，而且也过滤连出的连接。一些时候您可能只能连接远程机器22 端口，以及80 端口用来进行SSH 和网页浏览。

您可能希望访问一些其它的(也许与工作无关的) 服务，例如提供音乐的Ogg Vorbis 流媒体服务器。如果Ogg Vorbis server 在22 或80 端口以外的端口播放音乐，则您将无法访问它。

解决方法是建立一个到您的网络的防火墙之外的网络上的SSH 服务器，并通过它提供的通道连接到Ogg Vorbis 服务器上。

```
% ssh -2 -N -f -L 8888:music.example.com:8000 user@unfirewalled-system.example.org
user@unfirewalled-system.example.org's password: *****
```

现在您可以把客户程序指定到localhost 的8888 端口，它将把请求转发给music.example.com 的8000 端口，从而绕过防火墙。

14.11.9 允许用户登录AllowUsers 选项

通常限制哪些用户能够登录，以及从何处登录会是好主意。采用AllowUsers 选项能够方便地达到这一目的。例如，想要只允许root 用户从192.168.1.32 登录，就可以在/etc/ssh/sshd_config 文件中加入下述设置：

```
AllowUsers root@192.168.1.32
```

要允许用户admin 从任何地方登录，则只需列出用户名：

```
AllowUsers admin
```

可以在同一行指定多个用户，例如：

```
AllowUsers root@192.168.1.32 admin
```

注意：列出需要登录机器的用户很重要；否则他们将被锁在外面。

在完成对`/etc/ssh/sshd_config`的修改之后您必须告诉`sshd(8)`重新加载其配置文件，方法是执行：

```
# /etc/rc.d/sshd reload
```

14.11.10 进一步的资料

OpenSSH (<http://www.openssh.com/>)

`ssh(1)` `scp(1)` `ssh-keygen(1)` `ssh-agent(1)` `ssh-add(1)` `ssh_config(5)`

`sshd(8)` `sftp-server(8)` `sshd_config(5)`

14.12 文件系统访问控制表

作者Tom Rhodes.

与文件系统在其它方面的加强，如快照等一道，FreeBSD 5.0 及更高版本提供了通过文件系统访问控制表(ACLs)实现的安全机制。

访问控制表以高度兼容(POSIX.1e)的方式扩展了标准的UNIX 权限模型。这一特性使得管理员能够利用其优势设计更为复杂的安全模型。

如果想为UFS 文件系统启用ACL 支持，则需要添加下列选项：

```
options UFS_ACL
```

并重新编译内核。如果这个选项没有编译进内核，则在挂接支持ACL 的文件系统时将会收到警告。这个选项在GENERIC 内核中已经包含了。ACL 依赖于在文件系统上启用扩展属性。在新一代的UNIX file system，UFS2 中内建了这种支持。

注意：在UFS1 上配置扩展属性需要比UFS2 更多的管理开销。而且，在UFS2 上的扩展属性的性能也有极大的提高。因此，如果想要使用访问控制表，推荐使用UFS2 而不是UFS1。

ACL 可以在挂接时通过选项`acls` 来启动，它可以加入`/etc/fstab`。另外，也可以通过使用`tunefs(8)` 修改超级块中的ACL 标记来持久性地设置自动的挂接属性。一般而言，后一种方法是推荐的做法，其原因是：

- 挂接时的ACL 标记无法被重挂接(`mount(8) -u`) 改变，只有完整地`umount(8)` 并做一次新的`mount(8)` 才能改变它。这意味着ACLs 状态在系统启动之后就不可能在`root` 文件系统上发生变化了。另外也没有办法改变正在使用的文件系统的这个状态。
- 在超级块中的设置将使得文件系统总被以启用ACLs 的方式挂接，即使在`fstab` 中的对应项目没有作设置，或设备顺序发生变化时也是如此。这避免了不慎将文件系统以没有启用ACLs 的状态挂接，从而避免没有强制ACLs 这样的安全问题。

注意：可以修改ACL 行为，以允许在没有执行一次全新的`mount(8)` 的情况下启用它，但我们认为不鼓励在不启用ACL 的时候这么做是有必要的，因为如果启用了ACL，然后关掉它，然后在没有刷新扩展属性的情况下重新启用它是很容易造成问题的。一般而言，一旦启用了文件系统的ACLs 就不应该再关掉它，因为此时的文件系统的保

护措施可能和用户所期待的样子不再兼容，而重新启用ACL将重新把先前的ACL附着到文件上，而由于它们的权限发生了变化，就很可能造成无法预期的行为。

在察看目录时，启用了ACLs的文件将在通常的属性后面显示+ (加号)。例如：

```
drwx----- 2 robert  robert  512 Dec 27 11:54 private
drwxrwx---+ 2 robert  robert  512 Dec 23 10:57 directory1
drwxrwx---+ 2 robert  robert  512 Dec 22 10:20 directory2
drwxrwx---+ 2 robert  robert  512 Dec 27 11:57 directory3
drwxr-xr-x  2 robert  robert  512 Nov 10 11:54 public_html
```

这里我们看到了directory1, directory2, 以及directory3 目录使用了ACLs。而public_html 则没有。

14.12.1 使用ACL

文件系统ACL 可以使用getfacl(1) 工具来查看。例如，如果想查看test 的ACL 设置，所用的命令是：

```
% getfacl test
#file:
#owner:1001
#group:1001
user::rw-
group::r--
other::r--
```

要修改这个文件上的ACL 设置，则需要使用setfacl(1) 工具。例如：

```
% setfacl -k test
```

-k 参数将把所有当前定义的ACL 从文件或文件系统中删除。一般来说应该使用 -b 因为它会保持让ACL 正常工作的那些项不变。

```
% setfacl -m u:trhodes:rwx,group:web:r--,o:---- test
```

在前面的命令中，-m 选项被用来修改默认的ACL 项。由于已经被先前的命令删除，因此没有预先定义的项，于是默认的选项被恢复，并附加上指定的选项。请小心地检查，如果您加入了一个不存在的用户或组，那么将会在stdout 得到一条Invalid argument 的错误提示。

14.13 监视第三方安全问题

Contributed by Tom Rhodes.

过去几年中，安全领域在如何处理漏洞的评估方面取得了长足的进步。几乎每一个操作系统都越来越多地安装和配置了第三方工具，而系统被入侵的威胁也随之增加。

漏洞的评估是安全的一个关键因素，尽管FreeBSD 会发布基本系统的安全公告，然而为每一个第三方工具都发布安全公告则超出了FreeBSD Project 的能力。在这一前提下，一种减轻第三方漏洞的威胁，并警

告管理员存在已知的安全问题的方法也就应运而生。名为**Portaudit**的FreeBSD附加工具能够帮助您达成这一目的。

`security/portaudit port` 会下载一个数据库，这一数据库是由FreeBSD Security Team 和ports 开发人员维护的，其中包含了已知的安全问题。

要开始使用**Portaudit**，需要首先从Ports Collection 安装它：

```
# cd /usr/ports/security/portaudit && make install clean
```

在安装过程中，`periodic(8)`的配置文件将被修改，以便让**Portaudit**能够在每天的安全审计过程中运行。一定要保证发到root 帐号的每日安全审计邮件确实有人在读。除此之外不需要进行更多的配置了。

安装完成之后，管理员可以通过下面的命令来更新数据库，并查看目前安装的软件包中所存在的已知安全漏洞：

```
# portaudit -Fda
```

注意：由于每天执行`periodic(8)`时都会自动更新数据库，因此，运行这条命令是可选的。在这里只是作为例子给出。

在任何时候，如果希望对通过Ports Collection 安装的第三方软件工具进行审计，管理员都可以使用下面的命令：

```
# portaudit -a
```

针对存在漏洞的软件包，**Portaudit**将生成类似下面的输出：

```
Affected package: cups-base-1.1.22.0_1
Type of problem: cups-base -- HPGL buffer overflow vulnerability.
Reference: <http://www.FreeBSD.org/ports/portaudit/40a3bca2-6809-11d9-a9e7-0001020eed82.html>
```

```
1 problem(s) in your installed packages found.
```

```
You are advised to update or deinstall the affected package(s) immediately.
```

通过访问上面给出的URL，管理员能够了解关于那个漏洞的进一步信息。这些信息通常包括受到影响的FreeBSD Port 版本，以及其他可能包含安全公告的网站。

简而言之，**Portaudit**是一个强大的工具，并能够配合**Portupgrade port**来非常有效地工作。

14.14 FreeBSD 安全公告

作者Tom Rhodes.

像其它具有产品级品质的操作系统一样，FreeBSD 会发布“安全公告”。通常这类公告会只有在在相应的发行版本已经正确地打过补丁之后发到安全邮件列表并在勘误中说明。本节将介绍什么是安全公告，如何理解它，以及为系统打补丁的具体步骤。

14.14.1 安全公告看上去是什么样子？

FreeBSD 安全公告的样式类似下面的范例，这一例子来自 `freebsd-security-notifications` (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-security-notifications>) 邮件列表。

```
=====
FreeBSD-SA-XX:XX.UTIL                                Security Advisory
                                                    The FreeBSD Project
```

```
Topic:          denial of service due to some problem①

Category:       core②
Module:         sys③
Announced:     2003-09-23④
Credits:        Person@EMAIL-ADDRESS⑤
Affects:        All releases of FreeBSD⑥
                FreeBSD 4-STABLE prior to the correction date
Corrected:      2003-09-23 16:42:59 UTC (RELENG_4, 4.9-PRERELEASE)
                2003-09-23 20:08:42 UTC (RELENG_5_1, 5.1-RELEASE-p6)
                2003-09-23 20:07:06 UTC (RELENG_5_0, 5.0-RELEASE-p15)
                2003-09-23 16:44:58 UTC (RELENG_4_8, 4.8-RELEASE-p8)
                2003-09-23 16:47:34 UTC (RELENG_4_7, 4.7-RELEASE-p18)
                2003-09-23 16:49:46 UTC (RELENG_4_6, 4.6-RELEASE-p21)
                2003-09-23 16:51:24 UTC (RELENG_4_5, 4.5-RELEASE-p33)
                2003-09-23 16:52:45 UTC (RELENG_4_4, 4.4-RELEASE-p43)
                2003-09-23 16:54:39 UTC (RELENG_4_3, 4.3-RELEASE-p39)⑦
FreeBSD only:   NO⑧
```

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <http://www.FreeBSD.org/security/>.

I. Background⑨

II. Problem Description(10)

III. Impact(11)

IV. Workaround(12)

V. Solution(13)

VI. Correction details(14)

VII. References(15)

- ❶ **Topic(标题)** 一栏说明了问题到底是什么。它基本上是对所发现的安全问题及其所涉及的工具的描述。
- ❷ **Category (分类)** 是指系统中受到影响的组建，这一栏可能是`core`、`contrib`，或者`ports`之一。`core`分类表示安全弱点影响到了FreeBSD 操作系统的某个核心组件。`contrib`分类表示弱点存在于某个捐赠给FreeBSD Project 的软件，例如`sendmail`。最后是`ports`，它表示该弱点影响了Ports Collection 中的某个第三方软件。
- ❸ **Module(模块)** 一栏给出了组件的具体位置，例如`sys`。在这个例子中，可以看到`sys` 模块是存在问题的；因此，这个漏洞会影响某个在内核中的组件。
- ❹ **Announced(发布时间)** 一栏反映了与安全公告有关的数据是什么时候公之于众的。这说明安全团队已经证实问题确实存在，而补丁已经写入了FreeBSD 的代码库。
- ❺ **Credits(作者)** 一栏给出了注意到问题存在并报告它的个人或团体。
- ❻ **The Affects(影响范围)** 一栏给出了FreeBSD 的那些版本存在这个漏洞。对于内核来说，检视受影响的文件上执行的`ident` 输出可以帮助确认文件版本。对于`ports`，版本号在`/var/db/pkg` 里面的`port` 的名字后面列出。如果系统没有与FreeBSD CVS 代码库同步并每日构建，它很可能是有问题的。
- ❼ **Corrected(修正时间)** 一栏给出了发行版本中修正问题的具体日期、时间和时差。
- ❽ **FreeBSD only(仅FreeBSD)** 一栏说明了漏洞是否只影响FreeBSD，还是也影响一些其它操作系统。
- ❾ **Background(技术背景)** 一栏提供了受影响的组件的作用。多数时候这一部分会说明为什么FreeBSD 中包含了它，它的作用，以及它的一些原理。
- ❿ **Problem Description(问题描述)** 一栏深入阐述安全漏洞的技术细节。这部分有时会包括有问题的代码相关的详细情况，甚至是这个部件如何能够被恶意利用并打开漏洞的细节。
- ⓫ **Impact(影响)** 一栏描述了问题能够造成的影响类型。例如，可能导致拒绝服务攻击，权限提升，甚至导致得到超级用户的权限。
- ⓬ **Workaround(应急方案)** 一栏给出了系统管理员在暂时无法升级系统时可以采取的临时性对策。这些原因可能包括时间限制，网络资源的限制，或其它因素。不过无论如何，安全不能够被轻视，有问题的系统要么应该打补丁，要么应该实施这种应急方案。
- ⓭ **Solution(解决方案)** 一栏提供了如何给有问题的系统打补丁的方法。这是经过逐步测试和验证过的给系统打补丁并让其安全地工作的方法。
- ⓮ **=Correction Details(修正细节)** 一栏展示了针对CVS 分支或某个发行版的修正特征。同时也提供了每个分支上相关文件的版本号。
- ⓯ **References(文献)** 一栏通常会给出其它信息的来源。这可能包括URL，书籍、邮件列表以及新闻组。

14.15 进程记帐

Contributed by Tom Rhodes.

进程记帐是一种管理员可以使用的跟踪系统资源使用情况的手段，包括它们分配给了哪些用户、提供系统监视手段，并且可以精细到用户执行的每一个命令。

当然，这种做法是兼有利弊的。它的好处是，查找入侵时可以迅速把范围缩小到攻击者进入的时刻；而这样做的缺点，则是记帐会产生大量的日志，因而需要很多磁盘空间来存储它们。这一节将带领管理员一步一步地配置基本的进程记帐。

14.15.1 启用并利用进程记帐

在使用进程记帐之前，必须先启用它。要完成这项工作，需要运行下面的命令：

```
# touch /var/account/acct  
  
# accton /var/account/acct  
  
# echo 'accounting_enable="YES"' >> /etc/rc.conf
```

一旦启用之后，记帐就会开始跟踪CPU 统计数据、命令，等等。所有的记帐日志不是以可读的方式记录的，要查看它们，需要使用sa(8) 这个工具。如果没有给出其他参数，则sa 将按用户，以分钟为单位显示他们所使用的时间、总共的CPU 和用户时间，以及平均的I/O 操作数目，等等。

要显示关于刚刚发出的命令的相关信息，则应使用lastcomm(1) 工具。lastcomm 可以用来显示在某一ttys(5) 上的用户信息，例如：

```
# lastcomm ls  
trhodes ttyp1
```

将会显示出所有已知的trhodes 在ttyp1 终端上执行ls 的情况。

更多的可用选项在联机手册lastcomm(1)、acct(5) 和sa(8) 中有所介绍。

备注

1. 在FreeBSD 中标准的登录口令最长不能超过128 个字符。

第15章

集权式访问控制

Written by Tom Rhodes.

15.1 概要

FreeBSD 5.X 在POSIX.1e 草案的基础上引入了TrustedBSD 项目提供的新的安全性扩展。新安全机制中最重要的两个，是文件系统访问控制列表(ACL) 和集权式访问控制(MAC) 机制。集权式访问控制允许加载新的访问控制模块，并借此实施新的安全策略，其中一部分为一个很小的系统子集提供保护并加强特定的服务，其他的则对所有的主体和对象提供全面的标签式安全保护。定义中有关集权的部分源于如下事实，控制的实现由管理员和系统作出，而不像全权式访问控制(DAC, FreeBSD 中的标准文件以及System V IPC 权限) 那样是按照用户意愿进行的。

本章将集中讲述集权式访问控制框架(MAC 框架) 以及一套用以实施多种安全策略的插件式的安全策略模块。

阅读本章之后，您将了解：

- 目前FreeBSD 中具有哪些MAC 安全策略模块，以及与之相关的机制。
- MAC 安全策略模块将实施何种策略，以及标签式与非标签式策略之间的差异。
- 如何高效地配置系统令使其使用MAC 框架。
- 如何配置MAC 框架所提供的不同的安全策略模块。
- 如何用MAC 框架构建更为安全的环境，并举例说明。
- 如何测试MAC 配置以确保正确构建了框架。

阅读本章之前，您应该：

- 了解UNIX 和FreeBSD 的基础(第3 章)。
- 熟悉内核配置/编译(第8 章) 的基础。
- 对安全及其如何与FreeBSD 相配合有些了解；(第14 章)。

警告：对本章信息的不当使用可能导致丧失系统访问权，激怒用户，或者无法访问X11 提供的特性。更重要的是，MAC 不能用于彻底保护一个系统。MAC 框架仅用于增强现有安全策略；如果没有健全的安全条例以及定期的安全检查，系统将永远不会绝对安全。

此外还需要注意的是，本章中所包含的例子仅仅是例子。我们并不建议在一个生产用系统上进行这些特别的设置。实施各种安全策略模块需要谨慎的考虑，因为那些并不完全理解所有机制如何工作的人，可能会发现需要对整个系统中很多的文件或目录进行重新配置。

15.1.1 未涉及的内容

本章涵盖了与MAC 框架有关的诸多方面的安全问题；尽管如此，本章将不涉及新MAC 安全策略模块的开发成果。MAC 框架中所包含的一部分安全策略模块，具有一些用于测试及新模块开发的特定属性，其中包括`mac_test(4)`、`mac_stub(4)`以及`mac_none(4)`。关于这些安全策略模块及其提供的众多机制的详细信息，请参阅联机手册中的内容。

15.2 本章出现的重要术语

在阅读本章之前，有些关键术语需要解释，希望能藉此扫清可能出现的疑惑，并避免在文中对新术语、新信息进行生硬的介绍。

- **区间：**区间，是指一组被划分或隔离的程序和数据，其中，用户被明确地赋予了访问特定系统组件的权限。同时，区间也能够表达分组，例如工作组、部门、项目，或话题。可以通过使用区间来实施`need-to-know` 安全策略。
- **完整性：**作为一个关键概念，完整性是数据可信性的一种程度。若数据的完整性提高，则数据的可信性相应提高。
- **标签：**标签是一种可应用于文件、目录或系统其他对象的安全属性，它也可以被认为是一种机密性印鉴。当一个文件被施以标签时，其标签会描述这一文件的安全参数，并只允许拥有相似安全性设置的文件、用户、资源等访问该文件。标签值的涵义及解释取决于相应的策略配置：某些策略会将标签当作对某一对象的完整性和保密性的表述，而其它一些策略则会用标签保存访问规则。
- **程度：**对某种安全属性加强或削弱的设定。若程度增加，其安全性也相应增加。
- **多重标签(multilabel)：**`multilabel` 属性是一个文件系统选项。该选项可在单用户模式下通过`tunefs(8)` 程序进行设置。可以在引导时使用的`fstab(5)` 文件中，也可在创建新文件系统时进行配置。该选项将允许管理员对不同对象施以不同的MAC 标签。该选项仅适用于支持标签的安全策略模块。
- **对象：**对象或系统对象是一种实体，信息随**主体** 的导向在对象内部流动。对象包括目录、文件、区段、监视器、键盘、存储器、磁存储器、打印机及其它数据存储/转移设备。基本上，一个对象就是一个数据容器或一种系统资源。对**对象** 的访问实际上意味着对数据的访问。
- **策略：**一套用以规定如何达成目标的规则。**策略** 一般用以描述如何对特定对象进行操作。本章将在**安全策略**的范畴内讨论**策略**，一套用以控制数据和信息流并规定其访问者的规则，就是其中一例。
- **敏感性：**通常在讨论MLS 时使用。敏感性程度曾被用来描述数据应该有何等的重要或机密。若敏感性程度增加，则保密的重要性或数据的机密性相应增强。
- **单一标签：**整个文件系统使用一个标签对数据流实施访问控制，叫做单一标签。当文件系统使用此设置时，即无论何时当多重标签 选项未被设定时，所有文件都将遵守相同标签设定。
- **主体：**主体就是引起信息在两个**对象**间流动的任意活动实体，比如用户，用户处理器，系统进程等。在FreeBSD 中，主体几乎总是代表用户活跃在某一进程中的一个线程。

15.3 关于MAC 的说明

在掌握了所有新术语之后，我们从整体上来考虑MAC 是如何加强系统安全性的。MAC 框架提供的众多安全策略模块可以用来保护网络及文件系统，也可以禁止用户访问某些特定的端口、套接字及其它对象。将策略模块组合在一起以构建一个拥有多层次安全性的环境，也许是其最佳的使用方式，这可以通过

一次性加载多个安全策略模块来实现。在多层次安全环境中，多重策略模块可以有效地控制安全性，这一点与加强式策略不同。加强式策略一般加强仅具有某些特殊用途的系统对象的安全性。相比之下，多重策略的唯一不足是需要系统管理员先期设置好参数，如多重文件系统安全标志、每一位用户的网络访问权限等等。

与框架长久的效果相比，这些不足之处微乎其微。例如，为某种特殊配置选择其所需策略的能力，会使整体性能下降，但减少对无用策略的支持却可以提高系统整体性能，同时还可以为选择提供弹性空间。好的应用应该考虑到整体的安全性要求，并有效地实施框架提供的众多安全策略模块。

这样一个使用MAC特性的系统，至少要保证不允许用户任意更改安全属性；所有的用户实用工具、程序以及脚本，必须在所选安全策略模块提供的访问规则的约束下工作；并且系统管理员应掌握MAC访问规则的一切控制权。

细心选择正确的安全策略模块是系统管理员专有的职责。某些环境也许需要限制网络的访问控制权，在这种情况下，使用`mac_portacl(4)`、`mac_ifoff(4)`乃至`mac_biba(4)`安全策略模块都会是不错的开始；在其他情况下，系统对象也许需要严格的机密性，像`mac_bsextended(4)`和`mac_mls(4)`这样的安全策略模块就是为此而设。

对安全策略模块的决定可依据网络配置进行，也许只有特定的用户才应该被允许使用由`ssh(1)`提供的程序以访问网络或互联网，`mac_portacl(4)`安全策略模块应该成为这种情况下的选择。但对文件系统又该作些什么呢？是由特定的用户或群组来确定某些目录的访问权限，抑或是将特定对象设为保密以限制用户或组件访问特定文件？

在文件系统的例子中，也许访问对象的权限对某些用户是保密的，但对其他则不是。比如，一个庞大的开发团队，也许会被分成许多由几人组成的小组，A项目中的开发人员可能不被允许访问B项目开发人员创作的对象，但同时他们还需要访问由C项目开发人员创作的对象，这正符合上述情形。使用由MAC框架提供的不同策略，用户就可以被分成这种小组，然后被赋予适当区域的访问权，由此，我们就不用担心信息泄漏的问题了。

因此，每一种安全策略模块都有其处理系统整体安全问题的独特方法。对安全策略模块的选择应在对安全策略深思熟虑的基础之上进行。很多情况下，整体安全策略需要重新修正并在系统上实施。理解MAC框架提供的不同安全策略模块会帮助管理员就其面临的情形选择最佳的策略模块。

FreeBSD的默认内核并不包含MAC框架选项，因此，在尝试使用本章中的例子或信息之前，您应该添加以下内核选项：

options MAC

此外，内核还需要重新编译并且重新安装。

小心：尽管有关MAC的许多联机手册中都声明它们可以被编译到内核中，但对这些策略模块的使用仍可能导致锁死系统的网络及其他功能。使用MAC就像使用防火墙一样，因此必须要小心防止将系统完全锁死。在使用MAC时，应该考虑是否能够回退到之前的配置，在远程进行配置更应加倍小心。

15.4 理解MAC 标签

MAC标签是一种安全属性，它可以被应用于整个系统中的主体和对象。

配置标签时，用户必须能够确切理解其所进行的操作。对象所具有的属性取决于被加载的策略模块，不同策略模块解释其属性的方式也差别很大。由于缺乏理解或无法了解其间联系而导致的配置不当，会引起意想不到的，也许是不愿看到的系统异常。

对象上的安全标签是由安全策略模块决定的安全访问控制的一部分。在某些策略模块中，标签本身所包含的所有信息足以使其作出决策，而在其它一些安全策略模块中，标签则可能被作为一个庞大规则体系的一部分进行处理。

举例来说，在文件上设定**biba/low** 标签，意味着此标签隶属Biba 策略模块，其值为“low”。

某些在FreeBSD 中支持标签特性的策略会提供三个预定义的标签，分别是**low**、**high** 及**equal** 标签。尽管这些标签在不同安全策略模块中会对访问控制采取不同措施，但有一点是可以肯定的，那就是**low** 标签表示最低限度的设定，**equal** 标签会将主体或对象设定为被禁用的或不受影响的，**high** 标签则会应用Biba 及MLS 安全策略模块中允许的最高级别的设定。

在单一标签文件系统的环境中，同一对象上只会应用一个标签，于是，一套访问权限将被应用于整个系统，这也是很多环境所全部需要的。另一些应用场景中，我们需要将多重标签应用于文件系统的对象或主体，如此一来，就需要使用tunefs(8) 的**multilabel** 选项。

在使用Biba 和MLS 时可以配置数值标签，以精确地标示分级控制的中的程度。数值的程度可以用来划分或将信息按组分类，从而只允许同程度或更高度度的组对齐进行访问。

多数情况下，管理员将仅对整个文件系统设定单一标签。

等一下，这看起来很像DAC！但我认为MAC 确实只将控制权赋予了管理员。此声明依然有效。在某种程度上，**root** 是实施控制的用户，他配置安全策略模块以使用户们被分配到适当的类别/访问levels 中。唉，很多安全策略模块同样可以限制**root** 用户。对于对象的基本控制可能会下放给群组，但**root** 用户随时可以废除或更改这些设定。这就是如Biba 及MLS 这样一些安全策略模块所包含的**hierarchal/clearance** 模型。

15.4.1 配置标签

实际上，有关标签式安全策略模块配置的各种问题都是用基础系统组件实现的。这些命令为对象和主体配置以及配置的实施和验证提供了一个简便的接口。

所有的配置都应该通过**setfmac(8)** 及**setpmac(8)** 组件实施。**setfmac** 命令是用来对系统对象设置MAC 标签的，而**setpmac** 则是用来对系统主体设置标签的。例如：

```
# setfmac biba/high test
```

若以上命令不发生错误则会直接返回命令提示符，只有当发生错误时，这些命令才会给出提示，这和**chmod(1)** 和**chown(8)** 命令类似。某些情况下，以上命令产生的错误可能是**Permission denied**，一般在受限对象上设置或修改设置时会产生此错误。¹ 系统管理员可使用以下命令解决此问题：

```
# setfmac biba/high test
Permission denied
# setpmac biba/low setfmac biba/high test
# getfmac test
test: biba/high
```

如上所示，通过**setpmac** 对被调用的进程赋予不同的标签，以覆盖安全策略模块的设置。**getpmac** 组件通常用于当前运行的进程，如**sendmail**：尽管其使用进程编号来替代命令，其逻辑是相同的。如果用户试图对其无法访问的文件进行操作，根据所加载的安全策略模块的规则，函数**mac_set_link** 将会给出**Operation not permitted** 的错误提示。

15.4.1.1 一般标签类型

mac_biba(4)、**mac_mls(4)** 及**mac_lomac(4)** 策略模块提供了设定简单标签的功能，其值应该是**high**、**equal** 及**low** 之一。以下是对这些标签功能的简单描述：

- **low** 标签被认为是主体或对象所具有的最低层次的标签设定。对主体或对象采用此设定，将阻止其访问标签为**high**的对象或主体。
- **equal** 标签只能被用于不希望受策略控制的对象上。
- **high** 标签对对象或主体采用可能的最高设定。

至于每个策略模块，每种设定都会产生不同的信息流指令。阅读联机手册中相关的章节将进一步阐明这些一般标签配置的特点。

15.4.1.1.1 标签高级配置

如下所示，用于比较：区间+ 区间的数值等级数：

biba/10:2+3+6(5:2+3-20:2+3+4+5+6)

可被解释为：

“Biba 策略标签” / “等级10” : “区间2、3及6” : (“等级5 ...”)

本例中，第一个等级将被认为是“有效区间”的“有效等级”，第二个等级是低级等级，最后一个则是高级等级。大多数配置中不会使用这些设置，实际上，它们是为更高级的配置准备的。

当把它们应用在系统对象上时，则只有当前的等级/区间，因为它们反映可以实施访问控制的系统中可用的范围，以及网络接口。

等级和区间，可以用来在一对主体和对象之间建立一种称为“支配”的关系，这中关系可能是主体支配对象，对象支配主体，互不支配或互相支配。“互相支配”这种情况会在两个标签相等时发生。由于Biba的信息流特性，您可以设置一系列区间，“need to know”，这可能发生于项目之间，而对象也由其对应的区间。用户可以使用**su**和**setpmac**来将他们的权限进一步细分，以便在没有限制的区间里访问对象。

15.4.1.2 用户和标签设置

用户本身也需要设置标签，以使其文件和进程能够正确地与系统上定义的安全策略互动，这是通过使用登录分级在文件**login.conf**中配置的。每个使用标签的策略模块都会进行用户分级设定。

以下是一个使用所有策略模块的例子：

```
default:\
:copyright=/etc/COPYRIGHT:\
:welcome=/etc/motd:\
:setenv=MAIL=/var/mail/$,BLOCKSIZE=K:\
:path=~/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin:\
:manpath=/usr/share/man /usr/local/man:\
:nologin=/usr/sbin/nologin:\
:cputime=1h30m:\
:datasize=8M:\
:vmemoryuse=100M:\
:stacksize=2M:\
:memorylocked=4M:\
:memoryuse=8M:\
:filesize=8M:\
:coredumpsize=8M:\
```

```
:openfiles=24:\
:maxproc=32:\
:priority=0:\
:requirehome:\
:passwordtime=91d:\
:umask=022:\
:ignoretime@:\
:label=partition/13,mls/5,biba/10(5-15),lomac10[2]:
```

label 选项用以设定用户分级默认标签，该标签将由MAC执行。用户绝不会被允许更改该值，因此其从用户的观点看不是可选的。当然，在真实情况的配置中，管理员不会希望启用所有策略模块。我们建议您在实施以上配置之前阅读本章的其余部分。

注意：用户也许会在首次登录后更改其标签，尽管如此，这仅仅是策略的主观局限性。上面的例子告诉Biba策略，进程的最小完整性是为5，最大完整性为15，默认且有效的标签为10。进程将以10的完整性运行直至其决定更改标签，这可能是由于用户使用了setpmac命令(该操作将在登录时被Biba限制在一定用户范围之内)。

在所有情况下，修改login.conf之后，都必须使用cap_mkdb重编译登录分级capability数据库，这在接下来的例子和讨论中就会有所体现。

很多站点可能拥有数目可观的用户需要不同的用户分级，注意到这点是大有裨益的。深入来说就是需要事先做好计划，因为管理起来可能十分困难。

在FreeBSD以后的版本中，将包含一种将用户映射到标签的新方式，尽管如此，这也要到FreeBSD 5.3之后的某个时间才能实现。

15.4.1.3 网络接口和标签设定

也可以在网络接口上配置标签，以控制进出网络的数据流。在所有情况下，策略都会以适应对象的方式运作。例如，在biba中设置为高的用户，就不能访问标记为低的网络接口。

maclabel可以作为ifconfig的参数用于设置网络接口的MAC标签。例如：

```
# ifconfig bge0 maclabel biba/equal
```

将在bge(4)接口上设置biba/equal的MAC标签。当使用类似biba/high(low-high)这样的标签时，整个标签应使用引号括起来；否则将发生错误。

每一个支持标签的策略模块都提供了用于在网络接口上禁用该MAC标签的系统控制变量。将标签设置为equal的效果与此类似。请参见sysctl的输出、策略模块的联机手册，或本章接下来的内容，以了解更进一步的详情。

15.4.2 用单一标签还是多重标签？

默认情况下，系统采用的是singlelabel选项。但这对管理员意味着什么呢？两种策略之间存在很多的不同之处，它们在系统安全模型的灵活性方面，提供了不同的选择。

singlelabel只允许在每个subject或对象上使用一个标签，如biba/high。这降低了管理的开销，但也同时降低了支持标签的策略的灵活性。许多管理员可能更希望在安全策略中使用multilabel。

multilabel 选项允许每一个subject 或对象拥有各自独立的MAC 标签，起作用与标准的、只允许整个分区上使用一个的**singlelabel** 选项类似。**multilabel** 和**single** 标签选项只有对实现了标签功能的那些策略，如Biba、Lomac、MLS 以及SEBSD 才有意义。

很多情况下是不需要设置**multilabel** 的。考虑下列情形和安全模型：

- 使用了MAC 以及许多混合策略的FreeBSD web-服务器。
- 这台机器上的整个系统中只需要一个标签，即**biba/high**。此处的文件系统并不需要**multilabel** 选项，因为有效的label 只有一个。
- 因为这台机器将作为Web 服务器使用，因此应该以**biba/low** 运行Web 服务，以杜绝向上写。Biba 策略以及它如何运作将在稍后予以讨论，因此，如果您感觉前面的说明难以理解的话，请继续阅读下面的内容，再回来阅读这些内容就会有较为清晰的认识了。服务器可以使用设置为**biba/low** 的单独的分区，用于保持其运行环境的状态。这个例子中还省略了许多内容，例如，如何为数据配置访问限制、参数配置和用户的设置；它只是为前述的内容提供一个简单的例子。

如果打算使用非标签式策略，就不需要**multilabel** 选项了。这些策略包括**seeotheruids**、**portacl** 和**partition**。

另一个需要注意的事情是，在分区上使用**multilabel** 并建立基于**multilabel** 可能会提高系统管理的开销，因为文件系统中的所有对象都需要指定标签。这包括对目录、文件，甚至设备节点。

接下来的命令将在需要使用多个标签的文件系统上设置**multilabel**。这一操作只能在单用户模式下完成：

```
# tuneefs -l enable /
```

交换区不需要如此配置。

注意：某些用户可能会在根分区上配置**multilabel** 标志时遇到困难。如果发生这样的情况，请复查本章的第15.16 节。

15.4.3 用系统控制变量控制MAC

即使在没有加载任何模块的时候，也仍然有一些可以通过**sysctl** 接口来控制的MAC 特性。这些系统控制变量将在下面予以描述，在所有的例子中，数字一(1) 都表示启用，而数字零(0) 则表示禁用：

- **security.mac.enforce_fs** 表示在文件系统上启用MAC 策略。
- **security.mac.enforce_kld** 表示启用动态内核连接器(参见**kld(4)**) 上的MAC 内核连接策略。
- **security.mac.enforce_network** 表示启用MAC 网络策略。
- **security.mac.enforce_pipe** 表示启用MAC 管道策略。
- **security.mac.enforce_process** 表示启用使用进程间通讯机制的进程上的MAC 策略。
- **security.mac.enforce_socket** 表示启用socket 上的MAC 策略(参见**socket(2)** 联机手册)。
- **security.mac.enforce_system** 表示启用系统活动，如记账和重新启动的MAC 策略。
- **security.mac.enforce_vm** 表示启用虚拟内存系统上的MAC 策略。

注意: 每个策略或MAC 选项都支持通过系统控制变量来进行调整。这些选项通常都位于`security.mac.<策略名>`的树状结构之下。要查看所有的MAC 系统控制变量，可以使用下述命令：

```
# sysctl -da | grep mac
```

前面的所有基本MAC 策略默认都会启用。如果编入内核的模块被过分锁死，则可能无法与局域网或Internet 进行通讯，或发生其他严重问题。这也是为什么不完全鼓励将这些模块编入内核的原因。尽管这样做并不妨碍通过使用`sysctl` 来禁用这些策略，但以模块方式加载可以让管理员更容易地切换是否使用策略，而不需要构建和重新安装一套新系统。

15.5 模块配置

在MAC 框架中的每个模块，都可以像前述那样连编入内核，或作为运行时内核模块加载。推荐的做法，是通过在`/boot/loader.conf` 加入适当的设置，以便在系统启动时的初始化操作过程中加载这些模块。

接下来的一些小节，将讨论许多MAC 模块，并简单介绍它们的功能。此外，这一章还将介绍一些具体环境中的用例。某些模块支持一种称为标签(labeling) 的用法，它可以通过使用类似“允许做这个而不允许做那个” 的标签来实现访问控制。标签配置文件可以控制允许的文件访问方式、网络通讯，以及许多其他权限。在前一节中，我们已经展示了文件系统中如何通过`multilabel` 标志来启用基于文件或分区的访问控制的方法。

单标签配置在整个系统中只强制一个标签的限制，这也是`tunefs` 选项为什么是`multilabel` 的原因。

15.5.1 MAC seeotheruids 模块

模块名: `mac_seeotheruids.ko`

对应的内核配置: `options MAC_SEEOTHERUIDS`

引导选项: `mac_seeotheruids_load="YES"`

`mac_seeotheruids(4)` 模块模仿并扩展了`security.bsd.see_other_uids` 和`security.bsd.see_other_gids` `sysctl` 变量。这一模块并不需要预先配置标签，它能够透明地与其他模块协同工作。

加载模块之后，下列`sysctl` 变量可以用来控制其功能：

- `security.mac.seeotheruids.enabled` 将启用模块的功能，并使用默认的配置。这些默认设置将阻止用户看到其他用户的进程和socket。
- `security.mac.seeotheruids.specificgid_enabled` 将允许特定的组从这一策略中和面。要将某些组排除在这一策略之外，可以用`security.mac.seeotheruids.specificgid=xxx` `sysctl` 变量。前述例子中，`xxx` 应替换为希望不受限的组ID 的数值形式。
- `security.mac.seeotheruids.primarygroup_enabled` 可以用来将特定的主要组排除在策略之外。使用这一变量时，不能同时设置`security.mac.seeotheruids.specificgid_enabled`。

15.6 MAC bsdextended 模块

模块名: `mac_bsdextended.ko`

对应的内核配置: `options MAC_BSDEXTENDED`

引导选项: `mac_bsdextended_load="YES"`

`mac_bsdextended(4)` 模块能够强制文件系统防火墙策略。这一模块的策略提供了标准文件系统权限模型的一种扩展, 使得管理员能够建立一种类似防火墙的规则集, 以文件系统层次结构中的保护文件、实用程序, 以及目录。

这类策略可以通过工具 `ugidfw(8)` 工具来创建, 其语法类似 `ipfw(8)`。此外还可以通过使用 `libugidfw(3)` 库来开发其他的工具。

当使用这一模块时应极其小心; 不正确的使用将导致文件系统的某些部分无法访问。

15.6.1 例子

在加载了 `mac_bsdextended(4)` 模块之后, 下列命令可以用来列出当前的规则配置:

```
# ugidfw list
0 slots, 0 rules
```

如希望的那样, 目前还没有定义任何规则。这意味着一切都还可以访问。要创建一个阻止所有用户, 而保持 `root` 不受影响的规则, 只需运行下面的命令:

```
# ugidfw add subject not uid root new object not uid root mode n
```

注意: 在 FreeBSD 5.3 之前的版本中, `add` 参数并不存在。此时应使用 `set` 来代替它。请参见下面的命令例子。

这本身可能是一个很糟糕的主意, 因为它会阻止所有用户执行哪怕最简单的命令, 例如 `ls`。更富于爱心的规则可能是:

```
# ugidfw set 2 subject uid user1 object uid user2 mode n
# ugidfw set 3 subject uid user1 object gid user2 mode n
```

这将阻止任何 `user1` 对 `user2` 的主目录的全部访问, 包括目录列表。

`user1` 可以用 `not uid user2` 代替。这将同样的强制访问控制实施在所有用户, 而不是单个用户上。

注意: `root` 用户不会受到这些变动的影响。

我们已经给出了 `mac_bsdextended(4)` 模块如何帮助加强文件系统的大致介绍。要了解更进一步的信息, 请参见 `mac_bsdextended(4)` 和 `ugidfw(8)` 联机手册。

15.7 MAC ifoff 模块

模块名: `mac_ifoff.ko`

对应的内核配置: `options MAC_IFOFF`

引导选项: `mac_ifoff_load="YES"`

`mac_ifoff(4)` 模块完全是为了立即禁止网络接口, 以及阻止在系统初启时启用网络接口而设计的。它不需要再系统中配置任何标签, 也不依赖于其他MAC 模块。

绝大多数特性都可以通过调整下面的`sysctl` 来加以控制。

- `security.mac.ifoff.lo_enabled` 表示启用/禁用环回接口(`lo(4)`) 上的全部流量。
- `security.mac.ifoff.bpfrecv_enabled` 表示启用/禁用伯克利包过滤器(`bpf(4)`) 接口上的全部流量。
- `security.mac.ifoff.other_enabled` 将在所有其他接口启用/禁用网络。

最为常用的`mac_ifoff(4)` 用法之一是在不允许引导过程中出现网络流量的环境中监视网络。另一个建议的用法是撰写一个使用`security/aide` 的脚本, 以便自动地在受保护的目录中发现新的或修改过的文件时切断网络。

15.8 MAC portacl 模块

模块名: `mac_portacl.ko`

对应的内核配置: `MAC_PORTACL`

引导选项: `mac_portacl_load="YES"`

`mac_portacl(4)` 模块可以用来通过一系列`sysctl` 变量来限制绑定本地的TCP 和UDP 端口。本质上`mac_portacl(4)` 使得非-root 用户能够绑定到它所指定的特权端口, 也就是那些编号小于1024 的端口。

在加载之后, 这个模块将在所有的socket 上启用MAC 策略。可以调整下列一些配置:

- `security.mac.portacl.enabled` 将完全启用/禁用策略。²
- `security.mac.portacl.port_high` 将设置为`mac_portacl(4)` 所保护的最高端口号。
- `security.mac.portacl.suser_exempt` 如果设置为非零值, 表示将root 用户排除在策略之外。
- `security.mac.portacl.rules` 将指定实际的`mac_portacl` 策略; 请参见下文。

实际的`mac_portacl` 策略, 是在`security.mac.portacl.rules sysctl` 所指定的一个下列形式的字符串: `rule[,rule,...]` 其中可以给出任意多个规则。每一个规则的形式都是: `idtype:id:protocol:port`。这里的`idtype` 参数可以是`uid` 或`gid`, 分别表示将`id` 参数解释为用户id 或组id。`protocol` 参数可以用来确定希望应用到TCP 或UDP 协议上, 方法是把这一参数设置为`tcp` 或`udp`。最后的`port` 参数则给出了所指定的用户或组能够绑定的端口号。

注意: 由于规则集会直接由内核加以解释, 因此只能以数字形式表示用户ID、组ID, 以及端口等参数。换言之, 您不能使用用户、组, 或端口服务的名字来指定它们。

默认情况下, 在类-UNIX 系统中, 编号小于1024 的端口只能为特权进程使用或绑定, 也就是那些以root 身份运行的进程。为了让`mac_portacl(4)` 能够允许非特权进程绑定低于1024 的端口, 就必须首先禁

用标准的UNIX 限制。这可以通过把sysctl(8) 变量net.inet.ip.portrange.reservedlow 和net.inet.ip.portrange.reservedhigh 设置为0 来实现。

请参见下面的例子，或mac_portacl(4) 联机手册中的说明，以了解进一步的信息。

15.8.1 例子

下面的例子更好地展示了前面讨论的内容：

```
# sysctl security.mac.portacl.port_high=1023
# sysctl net.inet.ip.portrange.reservedlow=0 net.inet.ip.portrange.reservedhigh=0
```

首先我们需要设置使mac_portacl(4) 管理标准的特权端口，并禁用普通的UNIX 绑定限制。

```
# sysctl security.mac.portacl.suser_exempt=1
```

您的root 用户不应因此策略而失去特权，因此请把security.mac.portacl.suser_exempt 设置为一个非零的值。现在您已经成功地配置了 mac_portacl(4) 模块，并使其默认与类-UNIX 系统一样运行了。

```
# sysctl security.mac.portacl.rules=uid:80:tcp:80
```

允许UID 为80 的用户(正常情况下，应该是www 用户) 绑定到80 端口。这样www 用户就能够运行web 服务器，而不需要使用root 权限了。

```
# sysctl security.mac.portacl.rules=uid:1001:tcp:110,uid:1001:tcp:995
```

允许UID 为1001 的用户绑定TCP 端口110 (“pop3”) 和995 (“pop3s”)。这样用户就能够启动接受来发到110 和995 的连接请求的服务了。

15.9 包含标签功能的MAC 策略

接下来的几节中，将讨论使用标签的MAC 策略。

这一章从此处开始将集中于对mac_biba(4)、mac_lomac(4)、mac_partition(4)，以及mac_mls(4) 的介绍。

注意：此处提供的仅仅是示范的配置，不应用于在实际的生产环境中实施。这份文档的目标是在展示配置写法的同时，以实例的形式，对如何实施和进行测试予以介绍。

要让配置正确工作，首先需要进行一些准备工作。

15.9.1 准备使用标签策略

下述修改需要在login.conf 文件上实施：

- 需要增加一个insecure 级，或其他类似类型的分级。这里，insecure 级并不是必需的，只是作为例子加以展示；不同的配置完全可以使用其他的分级名称。
- insecure 级应包含下列配置和定义。其中的许多内容都可以根据需要修改，但定义了默认标签的行都是必需的，您应留下它们。

```

insecure:\
:copyright=/etc/COPYRIGHT:\
:welcome=/etc/motd:\
:setenv=MAIL=/var/mail/$,BLOCKSIZE=K:\
:path=~:/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin:\
:manpath=/usr/share/man /usr/local/man:\
:nologin=/usr/sbin/nologin:\
:cputime=1h30m:\
:datasize=8M:\
:vmemoryuse=100M:\
:stacksize=2M:\
:memorylocked=4M:\
:memoryuse=8M:\
:filesize=8M:\
:coredumpsize=8M:\
:openfiles=24:\
:maxproc=32:\
:priority=0:\
:requirehome:\
:passwordtime=91d:\
:umask=022:\
:ignoretime@:\
:label=partition/13,mls/5,biba/low:

```

需要在login.conf(5)上执行cap_mkdb(1)之后，用户才能够切换到新的分级。

root 用户名也应出现在某个登录级中；否则，root 执行每一个命令的时候，都需要使用setpmac。

警告：重建login.conf 数据库可能会导致daemon 级在稍后发生某些错误。简单地去掉注释掉daemon 的注释符并重建数据库，会有助于消除这类问题。

- 确保将要使用MAC 标签的所有分区，都能够支持multilabel。我们必须这样做，因为这里的很多例子中都包含了不同的、用于测试目的的标签。作为预防性措施之一，您应复查mount 命令的输出结果。
- 把将被应用更高级别的安全机制的那些用户转到新的用户class 中。运行pw(8) 或vipw(8) 可以完成这样的任务。

15.10 MAC partition (分区) 模块

模块名: mac_partition.ko

对应的内核配置: options MAC_PARTITION

引导选项: mac_partition_load="YES"

mac_partition(4) 策略将把进程基于其MAC 标签放到特定的“partitions” (分区) 中。这是一种特殊类型的jail(8)，但对两者进行比较意义不大。

这个模块应加到loader.conf(5) 文件中，以便在启动过程中启用这些规则。

绝大多数这一策略的配置是通过setpmac(8)工具来完成的，它将在后面介绍。这个策略可以使用下面的sysctl：

- security.mac.partition.enabled 将启用强制的MAC进程partitions。

当启用了这个规则时，用户将只被允许看到他们自己的进程，而无法使用某些工具。例如，在前面提到的insecure class 中的用户，将无法使用top命令，以及其他必需生成进程的命令。

要设置或删除partition标签中的工具，需要使用setpmac：

```
# setpmac partition/13 top
```

这将把top命令加入到insecure class 中的用户的标签集。注意，所有由insecure class 中的用户产生的进程，仍然会留在partition/13标签中。

15.10.1 例子

下面的命令将显示partition标签以及进程列表：

```
# ps Zax
```

接下来的这个命令将允许察看其他用户的进程partition标签，以及那个用户正在运行的进程：

```
# ps -ZU trhodes
```

注意：除非加载了mac_seeotheruids(4)策略，否则用户就看不到root的标签。

非常手工化的实现，可能会在/etc/rc.conf中禁用所有的服务，并用脚本来按不同的标签来启动它们。

注意：下面的几个策略支持基于所给出的三种标签的完整性设定。这些选项，连同它们的限制，在模块的联机手册中进行了进一步介绍。

15.11 MAC Multi-Level 安全模块

模块名：mac_mls.ko

对应的内核配置：options MAC_MLS

引导选项：mac_mls_load="YES"

mac_mls(4)策略，通过严格控制信息流向来控制系统中主体和对象的访问。

在MLS环境中，“clearance”（透明度）级别会在每一个主体或对象标签上进行设置，连同对应的区间。由于这些透明度或敏感度可以有六千多个层次，因此为每一个主体或对象进行配置将是一件让任何系统管理员都感到头疼的任务。所幸的是，这个策略中已经包含了三个“立即可用的”标签。

这些标签是`mls/low`、`mls/equal` 以及`mls/high`。由于这些标签已经在联机手册中进行了介绍，这里只给出简要的说明：

- `mls/low` 标签包含了最低配置，从而允许其他对象支配它。任何标记为`mls/low` 的对象将是地透明度的，从而不允许访问更高级别的信息。此外，这个标签也阻止拥有较高透明度的对象向其写入或传递信息。
- `mls/equal` 标签应放到不希望使用这一策略的对象上。
- `mls/high` 标签是允许的最高级别透明度。指定了这个标签的对象将支配系统中的其他对象；但是，它们将不允许向较低级别的对象泄露信息。

MLS 提供了：

- 提供了一些非层次分类的层次安全模型；
- 固定规则：不允许向上读，不允许向下写(主体可以读取同级或较低级别的对象，但不能读取高级别的。类似地，主体可以向同级或较高级写，而不能向下写)；
- 保密(防止不适当的数据透露)；
- 系统设计的基础要点，是在多个敏感级别之间并行地处理数据(而不泄露秘密的和机密的信息)。

下列`sysctl` 可以用来配置特殊服务和接口：

- `security.mac.mls.enabled` 用来启用/禁用MLS 策略。
- `security.mac.mls.ptys_equal` 将所有的`pty(4)` 设备标记为`mls/equal`。
- `security.mac.mls.revocation_enabled` 可以用来在标签转为较低`grade` 时撤销对象访问权。
- `security.mac.mls.max_compartments` 可以用来设置对象的最大区间层次；基本上，这也就是系统中所允许的最大区间数。

要管理MLS 标签，可以使用`setfmac(8)` 命令。要在对象上指定标签，需要使用下面的命令：

```
# setfmac mls/5 test
```

下述命令用于取得文件`test` 上的MLS 标签：

```
# getfmac test
```

这是MLS 策略特性的一个摘要。另一种方法是建立一个主策略文件，把它放到`/etc`，指定MLS 策略信息，并作为`setfmac` 命令的输入。这一方法将在其他策略之后进行介绍。

观察：拥有较低`clearance` 的对象不能够观察较高`clearance` 的进程。基本的策略是在每一个不应被读取的对象上应用`mls/high`，即使需要在其上进行写操作。在每所有不应被写的对象上应用`mls/low`，即使需要在其上进行读操作。最后，在其他对象上应用`mls/equal`。所有标记为`insecure` 的用户应被设置为`mls/low`。

15.12 MAC Biba 模块

模块名：`mac_biba.ko`

对应的内核配置：`options MAC_BIBA`

引导选项: `mac_biba_load="YES"`

`mac_biba(4)` 模块将加载MAC Biba 策略。这个策略与MLS 策略非常类似，只是信息流的规则有些相反的地方。通俗地说，这就是防止敏感信息向下传播，而MLS 策略则是防止敏感信息的向上传播；因而，这一节的许多内容都可以同时应用于两种策略。

在Biba 环境中，“integrity”（完整性）标签，将设置在每一个subject 或对象上。这些标签是按照层次级别建立的。如果对象或subject 的级别被提升，其完整性也随之提升。

被支持的标签是**biba/low**，**biba/equal** 以及**biba/high**；解释如下：

- **biba/low** 标签被认为是对象或subject 所能拥有的最低完整性级别。在对象或subject 上设置它，将阻止其在更高级别对象或subject 的写操作，虽然读仍被允许。
- **biba/equal** 标签只应在那些希望排除在策略之外的对象上设置。
- **biba/high** 允许向较低标签的对象上写，但不允许读那些对象。推荐在那些可能影响整个系统完整性的对象上设置这个标签。

Biba 提供了：

- 层次式的完整性级别，并提供了一组非层次式的完整性分类；
- 固定规则：不允许向上写，不允许向下读(与MLS 相反)。subject 可以在它自己和较低的级别写，但不能向更高级别实施写操作。类似地，subject 也可以读在其自己的，或更高级别的对象，但不能读取较低级别的对象；
- 完整性(防止对数据进行不正确的修改)；
- 完整性级别(而不是MLS 的敏感度级别)。

下列sysctl 可以用于维护Biba 策略。

- `security.mac.biba.enabled` 可以用来在机器上启用/禁用是否实施Biba 策略。
- `security.mac.biba.ptys_equal` 可以用来在pty(4) 设备上禁用Biba 策略。
- `security.mac.biba.revocation_enabled` 将在支配subject 发生变化时强制撤销对对象的访问权。

要操作系统对象上的Biba 策略，需要使用**setfmac** 和**getfmac** 命令：

```
# setfmac biba/low test
# getfmac test
test: biba/low
```

观察：较低完整性级别的subject 不能向较高完整性级别的subject 写；较高完整性级别的subject 也不能观察或读取较低完整性级别的对象。

15.13 MAC LOMAC 模块

模块名: `mac_lomac.ko`

对应的内核配置: `options MAC_LOMAC`

引导选项: `mac_lomac_load="YES"`

和MAC Biba 策略不同，`mac_lomac(4)` 策略只允许在降低了完整性级别之后，才允许在不破坏完整性规则的前提下访问较低完整性级别的对象。

MAC 版本的Low-watermark 完整性策略不应与较早的`lomac(4)` 实现相混淆，除了使用浮动的标签来支持subject 通过辅助级别compartment 降级之外，其工作方式与Biba 大体相似。这一词要的compartment 以`[auxgrade]` 的形式出现。当指定包含辅助级别的`lomac` 策略时，其形式应类似于：`lomac/10[2]` 这里数字二(2) 就是辅助级别。

MAC LOMAC 策略依赖于系统对象上存在普适的标签，这样就允许subject 来从较低完整性级别的对象读取，并对subject 的标签降级，以防止其在之后写高完整性级别的对象。这就是前面讨论的`[auxgrade]` 选项，因此这个策略能够提供更大的兼容性，而所需要的初始配置也要比Biba 少。

15.13.1 例子

与Biba 和MLS 策略类似；`setfmac` 和`setpmac` 工具可以用来在系统对象上放置标签：

```
# setfmac /usr/home/trhodes lomac/high[low]
# getfmac /usr/home/trhodes lomac/high[low]
```

注意，这里的辅助级别是`low`，这一特性只由MAC LOMAC 策略提供。

15.14 通过使用MAC 来实现安全的环境

下面给出了通过多种MAC 模块，并正确地配置策略来实现安全环境的例子。这只是一个测试，因此不应被看作四海一家的解决之道。仅仅实现一个策略，而忽略它不能解决任何问题，并可能在生产环境中产生灾难性的后果。

在开始这些操作之前，必须在每一个文件系统上设置`multilabel` 选项，这些操作在这一章开始的部分进行了介绍。不完成这些操作，将导致错误的结果。

15.14.1 创建一个insecure (不安全) 用户Class

首先是在`/etc/login.conf` 文件中加入一个新的用户class：

```
insecure:\
:copyright=/etc/COPYRIGHT:\
:welcome=/etc/motd:\
:setenv=MAIL=/var/mail/$,BLOCKSIZE=K:\
:path=~:/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin
:manpath=/usr/share/man /usr/local/man:\
:nologin=/usr/sbin/nologin:\
:cputime=1h30m:\
:datasize=8M:\
:vmemoryuse=100M:\
:stacksize=2M:\
:memorylocked=4M:\
:memoryuse=8M:\
:filesize=8M:\
:coredumpsize=8M:\
:openfiles=24:\
```

```
:maxproc=32:\
:priority=0:\
:requirehome:\
:passwordtime=91d:\
:umask=022:\
:ignoretime@:\
:label=partition/13,mls/5:
```

并在default用户class中加入:

```
:label=mls/equal,biba/equal,partition/15:
```

一旦完成上述操作,就需要运行下面的命令来重建数据库:

```
# cap_mkdb /etc/login.conf
```

15.14.2 配合正确的模块启动

在/boot/loader.conf中加入下面的配置,以保证系统初始化过程中加载那些模块:

```
mac_biba_load="YES"
mac_mls_load="YES"
mac_seeotheruids_load="YES"
mac_partition_load="YES"
```

15.14.3 将所有用户设置为不安全的

所有非root或系统的用户,现在需要一个登录class。登录class是必须的,否则这些用户将被禁止使用类似vi(1)这样的命令。下面的sh脚本应能完成这个工作:

```
# for x in `awk -F: '($3 >= 1001) && ($3 != 65534) { print $1 }' \
/etc/passwd`; do pw usermod $x -L insecure; done;
```

改完后,需要在/etc/master.passwd上运行cap_mkdb命令。

15.14.4 完成配置

现在需要创建一个contexts文件;下面的例子来自Robert Watson的策略示例,应放到/etc/policy.contexts中。

这是系统中的默认 BIBA/MLS 策略。

```
. *                biba/high,mls/high
/sbin/dhclient     biba/high(low),mls/high(low)
/dev(/.*)?         biba/equal,mls/equal
# This is not an exhaustive list of all "privileged" devices.
/dev/mdctl         biba/high,mls/high
/dev/pci           biba/high,mls/high
/dev/k?mem         biba/high,mls/high
```

```

/dev/io                biba/high,mls/high
/dev/agp.*             biba/high,mls/high
(/var)?/tmp(/.*)?     biba/equal,mls/equal
/tmp/\.X11-unix       biba/high(equal),mls/high(equal)
/tmp/\.X11-unix/. *   biba/equal,mls/equal
/proc(/.*)?           biba/equal,mls/equal
/mnt.*                biba/low,mls/low
(/usr)?/home          biba/high(low),mls/high(low)
(/usr)?/home/. *     biba/low,mls/low
/var/mail(/.*)?       biba/low,mls/low
/var/spool/mqueue(/.*)? biba/low,mls/low
(/mnt)?/cdrom(/.*)?   biba/high,mls/high
(/usr)?/home/(ftp|samba)(/.*)? biba/high,mls/high
/var/log/sendmail\st  biba/low,mls/low
/var/run/utmp         biba/equal,mls/equal
/var/log/(lastlog|wtmp) biba/equal,mls/equal

```

这个策略将通过在信息的上下行流上，根据左边列出的工具和目录实施限制来强制安全。

可以通过下面的命令将其读入我们的系统：

```

# setfsmac -ef /etc/policy.contexts /
# setfsmac -ef /etc/policy.contexts /usr

```

注意：上述文件系统布局，可能随环境而略有不同。

在/etc/mac.conf 文件中的main 小节需要进行下面的修改：

```

default_labels file ?biba,?mls
default_labels ifnet ?biba,?mls
default_labels process ?biba,?mls,?partition
default_labels socket ?biba,?mls

```

15.14.5 对配置进行测试

使用adduser 命令来增加用户，并把这个用户放到insecure class 中，以用于测试。

下面的例子中混合了root 和普通用户tests 的测试结果，并使用提示符来区别它们。

15.14.5.1 基本的标签测试

```

% getpmac
biba/15(15-15),mls/15(15-15),partition/15
# setpmac partition/15,mls/equal top

```

注意：在启动其他top 进程之前应该首先杀掉我们的这个top 进程。

15.14.5.2 MAC Seeotheruids 测试

```
% ps Zax
biba/15(15-15),mls/15(15-15),partition/15 1096 #C: S 0:00.03 -su (bash)
biba/15(15-15),mls/15(15-15),partition/15 1101 #C: R+ 0:00.01 ps Zax
```

我们应该看不到其他用户的进程。

15.14.5.3 MAC Partition 测试

为其他测试禁用MAC seeotheruids 策略:

```
# sysctl security.mac.seeotheruids.enabled=0
% ps Zax
LABEL PID TT STAT TIME COMMAND
biba/equal(low-high),mls/equal(low-high),partition/15 1122 #C: S+ 0:00.02 top
biba/15(15-15),mls/15(15-15),partition/15 1096 #C: S 0:00.05 -su (bash)
biba/15(15-15),mls/15(15-15),partition/15 1123 #C: R+ 0:00.01 ps Zax
```

现在所有的用户都应能够看到他们的partition 中的所有进程了。

15.14.5.4 测试Biba 和MLS 标签

```
# setpmac partition/15,mls/equal,biba/high\ (high-high\ ) top
% ps Zax
LABEL PID TT STAT TIME COMMAND
biba/high(high-high),mls/equal(low-high),partition/15 1251 #C: S+ 0:00.02 top
biba/15(15-15),mls/15(15-15),partition/15 1096 #C: S 0:00.06 -su (bash)
biba/15(15-15),mls/15(15-15),partition/15 1157 #C: R+ 0:00.00 ps Zax
```

Biba 策略允许我们读取标签为较高标签的对象。

```
# setpmac partition/15,mls/equal,biba/low top
% ps Zax
LABEL PID TT STAT TIME COMMAND
biba/15(15-15),mls/15(15-15),partition/15 1096 #C: S 0:00.07 -su (bash)
biba/15(15-15),mls/15(15-15),partition/15 1226 #C: R+ 0:00.01 ps Zax
```

Biba 策略不允许读取低标签的对象；但MLS 允许此类操作。

```
% ifconfig bge0 | grep maclabel
maclabel biba/low(low-low),mls/low(low-low)
% ping -c 1 192.0.34.166
PING 192.0.34.166 (192.0.34.166): 56 data bytes
ping: sendto: Permission denied
```

由于这个原因，用户将无法ping example.com 或其他主机。

要防止发生这类错误，需要运行下面的命令：

```
# sysctl security.mac.biba.trust_all_interfaces=1
```

这将把默认的接口标签置为不安全模式，这样就不会强制使用Biba策略了。

```
# ifconfig bge0 maclabel biba/equal\(\low-high\),mls/equal\(\low-high\)
% ping -c 1 192.0.34.166
PING 192.0.34.166 (192.0.34.166): 56 data bytes
64 bytes from 192.0.34.166: icmp_seq=0 ttl=50 time=204.455 ms
--- 192.0.34.166 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max/stddev = 204.455/204.455/204.455/0.000 ms
```

通过设置更为正确的标签，我们就能够发出ping请求了。

现在建立几个文件来测试一下读写操作：

```
# touch test1 test2 test3 test4 test5
# getfmac test1
test1: biba/equal,mls/equal
# setfmac biba/low test1 test2; setfmac biba/high test4 test5; \
  setfmac mls/low test1 test3; setfmac mls/high test2 test4
# setfmac mls/equal,biba/equal test3 && getfmac test?
test1: biba/low,mls/low
test2: biba/low,mls/high
test3: biba/equal,mls/equal
test4: biba/high,mls/high
test5: biba/high,mls/equal
# chown testuser:testuser test?
```

所有这些文件应属于testuser用户。现在测试一下读操作：

```
% ls
test1  test2  test3  test4  test5
% ls test?
ls: test1: Permission denied
ls: test2: Permission denied
ls: test4: Permission denied
test3  test5
```

没有允许我们observe pairs；例如：(biba/low,mls/low)，(biba/low,mls/high)以及(biba/high,mls/high)。因此，很显然读操作应该被拒绝。现在测试一下写操作：

```
% for i in 'echo test*'; do echo 1 > $i; done
-su: test1: Permission denied
-su: test4: Permission denied
-su: test5: Permission denied
```

和读操作的尝试类似，write pairs 不应允许这类操作；例如：(biba/low,mls/high)和(biba/equal,mls/equal)。

```
% cat test?
cat: test1: Permission denied
cat: test2: Permission denied
1
cat: test4: Permission denied
```

现在以root 身份进行:

```
# cat test2
1
```

15.15 另一个例子: 使用MAC 来约束Web 服务器

将配置一个独立的位置来保存web 数据, 并只允许特定的用户来访问。这样, 拥有biba/high 的进程就能够访问web 数据了。

首先需要创建一个用于保存web 数据的目录:

```
# mkdir /usr/home/cvs
```

接下来使用cvs 来对其进行初始化:

```
# cvs -d /usr/home/cvs init
```

第一件事是启用biba 策略, 因此应把mac_biba_enable="YES" 加入到/boot/loader.conf。当然, 这样做的前提是在内核中启用了MAC 支持。

从现在开始, 整个系统中的所有对象, 都会默认设置为biba/high。

必须在login.conf 中的default (默认) 用户class 上进行下列修改:

```
:ignoretime@:\
:umask=022:\
:label=biba/high:
```

现在每个用户都需要放到default class 中; 类似下面的命令:

```
# for x in `awk -F: '($3 >= 1001) && ($3 != 65534) { print $1 }' \
/etc/passwd`; do pw usermod $x -L default; done;
```

可以很快地完成这个工作。

接下来建立另一个class, web, 它是default 的一个副本, 但将标签设置为biba/low。

建立一个用于在cvs 中的主web 库的数据上工作的用户。这个用户必须被放到我们新建的那个登录class, web 中。

由于所有地方的默认值都是biba/high, 因此库也是一样的。web 数据必须同样地被用户读写; 然而, 由于我们的web 服务器将要提供biba/high 用户需要访问的数据, 因此必须将所有这些数据降级。

完成这些事情的最好工具是sh(1) 和cron(8), 它们已经由FreeBSD 提供了。下面的脚本将完成全部所需的工作:

```
PATH=/bin:/usr/bin:/usr/local/bin; export PATH;
CVSROOT=/home/repo; export CVSROOT;
cd /home/web;
cvs -qR checkout -P htdocs;
exit;
```

注意: 很多时候, `cvs ld tag` 必须放到web 站点的数据文件中。

现在可以把这个脚本放到web 的主目录中, 并增加下面的crontab(1) 项:

```
# Check out the web data as biba/low every twelve hours:
0 * /12 * * * web /home/web/checkout.sh
```

这样, 这台机器上每十二小时都会检出一HTML 源代码。

Web 服务器的默认启动方式也必须进行修改, 以便以biba/low 来启动服务。这可以通过对/usr/local/etc/rc.d/apache.sh 脚本进行下面的修改来完成:

```
command="setpmac biba/low /usr/local/sbin/httpd"
```

Apache 配置必须进行修改, 以便在biba/low 策略下工作。因为这时软件必须配置为在设置了biba/low 的目录中记录日志, 否则将返回access denied 错误。

注意: 完全按照上面的例子进行配置的话, docroot 应被设置为/home/web/htdocs; 否则, Apache 将无法查找其提供文档的目录。

同时, 也需要修改一些其他的配置变量, 包括PID 文件, Scoreboardfile, DocumentRoot、日志文件的位置, 以及其他需要写权限的配置。使用biba 时, 所有发生在没有 配置为biba/low 的写操作都会失败。

15.16 MAC 框架的故障排除

在开发过程中, 有一些用户报告了正常配置下出现的问题。其中的一些问题如下所示:

15.16.1 无法在/ 上启用multilabel 选项

multilabel 标志在根(/) 分区上没有保持启用状态!

看起来每五十个用户中就有一个遇到这样的问题, 当然, 在我们的初始配置过程中也出现过这样的问题。更进一步的观察使得我相信这个所谓的“bug” 是由于文档中不确切的描述, 或对其产生的误解造成的。无论它是因为什么引发的, 下面的步骤应该能够解决此问题:

1. 编辑/etc/fstab 并将根分区设置为ro, 表示只读。
2. 重新启动并进入单用户模式。
3. 在/ 上运行tune2fs -l enable
4. 重新启动并进入正常的模式。
5. 运行mount -urw / 并把/etc/fstab 中的ro 改回rw, 然后再次重新启动。
6. 再次检查来自mount 的输出, 已确认根文件系统上正确地设置了multilabel。

15.16.2 在MAC 之后无法启动X11 了

在使用MAC 建立安全的环境之后，就无法启动X 了！

这可能是由于MAC partition 策略，或者对某个MAC 标签策略进行了错误的配置导致的。要调试这个问题，请尝试：

1. 检查错误信息；如果用户是在insecure class 中，则partition 策略就可能导致问题。尝试将用户的class 重新改为default class，并使用cap_mkdb 命令重建数据库。如果这无法解决问题，则进入第二步。
2. 仔细检查标签策略。确认针对有问题的用户的策略是正确的，特别是X11 应用，以及/dev 项。
3. 如果这些都无法解决问题，将出错消息和对您的环境的描述，发送到TrustedBSD (<http://www.TrustedBSD.org>) 网站上的TrustedBSD 讨论邮件列表，或者FreeBSD 一般问题邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-questions>) 邮件列表。

15.16.3 Error: _secure_path(3) cannot stat .login_conf

当我试图从root 切换到其同中的其他用户时，出现了错误提示_secure_path: unable to state .login_conf。

这个提示通常在用户拥有高于它将要成为的那个用户的标签设定时出现。例如，如果系统上的一个用户joe 拥有默认的biba/low 标签，而root 用户拥有biba/high，它也就不能查看joe 的主目录，无论root 是否使用了su 来成为joe。这种情况下，Biba 完整性模型，就不会允许root 查看在较低完整性级别中的对象。

15.16.4 root 用户名被破坏了！

在普通模式，甚至是单用户模式中，root 不被识别。whoami 命令返回了0 (零) 而su 则提示who are you?。到底发生了什么？

标签策略被禁用可能会导致这样的问题，无论是通过sysctl(8) 或是卸载了策略模块。如果打算禁用策略，或者临时禁用它，则登录性能数据库需要重新配置，在其中删除label 选项。仔细检查login.conf 以确保所有的label 选项都已经删除，然后使用cap_mkdb 命令来重建数据库。

备注

1. 其它情况也能导致不同的执行失败。例如，文件可能并不隶属于尝试重标签该文件的用户，对象可能不存在或是只读的。文件的某一属性、进程的某一属性或新的自定义标签值的某一属性，将使集权式策略不允许进程重标签文件。例如：低完整性的用户试图修改高完整性文件的标签，或者低完整性的用户试图将低完整性文件的标签改为高完整性标签。
2. 由于一个bug，security.mac.portacl.enabled sysctl 变量在FreeBSD 5.2.1 和更早版本上并不起作用。

第16章

安全事件审计

原作Tom Rhodes.

16.1 概述

在FreeBSD 7-CURRENT 开发分支上包含了对于基于POSIX.1e 草案，Sun 所发布的BSM API 及文件格式的时间审计支持。事件审计功能，使得选择性地对涉及安全的系统事件进行记录成为可能，这可进一步为出现问题之后的验尸式分析、系统监控，以及入侵检测所用。经过在FreeBSD 7-CURRENT 中一段时间的沉淀之后，这一支持将被合并到FreeBSD 6-STABLE 并出现在之后的发行版中。

警告: FreeBSD 中的审计机制目前还是试验性的，只有在仔细考量部署风险之后，才应在生产系统上部署这一试验性的软件。

这一章将主要关注与安装和配置事件审计机制。同时，为了方便读者，也介绍了审计策略，并给出了一个实例加以说明。

读完这章，您将了解：

- 事件审计是什么，以及它如何工作。
- 如何在FreeBSD 上为用户和进程配置事件审计。

阅读这章之前，您应该：

- 理解UNIX 和FreeBSD 的基础知识(第3 章)。
- 熟悉关于内核配置和编译的基本方法(第8 章)。
- 熟悉安全知识以及如何在FreeBSD 运用它们(第14 章)。

警告: 事件审计可能会产生大量的日志文件数据，在某些配置中，可能每周都会产生超过数GB 的数据。管理员应完整地阅读完这一章的内容，以避免由于不当配置产生的自作自受型DoS。

在FreeBSD 中的事件审计机制，与SunTM 的基本安全模块，即BSM 库类似。因此，这些配置与Solaris 和Mac OS X/Darwin 操作系统之间可以完全互换。

16.2 您需要了解的一些关键术语

在开始阅读这章之前，首先需要解释一些关键的术语。这是为了清除一些由于引入新术语而带来的困惑和阅读障碍。

- **事件(event)**: 可审计事件是指能够被审计子系统记录的事件。管理员可以配置审计哪些事件。举例说来, 与安全有关的事件包括创建文件、建立网络连接, 以及以某一用户身份登录, 等等。任何事件必属于“有主(attributable)”, 即可以最终归于某一用户身份, 或“无主(non-attributable)”二者之一。举例而言, 无主事件可以是任何发生在登录过程成功之前的事件, 例如失败的登录尝试, 等等。
- **类(class)**: 事件可以指定为一个或多个类, 通常这是基于事件的一般类别来进行的, 例如“创建文件”、“访问文件”, 或“网络”。登录和注销事件, 则指定为`lo`类。通过使用类, 管理员能够指定更高层次的审计规则, 而无需一一指定每个需要进行记录的可审计操作。
- **记录(record)**: 记录是描述安全事件的一个日志项。典型的记录包括记录事件类型、与事件有关的主题(用户)信息、时间信息、相关的任何对象信息, 以及事件所关联的操作是否成功的信息。
- **账目(trail)**: 审计账目, 或日志文件, 包含了一系列描述安全事件的审计记录。典型情况下, 审计账目基本上是以事件发生的时间顺序记录的。只有获得授权的进程, 才能够向审计账目中提交记录。
- **前缀(prefix)**: 前缀是指被用来开关对成功和失败事件审计的配置元素。

16.3 安装审计支持

对于事件审计的支持, 已经随标准的`installworld`过程完成。管理员可以通过查看`/etc/security`的内容来确认这一点。您应能看到一些名字以`audit`开头的文件, 例如`audit_event`。

此外, 还必须加入内核部分的支持。这可以通过在本地的内核配置文件中加入下面一行来实现:

```
options AUDIT
```

接下来, 您应按照第8章中所介绍的步骤来完成一次内核的编译和安装。

一旦完成, 可以通过下列`rc.conf(5)`配置来启动审计服务:

```
auditd_enable="YES"
```

默认不启用的那些功能可以在此处以`auditd_flags`选项来增加。

16.4 对审计进行配置

所有用于安全审计的配置文件, 都可以在`/etc/security`找到。要启动审计服务, 下面这些文件必须存在:

- `audit_class` - 包含对于审计类的定义。
- `audit_control` - 控制审计子系统的特性, 例如默认审计类、在审计日志所在的卷上保留的最小空间, 等等。
- `audit_event` - 定义内核审计事件。它们多数都对应于某些系统调用。
- `audit_user` - 针对特定用户进行的事件审计。没有在此处指定的用户, 则按控制配置文件中的默认配置处理。
- `audit_warn` - 由`auditd`调用, 用于在意外情况, 如用于记录审计事件的空间过低时发出警告的`shell`脚本。

16.4.1 审计文件的语法

配置文件的语法看上去可能有点怪异，尽管用起来会很容易。管理员必须非常谨慎的一件事是改变系统的默认值，因为这样做可能会造成潜在的无法正确收集审计数据的问题。

审计子系统能够同时接受配置语法中的长短名字。接下来，我们将给出语法表。

下面是所支持的全部审计类：

- **all** - **all** - 设置全部审计标志。
- **ad** - **administrative** - 所有在系统上所进行的管理性操作。
- **ap** - **application** - 应用程序定义的动作。
- **cl** - **file_close** - 审计对**close**系统调用的操作。
- **ex** - **exec** - 审计程序或实用工具的执行。
- **fa** - **file_attr_acc** - 审计访问对象属性，例如**stat(1)**、**pathconf(2)**以及类似事件。
- **fc** - **file_creation** - 审计创建了文件的事件。
- **fd** - **file_deletion** - 审计所发生的文件删除事件。
- **fm** - **file_attr_mod** - 审计文件属性发生变化的事件，例如**chown(8)**、**chflags(1)**、**flock(2)**，等等。
- **fr** - **file_read** - 审计读取数据、文件以读方式打开等事件。
- **fw** - **file_write** - 审计写入数据、文件以写方式打开等事件。
- **io** - **ioctl** - 审计对**ioctl(2)**系统调用的使用。
- **ip** - **ipc** - 审计各种形式的进程间通信(IPC)，包括POSIX管道和System V IPC操作。
- **lo** - **login_logout** - 审计系统中发生的**login(1)**和**logout(1)**事件。
- **na** - **non_attrib** - 审计无法归类的事件。
- **no** - **no_class** - 空类，用于禁用事件审计。
- **nt** - **network** - 与网络操作有关的事件，例如**connect(2)**和**accept(2)**。
- **ot** - **other** - 审计各类杂项事件。
- **pc** - **process** - 审计进程操作，例如**exec(3)**和**exit(3)**。

下面是全部支持的审计前缀：

- **none** - 同时审计事件的成功和失败。例如，秩序列出一个事件类就可以同时审计其成功或失败。
- **+** - 只审计成功事件。
- **-** - 只审计失败事件。

警告：使用**all**类，无论是正还是负号作为前缀，都会以极快的速度产生大量的数据。

其他用于改变默认配置值得前缀：

- **^-** - 禁用对于失败事件的审计。

- `^+` - 启用对于成功事件的审计。
- `^-` - 同时禁用成功和失败事件的审计。

16.4.2 配置文件

多数情况下，在配置审计系统时，管理员只需修改两个文件：`audit_control` 和 `audit_user`。第一个文件控制系统级的审计参数，以及所有有主或无主事件的默认参数。第二个文件用于调整针对具体用户的审计级别和性质。

16.4.2.1 传说中的 `audit_control` 文件

`audit_control` 文件包含了一些基本的默认值，管理员通常会希望加以修改，有时甚至是设置一些新的配置。察看这个文件的内容，我们会发现：

```
dir:/var/audit
flags:lo
minfree:20
naflags:lo
```

这里的 `dir` 用于设置审计日志的默认存放目录。审计通常都会配置为保存在一个专用的文件系统之下，以避免审计系统与其它子系统在文件系统满的时候所产生的冲突。

`flags` 选项则用来设置系统级的默认。目前的设置，即 `lo` 配置审计所有的 `login(1)` 和 `logout(1)` 动作。而更为复杂的例子，`lo,ad,-all,^-fa,^-fc,^-cl` 表示审计所有的系统 `login(1)` 和 `logout(1)` 动作、所有管理动作，以及所有系统中失败的动作，但最后禁用对 `fa`、`fc`，以及 `cl` 的失败常是。尽管 `-all` 会打开所有事件的失败常是，但之后的选项中的 `^-` 前缀则会改变相应的设置。

请注意前一节也说明了配置是从左到右读取的。同样地，较为靠右的值可以替代靠左的值所设定的默认。

`minfree` 参数定义了用于审计的文件系统上，剩余空间的最小值。这一百分比值是相对于保存审计日志的文件系统来计算的。例如，如果 `dir` 指定了 `/var/audit` 而 `minfree` 设为两成(20)，则当 `/var` 文件系统有八成(80)空间被填满时将会给出警告消息。

`naflags` 参数用于指定无主事件——也就是那些并不与特定用户关联的事件的审计。

16.4.2.2 `audit_user` 文件

`audit_user` 文件允许管理员决定哪些系统用户所产生的哪些类的事件应被记录在案。

下面是 `audit_user` 文件中的一些默认值：

```
root:lo:no
audit:fc:no
```

注意默认值将审计所有的 `login/logout` 事件，而禁止审计所有其他由 `root` 完成的动作。这一配置也会审计所有文件创建操作，并禁止所有其他由 `audit` 用户完成的操作。尽管事件审计并不依赖特殊的用户才能正常工作，某些配置，特别是使用了 `MAC` 的环境中，却可能需要这个用户存在。

16.5 管理事件审计

由内核审计子系统写出的事件，并不能以普通文本的形式加以修改或阅读。这些数据以类似ktrace(1)和kdump(1)那样的方式来存储和访问，也就是说，只能通过使用praudit命令执行转存操作才能察看它们；审计账目可以通过auditreduce命令来减少，它能够根据您感兴趣的属性，例如用户、事件发生的时间，以及操作类型来选择查询记录。

例如，praudit能够将选定审计日志的完整内容，转存为普通的文本文件。要将整个审计日志转存，可使用：

```
# praudit /var/audit/AUDITFILE
```

这里AUDITFILE是希望查看的审计日志。由于审计日志可能包含大量的数据，管理员可能更希望选择某一特定用户的相关事件。要达到这个目的，可以使用下面的命令，这里我们选择的用户是trhodes：

```
# auditreduce -e trhodes /var/audit/AUDITFILE | praudit
```

这将选择保存在AUDITFILE中的所有由trhodes产生的审计日志。

还有许多其他选项可以在阅读审计记录时使用。请参见前述命令的联机书册，以获得进一步的解释。

16.5.1 审计日志文件的轮转

由于日志可靠性的要求，审计记账只由内核写入，且只能由auditd管理。管理员不应尝试使用newsyslog.conf(5)或其它工具来完成审计日志的轮转工作。您应使用audit管理工具来关闭审计、重新配置审计系统，并完成日志轮转。下面的命令将让审计服务创建新的审计日志，并发信号给内核要求其使用新的日志。旧日志将终止并被改名，此时，管理员就可以操作它了。

```
# audit -n
```

警告：如果auditd服务程序没有在运行，则前述命令将失败并给出错误提示。

在/etc/crontab加入如下设置，将使cron(8)每十二小时将日志轮转一次。

```
* * * * * root /usr/sbin/audit -n
```

这些修改会在您保存/etc/crontab后生效。

16.5.2 为其它用户指派审计复审权限

默认情况下，只有root用户拥有读取系统审计日志的权限。但您也可以将这种权限通过audit组的成员身份来指定给其它用户，因为审计目录和记账文件都是属于这个组的，而且是同组可读的。由于阅读审计日志的内容会提供关于用户和进程的大量行为信息，强烈建议在指派这一权限时谨慎行事。

第17章

存储

17.1 概述

这章介绍了FreeBSD 中磁盘的使用方法。包括内存盘，网络附属磁盘和标准的SCSI/IDE 存储设备，以及使用USB 的设备。

读完这章，您将了解到：

- FreeBSD 中用来描述硬盘上数据组织的术语(partitions and slices)。
- 如何在您的系统上增加硬盘。
- 如何配置FreeBSD 来使用USB 存储设备。
- 如何设置虚拟文件系统，例如内存磁盘。
- 如何使用配额来限制磁盘空间的使用。
- 如何增加磁盘安全来预防攻击。
- 如何刻录CD 和DVD 。
- 用于备份的多种存储媒介。
- 如何在FreeBSD 上使用备份程序。
- 如何备份到软磁盘。
- 文件系统快照是什么，以及如何有效地使用它们。

在读这章之前，您应该：

- 知道怎样去配置和安装新的FreeBSD 内核(第8 章)。

17.2 设备命名

下面是在FreeBSD 上被支持的物理存储设备和它们被分配的设备名。

表17-1. 物理磁盘命名规则

驱动器类型	驱动设备命名
IDE hard drives	ad
IDE CDROM drives	acd
SCSI hard drives and USB Mass storage devices	da
SCSI CDROM drives	cd
Assorted non-standard CDROM drives	mcd for Mitsumi CD-ROM, scd for Sony CD-ROM, matcd for Matsushita/Panasonic CD-ROM a

驱动器类型	驱动设备命名
Floppy drives	fd
SCSI tape drives	sa
IDE tape drives	ast
Flash drives	fla for DiskOnChip® Flash device
RAID drives	aacd for Adaptec AdvancedRAID, mlx and mlyd for Mylex, amrd for AMI MegaRAID, idad for Compaq Smart RAID, twed for 3ware® RAID.

表注: a. `matcd(4)` 驱动已经在2002年10月5日从FreeBSD 4.X 分支删去, FreeBSD 5.0 和之后的版本不再包含此驱动。

17.3 添加磁盘

Originally contributed by David O'Brien.

假设我们要给一台只有一个磁盘的机器增加一个新的SCSI 磁盘。首先需要关掉计算机, 然后按操作规程来安装驱动器, 控制器和驱动程序。由于各厂家生产的产品各不相同, 具体的安装细节不在此文档介绍之内。

以root 用户登录。安装完驱动后, 检查一下`/var/run/dmesg.boot` 有没有找到新的磁盘。在我们的例子中新增加的磁盘就是`da1`, 我们从`/1` 挂上它。(如果您正添加一个IDE 驱动器, 在4.0 版以前的系统里是`wd1`, 以后的版本的系统里是`ad1`)。

因为FreeBSD 运行在IBM-PC 兼容机上, 它必须遵循PC BIOS 分区规范。这与传统的BSD 分区是不同的。一个PC 的磁盘最高只能有四个BIOS 主分区。如果磁盘只安装FreeBSD 您可以使用**dedicated** 模式。另外, FreeBSD 必须安装在PC BIOS 支持的分区内。FreeBSD 把分区叫作**slices** 这可能会把人搞糊涂。您也可以在只安装FreeBSD 的磁盘上使用**slices**, 也可以在安装有其它操作系统的磁盘上使用**slices**。这不会影响其它操作系统的**fdisk** 分区工具。

在**slice** 方式表示下, 驱动器被添加到`/dev/da1s1e`。可以读作: SCSI 磁盘, 编号为1 (第二个SCSI 磁盘), **slice 1** (PC BIOS 分区1), 的BSD 分区**e**。在有些例子中, 也可以简化为`/dev/da1e`。

由于**bsdlable(8)** (在FreeBSD 4.X 中叫做**disklabel(8)**) 使用32-位的整数来表示扇区号, 因此在多数情况下它的表现力限于每个磁盘 $2^{32}-1$ 个扇区或2TB。**fdisk(8)** 格式允许的起始扇区号不能高于 $2^{32}-1$ 而分区长度也不能大于 $2^{32}-1$, 通常情况下这限制了分区大小最大为2TB 而磁盘大小则是4TB。**sunlabel(8)** 格式的限制是每个分区 $2^{32}-1$ 个扇区, 但允许8 个分区因此最大支持16TB 的磁盘。要使用更大的分区, 则应使用**gpt(8)**。

17.3.1 使用sysinstall(8)

1. 使用Sysinstall

您可以使用**sysinstall** 命令(在FreeBSD 5.2 之前是`/stand/sysinstall`), 选择它的使用菜单来分区和标记一个新的磁盘。需要有root 权限, 或者直接使用root 账户登录或者使用**su** 命令来切换到根用户。运行**sysinstall**, 然后选择**Configure** 菜单。在FreeBSD Configuration Menu 下, 上下滚动, 选择**Fdisk** 条目。

2. fdisk 分区编辑器

进入 **fdisk** 分区编辑器后，选择 **A**，FreeBSD 将使用全部的磁盘。当被告知 “remain cooperative with any future possible operating systems” 时，回答 **YES**。使用 **w** 保存刚才的修改。现在使用 **q** 退出 **FDISK** 编辑器。下面会看到有关 “主引导区” 的信息。现在您已经在运行的系统上添加了一个磁盘，因此应该选择 **None**。

3. Disk Label 编辑器

接下来，您应该退出 **sysinstall** 并且再次启动它，并按照上面的步骤直接进入 **Label** 选项。进入磁盘标签编辑器。这就是您要创建的 **BSD** 分区。一个磁盘最多可以有 8 个分区，标记为 **a-h**。有几个分区标签有特殊的用途。**a** 分区被用来作为根分区 (**/**)。系统磁盘（例如：从那儿启动的分区）必须有一个 **a** 分区。**b** 分区被用作交换分区，可以用很多磁盘用作交换分区。**c** 分区代表整个硬盘，或在 FreeBSD **slice** 模式下代表整个 **slice**。其它分区作为一般分区来使用。

sysinstall 的标签编辑器用 **e** 表示非 **root** 和非 **swap** 分区。在标签编辑器中，可以使用键入 **c** 创建一个文件系统。当提示这是否是一个 **FS**（文件系统）或 **swap** 时，选择 **FS**，然后给出一个加载点（如：**/mnt**）。当在 **post-install** 模式时添加一个磁盘，**sysinstall** 不会在 **/etc/fstab** 中创建记录，所以是否指定加载点并不重要。

现在已经准备把新标签写到磁盘上，然后创建一个文件系统，可以按下 **w**。出现任何错误都会不能创建新的分区。可以退出标签编辑器然后重新执行 **sysinstall**。

4. 完成

下面一步就是编辑 **/etc/fstab**，为您的磁盘添加一个新记录。

17.3.2 使用命令行工具

17.3.2.1 使用 Slices

这步安装将允许磁盘与可能安装在您计算机上的其它操作系统一起正确工作，而不会搞乱其它操作系统的分区。推荐使用这种方法来安装新磁盘，除非您有更好的理由再使用 **dedicated** 模式！

```
# dd if=/dev/zero of=/dev/da1 bs=1k count=1
# fdisk -BI da1 #初始化新磁盘
# disklabel -B -w -r da1s1 auto #加上标签
# disklabel -e da1s1 # 现在编辑您刚才创建的磁盘分区
# mkdir -p /1
# newfs /dev/da1s1e # 为您创建的每个分区重复这个操作
# mount /dev/da1s1e /1 # 挂上分区
# vi /etc/fstab # 完成之后，添加合适的记录到您的 /etc/fstab文件。
```

如果有一个 **IDE** 磁盘，记得要用 **ad** 来替换 **da**，4.X 以前的系统要用 **wd**。

17.3.2.2 专用模式

如果您并没有安装其它的操作系统，可以使用 **dedicated** 模式。记住这种模式可能会弄乱 **Microsoft** 的操作系统，但不会对它进行破坏。它不识别找到的 **IBM OS/2** 的 “appropriate” 分区。

```
# dd if=/dev/zero of=/dev/da1 bs=1k count=1
# disklabel -Brw da1 auto
# disklabel -e da1 # 创建 ‘e’ 分区
# newfs -d0 /dev/da1e
```

```
# mkdir -p /1
# vi /etc/fstab # 为 /dev/da1e添加一个记录
# mount /1
```

另一种方法:

```
# dd if=/dev/zero of=/dev/da1 count=2
# disklabel /dev/da1 | disklabel -BrR da1 /dev/stdin
# newfs /dev/da1e
# mkdir -p /1
# vi /etc/fstab # 为 /dev/da1e添加一个记录
# mount /1
```

注意: 从FreeBSD 5.1-RELEASE 版本开始, `bsdlabel(8)` 程序代替了老版本的`disklabel(8)` 程序。`bsdlabel(8)` 中大量过时的选项和参数也被取消。在上面的例子中选项 `-r` 可以使用`bsdlabel(8)`程序来删除。更多的信息, 请参考`bsdlabel(8)` 手册页。

17.4 RAID

17.4.1 软件RAID

17.4.1.1 连接磁盘驱动器配置(CCD)

Original work by Christopher Shumway. Revised by Jim Brown.

选择一个大容量存储比较好的解决方案, 最重要的因素是产品的速度、性能和成本。通常这三者不可能都满足;要获得比较快和可靠的大容量存储设备, 就比较昂贵。但如果将成本降下来, 那它的速度或可靠性就会打折扣。

在设计下面描述的系统时, 价格被选为最重要的因素, 接下来是速度和性能。这人系统的数据传输速度及大的取决于网络。性能也非常重要, CCD 驱动器上的所有数据都被备份到了CD-R 盘, 可以很容易的对数据进行恢复。

在选择一个大容量的存储解决方案时, 第一步是要设计您自己的需求。如果您的需求更偏重于速度和性能, 那么您的解决方案将不同于上面的设计。

17.4.1.1.1 安装硬件

除了IDE 系统磁盘外, 还有三个Western Digital 30GB、5400 RPM 的IDE 磁盘构成了大约90G 的连接磁盘驱动存储空间。最好是每个IDE 硬盘都使用一个自己的IDE 控制器和数据线, 为了降低成本, 没有使用更多的IDE 控制器, 取而代之配置跳线使每个IDE 控制器都拥有一个主盘和一个从盘。

重启后, 系统BIOS 被配置成自动检测硬盘。FreeBSD 检测到它们:

```
ad0: 19574MB <WDC WD205BA> [39770/16/63] at ata0-master UDMA33
ad1: 29333MB <WDC WD307AA> [59598/16/63] at ata0-slave UDMA33
ad2: 29333MB <WDC WD307AA> [59598/16/63] at ata1-master UDMA33
```

```
ad3: 29333MB <WDC WD307AA> [59598/16/63] at ata1-slave UDMA33
```

注意: 如果FreeBSD 没有检测到它们, 请确定它们的跳线是否设置正确。大多数IDE 磁盘有一个 “Cable Select” 跳线。这个**不是** 设置master/slave 硬盘的跳线。查阅文档信息来确定正确的跳线设置。

接下来考虑的是, 如何创建文件系统。应该好好研究一下vinum(8) (第19 章)和ccd(4) 两种方式, 在这里我们选择ccd(4)

17.4.1.1.2 安装CCD

ccd(4) 允许用户将几个相同的的磁盘通过一个逻辑文件系统连接起来。要使用ccd(4), 您需要在内核中配置ccd(4) 支持选项。把这行加入到内核配置文件中, 然后重建内核:

```
pseudo-device    ccd      4
```

在5.X 和以后的版本中, 您必须使用下面的行来代替:

```
device    ccd
```

注意: 在FreeBSD 5.X 里, 不必指定一系统的ccd(4) 设备, ccd(4) 设备将自动按需要创建新的——设备。

ccd(4) 在FreeBSD 3.0 或以后的版本中也可以作为一个内核模块来加载

要安装ccd(4), 首先需要使用disklabel(8) 来编辑硬盘:

```
disklabel -r -w ad1 auto
disklabel -r -w ad2 auto
disklabel -r -w ad3 auto
```

这儿把整个硬盘创建成ad1c, ad2c 和ad3c 。

注意: 从FreeBSD 5.1-RELEASE 开始, bsdlable(8) 程序代替了老版本的disklabel(8) 程序。bsdlable(8) 中大量过时的选项和参数也被取消; 在上面的例子中, 选项-r 应该被删掉。更多的信息可以参考bsdlable(8) 手册。

下一步是改变disklable 的类型。也可以使用disklabel(8) 来编辑:

```
disklabel -e ad1
disklabel -e ad2
disklabel -e ad3
```

这儿在每个已经设置了EDITOR 环境变量的磁盘上打开了disklable, 在我我例子中使用的是vi(1)。

可以看到:

```
8 partitions:
#          size      offset      fstype    [fsize bsize bps/cpg]
  c: 60074784         0      unused         0      0      0   # (Cyl.   0 - 59597)
```

添加一个新的e分区给ccd(4)用。这可以是c分区的一个拷贝，但fstype必须是4.2BSD。做完之后，您会看到一面这些：

```
8 partitions:
#          size      offset      fstype    [fsize bsize bps/cpg]
  c: 60074784         0      unused         0      0      0 # (Cyl.   0 - 59597)
  e: 60074784         0      4.2BSD         0      0      0 # (Cyl.   0 - 59597)
```

17.4.1.1.3 建立文件系统

ccd0c的设备节点可能不存在，所以要创建它，执行下面的命令：

```
cd /dev
sh MAKEDEV ccd0
```

注意：在FreeBSD 5.0中，devfs(5)将自动管理在/dev,里的设备结点，所以没有必要使用MAKEDEV命令。

现在已给每个磁盘都加上了标签，下面需要建立ccd(4)。要这样做，需要使用ccdconfig(8)工具，同时要提供类似下面的选项：

```
ccdconfig ccd0❶ 32❷ 0❸ /dev/ad1e❹ /dev/ad2e /dev/ad3e
```

每个选项的意义和用法如下所示：

- ❶ 配置设备的第一个参数，在这这是/dev/ccd0c。/dev/部分是任选项。
- ❷ 下一个参数是文件系统的插入页(interleave)。插入页定义了一个磁盘块中一个分段或条带(stripe)的大小，通常是512个字节。所以一个为32的插入页将是16,384字节。
- ❸ 插入页为ccdconfig(8)附带了标记。如果您要启用驱动器镜像，需要在这儿指定它。在这个配置中没有做ccd(4)的镜像，所以把它设为0(zero)。
- ❹ ccdconfig(8)的最后配置是设备的排列问题。使用完整的设备路径名。

运行ccdconfig(8)后ccd(4)就配置好了。现在要创建文件系统了，参考newfs(8)选项，执行下边的命令：

```
newfs /dev/ccd0c
```

17.4.1.1.4 自动创建

最后，要挂上ccd(4)，需要先配置它。把当前的配置文件写入/etc/ccd.conf中，使用下面的命令：

```
ccdconfig -g > /etc/ccd.conf
```

当重新启动系统时，如果/etc/ccd.conf存在，脚本/etc/rc就运行ccdconfig -C。这样就能自动配置ccd(4)以到它能被挂上。

注意：如果启动进入了单用户模式，在mount(8)上ccd(4)之前，需要执行下面的命令来配置队列：

```
ccdconfig -C
```

要自动挂接ccd(4),需要为ccd(4)在/etc/fstab中配置一个记录,以便在启动时它被挂上。如下所示:

```
/dev/ccd0c          /media      ufs         rw          2           2
```

17.4.1.2 Vinum 卷管理

Vinum 卷管理是一个实现虚拟磁盘的块驱动设备工具。它使磁盘从块设备的接口和数据映射中独立出来。与传统的存储设备相比,增加了灵活性、性能和可靠性。vinum(8)实现了RAID-0、RAID-1和RAID-5三种模式,它们即可以独立使用,也可组合使用。

参考第19章 得到更多vinum(8)的信息。

17.4.2 硬件RAID

FreeBSD支持很多硬件RAID控制器。这些硬件不需要FreeBSD指定软件来管理RAID系统。

使用BIOS支持的硬件,一般情况下这些硬件可以自行操作。下面是一个简明的描述设置一个Promise IDE RAID控制器。当硬件设备装好且系统重启后,屏幕上显示一个询问信息。接着进入硬件设置屏幕。在这里,您可以把所有的磁盘联合在一起使用。这样FreeBSD将磁盘看作一个驱动器。其它级别的RAID也可以相应的进行设置。

17.4.3 重建ATA RAID1阵列

FreeBSD允许您热插拔阵列中损坏的磁盘。在您重新启动系统之前请注意这一点。

您可能会在/var/log/messages或者在dmesg(8)的输出中看到类似下面这些的内容:

```
ad6 on monster1 suffered a hard error.
ad6: READ command timeout tag=0 serv=0 - resetting
ad6: trying fallback to PIO mode
ata3: resetting devices .. done
ad6: hard error reading fsbn 1116119 of 0-7 (ad6 bn 1116119; cn 1107 tn 4 sn 11)\
status=59 error=40
ar0: WARNING - mirror lost
```

使用atacontrol(8),查看更多信息:

```
# atactrol list
ATA channel 0:
Master:      no device present
Slave:      acd0 <HL-DT-ST CD-ROM GCR-8520B/1.00> ATA/ATAPI rev 0

ATA channel 1:
Master:      no device present
```

```
Slave:          no device present
```

```
ATA channel 2:
```

```
Master:  ad4 <MAXTOR 6L080J4/A93.0500> ATA/ATAPI rev 5
```

```
Slave:          no device present
```

```
ATA channel 3:
```

```
Master:  ad6 <MAXTOR 6L080J4/A93.0500> ATA/ATAPI rev 5
```

```
Slave:          no device present
```

```
# atactrol status ar0
```

```
ar0: ATA RAID1 subdisks: ad4 ad6 status: DEGRADED
```

1. 首先您应将包含故障盘的ata 通道卸下，以便安全地将其拆除：

```
# atactrol detach ata3
```

2. 换上磁盘

3. 重新挂接ata 通道：

```
# atactrol attach ata3
```

```
Master:  ad6 <MAXTOR 6L080J4/A93.0500> ATA/ATAPI rev 5
```

```
Slave:    no device present
```

4. 将新盘作为热备盘加入阵列：

```
# atactrol addspare ar0 ad6
```

5. 重建阵列：

```
# atactrol rebuild ar0
```

6. 可以通过下面的命令来查看进度：

```
# dmesg | tail -10
```

```
[output removed]
```

```
ad6: removed from configuration
```

```
ad6: deleted from ar0 disk1
```

```
ad6: inserted into ar0 disk1 as spare
```

```
# atactrol status ar0
```

```
ar0: ATA RAID1 subdisks: ad4 ad6 status: REBUILDING 0% completed
```

7. 等待操作完成。

17.5 USB 存储设备

Contributed by Marc Fonvieille.

到目前为止，有许多外部存储解决方案，例如：通用串行总线(USB)：硬盘、USB thumbdrives、CD-R burners 等等。FreeBSD 为这些设备提供了支持。

17.5.1 配置

USB 大容量存储设备驱动, 在`umass(4)`, 中提供了对USB 存储设备的支持。如果您使用**GENERIC** 内核, 您不必要改变配置文件里的任何内容。如果您使用了定制的内核, 就要确定下面的行出现在您的内核配置文件里:

```
device scbus
device da
device pass
device uhci
device ohci
device usb
device umass
```

`umass(4)` 驱动程序使用SCSI 子系统来访问USB 存储设备, 您的USB 设备将被系统看成为一个SCSI 设备。依靠您主板上的USB 芯片, 您只须选择`device uhci` 或`device ohci` 二者之一即可, 但是两者都加入内核配置文件当中也没有坏处。不要忘了如果您加入了上面的几行要重新编译和安装内核。

注意: 如果您的USB 设备是一个CD-R 或DVD 刻录机, SCSI CD-ROM 驱动程序, `cd(4)`, 就必须加入内核中通过下面这行:

```
device cd
```

因为刻录机被看作一个SCSI 设备`drive`, 驱动程序`atapicam(4)` 不应该在内核配置文件中。

从FreeBSD 5.X 开始, 对USB 2.0 控制器提供了内建的支持; 这一特性也被加入到了FreeBSD 4.10-RELEASE 和其后的4.X 版本。要获取对USB 2.0 的支持, 您需要在内核的编译配置中加入:

```
device ehci
```

注意, 如果需要USB 1.X 的支持, 您仍需要使用`uhci(4)` 和`ohci(4)` 驱动程序。

注意: 在FreeBSD 4.X 上, USB daemon (`usbd(8)`) 必须能够检测到正在运行的一些USB 设备。为了启用它, 添加`usbd_enable="YES"` 到您的`/etc/rc.conf` 文件里, 然后重新启动计算机。

17.5.2 测试配置

配置好后准备进行测试: 插入您的USB 设备, 在系统信息中(`dmesg(8)`), 应该会出现像下面的设备:

```
umass0: USB Solid state disk, rev 1.10/1.00, addr 2
GEOM: create disk da0 dp=0xc2d74850
da0 at umass-sim0 bus 0 target 0 lun 0
da0: <Generic Traveling Disk 1.11> Removable Direct Access SCSI-2 device
da0: 1.000MB/s transfers
da0: 126MB (258048 512 byte sectors: 64H 32S/T 126C)
```

当然啦, 商标, 设备标识(`da0`) 和其它的细节信息会根据您的配置不同而有所不同。

因为USB设备被看作SCSI设备中的一个，`camcontrol`命令也能够用来列出USB存储设备和系统的关联：

```
# camcontrol devlist
<Generic Traveling Disk 1.11>          at scbus0 target 0 lun 0 (da0,pass0)
```

如果设备要作成文件系统，您应该能够挂接它。第17.3节将帮助您格式化和创建分区在USB设备上，如果您需要。

如果您要去摘下设备(在此这前磁盘必须被`umount`)，在系统信息中您能够看到下面的信息：

```
umass0: at uhub0 port 1 (addr 2) disconnected
(da0:umass-sim0:0:0:0): lost device
(da0:umass-sim0:0:0:0): removing device entry
GEOM: destroy disk da0 dp=0xc2d74850
umass0: detached
```

17.5.3 深入阅读

除了Adding Disks和Mounting and Unmounting File Systems章之外，阅读`umass(4)`，`camcontrol(8)`，和`usbdevs(8)`也是很有益的。

17.6 创建和使用光学介质(CD)

Contributed by Mike Meyer.

17.6.1 介绍

CD与普通的磁盘相比有很多不同的特性。最初它们是不能被用户写入的。由于没有磁头和磁道移动时的延迟，所以它们可以连续的进行读取。方便的在两个系统之间进行数据的传输，比起相同大小的存储介质来说。

CD有磁道，这关系到数据读取时的连续性而不是物理磁盘的性能。要在FreeBSD中制作一个CD，您要准备好要写到CD上的数据文件，然后根据每个tracks写入到CD。

ISO 9660文件系统被设计用来处理这些差异。它通常不会对文件系统作限制。幸运的是，它提供了一个可扩展机制允许在制作CD时超越这些限制，而同时在不支持这些扩展的系统上仍旧能够进行工作。

`sysutils/port`包括了`mkisofs(8)`，这是一个可以用来生成包含ISO 9660文件系统的数据文件的程序。他也提供了对于一些扩展的支持选项，下面将详细介绍。

使用哪个工具来刻录CD依赖于CD刻录机是ATAPI还是其它类型的。ATAPI CD刻录器使用`burncd`程序，可以在基本系统中找到。SCSI和USB CD刻录机使用`cdrecord`程序，可以在`sysutils/cdrtools` port中找到。

`burncd`程序受到一系列支持设备的限制。如果想知道设备是否被支持，可以查看支持的CD-R/RW驱动器 (<http://www.freebsd.dk/ata/>) 列表。

注意：如果您运行的是FreeBSD 5.X、FreeBSD 4.8-RELEASE或更高版本，它将可能使用`cdrecord`和其它工作在一个ATAPI硬件ATAPI/CAM module为SCSI设备。

如果您想使用一个图形界面的CD刻录软件，您可以参考一下**X-CD-Roast**或**K3b**。这些工具作为安装包可以从sysutils/xcdroast和sysutils/k3b ports得到。**X-CD-Roast**和**K3b**需要ATAPI/CAM module和ATAPI硬件。

17.6.2 mkisofs

mkisofs(8)程序作为sysutils/cdrtools port的一部分，将生成ISO 9660文件系统，其中包含UNIX命名空间中的文件名。最简单的用法是：

```
# mkisofs -o imagefile.iso /path/to/tree
```

这个命令将创建一个包含ISO9660文件系统的imagefile.iso文件，它是目录树/path/to/tree的一个拷贝。在处理过程中，它将文件名称映射为标准的ISO9660文件系统的文件名，将排除那些不典型的ISO文件系统的文件。

有很多选项能够用来克服那些限制。特别的，-R选项能够启用Rock Ridge扩展一般的UNIX系统，-J选项能启用用于Microsoft系统的Joliet扩展，-hfs选项能用来创建用于Mac OS系统的HFS文件系统。

对于那些即将要在FreeBSD系统中使用CD的人来说，-u选项能用来消除所有文件名的限制。当使用-R选项时，它会产生一个文件系统映像，它与您从那儿启动FreeBSD树是一样的，虽然它在许多方面也违反了ISO 9660的标准。

最后一个常用的选项是-b。它用来指定启动映像的位置，用以生成“El Torito”启动CD。这个选项使用一个参数，用以指定将写入CD的目录的根。默认情况下，mkisofs(8)会以常说的“软盘模拟”方式来创建ISO，因此它希望引导影响的尺寸恰好是1200, 1440或2880 KB。某些引导加载器，例如FreeBSD发行版磁盘，并不使用模拟模式；这种情况下，需要使用-no-emul-boot选项。因此，如果/tmp/myboot是一个包含了在/tmp/myboot/boot/cdboot的可引导的FreeBSD系统，您就可以使用下面的命令在/tmp/bootable.iso生成ISO 9660文件系统：

```
# mkisofs -R -no-emul-boot -b boot/cdboot -o /tmp/bootable.iso /tmp/myboot
```

如果内核中已经配置了vn (FreeBSD 4.X)，或md (FreeBSD 5.X)，就可以挂上文件系统：

```
# vnconfig -e vn0c /tmp/bootable.iso
# mount -t cd9660 /dev/vn0c /mnt
```

在FreeBSD 4.X, 和FreeBSD 5.X中：

```
# mdconfig -a -t vnode -f /tmp/bootable.iso -u 0
# mount -t cd9660 /dev/md0 /mnt
```

可以发现/mnt和/tmp/myboot是一样的。

还可以使用mkisofs(8)的其它选项来调整它的行为。特别是修改ISO 9660的划分格式，创建Joliet和HFS格式的磁盘。查看mkisofs(8)手册页得到更多的帮助。

17.6.3 burncd

如果用的是ATAPE的CD刻录机，可以使用burncd命令来记录您的CD ISO映像文件。burncd命令是基本系统的一部分，中以使用/usr/sbin/burncd来安装。用法如下：

```
# burncd -f cddevice data imagefile.iso fixate
```

在`cddevice`上刻录一份`imagefile.iso`的副本。默认的设备是`/dev/acd0` (在FreeBSD 4.X下则是`/dev/acd0c`)。请参考`burncd(8)`以了解设置写入速度的参数, 如何在刻录完成之后自动弹出CD, 以及刻录音频数据。

17.6.4 cdrecord

如果没有一个ATAPI CD刻录机, 必须使用`cdrecord`来刻录您的CD。`cdrecord`不是基本系统的一部分; 必须从`sysutils/cdrtools`或适当的`package`安装它。基本系统的变化可能会引起这个程序的错误。可能是由“coaster”引起的。当升级系统时, 同时需要升级`port`, 或者如果已升级到`tracking -STABLE`, 那么使用新版本时也要升级`port`。

`cdrecord`有许多选项, 基本用法与`burncd`相似。刻录一个ISO 9660映像文件只需这样做:

```
# cdrecord dev=device imagefile.iso
```

使用`cdrecord`的比较巧妙的方法是找到使用的`dev`。要找到正确的设置, 可以使用`cdrecord`的`-scanbus`标记, 这会产生这样的结果:

```
# cdrecord -scanbus
Cdrecord 1.9 (i386-unknown-freebsd4.2) Copyright (C) 1995-2000 Jörg Schilling
Using libscg version 'schily-0.1'
scsibus0:
    0,0,0    0) 'SEAGATE ' 'ST39236LW      ' '0004' Disk
    0,1,0    1) 'SEAGATE ' 'ST39173W      ' '5958' Disk
    0,2,0    2) *
    0,3,0    3) 'iomega ' 'jaz 1GB        ' 'J.86' Removable Disk
    0,4,0    4) 'NEC      ' 'CD-ROM DRIVE:466' '1.26' Removable CD-ROM
    0,5,0    5) *
    0,6,0    6) *
    0,7,0    7) *
scsibus1:
    1,0,0   100) *
    1,1,0   101) *
    1,2,0   102) *
    1,3,0   103) *
    1,4,0   104) *
    1,5,0   105) 'YAMAHA ' 'CRW4260      ' '1.0q' Removable CD-ROM
    1,6,0   106) 'ARTEC  ' 'AM12S        ' '1.06' Scanner
    1,7,0   107) *
```

这个列表列出了设备的适当的`dev`值。找到您的CD burner, 使用三个用逗号分隔的数值来表示`dev`。在这个例子中, CRW是`dev=1,5,0`, 所以正确的输入应是`dev=1,5,0`。有一个很容易的方法可以指定这个值; 看看`cdrecord(1)`的介绍了解有关音轨, 控制速度和其他的东西。

17.6.5 复制音频CD

您可以这样复制CD, 把CD上面的音频数据解压缩出一系列的文件, 再把这些文件写到一张空白CD上。这个过程对于ATAPI和SCSI驱动器来说有些微的不同。

SCSI 驱动器

1. 使用cdda2wav 来解压缩音频。

```
% cdda2wav -v255 -D2,0 -B -Owav
```

2. 使用cdrecord 来写 .wav 文件。

```
% cdrecord -v dev=2,0 -dao -useinfo *.wav
```

确保2,0 被适当地设置了，具体方法在第17.6.4 节 中有所描述。

ATAPI 驱动器

1. ATAPI CD 驱动用/dev/acdtdnn表示每个轨道，这里d 是驱动器号，nn 是轨道号，由两位小数位组成，省略前缀零。所以第一个盘片上的第一个轨道就是/dev/acd0t01，第二个就是/dev/acd0t02，第三个就是/dev/acd0t03，等等。

请务必确认在/dev 中出现了对应的文件。如果您发现有某些项目缺失，则应强制系统重新识别介质：

```
# dd if=/dev/acd0 of=/dev/null count=1
```

注意：在FreeBSD 4.X 中，这些项的前缀并不包括零。如果发现/dev 缺少所需的项，可以用MAKEDEV 来生成：

```
# cd /dev
# sh MAKEDEV acd0t99
```

2. 使用dd(1) 解压缩每个轨道。当解压缩文件的时候您也必须使用一个特殊的块大小。

```
# dd if=/dev/acd0t01 of=track1.cdr bs=2352
# dd if=/dev/acd0t02 of=track2.cdr bs=2352
...
```

3. 使用burncd 把解压缩的文件刻录到光盘上。您必须指定这些文件是音频文件，这样burncd 会在刻录完成时结束光盘。

```
# burncd -f /dev/acd0 audio track1.cdr track2.cdr ... fixate
```

17.6.6 复制数据CD

您可以把数据CD 复制成一个与之等价的镜像文件，镜像文件可以使用mkisofs(8) 创建，您可以使用这个工具复制任何数据CD。这里给出的例子假定您的CDROM 设备acd0。代替您正确的CDROM 设备。在FreeBSD 4.X 下面，字符c 必须被附加到设备名的结尾处来指明是整个分区，或者对于CDROM，指明是整个光盘。

```
# dd if=/dev/acd0 of=file.iso bs=2048
```

现在您有一个镜像文件了，您可以像上面描述的那样把它刻录成CD。

17.6.7 使用数据CD

现在您已经创建了一张标准的数据CDROM，您或许想要挂载来读取上面的设备。默认情况下，mount(8) 假定文件系统是ufs 类型的。如果您尝试下面的命令：

```
# mount /dev/cd0 /mnt
```

您会得到一条 `Incorrect super block` 的错误信息，没有挂载成功。CDROM 不是 UFS 文件系统，所以试图这样挂载它是不可行的。您需要告诉 `mount(8)` 文件系统是 `ISO9660` 类型的，这样就可以。只需要指定 `mount(8)` 的 `-t cd9660` 选项。例如，如果您想要挂载 CDROM 设备，`/dev/cd0` 到 `/mnt` 目录，您需要执行：

```
# mount -t cd9660 /dev/cd0 /mnt
```

注意您的设备名(在这个例子中是 `/dev/cd0`)可能有所不同，取决于您的 CDROM 使用的接口。另外，`-t cd9660` 选项等同于执行 `mount_cd9660(8)`。上面的例子可以缩短为：

```
# mount_cd9660 /dev/cd0 /mnt
```

用这种方法您基本可以使用任何买到的数据 CDROM。然而某些有 ISO 9660 扩展的光盘可能会行为古怪。例如，`joliet` 光盘用两个字节的 `unicode` 字符存储所有的文件名。FreeBSD 内核还不能识别 `unicode` (重要!)，所以非英语字符被做了有问题的标记。(如果您正在运行 FreeBSD 4.3 或者以后的版本，CD9660 驱动包含了加载合适的 `unicode` 换算表的方法。一些常用编码的模块可以通过 `sysutils/cd9660_unicode port` 来安装。)

有时候，当您试图挂载 CDROM 的时候，会得到一条 `Device not configured` 的错误信息。这通常表明 CDROM 驱动认为托盘里没有光盘，或者驱动器在总线上不可见。需要几秒钟时间等待 CDROM 驱动器辨别已经接到反馈的信息，请耐心等待。

有时候，SCSI CDROM 可能会找不到，因为没有足够的时间来应答总线的 `reset` 信号。如果您有一个 SCSI CDROM 请将下面的选项添加到您的内核配置文件并重建您的内核。

```
options SCSI_DELAY=15000
```

这个告诉您的 SCSI 总线启动时暂停 15 秒钟，给您的 CDROM 驱动器足够的机会来应答总线 `reset` 信号。

17.6.8 刻录原始数据 CD

您可以选择把一个文件目录刻录到 CD 上而不用创建 ISO 9660 文件系统。有些人这么做是为了备份的目的。这个运行的比刻录一个标准 CD 速度要快的多：

```
# burncd -f /dev/acd1 -s 12 data archive.tar.gz fixate
```

要重新找回这样刻录到 CD 上的数据，您必须从原始设备节点读取数据：

```
# tar xzvf /dev/acd1
```

您不能像挂载一个通常的 CDROM 一样挂载这张光盘。这样的 CDROM 也不能在除了 FreeBSD 之外的任何操作系统上读出。如果您想要可以挂载 CD，或者和另一种操作系统共享数据，您必须像上面描述的那样使用 `mkisofs(8)`。

17.6.9 使用ATAPI/CAM 驱动

Contributed by Marc Fonvieille.

这个驱动允许ATAPI 设备(CD-ROM, CD-RW, DVD 驱动器等...)通过SCSI 子系统访问, 这样允许使用像sysutils/cdrdao 或者cdrecord(1) 这样的程序。

要使用这个驱动, 您需要把下面几行添加到您的内核配置文件中:

```
device atapicam
```

此外还需要在内核配置文件中加入:

```
device ata
device scbus
device cd
device pass
```

这些应该已经有了。

然后重建, 安装您的新内核, 重新启动机器。在启动过程中, 您的刻录机会被识别, 就像这样:

```
acd0: CD-RW <MATSHITA CD-RW/DVD-ROM UJDA740> at ata1-master PIO4
cd0 at ata1 bus 0 target 0 lun 0
cd0: <MATSHITA CDRW/DVD UJDA740 1.00> Removable CD-ROM SCSI-0 device
cd0: 16.000MB/s transfers
cd0: Attempt to query device size failed: NOT READY, Medium not present - tray closed
```

驱动器现在可以通过/dev/cd0 设备名访问了, 例如要挂载CD-ROM 到/mnt, 只需要键入下面的命令:

```
# mount -t cd9660 /dev/cd0 /mnt
```

作为root, 您可以运行下面的命令来得到刻录机的SCSI 地址:

```
# camcontrol devlist
<MATSHITA CDRW/DVD UJDA740 1.00> at scbus1 target 0 lun 0 (pass0,cd0)
```

这样1,0,0 就是SCSI 地址了, 可以被cdrecord(1) 和其他的SCSI 程序使用。

有关ATAPI/CAM 和SCSI 系统的更多信息, 可以参阅atapicam(4) 和cam(4) 手册页。

17.7 创建和使用光学介质(DVD)

Contributed by Marc Fonvieille. With inputs from Andy Polyakov.

17.7.1 介绍

和CD 相比, DVD 是下一代光学存储介质技术。DVD 可以容纳比任何CD 更多的数据, 已经成为现今视频出版业的标准。

我们称作可记录DVD 的有五种物理记录格式:

- DVD-R: 这是第一种可用的DVD 可记录格式。DVD-R 标准由DVD Forum (<http://www.dvdforum.com/forum.shtml>) 定义。这种格式是一次可写的。
- DVD-RW: 这是DVD-R 标准的可覆写版本。一张DVD-RW 可以被覆写大约1000 次。
- DVD-RAM: 这也是一种被DVD Forum 所支持的可覆写格式。DVD-RAM 可以被看作一种可移动硬盘。然而, 这种介质和大部分DVD-ROM 驱动器以及DVD-Video 播放器不兼容; 只有少数DVD 刻录机支持DVD-RAM。
- DVD+RW: 这是一种由DVD+RW Alliance (<http://www.dvdrw.com/>) 定义的可覆写格式。一张DVD+RW 可以被覆写大约1000 次。
- DVD+R: 这种格式是DVD+RW 格式的一次可写变种。

一张单层的可记录DVD 可以存储4,700,000,000 字节, 相当于4.38 GB 或者说4485 MB (1 千字节等于1024 字节)。

注意: 必须说明一下物理介质与应用程序的分歧。例如DVD-Video 是一种特殊的文件系统, 可以被覆写到任何可记录的DVD 物理介质上: DVD-R、DVD+R、DVD-RW 等等。在选择介质类型之前, 您一定要确认刻录机和DVD-Video 播放器(一种单独的播放器或者计算机上的DVD-ROM 驱动器) 是和这种介质兼容的。

17.7.2 配置

growisofs(1) 将被用来实施DVD 刻录。这个命令是**dvd+rw-tools** 工具集(sysutils/dvd+rw-tools) 的一部分。**dvd+rw-tools** 支持所有的DVD 介质类型。

这些工具将使用SCSI 子系统来访问设备, 因此ATAPI/CAM 支持 必须加入内核。如果您的刻录机采用USB 接口则不需要这么做, 请参考第17.5 节 来了解USB 设备配置的进一步详情。

此外, 还需要启用ATAPI 设备的DMA 支持。这一工作可以通过在/boot/loader.conf 文件中加入下面的行来完成:

```
hw.ata.atapi_dma="1"
```

试图使用**dvd+rw-tools** 之前您应该参考dvd+rw-tools 硬件兼容性列表 (<http://fy.chalmers.se/~appro/linux/DVD+RW/hcn.html>) 是否有与您的DVD 刻录机有关的信息。

注意: 如果您想要一个图形化的用户界面, 您应该看一看**K3b**(sysutils/k3b), 它提供了growisofs(1) 的一个友好界面和许多其他刻录工具。

17.7.3 刻录数据DVD

growisofs(1) 命令是mkisofs 的前端, 它会调用mkisofs(8) 来创建文件系统布局, 完成到DVD 上的刻录。这意味着您不需要在刻录之前创建数据映像。

要把/path/to/data 目录的数据刻录到DVD+R 或者DVD-R 上面, 使用下面的命令:

```
# growisofs -dvd-compat -Z /dev/cd0 -J -R /path/to/data
```

-J -R 选项传递给mkisofs(8) 用于文件系统创建(这种情况下: 带有joliet 和Rock Ridge 扩展的ISO 9660 文件系统), 参考mkisofs(8) 手册页了解更多细节。

选项-z 用来在任何情况下初始刻录会话: 不管多会话与否。DVD 设备, `/dev/cd0`, 必须依照您的配置做出改变。-dvd-compat 参数会结束光盘, 光盘成为不可附加的。这会提供更多的和DVD-ROM 驱动器的介质兼容性。

也可以刻录成一个pre-mastered 映像, 例如记录一个映像文件 *imagefile.iso*, 我们可以运行:

```
# growisofs -dvd-compat -Z /dev/cd0=imagefile.iso
```

刻录的速度可以被检测到并自动进行调整, 根据介质和驱动器的使用情况。如果您想强制改变速度, 可以使用-speed= 参数。更多的信息, 请看growisofs(1) 联机手册。

17.7.4 刻录DVD-Video

DVD-Video 是一个特殊的基于ISO 9660 和micro-UDF (M-UDF) 规范的文件系统。DVD-Video 也呈现了一个特殊的数据体系结构, 这就是为什么您需要一个特殊的程序像multimedia/dvdauthor 来制作DVD 的原因。

如果您已经有了DVD-Video 文件系统的映像, 就可以以同样的方式制作另一个映像, 可以参看前面章节的例子。如果您想制作DVD 并想放在特定的目录中, 如在目录 `/path/to/video` 中, 可以使用下面的命令来刻录DVD-Video:

```
# growisofs -Z /dev/cd0 -dvd-video /path/to/video
```

-dvd-video 选项将传递给mkisofs(8) 并指示它创建一个DVD-Video 文件系统布局。除此之外。-dvd-video 选项也包含了 -dvd-compat growisofs(1) 选项。

17.7.5 使用DVD+RW

不像CD-RW, 一个空白的DVD+RW 在每一次使用前必须先格式化。growisofs(1) 程序将会适时的自动对其进行适当的处理, 这是recommended 的方式。您也可以使用dvd+rw-format 来对DVD+RW 进行格式化:

```
# dvd+rw-format /dev/cd0
```

您只需要执行这样的操作一次, 牢记只有空白的DVD+RW 介质才需要格式化。您可以以前面章节同样的方式来刻录DVD+RW。

如果您想刻录新的数据(刻录一个新的完整的文件系统而不仅仅是追加一些数据) 到DVD+RW, 您不必再将其格式化成空白盘, 您只须要直接覆盖掉以前的记录即可。(执行一个新的初始化对话), 像这样:

```
# growisofs -Z /dev/cd0 -J -R /path/to/newdata
```

DVD+RW 格式化程序为简单的向以前的记录追加数据提供了可能性。这个操作有一个新的会话和一个已经存在的会话合并而成。它不需要多个写会话过程, growisofs(1) 将在介质上增加 ISO 9660 文件系统。

例如, 我们想追加一些数据到到我们以前的DVD+RW 上, 我们可以使用下面的命令:

```
# growisofs -M /dev/cd0 -J -R /path/to/nextdata
```

我们用来刻录初始会话的同样的mkisofs(8) 选项会在以后的写操作中使用。

注意: 如果您想获得与DVD-ROM 驱动更好的兼容性, 可以使用 `-dvd-compat` 选项。在DVD+RW 这种情况下, 将不能预防您添加数据。

如果出于某种原因您真的想要空白介质盘, 可以执行下面的命令:

```
# growisofs -Z /dev/cd0=/dev/zero
```

17.7.6 使用DVD-RW

DVD-RW 接受两种光盘格式: 增补顺序写入和受限式覆写。默认的DVD-RW 盘是顺序写入格式。

空白的DVD-RW 能够直接进行刻录而不需要格式化操作, 然而非空的顺序写入格式的DVD-RW 需要格式化才能写入新的初始区段。

要格式化一张DVD-RW 为顺序写入模式, 运行:

```
# dvd+rw-format -blank=full /dev/cd0
```

注意: 一次完全的格式化(`-blank=full`) 在1x 倍速的介质上将会花费大约1 个小时。快速格式化可以使用 `-blank` 选项来进行, 如果DVD-RW 要以Disk-At-Once (DAO) 模式刻录的话。要以DAO 模式刻录DVD-RW, 使用命令:

```
# growisofs -use-the-force-luke=dao -Z /dev/cd0=imagefile.iso
```

`-use-the-force-luke=dao` 选项不是必需的, 因为growisofs(1) 试图最低限度的检测(快速格式化) 介质并进行DAO 写入。

事实上对于任何DVD-RW 都应该使用受限式覆写模式, 这种格式比默认的增补顺序写入更加灵活。

在一张顺序DVD-RW 上写入数据, 使用和其他DVD 格式相同的说明:

```
# growisofs -Z /dev/cd0 -J -R /path/to/data
```

如果您想在您以前的刻录上附加数据, 您必须使用growisofs(1) 的 `-M` 选项。然而, 如果您在一张增补顺序写入模式的DVD-RW 上附加数据, 将会在盘上创建一个新的区段, 结果就是一张多区段光盘。

受限式覆写格式的DVD-RW 在新的初始化区段前不需要格式化, 您只是要用 `-Z` 选项覆写光盘, 这和DVD+RW 的情形是相似的。也可以用和DVD+RW 同样方式的 `-M` 选项把现存的ISO 9660 文件系统写入光盘。结果会是一张单区段DVD。

要把DVD-RW 置于受限式覆写格式, 必须使用下面的命令:

```
# dvd+rw-format /dev/cd0
```

更改回顺序写入模式使用:

```
# dvd+rw-format -blank=full /dev/cd0
```


17.7.7 多区段

几乎没有哪个DVD-ROM 驱动器支持多区段DVD，它们大多数时候都只读取第一个区段。顺序写入格式的DVD+R、DVD-R 和DVD-RW 可以支持多区段，DVD+RW 和DVD-RW 受限式覆写格式不存在多区段的概念。

在DVD+R、DVD-R 或者DVD-RW 的顺序写入格式下，一次初始化(未关闭) 区段之后使用下面的命令，将会在光盘上添加一个新的区段：

```
# growisofs -M /dev/cd0 -J -R /path/to/nextdata
```

对DVD+RW 或者DVD-RW 在受限式覆写模式下使用这条命令，会合并新区段到存在的区段中来附加数据。结果就是一张单区段光盘。这是在这些介质上用于在最初的写操作之后添加数据的方式。

注意：介质上的一些空间用于区段之间区段的开始与结束。因此，应该用大量的数据添加区段来优化介质空间。对于DVD+R 来说区段的数量限制为154，对于DVD-R 来说大约是2000，对于双层DVD+R 来说是127。

17.7.8 更多的信息

要获得更多的关于DVD 的信息dvd+rw-mediainfo /dev/cd0 命令可以运行来获得更多的信息。

更多的关于dvd+rw-tools 的信息可以在growisofs(1) 手册页找到，在dvd+rw-tools web site (<http://fy.chalmers.se/~appro/linux/DVD+RW/>) 和cdwrite mailing list (<http://lists.debian.org/cdwrite/>) 联接中也可找到。

注意：dvd+rw-mediainfo 命令的输出结果记录或媒体的问题被做成问题报告。没有这些输出，对你的帮助将会十分困难。

17.8 创建和使用软盘

原作Julio Merino. 重写Martin Karlsson.

把数据存储软盘上有时也是十分有用的。例如，当没有其它可靠的存储介质或要传递少量的数据到其它的计算机。

这一章将介绍怎样在FreeBSD 上使用软盘。在使用DOS 3.5 英寸软盘时首要要涉及的就是格式化，但其概念与其它的软盘格式化极为类似。

17.8.1 格式化软盘

17.8.1.1 设备

软盘的访问像其它设备一样是通过在/dev 中的条目来实现的。访问raw 软盘在4.X 和更早的版本，使用/dev/fdN, 这里N 标识设备号，通常为0，或/dev/fdNX, 这里X 标识为一个字符。

在5.0 或更新的版本中，简单的使用/dev/fdN。

17.8.1.1.1 4.X 以及更早版本的磁盘大小

也有`/dev/fdW.size`这样的设备，这里`size`代表软盘的含量以KB为单位。这个条目用在低级格式化时来确定磁盘的大小。下面的例子就是1440kB

有时这些条目必须在`/dev`目录中进行重建。可以这样做：

```
# cd /dev && ./MAKEDEV "fd*"
```

17.8.1.1.2 5.0 以及更新版本的磁盘大小

在5.0版本中，`devfs(5)`将自动管理在`/dev`目录中的设备，所以不推荐使用`MAKEDEV`命令。

如果期望得到确定大小的磁盘可以给`fdformat(1)`传递`-f`参数。支持的大小列在`fdcontrol(8)`中，但是建议和工作状态最好的1440kB。

17.8.1.2 格式化

一张软盘在使用这前必须先被低级格式化。通常卖主已经做过了，但格式化是检测介质完整性的一种好方法。尽管这有可能会强取大量（或少量）的硬盘大小，但大部分磁盘都能被格式化设计为1440kB。

低级格式化软盘你需要使用`fdformat(1)`命令。这个程序需要设备名作为参数。

要留意一切错误信息，这些信息能够帮助你确定磁盘的好与坏。

17.8.1.2.1 在4.X 以及更早版本中格式化

使用`/dev/fdW.size`设备来格式化软盘。插入一张新的3.5英寸的软盘在你的设备里：

```
# /usr/sbin/fdformat /dev/fd0.1440
```

17.8.1.2.2 在5.0 以及更新版本中格式化

使用`/dev/fdW`设备来格式化软盘。插入一张新的3.5英寸的软盘在你的设备中：

```
# /usr/sbin/fdformat -f 1440 /dev/fd0
```

17.8.2 磁盘标签

经过低级格式化后，你需要给它分配一个标签。这个磁盘标签以后会被销毁，但是系统却需要它来确定硬盘的大小。

新的磁盘标签将会接管整个磁盘，会包括所有合适的关于软盘的`geometry`信息。磁盘标签的`geometry`值列在`/etc/disktab`中。

你能够使用`disklabel(8)`像下面这样：

```
# /sbin/disklabel -B -r -w /dev/fd0 fd1440
```

注意: 从FreeBSD 5.1-RELEASE, 开始`bsdlabel(8)` 程序代替了旧版本的`disklabel(8)` 程序。随着`bsdlabel(8)` 一起许多陈旧的选项和参数也被清除了; 在上面的例子中, 选项`-r` 将被去掉。要想得到更多的信息, 请参考`bsdlabel(8)` 手册页。

17.8.3 文件系统

现在对软盘进行高级格式化。这会在它上面安置一个新的文件系统, 可使FreeBSD 来对它进行读写。在创建完新的文件系统后, 磁盘标签将被销毁, 所以如果你想重新格式化磁盘, 你必须重新创建磁盘标签。

软盘的文件系统可以选择UFS 或FAT。FAT 是通常情况下软盘比较好的选择。

要制作新的文件系统在软盘上, 可以使用下面的命令:

```
# /sbin/newfs_msdos /dev/fd0
```

现在磁盘已经可以进行读取和使用。

17.8.4 使用软盘

要使用软盘, 需要先使用`mount_msdos(8)` (在4.X 和更早的版本中) 或`mount_msdosfs(8)` (在5.0 或更新的版本中)。也可以使用在ports collection 中的`emulators/mtools` 程序。

17.9 用磁带机备份

主流的磁带机有4mm, 8mm, QIC, mini-cartridge 和DLT。

17.9.1 4mm (DDS: Digital Data Storage)

4mm 磁带机取代了QIC 而成为工作站备份数据在设备面停止了QIC 设备的生产。4mm 的驱动器更加小和安静, 但对于数据保存的可信度仍不及8mm 驱动器。它要比8mm 的便宜和小得多(3 x 2 x 0.5 inches, 76 x 51 x 12 mm)。和8mm 的一样, 读写头的寿命都不长, 因为它们同样使用螺旋式的方式来读写。

数据传输的速度约在~150 kB/s, 到~500 kB/s 之间, 可存储空间从1.3 GB 到2.0 GB 之间, 硬件压缩可使空间加倍。磁带库单元可以有6 台磁带机, 120 个磁带匣, 以自动切换的方式使用同一个磁带柜, 磁带库的容量可达240 GB。

DDS-3 标准现在支持的磁带机容量最高可达到12 GB (或压缩的24 GB)。

4mm 和8mm 同样都使用螺旋式读写的方式, 所有螺旋式读写的优点及缺点, 都可以在4mm 和8mm 磁带机上看到。

磁带在经过2,000 次的使用或100 次的全部备份后, 就该退休了。

17.9.2 8mm (Exabyte)

8mm 磁带机是最常见的SCSI 磁带机，也是磁带交换的最佳选择。几乎每个工作站都有一台2 GB 8mm 磁带机。8mm 磁带机可信度高、方便、安静。卡匣小(4.8 x 3.3 x 0.6 inches; 122 x 84 x 15 mm)而且不贵。8mm 磁带机的下边是一个短短的读写头，而读写头的寿命取决于磁带经过读写头时，相对高速运动情况。

数据传输速度约在250 kB/s 到500 kB/s 之间，可存储的空间从300 MB 到7 GB，硬件压缩可使空间加倍。磁带库单元可以有6 台磁带机，120 个磁带匣，以自动切换的方式使用同一个磁带柜，磁带库的容量可达840+ GB。

Exabyte “Mammoth” 模型支持12 GB 的容量在一个磁带上(压缩后可达24 GB)相当于普通磁带的二倍。

数据是使用螺旋式读写的方式记录在磁带上的，读写头和磁带约相差6 度，磁带以270 度缠绕着轴，并抵住读写头，轴适时地旋转，使得磁带具有高密度，从一端到另一端并可使磁道紧密地分布。

17.9.3 QIC

QIC-150 磁带和磁带机可能是最常见的磁带机和介质了。QIC 磁带机是最便宜的“正规” 备份设备。它的缺点在于介质的价格较高。QIC 磁带要比8mm 或4mm 磁带贵，每GB 的数据存储价格可能最高高出5 倍。但是，如果您的需求能够为半打磁带所满足的话，那么QIC 可能是明智之选。QIC 是最常见的磁带机。每个站点都会有某种密度的QIC。这有时是一种麻烦，QIC 有为数众多的密度，但在外观上相似(有时一样)的磁带。QIC 磁带机噪音很大。它们在寻址以及读写时都会发出声音。QIC 磁带的规格有(6 x 4 x 0.7 英寸; 152 x 102 x 17 毫米)。

数据传输的速度介于150 kB/s 到500 kB/s 之间，可存储的空间从40 MB 到15 GB。较新的QIC 磁带机具有硬件压缩的功能。QIC 的使用率愈来愈低，渐渐被DAT 所取代。

数据以磁道的方式记录在磁带上，磁道数及磁道的宽度会根据容量而有所不同。通常新的磁带机具有的向后兼容的读取功能（通常也具备写入的功能）。对于数据的安全性，QIC 具有不错的评价。

磁带机在经过5,000 次的使用后，就该退休了。

17.9.4 DLT

在这一章列出的磁带机中DLT 具有最快的数据传输率。1/2" (12.5mm) 的磁带包含在单轴的磁带匣(4 x 4 x 1 inches; 100 x 100 x 25 mm)中。磁带匣的一边是一个旋转匝道，通过匝道的开合，可以让磁带卷动。磁带匣内只有一个轴，而本章中所提到的其他磁带匣都是有两个轴的（9磁道磁带机例外）。

数据传输的速度约1.5 MB/s，是4mm, 8mm, 或QIC 磁带机的三倍。可存储的空间从10 GB 到20 GB，具有磁带机数据库。磁带机数据库单元可以有1 to 20 台磁带机，5 到900 个磁带匣，磁带机数据库的容量可达50 GB 到9 TB。

如果要压缩的话，DLT 型IV 格式的磁带机最高可支持70 GB 的存储容量。

数据存储在平行于磁带运行方向的磁道上（就像QIC 磁带），一次写入两个磁道。读写头的寿命相当长，每当磁带停止前进，磁带与读写头之间没有相对运动。

17.9.5 AIT

AIT 是Sony 开发的一种新格式，每个磁带最高可以存储50 GB。磁带机使用内存芯片来保存磁带上的索引内容。这个索引能够被磁带机驱动器快速阅读来搜索磁带上文件所处的位置，而不像其他的磁带机需要花几分钟的时间才能找到文件。像**SAMS:Alexandria** 这样的软件：能够操作四十或者更多的AIT 磁带库，直接使用内存芯片来进行通信把内容显示在屏幕上，以决定把什么文件备份到哪个磁带上，加载和恢复数据。

像这样的库成本大概在\$20,000 美元左右，零售市场可能还要贵一点。

17.9.6 第一次使用新的磁带机

当在一块完全空白的磁带上尝试定入数据时，会得到类似下面这样的错误信息：

```
sa0(ncr1:4:0): NOT READY asc:4,1
sa0(ncr1:4:0): Logical unit is in process of becoming ready
```

信息指出这块磁带没有块编号(block 编号为0)。在QIC-525 之后的所有QIC 磁带，都采用QIC-525 标准，必须写入一个Identifier Block。对于这种问题，有以下两种解决的办法：

- 用 `mt fsf 1` 可以让磁带机对磁带写入Identifier Block。
- 使用面板上的按钮磁带。

再插入一次，并存储dump 数据到磁带上。

这时dump 将传回DUMP: End of tape detected，然后您会得到这样的错误信息：HARDWARE FAILURE info:280 asc:80,96。

这时用 `mt rewind` 来倒转磁带。

磁带操作的后续操作就完成了。

17.10 用软盘备份

17.10.1 能够使用软盘来备份数据吗

软磁盘通常是用来备份的设备中不太合适的设备：

- 这种设备不太可靠，特别是长期使用。
- 备份和恢复都很慢
- 它们只有非常有限的存储容量。

然而，如果没有其它的备份数据的方法，那软盘备份总比没有备份要好。

如果必须使用软盘的话，必须确保盘片的质量。软盘在办公室中使用已经有许多年了。最好使用一些名牌厂商的产品以确保质量。

17.10.2 如何备份数据到软盘

最好的备份数据到软盘的方法是使用tar(1) 程序加上 -M 选项，它可以允许数据备份到多张软盘上。

要备份当前目录中所有的文件可以使用这个命令(需要有root权限):

```
# tar Mcvf /dev/fd0 *
```

当第一张盘满的时候，tar(1) 会指示您插入下一张盘，插入第二张盘之后就按回车。

Prepare volume #2 for /dev/fd0 and hit return:

这个步骤可能需要重复很多次，直到这些文件备份完成为止。

17.10.3 可以压缩备份吗

不幸的是，tar(1) 在为多卷文件作备份时是不允许使用 -z 选项的。当然，可以用gzip(1) 压缩所有的文件，把它们打包到磁盘，以后在用gunzip(1) 解开。

17.10.4 如何恢复备份

要恢复所有文件:

```
# tar Mxvf /dev/fd0
```

有两种方法来恢复软盘中的个别文件。首先，就要用第一张软盘启动:

```
# tar Mxvf /dev/fd0 filename
```

tar(1) 程序会提示您插入后面的软盘，直到它找到所需要的文件。

如果您知道哪个文件在哪个盘上，您就可以插入那张盘，然后使用上同同样的命令。如果软盘上的第一个文件与前面的文件是连续的，那tar(1) 命令会警告您它无法恢复，即使您不要求它这样做。

17.11 备份策略

原作Lowell Gilbert.

设计备份计划的第一要务是确认以下问题皆已考虑到:

- 磁盘故障
- 文件的意外删除
- 随机的文件损毁
- 机器完全损毁(例如火灾)，包括破坏全部在线备份。

针对上述的每个问题采用完全不同的技术来解决是完全可行的。除了只包含少量几乎没有价值数据的个人系统之外，一般来说很少有一种技术能够同时兼顾前面所有的需要。

可以采用的技术包括:

- 对整个系统的数据进行存档，备份到永久性的离线介质上。这种方法实际上能够提供针对前面所有问题的保护，但这样做通常很慢，而且恢复时会比较麻烦。您可以将备份置于近线或在线的状态，然而恢复文件仍然是一个难题，特别是对没有特权的那些用户而言。
- 文件系统快照。这种技术实际上只对无意中删除文件这一种情况有用，但在这种情况下它会提供非常大的帮助，而且访问迅速，操作容易。
- 直接复制整个文件系统和/或磁盘(例如周期性地对整个机器做rsync)。通常这对于在网络上的单一需求最为适用。要为磁盘故障提供更为通用的保护，通常这种方法要逊于RAID。对于恢复无意中删除的文件来说，这种方法基本上与UFS 快照属于同一层次，使用哪一个取决于您的喜好。
- RAID。它能够最大限度地减少磁盘故障导致的停机时间。其代价是需要处理更为频繁的磁盘故障(因为磁盘的数量增加了)，尽管这类故障不再需要作为非常紧急的事项来处理。
- 检查文件的指纹。mtree(8) 工具对于这种操作非常有用。尽管这并不是一个备份的技术，但它能够确保您有机会注意到那些您要求助于离线备份的事情。这对于离线备份非常重要，而且应有计划地加以检查。

很容易列举更多的技术，它们中有许多实际上是前面所列出的方法的变种。特别的需求通常会需要采用特别的技术(例如，备份在线运行的数据库，往往需要数据库软件提供某种方法来完成中间步骤)来满足。最重要的事情是，一定要了解需要将数据保护起来免受何种风险，以及发生问题时应该如何处理。

17.12 备份程序

有三个主要的备份程序dump(8)、tar(1)和cpio(1)。

17.12.1 Dump 和Restore

dump 和restore 是UNIX 传统的备份程序。它以block 而不是以文件为单位来备份数据、链接或目录。dump 备份的是设备上的整个文件系统，不能只备份一个文件系统的部分或是用到两个以上文件系统的目录树。dump 不会写文件和目录到磁带机，而是写入包含文件和目录的原始数据块。

注意: 如果在您的root 目录使用dump，将不需要备份/home、/usr 或其他目录，因为这些是典型的其他文件系统或符号连接到那些文件系统的加载点。

dump 是最早出现于AT&T UNIX 的Version 6 (约1975)。默认的参数适用于9-track 磁带(6250 bpi)，所以如果要用高密度的磁带（最高可达62,182 ftpi），就不能用默认的参数，而要另外指定参数。这些默认值必须在命令行被修改以更好地利用当前磁带机的功能。

rdump 和rrestore 可以通过网络在另一台计算机的磁带机上备份数据。这两个程序都是依靠rcmd(3)和ruserok(3)来访问远程的磁带机。因此，运行备份的用户必须要有远程主机的.rhosts 访问权。rdump 和rrestore 的参数必须适用于远程主机（例如，当您从FreeBSD 连到一台SUN 工作站knomodo 去使用磁带机时，使用：

```
# /sbin/rdump 0dsbfu 54000 13000 126 komodo:/dev/nsa8 /dev/da0a 2>&1
```

要注意的是：必须检查您在使用.rhosts 时的安全情况。

也可以通过使用ssh 用一个更安全的方式来使用dump 和restore 。

例17-1. 通过ssh 使用dump

```
# /sbin/dump -0uan -f - /usr | gzip -2 | ssh -c blowfish \
    targetuser@targetmachine.example.com dd of=/mybigfiles/dump-usr-l0.gz
```

或使用dump 的built-in 方法，设置环境变量RSH:

例17-2. 通过设置ssh 环境变量RSH 使用dump

```
# RSH=/usr/bin/ssh /sbin/dump -0uan -f targetuser@targetmachine.example.com:/dev/sa0 /usr
```

17.12.2 tar

tar(1) 也同样是在第6 版AT&T UNIX (大约是1975 前后) 出现的。tar 对文件系统直接操作；其作用是把文件和目录写入磁带。tar 并不支持cpio(1) 所提供的全部功能，但也不需要cpio 所需要使用的诡异的命令行管道。

在FreeBSD 5.3 和更高版本中，同时提供了GNU tar 和默认的bsdtar。GNU 的版本可以通过gtar 来使用。它通过与rdump 一样的语法来支持远程设备。要tar 到连接在名为komodo 的Sun 机器上的Exabyte 磁带机，可以使用：

```
# /usr/bin/gtar cf komodo:/dev/nsa8 . 2>&1
```

您也可以让bsdtar 通过管道和rsh 将数据发送到远程的磁带机上。

```
# tar cf - . | rsh hostname dd of=tape-device obs=20b
```

如果您担心通过网络备份会有安全问题，应当使用ssh，而不是rsh。

17.12.3 cpio

cpio(1) 是UNIX 最早用来作文件交换的磁带机程序。它有执行字节交换的选项，可以用几种不同的格式写入，并且可以将数据用管道传给其他程序。cpio 没办法自动查找目录树内的文件列表，必须通过标准输入stdin 来指定。

cpio 不支持通过网络的备份方式。可以使用pipeline 和rsh 来传送数据给远程的磁带机。

```
# for f in directory_list; do
find $f >> backup.list
done
# cpio -v -o --format=newc < backup.list | ssh user@host "cat > backup_device"
```

这里的directory_list 是要备份的目录列表，user@host 结合了将要执行备份的用户名和主机名，backup_device 是写入备份的设备（如/dev/nsa0）。

17.12.4 pax

pax(1) 是符合IEEE/POSIX 标准的程序。多年来各种不同版本的tar 和cpio 间有些 incompatibility。为了防止这种情况，并使其标准化，POSIX 出了这套新的工具程序。pax 尝试可以读写各种cpio 和tar 的格式，并可以自己增加新的格式。它的命令集比tar 更接近cpio。

17.12.5 Amanda

Amanda (Advanced Maryland Network Disk Archiver) 并非单一的程序，而是一个客户机/服务器模式的备份系统。一台 **Amanda** 服务器可以备份任意数量执行 **Amanda** 的客户机或是将连上 **Amanda** 服务器的计算机上的数据备份到一台磁带机上。一个常见的问题是，数据写入磁带机的时间将超过取行数据的时间，而 **Amanda** 解决了这个问题。它使用一个“holding disk”来同时备份几个文件系统。**Amanda** 建立“archive sets”的一组磁带，用来备份在 **Amanda** 的配置文件中列出的完整的文件系统。

Amanda 配置文件提供完整的备份控制及 **Amanda** 产生的网络传输。**Amanda** 可以使用上述任何一个设备程序来向磁带写入数据。**Amanda** 可以从 port 或 package 取得，它并非系统默认安装的。

17.12.6 Do Nothing 备份策略

“Do nothing”不是一个程序，而是被广泛使用的备份策略。不需要预算，不需要备份的计划表，全部都不用。如果您的数据发生了什么问题，忽略它！

如果您的时间和数据不值得您做这些事，那么“Do nothing”将是最好的备份程序。要注意的是，UNIX 是相当好用的工具，您可能在几个月内，就发现您已经收集了不少对您来说相当具有价值的文件和程序。

“Do nothing”对于像 `/usr/obj` 和其他可由您的计算机产生的文件来说，是最好的方法。例如这本手册包含有 HTML 或 PostScript 格式的文件。这些文档格式是从 SGML 输入文件创建的。创建 HTML 或 PostScript 格式的文件备份就没有必要了。只要经常备份 SGML 文件就够了。

17.12.7 哪个备份程序最好？

在 dump(8) 时期 Elizabeth D. Zwicky 测试了所有以上列出的备份程序。在各种各样怪异的文件系统中，`dump` 是您明智的选择。Elizabeth 建立起各种各样、奇怪或常见的文件系统，并用各种备份程序，测试在各种文件系统中备份及恢复数据。这些怪异之处包括：具有 holes 和一个 nulls block 的文件，文件名具有有趣字符，无法读写的文件及设备，在备份时改变文件大小，在备份时建立或删除的文件。她将结果刊登在：LISA V in Oct. 1991. See torture-testing Backup and Archive Programs (<http://berdmann.dyndns.org/zwicky/testdump.doc.html>).

17.12.8 应急恢复程序

17.12.8.1 在出现灾难前

在遇到灾难前，只需要执行以下四个步骤：

第一，打出您的每个磁盘驱动器的磁盘标签(例如：`disklabel da0 | lpr`)，文件系统表，(`/etc/fstab`)，以及所有启动信息，并将每个拷贝两份。

第二，确定遇到的情况时，用来启动及修复的软盘(`boot.flp` 和 `fixit.flp`) 具有您所有的设备代号。最简单的方法是用软盘启动，然后检查启动信息，如果设备都被列出，并且可以正常使用，就可以跳到第三步。

否则，必须建立两张传统的可启动软盘，并包含：`fdisk`, `disklabel`, `newfs`, `mount`，以及所有使用的备份程序。这些程序必须被静态的连接。如果使用的是 `dump`，那么这张软盘就必须包含 `restore`。

第三，定期将数据备份到磁带。任何在上次备份后的改变都无法恢复。记得将磁盘写保护。

第四，测试在第二步所建立的软盘及备份的磁带，将过程记录下来，并和这张可启动的软盘和磁带放在一起。也许您在恢复时会想要，而这份记录将防止您破坏您的磁带(怎么说呢？因为您可能将`tar xvf /dev/sa0`打成`tar cvf /dev/sa0`而重写了备份磁带)。

为了安全，您可以每次都做两份备份磁带及一张启动磁盘，并将其中一份备份磁带存放在其它地方。其它地方不是指同一栋办公大楼的地下室(世贸中心的一些公司应该学到了一些教训)，而是真的要让人的磁带离您的计算机远远的。

例17-3. 一个建立启动磁盘的shell 脚本例子:

```
#!/bin/sh
#
# create a restore floppy
#
# format the floppy
#
PATH=/bin:/sbin:/usr/sbin:/usr/bin

fdformat -q fd0
if [ $? -ne 0 ]
then
    echo "Bad floppy, please use a new one"
    exit 1
fi

# place boot blocks on the floppy
#
disklabel -w -B /dev/fd0c fd1440

#
# newfs the one and only partition
#
newfs -t 2 -u 18 -l 1 -c 40 -i 5120 -m 5 -o space /dev/fd0a

#
# mount the new floppy
#
mount /dev/fd0a /mnt

#
# create required directories
#
mkdir /mnt/dev
mkdir /mnt/bin
mkdir /mnt/sbin
mkdir /mnt/etc
mkdir /mnt/root
mkdir /mnt/mnt # for the root partition
mkdir /mnt/tmp
mkdir /mnt/var

#
# populate the directories
```

```

#
if [ ! -x /sys/compile/MINI/kernel ]
then
    cat << EOM
The MINI kernel does not exist, please create one.
Here is an example config file:
#
# MINI -- A kernel to get FreeBSD onto a disk.
#
machine          "i386"
cpu              "I486_CPU"
ident            MINI
maxusers         5

options          INET                      # needed for _tcp _icmpstat _ipstat
                                           #          _udpstat _tcpstat _udb
options          FFS                      #Berkeley Fast File System
options          FAT_CURSOR                #block cursor in syscons or pccons
options          SCSI_DELAY=15             #Be pessimistic about Joe SCSI device
options          NCONS=2                   #1 virtual consoles
options          USERCONFIG               #Allow user configuration with -c XXX

config           kernel root on da0 swap on da0 and da1 dumps on da0

device           isa0
device           pci0

device           fdc0 at isa? port "IO_FD1" bio irq 6 drq 2 vector fdintr
device           fd0 at fdc0 drive 0

device           ncr0

device           scbus0

device           sc0 at isa? port "IO_KBD" tty irq 1 vector scintr
device           npx0 at isa? port "IO_NPX" irq 13 vector npxintr

device           da0
device           da1
device           da2

device           sa0

pseudo-device    loop                     # required by INET
pseudo-device    gzip                     # Exec gzipped a.out's
EOM
    exit 1
fi

cp -f /sys/compile/MINI/kernel /mnt

gzip -c -best /sbin/init > /mnt/sbin/init
gzip -c -best /sbin/fsck > /mnt/sbin/fsck

```

```

gzip -c -best /sbin/mount > /mnt/sbin/mount
gzip -c -best /sbin/halt > /mnt/sbin/halt
gzip -c -best /sbin/restore > /mnt/sbin/restore

gzip -c -best /bin/sh > /mnt/bin/sh
gzip -c -best /bin/sync > /mnt/bin/sync

cp /root/.profile /mnt/root

cp -f /dev/MAKEDEV /mnt/dev
chmod 755 /mnt/dev/MAKEDEV

chmod 500 /mnt/sbin/init
chmod 555 /mnt/sbin/fsck /mnt/sbin/mount /mnt/sbin/halt
chmod 555 /mnt/bin/sh /mnt/bin/sync
chmod 6555 /mnt/sbin/restore

#
# create the devices nodes
#
cd /mnt/dev
./MAKEDEV std
./MAKEDEV da0
./MAKEDEV da1
./MAKEDEV da2
./MAKEDEV sa0
./MAKEDEV pty0
cd /

#
# create minimum file system table
#
cat > /mnt/etc/fstab <<EOM
/dev/fd0a    /      ufs    rw  1  1
EOM

#
# create minimum passwd file
#
cat > /mnt/etc/passwd <<EOM
root:*:0:0:Charlie &:/root:/bin/sh
EOM

cat > /mnt/etc/master.passwd <<EOM
root::0:0::0:0:Charlie &:/root:/bin/sh
EOM

chmod 600 /mnt/etc/master.passwd
chmod 644 /mnt/etc/passwd
/usr/sbin/pwd_mkdb -d/mnt/etc /mnt/etc/master.passwd

#
# umount the floppy and inform the user

```

```
#
/sbin/umount /mnt
echo "The floppy has been unmounted and is now ready."
```

17.12.8.2 出现灾难后

关键问题是：您的硬件是否幸免于难？由于已经做好了定期的备份工作，旖旎并不需要担心软件的问题。

如果硬件已经损毁，这些部分应该在尝试使用计算机之前换掉。

如果硬件还能用，检查一下您的软盘。如果使用定制的引导软盘，启动单用户模式(在boot: 提示后输入-s)。跳过下面一段。

如果您使用boot.flp 和fixit.flp 软盘，请继续阅读。将boot.flp 软盘插到计算机的第一个软驱并启动机器。此时，最初的安装菜单将显示在屏幕上。选择Fixit--Repair mode with CDRom or floppy. 选项。在得到提示后插入fixit.flp。restore 以及其他需要的程序，可以在/mnt2/rescue (对于FreeBSD 5.2 之前的版本，则是/mnt2/stand)。

分别恢复每一个文件系统

试着mount 上您的第一个磁盘的root 分区(例如：mount /dev/da0a /mnt)。假如这个磁盘标签已经损坏，使用disklabel 来重新分割并分配磁盘标签（利用您以前保留下来的数据）。使用newfs 来建立文件系统，并重新挂上软盘读写的root 分区(mount -u -o rw /mnt)。然后使用备份程序及备份磁带来修复文件系统(例如：restore vrf /dev/sa0)。最后Unmount 这个文件系统(例如：umount /mnt)。对于每个损坏的文件系统都重复一次。

当您的系统正常启动后，将您的数据备份到新的磁带。任何造成数据丢失的灾难都可能再次发生。现在花一些时间，也许可以使您免于下次的灾难。

17.13 网络、内存和File-Backed 文件系统

Reorganized and enhanced by Marc Fonvieille.

除了你的物理磁盘以外，插入你计算机的：软盘CDs，硬盘驱动器，等等；其它磁盘格式是不被FreeBSD - virtual disks支持的。

这还包括网络文件系统，例如Network File System 和Coda, 基于内存的文件系统和后备文件系统。

按照你运行的FreeBSD 版本，你可以使用不同的工具来创建和使用后备文件系统和内存文件系统。

注意: FreeBSD 4.X 用户可以使用MAKEDEV(8) 来创建需要的设备。FreeBSD 5.0 和更新的版本使用devfs(5) 来创建设备节点，对用户来说是透明的。

17.13.1 FreeBSD 4.X 下的File-Backed 文件系统

应用程序vnconfig(8) 可以配置和启用vnode 伪磁盘设备。一个vnode 代表一个文件。这就意味使用vnconfig(8) 可以用来创建和操作一个文件系统。也可以在文件中挂接一个软盘或CD 映像。

要使用vnconfig(8)，你需要在内核配置文件中vn(4)的支持：

```
pseudo-device vn
```

挂接一个存在的文件系统映像：

例17-4. 使用vnconfig 来挂接一个存在的文件系统映像在FreeBSD 4.X 系统上。

```
# vnconfig vn0 diskimage
# mount /dev/vn0c /mnt
```

使用vnconfig(8) 创建一个新的文件系统映像：

例17-5. 使用vnconfig 创建新的文件后援磁盘

```
# dd if=/dev/zero of=newimage bs=1k count=5k
5120+0 records in
5120+0 records out
# vnconfig -s labels -c vn0 newimage
# disklabel -r -w vn0 auto
# newfs vn0c
Warning: 2048 sector(s) in last cylinder unallocated
/dev/vn0c: 10240 sectors in 3 cylinders of 1 tracks, 4096 sectors
5.0MB in 1 cyl groups (16 c/g, 32.00MB/g, 1280 i/g)
super-block backups (for fsck -b #) at:
32
# mount /dev/vn0c /mnt
# df /mnt
```

Filesystem	1K-blocks	Used	Avail	Capacity	Mounted on
/dev/vn0c	4927	1	4532	0%	/mnt

17.13.2 采用文件后端的文件系统

在FreeBSD 5.X 和更新版本的系统中，可以用mdconfig(8) 程序来配置和启用内存磁盘，md(4)。要使用mdconfig(8)，就需要在内核配置文件中添加md(4) 模块来支持它：

```
device md
```

mdconfig(8) 命令支持三种类型的内存后备虚拟磁盘：使用malloc(9)，来分配内存磁盘，内存磁盘作为文件或作为备用的交换分区。一种使用方式是在文件中来挂接一个软盘和CD 映像。

挂接一个存在的文件系统映像：

例17-6. 使用mdconfig 挂载已经存在的文件系统映像

```
# mdconfig -a -t vnode -f diskimage -u 0
# mount /dev/md0 /mnt
```

使用mdconfig(8) 来创建一个新的文件系统映像：

例17-7. 使用mdconfig 创建一个新的文件后援磁盘

```
# dd if=/dev/zero of=newimage bs=1k count=5k
5120+0 records in
5120+0 records out
# mdconfig -a -t vnode -f newimage -u 0
# bsdlabel -w md0 auto
# newfs md0a
/dev/md0a: 5.0MB (10224 sectors) block size 16384, fragment size 2048
    using 4 cylinder groups of 1.25MB, 80 blks, 192 inodes.
super-block backups (for fsck -b #) at:
    160, 2720, 5280, 7840
# mount /dev/md0a /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md0a      4710    4  4330      0%    /mnt
```

如果你没有使用 `-u` 选项指定一个单位号 `mdconfig(8)` 将使用 `md(4)` 自动为它选择一个未使用的设备。分配给它的单位名将被输出到标准输出设备像 `md4`。想得到更多的关于 `mdconfig(8)` 的信息请参考手册页。

应用程序 `mdconfig(8)` 功能很强大，但在创建采用文件后端的文件系统时需要使用许多多行命令。为此 FreeBSD 5.0 也提供了一个名为 `mdmfs(8)` 的工具，该程序使用 `mdconfig(8)` 来配置 `md(4)` 盘，并在其上用 `newfs(8)` 创建 UFS 文件系统，然后用 `mount(8)` 挂接它。例如，如果想创建和挂接像上面那样的文件系统映像，只需简单地执行下面的步骤：

例17-8. 使用mdmfs 命令配置和挂接一个File-Backed 磁盘

```
# dd if=/dev/zero of=newimage bs=1k count=5k
5120+0 records in
5120+0 records out
# mdmfs -F newimage -s 5m md0 /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md0      4718    4  4338      0%    /mnt
```

如果你使用没有加单位号的 `md` 选项，`mdmfs(8)` 将使用 `md(4)` 的自动单位号特性来自动为其选择一个未使用的设备。更详细的 `mdmfs(8)`，请参考手册页。

17.13.3 FreeBSD 4.X 下的内存后备式文件系统

`md(4)` 驱动程序是一个简单有效的手段用来创建内存文件系统在 FreeBSD 4.X 系统上。`malloc(9)` 被用来分配内存。

简单的获得一个文件系统你需要准备，例如：`vnconfig(8)`

例17-9. FreeBSD 4.X 下的md 内存磁盘

```
# dd if=newimage of=/dev/md0
5120+0 records in
5120+0 records out
# mount /dev/md0c /mnt
# df /mnt
```

Filesystem	1K-blocks	Used	Avail	Capacity	Mounted on
/dev/md0c	4927	1	4532	0%	/mnt

更多的详情，请参考md(4)手册页。

17.13.4 以内存为后端的文件系统

同样的工具既可以用来创建以文件为后端的文件系统，也可以用来创建基于内存的文件系统：mdconfig(8)和mdmfs(8)。一般来说在建立以内存为后端的文件系统时，应使用“交换区作为后端(swap backing)”。使用交换区作为后端，并不意味着内存盘将被无条件地换出到交换区，它只是表示将根据需要从可换出的内存池中分配内存。此外，也可以使用malloc(9)作为后端的内存盘，但这种内存盘在内核内存不足时，有可能导致系统崩溃。

例17-10. 用mdconfig 创建一个新的内存后备磁盘

```
# mdconfig -a -t swap -s 5m -u 1
# newfs -U md1
/dev/md1: 5.0MB (10240 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 1.27MB, 81 blks, 192 inodes.
        with soft updates
super-block backups (for fsck -b #) at:
 160, 2752, 5344, 7936
# mount /dev/md1 /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity Mounted on
/dev/md1    4718      4  4338      0%    /mnt
```

例17-11. 使用mdmfs 来新建内存盘

```
# mdmfs -s 5m md2 /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity Mounted on
/dev/md2    4846      2  4458      0%    /mnt
```

17.13.5 从系统中移除内存盘

当一个内存后备式文件系统不再使用时，你应该释放掉系统的资源。每一件要做的事情就是摘掉文件系统，然后使用mdconfig(8)把磁盘从系统中分离出来释放资源。

例如分离和释放所有的资源使用/dev/md4 命令：

```
# mdconfig -d -u 4
```

mdconfig -l 命令可以列出关于配置md(4)设备的信息。

在FreeBSD 4.X 系统中，vnconfig(8) 命令用来分离设备。例如分离所有的资源使用/dev/vn4 命令：

```
# vnconfig -u vn4
```


17.14 文件系统快照

Contributed by Tom Rhodes.

FreeBSD 5.0 提供了一个和Soft Updates 关联的新功能: 文件系统快照

快照允许用户创建指定文件系统的映像, 并把它们当做一个文件来对待。快照文件必须在文件系统正在使用时创建, 一个用户对每个文件系统创建的快照不能大于20个。活动的快照文件被记录在超级块中, 所以它们可以在系统启动的时候一块进行挂接后摘掉。当一个快照不再需要时, 可以使用标准的rm(1) 使用来使其删除。快照可以以任何顺序进行移除, 但所有使用的快照不可能同时进行移除, 因为其它的快照将有可能互相引用一些块。

不可改的snapshot 文件标志, 是由mksnap_ffs(8) 在完成创建快照文件时设置的。unlink(1) 命令是一个特例, 以允许删除快照文件。

快照可以通过mount(8) 命令创建。将文件系统/var 的快照放到/var/snapshot/snap 可以使用下面的命令:

```
# mount -u -o snapshot /var/snapshot/snap /var
```

作为选择, 你也可以使用mksnap_ffs(8) 来创建一个快照:

```
# mksnap_ffs /var /var/snapshot/snap
```

可以查找文件系统快照文件(例如/var), 方法是使用find(1) 命令:

```
# find /var -flags snapshot
```

当快照文件被创建好后, 可以用于下面一些目的:

- 有些管理员用文件快照来进行备份, 因为快照可以被转移到CD 或磁带上。
- 文件系统一致性检查程序fsck(8) 可以用来检查快照文件。如果文件系统在挂接前是一致的, 则检查结果也一定是一致的(也就是不会做任何修改)。实际上这也正是后台fsck(8) 的操作过程。
- 在快照上运行dump(8) 程序。dump 将返回包含文件系统和快照的时间戳。dump(8) 也能够抓取快照, 使用-L 标志可以首先创建快照, 完成dump 映像之后再自动删除它。
- 用mount(8) 来挂接快照作为文件系统的一个冻结的镜像。要mount(8) 快照/var/snapshot/snap 运行:

```
# mdconfig -a -t vnode -f /var/snapshot/snap -u 4
# mount -r /dev/md4 /mnt
```

现在你就可以看到挂接在/mnt 目录下的/var 文件系统的快照。每一样东西都保存的像它创建时的状态一样。唯一例外的是更早的快照文件将表现为长度为0 的文件。用完快照文件之后可以把它卸下, 使用:

```
# umount /mnt
# mdconfig -d -u 4
```

想了解更多关于softupdates 和文件系统快照的信息, 包括技术说明, 可以访问Marshall Kirk McKusick 的WWW 站点<http://www.mckusick.com/>。

17.15 文件系统配额

配额是操作系统的一个可选择的属性，它允许限制用户使用的磁盘空间大小或是使用的文件数量。这可以防止某个用户占用所有的磁盘空间。

17.15.1 配置系统来启用磁盘配额

在决定使用磁盘配额前，确信磁盘配额已经在内核中配置好了。只要在在内核中配置文件中添加下面一行就行了：

```
options QUOTA
```

在默认情况下GENERIC 内核是不会启用这个功能的，所以必须配置、重建和安装一个定制的内核。请参考FreeBSD 内核配置第8章 这章了解更多有关内核配置的信息。

接下来，需要在/etc/rc.conf 中启用磁盘配额。可以通过添加下面这行来完成：

```
enable_quotas="YES"
```

为了更好的控制配额时的启动，还有另外一个可配置的变量。通常启动时，集成在每个文件系统上的配额会被配额检查程序quotacheck(8) 自动检查。配额检查功能能够确保在配额数据库中的数据正确地反映了文件系统的数据情况。这是一个很耗时间的处理进程，它会影响系统的启动时间。如果想跳过这一步，可以在文件/etc/rc.conf 加入下面这一行来达到目的：

```
check_quotas="NO"
```

最后，要编辑/etc/fstab 文件，以在每一个文件系统基础上雇用磁盘配额。这是启用用户和组配额，或同时启用用户和组配额的地方。

要在一个文件系统上启用每个用户的配额，可以在/etc/fstab 里添加userquota 选项在要雇用配额文件的系统上。例如：

```
/dev/da1s2g    /home    ufs rw,userquota 1 2
```

同样的，要启用组配额，使用groupquota 选项来代替userquota 选项。要同时启用用户和组配额，可以这样做：

```
/dev/da1s2g    /home    ufs rw,userquota,groupquota 1 2
```

默认情况下，配额文件是存放在文件系统的以quota.user 和quota.group 命名的根目录下。可以查看fstab(5) 联机手册了解更多信息。即使联机手册fstab(5) 说中以为配额文件指定其他的位置，这里并不推荐这样做，因为不同的配额工具不一定遵循这样的规则。

到这儿，可以用新内核重新启动系统。/etc/rc 将自动运行适当的命令来创建最初的配额文件，所以并不需要手动来创建任何零长度的配额文件。

在通常的操作过程中，并不要求手动运行quotacheck(8)、quotaon(8), 或quotaoff(8) 命令，然而可能需要阅读与他们的操作相似的联机手册。

17.15.2 设置配额限制

一旦您配置好了启用配额的系统，可以检查一下它们是真的有用。可以这样做：

```
# quota -v
```

您应该能够看到一行当前正在使用的每个文件系统启用的磁盘配额使用情况的摘要信息。

现在可以使用`edquota(8)`命令准备启用配额限制。

有几个有关如何强制限制用户或组可以分配到的磁盘空间大小的选项。您可以限制磁盘存储块的配额，或文件的数量，甚至同时限制两者。这些限制最终可分为两类：硬限制和软限制。

硬性限制是一种不能越过的限制。一旦用户达到了系统指定的硬性限制，他就无法在对应的文件系统分配到更多的资源。例如，如果文件系统上分给用户的硬性限制是500 KB，而现在已经用掉了490 KB，那么这个用户最多还能再分配10 KB的空间。换言之，如果这时试图再分配11 KB，则会失败。

软限制可以被有段时间限制性地被越过。这段时间可以被理解为允许限期，默认是一个星期。如果一个用户延缓时间太长的话，软限制将会变成硬限制，根本就不允许再继续占用磁盘配额。当用户因到软限制以下时，允许延期将重新开始计算。

下面是一个运行`edquota(8)`时看到的例子。当`edquota(8)`命令被调用时，会被转移进EDITOR环境变量指定的编辑器中，允许编辑配额限制。如果环境变量没有设置，默认在vi编辑器上进行。

```
# edquota -u test
```

```
Quotas for user test:
```

```
/usr: kbytes in use: 65, limits (soft = 50, hard = 75)
      inodes in use: 7, limits (soft = 50, hard = 60)
/usr/var: kbytes in use: 0, limits (soft = 50, hard = 75)
          inodes in use: 0, limits (soft = 50, hard = 60)
```

在每一个启用了磁盘配额的文件系统上，通常会看到两行。一行是block限制，另一行是inode限制。简单地改变要修改的配额限制的值。例如，提高这个用户软限制的数值到500，硬限制到600：

```
/usr: kbytes in use: 65, limits (soft = 50, hard = 75)
```

```
to:
```

```
/usr: kbytes in use: 65, limits (soft = 500, hard = 600)
```

当离开编辑器的时候，新的配额限制设置将会被保存。

有时，在UIDs的范围内设置配额限制是非常必要的。这可以通过在`edquota(8)`命令后面加上-p选项来完成。首先，给用户分配所需要的配额限制，然后运行命令`edquota -p protouser startuid-enduid`。例如，如果用户test已经有了所需要的配额限制，下面的命令可以被用来复制那些UIDs为10,000到19,999的配额限制：

```
# edquota -p test 10000-19999
```

更多细节请参考`edquota(8)`手册页。

17.15.3 检查配额限制和磁盘使用

即可以使用`quota(1)`也可以使用`repquota(8)`命令来检查配额限制和磁盘使用情况。`quota(1)`命令能够检查单个用户和组的配置使用情况。只有超级用户才可以检查其它用户的配额和磁盘使用情况。`repquota(8)`命令可以用来了解所有配额和磁盘的使用情况。

下面是一个使用`quota -v`命令后的输出情况：

Disk quotas for user test (uid 1002):

Filesystem	usage	quota	limit	grace	files	quota	limit	grace
/usr	65*	50	75	5days	7	50	60	
/usr/var	0	50	75		0	50	60	

前面以/usr 作为例子。此用户目前已经比软限制50 KB 超出了15 KB，还剩下5 天的宽限期。请注意，星号* 说明用户已经超出了其配额限制。

通常，如果用户没有使用文件系统上的磁盘空间，就不会在quota(1) 命令的输出中显示，即使已经为那个用户指定了配额。而使用-v 选项则会显示它们，例如前面例子中的/usr/var。

17.15.4 通过NFS 使用磁盘配额

配额能够在NFS 服务器上被配额子系统强迫使用。在NFS 客房端，rpc.rquotad(8) 命令可以使用quota 信息用于quota(1) 命令，可以允许用户察看它们的quota 统计信息。

可以这样在/etc/inetd.conf 中启用rpc.rquotad:

```
rquotad/1      dgram rpc/udp wait root /usr/libexec/rpc.rquotad rpc.rquotad
```

现在重启inetd:

```
# kill -HUP `cat /var/run/inetd.pid`
```

17.16 加密磁盘分区

Contributed by Lucky Green.

FreeBSD 提供了极好的数据保护措施，防止未授权的数据访问。文件权限和强制访问控制(MAC)(看第15 章) 可以帮助预防在操作系统处于运行状态和计算机加电时未授权的第三方访问数据。但是，和操作系统强制受权不相关的是，如果黑客有物理上访问计算机的可能，那他就可以简单的把计算机的硬件安装到另一个系统上拷贝出敏感的数据。

无论攻击者如何取得停机后的硬件或硬盘驱动器本身，FreeBSD **GEOM Based Disk Encryption (基于GEOM 的磁盘加密, gbde)** 和**geli** 加密子系统都能够保护计算机上的文件系统数据，使它们免受哪怕是训练有素的攻击者获得有用的资源。与那些只能加密单个文件的笨重的加密方法不同，gbde 和geli 能够透明地加密整个文件系统。明文数据不会出现在硬盘的任何地方。

17.16.1 使用gbde 对磁盘进行加密

1. 成为root

配置gbde 需要超级用户的权力。

```
% su -
Password:
```

2. 验证操作系统的版本

gbde(4) 需要FreeBSD 5.0 或更高的版本。

```
# uname -r
5.0-RELEASE
```

3. 在内核配置文件中添加对**gbde(4)**的支持

在您的内核配置中加入下面一行：

```
options GEOM_BDE
```

按照第8章所进行的介绍重新编译并安装内核。

重新引导进入新的内核。

17.16.1.1 准备加密盘

下面这个例子假设您添加了一个新的硬盘在您的系统并将拥有一个单独的加密分区。这个分区将挂接在/private目录下。**gbde**也可以用来加密/home和/var/mail，但是这需要更多的复杂命令来执行。

1. 添加新的硬盘

添加新的硬盘到系统中可以查看在第17.3节中的说明。这个例子的目的是说明一个新的硬盘分区已经添加到系统中如：`/dev/ad4s1c`。在例子中`/dev/ad0s1*`设备代表系统中存在的标准FreeBSD分区。

```
# ls /dev/ad*
/dev/ad0          /dev/ad0s1b      /dev/ad0s1e      /dev/ad4s1
/dev/ad0s1        /dev/ad0s1c      /dev/ad0s1f      /dev/ad4s1c
/dev/ad0s1a       /dev/ad0s1d      /dev/ad4
```

2. 创建一个目录来保存**gbde** Lock文件

```
# mkdir /etc/gbde
```

gbde lock文件包含了**gbde**需要访问的加密分区的信息。没有lock文件，**gbde**将不能解密包含在加密分区上的数据。每个加密分区使用一个独立的lock文件。

3. 初始化**gbde**分区

一个**gbde**分区在使用前必须被初始化，这个初始化过程只需要执行一次：

```
# gbde init /dev/ad4s1c -i -L /etc/gbde/ad4s1c
```

gbde(8)将打开您的编辑器，提示您去设置在一个模板文件中的配置变量。使用UFS1或UFS2，设置扇区大小为2048：

```
$FreeBSD: src/sbin/gbde/template.txt,v 1.1 2002/10/20 11:16:13 phk Exp $
#
# Sector size is the smallest unit of data which can be read or written.
# Making it too small decreases performance and decreases available space.
# Making it too large may prevent filesystems from working. 512 is the
# minimum and always safe. For UFS, use the fragment size
#
sector_size      =          2048
[...]
```

gbde(8)将让您输入两次用来加密数据的密钥短语。两次输入的密钥必须相同。**gbde**保护您数据的能力依靠您选择输入的密钥的质量。¹

gbde init命令为您的**gbde**分区创建了一个lock文件，在这个例子中存储在/etc/gbde/ad4s1c中。

小心: **gbde lock** 文件**必须**和加密分区上的内容一块备份。当一个**lock** 文件被独自删除时, 不能确定一个**gbde** 分区上的数据被解密过。没有**lock** 文件, 就是合法的磁盘所有者不经过大量细致的工作也将不能访问经过加密分区上的数据, 这是**gbde(8)** 在设计时整体上不支持。

4. 把加密分区和内核进行关联

```
# gbde attach /dev/ad4s1c -l /etc/gbde/ad4s1c
```

在加密分区的初始化过程中您将被要求提供一个密码短语。新的加密设备将在/dev 中显示为/dev/device_name.bde:

```
# ls /dev/ad*
/dev/ad0          /dev/ad0s1b      /dev/ad0s1e      /dev/ad4s1
/dev/ad0s1        /dev/ad0s1c      /dev/ad0s1f      /dev/ad4s1c
/dev/ad0s1a       /dev/ad0s1d      /dev/ad4          /dev/ad4s1c.bde
```

5. 在加密设备上创建文件系统

当加密设备和内核进行关联后, 您就可以使用**newfs(8)** 在此设备上创建文件系统, 使用**newfs(8)** 来初始化一个UFS2 文件系统比初始化一个UFS1 文件系统还要快, 推荐使用**-02** 选项。

注意: **-02** 选项在FreeBSD 5.1-RELEASE 或更新的版本中是默认的选项。

```
# newfs -U -02 /dev/ad4s1c.bde
```

注意: **newfs(8)** 命令必须在一个**gbde** 分区上执行, 这个分区通过一个存在的*.bde 设备名进行标识。

6. 挂接加密分区

为加密文件系统创建一个挂接点。

```
# mkdir /private
```

挂接加密文件系统。

```
# mount /dev/ad4s1c.bde /private
```

7. 校验加密文件系统是否有效

加密的文件系统现在对于**df(1)** 应该可见并可以使用。

```
% df -H
Filesystem      Size    Used Avail Capacity  Mounted on
/dev/ad0s1a     1037M    72M   883M      8%    /
/devfs           1.0K    1.0K     0B    100%   /dev
/dev/ad0s1f      8.1G    55K    7.5G     0%   /home
/dev/ad0s1e     1037M    1.1M   953M     0%   /tmp
/dev/ad0s1d      6.1G    1.9G    3.7G    35%   /usr
/dev/ad4s1c.bde  150G    4.1K   138G     0%   /private
```

17.16.1.2 挂接已有的加密文件系统

每次系统启动后，在使用加密文件系统前必须和内核重新进行关联，校验错误和再次挂接。使用的命令必须由root用户来执行。

1. 关联gbde 分区到内核

```
# gbde attach /dev/ad4s1c -l /etc/gbde/ad4s1c
```

接下来系统将提示您输入在初始化加密的**gbde** 分区时所用的密码短语。

2. 校验文件系统错误

加密文件系统不能列在/etc/fstab 文件中进行自动加载，在加载前必须手动运行fsck(8) 命令对文件系统进行错误检测。

```
# fsck -p -t ffs /dev/ad4s1c.bde
```

3. 挂接加密文件系统

```
# mount /dev/ad4s1c.bde /private
```

加密后的文件系统现在可以有效使用。

17.16.1.2.1 自动挂接加密分区

可以创建脚本来自动地附加、检测，并挂接加密分区，然而，处于安全考虑，这个脚本不应包含**gbde**(8) 密码。于此相反，我们建议这类脚本在控制台或通过ssh(1) 执行并要求用户输入口令。

从FreeBSD 5.2-RELEASE 开始，提供了一个新的rc.d 脚本。这个脚本的参数可以通过rc.conf(5) 来指定，例如：

```
gbde_autoattach_all="YES"
gbde_devices="ad4s1c"
```

在启动时将要求输入**gbde** 的口令。在输入正确的口令之后，**gbde** 加密分区将被自动挂接。对于将**gbde** 用在笔记本电脑上时，这就很有用了。

17.16.1.3 gbde 提供的密码学保护

gbde(8) 采用CBC 模式的128-位AES 来加密扇区数据。磁盘上的每个扇区都采用不同的AES 密钥来加密。要了解关于**gbde** 的密码学设计，包括扇区密钥如何从用户提供的口令字中生成等细节，请参考**gbde**(4)。

17.16.1.4 兼容性问题

sysinstall(8) 是和**gbde** 加密设备不兼容的。在启动sysinstall(8) 时必须将*.bde 设备和内核进行分离，否则在初始化探测设备时将引起冲突。与加密设备进行分离在我们的例子中使用如下的命令：

```
# gbde detach /dev/ad4s1c
```

还需要注意的是，由于vinum(4) 没有使用geom(4) 子系统，因此不能同时使用**gbde** 与**vinum** 卷。

17.16.2 使用geli对磁盘进行加密

撰写者Daniel Gerzo.

从FreeBSD 6.0 开始提供了一个新的密码学GEOM class ——geli。它目前由Pawel Jakub Dawidek <pjd@FreeBSD.org> 开发。Geli 与gbde 不同；它提供了一些不同的功能，并采用了不同的方式来进行密码学运算。

geli(8) 最重要的功能包括：

- 使用了crypto(9) 框架——如果系统中有加解密硬件加速设备，则geli 会自动加以利用。
- 支持多种加密算法(目前支持AES、Blowfish，以及3DES)。
- 允许对根分区进行加密。在系统启动时，将要求输入用于加密根分区的口令。
- 允许使用两个不同的密钥(例如，一个“个人密钥” 和一个“公司密钥”)。
- geli 速度很快——它只进行简单的扇区到扇区的加密。
- 允许备份和恢复主密钥。当用户必须销毁其密钥时，仍然可以通过从备份中恢复密钥来存取数据。
- 允许使用随机的一次性密钥来挂接磁盘——这对于交换区和临时文件系统非常有用。

更多geli 功能介绍可以在geli(8) 联机手册中找到。

下面的步骤介绍了如何启用FreeBSD 内核中的geli 支持，并解释了如何创建新的geli 加密provider。最后，还将对如何利用geli 创建加密的交换分区加以演示。

要使用geli，您必须运行FreeBSD 6.0-RELEASE 或更新版本。由于需要修改内核，因此您还需要拥有超级用户权限。

1. 在内核配置文件中加入geli 支持

在内核配置文件中加入下面两行：

```
options GEOM_ELI
device crypto
```

按照第8 章 介绍的步骤重新编译并安装内核。

另外，geli 也可以在系统引导时加载。这是通过在/boot/loader.conf 中增加下面的配置来实现的：

```
geom_eli_load="YES"
```

geli(8) 现在应该已经为内核所支持了。

2. 生成主密钥

下面的例子讲描述如何生成密钥文件，它将作为主密钥(Master Key) 的一部分，用于挂接到/private 的加密provider。这个密钥文件将提供一些随机数据来加密主密钥。同时，主密钥也会使用一个口令字来保护。Provider 的扇区尺寸为4kB。此外，这里的讨论将描述如何挂载geli provider，在其上创建文件系统，如何挂接并在其上工作，最后将其卸下。

建议您使用较大的扇区尺寸(例如4kB)，以获得更好的性能。

主密钥将由口令字保护，而密钥文件的数据来源则将是/dev/random。我们称之为provider 的/dev/da2.eli 的扇区尺寸将是4kB。

```
# dd if=/dev/random of=/root/da2.key bs=64 count=1
# geli init -s 4096 -K /root/da2.key /dev/da2
Enter new passphrase:
```


Reenter new passphrase:

同时使用口令字和密钥文件并不是必须的；您也可以只使用其中的一种来加密主密钥。

如果密钥文件写作“-”，则表示使用标准输入。下面是关于如何使用多个密钥文件的例子：

```
# cat keyfile1 keyfile2 keyfile3 | geli init -K - /dev/da2
```

3. 将provider与所生成的密钥关联

```
# geli attach -k /root/da2.key /dev/da2
```

Enter passphrase:

新的明文设备将被命名为/dev/da2.eli。

```
# ls /dev/da2*
```

```
/dev/da2 /dev/da2.eli
```

4. 创建新的文件系统

```
# dd if=/dev/random of=/dev/da2.eli bs=1m
```

```
# newfs /dev/da2.eli
```

```
# mount /dev/da2.eli /private
```

现在加密的文件系统应该已经可以被df(1)看到，并处于可用状态了。

```
# df -H
```

Filesystem	Size	Used	Avail	Capacity	Mounted on
/dev/ad0s1a	248M	89M	139M	38%	/
/devfs	1.0K	1.0K	0B	100%	/dev
/dev/ad0s1f	7.7G	2.3G	4.9G	32%	/usr
/dev/ad0s1d	989M	1.5M	909M	0%	/tmp
/dev/ad0s1e	3.9G	1.3G	2.3G	35%	/var
/dev/da2.eli	150G	4.1K	138G	0%	/private

5. 卸下卷并断开provider

一旦在加密分区上的工作完成，并且不再需要/private分区，就应考虑将其卸下并将geli加密分区从内核上断开。

```
# umount /private
```

```
# geli detach da2.eli
```

关于如何使用geli(8)的更多信息，可以在其联机手册中找到。

17.16.2.1 使用geli rc.d脚本

geli 提供了一个rc.d脚本，它可以用于简化geli的使用。通过rc.conf(5)配置geli的方法如下：

```
geli_devices="da2"
```

```
geli_da2_flags="-p -k /root/da2.key"
```

这会把/dev/da2配置为一个geli provider，其主密钥文件位于/root/da2.key，而geli在连接provider时将不使用口令字(注意只有在geli init阶段使用了-P才可以这样做)。系统将在关闭之前将geli provider断开。

关于如何配置rc.d的详细信息可以在使用手册的rc.d一节中找到。

17.17 对交换区进行加密

原作Christian Brüffer.

从FreeBSD 5.3-RELEASE 开始，FreeBSD 提供了易于配置的交换区加密机制。随所用的FreeBSD 版本，可用的配置选项会有所不同，而配置方法也会有一些差异。从FreeBSD 6.0-RELEASE 开始，已经可以使用**gbde(8)** 和**geli(8)** 两种加密系统来进行交换区的加密操作了。在更早的版本中，则只提供了**gbde(8)**。前面所说的这两种加密系统，都用到了**encswap** 这个rc.d 脚本。

在前面的小节如何加密磁盘分区 中，已经就不同的加密系统之间的区别进行了简单的讨论。

17.17.1 为什么需要对交换区进行加密？

与加密磁盘分区类似，加密交换区有助于保护敏感信息。为此，我们不妨考虑一个需要处理敏感信息的程序，例如，它需要处理口令。如果这些口令一直保持在物理内存中，则一切相安无事。然而，如果操作系统开始将内存页换出到交换区，以便为其他应用程序腾出内存时，这些口令就可能以未加密的形式写到磁盘上，并为攻击者所轻易获得。加密交换区能够有效地解决这类问题。

17.17.2 准备

注意：在本节余下的部分中，我们约定使用**ad0s1b** 作为交换区。

到目前为止，交换区仍是未加密的。很可能其中已经存有明文形式的口令或其他敏感数据。要纠正这一问题，首先应使用随机数来覆盖交换分区的数据：

```
# dd if=/dev/random of=/dev/ad0s1b bs=1m
```

17.17.3 使用**gbde(8)** 来加密交换区

如果使用FreeBSD 6.0-RELEASE 或更新的版本，则/etc/fstab 中与交换区对应的行中，设备名应追加**.bde** 后缀：

# Device	Mountpoint	FStype	Options	Dump	Pass#
/dev/ad0s1b.bde	none	swap	sw	0	0

对于FreeBSD 6.0-RELEASE 之前的版本，还需要在/etc/rc.conf 中加入：

```
gbde_swap_enable="YES"
```

17.17.4 使用**geli(8)** 来加密分区

另一种方法是使用**geli(8)** 来达到加密交换区的目的，其过程与使用**gbde(8)** 大体相似。此时，在/etc/fstab 中交换区对应的行中，设备名应追加**.eli** 后缀：

# Device	Mountpoint	FStype	Options	Dump	Pass#
----------	------------	--------	---------	------	-------

```
/dev/ad0s1b.eli          none          swap      sw          0          0
```

geli(8) 默认情况下使用密钥长度为256-位的AES 加密算法。

当然，这些默认值是可以通过/etc/rc.conf 中的geli_swap_flags 选项来修改的。下面的配置表示让rc.d 脚本encswap 创建一个geli(8) 交换区，在其上使用密钥长度为128-位的Blowfish 加密算法，4096 kilobyte 的扇区尺寸，并采用“最后一次关闭时卸下” 的策略：

```
geli_swap_flags="-a blowfish -l 128 -s 4096 -d"
```

请参见geli(8) 联机手册中关于onetime 命令的说明，以了解其他可用的选项。

17.17.5 验证所作的配置能够发挥作用

在重启系统之后，就可以使用swapinfo 命令来验证加密交换区是否已经在正常运转了。

如果使用了gbde(8)，则：

```
% swapinfo
Device          1K-blocks      Used      Avail Capacity
/dev/ad0s1b.bde   542720         0      542720      0%
```

如果使用了geli(8)，则：

```
% swapinfo
Device          1K-blocks      Used      Avail Capacity
/dev/ad0s1b.eli   542720         0      542720      0%
```

备注

1. 这个提示教您怎样选择一个安全易记的密钥短语，请看Diceware Passphrase (<http://world.std.com/~reinhold/diceware.html>) 网站。

第18章

GEOM: 模块化磁盘变换框架

原作Tom Rhodes.

18.1 概述

本章将介绍以FreeBSD GEOM 框架来使用磁盘。这包括了使用这一框架来配置的主要的RAID 控制工具。这一仗不会深入讨论GEOM 如何处理或控制I/O、其下层的子系统或代码。您可以从geom(4) 联机手册及其众多SEE ALSO 参考文献中得到这些信息。这一章也不是对RAID 配置的权威介绍，它只介绍由支持GEOM 的RAID 级别。

读完这章，您将了解：

- 通过GEOM 支持的RAID 类型。
- 如何使用基本工具来配置和管理不同的RAID 级别。
- 如何通过GEOM 使用镜像、条带、加密和挂接在远程的磁盘设备。
- 如何排除挂接在GEOM 框架上的磁盘设备的问题。

阅读这章之前，您应：

- 理解FreeBSD 如何处理磁盘设备(第17 章)。
- 了解如何配置和安装新的FreeBSD 内核(第8 章)。

18.2 GEOM 介绍

GEOM 允许访问和控制类(classes) ——主引导记录、BSD 标签(label)，等等——通过使用provider，或在/dev 中的特殊文件。它支持许多软件RAID 配置，GEOM 能够向操作系统，以及在其上运行的工具提供透明的访问方式。

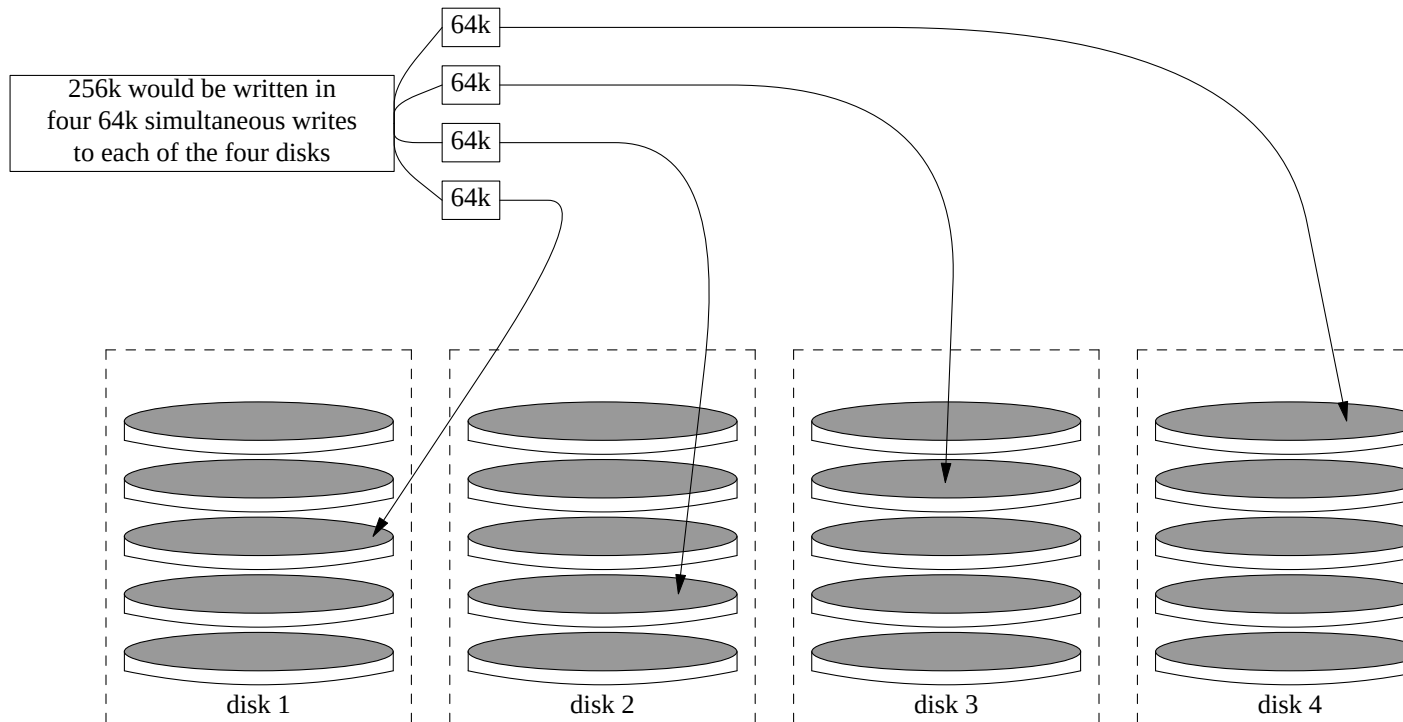
18.3 RAID0 - 条带

原作Tom Rhodes 和Murray Stokely.

条带是一种将多个磁盘驱动器合并为一个卷的方法。许多情况下，这是通过硬件控制器来完成的。GEOM 磁盘子系统提供了RAID0 的软件支持，它也成为磁盘条带。

在RAID0 系统中，数据被分为多个块，这些块将分别写入阵列的所有磁盘。与先前需要等待系统将256k 数据写到一块磁盘上不同，RAID0 系统，能够同时分别将打碎的64k 写到四块磁盘上，从而提供更好的I/O 性能。这一性能提升还能够通过使用多个磁盘控制器来进一步改进。

在RAID0 条带中的每一个盘的尺寸必须一样，因为I/O 请求是分散到多个盘上的，以便让这些盘上的读写并行完成。



在未格式化的ATA 磁盘上建立条带

1. 加载geom_stripe 模块:

```
# kldload geom_stripe.ko
```

2. 确信存在合适的挂接点(mount point)。如果这个卷将成为根分区，那么暂时把它挂接到其他位置i，如/mnt:

```
# mkdir /mnt
```

3. 确定将被做成条带卷的磁盘的设备名，并创建新的条带设备。举例而言，下面的命令可以把两个未用的、尚未分区的ATA 磁盘：/dev/ad2 和/dev/ad3 标记为条带卷成员。

```
# gstripe label -v st0 /dev/ad2 /dev/ad3
```

4. 此外还需要用下面的命令在新卷上创建分区表:

```
# bsdlabel -wB /dev/stripe/st0
```

5. 上述过程将在/dev/stripe 目录中的st0 设备基础上建立两个新设备。这包括st0a 和st0c。现在需要在st0a 设备上用下述newfs 命令来建立文件系统:

```
# newfs -U /dev/stripe/st0a
```

在屏幕上将滚过一些数字，整个操作应该能在数秒内完成。现在可以挂接刚刚做好的卷了。

下列命令可以用来手工挂接新创建的条带盘:

```
# mount /dev/stripe/st0a /mnt
```

要在启动过程中自动挂接这个条带上的文件系统，需要把关于卷的信息放到/etc/fstab 文件中:

```
# echo "/dev/stripe/st0a /mnt ufs rw 2 2" \
```

```
>> /etc/fstab
```

此外, `geom_stripe` 模块也必须通过在 `/boot/loader.conf` 中增加下述设置, 以便在系统初始化过程中自动加载。

```
# echo 'geom_stripe_load="YES"' >> /boot/loader.conf
```

18.4 RAID1 - 镜像

镜像是一种许多公司和家庭用户使用的不需中断的备份技术。当存在镜像时, 它的意思是说磁盘B简单地复制磁盘A。或者, 也可能是磁盘C+D复制磁盘A+B。无论磁盘如何配置, 共同的特征, 都是磁盘或卷的信息会被复制。随后, 这些信息可以很容易地恢复原样、备份, 而不需要造成服务或访问的停顿, 甚至其他更安全的地方。

要开始做这件事, 首先要确保系统中有两个同样大的磁盘驱动器, 下面的例子假定使用直接访问方式(Direct Access, da(4)) SCSI 的磁盘。

首先需要把FreeBSD安装到第一块磁盘上, 并建立两个分区。第一个分区将成为交换区, 其尺寸应该是两倍的RAM尺寸, 而余下的空间, 则作为根(/)文件系统来使用。当然, 也可以为其他挂接点划分不同的分区; 但是, 这将使难度提高一个量级, 因为您将不得不手工修改`bsdlablel(8)`和`fdisk(8)`的设置。

重新启动系统, 并等待其完全初始化完。当这个过程完成之后, 以root用户的身份登录。

创建`/dev/mirror/gm`设备, 并将其连接到`/dev/da1`:

```
# gmirror label -vnb round-robin gm0 /dev/da1
```

系统应会给出下列回应:

```
Metadata value stored on /dev/da1.
Done.
```

初始化GEOM, 这将加载`/boot/kernel/geom_mirror.ko`内核模块:

```
# gmirror load
```

注意: 这个命令应该会在`/dev/mirror`目录中创建`gm0`设备节点。

安装通用的`fdisk`标签以及引导区代码, 到刚刚创建的`gm0`设备上:

```
# fdisk -vBI /dev/mirror/gm0
```

接下来安装通用的`bsdlablel`信息:

```
# bsdlablel -wB /dev/mirror/gm0s1
```

注意: 如果存在多个区段(slice)或分区(partition), 则需要修改一部分上面命令的参数。它们必须与另一个盘上对应的区段和分区匹配。

使用newfs(8) 工具来, 在gm0s1a 设备节点上创建默认的文件系统:

```
# newfs -U /dev/mirror/gm0s1a
```

这将让系统输出很多信息和一系列数字。不必为此担心, 只需看看是否有错误提示就可以了, 如果没有问题, 接下来把它挂到/mnt 挂接点上面:

```
# mount /dev/mirror/gm0s1a /mnt
```

现在需要把所有引导盘上的数据迁移到新的文件系统上了。下面的例子使用了dump(8) 和restore(8) 这两个命令; 不过, 用dd(1) 在这里也可以达到完全一样的目的。

```
# dump -L -0 -f- / |(cd /mnt && restore -r -v -f-)
```

这个操作必须在所有文件系统上都作一遍。您可以将前述命令中的文件系统, 改为所希望的文件系统的位置。

接下来应该编辑复制出来的/mnt/etc/fstab 文件, 并删去或注释掉交换文件¹。修改其他文件系统对应的信息, 以便让它们使用新盘。参考下面的例子:

# Device	Mountpoint	FStype	Options	Dump	Pass#
#/dev/da0s2b	none	swap	sw	0	0
/dev/mirror/gm0s1a	/	ufs	rw	1	1

接下来需要建一个boot.conf 文件, 在当前和新盘的根分区上各放一份。这个文件将“帮助”系统的BIOS 从正确的驱动器上引导:

```
# echo "1:da(1,a)/boot/loader" > /boot.config
```

```
# echo "1:da(1,a)/boot/loader" > /mnt/boot.config
```

注意: 在所有的分区上都放这些是为了保证系统能够正确引导。如果由于某种原因系统无法从新的根分区读数据, 则还有一根救命稻草。

接下来, 在/boot/loader.conf 中加入一些新的设置:

```
# echo 'geom_mirror_load="YES"' >> /mnt/boot/loader.conf
```

者将让loader(8) 在系统初始化过程中自动加载geom_mirror.ko 模块。

最后重新启动系统:

```
# shutdown -r now
```

如果一切顺利, 系统将从gm0s1a 设备启动, 并给出login 提示等待用户登录。如果发生错误, 请查阅接下来的故障排除环节。我们接着将da0 磁盘也加入gm0 设备:

```
# gmirror configure -a gm0
# gmirror insert gm0 /dev/da0
```

此处-a 告诉gmirror(8) 采用自动同步, 或换言之: 自动地将磁盘的写操作做镜像处理。联机手册中详细解释了如何重建, 以及替换磁盘, 只不过它用data 表示这里的gm0。

18.4.1 故障排除

18.4.1.1 系统拒绝引导

如果系统引导时出现类似下面的提示:

```
ffs_mountroot: can't find rootvp
Root mount failed: 6
mountroot>
```

这种情况应使用电源或复位按钮重启机器。在引导菜单中, 选择第六(6)个选项。这将让系统进入loader(8)提示符。在此处手工加载内核模块:

```
OK? load geom_mirror.ko
OK? boot
```

如果这样做能解决问题, 则说明由于某种原因模块没有被正确加载。可以通过在内核配置文件中加入:

```
options GEOM_MIRROR
```

然后重新编译和安装内核来解决这个问题。

备注

1. 需要注意的是, 在**fstab**注释掉交换文件, 通常会需要您以其他方式重建交换空间。请参见第11.14节以了解进一步的细节。

第19章

Vinum 卷管理程序

Originally written by Greg Lehey.

19.1 概述

无论您有什么样的磁盘，总会有一些潜在问题：

- 它们可能容量太小。
- 它们可能速度太慢。
- 它们可能也太不可靠。

一些用户采取一些技术来保护他们免与受到这些问题的影响，例如使用多个，有些时候甚至是冗余的，磁盘。

除了支持许多种不同的硬件RAID 控制器之外，FreeBSD 的基本系统中包括了Vinum 卷管理器，它是一个用以实现磁盘驱动器的块设备。

Vinum 提供了比传统磁盘存储更好的灵活性、性能和可靠性，它还实现了RAID-0, RAID-1, 以及RAID-5 并可以单独和组合使用。

这一章对传统磁盘存储的潜在问题进行了简要说明，并介绍了Vinum 卷管理器。

注意：从FreeBSD 5 开始，对Vinum 进行了重写，以便使其符合GEOM 架构(第18 章)，而保留其原有的设计创意、术语，以及保存在磁盘上的元数据格式。这一重写的版本称为**gvinum**(表示 **GEOM vinum**)。接下来的文字中**Vinum** 是一个抽象的名字，通常并不具体指某一特定的实现。新版本中所有的指令都应通过**gvinum** 命令来操作，而对应的内核模块的名字，也由**vinum.ko** 改为了**geom_vinum.ko**，而在**/dev/vinum** 中的所有设备节点，也改为放到了**/dev/gvinum**。从FreeBSD 6 开始，旧版的Vinum 实现已不再提供。

19.2 磁盘容量太小

Vinum 是一个所谓的**卷管理工具**，是能够解决这三个问题的虚拟磁盘驱动程序。让我们来仔细地看看这些问题。已经有针对这些问题的很多方法被提出和实现了：

磁盘越大，存储的数据也就越多。您经常会发现您需要一个比您可使用的磁盘大得多的文件系统。无可否认，这个问题已经没有了十年前那样严峻了，但它仍然存在。通过创建一个在许多磁盘上存储数据的抽象设备，一些系统可以解决这个问题。

19.3 访问瓶颈

现代系统经常需要用高度并发的方式来访问数据。例如，巨大的FTP 或HTTP 服务器可以支持数以千计的并发会话，可以有多个连到外部世界的100 Mbit/s，这远远地超过了绝大多数磁盘的数据传输速率。

当前的磁盘驱动器最高可以以70 MB/s的速度传输数据,但这个值在一个有许多不受约束的进程访问一个驱动器的环境中变得并不重要,它们可能只完成了这些值的一小部分。这样一种情况下,从磁盘子系统的角度来看问题就更加有趣:重要的参数是在子系统上的负荷,换句话说就是传输占用了驱动器多少时间。

在任何磁盘传输中,驱动器必须先寻道,等待磁头访问第一个扇区,然后执行传输. 这些动作看起来可能很细小: 我们不会感有任何中断。

假设传输10 kB数据, : 现在的高性能磁盘平均寻道时间是3.5ms。最快的驱动器可以旋转在15,000 rpm, , 所以平均寻址时间为2ms. 在70 MB/s的速度传输时, 数据的传输时间大约150 μs, 几乎无法和寻址时间相比. 在这样一种情况下, 高效的传输也会降低到1 MB/s 显然传输的快慢依赖与所传输数据的大小。

对于这个瓶颈的一般和明显的解决方法是采用“多个磁盘”:而不是只使用一个大磁盘, 它使用几个比较小的磁盘联合起来形成一个大的磁盘. 每个磁盘都可以独立地进行传输数据, 所以通过使用多个磁盘大大提高了数据吞吐量。

当然, 所要求的吞吐量的提高要比磁盘的数量小得多。尽管每个驱动器并行传输数据, 但没有办法确保请求能够平均分配到每个驱动器上。不可避免一个驱动器的负载可能比另一个要高得多。

磁盘的负载平衡很大程度依赖于驱动器上数据的共享方式. 在下面的讨论中, 将磁盘存储想象成一个巨大的数据扇区, 像一本书的页那样用编号来设定地址. 最明显的方法是把虚拟磁盘分成许多连续的扇区组, 每个扇区大小就是独立的磁盘大小, 用这种方法来存储数据, 就像把一本厚厚的书分成很多小的章节。这个方法叫做**串联** 它有一个优点就是磁盘不需要有任何特定的大小关系。当访问到的虚拟磁盘根据它的地址空间来分布的时候, 它能工作得很好。当访问集中在一个比较小的区域的时候, 性能的提高没有显著的改进。图19-1 举例说明了用串联组织的方式来分配存储单元的顺序。

图19-1. 串联组织

Disk 1	Disk 2	Disk 3	Disk 4
0	6	10	12
1	7	11	13
2	8		14
3	9		15
4			16
5			17

另外一种影射方法是把地址空间分布在比较小的容量相同的磁盘上, 从而能够在不同的设备上存储它们。例如, 前256 个扇区可能存储在第一个磁盘上, 接着的256 个扇区存储在另一个磁盘上等等。写满最后一个磁盘后, 进程会重复以前的工作, 直到所有的磁盘被写满。这个影射叫做**分段(striping)** 或者RAID-0¹. 分段要求很精确地寻址, 通过多个磁盘进行数据传输的时候, 它可能会引起额外的I/O 负载, 但它也可能提供更多的连续负载。图19-2 显示了用分段形式分配的存储单元的顺序。

图19-2. 分段组织

Disk 1	Disk 2	Disk 3	Disk 4
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23

19.4 数据的完整性

当前磁盘的最后一个问题是它们不太可靠。虽然磁盘驱动器的可靠性在过去几年有了很大的提高，它们仍然是会损坏的服务器的最核心组件。当它们发生故障的时候，结果可能是灾难性的：替换一个坏的磁盘驱动器，然后恢复数据可能要花费几天时间。

解决这个问题的传统方法是建立镜像**镜象**，在不同的物理硬件上对数据做两个拷贝。由于RAID 的出现，所以这个技术也被叫做第一级RAID 或者RAID-1。任何写到卷的数据也会被写到镜象上，所以可以从任何一个拷贝读取数据，如果其中有一个失败了，数据就可以在其他驱动器上访问到。

镜象有两个问题：

- 价格。它需要两倍的存储容量。
- 性能影响。写入操作必须在两个驱动器上执行，所以它们花费两倍的带宽。读取数据并不会影响性能：看起来它们会更快。

一个可选的方案采用**parity**，其实现了RAID 2, 3, 4 和5。而其中，RAID-5 是我们最感兴趣的。在Vinum 的实现中，这是一个条带组织结构的变体，其中，每一个条带中都以一个专用的块，来保存其它块的奇偶校验值。这样，RAID-5 plex 除了在每个块中都包含了一个奇偶校验块之外，实现RAID-5 时也就和普通的条带plex 一样了。作为RAID-5 的一项要求，奇偶校验块在每一个条带中的顺序都是不同的。数据块的编号，决定了它的相对块号。

图19-3. RAID-5 的组织

Disk 1	Disk 2	Disk 3	Disk 4
0	1	2	Parity
3	4	Parity	5
6	Parity	7	8
Parity	9	10	11
12	13	14	Parity
15	16	Parity	17

与镜像相比，RAID-5 最显著的优势在于只需使用少得多的存储空间。读取类似于条带式存储的组织，但写入会慢得多，大约仅相当于读性能的25%。如果一个驱动器失效，则阵列仍然可以在降级的模式运行：读取来自正常的驱动器数据的操作照常进行，但读取失效的驱动器的数据，则来自于余下驱动器上相关的计算结果。

19.5 Vinum 目标

为了解决这些问题，Vinum 提出了一个四层的目标结构：

- 最显著的目标是虚拟磁盘，叫做**卷(volume)**。卷本质上与一个UNIX 磁盘驱动器有同样的属性，虽然它们是有些不太一样。它们没有大小的限制。
- 卷下面是**plexes**，每一个表示卷的所有地址空间。在层次结构中的这个水平能够提供冗余功能。可以把plex 想象成用一个镜像排列的方式组织起来的独立磁盘，每个都包含同样的数据。
- 由于Vinum 存在于UNIX 磁盘存储框架中，所以它也可能使用UNIX 分区作为多个磁盘plex 的组成部分，但事实上这并不可靠：UNIX 磁盘只能有有限数量的分区。取而代之，Vinum 把一个简单的UNIX 分区(the drive) 分解成叫做**subdisks**的相邻区域，它可以使用这个来为plex 建立块。
- Subdisks 位于Vinum 驱动器上，当前的UNIX 分区。Vinum 驱动器可以包含很多的subdisks。除了驱动器开始的一小块区域用来存储配置和描述信息以外，整个驱动器都可以用于存储数据。

下面的章节描述了这些目标提供了Vinum 所要求的功能的方法。

19.5.1 卷的大小要求

在Vinum的配置中，Plex可以把多个subdisk 分布在所有的驱动器上。结果，每个独立的驱动器的大小都不会限制plex 的大小，从而不会限制卷的大小

19.5.2 多余的数据存储

Vinum 通过给一个卷连上多个plex 来完成镜像的功能。每个plex 是一个在一个卷中的数据的描述。一个卷可以包含一个到八个plex。

Although虽然一个plex 描述了一个卷的所有数据，，但可能描述的部分被物理地丢失了。可能是设计的问题（没有为plex 部分定义一个subdisk）也可能是意外的故障（由于驱动器的故障导致）。只要至少有一个plex 能够为卷的完全地址范围提供数据，卷就能够正常工作。

19.5.3 性能问题

Vinum 在plex 水平既执行串联也执行分段：

- 一个串联的plex轮流使用每个subdisk 的地址空间。
- 一个分段的plex 在每个subdisk 上划分数据. Subdisk 必须是大小一样的，为了从一个连接的plex 中区分开它，必须至少有两个subdisk。

19.5.4 哪种plex 组织更有效？

FreeBSD 6.0提供的Vinum 版本能实现两种plex：

- 串联的plex 更加灵活：它们可以包含任何数量的subdisk，subdisk 也可能有不同的长度。Plex 可以通过添加额外的subdisk 来得到扩展。它们需要更少的CPU 时钟相对分段plexes, 尽管CPU 上的负载差异是不可测量的。另一方面，它们的负载可能不平衡，一个磁盘可能负载很重，而其他的可能很空闲。
- 分段(RAID-0) plexes 的最大优点是它们减少了负载不平衡的情况：通过选择一个最合适大小的分段(大约是256 kB), 您甚至可以在各个组成的驱动器上降低负载. 这种方法的缺点是在subdisk 上受到非常复杂的编码限制：它们必须是同样大小, 通过添加新的subdisk 来扩展一个plex 是非常复杂的, 以至Vinum 当前没有实现它. Vinum 利用一个额外的，代价不高的限制：一个分段的plex 必须有至少两个subdisk，因为否则的话，它是无法从一个连接的plex 进行区分的。

表19-1 总结一下每个plex 组织的优点和缺点.

表19-1. Vinum Plex组织图

Plex 类型	最少subdisks	可否添加subdisks	必须相同大小	应用
串联	1	可以	不可以	带有很大弹性和适中性能的大数据量存储。
分段	2	不可以	可以	大量并发访问时,具有较高性能。

19.6 一些例子

Vinum 维护着一个描述本系统中对象的**配置数据库**。开始时，用户可以在gvinum(8) 工具来从若干配置文件生成配置数据库。Vinum 在其控制的每个磁盘分区(在Vinum 中称为**device**) 上都保存配置数据库的副

本。这一数据库在每次状态变化时均会更新，因而重启每个Vinum对象时，都能够恢复其状态。

19.6.1 配置文件

配置文件描述了独立的Vinum，一个简单卷的定义可能是这样的：

```
drive a device /dev/da3h
volume myvol
plex org concat
sd length 512m drive a
```

这个文件描述了四个Vinum目标：

- **drive** 行描述了一个磁盘分区（驱动器）和与下面的硬件相关的它的位置。它给出了一个符号名**a**。这个与设备名称分开的符号名允许磁盘从一个位置移动到另一个位置而不会搞混。
- **volume** 行描述了一个卷。唯一的必须属性是名称，在这个例子中是**myvol**。
- **plex** 行定义了一个plex。唯一需要的参数是组织，在这个例子中是**concat**。没有名称是必然的：系统自动通过添加suffix **.p0** 来从卷名称产生一个名字，这里的**0**是在卷中的plex的编号。而这个plex将被叫做**myvol.p0**。
- **sd** 行描述了一个subdisk。最小的说明是存储subdisk的驱动器名称，和subdisk的长度。对于plex，没有名称也是必然的：系统自动通过添加suffix **.s0** 来分配源自plex的名称，这里**0**是plex中subdisk的编号。Vinum给这个subdisk命名为**myvol.p0.s0**。

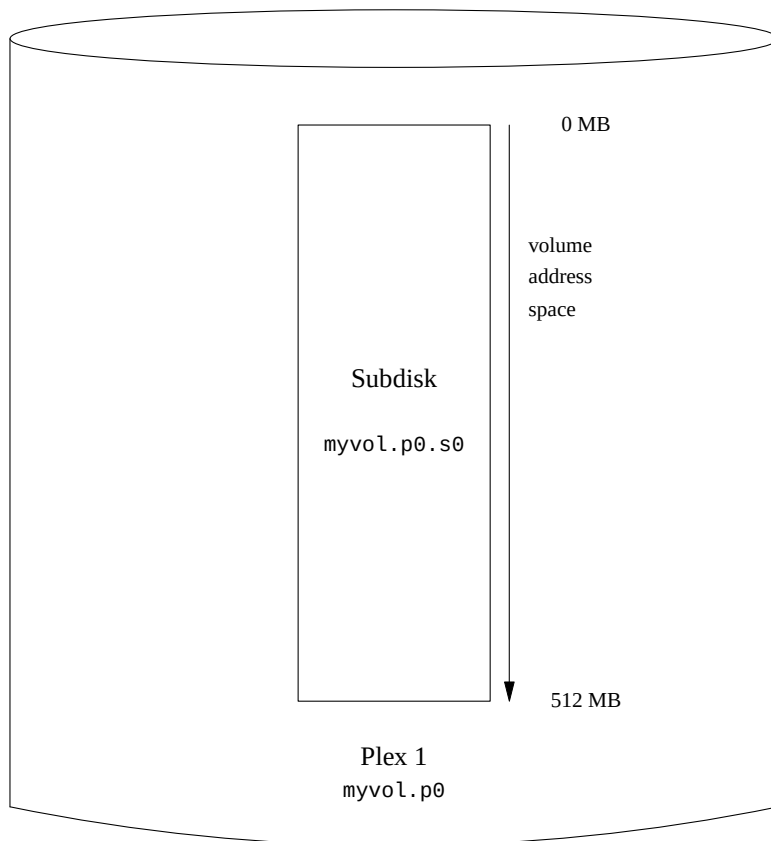
处理完这个文件后，gvinum(8)会产生下面的输出：

```
# gvinum -> create config1
Configuration summary
Drives:      1 (4 configured)
Volumes:     1 (4 configured)
Plexes:      1 (8 configured)
Subdisks:    1 (16 configured)
```

D a	State: up	Device /dev/da3h	Avail: 2061/2573 MB (80%)
V myvol	State: up	Plexes: 1	Size: 512 MB
P myvol.p0	C State: up	Subdisks: 1	Size: 512 MB
S myvol.p0.s0	State: up	P0: 0	B Size: 512 MB

这些输出内容展示了gvinum(8)的简要列表格式。在图19-4中用图形展示了这个配置。

图19-4. 一个简单的Vinum 卷



下面这个图显示了一个由按顺序排列的subdisk 组成的plex。在这个小小的例子中，卷包含一个plex，plex 包含一个subdisk。

这个卷本身和普通的磁盘分区相比并没有什么特别的优越性，它包含了一个plex，因此不是冗余的。这个plex 中包括了一个子磁盘，因此这和从磁盘分区分配存储没什么两样。接下来的几节，将介绍一些更有用的配置方法。

19.6.2 提高容错性：镜像

卷的容错性可以通过镜像来提高。在配置镜像卷时，确保plex 分布在不同的驱动器上十分重要，这样一个驱动器坏掉时，就不会同时影响两个plex。下面的配置将映射卷：

```
drive b device /dev/da4h
volume mirror
    plex org concat
        sd length 512m drive a
    plex org concat
```

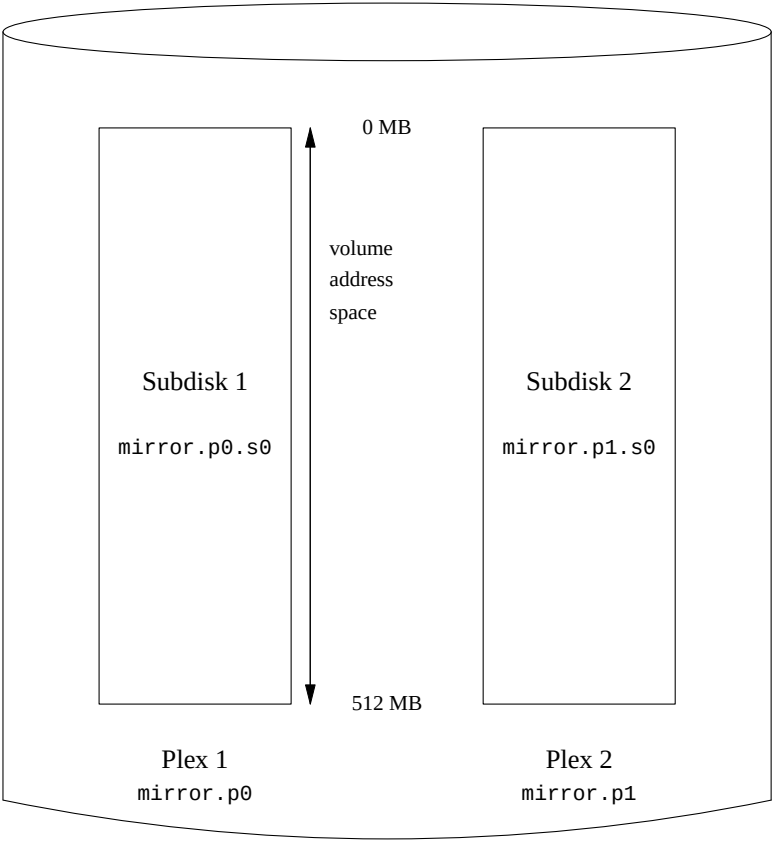
```
sd length 512m drive b
```

上面的例子中，并不需要再次指定驱动器a，因为Vinum 监控所有其配置数据库的对象。完成定义之后，配置如下所示：

Drives:	2 (4 configured)				
Volumes:	2 (4 configured)				
Plexes:	3 (8 configured)				
Subdisks:	3 (16 configured)				
D a	State: up	Device /dev/da3h	Avail: 1549/2573 MB (60%)		
D b	State: up	Device /dev/da4h	Avail: 2061/2573 MB (80%)		
V myvol	State: up	Plexes: 1	Size: 512 MB		
V mirror	State: up	Plexes: 2	Size: 512 MB		
P myvol.p0	C State: up	Subdisks: 1	Size: 512 MB		
P mirror.p0	C State: up	Subdisks: 1	Size: 512 MB		
P mirror.p1	C State: initializing	Subdisks: 1	Size: 512 MB		
S myvol.p0.s0	State: up	P0: 0	B Size: 512 MB		
S mirror.p0.s0	State: up	P0: 0	B Size: 512 MB		
S mirror.p1.s0	State: empty	P0: 0	B Size: 512 MB		

图19-5 以图形方式展示了其结构。

图19-5. 镜像Vinum 卷



这个例子中，每一个plex 包含了完整的512 MB 地址空间。在前面的例子中，plex 则只包括一个子盘。

19.6.3 优化性能

恰面例子中的镜像卷要比没有镜像的卷具有更好的容灾能力，但它的性能要差一些：每一次写入卷时，需要同时写道两个驱动器上，因而也就需要更大的磁盘访问带宽。如果希望非常好的性能，则需要另外一种方式：不做镜像，而将数据分成条带放到尽可能多的、不同的磁盘上。下面给出了一个跨越四个磁盘驱动器的plex 卷：

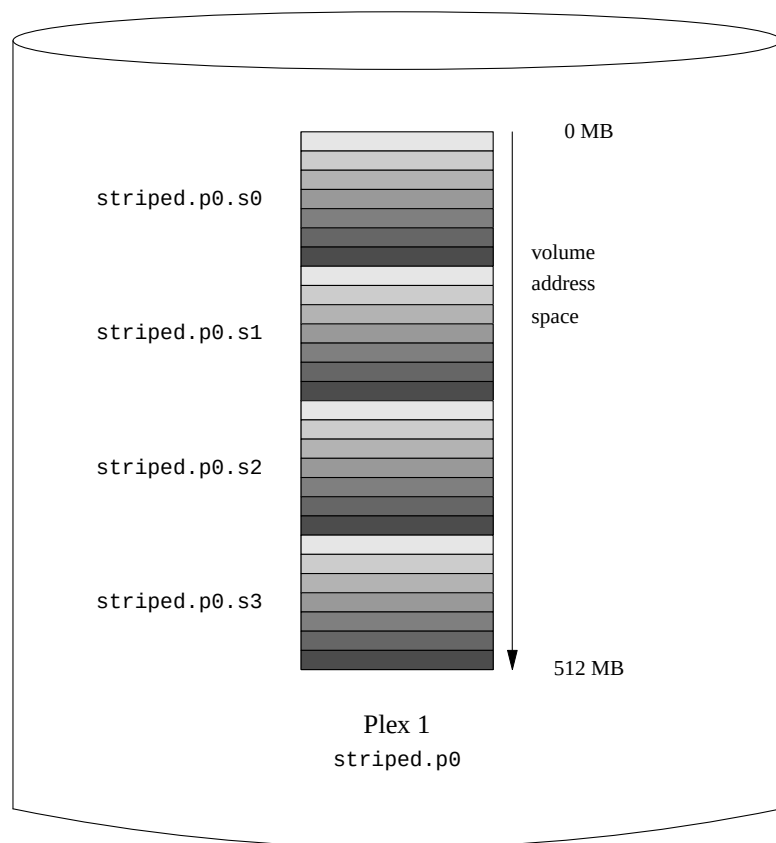
```
drive c device /dev/da5h
drive d device /dev/da6h
volume stripe
plex org striped 512k
  sd length 128m drive a
  sd length 128m drive b
  sd length 128m drive c
  sd length 128m drive d
```

和之前类似，并不需要定义Vinum 已经知道的驱动器。在完成定义之后，将得到如下配置：

```
Drives:      4 (4 configured)
Volumes:     3 (4 configured)
Plexes:      4 (8 configured)
Subdisks:    7 (16 configured)
```

D a	State: up	Device /dev/da3h	Avail: 1421/2573 MB (55%)
D b	State: up	Device /dev/da4h	Avail: 1933/2573 MB (75%)
D c	State: up	Device /dev/da5h	Avail: 2445/2573 MB (95%)
D d	State: up	Device /dev/da6h	Avail: 2445/2573 MB (95%)
V myvol	State: up	Plexes: 1 Size:	512 MB
V mirror	State: up	Plexes: 2 Size:	512 MB
V striped	State: up	Plexes: 1 Size:	512 MB
P myvol.p0	C State: up	Subdisks: 1 Size:	512 MB
P mirror.p0	C State: up	Subdisks: 1 Size:	512 MB
P mirror.p1	C State: initializing	Subdisks: 1 Size:	512 MB
P striped.p1	State: up	Subdisks: 1 Size:	512 MB
S myvol.p0.s0	State: up	P0: 0 B Size:	512 MB
S mirror.p0.s0	State: up	P0: 0 B Size:	512 MB
S mirror.p1.s0	State: empty	P0: 0 B Size:	512 MB
S striped.p0.s0	State: up	P0: 0 B Size:	128 MB
S striped.p0.s1	State: up	P0: 512 kB Size:	128 MB
S striped.p0.s2	State: up	P0: 1024 kB Size:	128 MB
S striped.p0.s3	State: up	P0: 1536 kB Size:	128 MB

图19-6. 条带化的Vinum 卷



这个卷在图19-6 中给出。条带的阴影部分，表示在plex 地址空间中的位置：颜色最浅的在最前面，而最深的在最后。

19.6.4 高性能容在

如果硬件足够多，也能够构建比标准UNIX 分区同时提高了容灾性和性能的卷。典型的配置文件类似：

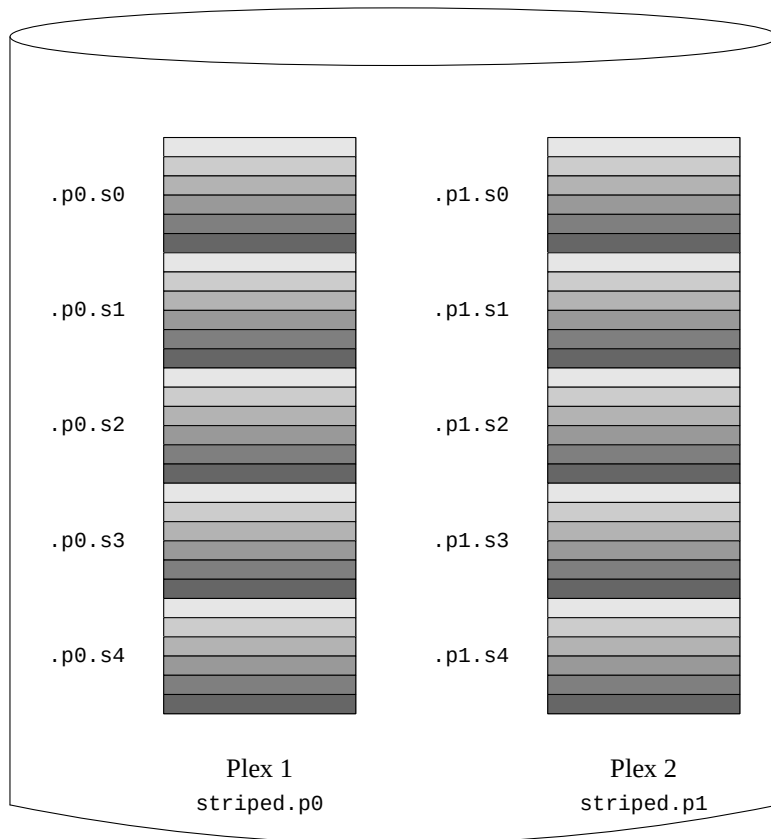
```
volume raid10
  plex org striped 512k
    sd length 102480k drive a
    sd length 102480k drive b
    sd length 102480k drive c
    sd length 102480k drive d
    sd length 102480k drive e
  plex org striped 512k
    sd length 102480k drive c
    sd length 102480k drive d
```

```
sd length 102480k drive e
sd length 102480k drive a
sd length 102480k drive b
```

第二个plex 中的子盘和第一个plex 中的错开了两个驱动器：这能够帮助确保即使同时访问两个驱动器，写操作也不会同时发生在同一个盘上。

图19-7 给出了该卷的结构。

图19-7. 镜像并条带化的Vinum 卷



19.7 对象命名

如前面所描述的那样，Vinum 会给plex 和子盘指定默认的名字，而这些名字也是可以定制的。不推荐盖面默认的名字：使用允许给对象任意命名的VERITAS 卷管理器的经验证明，这一灵活性并没有带来太多

的好处，相反，它很容易导致对象的混淆。

名字中可以包括任何非空白的字符，但一般来说，建议只使用字母、数字和下划线。卷、plex，以及子盘的名字，可以包含最多64个字符，而驱动器的名字，则最长可以使用32个字符。

Vinum对象会在/dev/gvinum之下生成设备接点。前述的配置将使Vinum创建以下设备节点：

-

注意： 这些内容仅适用于旧式的Vinum实现。

控制设备/dev/vinum/control和/dev/vinum/controlld，分别由gvinum(8)和Vinum服务使用。

- 每个卷对应的设备项。这些是Vinum使用的主要设备。因此，前述配置包括下列设备：
/dev/gvinum/myvol、/dev/gvinum/mirror、/dev/gvinum/striped、/dev/gvinum/raid5以及/dev/gvinum/raid10。

-

注意： 这些内容仅适用于旧式的Vinum实现。

一个包含每个驱动器对应项的/dev/vinum/drive目录。这些项事实上是指向对应磁盘节点的符号连接。

- 所有卷的直接项都存放在/dev/gvinum/中。
- 目录/dev/gvinum/plex，以及/dev/gvinum/sd中相应地存放了每个plex以及子盘的设备节点。

例如，考虑下面的配置文件：

```
drive drive1 device /dev/sd1h
drive drive2 device /dev/sd2h
drive drive3 device /dev/sd3h
drive drive4 device /dev/sd4h
volume s64 setupstate
plex org striped 64k
sd length 100m drive drive1
sd length 100m drive drive2
sd length 100m drive drive3
sd length 100m drive drive4
```

处理这个文件之后，gvinum(8)将在/dev/gvinum中建立下面的结构：

```
drwxr-xr-x  2 root  wheel      512 Apr 13 16:46 plex
crwxr-xr--  1 root  wheel    91,   2 Apr 13 16:46 s64
drwxr-xr-x  2 root  wheel      512 Apr 13 16:46 sd

/dev/vinum/plex:
total 0
```

```
crwxr-xr-- 1 root wheel 25, 0x10000002 Apr 13 16:46 s64.p0

/dev/vinum/sd:
total 0
crwxr-xr-- 1 root wheel 91, 0x20000002 Apr 13 16:46 s64.p0.s0
crwxr-xr-- 1 root wheel 91, 0x20100002 Apr 13 16:46 s64.p0.s1
crwxr-xr-- 1 root wheel 91, 0x20200002 Apr 13 16:46 s64.p0.s2
crwxr-xr-- 1 root wheel 91, 0x20300002 Apr 13 16:46 s64.p0.s3
```

虽然plex和子盘一般并不推荐指定名字，但还是必须给Vinum驱动器命名。这样，当把驱动器转移到不同的地方时，它仍然能够被自动地识别出来。驱动器名最长可以包含32个字符。

19.7.1 创建文件系统

对于系统而言，卷和磁盘是一样的。唯一的例外是，与UNIX驱动器不同，Vinum并不对卷进行分区，因而它也就不包含分区表。这导致修改了某些磁盘工具，特别是newfs(8)，它会试图将Vinum卷名当作分区标识。例如，磁盘驱动器的名字可能是/dev/ad0a或/dev/da2h。这些名字分别表达在第一个(0) IDE (ad) 磁盘上的第一个分区(a)，以及第三个(2) SCSI 磁盘(da)上的第八个分区(h)。于此相反，Vinum卷可能叫做/dev/gvinum/concat，这个名字和分区名没有什么关系。

一般而言，newfs(8)会试图解释磁盘的名字，如果它无法理解这个名字，则会给出错误提示。例如：

```
# newfs /dev/gvinum/concat
newfs: /dev/gvinum/concat: can't figure out file system partition
```

要在这个卷上创建文件系统，则需要使用newfs(8)：

```
# newfs /dev/gvinum/concat
```

注意：对于FreeBSD 5.0 之前的版本，newfs(8)还需要指定一个-v参数，而且其设备命名方式也是旧式的：

```
# newfs -v /dev/vinum/concat
```

19.8 配置Vinum

在GENERIC内核中，并不包含Vinum。可以编译一个定制的包含Vinum的内核，然而并不推荐这样做。启动Vinum的标准方法，是使用内核模块(kld)。甚至不需要使用kldload(8)来启动Vinum：在启动gvinum(8)时，它会检查这一模块是否已经加载，如果没有，则会自动地加载它。

19.8.1 启动

Vinum将配置信息，采用与配置文件一样的形式来存放到磁盘分区上。当从配置数据库中读取时，Vinum会识别一系列在配置文件中不可用的关键字。例如，磁盘配置文件可能包含下面的文字：

```
volume myvol state up
volume bigraid state down
plex name myvol.p0 state up org concat vol myvol
plex name myvol.p1 state up org concat vol myvol
plex name myvol.p2 state init org striped 512b vol myvol
```

```
plex name bigraid.p0 state initializing org raid5 512b vol bigraid
sd name myvol.p0.s0 drive a plex myvol.p0 state up len 1048576b driveoffset 265b plexoffset 0b
sd name myvol.p0.s1 drive b plex myvol.p0 state up len 1048576b driveoffset 265b plexoffset 1048576b
sd name myvol.p1.s0 drive c plex myvol.p1 state up len 1048576b driveoffset 265b plexoffset 0b
sd name myvol.p1.s1 drive d plex myvol.p1 state up len 1048576b driveoffset 265b plexoffset 1048576b
sd name myvol.p2.s0 drive a plex myvol.p2 state init len 524288b driveoffset 1048841b plexoffset 0b
sd name myvol.p2.s1 drive b plex myvol.p2 state init len 524288b driveoffset 1048841b plexoffset 524288b
sd name myvol.p2.s2 drive c plex myvol.p2 state init len 524288b driveoffset 1048841b plexoffset 1048576b
sd name myvol.p2.s3 drive d plex myvol.p2 state init len 524288b driveoffset 1048841b plexoffset 1572864b
sd name bigraid.p0.s0 drive a plex bigraid.p0 state initializing len 4194304b driveoff set 1573129b plexoffset 0b
sd name bigraid.p0.s1 drive b plex bigraid.p0 state initializing len 4194304b driveoff set 1573129b plexoffset 4194304b
sd name bigraid.p0.s2 drive c plex bigraid.p0 state initializing len 4194304b driveoff set 1573129b plexoffset 8388608b
sd name bigraid.p0.s3 drive d plex bigraid.p0 state initializing len 4194304b driveoff set 1573129b plexoffset 12582912b
sd name bigraid.p0.s4 drive e plex bigraid.p0 state initializing len 4194304b driveoff set 1573129b plexoffset 16777216b
```

这里最明显的区别是，指定了配置的位置信息、名称(这些在配置文件中还是可用的，但不鼓励用户自行指定)以及状态信息(这是用户不能指定的)。Vinum 并不在配置信息中保存关于驱动器的信息：它会扫描已经配置的磁盘驱动器上包含Vinum 标识的分区。这使得Vinum 能够在UNIX 驱动器被指定了不同的ID 时也能够正确识别它们。

19.8.1.1 自动启动

注意：这些内容仅适用于旧式的Vinum 实现。在Gvinum 内核模块加载时，总会执行自动启动操作。

要在引导系统时自动启动Vinum，需要在/etc/rc.conf 中加入下面的配置：

```
start_vinum="YES" # set to YES to start vinum
```

如果您的系统中没有/etc/rc.conf，创建一个并加入这些设置就可以了。这样，系统就会在启动时自动加载Vinum 的kld，并启动配置中所提到的所有对象。这是在挂接文件系统之前进行的，因此，fsck(8) 和挂接文件系统都能够自动地在Vinum 卷上进行。

当使用vinum start 命令来启动Vinum 时，Vinum 会从某一个Vinum 驱动器中读取配置数据库。正常情况下，每个驱动器上都包含了同样的配置数据库副本，因此从哪个驱动器上读取是无所谓的。但是，在系统崩溃之后，Vinum 就必须检测哪一个驱动器上的配置数据库是最新的，并从上面读取配置。如果需要，它会更新其它驱动器上的配置。

19.9 使用Vinum 作为根文件系统

如果文件系统使用完全镜像的Vinum 配置，有时也会希望根文件系统也作了镜像。这种配置要比镜像其它文件系统麻烦一些，因为：

- 根文件系统在引导过程中很早的时候就必须处于可用状态，因此Vinum 的基础设施在这一时刻就应该可用了。
- 包含根文件系统的卷，同时也保存了系统的引导程序和内核，因此它们必须能够被宿主系统的内建工具(例如PC 机的BIOS) 识别，而通常是没有办法让它们了解Vinum 的细节的。

下面几节中，术语“根卷” 标识包含根文件系统的Vinum 卷。把这个卷命名为"root" 可能是个不错的主意，不过从技术上说，并不严格地要求这样做。不过，接下来的命令例子都使用这个名字。

19.9.1 及早启动Vinum 以适应对根文件系统的要求

有许多关于它的尺度:

- Vinum 必须在启动时可以被内核使用。因此, 在第19.8.1.1 节 中所介绍的方法, 也就无法适应这一任务的需要了。在接下来的配置中, 也不能 设置start_vinum 参数。第一种方法是通过将Vinum 静态联编到内核中来实现, 这样, 它就在任何时候都可用了, 虽然一般并不需要这样。另一种方法是通过/boot/loader (第12.3.3 节) 来尽早加载vinum 内核模块, 这一操作发生在内核加载之前。这可以通过将下面的配置:

```
geom_vinum_load="YES"
```

加入到/boot/loader.conf 文件中来实现。

-

注意: 对Gvinum 而言, 所有的启动过程都是在内核模块加载时自动进行的, 因此上面的操作, 也就是所要进行的全部工作了。下面的文字介绍的是旧式的Vinum 系统, 保留它们的主要是为了方便那些使用旧版系统的用户。

Vinum 必须尽早初始化, 因为需要由它来提供根文件系统的卷。默认情况下, Vinum 的内核部分并不主动地查找可能包含Vinum 卷信息的驱动器, 而会等待管理员(或者某个启动脚本) 来执行vinum start 命令。

注意: 下面介绍的是FreeBSD 5.X 和更高版本所需的配置。对于FreeBSD 4.X 的配置方法与此不同, 在第19.9.5 节 中有所描述。

通过将下面的配置:

```
vinum.autostart="YES"
```

加入/boot/loader.conf, Vinum 将在内核部分初始化的过程中, 自动地扫描所有的驱动器以查找Vinum 信息。

需要说明的是, 并不需要指定内核到什么地方去找根文件系统。/boot/loader 会在/etc/fstab 中查找根文件系统的设备名, 并将这一信息转交给内核。当需要挂接根文件系统时, 内核会根据设备名来知道它由哪个驱动提供, 并将其转译为内部设备ID (major/minor 编号)。

19.9.2 让基于Vinum 的卷在引导时可以访问

因为目前的FreeBSD 引导程序只有7.5 KB 的代码, 并且已经承担了从UFS 文件系统中读取文件(例如/boot/loader) 的重任, 因此完全没有办法再让它去分析Vinum 配置数据中的Vinum 结构, 并找到引导卷本身的信息。因此, 需要一些技巧来为引导代码提供标准的"a" 分区, 而它则包含了根文件系统。

要让这些得以实现, 根卷需要满足下面的条件:

- 根卷不能是条带卷或RAID-5 卷。
- 根卷plex 不能包含连接的子盘。

需要说明的是，使用多个plex，每个plex都复制一份根文件系统的副本，是需要而且是可行的。然而，引导过程只能使用这些副本中的一个来引导系统，直到内核最终自行挂接根文件系统为止。这些plex中的每个子盘，在这之后会有它们自己的"a"分区，以表达每一个可以引导的设备。每一个"a"分区，尽管并不需要和其它包含根卷的plex处于各自驱动器的同一位置。但是，这样创建Vinum卷使得镜像卷相互对称，从而能够避免了混淆。

为了创建每一个根卷的"a"分区，需要完成下面的操作：

1. 使用下面的命令来了解根卷成员子盘的位置(从设备开始的偏移量)和尺寸：

```
# gvinum l -rv root
```

需要注意的是，Vinum 偏移量和尺寸的单位是字节。它们必须是512的整数倍，才能得到disklabel命令所需的块号。

2. 在每一个根卷成员设备上，执行命令：

```
# disklabel -e devname
```

这其中，对于没有slice(也就是fdisk)表的磁盘，devname必须是磁盘的名字(例如da0)，或者是slice的名字(例如ad0s1)。

如果设备上已经有了"a"分区(比如说，包含Vinum之前的根文件系统)，则应改为其它的名字，以便继续访问(如果需要的话)，但它并不会继续用于启动系统。注意，活动的分区(类似正挂接的根文件系统)不能被改名，因此，要完成这项工作，必须从“Fixit”盘启动，或者分两步操作，并(在镜像情形中)首先操作那些非引导盘。

然后，设备上Vinum分区的偏移(如果有的话)必须加到这个设备上根卷对应的子盘上。其结果值，将成为新的"a"分区的"offset"值。这个分区的"size"值，可以根据前面的配置计算得出。"fstype"应该是4.2BSD。"fsize"、"bsize"，以及"cpg"值，则应与文件系统的实际情况匹配，尽管在配置Vinum时并不重要。

这样，新的"a"分区，将创建并覆盖这一设备上的Vinum分区的范围。注意，disklabel只有在Vinum分区的fstype被标记为"vinum"时，才允许这样做。

3. 这就成了！所有的"a"分区现在都已存在，而且是根卷的一份副本。强烈建议您再次验证其结果，方法是：

```
# fsck -n /dev/devnamea
```

务必注意，所有包含控制信息的文件，都必须放到Vinum卷上的根文件系统。在启动新的Vinum根卷时，它们可能和实际在用的根文件系统不匹配。因此，/etc/fstab和/boot/loader.conf这两个文件需要特别地注意。

在下次重启时，引导程序需要从新的基于Vinum的根文件系统中获取适当的控制信息，并据此工作。在内核初始化过程的结尾部分，在所有的设备都被宣示之后，如果显示了下面的信息，则表示配置成功：

```
Mounting root from ufs:/dev/gvinum/root
```

19.9.3 基于Vinum的根文件系统的配置范例

在Vinum根卷配置好之后，gvinum l -rv root的输出可能类似下面的样子：

```
...
Subdisk root.p0.s0:
```



```
Size:          125829120 bytes (120 MB)
State: up
Plex root.p0 at offset 0 (0 B)
Drive disk0 (/dev/da0h) at offset 135680 (132 kB)
```

```
Subdisk root.p1.s0:
Size:          125829120 bytes (120 MB)
State: up
Plex root.p1 at offset 0 (0 B)
Drive disk1 (/dev/da1h) at offset 135680 (132 kB)
```

需要注意的值是135680，也就是偏移量(相对于/dev/da0h分区)。这相当于disklabel记法中的265个512-字节的磁盘块。类似地，根卷的尺寸是245760个512-字节的磁盘块。/dev/da1h中，包含了根卷的第二个副本，采用了同样的配置。

这些设备的disklabel类似下面的样子：

```
...
8 partitions:
#      size  offset  fstype  [fsize bsize bps/cpg]
a:   245760    281   4.2BSD   2048 16384    0  # (Cyl.   0* - 15*)
c: 71771688     0  unused     0     0    0  # (Cyl.   0 - 4467*)
h: 71771672    16   vinum                # (Cyl.   0* - 4467*)
```

可以看到，伪装的"a"分区的"size"参数和前面的一样，而"offset"参数则是Vinum分区"h"，以及设备中这一分区(或slice)的偏移量之和。这是一种典型的配置，它能够避免在第19.9.4.3节中介绍的问题。此外，我们也看到整个"a"分区完全处于设备上包含了Vinum数据的"h"分区之中。

注意，在上面的配置中，整个设备都是Vinum专用的，而且没有留下Vinum之前的根分区，因为它永久性地成为了新建的Vinum配置中的一个子盘。

19.9.4 故障排除

如果遇到了问题，则需要从中恢复的办法。下面列出了一些常见的缺陷，及其解决方法。

19.9.4.1 系统的引导程序加载了，但无法启动

如果由于某种原因系统不再继续启动，引导程序可以在10-秒倒计时的时候，按space键来停止。加载器变量(例如vinum.autostart)可以通过使用show命令来查看，并使用set和unset命令来设置。

如果遇到的问题是由于Vinum的内核模块没有列入预加载的列表，而没有正确加载，则简单使用load geom_vinum会有所帮助。

此后，可以使用boot -as来继续启动过程。选项-as会要求内核询问所挂接的根文件系统(-a)，并使引导过程在单用户模式停止(-s)，此时根文件系统是以只读方式挂接的。这样，及时只挂接了多plex卷中的一个plex，也不会引致plex之间数据不一致的问题。

当提示输入要挂接的根文件系统时，可以输入任何一个包含根文件的设备。如果正确地配置了/etc/fstab，则默认的应该是类似ufs:/dev/gvinum/root。一般可以使用类似ufs:da0d这样的设备来代替它，因为它通常包括了Vinum之前的根文件系统。需要注意的是，如果在这里输入了"a"分区，则它可能表达的实际上是Vinum根设备的一个子盘，而在镜像式配置中，这只会挂接镜像的根设备中的一个。如果之后将这个文件系统以读写方式挂接，则需要从Vinum根卷中删去其他的plex，否则这些卷中可能会包含不一致的数据。

19.9.4.2 只加载了主引导程序

如果/boot/loader 加载失败，而主引导程序加载正常(在启动时，屏幕最左边一列有一个旋转的线)，则可以尝试在此时中断主引导程序的过程，方法是按space 键。这将在引导的第二阶段暂停，具体可以参见第12.3.2 节。此时，可以尝试从另一个分区，例如原先包含根文件系统，并不再叫作"a" 的那个分区，启动。

19.9.4.3 无法启动，引导程序发生panic

这种情况一般是由于Vinum 安装过程中破坏了引导程序造成的。不幸的是，Vinum 目前只在分区开始的地方保留了4 KB 的空间，之后就开始写Vinum 头信息了。然而，目前第一阶段和第二阶段的引导程序，加上disklabel 嵌入的内容则需要8 KB。因此，如果Vinum 分区从偏移量0 开始，而这个slice 或磁盘能够启动，则Vinum 的安装将毁掉引导程序。

类似地，如果从上述情形中恢复，例如，从“Fixit” 盘启动，并通过disklabel -B 按照第12.3.2 节中介绍的方法来恢复引导程序，则引导程序会覆盖掉Vinum 头，这样Vinum 也就找不到它的磁盘了。尽管这并不会真的毁掉Vinum 的配置数据，或者Vinum 卷上的数据，并且可以通过输入一模一样的Vinum 配置数据来恢复，但从这种状况中完全恢复是非常困难的。要真正解决问题，必须将整个Vinum 分区向后移动至少4 KB，以便使Vinum 头和系统的引导程序不再冲突。

19.9.5 与FreeBSD 4.X 的区别

在FreeBSD 4.X 中，由于缺少那些让Vinum 自动扫描所有磁盘所需的内部函数，而检测根设备的内部ID 的代码不够智能，以至于无法自动处理类似/dev/vinum/root 这样的名字。因此，会有一些小差异。

必须明确地告诉Vinum 要扫描哪些磁盘，方法是在/boot/loader.conf 中加入：

```
vinum.drives="/dev/da0 /dev/da1"
```

所有可能包含Vinum 数据的盘在这里都应提及。基本原则是，宁多毋缺。此外，也无需明确指定slice 或分区，因为Vinum 在指定的驱动器上的所有slice 和分区上扫描Vinum 头。

由于用以分析根文件系统名字，并产生设备ID (major/minor 编号) 的程序，只能够处理“传统的” 类似/dev/ad0s1a 这样的设备名，因此它们不可能处理类似/dev/vinum/root 这样的根卷名。因此，Vinum 本身需要预先配置内核的一些内部参数，以便在初始化时能够保持根设备的ID。这可以通过加载器变量vinum.root 来配置，对应的/boot/loader.conf 设置是：

```
vinum.root="root"
```

现在，当内核初始化过程尝试找到要挂接的root 设备时，它将能看到是否已经有某个内核模块预先初始化了所需要的内核参数。这种情况下，并且所指定的根设备和来自加载器的根设备(也就是我们的"vinum") 的major 编号相符，则就是用预先分配的设备ID，而不是自己去找一个。这样，在通常的自动启动过程中，它就能够继续挂接Vinum 根卷来作为根文件系统了。

但是，当指定了boot -a 来要求在启动时手工选择根设备时，仍然是无法自动地分析Vinum 卷名的。如果输入的设备名与Vinum 设备不匹配，则major 编号的不匹配会使这个过程采用普通的分析过程，这样，输入ufs:da0d 就能够正常工作了。注意，一旦这个过程失败，则再输入ufs:vinum/root 将不能正常工作，因为它无法再被解析了。唯一的解决办法是，重新启动并从头开始(在“askroot” 提示处，可以省略/dev/。)

备注

1. RAID 代表廉价磁盘容错(**Redundant Array of Inexpensive Disks**) 提供各种容错机制，但后面这个术语可能有些让人误解：它不提供冗余功能。

第20章

本地化—**I18N/L10N**使用和设置

Contributed by Andrey Chernov. Rewritten by Michael C. Wu.

20.1 概述

FreeBSD是一个由分布于全世界的用户和贡献者支持的项目。本章将讨论FreeBSD的国际化和本地化的问题,允许非英语用户也能使用FreeBSD很好地工作。在系统和应用水平上,主要是通过执行i18n标准来实现的,所以这里我们将为读者提供详细的介绍。

读完这一章,您将了解到:

- 不同的语言和地域是如何在现代操作系统上进行编码的。
- 如何为您的登入shell设置本地化。
- 如何配置您的控制台为非英语语言。languages.
- 如何使用不同的语言来有效地使用X Windows。
- 在哪里可以找到更多有关开发符合i18n标准的应用程序的信息。

阅读这章之前,您应当了解:

- 怎样安装额外的第三程序(第4章)。

20.2 基础知识

20.2.1 I18N/L10N 是什么?

开发人员把internationalization简写成I18N,中间的数字是前后两个字母间的字母个数。L10N依据“localization”使用同样的命名规则。I18N/L10N方法、协议和应用结合在一起,允许用户使用他们自己所选择的语言。

I18N应用程序使用I18N工具来编程。它允许开发人员写一个简单的文件,就可以将显示的菜单和文本翻译成本地语言。我们非常鼓励程序员遵循这种规则。

20.2.2 为什么要使用I18N/L10N?

I18N/L10N标准能够很好地支持您查看、输入或处理非英语语言。

20.2.3 I18N支持哪些语言?

I18N和L10N不是FreeBSD特有的。当前,它能支持世界上绝大部分主力语言,包括但不限于:中文,德文,日文,朝鲜文,法文,俄文,越南文等等。

20.3 使用本地化语言

I18N不是FreeBSD特有的，它是一个规则。我们鼓励您帮助FreeBSD完善这一规则。

本地化设置需要具备三个条件：语言代码(Language Code)、国家代码(Country Code) 和编码(Encoding)。本地名字可以用下面这些部分来构造：

语言代码_国家代码. 编码

20.3.1 语言和国家代码

为了用特殊的语言来对FreeBSD系统进行本地化（或其他类UNIX系统），用户必须要知道相应的国家和语言代码（国家代码告诉应用程序使用哪一种语言规范）。此外，WEB浏览器，SMTP/POP服务器，web服务器等都是以此为基础的。下面就是一个国家和语言代码的例子：

语言/国家代码	描述
en_US	美国英语
ru_RU	俄语
zh_CN	简体中文

20.3.2 编码

一些语言不使用ASCII 编码，它们使用8-位，宽或多字节的字符，更多的信息请参考multibyte(3)。比较老的应用程序可能会无法识别它们，并误认为是控制字符。比较新的应用程序通常会认出8-位字符。随实现的不同，用户可能不得不将宽或多字节字符支持编入应用程序，或进行一些额外的配置，才能够正常使用它们。要输入和处理宽或多字节字符，FreeBSD Ports Collection (<http://www.FreeBSD.org/ports/index.html>) 已经为每种语言提供了不同的程序。请参考各个FreeBSD Port 中的I18N 文档。

特别需要指出的是，用户可能需要查看应用程序的文档，以确定如何正确地配置它，或需要为configure/Makefile/编译器指定什么样的参数。

记住下面这些：

- 特定语言的简单C字符集(参见multibyte(3))，例如ISO8859-1, ISO8859-15, KOI8-R, CP437。
- 宽字节或多字节编码，如EUC, Big5。

您可以在IANA Registry (<http://www.iana.org/assignments/character-sets>)检查一下现行的字符集列表。

注意：与此不同的是，FreeBSD 使用与X11-兼容的本地编码模式。

20.3.3 I18N应用程序

在FreeBSD Ports和Package系统里面，I18N应用程序已经使用I18N 来命名。然而它们不是总支持需要的语言。

20.3.4 本地化设置

通常只要在登入shell里面设置LANG为本地化，一般通过设置用户的`~/.login_conf` 或用户shell的启动文件 (`~/.profile`, `~/.bashrc`, `~/.cshrc`)。没有必要设置LC_CTYPE, LC_CTIME。更多的信息请参考特定语言的FreeBSD文档。

您应当在您的配置文件中设置下面两个变量：

- LANG 为POSIX设置本地化语言功能。
- MM_CHARSET应用程序的MIME字符集。

这包括用户的shell配置，特定的应用配置和X11配置。

20.3.4.1 设置本地化的方法

有两种方法来设置本地化，接下来都会描述。第一种(推荐)就是在登入分类里面指定环境变量。第二种方法是把环境变量加到shell的启动文件里面。

20.3.4.1.1 登入分类方法

这种方法允许把本地化名称和MIME字符集的环境变量赋给可能的shell，而不是加到每个特定shell的启动文件里面。用户级设置Level Setup 允许普通用户自己完成这个设置，而管理员级设置需要超级用户权限。

20.3.4.1.1.1 用户级设置

这有一个设置用户根目录文件`.login_conf`的小例子，它为上述两个变量设置了Latin-1编码。

```
me:\
:charset=ISO-8859-1:\
:lang=de_DE.ISO8859-1:
```

这是一个为`.login_conf`设置繁体中文的BIG-5编码的例子。应该设置下面的大部分变量，因为很多软件都没有为中文，日文和韩文设置正确的本地化变量。

```
#Users who do not wish to use monetary units or time formats
#of Taiwan can manually change each variable
me:\
:lang=zh_TW.Big5:\
:lc_all=zh_TW.Big5:\
:lc_collate=zh_TW.Big5:\
:lc_ctype=zh_TW.Big5:\
:lc_messages=zh_TW.Big5:\
:lc_monetary=zh_TW.Big5:\
:lc_numeric=zh_TW.Big5:\
:lc_time=zh_TW.Big5:\
:charset=big5:\
:xmodifiers="@im=xcin": #Setting the XIM Input Server
```

更多的信息参考管理员级设置和`login.conf(5)`

20.3.4.1.1.2 管理员级设置

检查用户的登入分类在/etc/login.conf里面是否设置了正确的语言。主要确定下面的几个设置:

```
language_name:accounts_title:\
:charset=MIME_charset:\
:lang=locale_name:\
:tc=default:
```

再次使用前面的Latin-1编码的例子:

```
german:German Users Accounts:\
:charset=ISO-8859-1:\
:lang=de_DE.ISO8859-1:\
:tc=default:
```

在修改用户的登入类型之前, 您应执行下面的命令

```
# cap_mkdb /etc/login.conf
```

以便使在/etc/login.conf 中新增的配置生效。

使用vipw(8) 改变登入类型。

使用vipw添加新用户, 看起来像下面这样:

```
user:password:1111:11:language:0:0:User Name:/home/user:/bin/sh
```

用adduser(8)改变登入类型。

用adduser添加新用户看起来像下面这样:

- 在/etc/adduser.conf里面设置defaultclass = 语言。应该记住, 您必须为使用其它语言的所有用户设置缺省类别。
- 每一次使用adduser(8)的时候, 一个特定语言的可选择性回答会像下面这样给出:
Enter login class: default []:
- 如果您打算给每一个用户使用另外一种语言, 您应该这样:

```
# adduser -class language
```

使用pw(8)改变登入类型。

如果您使用pw(8)来添加新用户, 应该这样使用:

```
# pw useradd user_name -L language
```

20.3.4.1.1.2 Shell启动文件方法

注意: 不推荐使用这种方法, 因为它需要给每一个可能的shell程序一个不同的启动文件。应该用登入分类方法来代替这种方法。

为了设置本地化名称和MIME字符集，只要在/etc/profile或/etc/csh.login启动文件里面设置这两个变量。下面我们使用德语做例子：

在/etc/profile里面：

```
LANG=de_DE.ISO8859-1; export LANG
MM_CHARSET=ISO-8859-1; export MM_CHARSET
```

或在/etc/csh.login里面：

```
setenv LANG de_DE.ISO8859-1
setenv MM_CHARSET ISO-8859-1
```

另外，您可以把上面的设置添加到/usr/share/skel/dot.profile（和前面的/etc/profile一样），或者/usr/share/skel/dot.login（和前面的/etc/csh.login一样）。

对于X11：

在\$HOME/.xinitrc里面：

```
LANG=de_DE.ISO8859-1; export LANG
```

或者：

```
setenv LANG de_DE.ISO8859-1
```

依赖您的shell(看上面)。

20.3.5 控制台设置

对于所有的简单C字符集，在/etc/rc.conf中用正在讨论的语言设置正确的控制台字符：

```
font8x16=font_name
font8x14=font_name
font8x8=font_name
```

这儿的font_name来自于/usr/share/syscons/fonts目录，不带.fnt后缀。

您还需要确定正确地为您的C字符集配置了keymap和screenmap，这一工作可以通过sysinstall（在FreeBSD 5.2之前的版本是/stand/sysinstall）来完成。。进入sysinstall之后，选择Configure，Console。此外，您也可以将下面的设置加入/etc/rc.conf：

```
scrnmap=screenmap_name
keymap=keymap_name
keychange="fkey_number sequence"
```

这儿的screenmap_name是来自/usr/share/syscons/scrnmaps目录，不带.scm后缀。一个带影射字体的屏幕布局通常被作为一个工作区，用来在VGA适配器字体矩阵上扩展8位到9位。如果屏幕字体是使用一个8位的排列，要移动这些字母离开这些区域。

如果您在/etc/rc.conf里面启用了moused daemon：

```
moused_enable="YES"
```


那么需要在下一段检查鼠标指针信息。

默认情况下，`syscons(4)`驱动程序的鼠标指针在字符集中占用0xd0-0xd3的范围。如果您的语言使用这个范围，您必须把指针范围移出这个范围。要在5.0以前的FreeBSD版本中启用工作区，需要在您的内核中添加下面这行：

```
options SC_MOUSE_CHAR=0x03
```

对于FreeBSD 4.4 和以后的版本，需要在`/etc/rc.conf` 中加入：

```
mousechar_start=3
```

这里，`keymap_name` 来自于`/usr/share/syscons/keymaps` 目录，但去掉了`.kbd` 后缀。如果不确定应该使用哪一个键盘布局，则可以使用`kbdmap(1)` 来测试，而无需反复重启。

通常，`keychange` 是设定功能键时，匹配选定的终端类型来说是必需的，因为功能键序列无法在键盘布局中定义。

此外您还应该检查并确认在`/etc/ttys` 中已经为所有的`tttyv*` 项配置了正确的终端类型。目前，相关的默认定义是：

字符集设置	终端类型
ISO8859-1 or ISO8859-15	cons25l1
ISO8859-2	cons25l2
ISO8859-7	cons25l7
KOI8-R	cons25r
KOI8-U	cons25u
CP437 (VGA default)	cons25
US-ASCII	cons25w

对于多字节字符语言，可以在您的`/usr/ports/language` 目录中使用正确的FreeBSD port。一些port以控制台出现，而系统把它作为串行`vtty`终端，因此，必须为X11 和伪串行控制台准备足够的`vtty`终端。下面是在控制台中使用其他语言的应用程序的部分列表：

语言	特定区域
Traditional Chinese (BIG-5)	chinese/big5con
Japanese	japanese/kon2-16dot or japanese/mule-freewnn
Korean	korean/han

20.3.6 X11设置

虽然X11不是FreeBSD计划的一部分，但我们已经为FreeBSD用户包含了一些信息。具体细节可以参考Xorg Web 站点 (<http://www.x.org/>) 或是您使用的X11 Server 的网站。

在`~/.Xresources`里面，您可以适当调整特定应用程序的I18N设置（如字体，菜单等）。

20.3.6.1 显示字体

安装Xorg 服务器(`x11-servers/xorg-server`) 或XFree86 服务

器(x11-servers/XFree86-4-Server)，然后安装对应语言的TrueType字体。请设置正确的地区信息，这将让您能够在菜单和其它地方看到所选择的语言。

20.3.6.2 输入非英语字符

X11输入方法(XIM)协议是所有X11客户端的一个新标准。所有将作为XIM客户端来写的X11应用程序从XIM输入服务器输入。不同的语言有几种XIM服务器可用。

20.3.7 打印机设置

一些简单的C字符集通常是用硬编码来编码进打印机的。更宽或多位的字符集需要特定的设置，我们推荐使用`apsfilter`。您也可以使用特定语言转换器把文档转换为PostScript或PDF格式。

20.3.8 内核和文件系统

FreeBSD的快速文件系统(FFS)是完全支持8-位字符的，因此它可以被用于任何简单的C字符集(参见`multibyte(3)`)，但在文件系统中不会保存字符集的名字；也就是说，它不加修改地保存8-位信息，而并不知道如何编码。正式说来，FFS目前还不支持任何形式的宽或多字节字符集。不过，某些宽或多字符集提供了独立的针对FFS的补丁来帮助启用关于它们的支持。目前这些要么是无法移植的，要么过于粗糙，因此我们不打算把它们加入到源代码中。请参考相关语言的Web站点，以了解关于这些补丁的进一步情况。

FreeBSD MS-DOS已经能够配置成用在MS-DOS上，Unicode字符集和可选的FreeBSD文件系统字符集的更多信息，请参考`mount_msdos(8)`手册页。

20.4 编译I18N程序

许多FreeBSD Ports已经支持I18N了。他们中的一些都用-I18N作标记。这些和其他很多程序已经内建I18N的支持，不需要考虑其他的事项了。

然而一些像MySQL这样的应用程序需要重新配置字符集，可在`Makefile`里面设置，或者直接把参数传递给`configure`。

20.5 本地化FreeBSD

20.5.1 俄语 (KOI8-R编码)

Originally contributed by Andrey Chernov.

关于KOI8-R编码的更多信息请查阅KOI8-R参考 (Russian Net Character Set) (<http://koi8.pp.ru/>)。

20.5.1.1 本地设置

把下面的行加入到您的`~/.login_conf`文件：

```
me:My Account:\
```

```
:charset=KOI8-R:\
:lang=ru_RU.KOI8-R:
```

参看前面的设置本地化的例子。

20.5.1.2 控制台设置

- 对于FreeBSD 5.0以前的版本，添加下面这行到内核配置文件：

```
options SC_MOUSE_CHAR=0x03
```

对于FreeBSD 4.4 和更高版本把下面一行加到/etc/rc.conf:

```
mousechar_start=3
```

- 在/etc/rc.conf里面使用如下设置：

```
keymap="ru.koi8-r"
scrnmap="koi8-r2cp866"
font8x16="cp866b-8x16"
font8x14="cp866-8x14"
font8x8="cp866-8x8"
```

- 对于/etc/ttys里面的ttyv*记录，要使用cons25r作为终端类型。

参看前面的设置控制台的例子。

20.5.1.3 打印机设置

既然绝大多数带俄语字符的打印机遵循CP866的标准，那么需要一个针对KOI8-R到CP866转换的特定输出过滤器。这样的一个过滤器默认的安装在于usr/libexec/lpr/ru/koi2alt。一个支持俄语的打印机的/etc/printcap记录看起来是这样的：

```
lp|Russian local line printer:\
:sh:of=/usr/libexec/lpr/ru/koi2alt:\
:lp=/dev/lpt0:sd=/var/spool/output/lpd:lf=/var/log/lpd-errs:
```

更多信息参考printcap(5)手册页。

20.5.1.4 MS-DOS文件系统和俄语文件名

下面的例子是在挂上MS-DOS 文件系统后，启用对俄语文件名支持的fstab(5)记录：

```
/dev/ad0s2      /dos/c  msdos  rw,-Wkoi2dos,-Lru_RU.KOI8-R 0 0
```

选项-L 用于选择地区名称，而-W 则用于设置字符转换表。要使用-W 选项，则一定要首先挂接/usr，然后再挂接MS-DOS 分区，因为转换表是放在/usr/libdata/msdosfs 的。要了解进一步的细节，请参考mount_msdos(8) 联机手册。

20.5.1.5 X11设置

1. 首先请进行前面介绍的非-X 的本地化设置。
2. 如果您正使用**Xorg**，请安装**x11-fonts/xorg-fonts-cyrillic package**。

检查您/etc/X11/xorg.conf 文件中的"Files" 小节。下面的行，应加到任何其它FontPath 项之前：

```
FontPath "/usr/X11R6/lib/X11/fonts/cyrillic/misc"
FontPath "/usr/X11R6/lib/X11/fonts/cyrillic/75dpi"
FontPath "/usr/X11R6/lib/X11/fonts/cyrillic/100dpi"
```

如果您使用一个高分辨率的显示模式，可以交换75 dpi 和100 dpi行。

3. 要激活俄语键盘，需要在xorg.conf 文件的"Keyboard" 小节中加入下列内容：

```
Option "XkbLayout" "us,ru"
Option "XkbOptions" "grp:toggle"
```

要确信XkbDisable 已经关闭(注释掉)了。

RUS/LAT的切换用**CapsLock**。老的**CapsLock**功能可以通过**Shift+CapsLock** 来模拟（只有在LAT模式的时候）。

对于grp:caps_toggle 而言，RUS/LAT 开关将作为**CapsLock** 使用。旧的**CapsLock** 功能仍可通过**Shift+CapsLock** (只对LAT 模式有效)。对于grp:toggle 而言RUS/LAT 开关则是**Right Alt**。由于不明原因，grp:caps_toggle 在**Xorg** 中无法使用。

如果您的键盘上有“Windows” 键，但发现RUS 模式下，某些非字母键映射不正常，则应在您的xorg.conf 文件中加入下面这行：

```
Option "XkbVariant" ",winkeys"
```

注意：俄语的XKB 键盘可能并不为某些不具备本地化功能的应用程序所支持。

注意：本地化程序最低限度应在程序启动时调用XtSetLanguageProc (NULL, NULL, NULL); 函数。

参见 KOI8-R for X Window (<http://koi8.pp.ru/xwin.html>) 以获得关于对X11 应用进行本地化的指导。

20.5.2 设置繁体中文

FreeBSD-Taiwan计划有一个使用很多中文ports的中文化指南在<http://netlab.cse.yzu.edu.tw/~statue/freebsd/zh-tut/>。目前，FreeBSD 中文化指南 的维护人员是沈俊兴<statue@freebsd.sinica.edu.tw>。

沈俊兴<statue@freebsd.sinica.edu.tw> 利用FreeBSD-Taiwan 的zh-L10N-tut建立了 Chinese FreeBSD Collection (CFC) (<http://netlab.cse.yzu.edu.tw/~statue/cfc/>)。相关的packages 和脚本等可以在<ftp://freebsd.csie.nctu.edu.tw/pub/taiwan/CFC/> 找到。

20.5.3 德语本地化（适合所有的ISO 8859-1语言）

Slaven Rezic <eserte at cs.tu-berlin.de> 写了一个在FreeBSD机器下如何使用日尔曼语言的德语指南。可以在<http://www.de.FreeBSD.org/de/umlaute/>下找到。

20.5.4 日语和韩语本地化

日语本地化请参考<http://www.jp.FreeBSD.org/>，韩语参考<http://www.kr.FreeBSD.org/>。

20.5.5 非英语的FreeBSD文档

一些FreeBSD的贡献者已经将部分FreeBSD文档翻译成了其他语言。可以通过主站 (<http://www.FreeBSD.org/index.html>) 或者 `/usr/share/doc` 查到。

第21章

最前沿

重新组织和部分更新，由Jim Mock. 原创：Jordan Hubbard、Poul-Henning Kamp、John Polstra 和Nik Clayton. 中文翻译：张雪平.

21.1 概述

FreeBSD 在两个发行版之间都有着持续的发展。对于喜欢冒险的人来说，有几种机制让您的系统与最新的发展保持同步。警告——冒险并不适合每一个人！本章将有助于您决定是紧跟最新发展还是坚持发行版。

读了本章后，您将了解到：

- FreeBSD-STABLE 和FreeBSD-CURRENT两个发展分支的不同点。
- 怎样使用CVSup，CVS或CTM保持您的系统更新。
- 如何使用make buildworld 等命令来重新编译和安装基本系统。

在读本章这前，您应该了解的：

- 正确设置网络连接(第27 章)。
- 知道怎样安装附加的第三方软件(第4 章)。

21.2 FreeBSD-CURRENT 和FreeBSD-STABLE 的对比

FreeBSD有两个开发分支：FreeBSD-CURRENT 和FreeBSD-STABLE。这部分将对每个做些说明，并且讲述您的系统如何与各自的树一同保持最新。先讨论FreeBSD-CURRENT，然后是FreeBSD-STABLE。

21.2.1 使用最新的FreeBSD CURRENT

我们再次强调，FreeBSD-CURRENT 是FreeBSD 开发的“最前沿”。FreeBSD-CURRENT 用户要有较高的技术能力，并且应该有能力自己解决困难的系统问题。如果您是个FreeBSD 新手，那么在安装之前最好三思。

21.2.1.1 FreeBSD-CURRENT 是什么？

FreeBSD-CURRENT 是FreeBSD 的发展前沿。包括了在下一个官方发行的软件中可能存在，也可能不存在的发展、实验性变化、传统机制。由于许多FreeBSD 开发者每天编译FreeBSD-CURRENT 源代码，有时这些代码会是不能编译的。虽然这些问题会很快解决，但不管是FreeBSD-CURRENT 引起的破坏还是急切的泛涵性(greatly desired functionality) 都将是您在您获取源代码的的时候值得注意的！

21.2.1.2 谁需要FreeBSD-CURRENT?

FreeBSD-CURRENT 适合下边三种主要兴趣团体:

1. FreeBSD 社区的成员: 积极工作在源码树的某部分的人和为保持“最新”为绝对需求的人。
2. FreeBSD 社区的成员: 为促使FreeBSD-CURRENT 保持尽可能的健全而愿花时间去解决问题的积极的测试员; 以及那些愿意提出关于FreeBSD 变化和总体方向的建设性建议并且提供补丁实现它们的人们。
3. 那些只是想关注或为了参考目的使用当前(current) 源码的人们(如, 为了阅读, 而不是执行)。这些人也偶尔做做注释或贡献代码。

21.2.1.3 FreeBSD-CURRENT 不是什么?

1. 追求最新功能, 您听说里面有一些很酷的新功能, 并希望成为您周围的人中第一个尝试它们的人。尽管您能够因此首先了解到最新的功能, 但这也意味着在出现新的bug 时您也首当其冲。
2. 修复错漏的快捷方式。任何FreeBSD-CURRENT 的既定版本在修复已知错漏的同时又可能会产生新的错漏。
3. 无所不在的“官方支持”。我们尽最大努力在3个“合法的” FreeBSD-CURRENT 组之一真诚给人们提供帮助, 但是我们没有时间提供技术支持。这并不是因为我们是那种不喜欢帮助人解困的无耻之徒(如果我们的是的话, 就不会制作FreeBSD 了)。我们不能每天简单地回复上百的消息, 而且我们继续发展FreeBSD! 在改善FreeBSD 和回复大量关于实验代码的问题之间如果要做个选择的话, 开发人员会选择前者。

21.2.1.4 使用FreeBSD-CURRENT

1. 加入freebsd-current (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-current>) 和cvs-all (<http://lists.FreeBSD.org/mailman/listinfo/cvs-all>) 列表。这个不仅仅是个好主意, 而且很重要。如果您不去freebsd-current (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-current>), 您就不会看到人们所做的关于系统当前状态的说明, 这样您就有可能在别人已经发现并解决了的一大堆问题面前难倒。更重要的是您会错过一些重要的公告---对于您的系统安全可能是至关重要的。

cvs-all (<http://lists.FreeBSD.org/mailman/listinfo/cvs-all>) 列表允许您看到每个变化的提交记录, 因为这些记录与其它相关信息是同步的。

要加入这些列表, 或其它可能的列表, 请访问<http://lists.FreeBSD.org/mailman/listinfo>, 并且点击您想订阅的列项。关于其它步骤的说明那里有提供。

2. 从FreeBSD 镜像站点获取源码。您有两种方式选择:
 - a. 与称作standard-supfile 的supfile 一起使用cvsup, 这个可以从/usr/share/examples/cvsup得到。这是最被推荐的方式, 因为它允许您一次获取整个集合, 以后就只取更改过的部分。许多人从cron 运行cvsup, 以保持他们的源码自动更新。您须要定制上边的supfile 样本, 并且配置cvsup 以适应您的环境。
 - b. 使用工具CTM。如果您的连接性能不太好(高价连接或只能通过电子邮件存取), CTM 是个选择。但这也颇有争议并且常常得到坏文件。因此很少使用它, 这也注定了不能长期用它来工作。对于使用9600 bps 或更快连接的人, 我们推荐使用CVSup。

3. 如果您获取源码是用于运行，而不只是看看，那么就获取**整个** FreeBSD-CURRENT，不要选部分。这样做的原因是源码的大部分都依赖于其他部分，要是您试着只编译其中一部分的话，保证您会陷入麻烦。

在编译FreeBSD-CURRENT之前，请仔细阅读/usr/src里的Makefile文件。尽管是部分的升级过程，您至少也要首先安装新的内核和重建系统。阅读FreeBSD-CURRENT邮件列表

(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-current>)邮件列表和/usr/src/UPDATING，会让您在其它循序渐进的过程中保持最新，这对于我们向下一个发行版转移是很有必要的。

4. 热心一点！如果您正运行FreeBSD-CURRENT，我们很想知道您关于它的一些想法，尤其是关于错漏修复或增进的建议。非常欢迎带有代码的建议！

21.2.2 使用最新的FreeBSD STABLE

21.2.2.1 FreeBSD-STABLE 是什么？

FreeBSD-STABLE 是我们的发展分支，我们的主要发行版就由此而来。这个分支会以不同速度变化，并且假定这些是第一次进入FreeBSD-CURRENT进行测试。然而，这**仍然**是个发展中的分支，这意味着在一定的時候，FreeBSD-STABLE 源码可能或不可能满足一些特殊的要求。它只不过是另一个工程发展途径，并不是终端用户的资源。

21.2.2.2 谁需要FreeBSD-STABLE？

如果您有兴趣追随FreeBSD的开发过程或为其做点贡献，尤其是和下一个“非计划”的FreeBSD发行版有关时，您应该考虑采用FreeBSD-STABLE。

尽管安全更新也会进入FreeBSD-STABLE分支，但您并不**必须**使用FreeBSD-STABLE来达到这样的目的。每一个FreeBSD的安全公告都会解释如何修复受到影响的发行版中的问题¹，而因为安全原因而去采用一个开发分支显然可能会同时引入一些不希望的修改。

尽管我们尽力确保FreeBSD-STABLE分支在任何时候都能够正确编译和运行，但没有人能够担保它在任何时候都总可以。此外，尽管代码在进入FreeBSD-STABLE之前都是在FreeBSD-CURRENT上完成开发，但使用FreeBSD-STABLE的人要比使用FreeBSD-CURRENT的更多。有证据显示，犄角旮旯里的各种问题有些时候仍然会由于在FreeBSD-CURRENT不那么明显而在FreeBSD-STABLE暴露出来。

基于这些原因，**不**推荐您盲目地追随FreeBSD-STABLE，并且，在粗略地测试过代码之前不要更新任何生产服务器到FreeBSD-STABLE也非常重要。

如果您没有用于完成这些工作的资源，我们推荐您使用最新的FreeBSD发行版，并使用发行版提供的二进制更新机制来在发行版之间完成迁移。

21.2.2.3 使用FreeBSD-STABLE

1. 加入freebsd-stable (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-stable>)列表。让您随时了解可能出现在FreeBSD-STABLE里的“build 依赖性”或其它需要特别注意的问题。当开发员正在考虑某些有争议的修复或更新时，他们就会在这个邮件列表里发表声明，给用户机会回应，看他们对于提出的变化是否还有什么问题。

cvs-all (<http://lists.FreeBSD.org/mailman/listinfo/cvs-all>) 列表允许您看到每一个变化的提交记录条目，这些变化是随着由可能的副作用引起的任何相关信息而产生的。

要加入这些列表或其他可用的，访问<http://lists.FreeBSD.org/mailman/listinfo> 并点击您希望订阅的列表。关于其它步骤的说明可以在那里看到。

2. 如果您正安装一个新系统，并希望它运行每月从FreeBSD-STABLE 编译的快照，请察看 Snapshots (<http://www.FreeBSD.org/snapshots/>) 网页以了解更多信息。另外，也可以从镜像站点 安装最新的FreeBSD-STABLE 发行版，并按照其中的说明将系统更新到最新的FreeBSD-STABLE 源代码。

如果您已经在运行较早的FreeBSD 版本，并希望通过源代码方式升级，则可以通过FreeBSD 镜像站点来完成。这可以通过两种方式进行：

- a. 与称作stable-supfile 的supfile 一起使用cvsup，这个可以从/usr/share/examples/cvsup 得到。这是最被推荐的方式，因为它允许您一次获取整个集合，以后就只取更改过的部分。许多人从cron 运行cvsup，以保持他们的源码自动更新。您须要定制上边的supfile 样本，并且配置cvsup 以适应您的环境。
 - b. 使用工具CTM。如果您的连接性能不太好(高价连接或只能通过电子邮件存取)，CTM 是个选择。但这也颇有争议并且常常得到坏文件。因此很少使用它，这也注定了不能长期用它来工作。对于使用9600 bps 或更快连接的人，我们推荐使用CVSup。
3. 本质上说，如果您需要快速存取源码并且不计较通信宽带的话，可以使用cvsup 或ftp。否则，就使用CTM。
 4. 在编译FreeBSD-STABLE 之前，请仔细阅读/usr/src 里的Makefile。您至少应该安装一个新的内核并重建系统，首先做为升级过程的一部分。阅读FreeBSD-STABLE 邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-stable>) 邮件列表和/usr/src/UPDATING，可能让您在它循序渐进的过程中保持更新，这在我们向下一发行版转移时是很有必要的。

21.3 同步您的源码

有许多方式通过互联网(或电子邮件)与FreeBSD 项目源码特定领域或所有领域保持更新，主要依赖于您的兴趣。我们提供的主要服务是匿名CVS、CVSup，和CTM。

警告：虽然只更新源码树中的部分是可能的，唯一被支持的更新过程是更新整个树、并且重编译用户区(如：在用户空间运行的所有程序，像/bin 和/sbin下边的)和内核源码。只更新源码树中的部分，或只有内核，或只有用户区(userland) 通常会出现错误。这些问题包括有编译错误、内核崩溃(kernel panics)、数据出错。

匿名CVS 和CVSup 使用下拉(pull) 模式来更新源代码。在CVSup 中，用户(或者cron 脚本) 会调用cvsup 程序，后者会同某一个cvsupd 服务进行交互，以更新您的文件。您接到的更新是更新时刻最新的，并且您只会收到那些需要的更新。您可以很容易地限制更新的范围，只更新那些您需要的文件。服务器端会根据您手头已有的文件即时地生成更新内容。匿名CVS 相对于CVSup 而言要简单一些，因为它只是对CVS 的一种扩展，让您可以从远程的CVS 代码库得到更新。CVSup 相对而言，要比匿名CVS 更有效率，然而后者却更容易使用。

另一种方法是CTM。这种方法并不能将您手头的代码与中央代码库中的版本进行比较，也不能下载它们。在主CTM 服务器上运行的脚本会每天执行多次，每次运行都能够自动地识别所有文件自上次运行以来

所发生的变化，如果发现有文件发生了变动，就会压缩、标上一个序列号，并进行便于使用电子邮件进行传送的编码操作(其中只包括可打印的ASCII 字符)。一旦接收到，这些“CTM deltas”就会被传送给ctm_rmail(1) 工具---可以自动进行解码、校验和应用这些变化到用户的复制的源码里。这个过程比CVSup更为有效，而且更少占用我们的服务器资源，因为它不仅仅采用下拉(pull) 模式，还采用上推(push) 模式。

当然，这样做也会带来一些不便。如果您不经意删除了您的压缩包的部分内容，CVSup 会检测到并为您重建破坏的部分。CTM 是不会这样做的，如果您删除了您的源码树中的某部分(并已不能恢复)，那么您就必须从破坏处(从最新的CVS “base delta”) 开始，使用CTM 或匿名CVS 进行重建，仅仅删除坏的数据并再同步。

21.4 重新编译“world”

只要您根据一定版本的FreeBSD (FreeBSD-STABLE、FreeBSD-CURRENT 等等)，已经同步了您本地的源码树，那么您就可以使用这些源码树来重建系统。

做好备份: 无需强调在行动之前 备份整个系统是多么的重要。尽管重新编译系统是(如果您按照文档的指示做的话) 一件很容易完成的工作，但出错也是在所难免的，另外，别人在源码里面引入的错误也可能造成系统无法引导。

请确信自己已经做过备份，并且在手边有恢复软盘或可以引导的光盘。您可能永远也不会用到它，但安全第一嘛！

订阅恰当的邮件列表: FreeBSD-STABLE 和FreeBSD-CURRENT 分支自然是发展中的。为FreeBSD 做贡献的都是人，偶尔也会犯错误。

有时这些错误没什么危害，只是引起您的系统生成新的诊断警告。有时是灾难性的，并导致您的系统不能惊动启动或破坏您的文件系统(甚至更糟)。

如果出现了类似的问题，贴一封“小心(heads up)” 帖到相关的邮件列表里，讲清问题的本质以及受影响的系统。在问题解决后，再贴封“解除(all clear)” 声明。

如果使用FreeBSD-STABLE 或FreeBSD-CURRENT 而又不阅读FreeBSD-STABLE 邮件列表(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-stable>) 和FreeBSD-CURRENT 邮件列表(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-current>) 各自的邮件列表，那么您是自找麻烦。

不要使用make world: 许多较早的文档推荐使用make world 来完成这项工作。这样做会跳过一些必要的步骤，因此只有在您知道自己在做什么的时候才可以这样做。几乎所有的情况下make world 都是不应该做的事情，您应该使用这里描述的方法。

21.4.1 更新系统的规范途径

要更新系统，就一定要首先查看/usr/src/UPDATING 文件，以了解buildworld 之前需要完成的步骤，然后使用下面的过程：

```
# make buildworld
# make buildkernel
# make installkernel
# reboot
```

注意: 有时, 可能需要额外地执行一次 `mergemaster -p` 才能够完成 `buildworld` 步骤。这些要求, 会在 `UPDATING` 中进行描述。一般而言, 您可以简单地跳过这一步, 只要进行的不是大跨度的 `FreeBSD` 版本升级。

在 `installkernel` 成功完成之后, 您需要引导到单用户模式(举例而言, 可以在加载器提示后输入 `boot -s`)。接下来执行:

```
# mergemaster -p
# make installworld
# mergemaster
# reboot
```

阅读进一步的说明: 前面所给出的, 只是帮助您开始工作的简要说明。要清楚地理解每一步, 特别是如果打算自行定制内核配置, 就应阅读下面的内容。

21.4.2 阅读 `/usr/src/UPDATING`

在您做其它事之前, 请阅读 `/usr/src/UPDATING` (或在您的源码里的等效的文件)。这个文件要包含有关于您可能遇到的问题的重要信息, 或指定了您可能使用到的命令的执行顺序。如果 `UPDATING` 与您这里读到相矛盾, 那就先依据 `UPDATING`。

重要: 正如先前所述, 阅读 `UPDATING` 并不能替代订阅正确的邮件列表。两都是互补的, 并不彼此排斥。

21.4.3 检查 `/etc/make.conf`

检查 `/usr/share/examples/etc/make.conf` (在 `FreeBSD 4.X` 中叫做 `/etc/defaults/make.conf`) 以及 `/etc/make.conf`。第一个文件包含了一些默认的定义—它们中的绝大多数都注释掉了。为了在重新编译系统时能够使用它们, 请把这些选项加入到 `/etc/make.conf`。请注意在 `/etc/make.conf` 中的任何设置同时也会影响每次运行 `make` 的结果, 因此设置一些适合自己系统的选项是一个好习惯。

一般的用户通常会从 `/usr/share/examples/etc/make.conf` (或者 `FreeBSD 4.X` 中的 `/etc/defaults/make.conf`) 复制 `CFLAGS` 和 `NO_PROFILE` (或者, 在 `FreeBSD 5.X` 和更早版本上, 是 `NOPROFILE`) 这样的设置到 `/etc/make.conf` 中并令它们生效。

请考虑其他的一些选项(例如 `COPTFLAGS`、`NOPORTDOCS` 等等), 看看是否合用。

21.4.4 更新 `/etc` 里边的文件

`/etc` 目录包含有除了您的系统启动时执行的脚本外大部分的系统配置信息。有些脚本随 `FreeBSD` 的版本而不同。

有些配置文件在天天运行的系统里也是要使用到的。尤其是 `/etc/group`。

偶尔, 作为安装过程的一部分, `make installworld` 会要求事先创建某些特定的用户或组。在进行升级时, 它们可能并不存在。这会给升级造成问题。有时, `make buildworld` 会检查它们是否已经存在。

最近就有个这样的例子，当时smmsp用户是被增加了的。当mtree(8)试着建立/var/spool/clientmqueue时，安装过程失败了。

解决办法是检查/usr/src/etc/group并把它与您的进行比较。如果在新文件里有而您的文件里没有的，就把它们复制过来。同样地，您把/etc/group里的任何这样的组进行更名---与/usr/src/etc/group中有相同GID，但不同名的那些。

自4.6-RELEASE开始，您可以通过-p选项以预建(pre-buildworld)模式运行mergemaster(8)。这样只是比较那些对于成功执行buildworld或installworld起关键作用的文件。在第一次时，如果早期的mergemaster版本不支持-p的话，就使用源码树中的新版本：

```
# cd /usr/src/usr.sbin/mergemaster
# ./mergemaster.sh -p
```

提示：如果您是个偏执狂(paranoid)，您可以检查您的系统看看哪个文件属于您已更名或删除了的那个组。

```
# find / -group GID -print
```

将显示所有GID组(可以是组名也可以是数字地组ID)所有的文件。

21.4.5 改为单用户模式

您可能想在单用户模式下编译系统。除了对更快处理事情显然有好处外，重装系统将接触许多重要的系统文件，包括所有标准系统二进制文件、库文件、包含(include)文件等等。在运行的系统里(尤其是同时系统里有激活的用户)更改这些文件是自寻烦恼。

另一种模式是在多用户模式下编译系统，然后转换到单用户模式下安装。如果您喜欢这种方式，只需在建立(build)完成后才执行下边的步骤。您推迟转换到单用户模式下直到您必须installkernel或installworld。

从运行的系统里，以超级用户方式执行：

```
# shutdown now
```

这样就会转换到单用户模式。

另外也可以，重启系统，在启动提示符处，输入-s标识。系统就会启动单用户。再在shell提示符处执行：

```
# fsck -p
# mount -u /
# mount -a -t ufs
# swapon -a
```

这会检查文件系统，重新装载/为读/写，参考/etc/fstab装载其它所有的UFS文件系统，然后打开交换(swapping)开关。

注意：如果您的CMOS时钟是设置为本地时间，而不是GMT(如果date(1)命令输出不能显示正确的时间和地区也有确有其事)，您可能也需要执行下边的命令：

```
# adjkerntz -i
```

这样可以确定您正确的本地时区设置——不这样做，您以后可能会碰到一些问题。

21.4.6 删除/usr/obj

随着重新构建系统的进行，编译结果会放到(默认情况下) /usr/obj 下。这些目录会映射到/usr/src。

通过删除这个目录，可以加速make buildworld的过程，并避免相互依赖关系等复杂的问题。

/usr/obj 中的某些文件可能设置了不可改标记(详情参见chflags(1))，需要首先去掉这些标志。

```
# cd /usr/obj
# chflags -R noschg *
# rm -rf *
```

21.4.7 重编译源码

21.4.7.1 保存输出

建议把执行make(1)后得到的输出存成一个文件。如果什么地方出了错，您就会有错误信息的备份。尽管这样不能帮您分析哪里出了错，但如果您把您的问题贴到某个邮件列表里就能帮助其他的人。

这样做最简单的办法是使用script(1)命令，同是带上参数指定存放输出的文件名。您应在重建系统之前立即这样做，然后在过程完成时输入exit。

```
# script /var/tmp/mw.out
Script started, output file is /var/tmp/mw.out
# make TARGET
... compile, compile, compile ...
# exit
Script done, ...
```

如果您这样做，就不要把文件存到/tmp里边。下次启动时，这个目录就会被清除掉。存放的最好地方是/var/tmp(如上个实例)或root的主目录。

21.4.7.2 编译基本系统

您必须在/usr/src目录里边：

```
# cd /usr/src
```

(当然，除非您的源码是在其它地方，真是这样的话更换成那个目录就行了)。

使用make(1)命令重建系统。这个命令会从Makefile(描述组成FreeBSD的程序应该怎样被重建，以什么样的顺序建立等等)里读取指令。

输入的一般命令格式如下：

```
# make -x -DVARIABLE target
```

这个例子里，-x是会传递给make(1)的一个选项。查看make(1)手册有您可用的选项例子。

`-DVARIBLE` 传递一个变量给Makefile。这些变量控制了Makefile的行为。这些同/etc/make.conf设置的变量一样，只是提供了另一种设置它们的方法。

```
# make -DNO_PROFILE target
```

是另一种指定不被建立(built)的先定库(profiled libraries)的方式，协同/etc/make.conf里的

```
NO_PROFILE= true # 避免编译性能分析库
```

一起使用。

目标(target)告诉make(1)什么该做。每个Makefile定义了一定数量不同的“目标(targets)”，然后您选择的目标就决定了什么会发生。

有些目标列在Makefile里的，但并不意味着您要执行。相反，建立过程(build process)利用它们把重建系统的一些必要的步骤分割成几个子步骤。

大部分的时间不需要向make(1)传递参数，因此您的命令看起来可能象这样：

```
# make target
```

从FreeBSD的2.2.5版本开始(实际上，是先在FreeBSD-CURRENT分支里第一次创建，然后在FreeBSD-STABLE的2.2.2和2.2.5两个版本间，进行了大翻新)，world target已经分成了两个部分：buildworld和installworld。从FreeBSD的5.3版开始，world target在默认时已经改为完全不动作，因为它事实上对于许多用户都具有相当的危险性。

正如名字所暗示的，buildworld在/usr/obj下边建立了一个全新的树，然后installworld就在当前的机器里安装这个树。

因为两个原因，这点很有用。首先，它允许您安全地完成建立(build)，而没有您运行的系统组成部分的影响。建立(build)是“自主的(self hosted)”。因为这样，您可以安全地在以多用户模式运行的机器里执行buildworld，而不用当心不良影响。但是依然推荐您在单用户模式时运行installworld。

第二，允许您使用NFS装载(NFS mounts)升级您网络里的多台计算机。如果您有三台A、B和C想进行升级，在A执行make buildworld和make installworld。然后从A NFS装载(NFS mount) B和C的/usr/src和/usr/obj，接着您就执行make installworld在B和C上安装建立(build)的结果。

尽管world target仍然存在，强烈建议您不要用它。

运行

```
# make buildworld
```

目前，我们提供了一个试验性的功能，可以在构建过程中为make指定-j参数，令其在构建过程中同时启动多个并发的进程。对于多CPU的机器而言，这样做有助于发挥其性能。不过，由于编译过程中的瓶颈主要是在IO而不是CPU上，因此它也会对单CPU的机器带来好处。

对典型的单CPU机器，可以使用：

```
# make -j4 buildworld
```

这样，make(1)会最多同时启动4个进程。从发到邮件列表中的经验看，这样做能带来最佳的性能。

如果您使用的机器有多颗CPU，并且配置了SMP的内核，也可以试试看6到10的数值，并观察是否能带来构建性能上的改善。

警告: 目前为止这仍然是试验性的功能，提交到源代码树上的变更，也随时可能导致这一功能不可用。如果您使用这个参数时发现无法构建world，在报告问题之前，应首先试试看去掉这个参数是否能修正问题。

当您通过源代码升级系统时，使用这一选项可能引致无法预测的后果。

21.4.7.3 耗时

有许多因素影响build时间，但通常一台带有128 MB 内存500 MHz 的Pentium III 要花费大约2 小时来build FreeBSD-STABLE 树，并且在整个过程中不带什么技巧或捷径。FreeBSD-CURRENT 树花的时间还要更长一点。

21.4.8 编译和安装新内核

要充分利用您的新系统，您应该重新编译内核。这是很有必要的，因为特定的内存结构已经发生了改变，像ps(1) 和top(1) 这样的程序会不能工作，除非内核同源码树的版本是一样的。

最简单、最安全的方式是build 并安装一个基于GENERIC 的内核。虽然GENERIC 可能没有适合您的系统的所有必要的设备，但它包括了启动您的系统到单用户模式所必需的内容。这是个不错的检测新系统是否工作正常的测试。在从GENERIC 启动、核实系统可以工作后，您就可以建立(build) 一个基于您的正常内核配置文件的新的内核了。

在新的FreeBSD 版本中，首先完成build world 然后再编译新内核非常重要。

注意: 如果您想建立一个定制内核，而且已经有了配置文件，只需象这样使用KERNCONF=MYKERNEL:

```
# cd /usr/src
# make buildkernel KERNCONF=MYKERNEL
# make installkernel KERNCONF=MYKERNEL
```

注意，如果您已把内核安全级别(kern.securelevel) 调高到了1 以上，而且还设置了noschg 或相似的标识到了您的内核二进制里边，您可能会发现转换到单用户模式里使用installkernel 是很有必要的。如果您没有设置它，则应该也能毫无问题地在多用户模式执行这两个命令。请参考init(8) 以了解更多关于内核安全级(kern.securelevel) 的信息；查看chflags(1) 了解更多关于不同文件标识的信息。

21.4.9 重启到单用户模式

您应该单用户模式测试新内核。照第21.4.5 节处的说明去做。

21.4.10 安装新的系统二进制(System Binaries)

如果您正建立一个足以使用make buildworld 的FreeBSD 版本，那么您现在应该使用installworld 来安装新的系统二进制。

执行

```
# cd /usr/src
# make installworld
```

注意: 如果在make buildworld 的命令行指定了变量, 您就必须在make installworld 命令行里指定同样的变量。对于其它的选项也不是必需的, 如, -j 就不能同installworld 一起使用。

举例, 您执行了:

```
# make -DNO_PROFILE buildworld
```

您就必须使用:

```
# make -DNO_PROFILE installworld
```

来安装结果, 否则就要试着安装先定(profiled) 的在make buildworld 阶段没有建立(built) 的二进制文件。

21.4.11 不是由make installworld 更新的更新文件

重新编译整个系统不会使用新的或改过的配置文件更新某些目录(尤其像/etc、/var 和/usr)

更新这些文件最简单的方式就是使用mergemaster(8), 手工去做也是可以的, 只要您愿意。不管您选择哪一种, 一定记得备份/etc 以防出错。

21.4.11.1 mergemaster

贡献者: Tom Rhodes.

mergemaster(8) 工具是个有针对性的脚本(Bourne script), 用于检测/etc 和/usr/src/etc 源码树里边的配置文件的不同点。这是保持系统配置文件同源码树里的一起更新的推荐方式。

在提示符里简单地输入mergemaster 就可以开始, 并观看它的开始过程。mergemaster 会建立一个临时的根(root)环境, 在/ 下, 放置各种系统配置文件。这些文件然后同当前安装到您系统里的进行比较。此时, 不同的文件会以diff(1) 格式进行显示, 使用+ 符号标识增加或修改的行, - 标识将完全删除的行或将被替换成新行。查看diff(1) 手册可以得到更多关于diff(1) 语法和文件不同点怎样显示的信息。

mergemaster(8) 会给您显示每个文件的不同处, 这样您就可以选择是删除新文件(相对临时文件), 是以未改状态安装临时文件, 是以当前安装的文件合并临时文件, 还是再看一次diff(1) 结果。

“选择删除临时文件” 将使mergemaster(8) 知道我们希望保留我们当前的文件不改, 并删除新的。并不推荐这个选择, 除非您没有更改当前文件的理由。任何时候在mergemaster(8) 提示符里输入?, 您就会得到帮助。如果选择跳过文件, 在其它文件处理完后再次进行。

“选择安装未修改临时文件” 将会使新文件替换当前的。对大部分未改的文件, 这是个最好的选择。

“选择合并文件” 将为您打开一个文本编辑器, 里边是两个文件的内容。您现在就可以一边合并它们, 一边在屏幕里查看, 同时从两者中选取部分生成最终文件。当两个文件一起比较时, l 键会选择左边的内容, r 会选择右边的。最终的输出是由两个部分组成的一个文件, 用它就可以安装了。这个选项通常用于用户修改了设置的文件。

“选择再次查看diff(1) 结果” 将会在提供给选择之前, 显示文件的不同处, 就象mergemaster(8) 所做的一样。

在mergemaster(8)完成了对系统文件的处理后，您会得到其它的选项。mergemaster(8)可能会问您是否需要重建密码文件，如果您的FreeBSD 版本超过5.0，还会问您是否想要执行MAKEDEV(8)，最后带上一个选项删除剩下的临时文件。

21.4.11.2 手动更新

如果想要手工更新，但不要只是从/usr/src/etc 把文件复制到/etc 就了事。有些文件是必须先“安装”的。这是因为/usr/src/etc 目录并不是想像的那样是/etc 目录的一个复制。事实上，有些文件是/etc 有的，而/usr/src/etc 里边没有。

如果您使用mergemaster(8) (作为推荐)，您可以向前跳到下一节。

手工做最简单的方式是安装这些文件到一个新的目录，完成后再来查找不同处。

备份您已有的/etc: 虽然，理论上，没有什么会自动访问这个目录，事情还是做稳操胜当一点。复制已有/etc 到一个安全的地方，如：

```
# cp -Rp /etc /etc.old
```

-R 完成递归复制(设者注：即可以复制目录以下的所有内容)，-p 保留文件的时间、所属等等。

您需要建立的一个虚目录(a dummy set of directories) 来安装新的/etc 和其它文件。/var/tmp/root 是个不错的选择，除此之外，还有一些子目录是需要的。

```
# mkdir /var/tmp/root
# cd /usr/src/etc
# make DESTDIR=/var/tmp/root distrib-dirs distribution
```

这样就建好了需要的目录结构，然后安装文件。在/var/tmp/root 下建立的大部分子目录是空的，而且要删除掉。最简单的方式是：

```
# cd /var/tmp/root
# find -d . -type d | xargs rmdir 2>/dev/null
```

这样会删除所有的空目录。(标准的错误信息被重定向到了/dev/null，以防止关于非空目录的警告。

/var/tmp/root 现在包含了应放在/ 下某个位置的所有文件。您现在必须仔细检查每一个文件，检测它们与您已有的文件有多大不同。

注意，有些已经安装在/var/tmp/root 下的文件有个“.”在开头。在写的时候，像这样唯一的文件是/var/tmp/root/ 和/var/tmp/root/root/ 里shell 启动文件，尽管可能有其它的(依赖于您什么时候读取这个)。确信使用ls -a 可以看到它们。

最简单的方式是使用diff(1) 去比较两个文件：

```
# diff /etc/shells /var/tmp/root/etc/shells
```

这会显示出/etc/shells 文件和新的/var/tmp/root/etc/shells 文件的不同处。用这些来决定是合并您已做的变化还是复制您的旧文件过来。

使用日戳(Time Stamp) 命名新的Root(根)目录(/var/tmp/root)，这样您可以轻松地比较两个版本的不同：频繁重建系统意味着必须频繁更新/etc，而这可能会有点烦琐。

在合并到/etc 的文件里，最新更改的您可以做个复制，由此加快这个(指更新)过程。下边就给出了一个怎样做的主意。

1. 像平常一样建立系统(Make the world)。当您想更新/etc 和其它目录里，给目标目录一个含有当前日期的名字。假如您是1998 年2 月14 日做的，您可以执行下边的：

```
# mkdir /var/tmp/root-19980214
# cd /usr/src/etc
# make DESTDIR=/var/tmp/root-19980214 \
    distrib-dirs distribution
```

2. 如上边列出的，从这个目录合并变化。

在您完成后，**不要** 删除/var/tmp/root-19980214 目录。

3. 在您下载了最新版的源码并改过后，执行第一步。这样将得到一个新的目录，可能叫做/var/tmp/root-19980221 (如果等了一周做的升级)。

4. 您现在能看到两个目录间的不同了---在隔周的时间里使用diff(1) 建立递归diff 产生的不同：

```
# cd /var/tmp
# diff -r root-19980214 root-19980221
```

一般情况下，这两种间的不同处比/var/tmp/root-19980221/etc 和/etc 之间的不同要小很多。因为不同点更小，也就更容易把这些变化移到您的/etc 目录里边。

5. 您现在可以删除早先的两个/var/tmp/root-* 目录：

```
# rm -rf /var/tmp/root-19980214
```

6. 每次您需要合并这些变化到/etc 里，就重复这个流程。

您可以使用date(1) 自动产生目录的名称：

```
# mkdir /var/tmp/root-$(date "+%Y%m%d")
```

21.4.12 更新/dev

注意：如果您正在运行FreeBSD 5.0 或更后的版本，您可以安全地跳过这部分。这些版本使用了devfs(5) 来透明地分配设备结点。

许多情况下，在有必要更新设备结点时，mergemaster(8) 工具就可以实现，并且可以自动地完成。这里的说明用于怎样手工更新设备结点。

考虑到安全，这里用的是多步流程。

1. 复制/var/tmp/root/dev/MAKEDEV 到/dev：

```
# cp /var/tmp/root/dev/MAKEDEV /dev
```

如果您使用mergemaster(8) 去更新/etc，那么您的MAKEDEV 脚本应该已经被更新过，虽然它不会影响检查(使用diff(1))，必要时手工复制一下。

2. 现在，给当前的/dev 做个快照。照的时候一定要注意每个文件名的许可(permissions)、所属(ownerships)、主从数字(major and minor numbers)，不必包括戳(time stamps)。最简单的方式是使用awk(1) 提取信息：

```
# cd /dev
# ls -l | awk '{print $1, $2, $3, $4, $5, $6, $NF}' > /var/tmp/dev.out
```

3. 重做设备结点：

```
# sh MAKEDEV all
```

4. 这时，把这个目录的另一个快照输出到/var/tmp/dev2.out。现在检查这两个文件，查找任何您没建立的设备结点。就该不会很多，但是保险一点总是好的。

```
# diff /var/tmp/dev.out /var/tmp/dev2.out
```

您可能注意到磁盘分区(disk slice) 的差别，它会像：

```
# sh MAKEDEV sd0s1
```

那样的命令重新建立分区入口(slice entries)。您的具体情况可能不同。

21.4.13 更新/stand

注意：这一步应被看作最后的扫尾工作。您可以安全地跳过这一步。如果正在使用的是FreeBSD 5.2 或更新的版本，/rescue 目录会为用户自动更新，其内容是在make installworld 过程中所生成的静态联编的可执行程序，这就不需要更新/stand (在FreeBSD 6.0 和更新版本中不再存在) 了。

为了完成，您可能想额外地更新/stand 里的文件。这些文件由链接到/stand/sysinstall 的二进制文件硬链接组成。这个文件要静态链接，以便没有其它文件系统时(尤其是/usr) 被装载时也能工作。

```
# cd /usr/src/release/sysinstall
# make all install
```

21.4.14 重启

现在完成了。在您检查所有内容都放置正确后，您可以重启系统了。只是简单的shutdown(8) 可以这样做：

```
# shutdown -r now
```

21.4.15 结束

恭喜！您现在成功升级了您的FreeBSD 系统。

如果还有轻微的错误，可以轻易地重建系统的选定部分。例如，在部分升级或合并/etc 时，您不小心删除了/etc/magic，file(1) 命令就会停止工作。这种情况下，执行下边进行修复：

```
# cd /usr/src/usr.bin/file
# make all install
```

21.4.16 问题

1. 每个变化您都须要重建系统吗?

这个不好说，因为要看变化的情况。如，如果您刚运行了 **CVSup**，并得到下边更新的文件：

```
src/games/cribbage/instr.c
src/games/sail/pl_main.c
src/release/sysinstall/config.c
src/release/sysinstall/media.c
src/share/mk/bsd.port.mk
```

这就不必重建整个系统。您只需到相关的子目录里执行 **make all install**，仅此而已。但是，如果有重大变化，如 **src/lib/libc/stdlib**，那么您就要重建系统或至少静态链接的那些部分(除了您增加的部分都是静态链接的)。

在这天后，就是您的事了。要是说每两个星期重建一下系统的话，您可能会高兴。或者您可能只想重做改变过的部分，确信您能找出所有依赖关系。

当然，所有这些依赖于您想升级的频率，和您是否想跟踪 **FreeBSD-STABLE** 或 **FreeBSD-CURRENT**。

2. 我的编译失败，并伴随有许多11 (或其它的数字信息) 号错误。是怎么回事呀?

这个通常表示硬件错误。(重)建系统是个强压测试系统硬件的有效的方式，并且常常产生内存错误。这些正好表示它们自己做为编译器离奇地死于收到的奇怪信息。

一个确信的指示器是如果重新开始 **make**，并且整个过程中会死在不同的点上。

对于这种情况，您没有什么可做的，除了更换机器里的部件，看是哪一个坏了。

3. 我完成后可以删除 **/usr/obj** 吗?

简短地说，可以。

/usr/obj 包含了所有在编译阶段生成的目标文件。通常，在 **make buildworld** 过程中第一步之一就是删除这个目录重新开始。这种情况下，在您完成后，保留 **/usr/obj** 没有多大意义，还可释放一大堆磁盘空间(通常在340 MB 左右)。

只是，如果您清楚您在干什么，您可以让 **make buildworld** 跳过这一步。这会让后继的 **build** 执行得更快，因为大部分的源码都不必再进行编译了。这个的另一面就在于敏感的依赖问题可以潜在，并以奇怪的方式引起 **build** 的失败。这在 **FreeBSD** 邮件列表里经常引起沸腾，当有人抱怨他们 **build** 失败时，并没意识到这是因为自己是想抄近路(意思是说少了些必要的步骤)。

4. 中断的 **build** 可以被恢复吗?

依赖于您在您找到问题之前整个过程进行了多远。

一般而言(当然这并不是硬性规定)，**make buildworld** 的过程中将会首先构建新版的基本构建工具(例如 **gcc(1)**，以及 **make(1)**) 和系统库。随后会安装这些工具和库。这些新版本的工具和库在随后将被用于重新编译和连接它们本身。整个系统(现在包括了常规的用户程序，例如 **ls(1)** 或 **grep(1)**) 会同新版的系统文件一起被重新构建。

如果您正处于最后一个阶段，并且了解它(因为您已经看过了所保存的输出) 则可以(相当安全地) 做：

```
... 问题修复 ...
# cd /usr/src
# make -DNO_CLEAN all
```

注意: 在FreeBSD 5.X 和更早版本中, 应使用-DNOCLEAN 代替。

这样就不会取消先前的make buildworld 所做的工作。

在“make buildworld”的输出中看到如下信息:

```
-----
Building everything..
-----
```

出现在make buildworld 的输出中, 则这样做应该不会有什问题。

如果没有看到这样的信息, 或者您不确定, 则从头开始构建将是万无一失的做法。

5. 我怎样加快建立系统的速度?

- 以单用户模式运行
- 把/usr/src 和/usr/obj 目录放到不同磁盘里的独立文件系统里。如果可能, 这些磁盘在不同的磁盘控制器里。
- 更好的, 是把这些文件系统放置到多个使用ccd(4) (连接磁盘驱动器--concatenated disk driver)设备的磁盘里。
- 关掉profiling (在/etc/make.conf 里设置 “NO_PROFILE=true”)。您差不多用不了它。
- 在/etc/make.conf 里也为CFLAGS 设置上-O -pipe。最佳优化-O2 会更慢, 而且-O 和-O2 之间的优化差别基本上可以忽略。-pipe 让编译器使用管道而不用临时文件进行通信, 这样可以减少磁盘存取(以内存作为代价)。
- 传递-jn 选项给make(1) 以便并发运行多个进程。这样就不会考虑您的是否是单个或多个处理器机器。
- 存放/usr/src 的文件系统可以使用noatime 选项被装载(或再装载)。这样会防止文件系统记录文件的存取时间。您可能并不需要这些信息。

```
# mount -u -o noatime /usr/src
```

警告: 这个例子里假定/usr/src 是在它自己的文件系统里。如果不是(例如假设它是/usr 的部分), 那么您就需要那个文件系统装载点, 而不是/usr/src。

- 存放/usr/obj 的文件系统可以使用async 选项被装载(或被再装载)。这会引起异步写盘。换句话说, 写是立即完成了, 而数据要延迟几秒才会写到盘里。这就允许写到一堆, 如此产生戏剧性的性能提高。

警告: 记住, 这个选项会使您的文件系统更加脆弱。使用这个选项增大了这样一个机率: 要是电源断了, 在机器重启后, 文件系统将处在不可恢复状态。

如果在这个文件系统里`/usr/obj`是很关键的，这不是问题。如果您有其它有价值的数据在同一个文件系统，那么在您使用这个选项这前，确认备份一下。

```
# mount -u -o async /usr/obj
```

警告：同上，如果`/usr/obj`不在自己的文件系统里，使用相关装载点的名字把它从例子里边替换掉。

6. 如果出现了错误我该怎么办？

绝对确信您的环境没有先前`build`留下的残余。这点够简单。

```
# chflags -R noschg /usr/obj/usr
# rm -rf /usr/obj/usr
# cd /usr/src
# make cleandir
# make cleandir
```

不错，`make cleandir`真的要执行两次。

然后重新开始整个过程，使用`make buildworld`开始。

如果您还有问题，就把错误和`uname -a`的输出发送到FreeBSD 一般问题邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-questions>) 邮件列表。准备回答其它关于您的设置的问题！

21.5 跟踪多台机器

贡献者Mike Meyer.

如果您有多台机器想跟踪同样的源码树，那么让它们都下载源码并重建所有东西，看起有点浪费资源：磁盘空间、网络带宽以及CPU 周期。解决的办法是让一台机器处理大部分的工作，而其它的机器通过NFS 装载(`mount`) 这些工作。这部分列举了一种这样做的方法。

21.5.1 准备

首先，确定一批机器，运行的二进制代码是同一套---我们称作**建造套件(build set)**。每台机器可以有定制内核，但他们运行的是相同的用户区二进制文件(`userland binaries`)。从这批机器中选择一台机器做为**建造机器(build machine)**。这将是用于建造(`build`)系统和内核的机器。想像一下，它应该是一台快速的机器，有足够的空余的CPU 来执行`make buildworld`。您也想要选一台机器做为**测试机器(test machine)**，这个将用于软件的更新生成产品之前对他们进行测试。这个**必须** 是一台您能提供的平时也可使用的机器。它可以是“建造机器”，但没这个必要。

在这个“建造套件”里的所有机器需要从同一台机器、同一个点上装载`/usr/obj`和`/usr/src`。理想地，它们在“建造机器”上的两个不同的驱动器里，但是在那台机器上可以进行NFS 装载。如果您有多个“建造套件”，`/usr/src`应该在某个“建造机器”上，而在其它机器上进行NFS 装载。

最后，确认“建造套件”里所有机器上的`/etc/make.conf`与“建造机器”里的相同。这意味着“建造机器”必须建造部分基本系统用于“建造套件”里所有机器的安装。同样，每台“建造机器”要有它自己的内核名字，使用`/etc/make.conf`里的`KERNCONF`进行设置，并且每台“建造机器”应该把它们列在`KERNCONF`里，同时把自己的内核列在最前。“建造机器”的`/usr/src/sys/arch/conf`里一定要有每台机器的内核配置文件，如果它想建造它们的内核的话。

21.5.2 基本系统

既然所有的妥当了，就准备建造所有的东西。如第21.4.7.2节中描述的一样在“建造机器”上建造内核和系统，但是什么也不安装。在建造结束后，转到“测试机器”上，安装您刚建造的内核。如果这台机器通过NFS装载了`/usr/src`和`/usr/obj`，在您重启到单用户模式里，您需要启动网络然后装载他们。最简单的方式是启动到多用户模式下，然后执行`shutdown now`转到单用户模式。一旦进入，您就可以安装新的内核和系统，并执行`mergemaster`，就像平常一样。完成后，重启返回到一般多用户模式操作这台机器。

在您确信所有在“测试机器”里都工作正常后，就使用相同的过程在“建造套件”里的其它机器里安装新的软件。

21.5.3 Ports

类似的想法是使用`ports`树。第一个关键的步骤是从同一台机子里装载`/usr/ports`到“建造套件”里的所有机子。然后正确设置`/etc/make.conf`共享`distfiles`。您应把`DISTDIR`设置到一个共享的目录里，那里可以被任何一个`root`用户写入，并且是由您的NFS装载映射的。设置每一台机子的`WRKDIRPREFIX`到一个本地建造(build)目录。最后，如果您要建造和发布包(`packages`)，那么您应该设置`PACKAGES`到一个类似于`DISTDIR`的目录。

备注

1. 这也不总是正确。我们不可能永远支持FreeBSD的旧发行版，尽管我们会在发布之后支持他们数年之久。关于FreeBSD目前对于旧发行版的支持政策的完整描述，请参见<http://www.FreeBSD.org/security/>。

IV. 网络通讯

FreeBSD 是目前以高性能网络服务为目的而部署范围最广的操作系统之一。讨论这些话题的章节包括：

- 串口通讯
- PPP 和以太网上的PPP
- 电子邮件
- 运行网络服务
- 防火墙
- 其他高级网络话题

这些章节主要供您在需要时参考。不需要以特定的顺序来阅读它们，此外，您开始在网络中使用FreeBSD之前也不必把它们都读完。

第22章

串口通讯

22.1 概述

UNIX 一直都是支持串口通讯的。事实上，早期的UNIX 系统就是利用串行线来输入和输出数据的。那时常见的“终端”包括一个每秒10个字符的串行打印机和键盘，现在这些已经发生了很大的变化。这章将介绍一些利用FreeBSD 进行串行通讯的方法。

读完这章，您将了解到：

- 如何通过终端连接到您的FreeBSD系统。
- 如何使用modem拨号到远程主机。
- 如何允许远程用户通过modem登录到您的系统。
- 如何从串行控制台引导您的系统。

阅读这章之前，您应当了解：

- 如何配置和安装一个新的内核(第8 章)。
- 理解UNIX 的权限和进程(第3 章)。
- 准备您打算在FreeBSD 中使用的串口设备(modem 或多插口卡) 的技术参考手册。

22.2 介绍

22.2.1 术语

bps

每秒位——数据的传输速度

DTE

数据终端设备——如您的计算机

DCE

数据通讯设备——如您的modem

RS-232

用于硬件串行通讯的EIA标准

当讨论通讯数据速度的时候，这节不会使用术语“baud”。Baud指电气标准传输率，它已经使用了很长时间，而“bps” (bits per second) 才是正确使用的术语(至少它不会打扰那些爱争吵的家伙)。

22.2.2 线缆和端口

要将modem 或终端与您的FreeBSD 系统相连，您的计算机需要一个串口，以及用于连接串口设备所需的线缆。如果您比较熟悉硬件及所需要的电缆，则可以跳过这节。

22.2.2.1 线缆

串口线缆有许多不同的种类。最常见的两种类型是null-modem 线缆和标准(“直联”)RS-232 线缆。您的硬件说明书中会介绍应使用的线缆种类。

22.2.2.1.1 Null-modem 线缆

null-modem 电缆会直接传送某些信号，如“Signal Ground”(信号地)，但对其他信号进行交换。例如，“Transmitted Data”(数据发送)引脚是连到另一端“Received Data”(数据接收)引脚的。

也可以自行制作null-modem 电缆给终端使用(例如，为了品质的要求)。下面的表格展示了RS-232C 信号，以及DB-25 连接器上的引脚。注意，标准也要求一根直通引脚1 到引脚1 的**保护地(Protective Ground)**线，但这通常都被省掉。某些终端在只有引脚2、3 和7 的时候，就已经能够正常使用了，而其他一些，则需要下面例子中所展示的不同的配置。

表22-1. DB-25 to DB-25 Null-Modem Cable

信号	引脚#		引脚#	信号
SG	7	连接到	7	SG
TD	2	连接到	3	RD
RD	3	连接到	2	TD
RTS	4	连接到	5	CTS
CTS	5	连接到	4	RTS
DTR	20	连接到	6	DSR
DTR	20	连接到	8	DCD
DSR	6	连接到	20	DTR
DCD	8	连接到	20	DTR

这里还有两种目前比较流行的其他接线方式。

表22-2. DB-9 到DB-9 Null-Modem 电缆

信号	引脚#		引脚#	信号
RD	2	接到	3	TD
TD	3	接到	2	RD
DTR	4	接到	6	DSR
DTR	4	接到	1	DCD
SG	5	接到	5	SG
DSR	6	接到	4	DTR
DCD	1	接到	4	DTR
RTS	7	接到	8	CTS
CTS	8	接到	7	RTS

表22-3. DB-9 到DB-25 Null-Modem 电缆

信号	引脚#	引脚#	信号
RD	2	DB-9 到DB-25 Null-Modem 电缆	TD
TD	3	接到	RD
DTR	4	接到	DSR
DTR	4	接到	DCD
SG	5	接到	SG
DSR	6	接到	DTR
DCD	1	接到	DTR
RTS	7	接到	CTS
CTS	8	接到	RTS

注意: 当某一段连接器上的一个引脚需要连接到对端的一对引脚时，通常是将那一对引脚使用一短线连接，而使用长线接到另一端的那个引脚。

上面的设计似乎更为流行。在其他变种中(在**RS-232 Made Easy** 这本书中进行了详细介绍) 则是SG 接SG，TD 接RD、RTS 和CTS 接DCD、DTR 接DSR，反之亦然。

22.2.2.1.2 标准RS-232C 线缆

标准的串口电缆会直接传送所有RS-232C 信号。也就是说，一头的“Transmitted Data” 引脚，会直接接到另一头的“Transmitted Data” 引脚。这包括将调制解调器接到您的FreeBSD 系统上的那种电缆，同样也适用于某些型号的终端。

22.2.2.2 端口

串行端口是FreeBSD主机与终端传输数据的设备。这节描述了端口的种类和它们在FreeBSD 上是如何编址的。

22.2.2.2.1 端口的种类

有好几种串口端口。在采购或制作线缆之前，您应确认它能够适合您的终端以及FreeBSD 系统。

绝大多数终端都提供DB-25 端口。个人计算机，也包括运行FreeBSD 的PC 机，通常会有DB-25 或DB-9 口。如果您的PC 上有多插口串口卡，则可能有RJ-12 或RJ-45 口。

请参见您硬件的文档以了解所用接口的规格。此外，您也可以通过观察外观来了解所用的端口。

22.2.2.2.2 端口名称Port Names

在FreeBSD中，您可以通过/dev 目录中的一个记录来访问每个串行端口。有两种不同的记录：

- 呼入端口被命名为`/dev/ttydN`，这里`N`是端口号，从零开始。通常，您使用呼入端口作为终端。呼入端口要求数据线使用载波检测(DCD)信号来工作。
- 呼出端口被命名为`/dev/cuadN`。您通常不使用呼出端口作为终端，只使用modem。如果串行线或终端不支持载波检测数据传输，您可以使用呼出端口。

注意: 在FreeBSD 5.X 和更早版本中，呼出端口的名字是`/dev/cuaaN`。

如果您已经连接一个终端到第一个串行端口(在MS-DOS 上是COM1)，则可以使用`/dev/ttyd0` 来作为终端。如果它是在第二个串行端口(COM2)，那就是`/dev/ttyd1`，等等。

22.2.3 内核配置

FreeBSD默认支持4个串行端口。在MS-DOS下，这些是COM1，COM2，COM3，和COM4。FreeBSD当前支持“dumb”多插口串行接口卡，如BocaBoard 1008 和2016，与许多Digiboard 和Stallion Technologies 制造的智能多接口卡一样好。然而，默认的内核只会寻找标准的COM端口。

要看看您的内核是否支持您的串口，只要在内核启动时查看一下启动信息，或使用`/sbin/dmesg` 命令重新检测内核启动信息。特别的，寻找以`sio`字符启动的信息。

提示: 如果想只察看包含`sio` 一词的消息，可以使用下面的命令：

```
# /sbin/dmesg | grep 'sio'
```

例如，在一个带有4个串口的系统上，这些是串口特定的内核启动信息：

```
sio0 at 0x3f8-0x3ff irq 4 on isa
sio0: type 16550A
sio1 at 0x2f8-0x2ff irq 3 on isa
sio1: type 16550A
sio2 at 0x3e8-0x3ef irq 5 on isa
sio2: type 16550A
sio3 at 0x2e8-0x2ef irq 9 on isa
sio3: type 16550A
```

如果内核未能认出所有的串口，可能需要通过修改`/boot/device.hints` 文件来进行一些配置。此外，也可以注释或完全删除掉您没有的设备。

在FreeBSD 4.X 中，必须修改内核配置文件来达到这一目的。要了解关于配置内核的详细信息，请参见第8 章。相关的设备如下：

```
device sio0 at isa? port IO_COM1 irq 4
device sio1 at isa? port IO_COM2 irq 3
device sio2 at isa? port IO_COM3 irq 5
device sio3 at isa? port IO_COM4 irq 9
```

请参见sio(4) 联机手册来了解关于串口，以及多插口卡配置的进一步细节。如果您正使用一个在不同版本的FreeBSD 上的文件请务必小心，因为设备参数和语法发生了变化。

注意：这里端口IO_COM1 代替了0x3f8，端口IO_COM2 代替了0x2f8，端口IO_COM3 代替了0x3e8，端口IO_COM4 代替了0x2e8，这些都是各自端口相应的端口地址。中断4，3，5，9都是经常用的中断。也要注意有些正常的串行端口可能无法在一些ISA总线的PC上共享中断(多插口板卡有板载的电子设备，允许在板上所有16550A 的设备共享一个或两个中断请求)。

22.2.4 设备特殊文件

在内核中，大多数设备都是通过“设备特殊文件”来访问的，这些文件一般位于/dev 目录中。sio 是通过/dev/ttydN (呼入) 和/dev/cuadN (呼出) 设备来访问的。此外，FreeBSD 也提供了初始化设备(在FreeBSD 6.X 上是/dev/ttydN.init 以及/dev/cuadN.init，而在FreeBSD 5.X 和更早版本上则是/dev/ttyidN 和/dev/cuaiaN) 以及锁设备(在FreeBSD 6.X 上是/dev/ttydN.lock 和/dev/cuadN.lock，而在FreeBSD 5.X 和更早版本上则是/dev/ttyldN 和/dev/cualaN)。初始化设备用于在打开端口时初始化其通讯参数，例如使用RTS/CTS 信号进行流控制的调制解调器的crtscs。锁设备则用于在端口上提供一个锁标志，防止用户或程序改变特定的参数；请参见termios(4)、sio(4)，以及stty(1) 的联机手册，以了解关于终端配置、锁和初始化设备，以及配置终端参数的详细信息。

22.2.4.1 编译设备指定文件

注意：从FreeBSD 5.0 开始，devfs(5) 文件系统将根据需要创建设备节点。如果您在运行启用devfs 的FreeBSD 版本，您就可以跳过这一节。

一个在/dev 目录下的叫做MAKEDEV 的shell 脚本管理着设备指定文件。要使用MAKEDEV 来建立拨号设备指定文件，可以使用COM1: (port 0)，cd 进入/dev，然后执行命令MAKEDEV ttyd0。同样地，要建立拨号设备指定文件以使用COM2: (port 1)，可以执行MAKEDEV ttyd1。

MAKEDEV 不仅仅创建/dev/ttydN 设备指定文件，也创建/dev/cuaaN，/dev/cuaiaN，/dev/cualaN，/dev/ttyldN，以及/dev/ttyidN节点。

建立完新设备指定文件后，需要检查文件的权限来确定谁可以在这些文件上读写——您可能不想让普通的用户使用您的modem 吧。在/dev/cua*文件上的默认权限应该是足够了：

```
crw-rw----  1 uucp      dialer    28, 129 Feb 15 14:38 /dev/cuaa1
crw-rw----  1 uucp      dialer    28, 161 Feb 15 14:38 /dev/cuaia1
crw-rw----  1 uucp      dialer    28, 193 Feb 15 14:38 /dev/cuala1
```

这些许可允许用户uucp和在组dialer 上的用户使用呼出设备。

22.2.5 串行端口配置

ttydN (或cuadN) 设备是您将要打开的应用程序的一般设备。当进程打开某个设备时，它将有一个终端I/O 设置的默认配置。您可以在命令行看看这些设置：

```
# stty -a -f /dev/ttyd1
```

当您修改了这个设备的设置，这个设置会生效，除非设备被关闭。当它被重新打开时，它将回到默认设置。要修改默认设置，您可以打开和调整“初始状态”设备的设置。例如，要为ttyd5 打开CLOCAL 模式，8位通讯和默认的XON/XOFF 流控制，输入：

```
# stty -f /dev/ttyd5.init clocal cs8 ixon ixoff
```

串口设备的系统级初始化，是由/etc/rc.d/serial 来控制的。这个文件会影响串口设备的默认设置。

注意：在FreeBSD 4.X 中，串口设备的初始化，是在/etc/rc.serial 中控制的。

为了防止应用程序修改某些设置，应修改“lock state” (锁状态) 设备。例如，要把ttyd5 的速率锁定为57600 bps，输入：

```
# stty -f /dev/ttyd5.lock 57600
```

现在，一个打开ttyd5 和设法改变端口速度的应用程序将被固定在57600bit/s。很自然地，您需要确定初始状态，然后用root帐户锁定状态设备的写入功能。

很显然，您应该只让root 用户可以初始化或锁定设备的状态。

22.3 终端

Contributed by Sean Kelly.

当您在计算机控制台或是在一个连接的网络上时，终端提供了一个方便和低成本的访问FreeBSD 系统的方法。这节描述了如何在FreeBSD 上使用终端。

22.3.1 终端的用法和类型

早期的UNIX 系统没有控制台。人们通过将终端连接到计算机的串口来登录和使用程序。它很像用modem 和一些终端软件来拨号进入一个远程的系统，只能执行文本的工作。

今天的PC 已经可以使用高质量的图形了，但与今天的其他UNIX操作系统一样，建立一个登录会话的能力仍然存在。通过使用一个终端连接到一个没有使用的串口，您就能登录和运行任何文本程序或在X 视窗系统中运行一个xterm 窗口程序。

对于商业用户，您可以把任何终端连接到FreeBSD 系统，然后把它们放在员工的桌面上。对于家庭用户，则可以使用一台比较老的IBM PC 或Macintosh 运行一个终端连接到一台运行FreeBSD 的高性能机器上。

对于FreeBSD，有三种终端：

- 哑终端
- 充当终端的PC
- X 终端

下面一小节将描述每一种终端。

22.3.1.1 哑终端

哑终端需要专门的好几种硬件，让您通过串行线连接到计算机。它们被叫做“哑”是因为它们只能用来显示，发送和接收文本。您不能在它上面运行任何程序。

有好几百种哑终端，包括Digital Equipment Corporation 的VT-100和Wyse的WY-75。只有几种可以在FreeBSD上工作。一些高端的终端可以显示图形，但只有某些软件包可以使用这些高级特性。

哑终端被广泛用于那些不需要图形应用的工作中。

22.3.1.2 充当终端的PC

如果一个哑终端 有足够的力量来显示，发送和接收文本，那任何个人计算机都可以作为一个哑终端。您所需要的只是适当的线缆和一些终端模拟软件。

这样一个配置被广泛运用于家庭。例如，如果您的妻子忙于在您的FreeBSD 系统控制台上工作，您也可以从一台低档的个人计算机登录到FreeBSD 系统执行一些文本的工作。

22.3.1.3 X 终端

X终端是最复杂的终端系统。它们通常需要使用以太网来连接。它们能显示任何X应用程序。

我们介绍X终端只是为了感兴趣。然而，本章不会涉及X终端的安装，配置或使用。

22.3.2 配置

这节描述了您在一个终端上启用一个登录会话，需要在FreeBSD 系统上配置些什么。假设您已经配置好了内核来支持串行端口，您就可以连接了。

在第12章 中曾经提到，`init` 进程依赖于系统启动时所有的处理控制和初始化。通过`init` 来执行的一些任务将先读取`/etc/ttys`文件，然后在可用的终端上启用一个`getty` 进程。`getty` 进程可用来阅读一个登录名和启动`login`程序。

然而，要为您的FreeBSD系统配置终端，您需要以`root` 身份执行下面的步骤：

1. 如果它不在那儿，您需要为串行端口在`/dev`目录下添加一行记录到`/etc/ttys`。
2. 指定`/usr/libexec/getty` 在端口上运行，然后从`/etc/gettytab` 文件指定适当的`getty` 类型。
3. 指定默认的终端类型。
4. 设置端口为“on”。
5. 确定端口是否为“secure”。
6. 迫使`init` 重新读取`/etc/ttys`文件。

作为可选的步骤，您可以通过在`/etc/gettytab` 中建立一个记录，在第2步创建一个定制的`getty` 类型来使用。本章不会介绍如何做。您可以参考`gettytab(5)` 和`getty(8)` 的联机手册了解更多信息。

22.3.2.1 添加一个记录到/etc/ttys

/etc/ttys文件列出了您FreeBSD系统上允许登录的所有端口。例如，第一个虚拟控制台ttyv0在这个文件中有一个记录。您可以使用这个记录登录进控制台。这个文件也包含其他虚拟控制台的记录，串口，和伪tty终端。对于一个硬连线的终端，只要列出串行端口的/dev记录而不需要/dev部分(例如，/dev/ttyv0可以被列为ttyv0)。

默认的FreeBSD安装包括一个支持最初四个串口ttyd0到ttyd3的/etc/ttys文件。如果您从那些端口中某一个使用终端，您不需要添加另一个记录。

例22-1. 在/etc/ttys中增加终端记录

假设我们连接两个终端给系统：一个Wyse-50和一个老的运行Procomm终端软件模拟一个VT-100终端的286IBM PC。在/etc/ttys文件中的相应的记录是这样的：

```
ttyd1① "/usr/libexec/getty std.38400"② wy50③ on④ insecure⑤
ttyd5 "/usr/libexec/getty std.19200" vt100 on insecure
```

- ① 第一部分指定了终端指定文件的名称，它可以在/dev中找到。
- ② 第二部分是在这行执行的命令，通常是getty(8)。getty初始化然后打开一行，设置速度，用户名的命令和执行登录程序。

getty程序在它的命令行接收一个参数(可选)，getty类型。一个getty类型会在终端行描述一个特征，像波特率和奇偶校验。getty程序从/etc/gettytab文件读取这些特征。

文件/etc/gettytab包含了许多老的和新的终端行记录。在很多例子中，启动文本std的记录将用硬连线终端来工作。这些记录忽略了奇偶性。这是一个从110到115200 bit/s的std记录。当然，您可以添加您自己的记录到这个文件。gettytab的联机手册提供了更多的信息。

当在/etc/ttys中设置getty类型的时候，确信在终端上的通讯设置匹配。在我们的例子中，Wyse-50不使用奇偶性，用38400 bit/s来连接。286 PC不使用奇偶性，用19200bit/s来连接。

- ③ 第三部分是通常连接到那个tty行的终端类型。对于拨号端口，unknown或dialup通常被用在这个地方。对于硬连线的终端，终端类型不会改变，所以您可以从termcap数据库文件中放一个真正的终端类型。

在我们的例子中，Wyse-50使用真正的终端类型，而运行Procomm的286 PC将被设置成在VT-100上的模拟。

- ④ 如果端口被启用，可以指定第四个部分。在第二部分，把它放在这儿将执行初始化进程来启动程序getty。如果您在这部分拖延，将没有getty，在端口上因此就没有登录。
- ⑤ 最后部分被用来指定端口是否安全。标记一个安全的端口意味着您信任它允许用root帐户从那个端口登录。不安全的端口不允许root登录。在一个不安全的端口上，用户必须用无特权的帐户登录，然后使用su或一个相似的机制来获得超级用户的权限。

22.3.2.2 重新读取/etc/ttys来强制init

对/etc/ttys文件做一个必要的修改后，您必须发送一个SIGHUP信号给初始化进程来迫使它重新读取配置文件，例如：

```
# kill -HUP 1
```


注意: `init` 总是系统运行时的第一个进程，因此它总是PID 1。

如果能够正确设置，所有的线缆都是适当的，终端将可以启用了，然后一个`getty`进程将在每个终端运行，您将在您的终端上看到登录命令行。

22.3.3 您的连接可能出现的问题

即使您小心翼翼地注意细节，您仍然可能会在设置终端时出错。这有一个有关问题和解决办法的列表：

22.3.3.1 没有登录命令出现：

确定终端被嵌入和打开了。如果把一台个人计算机充当一个终端，确信终端模拟软件运行在正确的串口上。

确信线缆被稳固地连接在终端和FreeBSD计算机上。确信用了正确的电缆。

确定终端和FreeBSD的传输速度和奇偶设置已经一致了。如果您有一个图像显示终端，确信对比度已经调节好了。如果它是一个可打印的终端，确信纸张和墨水已经就绪了。

确定一个`getty`进程正在运行和服务终端。例如，可以用`ps`命令得到运行`getty`程序的列表，键入：

```
# ps -axww|grep getty
```

您将看到一个终端的记录。例如，下面的显示表明一个`getty`正在第二个串行端口`ttyd1`运行，正在`/etc/gettytab`中使用`std.38400`的记录：

```
22189  d1  Is+      0:00.03 /usr/libexec/getty std.38400 ttyd1
```

如果没有`getty`进程运行，确信您已经在`/etc/ttys`中启用了端口。在修改完`/etc/ttys`文件后，记得运行`kill -HUP 1`。

如果`getty`进程确实在运行，但终端上仍然没有显示出登录提示，或者虽然显示了单缺不允许您输入，您的终端或电缆可能不支持硬件握手。请尝试将`/etc/ttys`中的`std.38400`改为`3wire.38400`并一定能够记得在改完`/etc/ttys`之后`kill -HUP 1`。`3wire`记录和`std`类似，但忽略硬件握手。您可能需要在使用`3wire`时减少波特率或启用软件流控制以避免缓冲区溢出。

22.3.3.2 出现一个“垃圾”而不是一个登录命令行

确信终端和FreeBSD使用相同的bit/s传输率和奇偶校验设置。检查一下`getty`进程确信当前使用正确的`getty`类型。如果没有，编辑`/etc/ttys`然后运行`kill -HUP 1`。

22.3.3.3 当键入密码时，字符两个两个出现

将终端(或终端模拟软件)从“半双工”或“本地回显”换成“全双工”。

22.4 拨入服务

Contributed by Guy Helmer. Additions by Sean Kelly.

为拨入服务配置FreeBSD系统与连接到终端是非常相似的，除非您正在使用modem来拨号而不是终端。

22.4.1 外置vs.内置modem

外置modem看起来很容易拨号。因为，外置modem可以通过储存在非易失性的RAM中的参数来配置，它们通常提供指示器来显示重要的RS-232信号的状态。不停闪光的信号灯能给用户留下比较深刻的印象，而且指示器也可以用来查看modem是否正常地工作。

内置modem通常缺乏非易失性的RAM，所以对它们的配置可能会限制在通过DIP 开关来设置。如果您的内置modem有指示灯，您也很难看得到。

22.4.1.1 Modem和线缆

如果您使用一个外置的modem，那您将需要适当的电缆线。一个标准的串行线应当足够长以至普通的信号能够连接上：

表22-4. 信号名称

缩写	全名
RD	收到数据(Received Data)
TD	传出数据(Transmitted Data)
DTR	数据终端就绪(Data Terminal Ready)
DSR	数据集就绪(Data Set Ready)
DCD	数据载波检测(Data Carrier Detect) (RS-232 的收到线路信号检测器)
SG	信号地(Signal Ground)
RTS	要求发送数据(Request to Send)
CTS	允许对方发送数据(Clear to Send)

FreeBSD 对速度超过2400 bps 的情形需要通过RTS 和CTS 信号来完成流控制，通过CD 信号来检测呼叫响应和挂机，并通过DTR 信号来在会话结束时对调制解调器进行复位。某些电缆在连接时没有提供全部需要的信号，这会给您带来问题，例如在挂断时登录会话不消失，这就有可能是电缆的问题。

与其它类UNIX 操作系统类似，FreeBSD 使用硬件信号来检测呼叫响应，以及在挂断时挂断并复位调制解调器。FreeBSD 避免发送命令给调制解调器，或监视其状态。如果您熟悉通过调制解调器来连接基于PC 的BBS 系统，这可能看起来有点难用。

22.4.2 串口的考虑

FreeBSD支持基于NS8250，NS16450，NS16550 和NS16550A 的EIA RS-232C通讯接口。8250和16450设备有单字符缓冲。16550设备提供了一个16 个字符的缓冲，可以提高更多的系统性能。因为单字符缓冲设备比16 个字符的缓冲需要更多的系统资源来工作，所以基于16550A的接口卡可能更好。如果系统没有活动的串口，或有较大的负载，16 字符缓冲的卡对于低错误率的通讯来说更好。

22.4.3 快速预览

对于终端，`init` 会在每个配置串口上为每个拨入连接产生一个 `getty` 进程。例如，如果一个 `modem` 被附带在 `/dev/ttyd0` 中，用命令 `ps ax` 可以显示下面这些：

```
4850 ?? I      0:00.09 /usr/libexec/getty V19200 ttyd0
```

当用户拨上 `modem`，并使用它进行连接时，`CD` 线就会被 `modem` 认出。内核注意到载波信号已经被检测到，需要完成 `getty` 端口的打开。`getty` 发送一个登录：在指定的初始线速度上的命令行。`Getty` 会检查合法的字符是否被接收，在典型的配置中，如果发现“垃圾”，`getty` 就会设法调节线速度，直到它接收到合理的字符。

用户在键入他/她的登录名称后，`getty` 执行 `/usr/bin/login`，这会要求用户输入密码来完成登录，然后启动用户的 `shell`。

22.4.4 配置文件

如果希望允许拨入您的 `FreeBSD` 系统，在 `/etc` 目录中有三个系统配置文件需要您关注。其一是 `/etc/gettytab`，其中包含用于 `/usr/libexec/getty` 服务的配置信息。其二是 `/etc/ttys`，它的作用是告诉 `/sbin/init` 哪些 `tty` 设备上应该运行 `getty`。最后，关于端口的初始化命令，应放到 `/etc/rc.d/serial` 脚本中。

关于在 `UNIX` 上配置拨入调制解调器有两种主要的流派。一种是将本地计算机到调制解调器的 `RS-232` 接口配置为固定速率。这样做的好处是，远程用户总能立即见到系统的登录提示符，而其缺点则是，系统并不知道用户真实的数据速率是多少，因而，类似 `Emacs` 这样的程序，也就无法调整它们绘制屏幕的方式，以便为慢速连接改善响应时间。

另一种流派将调制解调器的 `RS-232` 接口速率配置为随远程用户的连接速率变化。例如，对 `V.32bis` (14.4 Kbps) 连接，调制解调器会让自己的 `RS-232` 接口以 19.2 Kbps 的速率运行，而 2400 bps 连接，则会使调制解调器的 `RS-232` 接口以 2400 bps 的速率运行。由于 `getty` 并不能识别具体的调制解调器的连接速率反馈信息，因此，`getty` 会以初始速度给出一个 `login:` 提示，并检查用户的响应字符。如果用户看到乱码，则他们应知道此时应按下 `Enter` 键，直到看到可以辨认的提示符为止。如果数据速率不匹配，则 `getty` 会将用户输入的任何信息均视为“乱码”，并尝试以下一种速率来再次给出 `login:` 提示符。这一过程可能需要令人作呕地重复下去，不过一般而言，用户只要敲一两下键盘就能看到正确的提示符了。显然，这种登录过程看起来不如前面所介绍的“锁定速率”方法那样简单明了，但使用低速连接的用户，却可以在运行全屏幕程序时得到更好的交互响应。

这一节将尽可能公平地介绍关于配置的信息，但更着力于介绍调制解调器速率随连接速率变化的配置方法。

22.4.4.1 /etc/gettytab

`/etc/gettytab` 是一个用来配置 `getty` 信息的 `termcap` 风格的文件。请看看 `gettytab` 的联机手册了解完整的文件格式和功能列表。

22.4.4.1.1 锁定速度的配置

如果您把您的 `modem` 的数据通讯率锁定在一个特殊的速度上，您不需要对 `/etc/gettytab` 文件作任何变化。

22.4.4.1.2 匹配速度的配置

您将需要在/etc/gettytab 中设置一个记录来告诉getty 您希望在modem 上使用的速度。如果您的modem 的速率是2400 bit/s, 则可以使用现有的D2400 的记录。

```
#
# Fast dialup terminals, 2400/1200/300 rotary (can start either way)
#
D2400|d2400|Fast-Dial-2400:\
        :nx=D1200:tc=2400-baud:
3|D1200|Fast-Dial-1200:\
        :nx=D300:tc=1200-baud:
5|D300|Fast-Dial-300:\
        :nx=D2400:tc=300-baud:
```

如果您有一个更高速度的modem, 必须在/etc/gettytab 中添加一个记录。下面是一个让您可以以最高19.2 Kbit/s 的用在14.4 Kbit/s的modem上的接口记录:

```
#
# Additions for a V.32bis Modem
#
um|V300|High Speed Modem at 300,8-bit:\
        :nx=V19200:tc=std.300:
un|V1200|High Speed Modem at 1200,8-bit:\
        :nx=V300:tc=std.1200:
uo|V2400|High Speed Modem at 2400,8-bit:\
        :nx=V1200:tc=std.2400:
up|V9600|High Speed Modem at 9600,8-bit:\
        :nx=V2400:tc=std.9600:
uq|V19200|High Speed Modem at 19200,8-bit:\
        :nx=V9600:tc=std.19200:
```

这样做的结果是8-数据位, 没有奇偶校验的连接。

上面使用19.2 Kbit/s的连接速度的例子, 也可以使用9600 bit/s (for V.32), 2400 bit/s, 1200 bit/s, 300 bit/s, 直到19.2 Kbit/s。通讯率的调节使用nx= (“next table”) 来实现。每条线使用一个tc= (“table continuation”) 的记录来加速对于一个特殊传输率的标准设置。

如果您有28.8 Kbit/s的modem, 或您想使用它的14.4Kbit/s 模式, 就需要使用一个更高的超过19.2 Kbit/s 的通讯速度的modem。这是一个启动57.6 Kbit/s 的gettytab 记录的例子:

```
#
# Additions for a V.32bis or V.34 Modem
# Starting at 57.6 Kbps
#
vm|VH300|Very High Speed Modem at 300,8-bit:\
        :nx=VH57600:tc=std.300:
vn|VH1200|Very High Speed Modem at 1200,8-bit:\
        :nx=VH300:tc=std.1200:
vo|VH2400|Very High Speed Modem at 2400,8-bit:\
        :nx=VH1200:tc=std.2400:
vp|VH9600|Very High Speed Modem at 9600,8-bit:\
        :nx=VH2400:tc=std.9600:
vq|VH57600|Very High Speed Modem at 57600,8-bit:\
```

```
:nx=VH9600:tc=std.57600:
```

如果您的CPU 速度较低，或系统的负荷很重，而且没有16550A的串行端口，您可能会在57.6 Kbit/s 上得到sio “silo” 错误。

22.4.4.2 /etc/ttys

/etc/ttys文件的配置在例22-1中介绍过。配置modem 是相似的，但我们必须指定一个不同的终端类型。锁定速度和匹配速度配置的通用格式是：

```
ttyd0 "/usr/libexec/getty xxx" dialup on
```

上面的第一条是这个记录的设备特定文件——ttyd0 表示/dev/ttyd0 是这个getty 将被监视的文件。第二条"/usr/libexec/getty xxx" 是将运行在设备上的进程init。第三条，dialup，是默认的终端类型。第四个参数，on，指出了线路是可操作的init。也可能会有第五个参数，secure，但它将只被用作拥有物理安全的终端(如系统终端)。

默认的终端类型可能依赖于本地参考。拨号是传统的默认终端类型，以至用户可以定制它们的登录脚本来注意终端什么时候拨号，和自动调节它们的终端类型。然而，作者发现它很容易在它的站点上指定vt102 作为默认的终端类型，因为用户刚才在它们的远程系统上使用的是VT102模拟器。

您对/etc/ttys作修改之后，您可以发送init 进程给一个HUP 信号来重读文件。您可以使用下面的命令来发送信号：

```
# kill -HUP 1
```

如果这是您的第一次设置系统，您可能要在发信号init 之前等一下，等到您的modem 正确地配置并连接好。

22.4.4.2.1 锁定速度的配置

对于一个锁定速度的配置，您的ttys 记录必须有一个为getty 提供固定速度的记录。对于一个速度被锁定在19.2kbit/s 的modem，ttys 记录是这样的：

```
ttyd0 "/usr/libexec/getty std.19200" dialup on
```

如果您的modem 被锁定在一个不同的数据速度，为std.speed 使用适当的速度来代替std.19200。确信您使用了一个在/etc/gettytab 中列出的正确的类型。

22.4.4.2.2 匹配速度的设置

在一个匹配速度的设置中，您的ttys 录需要参考在/etc/gettytab 适当的起始“auto-baud” 记录。例如，如果您为一个以19.2 Kbit/s 开始的匹配速度的modem 添加上面建议的记录，您的ttys 记录可能是这样的：

```
ttyd0 "/usr/libexec/getty V19200" dialup on
```

22.4.4.3 /etc/rc.d/serial

高速调制解调器，如使用V.32、V.32bis，以及V.34的那些，需要使用硬件(RTS/CTS)流控制。您可以在/etc/rc.d/serial中增加stty命令来在FreeBSD内核中，为调制解调器设置硬件流控制标志。

例如，在1号串口(COM2)拨入和拨出设备上配置termios标志crtstcs，可以通过在/etc/rc.d/serial增加下面的设置来实现：

```
# Serial port initial configuration
stty -f /dev/ttyd1.init crtstcs
stty -f /dev/cuad1.init crtstcs
```

22.4.5 Modem 设置

如果您有一个modem，它的参数能被存储在非易失性的RAM中，您将必须使用一个终端程序来设置参数。使用同样的通讯速度来连接modem作为初始速度getty将使用 and 配置modem的非易失性RAM来适应这些要求：

- 连接时宣告CD
- 操作时宣告DTR；DTR消失时挂断线路并复位调制解调器
- CTS 传输数据流控制
- 禁用XON/XOFF流控制
- RTS 接收数据流控制
- 宁静模式(无返回码)
- 无命令回显

请阅读您modem的文档找到您需要用什么命令和DIP接口设置。

例如，要在一个USR Robotics Sportster 14400的外置modem上设置上面的参数，可以用下面这些命令：

```
ATZ
AT&C1&D2&H1&I0&R2&W
```

您也可能想要在modem上寻找机会调节这个设置，例如它是否使用V.42bis和MNP5压缩。

外置modem也有一些用来设置的DIP开关，也许您可以使用这些设置作为一个例子：

- Switch 1: UP —— DTR Normal
- Switch 2: N/A (Verbal Result Codes/Numeric Result Codes)
- Switch 3: UP —— Suppress Result Codes
- Switch 4: DOWN —— No echo, offline commands
- Switch 5: UP —— Auto Answer
- Switch 6: UP —— Carrier Detect Normal
- Switch 7: UP —— Load NVRAM Defaults
- Switch 8: N/A (Smart Mode/Dumb Mode)

在拨号modem上的结果代码应该被禁用/抑制，以避免当getty在modem处于命令模式并回显输入时错误地给出login:提示时可能造成的问题。这样可能导致getty与modem之间产生更长的不必要交互。

22.4.5.1 锁定速度的配置

对于锁定速度的配置，您需要配置modem来获得一个不依赖于通讯率的稳定的modem到计算机的传输率。在一个USR Sportster 14400 外置modem上，这些命令将锁定modem到计算机的传输率：

```
ATZ
AT&B1&W
```

22.4.5.2 匹配速度的配置

对于一个变速的配置，您需要配置modem调节它的串行端口传输率匹配接收的传输率。在一个USR Sportster 14400 的外置modem上，这些命令将锁定modem的错误修正传输率适合命令要求的速度，但允许串行端口速度适应没有纠错的连接：

```
ATZ
AT&B2&W
```

22.4.5.3 检查modem的配置

大多数高速的modem提供了用来查看当前操作参数的命令。在USR Sportster 14400外置modem上，命令ATI5显示了存储在非易失性RAM中的设置。要看看正确的modem操作参数，可以使用命令ATZ然后是ATI4。

如果您有一个不同牌子的modem，检查modem的使用手册看看如何双重检查您的modem的配置参数。

22.4.6 问题解答

这儿是几个检查拨号modem的步骤。

22.4.6.1 检查FreeBSD系统

把您的modem连接到FreeBSD系统，启动系统，然后，如果您的modem有一个指示灯，当登录时看看modem的DTR指示灯是否亮：会在系统控制台出现命令行如果它亮，意味着FreeBSD已经在适当的通讯端口启动了一个getty进程，等待modem接收一个呼叫。

如果DTR指示灯不亮，通过控制台登录到FreeBSD系统，然后执行一个ps ax命令来看FreeBSD是否正在正确的端口运行getty进程。您将在进程显示中看到像这样的一行：

```
114 ?? I      0:00.10 /usr/libexec/getty V19200 ttyd0
115 ?? I      0:00.10 /usr/libexec/getty V19200 ttyd1
```

如果您看到是这样的：

```
114 d0 I      0:00.10 /usr/libexec/getty V19200 ttyd0
```

modem 不接收呼叫，这意味着getty 已经在通讯端口打开了。这可以指出线缆有问题或modem 错误配置，因为getty 无法打开通讯端口。

如果您没有看到任何getty 进程等待打开想要的ttydN 端口，在/etc/ttys 中双击您的记录看看那儿是否有错误。另外，检查日志文件/var/log/messages 看看是否有一些来自init 或getty 的问题日志。如果有任何信息，仔细检查配置文件/etc/ttys 和/etc/gettytab，还有相应的设备文件/dev/ttydN，是否有错误，丢失记录，或丢失了设备指定文件。

22.4.6.2 尝试接入Try Dialing In

设法拨入系统。确信使用8位，没有奇偶检验，在远程系统上的1阻止位。如果您不能立刻得到一个命令行，试试每隔一秒按一下Enter。如果您仍没有看到一个登录：设法发送一个BREAK。如果您正使用一个高速的modem 来拨号，请在锁定拨号modem 的接口速度后再试试。

如果您不能得到一个登录：prompt，再检查一下/etc/gettytab，重复检查：

- 在/etc/ttys 中指定的初始可用的名称与/etc/gettytab 的一个可用的相匹配。
- 每个nx= 记录与另一个gettytab 可用名称匹配。
- 每个tc= 记录与另一个gettytab可用名称相匹配。

如果您拨号但FreeBSD 系统上的modem 没有回应，确信modem 能回应电话。如果modem 看起来配置正确了，通过检查modem 的指示灯来确认DTR 线连接正确。

如果您做了好几次，它仍然无法工作，打断一会，等会再试试。如果还不能工作，也许您应该发一封电子邮件给FreeBSD 一般问题邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-questions>) 寻求帮助。

22.5 拨出设备

下面将让您的主机通过modem 连接到另一台计算机上。这只要适当地建立一个终端作为远程主机就可以。

这可以用来登录进一个BBS。

如果您用PPP 有问题，那这种连接可以用来从Internet 上下载一个文件。如果您必须FTP 一些东西，而PPP 断了，使用终端会话来FTP 它们。然后使用zmodem 来把它们传输到您的机器上。

22.5.1 我的Stock Hayes Modem不被支持，我该怎么办？

事实上，联机手册对于这个的描述已经过时了。一个通用的Hayes拨号已经内建其中。只要在您的/etc/remote 文件中使用at=hayes。

Hayes 驱动不够“聪明” 只能认出一些比较新的modem 的高级特性——如BUSY、NO DIALTONE，或CONNECT 115200 的信息将被搞乱。当您使用的时候，您必须把这些信息关掉。(通过ATX0&W)。

另外，拨号的延迟是60 秒。您的modem 可能使用另外的时间或提示认为有其他的通讯问题。试试ATS7=45&W。

注意: 注意: 实际上tip 不支持所有的Hayes modems。解决方法是编辑/usr/src/usr.bin/tip/tip 目录中的tipconf.h 文件。很明显, 您需要它的源代码才能这样做。

把行#define HAYES 0 改为#define HAYES 1。然后make 并make install就可以了。

22.5.2 我如何输入这些AT 命令?

在/etc/remote 文件中增加一个“direct”项。举例而言, 如果您的调制解调器挂在第一个串口, 即/dev/cuad0 上, 则应添加下面这行:

```
cuad0:dv=/dev/cuad0:br#19200:pa=none
```

此处应使用您的modem 所支持的最高br bps 速率。接下来, 输入tip cuad0 就可以连到modem 上了。

此外, 也可以root 身份执行cu 命令:

```
# cu -lline -sspeed
```

line 是串口(例如/dev/cuad0) 而speed 则是速率(如57600)。当您输入完AT 之后, 按~. 即可退出。

22.5.3 现在pn @标记不能工作?

在电话号码中的@ 标记告诉计算机在/etc/phones 文件中查找一个电话号码。但@ 标记也是一个在像/etc/remote 这样的可用文件中的特殊字符。用一个反斜线符号退出:

```
pn=\\@
```

22.5.4 我如何在命令行拨电话号码?

在您的/etc/remote 文件中通常放着一个叫做“generic”的记录。例如:

```
tip115200|Dial any phone number at 115200 bps:\
      :dv=/dev/cuad0:br#115200:at=hayes:pa=none:du:
tip57600|Dial any phone number at 57600 bps:\
      :dv=/dev/cuad0:br#57600:at=hayes:pa=none:du:
```

然后, 可以执行:

```
# tip -115200 5551234
```

如果您更喜欢cu而不是tip, 使用一个通用的cu记录:

```
cu115200|Use cu to dial any number at 115200bps:\
      :dv=/dev/cuad1:br#57600:at=hayes:pa=none:du:
```

然后键入:

```
# cu 5551234 -s 115200
```

22.5.5 这么做时是否每次都需要重新输入bps 速率?

添加一项`tip1200` 或`cu1200`，并将bps 速率换成更合适的值。`tip` 的默认值是1200 bps，也就是为什么会有`tip1200` 这条记录的原因。虽然您并不需要使用1200 bps。

22.5.6 我通过一个终端服务器访问了很多主机。

除非每次都要等到您连接到主机然后键入`CONNECT <host>`，否则使用`tip` 的`cm` 功能。例如，在`/etc/remote` 中的这些记录：

```
pain|pain.deep13.com|Forrester's machine:\
      :cm=CONNECT pain\n:tc=deep13:
muffin|muffin.deep13.com|Frank's machine:\
      :cm=CONNECT muffin\n:tc=deep13:
deep13:Gizmonics Institute terminal server:\
      :dv=/dev/cuad2:br#38400:at=hayes:du:pa=none:pn=5551234:
```

将让您键入`tip pain` 或`tip muffin` 连接到主机`pain`或`muffin`，和`tip deep13` 连接到终端服务器。

22.5.7 tip能为每个站点试用多个线路吗?

经常有一个问题，一个大学有几个modem线路，几千个学生设法使用它们。

在`/etc/remote` 中为您的大学添加一个记录，然后为`pn` 功能使用`@` 标记：

```
big-university:\
      :pn=@:tc=dialout
dialout:\
      :dv=/dev/cuad3:br#9600:at=courier:du:pa=none:
```

接着，在`/etc/phones` 中列出大学的电话号码：

```
big-university 5551111
big-university 5551112
big-university 5551113
big-university 5551114
```

`tip` 将按顺序试用每一个，然后就停止。如果想继续测试，隔一段时间再运行`tip`。

22.5.8 为什么我必须键入Ctrl+P 两次才能发出Ctrl+P 一次?

Ctrl+P是默认的“强制”字符，被用来告诉`tip`下一个字符是文字的数据。您可以用`~s`给任何其他的字符设置强制字符，这意思是“设置一个变量”。

在新的一行键入`~sforce=single-char`。`single-char` 是任何简单的字符。如果您遗漏了`single-char`，那强制字符就是空字符，这可以键入`Ctrl+2` 或`Ctrl+Space`来完成。更好的`single-char` 是`Shift+Ctrl+6`，这只用在一些终端服务器上。

通过在您的`$HOME/.tiprc` 文件中指定下面这行，就可以得到您想要的任何强制字符：

```
force=<single-char>
```

22.5.9 突然我键入的每一样东西都变成了大写??

您一定是键入了**Ctrl+A**，即tip的“raise character”，会临时地指定成坏掉的caps-lock键。使用上面的~s来合理地设置各种raisechar。事实上，如果您不想使用这些特性的话，您可以用同样的方法设置强制字符。

这儿有一个很好的示例.tiprc文件，对Emacs用户来说，需要经常按**Ctrl+2**和**Ctrl+A**：

```
force=^^
raisechar=^^
```

The ^^ is **Shift+Ctrl+6**.

22.5.10 如何用tip做文件传输?

如果您正在与另一台UNIX系统对话，您可以用~p(put)和~t(take)发送和接收文件。这些命令可以在远程系统上运行cat和echo来接收和发送文件。语法是这样的：

```
~p local-file [remote-file]
```

```
~t remote-file [local-file]
```

由于没有错误校验，所以您需要使用其他协议，如zmodem。

22.5.11 我如何用tip运行zmodem?

要接收这些文件，可以在远程终端启动发送程序。然后，键入~c rz在本地开始接收它们。要发送文件，可以在远程终端启动接收程序。然后，键入~C sz files把它们发送到远程系统。

22.6 设置串行控制台

Contributed by Kazutaka YOKOTA. Based on a document by Bill Paul.

22.6.1 介绍

FreeBSD可以通过一个串口只使用一个哑(dumb)终端就可以启动一个系统。这样一种配置只有两种人能用：希望在机器上安装FreeBSD的系统管理员，他没有键盘或显示器，还有就是要调试内核或设备驱动程序的开发人员。

就象第12章描述的，FreeBSD采用一个三步的启动过程。最先两步储存在FreeBSD启动磁盘的启动slice的启动代码块中。引导块然后就被加载，接着运行第三步启动引导器(/boot/loader)。

为了设置串行控制台，您必须配置启动代码块，启动引导器代码和内核。

22.6.2 串行控制台的配置，简明版

这一节假定您使用默认的配置，只希望迅速地获得关于配置串口控制台的概览。

1. 使用串口电缆连接COM1 和控制终端。
2. 要在串口控制台上显示所有的引导信息，需要以超级用户的身份执行下面的命令：

```
# echo 'console="comconsole"' >> /boot/loader.conf
```
3. 编辑/etc/ttys 并把ttyd0 的off 改为on，dialup 改为vt100。否则通过串行控制台上将不会提示输入口令，从而导致潜在的安全漏洞。
4. 重新启动并观察是否生效。

如果需要不同的配置，更进一步的配置讨论可以在第22.6.3 节 找到。

22.6.3 串行控制台的设置S

1. 准备一个串行线缆。

您需要使用一个null-modem 的线缆或标准的串行线和一个null-modem 适配器。请参考第22.2.2 节 中有关串行线的讨论。

2. 拔掉键盘。

绝大多数的PC在开机检测的时候会检测到键盘，如果没有检测到键盘，则会出现错误。一些机器会提示缺少键盘，就不会继续引导系统。

如果您的计算机出现错误，但仍能继续启动，您可以不必理它。

如果您的计算机没有键盘拒绝启动，那您需要配置BIOS 来避免它。请参考您的主板的使用说明了解更多细节。

提示: 在BIOS 中将键盘设为“Not installed” (未安装)。现在您仍然无法使用键盘。这样做只是告诉BIOS 在启动时不要探测键盘。您的BIOS 不应抱怨键盘不存在。即使这一标志设置为“Not installed” 时，只要把键盘插上，它就仍可使用。

注意: 如果系统有PS/2 鼠标，如果幸运的话，您也可以象键盘一样把它拔下来，这是因为PS/2 鼠标与键盘的一些硬件是共享的，您的鼠标插上去，系统会认为键盘仍在那儿。

3. 插一个哑(dumb) 终端到COM1: (sio0) 。

如果您没有哑终端，可以使用一个比较老的带有一个modem 程序的PC/XT机器，或在其他UNIX 机器上的串口。如果您没有COM1: (sio0)，去找一个。这时，您就不能只能选择COM1: 来启动系统。如果您已经在另一台设备上使用COM1，您必须临时删除那个设备，然后安装一个新的系统引导块和内核。

4. 确信您的内核配置文件已经为COM1: (sio0) 设置了适当的标记:

有关的标记是:

0x10

启用控制台支持。如果没有设置它，则其他的控制台标记都会被忽略。现在，绝大多数的设置都有控制台的支持。这个标记的第一个就是首选的。这个单独选项是不能确保串口适用于控制台的，设置下面的标记或加上下面描述的 **-h** 选项，和这个放在一起。

0x20

无论是否使用了下面将要讨论的 **-h** 选项，都强制这个单元作为控制台(除非使用了更高优先级的控制台)。标志 **0x20** 必须与 **0x10** 一起使用。

0x40

预留这个单元(配合 **0x10**) 并让它不能用于普通的使用。您不应在希望作为控制台的串口单元上设置这个标志。这一标志是为内核远程调试准备的。参见开发者手册 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/developers-handbook/index.html) 以了解关于远程调试更进一步的情况。

注意: 在 FreeBSD 4.0-CURRENT 和以后的版本中，标志 **0x40** 通常是不同的，有另一个标记可以来指定一个串口用于远程调试。

例如:

```
device sio0 at isa? port IO_COM1 flags 0x10 irq 4
```

看看 `sio(4)` 的联机手册了解更多信息。

如果标记没有被设置，您必须运行 `UserConfig` 或重新编译内核。

5. 在启动磁盘的 `a` 分区的根目录创建 `boot.config` 文件。

这个文件将指导引导块代码如何启动系统。为了激活串行控制台，您必须有一个或多个下面的选项如果您要多个选项，在同一行必须都包含它们:

-h

切换内部和串行控制台。您使用这个来交换控制台设备。例如，如果您从内部控制台启动，您可以使用 **-h** 来直接使用启动引导器和内核来使用串口作为它的控制台设备。另外，如果您从串口启动，您可以使用 **-h** 来告诉启动引导器和内核使用显示设备作为控制台。

-D

切换单一和双重控制台配置。在单一配置中，控制台将是本机的控制台(显示设备)或串口。在双重控制台配置中，显示设备和串口将同时成为控制台，无论 **-h** 的选项的情形。然而，双控制台配置只在引导块运行的过程中起作用。一旦启动引导器获得控制，由 **-h** 选项指定的控制台将成为唯一的控制台。

-P

在启动时，探测键盘。如果键盘找不到，**-D** 和 **-h** 选项会自动设置。

注意: 由于当前版本引导块的空间限制，**-P** 选项只能探测扩展的键盘。少于 **101** 键的键盘将无法被探测到。如果您碰到这个情况，您必须避免使用 **-P** 选项。目前还没有绕过这个问题的办法。

使用 **-P** 选项来自动选择控制台，或使用 **-h** 选项来激活控制台。

您也可以使用boot联机文档中所描述的其他选项。

除了 **-P** 选项，所有选项将被传给启动引导器(/boot/loader)。启动引导器将通过检查 **-h** 选项的状态来决定是显示设备成为控制台，还是串口成为控制台。这表示如果您指定 **-D** 选项，但在 **/boot.config** 中没有 **-h** 选项，您在启动代码块时使用串口作为控制台。启动引导器将使用内部显示设备作为控制台。

6. 启动机器

当您启动您的FreeBSD时，引导块将把 **/boot.config** 的内容发给控制台。例如：

```
/boot.config: -P
Keyboard: no
```

如果您把 **-P** 放在 **/boot.config** 中并指出键盘存在或不存在，那将只出现第二行。这些信息会被定位到串口或内部控制台，或两者同时，这完全取决于 **/boot.config** 中的选项。

选项	送出消息的设备
none	内部控制台
-h	串行控制台
-D	串行控制台和内部控制台
-Dh	串行控制台和内部控制台
-P, 有键盘	内部控制台
-P, 无键盘	串行控制台

出现上面信息后，在引导块加载启动引导器和更多信息被映到屏幕之前将有一个小小的停顿。在通常情况下，您不需要打断启动进程，但为了确信设置是否正确，您也可以这样做。

在控制台上按 **Enter** 以外的任意键就能打断启动进程。引导块将进入命令行模式。您将看到：

```
>> FreeBSD/i386 B00T
Default: 0:ad(0,a)/boot/loader
boot:
```

检验上面出现的信息，可能是串口，或内部控制台，或两个同时，完全取决于您在 **/boot.config** 中的选项。如果信息出现在正确的控制台，按 **Enter** 继续启动进程。

如果您要使用串行控制台，但您没有看到命令行，那可能设置有问题。这时，输入 **-h** 然后按 **Enter/Return** 来告诉引导块(然后是启动引导器和内核)选择串口作为控制台。一旦系统起来了，就可以回去检查一下是什么出了问题。

启动引导器加载完后，您将进入启动进程的第三步，您仍然可以在启动引导器通过设定您喜欢的环境来切换内部控制台和串行控制台。参考第22.6.6节。

22.6.4 摘要

这是几个在这章要讨论的几个设置和选择的控制台的摘要。

22.6.4.1 例1: 您为sio0 设置标记0x10

```
device sio0 at isa? port IO_COM1 flags 0x10 irq 4
```

在/boot.config 中的选项	引导块执行时所用的控制台	引导加载器执行时所用的控制台	内核所用的控制台
无	内部	内部	内部
-h	串行	串行	串行
-D	串行和内部	内部	内部
-Dh	串行和内部	串行	串行
-P, 有键盘	内部	内部	内部
-P, 没有键盘	串行和内部	串行	串行

22.6.4.2 例2: 您为sio0设置标记为0x30

```
device sio0 at isa? port IO_COM1 flags 0x30 irq 4
```

在/boot.config 中的选项	引导块执行时所用的控制台	引导加载器执行时所用的控制台	内核所用的控制台
无	内部	内部	串行
-h	串行	串行	串行
-D	串行和内部	内部	串行
-Dh	串行和内部	串行	串行
-P, 有键盘	内部	内部	串行
-P, 没有键盘	串行and internal	串行	串行

22.6.5 串行控制台的提示

22.6.5.1 设置一个快速的串口速度

默认的串口被设置成9600波特，8数据位，无奇偶校验，1个停止位。如果您希望改变速度，就必须重新编译引导块。在/etc/make.conf 中添加下面一行，然后编译新的引导块：

```
BOOT_COMCONSOLE_SPEED=19200
```

参见第22.6.5.2 节 以了解如何编译和安装新的引导块。

如果串行控制台用其他方法来配置而不是在启动时用 -h，或内核使用的串行控制台与引导块使用的不同，就必须在内核配置中加入下面这行，并重新编译内核：

```
options CONSPEED=19200
```

22.6.5.2 使用sio0 以外的串口作为控制台

使用串口而不是sio0 作为控制台需要做一些重编译。如果您无论如何都要使用另一个串口，重新编译引导块，启动引导器和内核。

1. 取得内核源代码(参考第21 章)。
2. 编辑/etc/make.conf 文件，然后设置BOOT_COMCONSOLE_PORT作为您要使用(0x3f8、0x2f8、0x3E8 或0x2E8) 端口的地址。只有sio0 到sio3 (COM1 到COM4) 都可以使用；但多口串行卡将不会工作。不需要任何中断设置。
3. 创建一个定制的内核配置文件，在您要使用的串口添加合适的标记。例如，如果要将sio1 (COM2) 作为控制台：

```
device sio1 at isa? port IO_COM2 flags 0x10 irq 3
```

或

```
device sio1 at isa? port port IO_COM2 flags 0x30 irq 3
```

其他端口的控制台标记也不要设。

4. 重新编译和安装引导块：

```
# cd /sys/boot
# make clean
# make
# make install
```

5. 重建和安装内核。
6. 用disklabel(8) 将引导块写到启动盘上，然后从新内核启动。

22.6.5.3 通过串行线进入DDB调试器

```
options BREAK_TO_DEBUGGER
options DDB
```

22.6.5.4 在串行控制台上得到一个登录命令行

您可能希望通过串行线进入登录提示，现在您可以看到启动信息，通过串行控制台键入内核调试信息。可以这样做。

用一个编辑器打开/etc/ttys 文件，然后找到下面的行：

```
ttyd0 "/usr/libexec/getty std.9600" unknown off secure
ttyd1 "/usr/libexec/getty std.9600" unknown off secure
ttyd2 "/usr/libexec/getty std.9600" unknown off secure
ttyd3 "/usr/libexec/getty std.9600" unknown off secure
```

ttyd0 到ttyd3 相当于COM1 到COM4。可以打开或关闭某个端口。如果您已经改变了串口的速度，还必须改掉标准的9600 与当前的例如19200 相匹配。

您也可以改变终端的类型从不知名的到您串行终端的真实类型。编辑完这个文件，您必须kill -HUP 1 来使这个修改生效。

22.6.6 从启动引导器修改控制台

前面一节描述了如何通过调整引导块来设定串行控制台。本节将讲到在启动引导器中通过键入一些命令和环境变量来指定控制台。由于启动引导器会被启动进程的第三步所调用，引导块以后，在启动引导器中的设置将忽略在引导块中的设置。

22.6.6.1 配置串行控制台

您可以很容易地指定启动引导器和内核来使用串行控制台，只需要在`/boot/loader.rc`中写入下面这行：

```
set console="comconsole"
```

无论前一节中的引导块如何配置，这个设置都会生效。

您最好把上面一行放在文件的第一行，以便尽早地在启动时看到串行控制台的启动信息。

同样地，您可以指定内部控制台为：

```
set console="vidconsole"
```

如果您不设置启动引导环境变量控制台，启动引导器和内核将使用在引导块时用`-h`选项指定的控制台。

在3.2 以及更新的版本中，您可以在`/boot/loader.conf.local` 或`/boot/loader.conf` 中，而不是在`/boot/loader.rc` 指定控制台。用这种方法，您的`/boot/loader.rc` 文件将是这样的：

```
include /boot/loader.4th
start
```

然后，创建`/boot/loader.conf.local` 并加入下面的行。

```
console=comconsole
```

或

```
console=vidconsole
```

看看`loader.conf(5)` 的联机手册了解更多信息。

注意：目前，引导块还没有与引导加载器的`-p` 选项等价的选项，此外也没有在存在键盘时自动选则使用什么控制台的能力。

22.6.6.2 使用串口而不是sio0作为控制台

要使用一个串口而不是`sio0` 作为串行控制台需要重新编译启动引导器。下面的步骤跟第22.6.5.2 节描述的相似。

22.6.7 警告

这篇文章本意是想告诉人们如何设定没有显示设备或键盘的专用服务器。不幸的是，绝大多数系统没有键盘可以让您启动，而没有显示设备就不让您启动。使用AMI BIOS 的机器可以通过在CMOS 中将“graphics adapter”项设为“Not installed”来在启动时不要求显示适配器。

然而，许多机器并不支持这个选项，如果您的系统没有显示硬件就拒绝启动。对于这些机器，即使您没有显示器，也必须在机器上插上显示适配器。建议您试试采用AMI BIOS 的机器。

第23章

PPP 和SLIP

Restructured, reorganized, and updated by Jim Mock.

23.1 概述

FreeBSD 有很多方法可以将计算机与计算机连接起来。通过使用拨号modem 来建立网络或Internet 连接，或允许其他人通过您的机器来连上网络，这些都要求使用PPP 或SLIP。这章将详细介绍设置这些基于modem 的通信服务的方法。

读完这一章，您将了解：

- 如何设置用户级PPP。
- 如何设置内核级PPP。
- 如何设置PPPoE (PPP over Ethernet)。
- 如何设置PPPoA (PPP over ATM)。
- 如何配置和安装SLIP 客户端和服务端。

在阅读这章之前，您应：

- 熟悉基本的网络术语。
- 理解拨号连接和PPP、SLIP 的基础知识。

您可能想知道用户级PPP 与内核级PPP 之间的不同之处。回答很简单：用户级PPP 处理用户级的输入和输出数据，而不是内核级。在内核与用户区之间复制数据的花费要大一些，但它能提供具有更多特性的PPP实现。用户级PPP使用tun 设备与外界通信而内核级PPP 使用ppp 设备。

注意：除非需要与其它PPP 软件(比如pppd) 相区别，在这一章中，用户级PPP 就简称为ppp。另外，若没有额外的注明，本章所介绍的所有命令都需要root 权限。

23.2 使用用户级PPP

Updated and enhanced by Tom Rhodes. Originally contributed by Brian Somers. With input from Nik Clayton、Dirk Fröberg 和Peter Childs.

23.2.1 用户级PPP

23.2.1.1 前提条件

本章假定您具备如下条件：

- 您有一个ISP 提供的用于连接使用PPP 的帐号。
- 您需要一个连接到您的系统，并做了正确配置的modem 或其它设备，使您能连接到ISP。
- ISP 的拨号号码。
- 您的登录名称和密码(可能是一般的UNIX 风格的登录名和密码对，也可能是PAP 或CHAP 登录名和密码对。)
- 一个或多个域名服务器IP 地址。通常，您会从ISP处得到两个这样的IP地址。如果您至少得到了一个，就可以在文件ppp.conf 中加入enable dns 命令使ppp 设置域名服务。这个功能取决于ISP 对支持DNS 协商的具体实现。

下面的信息由您的ISP 提供，但不是必需的：

- ISP的网关IP地址. 网关是您要连接的且要被设为默认路由的主机. 如果您没有这个信息,您可以虚构一个,在连接时ISP的PPP服务器会自动告诉您正确的值.

这个虚构的IP号被ppp称为HISADDR.

- 需要使用的子网掩码.如果ISP没有提供,您可以安全地使用255.255.255.255.
- 如果ISP提供了一个静态的IP地址和主机名,可以输入它们.否则,让对方主机指定它认为合适的IP地址.

如果您不知道这些信息,请与您的ISP联系.

注意: 在这节中,所有作为样例显示的配置文件信息都对行进行了编号. 这些行号只是为了使解释和讨论变得方便,在真实当地用tab键和sp文件中并不存在. 缩进是必需的.

23.2.1.2 创建PPP设备节点

一般情况下,大多数用户只需要一个tun设备(/dev/tun0),提及tun0时,即指tunN,N是您系统中具体的号码.

若的FreeBSD(FreeBSD 4.X 及早前版本)没有启用devfs(5),应当先检查是否存在tun0设备,如果已经启用了devfs(5),这一步就没必要了(因为devfs(5)会根据需要创建设备).

为了确保tun0配置正确,最简单的方式是重新创建它.按照以下步骤可以重新创建设备:

```
# cd /dev
# sh MAKEDEV tun0
```

如果您的内核要有16个tunnel设备,您必须创建它们.可以通过执行以下命令完成:

```
# cd /dev
# sh MAKEDEV tun15
```

23.2.1.3 PPP自动化配置

ppp和pppd(PPP的内核级实现) 都使用/etc/ppp目录中的配置文件.用户级PPP的例子能在/usr/share/examples/ppp/中找到.

配置ppp要求根据您的需要编辑几个文件.编辑哪几个文件取决于您的IP是静态分配还是动态分配的.

23.2.1.3.1 PPP和静态IP地址

您需要编辑配置文件/etc/ppp/ppp.conf.如下所示.

注意: 以冒号:结尾的行从第一列(行首)开始, 其它所有的行都要使用空格或制表符(Tab) 来缩进。

```

1      default:
2          set log Phase Chat LCP IPCP CCP tun command
3          ident user-ppp VERSION (built COMPILATIONDATE)
4          set device /dev/cuaa0
5          set speed 115200
6          set dial "ABORT BUSY ABORT NO\\sCARRIER TIMEOUT 5 \
7                  \"\" AT OK-AT-OK ATE1Q0 OK \\dATDT\\t TIMEOUT 40 CONNECT"
8          set timeout 180
9          enable dns
10
11     provider:
12         set phone "(123) 456 7890"
13         set authname foo
14         set authkey bar
15         set login "TIMEOUT 10 \"\" \"\" gin:--gin: \\U word: \\P col: ppp"
16         set timeout 300
17         set ifaddr x.x.x.x y.y.y.y 255.255.255.255 0.0.0.0
18         add default HISADDR

```

行1:

指定默认的项.当PPP运行时这个项中的命令将自动执行.

行2:

启用登录参数.工作正常后,为避免产生过多的日志文件,这行应该简化为:

```
set log phase tun
```

行3:

告诉PPP怎样向对方自我标识. 如果在建立或使用连接时遇到任何麻烦,PPP就会向对方主机自我标识.对方主机管理员在处理这个问题时,这些信息会有用.

行4:

标明modem要连接的端口号.COM1是/dev/cuaa0, COM2 是/dev/cuaa1.

行5:

设置连接的速度.如果115200 不能工作,试试38400.

行6 & 7:

拨号字符串. 用户级PPP使用一种与chat(8)程序相似的语法. 请参考联机手册了解这种语言的相关信息.

注意,为了便于阅读此命令进行了换行.任何ppp.conf里的命令都可以这样做,前提是行的最后一个字符必须是“\”.

行8:

设置连接的时间间隔.默认是180秒,所以这一行是多余的.

行9:

告诉PPP向对方主机确认本地域名解析设置.如果您运行了本地的域名服务器,要注释或删除掉这一行.

行10:

为了可读性的需要设置一个空行.空行会被PPP忽略.

行11:

为“provider”指定一个项.可以改成ISP的名字.这样您以后就可以使用load ISP 开启连接.

行12:

设置提供商的电话号码.多个电话号码可以使用冒号(:)或管道符号(|)隔开.这两个字符的区别在ppp(8)的联机手册中有介绍.总的来讲,如果您要循环使用这些号码,可以使用冒号.如果您想使用第一个号码,当第一个号码失败了再用第二个号码,就使用管道符号.如所示的那样,要给整个电话号码加上引号(").

如果电话号码里有空格,必须用引号(")将其括起来.否则会造成简单却难以察觉的错误.

行13 & 14:

指定用户名和密码.当使用一个UNIX风格的命令提示符登录时,这些值可以用带有U \P参数的set login命令进行修改.当使用PAP或CHAP进行连接时,这些值在验证使用.

行15:

如果您使用的是PAP或者CHAP,在这里就不会有登录.要注释或删除掉这一行.请参考PAP和CHAP认证以获取更多细节.

登录命令是的语法是chat类型的.在这个例子中,是这样的:

```
J. Random Provider
login: foo
password: bar
protocol: ppp
```

您需要改变这个脚本以适合您自己的需要.当您第一次写这个脚本时,应当确保已经启用“chat”并处于登录状态,这样您才能确认通信是否正在按计划进行.

行16:

设置默认的超时时间.这里,连接若在300秒内无响应将被断开.如果您不想设置成超时,将这个值设置成0,或在命令行使用-ddial选项.

行17:

设置接口地址.字符串x.x.x.x需要用ISP提供给您的IP地址替换.字符串y.y.y.y要用ISP的网关IP地址替换(即您要连接的主机).如果ISP没有给您网关地址,可以使用10.0.0.2/0.如果您需要使用一个“猜到”的地址,请确保在/etc/ppp/ppp.linkup 中为每个PPP和动态IP地址指令创建了项.如果没有这一行,ppp 将无法运行-auto模式.

第18行:

添加一个到ISP网关的默认路由。HISADDR这个关键字会被第17行所指定的网关地址替换。这行必须出现在第17行之后,以免在HISADDR初始化之前使用它的值。

如果您不想使用 -auto 的PPP,则这行应挪到, ppp.linkup 文件中。

若您有一个静态IP地址,且使用 -auto 模式运行ppp(因为在连接之前已经正确设置了路由表项),那就不需要再向ppp.linkup 添加项。您可能希望在连接以后创建一个项来调用程序。这在以后的sendmail的例子中会解释。

示例配置文件可以在目录/usr/share/examples/ppp/中找到。

23.2.1.3.2 PPP和动态IP地址

如果ISP没给您指定静态的IP地址,ppp要被配置成能够与对方协商确定本地和远程地址。要完成这项工作,先要“猜”一个IP地址,然后允许ppp在连接后使用IP配置协议(IPCP)进行正确配置。ppp.conf的配置是与PPP和静态IP地址一样的,除了以下的改变:

```
17      set ifaddr 10.0.0.1/0 10.0.0.2/0 255.255.255.255
```

再次强调,不要包括行号,它只是一个引用标记。缩排一个空格是必须的。

行17:

/字符以后是PPP所要求的地址位码。您可以根据需要使用不同IP号码,但以上的例子永远是可行的。

最后的参数(0.0.0.0)告诉PPP从0.0.0.0而不是10.0.0.1开始协商地址,对于有些ISP,这是必需的。不要将0.0.0.0作为set ifaddr的第一个参数,因为这使得PPP在 -auto 模式时不能设置初始路由。

如果您不运行 -auto模式,就需要在/etc/ppp/ppp.linkup中创建一个项。连接建立之后,ppp.linkup被启用。这时候,ppp将指派接口地址,接着再添加路由表项:

```
1      provider:
2      add default HISADDR
```

Line 1:

为了建立连接,ppp会按照如下规则在ppp.linkup寻找项:首先,试图寻找相同的标签(如同在ppp.conf一样)。如果失败了,寻找作为网关IP地址的项,此项是四个八位字节的风格。如果依旧没有找到,就寻找MYADDR项

行2:

这行告诉ppp添加指向HISADDR的默认路由。HISADDR由通过IPCP协商得到的IP号替换。

参考/usr/share/examples/ppp/ppp.conf.sample
和/usr/share/examples/ppp/ppp.linkup.sample 中的pmdemand项以获取细节化的例子。

23.2.1.3.3 接收拨入

当要配置ppp接受来自LAN上的拨入时,您需要决定是否将包转给LAN。如果是的话,您就必须从LAN子网中给对方分配一个IP,需要在文件/etc/ppp/ppp.conf中使用命令enable proxy。您还应该确定文件/etc/rc.conf中包含以下内容:

```
gateway_enable="YES"
```

23.2.1.3.4 使用哪个getty?

配置FreeBSD的拨号服务描述了怎么使用命令getty(8)启动拨号服务。

除了getty 还有mgetty (<http://www.leo.org/~doering/mgetty/index.html>), 它是getty的智能版本,是按照拨号线的思想设计的。

使用mgetty的好处是它能积极地与modems进行talks, 这就意味着如果在/etc/ttys中的端口被关闭, 您的modem就不会回应拨入。

最新版本的mgetty (from 0.99beta onwards)也支持自动侦测PPP数据流,允许客户端不使用脚本就可以访问服务器。

参考Mgetty 和AutoPPP的联机手册了解更多信息。

23.2.1.3.5 PPP 权限

ppp命令通常必须作为root用户运行. 但如果想让一个普通用户将ppp运行于服务器模式(就像下面描述的那样),您必须要把此用户加入network组以使其获得运行ppp 的权限。

您还需要使用allow命令使用户能访问配置文件的一个或多个部分:

```
allow users fred mary
```

如果这个命令被用在default 部分中,您可以让指定的用户访问任何东西。

23.2.1.3.6 动态IP用户的PPP Shell

创建一个名为/etc/ppp/ppp-shell文件,加入以下内容:

```
#!/bin/sh
IDENT='echo $0 | sed -e 's/^.*-\(.*\)$/\1/'
CALLEDAS="$IDENT"
TTY='tty'

if [ x$IDENT = xdialup ]; then
    IDENT='basename $TTY'
fi

echo "PPP for $CALLEDAS on $TTY"
echo "Starting PPP for $IDENT"

exec /usr/sbin/ppp -direct $IDENT
```

这个脚本要有可执行属性. 然后通过如下命令创建一个指向此脚本且名为ppp-dialup的符号链接:

```
# ln -s ppp-shell /etc/ppp/ppp-dialup
```

您应该将这个脚本作为所有拨入用户的shell。以下是在文件/etc/passwd 中关于PPP 用户pchilds 的例子(切记, 不要直接修改这个密码文件, 用vipw(8) 来修改它)。


```
pchlds:*:1011:300:Peter Childs PPP:/home/ppp:/etc/ppp/ppp-dialup
```

创建一个名为/home/ppp的目录作为拨入用户的主目录, 包含以下这些空文件:

```
-r--r--r-- 1 root wheel 0 May 27 02:23 .hushlogin
-r--r--r-- 1 root wheel 0 May 27 02:22 .rhosts
```

这样就可以防止/etc/motd被显示出来.

23.2.1.3.7 静态IP用户的Shell

像上面那样创建ppp-shell文件, 为每个静态分配IP用户创建一个到ppp-shell的符号链接.

例如,如果您有三个拨号用户, fred,sam,和mary,您为他们路由C类网络,您需要键入以下内容:

```
# ln -s /etc/ppp/ppp-shell /etc/ppp/ppp-fred
# ln -s /etc/ppp/ppp-shell /etc/ppp/ppp-sam
# ln -s /etc/ppp/ppp-shell /etc/ppp/ppp-mary
```

每个用户的Shell必须被设成一个符号链接(例如用户mary的Shell应该是/etc/ppp/ppp-mary).

23.2.1.3.8 为动态IP用户设置ppp.conf

/etc/ppp/ppp.conf文件应该包含下面这些行:

```
default:
    set debug phase lcp chat
    set timeout 0

ttyd0:
    set ifaddr 203.14.100.1 203.14.100.20 255.255.255.255
    enable proxy

ttyd1:
    set ifaddr 203.14.100.1 203.14.100.21 255.255.255.255
    enable proxy
```

注意: 缩进得必须的.

default:项在每次会话时都会加载.每个在/etc/ttys中启用的行都必须为其创建一个相似于ttyd0:的项.每一行应该从动态IP 地址池中取得唯一的IP地址.

23.2.1.3.9 为静态IP用户配置ppp.conf

根据上面/usr/share/examples/ppp/ppp.conf文件的内容, 您必须为每个静态拨号用户添加一个项.我们继续以fred, sam, 和mary为例.

```
fred:
    set ifaddr 203.14.100.1 203.14.101.1 255.255.255.255
```

```
sam:
  set ifaddr 203.14.100.1 203.14.102.1 255.255.255.255
```

```
mary:
  set ifaddr 203.14.100.1 203.14.103.1 255.255.255.255
```

如果需要,/etc/ppp/ppp.linkup 也应该包括每个静态IP用户的路由信息.下面这一行为客户连接添加了203.14.101.0C类路由.

```
fred:
  add 203.14.101.0 netmask 255.255.255.0 HISADDR
```

```
sam:
  add 203.14.102.0 netmask 255.255.255.0 HISADDR
```

```
mary:
  add 203.14.103.0 netmask 255.255.255.0 HISADDR
```

23.2.1.3.10 mgetty 和AutoPPP

在配置和编译mgetty 时启用AUTO_PPP选项使mgetty能够探测PPP连接的LCP状态并自动产生PPP Shell. 但如果默认的login/password队列没有出现,那就必须使用PAP或CHAP来验证用户.

这节假定您已经为用户成功地配置,编译了带有AUTO_PPP选项的mgetty.

确认文件/usr/local/etc/mgetty+sendfax/login.config 包含以下内容:

```
/AutoPPP/ - - /etc/ppp/ppp-pap-dialup
```

这行告诉mgetty运行ppp-pap-dialup脚本来侦听PPP连接.

创建/etc/ppp/ppp-pap-dialup文件写入以下内容(此文件应该是可执行的):

```
#!/bin/sh
exec /usr/sbin/ppp -direct pap$IDENT
```

对应于每个在/etc/ttys的启用行,都要在/etc/ppp/ppp.conf 中创建相应的项.这和上面的定义是相同的.

```
pap:
  enable pap
  set ifaddr 203.14.100.1 203.14.100.20-203.14.100.40
  enable proxy
```

每个以这种方式登录的用户,都必须在/etc/ppp/ppp.secret 文件中给出用户名/口令,或者使用以下选项,来通过PAP 方式以/etc/passwd 文件提供的信息来完成身份验证。

```
enable passwdauth
```

如果您想为某些用户分配静态IP,可以在/etc/ppp/ppp.secret中将IP号作为第三个参数指定. 参看/usr/share/examples/ppp/ppp.secret.sample 中的例子.

23.2.1.3.11 MS Extensions

可以配置PPP以提供DNS和NetBIOS域名服务器地址。

要在PPP版本1.x中启用这些扩展,必须向/etc/ppp/ppp.conf的相关项加入以下行:

```
enable msextr
set ns 203.14.100.1 203.14.100.2
set nbns 203.14.100.5
```

PPP版本2及以上:

```
accept dns
set dns 203.14.100.1 203.14.100.2
set nbns 203.14.100.5
```

这将告诉客户端首选域名服务器和备用域名服务器。

在版本2及以上版本中,如果省略了set dns, PPP会使用/etc/resolv.conf中的值。

23.2.1.3.12 PAP 和CHAP验证

一些ISP将系统设置成使用PAP或CHAP机制来完成连接的验证部分。如果是这样,在您连接时ISP就不会给出login:提示符而是立即开始PPP对话。

PAP安全性要比CHAP差一些,但在这里安全性并不是问题,因为密码(即使用明文传送)只是通过串行线传送。黑客没有太多机会“窃听”。

参考PPP 和静态IP地址 或PPP 和动态IP地址 节,必须做以下修改:

```
13      set authname MyUserName
14      set authkey MyPassword
15      set login
```

第13行:

这一行指明您的PAP/CHAP用户名。您需要为MyUserName输入正确的值。

第14行:

这一行指明您的PAP/CHAP password密码。您需要为MyPassword 输入正确的值。另外,您可能希望加入一些额外的选项,例如:

```
16      accept PAP
```

或

```
16      accept CHAP
```

以明确您的意图,但PAP和CHAP都是被默认接受的。

Line 15:

Your ISP will not normally require that you log into the server if you are using PAP or CHAP. You must therefore disable your “set login” string.

23.2.1.3.13 即时改变您的ppp 配置

与后台运行的ppp程序进行对话是可能的,前提是设置了一个合适的诊断端口.做到这一点,需要把下面的行加入到您的配置中:

```
set server /var/run/ppp-tun%d DiagnosticPassword 0177
```

这行告诉PPP在指定的UNIX域socket中侦听,当用户连接时需要给出指定的密码.%d用tun设备号替换.一旦启用了socket,就可以在脚本中调用程序pppctl(8)来处理正在运行的PPP.

23.2.1.4 使用PPP网络地址翻译

PPP可以使用内建的NAT,而不需内核支持.这个功能可以通过在/etc/ppp/ppp.conf中的以下行启用:

```
nat enable yes
```

PPP NAT也可以使用命令行选项-nat启动.在文件/etc/rc.conf中也有ppp_nat项,且是默认启用的.

如果您使用了这个特性,您还会发现在/etc/ppp/ppp.conf中以下选项对于启用incoming connections forwarding是有用的:

```
nat port tcp 10.0.0.2:ftp ftp
nat port tcp 10.0.0.2:http http
```

```
or do not trust the outside at all
```

```
nat deny_incoming yes
```

23.2.1.5 最后的系统配置

现在您已配置了ppp,但在真正工作之前还有一些事情要做.它们都与编辑/etc/rc.conf有关.

从上依次往下看,确认设置了hostname= 行, e.g.:

```
hostname="foo.example.com"
```

如果您的ISP提供给您一个静态的IP和名字,将这个名字设为hostname是最合适的.

寻找network_interfaces 变量.如果要配置系统通过拨号连入ISP,一定要将tun0设备加入这个列表,否则就删除它.

```
network_interfaces="lo0 tun0"
ifconfig_tun0=
```

注意: ifconfig_tun0变量应该是空的,且要创建一个名为/etc/start_if.tun0的文件.这个文件应该包含这一行:

```
ppp -auto mysystem
```

此脚本在网络配置时被执行,开启PPP守护进程进入自动模式.如果这台机器充当一个LAN的网关,您可能希望使用-alias.参考相关联机手册了解更多细节.

务必在/etc/rc.conf 中, 把路由程序设置为NO:

```
router_enable="NO"
```

不启动routed 服务程序非常重要, 因为routed 总会删掉由ppp 所建立的默认路由。

此外, 还应该确保sendmail_flags 这一行没有-q 参数, 否则sendmail 将会不断地尝试查找网络, 而这样做将会导致机器不断地进行拨号。可以考虑:

```
sendmail_flags="-bd"
```

替代的作法是当每次PPP连接建立时您必须通过键入以下命令强制sendmail重新检查邮件队列:

```
# /usr/sbin/sendmail -q
```

您也可以在ppp.linkup使用!bg命令自动完成这些工作:

```
1 provider:
2   delete ALL
3   add 0 0 HISADDR
4   !bg sendmail -bd -q30m
```

如果您不喜欢这样做, 可以设立一个“dfilter” 以阻止SMTP传输, 参考相关文件了解更多细节。

现在您唯一要做的事是重新启动计算机。重起之后, 可以输入:

```
# ppp
```

然后是dial provider以开启PPP会话. 或者如果您想让ppp自动建立会话, 因为您有一个广域连接(且没有创建start_if.tun0 脚本), 键入:

```
# ppp -auto provider
```

23.2.1.6 总结

当第一次设置PPP时, 下面几步是必须的:

客户端:

1. 确保tun编译进了内核.
2. 确保tunw 设备文件在/dev 目录中是可用的.
3. 在/etc/ppp/ppp.conf中创建一个项. pmdemand示例应该适合于绝大多数ISP.
4. 如果您使用动态IP地址, 在/etc/ppp/ppp.linkup创建一个项.
5. 更新/etc/rc.conf 文件.
6. 如果您要求按需拨号, 创建一个start_if.tun0脚本.

服务器端:

1. 确保tun设备已编译入内核.
2. 确保tunw设备文件在/dev目录中是可用的.

3. 在/etc/passwd中创建一个项(使用vipw(8)程序).
4. 在用户的home目录创建一个运行ppp -direct direct-server或相似命令的profile.
5. 在/etc/ppp/ppp.conf中创建一个项.direct-server示例应该能满足要求.
6. 在/etc/ppp/ppp.linkup中创建一个项.
7. 更新/etc/rc.conf 文件.

23.3 使用内核级PPP

Parts originally contributed by Gennady B. Sorokopud 和Robert Huff.

23.3.1 设立内核级PPP

在开始设置内核级PPP时, 需要确信pppd已经被定位在/usr/sbin 中且存在/etc/ppp目录.

pppd能在两种模式下工作:

1. 作为一个“客户” ——您要通过PPP串行线或modem线把您的机器连接到互联网上.
2. 作为“服务器” ——计算机已经位于网络上,且被用于通过PPP与其它计算机连接.

两种情况您都需要设立一个选项文件, (/etc/ppp/options 或者是 ~/.ppprc 如果您的计算机有多个用户使用PPP).

您还需要一些modem/serial软件(comms/kermit就很适合), 使您能够拨号并与远程主机建立连接.

23.3.2 使用pppd作为客户端

Based on information provided by Trev Roydhouse.

下面这个/etc/ppp/options选项文件能够被用来与CISCO终端服务器的PPP线连接.

```
crtscts      # enable hardware flow control
modem        # modem control line
noipdefault  # remote PPP server must supply your IP address
              # if the remote host does not send your IP during IPCP
              # negotiation, remove this option
passive      # wait for LCP packets
domain ppp.foo.com      # put your domain name here

:<remote_ip>  # put the IP of remote PPP host here
              # it will be used to route packets via PPP link
              # if you didn't specified the noipdefault option
              # change this line to <local_ip>:<remote_ip>

defaultroute # put this if you want that PPP server will be your
              # default router
```

连接:

1. 使用**Kermit** (或其他modem 程序来拨号), 然后输入您的用户名和口令(或在远程主机上启用PPP 所需的其他信息)。
2. 退出**Kermit** (并不挂断连接)。
3. 键入下面这行:

```
# /usr/src/usr.sbin/pppd.new/pppd /dev/tty01 19200
```

一定要使用正确的速度和设备名。

现在您的计算机已经用PPP连接. 如果连接失败, 您可在文件/etc/ppp/options中添加debug选项, 察看控制台信息以跟踪问题.

下面这个/etc/ppp/pppup脚本能自动完成这三个步骤:

```
#!/bin/sh
ps ax |grep pppd |grep -v grep
pid='ps ax |grep pppd |grep -v grep|awk '{print $1;}'
if [ "X${pid}" != "X" ] ; then
    echo 'killing pppd, PID=' ${pid}
    kill ${pid}
fi
ps ax |grep kermi |grep -v grep
pid='ps ax |grep kermi |grep -v grep|awk '{print $1;}'
if [ "X${pid}" != "X" ] ; then
    echo 'killing kermi, PID=' ${pid}
    kill -9 ${pid}
fi

ifconfig ppp0 down
ifconfig ppp0 delete

kermi -y /etc/ppp/kermi.dial
pppd /dev/tty01 19200
```

/etc/ppp/kermi.dial 是一个**Kermit** 脚本, 它会完成拨号, 并在远程主机上完成所有需要的身份验证过程(这份文档的最后有一个脚本实例)。

使用下面这个脚本/etc/ppp/pppdown断开PPP连线:

```
#!/bin/sh
pid='ps ax |grep pppd |grep -v grep|awk '{print $1;}'
if [ X${pid} != "X" ] ; then
    echo 'killing pppd, PID=' ${pid}
    kill -TERM ${pid}
fi

ps ax |grep kermi |grep -v grep
pid='ps ax |grep kermi |grep -v grep|awk '{print $1;}'
if [ "X${pid}" != "X" ] ; then
    echo 'killing kermi, PID=' ${pid}
    kill -9 ${pid}
```

```
fi
```

```
/sbin/ifconfig ppp0 down
/sbin/ifconfig ppp0 delete
kermit -y /etc/ppp/kermit.hup
/etc/ppp/ppptest
```

通过执行/usr/etc/ppp/ppptest,看看pppd是否仍在运行:

```
#!/bin/sh
pid='ps ax| grep pppd |grep -v grep|awk '{print $1;}'
if [ X${pid} != "X" ] ; then
    echo 'pppd running: PID=' ${pid-NONE}
else
    echo 'No pppd running.'
fi
set -x
netstat -n -I ppp0
ifconfig ppp0
```

执行脚本/etc/ppp/kermit.hup以挂起modem,这个文件包含:

```
set line /dev/tty01 ; put your modem device here
set speed 19200
set file type binary
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
set flow none

pau 1
out +++
inp 5 OK
out ATH0\13
echo \13
exit
```

也可以用chat 代替kermit:

以下两个文件用以建立pppd连接.

/etc/ppp/options:

```
/dev/cuaa1 115200

crtscts # enable hardware flow control
modem # modem control line
connect "/usr/bin/chat -f /etc/ppp/login.chat.script"
noipdefault # remote PPP serve must supply your IP address
# if the remote host doesn't send your IP during
```



```

                # IPCP negotiation, remove this option
passive         # wait for LCP packets
domain <your.domain> # put your domain name here

: # put the IP of remote PPP host here
    # it will be used to route packets via PPP link
    # if you didn't specified the noipdefault option
    # change this line to <local_ip>:<remote_ip>

defaultroute # put this if you want that PPP server will be
    # your default router

/etc/ppp/login.chat.script:

```

注意: 以下内容应该放在一行内.

```

ABORT BUSY ABORT 'NO CARRIER' "" AT OK ATDT<phone.number>
CONNECT "" TIMEOUT 10 ogin:-\\r-ogin: <login-id>
TIMEOUT 5 sword: <password>

```

一旦这些被安装且修改正确,您所要做的就是运行pppd,就像这样:

```
# pppd
```

23.3.3 使用pppd作为服务器

/etc/ppp/options要包括下面这些内容:

```

rtscts          # Hardware flow control
netmask 255.255.255.0 # netmask (not required)
192.114.208.20:192.114.208.165 # IP's of local and remote hosts
                                # local ip must be different from one
                                # you assigned to the Ethernet (or other)
                                # interface on your machine.
                                # remote IP is IP address that will be
                                # assigned to the remote machine
domain ppp.foo.com # your domain
passive            # wait for LCP
modem             # modem line

```

下面这个脚本/etc/ppp/pppserv 使pppd以服务器方式启动:

```

#!/bin/sh
ps ax |grep pppd |grep -v grep
pid='ps ax |grep pppd |grep -v grep|awk '{print $1;}''
if [ "X${pid}" != "X" ] ; then
    echo 'killing pppd, PID=' ${pid}
    kill ${pid}
fi
ps ax |grep kermi |grep -v grep

```

```

pid='ps ax |grep kermi |grep -v grep|awk '{print $1;}'
if [ "X${pid}" != "X" ] ; then
    echo 'killing kermi, PID=' ${pid}
    kill -9 ${pid}
fi

# reset ppp interface
ifconfig ppp0 down
ifconfig ppp0 delete

# enable autoanswer mode
kermi -y /etc/ppp/kermi.ans

# run ppp
pppd /dev/tty01 19200

```

使用脚本/etc/ppp/pppservdown停止服务器:

```

#!/bin/sh
ps ax |grep pppd |grep -v grep
pid='ps ax |grep pppd |grep -v grep|awk '{print $1;}'
if [ "X${pid}" != "X" ] ; then
    echo 'killing pppd, PID=' ${pid}
    kill ${pid}
fi
ps ax |grep kermi |grep -v grep
pid='ps ax |grep kermi |grep -v grep|awk '{print $1;}'
if [ "X${pid}" != "X" ] ; then
    echo 'killing kermi, PID=' ${pid}
    kill -9 ${pid}
fi
ifconfig ppp0 down
ifconfig ppp0 delete

kermi -y /etc/ppp/kermi.noans

```

The following **Kermi** script (/etc/ppp/kermi.ans) will enable/disable autoanswer mode on your modem. It should look like this:

```

set line /dev/tty01
set speed 19200
set file type binary
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
set flow none

pau 1
out +++

```

```

inp 5 OK
out ATH0\13
inp 5 OK
echo \13
out ATS0=1\13    ; change this to out ATS0=0\13 if you want to disable
                  ; autoanswer mode

inp 5 OK
echo \13
exit

```

一个名为/etc/ppp/kermit.dial的脚本用于向远程主机进行拨号和验证.您要根据需要定制它.要加入您的登录名和密码.您还要根据modem和远程主机的反应更改输入语句.

```

;
; put the com line attached to the modem here:
;
set line /dev/tty01
;
; put the modem speed here:
;
set speed 19200
set file type binary          ; full 8 bit file xfer
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
set flow none
set modem hayes
set dial hangup off
set carrier auto              ; Then SET CARRIER if necessary,
set dial display on           ; Then SET DIAL if necessary,
set input echo on
set input timeout proceed
set input case ignore
def \%x 0                      ; login prompt counter
goto slhup

:slcmd                        ; put the modem in command mode
echo Put the modem in command mode.
clear                          ; Clear unread characters from input buffer
pause 1
output +++                     ; hayes escape sequence
input 1 OK\13\10               ; wait for OK
if success goto slhup
output \13
pause 1
output at\13
input 1 OK\13\10
if fail goto slcmd             ; if modem doesn't answer OK, try again

```

```

:slhup                                ; hang up the phone
clear                                ; Clear unread characters from input buffer
pause 1
echo Hanging up the phone.
output ath0\13                        ; hayes command for on hook
input 2 OK\13\10
if fail goto slcmd                    ; if no OK answer, put modem in command mode

:sldial                                ; dial the number
pause 1
echo Dialing.
output atdt9,550311\13\10             ; put phone number here
assign \%x 0                          ; zero the time counter

:look
clear                                ; Clear unread characters from input buffer
increment \%x                         ; Count the seconds
input 1 {CONNECT }
if success goto sllogin
reinput 1 {NO CARRIER\13\10}
if success goto sldial
reinput 1 {NO DIALTONE\13\10}
if success goto slnodial
reinput 1 {\255}
if success goto slhup
reinput 1 {\127}
if success goto slhup
if < \%x 60 goto look
else goto slhup

:sllogin                              ; login
assign \%x 0                          ; zero the time counter
pause 1
echo Looking for login prompt.

:slloop
increment \%x                         ; Count the seconds
clear                                ; Clear unread characters from input buffer
output \13
;
; put your expected login prompt here:
;
input 1 {Username: }
if success goto sluid
reinput 1 {\255}
if success goto slhup
reinput 1 {\127}
if success goto slhup
if < \%x 10 goto slloop               ; try 10 times to get a login prompt
else goto slhup                      ; hang up and start again if 10 failures

:sluid
;

```

```

; put your userid here:
;
output ppp-login\13
input 1 {Password: }
;
; put your password here:
;
output ppp-password\13
input 1 {Entering SLIP mode.}
echo
quit

:slnodial
echo \7No dialtone. Check the telephone line!\7
exit 1

; local variables:
; mode: csh
; comment-start: "; "
; comment-start-skip: "; "
; end:

```

23.4 PPP 连接故障排除

Contributed by Tom Rhodes.

本节将讲述通过modem连接使用PPP时可能出现的问题. 例如,您可能需要确切地知道您拨入的系统会出现一个怎样的命令行提示符.有些ISP会提供ssword提示符,而其它的可能会出现password; 如果没有根据情况的不同相应地编写ppp脚本,登录就会失败.诊断ppp最常用的方法是手动进行连接. 以下的信息会一步一步地带您完成手动连接.

23.4.1 检查设备节点

如果您的内核是经过重新配置的,那么就需要检查sio设备. 如果没有配置过内核,就没什么可担心的了.只要查看dmesg的输出以找到modem设备:

```
# dmesg | grep sio
```

您应该找到与sio设备有关的输出. 这些就是我们需要的COM端口. 如果您的modem按照标准串行端口工作,您能在sio1或COM2找到它. 如果是这样,您只需创建serial设备,而不必重建内核. cd到/dev目录,然后运行MAKEDEV脚本:

```
# sh MAKEDEV cuaa0 cuaa1 cuaa2 cuaa3
```

它会为您的系统创建串行(serial)设备. 如果modem设备连接在sio1接口(在DOS中称为COM2),那么您的modem将会是/dev/cuaa1。

23.4.2 手动连接

通过手动控制ppp来连接Internet 是诊断连接及获知ISP处理PPP客户端方式的一个快速,简单的方法. 让我们从PPP 命令行开始.在所有的例子中我们使用example作为运行PPP主机的主机名.键入ppp 命令打开ppp:

```
# ppp
```

现在我们已经打开了ppp.

```
ppp ON example> set device /dev/cuaa1
```

设置modem设备,在本例子中是cuaa1.

```
ppp ON example> set speed 115200
```

设置连接速度,在本例中我们使用115,200 kbps.

```
ppp ON example> enable dns
```

使ppp配置域名服务, 在文件/etc/resolv.conf中添加域名服务器行. 如果ppp不能确定我们的主机名,可以在稍后设置.

```
ppp ON example> term
```

切换到“终端”样我们就能手动地控制模式,这modem.

```
deflink: Entering terminal mode on /dev/cuaa1
type '~h' for help
```

```
at
OK
atdt123456789
```

使用命令at初始化modem, 然后使用atdt和ISP给您的号码进行拨号.

```
CONNECT
```

连接配置,如果我们遇到了与硬件无关的连接问题,可以在这里尝试解决.

```
ISP Login:myusername
```

这里提示您输入用户名,输入ISP提供的用户名然后按回车.

```
ISP Pass:mypassword
```

这时提示我们输入密码,输入ISP提供的密码. 如同登录FreeBSD,密码不会显示.

```
Shell or PPP:ppp
```

由于ISP的不同,这个提示符可能不会出现.这里我们被问及:是使用一个运行于提供商端的Shell还是启动ppp. 这本例中,我们选择使用ppp因为我们想得到Internet连接.

```
Ppp ON example>
```

注意在这个例子中,第一个p已经大写.这显示我们已经成功地连接上了ISP.

PPp ON example>

我们已经成功通过了ISP的验证,正在等待分配IP地址.

PPP ON example>

我们得到了一个IP 地址,成功地完成了连接.

PPP ON example>add default HISADDR

这里,我们添加默认路由.在能与外界通信之前我们需要这样做,因为现在我们只与服务器端建立了连接.如果由于已存在的路由而导致操作失败,您可以在add前加!号.作为另外一种方式,您也可以在真正连接之前设置这些(指add default HISADDR),ppp会根据这项设定协商取得一个新的路由.

如果一切顺利,现在我们应该能得到一个活动的Internet连接,可以使用**CTRL+z**使其转入后台.如果您发现PPP重新变为ppp,那代表我们失去了连接..大写的P表明我们有到ISP的连接而小写的p表明由于某种原因我们失去了连接.这便于我们了解连接状态. ppp 只有这两个状态.

23.4.2.1 诊断排错

如果您有一根直连线且似乎不能建立连接,要使用set ctsrts off以关闭字节流的CTS/RTS.这种情况一般发生在连接兼容PPP的终端服务器时.当它向通信连接写入数据时,PPP就会挂起,一直等待一个CTS,或者一个不可能出现的Clear to Send信号.如果使用了这个选项,您还应使用set accmap选项,某些存在缺陷的硬件在完成端对端发送特定字符,特别是XON/XOFF时可能会遇到困难.请参见ppp(8)联机手册以了解关于可用选项的更多细节,以及如何使用它们.

如果您有一个比较旧的modem,您要用set parity even.奇偶校验的默认设置是none,但在旧式的(当流量大量增加时)调制解调器和某些ISP被用来纠错.您需要使用这个选项才能使用Compuserve ISP.

PPP可能并不返回命令模式,这通常是ISP等待您这一端发起协商时发生了错误.此时,使用~p命令将强制ppp开始发送配置信息.

如果您没有看到登陆提示,则很可能需要使用PAP或CHAP验证来代替前面例子中的UNIX风格验证.要使用PAP或CHAP只需在进入终端模式之前把下面的选项加入PPP:

ppp ON example> set authname myusername

此处myusername应改为您的ISP分配给您的用户名。

ppp ON example> set authkey mypassword

此处mypassword应该为您的ISP分配给您的口令。

如果连接正常,但无法查找域名,请尝试ping(8)某个IP地址来看看是否返回了信息.如果您发现百分之百(100%)丢包,那么您很可能没有分配默认路由.请仔细检查选项add default HISADDR是否在连接时被设置了.如果您能连接到远程的IP地址则有可能域名解析服务器的地址没有被加入到/etc/resolv.conf.这个文件应该是下面的样子:

```
domain example.com
nameserver x.x.x.x
nameserver y.y.y.y
```

此处x.x.x.x和y.y.y.y应该改为您的ISP的DNS服务器的IP地址。这一信息在您注册时可能会提供给您，不过通常只需给ISP打个电话就能知道了。

您还可以让syslog(3)为您的PPP连接提供日志。只需增加：

```
!ppp
*. *      /var/log/ppp.log
```

到/etc/syslog.conf中。绝大多数情况下，这个功能默认已经打开了。

23.5 使用基于以太网的PPP(PPPoE)

Contributed (from <http://node.to/freebsd/how-tos/how-to-freebsd-pppoe.html>) by Jim Mock.

本节将介绍如何建立基于以太网的PPP (PPPoE)。

23.5.1 配置内核

对于PPPOE,并没有必须的内核配置. 如果必需的netgraph支持没有编译入内核,它可以由ppp动态加载.

23.5.2 设置ppp.conf

以下是一个ppp.conf的例子：

```
default:
  set log Phase tun command # you can add more detailed logging if you wish
  set ifaddr 10.0.0.1/0 10.0.0.2/0

name_of_service_provider:
  set device PPPoE:xl1 # replace xl1 with your Ethernet device
  set authname YOURLOGINNAME
  set authkey YOURPASSWORD
  set dial
  set login
  add default HISADDR
```

23.5.3 运行ppp

作为root,您可以执行：

```
# ppp -ddial name_of_service_provider
```


23.5.4 启动时运行ppp

在文件/etc/rc.conf加入以下内容:

```
ppp_enable="YES"
ppp_mode="ddial"
ppp_nat="YES" # if you want to enable nat for your local network, otherwise NO
ppp_profile="name_of_service_provider"
```

23.5.5 使用PPPoE 服务标签

在某些时候,有必要使用一个服务标签来建立您的连接.服务标签用于区分同一网络中的不同服务器.

您可以在ISP提供的文档中找到必要的服务标签信息.若不能找到,向您的ISP询求技术支持.

作为最后的方法,您可以试试Roaring Penguin PPPoE (<http://www.roaringpenguin.com/pppoe/>), 它可以在Ports Collection 中找到.然而需要注意的是,它可能会清楚modem 的固件,并使其无法正常工作,因此一定要仔细考虑之后再做这个操作.简单地安装由服务提供商随modem 提供的程序.随后,选择System 菜单.您的配置文件应该会在哪里列出.一般来说它的名字应该是ISP.

配置文件名(service tag, 服务标签) 将被用于PPPoE 在ppp.conf 中的配置项,作为服务商set device 命令的一部分(参见ppp(8) 联机手册以了解更多细节).它应该类似下面的样子:

```
set device PPPoE:x11:ISP
```

记住将x11换成实际的以太网设备.

记住将ISP 换成您刚刚找到的profile名.

获得更多的信息,请参考:

- Cheaper Broadband with FreeBSD on DSL (<http://renaud.waldura.com/doc/freebsd/pppoe/>) by Renaud Waldura.
- Nutzung von T-DSL und T-Online mit FreeBSD (<http://www.ruhr.de/home/nathan/FreeBSD/tdsl-freebsd.html>) by Udo Erdelhoff (in German).

23.5.6 带有一个3Com® HomeConnect®ADSL Modem的PPPOE双重连接

这个modem不遵循RFC 2516 (<http://www.faqs.org/rfcs/rfc2516.html>) (**A Method for transmitting PPP over Ethernet (PPPoE)**, written by L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, and R. Wheeler). 而是使用不同的数据包格式作为以太网的框架.请向3Com (<http://www.3com.com/>)抱怨,如果您认为它应该遵守PPPOE的规范.

为了让FreeBSD能够与这个设备通信,必须设置sysctl.通过更改/etc/sysctl.conf,这一步可以在启动时自动完成:

```
net.graph.nonstandard_pppoe=1
```

或者,也可以直接执行下面的命令:

```
# sysctl net.graph.nonstandard_pppoe=1
```

很不幸，由于这是系统全局设置，无法同时与正常的PPP客户端(或服务器)和3ComHomeConnect® ADSL Modem通信。

23.6 Using PPP over ATM (PPPoA)

以下将介绍如何设置基于ATM的PPP(PPPoA)。PPPoA是欧洲DSL提供商的普遍选择。

23.6.1 使用带有一个Alcatel SpeedTouch™ USB的PPPoA

针对这一设备的PPPoA支持，在FreeBSD中是作为port提供的，因为其固件使用了阿尔卡特许可协议(http://www.speedtouchdsl.com/disclaimer_lx.htm)，因而不能与FreeBSD的基本系统一起免费地再发布。

使用Ports Collection可以非常方便地安装net/pppoa port，之后按照它提供的指使操作就可以了。

和许多USB设备类似，阿尔卡特的SpeedTouch™ USB需要从主机上下载固件才能够正常工作。您可以在FreeBSD中将此操作自动化，这样当设备插到某个USB口的时候就会自动下载固件了。可以在/etc/usbd.conf文件中加入下面的信息来让它自动完成固件的传送。注意，必须以root用户的身份编辑它。

```
device "Alcatel SpeedTouch USB"
    devname "ugen[0-9] +"
    vendor 0x06b9
    product 0x4061
    attach "/usr/local/sbin/modem_run -f /usr/local/libdata/mgmt.o"
```

要启动USB守护进程usbd，在/etc/rc.conf加入以下行：

```
usbd_enable="YES"
```

也可以将ppp设置成启动时拨号。向/etc/rc.conf加入以下这几行。同样地您需要以root用户登录。

```
ppp_enable="YES"
ppp_mode="ddial"
ppp_profile="adsl"
```

为了使其正常工作，您需要使用net/pppoa port提供的ppp.conf样例。

23.6.2 使用mpd

可以使用mpd来连接多种类型的服务，特别是PPTP服务。您可以在Ports Collection中找到mpd，它的位置是net/mpd。许多ADSL modem需要在modem和计算机之间建立一条PPTP隧道，而阿尔卡特SpeedTouch Home正是其中的一种。

首先需要从port完成安装，然后才能配置mpd来满足您的需要，并完成服务商的配置。port会把一系列包括了详细注解的配置文件实例放到PREFIX/etc/mpd/。注意，这里的PREFIX表示ports安装的目录，默认情况下，应该是/usr/local/。关于配置mpd的完整说明，会以HTML格式随port一起安装。这些文件将放在PREFIX/share/doc/mpd/。下面是通过mpd连接ADSL服务的一个简单例子。配置被分别放到了两个文件中，第一个是mpd.conf：

```
default:
```

```

load adsl

adsl:
    new -i ng0 adsl adsl
    set bundle authname username ❶
    set bundle password password ❷
    set bundle disable multilink

    set link no pap acfcomp protocomp
    set link disable chap
    set link accept chap
    set link keep-alive 30 10

    set ipcp no vjcomp
    set ipcp ranges 0.0.0.0/0 0.0.0.0/0

    set iface route default
    set iface disable on-demand
    set iface enable proxy-arp
    set iface idle 0

    open

```

❶ *username*用来向您的ISP进行验证.

❷ *password*用来向您的ISP进行验证.

*mpd.links*包含连接的信息:

```

adsl:
    set link type pptp
    set pptp mode active
    set pptp enable originate outcall
    set pptp self 10.0.0.1 ❶
    set pptp peer 10.0.0.138 ❷

```

❶ 运行*mpd*的主机的IP地址.

❷ ADSL modem的IP地址.Alcatel SpeedTouch Home 默认的是10.0.0.138.

初始化连接:

```
# mpd -b adsl
```

您可以通过以下命令查看连接状态:

```
% ifconfig ng0
ng0: flags=88d1<UP,POINTOPOINT,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1500
    inet 216.136.204.117 --> 204.152.186.171 netmask 0xffffffff

```

使用*mpd*连接ADSL服务是推荐的方式.

23.6.3 使用pptpclient

也可以使用net/pptpclient连接其它的PPPoA.

为了使用net/pptpclient连接DSL服务,需要安装port或package并编辑/etc/ppp/ppp.conf.您需要有root权限以进行这两项操作.以下是ppp.conf中的一个示例项.参考ppp的联机手册ppp(8),以获取更多有关ppp.conf 选项的信息.

```
adsl:
set log phase chat lcp ipcp ccp tun command
set timeout 0
enable dns
set authname username ❶
set authkey password ❷
set ifaddr 0 0
add default HISADDR
```

❶ The username of your account with the DSL provider.

❷ The password for your account.

警告: 由于您必须将帐号密码以明文的方式放入ppp.conf 您应该确保没有任何人能看到此文件的内容.以下一系列命令将会确保此文件只对root用户可读.参考chmod(1)和chown(8) 的联机手册以获得更多信息.

```
# chown root:wheel /etc/ppp/ppp.conf
# chmod 600 /etc/ppp/ppp.conf
```

以下将为到DSL路由器的会话打开一个tunnel. 以太网DSL modem有一个设置的局域网IP地址. 以Alcatel SpeedTouch Home为例,这个地址是10.0.0.138.路由器的文档应该会告诉您它使用地址.执行以下命令以打开tunnel并开始会话:

```
# pptp address adsl
```

提示: 您应该在命令的最后加上("&")号,否则pptp 无法返回到命令行提示符.

要创建一个tun虚拟设备用于进程pptp 和ppp 之间的交互.一旦您返回到了命令行,或者pptp 进程确认了一个连接,您可以这样检查tunnel设备:

```
% ifconfig tun0
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
    inet 216.136.204.21 --> 204.152.186.171 netmask 0xffffffff00
    Opened by PID 918
```

如果您无法连接,一般可以通过telnet或者web浏览器检查路由器(modem)的配置. 如果依旧无法连接,您应该检查pptp的输出及ppp的日志文件/var/log/ppp.log 以获得线索.

23.7 使用SLIP

Originally contributed by Satoshi Asami. With input from Guy Helmer 和Piero Serini.

23.7.1 设置SLIP客户端

下面是在静态主机网络上配置FreeBSD 机器使用SLIP 的方法。对于动态主机名分配(您的地址会随每次拨号而不同)，您可能需要稍复杂一些的设置。

首先，您需要确认调制解调器所连接的串口。许多人会设置一个符号连接，例如`/dev/modem`，用以指向实际的设备名，`/dev/cuaaN` (或在FreeBSD 6.X 下是`/dev/cuadN`)。这样您就可以对实际的设备名进行抽象，以备调制解调器换到其他串口时方便调整之用。不然，在系统中修改一大堆`/etc` 下的文件以及`.kermrc` 将是非常麻烦的事情！

注意：`/dev/cuaa0` (or `/dev/cuad0` under FreeBSD 6.X) is COM1, `cuaa1` (or `/dev/cuad1`) is COM2, etc.

确保您的内核文件包含以下内容：

```
device    sl
```

对于FreeBSD 4.X，则是：

```
pseudo-device    sl        1
```

这包含在GENERIC内核,所以这应该不会是个问题,除非您已经删除了它。

23.7.1.1 只需做一次的事情

1. 把您本地网络上的机器、网关以及域名服务器，都加入到`/etc/hosts` 文件中。我们的是下面这个样子：

```
127.0.0.1          localhost loghost
136.152.64.181     water.CS.Example.EDU water.CS water
136.152.64.1       inr-3.CS.Example.EDU inr-3 slip-gateway
128.32.136.9       ns1.Example.EDU ns1
128.32.136.12      ns2.Example.EDU ns2
```

2. 在FreeBSD 5.0 之前的版本中，请务必确保`/etc/host.conf` 中的`hosts` 在`bind` 之前出现。从FreeBSD 5.0 开始，系统转而使用`/etc/nsswitch.conf` 文件，请确认在这个文件中`hosts` 一行里，`files` 出现在`dns` 之前。如果没有这些参数，可能会发生很奇怪的事情。
3. 编辑`/etc/rc.conf`.

1. 编辑以下这行设置主机名(hostname):

```
hostname="myname.my.domain"
```

应该用您主机的Internet全名代替。

2. 改变这一行以指明默认的路由:

```
defaultrouter="NO"
```

改为:

```
defaultrouter="slip-gateway"
```

4. 创建文件/etc/resolv.conf,写入以下内容:

```
domain CS.Example.EDU
nameserver 128.32.136.9
nameserver 128.32.136.12
```

正如您看到的, 这些行设置了域名服务器.当然,实际的域名和IP地址取决于您的环境.

5. 设置root和toor的密码(其它任何没有密码的帐号).
6. 重启计算机,然后确认使用了正确的主机名.

23.7.1.2 创建一个SLIP连接

1. 在命令提示符之后输入slip 进行拨号, 输入您的机器名和口令。具体需要输入什么, 与您的环境密切相关。如果使用Kermit, 则可以使用类似下面的脚本:

```
# kermit setup
set modem Hayes
set line /dev/modem
set speed 115200
set parity none
set flow rts/cts
set terminal bytesize 8
set file type binary
# The next macro will dial up and login
define slip dial 643-9600, input 10 =>, if failure stop, -
output slip\x0d, input 10 Username:, if failure stop, -
output silvia\x0d, input 10 Password:, if failure stop, -
output ***\x0d, echo \x0aCONNECTED\x0a
```

当然, 您还需要修改用户名和口令来满足实际需要。完成这些操作之后, 只需在Kermit 提示符之后输入slip 就可以连接了。

注意: 将密码以纯文本的形式存放在文件系统无论如何都是个坏主意。请考虑这样做的风险。

2. 在这里退出Kermit (也可以用Ctrl-z 将其挂起), 以root 用户键入:

```
# slattach -h -c -s 115200 /dev/modem
```

如果您能ping通路由器另一端的主机,就是连接好了! 如果不行, 您可以使用-a选项代替-c作为slattach的参数.

23.7.1.3 关闭连接

按下面的步骤做:

```
# kill -INT 'cat /var/run/slattach.modem.pid'
```

来杀掉`slattach`。切记上述操作只有以`root` 身份才能完成。接下来回到`kermit` (如果之前是将它挂起了, 则使用`fg`) 并退出(`q`)。

在`slattach(8)` 联机手册中提到, 必须使用`ifconfig sl0 down` 才能将接口标记为关闭, 但和这样做似乎没有什么区别。(`ifconfig sl0` 仍然报告同样的东西。)

有时, 您的`modem` 可能会拒绝挂断。这种情况下, 只需重新启动`kermit` 并再次退出它就可以了。一般来说试二次就可以了。

23.7.1.4 问题解答

如果还不行, 尽管发邮件到`freebsd-net` (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-net>) 邮件列表来提问。常见的问题包括:

- 执行`slattach`时不使用`-c`和`-a`选项(这应该不是关键的,但有些用户报告这样做解决了问题.)
- 使用`sl0`替换`sl0` (在一些字体下很难看出不同).
- 试试`ifconfig sl0`来查看您的接口状态.例如,您可以这样做:

```
# ifconfig sl0
sl0: flags=10<POINTOPOINT>
    inet 136.152.64.181 --> 136.152.64.1 netmask ffffffff00
```

- 如果在使用`ping(8)` 时得到了`no route to host` 这样的提示, 则说明您的路由表可能有问题。可以用`netstat -r` 命令来显示当前的路由:

```
# netstat -r
Routing tables
Destination      Gateway            Flags      Refs      Use  IfaceMTU    Rtt      Netmasks:

(root node)
(root node)

Route Tree for Protocol Family inet:
(root node) =>
default          inr-3.Example.EDU UG          8    224515  sl0 -        -
localhost.Exampl localhost.Example. UH          5     42127  lo0 -        0.438
inr-3.Example.ED water.CS.Example.E UH          1         0  sl0 -        -
water.CS.Example localhost.Example. UGH         34  47641234 lo0 -        0.438
(root node)
```

前述的例子来自于一个非常繁忙的系统. 您系统上的这些数字会因网络活动的不同而改变.

23.7.2 设置SLIP服务器

本文提供了在FreeBSD 上设置SLIP 服务, 也就是如何配置您的系统, 使其能在远程SLIP 客户端登录时自动地开启连接的建议。

23.7.2.1 前提条件

这一节本身就是非常技术性的, 所以要求有一定的背景知识. 本节假定您熟悉TCP/IP网络协议, 特别是网络和结点寻址, 网络地址掩网, 划分子网, 路由, 路由协议(比如RIP). 在一个拨号服务器上配置SLIP需要这些概念性的知识. 如果您不熟悉它们, 请先阅读Craig Hunt的**TCP/IP 网络管理** 由O'Reilly & Associates, Inc. 出版(ISBN号为0-937175-82-X), 或者Douglas Comer有关TCP/IP 协议的书籍.

此外还假定您已经配置好了您的调制解调器以及相应的系统文件, 以允许通过调制解调器进行登录. 如果您还没有为此配置好系统, 请参见第22.4 节 以了解关于如何进行拨号服务的配置. 您可能也会想看一看sio(4) 的联机手册, 以了解关于串口设备驱动的进一步信息, 以及ttys(5)、gettytab(5)、getty(8) & init(8) 上关于怎样配置系统来接受来自调制解调器的登录请求的具体情况, 还有stty(1) 以了解关于设置串口参数(例如clocal 表示串口直联) 等.

23.7.2.2 快速浏览

使用FreeBSD作为SLIP服务器, 在典型配置时, 它是这样工作的: 一个SLIP客户拨号并以专用的login ID登录到FreeBSD SLIP服务器系统. 这个用户使用/usr/sbin/sliplogin 作为shell. sliplogin程序在文件/etc/sliphone/slip.hosts中查找这个用户的项, 如果找到了匹配项, 就将串行线连接到一个可用的SLIP接口, 然后运行shell脚本/etc/sliphone/slip.login 以配置SLIP接口.

23.7.2.2.1 一个SLIP服务器登录的例子

例如, 如果一个SLIP用户的ID是Shelmerg, 在/etc/master.passwd中Shelmerg的项如下的所示:

```
Shelmerg:password:1964:89::0:0:Guy Helmer - SLIP:/usr/users/Shelmerg:/usr/sbin/sliplogin
```

Shelmerg登录时, sliplogin在文件/etc/sliphone/slip.hosts中搜索与用户ID匹配的行; 如下所示:

```
Shelmerg      dc-slip sl-helmer      0xfffffc00      autocomp
```

sliplogin找到这条匹配行, 并将串行线与另一个可用的SLIP接口连起来, 然后执行/etc/sliphone/slip.login脚本:

```
/etc/sliphone/slip.login 0 19200 Shelmerg dc-slip sl-helmer 0xfffffc00 autocomp
```

如果一切顺利/etc/sliphone/slip.login 将在sliplogin绑定的SLIP 接口上发出ifconfig (前述的例子中是SLIP 接口0, 这是slip.login 的第一个参数), 以设置本地IP 地址(dc-slip)、远程IP 地址(sl-helmer)、这一SLIP 接口的子网掩码(0xfffffc00), 以及任何其他标志(autocomp)。如果发生错误, sliplogin 通常会通过syslogd 的daemon facility 记下有用的信息, 前者会把这些信息保存到/var/log/messages (参见syslogd(8) 和syslog.conf(5) 以及/etc/syslog.conf 的联机手册, 以了解syslogd 在记录什么, 以及这些内容将被记在哪里)。

23.7.2.3 内核配置

FreeBSD 的默认内核(GENERIC) 提供了SLIP (sl(4)) 支持; 使用定制的内核时, 您必须把下面的设置加入到配置文件:

```
device    sl
```

在FreeBSD 4.X 下, 则是:

pseudo-device sl 2

注意: 行末的数字表示允许同时使用的最大SLIP 连接数。从FreeBSD 5.0 开始, sl(4) 驱动具有了“自动克隆” 的能力, 因而不需要这一设置。

默认情况下, 您的FreeBSD 计算机不会转发包。如果您希望将FreeBSD SLIP 服务器作为路由器使用, 就需要修改/etc/rc.conf 文件, 并加入一项将gateway_enable 变量设为YES 的设制。

接下来需要重新启动以便使新设置生效。

请参见第8 章 以了解如何配置FreeBSD 内核, 并获得在重新配置内核方面的指导。

23.7.2.4 Sliplogin配置

正如先前所提到的, /etc/sliphome目录有三个文件构成/usr/sbin/sliplogin的配置(参考sliplogin的联机手册sliplogin(8)): slip.hosts, 定义SLIP用户及有关IP地址; slip.login, 一般只配置SLIP接口; 文件slip.logout(可选的), 串行连接终止时, 撤消slip.login所做的修改。

23.7.2.4.1 slip.hosts Configuration

/etc/sliphome/slip.hosts里的每行包含至少四个元素,元素之间由空格隔开:

- SLIP用户的登录ID
- SLIP连接的本地地址(指SLIP服务器)
- SLIP连接的远程地址
- 网络掩网

本地和远程地址可以是主机名(通过文件/etc/hosts或者域名服务解析为IP地址, 在FreeBSD 5.X上这取决于文件/etc/nsswitch.conf的设置; 而在FreeBSD 4.X里,则是/etc/host.conf),网络掩网可以是一个能通过文件/etc/networks解析的名字.在一个样例系统中, /etc/sliphome/slip.hosts是这样的:

```
#
# login local-addr      remote-addr      mask          opt1    opt2
#                               (normal,compress,noicmp)
#
Shelmerg  dc-slip       sl-helmerg     0xfffffc00    autocomp
```

在这行末尾是一或多个选项:

- normal —— 不压缩报头
- compress —— 压缩报头
- autocomp —— 如果远程端允许,压缩报头
- noicmp —— 禁用ICMP数据包(这样就会丢弃所有的“ping”数据包,不占用您的带宽)

对SLIP连接的本地及远程地址的选择取决是您准备在SLIP服务器上使用TCP/IP 子网还是使用“ARP代理”(它并不是“真正的”ARP代理,而是我们在本节用于介绍的术语). 如果您不能确定选择何种方式或者如何分配地址,请参考“前提条件”(第23.7.2.1 节)里列出的TCP/IP书籍或者向您的IP网络管理员请教。

如果您准备为您的SLIP客户使用一个独立的子网, 您需要先从分配得到的网络号中取出一个子网号然后再在这个子网里给每个SLIP客户分配IP地址. 然后您还需要通过SLIP服务器在最近的IP路由器上配置一个指向SLIP子网的静态路由.

如果您要使用“代理ARP”的方式, 您需要从SLIP服务器的以太网中为每个SLIP客户分配IP地址, 还必须修改/etc/sliphome/slip.login 和/etc/sliphome/slip.logout脚本以使用arp(8)来管理proxy-ARP在服务器ARP表中的项.

23.7.2.4.2 slip.login Configuration

典型的/etc/sliphome/slip.login 如下所示:

```
#!/bin/sh -
#
#      @(#)slip.login  5.1 (Berkeley) 7/1/90

#
# generic login file for a slip line.  sliplogin invokes this with
# the parameters:
#      1      2      3      4      5      6      7-n
#  slipunit  ttyspeed loginname local-addr remote-addr mask opt-args
#
/sbin/ifconfig sl$1 inet $4 $5 netmask $6
```

这个slip.login脚本仅仅为带有相应本地及远程地址和掩码的SLIP接口执行ifconfig.

如果您决定使用“ARP代理”方式(而非为您的SLIP客户使用独立的子网), 您的/etc/sliphome/slip.login 应该是这样:

```
#!/bin/sh -
#
#      @(#)slip.login  5.1 (Berkeley) 7/1/90

#
# generic login file for a slip line.  sliplogin invokes this with
# the parameters:
#      1      2      3      4      5      6      7-n
#  slipunit  ttyspeed loginname local-addr remote-addr mask opt-args
#
/sbin/ifconfig sl$1 inet $4 $5 netmask $6
# Answer ARP requests for the SLIP client with our Ethernet addr
/usr/sbin/arp -s $5 00:11:22:33:44:55 pub
```

slip.login新加的行arp -s \$5 00:11:22:33:44:55 pub在SLIP服务器的ARP表中加入了一个表项. 这个ARP项使得每当这个以太网上的其它IP节点对SLIP客户端IP地址进行ARP请求时, SLIP服务器会以自己的以太网MAC地址作为回应.

当使用以上的例子时, 一定要将以太网MAC地址(00:11:22:33:44:55)替换成您系统网卡的MAC地址, 否则“ARP代理”将完全无法工作! 您可以查看netstat -i 输出结果以取得以太网MAC地址; 输出的第二行应该是这样:

```
ed0    1500  <Link>0.2.c1.28.5f.4a          191923 0    129457    0    116
```

这行表明这个系统的以太网MAC地址是00:02:c1:28:5f:4a——netstat -i输出的以太网MAC地址必须改成用冒号隔开,并且要单个十六进制数前加上. 这是arp(8)要求的格式;参考arp(8) 的联机手册以获取完整的使用方法。

注意: 在编写/etc/sliphome/slip.login 和/etc/sliphome/slip.logout 时,一定要设置“可执行”(execute)位(换言之, chmod 755 /etc/sliphome/slip.login /etc/sliphome/slip.logout), 否则sliplogin将无法执行它。

23.7.2.4.3 slip.logout 配置

/etc/sliphome/slip.logout并不是必需的(除非您使用了“ARP代理”),如果您准备创建它,这里有一个基本的slip.logout 脚本的例子:

```
#!/bin/sh -
#
#      slip.logout

#
# logout file for a slip line.  sliplogin invokes this with
# the parameters:
#      1      2      3      4      5      6      7-n
#  slipunit ttyspeed loginname local-addr remote-addr mask opt-args
#
/sbin/ifconfig sl$1 down
```

If you are using “proxy ARP”, you will want to have /etc/sliphome/slip.logout remove the ARP entry for the SLIP client:

```
#!/bin/sh -
#
#      @(#)slip.logout

#
# logout file for a slip line.  sliplogin invokes this with
# the parameters:
#      1      2      3      4      5      6      7-n
#  slipunit ttyspeed loginname local-addr remote-addr mask opt-args
#
/sbin/ifconfig sl$1 down
# Quit answering ARP requests for the SLIP client
/usr/sbin/arp -d $5
```

arp -d \$5 将删除由“代理ARP” slip.login 在SLIP 客户程序登录时所生成的ARP 项。

再次强调: 建立/etc/sliphome/slip.logout 之后,一定要设置可执行位(也就是说, chmod 755 /etc/sliphome/slip.logout)。

23.7.2.5 路由考虑

如果没有使用“代理ARP”的方法来在您的SLIP 客户机和网络的其余部分(也可能是Internet)之间路由数据包,您可能需要增加离您最近的默认路由器的静态路由,以便通过SLIP 服务器来在SLIP 客户机子网上进行路由。

23.7.2.5.1 静态路由

向您最近的默认路由添加一个静态路由可以说是很麻烦(或者说不可能,如果您没有权限这么做)。如果在您的组织中使用多路由器网络,有些路由器(比如Cisco 和Proton 生产的)不但要配置指向SLIP 子网的路由,而且还需要配置将哪些静态路由传给其它的路由器。所以一些专家意见和问题解答对于使基于静态路由表的路由正常工作很有必要。

23.7.2.5.2 运行GateD®

注意: GateD现在是一个私有软件,无法取得它的源代码(GateD (<http://www.gated.org/>)上有更多的信息). This section only exists to ensure backwards compatibility for those that are still using an older version.

另一种避免静态路由所造成的头疼的方法,是在您的FreeBSD SLIP 服务器上安装GateD,并配置它使用合适的路由协议(RIP/OSPF/BGP/EGP)来告诉其他路由器您的SLIP 子网的存在。您需要编写一个/etc/gated.conf 文件来配置GateD; 这里是FreeBSD SLIP 服务器作者编写的一个例子:

```
#
# gated configuration file for dc.dsu.edu; for gated version 3.5alpha5
# Only broadcast RIP information for xxx.xxx.yy out the ed Ethernet interface
#
#
# tracing options
#
traceoptions "/var/tmp/gated.output" replace size 100k files 2 general ;

rip yes {
    interface sl noripout noripin ;
    interface ed ripin ripout version 1 ;
    traceoptions route ;
} ;

#
# Turn on a bunch of tracing info for the interface to the kernel:
kernel {
    traceoptions remnants request routes info interface ;
} ;

#
# Propagate the route to xxx.xxx.yy out the Ethernet interface via RIP
#

export proto rip interface ed {
    proto direct {
        xxx.xxx.yy mask 255.255.252.0 metric 1; # SLIP connections
```

```

    } ;
} ;

#
# Accept routes from RIP via ed Ethernet interfaces

import proto rip interface ed {
    all ;
} ;

```

上面这个`gated.conf` 示例文件，将把关于SLIP子网`xxx.xxx.yy` 的信息，通过RIP广播到Ethernet上；如果您使用了的Ethernet驱动不是`ed`，则需要把`ed` 改为相应的网络接口。这个例子也配置了将跟踪信息写到`/var/tmp/gated.output` 以提供调试GateD活动的信息；当然，如果GateD工作正常，就可以关闭这些跟踪信息了。您需要把`xxx.xxx.yy` 改成您自己的SLIP子网(一定要同时修改`proto direct` 小节)。

一旦在系统中安装并配置了GateD，就可以告诉FreeBSD启动脚本来运行GateD而不是`routed`了。最简单的办法，是配置`router` 和`router_flags` 两个`/etc/rc.conf` 变量。请参见GateD的联机手册，以了解更多关于命令行参数的信息。

第24章

电子邮件

Original work by Bill Lloyd. Rewritten by Jim Mock.

24.1 概述

“电子邮件”，或通常所说的email，是现今使用最广泛的通信方式之一。本章将对如何在FreeBSD上运行邮件服务，以及如何使用FreeBSD来收发电子邮件作基本的介绍；然而，它并不是一份完整的参考手册，实际上，许多需要考虑的重要事项都没有提及。我们推荐读者阅读附录B中的参考书籍，以获得对于这部分的全面认识。

读完这章，您将了解：

- 那些软件与收发电子邮件有关。
- FreeBSD下的基本**sendmail**配置文件在哪里。
- 本地和远程邮箱之间的区别。
- 如何阻止垃圾邮件制造者非法地使用您的邮件服务器作为转发中继。
- 如何安装和配置用于替代**sendmail**的其他邮件传输代理。
- 如何处理常见的邮件服务器问题。
- 如何使用SMTP和UUCP。
- 如何设置系统使其只能发送邮件。
- 如何在拨号连接时使用邮件。
- 如何配置SMTP验证以增加安全性。
- 如何安装并使用用户邮件代理，如**mutt**来收发邮件。
- 如何从远程的POP或IMAP服务器上下载邮件。
- 如何在进入的邮件上自动地应用过滤器和规则。

阅读本章之前，您需要：

- 正确地配置您的网络连接(第27章)。
- 正确地为您的邮件服务器配置DNS信息(第25章)。
- 知道如何安装第三方软件(第4章)。

24.2 使用电子邮件

邮件交换可以分为5部分。它们是：用户端程序、服务端守护进程、DNS、远程或本地的邮箱、当然，还有邮件主机自己。

24.2.1 用户端程序

这包括一些基于命令行的程序，例如**mutt**、**pine**、**elm**和**mail**，以及类似**balsa**、**xfmail**这样的GUI程序。此外，还有我们更“熟悉的”**WWW**浏览器这样的程序。这些程序简单地通过调用服务守护进程把邮件事务交给本地的“邮件主机”，或者通过**TCP**把邮件发出去。

24.2.2 邮件主机上使用的服务程序

FreeBSD 默认情况下采用**sendmail**，但它也支持为数众多的其它邮件服务程序，这其中包括：

- **exim**;
- **postfix**;
- **qmail**.

邮件服务器后台守护程序通常有两个功能——接收外面发来的邮件和把邮件传送出去。但它不负责使用类似**POP**或**IMAP**这样的协议来帮您阅读邮件，也不负责连接到本地的**mbox**或**Maildir**信箱。您可能需要其它的服务程序来完成这些任务。

警告: 较早版本的**sendmail**有一些严重的安全问题，他们可能导致攻击者从本地和/或远程操作您的电脑。您应该确认自己使用的是最新版本以避免这些问题。另外，也可以从**FreeBSD Ports Collection**来安装其它的**MTA**。

24.2.3 Email 和DNS

域名系统(**DNS**)及其服务程序**named**在email的投递过程当中扮演着很重要的角色。为了能够从您的站点向其它的站点传递邮件，服务程序需要通过**DNS**查找接收邮件的远程站点的位置。类似地，在远程站点向您的主机投递邮件时也会发生这样的查找。

DNS负责将主机名映射为**IP**地址，同时，也需要保存递送邮件时所需要的信息，这些信息称作**MX**记录。**MX** (**M**ail **eX**changer，邮件交换)记录指定了哪个，或哪些主机能够接收特定域下的邮件。如果您没有为主机名或域名设置**MX**记录，则邮件将被直接递交给主机名对应**IP**所在的主机。

您可以通过**host(1)**命令来查找任何域或主机名对应的**MX**记录，如下面的例子所示：

```
% host -t mx FreeBSD.org
FreeBSD.org mail is handled (pri=10) by mx1.FreeBSD.org
```

24.2.4 接收邮件

为您的域接收邮件是通过邮件服务器来完成的。它收集发送给您的域的那些邮件，并保存到**mbox** (存储邮件默认的方法)或**Maildir**格式，这取决于您采用的配置。一旦邮件被保存下来，就可以在本地通过类似**mail(1)**或**mutt**这样的程序，或在远程通过**POP**或**IMAP**这样的协议来读取了。简单地说，如果您只在本地阅读邮件，那就没有必要安装**POP**或**IMAP**服务。

24.2.4.1 通过POP 和IMAP 访问远程的邮件

如果希望在远程访问邮箱，就需要访问POP 或IMAP 服务器。这些协议允许用户从远程方便地访问他们的信箱。尽管POP 和IMAP 都允许用户从远程访问信箱，但IMAP 有很多优点，这包括：

- IMAP 既可以从远程服务器上抓取邮件，也可以把邮件放上去。
- IMAP 支持并发更新。
- IMAP 对于使用低速网络的用户尤为有用，因为它能够让这些用户把邮件的结构下载下去，而无需立即下载整个邮件。它还可以在服务器端执行类似查找这样的操作，以减少客户机和服务器之间的通讯量。

您可以按照下面的步骤来安装和配置POP 或IMAP 服务器：

1. 选择一个最符合需要的IMAP 或POP 服务器。下列POP 和IMAP 服务器是最著名的，而且都有很多成功案例：
 - **qpopper**;
 - **teapop**;
 - **imap-uw**;
 - **courier-imap**;
2. 通过ports collection 安装POP 或IMAP 服务。
3. 根据需要修改/etc/inetd.conf 来加载POP 或IMAP 服务。

警告：此外还应注意的是POP 和IMAP 传递的信息，包括用户名和口令等等，通常都是明文的。这意味着如果您希望加密传输过程中的信息，可能需要考虑使用ssh(1) 隧道。关于如何实施隧道在第14.11.8 节 中进行了详细阐述。

24.2.4.2 操作本地的信箱

信箱可以在邮件服务器本地直接用MUA 来进行操作。这通常是通过**mutt** 或**mail(1)** 这样的用用程序实现的。

24.2.5 邮件服务器

邮件服务器是通过服务器给的一个名字,这也正是它能在您的主机和网络上发送和接收邮件的原因。

24.3 sendmail 配置

作者: Christopher Shumway.

sendmail(8) 是FreeBSD 中的默认邮件传输代理(MTA)。**sendmail** 的任务是从邮件用户代理(MUA) 接收邮件然后根据配置文件的定义把它们送给配置好的的寄送程序。**sendmail** 也能接受网络连接，并且发送邮件到本地邮箱或者发送它到其它程序。

sendmail 使用下列配置文件:

文件名	功能
/etc/mail/access	sendmail 访问数据库文件
/etc/mail/aliases	邮箱别名
/etc/mail/local-host-names	sendmail 接收邮件主机列表
/etc/mail/mailer.conf	邮寄配置程序
/etc/mail/mailertable	邮件分发列表
/etc/mail/sendmail.cf	sendmail 的主配置文件
/etc/mail/virtusertable	虚拟用户和域列表

24.3.1 /etc/mail/access

访问数据库定义了什么主机或者IP 地址可以访问本地邮件服务器和它们是哪种类型的访问。主机可能会列出OK、REJECT、RELAY 或者简单的通过**sendmail** 的出错处理程序检测一个给定的邮件错误。主机默认列出OK, 允许传送邮件到主机, 只要邮件的最后目的地是本地主机。列出REJECT 将拒绝所有的邮件连接。如果带有RELAY 选项的主机将被允许通过这个邮件服务器发送邮件到任何地方。

例24-1. 配置**sendmail** 的访问许可数据库

```
cyberspammer.com      550 We do not accept mail from spammers
FREE.STEALTH.MAILER@  550 We do not accept mail from spammers
another.source.of.spam REJECT
okay.cyberspammer.com OK
128.32                RELAY
```

在上面的例子中我们有5 条记录。与左边列表匹配的发件人受到右边列表动作的影响。前边的两个例子给出了**sendmail** 的出错处理程序检测到的错误代码。当一个邮件与左边列表相匹配时, 这个信息会被打印到远程主机上。下一条记录拒绝来自Internet 上的一个特别主机的邮件another.source.of.spam。接下来的记录允许来自okay.cyberspammer.com 的邮件连接, 这条记录比上面那行cyberspammer.com 更准确。更多的准确匹配使不准确的匹配无效。最后一行允许电子邮件从主机和128.32 开头的IP 地址转发。这些主机将被允许通过这台邮件服务器前往其它邮件服务器发送邮件。

当这个文件被升级的时候, 您必须在/etc/mail/ 运行make 升级数据库。

24.3.2 /etc/mail/aliases

别名数据库包含一个扩展到用户, 程序或者其它别名的虚拟邮箱列表。下面是一些在/etc/mail/aliases 中使用的例子:

例24-2. 邮件别名

```
root: localuser
ftp-bugs: joe,eric,paul
bit.bucket: /dev/null
procmail: "|/usr/local/bin/procmail"
```

这个文件的格式很简单；冒号左边的邮箱名，会被展开成右边的形式。第一个例子简单地将`root`邮箱扩展为`localuser`，之后将继续在别名数据库中进行查找。如果没有找到匹配的记录，则邮件会被发给本地用户`localuser`。第二个例子展示了一个邮件列表。发送到`ftp-bugs`的邮件会被展开成`joe`，`eric`和`paul`这三个邮箱。注意也可以通过`<user@example.com>`这样的形式来指定远程的邮箱。接下来的例子展示了如何把邮件写入到文件中，这个例子中是`/dev/null`。最后一个例子展示了如何将邮件发给一个程序，具体而言是通过UNIX管道发到`/usr/local/bin/procmail`的标准输入。

更新此文件时，您需要在`/etc/mail/`中使用`make`来更新数据库。

24.3.3 /etc/mail/local-host-names

这是一个`sendmail(8)`被接受为一个本地主机名的主机名列表。可以放入任何`sendmail`将从那里收发邮件的域名或主机。例如，如果这个邮件服务器从域`example.com`和主机`mail.example.com`接收邮件，它的`local-host-names`文件，可以看起来象如下这样：

```
example.com
mail.example.com
```

当这个文件被升级，`sendmail(8)`必须重新启动，以便更新设置。

24.3.4 /etc/mail/sendmail.cf

`sendmail`的主配置文件`sendmail.cf`控制着`sendmail`的所有行为，包括从重写邮件地址到打印拒绝远程邮件服务器信息等所有事。当然，作为一个不同的角色，这个配置文件是相当复杂的，它的细节部分已经超出了本节的范围。幸运的是，这个文件对于标准的邮件服务器来说很少需要被改动。

`sendmail`主配置文件可以用`m4(1)`宏定义`sendmail`的特性和行为。它的细节请看`/usr/src/contrib/sendmail/cf/README`。

当这个文件被修改时，`sendmail`必须重新启动以便对新修改生效。

24.3.5 /etc/mail/virtusertable

`virtusertable`映射虚拟域名和邮箱到真实的邮箱。这些邮箱可以是本地的、远程的、`/etc/mail/aliases`中定义的别名或一个文件。

例24-3. 虚拟域邮件映射的例子

```
root@example.com          root
postmaster@example.com    postmaster@noc.example.net
@example.com              joe
```

在上面这个例子中，我们映射了一个域`example.com`。这个文件是按照从上到下，首个匹配的方式来处理的。第一项将`<root@example.com>`映射到本地邮箱`root`。下一项则将`<postmaster@example.com>`映射到位于`noc.example.net`的`postmaster`。最后，如果没有来自`example.com`的匹配，则将使用最后一条映射，它表示将所有的其它邮件发给`example.com`域的某个人。这样，将映射到本地信箱`joe`。

24.4 改变您的邮件传输代理程序

Written by Andrew Boothman. Information taken from e-mails written by Gregory Neil Shapiro.

先前已经提到，FreeBSD 中的**sendmail** 已经安装了您的MTA (邮件传输代理程序)。因此它负责着您的收发邮件的工作。

然而，基于不同的理由，一些系统管理员想要改变他们系统的MTA。这些理由从简单的想要尝试另一个MTA，到需要一个特殊的特性或者package 依赖某个邮寄程序等等。幸运的是，不管是什么理由，FreeBSD 都能容易的改变它。

24.4.1 安装一个新的MTA

对于可用的MTA 您有很多的选择。一个好的出发点是FreeBSD Ports Collection，在那里您能找到很多。当然您可以从任何位置不受任何限制的使用MTA，只要您能让它运行在FreeBSD 下。

开始安装您的新MTA。一旦它被安装，它可以让您有机会决定它是否能满足您的需要和在接管**sendmail** 之前让您有机会配置您的新软件。当完成这些之后，您应该确信安装的新软件不会尝试更改系统的二进制文件例如象/usr/bin/sendmail。除此以外，您的新邮件软件启用之前要已经配置好它。

具体配置请参考您所选择的MTA 软件的配置文档或其它相关资料。

24.4.2 禁用sendmail

用以启动**sendmail** 的流程，在4.5-RELEASE、4.6-RELEASE 以及之后的版本中，存在着十分显著的不同。因此，用于禁用它的方法，也就有许多不同之处。

警告: 如果您打算禁用**sendmail** 的邮件发出服务，保持系统中有一个替代它的、可用的邮件递送系统就非常重要。如果您不这样做的话，类似periodic(8) 这样的系统功能就无法如预期的那样，通过邮件来传送其执行结果。您系统中的许多部分可能都假定有可用的**sendmail**-兼容系统。如果这些应用程序继续使用**sendmail** 的执行文件来发送邮件，而您又禁用了它，则邮件将进入**sendmail** 的非活跃(inactive) 队列，而永远不会被送达。

24.4.2.1 FreeBSD 4.5-STABLE 版本2002/4/4 之前和更早前版本(包括4.5-RELEASE 及更早版本)

输入:

```
sendmail_enable="NO"
```

到/etc/rc.conf 文件。它将停用**sendmail** 接收邮件服务，但是如果/etc/mail/mailer.conf 文件(见下文) 没有被改变，**sendmail** 将仍然可以发送邮件。

24.4.2.2 FreeBSD 4.5-STABLE 版本2002/4/4 之后和以后的版本(包括4.6-RELEASE 及后续版本)

要完全地禁用**sendmail**，包括邮件的发出服务，您就必须将

```
sendmail_enable="NONE"
```

写在/etc/rc.conf 中。

如果您只是希望禁用**sendmail** 的接信服务，则应将

```
sendmail_enable="NO"
```

写到/etc/rc.conf中。不过，即使禁用了接信服务，本地的送信仍将正常工作。关于**sendmail**的启动选项的更多信息，可以在rc.sendmail(8)联机手册中找到。

24.4.2.3 FreeBSD 5.0-STABLE 和更高版本

要彻底禁用包括邮件送出服务在内的所有**sendmail**功能，必须将

```
sendmail_enable="NO"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO"
```

写入/etc/rc.conf。

如果只是想要停止**sendmail**的接收邮件服务，您应该在/etc/rc.conf文件中设置

```
sendmail_enable="NO"
```

更多的有关**sendmail**可用的启动选项，参看rc.sendmail(8)联机手册。

24.4.3 机器引导时运行您的新MTA

您也许有两种方法在机器引导时运行您的新MTA，这个也倚赖您所运行的FreeBSD版本。

24.4.3.1 FreeBSD 4.5-STABLE 版本2002/4/11 以前(包括4.5-RELEASE 及更早版本)

在/usr/local/etc/rc.d/中添加一个以.sh为后缀的脚本文件，并可以用root身份运行。这个脚本应该接受start和stop参数。用如下命令启动这个脚本

```
/usr/local/etc/rc.d/supermailer.sh start
```

您也可以手工启动这个服务。如果想要停止它，系统脚本将使用stop选项，运行如下命令

```
/usr/local/etc/rc.d/supermailer.sh stop
```

您也可以手工停止正在系统运行的服务。

24.4.3.2 FreeBSD 4.5-STABLE 版本2002/4/11 以后(包括4.6-RELEASE 及后续版本)

在FreeBSD较后来的版本，您可以使用上面的方法或者在/etc/rc.conf文件做如下设置

```
mta_start_script="filename"
```

*filename*是您想要在引导时执行的MTA脚本文件的名称。

24.4.4 替换系统默认的邮寄程序sendmail

因为**sendmail** 程序是一个在UNIX 系统下普遍存在的一个标准的软件，一些软件就假定它已经被安装并且配置好。基于这个原因，许多其它的MTA 提供者都提供了兼容**sendmail** 的命令行界面来执行。这使它们象“混入” **sendmail** 一样变的很容易掌握。

因此，如果您使用其它的邮寄程序，您必须确定这个软件是去尝试运行标准的**sendmail** 二进制，就象/usr/bin/sendmail，还是运行您自己选择的替换邮寄程序。幸运的是，FreeBSD 提供了一个系统调用mailwrapper(8)，它能为您做这件工作。

当**sendmail** 安装后被运行，您可以在/etc/mail/mailer.conf 中找到如下行：

```
sendmail /usr/libexec/sendmail/sendmail
send-mail /usr/libexec/sendmail/sendmail
mailq /usr/libexec/sendmail/sendmail
newaliases /usr/libexec/sendmail/sendmail
hoststat /usr/libexec/sendmail/sendmail
purgestat /usr/libexec/sendmail/sendmail
```

这个的意思就是当这些公共命令(例如sendmail 它本身) 运行时，系统实际上调用了**sendmail** 指定的mailwrapper 的副本，它检查mailer.conf 并且运行/usr/libexec/sendmail/sendmail 做为替代。当默认的**sendmail** 功能被调用，系统将很容易的改变实际上运行的二进制文件。

因此如果您想要/usr/local/supermailer/bin/sendmail-compat 替换**sendmail** 被运行，您应该改变/etc/mail/mailer.conf 文件为：

```
sendmail /usr/local/supermailer/bin/sendmail-compat
send-mail /usr/local/supermailer/bin/sendmail-compat
mailq /usr/local/supermailer/bin/mailq-compat
newaliases /usr/local/supermailer/bin/newaliases-compat
hoststat /usr/local/supermailer/bin/hoststat-compat
purgestat /usr/local/supermailer/bin/purgestat-compat
```

24.4.5 最后

一旦做完您想要配置的每件事，您应该杀掉**sendmail** 进程并且启动属于您的新软件的进程，或者简单的重启。重启也将给您机会保证您正确的配置您的系统，在引导的时候自动的运行您新的MTA。

24.5 疑难解答

1. 为什么必须在我的站点的主机上使用FQDN?

您可能会发现主机实际上是在另外一个域里面，例如，如果您是在foo.bar.edu 里，而您要找一台叫mumble 的主机，它在bar.edu 域里，您就必须用完整的域名mumble.bar.edu，而不是用mumble。

传统上，这在BSD BIND resolvers 中是可行的。然而目前随FreeBSD 附带的**BIND** 已不为同一域外提供缩写服务。所以，这个不完整的主机名mumble 必须以mumble.foo.bar.edu 这种形式才能被找到，或者将在根域中搜索它。

这跟以前的处理是不同的，以前版本将会继续寻找mumble.bar.edu 和mumble.edu。如果您想要了解这种方式是否是好，或者它有什么安全方面的漏洞，请参阅RFC 1535 文档。

如果您想要一个好的工作环境，您可以使用如下行：

```
search foo.bar.edu bar.edu
```

替换先前旧的版本：

```
domain foo.bar.edu
```

把这行放在您的/etc/resolv.conf 文件中。然而，请一定要确定这样的搜寻顺序不会造成RFC 1535 里提到的“boundary between local and public administration”问题。

2. sendmail 提示信息mail loops back to myself

下面是sendmail FAQ 中的回答：

我得到了如下的信息：

```
553 MX list for domain.net points back to relay.domain.net
554 <user@domain.net>... Local configuration error
```

我如何解决这个问题？

您已经通过 MX 记录指定把发送给特定的域（例如，domain.net）的邮件被转寄到指定的主机（在这个例子中，relay.domain.net），而这台机器并不认为它自己是 domain.net。请把 domain.net 添加到/etc/mail/local-host-names 文件中 [在 8.10 版之前是 /etc/sendmail.cw]（如果您使用 FEATURE(use_cw_file) 的话）或者在 /etc/mail/sendmail.cf 中添加“Cw domain.net”。

sendmail 的FAQ 可以在<http://www.sendmail.org/faq/> 找到，如果您想要对您的邮件做任何“调整”，则推荐首先看一看它。

3. 我如何在一个拨号主机上运行一个邮件服务？

您想要把局域网上的FreeBSD 主机连接到互连网上，而这台FreeBSD 主机将会成为这个局域网的邮件网关，这个拨号连接不必一直保持在连接状态。

最少有两种方法可以满足您的要求。一种方法就是使用UUCP。

另一种方法是找到一个专职的服务器来为您的域提供副MX 主机服务。例如，如果您公司的域名是example.com，您的互连网服务提供者把example.net 作为您域的副MX 服务：

example.com.	MX	10	example.com.
	MX	20	example.net.

只有一台主机被指定当做您的最终收信主机(在example.com 主机的/etc/mail/sendmail.cf 文件中添加Cw example.com)。

当sendmail 试图分发邮件的时候，它会尝试通过modem 连接到您(example.com)。因为您并不在线，所以总是会得到一个超时的错误。sendmail 将会把邮件发送到副MX 主机，也就是说，您的互连网服务提供者(example.net)。副MX 主机将周期性的尝试连接并发送邮件到您的主机(example.com)。

您也许想要使用下面的这个登录脚本：

```
#!/bin/sh
# Put me in /usr/local/bin/pppmyisp
( sleep 60 ; /usr/sbin/sendmail -q ) &
/usr/sbin/ppp -direct pppmyisp
```

如果您想要为一个用户建立一个分开登录的脚本，您可以使用 `sendmail -qRexample.com` 替换上面的脚本。这样将使所有的邮件按照您的 `example.com` 队列立即被处理。

更深入的方法可以参考下面这段：

这段信息是从 FreeBSD Internet 服务提供商的邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-isp>) 拿来的。

- > 我们为用户提供副 **MX** 主机服务。用户每天都会上线好几次
- > 并且自动把信件取回主 **MX** 主机
- > (当有他们的邮件时我们并没有通知他们)。
- > 我们的 **mailqueue** 程序每 30 分钟清一次邮件队列。那段时间他们
- > 就必须上线 30 分钟以确保他们的信件送达他们的主 **MX** 主机。
- >
- > 有任何指令可以用 **sendmail** 寄出所有邮件么？
- > 普通用户在我们的机器上当然没有 **root** 权限。

在 `sendmail.cf` 的 “**privacy flags**” 部分，有这样的设定
`Opgoaway,restrictqrun`

移除 `restrictqrun` 可以让非 **root** 用户启动队列处理的程序。
您可能也要重新安排您的 **MX** 设定。我们是用户的 **MX** 主机，
而且我们还设定了这个：

```
# If we are the best MX for a host, try directly instead of generating # local config error.
OwTrue
```

这样的话远程机器会直接把信送给您，而不会尝试连接您的用户的机器。
然后您就可以把邮件发送到您的用户。这个设定只对
“主机” 有效，所以您必须让您的用户在 **DNS** 中把他们的邮件主机设置为
“**customer.com**” 或者
“**hostname.customer.com**”。只要为 “**customer.com**” 在 **DNS**
里添加一个 **A** 记录就可以了。

4. 为什么当我发送邮件到其它主机总是有 **Relaying Denied** 出错信息？

默认的 FreeBSD 安装中，**sendmail** 会配置为只发送来自它所在主机上的邮件。例如，如果有可用的 **POP** 服务器，则用户将可以从学校、公司或其他什么地方检查邮件，但他们仍然无法从远程直接发送邮件。通常，在几次尝试之后，**MAILER-DAEMON** 将发出一封包含 **5.7 Relaying Denied** 错误信息的邮件。

有很多方法可以避免这种现象。最直截了当的方法是把您的 **ISP** 的地址放到 `/etc/mail/relay-domains` 文件中。完成这项工作的简单的方法是：

```
# echo "your.isp.example.com" > /etc/mail/relay-domains
```

建立或编辑这个文件以后您必须重新启动 **sendmail**。如果您是一个管理员并且不希望在本地上发送邮件，或者想要在其它的机器甚至其它的 **ISP** 上使用一个客户端系统，这个方法是很方便的。如果您仅有一到两个邮

件帐户它也非常有用。如果有大量的地址需要添加，您可以很简单的使用您喜欢的文本编辑器打开这个文件添加域名，每行一个：

```
your.isp.example.com
other.isp.example.net
users-isp.example.org
www.example.org
```

现在邮件可以通过您的系统传送，这个列表中存在的主机(前提是用户在您的系统上已经有一个帐户) 将可以成功的发送。这是一个允许正常的远程用户从您的系统发送邮件，并且阻止其它非法用户通过您系统发送垃圾邮件的好方法。

24.6 高级主题

下面这节将介绍邮件配置和为整个域安装邮件。

24.6.1 基本配置

在邮箱外，只要您设置/etc/resolv.conf 或者运行您自己的名字服务器，您就可以发送邮件到外部的主机。如果您想要您的邮件发送给某个特定的MTA(例如，**sendmail**) 在您的FreeBSD 主机上，有两个方法：

- 运行您自己的域名服务器和您自己的域。例如，FreeBSD.org
- 获得直接分发给您主机的邮件。您可以直接使用您当前的DNS 名称。例如，example.FreeBSD.org。

不管您选择上面那种方法，为了直接在您的主机上发送邮件，必须有一个静态的IP 地址(不是象PPP 拨号一样的动态地址)。如果您在防火墙后面，它必须让SMTP 协议通过。如果您想要在您的主机上直接的收取邮件，您必须确定两件事：

- 确定在您DNS 中的MX 记录(最小编号的)指向您的IP 地址。
- 确定在您DNS 中的MX 记录没有禁止您的主机。

上面的每条记录都允许您在您的主机直接接收邮件。

试试这个：

```
# hostname
example.FreeBSD.org
# host example.FreeBSD.org
example.FreeBSD.org has address 204.216.27.XX
```

如果您看到这些，则直接发往<your login@example.FreeBSD.org> 应该已经可以正常工作了(假设sendmail 已经在example.FreeBSD.org 上正确启动了)。

如果您看到这些：

```
# host example.FreeBSD.org
example.FreeBSD.org has address 204.216.27.XX
```


`example.FreeBSD.org` mail is handled (pri=10) by `hub.FreeBSD.org`

所有发送到主机(`example.FreeBSD.org`)的邮件在相同的用户名下将会被`hub`终止的收集,而不是直接发送到您的主机。

上面的信息是通过您的DNS服务器来处理的。支持邮件路由信息的DNS记录是**邮件交换**记录。如果MX记录不存在,邮件将通过它自己的IP地址被直接的发送到主机。

`freefall.FreeBSD.org`的MX记录如下所示:

```
freefall MX 30 mail.crl.net
freefall MX 40 agora.rdrop.com
freefall MX 10 freefall.FreeBSD.org
freefall MX 20 who.cdrom.com
```

正如您说看到的, `freefall` 有很多MX记录。最小编号的MX记录是直接接收邮件的主机。如果因为一些原因它不可用,其它(有时会访问“backup MXes”)接收信息将会暂时接替并做临时的排列。

为了有效的使用交换式MX站点,应当从您的机器上分离一些Internet连接。您的ISP 或者其它友好的站点可以没有任何问题的为您提供这个服务。

24.6.2 Mail for Your Domain

为了设置一个“邮件主机”(又称邮件服务器)您必须要把许多邮件发送到与它相连的几个工作站中。基本上,您想要“要求”在您域的每个主机的所有邮件(在这个例子里是`*.FreeBSD.org`)转向到您的邮件服务器,从而使您的用户可以在主邮件服务器里接收他们的邮件。

要使工作最简单,带有同样**用户名**的帐户应该同时存在于两台机器上。使用`adduser(8)`来这样做。

您将使用的邮件主机必须为每个工作站指定一个邮件交换。您可以在DNS中这样配置:

```
example.FreeBSD.org A 204.216.27.XX ; Workstation
MX 10 hub.FreeBSD.org ; Mailhost
```

无论A记录指向哪,这将为工作站重新定位到邮件主机。邮件将被发送到MX主机。

您不能自己这样做除非您运行着一个DNS服务器。如果不是这样,或者不能运行您自己的DNS服务器,告诉您的ISP或者给您提供DNS服务的人。

如果您正在使用虚拟邮件主机,下面的信息将会对您有用。在这个例子里,我们假定您有一个客户并且他有自己的域,这个例子中是`customer1.org`,您要把`customer1.org`所有的邮件发送到您的邮件主机`mail.myhost.com`。您的DNS记录应该是这样:

```
customer1.org MX 10 mail.myhost.com
```

您不需要有个A记录,如果您只为域`customer1.org`处理邮件。

注意: 必须清楚`customer1.org`将不能工作,除非存在一个A记录。

最后一件您必须要做的事是告诉**sendmail**接受邮件的是什么域和(或)主机名。这里有好几种方法。下面方法可以任选一种:

- 添加您的主机到/etc/mail/local-host-names 文件中，如果您使用的是FEATURE(use_cw_file)。如果您使用**sendmail** 8.10 或者更高版本，文件是/etc/sendmail.cw。
- 添加一行Cwyour.host.com 到您的/etc/sendmail.cf 或/etc/mail/sendmail.cf 文件，如果您使用**sendmail** 8.10 或者更高版本。

24.7 SMTP 与UUCP

sendmail 的配置，在FreeBSD 中已经配置好为您的站点直接连接Internet。如果站点希望他们的邮件通过UUCP 交换，则必须安装其它的**sendmail** 配置文件。

手工的配置/etc/mail/sendmail.cf 是一个高级主题。**sendmail** 8 版本通过m4(1) 预处理生成一个配置文件，实际上这个配置发生在一个比较高的抽象层。m4(1) 配置文件可以在/usr/src/usr.sbin/sendmail/cf 下找到。

如果您没有在系统上安装全部源码，则可以从单独的压缩文件中提取**sendmail** 配置文件。假定您的FreeBSD 源码CDROM 已经被mount:

```
# cd /cdrom/src
# cat scontrib.?? | tar xzf - -C /usr/src/contrib/sendmail
```

这个提取只有几百K 字节。cf 目录中的README 文件能够为您提供一个到m4(1) 配置的基本的介绍。

最好的支持UUCP 传送的方法是使用mailertable 的特点。建立一个资料库让**sendmail** 可以使用它自己的路由决策。

首先，您必须建立您自己的.mc 文件。/usr/src/usr.sbin/sendmail/cf/cf 目录包含一些例子。假定您已经命名自己的文件叫做foo.mc，您要做的只是把它转换成一个有效的sendmail.cf:

```
# cd /usr/src/usr.sbin/sendmail/cf/cf
# make foo.cf
# cp foo.cf /etc/mail/sendmail.cf
```

一个典型的.mc 文件看起来可能象这样:

```
VERSIONID('Your version number') OSTYPE(bsd4.4)

FEATURE(accept_unresolvable_domains)
FEATURE(nocanonify)
FEATURE(mailertable, 'hash -o /etc/mail/mailertable')

define('UUCP_RELAY', your.uucp.relay)
define('UUCP_MAX_SIZE', 200000)
define('confDONT_PROBE_INTERFACES')

MAILER(local)
MAILER(smtp)
MAILER(uucp)

Cw    your.alias.host.name
Cw    youruucpnodename.UUCP
```

`accept_unresolvable_domains`、`nocanonify` 和 `confDONT_PROBE_INTERFACES` 特性将避免在传送邮件时使用DNS的机会。`UUCP_RELAY` 项是支持UUCP 传送所必须的。简单的放入一个Internet 上可以处理UUCP 虚拟域地址的主机名。通常，您在这里填入您ISP 邮件的回复处。

一旦您做完这些，您还需要这个`/etc/mail/mailertable` 文件。如果您只有一个用来传递所有邮件的对外通道的话，以下的文件就足够了：

```
#
# makemap hash /etc/mail/mailertable.db < /etc/mail/mailertable
.
                                uucp-dom:your.uucp.relay
```

一个更复杂点的例子象这样：

```
#
# makemap hash /etc/mail/mailertable.db < /etc/mail/mailertable
#
horus.interface-business.de    uucp-dom:horus
.interface-business.de        uucp-dom:if-bus
interface-business.de          uucp-dom:if-bus
.heep.sax.de                   smtp8:%1
horus.UUCP                     uucp-dom:horus
if-bus.UUCP                    uucp-dom:if-bus
.                               uucp-dom:
```

头三行处理域地址邮件，不应该被传送出默认的路由，而由某些UUCP 邻居取代的特殊情况，这是为了走“捷径”。下一行处理本地网的邮件让它可以使用SMTP 来传送。最后，UUCP 邻居提起。UUCP 虚拟域的记载，允许一个 `uucp-neighbor !recipient` 推翻默认规则。最后一行则以一个单独的句点最为结束，以UUCP 传送到提供您所有的邮件网关的UUCP 邻居。所有在 `uucp-dom:` 关键字里的节点名称必须是有效的UUCP 邻居，您可以用 `uuname` 去确认。

提醒您这个文件在使用前必须被转换成DBM 数据库文件。最好在 `mailertable` 最上面用注解写出命令行来完成这个工作。当您每次更换您的 `mailertable` 后您总是需要执行这个命令。

最后提示：如果您不确定某个特定的路径可用，记得把 `-bt` 选项加到 `sendmail`。这会将 `sendmail` 启动在地址检测模式。只要按下 `3,0`，接着输入您希望测试的邮件路径位置。最后一行告诉您使用邮件代理程序，代理程序会通知目的主机以及(可能转换) 地址。要离开此模式请按 `Ctrl+D`。

```
% sendmail -bt
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
> 3,0 foo@example.com
canonify          input: foo @ example . com
...
parse            returns: $# uucp-dom $@ your.uucp.relay $: foo < @ example . com . >
> ^D
```

24.8 只发送邮件的配置

Contributed by Bill Moran.

许多时候，可能只希望通过转发服务器来发送邮件。典型的情况包括：

- 使用桌面机，但希望通过类似**send-pr(1)** 这样的程序发送邮件。这样就需要使用ISP 的邮件转发服务器。
- 不在本地处理邮件的服务器，但它需要把邮件交给转发服务器来进行处理。

几乎任何一个MTA 都能够胜任这样的工作。然而不幸的是，要把一个全功能的MTA 正确地配置为只把邮件交给其他服务器是一件很困难的事情。使用**sendmail** 以及**postfix** 这样的程序，多少有些杀鸡用牛刀的感觉。

此外，如果您使用典型的Internet 访问服务，您的协议可能会包含禁止运行“邮件服务器” 的条款。

满足这些需要最简单的办法是安装**mail/ssmtp** port。以root 身份执行下面的命令：

```
# cd /usr/ports/mail/ssmtp
# make install replace clean
```

一旦装好，**mail/ssmtp** 就可以用四行**/usr/local/etc/ssmtp/ssmtp.conf** 来配置：

```
root=yourrealemail@example.com
mailhub=mail.example.com
rewriteDomain=example.com
hostname=_HOSTNAME_
```

请确认您为root 使用了真实的电子邮件地址。用您的ISP 提供的外发邮件转发服务器名称，替换掉**mail.example.com** (某些ISP 可能将其称为“外发邮件服务器” 或“SMTP 服务器”)。

接下来需要确认禁用了**sendmail**，包括邮件发出服务在内。请参见第24.4.2 节 以了解进一步的细节。

mail/ssmtp 也提供了一些其他选项。请参见在**/usr/local/etc/ssmtp** 中的示例配置，或者**ssmtp** 的联机手册来得到一些例子和更多的其他信息。

以这种方式配置**ssmtp**，能够让您计算机上的任何需要发送邮件的软件都正常运转，而不必冒违反ISP 的使用政策，或使您的电脑被劫持用于发送垃圾邮件的风险。

24.9 拨号连接时使用邮件传送

如果您有静态的IP 地址，就应该不用修改任何默认的配置。将主机名设置为分配给您的Internet 名称，其他的事情**sendmail** 都会替您做好。

如果您的IP 地址是动态分配的，并使用PPP 连接拨入Internet，则您可能会从ISP 的邮件服务器上得到一个信箱。这里我们假设您的ISP 的域名是**example.net**，您的用户名是**user**，您把自己的机器称作**bsd.home**，而您的ISP 告诉您可以使用**relay.example.net** 来转发邮件。

为了从邮箱收取邮件，需要安装一个收信代理。**fetchmail** 是一个能够支持许多种不同协议的不错的选择。这个程序可以通过**package** 或**Ports Collection (mail/fetchmail)** 来安装。通常，您的ISP 会提供POP。如果您使用用户PPP，您还可以在Internet 连接建立时自动地抓取邮件，这可以通过在**/etc/ppp/ppp.linkup** 中增加如下的项来实现：

```
MYADDR:
!bg su user -c fetchmail
```

如果您正使用**sendmail** (如下所示) 来为非本地用户传送邮件，则可能需要让**sendmail** 在您的Internet 连接建立时立即传送邮件队列。要完成这项工作，应该把下面的命令放到**/etc/ppp/ppp.linkup** 中的**fetchmail** 之后

```
!bg su user -c "sendmail -q"
```

假设您在`bsd.home`上有一个`user`用户。在`bsd.home`上的`user`主目录中创建一个`.fetchmailrc`文件:

```
poll example.net protocol pop3 fetchall pass MySecret
```

因为包含了密码`MySecret`，这个文件应该只有`user`可读。

要使用正确的`from:`头来发送文件，您必须告诉`sendmail`使用`<user@example.net>`而不是`i<user@bsd.home>`。另外，您可能也需要要求`sendmail`通过`relay.example.net`来发送邮件，以便更快地传送它们。

以下的`.mc`文件应该可以满足您的需求:

```
VERSIONID('bsd.home.mc version 1.0')
OSTYPE(bsd4.4)dnl
FEATURE(nouucp)dnl
MAILER(local)dnl
MAILER(smtp)dnl
Cwlocalhost
Cwbsd.home
MASQUERADE_AS('example.net')dnl
FEATURE(allmasquerade)dnl
FEATURE(masquerade_envelope)dnl
FEATURE(nocanonify)dnl
FEATURE(nodns)dnl
define('SMART_HOST', 'relay.example.net')
Dmbsd.home
define('confDOMAIN_NAME', 'bsd.home')dnl
define('confDELIVERY_MODE', 'deferred')dnl
```

如何转换这个`.mc`文件到`sendmail.cf`文件的细节，请参考前面的章节。另外，在更新`sendmail.cf`文件后，不要忘记重启`sendmail`。

24.10 SMTP 验证

作者: *James Gorham*.

在您的邮件服务器上启用SMTP验证有很多好处。SMTP验证可以让`sendmail`多一重安全保障，而且也使得使用不同机器的漫游用户能够使用同一个邮件服务器，而不需要每次都修改它们的邮件客户端配置。

1. 从ports中安装`security/cyrus-sasl`。您可以从`security/cyrus-sasl`找到它。`security/cyrus-sasl`有一系列编译时可选的选项，包括我们将要使用的验证方式等等。请务必选择`pwcheck`。
2. 安装完`security/cyrus-sasl`之后，编辑`/usr/local/lib/sasl/Sendmail.conf` (如果不存在则建立) 并在其中增加:

```
pwcheck_method: passwd
```

这个方法将允许`sendmail`依照您的FreeBSD `passwd`数据库进行验证。这将为每个用户建立一个新用户名设置和口令使用SMTP验证减少麻烦，并且保证登录和邮件口令是相同的。

3. 现在编辑`/etc/make.conf`文件，添加如下行:

```
SENDMAIL_CFLAGS=-I/usr/local/include/sasl -DSASL
SENDMAIL_LDFLAGS=-L/usr/local/lib
SENDMAIL_LDADD=-lsasl
```

这些行将给**sendmail** 合适的配置选项，为在编译时链接到**cyrus-sasl**。确定**cyrus-sasl** 被安装之前重新编译**sendmail**。

4. 重新编译**sendmail** 运行如下命令：

```
# cd /usr/src/usr.sbin/sendmail
# make cleandir
# make obj
# make
# make install
```

如果**/usr/src** 和共享库没有大的变化并且它们都必须可用，**sendmail** 编译应该没有任何问题。

5. **sendmail** 被重新编译和安装后，编辑您的**/etc/mail/freebsd.mc** 文件(或者无论您选择使用的您的哪个.mc 文件。许多管理员选择使用跟**hostname(1)** 一样的唯一的.mc 文件输出)。添加这些行在这个文件：

```
dn1 set SASL options
TRUST_AUTH_MECH('GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN')dn1
define('confAUTH_MECHANISMS', 'GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN')dn1
define('confDEF_AUTH_INFO', '/etc/mail/auth-info')dn1
```

这些选项配置有不同的方法，对于**sendmail** 验证用户。如果您想要使用除**pwcheck** 之外的方法，请参考相关文档。

6. 最后，在**/etc/mail** 运行**make(1)**。它将建立您的新.mc 文件并建立一个.cf 文件命名为**freebsd.cf** (或者您想使用您的其它名字的.mc 文件)。接着使用命令**make install restart**，这将复制文件到**sendmail.cf**，并且正确的重新启动**sendmail**。更多有关这个过程的信息，您可以参考**/etc/mail/Makefile** 文件。

如果所每个步骤都做对了，您应该可以通过您的邮件客户端进入您的登录信息并且传送一个测试信息。更多的分析，设置**sendmail** 的**LogLevel** 到13 并且查看**/var/log/maillog** 中的信息。

您也许希望添加下面的行到**/etc/rc.conf** 文件，这样，服务就会重启之后自动运行：

```
cyrus_pwcheck_enable="YES"
```

这将保证**SMTP_AUTH** 初始化在系统启动时自动运行。

更多的信息，请参看**sendmail** 相关页 **SMTP 验证** (<http://www.sendmail.org/~ca/email/auth.html>)。

24.11 邮件用户代理

Contributed by Marc Silver.

邮件用户代理(MUA) 是一个用于收发邮件的应用程序。更进一步，随着电子邮件的“演化” 并愈发复杂，MUA 在和电子邮件相结合方面变得日趋强大；这为用户提供了更多的功能和灵活性。**FreeBSD** 包含了对于众多邮件用户代理的支持，所有这些都可以通过**FreeBSD Ports Collection** 来轻松安装。用户可以选择类似**evolution** 以及**balsa** 这样的图形界面程序，也可以选择类似**mutt**、**pine** 或**mail** 这样的控制台程序，或者某些大型机构使用的**web** 界面。

24.11.1 mail

mail(1) 是FreeBSD 中默认的邮件用户代理(MUA)。它是一个基于控制台的MUA，提供了所有用于收发文本形式的电子邮件所需的基本功能，虽然它处理附件的能力有限，而且只支持本地的信箱。

虽然**mail** 没有内建的POP 或IMAP 服务器支持，然而这些信箱可以通过类似**fetchmail** 这样的应用程序，来下载到本地的**mbox** 文件中。这一应用程序在本章的稍后部分(第24.12 节) 进行了介绍。

要收发邮件，只需简单地使用**mail** 命令，如下所示：

```
% mail
```

用户保存在**/var/mail** 中的信箱的内容会被**mail** 程序自动地读取。如果信箱是空的，程序会退出并给出一个消息表示没有邮件。一旦读完了信箱，将启动应用程序的界面，并列出邮件。所有的邮件会被自动编号，类似下面的样子：

```
Mail version 8.1 6/6/93.  Type ? for help.
"/var/mail/marcs": 3 messages 3 new
>N  1 root@localhost      Mon Mar  8 14:05  14/510  "test"
  N  2 root@localhost      Mon Mar  8 14:05  14/509  "user account"
  N  3 root@localhost      Mon Mar  8 14:05  14/509  "sample"
```

现在，您通过使用**mail** 的**t** 命令，并给出邮件的编号，就可以看到邮件了。在这个例子中，我们将阅读第一封邮件：

```
& t 1
Message 1:
From root@localhost  Mon Mar  8 14:05:52 2004
X-Original-To: marcs@localhost
Delivered-To: marcs@localhost
To: marcs@localhost
Subject: test
Date: Mon,  8 Mar 2004 14:05:52 +0200 (SAST)
From: root@localhost (Charlie Root)
```

```
This is a test message, please reply if you receive it.
```

正如在上面的例子中所看到的，**t** 键将显示完整的邮件头。要再次查看邮件的列表，可以使用**h** 键。

如果需要回复邮件，也可以使用**mail** 来完成，方法是使用**R** 或**r** 这两个**mail** 键。**R** 键会要求**mail** 只回复发送邮件的人，而**r** 不仅回复发送邮件的人，而且也会将回复抄送给原来邮件的其他接收者。如果需要，也可以在这些命令后面指定邮件的编号。做完这些之后，就可以输入回复了，在邮件的最后应该有一个只有**.** 的行，例如：

```
& R 1
To: root@localhost
Subject: Re: test

Thank you, I did get your email.
.
EOT
```

要发出新邮件，可以使用**m**，后面接收件人的邮件地址。多个收件人之间，应该使用**,** 隔开。接下来需要输入邮件的主题，然后是正文。同样的，在邮件最后需要一个只有**.** 的空行表示结束。

```
& mail root@localhost
Subject: I mastered mail
```

```
Now I can send and receive email using mail ... :)
.
```

```
EOT
```

在mail工具中，可以用`?`来显示帮助，而参考mail(1)联机手册则可以获得更多关于mail的帮助信息。

注意：正如前面所提到的那样，mail(1)命令在设计时没有考虑到要处理附件，因而在这方面他的功能很弱。新的MUA，如mutt，能够更好地处理附件。但如果您仍然希望使用mail命令，那么converters/mpack port则是一个值得考虑的附加工具。

24.11.2 mutt

mutt是一个短小精悍的邮件用户代理，它提供了许多卓越的功能，包括：

- 能够按线索阅读邮件；
- 支持使用PGP对邮件进行数字签名和加密；
- 支持MIME；
- 支持Maildir；
- 高度可定制。

所有这些特性，都使得mutt得以跻身于目前最先进的邮件用户代理的行列。请参考<http://www.mutt.org>以了解更多关于mutt的资料。

稳定版本的mutt可以通过mail/mutt port来安装，而开发版本，则可以通过使用mail/mutt-devel port安装。通过port安装之后，可以通过下面的命令来启动mutt：

```
% mutt
```

mutt会自动读取/var/mail中的用户信箱，并显示其内容。如果用户信箱中没有邮件，则mutt将等待来自用户的命令。下面的例子展示了mutt列出邮件的情形：


```

q:Quit  d:Del  u:Undel  s:Save  m:Mail  r:Reply  g:Group  ?:Help
1 N    Mar 09 Super-User      ( 1) test
2 N    Mar 09 Super-User      ( 1) user account
3 N    Mar 09 Super-User      ( 1) sample

--Mutt: /var/mail/marcs [Msgs:3 New:3 1.6K]---(date/date)----- (all)---

```

要阅读邮件，只需用光标键选择它，然后按**Enter** 键。以下是**mutt** 显示邮件的例子：

```

i:Exit  -:PrevPg  <Space>:NextPg  v:View Attachm.  d:Del  r:Reply  j:Next  ?:Help
X-Original-To: marcs@localhost
Delivered-To: marcs@localhost
To: marcs@localhost
Subject: test
Date: Tue, 9 Mar 2004 10:28:36 +0200 (SAST)
From: Super-User <root@localhost>

This is a test message, please reply if you receive it.

--N  - 1/1: Super-User      test      -- (all)

```

和mail(1) 类似，**mutt** 允许用户只回复发件人，或者回复所有人。如果只想回复发信任，使用**r** 快捷键。要回复所有人(group reply)，可以用**g** 快捷键。

注意：**mutt** 会使用vi(1) 命令作为编辑器，用于创建和回复邮件。这一行为可以通过建立用户自己的**.muttrc** 文件来订制，方法是修改**editor** 变量。

要撰写新邮件，需要首先按**m**。在输入了有效的邮件主题之后，**mutt** 将启动vi(1)，您可以在其中撰写邮件。写好邮件的内容之后，存盘并退出vi，则**mutt** 将继续，并显示一些关于将发出的邮件的摘要信息。要发送邮件，只需按**y**。下面给出了摘要信息的一个例子：

```

g:Send q:Abort t:To c:CC s:Subj a:Attach file d:Descrip ?:Help
  From: Marc Silver <marcs@localhost>
  To: Super-User <root@localhost>
  Cc:
  Bcc:
  Subject: Re: test
  Reply-To:
  Fcc:
  Security: Clear

-- Attachments
- I 1 /tmp/mutt-bsd-c0hobscQ [text/plain, 7bit, us-ascii, 1.1K]

-- Mutt: Compose [Approx. msg size: 1.1K Atts: 1]--

```

mutt 也提供了相当详尽的帮助，在绝大多数菜单中，都可以使用`?`键将其呼出。屏幕顶行中也会给出常用的快捷键。

24.11.3 pine

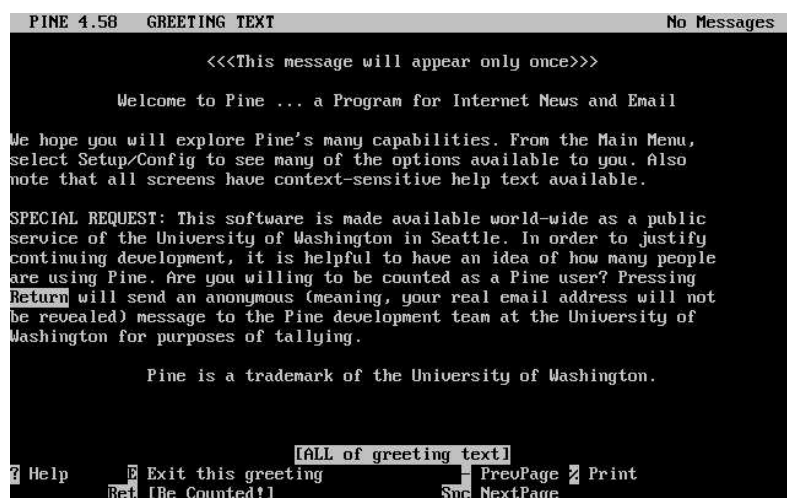
pine 主要是针对初学者设计的，但也提供了一些高级功能。

警告: 过去，**pine** 软件被发现有许多远程漏洞，这些漏洞会允许远程的攻击者在用户的本地系统上，通过发送精心炮制的邮件来执行任意的代码。所有的**已知**问题都已经被修正了，但**pine**的代码是以很不安全的风格编写的，并且FreeBSD安全官相信仍然有一些尚未被发现的安全漏洞。您应当考虑并承担安装**pine**可能带来的风险。

最新版本的**pine**可以通过使用`mail/pine4 port`来安装。装好之后，**pine**可以通过下面的命令启动：

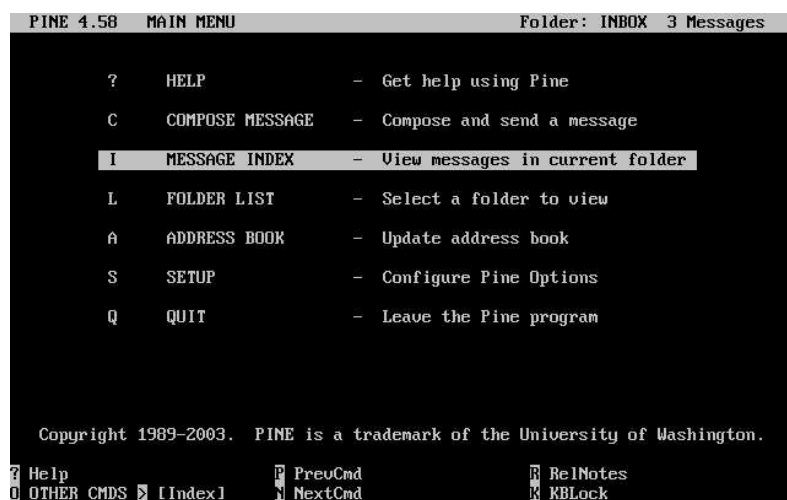
```
% pine
```

第一次启动**pine**时，它会显示出一个欢迎页，并给出简要的介绍，以及**pine**开发小组要求用户匿名发送一封邮件，以便帮助他们了解有多少用户在使用他们开发的客户程序的请求。要发送这封匿名的邮件，请按`Enter`，您也可以按`E`退出，而不发送匿名邮件。下面是欢迎页的一个例子：



接下来展现给用户的将是主菜单，可以很容易地通过光标键在上面进行选择。这个主菜单提供了用于撰写新邮件、浏览邮件目录，甚至管理地址簿等等的快捷方式。主菜单下面是完成各种功能的快捷键说明。

由pine 打开的默认目录是inbox。要查看邮件所以in，应按I，或选择下面所示的MESSAGE INDEX 选项：



邮件索引展示了当前目录下的邮件，可以使用光标键翻阅。按Enter 键阅读高亮选定的邮件。

```

PINE 4.58  MESSAGE INDEX                               Folder: INBOX  Message 1 of 3 ANS
-----
A  1 Mar  9 Super-User      (471) test
A  2 Mar  9 Super-User      (479) user account
A  3 Mar  9 Super-User      (473) sample

? Help  < FldrList  P PrevMsg  - PrevPage  D Delete  R Reply
0 OTHER CMDS > [ViewMsg] N NextMsg  Spc NextPage  U Undelete  F Forward

```

在上面的截屏中，使用**pine**显示了一封示例邮件。在屏幕底部也显示了快捷键供参考。其中的一个例子是**r**键，它告诉MUA回复正显示的邮件。

```

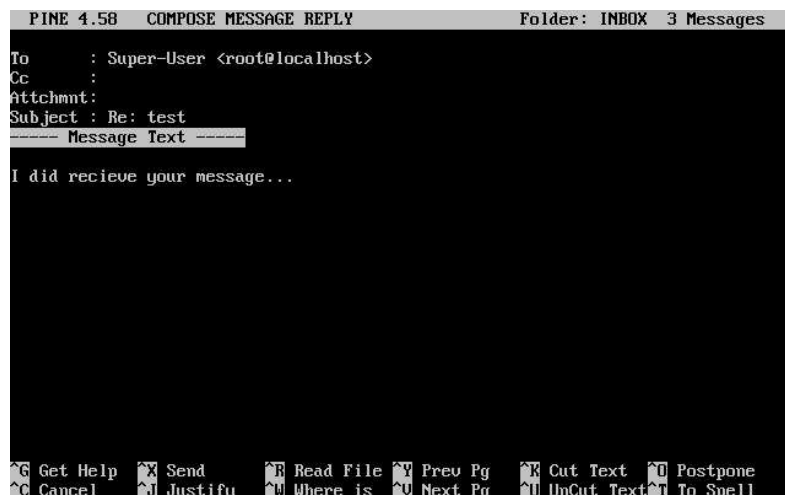
PINE 4.58  MESSAGE TEXT                               Folder: INBOX  Message 1 of 3 ALL ANS
-----
Date: Tue,  9 Mar 2004 10:28:36 +0200 (SAST)
From: Super-User <root@localhost>
To: marcs@localhost
Subject: test

This is a test message, please reply if you receive it.

[ALL of message]
? Help  < MsgIndex  P PrevMsg  - PrevPage  D Delete  R Reply
0 OTHER CMDS > ViewAttch N NextMsg  Spc NextPage  U Undelete  F Forward

```

在**pine**中回复邮件，是通过**pico**编辑器完成的，后者默认情况下会随**pine**一起安装。而**pico**工具使得浏览邮件变得更加简单，并且要比vi(1)或mail(1)更能容忍误操作。回复写好之后，可以用**Ctrl+X**来发出它。此前，**pine**程序会要求确认。



pine 程序可以通过使用主菜单中的**SETUP** 选项来进行定制。请参考<http://www.washington.edu/pine/> 来了解更多信息。

24.12 使用fetchmail

Contributed by Marc Silver.

fetchmail 是一个全功能的IMAP 和POP 客户程序，它允许用户自动地从远程的IMAP 和POP 服务器上下载邮件，并保存到本地的信箱中；这样，访问这些邮件就变得更方便了。**fetchmail** 可以通过**mail/fetchmail port** 安装，它提供了许多有用的功能，其中包括：

- 支持POP3、APOP、KPOP、IMAP、ETRNL 以及ODMR 协议。
- 通过SMTP 转发邮件，这使得过滤、转发，以及邮件别名能够正常工作。
- 能够以服务程序的方式运行，并周期性地检查邮件。
- 能够从多个信箱收取邮件，并根据配置，将这些邮件转发给不同的本地用户。

尽管介绍全部**fetchmail** 的功能超出了本书的范围，但这里仍然介绍了其基本的功能。**fetchmail** 工具需要一个名为**.fetchmailrc** 的配置文件才能正常工作。这个文件中包含了服务器信息，以及登录使用的凭据。由于这个文件包含敏感内容，建议将其设置为只有属主所有，使用下面的命令：

```
% chmod 600 .fetchmailrc
```

下面的**.fetchmailrc** 提供了一个将某一用户的信箱通过POP 下载到本地的例子。它告诉**fetchmail** 连接到example.com，并使用用户名joesoap 和口令XXX。这个例子假定joesoap 同时也是本地的系统用户。

```
poll example.com protocol pop3 username "joesoap" password "XXX"
```

下一个例子将连接多个POP 和IMAP 服务器，并根据需要转到不同的本地用户：

```
poll example.com proto pop3:
user "joesoap", with password "XXX", is "jsoap" here;
user "andrea", with password "XXXX";
poll example2.net proto imap:
```

```
user "john", with password "XXXXX", is "myth" here;
```

另外，**fetchmail** 也可以通过指定 **-d** 参数，并给出**fetchmail** 在轮询 **.fetchmailrc** 文件中列出的服务器的时间间隔，来以服务程序的方式运行。下面的例子会让**fetchmail** 每600 秒轮询一次：

```
% fetchmail -d 600
```

更多关于**fetchmail** 的资料，可以在<http://fetchmail.berlios.de/> 找到。

24.13 使用procmail

Contributed by Marc Silver.

procmail 是一个强大得惊人的过滤进入邮件的应用程序。它允许用户定义“规则”，并用这些规则来匹配进入的邮件，进而执行某些特定的功能，或将这些邮件转发到其他信箱和/或邮件地址。**procmail** 可以通过 **mail/procmail port** 来安装。装好之后，可以直接把它集成到绝大多数MTA 中；请参考您使用的MTA 的文档了解具体的作法。另外，**procmail** 可允许通过把下面的设置加入到用户主目录中的 **.forward** 文件中，来启用**procmail** 功能：

```
"|exec /usr/local/bin/procmail || exit 75"
```

接下来我们将介绍一些基本的**procmail** 规则，以及它们都是做什么的。各种各样的规则，都应该写到 **.procmailrc** 文件中，而这个文件则必须放在用户的主目录下。

主要的规则，也可以在**procmailex(5)** 联机手册中找到。

将所有来自<user@example.com> 的邮件，转发到外部地址<goodmail@example2.com>：

```
:0
* ^From.*user@example.com
! goodmail@example2.com
```

转发所有不超过1000 字节的邮件到外部地址<goodmail@example2.com>：

```
:0
* < 1000
! goodmail@example2.com
```

把所有发送到<alternate@example.com> 的邮件放到信箱**alternate** 中：

```
:0
* ^TOalternate@example.com
alternate
```

将所有标题为“Spam” 的邮件发到/dev/null：

```
:0
^Subject:.*Spam
/dev/null
```

将收到的所有FreeBSD.org 邮件列表的邮件，转发到各自的信箱：

```
:0
```

```
* ^Sender:.owner-freebsd-\/[^\@]+\@FreeBSD.ORG
{
LISTNAME=${MATCH}
:0
* LISTNAME??^\/[^\@]+
FreeBSD-${MATCH}
}
```

第25章

网络服务器

Reorganized by Murray Stokely.

25.1 概要

本章将覆盖某些在UNIX系统上常用的网络服务。话题将会涉及如何安装、配置、测试和维护多种不同类型的网络服务。本章节中将提供大量配置文件的样例，期望能够对您有所裨益。

在读完本章之后，您将会知道：

- 如何管理**inetd**。
- 如何设置运行一个网络文件系统。
- 如何配置一个网络信息服务器以共享用户帐号。
- 如何通过DHCP自动配置网络。
- 如何配置一个域名服务器。
- 如何设置Apache HTTP服务器。
- 如何设置文件传输（FTP）服务器。
- 如何使用Samba为Windows客户端设置文件和打印服务。
- 如何同步时间和日期，以及如何设置使用NTP协议的时间服务器。

在阅读此章节之前，您应当：

- 理解有关/etc/rc中脚本的基本知识。
- 熟悉基本网络术语。
- 懂得如何安装额外的第三方软件（第4章）。

25.2 **inetd** “超级服务器”

Contributed by Chern Lee. 为FreeBSD 6.1-RELEASE 进行了更新，由The FreeBSD Documentation Project.

25.2.1 总览

inetd(8)有时也被称作“Internet 超级服务器”，因为它可以为多种服务管理连接。当**inetd** 接到连接时，它能够确定连接所需的程序，启动相应的进程，并把**socket** 交给它(服务**socket** 会作为程序的标准输入、输出和错误输出描述符)。使用**inetd** 来运行那些负载不重的服务有助于降低系统负载，因为它不需要为每个服务都启动独立的服务程序。

一般说来，**inetd** 主要用于启动其它服务程序，但它也有能力直接处理某些简单的服务，例如**chargen**、**auth**，以及**daytime**。

这一节将介绍关于如何通过命令行选项，以及配置文件`/etc/inetd.conf`来对**inetd**进行配置的一些基础知识。

25.2.2 设置

inetd是通过`rc(8)`系统启动的。`inetd_enable`选项默认设为**NO**，但可以在安装系统时，由用户根据需要，通过**sysinstall**来打开。将

```
inetd_enable="YES"
```

或

```
inetd_enable="NO"
```

写入`/etc/rc.conf`可以启用或禁用系统启动时**inetd**的自动启动。命令：

```
/etc/rc.d/inetd rcvar
```

可以显示目前的设置。

此外，您还可以通过**inetd_flags**参数来向**inetd**传递额外的其它参数。

25.2.3 命令行选项

与多数服务程序类似，**inetd**也提供了为数众多的用以控制其行为的参数。完整的参数列表如下：

```
inetd [-d] [-l] [-w] [-W] [-c maximum] [-C rate] [-a address | hostname] [-p
filename] [-R rate] [-s maximum] [configuration file]
```

这些参数都可以通过`/etc/rc.conf`的**inetd_flags**选项来传给**inetd**。默认情况下，**inetd_flags**设为**-ww -C 60**，者表示希望为**inetd**的服务启用TCP wrapping，并阻止来自同一IP每分钟超过60次的请求。

初学的用户可能会很高兴地发现这些选项通常并不需要进行修改，前面提到的速率限制选项在您的服务器收到过量请求的连接时，则会有效地发挥作用。完整的参数列表，可以在**inetd(8)**联机手册中找到。

-c maximum

指定单个服务的最大并发访问数量，默认为不限。也可以在此服务的具体配置里面通过**max-child**改掉。

-C rate

指定单个服务一分钟内能被单个IP地址调用的最大次数，默认不限。也可以在此服务的具体配置里面通过**max-connections-per-ip-per-minute**改掉。

-R rate

指定单个服务一分钟内能被调用的最大次数，默认为256。设为0则允许不限次数调用。

-s maximum

指定同一IP同时请求同一服务时允许的最大值；默认值为不限制。您可以通过**max-child-per-ip**参数来以服务为单位进行限制。

25.2.4 inetd.conf

对于inetd 的配置，是通过/etc/inetd.conf 文件来完成的。
在修改了/etc/inetd.conf 之后，可以使用下面的命令来强制inetd 重新读取配置文件：

例25-1. 重新加载inetd 配置文件

```
# /etc/rc.d/inetd reload
```

配置文件中的每一行都是一个独立的服务程序。在这个文件中，前面有“#” 的内容被认为是注释。/etc/inetd.conf 文件的格式如下：

```
service-name
socket-type
protocol
{wait|nowait}[/max-child[/max-connections-per-ip-per-minute[/max-child-per-ip]]]
user[:group][[/login-class]]
server-program
server-program-arguments
```

下面是针对IPv4 的ftpd(8) 服务的例子：

```
ftp      stream  tcp      nowait  root    /usr/libexec/ftpd      ftpd -l
```

service-name

指明各个服务的服务名。其服务名必须与/etc/services中列出的一致。这将决定inetd会监听哪个port。一旦有新的服务需要添加，必须先在/etc/services里面添加。

socket-type

可以是stream、dgram、raw或者seqpacket。stream用在基于连接的，TCP 服务；而dgram被用于服务用于UDP传输协议。

protocol

下列之一：

协议	说明
tcp, tcp4	TCP IPv4
udp, udp4	UDP IPv4
tcp6	TCP IPv6
udp6	UDP IPv6
tcp46	Both TCP IPv4 and v6
udp46	Both UDP IPv4 and v6

```
{wait|nowait}[/max-child[/max-connections-per-ip-per-minute[/max-child-per-ip]]]
```

wait|nowait 指明从inetd 里头调用的服务是否可以自己处理socket。dgramsocket类型必须使用wait，而stream socket daemons，由于通常使用多线程方式，应当使用nowait.wait 通常usually 把多

个socket丢给单个服务进程，而**nowait** 则会为每个新的socket生成一个子进程。

使用**max-child**选项可以设定针对服务，**inetd**可以派生出来的最大子进程数量。如果某特定服务需要限定最高10个实例，把**/10** 放到**nowait**后头就可以了。指定**/0** 表示不限制子进程的数量。

除了**max-child** 之外，还有两个选项可以限制来自同一位置到特定服务的最大连接数。**max-connections-per-ip-per-minute** 可以限制特定IP 地址每分钟的总连接数，例如，限制任何IP 地址每分钟最多连接十次。**max-child-per-ip** 则可以限制为某一IP 地址在任何时候所启动的子进程数量。这些选项对于防止针对服务器有意或无意的资源耗竭和拒绝服务(DoS) 攻击十分有用。

这个字段中，必须指定**wait** 或**nowait** 两者之一。

而**max-child**、**max-connections-per-ip-per-minute** 和**max-child-per-ip** 则是可选项。

流式多线程服务，并且不配置任何**max-child**、**max-connections-per-ip-per-minute** 或**max-child-per-ip** 限制时，其配置为：**nowait**。

同一个服务，但希望将服务启动的数量限制为十个时，则是：**nowait/10**。

同样配置，限制每个IP 地址每分钟最多连接二十次，而同时启动的子进程最多十个，应写作：**nowait/10/20**。

下面是**fingerd(8)** 服务的默认配置：

```
finger stream tcp      nowait/3/10 nobody /usr/libexec/fingerd fingerd -s
```

最后这个例子中，将子进程数限制为100 个，而任意IP 最多同时建立5 个连接：**nowait/100/0/5**。

user

该开关指定服务将以什么用户身份运行。一般而言，服务运行身份是**root**。基于安全目的，可以看到有些服务以**daemon**身份，或者是最小特权的**nobody**身份运行。

server-program

当连接到来时，执行服务程序的全路径。如果服务是由**inetd**内置提供的，以**internal**代替。

server-program-arguments

当**server-program**调用到时，该开关的值通过**argv[0]**通过传递给服务而工作。如果命令行为：**mydaemon -d**，则**mydaemon -d**为**server-program-arguments** 开关的值。同样的，如果服务是由**inetd** 内置提供的，这里还是**internal**。

25.2.5 Security

随安装时所选的模式不同，许多**inetd** 的服务可能已经默认启用。如果确实不需要某个特定的服务，则应考虑禁用它。在**/etc/inetd.conf** 中，将对应服务的那行前面加上“**#**”，然后重新加载**inetd** 配置就可以了。某些服务，例如**fingerd**，可能是完全不需要的，因为它们提供的信息可能对攻击者有用。

某些服务在设计时是缺少安全意识的，或者有过长或压根没有连接请求的超时机制。这使得攻击者能够通过缓慢地对这些服务发起连接，并耗尽可用的资源。对于这种情况，设置**max-connections-per-ip-per-minute**、**max-child** 或**max-child-per-ip** 限制，来制约服务的行为是个好办法。

默认情况下，**TCP wrapping** 是打开的。参考**hosts_access(5)** 手册，以获得更多关于在各种**inetd** 调用的服务上设置**TCP**限制的信息。

25.2.6 杂项

daytime、**time**、**echo**、**discard**、**chargen**，以及**auth**都是由**inetd**提供的内建服务。

auth服务提供了网络身份服务，它可以配置为提供不同级别的服务，而其它服务则通常只能简单的打开或关闭。

参考**inetd(8)**手册获得更多信息。

25.3 网络文件系统（NFS）

Reorganized and enhanced by Tom Rhodes. Written by Bill Swingle.

网络文件系统是FreeBSD支持的文件系统中的一种，也被称为NFS。NFS允许一个系统在网络上与它人共享目录和文件。通过使用NFS，用户和程序可以象访问本地文件一样访问远端系统上的文件。

以下是NFS最显而易见的好处：

- 本地工作站使用更少的磁盘空间，因为通常的数据可以存放在一台机器上而且可以通过网络访问到。
- 用户不必在每个网络上机器里头都有一个home目录。Home目录可以被放在NFS服务器上并且在网络上处处可用。
- 诸如软驱，CDROM，和Zip®之类的存储设备可以在网络上面被别的机器使用。这可以减少整个网络上的可移动介质设备的数量。

25.3.1 NFS是如何工作的

NFS至少包括两个主要的部分：一台服务器，以及至少一台客户机，客户机远程地访问保存在服务器上的数据。要让这一切运转起来，需要配置并运行几个程序。

注意：在FreeBSD 4.X中，**portmap**工具将发挥后续版本中**rpcbind**工具的作用。因此，在FreeBSD 4.X中，您可能需要把后续例子中的**rpcbind**改成**portmap**以便使用。

服务器必须运行以下服务：

服务	描述
nfsd	NFS，为来自NFS客户端的请求服务。
mountd	NFS挂载服务，处理 nfsd(8) 递交过来的请求。
rpcbind	此服务允许NFS客户程序查询正在被NFS服务使用的端口。

客户端同样运行一些进程，比如**nfsiod**。**nfsiod**处理来自NFS的请求。这是可选的，而且可以提高性能，对于普通和正确的操作来说并不是必须的。参考**nfsiod(8)**手册获得更多信息。

25.3.2 配置NFS

NFS的配置过程相对简单。这个过程只需要对/etc/rc.conf文件作一些简单修改。

在NFS服务器这端，确认/etc/rc.conf 文件里头以下开关都配上了：

```
rpcbind_enable="YES"
nfs_server_enable="YES"
mountd_flags="-r"
```

只要NFS服务被置为enable，**mountd** 就能自动运行。

在客户端一侧，确认下面这个开关出现在/etc/rc.conf里头：

```
nfs_client_enable="YES"
```

/etc/exports文件指定了哪个文件系统NFS应该输出（有时被称为“共享”）。/etc/exports里面每行指定一个输出的文件系统和哪些机器可以访问该文件系统。在指定机器访问权限的同时，访问选项开关也可以被指定。有很多开关可以被用在这个文件里头，不过不会在这里详细谈。您可以通过阅读exports(5)手册来发现这些开关。

以下是一些/etc/exports的例子：

紧接着的这个例子说明了如何输出一个文件系统，尽管具体设定和您的环境以及网络配置有关。作为实例，为了输出/cdrom 到三个的例子机器，它们有同样域名（因此他们的域名不大对）或者在您的/etc/hosts文件里头有记录。-ro 标志将被输出的文件系统置为只读。由于这个标志，远程系统将无法在被输出的文件系统上写入任何变动。

```
/cdrom -ro host1 host2 host3
```

下面的例子可以输出/home给三个以IP地址方式表示的主机。对于在没有配置DNS服务器的私有网络里头，这很有用。此外，the /etc/hosts 文件也可以用以配置主机名；参看hosts(5)。-alldirs 标记允许子目录被作为挂载点。也就是说，客户端可以根据需要挂载需要的目录。

```
/home -alldirs 10.0.0.2 10.0.0.3 10.0.0.4
```

下面几行输出/a，以便两个来自不同域的客户端可以访问文件系统。-maproot=root 标记授权远端系统上的root 用户在被输出的文件系统上以root身份进行读写。如果没有特别指定-maproot=root 标记，则即使用户在远端系统上是root 身份，也不能修改被输出文件系统上的文件。

```
/a -maproot=root host.example.com box.example.org
```

为了能够访问到被输出的文件系统，客户端必须被授权。请确认客户端在您的/etc/exports 被列出。

在/etc/exports 里头，每一行里面，输出信息和文件系统一一对应。一个远程主机每次只能对应一个文件系统。而且只能有一个默认入口。比如，假设/usr 是独立的文件系统。这个/etc/exports 就是无效的：

```
# Invalid when /usr is one file system
/usr/src client
/usr/ports client
```

一个文件系统，/usr，有两行指定输出到同一主机，client. 解决这一问题的正确的格式是：

```
/usr/src /usr/ports client
```

The properties of one file system exported to a given host must all occur on one line. Lines without a client specified are treated as a single host. This limits how you can export file systems, but for most people this is not an issue.

下面是一个有效输出列表的例子，`/usr` and `/exports` 是本地文件系统：

```
# Export src and ports to client01 and client02, but only
# client01 has root privileges on it
/usr/src /usr/ports -maproot=root    client01
/usr/src /usr/ports                  client02
# The client machines have root and can mount anywhere
# on /exports. Anyone in the world can mount /exports/obj read-only
/exports -alldirs -maproot=root      client01 client02
/exports/obj -ro
```

一旦修改`/etc/exports`了之后，为了让变动生效，您必须重启`mountd`。可以通过对`mountd`进程发送HUP信号重启：

```
# kill -HUP `cat /var/run/mountd.pid`
```

另外，系统重启动可以让FreeBSD把一切都弄好。尽管如此，重启不是必须的。以`root`身份执行下面的命令可以搞定一切。

在NFS服务器端：

```
# rpcbind
# nfsd -u -t -n 4
# mountd -r
```

在NFS客户端：

```
# nfsiod -n 4
```

现在每件事情都应该就绪，以备挂载一个远端文件系统。在这些例子里头，服务器名字将是：`server`，而客户端的名字将是：`client`。如果您只打算临时挂载一个远端文件系统或者只是打算作测试配置正确与否，只要在客户端以`root`身份执行下面的命令：

```
# mount server:/home /mnt
```

这条命令会把服务端的`/home`目录挂载到客户端的`/mnt`上。如果配置正确，您应该可以进入客户端的`/mnt`目录并且看到所有服务端的文件。

如果您打算让系统每次在重启动的时候都自动挂载远端的文件系统，把那个文件系统加到`/etc/fstab`文件里头去。下面是例子：

```
server:/home /mnt nfs rw 0 0
```

`fstab(5)`手册里有所有可用的开关。

25.3.3 实际应用

NFS有很多实际应用。下面是比较常见的一些：

- 多个机器共享一台CDROM或者其他设备。这对于在多台机器中安装软件来说更加便宜跟方便。
- 在大型网络中，配置一台中心NFS服务器用来放置所有用户的`home`目录可能会带来便利。这些目录能被输出到网络以便用户不管在哪台工作站上登录，总能得到相同的`home`目录。

- 几台机器可以有通用的/usr/ports/distfiles 目录。这样的话，当您需要在几台机器上安装port时，您可以无需在每台设备上下载而快速访问源码。

25.3.4 通过amd 自动地挂接

Contributed by Wylie Stilwell. Rewritten by Chern Lee.

amd(8) (自动挂接服务) 能够自动地在访问时挂接远程的文件系统。如果文件系统在一时间之内没有活动，则会被amd 自动卸下。通过使用amd，能够提供一个持久挂接以外的选择，而后者往往需要列入/etc/fstab。

amd 通过将自己以NFS 服务器的形式，附加到/host 和/net 目录上来工作。当访问这些目录中的文件时，amd 将查找相应的远程挂接点，并自动地挂接。/net 用于挂接远程IP 地址上导出的文件系统，而/host 则用于挂接远程主机名上的文件系统。

访问/host/foobar/usr 中的文件，相当于告诉amd 尝试挂接在主机foobar 上导出的/usr。

例25-2. 通过amd 来挂接导出的文件系统

您可以通过使用showmount 命令来查看远程主机上导出的文件系统。例如，要查看foobar 上导出的文件系统，可以用：

```
% showmount -e foobar
Exports list on foobar:
/usr                10.10.10.0
/a                  10.10.10.0
% cd /host/foobar/usr
```

如同在前面例子中所看到的，showmount 显示了导出的/usr。当进入/host/foobar/usr 这个目录时，amd 将尝试解析主机名foobar 并自动地挂接需要的文件系统导出。

amd 可以通过启动脚本来启动，方法是在/etc/rc.conf 中加入：

```
amd_enable="YES"
```

除此之外，还可以给amd 通过amd_flags 选项来传递额外的参数。默认情况下，amd_flags 为：

```
amd_flags="-a /.amd_mnt -l syslog /host /etc/amd.map /net /etc/amd.map"
```

/etc/amd.map 文件定义了挂接导出文件系统时所使用的默认选项。/etc/amd.conf 文件，则定义了更多关于amd 的高级功能选项。

请参考amd(8) 和amd.conf(5) 联机手册，以了解进一步的情况。

25.3.5 与其他系统集成时的常见问题

Contributed by John Lind.

某些特定的ISA PC 系统上的以太网适配器上有一些限制，这些限制可能会导致严重的网络问题，特别是与NFS 配合使用时。这些问题并非FreeBSD 所特有的，但FreeBSD 系统会受到这些问题的影响。

这样的问题，几乎总是在当(FreeBSD) PC 系统与高性能的工作站，例如Silicon Graphics, Inc., 和Sun Microsystems, Inc. 的工作站联网时发生。NFS 挂接能够正常工作，而且一些操作也可能成功，但服务器会

很快变得对客户机不太理会，虽然对其他客户机的请求仍然能够正常处理。这种情况通常发生在客户端，无论它是一个FreeBSD系统或是终端。在许多系统上，一旦发生了这样的问题，通常没办法正常地关闭客户机。唯一的办法通常是让终端复位，因为这一NFS状况没有办法被解决。

尽管“正确的”解决办法，是为FreeBSD系统配备一块高性能的、适用的以太网适配器，然而也有办法绕过问题并得到相对满意的结果。如果FreeBSD系统是服务器，则在客户机挂接时，应该指定 `-w=1024`。如果FreeBSD系统是客户机，则应加入 `-r=1024` 参数。这些选项可以通过在对应的fstab的第四个字段加入，以便让客户机能够自动地挂接，或者通过mount(8)的 `-o` 参数在手工挂接时指定。

还需要注意的是另一个问题，有时会被误认为是和上面一样的问题。这个问题多见于NFS服务器和客户机在不同的网络上时。如果是这种情况，一定要确定您的路由器确实把必需的UDP信息路由到了目的地，否则您将什么也做不了。

下面的例子中，fastws是主机(接口)的名字，它是一台高性能的终端，而freebox是另一台主机(接口)的名字，它是一个使用较低性能的以太网适配器的FreeBSD系统。同时，/sharedfs将被导出成为NFS文件系统(参见exports(5))，而/project将是客户机上挂接这一导出文件系统的挂接点。所有的应用场景中，请注意附加选项，例如hard或soft以及bg可能是您的应用所需要的。

关于FreeBSD系统(freebox)作为客户机的示范/etc/fstab文件，见于freebox之上：

```
fastws:/sharedfs /project nfs rw,-r=1024 0 0
```

在freebox上手工挂接：

```
# mount -t nfs -o -r=1024 fastws:/sharedfs /project
```

以FreeBSD系统作为服务器的例子，是fastws上的/etc/fstab：

```
freebox:/sharedfs /project nfs rw,-w=1024 0 0
```

在fastws上手工挂接的命令是：

```
# mount -t nfs -o -w=1024 freebox:/sharedfs /project
```

几乎所有的16-位以太网控制器，都能够在没有上述读写尺寸限制的情况下正常工作。

对于那些关心到底是什么问题的人，下面是失败如何发生的解释，同时这也说明了为什么这是一个无法恢复的问题。典型情况下，NFS会使用一个“块”为单位进行操作，其尺寸是8 K(虽然它可能会将操作分成更小尺寸的分片)。由于最大的以太网包尺寸大约是1500字节，因此NFS“块”会分成多个以太网包，虽然在更高层的代码看来它仍然是一个完整的单元，并在接收方重新组装，作为一个整体来确认。高性能的工作站，可以将构成NFS单元的包迅速发出，其节奏会快到标准允许的最大限度。在容量较小的卡上，后来的包会冲掉同一单元内的较早的包，因而整个单元无法被重建或确认。其结果是，工作站将超时并重试，但仍然是完整的8 K单元，这一过程将无休止地重复下去。

如果将单元尺寸限制在以太网包尺寸之下，我们就能够确保每一个以太网包都能够被独立地接收和确认，从而避免了上面的死锁情形。

溢出在高性能工作站将数据库投向PC系统时仍会发生，但在更好的网卡上，能够保证这类溢出不会在每一个NFS“单元”上都发生。当出现溢出时，被影响的单元被重传，因而此时有很大的机会它将被正确接收、重组，并确认。

25.4 网络信息服务(NIS/YP)

Written by Bill Swingle. Enhanced by Eric Ogren 和Udo Erdelhoff.

25.4.1 它是什么？

NIS，表示网络信息服务(Network Information Services)，最初由Sun Microsystems 开发，用于UNIX (最初是SunOS) 系统的集中管理。目前，它基本上已经成为了业界标准；所有主流类UNIX 系统(Solaris, HP-UX, AIX®, Linux, NetBSD, OpenBSD, FreeBSD, 等等) 都支持NIS。

NIS 也就是人们所熟知的黄页(Yellow Pages)，但由于商标的问题，Sun 将其改名为现在的名字。旧的术语(以及yp)，仍然经常可以看到，并被广泛使用。

这是一个基于RPC 的客户机/服务器系统，它允许在一个NIS 域中的一组机器共享一系列配置文件。这样，系统管理员就可以配置只包含最基本配置数据的NIS 客户机系统，并在单点上增加、删除或修改配置数据。

尽管实现的内部细节截然不同，这和Windows NT® 域系统非常类似，以至于可以将两者的基本功能相互类比。

25.4.2 您应该知道的术语和进程

有一系列术语和重要的用户进程将在您在FreeBSD 上实现NIS 时用到，无论是在创建NIS 服务器，或作为NIS 客户机：

术语	说明
NIS 域名	NIS 主服务器和所有其客户机(包括从服务器) 会使用同一NIS 域名。和Windows NT 域名类似，NIS 域名与DNS 无关。
rpcbind	必须运行这个程序，才能够启用RPC (远程过程调用，NIS 用到的一种网络协议)。如果没有运行 rpcbind ，则没有办法运行NIS 服务器，或作为NIS 客户机(对于FreeBSD 4.X， portmap 完成 rpcbind 的功能)。
ypbind	“绑定(bind)” NIS 客户机到它的NIS 服务器上。这样，它将从系统中获取NIS 域名，并使用RPC 连接到服务器上。 ypbind 是NIS 环境中，客户机-服务器通讯的核心；如果客户机上的 ypbind 死掉的话，它将无法访问NIS 服务器。
ypserv	只应在NIS 服务器上运行它；这是NIS 的服务器进程。如果 ypserv(8) 死掉的话，则服务器将不再具有响应NIS 请求的能力(此时，如果有从服务器的话，则会接管操作)。有一些NIS 的实现(但不是FreeBSD 的这个) 的客户机上，如果之前用过一台服务器，而那一台服务器死掉的话，并不尝试重新连接到另一个服务器。通常，发生这种情况时，唯一的办法就是重新启动服务器进程(或者，甚至重新启动服务器) 或客户机上的 ypbind 进程。
rpc.yppasswdd	另一个只应在NIS 主服务器上运行的进程；这是一个服务程序，其作用是允许NIS 客户机改变它们的NIS 口令。如果没有运行这个服务，用户将必须登录到NIS 主服务器上，并在那里修改口令。

25.4.3 它是如何工作的？

在NIS 环境中，有三种类型的主机：主服务器，从服务器，以及客户机。服务器的作用是充当主机配

置信息的中央数据库。主服务器上保存着这些信息的权威副本，而从服务器则是保存这些信息的冗余副本。客户机依赖于服务器向它们提供这些信息。

许多文件的信息可以通过这种方式来共享。通常情况下，`master.passwd`、`group`，以及`hosts`是通过NIS分发的。无论什么时候，如果客户机上的某个进程请求这些本应在本地的文件中的资料的时候，它都会向所绑定的NIS服务器发出请求，而不使用本地的版本。

25.4.3.1 机器类型

- 一台**NIS 主服务器**。这台服务器，和Windows NT 域控制器类似，会维护所有NIS 客户机所使用的文件。`passwd`，`group`，以及许多其他NIS 客户机所使用的文件，都被存放到主服务器上。

注意: 可以将一台NIS 主服务器用在多个NIS 域中。然而，本书不打算对这种配置进行介绍，因为这种配置，通常只出现在小规模NIS 环境中。

- **NIS 从服务器**。这一概念，与Windows NT 的备份域控制器类似。NIS 从服务器，用于维护NIS 主服务器的数据文件副本。NIS 从服务器提供了一种冗余，这在许多重要的环境中是必需的。此外，它也帮助减轻了主服务器的负荷：NIS 客户机总是挂接到最先响应它们的NIS 服务器上，而这也包括来自从服务器的响应。
- **NIS 客户机**。NIS 客户机，和多数Windows NT 工作站类似，通过NIS 服务器(或对于Windows NT 工作站，则是Windows NT 域控制器)来完成登录时的身份验证过程。

25.4.4 使用NIS/YP

这一节将通过实例介绍如何配置NIS 环境。

注意: 这一节假定您正运行的是FreeBSD 3.3 或更高版本。这里给出的方法或许可以在FreeBSD 3.0 以上的其他版本上使用，但不保证。

25.4.4.1 规划

假定您正在管理大学中的一个小型实验室。在这个实验室中，有15 台FreeBSD 机器，目前尚没有集中的管理点；每一台机器上有自己的`/etc/passwd` 和`/etc/master.passwd`。这些文件通过人工干预的方法来保持与其他机器上版本的同步；目前，如果您在实验室中增加一个用户，将不得不在所有15 台机器上手工执行`adduser` 命令。毋庸置疑，这一现状必须改变，因此您决定将整个实验室转为使用NIS，并使用两台机器作为服务器。

因此，实验室的配置应该是这样的：

机器名	IP 地址	机器的角色
ellington	10.0.0.2	NIS 主服务器
coltrane	10.0.0.3	NIS 从服务器

机器名	IP 地址	机器的角色
basie	10.0.0.4	教员工作站
bird	10.0.0.5	客户机
cli[1-11]	10.0.0.[6-17]	其他客户机

如果您是首次配置NIS，仔细思考如何进行规划就十分重要。无论您的网络的大小如何，都必须进行几个决策。

25.4.4.1.1 选择NIS 域名

这可能不是您过去使用的“域名(domainname)”，它的规范的叫法，应该是“NIS 域名”。当客户机广播对此信息的请求时，它会将NIS 域的名字作为请求的一部分发出。这样，统一网络上的多个服务器，就能够知道谁应该回应请求。您可以把NIS 域名想象成以某种方式相关的一组主机的名字。

一些机构会选择使用它们的Internet 域名来作为NIS 域名。并不推荐这样做，因为在调试网络问题时，这可能会导致不必要的困扰。NIS 域名应该是在您网络上唯一的，并且有助于了解它所描述的到底是哪一组机器。例如对于Acme 公司的美工部门，可以考虑使用“acme-art”这样的NIS 域名。在这个例子中，您使用的域名是test-domain。

然而，某些操作系统(最著名的是SunOS)会使用其NIS 域名作为Internet 域名。如果您的网络上存在包含这类限制的机器，就必须使用Internet 域名来作为您的NIS 域名。

25.4.4.1.2 服务器的物理要求

选择NIS 服务器时，需要时刻牢记一些东西。NIS 的一个不太好的特性就是其客户机对于服务器的依赖程度。如果客户机无法与其NIS 域的服务器联系，则这台机器通常会陷于不可用的状态。缺少用户和组信息，会使绝大多数系统进入短暂的冻结状态。基于这样的考虑，您需要选择一台不经常重新启动，或用于开发的机器来承担其责任。如果您的网络不太忙，也可以使用运行着其他服务的机器来安放NIS 服务，只是需要注意，一旦NIS 服务器不可用，则所有的NIS 客户机都会受到影响。

25.4.4.2 NIS 服务器

所有的NIS 信息的正规版本，都被保存在一台单独的称作NIS 主服务器的机器上。用于保存这些信息的数据库，称为NIS 映射(map)。在FreeBSD 中，这些映射被保存在/var/yp/[domainname] 里，其中[domainname] 是提供服务的NIS 域的名字。一台NIS 服务器，可以同时支持多个域，因此可以建立很多这样的目录，所支撑一个域对应一个。每一个域都会有一组独立的映射。

NIS 主和从服务器，通过ypserv 服务程序来处理所有的NIS 请求。ypserv 有责任接收来自NIS 客户机的请求，翻译请求的域，并将名字映射为相关的数据库文件的路径，然后将来自数据库的数据传回客户机。

25.4.4.2.1 配置NIS 主服务器

配置主NIS 服务器相对而言十分的简单，而其具体步骤则取决于您的需要。FreeBSD 提供了一步到位的NIS 支持。您需要做的全部事情，只是在/etc/rc.conf 中加入一些配置，其他工作会由FreeBSD 完成。

- 1.
 nisdomainname="test-domain"

这一行将在网络启动(例如重新启动)时, 把NIS 域名配置为test-domain。

2.

```
nis_server_enable="YES"
```

这将要求FreeBSD 在网络子系统启动之后立即启动NIS 服务进程。

3.

```
nis_yppasswdd_enable="YES"
```

这将启用rpc.yppasswdd 服务程序, 如前面提到的, 它允许用户在客户机上修改自己的NIS 口令。

注意: 随NIS 配置的不同, 可能还需要增加其他一些项目。请参见关于NIS 服务器同时充当NIS 客户机 这一节, 以了解进一步的情况。

现在, 所需要做的最后的工作是以超级用户身份执行/etc/netstart 命令。这将依据/etc/rc.conf 为您配置好所有的东西。

25.4.4.2.2 初始化NIS 映射

NIS 映射 是一些数据库文件, 它们位于/var/yp 目录中。这些文件基本上都是根据NIS 主服务器的/etc 目录自动生成的, 唯一的例外是: /etc/master.passwd 文件。一般来说, 您会有非常充分的理由不将root 以及其他管理帐号的口令发到所有NIS 域上的服务器上。因此, 在开始初始化NIS 映射之前, 我们应该:

```
# cp /etc/master.passwd /var/yp/master.passwd
# cd /var/yp
# vi master.passwd
```

这里, 删除掉和系统有关的帐号对应的项(bin、tty、kmem、games, 等等), 以及其他不希望被扩散到NIS 客户机的帐号(例如root 和任何其他UID 0 (超级用户) 的帐号)。

注意: 确认/var/yp/master.passwd 这个文件是同组, 其他以及其他用户不可读的(模式600)! 如果需要的话, 用chmod 命令来改它。

完成这些工作之后, 就可以初始化NIS 映射了! FreeBSD 提供了一个名为ypinit 的脚本来帮助您完成这项工作(详细信息, 请见其联机手册)。请注意, 这个脚本在绝大多数UNIX 操作系统上都可以找到, 但并不是所有操作系统的都提供。在Digital UNIX/Compaq Tru64 UNIX 上它的名字是ypsetup。由于我们正在生成的是NIS 主服务器的映射, 因此应该使用ypinit 的-m 参数。如果已经完成了上述步骤, 要生成NIS 映射, 只需执行:

```
ellington# ypinit -m test-domain
Server Type: MASTER Domain: test-domain
Creating an YP server will require that you answer a few questions.
Questions will all be asked at the beginning of the procedure.
Do you want this procedure to quit on non-fatal errors? [y/n: n] n
Ok, please remember to go back and redo manually whatever fails.
If you don't, something might not work.
At this point, we have to construct a list of this domains YP servers.
```

```
rod.darktech.org is already known as master server.
Please continue to add any slave servers, one per line. When you are
done with the list, type a <control D>.
master server   : ellington
next host to add: coltrane
next host to add: ^D
The current list of NIS servers looks like this:
ellington
coltrane
Is this correct? [y/n: y] y

[..output from map generation..]

NIS Map update completed.
ellington has been setup as an YP master server without any errors.
```

ypinit 应该会根据/var/yp/Makefile.dist 来创建/var/yp/Makefile 文件。创建完之后，这个文件会假定您正在操作只有FreeBSD 及其德单服务器NIS 环境。由于test-domain 还有一个从服务器，您必须编辑/var/yp/Makefile:

```
ellington# vi /var/yp/Makefile
```

应该能够看到这样一行，其内容是

```
NOPUSH = "True"
```

(如果还没有注释掉的话)。

25.4.4.2.3 配置NIS 从服务器

配置NIS 从服务器，甚至比配置主服务器还要简单。登录到从服务器上，并按照前面的方法，编辑/etc/rc.conf 文件。唯一的区别是，在运行ypinit 时需要使用-s 参数。这里的-s 选项，同时要求提供NIS 主服务器的名字，因此我们的命令行应该是：

```
coltrane# ypinit -s ellington test-domain
```

```
Server Type: SLAVE Domain: test-domain Master: ellington
```

```
Creating an YP server will require that you answer a few questions.
Questions will all be asked at the beginning of the procedure.
```

```
Do you want this procedure to quit on non-fatal errors? [y/n: n] n
```

```
Ok, please remember to go back and redo manually whatever fails.
If you don't, something might not work.
There will be no further questions. The remainder of the procedure
should take a few minutes, to copy the databases from ellington.
Transferring netgroup...
ypxfr: Exiting: Map successfully transferred
Transferring netgroup.byuser...
ypxfr: Exiting: Map successfully transferred
Transferring netgroup.byhost...
```

```

ypxfr: Exiting: Map successfully transferred
Transferring master.passwd.byuid...
ypxfr: Exiting: Map successfully transferred
Transferring passwd.byuid...
ypxfr: Exiting: Map successfully transferred
Transferring passwd.byname...
ypxfr: Exiting: Map successfully transferred
Transferring group.bygid...
ypxfr: Exiting: Map successfully transferred
Transferring group.byname...
ypxfr: Exiting: Map successfully transferred
Transferring services.byname...
ypxfr: Exiting: Map successfully transferred
Transferring rpc.bynumber...
ypxfr: Exiting: Map successfully transferred
Transferring rpc.byname...
ypxfr: Exiting: Map successfully transferred
Transferring protocols.byname...
ypxfr: Exiting: Map successfully transferred
Transferring master.passwd.byname...
ypxfr: Exiting: Map successfully transferred
Transferring networks.byname...
ypxfr: Exiting: Map successfully transferred
Transferring networks.byaddr...
ypxfr: Exiting: Map successfully transferred
Transferring netid.byname...
ypxfr: Exiting: Map successfully transferred
Transferring hosts.byaddr...
ypxfr: Exiting: Map successfully transferred
Transferring protocols.bynumber...
ypxfr: Exiting: Map successfully transferred
Transferring ypservers...
ypxfr: Exiting: Map successfully transferred
Transferring hosts.byname...
ypxfr: Exiting: Map successfully transferred

```

coltrane has been setup as an YP slave server without any errors.
Don't forget to update map ypservers on ellington.

现在应该会有一个叫做`/var/yp/test-domain`的目录。在这个目录中，应该保存NIS主服务器上的映射的副本。接下来需要确定这些文件都及时地同步更新了。在从服务器上，下面的`/etc/crontab`项将帮助您确保这一点：

```

20      *      *      *      *      root    /usr/libexec/ypxfr passwd.byname
21      *      *      *      *      root    /usr/libexec/ypxfr passwd.byuid

```

这两行将强制从服务器将映射与主服务器同步。由于主服务器会场时确保所有其NIS映射的变动都与从服务器知会，因此这些项并不是绝对必需的，尽管如此，强制更新能够保证这些对依赖于服务器的系统至关重要的口令信息及时地同步，同时，在繁忙的网络上，有时也会出现映射同步更新不完全的情况。

现在，在从服务器上执行`/etc/netstart`，就可以启动NIS服务了。

25.4.4.3 NIS 客户机

NIS 客户机通过ypbind 服务程序来与特定的NIS 服务器建立一种称作绑定的联系。ypbind 会检查系统的默认域(这是通过domainname 命令来设置的), 并开始在本机网络上广播RPC 请求。这些请求会指定ypbind 尝试绑定的域名。如果已经配置了服务器, 并且这些服务器接到了广播, 它将回应ypbind, 后者则记录服务器的地址。如果有多个可用的服务器(例如一个主服务器, 加上多个从服务器), ypbind 将使用第一个响应的地址。从这一时刻开始, 客户机把所有的NIS 请求直接发给那个服务器。ypbind 偶尔会“ping”服务器以确认其仍然在正常运行。如果在合理的时间内没有得到响应, 则ypbind 会把域标记为未绑定, 并再次发起广播, 以期找到另一台服务器。

25.4.4.3.1 设置NIS 客户机

配置一台FreeBSD 机器作为NIS 客户机是非常简单的。

1. 编辑/etc/rc.conf 文件, 并在其中加上下面几行, 以设置NIS 域名, 并在网络启动时启动ypbind:

```
nisdomainname="test-domain"
nis_client_enable="YES"
```

2. 要从NIS 服务器导入所有的口令项, 需要从您的/etc/master.passwd 文件中删除所有用户, 并使用vipw 在这个文件的最后一行加入:

```
+:::~::~:
```

注意: 这一行将让NFS 服务器的口令映射中的帐号能够登录。也有很多修改这一行来配置NIS 客户机的办法。请参见稍后的netgroups 小节 以了解进一步的情况。要了解更多信息, 可以参阅O'Reilly 的Managing NFS and NIS 这本书。

注意: 需要至少保留一个本地帐号(也就是不通过NIS 导入) 在您的/etc/master.passwd 文件中, 而这个帐号应该是wheel 组的成员。如果NIS 发生不测, 这个帐号可以用来远程登录, 成为root, 并修正问题。

3. 要从NIS 服务器上导入组信息, 需要在/etc/group 文件末尾加入:

```
+:::~::~:
```

完成这些步骤之后, 就应该可以通过运行ypcat passwd 来看到NIS 服务器的口令映射了。

25.4.5 NIS 的安全性

基本上, 任何远程用户都可以发起一个RPC 到ypserv(8) 并获得您的NIS 映射的内容, 如果远程用户了解您的域名的话。要避免这类未经授权的访问, ypserv(8) 支持一个称为“securenets” 的特性, 用以将访问限制在一组特定的机器上。在启动过程中, ypserv(8) 会尝试从/var/yp/securenets 中加载securenet 信息。

注意: 这个路径随-p 参数改变。这个文件包含了一些项, 每一项中包含了一个网络标识和子网掩码, 中间用空格分开。以“#” 开头的行会被认为是注释。示范的securenets 文件如下所示:

```
# allow connections from local host -- mandatory
127.0.0.1      255.255.255.255
# allow connections from any host
# on the 192.168.128.0 network
192.168.128.0 255.255.255.0
# allow connections from any host
# between 10.0.0.0 to 10.0.15.255
# this includes the machines in the testlab
10.0.0.0      255.255.240.0
```

如果ypserv(8) 接到了来自匹配上述任一规则的地址的请求，则它会正常处理请求。反之，则请求将被忽略，并记录一条警告信息。如果/var/yp/securenets 文件不存在，则ypserv 会允许来自任意主机的请求。

ypserv 程序也支持Wietse Venema 的**TCP Wrapper** 软件包。这样，管理员就能够使用**TCP Wrapper** 的配置文件来代替/var/yp/securenets 完成访问控制。

注意：尽管这两种访问控制机制都能够提供某种程度的安全，但是，和特权端口检查一样，它们无法避免“IP 伪造”攻击。您的防火墙应该阻止所有与NIS 有关的访问。

使用/var/yp/securenets 的服务器，可能会无法为某些使用陈旧的**TCP/IP** 实现的**NIS** 客户机服务。这些实现可能会在广播时，将主机位都设置为0，或在计算广播地址时忽略子网掩码。尽管这些问题可以通过修改客户机的配置来解决，其他一些问题也可能导致不得不淘汰那些客户机系统，或者不使用/var/yp/securenets。

在使用陈旧的**TCP/IP** 实现的系统上，使用/var/yp/securenets 是一个非常糟糕的做法，因为这将导致您的网络上的**NIS** 丧失大部分功能。

使用**TCP Wrapper** 软件包，会导致您的**NIS** 服务器的响应延迟增加。而增加的延迟，则可能会导致客户端程序超时，特别是在繁忙的网络或者很慢的**NIS** 服务器上。如果您的某个客户机因此而产生一些异常，则应将这些客户机变为**NIS** 从服务器，并强制其绑定自己。

25.4.6 不允许某些用户登录

在我们的实验室中，basie 这台机器，是一台教员专用的工作站。我们不希望将这台机器拿出**NIS** 域，而主**NIS** 服务器上的passwd 文件，则同时包含了教员和学生的帐号。这时应该怎么做？

有一种办法来禁止特定的用户登录机器，即使他们身处**NIS** 数据库之中。要完成这一工作，只需要在客户机的/etc/master.passwd 文件中加入一些-username 这样的项，其中，username 是希望禁止登录的用户名。一般推荐使用vipw 来完成这个工作，因为vipw 会对您在/etc/master.passwd 文件上所作的修改进行合法性检查，并在编辑结束时重新构建口令数据库。例如，如果希望禁止用户bill 登录basie，我们应该：

```
basie# vipw
[在末尾加入 -bill, 并退出]
vipw: rebuilding the database...
vipw: done

basie# cat /etc/master.passwd

root:[password]:0:0::0:0:The super-user:/root:/bin/csh
```



```
toor:[password]:0:0::0:0:The other super-user:/root:/bin/sh
daemon*:1:1::0:0:Owner of many system processes:/root:/sbin/nologin
operator*:2:5::0:0:System &:/sbin/nologin
bin*:3:7::0:0:Binaries Commands and Source,,:/sbin/nologin
tty*:4:65533::0:0:Tty Sandbox:/sbin/nologin
kmem*:5:65533::0:0:KMem Sandbox:/sbin/nologin
games*:7:13::0:0:Games pseudo-user:/usr/games:/sbin/nologin
news*:8:8::0:0:News Subsystem:/sbin/nologin
man*:9:9::0:0:Mister Man Pages:/usr/share/man:/sbin/nologin
bind*:53:53::0:0:Bind Sandbox:/sbin/nologin
uucp*:66:66::0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/libexec/uucp/uucico
xten*:67:67::0:0:X-10 daemon:/usr/local/xten:/sbin/nologin
pop*:68:6::0:0:Post Office Owner:/nonexistent:/sbin/nologin
nobody*:65534:65534::0:0:Unprivileged user:/nonexistent:/sbin/nologin
+:::
-bill

basie#
```

25.4.7 使用Netgroups

Contributed by Udo Erdelhoff.

前一节介绍的方法，在您需要为非常少的用户和/或机器进行特殊的规则配置时还算凑合。在更大的网络上，您一定会忘记禁止某些用户登录到敏感的机器上，或者，甚至必须单独地修改每一台机器的配置，因而丢掉了NIS 最重要的优越性：集中式 管理。

NIS 开发人员为这个问题提供的解决方案，被称作netgroups。它们的作用和语义，基本上可以等同于UNIX 文件系统上使用的组。主要的区别是它们没有数字化的ID，以及可以在netgroup 中同时包含用户和其他netgroup。

Netgroups 被设计用来处理大的、复杂的包含数百用户和机器的网络。一方面，在您不得不处理这类情形时，这是一个很有用的东西。而另一方面，它的复杂性又使得通过非常简单的例子很难解释netgroup 到底是什么。这一节的其余部分的例子将展示这个问题。

假设您在实验室中成功地部署NIS 引起了上司的兴趣。您接下来的任务是将NIS 域扩展，以覆盖校园中的一些其他的机器。下面两个表格中包括了新用户和新机器，及其简要说明。

用户名	说明
alpha, beta	IT 部门的普通雇员
charlie, delta	IT 部门的学徒
echo, foxtrott, golf, ...	普通雇员
able, baker, ...	目前的实习生

机器名	说明
war, death, famine, pollution	最重要的服务器。只有IT 部门的雇员才允许登录这些机器。
pride, greed, envy, wrath, lust, sloth	不太重要的服务器，所有IT 部门的成员，都可以登录这些机器。

机器名	说明
one, two, three, four, ...	普通工作站。只有真正的雇员才允许登录这些机器。
trashcan	一台不包含关键数据的旧机器。即使是实习生，也允许登录它。

如果您尝试通过一个一个地阻止用户来实现这些限制，就需要在每一个系统的passwd 文件中，为每一个不允许登录该系统的用户添加对应的-user 行。如果忘记了任何一个，就可能会造成问题。在进行初始配置时，正确地配置也许不是什么问题，但随着日复一日地添加新用户，总有一天您会忘记为新用户添加某个行。毕竟，Murphy 是一个乐观的人。

使用netgroups 来处理这一状况可以带来许多好处。不需要单独地处理每一个用户；您可以赋予用户一个或多个netgroups 身份，并允许或禁止某一个netgroup 的所有成员登录。如果添加了新的机器，只需要定义netgroup 的登录限制。如果增加了新用户，也只需要将用户加入一个或多个netgroup。这些变化是相互独立的：不再需要“对每一个用户和机器执行……”。如果您的NIS 配置经过了谨慎的规划，就只需要修改一个中央的配置文件，就能够允许或禁止访问某台机器的权限了。

第一步是初始化NIS 映射netgroup。FreeBSD 的ypinit(8) 默认情况下并不创建这个映射，但它的NIS 实现能够在创建这个映射之后立即对其提供支持。要创建空映射，简单地输入

```
ellington# vi /var/yp/netgroup
```

并开始增加内容。在我们的例子中，至少需要四个netgroup：IT 雇员，IT 学徒，普通雇员和实习生。

```
IT_EMP    (,alpha,test-domain)    (,beta,test-domain)
IT_APP    (,charlie,test-domain)  (,delta,test-domain)
USERS     (,echo,test-domain)     (,foxtrott,test-domain) \
          (,golf,test-domain)
INTERNS   (,able,test-domain)     (,baker,test-domain)
```

IT_EMP, IT_APP 等等，是netgroup 的名字。每一个括号中的组中，都有一些用户帐号。组中的三个字段是：

1. 在哪些机器上能够使用这些项。如果不指定主机名，则项在所有机器上都有效。如果指定了主机，则很容易造成混淆。
2. 属于这个netgroup 的帐号。
3. 帐号的NIS 域。您可以从其他NIS 域中把帐号导入到您的netgroup 中，如果您管理多个NIS 域的话。

每一个字段都可以包括通配符。参见netgroup(5) 了解更多细节。

注意：Netgroup 的名字一般来说不应超过8 个字符，特别是当您的NIS 域中有机器打算运行其它操作系统的时候。名字是区分大小写的；使用大写字母作为netgroup 的名字，能够让您更容易地区分用户、机器和netgroup 的名字。

某些NIS 客户程序(FreeBSD 以外的那些) 可能无法处理含有大量项的netgroup。例如，某些早期版本的SunOS 会在netgroup 中包含多于15 个项时出现问题。要绕过这个问题，可以创建多个子netgroup，每一个中包含少于15 个用户，以及一个包含所有子netgroup 的真正的netgroup：

```
BIGGRP1   (,joe1,domain) (,joe2,domain) (,joe3,domain) [...]
BIGGRP2   (,joe16,domain) (,joe17,domain) [...]
BIGGRP3   (,joe31,domain) (,joe32,domain)
BIGGROUP  BIGGRP1 BIGGRP2 BIGGRP3
```

如果需要超过225 个用户，可以继续重复上面的过程。

激活并分发新的NIS 映射非常简单：

```
ellington# cd /var/yp
ellington# make
```

这个操作会生成三个NIS 映射，即netgroup、netgroup.byhost 和netgroup.byuser。用ypcat(1) 可以检查这些NIS 映射是否可用了：

```
ellington% ypcat -k netgroup
ellington% ypcat -k netgroup.byhost
ellington% ypcat -k netgroup.byuser
```

第一个命令的输出，应该与/var/yp/netgroup 的内容相近。第二个命令，如果没有指定本机专有的netgroup，则应该没有输出。第三个命令，则用于显示某个用户对应的netgroup 列表。

客户机的设置也很简单。要配置服务器war，只需进入vipw(8) 并把

```
+:::~:
```

改为

```
+@IT_EMP:~:
```

现在，只有netgroup IT_EMP 中定义的用户会被导入到war 的口令数据库中，因此只有这些用户能够登录。

不过，这个限制也会作用于shell 的~，以及所有在用户名和数字用户ID 之间实施转换的函数的功能。换言之，cd ~user 将不会正常工作，而ls -l 也将显示数字的ID 而不是用户名，并且find . -user joe -print 将失败，并给出No such user 的错误信息。要修正这个问题，您需要导入所有的用户项，而不允许他们登录服务器。

这可以通过在/etc/master.passwd 加入另一行来完成。这行的内容是：

+:::~:/sbin/nologin，意思是“导入所有的项，但导入项的shell 则替换为/sbin/nologin”。通过在/etc/master.passwd 中增加默认值，可以替换掉passwd 中的任意字段。

警告：务必确认+:::~:/sbin/nologin 这一行出现在+@IT_EMP:~: 之后。否则，所有从NIS 导入的用户帐号将以/sbin/nologin 作为登录shell。

完成上面的修改之后，在IT 部门有了新员工时，只需修改一个NIS 映射就足够了。您也可以类似的方法，在不太重要的服务器上，把先前本地版本的/etc/master.passwd 中的+:::~: 改为：

```
+@IT_EMP:~:
+@IT_APP:~:
+:::~:/sbin/nologin
```

相关的用于普通工作站的配置则应是：

```
+@IT_EMP:~:
+@USERS:~:
```

```
+:::::::::/sbin/nologin
```

一切平安无事，直到数周后，有一天策略发生了变化：IT 部门也开始招收实习生了。IT 实习生允许使用普通的终端，以及不太重要的服务器；而IT 学徒，则可以登录主服务器。您增加了新的netgroup **IT_INTERN**，以及新的IT 实习生到这个netgroup 并开始修改每一台机器上的配置……老话说得好：“牵一发，动全身”。

NIS 通过netgroup 来建立netgroup 的能力，正可以避免这样的情形。一种可能的方法是建立基于角色的netgroup。例如，您可以创建称为**BIGSRV**的netgroup，用于定义最重要的服务器上的登录限制，以及另一个成为**SMALLSRV**的netgroup，用以定义次重要的服务器，以及第三个，用于普通工作站的netgroup **USERBOX**。这三个netgroup 中的每一个，都包含了允许登录到这些机器上的所有netgroup。您的NIS 映射中的新项如下所示：

```
BIGSRV    IT_EMP  IT_APP
SMALLSRV  IT_EMP  IT_APP  ITINTERN
USERBOX   IT_EMP  ITINTERN  USERS
```

这种定义登录限制的方法，在您能够将机器分组并加以限制的时候可以工作的相当好。不行的是，这是种例外，而非规律。多数时候，需要按机器去定义登录限制。

与机器相关的netgroup 定义，是处理上述策略改动的另一种可能的方法。此时，每台机器的/etc/master.passwd 中，都包含两个“+”开头的行。第一个用于添加允许登录的netgroup 帐号，而第二个则用于增加其它帐号，并把shell 设置为/sbin/nologin。使用“全大写”的机器名作为netgroup 名是个好主意。换言之，这些行应该类似于：

```
+@BOXNAME:::::::::
+:::::::::/sbin/nologin
```

一旦在所有机器上都完成了这样的修改，就再也不需要修改本地的/etc/master.passwd 了。所有未来的修改都可以在NIS 映射中进行。这里是一个例子，其中展示了在这一应用情景中所需要的netgroup 映射，以及其它一些常用的技巧：

```
# Define groups of users first
IT_EMP    (,alpha,test-domain)    (,beta,test-domain)
IT_APP    (,charlie,test-domain)  (,delta,test-domain)
DEPT1     (,echo,test-domain)     (,foxtrott,test-domain)
DEPT2     (,golf,test-domain)     (,hotel,test-domain)
DEPT3     (,india,test-domain)    (,juliet,test-domain)
ITINTERN  (,kilo,test-domain)     (,lima,test-domain)
D_INTERNS (,able,test-domain)     (,baker,test-domain)
#
# Now, define some groups based on roles
USERS     DEPT1  DEPT2  DEPT3
BIGSRV    IT_EMP IT_APP
SMALLSRV  IT_EMP IT_APP  ITINTERN
USERBOX   IT_EMP ITINTERN  USERS
#
# And a groups for a special tasks
# Allow echo and golf to access our anti-virus-machine
SECURITY IT_EMP (,echo,test-domain) (,golf,test-domain)
#
# machine-based netgroups
# Our main servers
```

```

WAR          BIGSRV
FAMINE       BIGSRV
# User india needs access to this server
POLLUTION    BIGSRV  (,india,test-domain)
#
# This one is really important and needs more access restrictions
DEATH        IT_EMP
#
# The anti-virus-machine mentioned above
ONE          SECURITY
#
# Restrict a machine to a single user
TWO          (,hotel,test-domain)
# [...more groups to follow]

```

如果您正使用某种数据库来管理帐号，应该可以使用您的数据库的报告工具来创建映射的第一部分。这样，新用户就自动地可以访问这些机器了。

最后的提醒：使用基于机器的netgroup并不是普适的。如果正在为学生实验室部署数十台甚至上百台同样的机器，您应该使用基于角色的netgroup，而不是基于机器的netgroup，以便把NIS映射的尺寸保持在一个合理的范围内。

25.4.8 需要牢记的事项

这里是一些其它在使用NIS环境时需要注意的地方。

- 每次需要在实验室中增加新用户时，必须只在NIS服务器上加入用户，而且一定要记得重建NIS映射。如果您忘记了这样做，新用户将无法登录除NIS主服务器之外的任何其它机器。例如，如果要在实验室增加新用户jsmith，我们需要：

```

# pw useradd jsmith
# cd /var/yp
# make test-domain

```

也可以运行adduser jsmith而不是pw useradd jsmith.

- 将管理用的帐号排除在NIS映射之外。一般来说，您不希望这些管理帐号和口令被扩散到那些包含不应使用它们的用户的机器上。
- 确保NIS主和从服务器的安全，并尽可能减少其停机时间。如果有人攻入或简单地关闭这些机器，则整个实验室的任也就无法登录了。

这是集中式管理系统中最薄弱的环节。如果没有保护好NIS服务器，您就有大批愤怒的用户需要对付了！

25.4.9 NIS v1 兼容性

FreeBSD的ypserv提供了某些为NIS v1客户提供服务的支持能力。FreeBSD的NIS实现，只使用NIS v2协议，但其它实现可能会包含v1协议，以提供对旧系统的向下兼容能力。随这些系统提供的ypbind服务将首先尝试绑定NIS v1服务器，即使它们并不真的需要它(有些甚至可能会一直广播搜索请求，即使已经从某台v2服务器得到了回应也是如此)。注意，尽管支持一般的客户机调用，这个版本的ypserv并不能处理v1

的映射传送请求；因而，它就不能与较早的支持v1协议的NIS服务器配合使用，无论是作为主服务器还是从服务器。幸运的是，现今应该已经没有仍然在用的这样的服务器了。

25.4.10 同时作为NIS 客户机的NIS 服务器

在多服务器域的环境中，如果服务器同时作为NIS客户，在运行ypserv时要特别小心。一般来说，强制服务器绑定自己要比允许它们广播绑定请求要好，因为这种情况下它们可能会相互绑定。某些怪异的故障，很可能是由于某一台服务器停机，而其它服务器都依赖其服务所导致的。最终，所有的客户机都会超时并绑定到其它服务器，但这个延迟可能会相当可观，而且恢复之后仍然存在再次发生此类问题的隐患。

您可以强制一台机器绑定到特定的服务器，这是通过ypbind的-s参数来完成的。如果不希望每次启动NIS服务器时都手工完成这项工作，可以在/etc/rc.conf中加入：

```
nis_client_enable="YES" # run client stuff as well
nis_client_flags="-S NIS domain,server"
```

参见ypbind(8)以了解更多情况。

25.4.11 口令格式

在实现NIS时，口令格式的兼容性问题是一种最为常见的问题。假如您的NIS服务器使用DES加密口令，则它只能支持使用DES的客户机。例如，如果您的网络上有Solaris NIS客户机，则几乎肯定需要使用DES加密口令。

要检查您的服务器和客户机使用的口令格式，需要查看/etc/login.conf。如果主机被配置为使用DES加密的口令，则default class将包含类似这样的项：

```
default:\
:passwd_format=des:\
:copyright=/etc/COPYRIGHT:\
[Further entries elided]
```

其他一些可能的passwd_format包括blf和md5（分别对应于Blowfish和MD5加密口令）。

如果修改了/etc/login.conf，就必须重建登录性能数据库，这是通过以root身份运行下面的程序来完成的：

```
# cap_mkdb /etc/login.conf
```

注意：已经在/etc/master.passwd中的口令的格式不会被更新，直到用户在登录性能数据库重建之后首次修改口令为止。

接下来，为了确保所有的口令都按照您选择的格式加密了，还需要检查/etc/auth.conf中crypt_default给出的优先选择的口令格式。要完成此工作，将您选择的格式放到列表的第一项。例如，当使用DES加密的口令时，对应项应为：

```
crypt_default = des blf md5
```

在每一台基于FreeBSD的NIS服务器和客户机上完成上述工作之后，就可以肯定您的网络上它们都在使用同样的口令格式了。如果在NIS客户机上做身份验证时发生问题，这也是第一个可能出现问题的地方。注意：如果您希望在混合的网络上部署NIS服务器，可能就需要在所有系统上都使用DES，因为这是所有系统都能够支持的最低限度的公共标准。

25.5 网络自动配置(DHCP)

Written by Greg Sutter.

25.5.1 什么是DHCP?

DHCP，动态主机配置协议，是一种让系统得以连接到网络上，并获取所需要的配置参数手段。FreeBSD 6.0 之前的版本，采用的是ISC (Internet Software Consortium) 的DHCP 客户端(dhclient(8)) 实现。更高版本使用的则是来自OpenBSD 3.7 的OpenBSD dhclient。这里提供的所有关于dhclient 的信息，都是以ISC 或OpenBSD DHCP 客户端程序为准的。DHCP 服务器是ISC 软件包的一部分。

25.5.2 这一节都介绍哪些内容

这一节描述了ISC 和DHCP 系统中的客户端，以及和ISC DHCP 系统中的服务器端的组件。客户端程序，dhclient，是随FreeBSD 作为它的一部分提供的；而服务器部分，则可以通过net/isc-dhcp3-server port 得到。dhclient(8)、dhcp-options(5)、以及dhclient.conf(5) 联机手册，加上下面所介绍的参考文献，都是非常有用的资源。

25.5.3 它如何工作

当DHCP 客户程序，dhclient 在客户机上运行时，它会开始广播请求配置信息的信息。默认情况下，这些请求是在UDP 端口68 上。服务器通过UDP 67 给出响应，向客户机提供一个IP 地址，以及其他有关的配置参数，例如子网掩码、路由器，以及DNS 服务器。所有这些信息都会以DHCP “lease” 的形式给出，并且只在一段特定的时间内有效(这是由DHCP 服务器的维护者配置的)。这样，那些已经断开网络的客户机使用的陈旧的IP 地址就能被自动地回收了。

DHCP 客户程序可以从服务器端获取大量的信息。关于能获得的信息的详细列表，请参考dhcp-options(5)。

25.5.4 FreeBSD 集成

FreeBSD 完全地集成了ISC 或OpenBSD 的DHCP 客户端，dhclient (取决于您运行的FreeBSD 版本)。DHCP 客户端被安装程序直接支持，并且是基本系统的一部分。这使得您不再需要去了解那些已经运行了DHCP 服务器的网络的具体配置参数。从FreeBSD 3.2 开始，每一个发行版中均包含dhclient。

sysinstall 能够支持DHCP。在sysinstall 中配置网络接口时，它询问的第二个问题便是：“Do you want to try DHCP configuration of the interface? (您是否希望在此接口上尝试DHCP 配置?)”。如果做肯定的回答，则将运行dhclient，一旦成功，则将自动地填写网络配置信息。

要在系统启动时使用DHCP，您必须做两件事：

- 您的内核中，必须包含**bpf**设备。如果需要这样做，需要将**device bpf** (对于FreeBSD 4.X来说，则应该是**pseudo-device bpf**) 添加到内核的编译配置文件中，并重新编译内核。要了解关于编译内核的进一步信息，请参见第8章。

bpf设备已经是FreeBSD发行版中默认的**GENERIC**内核的一部分了，因此如果您没有对内核进行定制，则不用创建一份新的内核配置文件，**DHCP**就能工作了。

注意: 对于那些安全意识很强的人来说，您应该知道**bpf**也是包侦听工具能够正确工作的条件之一(当然，它们还需要以**root**身份运行才行)。**bpf**是使用**DHCP**所必须的，但如果您对安全非常敏感，则很可能会有理由不把**bpf**加入到您的内核配置中，直到您真的需要使用**DHCP**为止。

- 编辑您的/etc/rc.conf 并加入下面的设置:

```
ifconfig_fxp0="DHCP"
```

注意: 务必将**fxp0**替换为您希望自动配置的网络接口的名字，您可以在第11.8节找到更进一步的介绍。

如果您希望使用另一位置的**dhclient**，或者需要给**dhclient**传递其他参数，还可以添加下面的配置(根据需要进行修改):

```
dhcp_program="/sbin/dhclient"
dhcp_flags=""
```

DHCP服务器，**dhcpcd**，是作为net/isc-dhcp3-server port的一部分提供的。这个port包括了ISC **DHCP**服务器及其文档。

25.5.5 文件

- /etc/dhclient.conf

dhclient需要一个配置文件，**/etc/dhclient.conf**。一般说来，这个文件中只包括注释，而默认值基本上都是合理的。这个配置文件在**dhclient.conf(5)**联机手册中进行了进一步的阐述。

- /sbin/dhclient

dhclient是一个静态连编的，它被安装到**/sbin**中。**dhclient(8)**联机手册给出了关于**dhclient**的进一步细节。

- /sbin/dhclient-script

dhclient-script是一个FreeBSD专用的**DHCP**客户端配置脚本。在**dhclient-script(8)**中对它进行了描述，但一般来说，用户不需要对其进行任何修改，就能够让一切正常运转了。

- /var/db/dhclient.leases

DHCP客户程序会维护一个数据库来保存有效的**lease**，它们被以日志的形式保存到这个文件中。**dhclient.leases(5)**给出了更为细致的介绍。

25.5.6 进阶读物

DHCP 协议的完整描述是RFC 2131 (<http://www.freessoft.org/CIE/RFC/2131/>)。关于它的其他信息资源的站点<http://www.dhcp.org/> 也提供了详尽的资料。

25.5.7 安装和配置DHCP 服务器

25.5.7.1 这一章包含哪些内容

这一章提供了关于如何在FreeBSD 系统上使用ISC (Internet 软件协会) 的DHCP 实现套件来架设DHCP 服务器的信息。

DHCP 套件中的服务器部分并没有作为FreeBSD 的一部分来提供, 因此您需要安装net/isc-dhcp3-server port 才能提供这个服务。请参见第4 章 以了解关于如何使用Ports Collection 的进一步详情。

25.5.7.2 安装DHCP 服务器

为了在您的FreeBSD 系统上进行配置以便作为DHCP 服务器来使用, 需要把bpf(4) 设备编译进内核。要完成这项工作, 需要将device bpf (如果使用FreeBSD 4.X 的话, 则写作pseudo-device bpf) 加入到您的内核配置文件中, 并重新联编内核。要得到关于如何联编内核的进一步信息, 请参见第8 章。

bpf 设备是FreeBSD 所附带的GENERIC 内核中已经联入的组件, 因此您并不需要为了让DHCP 正常工作而特地定制内核。

注意: 如果您有较强的安全意识, 应该注意bpf 同时也是让监听包程序能够正确工作的设备(尽管这类程序仍然需要以特权用户身份运行)。bpf 是 使用DHCP 所必需的, 但如果您对安全非常敏感, 您可能会不希望将bpf 放进内核, 直到您真的认为DHCP 是必需的为止。

接下来要做的是编辑示范的dhcpd.conf, 它由net/isc-dhcp3-server port 安装。默认情况下, 它的名字应该是/usr/local/etc/dhcpd.conf.sample, 在开始修改之前, 您需要把它复制为/usr/local/etc/dhcpd.conf。

25.5.7.3 配置DHCP 服务器

dhcpd.conf 包含了一系列关于子网和主机的定义, 下面的例子可以帮助您理解它:

```
option domain-name "example.com";❶
option domain-name-servers 192.168.4.100;❷
option subnet-mask 255.255.255.0;❸

default-lease-time 3600;❹
max-lease-time 86400;❺
ddns-update-style none;❻

subnet 192.168.4.0 netmask 255.255.255.0 {
    range 192.168.4.129 192.168.4.254;❼
    option routers 192.168.4.1;❽
```

```

}

host mailhost {
    hardware ethernet 02:03:04:05:06:07;⑨
    fixed-address mailhost.example.com;(10)
}

```

- ❶ 这个选项指定了提供给客户机作为默认搜索域的域名。请参考`resolv.conf(5)`以了解关于这一概念的详情。
- ❷ 这个选项用于指定一组客户机使用的DNS服务器，它们之间以逗号分隔。
- ❸ 提供给客户机的子网掩码。
- ❹ 客户机可以请求租约的有效期，而如果没有，则服务器将指定一个租约有效期，也就是这个值(单位是秒)。
- ❺ 这是服务器允许租出地址的最大时长。如果客户机请求了更长的租期，则它将得到一个地址，但其租期仅限于`max-lease-time`秒。
- ❻ 这个选项用于指定DHCP服务器在一个地址被接受或释放时是否应对应尝试更新DNS。在ISC实现中，这一选项是**必须指定的**。
- ❼ 指定地址池中可以用来分配给客户机的IP地址范围。在这个范围之间，以及其边界的IP地址将分配给客户机。
- ❽ 定义客户机的默认网关。
- ❾ 主机的硬件MAC地址(这样DHCP服务器就能够在接到请求时知道请求的主机身份)。
- (10) 指定总是得到同一IP地址的主机。请注意在此处使用主机名是对的，因为DHCP服务器会在返回租借地址信息之前自行解析主机名。

一旦您撰写完`dhcpd.conf`，就可以用下面的命令来启动服务：

```
# /usr/local/etc/rc.d/isc-dhcpd.sh start
```

如果未来您需要修改服务器的配置，请务必牢记发送SIGHUP信号给`dhcpd`并不会导致配置文件的重新加载，而这在其他服务程序中则是比较普遍的约定。您需要发送SIGTERM信号来停止进程，然后使用上面的命令来重新启动它。

25.5.7.4 文件

- `/usr/local/sbin/dhcpd`

`dhcpd`是静态连接的，并安装到`/usr/local/sbin`中。随`port`安装的`dhcpd(8)`联机手册提供了关于`dhcpd`更为详尽的信息。

- `/usr/local/etc/dhcpd.conf`

`dhcpd`需要配置文件，即`/usr/local/etc/dhcpd.conf`才能够向客户机提供服务。这个文件需要包括应提供给客户机的所有信息，以及关于服务器运行的其他信息。此配置文件的详细描述可以在随`port`安装的`dhcpd.conf(5)`联机手册上找到。

- `/var/db/dhcpd.leases`

DHCP 服务器会维护一个它签发的租用地地址数据库，并保存在这个文件中，这个文件是以日志的形式保存的。随port 安装的dhcpcd.leases(5) 联机手册提供了更详细的描述。

- /usr/local/sbin/dhcrelay

dhcrelay 在更为复杂的环境中，可以用来支持使用DHCP 服务器转发请求给另一个独立网络上的DHCP 服务器。如果您需要这个功能，需要安装net/isc-dhcp3-relay port。dhcrelay(8) 联机手册提供了更为详尽的介绍。

25.6 域名系统(DNS)

Contributed by Chern Lee.

25.6.1 纵览

FreeBSD 在默认情况下使用一个版本的BIND (Berkeley Internet Name Domain)，这是目前最为流行的DNS 协议实现。DNS 是一种协议，可以通过它将域名同IP 地址相互对应。例如，查询www.FreeBSD.org 将得到FreeBSD Project 的web 服务器的IP 地址，而查询ftp.FreeBSD.org 则将得到响应的FTP 机器的IP 地址。类似地，也可以做相反的事情。查询IP 地址可以得到其主机名。当然，完成DNS 查询并不需要在系统中运行域名服务器。

DNS 在Internet 上通过一组略显复杂的权威根域名服务器来组织，它的其余部分则由较小规模的域名服务器组成，这些服务器提供少量的域名解析服务，并对域名信息进行缓存。

这份文档介绍的是BIND 8.x，因为它是FreeBSD 中使用的稳定版本。FreeBSD 5.3 以及更高版本则包含了BIND9 及其配置的说明可以在这一章的后一部分找到。使用FreeBSD 5.2 以及更早版本的用户，可以通过net/bind9 port 来安装BIND9。

RFC1034 和RFC1035 定义了DNS 协议。

目前，BIND 由Internet Software Consortium <http://www.isc.org/> 维护。

25.6.2 术语

要理解这份文档，需要首先了解一些相关的DNS 术语。

术语	定义
正向DNS (Forward DNS)	将域名映射到IP 地址
原点(Origin)	表示特定域文件所在的域
named, BIND, 域名服务器(name server)	在FreeBSD 中BIND 域名服务器软件包的常见叫法
解析器(Resolver)	计算机用以向域名服务器查询域名信息的一个系统进程
反向DNS (Reverse DNS)	与正向DNS 相对；将IP 地址映射为主机名
根域	Internet 域层次的起点。所有的域都在根域之下，类似文件系统中，文件都在根目录之下那样。
域(Zone)	独立的域，子域，或者由同一机构管理的DNS 的一部分。

域的例子：

- . 是根域。
- org. 是一个根域下的域。
- example.org. 是org. 之下的域。
- foo.example.org. 是example.org. 域的子域。
- 1.2.3.in-addr.arpa 是用于表达3.2.1.* IP 地址空间之下所有IP 地址的域。

如您所见，域名中最细节的部分在它的左边。举例来说，example.org. 要比org. 更小，就像org. 要比根域更小一样。主机名的格局和文件系统类似：/dev 目录在根目录中，等等。

25.6.3 运行域名服务器的理由

域名服务器通常会有两种形式：权威域名服务器，以及缓存域名服务器。

下列情况需要有权威域名服务器：

- 想要向全世界提供DNS 信息，并对请求给出权威应答。
- 注册了类似example.org 的域，而需要将IP 指定到其下的主机名上。
- 某个IP 地址块需要反向DNS 项(IP 到主机名)。
- 需要备份服务器，或常说的从(slave) 服务器，在主服务器出现问题或无法访问时来应答查询请求。

下列情况需要有缓存域名服务器：

- 本地的DNS 服务器能够缓存，并比直接向外界的域名服务器请求更快地得到应答。
- 减少所需的总体网络流量(DNS 流量通常占全部Internet 流量的5% 或更多)。

当有人查询www.FreeBSD.org 时，解析器通常会向上级ISP 的域名服务器发出请求，并获得回应。如果有本地的缓存DNS 服务器，查询只有在第一次被缓存DNS 服务器发到外部世界。其他的查询不会发向局域网外，因为它们已经有在本地的缓存了。

25.6.4 DNS 如何运作

在FreeBSD 中，BIND 服务程序被称为**named**，其原因显而易见。

文件	描述
named	BIND 服务程序
ndc	域名服务控制程序
/etc/namedb	BIND 存放域名信息的位置
/etc/namedb/named.conf	域名服务配置文件

域文件通常被放在/etc/namedb 目录中，它们包含域名服务器所提供的DNS 域的信息。

25.6.5 启动BIND

由于BIND 会在默认情况下安装，因此配置它相对而言很简单。

要确保named 服务程序在引导时被自动启动，把下面的行加到/etc/rc.conf 中：

```
named_enable="YES"
```

要手工启动服务(在完成配置之后)：

```
# ndc start
```

25.6.6 配置文件

25.6.6.1 使用make-localhost

一定要：

```
# cd /etc/namedb
# sh make-localhost
```

以便创建正确的本地DNS 反向解析域文件/etc/namedb/master/localhost.rev.

25.6.6.2 /etc/namedb/named.conf

```
// $FreeBSD$
//
// Refer to the named(8) manual page for details.  If you are ever going
// to setup a primary server, make sure you've understood the hairy
// details of how DNS is working.  Even with simple mistakes, you can
// break connectivity for affected parties, or cause huge amount of
// useless Internet traffic.

options {
    directory "/etc/namedb";

    // In addition to the "forwarders" clause, you can force your name
    // server to never initiate queries of its own, but always ask its
    // forwarders only, by enabling the following line:
    //
    //     forward only;

    // If you've got a DNS server around at your upstream provider, enter
    // its IP address here, and enable the line below.  This will make you
    // benefit from its cache, thus reduce overall DNS traffic in the
    // Internet.
    /*
        forwarders {
            127.0.0.1;
        };
    */
}
```

如注视所说，要从上级的缓存中受益，可以在此处启用**forwarders**。在一般情况下，域名服务器会逐级地查询Internet 来找到特定的域名服务器，直到得到答案为止。启用这个将让它首先查询上级域名服务器(或另外提供的域名服务器)，从而从它们的缓存中得到结果。如果上级域名服务器的负载很重，在更快的域名服务器上启用它将有助于改善服务品质。

警告: 127.0.0.1 不会 正常工作。一定要把地址改为您上级服务器的IP 地址。

```

/*
 * If there is a firewall between you and name servers you want
 * to talk to, you might need to uncomment the query-source
 * directive below. Previous versions of BIND always asked
 * questions using port 53, but BIND 8.1 uses an unprivileged
 * port by default.
 */
// query-source address * port 53;

/*
 * If running in a sandbox, you may have to specify a different
 * location for the dumpfile.
 */
// dump-file "s/named_dump.db";
};

// Note: the following will be supported in a future release.
/*
host { any; } {
    topology {
        127.0.0.0/8;
    };
};
*/

// Setting up secondaries is way easier and the rough picture for this
// is explained below.
//
// If you enable a local name server, don't forget to enter 127.0.0.1
// into your /etc/resolv.conf so this server will be queried first.
// Also, make sure to enable it in /etc/rc.conf.

zone "." {
    type hint;
    file "named.root";
};

zone "0.0.127.IN-ADDR.ARPA" {
    type master;
    file "localhost.rev";
};

// NB: Do not use the IP addresses below, they are faked, and only
// serve demonstration/documentation purposes!

```

```
//
// Example secondary config entries. It can be convenient to become
// a secondary at least for the zone where your own domain is in. Ask
// your network administrator for the IP address of the responsible
// primary.
//
// Never forget to include the reverse lookup (IN-ADDR.ARPA) zone!
// (This is the first bytes of the respective IP address, in reverse
// order, with ".IN-ADDR.ARPA" appended.)
//
// Before starting to setup a primary zone, better make sure you fully
// understand how DNS and BIND works, however. There are sometimes
// unobvious pitfalls. Setting up a secondary is comparably simpler.
//
// NB: Don't blindly enable the examples below. :-) Use actual names
// and addresses instead.
//
// NOTE!!! FreeBSD runs BIND in a sandbox (see named_flags in rc.conf).
// The directory containing the secondary zones must be write accessible
// to BIND. The following sequence is suggested:
//
//      mkdir /etc/namedb/s
//      chown bind:bind /etc/namedb/s
//      chmod 750 /etc/namedb/s
```

For more information on running BIND in a sandbox, see Running named in a sandbox.

```
/*
zone "example.com" {
    type slave;
    file "s/example.com.bak";
    masters {
        192.168.1.1;
    };
};

zone "0.168.192.in-addr.arpa" {
    type slave;
    file "s/0.168.192.in-addr.arpa.bak";
    masters {
        192.168.1.1;
    };
};
*/
```

在named.conf 中，这是一些转发用的从域以及反向域的例子。

对于每一个新域，域对应的项必须加到named.conf 中。

例如，最简单的用于example.org 域的条目类似下面的样子：

```
zone "example.org" {
    type master;
    file "example.org";
```

```
};
```

这是一个主域，它由type 语句标识出来，而信息则在/etc/namedb/example.org 域文件中，这是由file 语句指定的。

```
zone "example.org" {
type slave;
file "example.org";
};
```

在从域的例子中，域的信息从该域的某个主服务器传送过来，并保存在指定的文件中。如果主服务器死掉了或不可达，从域名服务器将使用这些传过来的域信息，从而完成应答。

25.6.6.3 域信息文件

以下是一个用于example.org 域的主域文件(保存为/etc/namedb/example.org):

```
$TTL 3600

example.org. IN SOA ns1.example.org. admin.example.org. (
                                5           ; Serial
                                10800        ; Refresh
                                3600         ; Retry
                                604800       ; Expire
                                86400 )      ; Minimum TTL

; DNS Servers
@      IN NS      ns1.example.org.
@      IN NS      ns2.example.org.

; Machine Names
localhost      IN A      127.0.0.1
ns1            IN A      3.2.1.2
ns2            IN A      3.2.1.3
mail           IN A      3.2.1.10
@             IN A      3.2.1.30

; Aliases
www           IN CNAME   @

; MX Record
@             IN MX      10      mail.example.org.
```

请注意以“.”结尾的主机名是全称主机名，而结尾没有“.”的则是相对于原点的主机名。例如，www 将被转换为www.原点. 在这个假想的域信息文件中，我们的原点是example.org.，因此www 将被当作www.example.org.。

域信息文件的格式如下：

记录名	IN	记录类型	值
-----	----	------	---

最常用的DNS 记录：

SOA

域权威开始

NS

权威域名服务器

A

主机地址

CNAME

别名对应的正规名称

MX

邮件传递服务器

PTR

域名指针(用于反向DNS)

```
example.org. IN SOA ns1.example.org. admin.example.org. (  
                    5                ; Serial  
                    10800             ; Refresh after 3 hours  
                    3600              ; Retry after 1 hour  
                    604800            ; Expire after 1 week  
                    86400 )           ; Minimum TTL of 1 day
```

example.org.

域名，同时也是这个域信息文件的原点。

ns1.example.org.

该域的主/权威域名服务器。

admin.example.org.

此域的负责人的电子邮件地址，其中“@”被换掉了。(<admin@example.org> 对应admin.example.org)

5

文件的序号。每次修改域文件时都必须增加这个数字。现今，许多管理员会考虑使用yyyymmddrr 这样的格式来表示序号。2001041002 通常表示上次修改于04/10/2001，而后面的02则表示在那天的第几次修改。序号非常重要，它用于通知从域服务器更新数据。

```
@          IN NS          ns1.example.org.
```

这是一个NS项。每个准备提供权威应答的服务器都必须有一个对应项。这里的@表示example.org.。@会被理解为原点。

```
localhost      IN A      127.0.0.1  
ns1             IN A      3.2.1.2
```

```

ns2          IN A      3.2.1.3
mail         IN A      3.2.1.10
@            IN A      3.2.1.30

```

A 记录代表及其名。如上面看到的, `ns1.example.org` 将解析为 `3.2.1.2`。在此再次使用了原点符, `@`, 它表示 `example.org` 应解析为 `3.2.1.30`。

```

www          IN CNAME  @

```

正规名记录通常用于对某台机器的别名给出对应的正式名字。在这个例子中, `www` 是名字为原点, 或者说 `example.org` (`3.2.1.30`) 那台机器的别名。CNAMEs 可以用来提供主机的别名, 或将同一名字在多台机器上作轮询。

```

@            IN MX     10      mail.example.org.

```

MX 记录表示哪个邮件服务器负责接收发到这个域的邮件。`mail.example.org` 是邮件服务器的主机名, 而 `10` 则是它的优先级。

可以有多台邮件服务器, 其优先级分别是 `3, 2, 1`。向 `example.org` 进行投递的邮件服务器首先会尝试优先级最高(数字最小)的 **MX**, 然后是较低优先级的, 等等, 直到成功地投递了邮件为止。

对于 `in-addr.arpa` 域名信息文件(反向DNS), 使用了同样的格式, 只是 **PTR** 项代替了 **A** 或 **CNAME** 的位置。

```

$TTL 3600

```

```

1.2.3.in-addr.arpa. IN SOA ns1.example.org. admin.example.org. (
                        5                      ; Serial
                        10800                   ; Refresh
                        3600                    ; Retry
                        604800                  ; Expire
                        3600 )                  ; Minimum

```

```

@            IN NS     ns1.example.org.
@            IN NS     ns2.example.org.

2           IN PTR     ns1.example.org.
3           IN PTR     ns2.example.org.
10          IN PTR     mail.example.org.
30          IN PTR     example.org.

```

这个文件给出了上述假想域中 **IP** 地址到域名的映射关系。

25.6.7 缓存域名服务器

缓存域名服务器是对任何域都不提供权威解析的域名服务器。它自己简单地完成查询, 并记住这些查询以备后续使用。要建立这样的服务器, 只需像平时一样配置一个域名服务器, 而不配置域就可以了。

25.6.8 在沙盒中运行named

要更安全地运行named(8)，应该以非特权用户来运行它，并配置为chroot(8)到一个沙盒目录中。这使得named 服务无法访问任何沙盒外面的东西。假如named 被攻破，这将减少它所能带来的破坏。默认情况下，FreeBSD 提供了名为bind 的用户和组来完成这样的目的。

注意：许多人建议不这样做，而named 配置为chroot，您应该在一个jail(8) 中运行named。这一节并不涵盖这种情形。

由于named 没有办法访问沙盒外面的任何东西(例如共享库，日志socket 等等)，您需要做许多事情来让named 正常工作。下面的清单假定沙盒是/etc/namedb 而您没有事先改过这个目录中的内容。以root 的身份完成下列步骤：

- 创建named 需要访问的所有目录：

```
# cd /etc/namedb
# mkdir -p bin dev etc var/tmp var/run master slave
# chown bind:bind slave var/*❶
```

❶ named 只需要写这些目录，这也是我们赋予它的全部权限。

- 重新组织基本的域和配置文件：

```
# cp /etc/localtime etc❶
# mv named.conf etc && ln -sf etc/named.conf
# mv named.root master
# sh make-localhost
# cat > master/named.localhost
$ORIGIN localhost.
$TTL 6h
@ IN SOA localhost. postmaster.localhost. (
1 ; serial
3600 ; refresh
1800 ; retry
604800 ; expiration
3600 ) ; minimum
IN NS localhost.
IN A 127.0.0.1
^D
```

❶ 这使得named 能够将正确的时间传递给syslogd(8)。

-

如果您在运行FreeBSD 在4.9-RELEASE 之前的版本，需要联编一个静态连接的named-xfer，并将其复制到沙盒中：

```
# cd /usr/src/lib/libisc
# make cleandir && make cleandir && make depend && make all
# cd /usr/src/lib/libbind
# make cleandir && make cleandir && make depend && make all
# cd /usr/src/libexec/named-xfer
```

```
# make cleandir && make cleandir && make depend && make NOSHARED=yes all
# cp named-xfer /etc/namedb/bin && chmod 555 /etc/namedb/bin/named-xfer❶
```

在把静态连接的named-xfer 装好之后需要清理一下，以免将过时的库或程序留在您的源代码副本中：

```
# cd /usr/src/lib/libisc
# make cleandir
# cd /usr/src/lib/libbind
# make cleandir
# cd /usr/src/libexec/named-xfer
# make cleandir
```

❶ 据说这一步有时会失败。如果您遇到这样的问题，执行下面的命令：

```
# cd /usr/src && make cleandir && make cleandir
```

并删除/usr/obj 目录：

```
# rm -fr /usr/obj && mkdir /usr/obj
```

这将把任何“垃圾”从您的源代码目录中删除，而后续工作将得以正常进行。

如果您运行FreeBSD 的4.9-RELEASE 或更新的版本，则默认情况下/usr/libexec 中的named-xfer 副本已经是静态连接的了。您可以简单地把它用cp(1) 复制到沙盒中。

- 做一个named 能够看到并写入的dev/null：

```
# cd /etc/namedb/dev && mknod null c 2 2
# chmod 666 null
```

- 将/var/run/ndc 符号链接到/etc/namedb/var/run/ndc：

```
# ln -sf /etc/namedb/var/run/ndc /var/run/ndc
```

注意：这个非常简单的措施有效地避免了您每次都必须指定-c 参数来启动ndc(8) 的麻烦。由于/var/run 中的内容会在启动时被删除，把上述命令加入到root 的crontab(5) 中，并指定@reboot 选项会很有用。

- 配置syslogd(8) 来创建一个named 可以写的log socket。要完成它，需要将-l /etc/namedb/dev/log 加到/etc/rc.conf 的syslogd_flags 变量中。

- 启动named 并让它自动地把自己chroot 到沙盒中，方法是把下面的内容加到/etc/rc.conf：

```
named_enable="YES"
named_flags="-u bind -g bind -t /etc/namedb /etc/named.conf"
```

注意：请注意配置文件/etc/named.conf 是以相对于沙盒的完整路径来指定的，例如上面那一行，文件所在的目录实际上是/etc/namedb/etc/named.conf。

下一步是编辑/etc/namedb/etc/named.conf 让named 直到需要加载哪些域，以及它们在磁盘上的位置。您可以用注释掉的那个例子(没有明确地注释掉的哪些和不在沙盒中运行DNS 服务器时的配置无异)：

```

options {
    directory "/";❶
    named-xfer "/bin/named-xfer";❷
    version ""; // Don't reveal BIND version
    query-source address * port 53;
};
// ndc control socket
controls {
    unix "/var/run/ndc" perm 0600 owner 0 group 0;
};
// Zones follow:
zone "localhost" IN {
    type master;
    file "master/named.localhost";❸
    allow-transfer { localhost; };
    notify no;
};
zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "master/localhost.rev";
    allow-transfer { localhost; };
    notify no;
};
zone "." IN {
    type hint;
    file "master/named.root";
};
zone "private.example.net" in {
    type master;
    file "master/private.example.net.db";
allow-transfer { 192.168.10.0/24; };
};
zone "10.168.192.in-addr.arpa" in {
    type slave;
    masters { 192.168.10.2; };
    file "slave/192.168.10.db";❹
};

```

- ❶ `directory` 语句被指定为`/`，因为所有的**named**需要在这个文件中(这相当于在“普通”模式下运行时的`/etc/namedb`)。
- ❷ 指定到**named-xfer**执行文件的完整路径(相对**named**的参照系)。这是必须的步骤，因为**named**在默认情况下会从`/usr/libexec`查找**named-xfer**。
- ❸ 指定文件名(相对于前面的**directory**语句指定的目录)，**named**将在这里查找域信息文件。
- ❹ 指定文件名(相对于前面的**directory**语句指定的目录)，**named**将在这里写入成功地从主服务器拿到的域信息文件副本。这使为什么我们在前面的步骤中将**slave**的属主改为**bind**的原因。

完成这些配置之后，您可以重新启动服务器，或重启**syslogd(8)**服务并启动**named(8)**，以确认**syslogd_flags**和**named_flags**的新值生效了。现在您应该已经在沙盒中运行**named**了！

25.6.9 安全

尽管BIND 是最为常用的DNS 实现，但它总是有一些安全问题。时常会有人发现一些可能的甚至可以利用的安全漏洞。

经常阅读CERT (<http://www.cert.org/>) 的安全公告并订阅FreeBSD 安全问题通知邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-security-notifications>) 会是一个帮助您时刻了解最新Internet 和FreeBSD 安全问题的好习惯。

提示: 如果出现了问题，将代码升级到最新版本并重新联编**named** 不会带来任何麻烦。

25.6.10 进一步阅读

BIND/**named** 联机手册: `ndc(8)` `named(8)` `named.conf(5)`

- 官方的ISC BIND 页面 (<http://www.isc.org/products/BIND/>)
- BIND FAQ (<http://www.nominum.com/getOpenSourceResource.php?id=6>)
- O'Reilly DNS 和BIND 第4版 (<http://www.oreilly.com/catalog/dns4/>)
- RFC1034 - 域名- 概念和工具 (<ftp://ftp.isi.edu/in-notes/rfc1034.txt>)
- RFC1035 - 域名- 实现及其标准 (<ftp://ftp.isi.edu/in-notes/rfc1035.txt>)

25.7 BIND9 和FreeBSD

撰写者Tom Rhodes.

随着FreeBSD 5.3 版本的发布，BIND9 DNS 服务软件正式成为了发行版本的一部分。新的安全特性，文件布局，以及自动的chroot(8) 配置也加入进来。这一节分成两部分，第一部分讨论了新增特性以及如何配置它们；后一部分则讲述了升级过程，帮助用户迁移到FreeBSD 5.3。从现在起，服务器将被简单地写作**named(8)** 或BIND。这一节跳过了前一节所介绍的那些术语，以及一些理论上的讨论；因此，建议您在继续阅读之前首先看一看前面的章节。

目前，**named** 的配置文件存放在`/var/named/etc/namedb/`，在使用之前需要进行一些修改。这也是进行绝大多数相关配置的地方。

25.7.1 主域的配置

要配置主域，应首先进入`/var/named/etc/namedb/` 并执行下面的命令：

```
# sh make-localhost
```

如果一切正常，则在**master** 目录中将出现两个新文件。它们的名字应该是用于本地域名解析的**localhost.rev**，以及用于IPv6 配置的**localhost-v6.rev**。作为默认的配置文件的，关于它们的配置已经在**named.conf** 文件中定义了。

25.7.2 从域的配置

可以通过配置从域来提供额外的域或子域的解析。多数情况下，`master/localhost.rev` 文件可以直接复制到`slave` 目录中并进行修改。此后，这些文件应该加入到`named.conf`，类似下面的`example.com` 配置：

```
zone "example.com" {
    type slave;
    file "slave/example.com";
    masters {
        10.0.0.1;
    };
};

zone "0.168.192.in-addr.arpa" {
    type slave;
    file "slave/0.168.192.in-addr.arpa";
    masters {
        10.0.0.1;
    };
};
```

请注意在这个例子中，主服务器的IP 地址指明了我们要从哪里把域传过来；那台服务器本身并不一定要作为对外的DNS 服务器来用。

25.7.3 系统的初始配置

为了让**named** 服务能够在系统启动时自动加载，需要把下面的选项加到`rc.conf` 文件中：

```
named_enable="YES"
```

尽管还有其他的一些可用选项，这是运行域名服务器所需要的最小配置。请参考`rc.conf(5)` 联机手册了解更多的选项。如果不需要继续在`rc.conf` 文件中进行其他配置了，就可以通过下面的命令来启动**named**：

```
# /etc/rc.d/named start
```

25.7.4 BIND9 的安全

尽管FreeBSD 会自动地将**named** 放到一个chroot(8) 环境中，您仍然可以采取一些更为严密的措施来防止潜在的针对DNS 服务的攻击。

25.7.4.1 查询访问控制表

查询访问控制表可以用来限制对于域的查询。这些配置通过在`acl` 语句中列出的IP 地址来发挥作用。要允许一个子网查询`example.org` 中的主机，可以做下面的定义：

```
acl "example.com" {
    192.168.0.0/24;
};
```

```

zone "example.com" {
    type slave;
    file "slave/example.com";
    masters {
        10.0.0.1;
    };
allow-query { example.com; };
};

zone "0.168.192.in-addr.arpa" {
    type slave;
    file "slave/0.168.192.in-addr.arpa";
    masters {
        10.0.0.1;
    };
allow-query { example.com; };
};

```

25.7.4.2 限制版本查询

允许查询DNS 服务的版本，可能会给攻击者敞开方便之门。心存恶意的用户能够利用这一信息找到存在已知漏洞的服务器，并利用这些漏洞来实施攻击。

警告：配置伪造的版本号并不能阻止服务器被使用已知的攻击手段进行攻击。唯一能够确保安全的办法是将服务器升级到没有已知问题的版本。

伪造的版本号可以通过named.conf 的options 小节来指定：

```

options {
    directory      "/etc/namedb";
    pid-file       "/var/run/named/pid";
    dump-file      "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";
    version "None of your business";
};

```

25.8 Apache HTTP 服务器

Contributed by Murray Stokely.

25.8.1 纵览

FreeBSD 被用于运行许多全球最为繁忙的web 站点。大多数Internet 上的web 服务器，都使用**Apache HTTP 服务器**。**Apache** 软件包可以在您的FreeBSD 安装盘上找到。如果没有在首次安装时附带安装**Apache**，则可以通过www/apache13 或www/apache20 port 来安装。

一旦成功地安装了 **Apache**，就必须对其进行配置。

注意: 这一节介绍了 **1.3.X** 版本的 **Apache HTTP 服务器** 的配置，因为它是随 **FreeBSD** 一同使用的最多的版本。**Apache 2.X** 引入了很多新技术，但在此并不讨论。要了解关于 **Apache 2.X** 的更多资料，请参见 <http://httpd.apache.org/>。

25.8.2 配置

主要的 **Apache HTTP Server** 配置文件，在 **FreeBSD** 上会安装为 `/usr/local/etc/apache/httpd.conf`。这是一个典型的 **UNIX** 文本配置文件，它使用 `#` 作为注释符。关于全部配置选项的详尽介绍超出了本书的范围，这里将只介绍最常被修改的那些。

ServerRoot `"/usr/local"`

这指定了 **Apache** 安装的顶级目录。执行文件被放到服务器根目录(server root)的 `bin` 和 `sbin` 子目录中，而配置文件则位于 `etc/apache`。

ServerAdmin `you@your.address`

这个地址是在服务器发生问题时应发送电子邮件的地址，它会出现在服务器生成的页面上，例如错误页面。

ServerName `www.example.com`

ServerName 允许您配置发送回客户端的主机名，如果您的服务器被用户以别的名字访问(例如，使用 `www` 而不是主机本身的真实名字)。

DocumentRoot `"/usr/local/www/data"`

DocumentRoot: 这个目录是您的文档所在的目录。默认情况下，所有的请求都会从这个位置去获取，但也可以通过符号连接和别名指定其它的位置。

在修改配置之前备份 **Apache** 的配置文件永远是一个好习惯。一旦对初始配置满意了，就可以开始运行 **Apache** 了。

25.8.3 运行Apache

与许多其它网络服务不同，**Apache** 并不依赖 **inetd** 超级服务器来运行。一般情况下会把它配置为一个独立的服务器，以期在客户的 **web** 浏览器连入 **HTTP** 请求时，能够获得更好的性能。它提供了一个 **shell** 脚本来使启动、停止和重新启动服务器变得尽可能地简单。首次启动 **Apache**，只需执行：

```
# /usr/local/sbin/apachectl start
```

可以在任何时候使用下面的命令来停止服务：

```
# /usr/local/sbin/apachectl stop
```

当由于某种原因修改了配置文件之后，需要重启服务器：

```
# /usr/local/sbin/apachectl restart
```

要在重启**Apache** 服务器时不中断当前的连接，则应运行：

```
# /usr/local/sbin/apachectl graceful
```

更多的信息，可以在**apachectl**(8) 联机手册中找到。

要在系统启动时启动**Apache**，则应在/etc/rc.conf 中加入：

```
apache_enable="YES"
```

如果您希望在系统引导时启动**Apache** httpd 程序并指定其它一些选项，则可以把下面的行加到rc.conf：

```
apache_flags=""
```

现在web 服务器就开始运行了，您可以使用web 浏览器打开http://localhost/。默认显示的web 页面是/usr/local/www/data/index.html。

25.8.4 虚拟主机

Apache 支持两种不同类型的虚拟主机。第一种方法是基于名字的虚拟主机。基于名字的虚拟主机使用客户机发来的HTTP/1.1 头来辨别主机名。这使得不同的域得以共享同一个IP 地址。

要配置**Apache** 来使用基于名字的虚拟主机，需要把类似下面的项加到您的httpd.conf 中：

```
NameVirtualHost *
```

如果您的web 服务器的名字是www.domain.tld，而您希望建立一个www.someotherdomain.tld 的虚拟域，则应在httpd.conf 中加入：

```
<VirtualHost *>
ServerName www.domain.tld
DocumentRoot /www/domain.tld
</VirtualHost>

<VirtualHost *>
ServerName www.someotherdomain.tld
DocumentRoot /www/someotherdomain.tld
</VirtualHost>
```

您需要把上面的地址和文档路径改为所使用的那些。

要了解关于虚拟主机的更多信息，请参考官方的**Apache** 文档，这些文档可以在<http://httpd.apache.org/docs/vhosts/> 找到。

25.8.5 Apache 模块

有许多不同的**Apache** 模块，它们可以在基本的服务器基础上提供许多附加的功能。FreeBSD 的Ports Collection 为安装**Apache** 和常用的附加模块提供了非常方便的方法。

25.8.5.1 mod_ssl

mod_ssl 这个模块使用OpenSSL 库，来提供通过安全套接字层(SSL v2/v3) 和传输层安全(TLS v1) 协议的强加密能力。这个模块提供了从某一受信的证书签署机构申请签名证书所需的所有工具，您可以藉此在FreeBSD 上运行安全的web 服务器。

如果您未曾安装**Apache**，也可以直接安装一份包含了**mod_ssl** 的版本的**Apache 1.3.X**，其方法是通过**www/apache13-modssl** port 来进行。SSL 支持已经作为**Apache 2.X** 的一部分提供，您可以通过**www/apache20** port 来安装后者。

25.8.5.2 使用Perl & PHP 的动态网站

在过去几年中，越来越多的企业开始通过Internet 以期扩大它们的收入和影响。这也为交互式web 内容提出了更多的要求。尽管一些公司，如Microsoft，提供了基于它们专有产品的解决方案，但开源社区也给出了自己的答案。目前，最为常用的动态web 内容实现两种方法是**mod_perl** & **mod_php**。

25.8.5.2.1 mod_perl

Apache/Perl 集成计划，将Perl 程序设计语言的强大功能，与**Apache HTTP 服务器** 紧密地结合到了一起。通过**mod_perl** 模块，可以完全使用Perl 来撰写**Apache** 模块。此外，服务器中嵌入的持久性解释器，消除了由于启动外部的解释器为Perl 脚本的启动所造成的性能损失。

mod_perl 通过多种方式提供。要使用**mod_perl**，应该注意**mod_perl 1.0** 只能配合**Apache 1.3** 而**mod_perl 2.0** 只能配合**Apache 2** 使用。**mod_perl 1.0** 可以通过**www/mod_perl** 安装，而以静态方式联编的版本，则可以通过**www/apache13-modperl** 来安装。**mod_perl 2.0** 则可以通过**www/mod_perl2** 安装。

25.8.5.2.2 mod_php

Written by Tom Rhodes.

PHP，也称为“PHP: Hypertext Preprocessor”，是一种通用的脚本语言，并且特别适合于Web 开发。它能够很容易地嵌入到HTML 之中，其语法接近于C、Java，以及Perl，以期让web 开发人员的一迅速撰写动态生成的页面。

要获得用于**Apache** web 服务器的PHP5 支持，可以从安装**www/mod_php5** port 开始。

上述操作将安装并配置用于支持动态PHP 应用程序所需的模块。请检查并确认在**/usr/local/etc/apache/httpd.conf** 中已经加入了下面的小节：

```
LoadModule php5_module          libexec/apache/libphp5.so

AddModule mod_php5.c
<IfModule mod_php5.c>
    DirectoryIndex index.php index.html
</IfModule>
<IfModule mod_php5.c>
    AddType application/x-httpd-php .php
    AddType application/x-httpd-php-source .phps
</IfModule>
```

这些工作完成之后，还需要使用**apachectl** 命令来完成一次graceful restart 以便加载PHP 模块：

```
# apachectl graceful
```

在FreeBSD中的PHP支持是高度模块化的，因此基本安装的功能十分有限。增加其他功能的支持非常简单，只需通过`lang/php5-extensions port`即可完成。这个`port`提供了一个菜单驱动的界面来帮助完成PHP扩展的安装。另外，也可以通过对应的`port`来单独安装扩展。

例如，要将对于MySQL数据库服务器的支持加入PHP5，只需简单地安装`databases/php5-mysql port`。

安装完扩展之后，必须重新启动Apache服务器，来令其适应新的配置变更：

```
# apachectl graceful
```

25.9 文件传输协议(FTP)

Contributed by Murray Stokely.

25.9.1 纵览

文件传输协议(FTP)为用户提供了一个简单的，与FTP服务器交换文件的方法。FreeBSD系统中包含了FTP服务软件，`ftpd`。这使得在FreeBSD上建立和管理FTP服务器变得非常简单。

25.9.2 配置

最重要的配置步骤是决定允许哪些帐号访问FTP服务器。一般的FreeBSD系统包含了一系列系统帐号分别用于执行不同的服务程序，但未知的用户不应被允许登录并使用这些帐号。`/etc/ftpusers`文件中，列出了不允许通过FTP访问的用户。默认情况下，这包含了前述的系统帐号，但也可以在这里加入其它不应通过FTP访问的用户。

您可能会希望限制通过FTP登录的某些用户，而不是完全阻止他们使用FTP。这可以通过`/etc/ftpchroot`文件来完成。这一文件列出了希望对FTP访问进行限制的用户和组的表。而在`ftpchroot(5)`联机手册中，已经对此进行了详尽的介绍，故而不再赘述。

如果您想要在服务器上启用匿名的FTP访问，则必须建立一个名为`ftp`的FreeBSD用户。这样，用户就可以使用`ftp`或`anonymous`和任意的口令(习惯上，应该是以那个用户的邮件地址作为口令)来登录和访问您的FTP服务器。FTP服务器将在匿名用户登录时调用`chroot(2)`，以便将其访问限制在`ftp`用户的主目录中。

有两个文本文件可以用来指定显示在FTP客户程序中的欢迎文字。`/etc/ftpwelcome`文件中的内容将在用户连接上之后，在登录提示之前显示。在成功的登录之后，将显示`/etc/ftpmotd`文件中的内容。请注意后者是相对于登录环境的，因此对于匿名用户而言，将显示`~ftp/etc/ftpmotd`。

一旦正确地配置了FTP服务器，就必须在`/etc/inetd.conf`中启用它。这里需要做的全部工作就是将注释符“#”从已有的`ftpd`行之前去掉：

```
ftp stream tcp nowait root /usr/libexec/ftpd ftpd -l
```

如例25-1所介绍的那样，修改这个文件之后，必须让`inetd`重新加载它，才能使新的设置生效。

现在可以通过输入下面的命令来登录您的FTP服务器了：

```
% ftp localhost
```

25.9.3 维护

ftpd 服务程序使用syslog(3) 来记录消息。默认情况下，系统日志将把和FTP 相关的消息记录到/var/log/xferlog 文件中。FTP 日志的位置，可以通过修改/etc/syslog.conf 中如下所示的行来修改：

```
ftp.info      /var/log/xferlog
```

一定要小心对待在匿名FTP 服务器中可能遇到的潜在问题。一般而言，允许匿名用户上传文件应三思。您可能发现自己的FTP 站点成为了交易未经授权的商业软件的论坛，或发生更糟糕的情况。如果不需要匿名的FTP 上传，可以在文件上配置权限，使得您能够在其它匿名用户能够下载这些文件之前复查它们。

25.10 为Microsoft® Windows 客户机提供文件和打印服务(Samba)

Contributed by Murray Stokely.

25.10.1 纵览

Samba 是一个流行的开源软件包，它提供了针对Microsoft Windows 客户机的文件和打印服务。这类客户机可以连接并使用FreeBSD 系统上的文件空间，就如同使用本地的磁盘一样，或者像使用本地打印机一样使用FreeBSD 上的打印机。

Samba 软件包可以在您的FreeBSD 安装盘上找到。如果您没有在初次安装FreeBSD 时安装**Samba**，则可以通过net/samba3 port 或package 来安装。

25.10.2 配置

默认的**Samba** 配置文件会以/usr/local/etc/smb.conf.default 的名字安装。这个文件必须复制为/usr/local/etc/smb.conf 并进行定制，才能开始使用**Samba**。

smb.conf 文件中包含了**Samba** 的运行时配置信息，例如对于打印机的定义，以及希望共享给Windows 客户机的“共享文件系统”。**Samba** 软件包包含了一个称为swat 的web 管理工具，后者提供了配置smb.conf 文件的简单方法。

25.10.2.1 使用Samba Web 管理工具(SWAT)

Samba Web 管理工具(SWAT) 是一个通过inetd 运行的服务程序。因此，需要把/etc/inetd.conf 中下面几行的注释去掉，才能够使用swat 来配置**Samba**：

```
swat    stream  tcp      nowait/400    root    /usr/local/sbin/swat
```

如例25-1 中所介绍的那样，在修改了这个配置文件之后，必须让inetd 重新加载配置，才能使其生效。

一旦在inetd.conf 中启用了swat，就可以用浏览器访问connect to http://localhost:901 了。您将首先使用系统的root 帐号登录。

只要成功地登录进了 **Samba** 配置页面，就可以浏览系统的文档，或从 **Globals**(全局) 选项卡开始配置了。**Globals** 小节对应于 **[global]** 小节中的变量，前者位于 `/usr/local/etc/smb.conf` 中。

25.10.2.2 全局配置

无论是使用 **swat**，还是直接编辑 `/usr/local/etc/smb.conf`，通常首先要配置的 **Samba** 选项都是：

workgroup

NT 域名或工作组名，其他计算机将通过这些名字来找到服务器。

netbios name

这个选项用于设置 **Samba** 服务器的 NetBIOS 名字。默认情况下，这是所在主机的 DNS 名字的第一部分。

server string

这个选项用于设置通过 `net view` 命令，以及某些其他网络工具可以查看到的关于服务器的说明性文字。

25.10.2.3 安全配置

在 `/usr/local/etc/smb.conf` 中的两个最重要的配置，是选定的安全模型，以及客户机上用户的口令存放后端。下面的语句控制这些选项：

security

最常见的选项形式是 `security = share` 和 `security = user`。如果您的客户机使用用户名，并且这些用户名与您的 FreeBSD 机器一致，一般应选择用户级(**user**) 安全。这是默认的安全策略，它要求客户机首先登录，然后才能访问共享的资源。

如果采用共享级(**share**) 安全，则客户机不需要用有效的用户名和口令登录服务器，就能够连接共享的资源。这是较早版本的 **Samba** 中的默认值。

passdb backend

Samba 提供了若干种不同的验证后端模型。您可以通过 LDAP、NIS+、SQL 数据库，或经过修改的口令文件，来完成客户端的身份验证。默认的验证模式是 `smbpasswd`，这也是本章将介绍的全部内容。

假设您使用的是默认的 `smbpasswd` 后端，则必须首先创建一个 `/usr/local/private/smbpasswd` 文件，来允许 **Samba** 对客户进行身份验证。如果您打算让所有的 UNIX 用户帐号都能够从 Windows 客户机上登录，可以使用下面的命令：

```
# grep -v "^#" /etc/passwd | make_smbpasswd > /usr/local/private/smbpasswd
# chmod 600 /usr/local/private/smbpasswd
```

请参见 **Samba** 的文档，以了解关于配置选项的进一步信息。按照前面给出的描述，您应该已经可以启动 **Samba** 了。

25.10.3 启动Samba

要在系统引导时启动**Samba**，将下面的配置加入/etc/rc.conf:

```
samba_enable="YES"
```

现在可以在任何时候通过下面的命令来启动**Samba**了:

```
# /usr/local/etc/rc.d/samba.sh start
Starting SAMBA: removing stale tdb's :
Starting nmbd.
Starting smbd.
```

Samba 事实上包含了三个相互独立的服务程序。您应该能够看到**nmbd** 和**smbd** 两个服务程序都是通过**samba.sh** 脚本启动的。如果在**smb.conf** 中启用了**winbind** 名字解析服务，则应该可以看到**winbindd** 服务被启动起来。

可以在任何时候通过下面的命令来停止运行**Samba**:

```
# /usr/local/etc/rc.d/samba.sh stop
```

Samba 是一个复杂的软件包，它提供了用于与Microsoft Windows 网络进行集成的各式各样的功能。要了解关于这里所介绍的基本安装以外的其它功能，请访问<http://www.samba.org>。

25.11 通过NTP 进行时钟同步

Contributed by Tom Hukins.

25.11.1 纵览

随着时间的推移，计算机的时钟会倾向于漂移。网络时间协议(NTP) 是一种确保您的时钟保持准确的方法。

许多Internet 服务依赖于，或极大地受益于本地计算机时钟的准确性。例如，web 服务器可能会接收到一个请求，要求如果文件在某一时刻之后修改过才发送它。在局域网环境中，共享文件的计算机之间的时钟是否同步至关重要，因为这样才能使时间戳保持一致。类似**cron(8)** 这样的程序，也依赖于正确的系统时钟，才能够准确地执行操作。

FreeBSD 附带了**ntpd(8)** NTP 服务器，它可以用于查询其它的NTP 服务器，并配置本地计算机的时钟，或者为其它机器提供服务。

25.11.2 选择合适的NTP 服务器

为了同步您的系统时钟，需要首先找到至少一个NTP 服务器以供使用。网络管理员，或ISP 都可能会提供用于这样目的的NTP 服务器——请查看他们的文档以了解是否是这样。另外，也有一个在线的公开的NTP 服务器列表 (<http://ntp.isc.org/bin/view/Servers/WebHome>)，您可以从中选一个较近的NTP 服务器。请确认您选择的服务器的访问策略，如果需要的话，申请一下所需的许可。

选择多个相互不连接的NTP 服务器是一个好主意，这样在某个服务器不可达，或者时钟不可靠时就可以有别的选择。这是因为，**ntpd(8)** 会智能地选择它收到的响应——它会更倾向于使用可靠的服务器。

25.11.3 配置您的机器

25.11.3.1 基本配置

如果只想在系统启动时同步时钟，则可以使用`ntpdate(8)`。对于经常重新启动，并且不需要经常同步的桌面系统来说这比较适合，但绝大多数机器都应该运行`ntpd(8)`。

在引导时使用`ntpdate(8)`来配合运行`ntpd(8)`也是一个好主意。`ntpd(8)`渐进地修正时钟，而`ntpdate(8)`则直接设置时钟，无论机器的当前时间和正确时间有多大的偏差。

要启用引导时的`ntpdate(8)`，需要把`ntpdate_enable="YES"`加到`/etc/rc.conf`中。此外，还需要通过`ntpdate_flags`来设置同步的服务器和选项，它们将传递给`ntpdate(8)`。

25.11.3.2 一般配置

NTP是通过`/etc/ntp.conf`文件来进行配置的，其格式在`ntp.conf(5)`中进行了描述。下面是一个例子：

```
server ntplocal.example.com prefer
server timeserver.example.org
server ntp2a.example.net

driftfile /var/db/ntp.drift
```

这里，`server`选项指定了使用哪一个服务器，每一个服务器都列为移行。如果某一台服务器上指定了`prefer` (偏好) 参数，如上面的`ntplocal.example.com`，则会优先选择这个服务器。如果偏好的服务器和其他服务器的响应存在显著的差别，则丢弃它的响应，否则将使用来自它的响应，而不理会其他服务器。一般来说，`prefer`参数应该标注在非常精确的NTP时源，例如那些包含特殊的时间监控硬件的服务器上。

而`driftfile`选项，则指定了用来保存系统时钟频率偏差的文件。`ntpd(8)`程序使用它来自动地补偿时钟的自然漂移，从而使时钟即使在切断了外来时源的情况下，仍能保持相当的准确度。

另外，`driftfile`选项也保存上一次响应所使用的NTP服务器的信息。这个文件包含了NTP的内部信息，它不应被任何其他进程修改。

25.11.3.3 控制您的服务器的访问

默认情况下，NTP服务器可以被整个Internet上的主机访问。如果在`/etc/ntp.conf`中指定`restrict`参数，则可以控制允许哪些机器访问您的服务器。

如果希望拒绝所有的机器访问您的NTP服务器，只需在`/etc/ntp.conf`中加入：

```
restrict default ignore
```

如果只希望子网内的机器通过您的服务器同步时钟，而不允许它们配置为服务器，或作为同步时钟的节点来用时，则加入

```
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
```

这里，需要把`192.168.1.0`改为您网络上的IP地址，并把`255.255.255.0`改为您子网的掩码。

`/etc/ntp.conf` 可能包含多个 `restrict` 选项。要了解进一步的细节，请参见 `ntp.conf(5)` 的 `Access Control Support`(访问控制支持) 小节。

25.11.4 运行NTP 服务器

要让NTP服务器在系统启动时随之开启，需要把 `ntp_enable="YES"` 加入到 `/etc/rc.conf` 中。如果希望向 `ntpd(8)` 传递更多参数，需要编辑 `/etc/rc.conf` 中的 `ntpd_flags`。

要在不重新启动机器的前提下启动服务器，需要手工运行 `ntpd`，并带上 `/etc/rc.conf` 中的 `ntpd_flags` 所指定的参数。例如：

```
# ntpd -p /var/run/ntpd.pid
```

注意：在FreeBSD 4.X 中，需要把上述参数中的 `ntpd` 改为 `xntpd`。

25.11.5 在临时性的Internet 连接上使用ntpd

`ntpd(8)` 程序的正常工作并不需要永久性的Internet 连接。然而，如果您的临时性连接是配置为按需拨号的，那么防止NTP 通讯频繁触发拨号，或保持连接就有必要了。如果您使用用户级PPP，可以使用 `filter` 语句，在 `/etc/ppp/ppp.conf` 中进行必要的设置。例如：

```
set filter dial 0 deny udp src eq 123
# Prevent NTP traffic from initiating dial out
set filter dial 1 permit 0 0
set filter alive 0 deny udp src eq 123
# Prevent incoming NTP traffic from keeping the connection open
set filter alive 1 deny udp dst eq 123
# Prevent outgoing NTP traffic from keeping the connection open
set filter alive 2 permit 0/0 0/0
```

要了解进一步的信息，请参考 `ppp(8)` 的 `PACKET FILTERING`(包过滤) 小节，以及 `/usr/share/examples/ppp/` 中的例子。

注意：某些Internet 访问提供商会阻止低编号的端口，这会导致NTP 无法正常工作，因为响应无法到达您的机器。

25.11.6 进一步的信息

关于NTP 服务器的文档，可以在 `/usr/share/doc/ntp/` 找到HTML 格式的版本。

第26章

防火墙

Contributed by Joseph J. Barbish. Converted to SGML and updated by Brad Davis.

26.1 入门

防火墙的存在，使得过滤出入系统的数据流成为可能。防火墙可以使用一组或多组“规则(rules)”，来检查出入您的网络连接的数据包，并决定允许或阻止它们通过。这些规则通常可以检查数据包的某个或某些特征，这些特征包括，但不必限于协议类型、来源或目的主机地址，以及来源或目的端口。

防火墙可以大幅度地改善主机或网络的安全。它可以用来完成下面的任务：

- 保护和隔离应用程序、服务程序，以及您内部网络上的机器，不受那些来自公共的Internet网络上您所不希望的数据流量的干扰。
- 限制或禁止从内部网访问公共的Internet上的服务。
- 支持网络地址转换(NAT)，它使得您的内部网络能够使用私有的IP地址，并分享一条通往公共的Internet的连接(使用一个IP地址，或者一组公网地址)。

读完这章，您将了解：

- 如何正确地定义包过滤规则。
- FreeBSD中内建的集中防火墙之间的差异。
- 如何使用和配置OpenBSD的PF防火墙。
- 如何使用和配置IPFILTER。
- 如何使用和配置IPFW。

阅读这章之前，您需要：

- 理解基本的FreeBSD和Internet概念。

26.2 防火墙的概念

建立防火墙规则集的基本方法有两种：“包容式的”或“排斥式的”。排斥式的防火墙，允许除了禁止的那些数据之外的所有网络流量通过。包容式的防火墙正好相反。后者只允许符合规则的流量通过，而其他所有的流量都被阻止。

包容式防火墙一般说来要比排斥式防火墙安全，因为他们显著地降低了由于允许不希望的网络流量通过所带来的风险。

如果使用了“带状态功能的防火墙(stateful firewall)”，则安全机制可以进一步地细化。带状态功能的防火墙能够记录通过防火墙的连接，进而只允许与现有连接匹配的连接，或创建新的连接。带状态功能的防火墙的缺点，则是在很短时间内有大量的连接请求时，它们可能会受到拒绝服务(DoS)攻击。绝大多数防火墙都提供了同时启用两种防火墙的能力，以便为站点提供更好的保护。

26.3 防火墙软件包

FreeBSD 的基本系统内建了三种不同的防火墙软件包。它们是**IPFILTER** (也被称作**IPF**)、**IPFIREWALL** (也被称作**IPFW**)，以及**OpenBSD** 的**PacketFilter** (也被称为**PF**)。FreeBSD 也提供了两个内建的、用于流量整形(基本上是控制带宽占用)的软件包：**altq(4)** 和**dummynet(4)**。**Dummynet** 在过去一直和**IPFW** 紧密集成，而**ALTQ** 则需要配合**IPF/PF** 使用。**IPF**、**IPFW**，以及**PF** 都是用规则来控制是否允许数据包出入您的系统，虽然它们采取了不同的实现方法和规则语法。

FreeBSD 包含多个内建的防火墙软件包的原因在于，不同的人会有不同的需求和偏好。任何一个防火墙软件包都很难说是最好的。

作者倾向于使用**IPFILTER**，因为它提供的状态式规则，在**NAT** 的环境中要简单许多，而且它内建了**ftp** 代理，这简化了使用外部**FTP** 服务时所需的配置。

由于所有的防火墙都基于检查所选定的包控制字段来实现功能，撰写防火墙规则集时，就必须了解**TCP/IP** 是如何工作的，以及包的控制字段在正常会话交互中的作用。您可以在这个网站找到一份很好的解释文档：<http://www.ipprimer.com/overview.cfm>。

26.4 OpenBSD Packet Filter (PF) 和ALTQ

2003 年7 月，OpenBSD 的防火墙，也就是常说的**PF** 被成功地移植到了FreeBSD 上，并可以通过FreeBSD Ports Collection 来安装了；第一个将**PF** 集成到基本系统中的版本是2004 年11 月发行的FreeBSD 5.3。**PF** 是一个完整的提供了大量功能的防火墙软件，并提供了可选的**ALTQ** (交错队列，Alternate Queuing) 功能。**ALTQ** 提供了服务品质(QoS) 带宽整形功能，这个功能能够以基于过滤规则的方式来保障不同服务的带宽。OpenBSD Project 在维护**PF** 用户指南方面已经做了非常卓越的工作，因此我们打算在这本使用手册中进行更进一步的阐述，以避免不必要的重复劳动。

PF 在各种FreeBSD 发行版上的可用情况如下所示：

FreeBSD 版本	PF 可用情况
4.X 之前的版本	PF 在FreeBSD 4.X 之前的版本分支上不可用。
所有4.X 版本分支上的版本	PF 作为 KAME 的一部分提供。
5.X 在5.3-RELEASE 之前的版本	security/pf port 可以用来在这些FreeBSD 版本上安装 PF 。这些版本主要是供开发人员，以及预览早期的5.X 版本上使用的。强烈建议升级到5.3-RELEASE 或更新的FreeBSD 版本。
5.3-RELEASE 以及之后的版本	PF 已经成为了基本系统的一部分。请不要尝试使用 security/pf port 在这些FreeBSD 版本上安装它，因为这样做是没有作用的。请使用基本系统中的 pf(4) 支持。

更多的详细信息，可以在FreeBSD 版本的**PF** 网站上找到：<http://pf4freebsd.love2party.net/>。

26.4.1 启用PF

PF 作为FreeBSD 5.3 和更高版本基本系统安装的一部分，作为一个可以动态加载的模块出现。如果在**rc.conf** 中配置了**pf_enable="YES"** 则系统会自动加载对应的内核模块。可加载内核模块在构建时启用了**pflog(4)**。

注意: 这个模块假定`options INET` 和`device bpf` 是存在的。除非编译时指定了`NOINET6` (对FreeBSD 6.0-RELEASE 之前的版本) 或`NO_INET6` (对更新一些的版本) (例如在`make.conf(5)` 中定义) 它还需要`options INET6`。

一旦加载了这个内核模块，或者将PF 支持静态联编进内核，就可以随时通过`pfctl` 来启用或禁用`pf` 了。

下面的例子展示了如何启用`pf`:

```
# pfctl -e
```

`pfctl` 命令提供了一种与`pf` 防火墙交互的方法。要了解进一步的信息，参考`pfctl(8)` 联机手册是一个不错的办法。

26.4.2 内核选项

将下面这些选项加入到FreeBSD 内核的编译配置文件中并不是启用PF 的强制性要求。这里列出它们主要是为了介绍一些背景信息。将PF 编译到内核中之后，就不再需要使用可加载内核模块了。

如何在内核编译配置中加入对于PF 选项的例子可以在内核源代码中的`/usr/src/sys/conf/NOTES` 这个文件中找到。这里列举如下:

```
device pf
device pflog
device pfsync
```

`device pf` 用于启用“Packet Filter” 防火墙的支持。

`device pflog` 启用可选的`pflog(4)` 伪网络设备，用以通过`bpf(4)` 描述符来记录流量。`pflogd(8)` 服务可以用来存储信息，并把它们以日志形式记录到磁盘上。

`device pfsync` 启用可选的`pfsync(4)` 伪网络设备，用以监视“状态变更”。由于这不是那个可加载内核模块的一部分，因此如果需要使用它，就必须自行编译定制的内核了。

这些设置只有在您使用它们构建和安装新内核之后才会生效。

26.4.3 可用的rc.conf 选项

您需要在`/etc/rc.conf` 中添加如下配置，以便在启动时激活PF:

```
pf_enable="YES"           # 启用 PF (如果需要的话， 自动加载内核模块)
pf_rules="/etc/pf.conf"   # pf 使用的规则定义文件
pf_flags=""               # 启动时传递给 pfctl 的其他选项
pflog_enable="YES"        # 启动 pflogd(8)
pflog_logfile="/var/log/pflog" # pflogd 用于记录日志的文件名
pflog_flags=""            # 启动时传递给 pflogd 的其他选项
```

如果您的防火墙后面有一个LAN，而且需要通过它来转发LAN 上的包，或进行NAT，还必须同时启用下述选项:

```
gateway_enable="YES"      # 启用作为 LAN 网关的功能
```

26.4.4 启用ALTQ

ALTQ 只有在作为编译选项加入到FreeBSD 内核时，才能使用。ALTQ 目前还不是所有的可用网卡驱动都能够支持的。请参见altq(4) 联机手册了解您正使用的FreeBSD 版本中的驱动支持情况。下面这些选项将启用ALTQ 以及一些附加的功能。

```
options      ALTQ
options      ALTQ_CBQ      # Class Bases Queuing (CBQ)
options      ALTQ_RED      # Random Early Detection (RED)
options      ALTQ_RIO      # RED In/Out
options      ALTQ_HFSC     # Hierarchical Packet Scheduler (HFSC)
options      ALTQ_PRIQ     # Priority Queuing (PRIQ)
options      ALTQ_NOPCC    # Required for SMP build
```

options ALTQ 将启用ALTQ 框架的支持。

options ALTQ_CBQ 用于启用基于分类的队列(CBQ) 支持。CBQ 允许您将连接分成不同的类别，或者说，队列，以便在规则中为它们指定不同的优先级。

options ALTQ_RED 将启用随机预检测(RED)。RED 是一种用于防止网络拥塞的技术。RED 度量队列的长度，并将其与队列的最大和最小长度阈值进行比较。如果队列过长，则新的包将被丢弃。如名所示，RED 从不同的连接中随机地丢弃数据包。

options ALTQ_RIO 将启用出入的随机预检测。

options ALTQ_HFSC 启用层次式公平服务平滑包调度器。要了解关于HFSC 进一步的信息，请参见<http://www-2.cs.cmu.edu/~hzhang/HFSC/main.html>。

options ALTQ_PRIQ 启用优先队列(PRIQ)。PRIQ 首先允许高优先级队列中的包通过。

options ALTQ_NOPCC 启用ALTQ 的SMP 支持。如果是SMP 系统，则必须使用它。

26.4.5 建立过滤规则

Packet Filter 会从pf.conf(5) 文件中读取配置规则，并根据那里的规则修改、丢弃或让数据包通过。默认安装的FreeBSD 已经提供了一格默认的、包含一些有用例子和注释的/etc/pf.conf。

尽管FreeBSD 提供了自己的/etc/pf.conf，但这个文件和OpenBSD 中的语法是一样的。OpenBSD 开发团队提供了一个非常好的配置pf 资源，它可以在<http://www.openbsd.org/faq/pf/> 找到。

警告: 在浏览pf 用户手册时，请时刻注意，在FreeBSD 中所包含的pf 的版本和OpenBSD 中是不一样的。在FreeBSD 5.X 中pf 相当于OpenBSD 3.5 中的版本，而FreeBSD 6.X 中则相当于OpenBSD 3.7。

关于pf 的配置和使用问题，可以在FreeBSD packet filter 邮件列表(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-pf>) 提出。当然，在提出问题之前，别忘了查阅邮件列表的存档。

26.5 IPFILTER (IPF) 防火墙

注意: 这一节的内容正在撰写中。其内容可能不总是十分准确。

IPFILTER 的作者是Darren Reed。IPFILTER 是独立于操作系统的：它是一个开放源代码的应用，并且已经被移植到了FreeBSD、NetBSD、OpenBSD、SunOS、HP/UX，以及Solaris操作系统上。IPFILTER 的支持和维护都相当活跃，并且有规律地发布更新版本。

IPFILTER 基于内核模式的防火墙和NAT 机制，这些机制可以通过用户模式运行的接口程序中进行控制。防火墙规则可以使用ipf(8) 工具来动态地设置和删除。NAT 规则可以通过ipnat(1) 工具来维护。ipfstat(8) 工具则可以用来显示IPFILTER 内核部分的统计数据。最后，使用ipmon(8) 程序可以把IPFILTER 的动作记录到系统日志文件中。

IPF 最初是使用一组“以最后匹配的规则为准”的策略来实现的，这种方式只能支持无状态的规则。随着时代的进步，IPF 被逐渐增强，并加入了“quick”选项，以及支持状态的“keep state”选项，这使得规则处理逻辑变得更富有现代气息。IPF 的官方文档介绍了传统的规则编写方法和文件处理逻辑。新增的功能只是作为一些附加的选项出现，如果能完全理解这些功能，则对于建立更安全的防火墙就很有好处。

这一节中主要是针对“quick”选项，以及支持状态的“keep state”选项的介绍。这是包容式防火墙规则集最基本的编写要素。

包容式防火墙只允许与规则匹配的包通过。这样，您就既能够控制来自防火墙后面的机器请求Internet 公网上的那些服务，同时也可以控制来自Internet 的请求能够访问内部网上的哪些服务。所有其它的访问请求都会被阻止，并记录下来。包容式防火墙一般而言要远比排斥式的要安全，而且也只需要定义允许哪些访问通过。

要获得关于传统规则处理方式的详细信息，请参考：http://www.obfuscation.org/ipf/ipf-howto.html#TOC_1 以及<http://coombs.anu.edu.au/~avalon/ip-filter.html>。

IPF FAQ 可以在<http://www.phildev.net/ipf/index.html> 找到。

26.5.1 启用IPF

IPF 作为FreeBSD 基本安装的一部分，以一个独立的内核模块的形式提供。如果在rc.conf 中配置了 `ipfilter_enable="YES"`，系统就会自动地动态加载IPF 内核模块。这个内核模块在创建时启用了日志支持，并加入了`default pass all`选项。如果只是需要把默认的规则设置为`block all`的话，并不需要把IPF 编译到内核中。可以简单地通过把这条规则加入自己的规则集来达到同样的目的。

26.5.2 内核选项

下面这些FreeBSD 内核编译选项并不是启用IPF 所必需的。这里只是作为背景知识来加以阐述。如果将IPF 编入了内核，则对应的内核模块将不被使用。

关于IPF 选项语句的内核编译配置的例子，可以在内核源代码中的`/usr/src/sys/conf/NOTES` 找到(对于FreeBSD 4.X 来说，则是`/usr/src/sys/arch/conf/LINT`) 并这里列举如下：

```
options IPFILTER
options IPFILTER_LOG
options IPFILTER_DEFAULT_BLOCK
```

`options IPFILTER` 用于启用“IPFILTER” 防火墙的支持。

`options IPFILTER_LOG` 用于启用IPF 的日志支持，所有匹配了包含`log` 的规则包，都会被记录到ipl 这个包记录伪——设备中。

`options IPFILTER_DEFAULT_BLOCK` 将改变防火墙的默认动作，进而，所有不匹配防火墙的pass 规则的包都会被阻止。

这些选项只有在您重新编译并安装内核之后才会生效。

26.5.3 可用的rc.conf 选项

要在启动时激活IPF，您需要在`/etc/rc.conf` 中增加下面的设置：

```
ipfilter_enable="YES"           # 启动 ipf 防火墙
ipfilter_rules="/etc/ipf.rules" # 将被加载的规则定义， 这是一个文本文件
ipmon_enable="YES"             # 启动 IP 监视日志
ipmon_flags="-Ds"              # D = 作为服务程序启动
                                # s = 使用 syslog 记录
                                # v = 记录 tcp 窗口大小、 ack 和序号(seq)
                                # n = 将 IP 和端口映射为名字
```

如果您的LAN 在防火墙后面，并且使用了保留的私有IP 地址范围，那就需要增加下面的一些选项来启用NAT 功能：

```
gateway_enable="YES"           # 启用作为 LAN 网关的功能
ipnat_enable="YES"             # 启动 ipnat 功能
ipnat_rules="/etc/ipnat.rules" # 用于 ipnat 的规则定义文件
```

26.5.4 IPF

`ipf` 命令可以用来加载您自己的规则文件。一般情况下，您可以建立一个包括您自定义的规则的文件，并使用这个命令来替换掉正在运行的防火墙中的内部规则：

```
# ipf -Fa -f /etc/ipf.rules
```

`-Fa` 表示清除所有的内部规则表。

`-f` 用于指定将要被读取的规则定义文件。

这个功能使得您能够修改自定义的规则文件，通过运行上面的IPF 命令，可以将正在运行的防火墙刷新为使用全新的规则集，而不需要重新启动系统。这对于测试新的规则来说就很方便，因为您可以任意执行上面的命令。

请参考`ipf(8)` 联机手册以了解这个命令提供的其它选项。

`ipf(8)` 命令假定规则文件是一个标准的文本文件。它不能处理使用符号代换的脚本。

也确实有办法利用脚本的非常强大的符号替换能力来构建IPF 规则。要了解进一步的细节，请参考第26.5.9 节。

26.5.5 IPFSTAT

默认情况下，`ipfstat(8)` 会获取并显示所有的累积统计，这些统计是防火墙启动以来用户定义的规则匹配的出入流量，您可以通过使用`ipf -Z` 命令来将这些计数器清零。

请参见`ipfstat(8)` 联机手册以了解进一步的细节。

默认的ipfstat(8) 命令输出类似于下面的样子:

```
input packets: blocked 99286 passed 1255609 nomatch 14686 counted 0
output packets: blocked 4200 passed 1284345 nomatch 14687 counted 0
input packets logged: blocked 99286 passed 0
output packets logged: blocked 0 passed 0
packets logged: input 0 output 0
log failures: input 3898 output 0
fragment state(in): kept 0 lost 0
fragment state(out): kept 0 lost 0
packet state(in): kept 169364 lost 0
packet state(out): kept 431395 lost 0
ICMP replies: 0 TCP RSTs sent: 0
Result cache hits(in): 1215208 (out): 1098963
IN Pullups succeeded: 2 failed: 0
OUT Pullups succeeded: 0 failed: 0
Fastroute successes: 0 failures: 0
TCP cksum fails(in): 0 (out): 0
Packet log flags set: (0)
```

如果使用了 **-i** (进入流量) 或者 **-o** (输出流量), 它就只获取并显示内核中所安装的对应该过滤器规则的统计数据。

ipfstat -in 以规则号的形式显示进入的内部规则表。

ipfstat -on 以规则号的形式显示流出的内部规则表。

输出和下面的类似:

```
@1 pass out on xl0 from any to any
@2 block out on dc0 from any to any
@3 pass out quick on dc0 proto tcp/udp from any to any keep state
```

ipfstat -ih 显示内部规则表中的进入流量, 每一个匹配规则前面会同时显示匹配的次数。

ipfstat -oh 显示内部规则表中的流出流量, 每一个匹配规则前面会同时显示匹配的次数。

输出和下面的类似:

```
2451423 pass out on xl0 from any to any
354727 block out on dc0 from any to any
430918 pass out quick on dc0 proto tcp/udp from any to any keep state
```

ipfstat 命令的一个重要的功能可以通过指定 **-t** 参数来使用, 它会以类似 **top(1)** 的显示 **FreeBSD** 正运行的进程表的方式来显示统计数据。当您的防火墙正在受到攻击的时候, 这个功能让您得以识别、试验, 并查看攻击的数据包。这个选项还还提供了实时选择希望监视的目的或源IP、端口或协议的能力。请参见 **ipfstat(8)** 联机手册以了解详细信息。

26.5.6 IPMON

为了使 **ipmon** 能够正确工作, 必须打开 **IPFILTER_LOG** 这个内核选项。这个命令提供了两种不同的使用模式。内建模式是默认的模式, 如果您不指定 **-D** 参数, 就会采用这种模式。

服务模式是持续地通过系统日志来记录的工作模式, 这样, 您就可以通过查看日志来了解过去曾经发生过的事情。这种模式是 **FreeBSD** 和 **IPFILTER** 配合工作的模式。由于在 **FreeBSD** 中提供了一个内建的系统

日志自动轮转功能，因此，使用syslogd比默认的将日志信息记录到一个普通文件要好。在默认的rc.conf文件中，您会看到一个ipmon_flags语句，指定了-Ds标志：

```
ipmon_flags="-Ds"           # D = 作为服务程序启动
                          # s = 使用 syslog 记录
                          # v = 记录 tcp 窗口大小、ack 和序号(seq)
                          # n = 将 IP 和端口映射为名字
```

记录日志的好处是很明显的。它提供了在事后重新审查相关信息，例如哪些包被丢弃，以及这些包的来源地址等等。这将为查找攻击者提供非常有用的第一手资料。

即使启用了日志机制，IPF 仍然不会对其规则进行任何日志记录工作。防火墙管理员可以决定规则集中的哪些应记录日志，并在这些规则上加入log关键字。一般来说，只应记录拒绝性的规则。

作为惯例，通常会有一条默认的、拒绝所有网络流量的规则，并指定log关键字，作为您的规则集的最后一条。这样，您就能够看到所有没有匹配任何规则的数据包。

26.5.7 IPMON 的日志

Syslogd 使用特殊的方法对日志数据进行分类。它使用称为“facility”和“level”的组。以-Ds模式运行的IPMON采用security(在4.X中是local0)作为“facility”名。所有由IPMON记录的数据都会进入security(在4.X中是local0)。如果需要，可以用下列levels来进一步区分数据：

```
LOG_INFO - 使用 "log" 关键字指定的通过或阻止动作
LOG_NOTICE - 同时记录通过的那些数据包
LOG_WARNING - 同时记录阻止的数据包
LOG_ERR - 进一步记录含不完整的包头的数据包
```

要设置IPFILTER来将所有数据记录到/var/log/ipfilter.log，需要首先建立这个文件。下面的命令可以完成这个工作：

```
# touch /var/log/ipfilter.log
```

syslog功能可以通过在/etc/syslog.conf文件中的语句来定义。syslog.conf提供了相当多的用以控制syslog如何处理类似IPF这样的应用程序所产生的系统消息的方法。

对FreeBSD 5.X和更新版本，将下列语句加到/etc/syslog.conf：

```
security.* /var/log/ipfilter.log
```

对于FreeBSD 4.X则应在/etc/syslog.conf中加入：

```
local0.* /var/log/ipfilter.log
```

这里的security.*(对4.X则是local0)表示把所有的相关日志信息写到指定的文件中。

要让/etc/syslog.conf中的修改立即生效，您可以重新启动计算机，或者通过执行/etc/rc.d/syslogd reload来让它重新读取/etc/syslog.conf(在FreeBSD 4.X中，则是killall -HUP syslogd)。

不要忘了修改/etc/newsyslog.conf来让您刚创建的日志进行轮转。

26.5.8 记录消息的格式

由ipmon生成的消息由空格分隔的数据字段组成。所有的消息都包含的字段是：

1. 接到数据包的日期。
2. 接到数据包的时间。其格式为HH:MM:SS.F，分别是小时、分钟、秒，以及分秒(这个数字可能有许多位)。
3. 处理数据包的网络接口名字，例如dc0。
4. 组和规则的编号，例如@0:17。

可以通过ipfstat -in 来查看这些信息。

1. 动作：p 表示通过，b 表示阻止，S 表示包头不全，n 表示没有匹配任何规则，L 表示log 规则。显示这些标志的顺序是：S, p, b, n, L。大写的P 或B 表示记录包的原因是某个全局的日志配置，而不是某个特定的规则。
2. 地址。这实际上包括三部分：源地址和端口(以逗号分开)，一个-> 符号，以及目的地址和端口。209.53.17.22,80-> 198.73.220.17,1722。
3. PR，后跟协议名称或编号，例如，PR tcp。
4. len，后跟包头的长度，以及包的总长度，例如len 20 40。

对于TCP 包，则还会包括一个附加的字段，由一个连字号开始，之后是表示所设置的标志的一个字母。请参见ipmon(8) 联机手册，以了解这些字母所对应的标志。

对于ICMP 包，则在最后会有两个字段。前一个总是“ICMP”，而后一个则是ICMP 消息和子消息的类型，中间以斜线分靠，例如ICMP 3/3 表示端口不可达消息。

26.5.9 构建采用符号替换的规则脚本

一些有经验的IPF 会创建包含规则的文件，并把它编写成能够与符号替换脚本兼容的方式。这样做最大的好处是，它能够让您只修改符号名字所代表的值，而在脚本执行时直接替换掉所有的名符。作为脚本，您可以使用符号替换来把那些经常使用的值直接用于多个规则。下面我们将给出一个例子。

这个脚本所使用的语法与sh、csh，以及tcsh 脚本。

符号替换的前缀字段是美元符号：\$。

符号字段不使用\$ 前缀。

希望替换符号字段的值，必须使用双引号(") 括起来。

您的规则文件的开头类似这样：

```
##### IPF 规则脚本的开头 #####
oif="dc0"           # 外网接口的名字
odns="192.0.2.11"   # ISP 的 DNS 服务器 IP 地址
myip="192.0.2.7"    # 来自 ISP 的静态 IP 地址
ks="keep state"
fks="flags S keep state"

# 可以使用这个脚本来建立 /etc/ipf.rules 文件，
# 也可以 "直接地" 运行它。
```

```
#
# 请删除两个注释号之一。
#
# 1) 保留下面一行， 则创建 /etc/ipf.rules:
#cat > /etc/ipf.rules << EOF
#
# 2) 保留下面一行， 则 "直接地" 运行脚本:
/sbin/ipf -Fa -f - << EOF

# 允许发出到我的 ISP 的域名服务器的访问
pass out quick on $oif proto tcp from any to $odns port = 53 $fks
pass out quick on $oif proto udp from any to $odns port = 53 $ks

# 允许发出未加密的 www 访问请求
pass out quick on $oif proto tcp from $myip to any port = 80 $fks

# 允许发出使用 TLS SSL 加密的 https www 访问请求
pass out quick on $oif proto tcp from $myip to any port = 443 $fks
EOF
##### IPF 规则脚本的结束 #####
```

这就是所需的全部内容。这个规则本身并不重要，它们主要是用于体现如何使用符号代换字段，以及如何完成值的替换。如果上面的例子的名字是/etc/ipf.rules.script，就可以通过输入下面的命令来重新加载规则：

```
# sh /etc/ipf.rules.script
```

在规则文件中嵌入符号有一个问题：IPF 无法识别符号替换，因此它不能直接地读取这样的脚本。

这个脚本可以使用下面两种方法之一来使用：

- 去掉cat 之前的注释，并注释掉/sbin/ipf 开头的那一行。像其他配置一样，将ipfilter_enable="YES" 放到/etc/rc.conf 文件中，并在此后立刻执行脚本，以创建或更新/etc/ipf.rules。
- 通过把ipfilter_enable="NO" (这是默认值) 加到/etc/rc.conf 中，来禁止系统启动脚本开启IPFILTER。

在/usr/local/etc/rc.d/ 启动目录中增加一个类似下面的脚本。应该给它起一个显而易见的名字，例如ipf.loadrules.sh。请注意，.sh 扩展名是必需的。

```
#!/bin/sh
sh /etc/ipf.rules.script
```

脚本文件必须设置为属于root，并且属主可读、可写、可执行。

```
# chmod 700 /usr/local/etc/rc.d/ipf.loadrules.sh
```

这样，在系统启动时，就会自动加载您的IPF 规则了。

26.5.10 IPF 规则集

规则集是指一组编写好的依据包的值决策允许通过或阻止ipf 规则。包的双向交换组成了一个会话交互。防火墙规则集对同一个包会进行两次处理，第一次是它从公网的Internet 主机到达的时候，第二次是它

离开并返回初始的Internet 公网主机的时候。每一个TCP/IP 服务(例如telnet, www, 邮件等等) 是由协议预先定义的源或目的IP 地址, 以及源或目的端口。这是最基本的一些可以为防火墙规则所利用的, 判别是否允许服务通过的标准。

IPF 最初被写成使用一组称作“以最后匹配的规则为准” 的处理逻辑, 且只能处理无状态的规则。随着时代的发展, IPF 进行了改进, 并提供了“quick” 选项, 以及一个有状态的“keep state” 选项。后者使处理逻辑迅速地跟上了时代的步伐。

这一节中提供的一些指导, 是基于使用包含“quick” 选项和有状态的“keep state” 选项来进行阐述的。这些是编写包容式防火墙规则集的基本要素。

包容式防火墙只允许与规则匹配的服务通过。这样, 您就既能够控制来自防火墙后面的机器请求Internet 公网上的那些服务, 同时也可以控制来自Internet 的请求能够访问内部网上的哪些服务。所有其它的访问请求都会被阻止, 并记录下来。包容式防火墙一般而言要远比排斥式的要安全, 而且也只需要定义允许哪些访问通过。

警告: 当对防火墙规则进行操作时, 应该**谨慎行事**。某些配置可能会**将您反锁在** 服务器外面。安全起见, 您可以考虑在第一次进行防火墙配置时在本地控制台上, 而不是远程, 例如通过**ssh** 来进行。

26.5.11 规则语法

这里给出的规则语法已经简化到只处理那些新式的带状态规则, 并且都是“第一个匹配的规则获胜”逻辑的。要了解完整的传统规则语法描述, 请参见ipf(8) 联机手册。

以# 字符开头的内容会被认为是注释。这些注释可以出现在一行规则的末尾, 或者独占一行。空行会被忽略。

规则由关键字组成。这些关键字必须以一定的顺序, 从左到右出现在一行上。接下来的文字中关键字将使用粗体表示。某些关键字可能提供了子选项, 这些子选项本身可能也是关键字, 而且可能会提供更多的子选项。下面的文字中, 每种语法都使用粗体的小节标题呈现, 并介绍了其上下文。

ACTION IN-OUT OPTIONS SELECTION STATEFUL PROTO SRC_ADDR, DST_ADDR OBJECT PORT_NUM TCP_FLAG STATEFUL

ACTION = block | pass

IN-OUT = in | out

OPTIONS = log | quick | on 网络接口的名字

SELECTION = proto 协议名称| 源/目的IP | port = 端口号| flags 标志值

PROTO = tcp/udp | udp | tcp | icmp

SRC_ADDR, DST_ADDR = all | from 对象to 对象

OBJECT = IP地址| any

PORT_NUM = port 端口号

TCP_FLAG = S

STATEFUL = keep state

26.5.11.1 ACTION (动作)

动作对表示匹配规则的包应采取什么动作。每一个规则**必须** 包含一个动作。可以使用下面两种动作之一:

block 表示如果规则与包匹配, 则丢弃包。

pass 表示如果规则与包匹配, 则允许包通过防火墙。

26.5.11.2 IN-OUT

每个过滤器规则都必须明确地指定是流入还是流出的规则。下一个关键字必须要么是**in**, 要么是**out**, 否则将无法通过语法检查。

in 表示规则应被应用于刚刚从Internet 公网上收到的数据包。

out 表示规则应被应用于即将发出到Internet 的数据包。

26.5.11.3 OPTIONS

注意: 这些选项必须按下面指定的顺序出现。

log 表示包头应被写入到**ipl** 日志(如前面LOGGING 小节所介绍的那样), 如果它与规则匹配的话。

quick 表示如果给出的参数与包匹配, 则以这个规则为准, 这使得能够"短路" 掉后面的规则。这个选项对于使用新式的处理逻辑是必需的。

on 表示将网络接口的名称作为筛选参数的一部分。接口的名字会在**ifconfig(8)** 的输出中显示。使用这个选项, 则规则只会应用到某一个网络接口上的出入数据包上。要配置新式的处理逻辑, 必须使用这个选项。

当记录包时, 包的头会被写入到**IPL** 包日志伪设备中。紧跟**log** 关键字, 可以使用下面几个修饰符(按照下列顺序):

body 表示应同时记录包的前128 字节的内容。

first 如果**log** 关键字和“**keep state**” 选项同时使用, 则这个选项只在第一个包上触发, 这样就不用记录每一个“**keep state**” 包信息了。

26.5.11.4 SELECTION

这一节所介绍的关键字可以用于所检察的包的属性。有一个关键字主题, 以及一组子选项关键字, 您必须从他们中选择一个。以下是一些通用的属性, 它们必须按下面的顺序使用:

26.5.11.5 PROTO

proto 是一个主题关键字, 它必须与某个相关的子选项关键字配合使用。这个值的作用是匹配某个特定的协议。要使用新式的规则处理逻辑, 就必须使用这个选项。

tcp/udp | udp | tcp | icmp 或其他在**/etc/protocols** 中定义的协议。特殊的协议关键字**tcp/udp** 可以用于匹配TCP 或UDP 包, 引入这个关键字的作用是为了避免大量的重复规则的麻烦。

26.5.11.6 SRC_ADDR/DST_ADDR

使用all关键词，基本上相当于“from any to any”在没有配合其他关键字的情形。

from src to dst: from和to关键字主要是用来匹配IP地址。所有的规则都必须同时给出源和目的两个参数。any是一个可以用于匹配任意IP地址的特殊关键字。例如，您可以使用“from any to any”或“from 0.0.0.0/0 to any”或“from any to 0.0.0.0/0”或“from 0.0.0.0 to any”以及“from any to 0.0.0.0”。

IP地址可以按句点分隔的IP地址/掩码长度的方式来指定，也可以只指定一个句点分隔的IP地址。

如果无法使用子网掩码来表示IP的话，表达地址就会很麻烦。请参见下面的网页了解如何撰写掩码长度：<http://jodies.de/ipcalc>。

26.5.11.7 PORT

如果为源或目的指定了匹配端口，规则就只能应用于TCP和UDP包了。当编写端口比较规则时，可以指定/etc/services中所定义的名字，也可以直接用端口号来指定。如果端口号出现在源对象一侧，则被认为是源端口号；反之，则被认为是目的端口号。要使用新式的规则处理逻辑，就必须与to对象配合使用这个选项。使用的例子：“from any to any port = 80”。

端口的比较是以数字的形式进行的，可以使用比较算符来指定，也可以指定一个范围。

port "=" | "!=" | "<" | ">" | "<=" | ">=" | "eq" | "ne" | "lt" | "gt" | "le" | "ge".

要指定端口范围，可以使用"<>" | "><"。

警告：在源和目的匹配参数之后，需要使用下面两个参数，才能够使用新式的规则处理逻辑。

26.5.11.8 TCP_FLAG

标志只对TCP过滤使用。这些字母用来表达TCP包头的标志。

新式的规则处理逻辑使用flags s参数来识别tcp会话开始的请求。

26.5.11.9 STATEFUL

keep state表示如果有一个包与规则匹配，则其筛选参数应激活有状态的过滤机制。

注意：如果使用新式的处理逻辑，则这个选项是必需的。

26.5.12 有状态过滤

有状态过滤将网络流量当作一种双向的包交换来处理。如果激活它，keep-state会动态地为每一个相关的包在双向会话交互过程中产生内部规则。它能够确认发起者和包的目的地之间的会话是有效的双向包交换过程的一部分。如果包与这些规则不符，则将自动地拒绝。

状态保持也使得ICMP包能够与TCP或UDP会话相关。因此，如果您在浏览网站时收到允许的状态保持规则匹配的ICMP类型3代码4响应，则这些响应会被自动地允许进入。所有IPF能够处理的包，都可以作为某种活跃会话的一部分，即使它是另一种协议的，也会被允许进入。

所发生的事情是：

将要通过联入公网的网络接口发出的包，首先会经过动态状态表的检查。如果包与会话中预期的下一个包匹配，则防火墙就会允许包通过，而会话的交互流信息也会在动态状态表中进行更新，而其他的包，则将使用发出规则集来检查。

发到联入Internet公网的包，也会首先经过动态规则表的检查。如果与会话中预期的下一个包匹配，则防火墙就允许它通过，并更新动态状态表。其他包仍会使用进入规则集进行检查。

当会话结束时，对应的项会在动态状态表中删除。

有状态过滤使得您能够集中于阻止/允许新的会话。一旦新会话被允许通过，则所有后续的包就都被自动地允许通过，而伪造的包则被自动地拒绝。如果新的会话被阻止，则后续的包也都不会被允许通过。有状态过滤从技术角度而言，在阻止目前攻击者常用的洪水式攻击来说，具有更好的抗御能力。

26.5.13 包容式规则集的例子

下面的规则集是如何编写非常安全的包容式防火墙规则集的一个范例。包容式防火墙只让允许的服务通过，而所有其他的访问都会被默认地拒绝。所有的防火墙都有至少两个接口对应的默认规则，从而使防火墙能够正常工作。

所有的类UNIX系统，包括FreeBSD都使用lo0和IP地址127.0.0.1用于操作系统中内部的通讯。防火墙规则必须允许这些包无阻碍地通过。

接入Internet公网的网络接口，是放置规则并允许将访问请求发到Internet以及接收响应的地方。这有可能是用户模式的PPP tun0接口，如果您的网卡同DSL或电缆调制解调器相联的话。

如果有至少一个网卡与防火墙后的内网LAN相联，这些网络接口就应该有一个规则来允许来自这些LAN接口的包无阻碍地通过。

一般说来，规则应被组织为三个主要的小节：所有允许自由通过的接口规则，发到公网接口的规则，以及进入公网接口的规则。

每一个公网接口规则中，经常会匹配到的规则应该放置在尽可能靠前的位置。而最后一个规则应该是阻止包通过，并记录它们。

下面防火墙规则集中，Outbound部分是一些使用'pass'的规则，这些规则指定了允许访问的公网Internet服务，并且指定了'quick'、'on'、'proto'、'port'，以及'keep state'这些选项。'proto tcp'规则还指定了'flag'这个选项，这样会话的第一个包将出发状态机制。

接下来的Inbound一节，则首先阻止所有不希望的数据包。这样做有两个原因，其一是被阻止的包可能会被后面的规则允许，从而并不妨碍获得授权的服务正常工作；其二是这避免了那些不常见的包由于匹配到最后一条规则而触发日志，规则集中的最后一条规则是阻止并记录所有的包，通过这样的记录，就比较容易找到攻击系统的人，并为采取法律措施收集证据。

需要注意的另一件事情是，如果收到了不希望的数据包，则这些包会被丢弃，而不是给出什么响应。这样做的好处是，攻击者无法了解包是否已经被您的系统收到。攻击者所能了解到的信息越少，攻陷您的系统所需要花费的时间也就越长。我们在这里记录的连入的'nmap OS指纹'探测企图，一般来说正是攻击者所做的第一件事。

如果您看到了'log first'规则的日志，就应该用ipfstat -hio命令来看看那个规则被匹配的次数，以便了解系统是否正在或曾被攻击。

如果记录的包的端口号并不是您所知道的，可以在`/etc/services`或<http://www.securitystats.com/tools/portsearch.php>了解端口号通常的用途。

参考下面的网页，了解木马使用的端口：<http://www.simovits.com/trojans/trojans.html>。

下面是我在自己的系统中使用的完整的，非常安全的‘包容式’防火墙规则集。直接使用这个规则集不会给您造成问题，您所要做的是注释掉那些您不需要的服务。

如果在日志中发现了希望阻止的记录，只需在`inbound`小节中增加一条阻止规则集可。

您必须将每一个规则中的`dc0`替换为您系统上接入Internet的网络接口名称，例如，用户环境下的PPP应该是`tun0`。

在`/etc/ipf.rules`中加入下面的内容：

```
#####
# No restrictions on Inside LAN Interface for private network
# Not needed unless you have LAN
#####

#pass out quick on xl0 all
#pass in quick on xl0 all

#####
# No restrictions on Loopback Interface
#####
pass in quick on lo0 all
pass out quick on lo0 all

#####
# Interface facing Public Internet (Outbound Section)
# Interrogate session start requests originating from behind the
# firewall on the private network
# or from this gateway server destined for the public Internet.
#####

# Allow out access to my ISP's Domain name server.
# xxx must be the IP address of your ISP's DNS.
# Dup these lines if your ISP has more than one DNS server
# Get the IP addresses from /etc/resolv.conf file
pass out quick on dc0 proto tcp from any to xxx port = 53 flags S keep state
pass out quick on dc0 proto udp from any to xxx port = 53 keep state

# Allow out access to my ISP's DHCP server for cable or DSL networks.
# This rule is not needed for 'user ppp' type connection to the
# public Internet, so you can delete this whole group.
# Use the following rule and check log for IP address.
# Then put IP address in commented out rule & delete first rule
pass out log quick on dc0 proto udp from any to any port = 67 keep state
#pass out quick on dc0 proto udp from any to z.z.z.z port = 67 keep state

# Allow out non-secure standard www function
pass out quick on dc0 proto tcp from any to any port = 80 flags S keep state
```



```

# Allow out secure www function https over TLS SSL
pass out quick on dc0 proto tcp from any to any port = 443 flags S keep state

# Allow out send & get email function
pass out quick on dc0 proto tcp from any to any port = 110 flags S keep state
pass out quick on dc0 proto tcp from any to any port = 25 flags S keep state

# Allow out Time
pass out quick on dc0 proto tcp from any to any port = 37 flags S keep state

# Allow out nntp news
pass out quick on dc0 proto tcp from any to any port = 119 flags S keep state

# Allow out gateway & LAN users non-secure FTP ( both passive & active modes)
# This function uses the IPNAT built in FTP proxy function coded in
# the nat rules file to make this single rule function correctly.
# If you want to use the pkg_add command to install application packages
# on your gateway system you need this rule.
pass out quick on dc0 proto tcp from any to any port = 21 flags S keep state

# Allow out secure FTP, Telnet, and SCP
# This function is using SSH (secure shell)
pass out quick on dc0 proto tcp from any to any port = 22 flags S keep state

# Allow out non-secure Telnet
pass out quick on dc0 proto tcp from any to any port = 23 flags S keep state

# Allow out FBSD CVSUP function
pass out quick on dc0 proto tcp from any to any port = 5999 flags S keep state

# Allow out ping to public Internet
pass out quick on dc0 proto icmp from any to any icmp-type 8 keep state

# Allow out whois for LAN PC to public Internet
pass out quick on dc0 proto tcp from any to any port = 43 flags S keep state

# Block and log only the first occurrence of everything
# else that's trying to get out.
# This rule enforces the block all by default logic.
block out log first quick on dc0 all

#####
# Interface facing Public Internet (Inbound Section)
# Interrogate packets originating from the public Internet
# destined for this gateway server or the private network.
#####

# Block all inbound traffic from non-routable or reserved address spaces
block in quick on dc0 from 192.168.0.0/16 to any      #RFC 1918 private IP
block in quick on dc0 from 172.16.0.0/12 to any      #RFC 1918 private IP
block in quick on dc0 from 10.0.0.0/8 to any         #RFC 1918 private IP
block in quick on dc0 from 127.0.0.0/8 to any        #loopback
block in quick on dc0 from 0.0.0.0/8 to any          #loopback

```

```

block in quick on dc0 from 169.254.0.0/16 to any      #DHCP auto-config
block in quick on dc0 from 192.0.2.0/24 to any      #reserved for docs
block in quick on dc0 from 204.152.64.0/23 to any   #Sun cluster interconnect
block in quick on dc0 from 224.0.0.0/3 to any      #Class D & E multicast

##### Block a bunch of different nasty things. #####
# That I do not want to see in the log

# Block frags
block in quick on dc0 all with frags

# Block short tcp packets
block in quick on dc0 proto tcp all with short

# block source routed packets
block in quick on dc0 all with opt lsrr
block in quick on dc0 all with opt ssrr

# Block nmap OS fingerprint attempts
# Log first occurrence of these so I can get their IP address
block in log first quick on dc0 proto tcp from any to any flags FUP

# Block anything with special options
block in quick on dc0 all with ipopts

# Block public pings
block in quick on dc0 proto icmp all icmp-type 8

# Block ident
block in quick on dc0 proto tcp from any to any port = 113

# Block all Netbios service. 137=name, 138=datagram, 139=session
# Netbios is MS/Windows sharing services.
# Block MS/Windows hosts2 name server requests 81
block in log first quick on dc0 proto tcp/udp from any to any port = 137
block in log first quick on dc0 proto tcp/udp from any to any port = 138
block in log first quick on dc0 proto tcp/udp from any to any port = 139
block in log first quick on dc0 proto tcp/udp from any to any port = 81

# Allow traffic in from ISP's DHCP server. This rule must contain
# the IP address of your ISP's DHCP server as it's the only
# authorized source to send this packet type. Only necessary for
# cable or DSL configurations. This rule is not needed for
# 'user ppp' type connection to the public Internet.
# This is the same IP address you captured and
# used in the outbound section.
pass in quick on dc0 proto udp from z.z.z.z to any port = 68 keep state

# Allow in standard www function because I have apache server
pass in quick on dc0 proto tcp from any to any port = 80 flags S keep state

# Allow in non-secure Telnet session from public Internet
# labeled non-secure because ID/PW passed over public Internet as clear text.

```

```
# Delete this sample group if you do not have telnet server enabled.
#pass in quick on dc0 proto tcp from any to any port = 23 flags S keep state

# Allow in secure FTP, Telnet, and SCP from public Internet
# This function is using SSH (secure shell)
pass in quick on dc0 proto tcp from any to any port = 22 flags S keep state

# Block and log only first occurrence of all remaining traffic
# coming into the firewall. The logging of only the first
# occurrence stops a .denial of service. attack targeted
# at filling up your log file space.
# This rule enforces the block all by default logic.
block in log first quick on dc0 all
##### End of rules file #####
```

26.5.14 NAT

NAT 是网络地址转换(Network Address Translation) 的缩写。对于那些熟悉Linux 的人来说, 这个概念叫做IP 伪装(Masquerading); NAT 和IP 伪装是完全一样的概念。由IPF 的NAT 提供的一项功能是, 将防火墙后的本地局域网(LAN) 共享一个ISP 提供的IP 地址来接入Internet 公网。

有些人可能会问, 为什么需要这么做。一般而言, ISP 会为非商业用户提供动态的IP 地址。动态地址意味着每次登录到ISP 都有可能得到不同的IP 地址, 无论是采用电话拨号登录, 或使用cable 以及DSL 调制解调器的方式。这个IP 是您与Internet 公网交互时使用的身份。

现在考虑家中有五台PC 需要访问Internet 的情形。您可能需要向ISP 为每一台PC 所使用的独立的Internet 账号付费, 并且拥有五根电话线。

有了NAT, 您就只需要一个ISP 账号, 然后将另外四台PC 的网卡通过交换机连接起来, 并通过运行FreeBSD 系统的那台机器作为网关连接出去。NAT 会自动地将每一台PC 在内网的LAN IP 地址, 在离开防火墙时转换为公网的IP 地址。此外, 当数据包返回时, 也将进行逆向的转换。

NAT 通常是在没有向ISP 请求许可, 或事先知会的情况下进行的, 因而如果被发现, 有时可能会成为ISP 撤销您的账号的一个借口。商业用户一般来说会购买昂贵得多的Internet 线路, 通常会获得一组长期有效的静态IP 地址块。ISP 一般会希望并同意商业用户在他们的内网中使用NAT。

在IP 地址空间中, 有一些特殊的范围是保留供经过NAT 的内网LAN IP 地址使用的。根据RFC 1918, 您可以使用下面这些IP 范围用于内网, 它们不会在Internet 公网上路由:

起始IP 10.0.0.0	-	结束IP 10.255.255.255
起始IP 172.16.0.0	-	结束IP 172.31.255.255
起始IP 192.168.0.0	-	结束IP 192.168.255.255

26.5.15 IPNAT

NAT 规则是通过ipnat 命令加载的。默认情况下, NAT 规则会保存在/etc/ipnat.rules 文件中。请参见ipnat(1) 了解更多的详情。

如果在NAT 已经启动之后想要修改NAT 规则, 可以修改保存NAT 规则的那个文件, 然后在执行ipnat 命令时加上-CF 参数, 以删除在用的NAT 内部规则表, 以及所有地址翻译表中已有的项。

要重新加载NAT 规则，可以使用类似下面的命令：

```
# ipnat -CF -f /etc/ipnat.rules
```

如果想要看看您系统上NAT 的统计信息，可以用下面的命令：

```
# ipnat -s
```

要列出当前的NAT 表的映射关系，使用下面的命令：

```
# ipnat -l
```

要显示详细的信息并显示与规则处理和当前的规则/表项：

```
# ipnat -v
```

26.5.16 IPNAT 规则

NAT 规则非常的灵活，能够适应商业用户和家庭用户的各种不同的需求。

这里所介绍的规则语法已经被简化，以适应非商用环境中的一般情况。完整的规则语法描述，请参考ipnat(5) 联机手册中的介绍。

NAT 规则的写法与下面的例子类似：

```
map IF LAN_IP_RANGE -> PUBLIC_ADDRESS
```

关键词map 出现在规则的最前面。

将IF 替换为对外的网络接口名。

LAN_IP_RANGE 是内网中的客户机使用的地址范围。通常情况下，这应该是类似192.168.1.0/24 的地址。

PUBLIC_ADDRESS 既可以是外网的IP 地址，也可以是0/32 这个特殊的关键字，它表示分配到IF 上的所有地址。

26.5.17 NAT 的工作原理

当包从LAN 到达防火墙，而目的地址是公网地址时，它首先会通过outbound 过滤规则。接下来，NAT 会得到包，并按自顶向下的顺序处理规则，而第一个匹配的规则将生效。NAT 接下来会根据包对应的接口名字和源IP 地址检查所有的规则。如果包和某个NAT 规则匹配，则会检查包的[源IP 地址，例如，内网的IP 地址] 是否在NAT 规则中箭头左侧指定的IP 地址范围匹配。如果匹配，则包的原地址将被根据用0/32 关键字指定的IP 地址重写。NAT 将向它的内部NAT 表发送此地址，这样，当包从Internet 公网中返回时，就能够把地址映射回原先的内网IP 地址，并在随后使用过滤器规则来处理。

26.5.18 启用IPNAT

要启用IPNAT，只需在/etc/rc.conf 中加入下面一些语句。

使机器能够在不同的网络接口之间进行包的转发，需要：

```
gateway_enable="YES"
```

每次开机时自动启动IPNAT:

```
ipnat_enable="YES"
```

指定IPNAT 规则集文件:

```
ipnat_rules="/etc/ipnat.rules"
```

26.5.19 大型LAN 中的NAT

对于在一个LAN 中有大量PC, 以及包含多个LAN 的情形, 把所有的内网IP 地址都映射到同一个公网IP 上会导致资源不够的问题, 因为同一个端口可能在许多做了NAT 的LAN PC 上被多次使用, 并导致碰撞。有两种方法来缓解这个难题。

26.5.19.1 指定使用哪些端口

普通的NAT 规则类似于:

```
map dc0 192.168.1.0/24 -> 0/32
```

上面的规则中, 包的源端口在包通过IPNAT 时时不会发生变化的。通过使用portmap 关键字, 您可以要求IPNAT 只使用一定范围内的端口地址。比如说, 下面的规则将让IPNAT 把源端口改为指定范围内的端口:

```
map dc0 192.168.1.0/24 -> 0/32 portmap tcp/udp 20000:60000
```

使用auto 关键字可以让配置变得更简单一些, 它会要求IPNAT 自动地检测可用的端口并使用:

```
map dc0 192.168.1.0/24 -> 0/32 portmap tcp/udp auto
```

26.5.19.2 使用公网地址池

对于很大的LAN 来说, 总会有一个临界值, 此时LAN 的地址会多到没办法使用一个公网地址表达的程度。这时, 类似下面的规则需要进行修改:

```
map dc0 192.168.1.0/24 -> 204.134.75.1
```

目前的这个规则, 将所有的链接都通过204.134.75.1 来映射。可以把它改为一个范围:

```
map dc0 192.168.1.0/24 -> 204.134.75.1-10
```

或者使用CIDR 记法指定的一组地址:

```
map dc0 192.168.1.0/24 -> 204.134.75.0/24
```

26.5.20 端口重定向

非常流行的一种做法是，将web服务器、邮件服务器、数据库服务器以及DNS分别放到LAN上的不同的PC上。这种情况下，来自这些服务器的网络流量仍然应该被NAT，但必须有办法把进入的流量发到对应的局域网的PC上。IPNAT提供了NAT重定向机制来解决这个问题。考虑下面的情况，您的web服务器的LAN地址是10.0.10.25，而您的唯一的公网IP地址是20.20.20.5，则可以编写这样的规则：

```
rdr dc0 20.20.20.5/32 port 80 -> 10.0.10.25 port 80
```

或者：

```
rdr dc0 0/32 port 80 -> 10.0.10.25 port 80
```

另外，也可以让LAN地址10.0.10.33上运行的LAN DNS服务器来处理公网上的DNS请求：

```
rdr dc0 20.20.20.5/32 port 53 -> 10.0.10.33 port 53 udp
```

26.5.21 FTP 和NAT

FTP是一个在Internet如今天这样为人所熟知之前就已经出现的恐龙，那时，研究机构 and 大学是通过租用的线路连到一起的，而FTP则被用于在科研人员之间共享大文件。那时，数据的安全性并不是需要考虑的事情。若干年之后，FTP协议则被埋进了正在形成中的Internet骨干，而它使用明文来交换用户名和口令的缺点，并没有随着新出现的一些安全需求而得到改变。FTP提供了两种不同的风格，即主动模式和被动模式。两者的区别在于数据通道的建立方式。被动模式相对而言要更加安全，因为数据通道是由发起ftp会话的一方建立的。关于FTP以及它所提供的不同模式，在<http://www.slacksite.com/other/ftp.html>进行了很好的阐述。

26.5.21.1 IPNAT 规则

IPNAT提供了一个内建的FTP代理选项，它可以在NAT map规则中指定。它能够监视所有外发的FTP主动或被动模式的会话开始请求，并动态地创建临时性的过滤器规则，只打开用于数据通道的端口号。这样，就消除了FTP一般会给防火墙带来的，需要大范围地打开高端口所可能带来的安全隐患。

下面的规则可以处理来自内网的FTP访问：

```
map dc0 10.0.10.0/29 -> 0/32 proxy port 21 ftp/tcp
```

这个规则能够处理来自网关的FTP访问：

```
map dc0 0.0.0.0/0 -> 0/32 proxy port 21 ftp/tcp
```

这个则处理所有来自内网的非FTP网络流量：

```
map dc0 10.0.10.0/29 -> 0/32
```

FTP map规则应该在普通的map规则之前出现。所有的包会从最上面的第一个规则开始进行检查。匹配的顺序是网卡名称，内网源IP地址，以及它是否是FTP包。如果所有这些规则都匹配成功，则FTP代理将建立一个临时的过滤规则，以便让FTP会话的数据包能够正常出入，同时对这些包进行NAT。所有的LAN数据包，如果没有匹配第一条规则，则会继续尝试匹配下面的规则，并最终被NAT。

26.5.21.2 IPNAT FTP 过滤规则

如果使用了NAT FTP 代理，则只需要为FTP 创建一个规则。

如果没有使用FTP 代理，则需要下面三个规则：

```
# Allow out LAN PC client FTP to public Internet
# Active and passive modes
pass out quick on rl0 proto tcp from any to any port = 21 flags S keep state

# Allow out passive mode data channel high order port numbers
pass out quick on rl0 proto tcp from any to any port > 1024 flags S keep state

# Active mode let data channel in from FTP server
pass in quick on rl0 proto tcp from any to any port = 20 flags S keep state
```

26.5.21.3 FTP NAT 代理的bug

在FreeBSD 4.9 中提供了IPFILTER 的3.4.31 版。在整个FTP 会话直到将要结束之前，FTP 代理都会像文档中介绍的那样。但一旦有一方要求关闭会话，则来自远程FTP 服务器21 端口的一个包会被阻止，并在日志中记下这一情况。NAT FTP/代理显然过早地删除了临时规则，而不是等待远程FTP 服务器确认它。有人就这个问题在IPF 的邮件列表中发表了问题报告。

解决这个问题的方法是，要么增加一条过滤规则来摆脱不希望的日志消息，或者什么都不做，并忽略日志中的FTP 连入错误信息。绝大多数人并不经常使用外部的FTP 服务。

```
block in quick on rl0 proto tcp from any to any port = 21
```

26.6 IPFW

注意：这一节的内容正在撰写中。其内容可能不总是十分准确。

IPFIREWALL (IPFW) 是一个由FreeBSD 发起的防火墙应用软件，它由FreeBSD 的志愿者成员编写和维护。它使用了传统的无状态规则，以及传统的规则编写技巧，以期达到所谓的简单状态逻辑。

标准的FreeBSD 安装中，IPFW 所给出的规则集例子(可以在/etc/rc.firewall 中找到)非常简单，以至于没有办法不加修改地加以使用。那个例子中没有使用状态过滤，而这对于许多配置都非常有好处，因此这一节并不以系统自带的例子作为基础。

IPFW 的无状态规则语法，是由一种提供复杂的选择能力的技术支持的，这种技术远远超出了一般的防火墙安装人员的知识水平。IPFW 是为满足专业用户，以及掌握先进技术的电脑爱好者们对于高级的包选择需求而设计的。要完全释放IPFW 的规则所拥有的强大能力，需要对不同的协议的细节有深入的了解，并根据它们独特的包头信息来编写规则。这一级别的详细阐述超出了这本手册的范围。

IPFW 由其部分组成，其主要组件是内核的防火墙过滤规则处理器，及其集成的数据包记帐工具、日志工具、用以触发NAT 工具的'divert' (转发) 规则、高级特殊用途工具、dummynet 流量整形机制，'fwd rule' 转发工具，桥接工具，以及ipstealth 工具。

26.6.1 启用IPFW

IPFW 是基本的FreeBSD 安装的一部分，以单独的可加载内核模块的形式提供。如果在`rc.conf` 中加入`firewall_enable="YES"` 语句，就会自动地加载对应的内核模块。除非您打算使用由它提供的NAT 功能，一般情况下并不需要把IPFW 编进FreeBSD 的内核。

如果将`firewall_enable="YES"` 加入到`rc.conf` 中并重新启动系统，则下列信息将在启动过程中，以高亮的白色显示出来：

```
ipfw2 initialized, divert disabled, rule-based forwarding disabled, default to deny, logging disabled
```

可加载内核模块在编译时加入了记录日志的能力。要启用日志功能，并配置详细日志记录的限制，需要在`/etc/sysctl.conf` 中加入一些配置。这些设置将在重新启动之后生效：

```
net.inet.ip.fw.verbose=1
net.inet.ip.fw.verbose_limit=5
```

26.6.2 内核选项

把下列选项在编译FreeBSD 内核时就加入，并不是启用IPFW 所必需的，除非您需要使用NAT 功能。这里只是将这些选项作为背景知识来介绍。

```
options      IPFIREWALL
```

这个选项将IPFW 作为内核的一部分来启用。

```
options      IPFIREWALL_VERBOSE
```

这个选项将启用记录通过IPFW 的匹配了包含'log' 关键字规则的每一个包的功能。

```
options      IPFIREWALL_VERBOSE_LIMIT=5
```

以每项的方式，限制通过syslogd(8) 记录的包的个数。如果在比较恶劣的环境下记录防火墙的活动可能会需要这个选项。它能够避免潜在的针对syslog 的洪水式拒绝服务攻击。

```
options      IPFIREWALL_DEFAULT_TO_ACCEPT
```

这个选项默认地允许所有的包通过防火墙，如果您是第一次配置防火墙，使用这个选项将是一个不错的主意。

```
options      IPV6FIREWALL
options      IPV6FIREWALL_VERBOSE
options      IPV6FIREWALL_VERBOSE_LIMIT
options      IPV6FIREWALL_DEFAULT_TO_ACCEPT
```

这些选项与IPv4 的对应选项功能一样，它们是针对IPv6 的。如果不使用IPv6，则不带任何规则的IPV6FIREWALL 将阻止所有的IPv6 包。

```
options      IPDIVERT
```

这一选项启用NAT 功能。

注意: 如果内核选项中没有加入IPFWALL_DEFAULT_TO_ACCEPT, 或将您的防火墙设置配置为允许所有的进入包, 则所有发到本机或发出的包都会被阻止。

26.6.3 /etc/rc.conf Options

如果没有将IPFW 编入内核, 则您需要在/etc/rc.conf 中加入下列语句来加载它:

```
firewall_enable="YES"
```

用以激活您的防火墙规则的配置脚本:

```
firewall_script="/etc/ipfw.rules"
```

启用日志:

```
firewall_logging="YES"
```

警告: 设置firewall_logging 的唯一作用是, 系统将把net.inet.ip.fw.verbose sysctl 变量置为1 (参见第26.6.1 节)。并没有能够设置日志限制的rc.conf 变量, 不过这种限制可以通过设置某些sysctl 变量来完成, 可以手工进行操作, 也可以写到/etc/sysctl.conf 文件中:

```
net.inet.ip.fw.verbose_limit=5
```

如果您的计算机是作为网关使用的, 也就是它通过natd(8) 提供网络地址翻译(NAT), 请参见第27.8 节以了解需要在/etc/rc.conf 中配置的选项。

26.6.4 IPFW 命令

ipfw 命令是在防火墙运行时, 用于在其内部规则表中手工逐条添加或删除防火墙规则的标准工具。这一方法的问题在于, 一旦您的关闭计算机或停机, 则所有增加或删除或修改的规则也就丢掉了。把所有的规则都写到一个文件中, 并在启动时使用这个文件来加载规则, 或一次大批量地替换防火墙规则, 那么推荐使用这里介绍的方法。

ipfw 的另一个非常实用的功能是将所有正在运行的防火墙规则显示出来。IPFW 的记账机制会为每一个规则动态地创建计数器, 用以记录与它们匹配的包的数量。在测试规则的过程中, 列出规则及其计数器是了解它们是否工作正常的重要手段。

按顺序列出所有的规则:

```
# ipfw list
```

列出所有的规则, 同时给出最后一次匹配的时间戳:

```
# ipfw -t list
```

列出所有的记账信息、匹配规则的包的数量, 以及规则本身。第一列是规则的编号, 随后是发出包匹配的数量, 进入包的匹配数量, 最后是规则本身。

```
# ipfw -a list
```

列出所有的动态规则和静态规则:

```
# ipfw -d list
```

同时显示已过期的动态规则:

```
# ipfw -d -e list
```

将计数器清零:

```
# ipfw zero
```

只把规则号为`NUM`的计数器清零:

```
# ipfw zero NUM
```

26.6.5 IPFW 规则集

规则集是一组根据包中选择的数值使用`allow`或`deny`写出的`ipfw`规则。在两个主机之前的双向包交换组成了一个会话交互。防火墙规则集，会对同一个包处理两次：第一次是包从公网上到达防火墙时，而第二次则是包返回Internet公网上的主机时。每一个TCP/IP服务(例如telnet, www, mail, 等等)，都有事先定义好的协议，以及一个端口号。这可以作为建立允许或阻止规则时的基本选择依据。

当有数据包进入防火墙时，会从规则集里的第一个规则开始进行比较，并自顶向下地进行匹配。当包与某个选择规则参数相匹配时，将会执行规则所定义的动作，并停止规则集搜索。这种策略，通常也被称作“最先匹配者获胜”的搜索方法。如果没有任何与包相匹配的规则，那么它会根据强制的`ipfw`默认规则，也就是65535号规则截获。一般情况下这个规则是阻止包，而且不给出任何回应。

注意: 如果规则定义的动作是`count`、`skipto`或`tee`规则的话，搜索会继续。

这里所介绍的规则，都是使用了那些包含状态功能的，也就是‘keep state’、‘limit’、‘in’/‘out’、或者‘via’选项的规则。这是编写包容式防火墙规则集所需的基本框架。

包容式防火墙只允许与规则匹配的包通过。这样，您就既能够控制来自防火墙后面的机器请求Internet公网上的那些服务，同时也可以控制来自Internet的请求能够访问内部网上的哪些服务。所有其它的访问请求都会被阻止，并记录下来。包容式防火墙一般而言要远比排斥式的要安全，而且也只需要定义允许哪些访问通过。

警告: 在操作防火墙规则时应谨慎行事，如果操作不当，有可能将自己反锁在外面。

26.6.5.1 规则语法

这里所介绍的规则语法已经经过了简化，只包括了建立标准的包容式防火墙规则集所必需的那些。要了解完整的规则语法说明，请参见`ipfw(8)`联机手册。

规则是由关键字组成的：这些关键字必须以特定的顺序从左到右书写。下面的介绍中，关键字使用粗体表示。某些关键字还包括了子选项，这些自选向本身可能也是关键字，有些还可以包含更多的子选项。

用于表示开始一段注释。它可以出现在一个规则的后面，也可以独占一行。空行会被忽略。

CMD RULE_NUMBER ACTION LOGGING SELECTION STATEFUL

26.6.5.1.1 CMD

每一个新的规则都应以**add** 作为前缀，它表示将规则加入内部表。

26.6.5.1.2 RULE_NUMBER

每一个规则都必须包含一个规则编号。

26.6.5.1.3 ACTION

每一个规则可以与下列的动作之一相关联，所指定的动作将在进入的数据包与规则所指定的选择标准相匹配时执行。

allow | accept | pass | permit

这些关键字都表示允许匹配规则的包通过防火墙，并停止继续搜索规则。

check-state

根据动态规则表检查数据包。如果匹配，则执行规则所指定的动作，亦即生成动态规则；否则，转移到下一个规则。**check-state** 规则没有选择标准。如果规则集中没有**check-state** 规则，则会在第一个**keep-state** 或**limit** 规则处，对动态规则表实施检查。

deny | drop

这两个关键字都表示丢弃匹配规则的包。同时，停止继续搜索规则。

26.6.5.1.4 LOGGING

log or logamount

当数据包与带**log** 关键字的规则匹配时，将通过名为**SECURITY** 的facility 来把消息记录到syslogd。只有在记录的次数没有超过**logamount** 参数所指定的次数时，才会记录日志。如果没有指定**logamount**，则会以sysctl 变量**net.inet.ip.fw.verbose_limit** 所指定的限制为准。如果将这两种限制值之一指定为零，则表示不作限制。万一达到了限制数，可以通过将规则的日志计数或包计数清零来重新启用日志，请参见**ipfw reset log** 命令来了解细节。

注意：日志是在所有其他匹配条件都验证成功之后，在针对包实施最终动作(**accept, deny**) 之前进行的。您可以自行决定哪些规则应启用日志。

26.6.5.1.5 SELECTION

这一节所介绍的关键字主要用来描述检查包的哪些属性，用以判断包是否与规则相匹配。下面是一些通用的用于匹配包特征的属性，它们必须按顺序使用：

udp | tcp | icmp

也可以指定在`/etc/protocols`中所定义的协议。这个值定义的是匹配的协议，在规则中必须指定它。

from src to dst

`from` 和 `to` 关键字用于匹配IP地址。规则中必须同时指定源和目的两个参数。如果需要匹配任意IP地址，可以使用特殊关键字`any`。还有一个特殊关键字，即`me`，用于匹配您的FreeBSD系统上所有网络接口上所配置的IP地址，它可以用于表达网络上的其他计算机到防火墙(也就是本机)，例如`'from me to any'` 或 `'from any to me'` 或 `'from 0.0.0.0/0 to any'` 或 `'from any to 0.0.0.0/0'` 或 `'from 0.0.0.0 to any'` 或 `'from any to 0.0.0.0'` 以及 `'from me to 0.0.0.0'`。IP地址可以通过带点的IP地址/掩码长度，或者一个带点的IP地址的形式来指定。这是编写规则时所必需的。如果不清楚如何写掩码长度，请参见<http://jodies.de/ipcalc>。

port number

这个参数主要用于那些支持端口号的协议(例如TCP和UDP)。如果要通过端口号匹配某个协议，就必须指定这个参数。此外，也可以通过服务的名字(根据`/etc/services`)来指定服务，这样会比使用数字指定端口号直观一些。

in | out

相应地，匹配进入和发出的包。这里的`in` 和 `out` 都是关键字，在编写匹配规则时，必需作为其他条件的一部分来使用。

via IF

根据指定的网络接口的名称精确地匹配进出的包。这里的`via` 关键字将使得接口名称成为匹配过程的一部分。

setup

要匹配TCP会话的发起请求，就必须使用它。

keep-state

这是一个必须使用的关键字。在发生匹配时，防火墙将创建一个动态规则，其默认行为是，匹配使用同一协议的、从源到目的IP/端口的双向网络流量。

limit {src-addr | src-port | dst-addr | dst-port}

防火墙只允许匹配规则时，与指定的参数相同的`N`个连接。可以指定至少一个源或目的地址及端口。`'limit'` 和 `'keep-state'` 不能在同一规则中同时使用。`'limit'` 提供了与 `'keep-state'` 相同的功能，并增加了一些独有的能力。

26.6.5.2 状态规则选项

有状态过滤将网络流量当作一种双向的包交换来处理。它提供了一种额外的检查能力，用以检测会话中的包是否来自最初的发送者，并在遵循双向包交换的规则进行会话。如果包与这些规则不符，则将自动地拒绝它们。

`'check-state'` 用来识别在IPFW规则集中的包是否符合动态规则机制的规则。如果匹配，则允许包通过，此时防火墙将创建一个新的动态规则来匹配双向交换中的下一个包。如果不匹配，则将继续尝试规则集中的下一个规则。

动态规则机制在SYN-flood攻击下是脆弱的，因为这种情况会产生大量的动态规则，从而耗尽资源。为了抵抗这种攻击，从FreeBSD 4.5版开始，加入了一个叫做limit的新选项。这个选项可以用来限制符合规则的会话允许的并发连接数。如果动态规则表中的规则数超过限制，则包将被丢弃。

26.6.5.3 记录防火墙消息

记录日志的好处是显而易见的：它提供了在事后检查所发生的状况的方法，例如哪些包被丢弃了，这些包的来源和目的地，从而为您提供找到攻击者所需的证据。

即使启用了日志机制，IPFW也不会自行生成任何规则的日志。防火墙管理员需要指定规则集中的哪些规则应该记录日志，并在这些规则上增加log动作。一般来说，只有deny规则应记录日志，例如对于进入的ICMP ping的deny规则。另外，复制默认的ipfw终极deny规则，并加入log动作来作为您的规则集的最后一条规则也是很常见的用法。这样，您就能看到没有匹配任何一条规则的那些数据包。

日志是一把双刃剑，如果不谨慎地加以利用，则可能会陷入过多的日志数据中，并导致磁盘被日志塞满。将磁盘填满是DoS攻击最为老套的手法之一。由于日志除了会写入磁盘之外，还会输出到root的控制台屏幕上，因此有过多的日志信息是很让人恼火的事情。

IPFIREWALL_VERBOSE_LIMIT=5 内核选项将限制同一个规则发到系统日志程序syslogd的连续消息的数量。当内核启用了这个选项时，某一特定规则所产生的连续消息的数量将封顶为这个数字。一般来说，没有办法从连续200条一模一样的日志信息中获取更多有用的信息。举例来说，如果同一个规则产生了5次消息并被记录到syslogd，余下的相同的消息将被计数，并像下面这样发给syslogd：

```
last message repeated 45 times
```

所有记录的数据包包消息，默认情况下会最终写到/var/log/security文件中，后者在/etc/syslog.conf文件里进行了定义。

26.6.5.4 编写规则脚本

绝大多数有经验的IPFW用户会创建一个包含规则的文件，并且，按能够以脚本形式运行的方式来书写。这样做最大的一个好处是，可以大批量地刷新防火墙规则，而无须重新启动系统就能够激活它们。这种方法在测试新规则时会非常方便，因为同一过程在需要时可以多次执行。作为脚本，您可以使用符号替换来撰写那些经常需要使用的值，并用同一个符号在多个规则中反复地表达它。下面将给出一个例子。

这个脚本使用的语法同'sh'、'csh'以及'tcsh'脚本兼容。符号替换字段使用美元符号\$作为前缀。符号字段本身并不使用\$前缀。符号替换字段的值必须使用"双引号"括起来。

可以使用类似下面的规则文件：

```
##### start of example ipfw rules script #####
#
ipfw -q -f flush      # Delete all rules
# Set defaults
oif="tun0"           # out interface
odns="192.0.2.11"     # ISP's DNS server IP address
cmd="ipfw -q add "    # build rule prefix
ks="keep-state"       # just too lazy to key this each time
$cmd 00500 check-state
$cmd 00502 deny all from any to any frag
$cmd 00501 deny tcp from any to any established
$cmd 00600 allow tcp from any to any 80 out via $oif setup $ks
```

```
$cmd 00610 allow tcp from any to $odns 53 out via $oif setup $ks
$cmd 00611 allow udp from any to $odns 53 out via $oif $ks
##### End of example ipfw rules script #####
```

这就是所要做的全部事情了。例子中的规则并不重要，它们主要是用来表示如何使用符号替换。

如果把上面的例子保存到/etc/ipfw.rules 文件中，您就可以通过输入下面的命令来加载它。

```
# sh /etc/ipfw.rules
```

/etc/ipfw.rules 这个文件可以放到任何位置，也可以命名为随便什么别的名字。

也可以手工执行下面的命令来达到类似的目的：

```
# ipfw -q -f flush
# ipfw -q add check-state
# ipfw -q add deny all from any to any frag
# ipfw -q add deny tcp from any to any established
# ipfw -q add allow tcp from any to any 80 out via tun0 setup keep-state
# ipfw -q add allow tcp from any to 192.0.2.11 53 out via tun0 setup keep-state
# ipfw -q add 00611 allow udp from any to 192.0.2.11 53 out via tun0 keep-state
```

26.6.5.5 带状态规则集

以下的这组非-NAT 规则集，是如何编写非常安全的‘包容式’防火墙的一个例子。包容式防火墙只允许匹配了pass 规则的包通过，而默认阻止所有的其他数据包。必须有至少两个网络接口，并且在其上配置了规则才能使防火墙正常工作。

所有类UNIX 操作系统，也包括FreeBSD，都设计为允许使用网络接口lo0 和IP 地址127.0.0.1 来完成操作系统内部的通讯。防火墙必须包含一组规则，使这些数据包能够无障碍地收发。

接入Internet 公网的那个网络接口上，应该配置授权和访问控制，来限制对外的访问，以及来自Internet 公网的访问。这个接口很可能是您的ppp 接口，例如tun0，或者您接在DSL 或电缆modem 上的网卡。

如果有至少一个网卡接入了防火墙后的内网LAN，则必须为这些接口配置规则，以便让这些接口之间的包能够顺畅地通过。

所有的规则应被组织为三个部分，所有应无阻碍地通过的规则，公网的发出规则，以及公网的接收规则。

公网接口相关的规则的顺序，应该是最经常用到的放在尽可能靠前的位置，而最后一个规则，则应该是阻止那个接口在那一方向上的包。

发出部分的规则只包含一些‘allow’ 规则，允许选定的那些唯一区分协议的端口号所指定的协议通过，以允许访问Internet 公网上的这些服务。所有的规则中都指定了proto, port, in/out, via 以及keep state 这些选项。‘proto tcp’ 规则同时指定‘setup’ 选项，来区分开始协议会话的包，以触发将包放入keep state 规则表中的动作。

接收部分则首先阻止所有不希望的包，在这里有两个目的。首先是，这些包被禁止掉之后，就不会由于匹配了后面的某个规则而被允许。其次，明确地禁止这些包，就不会再在日志中记录它们而形成干扰。防火墙的最后一条规则是阻止并记录所有包，这样，您就可以留下用于起诉攻击您的系统的人的有用记录。

另一件需要注意的事情是，不希望的数据包一般来说不会有任何响应，这些数据包会被丢弃并消失。这样，攻击者也就无法了解他的数据包是否到达了您的系统。而攻击者了解的信息越少，它们攻陷系统所

需的时间也就越长。当记录的包使用的端口号不是您所熟悉的那些时，可以看一看/etc/services/ 或到<http://www.securitystats.com/tools/portsearch.php> 并查找一下端口号，以了解其用途。另外，您也可以在这个网页上了解常见木马所使用的端口：<http://www.simovits.com/trojans/trojans.html>。

26.6.5.6 包容式规则集的例子

下面是一个非-NAT 的规则集，它是一个完整的包容式规则集。使用它作为您的规则集不会有什么问题。只需把那些不需要的服务对应的pass 规则注释掉就可以了。如果您在日志中看到消息，而且不想再看到它们，只需在接收部分增加一个一个deny 规则。您可能需要把'dc0' 改为接入公网的接口的名字。对于使用用户态ppp 的用户而言，应该是'tun0'。

您可以看出这些规则中的模式。

- 所有请求Internet 公网上服务的会话开始包，都使用了keep-state。
- 所有来自Internet 的授权服务请求，都采用了limit 选项来防止洪水式攻击。
- 所有的规则都使用了in 或者out 来说明方向。
- 所有的规则都使用了via 接口名来指定应该匹配通过哪一个接口的包。

这些规则都应放到/etc/ipfw.rules。

```
##### Start of IPFW rules file #####
# Flush out the list before we begin.
ipfw -q -f flush

# Set rules command prefix
cmd="ipfw -q add"
pif="dc0"      # public interface name of NIC
               # facing the public Internet

#####
# No restrictions on Inside LAN Interface for private network
# Not needed unless you have LAN.
# Change xl0 to your LAN NIC interface name
#####
$cmd 00005 allow all from any to any via xl0

#####
# No restrictions on Loopback Interface
#####
$cmd 00010 allow all from any to any via lo0

#####
# Allow the packet through if it has previous been added to the
# the "dynamic" rules table by a allow keep-state statement.
#####
$cmd 00015 check-state

#####
# Interface facing Public Internet (Outbound Section)
# Interrogate session start requests originating from behind the
# firewall on the private network or from this gateway server
```

```

# destine for the public Internet.
#####

# Allow out access to my ISP's Domain name server.
# x.x.x.x must be the IP address of your ISP.s DNS
# Dup these lines if your ISP has more than one DNS server
# Get the IP addresses from /etc/resolv.conf file
$cmd 00110 allow tcp from any to x.x.x.x 53 out via $pif setup keep-state
$cmd 00111 allow udp from any to x.x.x.x 53 out via $pif keep-state

# Allow out access to my ISP's DHCP server for cable/DSL configurations.
# This rule is not needed for .user ppp. connection to the public Internet.
# so you can delete this whole group.
# Use the following rule and check log for IP address.
# Then put IP address in commented out rule & delete first rule
$cmd 00120 allow log udp from any to any 67 out via $pif keep-state
#$cmd 00120 allow udp from any to x.x.x.x 67 out via $pif keep-state

# Allow out non-secure standard www function
$cmd 00200 allow tcp from any to any 80 out via $pif setup keep-state

# Allow out secure www function https over TLS SSL
$cmd 00220 allow tcp from any to any 443 out via $pif setup keep-state

# Allow out send & get email function
$cmd 00230 allow tcp from any to any 25 out via $pif setup keep-state
$cmd 00231 allow tcp from any to any 110 out via $pif setup keep-state

# Allow out FBSD (make install & CVSUP) functions
# Basically give user root "GOD" privileges.
$cmd 00240 allow tcp from me to any out via $pif setup keep-state uid root

# Allow out ping
$cmd 00250 allow icmp from any to any out via $pif keep-state

# Allow out Time
$cmd 00260 allow tcp from any to any 37 out via $pif setup keep-state

# Allow out nntp news (i.e. news groups)
$cmd 00270 allow tcp from any to any 119 out via $pif setup keep-state

# Allow out secure FTP, Telnet, and SCP
# This function is using SSH (secure shell)
$cmd 00280 allow tcp from any to any 22 out via $pif setup keep-state

# Allow out whois
$cmd 00290 allow tcp from any to any 43 out via $pif setup keep-state

# deny and log everything else that.s trying to get out.
# This rule enforces the block all by default logic.
$cmd 00299 deny log all from any to any out via $pif

#####

```



```

# Interface facing Public Internet (Inbound Section)
# Interrogate packets originating from the public Internet
# destined for this gateway server or the private network.
#####

# Deny all inbound traffic from non-routable reserved address spaces
$cmd 00300 deny all from 192.168.0.0/16 to any in via $pif #RFC 1918 private IP
$cmd 00301 deny all from 172.16.0.0/12 to any in via $pif #RFC 1918 private IP
$cmd 00302 deny all from 10.0.0.0/8 to any in via $pif #RFC 1918 private IP
$cmd 00303 deny all from 127.0.0.0/8 to any in via $pif #loopback
$cmd 00304 deny all from 0.0.0.0/8 to any in via $pif #loopback
$cmd 00305 deny all from 169.254.0.0/16 to any in via $pif #DHCP auto-config
$cmd 00306 deny all from 192.0.2.0/24 to any in via $pif #reserved for docs
$cmd 00307 deny all from 204.152.64.0/23 to any in via $pif #Sun cluster interconnect
$cmd 00308 deny all from 224.0.0.0/3 to any in via $pif #Class D & E multicast

# Deny public pings
$cmd 00310 deny icmp from any to any in via $pif

# Deny ident
$cmd 00315 deny tcp from any to any 113 in via $pif

# Deny all Netbios service. 137=name, 138=datagram, 139=session
# Netbios is MS/Windows sharing services.
# Block MS/Windows hosts2 name server requests 81
$cmd 00320 deny tcp from any to any 137 in via $pif
$cmd 00321 deny tcp from any to any 138 in via $pif
$cmd 00322 deny tcp from any to any 139 in via $pif
$cmd 00323 deny tcp from any to any 81 in via $pif

# Deny any late arriving packets
$cmd 00330 deny all from any to any frag in via $pif

# Deny ACK packets that did not match the dynamic rule table
$cmd 00332 deny tcp from any to any established in via $pif

# Allow traffic in from ISP's DHCP server. This rule must contain
# the IP address of your ISP's DHCP server as it's the only
# authorized source to send this packet type.
# Only necessary for cable or DSL configurations.
# This rule is not needed for .user ppp. type connection to
# the public Internet. This is the same IP address you captured
# and used in the outbound section.
#$cmd 00360 allow udp from any to x.x.x.x 67 in via $pif keep-state

# Allow in standard www function because I have apache server
$cmd 00400 allow tcp from any to me 80 in via $pif setup limit src-addr 2

# Allow in secure FTP, Telnet, and SCP from public Internet
$cmd 00410 allow tcp from any to me 22 in via $pif setup limit src-addr 2

# Allow in non-secure Telnet session from public Internet
# labeled non-secure because ID & PW are passed over public

```

```
# Internet as clear text.
# Delete this sample group if you do not have telnet server enabled.
$cmd 00420 allow tcp from any to me 23 in via $pif setup limit src-addr 2

# Reject & Log all incoming connections from the outside
$cmd 00499 deny log all from any to any in via $pif

# Everything else is denied by default
# deny and log all packets that fell through to see what they are
$cmd 00999 deny log all from any to any
##### End of IPFW rules file #####
```

26.6.5.7 一个NAT 和带状态规则集的例子

要使用IPFW 的NAT 功能，还需要进行一些额外的配置。除了其他IPFIREWALL 语句之外，还需要在内核编译配置中加上'option divert' 语句。

在/etc/rc.conf 中，除了普通的IPFW 配置之外，还需要加入：

```
natd_enable="YES"           # Enable NATD function
natd_interface="rl0"        # interface name of public Internet NIC
natd_flags="-dynamic -m"    # -m = preserve port numbers if possible
```

将带状态规则与转发natd 规则(网络地址转换) 会使规则集的编写变得非常复杂。check-state 的位置，以及'divert natd' 规则将变得非常关键。这样一来，就不再有简单的顺序处理逻辑流程了。提供了一种新的动作类型，称为'skipto'。要使用skipto 命令，就必须给每一个规则进行编号，以确定skipto 规则号是您希望跳转到的位置。

下面给出了一些未加注释的例子来说明如何编写这样的规则，用以帮助您理解包处理规则集的处理顺序。

处理流程从规则文件最上边的第一个规则开始处理，并自顶向下地尝试每一个规则，直到找到匹配的规则，且数据包从防火墙中放出为止。请注意规则号100 101, 450, 500, 以及510 的位置非常重要。这些规则控制发出和接收的包的地址转换过程，这样它们在keep-state 动态表中的对应项中就能够与内网的LAN IP 地址关联。另一个需要注意的是，所有的allow 和deny 规则都指定了包的方向(也就是outbound 或inbound) 以及网络接口。最后，请注意所有发出的会话请求都会请求skipto rule 500 以完成网络地址转换。

下面以LAN 用户使用web 浏览器访问一个web 页面为例。Web 页面使用80 来完成通讯。当包进入防火墙时，规则100 并不匹配，因为它是发出而不是收到的包。它能够通过规则101，因为这是第一个包，因而它还没有进入动态状态保持表。包最终到达规则125，并匹配该规则。最终，它会通过接入Internet 公网的网卡发出。这之前，包的源地址仍然是内网IP 地址。一旦匹配这个规则，就会触发两个动作。keep-state 选项会把这个规则发到keep-state 动态规则表中，并执行所指定的动作。动作是发到规则表中的信息的一部分。在这个例子中，这个动作是"skipto rule 500"。规则500 NAT 包的IP 地址，并将其发出。请务必牢记，这一步非常重要。接下来，数据包将到达目的地，之后返回并从规则集的第一条规则开始处理。这一次，它将规则100 匹配，其目的IP 地址将被映射回对应的内网LAN IP 地址。其后，它会被check-state 规则处理，进而在暨存会话表中找到对应项，并发到LAN。数据包接下来发到了内网LAN PC 上，而后者则会发送从远程服务器请求下一段数据的新数据包。这个包会再次由check-state 规则检查，并找到发出的表项，并执行其关联的动作，即'skipto 500'。包跳转到规则500 并被NAT 后发出。

在接收一侧，已经存在的会话的数据包，会被check-state 规则自动地处理，并放到转发natd 规则。我们需要解决的问题是，阻止所有的坏数据包，而只允许授权的服务。例如在防火墙上运行了Apache 服务，而我们希望人们在访问Internet 公网的同时，也能够访问本地的web 站点。新的接入开始请求包将匹配规

则100，而IP地址则为防火墙所在的服务器而映射到了LAN IP。此后，包会匹配所有我们希望检查的那些令人生厌的东西，并最终匹配规则425。一旦发生匹配，会发生两件事。数据包会被发到keep-state动态表，但此时，所有来自那个源IP的会话请求的数量会被限制为2。这一做法能够挫败针对指定端口上服务的DoS攻击。动作同时指定了包应被发到LAN上。包返回时，check-state规则会识别出包属于某一已经存在的会话交互，并直接把它发到规则500做NAT，并发到发出接口。

示范规则集#1:

```
#!/bin/sh
cmd="ipfw -q add"
skip="skipto 500"
pif=rl0
ks="keep-state"
good_tcpo="22,25,37,43,53,80,443,110,119"

ipfw -q -f flush

$cmd 002 allow all from any to any via xl0 # exclude LAN traffic
$cmd 003 allow all from any to any via lo0 # exclude loopback traffic

$cmd 100 divert natd ip from any to any in via $pif
$cmd 101 check-state

# Authorized outbound packets
$cmd 120 $skip udp from any to xx.168.240.2 53 out via $pif $ks
$cmd 121 $skip udp from any to xx.168.240.5 53 out via $pif $ks
$cmd 125 $skip tcp from any to any $good_tcpo out via $pif setup $ks
$cmd 130 $skip icmp from any to any out via $pif $ks
$cmd 135 $skip udp from any to any 123 out via $pif $ks

# Deny all inbound traffic from non-routable reserved address spaces
$cmd 300 deny all from 192.168.0.0/16 to any in via $pif #RFC 1918 private IP
$cmd 301 deny all from 172.16.0.0/12 to any in via $pif #RFC 1918 private IP
$cmd 302 deny all from 10.0.0.0/8 to any in via $pif #RFC 1918 private IP
$cmd 303 deny all from 127.0.0.0/8 to any in via $pif #loopback
$cmd 304 deny all from 0.0.0.0/8 to any in via $pif #loopback
$cmd 305 deny all from 169.254.0.0/16 to any in via $pif #DHCP auto-config
$cmd 306 deny all from 192.0.2.0/24 to any in via $pif #reserved for docs
$cmd 307 deny all from 204.152.64.0/23 to any in via $pif #Sun cluster
$cmd 308 deny all from 224.0.0.0/3 to any in via $pif #Class D & E multicast

# Authorized inbound packets
$cmd 400 allow udp from xx.70.207.54 to any 68 in $ks
$cmd 420 allow tcp from any to me 80 in via $pif setup limit src-addr 1

$cmd 450 deny log ip from any to any

# This is skipto location for outbound stateful rules
$cmd 500 divert natd ip from any to any out via $pif
$cmd 510 allow ip from any to any
```

```
##### end of rules #####
```

下面的这个规则集基本上和上面一样，但使用了易于读懂的编写方式，并给出了相当多的注解，以帮助经验较少的IPFW规则编写者更好地理解这些规则到底在做什么。

示范规则集#2:

```
#!/bin/sh
##### Start of IPFW rules file #####
# Flush out the list before we begin.
ipfw -q -f flush

# Set rules command prefix
cmd="ipfw -q add"
skip="skipto 800"
pif="rl0"      # public interface name of NIC
               # facing the public Internet

#####
# No restrictions on Inside LAN Interface for private network
# Change xl0 to your LAN NIC interface name
#####
$cmd 005 allow all from any to any via xl0

#####
# No restrictions on Loopback Interface
#####
$cmd 010 allow all from any to any via lo0

#####
# check if packet is inbound and nat address if it is
#####
$cmd 014 divert natd ip from any to any in via $pif

#####
# Allow the packet through if it has previous been added to the
# the "dynamic" rules table by a allow keep-state statement.
#####
$cmd 015 check-state

#####
# Interface facing Public Internet (Outbound Section)
# Interrogate session start requests originating from behind the
# firewall on the private network or from this gateway server
# destined for the public Internet.
#####

# Allow out access to my ISP's Domain name server.
# x.x.x.x must be the IP address of your ISP's DNS
# Dup these lines if your ISP has more than one DNS server
# Get the IP addresses from /etc/resolv.conf file
$cmd 020 $skip tcp from any to x.x.x.x 53 out via $pif setup keep-state
```

```

# Allow out access to my ISP's DHCP server for cable/DSL configurations.
$cmd 030 $skip udp from any to x.x.x.x 67 out via $pif keep-state

# Allow out non-secure standard www function
$cmd 040 $skip tcp from any to any 80 out via $pif setup keep-state

# Allow out secure www function https over TLS SSL
$cmd 050 $skip tcp from any to any 443 out via $pif setup keep-state

# Allow out send & get email function
$cmd 060 $skip tcp from any to any 25 out via $pif setup keep-state
$cmd 061 $skip tcp from any to any 110 out via $pif setup keep-state

# Allow out FreeBSD (make install & CVSUP) functions
# Basically give user root "GOD" privileges.
$cmd 070 $skip tcp from me to any out via $pif setup keep-state uid root

# Allow out ping
$cmd 080 $skip icmp from any to any out via $pif keep-state

# Allow out Time
$cmd 090 $skip tcp from any to any 37 out via $pif setup keep-state

# Allow out nntp news (i.e. news groups)
$cmd 100 $skip tcp from any to any 119 out via $pif setup keep-state

# Allow out secure FTP, Telnet, and SCP
# This function is using SSH (secure shell)
$cmd 110 $skip tcp from any to any 22 out via $pif setup keep-state

# Allow out whois
$cmd 120 $skip tcp from any to any 43 out via $pif setup keep-state

# Allow ntp time server
$cmd 130 $skip udp from any to any 123 out via $pif keep-state

#####
# Interface facing Public Internet (Inbound Section)
# Interrogate packets originating from the public Internet
# destined for this gateway server or the private network.
#####

# Deny all inbound traffic from non-routable reserved address spaces
$cmd 300 deny all from 192.168.0.0/16 to any in via $pif #RFC 1918 private IP
$cmd 301 deny all from 172.16.0.0/12 to any in via $pif #RFC 1918 private IP
$cmd 302 deny all from 10.0.0.0/8 to any in via $pif #RFC 1918 private IP
$cmd 303 deny all from 127.0.0.0/8 to any in via $pif #loopback
$cmd 304 deny all from 0.0.0.0/8 to any in via $pif #loopback
$cmd 305 deny all from 169.254.0.0/16 to any in via $pif #DHCP auto-config
$cmd 306 deny all from 192.0.2.0/24 to any in via $pif #reserved for docs
$cmd 307 deny all from 204.152.64.0/23 to any in via $pif #Sun cluster
$cmd 308 deny all from 224.0.0.0/3 to any in via $pif #Class D & E multicast

```

```

# Deny ident
$cmd 315 deny tcp from any to any 113 in via $pif

# Deny all Netbios service. 137=name, 138=datagram, 139=session
# Netbios is MS/Windows sharing services.
# Block MS/Windows hosts2 name server requests 81
$cmd 320 deny tcp from any to any 137 in via $pif
$cmd 321 deny tcp from any to any 138 in via $pif
$cmd 322 deny tcp from any to any 139 in via $pif
$cmd 323 deny tcp from any to any 81 in via $pif

# Deny any late arriving packets
$cmd 330 deny all from any to any frag in via $pif

# Deny ACK packets that did not match the dynamic rule table
$cmd 332 deny tcp from any to any established in via $pif

# Allow traffic in from ISP's DHCP server. This rule must contain
# the IP address of your ISP's DHCP server as it's the only
# authorized source to send this packet type.
# Only necessary for cable or DSL configurations.
# This rule is not needed for 'user ppp' type connection to
# the public Internet. This is the same IP address you captured
# and used in the outbound section.
$cmd 360 allow udp from x.x.x.x to any 68 in via $pif keep-state

# Allow in standard www function because I have Apache server
$cmd 370 allow tcp from any to me 80 in via $pif setup limit src-addr 2

# Allow in secure FTP, Telnet, and SCP from public Internet
$cmd 380 allow tcp from any to me 22 in via $pif setup limit src-addr 2

# Allow in non-secure Telnet session from public Internet
# labeled non-secure because ID & PW are passed over public
# Internet as clear text.
# Delete this sample group if you do not have telnet server enabled.
$cmd 390 allow tcp from any to me 23 in via $pif setup limit src-addr 2

# Reject & Log all unauthorized incoming connections from the public Internet
$cmd 400 deny log all from any to any in via $pif

# Reject & Log all unauthorized out going connections to the public Internet
$cmd 450 deny log all from any to any out via $pif

# This is skipto location for outbound stateful rules
$cmd 800 divert natd ip from any to any out via $pif
$cmd 801 allow ip from any to any

# Everything else is denied by default
# deny and log all packets that fell through to see what they are
$cmd 999 deny log all from any to any
##### End of IPFW rules file #####

```

第27章

高级网络

27.1 概述

本章将介绍许多与高级网络有关的话题。

读完这一章，您将了解：

- 关于网关和路由的基础知识。
- 如何安装IEEE 802.11 和Bluetooth®(蓝牙)设备。
- 怎样用FreeBSD 做"桥接(bridge)"。
- 如何为无盘机设置网络启动。
- 如何设置网络地址转换(NAT)。
- 如何使用PLIP 连接两台计算机。
- 如何在FreeBSD 主机上设置IPv6。
- 如何配置ATM。

在读这章之前，您应该：

- 理解/etc/rc 脚本的基本知识。
- 知道相关的基本网络术语。
- 了解如何配置和安装新的FreeBSD 内核(第8 章)。
- 了解如何安装第三方软件(第4 章)。

27.2 网关和路由

贡献者: Coranth Gryphon. 中文翻译: 张雪平和袁苏义.

为了让一台主机在网能找到另一台主机，就必须要有的一种机制来描述如何从一台主机连至另一台上。这一过程就是**路由选择(routing)**。“路由”是一对预先定义的地址：“目的地(destination)”和“网关(gateway)”。这对地址说明了，想要到达**目的地(destination)**，就需要通过**网关(gateway)**进行通信。目的地址有三种类型：单个主机，子网(subnets) 和“默认(default)”。如果没有应用其它路由，就会使用“默认路由”。关于默认路由将在后面进行更多的讨论。网关也有三种类型：单个主机，接口(也叫“连接(links)”) 和以太网硬件地址(MAC addresses)。

27.2.1 实例

为了说明路由选择的各个部分，首先来看看下面的例子。这是netstat 命令的输出：

```
% netstat -r
```

Routing tables

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	outside-gw	UGSc	37	418	ppp0	
localhost	localhost	UH	0	181	lo0	
test0	0:e0:b5:36:cf:4f	UHLW	5	63288	ed0	77
10.20.30.255	link#1	UHLW	1	2421		
example.com	link#1	UC	0	0		
host1	0:e0:a8:37:8:1e	UHLW	3	4601	lo0	
host2	0:e0:a8:37:8:1e	UHLW	0	5	lo0 =>	
host2.example.com	link#1	UC	0	0		
224	link#1	UC	0	0		

头两行指定默认路由(我们会在下一节说明)和本机(localhost)路由。

这张路由表里指定用于localhost的接口(Netif列)是lo0,也就是大家熟知的“回环设备”。它使得所有以此为“目的地”的通信留在本机,而不是通过LAN发出,因为它会在开始的地方就结束并返回。

接着出现的是以0:e0:开头的地址。这些是以太网硬件地址,也称为MAC地址。FreeBSD会自动识别在同一个以太网中的任何主机(如test0),并为其新增一个路由,并通过那个以太网接口——ed0直接与它通讯(译者注:那台主机。与这类路由表相关的也有一个超时项(Expire列),当我们在指定时间内没有收到从那个主机发来的信息,这项就派上用场了。这种情况下,到这个主机的路由就会被自动删除。这些主机被使用一种叫做RIP(路由信息协议--Routing Information Protocol)的机制所识别,这种机制利用基于“最短路径选择(shortest path determination)”的办法计算出到本地主机的路由。

FreeBSD也会为本地子网添加子网路由(10.20.30.255是子网10.20.30的广播地址,而example.com是这个子网相联的域名)。名称link#1代表主机上的第一块以太网卡。您会发现,对于它们没有指定另外的接口。

这两个组(本地网络主机和本地子网)的路由是由守护进程routed自动配置的。如果它没有运行,那就只有被静态定义(例如,明确输入的)的路由才存在了。

host1行代表我们的主机,它通过以太网地址来识别。因为我们是发送端,FreeBSD知道使用回还接口(lo0)而不是通过以太网接口来进行发送。

两个host2是我们使用ifconfig(8)别名(请看关于以太网的那部分就会知道我们为什么这么做)时产生的一个实例。在lo0接口之后的=>符号表明我们不仅使用了回环(因为这个地址也涉及了本地主机),而且明确指出它是个别名。这类路由只有在支持别名的主机上才能显现出来。所有本地网上的其它的主机对于这类路由只会简单拥有link#1。

最后一行(目标子网224)用于处理多播它会覆盖到其它的区域。

最后,每个路由的不同属性可以在Flags列中看到。下边是个关于这些标志和它们的含义的一个简表:

U	Up: 路由处于活动状态。
H	Host: 路由目标是单个主机。
G	Gateway: 所有发到目的地的网络传到这一远程系统上,并由它决定最后发到哪里。
S	Static: 这个路由是手工配置的,不是由系统自动生成的。
C	Clone: 生成一个新的路由,通过这个路由我们可以连接上这些主机。这种类型的路由通常用于本地网络。
W	WasCloned: 指明一个路由它是基于本地区域网络(克隆)路由自动配置的。

L Link: 路由涉及到了以太网硬件。

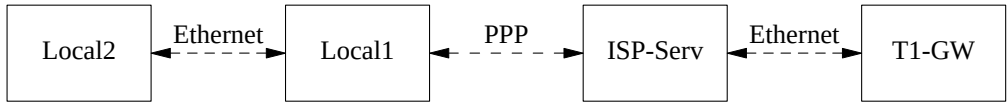
27.2.2 默认路由

当本地系统需要与远程主机建立连接时，它会检查路由表以决定是否已有已知路径存在。如果远程主机属于一个我们已知如何到达(克隆的路由)的子网内，那么系统会检查查看沿着那个接口是否能够连接。

如果所有已知路径都失败，系统还有最后一个选择：“默认”路由。这个路由是特殊类型的网关路由(通常只有一个存在于系统里)，并且总是在标志栏使用一个c来进行标识。对于本地区域网络里的主机，这个网关被设置到任何与外界有直接连接的机子里(无论是通过PPP、DSL、cable modem、T1 或其它的网络接口连接)。

如果您正为某台本身就做为网关连接外界的机子配置默认路由的话，那么该默认路由应该是您的“互联网服务商(ISP)”那方的网关机子。

让我们来看一个关于默认路由的例子。这是个很普遍的配置：



主机Local1 和Local2 在您那边。Local1 通过PPP 拨号连接到了ISP。这个PPP 服务器通过一个局域网连接到另一台网关机子它又通过一个外部接口连接到ISP 提供的互联网上。

您的每一台机子的默认路由应该是：

Host	Default Gateway	Interface
Local2	Local1	Ethernet
Local1	T1-GW	PPP

一个常见的问题是“我们为什么(或怎样)能T1-GW 设置成为Local1 默认网关，而不是它所连接ISP 服务器？”

记住，因为PPP 接口使用的一个地址是在ISP 的局域网里的，用于您那边的连接，对于ISP 的局域网里的其它机子，其路由会自动产生。因此，您就已经知道了如何到达机子T1-GW，那么也就没必要中那一步了发送通信给ISP 服务器。

通常使用地址x.x.x.1 做为一个局域网的网关。因此(使用相同的例子)，如果您本地的C 类地址空间是10.20.30，而您的ISP 使用的是10.9.9，那么默认路由表将是：

Host	Default Route
Local2 (10.20.30.2)	Local1 (10.20.30.1)
Local1 (10.20.30.1, 10.9.9.30)	T1-GW (10.9.9.1)

您可以很轻易地通过/etc/rc.conf 文件设定默认路由。在我们的实例里，在主机Local2 里，我们在文件/etc/rc.conf 里增加了下边内容：

```
defaultrouter="10.20.30.1"
```

也可以直接在命令行使用route(8) 命令：

```
# route add default 10.20.30.1
```

要了解关于如何手工维护网络路由表的进一步细节，请参考route(8) 联机手册。

27.2.3 重宿主机(Dual Homed Hosts)

还有一种其它类型的配置是我们要提及的，这就是一个主机处于两个不同的网络。技术上，任何做为网关(上边的实例中，使用了PPP 连接) 的机器就算作是重宿主机。但这个词实际上仅用来指那种处于两个局域网这中的机器。

有一种情形，一台机器有两个网卡，对于各个子网都有各自的一个地址。另一种情况，这台机器仅有一张网卡，但使用ifconfig(8) 做了别名。如果有两个独立的以太网在使用的情形就使用前者，如果只有一个物理网段，但逻辑上分成了两个独立的子网，就使用后者。

每种情况都要设置路由表以便两子网都知道这台主机是到其它子网的网关入站路由(inbound route)。将一台主机配置成两个子网间的路由器，这种配置经常在我们需要实现单向或双向的包过滤或防火墙时被用到。

如果想让主机在两个接口间转发数据包，您需要激活FreeBSD 的这项功能。至于怎么做，请看下一部分了解更多。

27.2.4 建立路由器

网络路由器只是一个将数据包从一个接口转发到另一个接口的系统。互联网标准和良好的工程实践阻止了FreeBSD 计划在FreeBSD 中把它置成默认地。您在可以在rc.conf(5) 中改变下列变量的值为YES，使用这个功能生效：

```
gateway_enable=YES          # Set to YES if this host will be a gateway
```

这个选项会把sysctl(8) 变量net.inet.ip.forwarding 设置成1。如果您要临时地停止路由，您可以把它重为0。

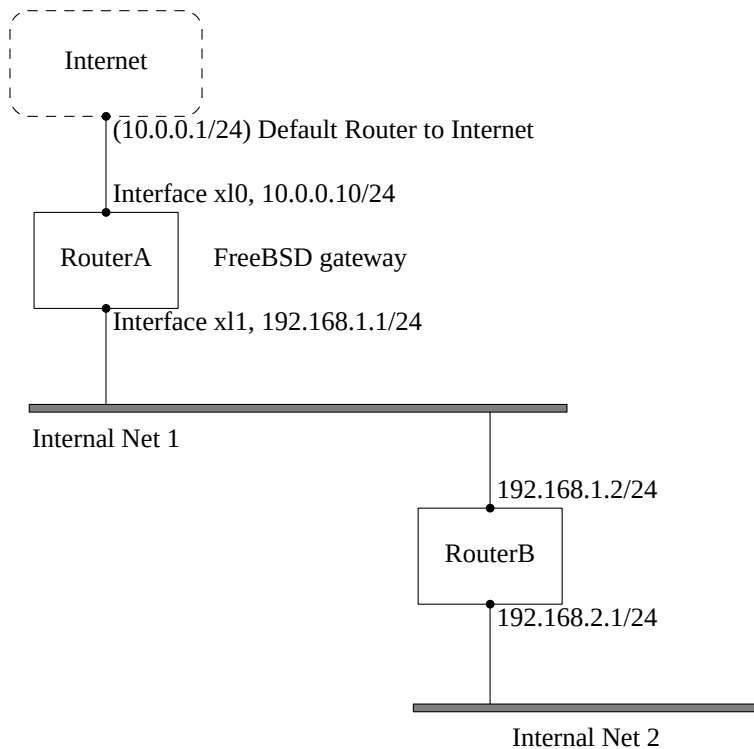
新的路由器需要有路由才知道将数据传向何处。如果网络够简单，您可以使用静态路由。FreeBSD 也自带一个标准的BSD路由选择守护进程routed(8)，称之为RIP (version 1和version 2) 和IRDP。对BGP v4，OSPF v2 和其它复杂路由选择协议的支持可以从net/zebra 包中得到。像GateD 一样的商业产品也提供了更复杂的网络路由解决方案。

27.2.5 设置静态路由

贡献者: Coranth Gryphon. 中文翻译: 张雪平和袁苏义.

27.2.5.1 手动配置

假设如下这样一个网络：



在这里，RouterA 是我们的FreeBSD 机器，它充当连接到互联网其它部分的路由器的角色。默认路由设置为10.0.0.1，它就允许与外界连接。我们假定已经正确配置了RouterB，并且知道如何连接到想去的任何地方。(在这个图里很简单。只须在RouterB上增加默认路由，使用192.168.1.1 做为网关。)

如果我们查看一下RouterA的路由表，我们会看到如下一些内容：

```
% netstat -nr
Routing tables
```

```
Internet:
Destination      Gateway          Flags    Refs      Use  Netif  Expire
default          10.0.0.1        UGS      0         49378  xl0
127.0.0.1        127.0.0.1       UH       0          6     lo0
10.0.0/24        link#1          UC       0          0     xl0
192.168.1/24     link#2          UC       0          0     xl1
```

使用当前的路由表，RouterA 是不能到达我们的内网Internal Net 2 的。它没有到192.168.2.0/24 的路由。一种可以接受的方法是手工增加这条路由。以下的命令会把Internal Net 2 网络加入到RouterA 的路由表中，使用192.168.1.2 做为下一个跳跃：

```
# route add -net 192.168.2.0/24 192.168.1.2
```

现在RouterA 就可以到达192.168.2.0/24 网络上的任何主机了。

27.2.5.2 永久配置

上面的实例对于运行着的系统来说配置静态路由是相当不错了。只是，有一个问题如果您重启您的FreeBSD 机器，路由信息就会消失。处理附加的静态路由的方法是把它放到您的/etc/rc.conf 文件里

去。

```
# Add Internal Net 2 as a static route
static_routes="internalnet2"
route_internalnet2="-net 192.168.2.0/24 192.168.1.2"
```

配置变量`static_routes` 是一串以空格格开的字符串。每一串表示一个路由名字。在上面的例子中我们中有一个串在`static_routes` 里。这个字符串中`internalnet2`。然后我们新增一个配置变量`route_internalnet2`，这里我们把所有传给`route(8)`命令的参数拿了过来。在上面的实例中的我使用的命令是：

```
# route add -net 192.168.2.0/24 192.168.1.2
```

因此，我们需要的是`"-net 192.168.2.0/24 192.168.1.2"`。

前边已经提到，可以把多个静态路由的名称，放到`static_routes` 里边。接着我们就来建立多个静态路由。下面几行所展示的，是在一个假想的路由器上增加`192.168.0.0/24` 和`192.168.1.0/24` 之间静态路由的例子：

```
static_routes="net1 net2"
route_net1="-net 192.168.0.0/24 192.168.0.1"
route_net2="-net 192.168.1.0/24 192.168.1.1"
```

27.2.6 路由传播

我们已经讨论了如何定义通向外界的路由，但未谈及外界是如何找到我们的。

我们已经知道可以设置路由表，这样任何指向特定地址空间(在我们的例子中是一个C 类子网) 的数据都会被送往网络上特定的主机，然后由这台主机向地址空间内部转发数据。

当您得到一个分配给您的网络的地址空间时，ISP(网络服务商)会设置它们的路由表，这样指向您子网的数据就会通过PPP 连接下载到您的网络。但是其它跨越国界的网络是如何知道将数据传给您的ISP 的呢？

有一个系统(很像分布式DNS 信息系统)，它一直跟踪被分配的地址空间，并说明它们连接到互联网骨干(Internet backbone)的点。“骨干(Backbone)” 指的是负责全世界和跨国的传输的主要干线。每一台骨干主机(backbone machine)有一份主要表集的拷贝，它将发送给特定网络的数据导向相应的骨干载体上(backbone carrier)，从结点往下遍历服务提供商链，直到数据到达您的网络。

服务提供商的任务是向骨干网络广播他们就是到到达您的网点的连接结点(以及进入的路径)。这就是路由传播。

27.2.7 问题解答

有时候，路由传播会有一个问题，一些网络无法与您连接。或许能帮您找出路由是在哪里中断的最有用的命令就是`traceroute(8)`了。当您无法与远程主机连接时，这个命令一样有用(例如`ping(8)`失败)。

`traceroute(8)` 命令将以您想连接的主机的名字作为参数执行。不管是到达了目标，还是因为没有连接而终止，它都会显示所经过的所有网关主机。

想了解更多的信息，查看`traceroute(8)` 的手册。

27.2.8 多播路由

FreeBSD 一开始就支持多播应用软件和多播路由选择。多播程序并不要求FreeBSD的任何特殊的配置，就可以工作得很好。多播路由需要支持被编译入内核：

```
options MROUTING
```

另外，多播路由守护进程mROUTED(8) 必须通过/etc/mROUTED.conf 配置来开启通道和DVMRP。更多关于多播路由配置的信息可以在mROUTED(8) 的手册里找到。

27.3 无线网络

作者: Eric Anderson. 中文翻译: 张雪平和袁苏义.

27.3.1 简介

如果可以使用没有烦人的随时都通过网线连接的计算机，会真的很有用。FreeBSD 可以充当无线客户端，甚至可以做为无线“接入点(access point)”。

27.3.2 无线操作模式

802.11无线设备有两种不同的配置方式: BSS 和IBSS.

27.3.2.1 BSS 模式

BSS 模式是常用的模式。它也被叫做“底层结构(infrastructure)”模式。在此种模式里，一些无线接入点连接到有线网络。每个无线网络有个名字。这个名字被称为网络的SSID。

无线客户端连接到这些无线接入点上。IEEE 802.11 标准定义了用于无线网络连接的协议。在设定了SSID 后，一个无线客户端可以连接到一个指定的网络。若不明确指定SSID，一个无线客户端可以被连接到任何的网路。

27.3.2.2 IBSS 模式

IBSS 模式，也叫专属(ad-hoc)模式，是设计来进行点对点的连接的。实际上有两种类型的专属模式。一种是IBSS 模式，也叫"ad-hoc" 或"IEEE ad-hoc"模式。这个模式由IEEE 802.11 标准定义。第二个叫做演示专属(demo ad-hoc) 模式或朗讯专属(Lucent ad-hoc) 模式(而有时与专属模式是混淆的)。这个是早先的，准802.11 专属模式，并且应该只用于过渡性的安装里。对于两类专属模式我不再做进一步介绍了。

27.3.3 底层结构(Infrastructure) 模式

27.3.3.1 接入点

接入点是一种无线网络设备，它允许一个或更多的无线客户端使用此设备作为中心集线器(hub)。使用接入点时，所有的客户端通过接入点通信。常用多个接入点来覆盖一个完整的区域，比如一所住房、一片

商业区，或一座公园。

接入点一般具有多个网络连接：无线网卡、一块或多块用于连接其它网络有线的以太网适配器。

可以购买预建的接入点，您也可以使用FreeBSD 及其兼容的无线网卡自己建立接入点。一些产商制造了带有不同功能的无线接入点和无线网卡。

27.3.3.2 建立FreeBSD 接入点

27.3.3.2.1 要求

为了在FreeBSD 上建立接入点，您要有一块兼容的无线网卡。至今为止，FreeBSD 只支持带有Prism 芯片组的网卡。您还需要被FreeBSD 支持的有线网卡(这个不难找到，FreeBSD 支持很多不同的设备)。在这里，我们假定您要桥接(bridge(4)) 有线网卡连接的网络与无线设备之间的所有传输。

FreeBSD 用来实现接入点的"hostap"功能与一定版本的firmware (固件) 工作得很好。Prism 2 网卡应该使用firmware1.3.4或更新的版本。Prism 2.5 和Prism 3 网卡应使用firmware1.4.9。老版本的firmware 可能无法正常工作。这时候，升级网卡的唯一方式是使用厂商提供的Windows firmware 升级工具。

27.3.3.2.2 设置并运行

首先，确保您的系统能识别无线网卡：

```
# ifconfig -a
wi0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet6 fe80::202:2dff:fe2d:c938%wi0 prefixlen 64 scopeid 0x7
    inet 0.0.0.0 netmask 0xff000000 broadcast 255.255.255.255
    ether 00:09:2d:2d:c9:50
    media: IEEE 802.11 Wireless Ethernet autoselect (DS/2Mbps)
    status: no carrier
    ssid ""
    stationname "FreeBSD Wireless node"
    channel 10 authmode OPEN powersavemode OFF powersavesleep 100
    wepmode OFF weptxkey 1
```

现在不用考虑细节部分，只要确认有信息表明您已安装了无线网卡。如果您无法找到无线接口，您可能使用的是PC 卡，需要查看pccardc(8) 和pccardd(8) 联机手册以获取更多信息。

下一步，您需要加载一个模块使FreeBSD 的桥接部分为接入点作好准备。加载桥接bridge(4) 模块，只需运行以下命令：

```
# kldload bridge
```

加载模块应该不会产生任何错误。如果发生了错误，您就需要将桥接bridge(4) 代码编译入内核。手册的桥接(Bridging) 部分应该能帮您完成这个任务。

现在已经完成了桥接的组件，接着我们需要告诉内核将哪些接口桥接在一起。我们使用sysctl(8) 来完成：

```
# sysctl net.link.ether.bridge.enable=1
# sysctl net.link.ether.bridge.config="wi0 xl0"
# sysctl net.inet.ip.forwarding=1
```

在FreeBSD 5.2 之前的版本中，则必须使用下面的选项：

```
# sysctl net.link.ether.bridge=1
# sysctl net.link.ether.bridge_cfg="wi0,xl0"
# sysctl net.inet.ip.forwarding=1
```

现在来设置并启动无线网卡。以下的命令将网卡设置为接入点状态：

```
# ifconfig wi0 ssid my_net channel 11 media DS/11Mbps mediaopt hostap up stationname "FreeBSD AP"
```

ifconfig(8) 行用于启动wi0 接口，并把它SSID 设置为my_net，还有把工作站名设置为FreeBSD AP。media DS/11Mbps 是把卡设置成11Mbps 模式，它是任何mediaopt产生作用所必需的。mediaopt hostap 选项把接口设置成接入点模式。channel 11 选项设置为要使用的802.11b channel(频道)。wicontrol(8) 手册包含一些有效的channel选项。

现在应该启动并运行着一个完全功能的接入点。推荐阅读wicontrol(8)，ifconfig(8) 和wi(4) 以求更深入的了解。

同样建议您阅读接着关于加密那一节。

27.3.3.2.3 状态信息

一旦接入点配置完成且可操作，操作者都会希望查看连入接入点的客户。在任何时候，都可以键入：

```
# wicontrol -l
1 station:
00:09:b7:7b:9d:16 asid=04c0, flags=3<ASSOC,AUTH>, caps=1<ESS>, rates=f<1M,2M,5.5M,11M>, sig=38.
```

显示连接了一个站点，接着的是各种参数。显示的信号通常只作为强度的相对指示。到dBm 或其它单元的转换因firmware 版本的不同而有所差异。

27.3.3.3 客户端

一个无线客户端是一个连入接入点或直接连接另一个客户端的系统。

一般地，无线客户端只有一个网络设备，也就是无线网卡。

配置无线客户端的方法有好几种。基于不同的无线模式，一般有BSS (infrastructure 模式，它需要一个接入点) 和IBSS 模式(ad-hoc，或点对点模式)。在我们的例子中我们使用了最流行的BSS模式，讨论接入点。

27.3.3.3.1 要求

将FreeBSD设置为无线客户端事实上只有一个条件。就是您需要有一块能被FreeBSD支持的无线网卡。

27.3.3.3.2 设置FreeBSD无线客户端

在开始之前，您需要了解有关要连入的无线网络的一些信息。在本例中，我们将连入一个名为my_net 的无线网络，且关闭了加密功能。

注意: 在本例中, 我们不使用加密, 这是非常危险的。在下一节中, 您将会学到如何开启加密和这样做的重要性的原因, 以及为什么一些加密技术仍不能完全地保护您。

确保您的网卡能被FreeBSD 识别:

```
# ifconfig -a
wi0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet6 fe80::202:2dff:fe2d:c938%wi0 prefixlen 64 scopeid 0x7
    inet 0.0.0.0 netmask 0xff000000 broadcast 255.255.255.255
    ether 00:09:2d:2d:c9:50
    media: IEEE 802.11 Wireless Ethernet autoselect (DS/2Mbps)
    status: no carrier
    ssid ""
    stationname "FreeBSD Wireless node"
    channel 10 authmode OPEN powersavemode OFF powersavesleep 100
    wepmode OFF weptxkey 1
```

现在, 我们要正确地设置网卡:

```
# ifconfig wi0 inet 192.168.0.20 netmask 255.255.255.0 ssid my_net
```

将192.168.0.20 和255.255.255.0 替换为有线网络上合法的IP 地址和网络掩码。记住, 接入点桥连了无线网络和有线网络之间的数据, 所以对于网络上的其它设备来说, 您就如同在有线网络上。

完成了这些, 您应该能ping 通有线网络上的主机, 就像是通过有线网络连接的一样。

如果您遇到了问题, 确认您是否连上了接入点:

```
# ifconfig wi0
```

此命令会返回一些信息, 您应该能看到:

```
status: associated
```

如果显示没有连接上(associated), 那您可能在接入点的范围以外, 需要关闭加密或者可能有配置问题。

27.3.3.4 加密

无线网络的加密非常重要因为您无法让网络处于一个被良好保护的区域。您的无线数据会向整个社区广播, 任何人都可以读到它。这就需要加密。通过加密向电波发送的数据, 使得任何有兴趣的组织从电波中提取数据变得更难。

加密客户端与接入点之间数据的最常用的方法有两种: WEP和ipsec(4)。

27.3.3.4.1 WEP

WEP 是Wired Equivalency Protocol(有线等效协议) 的缩写。WEP试图使无线网络变得如有线网络一样安全与可靠。不幸的是它已经被攻破, 是很容易被破解的。这也意味着它不适用于加密敏感数据。

但有总比没有好, 使用以下命令FreeBSD 接入点上打开WEP:


```
# ifconfig wi0 inet up ssid my_net wepmode on wepkey 0x1234567890 media DS/11Mbps mediaopt hostap
```

您可以使用以下这个命令在客户端上打开WEP:

```
# ifconfig wi0 inet 192.168.0.20 netmask 255.255.255.0 ssid my_net wepmode on wepkey 0x1234567890
```

注意您应该将0x1234567890 替换为更独特的密钥。

27.3.3.4.2 IPsec

ipsec(4) 是一个更加强大的网络数据加密工具。它无疑是加密无线网络数据的首选。在手册的IPsec 部分, 您将能更多了解ipsec(4) 的安全性及其实现。

27.3.3.5 工具

有少量用于诊断和设置无线网络的工具, 这里我们将介绍几个这样的工具。

27.3.3.5.1 bsd-airtools 包

bsd-airtools 包是一套完整的工具集, 包括了用于破解WEP 密匙的无线审核工具, 接入点检测等等。

bsd-airtools 工具集可以用net-mgmt/bsd-airtools port 来安装。关于安装ports 的信息可以在手册的第4 章 里找到。

dstumbler 是一个用于接入点发现和显示音噪比(noise ratio) 图表的工具。在您启动运行接入点有困难时, **dstumbler** 可能会帮您大忙。

为了测试无线网络的安全性, 您可以选用“dweputils” (dwepcrack, dwepdump 和dwekeygen) 来帮您测定WEP 是否是您的无线网络安全需要的正确解决方案。

27.3.3.5.2 wicontrol, ancontrol 和raycontrol 工具集

这些工具用于控制无线网卡在无线网络上行为。在以上的例子中, 我们选择了wicontrol(8), 因为我们的无线网卡是wi0 接口。如果您有Cisco (思科) 的无线设备, 出现的将是an0, 于是您可以使用ancontrol(8)。

27.3.3.5.3 ifconfig 命令

ifconfig(8) 命令可以用来处理大量与wicontrol(8) 相同的设置, 但它还是少了几个选项。查看ifconfig(8) 可以了解到命令行参数和选项。

27.3.3.6 支持的卡

27.3.3.6.1 接入点

现在唯一被支持用于BSS (作为接入点) 模式的卡都是基于Prism 2、2.5, 或3 芯片组的。要完整的列表, 查看wi(4)。

27.3.3.6.2 802.11b 客户端

现在几乎所有的802.11b无线网卡都能被FreeBSD支持。大多数基于Prism、Spectrum24、Hermes、Aironet和Raylink的网卡能在IBSS (ad-hoc, peer-to-peer, 和BSS)模式下工作。

27.3.3.6.3 802.11a & 802.11g 客户端

ath(4)设备驱动能够支持802.11a和802.11g。如果您的网卡采用的是Atheros芯片组,就可以使用这个驱动。

不幸的是,由于认为设计许多敏感的商业机密,许多厂商至今仍不愿意将把驱动程序作为开放源代码形式发布列入时间表。因此,FreeBSD以及其它操作系统的开发人员只剩下了两种选择:要么经历长时间的痛苦过程来对驱动进行逆向工程,要么使用现存的为Microsoft Windows平台编译好的驱动程序。许多开发人员,包括参与FreeBSD的那些,选择了后者。

得益于Bill Paul (wpaul)的工作,从FreeBSD 5.3-RELEASE开始,已经可以“直接”支持网络驱动接口规范(NDIS)。FreeBSD NDISulator (也被称为Project Evil)可以支持二进制形式的Windows驱动程序,并让它相信正在运行的是Windows。这是一个相对较新的功能,但许多测试证明,它确实相当有效。

要使用NDISulator,您需要三件东西:

1. 内核源代码
2. 二进制形式的Windows XP 驱动程序(扩展名是.SYS)
3. Windows XP 驱动程序配置文件(扩展名是.INF)

您可能需要编译ndis(4)袖珍端口驱动封装模块。这一操作需要以root身份来完成:

```
# cd /usr/src/sys/modules/ndis
# make && make install
```

找到您的卡所需的文件。一般来说,您应该能在随卡的CD或者制造商的网站上找到。下面的例子中,我们将使用W32DRIVER.SYS和W32DRIVER.INF这两个名字。

接下来的步骤是将二进制形式的驱动程序组装成内核模块。要完成这一任务,需要以root身份进入if_ndis模块的目录,并将Windows驱动程序复制到这里:

```
# cd /usr/src/sys/modules/if_ndis
# cp /path/to/driver/W32DRIVER.SYS ./
# cp /path/to/driver/W32DRIVER.INF ./
```

接下来我们将使用ndiscvt工具来创建驱动定义的头文件ndis_driver_data.h,用以构建驱动程序:

```
# ndiscvt -i W32DRIVER.INF -s W32DRIVER.SYS -o ndis_driver_data.h
```

选项-i和-s分别用于指定配置和二进制形式的驱动程序。我们使用-o ndis_driver_data.h参数,因为Makefile在构建内核模块时会查找它。

注意: 某些Windows驱动程序需要一些额外的文件才能正常工作。您可以把它们放到ndiscvt命令的-f参数后面。请参考ndiscvt(8)联机手册了解更多详情。

最后，就可以构建并安装内核模块了：

```
# make && make install
```

要使用驱动程序，您需要加在适当的内核模块：

```
# kldload ndis
# kldload if_ndis
```

第一个命令会加载NDIS 袖珍端口驱动封装模块，第二个则加载实际的网卡。请查看dmesg(8) 的输出以了解是否在加载过程中存在错误。如果一切正常，您应该能看到类似下面的输出：

```
ndis0: <Wireless-G PCI Adapter> mem 0xf4100000-0xf4101fff irq 3 at device 8.0 on pci1
ndis0: NDIS API version: 5.0
ndis0: Ethernet address: 0a:b1:2c:d3:4e:f5
ndis0: 11b rates: 1Mbps 2Mbps 5.5Mbps 11Mbps
ndis0: 11g rates: 6Mbps 9Mbps 12Mbps 18Mbps 36Mbps 48Mbps 54Mbps
```

这里您可以像使用其它任何无线设备(例如wi0) 那样使用ndis0 设备。具体细节可以参考线面章节的讨论。

27.4 蓝牙

作者: Pav Lucistnik. 中文翻译: 张雪平和袁苏义.

27.4.1 简介

Bluetooth (蓝牙) 是一项无线技术，用于建立带宽为2.4GHZ，波长为10 米的私有网络。网络一般是由便携式设备，比如手机(cellular phone)，掌上电脑(handhelds) 和膝上电脑(laptops) 以ad-hoc 形式组成。不象其它流行的无线技术Wi-Fi，Bluetooth 提供了更高级的服务层面，像类FTP 的文件服务、文件推送(file pushing)、语音传送、串行线模拟等等。

在FreeBSD 里，蓝牙栈(Bluetooth stack) 通过使用Netgraph 框架(请看netgraph(4)) 来的实现。大量的"Bluetooth USB dongle"由ng_ubt(4) 驱动程序支持。基于Broadcom BCM2033 芯片组的Bluetooth 设备可以通过ubtbcmfw(4) 和ng_ubt(4) 驱动程序支持。3Com Bluetooth PC 卡3CRWB60-A 由ng_bt3c(4) 驱动程序支持。基于Serial 和UART 的蓝牙设备由sio(4)、ng_h4(4) 和hcseriald(8)。本节介绍USB Bluetooth dongle 的使用。在FreeBSD 5.0 及更新的系统里，都可以支持Bluetooth。

27.4.2 插入设备

默认的Bluetooth 设备驱动程序已存在于内核模块里。接入设备前，您需要将驱动程序加载入内核：

```
# kldload ng_ubt
```

如果系统启动时Bluetooth 设备已经存在于系统里，那么从/boot/loader.conf 里加载这个模块：

```
ng_ubt_load="YES"
```

插入USB dongle。控制台(console)(或syslog中)会出现类似如下的信息:

```
ubt0: vendor 0x0a12 product 0x0001, rev 1.10/5.25, addr 2
ubt0: Interface 0 endpoints: interrupt=0x81, bulk-in=0x82, bulk-out=0x2
ubt0: Interface 1 (alt.config 5) endpoints: isoc-in=0x83, isoc-out=0x3,
      wMaxPacketSize=49, nframes=6, buffer size=294
```

注意: 在FreeBSD 6.0, 以及FreeBSD 5.X 系列中5.5 之前的版本上, 蓝牙栈必须手动启动。在FreeBSD 5.5、6.1 以及更新一些版本上, 这一工作会由devd(8) 自动完成。

复制/usr/share/examples/netgraph/bluetooth/rc.bluetooth 到一个合适的地方, 如/etc/rc.bluetooth。这个脚本用于启动和停止Bluetooth stack (蓝牙栈)。最好在拔出设备前停止stack(stack), 当然也不是非做不可。启动stack (栈) 时, 会得到如下的输出:

```
# /etc/rc.bluetooth start ubt0
BD_ADDR: 00:02:72:00:d4:1a
Features: 0xff 0xff 0xf 00 00 00 00 00
<3-Slot> <5-Slot> <Encryption> <Slot offset>
<Timing accuracy> <Switch> <Hold mode> <Sniff mode>
<Park mode> <RSSI> <Channel quality> <SCO link>
<HV2 packets> <HV3 packets> <u-law log> <A-law log> <CVSD>
<Paging scheme> <Power control> <Transparent SCO data>
Max. ACL packet size: 192 bytes
Number of ACL packets: 8
Max. SCO packet size: 64 bytes
Number of SCO packets: 8
```

27.4.3 主控制器接口(HCI)

主控制器接口(HCI) 提供了通向基带控制器和连接管理器的命令接口及访问硬件状态字和控制寄存器的通道。这个接口提供了访问蓝牙基带(Bluetooth baseband) 功能的统一方式。主机上的HCI 层与蓝牙硬件上的HCI 固件交换数据和命令。主控制器的传输层(如物理总线) 驱动程序提供两个HCI 层交换信息的能力。

为每个蓝牙(Bluetooth) 设备创建一个hci 类型的Netgraph 结点。HCI 结点一般连接蓝牙设备的驱动结点(下行流) 和L2CAP 结点(上行流)。所有的HCI操作必须在HCI 结点上进行而不是设备驱动结点。HCI 结点的默认名是“devicehci”。更多细节请参考ng_hci(4) 的联机手册。

最常见的任务是发现在RF proximity 中的蓝牙(Bluetooth) 设备。这个就叫做质询(inquiry)。质询及HCI 相关的操作可以由hccontrol(8) 工具来完成。以下的例子展示如何找出范围内的蓝牙设备。在几秒钟内您应该得到一张设备列表。注意远程主机只有被置于discoverable(可发现) 模式才能答应质询。

```
% hccontrol -n ubt0hci inquiry
Inquiry result, num_responses=1
Inquiry result #0
    BD_ADDR: 00:80:37:29:19:a4
    Page Scan Rep. Mode: 0x1
    Page Scan Period Mode: 00
    Page Scan Mode: 00
    Class: 52:02:04
    Clock offset: 0x78ef
Inquiry complete. Status: No error [00]
```

BD_ADDR 是蓝牙设备的特定地址，类似于网卡的MAC 地址。需要用此地址与某个设备进一步地通信。可以为BD_ADDR 分配由人可读的名字(human readable name)。文件/etc/bluetooth/hosts 包含已知蓝牙主机的信息。下面的例子展示如何获得分配给远程设备的可读名。

```
% hccontrol -n ubt0hci remote_name_request 00:80:37:29:19:a4
BD_ADDR: 00:80:37:29:19:a4
Name: Pav's T39
```

如果在远程蓝牙上运行质询，您会发现您的计算机是“your.host.name(ubt0)”。分配给本地设备的名字可随时改变。

蓝牙系统提供点对点连接(只有两个蓝牙设备参与)和点对多点连接。在点对多点连接中，连接由多个蓝牙设备共享。以下的例子展示如何取得本地设备的活动基带(baseband) 连接列表。

```
% hccontrol -n ubt0hci read_connection_list
Remote BD_ADDR      Handle Type Mode Role Encrypt Pending Queue State
00:80:37:29:19:a4   41  ACL    0  MAST  NONE      0      0 OPEN
```

connection handle(连接柄) 在需要终止基带连接时有用。注意：一般不需要手动完成。栈(stack) 会自动终止不活动的基带连接。

```
# hccontrol -n ubt0hci disconnect 41
Connection handle: 41
Reason: Connection terminated by local host [0x16]
```

参考hccontrol help 获取完整的HCI 命令列表。大部分HCI 命令不需要超级用户权限。

27.4.4 逻辑连接控制和适配协议(L2CAP)

逻辑连接控制和适配协议(L2CAP) 为上层协议提供面向连接和无连接的数据服务，并提供多协议功能和分割重组操作。L2CAP 允许上层协议和应用软件传输和接收最大长度为64K 的L2CAP 数据包。

L2CAP 基于**通道(channel)** 的概念。通道(Channel) 是位于基带(baseband) 连接之上的逻辑连接。每个通道以多对一的方式绑定一个单一协议(single protocol)。多个通道可以绑定同一个协议，但一个通道不可以绑定多个协议。每个在通道里接收到的L2CAP 数据包被传到相应的上层协议。多个通道可共享同一个基带连接。

为每个蓝牙(Bluetooth) 设备创建一个l2cap 类型的Netgraph 结点。L2CAP 结点一般连接HCI 结点(下行流)和蓝牙设备的驱动结点(上行流)。L2CAP 结点的默认名是“device12cap”。更多细节请参考ng_l2cap(4) 的联机手册。

一个有用的命令是l2ping(8)，它可以用来ping 其它设备。一些蓝牙实现可能不会返回所有发送给它们的数据，所以下例中的0 bytes 是正常的。

```
# l2ping -a 00:80:37:29:19:a4
0 bytes from 0:80:37:29:19:a4 seq_no=0 time=48.633 ms result=0
0 bytes from 0:80:37:29:19:a4 seq_no=1 time=37.551 ms result=0
0 bytes from 0:80:37:29:19:a4 seq_no=2 time=28.324 ms result=0
0 bytes from 0:80:37:29:19:a4 seq_no=3 time=46.150 ms result=0
```

l2control(8) 工具用于在L2CAP 上进行多种操作。以下这个例子展示如何取得本地设备的逻辑连接(通道) 和基带连接的列表：

```
% l2control -a 00:02:72:00:d4:1a read_channel_list
L2CAP channels:
Remote BD_ADDR      SCID/ DCID   PSM   IMTU/ OMTU State
00:07:e0:00:0b:ca   66/   64     3    132/  672 OPEN
% l2control -a 00:02:72:00:d4:1a read_connection_list
L2CAP connections:
Remote BD_ADDR      Handle Flags Pending State
00:07:e0:00:0b:ca   41 0           0 OPEN
```

另一个诊断工具是btsockstat(1)。它完成与netstat(1)类似的操作，只是用了蓝牙网络相关的数据结构。以下这个例子显示与l2control(8)相同的逻辑连接。

```
% btsockstat
Active L2CAP sockets
PCB      Recv-Q Send-Q Local address/PSM      Foreign address  CID   State
c2afe900  0        0 00:02:72:00:d4:1a/3    00:07:e0:00:0b:ca 66    OPEN
Active RFCOMM sessions
L2PCB    PCB      Flag MTU   Out-Q DLCs State
c2afe900 c2b53380 1    127    0     Yes  OPEN
Active RFCOMM sockets
PCB      Recv-Q Send-Q Local address      Foreign address  Chan DLCI State
c2e8bc80  0      250 00:02:72:00:d4:1a 00:07:e0:00:0b:ca 3     6    OPEN
```

27.4.5 RFCOMM 协议

RFCOMM 协议提供基于L2CAP 协议的串行端口模拟。该协议基于ETSI TS 07.10 标准。RFCOMM 是一个简单的传输协议，附加了模拟9 针RS-232(EIATIA-232-E) 串行端口的定义。RFCOMM 协议最多支持60 个并发连接(RFCOMM通道)。

为了实现RFCOMM，运行于不同设备上的应用程序建立起一条关于它们之间通信段的通信路径。RFCOMM实际上适用于使用串行端口的应用软件。通信段是一个设备到另一个设备的蓝牙连接(直接连接)。

RFCOMM 关心的只是直接连接设备之间的连接，或在网络里一个设备与modem 之间的连接。RFCOMM 能支持其它的配置，比如在一端通过蓝牙无线技术通讯而在另一端使用有线接口。

在FreeBSD，RFCOMM 协议在蓝牙套接字层(Bluetooth sockets layer) 实现。

27.4.6 设备的结对(Pairing of Devices)

默认情况下，蓝牙通信是不需要验证的，任何设备可与其它任何设备对话。一个蓝牙设备(比如手机)可以选择通过验证以提供某种特殊服务(比如拨号服务)。蓝牙验证一般使用**PIN码(PIN codes)**。一个PIN 码是最长为16 个字符的ASCII 字符串。用户需要在两个设备中输入相同的PIN码。用户输入了PIN 码后，两个设备会生成一个**连接密匙(link key)**。接着连接密匙可以存储在设备或存储器中。连接时两个设备会使用先前生成的连接密匙。以上介绍的过程被称为**结对(pairing)**。注意如果任何一方丢失了连接密匙，必须重新进行结对。

守护进程hcsecd(8) 负责处理所有蓝牙验证请求。默认的配置文件是/etc/bluetooth/hcsecd.conf。下面的例子显示一个手机的PIN 码被预设为“1234”：

```
device {
```

```

bdaddr 00:80:37:29:19:a4;
name   "Pav's T39";
key     nokey;
pin     "1234";
}

```

PIN 码没有限制(除了长度)。有些设备(例如蓝牙耳机)会有一个预置的PIN 码。`-d` 开关强制`hcsecd(8)` 守护进程处于前台, 因此很容易看清发生了什么。设置远端设备准备接收结对(pairing), 然后启动蓝牙连接到远端设备。远端设备应该回应接收了结对并请求PIN码。输入与`hcsecd.conf` 中一样的PIN 码。现在您的个人计算机已经与远程设备结对了。另外您也可以远程设备上初始结点。

在FreeBSD 5.5、6.1 以及更新版本上, 可以通过在`/etc/rc.conf` 文件中增加下面的行, 以便让`hcsecd` 在系统启动时自动运行:

```
hcsecd_enable="YES"
```

以下是简单的`hcsecd` 服务输出样本:

```

hcsecd[16484]: Got Link_Key_Request event from 'ubt0hci', remote bdaddr 0:80:37:29:19:a4
hcsecd[16484]: Found matching entry, remote bdaddr 0:80:37:29:19:a4, name 'Pav's T39', link key d
hcsecd[16484]: Sending Link_Key_Negative_Reply to 'ubt0hci' for remote bdaddr 0:80:37:29:19:a4
hcsecd[16484]: Got PIN_Code_Request event from 'ubt0hci', remote bdaddr 0:80:37:29:19:a4
hcsecd[16484]: Found matching entry, remote bdaddr 0:80:37:29:19:a4, name 'Pav's T39', PIN code e
hcsecd[16484]: Sending PIN_Code_Reply to 'ubt0hci' for remote bdaddr 0:80:37:29:19:a4

```

27.4.7 服务发现协议(SDP)

服务发现协议(SDP)提供给客户端软件一种方法, 它能发现由服务器软件提供的服务及属性。服务的属性包括所提供服务的类型或类别, 使用该服务所需要的机制或协议。

SDP 包括SDP 服务器和SDP 客户端之间的通信。服务器维护一张服务记录列表, 它介绍服务器上服务的特性。每个服务记录包含关于单个服务的信息。通过发出SDP 请求, 客户端会得到服务记录列表的信息。如果客户端(或者客户端上的应用软件)决定使用一个服务, 为了使用这个服务它必须与服务提供都建立一个独立的连接。SDP 提供了发现服务及其属性的机制, 但它并不提供使用这些服务的机制。

一般地, SDP客户端按照服务的某种期望特征来搜索服务。但是, 即使没有任何关于由SDP 服务端提供的服务的预设信息, 有时也能令人满意地发现它的服务记录里所描述的是哪种服务类型。这种发现所提供服务的过程称为**浏览(browsing)**。

蓝牙SDP 服务端`sdpd(8)` 和命令行客户端`sdpcontrol(8)` 都包括在了标准的FreeBSD 安装里。下面的例子展示如何进行SDP 浏览查询。

```

% sdpcontrol -a 00:01:03:fc:6e:ec browse
Record Handle: 00000000
Service Class ID List:
    Service Discovery Server (0x1000)
Protocol Descriptor List:
    L2CAP (0x0100)
        Protocol specific parameter #1: u/int/uuid16 1
        Protocol specific parameter #2: u/int/uuid16 1

Record Handle: 0x00000001
Service Class ID List:

```

```

Browse Group Descriptor (0x1001)

Record Handle: 0x00000002
Service Class ID List:
    LAN Access Using PPP (0x1102)
Protocol Descriptor List:
    L2CAP (0x0100)
    RFCOMM (0x0003)
        Protocol specific parameter #1: u/int8/bool 1
Bluetooth Profile Descriptor List:
    LAN Access Using PPP (0x1102) ver. 1.0

```

...等等。注意每个服务有一个属性(比如RFCOMM 通道)列表。根据服务您可能需要为一些属性做个注释。有些“蓝牙实现(Bluetooth implementation)”不支持服务浏览，可能会返回一个空列表。这种情况，可以搜索指定的服务。下面的例子展示如何搜索OBEX Object Push (OPUSH) 服务：

```
% sdpcontrol -a 00:01:03:fc:6e:ec search OPUSH
```

要在FreeBSD 里为蓝牙客户端提供服务，可以使用sdpd(8) 服务。在FreeBSD 5.5、6.1 和更新版本之上，可以通过在/etc/rc.conf 中加入下面的行：

```
sdpd_enable="YES"
```

接下来使用下面的命令来启动sdpd 服务：

```
# /etc/rc.d/sdpd start
```

在FreeBSD 6.0，以及5.5 之前的FreeBSD 5.X 版本上，sdpd 没有集成进系统启动脚本。它可以用下面的命令来手动启动：

```
# sdpd
```

需要为远端提供蓝牙服务的本地的服务程序会使用本地SDP 进程注册服务。像这样的程序就有rfcomm_pppd(8)。一旦启动它，就会使用本地SDP 进程注册蓝牙LAN 服务。

使用本地SDP 进程注册的服务列表，可以通过本地控制通道发出SDP 浏览查询获得：

```
# sdpcontrol -l browse
```

27.4.8 拨号网络(DUN) 和使用PPP(LAN) 层面的网络接入

拨号网络(DUN) 配置通常与modem 和手机一起使用。如下是这一配置所涉及的内容：

- 计算机使用手机或modem 作为无线modem 来连接拨号因特网连入服务器，或者使用其它的拨号服务；
- 计算机使用手机或modem 接收数据请求。

使用PPP(LAN) 层面的网络接入常使用在如下情形：

- 单个蓝牙设备的局域网连入；
- 多个蓝牙设备的局域网接入；

- PC 到PC (使用基于串行线模拟的PPP 网络)。

在FreeBSD 中, 两个层面使用pppd(8) 和rfcomm_pppd(8) (一种封装器, 可以将RFCOMM 蓝牙连接转换为PPP 可操作的东西) 来实现。在使用任何层面之前, 一个新的PPP 标识必须在/etc/ppp/ppp.conf 中建立。想要实例请参考rfcomm_pppd(8)。

在下面的例子中, rfcomm_pppd(8) 用来在NUN RFCOMM 通道上打开一个到BD_ADDR 为00:80:37:29:19:a4 的设备的RFCOMM 连接。具体的RFCOMM 通道号要通过SDP 从远端设备获得。也可以手动指定通RFCOMM, 这种情况下rfcomm_pppd(8) 将不能执行SDP 查询。使用sdpcontrol(8) 来查找远端设备上的RFCOMM 通道。

```
# rfcomm_pppd -a 00:80:37:29:19:a4 -c -C dun -l rfcomm-dialup
```

为了提供PPP(LAN) 网络接入服务, 必须运行sdpd(8) 服务。一个新的LAN 客户端条目必须在/etc/ppp/ppp.conf 文件中建立。想要实例请参考rfcomm_pppd(8)。最后, 在有效地通道号上开始RFCOMM PPP 服务。RFCOMM PPP 服务会使用本地SDP 进程自动注册蓝牙LAN 服务。下面的例子展示如何启动RFCOMM PPP 服务。

```
# rfcomm_pppd -s -C 7 -l rfcomm-server
```

27.4.9 OBEX 对象推送(OBEX Object Push - OPUSH) 层面

OBEX协议被广泛地用于移动设备之间简单的文件传输。它的主要用处是在红外线通信领域, 被用于笔记本或手持设备之间的一般文件传输。

OBEX 服务器和客户端由第三方软件包obexapp实现, 它可以从comms/obexapp port 安装。

OBEX 客户端用于向OBEX 服务器推入或接出对象。一个对象可以是(举个例子)商业卡片或约会。OBEX 客户能通过SDP 从远程设备取得RFCOMM 通道号。这可以通过指定服务名代替RFCOMM 通道号来完成。支持的服务名是有: IrMC、FTRN 和OPUSH。也可以用数字来指定RFCOMM 通道号。下面是一个OBEX 会话的例子, 一个设备信息对象从手机中被拉出, 一个新的对象被推入手机的目录。

```
% obexapp -a 00:80:37:29:19:a4 -C IrMC
obex> get telecom/devinfo.txt devinfo-t39.txt
Success, response: OK, Success (0x20)
obex> put new.vcf
Success, response: OK, Success (0x20)
obex> di
Success, response: OK, Success (0x20)
```

为了提供OBEX 推入服务, sdpd(8) 必须处于运行状态。必须创建一个根目录用于存放所有进入的对象。根文件夹的默认路径是/var/spool/obex。最后, 在有效的RFCOMM 通道号上开始OBEX 服务。OBEX 服务会使用SDP 进程自动注册OBEX 对象推送(OBEX Object Push) 服务。下面的例子展示如何启动OBEX 服务。

```
# obexapp -s -C 10
```

27.4.10 串口(SP)层面

串口(SP)层面允许蓝牙设备完成RS232 (或类似) 串口线的仿真。这个层面所涉及到情形是, 通过虚拟串口使用蓝牙代替线缆来处理以前的程序。

工具`rfcomm_sppd(1)`来实现串口层。“Pseudo tty”用来作为虚拟的串口。下面的例子展示如何连接远程设备的串口服务。注意您不必指定RFCOMM通道`rfcomm_sppd(1)`能够通过SDP从远端设备那里获得。如果您想代替它的话，可以在命令行里指定RFCOMM通道来实现：

```
# rfcomm_sppd -a 00:07:E0:00:0B:CA -t /dev/ttyp6
rfcomm_sppd[94692]: Starting on /dev/ttyp6...
```

一旦连接上，“pseudo tty”就可以充当串口了：

```
# cu -l ttyp6
```

27.4.11 问题解答

27.4.11.1 不能连接远端设备

一些较老的蓝牙设备并不支持角色转换(role switching)。默认情况下，FreeBSD接受一个新的连接时，它会尝试进行角色转换并成为主控端(master)。不支持角色转换的设备将无法连接。注意角色转换是在新连接建立时运行的，因此如果远程设备不支持角色转换，就不可能向它发出请求。一个HCI选项用来在本地端禁用角色转换。

```
# hccontrol -n ubt0hci write_node_role_switch 0
```

27.4.11.2 如果有错，能否知道到底正在发生什么？

可以。需要借助第三方软件包**hcidump**，它可以通过`comms/hcidump port`来安装。**hcidump**工具和**tcpdump(1)**非常相像。它可以用来显示蓝牙数据包的内容，并将其记录到文件中。

27.5 桥接

作者: Steve Peterson. 中文翻译: 张雪平和袁苏义.

27.5.1 简介

有时候需要将一个物理网络分成两个独立的网段，而无需创建新的IP子网和连接两个网段的路由器。以这种方式连接两个网络的设备称为“网桥(bridge)”。有两个网络接口的FreeBSD系统可以作为网桥。

网桥通过学习每个网络接口上的MAC层地址(以太网地址)工作。只当数据包的源地址和目标地址处于不同网络时网桥才进行转发。

在很多方面，网桥就像一个带有很少端口的以太网交换机。

27.5.2 适合桥接的情况

目前，有两种常见的情况下使用网桥。

27.5.2.1 网段上存在高流量

一种情况是您的物理网段流量过载，但是您不希望划分子网以路由器连接两个子网。

让我们考虑一个关于报社的例子，它的编辑部和产品部处于同一子网中。所有的编辑用户都使用服务器A的文件服务，而产品部使用服务器B。一个以太网将所有的用户连接在一起，高的流量负载使得网络速度变慢。

如果编辑部的用户能被分隔到一个网段中，产品部用户被分隔到另一个网段中那么这两个网段可以通过网桥连接起来。只当数据包目标为网桥“其它”端接口时，它才会被传到其它的网络上这样就减少了各个网络的拥塞。

27.5.2.2 过滤/数据整形防火墙

第二种常见的情况是需要防火墙的地方没有进行网络地址转换(NAT)。

一个例子是一个小公司，它通过DSL或ISDN连接到ISP。它拥有13个ISP分配的全局IP地址和10台PC。在这种情况下，由于划分子网的问题，使用基于路由的防火墙存在一定难度。

一个基于网桥的防火墙可以成接在DSL/ISDN路由器的后面而免去了所有的IP号问题。

27.5.3 配置网桥

27.5.3.1 选择网络接口卡

一个网桥至少需要两块网卡才能运行。不幸的是，并不是所有的网卡都能被FreeBSD 4.0支持用于桥接。阅读bridge(4)了解所支持网卡的细节。

在继续之前要先安装并测试这两块网卡。

27.5.3.2 改变内核配置

为了激活内核对桥接的支持，增加以下语句：

```
options BRIDGE
```

到您的内核配置文件里，然后重建内核。

27.5.3.3 防火墙支持

如果您打算把网桥作为防火墙来使用，则还需要加入IPFIREWALL的设置。请参考第26章以了解关于将网桥配置为防火墙的其它信息。

如果允许非IP(non-IP)数据包(比如ARP)穿过网桥，必须设置一个防火墙(firewall)选项。这个选项是IPFIREWALL_DEFAULT_TO_ACCEPT。注意：这个选项改变了默认的规则使得防火墙接受任何的数据包。在您设置这些规则前，请确认这些规则可能会产生什么后果。

27.5.3.4 数据传输支持

如果您希望将网桥作为一个数据传输器，您需要向内核文件中加入DUMMYNET 选项。阅读dummynet(4) 以做进一步了解。

27.5.4 激活网桥

增加下行：

```
net.link.ether.bridge.enable=1
```

到/etc/sysctl.conf 里，以便在运行时激活网桥，然后加下行：

```
net.link.ether.bridge.config=if1,if2
```

以便在指定的接口上激活网桥(使用您的两个网络接口的名字替换`if1` 和`if2`)。如果您希望用ipfw(8) 来过滤桥接的数据包，您还应该加入：

```
net.link.ether.bridge.ipfw=1
```

这样一行。

对于FreeBSD 5.2-RELEASE 和更早的版本，则应使用下面的配置：

```
net.link.ether.bridge=1
net.link.ether.bridge_cfg=if1,if2
net.link.ether.bridge_ipfw=1
```

27.5.5 其它信息

如果您希望可以从网络上ssh(1) 进入网桥，给一个网卡分配IP 地址就可以了。原则上给两张卡分配一个地址是很不好的。

如果网络中有多个网桥，任何两个工作站之间的路径不能多于一条。技术上说，它的意思是不支持生成连接树管理。

网桥会增加ping(8) 的延迟时间，尤其是不同网段之间的传输。

27.6 无盘操作

更新: Jean-François Dockès. 重新组织及增强: Alex Dupre. 中文翻译: 张雪平和袁苏义.

FreeBSD 主机可以从网络启动而无需本地磁盘就可操作，使用的是从NFS 服务器装载的文件系统。除了标准的配置文件，无需任何的系统修改。很容易设置这样的系统因为所有必要的元素都很容易得到：

- 至少有两种可能的方法从网络加载内核：
 - PXE: Intel 的先启动执行环境(Preboot Execution Environment) 系统是一种灵活的引导ROM 模式，这个ROM 内建在一些网卡或主板的中。查看pxeboot(8) 以获取更多细节。

- **Etherboot port (net/etherboot)** 产生通过网络加载内核的可ROM 代码。这些代码可以烧入网卡上的PROM 上，或从本地软盘(或硬盘) 驱动器加载，或从运行着的MS-DOS 系统加载。它支持多种网卡。
- 一个样板脚本(/usr/share/examples/diskless/clone_root)简化了对服务器上的工作站根文件系统的创建和维护。这个脚本需要少量的自定义，但您能很快的熟悉它。
- /etc 存在标准的系统启动文件用于侦测和支持无盘的系统启动。
- 可以向NFS 文件或本地磁盘进行交换(如果需要的话)。

设置无盘工作站有许多方法。有很多相关的元素大部分可以自定义以适合本地情况。以下将介绍一个完整系统的安装，强调的是简单性和与标准FreeBSD 启动脚本的兼容。介绍的系统有以下特性：

- 无盘工作站使用一个共享的只读/ 文件系统和一个共享的只读/usr 。
- root 文件系统是一份标准的FreeBSD 根文件系统(一般是服务器的)，只是一些配置文件被特定于无盘操作的配置文件覆盖。
- root 文件系统必须可写的部分被mfs(8) (FreeBSD 4.X) 或md(4) (FreeBSD 5.X) 文件系统覆盖。任何的改写在重启后都会丢失。
- 内核由**etherboot** 或PXE 传送和加载，有些情况可能会指定使用其中之一。

小心: 如上所述，这个系统是不安全的。它应该处于网络的受保护区域并不被其它主机信任。

这部分所有的信息都已使用FreeBSD releases 4.9-RELEASE 和5.2.1-RELEASE 测试过。文本主是使用4.X 格式组织的。为适应5.X 的改变，都有注释被加入。

27.6.1 背景信息

设置无盘工作站相对要简单而又易出错。有时分析一些原因是很难的。例如：

- 编译时选项在运行时可能产生不同的行为。
- 出错信息经常是加密了的或根本就没有。

在这里，涉及到的一些背景知识对于可能出现的问题的解决是很有帮助的。

要成功地引导系统还有些操作需要做。

- 机器需要获取初始的参数，如它的IP 地址、执行文件、服务器名、根路径。这个可以使用或BOOTP 协议来完成。DHCP 是BOOTP 的兼容扩展，并使用相同的端口和基本包格式。

只使用BOOTP 来配置系统也是可行的。bootpd(8) 服务程序被包含在基本的FreeBSD 系统里。

不过，DHCP 相比BOOTP 有几个好处(更好的配置文件，使用PXE 的可能性，以及许多其它并不直接相关的无盘操作)，接着我们会要描述一个DHCP 配置，可能的话会利用与使用bootpd(8) 相同的例子。这个样板配置会使用ISC DHCP 软件包(3.0.1.r12 发行版安装在测试服务器上)。

- 机器需要传送一个或多个程序到本地内存。TFTP 或NFS 会被使用。选择TFTP 还是NFS 需要在几个地方的“编译时间”选项里设置。通常的错误源是为文件名指定了错误的协议：TFTP 通常从服务器里的一个单一目录传送所有文件，并需要相对这个目录的文件名。NFS 需要的是绝对文件路径。

- 介于启动程序和内核之间的可能的部分需要被初始化并执行。在这部分有几个重要的变量：
 - PXE 会装入pxeboot(8)它是FreeBSD 第三阶段装载器的修改版。loader(8) 会获得许多参数用于系统启动，并在传送控制之前把它们留在内核环境里。在这种情况下，使用GENERIC 内核就可能了。
 - **Etherboot** 会做很少的准备直接装载内核。您要使用指定的选项建立(build) 内核。

PXE 和**Etherboot** 在4.X 系统里工作得一样的好。因为5.X 内核通常让loader(8) 做了更多的事情，PXE 比较适合5.X 系统。

如果您的BIOS 和网卡支持PXE，您应该使用它。当然，使用**Etherboot** 依然可以启动5.X 系统。

- 最后，机器需要访问它的文件系统。NFS 使用在所有的情况下。

查看diskless(8) 手册页。

27.6.2 安装说明

27.6.2.1 配置使用ISC DHCP

ISC DHCP 服务器可以回应BOOTP 和DHCP 的请求。

对于4.9的发行版，**ISC DHCP 3.0** 并不属于基本系统。首先您需要安装net/isc-dhcp3-server port 或相应的“包”。

一旦安装了**ISC DHCP**，还需要一个配置文件才能运行(通常名叫usr/local/etc/dhcpd.conf)。这里有个注释过的例子，里边主机margaux 使用**Etherboot**，而主机corbieres 使用PXE:

```
default-lease-time 600;
max-lease-time 7200;
authoritative;

option domain-name "example.com";
option domain-name-servers 192.168.4.1;
option routers 192.168.4.1;

subnet 192.168.4.0 netmask 255.255.255.0 {
    use-host-decl-names on; ❶
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.4.255;

    host margaux {
        hardware ethernet 01:23:45:67:89:ab;
        fixed-address margaux.example.com;
        next-server 192.168.4.4; ❷
        filename "/data/misc/kernel.diskless"; ❸
        option root-path "192.168.4.4:/data/misc/diskless"; ❹
    }
    host corbieres {
        hardware ethernet 00:02:b3:27:62:df;
        fixed-address corbieres.example.com;
        next-server 192.168.4.4;
        filename "pxeboot";
        option root-path "192.168.4.4:/data/misc/diskless";
    }
}
```

```
}
```

- ❶ 这个选项告诉**dhcpcd** 发送**host** 里声明的用于无盘主机的主机名的值。另外可能会增加一个**option host-name margaux** 到**host** 声明里。
- ❷ **next-server** 正式指定TFTP 或NFS 服务用于载入装载机或内核文件(默认使用的是相同的主机作为DHCP 服务器)。
- ❸ **filename** 正式定义这样的文件**etherboot** 或PXE 为执行下一步将装载它。根据使用的传输方式, 它必须要指定。**Etherboot** 可以被编译来使用NFS 或TFTP。FreeBSD port 默认配置了NFS。PXE 使用TFTP, 这就是为什么在这里使用相对文件名(这可能依赖于TFTP 服务器配置, 不过会相当典型)。同样, PXE 会装载pxeboot, 而不是内核。另外有几个很有意思的可能, 如从FreeBSD CD-ROM 的/boot 目录装载pxeboot (因为pxeboot(8) 能够装载GENERIC 内核, 这就使得可以使用PXE 从远程的CD-ROM 里启动)。
- ❹ **root-path** 选项定义到根(**root**) 文件系统的路径, 通常是NFS 符号。当使用PXE 时, 只要您不启用内核里的BOOTP 选项, 可以不管主机的IP。NFS 服务器然后就如同TFTP 一样。

27.6.2.2 配置使用BOOTP

这里紧跟的是一个等效的**bootpd** 配置(减少到一个客户端)。这个可以在/etc/bootptab 里找到。

请注意: 为了使用BOOTP, **etherboot** 必须使用非默认选项**NO_DHCP_SUPPORT** 来进行编译, 而且PXE 需要 DHCP。**bootpd** 的唯一可见的好处是它存在于基本系统中。

```
.def100:\
:hn:ht=1:sa=192.168.4.4:vm=rfc1048:\
:sm=255.255.255.0:\
:ds=192.168.4.1:\
:gw=192.168.4.1:\
:hd="/tftpboot":\
:bf="/kernel.diskless":\
:rp="192.168.4.4:/data/misc/diskless":
```

```
margaux:ha=0123456789ab:tc=.def100
```

27.6.2.3 使用Etherboot准备启动程序

Etherboot 的网站 (<http://etherboot.sourceforge.net>) 包含有更多的文档 (<http://etherboot.sourceforge.net/doc/html/userman/t1.html>) 主要瞄准的是Linux 系统, 但无疑包含有有用的信息。如下列出的是关于在FreeBSD 系统里使用**Etherboot**。

首先您必须安装net/etherboot 包或port。

您可以改变**Etherboot** 的配置(如使用TFTP 来代替NFS), 方法是修改Config 文件在**Etherboot** 源目录里。

对于我们的设置, 我们要使用一张启动软盘。对于其它的方法(PROM, 或MS-DOS程序), 请参考**Etherboot** 文档。

想要使用启动软盘，先插入一张软盘到安装有**Etherboot**的机器的驱动器里，然后把当前路径改到**src**目录在**Etherboot**树下，接着输入：

```
# gmake bin32/devicetype.fd0
```

devicetype 依赖于无盘工作站上的以太网卡的类型。参考在同一个目录下的**NIC**文件确认正确的*devicetype*。

27.6.2.4 使用PXE启动

默认地，**pxeboot(8)** 装载器通过**NFS** 装载内核。它可以编译来使用**TFTP**通过在文件**/etc/make.conf**里指定**LOADER_TFTP_SUPPORT**选项来代替。查看**/etc/defaults/make.conf**里的注释(或**5.X**系统的**/usr/share/examples/etc/make.conf**)可以获得指导。

其它有两个未说明的**make.conf**选项它可能对于设置一系列控制台无盘机器会有用：**BOOT_PXEldr_PROBE_KEYBOARD**和**BOOT_PXEldr_ALWAYS_SERIAL** (后者只存在于**FreeBSD 5.X**里)。

当机器启动里，要使用**PXE**，通常要选择**Boot from network**选项在**BIOS**设置里，或者在**PC**初始化的时候输入一个功能键(function key)。

27.6.2.5 配置TFTP和NFS服务器

如果您正在使用**PXE**或**Etherboot**配置使用了**TFTP**，那么您需要在文件服务器上启用**tftpd**：

1. 建立一个目录从那里**tftpd**可以提供文件服务，如**/tftpboot**。
2. 把这一行加入到**/etc/inetd.conf**里：

```
tftp dgram udp wait root /usr/libexec/tftpd tftpd -l -s /tftpboot
```

注意：好像有一些版本的**PXE**需要**TCP**版本的**TFTP**。在这种情况下，加入第二行，使用**stream tcp**来代替**dgram udp**。

3. 让**inetd**重读它的配置文件：

```
# kill -HUP `cat /var/run/inetd.pid`
```

您能把**tftpboot**目录放到服务器上的任何地方。确定这个位置设置在**inetd.conf**和**dhcpd.conf**里。

在所有的情况下，您都需要启用**NFS**，并且**NFS**服务器上导出相应的文件系统。

1. 把这一行加入到**/etc/rc.conf**里：
nfs_server_enable="YES"
2. 通过往**/etc/exports**里加入下面几行(调整“载入点”列，并且使用无盘工作站的名字替换**margaux corbieres**)，导出文件系统无盘根目录存在于此：
/data/misc -alldirs -ro margaux corbieres
3. 让**mountd**重读它的配置文件。如果您真的需要启用第一步的**/etc/rc.conf**里**NFS**，您可能就要重启系统了。


```
# kill -HUP 'cat /var/run/mountd.pid'
```

27.6.2.6 建立无盘内核

如果您在使用**Etherboot**，您需要为无盘客户端建立内核配置文件，使用如下选项(除了常使用的外):

```
options      BOOTP          # Use BOOTP to obtain IP address/hostname
options      BOOTP_NFSROOT  # NFS mount root filesystem using BOOTP info
```

您可能也想使用BOOTP_NFSV3, BOOT_COMPAT 和BOOTP_WIRED_TO (参考4.X 里的LINT 或5.X里的NOTES)。

这些名字具有历史性，并且有些有些误导，因为它们实际上启用了内核里(它可能强制限制BOOTP或DHCP 的使用)，与DHCP 和BOOTP 的无关的应用。

编译内核(参考第8 章)，然后将它复制到dhcpd.conf 里指定的地方。

注意: 当使用PXE 里，使用以上选项建立内核并不做严格要求(尽管建议这样做)。启用它们会在内核启动时引起更多的DHCP 提及过的请求，带来的小小的风险是在有些特殊情况下新值和由pxeboot(8) 取回的值之间的不一致性。使用它们的好处是主机名会被附带设置。否则，您就需要使用其它的方法来设置主机名，如在客户端指定的rc.conf 文件里。

注意: 为了使带有**Etherboot** 的5.X 内核可引导，就需要把设备提示(device hint) 编译进去。通常要在配置文件(查看NOTES 配置注释文件) 里设置下列选项:

```
hints "GENERIC.hints"
```

27.6.2.7 准备根(root)文件系统

您需要为无盘工作站建立根文件系统，位置列在dhcpd.conf 里的root-path 里边。下面部分描述了要这样做的两种方法:

27.6.2.7.1 使用clone_root 脚本

这是建立根文件系统最快的方法，只是目前只在FreeBSD4.X 里支持。这个shell 脚本位于/usr/share/examples/diskless/clone_root 并且需要定制，至少需要调整将会被建立文件系统的地方(DEST 可变)。

参考用于指导的脚本的最前边的注释。它们说明了如何建立一个基本文件系统，并且如果根据特定版本的无盘工作站、子网或个人工作站选择性地忽略。它们也为无盘的/etc/fstab 的/etc/rc.conf 文件给出了例子。

在/usr/share/examples/diskless 里的README 文件包含了许多有趣的背景信息，但是，他们同diskless 目录里的其它例子一起，实际上说明了一种配置方法与被clone_root 和/etc 里的系统启动脚本使用的完全不同，这个有点迷人。使用它们只用做参考，除非您使用它们所描述的方法这种情况下您需要定制rc 脚本。

27.6.2.7.2 使用标准的make world 程序

这种方法可以应用到FreeBSD 4.X 或5.X, 而且会安装一个彻底干净的系统(不仅仅是根文件系统)到DESTDIR。您需要做的就是简单地执行下面的脚本:

```
#!/bin/sh
export DESTDIR=/data/misc/diskless
mkdir -p ${DESTDIR}
cd /usr/src; make world && make kernel
cd /usr/src/etc; make distribution
```

一旦完成, 您可能需要定制/etc/rc.conf 和/etc/fstab根据您的需要放到DESTDIR里。

27.6.2.8 配置swap(交换)

如果需要, 位于服务器上的交换文件可以通过NFS 来访问。完成它的一种普遍使用的方法在5.X 的发行版里已不再继续(使用)。

27.6.2.8.1 NFS与FreeBSD 4.X 之间的Swap(交换)

交换文件的位置和大小可以使用BOOTP/DHCP 来指定, FreeBSD 指定的选项是128 和129。用于ISC DHCP 3.0 或bootpd的配置文件例子如下:

1. 把下边几行加到dhcpd.conf 里:

```
# Global section
option swap-path code 128 = string;
option swap-size code 129 = integer 32;

host margaux {
    ... # Standard lines, see above
    option swap-path "192.168.4.4:/netswapvolume/netswap";
    option swap-size 64000;
}
```

swap-path 指的是存放交换文件存的路径。每个文件会命名为swap.client-ip。

旧版的dhcpd 使用的风格是option option-128 "... , 这个已不在支持。

/etc/bootptab 会使用下面的格式代替:

```
T128="192.168.4.4:/netswapvolume/netswap":T129=0000fa00
```

注意: 在/etc/bootptab 里, 交换大小必须以十六进制表示。

2. 在NFS 交换文件服务器上, 建立交换文件:

```
# mkdir /netswapvolume/netswap
# cd /netswapvolume/netswap
# dd if=/dev/zero bs=1024 count=64000 of=swap.192.168.4.6
# chmod 0600 swap.192.168.4.6
```

192.168.4.6 是无盘客户端的IP 地址。

3. 在NFS 交换文件服务器上，增加下面几行到/etc/exports:

```
/netswapvolume -maproot=0:10 -alldirs margaux corbieres
```

然后让mountd 重读exports文件，同上。

27.6.2.8.2 NFS 与FreeBSD &os 5.X 之间的Swap(交换)

内核并不支持在引导时启用NFS 交换区。交换区必须通过启动脚本启用，其过程是挂接一个可写的文件系统，并在其上创建并启用交换文件。要建立尺寸合适的交换文件，可以这样做：

```
# dd if=/dev/zero of=/path/to/swapfile bs=1k count=1 oseek=100000
```

要启用它，您须要把下面几行加到rc.conf里：

```
swapfile=/path/to/swapfile
```

27.6.2.9 杂项问题

27.6.2.9.1 运行时/usr 是只读在

如果无盘工作站是配置来支持X，那么您就必须调整XDM 配置文件，因为它默认把错误信息写到/usr。

27.6.2.9.2 使用非FreeBSD 服务器

当用作根文件系统的服务器运行的是非FreeBSD，您须要在FreeBSD 机器上建立根文件系统，然后把它复制到它的目的地，使用的命令可以是tar 或cpio。

在这种情况下，有时对于/dev 里的一些特殊的文件会有问题，原因就是不同的“最大/最小”整数大小。一种解决的方法就是从非FreeBSD 服务里导出一个目录，并把它载入FreeBSD 到机子上，然后在FreeBSD 机子上执行MAKEDEV 来建立正确的设备条目(FreeBSD 5.0及新版使用devfs(5) 来为用户透明地分派设备节点，在这些版本上执行MAKEDEV 是毫无意义的)。

27.7 ISDN

关于ISDN 技术和硬件的一个好的资源是Dan Kegel 的ISDN 主页 (<http://www.alumni.caltech.edu/~dank/isdn/>)。

一个快速简单的到ISDN 的路线图如下：

- 如果您住在欧洲，您可能要查看一下ISDN卡部分。
- 如果您正计划首要地使用ISDN基于拨号非专用线路连接到带有提供商的互联网，您可能要了解一下终端适配器。如果您更改提供商的话，这会给您带来最大的灵活性、最小的麻烦。
- 如果您连接了两个局域网(LAN)，或使用了专用的ISDN连线连接到互联网，您可能要考虑选择单独的路由器/网桥。

在决定选择哪一种方案的时候，价格是个很关键的因素。下面列有从不算贵到最贵的选择：

27.7.1 ISDN 卡

贡献者: Hellmuth Michaelis. 中文翻译: 张雪平.

FreeBSD 的ISDN 工具通过被动卡(passive card) 仅支持DSS1/Q.931(或Euro-ISDN) 标准。启动FreeBSD 4.4, 有些主动卡(active card) 也被支持, 这时它也支持其它发信协议; 包括有最先支持的“Primary Rate (PRI) ISDN”卡。

isdn4bsd 软件允许连接到其它ISDN 路由器, 使用的是原始的HDLC 上的IP 或利用同步PPP: 使用带有**isppp** (一个修改过的**sppp**(4) 驱动程序)的PPP 内核, 或使用用户区(userland) **ppp**(8)。通过使用userland **ppp**(8), 两个或更多ISDN 的B 通道联结变得可能。除了许多如300 波特(Baud) 的软modem 一样的工具外, 还可以实现电话应答机应用。

在FreeBSD 里, 正有更多的PC ISDN 卡被支持; 报告显示在整个欧洲及世界的其它许多地区可以成功使用。

被支持的主动型ISDN 卡主要是带有Infineon (以前的Siemens) ISAC/HSCX/IPAC ISDN 芯片组, 另外还有带有Cologne (只有ISA 总线) 芯片的ISDN 卡、带有Winbond W6692 芯片的PCI 卡、一部分带有Tiger300/320/ISAC 芯片组的卡以及带有一些商家专有的芯片组的卡(如AVM Fritz!Card PCI V.1.0 和the AVM Fritz!Card PnP)。

当前积极的支持的ISDN 卡有AVM B1 (ISA 和PCI) BRI 卡和AVM T1 PCI PRI 卡。

关于**isdn4bsd** 的文档, 请查看FreeBSD 系统里的/usr/share/examples/isdn/ 目录或查看**isdn4bsd** 的主页 (<http://www.freebsd-support.de/i4b/>), 那里也有提示、勘误表以及更多的文档(如**isdn4bsd**手册 (<http://people.FreeBSD.org/~hm/>))。

要是您有兴趣增加对不同ISDN 协议的支持, 对当前还不支持的ISDN PC 卡的支持或想增强**isdn4bsd** 的性能, 请联系Hellmuth Michaelis <hm@FreeBSD.org>。

对于安装、配置以及**isdn4bsd** 故障排除的问题, 可以利用**freebsd-isdn** (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-isdn>) 邮件列表。

27.7.2 ISDN 终端适配器

终端适配器(TA) 对于ISDN 就好比modem 对于常规电话线。

许多TA 使用标准的Hayes modem AT 命令集, 并且可以降级来代替modem。

TA 基本的运作同modem 一样, 不同之处是连接和整个速度更比老modem 更快。同modem 的安装一样, 您也需要配置PPP。确认您的串口速度已足够高。

使用TA 连接互联网提供商的主要好处是您可以做动态的PPP。由于IP 地址空间变得越来越紧张, 许多提供商都不愿再提供静态IP。许多的独立的路由器是不支持动态IP 分配的。

TA 完全依赖于您在运行的PPP 进程，以完成它们的功能和稳定的连接。这可以让您在FreeBSD 机子里轻易地从使用modem 升级到ISDN，要是您已经安装了PPP 的话。只是，在您使用PPP 程序时所体验到任何问题同时也存在。

如果您想要最大的稳定性，请使用PPP 内核选项，而不要使用userland PPP。

下面的TA 就可以同FreeBSD 一起工作：

- Motorola BitSurfer 和Bitsurfer Pro
- Adtran

大部分其它的TA 也可能工作，TA 提供商试图让他们的产品可以接受大部分的标准modem AT 命令集。

对于外置TA 的实际问题是：象modem 要一样，您机子需要有一个好的串行卡。

想要更深入地理解串行设备以及异步和同步串口这间的不同点，您就要读读FreeBSD 串行硬件 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/serial-uart/index.html)教程了。

TA 将标准的PC 串口(同步的) 限制到了115.2 Kbs，即使您有128 Kbs 的连接。想要完全利用ISDN 有能力达到的128 Kbs，您就需要把TA 移到同步串行卡上。

当心被骗去买一个内置的TA 以及自认为可以避免同步/异步问题。内置的TA 只是简单地将一张标准PC 串口芯片内建在里边。所做的这些只是让您省去买另一根串行线以及省去寻找另一个空的插孔。

带有TA 的同步卡至少和一个独立的路由器同样快地，而且仅使用一个简单的386 FreeBSD 盒驱动它。

选择同步卡/TA 还是独立的路由器，是个要高度谨慎的问题。在邮件列表里有些相关的讨论。我们建议您去搜索一下关于完整讨论的记录 (<http://www.FreeBSD.org/search/index.html>)。

27.7.3 单独的ISDN 桥/路由器

ISDN 桥或路由器根本就没有指定要FreeBSD 或其它任何的操作系统。更多完整的关于路由和桥接技术的描述，请参考网络指南的书籍。

这部分的内容里，路由器和桥接这两个词汇将会交替地使用。

随着ISDN 路由器/桥的价格下滑，对它们的选择也会变得越来越流行。ISDN 路由器是一个小盒子，可以直接地接入您的本地以太网，并且自我管理到其它桥/路由器的连接。它有个内建的软件用于与通信通过PPP 和其它流行的协议。

路由器有比标准TA 更快的吞吐量，因为它会使用完全同步的ISDN 连接。

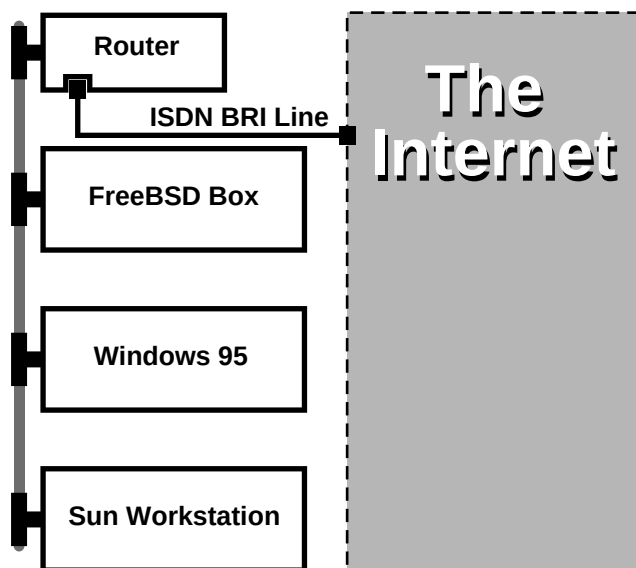
使用ISDN 路由器和桥的主要问题是两个生产商之间的协同性仍存在问题。如果您计划连接到互联网提供商，您应该跟他们进行交涉。

如果您计划连接两个局域网网段，如您的家庭网和办公网，这将是最低维护的解决方案。因为您买的设备是用于连接两边的，可以保证这种连接一定会成功。

例如连接到家里的计算机，或者是办公网里的一个分支连接到办公主网，那么下面的设置就可能用到：

例27-1. 办公室局部或家庭网

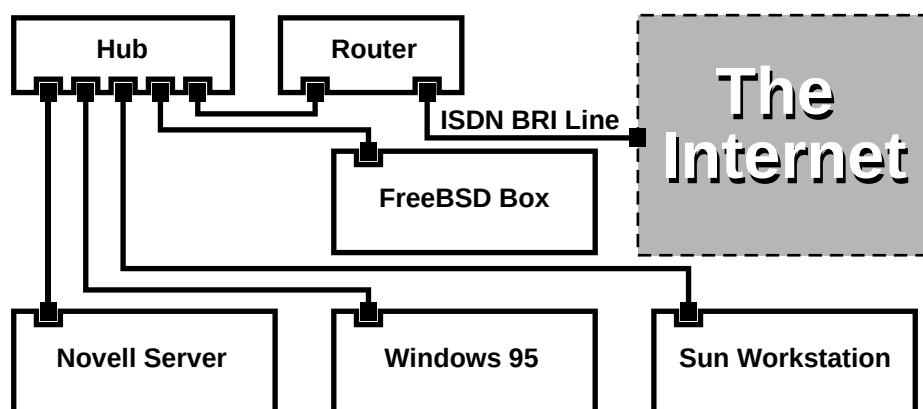
网络使用基于总线拓扑的10 base 2 以太网(“瘦网(thinnet)”)。如果有必要，用网线连接路由器和AUI/10BT 收发器。



如果您的家里或办公室支部里只有一台计算机，您可以使用一根交叉的双绞线直接连接那台独立路由器。

例27-2. 主办公室或其它网络

网络使用的是星形拓扑的10 base T 以太网(“双绞线”)。



大部分路由器/网桥有一大好处就是，它们允许您在同一时间，有两个分开独立的 PPP 连接到两个分开的点上。这点在许多的TA 上是不支持的，除非带有两个串口的特定模式(通常都很贵)。请不要把它与通道连接、MPP 等相混淆。

这是个非常有用的功能，例如，如果在您的办公室里您有个专有的ISDN 连接，而且您想接入到里边，但休想让另一根ISDN 线也能工作。办公室里的路由器能够管理专有的B通道连接到互联网(64 Kbps) 以及使用另一个通道B 来完成单独的数据连接。第二个B 通道可以用于拨进、拨出或动态与第一个B通道进行连接(MPP等)，以获取更大宽带。

以太网桥也允许您传输的不仅仅是IP 通信。您也可以发送IPX/SPX 或其它任何您所使用的协议。

27.8 网络地址转换

作者: Chern Lee, 译者: 李鑫.

27.8.1 概要

FreeBSD 的网络地址转换服务，通常也被叫做natd(8)，是一个能够接收连入的未处理IP 包，将源地址修改为本级地址然后重新将这些包注入到发出IP 包流中。natd(8) 同时修改源地址和端口，当接收到响应数据时，它作逆向转换以便把数据发回原先的请求者。

NAT 最常见的用途是为人们所熟知的Internet 连接共享。

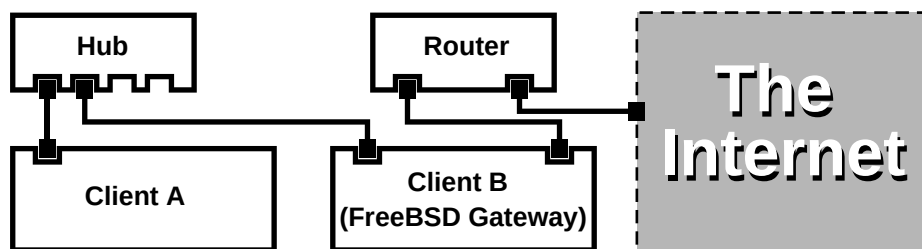
27.8.2 安装

随着IPv4 的IP 地址空间的日益枯竭，以及使用如DSL 和电缆等高速连接的用户逐渐增多，越来越多的人开始需要Internet 连接共享这样的解决方案。由于能够将许多计算机通过一个对外的IP 地址进行接入，natd(8) 成为了一个理想的选择。

更为常见的情况，一个用户通过电缆或者DSL 线路接入，并拥有一个IP 地址，同时，希望通过这台接入Internet 的计算机来为LAN 上更多的计算机提供接入服务。

为了完成这一任务，接入Internet 的FreeBSD 机器必须扮演网关的角色。这台网关必须有两块网卡——一块用于连接Internet 路由器，另一块用来连接LAN。所有LAN 上的机器通过Hub 或交换机进行连接。

注意: 有多种方法能够通过FreeBSD 网关将LAN 接入Internet。这个例子只介绍了有至少两块网卡的网关。



上述配置被广泛地用于共享Internet 连接。LAN 中的一台机器连接到Internet 中。其余的计算机则通过那台“网关” 机来连接Internet。

27.8.3 配置

下面这些选项必须放到内核配置文件中：

```
options IPFIREWALL
```

options IPDIVERT

此外，下列是一些可选的选项：

```
options IPFIREWALL_DEFAULT_TO_ACCEPT
options IPFIREWALL_VERBOSE
```

这些配置必须放到/etc/rc.conf 中：

```
gateway_enable="YES" ❶
firewall_enable="YES" ❷
firewall_type="OPEN" ❸
natd_enable="YES"
natd_interface="fxp0" ❹
natd_flags="" ❺
```

- ❶ 将机器配置为网关。执行sysctl net.inet.ip.forwarding=1 效果相同。
- ❷ 在启动时启用/etc/rc.firewall 中的防火墙规则。
- ❸ 指定一个预定义的允许所有包进入的防火墙规则集。参见/etc/rc.firewall 以了解其他类型的规则集。
- ❹ 指定通过哪个网络接口转发包(接入Internet 的那一个)。
- ❺ 其他希望在启动时传递给natd(8) 的参数。

在/etc/rc.conf 中加入上述选项将在系统启动时运行natd -interface fxp0。这一工作也可以手工完成。

注意：当有太多选项要传递时，也可以使用一个natd(8) 的配置文件来完成。这种情况下，这个配置文件必须通过在/etc/rc.conf 里增加下面内容来定义：

```
natd_flags="-f /etc/natd.conf"
```

/etc/natd.conf 文件会包含一个配置选项列表，每行一个。在紧跟部分的例子里将使用下面的文件：

```
redirect_port tcp 192.168.0.2:6667 6667
redirect_port tcp 192.168.0.3:80 80
```

关于配置文件的更多信息，参考natd(8) 手册页中关于-f 选项那一部分。

在LAN后面的每一台机子和接口应该被分配私有地址空间(由RFC 1918 (ftp://ftp.isi.edu/in-notes/rfc1918.txt)定义) 里的IP 地址，并且默认网关设成natd 机子的内连IP 地址。

例如：客户端A 和B 在LAN 后面，IP 地址是192.168.0.2 和192.168.0.3，同时natd 机子的LAN 接口上的IP 地址是192.168.0.1。客户端A 和B 的默认网关必须要设成natd 机子的IP 192.168.0.1。natd 机子外连，或互联网接口不需要为了natd(8) 而做任何特别的修改就可工作。

27.8.4 端口重定向

使用natd(8)的缺点就是LAN客户不能从互联网访问。LAN上的客户可以进行到外面的连接，而不能接收进来的连接。如果想在LAN的客户端机子上运行互联网服务，这就会有问题。对此的一种简单方法是在natd机子上重定向选定的互联网端口到LAN客户端。

例如：在客户端A上运行IRC服务，而在客户端B上运行web服务。想要正确的工作，在端口6667 (IRC) 和80 (web) 上接收到的连接就必须重定向到相应的机子上。

-redirect_port 需要使用适当的选项传送给natd(8)。语法如下：

```
-redirect_port proto targetIP:targetPORT[-targetPORT]
                [aliasIP:]aliasPORT[-aliasPORT]
                [remoteIP[:remotePORT[-remotePORT]]]
```

在上面的例子中，参数应该是：

```
-redirect_port tcp 192.168.0.2:6667 6667
-redirect_port tcp 192.168.0.3:80 80
```

这就会重定向适当的tcp端口到LAN上的客户端机子。

-redirect_port 参数可以用来指出端口范围来代替单个端口。例如，tcp 192.168.0.2:2000-3000 2000-3000 就会把所有在端口2000到3000上接收到的连接重定向到主机A上的端口2000到3000。

当直接运行natd(8)时，就可以使用这些选项，把它们放到/etc/rc.conf里的natd_flags=""选项上，或通过一个配置文件进行传送。

想要更多配置选项，请参考natd(8)。

27.8.5 地址重定向

如果有几个IP地址提供，那么地址重定向就会很有用，然而他们必须在一个机子上。使用它，natd(8)就可以分配给每一个LAN客户端它们自己的外部IP地址。natd(8)然后会使用适当的的外部IP地址重写从LAN客户端外出的数据包，以及重定向所有进来的数据包一定的IP地址回到特定的LAN客户端。这也叫做静态NAT。例如，IP地址128.1.1.1、128.1.1.2和128.1.1.3属于natd网关机子。128.1.1.1可以用来作natd网关机子的外连IP地址，而128.1.1.2和128.1.1.3用来转发回LAN客户端A和B。

-redirect_address 语法如下：

```
-redirect_address localIP publicIP
```

localIP

LAN客户端的内部IP地址。

publicIP

相应LAN客户端的外部IP地址。

在这个例子里，参数是：

```
-redirect_address 192.168.0.2 128.1.1.2 -redirect_address 192.168.0.3 128.1.1.3
```

象-redirect_port一样，这些参数也是放在/etc/rc.conf里的natd_flags=""选项上，或通过一个配置文件传送给它。使用地址重定向，就没有必要用端口重定向了，因为所有在某个IP地址上收到的数据都被重定向了。

在natd机子上的外部IP地址必须激活并且别名到(aliasd)外连接口。要这么做就看看rc.conf(5)。

27.9 并口电缆IP (PLIP)

PLIP 允许我们在两个并口间运行TCP/IP。在使用笔记本电脑，或没有网卡的计算机时，这会非常有用。这一节中，我们将讨论：

- 制作用于并口的(laplink) 线缆。
- 使用PLIP 连接两台计算机。

27.9.1 制作并口电缆。

您可以在许多计算机供应店里买到并口电缆。如果买不到，或者希望自行制作，则可以参阅下面的表格，它介绍了如何利用普通的打印机并口电缆来改制：

表27-1. 用于网络连接的并口电缆接线方式

A-name	A 端	B 端	描述	Post/Bit
DATA0 -ERROR	2 15	15 2	数据	0/0x01 1/0x08
DATA1 +SLCT	3 13	13 3	数据	0/0x02 1/0x10
DATA2 +PE	4 12	12 4	数据	0/0x04 1/0x20
DATA3 -ACK	5 10	10 5	脉冲(Strobe)	0/0x08 1/0x40
DATA4 BUSY	6 11	11 6	数据	0/0x10 1/0x80
GND	18-25	18-25	GND	-

27.9.2 设置PLIP

首先，您需要一根laplink 线。然后，确认两台计算机的内核都有对lpt(4) 驱动程序的支持：

```
# grep lp /var/run/dmesg.boot
lpt0: <Printer> on ppbus0
lpt0: Interrupt-driven port
```

并口必须是一个中断驱动的端口，在FreeBSD 4.X 里，您的内核配置文件应该有一行和下面的差不多：

```
device ppc0 at isa? irq 7
```

在FreeBSD 5.X 中，/boot/device.hints 文件中应包含下面的行：

```
hint.ppc.0.at="isa"
hint.ppc.0.irq="7"
```

然后检查内核配置文件中是否有一行device plip 或加载了plip.ko 内核模块。这两种情况下，在使用ifconfig(8) 命令时都会显示并口对应的网络接口，类似这样：

```
# ifconfig plip0
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
```

用laplink 线接通两台计算机的并口。

在两边以root 身份配置通讯参数。例如，如果你希望将host1 通过另一台机器host2 连接：

```

                host1 <-----> host2
IP Address      10.0.0.1      10.0.0.2

```

配置host1上的网络接口，照此做：

```
# ifconfig plip0 10.0.0.1 10.0.0.2
```

配置host2上的网络接口，照此做：

```
# ifconfig plip0 10.0.0.2 10.0.0.1
```

您现在应该有个工作的连接了。想要更详细的信息，请阅读lp(4)和lpt(4)手册页。

您还应该增加两个主机到/etc/hosts：

```

127.0.0.1          localhost.my.domain localhost
10.0.0.1           host1.my.domain host1
10.0.0.2           host2.my.domain

```

要确认连接是否工作，可以到每一台机子上，然后ping另外一台。例如，在host1上：

```

# ifconfig plip0
plip0: flags=8851<UP,POINTOPOINT,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 10.0.0.1 --> 10.0.0.2 netmask 0xff000000
# netstat -r
Routing tables

Internet:
Destination      Gateway          Flags      Refs      Use      Netif Expire
host2             host1            UH         0         0         plip0

# ping -c 4 host2
PING host2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=255 time=2.774 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=255 time=2.530 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=255 time=2.556 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=255 time=2.714 ms

--- host2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.530/2.643/2.774/0.103 ms

```

27.10 IPv6

原始作者：Aaron Kaplan. 重新组织和增加：Tom Rhodes. 中文翻译：张雪平. Extended by Brad Davis.

IPv6 (也被称作IPng “下一代IP”) 是中所周知的IP协议(也被叫做IPv4)的新版本。和其他现代的*BSD系统一样，FreeBSD包含了KAME的IPv6参考实现。因此，您的FreeBSD系统包含了尝试IPv6所需要的所有工具。这一节主要集中讨论如何配置和使用IPv6。

在1990年代早期，人们开始担心可用的IPv4地址空间在不断地缩小。随着Internet的爆炸式发展，主要的两个担心是：

- 用尽所有的地址。当然现在这个问题已经不再那样尖锐，因为RFC1918 私有地址空间(10.0.0.0/8、172.16.0.0/12，以及192.168.0.0/16)和网络地址转换(NAT) 技术已经被广泛采用。
- 路由表条目变得太大。这点今天仍然是焦点。

IPv6 解决这些和其它许多的问题:

- 128 位地址空间。换句话说，理论上有340,282,366,920,938,463,463,374,607,431,768,211,456 个地址可以使用。这意味着在我们的地球上每平方米大约有 $6.67 * 10^{27}$ 个IPv6 地址。
- 路由器仅在它们的路由表里存放网络地址集，这就减少路由表的平均空间到8192 个条目。

IPv6 还有其它许多有用的功能，如:

- 地址自动配置(RFC2462 (<http://www.ietf.org/rfc/rfc2462.txt>))
- Anycast (任意播) 地址(“一对多”)
- 强制的多播地址
- IPsec (IP 安全)
- 简单的头结构
- 移动的(Mobile) IP
- IPv6 到IPv4 的转换机制

要更多信息，请查看:

- IPv6 概观，在 playground.sun.com (<http://playground.sun.com/pub/ipng/html/ipng-main.html>)
- KAME.net (<http://www.kame.net>)
- 6bone.net (<http://www.6bone.net>)

27.10.1 关于IPv6 地址的背景知识

有几种不同类型的IPv6 地址: Unicast, Anycast 和Multicast。

Unicast 地址是为人们所熟知的地址。一个被发送到unicast 地址的包实际上会到达属于这个地址的接口。

Anycast 地址语义上与unicast 地址没有差别，只是它们强调一组接口。指定为anycast 地址的包会到达最近的(以路由为单位) 接口。Anycast 地址可能只被路由器使用。

Multicast 地址标识一组接口。指定为multicast 地址的包会到达属于multicast 组的所有的接口。

注意: IPv4 广播地址(通常为xxx.xxx.xxx.255) 由IPv6 的multicast 地址来表示。

表27-2. 保留的IPv6 地址

IPv6 地址	预定长度(bits)	描述	备注
::	128 bits	未指定	类似IPv4 中的0.0.0.0
:::1	128 bits	环回地址	类似IPv4 中的127.0.0.1

IPv6 地址	预定长度(bits)	描述	备注
::00:xx:xx:xx:xx	96 bits	嵌入的IPv4	低32 bits 是IPv4 地址。这也称作“IPv4 兼容IPv6 地址”
::ff:xx:xx:xx:xx	96 bits	IPv4 影射的IPv6 地址	低的32 bits 是IPv4 地址。用于那些不支持IPv6 的主机。
fe80:: - feb::	10 bits	链路环回	类似IPv4 的环回地址。
fec0:: - fef::	10 bits	站点环回	
ff::	8 bits	多播	
001 (base 2)	3 bits	全球多播	所有的全球多播地址都指定到这个地址池中。前三个二进制位是“001”。

27.10.2 IPv6 地址的读法

规范形式被描述为: x:x:x:x:x:x:x, 每一个“x”就是一个16位的16进制值。当然, 每个十六进制块以三个“0”开始头的也可以省略。如FEBC:A574:382B:23C1:AA49:4592:4EFE:9982

通常一个地址会有很长的子串全部为零, 因此每个地址的这种子串常被简写为“::”。例如: fe80::1 对应的规范形式是fe80:0000:0000:0000:0000:0000:0000:0001。

第三种形式是以众所周知的用点“.”作为分隔符的十进制IPv4形式, 写出最后32 Bit 的部分。例如2002::10.0.0.1对应的十进制正规表达方式是2002:0000:0000:0000:0000:0000:0a00:0001 它也相当于写成2002::a00:1。

到现在, 读者应该能理解下面的内容了:

ifconfig

```
rl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    inet 10.0.0.10 netmask 0xffffffff00 broadcast 10.0.0.255
    inet6 fe80::200:21ff:fe03:8e1%rl0 prefixlen 64 scopeid 0x1
    ether 00:00:21:03:08:e1
    media: Ethernet autoselect (100baseTX )
    status: active
```

fe80::200:21ff:fe03:8e1%rl0 是一个自动配置的链路环回地址。它作为自动配置的一部分由MAC生成。

关于IPv6 地址的结构的信息, 请参看RFC3513 (<http://www.ietf.org/rfc/rfc3513.txt>)。

27.10.3 进行连接

目前, 有四种方式可以连接到其它IPv6 主机和网络:

- 加入试验性的6bone(骨干)
- 从您的上一级提供商那里获得IPv6 网络。与您的互联网提供商讨论以求指导。

- 使用6-to-4 通道(RFC3068 (<http://www.ietf.org/rfc/rfc3068.txt>))
- 如果您是括号连接(dial-up connection), 请使用net/freenet6 port。

这里我们就讨论如何连接到6bone, 因为它目前看来是最流行的一种方式。

首先看一下6bone (<http://www.6bone.net/>) 网站, 并找出离您最近的6bone 连接。给某位值得信赖的人写信过去, 如果运气好, 您就会得到关于如何设置您的连接的指导。通常这包括了设置GRE (gif) 通道。

这里有一个典型的关于设置gif(4) 通道的例子。

```
# ifconfig gif0 create
# ifconfig gif0
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
# ifconfig gif0 tunnel MY_IPv4_ADDR MY_IPv4_REMOTE_TUNNEL_ENDPOINT_ADDR
# ifconfig gif0 inet6 alias MY_ASSIGNED_IPv6_TUNNEL_ENDPOINT_ADDR MY_IPv6_REMOTE_TUNNEL_ENDPOINT_ADDR
```

把大写字母换成您从上一级6bone 节点收到的信息。

这样就建立了通道。通过ping6(8) ff02::1%gif0, 检查通道是否工作。您应该会收到两个ping 回应。

注意: 或许您会对地址ff02::1%gif0 感兴趣, 它是一个multicast 地址。%gif0 表明在网络接口gif0 上的multicast 地址已经用上了。因为我们ping 一个multicast 地址的时候, 通道的另一端也应该会回应。

到现在, 设置一个到6bone 上级连接的路由应该是相当简单了。

```
# route add -inet6 default -interface gif0
# ping6 -n MY_UPLINK

# traceroute6 www.jp.FreeBSD.org
(3ffe:505:2008:1:2a0:24ff:fe57:e561) from 3ffe:8060:100::40:2, 30 hops max, 12 byte packets
 1  atnet-meta6  14.147 ms  15.499 ms  24.319 ms
 2  6bone-gw2-ATNET-NT.ipv6.tilab.com  103.408 ms  95.072 ms *
 3  3ffe:1831:0:ffff::4  138.645 ms  134.437 ms  144.257 ms
 4  3ffe:1810:0:6:290:27ff:fe79:7677  282.975 ms  278.666 ms  292.811 ms
 5  3ffe:1800:0:ff00::4  400.131 ms  396.324 ms  394.769 ms
 6  3ffe:1800:0:3:290:27ff:fe14:cdee  394.712 ms  397.19 ms  394.102 ms
```

这个输出可能随机器而不同。到现在, 您应该可以到达IPv6 站点www.kame.net (<http://www.kame.net>), 并看到那只正跳舞的乌龟——如果您有一个支持IPv6 的浏览器, 如www/mozilla、**Konqueror** (x11/kdebase3的一部分) 或www/epiphany。

27.10.4 IPv6 世界里的DNS

对于IPv6 有两种类型的DNS 记录: IETF 已经宣布A6 是过时标准; 现行的标准是AAAA 记录。

使用AAAA记录是很简单的。通过增加下面内容, 给您的主机分配您刚才接收到的新的IPv6 地址:

```
MYHOSTNAME          AAAA      MYIPv6ADDR
```

到您的主域DNS 文件里, 就可以完成。要是您自己没有DNS 域服务, 您可以询问您的DNS 提供商。目前的bind 版本(version 8.3 与9) 和dns/djbdns(含IPv6补丁) 支持AAAA 记录。

27.10.5 在/etc/rc.conf 中进行所需的修改

27.10.5.1 IPv6 客户机设置

这些设置将帮助您把一台您LAN 上的机器配置为一台客户机，而不是路由器。要让rtsol(8) 在启动时自动配置您的网卡，只需添加：

```
ipv6_enable="YES"
```

要自动地静态指定IP 地址，例如 2001:471:1f11:251:290:27ff:fee0:2093，到fxp0 上，则写上：

```
ipv6_ifconfig_fxp0="2001:471:1f11:251:290:27ff:fee0:2093"
```

要指定2001:471:1f11:251::1 作为默认路由，需要在/etc/rc.conf 中加入：

```
ipv6_defaultrouter="2001:471:1f11:251::1"
```

27.10.5.2 IPv6 路由器/网关配置

这将帮助您从隧道提供商，例如6bone (<http://www.6bone.net/>) 那里取得必要的资料，并将这些资料转化为在重启时能够保持住的设置。要在启动时恢复您的隧道，需要在/etc/rc.conf 中增加：

列出要配置的通用隧道接口，例如gif0：

```
gif_interfaces="gif0"
```

配置该接口使用本地端地址MY_IPv4_ADDR 和远程端地址REMOTE_IPv4_ADDR：

```
gifconfig_gif0="MY_IPv4_ADDR REMOTE_IPv4_ADDR"
```

应用分配给您用于IPv6 隧道远端的IPv6 地址，需要增加：

```
ipv6_ifconfig_gif0="MY_ASSIGNED_IPv6_TUNNEL_ENDPOINT_ADDR"
```

此后设置IPv6 的默认路由。这是IPv6 隧道的另一端：

```
ipv6_defaultrouter="MY_IPv6_REMOTE_TUNNEL_ENDPOINT_ADDR"
```

27.10.5.3 IPv6 隧道配置

如果服务器将您的网络通过IPv6 路由到世界的其他角落，您需要在/etc/rc.conf 中添加下面的配置：

```
ipv6_gateway_enable="YES"
```

27.10.6 路由宣告和主机自动配置

这节将帮助您配置rtadvd(8) 来宣示默认的IPv6 路由。

要启用rtadvd(8) 您需要在/etc/rc.conf 中添加：

```
rtadvd_enable="YES"
```

指定由哪个网络接口来完成IPv6 路由请求非常重要。举例来说，让rtadvd(8) 使用fxp0:

```
rtadvd_interfaces="fxp0"
```

接下来我们需要创建配置文件，/etc/rtadvd.conf。示例如下:

```
fxp0:\n:addrs#1:addr="2001:471:1f11:246::":prefixlen#64:tc=ether:
```

将fxp0 改为您打算使用的接口名。

接下来，将2001:471:1f11:246:: 改为分配给您的地址前缀。

如果您拥有专用的/64 子网，则不需要修改其他设置。反之，您需要把prefixlen# 改为正确的值。

27.11 异步传输模式(ATM)

贡献者: Harti Brandt. 中文翻译: 张雪平.

27.11.1 配置classical IP over ATM (PVCs)

Classical IP over ATM (CLIP) 是一种最简单的使用带IP 的ATM 的方法。这种方法可以用在交换式连接(SVC) 和永久连接(PVC) 上。这部分描述的就是配置基于PVC 的网络。

27.11.1.1 完全互连的配置

第一种使用PVC来设置CLIP 的方式就是通过专用的PVC 让网络里的每一台机子都互连在一起。尽管这样配置起来很简单，但对于数量更多一点的机子来说就有些不切实际了。例如我们有四台机子在网络里，每一台都使用一张ATM 适配器卡连接到ATM 网络。第一步就是规划IP 地址和机子间的ATM 连接。我们使用下面的:

主机	IP 地址
hostA	192.168.173.1
hostB	192.168.173.2
hostC	192.168.173.3
hostD	192.168.173.4

为了建造完全交错的网络，我们需要在第一对机子间有一个ATM 连接:

机器	VPI.VCI 对
hostA - hostB	0.100
hostA - hostC	0.101
hostA - hostD	0.102
hostB - hostC	0.103
hostB - hostD	0.104

机器	VPI.VCI 对
hostC - hostD	0.105

在每一个连接端VPI和VCI的值都可能会不同，只是为了简单起见，我们假定它们是一样的。下一步我们需要配置每一个主机上的ATM接口：

```
hostA# ifconfig hatm0 192.168.173.1 up
hostB# ifconfig hatm0 192.168.173.2 up
hostC# ifconfig hatm0 192.168.173.3 up
hostD# ifconfig hatm0 192.168.173.4 up
```

假定所有主机上的ATM接口都是hatm0。现在PVC需要配置到hostA上(我们假定它们都已经配置在了ATM交换机上，至于怎么做的，您就需要参考一下该交换机的手册了)。

```
hostA# atmconfig natm add 192.168.173.2 hatm0 0 100 llc/snap ubr
hostA# atmconfig natm add 192.168.173.3 hatm0 0 101 llc/snap ubr
hostA# atmconfig natm add 192.168.173.4 hatm0 0 102 llc/snap ubr

hostB# atmconfig natm add 192.168.173.1 hatm0 0 100 llc/snap ubr
hostB# atmconfig natm add 192.168.173.3 hatm0 0 103 llc/snap ubr
hostB# atmconfig natm add 192.168.173.4 hatm0 0 104 llc/snap ubr

hostC# atmconfig natm add 192.168.173.1 hatm0 0 101 llc/snap ubr
hostC# atmconfig natm add 192.168.173.2 hatm0 0 103 llc/snap ubr
hostC# atmconfig natm add 192.168.173.4 hatm0 0 105 llc/snap ubr

hostD# atmconfig natm add 192.168.173.1 hatm0 0 102 llc/snap ubr
hostD# atmconfig natm add 192.168.173.2 hatm0 0 104 llc/snap ubr
hostD# atmconfig natm add 192.168.173.3 hatm0 0 105 llc/snap ubr
```

当然，除UBR外其它的通信协定也可让ATM适配器支持这些。此种情况下，通信协定的名字要跟人通信参数后边。工具atmconfig(8)的帮助可以这样得到：

```
# atmconfig help natm add
```

或者在atmconfig(8)手册页里得到。

相同的配置也可以通过/etc/rc.conf来完成。对于hostA，看起来就象这样：

```
network_interfaces="lo0 hatm0"
ifconfig_hat0="inet 192.168.173.1 up"
natm_static_routes="hostB hostC hostD"
route_hostB="192.168.173.2 hatm0 0 100 llc/snap ubr"
route_hostC="192.168.173.3 hatm0 0 101 llc/snap ubr"
route_hostD="192.168.173.4 hatm0 0 102 llc/snap ubr"
```

所有CLIP路由的当前状态可以使用如下命令获得：

```
hostA# atmconfig natm show
```

V. 附录

附录A.

获取FreeBSD

A.1 CDROM 和DVD 发行商

A.1.1 零售盒装产品

可以从下面几个零售商那里买到FreeBSD 的盒装产品(FreeBSD CD, 附加软件, 印刷文档):

- CompUSA
WWW: <http://www.compusa.com/>
- Frys Electronics
WWW: <http://www.frys.com/>

A.1.2 CD 和DVD 光盘

FreeBSD CD 和DVD 光盘可以从许多在线零售商那里买到:

- BSD Mall by Daemon News
PO Box 161
Nauvoo, IL 62354
USA
Phone: +1 866 273-6255
Fax: +1 217 453-9956
Email: <sales@bsdmall.com>
WWW: <http://www.bsdmall.com/freebsd1.html>
- BSD-Systems
Email: <info@bsd-systems.co.uk>
WWW: <http://www.bsd-systems.co.uk>
- fastdiscs.com
6 Eltham Close
Leeds, LS6 2TY
United Kingdom
Phone: +44 870 1995 171
Email: <sales@fastdiscs.com>
WWW: <http://fastdiscs.com/freebsd/>
- FreeBSD Mall, Inc.
3623 Sanford Street
Concord, CA 94520-1405
USA
Phone: +1 925 674-0783

Fax: +1 925 674-0821

Email: <info@freebsdmail.com>

WWW: <http://www.freebsdmail.com/>

- Hinner EDV
St. Augustinus-Str. 10
D-81825 München
Germany
Phone: (089) 428 419
WWW: <http://www.hinner.de/linux/freebsd.html>
- Ikarios
22-24 rue Voltaire
92000 Nanterre
France
WWW: <http://ikarios.com/form/#freebsd>
- JMC Software
Ireland
Phone: 353 1 6291282
WWW: <http://www.thelinuxmall.com>
- Linux CD Mall
Private Bag MBE N348
Auckland 1030
New Zealand
Phone: +64 21 866529
WWW: <http://www.linuxcdmall.co.nz/>
- The Linux Emporium
Hilliard House, Lester Way
Wallingford
OX10 9TA
United Kingdom
Phone: +44 1491 837010
Fax: +44 1491 837016
WWW: <http://www.linuxemporium.co.uk/products/freebsd/>
- Linux+ DVD Magazine
Lewartowskiego 6
Warsaw
00-190
Poland
Phone: +48 22 860 18 18
Email: <editors@lpmagazine.org>
WWW: <http://www.lpmagazine.org/>
- Linux System Labs Australia
21 Ray Drive
Balwyn North
VIC - 3104
Australia

Phone: +61 3 9857 5918
Fax: +61 3 9857 8974
WWW: <http://www.lsl.com.au>

- LinuxCenter.Ru
Galernaya Street, 55
Saint-Petersburg
190000
Russia
Phone: +7-812-3125208
Email: <info@linuxcenter.ru>
WWW: <http://linuxcenter.ru/freebsd>

A.1.3 发行人

如果您是销售商并且想销售FreeBSD CDROM 产品, 请和发行人联系:

- Cylogistics
809B Cuesta Dr., #2149
Mountain View, CA 94040
USA
Phone: +1 650 694-4949
Fax: +1 650 694-4953
Email: <sales@cylogistics.com>
WWW: <http://www.cylogistics.com/>
- Ingram Micro
1600 E. St. Andrew Place
Santa Ana, CA 92705-4926
USA
Phone: 1 (800) 456-8000
WWW: <http://www.ingrammicro.com/>
- Kudzu, LLC
7375 Washington Ave. S.
Edina, MN 55439
USA
Phone: +1 952 947-0822
Fax: +1 952 947-0876
Email: <sales@kudzuenterprises.com>
- LinuxCenter.Ru
Galernaya Street, 55
Saint-Petersburg
190000
Russia
Phone: +7-812-3125208
Email: <info@linuxcenter.ru>
WWW: <http://linuxcenter.ru/freebsd>

- Navarre Corp
7400 49th Ave South
New Hope, MN 55428
USA
Phone: +1 763 535-8333
Fax: +1 763 535-0341
WWW: <http://www.navarre.com/>

A.2 FTP 站点

官方的FreeBSD 源代码可以从遍布全球的镜像站点通过匿名FTP 下载。站点<ftp://ftp.FreeBSD.org/pub/FreeBSD/> 有着良好的网络连接并且允许大量的并发连接，但是您或许更想找一个“更近的” 镜像站点(特别是当您想进行某种形式的镜像的时候)。

FreeBSD 镜像站点数据库 (<http://mirrorlist.FreeBSD.org/>)要比使用手册中的镜像列表更加精确，因为它从DNS 中获取信息而不依赖于静态的主机列表。

FreeBSD 可以从下面这些镜像站点通过匿名FTP 下载。如果您选择了通过匿名FTP 获取FreeBSD，请尽量使用离您比较近的站点。被列为“主镜像站点” 的镜像站点一般都有完整的FreeBSD 文件(针对每种体系结构的所有当前可用的版本)，您或许从您所在的国家或地区的站点下载会得到更快的下载速度。每个站点提供了最流行的体系结构的最近的版本而有可能不提供完整的FreeBSD 存档。所有的站点都提供匿名FTP 访问而有些站点也提供其他的访问方式。对每个站点可用的访问方式在其主机名后有所说明。

中央服务器, 主要镜像站点, Israel, 阿根廷, 爱尔兰, 爱沙尼亚, 奥地利, 澳大利亚, 巴西, 保加利亚, 冰岛, 波兰, 丹麦, 德国, 俄罗斯, 法国, 芬兰, 韩国, 荷兰, 加拿大, 捷克共和国, 克罗地亚, 拉脱维亚, 立陶宛, 罗马尼亚, 美国, 南非, 挪威, 葡萄牙, 日本, 瑞典, 瑞士, 沙特阿拉伯, 斯洛伐克共和国, 斯洛文尼亚, 土耳其, 乌克兰, 西班牙, 希腊, 新加坡, 新西兰, 匈牙利, 意大利, 印度尼西亚, 英国, 中国大陆, 中国台湾, 中国香港。

(2006/03/25 21:54:18 UTC 更新)

中央服务器

- <ftp://ftp.FreeBSD.org/pub/FreeBSD/> (ftp)

主要镜像站点

如有问题，请和负责相关子域服务器的管理员<mirror-admin@FreeBSD.org>联系。

- <ftp://ftp1.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp4.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp6.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp7.FreeBSD.org/pub/FreeBSD/> (ftp)

- <ftp://ftp8.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp9.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp10.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp11.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp12.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp13.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp14.FreeBSD.org/pub/FreeBSD/> (ftp)

Israel

如有问题，请和负责相关子域服务器的管理员<hostmaster@il.FreeBSD.org>联系。

- <ftp://ftp.il.FreeBSD.org/pub/FreeBSD/> (ftp / ftpv6)

阿根廷

如有问题，请和负责相关子域服务器的管理员<hostmaster@ar.FreeBSD.org>联系。

- <ftp://ftp.ar.FreeBSD.org/pub/FreeBSD/> (ftp)

爱尔兰

如有问题，请和负责相关子域服务器的管理员<hostmaster@ie.FreeBSD.org>联系。

- <ftp://ftp.ie.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.ie.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp2.ie.FreeBSD.org/pub/FreeBSD/>) / rsync)
- <ftp://ftp3.ie.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp3.ie.FreeBSD.org/pub/FreeBSD/>) / rsync)

爱沙尼亚

如有问题，请和负责相关子域服务器的管理员<hostmaster@ee.FreeBSD.org>联系。

- <ftp://ftp.ee.FreeBSD.org/pub/FreeBSD/> (ftp)

奥地利

如有问题，请和负责相关子域服务器的管理员<hostmaster@at.FreeBSD.org>联系。

- <ftp://ftp.at.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp.at.FreeBSD.org/pub/FreeBSD/>))
- <ftp://ftp2.at.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp2.at.freebsd.org/pub/FreeBSD/>) / rsync)

澳大利亚

如有问题，请与负责相关子域服务器的管理员<hostmaster@au.FreeBSD.org>联系。

- <ftp://ftp.au.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.au.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.au.FreeBSD.org/pub/FreeBSD/> (ftp)

巴西

如有问题，请与负责相关子域服务器的管理员<hostmaster@br.FreeBSD.org>联系。

- <ftp://ftp.br.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp.br.FreeBSD.org/>))
- <ftp://ftp2.br.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.br.FreeBSD.org/pub/FreeBSD/> (ftp / rsync)
- <ftp://ftp4.br.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.br.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp6.br.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp7.br.FreeBSD.org/pub/FreeBSD/> (ftp)

保加利亚

如有问题，请与负责相关子域服务器的管理员<hostmaster@bg.FreeBSD.org>联系。

- <ftp://ftp.bg.FreeBSD.org/pub/FreeBSD/> (ftp / rsync)
- <ftp://ftp2.bg.FreeBSD.org/pub/FreeBSD/> (ftp / rsync)

冰岛

如有问题，请与负责相关子域服务器的管理员<hostmaster@is.FreeBSD.org>联系。

- <ftp://ftp.is.FreeBSD.org/pub/FreeBSD/> (ftp / rsync)

波兰

如有问题，请与负责相关子域服务器的管理员<hostmaster@pl.FreeBSD.org>联系。

- <ftp://ftp.pl.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.pl.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.pl.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.pl.FreeBSD.org/pub/FreeBSD/> (ftp)

丹麦

如有问题，请与负责相关子域服务器的管理员<hostmaster@dk.FreeBSD.org>联系。

- <ftp://ftp.dk.FreeBSD.org/pub/FreeBSD/> (ftp / ftpv6 / http (<http://ftp.dk.FreeBSD.org/pub/FreeBSD/>))
- <ftp://ftp2.dk.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.dk.FreeBSD.org/pub/FreeBSD/> (ftp)

德国

如有问题，请与负责相关子域服务器的管理员<de-bsd-hubs@de.FreeBSD.org>联系。

- <ftp://ftp.de.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.de.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp2.de.FreeBSD.org/pub/FreeBSD/>) / rsync)
- <ftp://ftp3.de.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp4.de.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp4.de.FreeBSD.org/pub/FreeBSD/>) / rsync)
- <ftp://ftp5.de.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp6.de.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp7.de.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp7.de.FreeBSD.org/pub/FreeBSD/>))
- <ftp://ftp8.de.FreeBSD.org/pub/FreeBSD/> (ftp)

俄罗斯

如有问题，请与负责相关子域服务器的管理员<hostmaster@ru.FreeBSD.org>联系。

- <ftp://ftp.ru.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.ru.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp2.ru.FreeBSD.org/pub/FreeBSD/>) / rsync)
- <ftp://ftp3.ru.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp4.ru.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.ru.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp5.ru.FreeBSD.org/pub/FreeBSD/>) / rsync)

法国

如有问题，请与负责相关子域服务器的管理员<hostmaster@fr.FreeBSD.org>联系。

- <ftp://ftp.fr.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.fr.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.fr.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.fr.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp6.fr.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp7.fr.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp8.fr.FreeBSD.org/pub/FreeBSD/> (ftp)

芬兰

如有问题，请与负责相关子域服务器的管理员<hostmaster@fi.FreeBSD.org>联系。

- <ftp://ftp.fi.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.fi.FreeBSD.org/pub/FreeBSD/> (ftp)

韩国

如有问题，请与负责相关子域服务器的管理员<hostmaster@kr.FreeBSD.org>联系。

- <ftp://ftp.kr.FreeBSD.org/pub/FreeBSD/> (ftp / rsync)
- <ftp://ftp2.kr.FreeBSD.org/pub/FreeBSD/> (ftp)

荷兰

如有问题，请与负责相关子域服务器的管理员<hostmaster@nl.FreeBSD.org>联系。

- <ftp://ftp.nl.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp.nl.FreeBSD.org/os/FreeBSD/>) / rsync)
- <ftp://ftp2.nl.FreeBSD.org/pub/FreeBSD/> (ftp)

加拿大

如有问题，请与负责相关子域服务器的管理员<hostmaster@ca.FreeBSD.org>联系。

- <ftp://ftp.ca.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.ca.FreeBSD.org/> (ftp)
- <ftp://ftp3.ca.FreeBSD.org/pub/FreeBSD/> (ftp)

捷克共和国

如有问题，请与负责相关子域服务器的管理员<hostmaster@cz.FreeBSD.org>联系。

- <ftp://ftp.cz.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp.cz.FreeBSD.org/pub/FreeBSD/>) / rsync)

克罗地亚

如有问题，请与负责相关子域服务器的管理员<hostmaster@hr.FreeBSD.org>联系。

- <ftp://ftp.hr.FreeBSD.org/pub/FreeBSD/> (ftp)

拉脱维亚

如有问题，请与负责相关子域服务器的管理员<hostmaster@lv.FreeBSD.org>联系。

- <ftp://ftp.lv.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp.lv.FreeBSD.org/pub/FreeBSD/>))
- <ftp://ftp2.lv.FreeBSD.org/pub/FreeBSD/> (ftp)

立陶宛

如有问题，请与负责相关子域服务器的管理员<hostmaster@lt.FreeBSD.org>联系。

- <ftp://ftp.lt.FreeBSD.org/pub/FreeBSD/> (ftp)

罗马尼亚

如有问题，请与负责相关子域服务器的管理员<hostmaster@ro.FreeBSD.org>联系。

- <ftp://ftp.ro.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp1.ro.FreeBSD.org/pub/FreeBSD/> (ftp / ftpv6)

美国

如有问题，请与负责相关子域服务器的管理员<hostmaster@us.FreeBSD.org>联系。

- <ftp://ftp1.us.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.us.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.us.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp4.us.FreeBSD.org/pub/FreeBSD/> (ftp / ftpv6)
- <ftp://ftp5.us.FreeBSD.org/pub/FreeBSD/> (ftp / rsync)
- <ftp://ftp6.us.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp6.us.FreeBSD.org/pub/FreeBSD/>))
- <ftp://ftp7.us.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp7.us.FreeBSD.org/pub/FreeBSD/>) / rsync)
- <ftp://ftp8.us.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp9.us.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp9.us.FreeBSD.org/pub/os/FreeBSD/>))
- <ftp://ftp10.us.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp11.us.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp12.us.FreeBSD.org/pub/FreeBSD/> (ftp / rsync)
- <ftp://ftp13.us.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp13.us.FreeBSD.org/pub/FreeBSD/>) / rsync)
- <ftp://ftp14.us.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp15.us.FreeBSD.org/pub/FreeBSD/> (ftp)

南非

如有问题，请与负责相关子域服务器的管理员<hostmaster@za.FreeBSD.org>联系。

- <ftp://ftp.za.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.za.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.za.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp4.za.FreeBSD.org/pub/FreeBSD/> (ftp)

挪威

如有问题，请与负责相关子域服务器的管理员<hostmaster@no.FreeBSD.org>联系。

- <ftp://ftp.no.FreeBSD.org/pub/FreeBSD/> (ftp / rsync)
- <ftp://ftp3.no.FreeBSD.org/pub/FreeBSD/> (ftp)

葡萄牙

如有问题，请与负责相关子域服务器的管理员<hostmaster@pt.FreeBSD.org>联系。

- <ftp://ftp.pt.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.pt.FreeBSD.org/pub/freebsd/> (ftp)
- <ftp://ftp4.pt.FreeBSD.org/pub/ISO/FreeBSD/> (ftp)

日本

如有问题，请与负责相关子域服务器的管理员<hostmaster@jp.FreeBSD.org>联系。

- <ftp://ftp.jp.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.jp.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.jp.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp4.jp.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.jp.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp6.jp.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp7.jp.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp8.jp.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp9.jp.FreeBSD.org/pub/FreeBSD/> (ftp)

瑞典

如有问题，请与负责相关子域服务器的管理员<hostmaster@se.FreeBSD.org>联系。

- <ftp://ftp.se.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.se.FreeBSD.org/pub/FreeBSD/> (ftp)

- <ftp://ftp3.se.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.se.FreeBSD.org/pub/FreeBSD/> (ftp / [http \(http://ftp5.se.FreeBSD.org/\) / rsync](http://ftp5.se.FreeBSD.org/))

瑞士

如有问题，请和负责相关子域服务器的管理员<hostmaster@ch.FreeBSD.org>联系。

- <ftp://ftp.ch.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.ch.FreeBSD.org/pub/FreeBSD/> (ftp)

沙特阿拉伯

如有问题，请和负责相关子域服务器的管理员<ftpadmin@isu.net.sa>联系。

- <ftp://ftp.isu.net.sa/pub/mirrors/ftp.freebsd.org/> (ftp)

斯洛伐克共和国

如有问题，请和负责相关子域服务器的管理员<hostmaster@sk.FreeBSD.org>联系。

- <ftp://ftp.sk.FreeBSD.org/pub/FreeBSD/> (ftp / [ftp6 \(ftp://ftp.sk.FreeBSD.org/pub/FreeBSD/\) / http \(http://ftp.sk.FreeBSD.org/pub/FreeBSD/\) / http6 \(http://ftp.sk.FreeBSD.org/pub/FreeBSD/\)\)](ftp://ftp.sk.FreeBSD.org/pub/FreeBSD/))

斯洛文尼亚

如有问题，请和负责相关子域服务器的管理员<hostmaster@si.FreeBSD.org>联系。

- <ftp://ftp.si.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.si.FreeBSD.org/pub/FreeBSD/> (ftp)

土耳其

- <ftp://ftp.tr.FreeBSD.org/pub/FreeBSD/> (ftp)

乌克兰

- <ftp://ftp.ua.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.ua.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.ua.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.ua.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp6.ua.FreeBSD.org/pub/FreeBSD/> (ftp)

- <ftp://ftp7.ua.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp8.ua.FreeBSD.org/pub/FreeBSD/> (ftp)

西班牙

如有问题，请和负责相关子域服务器的管理员<hostmaster@es.FreeBSD.org>联系。

- <ftp://ftp.es.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.es.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp3.es.FreeBSD.org/pub/FreeBSD/> (ftp)

希腊

如有问题，请和负责相关子域服务器的管理员<hostmaster@gr.FreeBSD.org>联系。

- <ftp://ftp.gr.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.gr.FreeBSD.org/pub/FreeBSD/> (ftp)

新加坡

如有问题，请和负责相关子域服务器的管理员<hostmaster@sg.FreeBSD.org>联系。

- <ftp://ftp.sg.FreeBSD.org/pub/FreeBSD/> (ftp / [http \(http://ftp.sg.FreeBSD.org/pub/FreeBSD/\) / rsync](http://ftp.sg.FreeBSD.org/pub/FreeBSD/))

新西兰

- <ftp://ftp.nz.FreeBSD.org/pub/FreeBSD/> (ftp)

匈牙利

如有问题，请和负责相关子域服务器的管理员<mohacsi@ik.bme.hu>联系。

- <ftp://ftp.hu.FreeBSD.org/pub/FreeBSD/> (ftp / [http \(http://ftp.hu.FreeBSD.org/\) / rsync](http://ftp.hu.FreeBSD.org/))
- <ftp://ftp2.hu.FreeBSD.org/pub/FreeBSD/> (ftp)

意大利

如有问题，请和负责相关子域服务器的管理员<hostmaster@it.FreeBSD.org>联系。

- <ftp://ftp.it.FreeBSD.org/pub/FreeBSD/> (ftp)

印度尼西亚

如有问题，请与负责相关子域服务器的管理员<hostmaster@id.FreeBSD.org>联系。

- <ftp://ftp.id.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp.id.FreeBSD.org/>) / rsync)

英国

如有问题，请与负责相关子域服务器的管理员<hostmaster@uk.FreeBSD.org>联系。

- <ftp://ftp.uk.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.uk.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp2.uk.FreeBSD.org/>) / rsync)
- <ftp://ftp3.uk.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp4.uk.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.uk.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp6.uk.FreeBSD.org/pub/FreeBSD/> (ftp)

中国大陆

如有问题，请与负责相关子域服务器的管理员<hostmaster@cn.FreeBSD.org>联系。

- <ftp://ftp.cn.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.cn.FreeBSD.org/pub/FreeBSD/> (ftp)

中国台湾

如有问题，请与负责相关子域服务器的管理员<hostmaster@tw.FreeBSD.org>联系。

- <ftp://ftp.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp2.tw.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp2.tw.FreeBSD.org/pub/FreeBSD/>) / rsync)
- <ftp://ftp3.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp4.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp5.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp6.tw.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp6.tw.FreeBSD.org/>))
- <ftp://ftp7.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp8.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp9.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp10.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp11.tw.FreeBSD.org/pub/FreeBSD/> (ftp / http (<http://ftp11.tw.FreeBSD.org/FreeBSD/>))
- <ftp://ftp12.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp13.tw.FreeBSD.org/pub/FreeBSD/> (ftp)
- <ftp://ftp14.tw.FreeBSD.org/pub/FreeBSD/> (ftp)

- <ftp://ftp15.tw.FreeBSD.org/pub/FreeBSD/> (ftp)

中国香港

- <ftp://ftp.hk.FreeBSD.org/pub/FreeBSD/> (ftp)

A.3 匿名CVS

A.3.1 概述

匿名CVS(或人们常说的**anoncvs**)是由和FreeBSD 附带的CVS 实用工具提供的用于和远程的CVS 代码库同步的一种特性。尤其是，它允许FreeBSD 用户不需要特殊的权限对任何一台FreeBSD 项目的官方**anoncvs** 服务器执行只读的CVS 操作。要使用它，简单的设置CVSR00T 环境变量指向适当的**anoncvs** 服务器，输入**cvs login** 命令并提供广为人知的密码“**anoncvs**”，然后使用**cvs(1)** 命令像访问任何本地仓库一样来访问它。

注意: **cvs login** 命令把用来登录CVS 服务器的密码储存在您的HOME 目录中一个叫**.cvspass** 的文件里。如果这个文件不存在，第一次使用**cvs login** 的时候可能会出错。请创建一个空的**.cvspass** 文件，然后试试重新登录。

也可以这么说CVSup 和**anoncvs** 服务本质上提供了同样的功能，但是有各种各样不同的场合可以影响用户对同步方式的选择。简单来说，**CVSup** 在网络资源利用方面更加有效，而且是到目前为止在两者之中技术上更成熟的除了成本方面。要使用**CVSup**，在下载任何东西之前必须首先安装配置特定的客户端，而且只能用于下载相当大块的**CVSup** 称作**collections**。

相比之下，**anoncvs** 可以通过CVS 模块名来从单个文件里检出任何东西并赋给特定的程序(比如**ls** 或者**grep**)。当然，**anoncvs** 也只适用于对CVS 仓库的只读操作，所以如果您是想用和FreeBSD 项目共享的仓库提供本地开发的话，**CVSup** 几乎是您唯一的选择。

A.3.2 使用匿名CVS

配置**cvs(1)** 使用匿名CVS 仓库可以简单的设定CVSR00T 环境变量指向FreeBSD 项目的**anoncvs** 服务器之一。到此书写作为止，下面的服务器都是可用的：

- 奥地利: `:pserver:anoncvs@anoncvs.at.FreeBSD.org:/home/ncvs` (使用**cvs login** 然后在提示输入口令时输入任意口令。)
- 法国: `:pserver:anoncvs@anoncvs.fr.FreeBSD.org:/home/ncvs` (**pserver** (口令是“**anoncvs**”), **ssh** (没有口令))
- 德国: `:pserver:anoncvs@anoncvs.de.FreeBSD.org:/home/ncvs` (Use **cvs login** and enter the password “**anoncvs**” when prompted.)
- 德国: `:pserver:anoncvs@anoncvs2.de.FreeBSD.org:/home/ncvs` (**rsh**, **pserver**, **ssh**, **ssh/2022**)

- 日本: `pserver:anoncvs@anoncvs.jp.FreeBSD.org:/home/ncvs` (Use `cvs login` and enter the password “anoncvs” when prompted.)
- 美国: `freebsdanoncvs@anoncvs.FreeBSD.org:/home/ncvs` (仅ssh - 无口令)
 SSH HostKey: 1024 a1:e7:46:de:fb:56:ef:05:bc:73:aa:91:09:da:f7:f4 root@sanmateo.ecn.purdue.edu
 SSH2 HostKey: 1024 52:02:38:1a:2f:a8:71:d3:f5:83:93:8d:aa:00:6f:65 ssh_host_dsa_key.pub
- USA: `anoncvs@anoncvs1.FreeBSD.org:/home/ncvs` (仅ssh - 无口令)
 SSH HostKey: 1024 8b:c4:6f:9a:7e:65:8a:eb:50:50:29:7c:a1:47:03:bc root@ender.liquidneon.com
 SSH2 HostKey: 2048 4d:59:19:7b:ea:9b:76:0b:ca:ee:da:26:e2:3a:83:b8 ssh_host_dsa_key.pub

因为CVS 实际上允许“检出”曾经存在的(或者, 某种情况下将会存在) FreeBSD 源代码的任意版本, 您需要熟悉`cvs(1)`的版本(`-r`)参数, 以及在FreeBSD 代码库中可用的值。

有两种标签, 修订标签和分支标签。修订标签特指一个特定的修订版本。含义始终是不变的。分支标签, 另一方面, 指代给定时间给定开发分支的最新修订, 因为分支标签不涉及特定的修订版本, 它明天所代表的含义就可能和今天的不同。

第A.7节 包括了用户可能感兴趣的修订标签。另外, 这里面没有一个可以用于Ports Collection, 因为它没有多个修订版本。

当您指定一个分支标签, 您通常会得到那个开发分支的文件最新版本。如果您希望得到一些旧的版本, 您可以用`-D date`标记制定一个日期。察看`cvs(1)`手册页了解更多细节。

A.3.3 示例

在这之前强烈建议您通读`cvs(1)`的手册页, 这里有一些简单的例子来展示如何使用匿名CVS:

例A-1. 从-CURRENT 检出些东西(`ls(1)`):

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.jp.FreeBSD.org:/home/ncvs
% cvs login
在提示符处, 输入密码 “anoncvs” .
% cvs co ls
```

例A-2. 通过SSH 检出整个src/ 代码树:

```
% cvs -d freebsdanoncvs@anoncvs.FreeBSD.org:/home/ncvs co src
The authenticity of host 'anoncvs.freebsd.org (128.46.156.46)' can't be established.
DSA key fingerprint is 52:02:38:1a:2f:a8:71:d3:f5:83:93:8d:aa:00:6f:65.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'anoncvs.freebsd.org' (DSA) to the list of known hosts.
```

例A-3. 检出6-STABLE 分支中的ls(1) 版本:

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.jp.FreeBSD.org:/home/ncvs
% cvs login
在提示符处, 输入密码 “anoncvs” 。
% cvs co -rRELENG_6 ls
```

例A-4. 创建ls(1) 的变化列表(用标准的diff)

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.jp.FreeBSD.org:/home/ncvs
% cvs login
在提示符处, 输入密码 “anoncvs” 。
% cvs rdiff -u -rRELENG_5_3_0_RELEASE -rRELENG_5_4_0_RELEASE ls
```

例A-5. 找出可以使用的其它的模块名:

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.jp.FreeBSD.org:/home/ncvs
% cvs login
在提示符处, 输入密码 “anoncvs” 。
% cvs co modules
% more modules/modules
```

A.3.4 其他资源

下面附加的资源可能对学习CVS 有帮助:

- CVS 指南 (<http://www.csc.calpoly.edu/~dbutler/tutorials/winter96/cvs/>) 来自Cal Poly。
- CVS 主页 (<http://ximbiot.com/cvs/wiki/>), CVS 开发和支持社区。
- CVSweb (<http://www.FreeBSD.org/cgi/cvsweb.cgi>) 是FreeBSD 项目的CVS web 界面。

A.4 使用CTM

CTM 是保持远程目录树和中央服务器目录树同步的一种方法。它被开发用于FreeBSD 的源代码树, 虽然其他人随着时间推移会发现它可以用于其他目的。当前几乎没有, 也或者只有很少的文档讲述创建deltas 的步骤, 所以如果您希望使用**CTM** 去做其它事情, 请联系ctm-users (<http://lists.FreeBSD.org/mailman/listinfo/ctm-users>) 邮件列表了解更多信息。

A.4.1 为什么我该使用CTM?

CTM 会给您一份FreeBSD 源代码树的本地拷贝。代码树有很多的“flavors” 可用。不管您是希望跟踪完整的CVS 树还是只是一个分支, **CTM** 都会给您提供信息。如果您是FreeBSD 上的一个活跃的开发者, 但是缺乏或者不存在TCP/IP 连接, 或者只是希望把变化自动发送给您, **CTM** 就是适合您的。对于最积极的分支您将会每天获得三个以上的deltas。然而, 您应该考虑通过邮件来自动发送。升级的大小总是保证尽可能的小。通常小于5K, 也偶然(十分之一可能)会有10-50K, 也不时地有个大的100K+ 甚至更大的。

您也需要让自己了解直接和开发代码而不是预发行版本打交道的各种警告。这种情况会很显著, 如果您选择了“current” 代码的话。强烈建议您阅读和FreeBSD 保持同步。

A.4.2 使用CTM 我需要什么？

您需要两样东西：**CTM** 程序，还有初始的deltas 来feed it(达到“current”级别)。

CTM 程序从版本2.0 发布以来已经是FreeBSD 的一部分了，如果您有一份源代码拷贝的话它位于/usr/src/usr.sbin/ctm。

您喂给**CTM** 的“deltas” 可以有两种方式，FTP 或者email。如果您有普通的访问Internet 的FTP 权限，那么下面的FTP 站点支持访问**CTM**：

`ftp://ftp.FreeBSD.org/pub/FreeBSD/CTM/`

或者看看这一小节镜像。

FTP 访问相关的目录并取得README 文件，从那里开始。

如果您希望通过email 得到您的deltas：

订阅一个**CTM** 分发列表。ctm-cvs-cur (<http://lists.FreeBSD.org/mailman/listinfo/ctm-cvs-cur>) 支持完整的CVS 树。ctm-src-cur (<http://lists.FreeBSD.org/mailman/listinfo/ctm-src-cur>) 支持最新的开发分支。ctm-src-4 (<http://lists.FreeBSD.org/mailman/listinfo/ctm-src-4>) 支持4.X 发行分支，等等。。(如果您不知道如何订阅邮件列表，点击上面的列表名或者到<http://lists.FreeBSD.org/mailman/listinfo> 点击您希望订阅的列表。列表页包含了所有必要的订阅指导。)

当您开始接收到您邮件中的**CTM** 升级时，您可以使用ctm_rmail 程序来解压并应用它们。事实上如果您想要让进程以全自动的形式运行的话，您可以通过在/etc/aliases 中设置直接使用ctm_rmail 程序。查看ctm_rmail 手册页了解更多细节。

注意：不管您使用什么方法得到**CTM** deltas，您都应该订阅ctm-announce (<http://lists.FreeBSD.org/mailman/listinfo/ctm-announce>) 邮件列表。以后会有单独的地方提交有关**CTM** 系统的操作的公告。点击上面的邮件列表名并按照指示订阅邮件列表。

A.4.3 第一次使用CTM

在您开始使用**CTM** delta 之前，您需要获得一个起始点。

首先您应该确定您已经有了什么。每个人都可以从一个“空”目录开始。您必须用一个初始的“空的” delta 来开始您的**CTM** 支持树。曾经为了您的便利这些“起始” deltas 被有意的通过CD 来发行，然而现在已经不这样做了。

因为代码树有数十兆字节，您应该更喜欢从手头上已经有的东西开始。如果您有一张-RELEASE CD 光盘，您可以从里面拷贝或者解压缩一份初始代码出来。这会节省非常多的数据传输量。

您会发现这些“初始的” deltas 名字的数字后面都有个x (比如src-cur.3210XEmpty.gz)。后面加一个x 的设计符合您的初始“seed” 的由来。Empty 是一个空目录。通常一个基本的从Empty 开始的转换由100 个deltas 构成。顺便说一下，他们都很大！70 到80 兆字节的gzip 压缩的数据对于XEmpty deltas 是很平常的。

一旦您已经选定了一个基本的delta 开始，您就需要比这个数高的所有的delta。

A.4.4 在您的日常生活中使用CTM

要应用deltas，简单的键入：

```
# cd /where/ever/you/want/the/stuff
# ctm -v -v /where/you/store/your/deltas/src-xxx.*
```

CTM 能够理解被gzip 压缩的deltas，所以您不需要先gunzip 他们，这可以节省磁盘空间。

除非觉得整个过程非常可靠，**CTM** 不会涉及到您的代码树的。您也可以使用 -c 标记来校验delta，这样**CTM** 就不会涉及代码树；它会只校验delta 的完整性看看是否可以安全的用于您的当前代码树。

CTM 还有其他的一些参数，查看手册页或者源代码了解更多信息。

这真的就是全部的事情了。每次得到一个新的delta，就通过**CTM** 运行它来保证您的代码是最新的。

如果这些deltas 很难重新下载的话不要删除它们。有些东西坏掉的时候您会想到保留它们的。即使您只有软盘，也请考虑使用fdwrite 来做一份拷贝。

A.4.5 维持您本地的变动

作为一名开发者喜欢实验，改动代码树中的文件。**CTM** 用一种受限的方式支持本地修改：再检查文件foo 存在之前，首先查找foo.ctm。如果这个文件存在，**CTM** 会对它操作而不是foo。

这种行为给我们提供了一种简单的方式来维持本地的改动：只要复制您计划修改的文件并用.ctm 的后缀重新命名。然后就可以自由的修改代码了，**CTM** 会更新.ctm 文件到最新版本。

A.4.6 其他有趣的CTM 选项

A.4.6.1 正确的找出哪些将被更新

您可以确定变动列表，**CTM** 可以做到，在您的代码库上使用**CTM** 的-l 选项。

这很有用如果您想要保存改动的日志，pre- 或者post- 用各种风格处理修改的文件的纪录，或者仅仅是想感受一下孩子般的疯狂。

A.4.6.2 在升级前制作备份

有时您可能想备份将要被**CTM** 升级所改动的所有文件。

指定-B backup-file 选项会导致**CTM** 备份将要被给定的**CTM** delta 改动的所有文件到backup-file。

A.4.6.3 限定受升级影响的文件

有时您可能对限定一个给定的**CTM** 升级的范围感兴趣，也有可能想知道怎样从一系列deltas 中解压缩一部分文件。

您可以通过使用-e 和-x 选项指定过滤规则表达式来控制**CTM** 即将对之操作的文件列表。

例如，要从您保存的**CTM** deltas 集里解压缩出一个最新的lib/libc/Makefile 文件，运行这个命令：

```
# cd /where/ever/you/want/to/extract/it/
# ctm -e '^lib/libc/Makefile' ~ctm/src-xxx.*
```

对于每一个在**CTM delta** 中指定的文件，**-e** 和 **-x** 选项按照命令行给定的顺序应用。文件只有在所有的 **-e** 和 **-x** 被应用之后标记为合格之后才能被**CTM** 操作。

A.4.7 CTM 未来的计划

其中几项：

- 在**CTM** 中使用一些认证方式，这样来允许察觉冒充的**CTM** 补丁。
- 整理**CTM** 的选项，它们变得杂乱而违反直觉了。

A.4.8 杂项

也有一系列的ports collection 的deltas，但是人们对它的兴致还没有那么高。

A.4.9 CTM 镜像

CTM/FreeBSD 可以在下面的镜像站点通过匿名FTP 下载。如果您选择通过匿名FTP 获取**CTM**，请试着使用一个离您较近的站点。

如果有问题，请联系ctm-users (<http://lists.FreeBSD.org/mailman/listinfo/ctm-users>) 邮件列表。

加利福尼亚州，海湾地区，官方源代码

- <ftp://ftp.FreeBSD.org/pub/FreeBSD/development/CTM/>

南非，旧的deltas 的备份服务器

- <ftp://ftp.za.FreeBSD.org/pub/FreeBSD/CTM/>

中国台湾

- <ftp://ctm.tw.FreeBSD.org/pub/FreeBSD/development/CTM/>
- <ftp://ctm2.tw.FreeBSD.org/pub/FreeBSD/development/CTM/>
- <ftp://ctm3.tw.FreeBSD.org/pub/FreeBSD/development/CTM/>

如果您在您附近找不到镜像或者镜像不完整，试着使用搜索引擎比如alltheweb (<http://www.alltheweb.com/>).

A.5 使用CVSup

A.5.1 概述

CVSup 是一个用于从远程服务器主机上的主CVS 仓库发布和升级源代码树的软件包。FreeBSD 的源代码维护在加利福尼亚州一台主开发服务器的CVS 仓库里。有了**CVSup**，FreeBSD 用户可以很容易的保持他们自己的源代码树更新。

CVSup 使用所谓的升级**pull** 模式。在**pull** 模式下，客户端在需要的时候向服务器端请求更新。服务器被动的等待客户端的升级请求。因此所有的升级都是客户端发起的。服务器决不会发送未请求的升级。用户必须手动运行**CVSup** 客户端获取更新，或者设置一个**cron** 作业来让它以固定的规律自动运行。

术语**CVSup**用大写字母写正是表示，代表了完整的软件包。它的主要组件是运行在每个用户机器上的客户端**cvsup**，和运行在每个FreeBSD 镜像站点上的服务器端**cvsupd**。

当您阅读FreeBSD 文档和邮件列表时，您可能会看见**sup**。**Sup** 是**CVSup** 的前身，有着相似的目的。**CVSup** 使用很多和**sup** 相同的方式，而且，它还是用使用和**sup** 的兼容的配置文件。**Sup** 已经不再被FreeBSD 项目使用了，因为**CVSup** 既快又有更好的灵活性。

A.5.2 安装

安装**CVSup** 最简单的方式就是使用FreeBSD packages collection 中预编译的**net/cvsup** 包。如果您想从源代码构建**CVSup**，您可以使用**net/cvsup port**。但是预先警告一下：**net/cvsup port** 依赖于Modula-3 系统，会花费相当的时间和磁盘空间来下载编译。

注意：如果想在没有安装**XFree86** 或**Xorg** 的计算机，例如服务器上使用**CVSup**，则只能使用不包含**CVSup GUI** 的**net/cvsup-without-gui**。

A.5.3 CVSup 配置

CVSup 的操作被一个叫做**supfile** 的配置文件所控制。在目录**/usr/share/examples/cvsup/** 下面有一些示例的**supfiles**。

supfile 中的信息解答了**CVSup** 下面的几个问题：

- 您想接收哪些文件？
- 您想要它们的哪个版本？
- 您想从哪里获取它们？
- 您想把它们放在您自己机器的什么地方？
- 您想把您的状态文件放在哪？

在下面的章节里，我们通过依次回答这些问题来创建一个典型的**supfile** 文件。首先，我们描述一下**supfile** 的整体构成。

supfile 是个文本文件。注释用**#** 开头，至行尾有效。空行和只包含注释的行会被忽略。

每个保留行描述一批用户希望接收的文件。每行以“collection”，由服务器端定义的合理的文件分组，的名字开头。collection 的名字告诉服务器您想要的文件。collection 名字结束或者有更多的字段，用空格分隔。这些字段回答了上面列出的问题。字段类型有两种：标记字段和值字段。标记字段由独立的关键词组成，比如，delete 或者compress。值字段也用关键词开头，关键词后面跟= 和第二个词而没有空格。例如，release=cvs 是一个值字段。

一个典型的supfile 往往接收多于一个的collection。创建supfile 的一种方式是为每一个collection 指定相关的字段。然而，这样使得supfile 的行变得特别长，很不方便，因为supfile 中的所有collection 的大部分字段都是相同的。CVSup 提供了一个默认机制来避免这些问题。用特定的伪collection 名*default 开头的行可以被用来设置标记和值为supfile 中随后的collection 中的默认值。默认值可以通过为这个collection 自身指定不同的值来对单个的collection 覆盖设置，也可以在mid-supfile 中通过附加的*default 行改变或扩充。

知道了这些，我们现在就可以开始创建一个用于接收和升级FreeBSD-CURRENT 主源代码树的supfile 文件了。

- 您想接收哪些文件？

通过CVSup 可用的文件组织成叫做“collections”的名称组。这些可用的collection 在随后的章节 中描述。在这个例子里，我们希望接收FreeBSD 系统的完整的主代码树。有一个单独的大的collection src-all 让我们完成这个。创建我们的supfile 的第一步，我们简单的列出这些collection，每个一行(在这个例子里，只有一行)：

```
src-all
```

- 您想要他们的哪个版本？

通过CVSup，您实际上可以接收曾经存在的源代码的任何版本。这是有可能的，因为cvsupd 服务器直接通过CVS 仓库工作，那包含了所有的版本。您可以用tag= 和date= 值字段指定一个您想要的版本。

警告：仔细的正确指定任何tag= 字段。有一些tag 只对特定的collection 文件合法。如果您指定了一个不正确的或者拼写错误的tag，CVSup 会删除您可能不想删除的文件。特别地，对ports-* collection 只使用tag=。

tag= 字段在仓库中表示为一个符号标签。有两种标签，修订标签和分支标签。修订标签代表一个特定的修订版本。它的含义是一成不变的。分支标签，另一方面，代表给定开发线上给定时间的最新修订。因为分支标签不代表一个特定的修订版本，它明天的含义就可能和今天的有所不同。

第A.7 节 包含了用户可能感兴趣的分支标签。当在CVSup 的配置文件中指定标签的时候，必须用tag= 开头(RELENG_4 会变成tag=RELENG_4)。记住只有tag= 可以用于Ports Collection。

警告：注意像看到的那样正确的输入标签名。CVSup 不能辨别合法和不合法标签。如果您拼写错了标签名，CVSup 会像您指定了一个没有任何文件的合法标签一样工作，那会删除您已经存在的代码。

当您指定一个分支标签的时候，您通常会收到开发线上文件的最新版本。如果您希望接收一些过时的版本，您可以通过用date= 值字段指定一个日期来做到。cvsup(1) 手册页解释了如何做。

对于我们的示例来说，我们希望接收FreeBSD-CURRENT。我们在我们的supfile 的开头添加这行：

```
*default tag=.
```

有一个重要的特例，如果您既没指定tag= 字段也没指定date= 字段的情况。这种情况下，您会收到直接来自于服务器CVS 仓库的真实的RCS 文件，而不是某一特定版本。开发人员一般喜欢这种操作模式。通

过在他们的系统上维护一份仓库自身的副本，他们可以浏览修订历史以及检查文件过去的版本。然而，这个好处是以大量的磁盘空间为代价的。

- 您想从哪里获取他们？

我们使用`host=`字段来告诉`cvsup`从哪里获取更新。任何一个CVSup 镜像站点都可以，虽然您应该选择一个离您比较近的站点。在这个例子里我们将使用一个虚拟的FreeBSD 发布站点，`cvsup99.FreeBSD.org`：

```
*default host=cvsup99.FreeBSD.org
```

您需要在运行**CVSup**之前把这个改成一个实际存在的站点。在任何`cvsup`运行的特定时刻，您都可以在命令行上使用`-h hostname`选项来覆盖主机设置。

- 您想把它们放在您自己机器的什么地方？

`prefix=`字段告诉`cvsup`把接收的文件放在哪里。在这个例子里，我们把源代码文件直接放进我们的主源代码树，`/usr/src`。`src`目录已经隐含在我们选择接收的`collection`里了，所以正确的写法是：

```
*default prefix=/usr
```

- `cvsup` 在哪里维护它的状态文件？

CVSup 客户端在被叫做“base”的目录里维护了几个状态文件。这些文件帮助**CVSup**更有效的工作，通过跟踪您已经接收到哪些更新的方式。我们将使用标准的base 目录，`/var/db`：

```
*default base=/var/db
```

如果您的base 目录还不存在，现在最好创建它。如果base 目录不存在，`cvsup` 客户端会拒绝工作。

- 其他的supfile 设置：

在supfile 中有一些其他选项需要介绍一下：

```
*default release=cvs delete use-rel-suffix compress
```

`release=cvs` 显示服务器应该从FreeBSD 的主CVS 仓库中获取信息。事实上总是这样的，但是也有可能超出这个讨论的范围。

`delete` 给**CVSup** 权限删除文件。您应该总是指定这个，这样**CVSup** 可以保证您的源代码树完全更新。**CVSup** 很小心的只删除那些不再依赖的文件。您拥有的任何额外的文件会被严格的保留。

`use-rel-suffix` 是... 不可思议的。如果您真的想了解它，查看`cvsup(1)` 手册页。否则，就指定而不用担心这个。

`compress` 启用gzip 风格的信道压缩。如果您的网络连接是T1 或者更快，您可能不想使用压缩。否则，它非常有帮助。

- 把它们放在一起：

这是我们的示例的完整supfile 文件：

```
*default tag=.
*default host=cvsup99.FreeBSD.org
*default prefix=/usr
*default base=/var/db
*default release=cvs delete use-rel-suffix compress
```

```
src-all
```


A.5.3.1 refuse 文件

像上面提到的，CVSup 使用一种 **pull** 方法。基本上，这意味着您要连接到 CVSup 服务器，服务器说，“这有些您能下载的东西...”，然后您的客户端反应“好，我要这个，这个，这个，还有这个。”在默认的配置中，CVSup 客户端会取回您在配置文件中选定的 **collection** 和标签的每个文件。然而，并不总是您想要的，尤其是您在同步 **doc**，**ports**，或者 **www** 树——大部分人都不能阅读四种或者五种语言，因此他们不需要下载特定语言的文件。如果您在 CVSup Ports Collection，您可以通过单独指定每个 **collection** 来避免这个(比如，**ports-astrology**，**ports-biology**，等等取代简单的说明 **ports-all**)。然而，因为 **doc** 和 **www** 树没有特定语言的 **collection**，您必须使用 CVSup 许多极好的特性之一：**refuse** 文件。

refuse 文件本质上是告诉 CVSup 它不应该从 **collection** 中取得某些文件；换句话说，它告诉客户端拒绝来自服务器的特定的文件。**refuse** 文件可以在 **base/sup/** 中找到(或者，如果您没有，应该创建一个)。**base** 在您的 **supfile** 中定义；默认情况下，**base** 就是 **/var/db**，这意味着默认的 **refuse** 文件就是 **/var/db/sup/refuse**。

refuse 文件的格式很简单；它仅仅包含您不希望下载的文件和目录名。例如，如果您除了英语和德语之外不会讲其他语言，而且也不打算阅读德文的文档翻译版本，则可以把下面这些放在您的 **refuse** 文件里：

```
doc/bn_*
doc/da_*
doc/de_*
doc/el_*
doc/es_*
doc/fr_*
doc/it_*
doc/ja_*
doc/nl_*
doc/no_*
doc/pl_*
doc/pt_*
doc/ru_*
doc/sr_*
doc/tr_*
doc/zh_*
```

等等其他语言(您可以通过浏览 FreeBSD CVS 仓库 (<http://www.FreeBSD.org/cgi/cvsweb.cgi/>)找到完整的列表)。

有这个非常有用的特性，那些慢速连接或者要为他们的 Internet 连接按时付费的用户就可以节省宝贵的时间因为他们不再需要下载那些从来不用文件。要了解 **refuse** 文件的更多信息以及其它 CVSup 的优雅的特性，请浏览它的手册页。

A.5.4 运行 CVSup

您现在准备尝试升级了。命令很简单：

```
# cvsup supfile
```

supfile 的位置当然就是您刚刚创建的 **supfile** 文件名啦。如果您在 X11 下面运行，**cvsup** 会显示一个有一些可以做平常事情的按钮的 GUI 窗口。按 **go** 按钮，然后看着它运行。

在这个例子里您将要升级您目前的`/usr/src`树，您将需要用`root`来运行程序，这样`cvsup`有需要的权限来更新您的文件。刚刚创建了您的配置文件，又从来没有使用过这个程序，紧张不安是可以理解的。有一个简单的方法不改变您当前的文件来做一次试验性的运行。只要在方便的地方创建一个空目录，并在命令行上作为一个额外的参数说明：

```
# mkdir /var/tmp/dest
# cvsup supfile /var/tmp/dest
```

您指定的目录会作为所有文件更新的目的路径。**CVSup**会检查您在`/usr/src`中的文件，但是不会修改或删除。任何文件更新都会被放到`/var/tmp/dest/usr/src`里了。在这种方式下运行**CVSup**也会把它的`base`目录状态文件保持原样。这些文件的新版本会被写到指定的目录。因为您有`/usr/src`目录的读权限，所以执行这种试验性的运行甚至不需要使用`root`用户。

如果您没有运行X11 或者不喜欢GUI，当您运行`cvsup`的时候需要在命令行添加两个选项：

```
# cvsup -g -L 2 supfile
```

`-g`告诉**CVSup**不要使用GUI。如果您没在运行X11 这个是自动的，否则您必须指定它。

`-L 2`告诉**CVSup**输出所有正在升级的文件的细节。有三个等级可以选择，从`-L 0`到`-L 2`。默认是0，意味着除了错误消息什么都不输出。

还有许多其它的选项可用。想要一个简短的列表，输入`cvsup -H`。要查看更详细的描述，请查看手册页。

一旦您对升级工作的方式满意了，您就可以使用`cron(8)`来安排规则的运行**CVSup**。很显然的，您不应该让**CVSup**通过`cron(8)`运行的时候使用它的GUI。

A.5.5 CVSup 文件collection

CVSup可用的文件collection 是分级组织的。有几个大的collection，然后它们有分成更小的子collection。接收一个大的collection 等同于接收它的每一个子collection。collection 的等级关系在下面列表中通过缩进的使用反映出来。

最常用的collection 是`src-all`，和`ports-all`。其它的collection 只被有着特定目的的小部分人使用，有些站点可能不全部支持。

```
cvsrc-all release=cvsrc
```

FreeBSD 主CVS 仓库，包含密码系统的代码。

```
distrib release=cvsrc
```

FreeBSD 发行版本和镜像相关的文件。

```
doc-all release=cvsrc
```

FreeBSD 使用手册和其它文档的源代码。其中不包含FreeBSD web 站点的文件。

```
ports-all release=cvsrc
```

FreeBSD Ports Collection。

重要: 如果您不想升级全部的ports-all(整个ports 树), 而只是使用下面列出的一个子集, 请确保您总是升级了ports-base 子collection! 无论何时在ports 构建下层构造有所改变的时候都会通过ports-base 表现出来, 事实上某些改变会很快被“实际的” ports 使用, 因此, 如果您只升级了“实际的” ports 而他们使用了一些新的特性, 就有极大的可能编译会因一些神秘的错误信息而失败。这种情况下**非常快速**的要做的事情就是确保您的ports-base 子collection 更新到最新。

重要: 要自行构建ports/INDEX, 您**必须** 接受ports-all (完整的ports tree)。在部分ports tree 上构建ports/INDEX 是不被支持的。请参见 FAQ (http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/faq/applications.html#MAKE-INDEX)。

ports-accessibility release=cvs

用以帮助残疾用户的软件。

ports-arabic release=cvs

阿拉伯语支持。

ports-archivers release=cvs

存档工具。

ports-astro release=cvs

天文相关的ports。

ports-audio release=cvs

声音支持。

ports-base release=cvs

Ports Collection 构建下部构造- 位于/usr/ports 的Mk/ 和Tools/ 子目录的各种各样的文件。

注意: 请查看 重要警告: 您应该**总是**更新这个子collection, 无论您更新FreeBSD Ports Collection 的任何部分的时候!

ports-benchmarks release=cvs

基准。

ports-biology release=cvs

生物学。

ports-cad release=cvs

计算机辅助设计工具。

`ports-chinese release=cv`s

中文语言支持。

`ports-comms release=cv`s

通信软件。

`ports-converters release=cv`s

字符编码转换。

`ports-databases release=cv`s

数据库

`ports-deskutils release=cv`s

计算机发明前常出现在桌面上的东西。

`ports-devel release=cv`s

开发工具。

`ports-dns release=cv`s

DNS 相关软件。

`ports-editors release=cv`s

编辑器

`ports-emulators release=cv`s

其它操作系统的模拟器

`ports-finance release=cv`s

货币，金融相关应用程序。

`ports-ftp release=cv`s

FTP 客户端和服务端工具。

`ports-games release=cv`s

游戏

`ports-german release=cv`s

德语支持。

`ports-graphics release=cv`s

图形图像工具。

`ports-hebrew release=cv`s

希伯来语支持。

`ports-hungarian release=cv`s

匈牙利语言支持。

`ports-irc release=cv`s

Internet 多线交谈(IRC)工具。

`ports-japanese release=cv`s

日语支持。

`ports-java release=cv`s

Java 工具。

`ports-korean release=cv`s

韩国语言支持。

`ports-lang release=cv`s

编程语言。

`ports-mail release=cv`s

邮件软件。

`ports-math release=cv`s

数值计算软件。

`ports-mbone release=cv`s

MBone 应用程序。

`ports-misc release=cv`s

杂样工具。

`ports-multimedia release=cv`s

多媒体软件。

`ports-net release=cv`s

网络软件。

`ports-net-im release=cv`s

即时消息软件。

`ports-net-mgmt release=cv`s

网管软件。

`ports-net-p2p release=cv`s

对等网(peer to peer network) 应用。

`ports-news release=cv`s

USENET 新闻软件。

`ports-palm release=cv`s

Palm™ 系列软件支持。

`ports-polish release=cv`s

波兰语支持。

`ports-portuguese release=cv`s

葡萄牙语支持。

`ports-print release=cv`s

打印软件。

`ports-russian release=cv`s

俄语支持。

`ports-science release=cv`s

科学计算。

`ports-security release=cv`s

安全工具。

`ports-shells release=cv`s

命令行shell。

`ports-sysutils release=cv`s

系统实用工具。

`ports-textproc release=cv`s

文本处理工具(不包含桌面出版)。

`ports-ukrainian release=cv`s

乌克兰语支持。

`ports-vietnamese release=cv`s

越南语支持。

`ports-www release=cv`s

万维网(WWW)相关软件。

`ports-x11 release=cv`s

支持X window 系统的ports。

`ports-x11-clocks release=cv`

X11 时钟。

`ports-x11-fm release=cv`

X11 文件管理器。

`ports-x11-fonts release=cv`

X11 字体和字体工具。

`ports-x11-toolkits release=cv`

X11 工具包。

`ports-x11-servers release=cv`

X11 服务器。

`ports-x11-themes release=cv`

X11 主题。

`ports-x11-wm release=cv`

X11 窗口管理器。

`src-all release=cv`

FreeBSD 主代码，包含密码系统的代码。

`src-base release=cv`

/usr/src 顶层的各式各样的文件。

`src-bin release=cv`

但用户模式下可能用到的用户工具(/usr/src/bin)。

`src-contrib release=cv`

FreeBSD 项目之外的工具和库，通常在FreeBSD 中不作修改(/usr/src/contrib)。

`src-crypto release=cv`

FreeBSD 项目之外的密码系统工具和库，通常在FreeBSD 中不作修改(/usr/src/crypto)。

`src-eBones release=cv`

Kerberos 和DES (/usr/src/eBones)。没有在当前的FreeBSD 发行中使用。

`src-etc release=cv`

系统配置文件(/usr/src/etc)。

`src-games release=cvs`
游戏(/usr/src/games)。

`src-gnu release=cvs`
GNU 公共许可协议的工具(/usr/src/gnu)。

`src-include release=cvs`
头文件(/usr/src/include)。

`src-kerberos5 release=cvs`
Kerberos5 安全包(/usr/src/kerberos5)。

`src-kerberosIV release=cvs`
KerberosIV 安全包(/usr/src/kerberosIV)。

`src-lib release=cvs`
库(/usr/src/lib)。

`src-libexec release=cvs`
通常被其它程序调用的系统程序(/usr/src/libexec)。

`src-release release=cvs`
生成FreeBSD 版本必需的文件(/usr/src/release)。

`src-sbin release=cvs`
但用户模式的系统工具(/usr/src/sbin)。

`src-secure release=cvs`
密码相关库和命令(/usr/src/secure)。

`src-share release=cvs`
跨多个平台的共享的文件(/usr/src/share)。

`src-sys release=cvs`
内核(/usr/src/sys)。

`src-sys-crypto release=cvs`
内核密码系统代码(/usr/src/sys/crypto)。

`src-tools release=cvs`
维护FreeBSD 的各种各样的工具(/usr/src/tools)。

`src-usrbin release=cvs`
用户工具(/usr/src/usr.bin)。

`src-usrsbin release=cvs`

系统工具(/usr/src/usr.sbin)。

`www release=cvs`

FreeBSD WWW 站点的源代码。

`distrib release=self`

CVSup 服务器的配置文件。用于**CVSup** 镜像站点。

`gnats release=current`

GNATS bug 跟踪数据库。

`mail-archive release=current`

FreeBSD 邮件列表存档。

`www release=current`

预处理过的FreeBSD WWW 站点文件(不是源文件)。用于WWW 镜像站点。

A.5.6 更多信息

CVSup FAQ 和关于**CVSup** 的其它信息, 请查看 **CVSup** 主页 (<http://www.polstra.com/projects/freeware/CVSup/>)。

大多数**CVSup** 的和FreeBSD 相关的讨论都在FreeBSD 技术讨论邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-hackers>)。软件的新版本在那发布, 还有FreeBSD 公告邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-announce>)。

问题和bug 报告应该发给程序作者<cvsup-bugs@polstra.com>。

A.5.7 CVSup 站点

FreeBSD 的**CVSup** 服务器运行于下列站点:

中央服务器, 主要镜像站点, 阿根廷, 爱尔兰, 爱沙尼亚, 奥地利, 澳大利亚, 巴西, 保加利亚, 冰岛, 波兰, 丹麦, 德国, 俄罗斯, 法国, 菲律宾, 芬兰, 哥斯达黎加, 韩国, 荷兰, 吉尔吉斯斯坦, 加拿大, 捷克共和国, 科威特, 拉脱维亚, 立陶宛, 罗马尼亚, 美国, 南非, 挪威, 葡萄牙, 日本, 瑞典, 瑞士, 圣马力诺, 斯洛伐克共和国, 斯洛文尼亚, 泰国, 土耳其, 乌克兰, 西班牙, 希腊, 新加坡, 新西兰, 匈牙利, 意大利, 印度尼西亚, 英国, 中国大陆, 中国台湾。

(2006/03/25 21:54:18 UTC 更新)

中央服务器

- cvsup.FreeBSD.org

主要镜像站点

- cvsup1.FreeBSD.org
- cvsup2.FreeBSD.org
- cvsup3.FreeBSD.org
- cvsup4.FreeBSD.org
- cvsup5.FreeBSD.org
- cvsup6.FreeBSD.org
- cvsup7.FreeBSD.org
- cvsup8.FreeBSD.org
- cvsup9.FreeBSD.org
- cvsup10.FreeBSD.org
- cvsup11.FreeBSD.org
- cvsup12.FreeBSD.org
- cvsup13.FreeBSD.org
- cvsup14.FreeBSD.org
- cvsup15.FreeBSD.org
- cvsup16.FreeBSD.org
- cvsup18.FreeBSD.org

阿根廷

- cvsup.ar.FreeBSD.org

爱尔兰

- cvsup.ie.FreeBSD.org

爱沙尼亚

- cvsup.ee.FreeBSD.org

奥地利

- cvsup.at.FreeBSD.org
- cvsup2.at.FreeBSD.org

澳大利亚

- cvsup.au.FreeBSD.org
- cvsup2.au.FreeBSD.org
- cvsup3.au.FreeBSD.org
- cvsup4.au.FreeBSD.org
- cvsup5.au.FreeBSD.org
- cvsup6.au.FreeBSD.org
- cvsup7.au.FreeBSD.org

巴西

- cvsup.br.FreeBSD.org
- cvsup2.br.FreeBSD.org
- cvsup3.br.FreeBSD.org
- cvsup4.br.FreeBSD.org
- cvsup5.br.FreeBSD.org

保加利亚

- cvsup.bg.FreeBSD.org

冰岛

- cvsup.is.FreeBSD.org

波兰

- cvsup.pl.FreeBSD.org
- cvsup2.pl.FreeBSD.org
- cvsup3.pl.FreeBSD.org

丹麦

- cvsup.dk.FreeBSD.org
- cvsup2.dk.FreeBSD.org
- cvsup3.dk.FreeBSD.org

德国

- cvsup.de.FreeBSD.org
- cvsup2.de.FreeBSD.org
- cvsup3.de.FreeBSD.org
- cvsup4.de.FreeBSD.org
- cvsup5.de.FreeBSD.org
- cvsup6.de.FreeBSD.org
- cvsup7.de.FreeBSD.org
- cvsup8.de.FreeBSD.org

俄罗斯

- cvsup.ru.FreeBSD.org
- cvsup2.ru.FreeBSD.org
- cvsup3.ru.FreeBSD.org
- cvsup4.ru.FreeBSD.org
- cvsup5.ru.FreeBSD.org
- cvsup6.ru.FreeBSD.org
- cvsup7.ru.FreeBSD.org

法国

- cvsup.fr.FreeBSD.org
- cvsup2.fr.FreeBSD.org
- cvsup3.fr.FreeBSD.org
- cvsup4.fr.FreeBSD.org
- cvsup5.fr.FreeBSD.org
- cvsup8.fr.FreeBSD.org

菲律宾

- cvsup1.ph.FreeBSD.org

芬兰

- cvsup.fi.FreeBSD.org
- cvsup2.fi.FreeBSD.org

哥斯达黎加

- cvsup1.cr.FreeBSD.org

韩国

- cvsup.kr.FreeBSD.org
- cvsup2.kr.FreeBSD.org
- cvsup3.kr.FreeBSD.org

荷兰

- cvsup.nl.FreeBSD.org
- cvsup2.nl.FreeBSD.org
- cvsup3.nl.FreeBSD.org

- cvsup5.nl.FreeBSD.org

吉尔吉斯斯坦

- cvsup.kg.FreeBSD.org

加拿大

- cvsup1.ca.FreeBSD.org

捷克共和国

- cvsup.cz.FreeBSD.org

科威特

- cvsup1.kw.FreeBSD.org

拉脱维亚

- cvsup.lv.FreeBSD.org
- cvsup2.lv.FreeBSD.org

立陶宛

- cvsup.lt.FreeBSD.org
- cvsup2.lt.FreeBSD.org
- cvsup3.lt.FreeBSD.org

罗马尼亚

- cvsup.ro.FreeBSD.org
- cvsup1.ro.FreeBSD.org

- cvsup2.ro.FreeBSD.org
- cvsup3.ro.FreeBSD.org

美国

- cvsup1.us.FreeBSD.org
- cvsup2.us.FreeBSD.org
- cvsup3.us.FreeBSD.org
- cvsup4.us.FreeBSD.org
- cvsup5.us.FreeBSD.org
- cvsup6.us.FreeBSD.org
- cvsup7.us.FreeBSD.org
- cvsup8.us.FreeBSD.org
- cvsup9.us.FreeBSD.org
- cvsup10.us.FreeBSD.org
- cvsup11.us.FreeBSD.org
- cvsup12.us.FreeBSD.org
- cvsup13.us.FreeBSD.org
- cvsup14.us.FreeBSD.org
- cvsup15.us.FreeBSD.org
- cvsup16.us.FreeBSD.org
- cvsup18.us.FreeBSD.org

南非

- cvsup.za.FreeBSD.org
- cvsup2.za.FreeBSD.org

挪威

- cvsup.no.FreeBSD.org

葡萄牙

- cvsup.pt.FreeBSD.org
- cvsup2.pt.FreeBSD.org
- cvsup3.pt.FreeBSD.org

日本

- cvsup.jp.FreeBSD.org
- cvsup2.jp.FreeBSD.org
- cvsup3.jp.FreeBSD.org
- cvsup4.jp.FreeBSD.org
- cvsup5.jp.FreeBSD.org
- cvsup6.jp.FreeBSD.org

瑞典

- cvsup.se.FreeBSD.org
- cvsup3.se.FreeBSD.org

瑞士

- cvsup.ch.FreeBSD.org

圣马力诺

- cvsup.sm.FreeBSD.org

斯洛伐克共和国

- cvsup.sk.FreeBSD.org
- cvsup2.sk.FreeBSD.org

斯洛文尼亚

- cvsup.si.FreeBSD.org
- cvsup2.si.FreeBSD.org

泰国

- cvsup.th.FreeBSD.org

土耳其

- cvsup.tr.FreeBSD.org

乌克兰

- cvsup2.ua.FreeBSD.org
- cvsup3.ua.FreeBSD.org
- cvsup4.ua.FreeBSD.org
- cvsup5.ua.FreeBSD.org
- cvsup6.ua.FreeBSD.org
- cvsup7.ua.FreeBSD.org

西班牙

- cvsup.es.FreeBSD.org
- cvsup2.es.FreeBSD.org
- cvsup3.es.FreeBSD.org

希腊

- cvsup.gr.FreeBSD.org
- cvsup2.gr.FreeBSD.org

新加坡

- cvsup.sg.FreeBSD.org

新西兰

- cvsup.nz.FreeBSD.org

匈牙利

- cvsup.hu.FreeBSD.org

意大利

- cvsup.it.FreeBSD.org

印度尼西亚

- cvsup.id.FreeBSD.org

英国

- cvsup.uk.FreeBSD.org
- cvsup2.uk.FreeBSD.org
- cvsup3.uk.FreeBSD.org
- cvsup4.uk.FreeBSD.org

中国大陆

- cvsup.cn.FreeBSD.org
- cvsup2.cn.FreeBSD.org
- cvsup3.cn.FreeBSD.org
- cvsup4.cn.FreeBSD.org

- cvsup5.cn.FreeBSD.org

中国台湾

- cvsup.tw.FreeBSD.org
- cvsup3.tw.FreeBSD.org
- cvsup4.tw.FreeBSD.org
- cvsup5.tw.FreeBSD.org
- cvsup6.tw.FreeBSD.org
- cvsup7.tw.FreeBSD.org
- cvsup8.tw.FreeBSD.org
- cvsup9.tw.FreeBSD.org
- cvsup10.tw.FreeBSD.org
- cvsup11.tw.FreeBSD.org
- cvsup12.tw.FreeBSD.org
- cvsup13.tw.FreeBSD.org

A.6 使用Portsnap

A.6.1 介绍

Portsnap 是一套用以安全地分发FreeBSD的系统。每隔大约一个小时，就会生成一份ports的最新“快照”，它会被打包并进行数字签名。这些文件接下来将通过HTTP来分发。

与CVSup类似，**Portsnap**采用拉(pull)的模式来进行更新：经过打包并签名的ports tree被放在web服务器上，被动地等待用户请求它们。用户需要手工运行portsnap(8)来下载更新，或者设置cron(8)任务来自动地进行更新。

由于一些技术原因，**Portsnap**并不自动地直接更新位于/usr/ports/目录中的“实际的”ports tree；与此相反，它默认情况下只操作位于/var/db/portsnap/的压缩的ports tree副本，而这个副本则用于更新实际的ports tree。

注意：如果**Portsnap**是通过FreeBSD Ports Collection安装的，则这份压缩快照的默认位置则是/usr/local/portsnap/而非/var/db/portsnap/。

A.6.2 安装

在FreeBSD 6.0 和更新版本上，**Portsnap** 已经成为FreeBSD 基本系统的一部分。在较早版本的FreeBSD 中，它可由sysutils/portsnap port 来安装。

A.6.3 Portsnap 的配置

Portsnap 的操作，是通过/etc/portsnap.conf 配置文件来控制的。对于多数用户来说，默认的配置 文件已经可用了；要了解进一步的细节，则应参考portsnap.conf(5) 联机手册。

注意：假如**Portsnap** 是通过FreeBSD Ports Collection 安装的，则它将使用配置文件/usr/local/etc/portsnap.conf 而非/etc/portsnap.conf。这个文件并不随port 的安装自动创建，但我们 提供了一个示例的配置文件；将其复制到合适的位置，然后运行下面的命令：

```
# cd /usr/local/etc && cp portsnap.conf.sample portsnap.conf
```

A.6.4 首次运行Portsnap

在首次运行portsnap(8) 时，它需要将整个ports tree 的压缩快照下载到/var/db/portsnap/ (或者，如 果**Portsnap** 是通过Ports Collection 安装的，则是/usr/local/portsnap/)。在2006 年初，其下载尺寸大约 是41 MB。

```
# portsnap fetch
```

一旦下载了压缩的快照，就可以将它释放成为位于/usr/ports/ 中的“实际的” ports tree 了。即时之 前那个目录中已经有了一份ports tree 也需要这样做(例如，通过使用CVSup)，因为这个操作，将为后续 的portsnap 决定更新ports tree 的哪一部份提供基础。

```
# portsnap extract
```

注意：在默认安装中，并不会自动建立/usr/ports。在使用portsnap 之前应该先建立它。

A.6.5 更新Ports Tree

在首次下载压缩的ports tree 快照，并将其释放到/usr/ports/ 之后，更新ports tree 包含下面两 步：**fetch**(下载) 对于压缩快照的更新，并使用它们来**update**(更新) 实际的ports tree。这两步可以通过一 个portsnap 命令来完成：

```
# portsnap fetch update
```

注意：较早版本的portsnap 并不支持这种写法。如果不能用的话，试试看下面的：

```
# portsnap fetch
# portsnap update
```

A.6.6 通过cron 来运行Portsnap

为了避免对于**Portsnap** 服务器的“快闪”式访问，`portsnap fetch` 不支持作为**cron**(8) 任务来运行。与此相反，提供了一个特殊的**portsnap cron** 命令，它在开始下载更新之前会随机等待最多3600 秒。

此外，强烈建议不要将**portsnap update** 作为**cron** 任务来运行，因为它可能给正在同时进行的**port** 安装带来大问题。不过，更新**ports** 的**INDEX** 文件一般并无大碍，这可以通过**portsnap** 的**-I** 参数来实现(显然，如果**portsnap -I update** 是通过**cron** 来运行的，就需要在之后执行不带**-I** 的**portsnap update** 来更新**ports tree** 余下的部分了。)

可以在**/etc/crontab** 中加入下列设置，以便让**portsnap** 更新其压缩快照，以及位于**/usr/ports/** 中的**INDEX** 文件，并在有**port** 过期时发出邮件通知：

```
0 3 * * * root portsnap -I cron update && pkg_version -vIL=
```

注意：如果系统时钟没有设置为使用本地时区，请将3 改为一介于0 和23 的随机值，以便让**Portsnap** 服务器的负载更为平均。

注意：某些较早版本的**portsnap**，并不支持在一次调用**portsnap** 时使用多个命令(例如，`cron update`)。如果这样不行，请将**portsnap -I cron update** 改为**portsnap cron && portsnap -I update**。

A.7 CVS 标签

当使用**cv**s 或者**CVSup** 获取和升级源代码的时候，必须指定一个修订标签。修订标签代表**FreeBSD** 开发的一个特定分支，或者一个特定的时间点。第一种叫做“分支标签”，第二种叫做“版本标签”。

A.7.1 分支标签

所有这些，除了**HEAD** (这个总是合法标签)以外，只适用于**src/** 树。**ports/**，**doc/**，和**www/** 树没有分支。

HEAD

主线的符号名，或者说**FreeBSD-CURRENT**。当没有指定修订版本的时候也是默认的。

在**CVSup** 里，这个标签通过一个**.** 来反映出来(不是标点，而是一个**.** 字符)。

注意：在**CVS** 里，当没有修订标签指定时这是默认的。在一台**STABLE** 机器上检出或者升级到**CURRENT** 源代码通常**不是** 一个好主意，除非这是您的本意。

RELENG_6

这是FreeBSD-6.X 的开发分支，也被称作FreeBSD 6-STABLE。

RELENG_6_0

FreeBSD-6.0 的发行版分支，只用于安全公告，以及其他重要更新。

RELENG_5

这是FreeBSD-5.X 的开发分支，也被称作FreeBSD 5-STABLE。

RELENG_5_4

FreeBSD-5.4 安全分支。只被安全公告和其它重要更新使用。

RELENG_5_3

FreeBSD-5.3 安全分支。只被安全公告和其它重要更新使用。

RELENG_5_2

针对FreeBSD-5.2 和FreeBSD-5.2.1 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_5_1

针对FreeBSD-5.1 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_5_0

针对FreeBSD-5.0 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_4

FreeBSD-4.X 开发线，也被叫做FreeBSD-STABLE。

RELENG_4_11

FreeBSD-4.11 发行版，只被安全公告和其它重要更新使用。

RELENG_4_10

针对FreeBSD-4.10 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_4_9

针对FreeBSD-4.9 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_4_8

针对FreeBSD-4.8 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_4_7

针对FreeBSD-4.7 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_4_6

针对FreeBSD-4.6 和FreeBSD-4.6.2 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_4_5

针对FreeBSD-4.5 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_4_4

针对FreeBSD-4.4 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_4_3

针对FreeBSD-4.3 的发行版本分支，只做安全咨询和其它紧急的修正。

RELENG_3

FreeBSD-3.X 的开发线，也被叫做3.X-STABLE。

RELENG_2_2

FreeBSD-2.2.X 的开发线，也被叫做2.2-STABLE。这个分支过于陈旧了。

A.7.2 版本标签

当一个特定的FreeBSD 版本发行时，这些标签代表了一个指定的时间点。发布工程进程在Release Engineering Information (<http://www.FreeBSD.org/releeng/>) 和Release Process (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/releeng/release-proc.html) 文档中被详细描述。src 树使用以RELENG_ 开头的标签。ports 和doc 树使用以RELEASE 开头的标签。最后，www 树上不会有任何特定发行版的标签。

RELENG_6_0_0_RELEASE

FreeBSD 6.0

RELENG_5_4_0_RELEASE

FreeBSD 5.4

RELENG_4_11_0_RELEASE

FreeBSD 4.11

RELENG_5_3_0_RELEASE

FreeBSD 5.3

RELENG_4_10_0_RELEASE

FreeBSD 4.10

RELENG_5_2_1_RELEASE

FreeBSD 5.2.1

RELENG_5_2_0_RELEASE

FreeBSD 5.2

RELENG_4_9_0_RELEASE

FreeBSD 4.9

RELENG_5_1_0_RELEASE

FreeBSD 5.1

RELENG_4_8_0_RELEASE

FreeBSD 4.8

RELENG_5_0_0_RELEASE

FreeBSD 5.0

RELENG_4_7_0_RELEASE

FreeBSD 4.7

RELENG_4_6_2_RELEASE

FreeBSD 4.6.2

RELENG_4_6_1_RELEASE

FreeBSD 4.6.1

RELENG_4_6_0_RELEASE

FreeBSD 4.6

RELENG_4_5_0_RELEASE

FreeBSD 4.5

RELENG_4_4_0_RELEASE

FreeBSD 4.4

RELENG_4_3_0_RELEASE

FreeBSD 4.3

RELENG_4_2_0_RELEASE

FreeBSD 4.2

RELENG_4_1_1_RELEASE

FreeBSD 4.1.1

RELENG_4_1_0_RELEASE

FreeBSD 4.1

RELENG_4_0_0_RELEASE

FreeBSD 4.0

RELENG_3_5_0_RELEASE

FreeBSD-3.5

RELENG_3_4_0_RELEASE

FreeBSD-3.4

RELENG_3_3_0_RELEASE

FreeBSD-3.3

RELENG_3_2_0_RELEASE

FreeBSD-3.2

RELENG_3_1_0_RELEASE

FreeBSD-3.1

RELENG_3_0_0_RELEASE

FreeBSD-3.0

RELENG_2_2_8_RELEASE

FreeBSD-2.2.8

RELENG_2_2_7_RELEASE

FreeBSD-2.2.7

RELENG_2_2_6_RELEASE

FreeBSD-2.2.6

RELENG_2_2_5_RELEASE

FreeBSD-2.2.5

RELENG_2_2_2_RELEASE

FreeBSD-2.2.2

RELENG_2_2_1_RELEASE

FreeBSD-2.2.1

RELENG_2_2_0_RELEASE

FreeBSD-2.2.0

A.8 AFS 站点

FreeBSD 的AFS 服务器运行于下面的站点:

瑞典

文件的路径是: /afs/stacken.kth.se/ftp/pub/FreeBSD/

```
stacken.kth.se      # Stacken Computer Club, KTH, Sweden
130.237.234.43     #hot.stacken.kth.se
130.237.237.230    #fishburger.stacken.kth.se
130.237.234.3      #milko.stacken.kth.se
```

维护者<ftp@stacken.kth.se>

A.9 rsync 站点

下面的站点让FreeBSD 可以通过rsync 协议下载。**rsync** 实用程序和rcp(1) 的工作方式很相像，但是有更多的选项，使用rsync 远程更新协议只传输两份文件的不同之处，因此能够大幅度的提高网络同步速率。如果您是FreeBSD FTP 服务器或者CVS 仓库的镜像站点，这一点非常有用。**rsync** 套件可以工作在许多种操作系统上，在FreeBSD 上，查看net/rsync port 或者使用package。

捷克共和国

rsync://ftp.cz.FreeBSD.org/

可用的collection:

- ftp: FreeBSD FTP 服务器的部分镜像。
- FreeBSD: FreeBSD FTP 服务器的完整镜像。

德国

rsync://grappa.unix-ag.uni-kl.de/

可用的collection:

- freebsd-cvs: 完整的FreeBSD CVS 仓库。

这台服务器也镜像NetBSD 和OpenBSD 项目，还有其他的一些项目的CVS 仓库。

荷兰

rsync://ftp.nl.FreeBSD.org/

可用的collection:

- vol/4/freebsd-core: 对于FreeBSD FTP 服务器的完整镜像。

英国

rsync://rsync.mirror.ac.uk/

可用的collection:

- ftp.FreeBSD.org: FreeBSD FTP 服务器的完整镜像。

美国

`rsync://ftp-master.FreeBSD.org/`

服务器只供FreeBSD 主镜像站点使用。

可用的collection:

- FreeBSD: FreeBSD FTP 服务器的主要存档。
- acl: FreeBSD 主ACL 列表。

`rsync://ftp13.FreeBSD.org/`

可用的collection:

- FreeBSD: FreeBSD FTP 服务器的完整镜像。

附录B.

参考文献

尽管手册页能够提供对于FreeBSD 操作系统最为权威的参考资料，它们有时却不能告诉我们如何让整个系统很好地运转起来。因此，一本关于UNIX 系统管理的好书，以及一份好的用户手册是不可或缺的。

B.1 关于FreeBSD 的专业书籍与杂志

非英文的书籍和杂志：

- FreeBSD 入门与应用 (<http://jdli.tw.FreeBSD.org/publication/book/freebsd2/index.htm>) (繁体中文)。
- FreeBSD 技术内幕(中译本)，机械工业出版社 (<http://www.hzbook.com/>)。ISBN 7-111-10201-0。
- FreeBSD 使用大全第一版，机械工业出版社。ISBN 7-111-07482-3。
- FreeBSD 使用大全第二版，机械工业出版社。ISBN 7-111-10286-X。
- FreeBSD Handbook (第二版中译本)，人民邮电出版社 (<http://www.ptpress.com.cn/>)。ISBN 7-115-10541-3。
- FreeBSD 3.x Internet 高级服务器的架设与管理清华大学出版社 (<http://www.tup.tsinghua.edu.cn/>)。ISBN 7-900625-66-6。
- FreeBSD & Windows 集成组网实务，中国铁道出版社。ISBN 7-113-03845-X。
- FreeBSD 网站架设实务，中国铁道出版社。ISBN 7-113-03423-3。
- FreeBSD for PC 98'ers (日文，出版商：SHUWA System Co, LTD. ISBN 4-87966-468-5 C3055 P2900E)。
- FreeBSD (日文，出版商：CUTT. ISBN 4-906391-22-2 C3055 P2400E)。
- Complete Introduction to FreeBSD (<http://www.shoeisha.com/book/Detail.asp?bid=650>) (日文，出版商：Shoeisha Co., Ltd (<http://www.shoeisha.co.jp/>)). ISBN 4-88135-473-6 P3600E。
- Personal UNIX Starter Kit FreeBSD (<http://www.ascii.co.jp/pb/book1/shinkan/detail/1322785.html>) (日文，出版商：ASCII (<http://www.ascii.co.jp/>)). ISBN 4-7561-1733-3 P3000E。
- FreeBSD Handbook (日文译本，出版商：ASCII (<http://www.ascii.co.jp/>)). ISBN 4-7561-1580-2 P3800E。
- FreeBSD mit Methode (德文，出版商：Computer und Literatur Verlag (<http://www.cul.de/>)/Vertrieb Hanser, 1998. ISBN 3-932311-31-0。
- FreeBSD 4 - Installieren, Konfigurieren, Administrieren (<http://www.cul.de/freebsd.html>) (德文，出版商：Computer und Literatur Verlag (<http://www.cul.de/>), 2001. ISBN 3-932311-88-4。
- FreeBSD 5 - Installieren, Konfigurieren, Administrieren (<http://www.cul.de/freebsd.html>) (德文)，出版商：Computer und Literatur Verlag (<http://www.cul.de/>), 2003. ISBN 3-936546-06-1。
- FreeBSD de Luxe (<http://www.mitp.de/vmi/mitp/detail/pWert/1343/>) (德文)，出版商：Verlag Moderne Industrie (<http://www.mitp.de/>), 2003. ISBN 3-8266-1343-0。
- FreeBSD Install and Utilization Manual (<http://www.pc.mycom.co.jp/FreeBSD/install-manual.html>) (日文)，出版商：Mainichi Communications Inc. (<http://www.pc.mycom.co.jp/>)。
- Onno W Purbo, Dodi Maryanto, Syahrial Hubbany, Widjil Widodo **Building Internet Server with FreeBSD** (<http://maxwell.itb.ac.id/>) (印尼文)，出版商：Elex Media Komputindo (<http://www.elexmedia.co.id/>)。

英文版的书籍和杂志:

- Absolute BSD: The Ultimate Guide to FreeBSD (<http://www.AbsoluteBSD.com/>), 出版商: No Starch Press (<http://www.nostarch.com/>), 2002. ISBN: 1886411743
- The Complete FreeBSD (<http://www.freebsdmail.com/cgi-bin/fm/bsdcomp>), 出版商: O'Reilly (<http://www.oreilly.com/>), 2003. ISBN: 0596005164
- The FreeBSD Corporate Networker's Guide (<http://www.freebsd-corp-net-guide.com/>), 出版商: Addison-Wesley (<http://www.awl.com/awl/>), 2000. ISBN: 0201704811
- FreeBSD: An Open-Source Operating System for Your Personal Computer (<http://andrsn.stanford.edu/FreeBSD/introbook/>), 出版商: The Bit Tree Press, 2001. ISBN: 0971204500
- Teach Yourself FreeBSD in 24 Hours, 出版商: Sams (<http://www.sampublishing.com/>), 2002. ISBN: 0672324245
- FreeBSD unleashed, 出版商: Sams (<http://www.sampublishing.com/>), 2002. ISBN: 0672324563
- FreeBSD: The Complete Reference, 出版商: McGrawHill (<http://books.mcgraw-hill.com>), 2003. ISBN: 0072224096

B.2 用户指南

- Computer Systems Research Group, UC Berkeley. **4.4BSD User's Reference Manual**. O'Reilly & Associates, Inc., 1994. ISBN 1-56592-075-9
- Computer Systems Research Group, UC Berkeley. **4.4BSD User's Supplementary Documents**. O'Reilly & Associates, Inc., 1994. ISBN 1-56592-076-7
- **UNIX in a Nutshell**. O'Reilly & Associates, Inc., 1990. ISBN 093717520X
- Mui, Linda. **What You Need To Know When You Can't Find Your UNIX System Administrator**. O'Reilly & Associates, Inc., 1995. ISBN 1-56592-104-6
- Ohio State University (<http://www-wks.acs.ohio-state.edu/>) 编写了一份UNIX 介绍性课程 (http://www-wks.acs.ohio-state.edu/unix_course/unix.html), 并提供在线的HTML 和PostScript 版本。
- 这份文档的意大利文翻译 (http://www.FreeBSD.org/doc/it_IT.ISO8859-15/books/unix-introduction/index.html) 是FreeBSD Italian Documentation Project 的一部分。
- Jpman Project, Japan FreeBSD Users Group (<http://www.jp.FreeBSD.org/>). FreeBSD User's Reference Manual (<http://www.pc.mycom.co.jp/FreeBSD/urm.html>) (日文译本). Mainichi Communications Inc. (<http://www.pc.mycom.co.jp/>), 1998. ISBN4-8399-0088-4 P3800E.
- Edinburgh University (<http://www.ed.ac.uk/>) has written an Online Guide (<http://unixhelp.ed.ac.uk/>) for newcomers to the UNIX environment.

B.3 管理员指南

- Albitz, Paul and Liu, Cricket. **DNS and BIND**, 4th Ed. O'Reilly & Associates, Inc., 2001. ISBN 1-59600-158-4

- Computer Systems Research Group, UC Berkeley. **4.4BSD System Manager's Manual**. O'Reilly & Associates, Inc., 1994. ISBN 1-56592-080-5
- Costales, Brian, et al. **Sendmail**, 2nd Ed. O'Reilly & Associates, Inc., 1997. ISBN 1-56592-222-0
- Frisch, Aileen. **Essential System Administration**, 2nd Ed. O'Reilly & Associates, Inc., 1995. ISBN 1-56592-127-5
- Hunt, Craig. **TCP/IP Network Administration**, 2nd Ed. O'Reilly & Associates, Inc., 1997. ISBN 1-56592-322-7
- Nemeth, Evi. **UNIX System Administration Handbook**. 3rd Ed. Prentice Hall, 2000. ISBN 0-13-020601-6
- Stern, Hal **Managing NFS and NIS** O'Reilly & Associates, Inc., 1991. ISBN 0-937175-75-7
- Jpman Project, Japan FreeBSD Users Group (<http://www.jp.FreeBSD.org/>). FreeBSD System Administrator's Manual (<http://www.pc.mycom.co.jp/FreeBSD/sam.html>) (日文译本). Mainichi Communications Inc. (<http://www.pc.mycom.co.jp/>), 1998. ISBN4-8399-0109-0 P3300E.
- Dreyfus, Emmanuel. Cahiers de l'Admin: BSD (<http://www.eyrolles.com/Informatique/Livre/9782212114638/>) 2nd Ed. (in French), Eyrolles, 2004. ISBN 2-212-11463-X

B.4 开发指南

- Asente, Paul, Converse, Diana, and Swick, Ralph. **X Window System Toolkit**. Digital Press, 1998. ISBN 1-55558-178-1
- Computer Systems Research Group, UC Berkeley. **4.4BSD Programmer's Reference Manual**. O'Reilly & Associates, Inc., 1994. ISBN 1-56592-078-3
- Computer Systems Research Group, UC Berkeley. **4.4BSD Programmer's Supplementary Documents**. O'Reilly & Associates, Inc., 1994. ISBN 1-56592-079-1
- Harbison, Samuel P. and Steele, Guy L. Jr. **C: A Reference Manual**. 4th ed. Prentice Hall, 1995. ISBN 0-13-326224-3
- Kernighan, Brian and Dennis M. Ritchie. **The C Programming Language**. 2nd Ed. PTR Prentice Hall, 1988. ISBN 0-13-110362-8
- Lehey, Greg. **Porting UNIX Software**. O'Reilly & Associates, Inc., 1995. ISBN 1-56592-126-7
- Plauger, P. J. **The Standard C Library**. Prentice Hall, 1992. ISBN 0-13-131509-9
- Spinellis, Diomidis. **Code Reading: The Open Source Perspective** (<http://www.spinellis.gr/codereading/>). Addison-Wesley, 2003. ISBN 0-201-79940-5
- Stevens, W. Richard. **Advanced Programming in the UNIX Environment**. Reading, Mass. : Addison-Wesley, 1992. ISBN 0-201-56317-7
- Stevens, W. Richard. **UNIX Network Programming**. 2nd Ed, PTR Prentice Hall, 1998. ISBN 0-13-490012-X
- Wells, Bill. "Writing Serial Drivers for UNIX" . **Dr. Dobbs's Journal**. 19(15), December 1994. pp68-71, 97-99.

B.5 操作系统原理

- Andleigh, Prabhat K. **UNIX System Architecture**. Prentice-Hall, Inc., 1990. ISBN 0-13-949843-5
 - Jolitz, William. “Porting UNIX to the 386” . **Dr. Dobb’s Journal**. 1991年1月 - 1992年6月
 - Leffler, Samuel J., Marshall Kirk McKusick, Michael J Karels and John Quarterman **The Design and Implementation of the 4.3BSD UNIX Operating System**. Reading, Mass. : Addison-Wesley, 1989. ISBN 0-201-06196-1
 - Leffler, Samuel J., Marshall Kirk McKusick, **The Design and Implementation of the 4.3BSD UNIX Operating System: Answer Book**. Reading, Mass. : Addison-Wesley, 1991. ISBN 0-201-54629-9
 - McKusick, Marshall Kirk, Keith Bostic, Michael J Karels, and John Quarterman. **The Design and Implementation of the 4.4BSD Operating System**. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-54979-4
- (这本书的第二章的在线版本 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/design-44bsd/book.html) 是FreeBSD Documentation Project 的一部分, 另外, 第九章可以在 [这里](http://www.netapp.com/tech_library/nfsbook.html) (http://www.netapp.com/tech_library/nfsbook.html) 找到。)
- Marshall Kirk McKusick, George V. Neville-Neil **The Design and Implementation of the FreeBSD Operating System**. Boston, Mass. : Addison-Wesley, 2004. ISBN 0-201-70245-2
 - Stevens, W. Richard. **TCP/IP Illustrated, Volume 1: The Protocols**. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-63346-9
 - Schimmel, Curt. **Unix Systems for Modern Architectures**. Reading, Mass. : Addison-Wesley, 1994. ISBN 0-201-63338-8
 - Stevens, W. Richard. **TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP and the UNIX Domain Protocols**. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-63495-3
 - Vahalia, Uresh. **UNIX Internals -- The New Frontiers**. Prentice Hall, 1996. ISBN 0-13-101908-2
 - Wright, Gary R. and W. Richard Stevens. **TCP/IP Illustrated, Volume 2: The Implementation**. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-63354-X

B.6 信息安全方面的参考文献

- Cheswick, William R. and Steven M. Bellovin. **Firewalls and Internet Security: Repelling the Wily Hacker**. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-63357-4
- Garfinkel, Simson and Gene Spafford. **Practical UNIX & Internet Security**. 2nd Ed. O’Reilly & Associates, Inc., 1996. ISBN 1-56592-148-8
- Garfinkel, Simson. **PGP Pretty Good Privacy** O’Reilly & Associates, Inc., 1995. ISBN 1-56592-098-8

B.7 硬件参考

- Anderson, Don and Tom Shanley. **Pentium Processor System Architecture**. 2nd Ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40992-5
- Ferraro, Richard F. **Programmer's Guide to the EGA, VGA, and Super VGA Cards**. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-62490-7
- Intel 公司在他们的开发人员网站 (<http://developer.intel.com/>)上, 提供了关于他们的CPU, 芯片组, 以及标准的文档。多数是PDF文件。
- Shanley, Tom. **80486 System Architecture**. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40994-1
- Shanley, Tom. **ISA System Architecture**. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40996-8
- Shanley, Tom. **PCI System Architecture**. 4th ed. Reading, Mass. : Addison-Wesley, 1999. ISBN 0-201-30974-2
- Van Gilluwe, Frank. **The Undocumented PC**, 2nd Ed. Reading, Mass: Addison-Wesley Pub. Co., 1996. ISBN 0-201-47950-8
- Messmer, Hans-Peter. **The Indispensable PC Hardware Book**, 4th Ed. Reading, Mass: Addison-Wesley Pub. Co., 2002. ISBN 0-201-59616-4

B.8 UNIX 历史

- Lion, John **Lion's Commentary on UNIX, 6th Ed. With Source Code**. ITP Media Group, 1996. ISBN 1573980137
- Raymond, Eric S. **The New Hacker's Dictionary, 3rd edition**. MIT Press, 1996. ISBN 0-262-68092-0. 它也被称作Jargon File (<http://www.catb.org/~esr/jargon/html/index.html>)
- Salus, Peter H. **A quarter century of UNIX**. Addison-Wesley Publishing Company, Inc., 1994. ISBN 0-201-54777-5
- Simon Garfinkel, Daniel Weise, Steven Strassmann. **The UNIX-HATERS Handbook**. IDG Books Worldwide, Inc., 1994. ISBN 1-56884-203-1. Out of print, but available online (<http://research.microsoft.com/~daniel/unix-haters.html>).
- Don Libes, Sandy Ressler **Life with UNIX** ——special edition. Prentice-Hall, Inc., 1989. ISBN 0-13-536657-7
- **BSD 族谱**. <http://www.FreeBSD.org/cgi/cvsweb.cgi/src/share/misc/bsd-family-tree> 或在FreeBSD 机器上的/usr/share/misc/bsd-family-tree。
- **The BSD Release Announcements collection**. 1997. <http://www.de.FreeBSD.org/de/ftp/releases/>
- **Networked Computer Science Technical Reports Library**. <http://www.ncstrl.org/>
- **Old BSD releases from the Computer Systems Research group (CSRG)**. <http://www.mckusick.com/csrg/>: The 4CD set covers all BSD versions from 1BSD to 4.4BSD and 4.4BSD-Lite2 (but not 2.11BSD, unfortunately). The last disk also holds the final sources plus the SCCS files.

B.9 各种期刊

- **The C/C++ Users Journal**. R&D Publications Inc. ISSN 1075-2838
- **Sys Admin** —— **The Journal for UNIX System Administrators** Miller Freeman, Inc., ISSN 1061-2688
- **freeX** —— **Das Magazin für Linux - BSD - UNIX** (德文) Computer- und Literaturverlag GmbH, ISSN 1436-7033

附录C.

Internet上的资源

发展迅猛的FreeBSD使得现有的印刷、平面媒体跟不上它的发展进度！而电子版的也许是最好的，通常是唯一一个可以跟上最新发展方向的。FreeBSD来自于志愿者的成果，用户社区通常也扮演着是“技术支持部门”的角色。通过电子邮件和USENET新闻组可以很快的找到他们。

以下列出了尽量多的联系FreeBSD用户社区的方式。如果您发现有其他的资源没有被包括在这儿，请告诉FreeBSD 文档计划邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-doc>)，以便将它们加入到这里。

C.1 邮件列表

虽然大部分的FreeBSD开发人员都会阅读USENET，如果您只将问题发表在comp.unix.bsd.freebsd.* 其中之一的讨论组上，我们也不能保证我们永远可以及时了解您的问题。如果您将问题发到适当的邮件列表上，您不但可以同时让FreeBSD研发人员和其他的读者看到，通常也可以得到一个较好的（至少会比较快）的回应。

本文的最后给出了各个不同的邮件列表的使用规则。在订阅其中任何一个列表之前，请先阅读使用条文。现在订阅这些邮件列表的人每天都会收到上百封关于FreeBSD的信件。设立列表的使用条文有助于维护讨论质量。否则这些讨论计划的列表将失去其意义。

如果不知道哪个邮件列表适合于发送您的问题，请参见如何从FreeBSD-questions 邮件列表中更快地得到答案 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/freebsd-questions)。

在列表中发送任何问题之前，请首先学习使用邮件列表的最佳方式，例如如何通过阅读 邮件列表常见问题回答集 (http://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/mailling-list-faq) (FAQ) 文档，来避免经常重复的讨论。

全部的邮件列表记录都可以在FreeBSD World Wide Web服务器 (<http://www.FreeBSD.org/search/index.html>)上找到。此服务器提供了很棒的关键词搜寻功能，可让您找到FAQ的解答。而在邮件列表上提问之前，请先搜寻是否已有答案。

C.1.1 列表摘要

一般性的列表: 以下的列表都是一般性的，而且可以自由地加入，鼓励大家加入他们:

目录	用途
cvs-all (http://lists.FreeBSD.org/mailman/listinfo/cvs-all)	FreeBSD源代码的变动
freebsd-advocacy (http://lists.FreeBSD.org/mailman/listinfo/freebsd-advocacy)	FreeBSD鼓吹者
freebsd-announce (http://lists.FreeBSD.org/mailman/listinfo/freebsd-announce)	重要的事件和里程碑

目录	用途
freebsd-arch (http://lists.FreeBSD.org/mailman/listinfo/freebsd-arch)	架构和设计的讨论
freebsd-bugbusters (http://lists.FreeBSD.org/mailman/listinfo/freebsd-bugbusters)	与FreeBSD问题报告数据库和有关工具维护相关的讨论
freebsd-bugs (http://lists.FreeBSD.org/mailman/listinfo/freebsd-bugs)	报告FreeBSD的Bug
freebsd-chat (http://lists.FreeBSD.org/mailman/listinfo/freebsd-chat)	和技术无关的FreeBSD讨论区
freebsd-current (http://lists.FreeBSD.org/mailman/listinfo/freebsd-current)	讨论使用FreeBSD-CURRENT 有关的一些问题
freebsd-isp (http://lists.FreeBSD.org/mailman/listinfo/freebsd-isp)	ISP使用FreeBSD的讨论
freebsd-jobs (http://lists.FreeBSD.org/mailman/listinfo/freebsd-jobs)	与FreeBSD有关的工作机会
freebsd-policy (http://lists.FreeBSD.org/mailman/listinfo/freebsd-policy)	FreeBSD核心团队方针讨论。低流量并且只读的
freebsd-questions (http://lists.FreeBSD.org/mailman/listinfo/freebsd-questions)	用户问题和技术支持
freebsd-security-notifications (http://lists.FreeBSD.org/mailman/listinfo/freebsd-security-notifications)	安全通知
freebsd-stable (http://lists.FreeBSD.org/mailman/listinfo/freebsd-stable)	讨论使用FreeBSD-STABLE 有关的一些问题
freebsd-test (http://lists.FreeBSD.org/mailman/listinfo/freebsd-test)	在真正发送一个邮件到邮件列表之前可以先发送到这里测试

技术性的邮件列表: 以下的邮件列表是用来讨论技术性问题的。在加入订阅及讨论之前请务必认真阅读每个列表主题，因为他们讨论的内容都是严格地被限制着的。

目录	用途
freebsd-acpi (http://lists.FreeBSD.org/mailman/listinfo/freebsd-acpi)	ACPI 和电源管理的开发
freebsd-afs (http://lists.FreeBSD.org/mailman/listinfo/freebsd-afs)	将AFS 移植到FreeBSD
freebsd-aic7xxx (http://lists.FreeBSD.org/mailman/listinfo/aic7xxx)	为Adaptec AIC 7xxx 开发驱动

目录	用途
freebsd-alpha (http://lists.FreeBSD.org/mailman/listinfo/freebsd-alpha)	将FreeBSD 移植到Alpha 工作站
freebsd-amd64 (http://lists.FreeBSD.org/mailman/listinfo/freebsd-amd64)	将FreeBSD 移植到AMD64 系统
freebsd-apache (http://lists.FreeBSD.org/mailman/listinfo/freebsd-apache)	关于与 Apache 有关的ports 的讨论
freebsd-arm (http://lists.FreeBSD.org/mailman/listinfo/freebsd-arm)	将FreeBSD 移植到ARM® 处理器
freebsd-atm (http://lists.FreeBSD.org/mailman/listinfo/freebsd-atm)	在FreeBSD 上使用ATM 网络
freebsd-audit (http://lists.FreeBSD.org/mailman/listinfo/freebsd-audit)	源代码审核
freebsd-binup (http://lists.FreeBSD.org/mailman/listinfo/freebsd-binup)	二进制更新系统的设计和开发
freebsd-bluetooth (http://lists.FreeBSD.org/mailman/listinfo/freebsd-bluetooth)	在FreeBSD 上使用Bluetooth 技术
freebsd-cluster (http://lists.FreeBSD.org/mailman/listinfo/freebsd-cluster)	在集群环境中使用FreeBSD
freebsd-cvswb (http://lists.FreeBSD.org/mailman/listinfo/freebsd-cvswb)	CVSweb 维护
freebsd-database (http://lists.FreeBSD.org/mailman/listinfo/freebsd-database)	讨论FreeBSD 下开发和使用数据库
freebsd-doc (http://lists.FreeBSD.org/mailman/listinfo/freebsd-doc)	创建FreeBSD 相关文档
freebsd-drivers (http://lists.FreeBSD.org/mailman/listinfo/freebsd-drivers)	为FreeBSD 撰写驱动
freebsd-eclipse (http://lists.FreeBSD.org/mailman/listinfo/freebsd-eclipse)	FreeBSD 上的Eclipse IDE、工具、富客户应用，以及ports 的用户讨论。

目录	用途
freebsd-emulation (http://lists.FreeBSD.org/mailman/listinfo/freebsd-emulation)	在FreeBSD 上模拟其它系统, 如Linux/MS-DOS/Windows
freebsd-firewire (http://lists.FreeBSD.org/mailman/listinfo/freebsd-firewire)	FreeBSD 的FireWire® (iLink, IEEE 1394) 技术讨论
freebsd-fs (http://lists.FreeBSD.org/mailman/listinfo/freebsd-fs)	文件系统
freebsd-geom (http://lists.FreeBSD.org/mailman/listinfo/freebsd-geom)	针对GEOM 的讨论和实现
freebsd-gnome (http://lists.FreeBSD.org/mailman/listinfo/freebsd-gnome)	移植 GNOME 和 GNOME 应用程序
freebsd-hackers (http://lists.FreeBSD.org/mailman/listinfo/freebsd-hackers)	一般性的技术讨论
freebsd-hardware (http://lists.FreeBSD.org/mailman/listinfo/freebsd-hardware)	一般性的支持FreeBSD 的硬件的讨论
freebsd-i18n (http://lists.FreeBSD.org/mailman/listinfo/freebsd-i18n)	FreeBSD 的国际化
freebsd-ia32 (http://lists.FreeBSD.org/mailman/listinfo/freebsd-ia32)	在IA-32 (Intel x86) 平台上运行FreeBSD
freebsd-ia64 (http://lists.FreeBSD.org/mailman/listinfo/freebsd-ia64)	将FreeBSD 移植到Intel 即将推出的IA64 系统
freebsd-ipfw (http://lists.FreeBSD.org/mailman/listinfo/freebsd-ipfw)	关于IP 防火墙代码再设计的技术性讨论
freebsd-isdn (http://lists.FreeBSD.org/mailman/listinfo/freebsd-isdn)	ISDN开发人员
freebsd-java (http://lists.FreeBSD.org/mailman/listinfo/freebsd-java)	Java 开发人员以及移植JDKs 到FreeBSD 的人们
freebsd-kde (http://freebsd.kde.org/mailman/listinfo/kde-freebsd)	移植 KDE 和 KDE 应用程序
freebsd-lfs (http://lists.FreeBSD.org/mailman/listinfo/freebsd-lfs)	移植LFS 到FreeBSD上
freebsd-libh (http://lists.FreeBSD.org/mailman/listinfo/freebsd-libh)	第二代的安装和package 系统
freebsd-mips (http://lists.FreeBSD.org/mailman/listinfo/freebsd-mips)	移植FreeBSD 到MIPS®

目录

freebsd-mobile
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-mobile>)

freebsd-mozilla
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-mozilla>)

freebsd-multimedia
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-multimedia>)

freebsd-new-bus
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-new-bus>)

freebsd-net
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-net>)

freebsd-openoffice
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-openoffice>)

freebsd-performance
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-performance>)

freebsd-perl
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-perl>)

freebsd-pf
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-pf>)

freebsd-platforms
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-platforms>)

freebsd-ports
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ports>)

freebsd-ports-bugs
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ports-bugs>)

freebsd-ppc
 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ppc>)

用途

关于便携式计算机的讨论

移植**Mozilla** 到FreeBSD 上

多媒体应用程序

技术讨论关于总线架构

网络子系统和TCP/IP 源代码的讨论

移植**OpenOffice.org** 和**StarOffice** 到FreeBSD 上

高性能、负载下安装后的性能调整问题

许多与perl 相关的ports 的维护

关于packet filter 防火墙系统的讨论

关于向非Intel 架构的平台上移植的讨论

关于Ports Collection 的讨论

ports bugs/PRs讨论

移植FreeBSD 到PowerPC®

目录

freebsd-proliant
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-proliant>)

freebsd-python
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-python>)

freebsd-qa
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-qa>)

freebsd-rc
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-rc>)

freebsd-realtime
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-realtime>)

freebsd-scsi
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-scsi>)

freebsd-security
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-security>)

freebsd-small
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-small>)

freebsd-smp
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-smp>)

freebsd-sparc64
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-sparc64>)

freebsd-standards
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-standards>)

freebsd-threads
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-threads>)

freebsd-testing
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-testing>)

freebsd-tokenring
(<http://lists.FreeBSD.org/mailman/listinfo/freebsd-tokenring>)

用途

关于FreeBSD 在HP ProLiant 服务器平台上的技术讨论

FreeBSD 专属的Python 问题

质量保证(QA)讨论, 通常在未发布之前

关于rc.d 系统及其开发的讨论

FreeBSD 实时扩展的开发

SCSI 子系统

系统安全

在嵌入式系统上使用FreeBSD

有关对称多处理器的设计讨论

移植FreeBSD 到Sparc® 系统

让FreeBSD 顺应C99 以及POSIX 标准

线程

FreeBSD 性能和稳定性测试

在FreeBSD 中支持Token Ring

目录	用途
freebsd-usb (http://lists.FreeBSD.org/mailman/listinfo/freebsd-usb)	关于FreeBSD 的USB 支持的讨论
freebsd-vuxml (http://lists.FreeBSD.org/mailman/listinfo/freebsd-vuxml)	关于VuXML 的问题讨论
freebsd-x11 (http://lists.FreeBSD.org/mailman/listinfo/freebsd-x11)	维护和支持在FreeBSD 上运行的X11

限制订阅的列表: 以下的列表是针对某些特定的读者而设的, 而且并不适合被当成是一般公开讨论区。您最好在某一技术讨论区参与讨论后再选择订阅这些限制订阅的邮件列表, 因为这样您可以了解到在这些讨论区发言所需要的礼仪。

目录	用途
freebsd-hubs (http://lists.FreeBSD.org/mailman/listinfo/freebsd-hubs)	运行镜像站点的成员(支持基本服务)
freebsd-user-groups (http://lists.FreeBSD.org/mailman/listinfo/freebsd-user-groups)	用户组调整
freebsd-vendors (http://lists.FreeBSD.org/mailman/listinfo/freebsd-vendors)	商家在发布之前的调整
freebsd-www (http://lists.FreeBSD.org/mailman/listinfo/freebsd-www)	www.FreeBSD.org (http://www.FreeBSD.org/index.html)的维护

分类列表: 所有以上的列表在一个分类格式里面是可利用的。一旦订阅了一个列表, 您可以在您的账号选项里面设置您的分类选项。

CVS列表: 以下的邮件是给对FreeBSD源代码的变更记录有兴趣的人看的, 而且它们是只读的邮件列表, 您不能发Email给他们。

列表	源位置	描述
cvs-all (http://lists.FreeBSD.org/mailman/listinfo/cvs-all)	/usr/(CVSROOT doc ports project src)	所有对源代码的改变纪录(其他CVS commit 列表的超集)
cvs-doc (http://lists.FreeBSD.org/mailman/listinfo/cvs-doc)	/usr/(doc www)	所有对doc 和www 源代码的改变纪录
cvs-ports (http://lists.FreeBSD.org/mailman/listinfo/cvs-ports)	/usr/ports	所有对ports 源代码的改变纪录

列表	源位置	描述
cvs-projects (http://lists.FreeBSD.org/mailman/listinfo/cvs-projects)	/usr/projects	所有对projects 源代码的改变记录
cvs-src (http://lists.FreeBSD.org/mailman/listinfo/cvs-src)	/usr/src	所有对src 源代码的改变记录

C.1.2 如何订阅

订阅一个列表，点击上面的列表名字或到<http://lists.FreeBSD.org/mailman/listinfo> 并点击进入您感兴趣的列表，这个列表的页面包含了所必需的订阅操作指南。

其实您只需发送邮件到<列表名@FreeBSD.org>。它将被再次转发到全世界的这个邮件列表的成员。

点击上面的URL，在列表的底部可以从订阅的列表中退出。也可以发送一个电子邮件到<列表名-unsubscribe@FreeBSD.org> 来退订。

此外，我们要求您必须保持在技术性的邮件列表中只是讨论技术。如果您只是对一些重要的公告感兴趣，建议您加入FreeBSD 公告邮件列表 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-announce>)，它的通信量比较低。

C.1.3 列表规章

所有 FreeBSD 的邮件列表都有同样的基本规则，所有人必须按照规则来做。违反这些规则时，FreeBSD Postmaster <postmaster@FreeBSD.org> 会在前两次发送警告，如果第三次违反，FreeBSD Postmaster 将从所有FreeBSD 的邮件列表中删除这样的人，并过滤来自发信人之后的所有邮件。我们很遗憾必须要遵守这样的规则，但今天的互联网是一个很混乱的环境，它上面的很多约束机制，都相当脆弱。

具体规则：

- 任何发表的主题都应当附合基本的列表概况。例如，如果列表是有关技术问题的，那您发表的文章包含技术讨论。不要把不相关的讨论放在一起。对于没有主题的自由形式的讨论，可以使用FreeBSD-chat <freebsd-chat@FreeBSD.org>。
- 不要将同一个问题发送到超过两个的邮件列表上，当有一个清晰和明显的必须要发表到两个列表的要求时，也只能是两个。对于大多数的列表，已经有相当多的订户了，除了一些比较深奥的问题(如“-stable & -scsi”)，没有必要同时将一个问题发到多个列表上。如果一个信息以这种方式（多个邮件列表在Cc行出现）被发送给您，那Cc行在把它再发送出去之前也将被整理。无论谁是最初发表者，都会导致您自己的交叉发送。
- 不容许进行人身攻击和亵渎（在前后的争论中），包括用户和开发人员。应当遵守最起码的网络礼节，象需要征得同意才可以引用或张贴私人邮件等。然而，也有非常少的情况下，这样的内容会符合列表规章，因此，它会在最初给予警告（或禁止）。
- 严格的禁止非FreeBSD相关产品或服务的广告，一旦发现将马上取缔。

单独的列表规章：

freebsd-acpi (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-acpi>)

ACPI和电源管理开发

freebsd-afs (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-afs>)

Andrew文件系统

这个列表是用来讨论porting和从CMU/Transarc使用AFS。

freebsd-announce (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-announce>)

重要事件/里程碑

这是一个发布FreeBSD重大事件的邮件列表。这包括有关snapshots和其他版本的公告，新的FreeBSD的性能的公告，还可以用于指派志愿者等等。这个列表比较小。

freebsd-arch (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-arch>)

架构和设计讨论

这个列表是讨论FreeBSD的架构。本质上应保证内容的纯技术性。例如主题是：

- 如何重新创建系统使其同时有几个自己构造的系统运行。
- 需要什么才能修复VFS来使Heidemann层工作。
- 我们怎么改变设备驱动程序接口以便能够在多种总线和体系结构上使用同样的驱动程序。
- 如何写一个网络驱动。

freebsd-audit (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-audit>)

源代码审核计划

这个针对FreeBSD源代码审核计划的邮件列表，虽然这最初是针对安全方面代码修正的讨论，现在它已经扩展到任何代码修正的讨论。

这个列表涉及补丁方面的问题比较多，可能普通的FreeBSD用户对此不感兴趣。不与一个特定的代码修正相关的安全讨论将放在freebsd-security中。相反的，所有的开发人员都被鼓励把他们的补丁发到这儿来，特别是如果他们发现有一个错误可能会影响系统的完整性时。

freebsd-binup (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-binup>)

FreeBSD二进制升级计划

这个列表主要是讨论二进制升级binup系统。设计问题，执行细节，补丁，错误报告，状态报告，特性要求，提交日志，和所有其他与binup相关的东西都可以。

freebsd-bluetooth (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-bluetooth>)

FreeBSD 上的Bluetooth

这是一个FreeBSD的Bluetooth用户聚集的讨论区。这里欢迎关于设计问题、实现细节、补丁、问题报告、开发进度报告，功能需求以及其他与Bluetooth相关的讨论。

freebsd-bugbusters (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-bugbusters>)

同等问题报告处理结果

这个列表的目的是作为一个调整和讨论论坛来服务于Bug列表的成员，Bugbuster列表成员和其他任何的对PR数据库真正的有兴趣的成员。这个列表不是为了讨论关于Bug细节，补丁或PRs。

freebsd-bugs (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-bugs>)

Bug报告

这是一个报告FreeBSD的Bug的邮件列表。可以随时通过send-pr(1) 命令或WEB页面 (<http://www.FreeBSD.org/send-pr.html>)来提交Bug。

freebsd-chat (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-chat>)

与FreeBSD社区相关的非技术性项目

这个列表超出了其他有关非技术、社会信息的内容。包括谈论Jordan看起来是否像一个机敏的侦探，是否句首的字母要大写，谁喝了很多咖啡，哪儿的啤酒酿造的最好，谁在他们的地下室里酿造了啤酒等等。对于偶然宣布重大的事件（例如：将要举行的聚会，婚礼，生日，新工作等等）也能使用这种技术列表，除上述列举之外任何事情都可以发布在-chat列表上。

freebsd-core

FreeBSD核心团队

这是一个只供核心成员内部使用的邮件列表，只有当一个与FreeBSD相关的严重的事情需要裁决或严格审核时，才能发送消息到这个邮件列表。

freebsd-current (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-current>)

关于使用FreeBSD-CURRENT版的讨论

这是一个针对FreeBSD-CURRENT用户的邮件列表。它包括一些可能影响用户的新特性的警告，使用FreeBSD-current的一些指导。任何运行“CURRENT”的人必须同意这个列表，这是一个纯技术的邮件列表。

freebsd-cvsweb (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-cvsweb>)

FreeBSD CVSweb计划

关于FreeBSD-CVSweb的使用，开发和维护的技术性讨论。

freebsd-doc (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-doc>)

文档计划

这个邮件列表是与FreeBSD创建的文档的出版和计划的讨论。这个邮件列表的成员都会提交到“The FreeBSD Documentation Project”。它是一个开放的列表，可以自由地加入和做贡献！

freebsd-drivers (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-drivers>)

为FreeBSD 撰写设备驱动

这是关于FreeBSD 上的设备驱动的技术论坛。它主要供编写设备驱动的开发人员提出关于如何使用FreeBSD 内核提供的API 来编写设备驱动程序的问题。

freebsd-eclipse (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-eclipse>)

FreeBSD 上的Eclipse IDE、工具、富客户应用，以及ports 的用户讨论。

这个邮件列表的目的，是为在FreeBSD 平台上选择、安装、使用、开发和维护Eclipse IDE、工具、富客户应用的用户，提供互助式支持，以及为将Eclipse IDE 和插件移植到FreeBSD 环境中提供帮助。

另一个目的是建立一个在Eclipse 社区和FreeBSD 社区之间的交流管道，以达到互惠互利。

尽管这个列表主要关注的是Eclipse 用户的诉求，它也为使用Eclipse 框架开发FreeBSD 专用的应用提供了论坛。

freebsd-emulation (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-emulation>)

模拟其他系统，例如Linux/MS-DOS/Windows

这是一个讨论关于如何在FreeBSD 上运行为其他操作系统所撰写的程序的论坛。

freebsd-firewire (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-firewire>)

FireWire (iLink, IEEE 1394)

这个邮件列表是关于FreeBSD子系统FireWire (aka IEEE 1394 aka iLink)的设计和执行。相关特定的主题包括标准，总线设计和他们的协议，适配器板/卡/芯片设置，及他们的正确的代码的结构和实施。

freebsd-fs (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-fs>)

文件系统

关于FreeBSD文件系统的讨论。这是一个纯技术的邮件列表。

freebsd-geom (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-geom>)

GEOM

针对GEOM和相关执行的讨论。这是一个纯技术的邮件列表。

freebsd-gnome (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-gnome>)

GNOME

讨论关于在FreeBSD系统上的GNOME桌面环境这是一个纯技术的邮件列表。

freebsd-ipfw (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ipfw>)

IP防火墙

这是关于在FreeBSD里重新设计IP防火墙代码的技术讨论论坛。

freebsd-ia64 (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ia64>)

移植FreeBSD到IA64

这是一个有关将FreeBSD移植到Intel IA64架构上的技术讨论列表，讨论一些相关的问题与解决方案。也欢迎对这些问题感兴趣的个别讨论者。

freebsd-isdn (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-isdn>)

ISDN通信

这是一个FreeBSD支持的ISDN系统开发的邮件列表。

freebsd-java (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-java>)

Java开发

这是一个讨论Java 应用开发和JDKs的porting与维护的邮件列表。

freebsd-jobs (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-jobs>)

工作的提供和寻找

这个论坛是针对与FreeBSD 相关的雇佣信息和个人简历，比如：如果您想找一个与FreeBSD 相关的工作或有一个工作需要FreeBSD 这是一个让您来广告的好地方。这不是对一般性雇佣问题的邮件列表，对这个问题已经有了足够多的论坛。

注意这个列表，像其他的FreeBSD.org 邮件列表一样是会分发给全世界的订阅者的。因此，您需要明白关于位置和地域问题，确定之间是容易联系和可合作的。

Email最好应该使用——纯文本格式，不过基本的PDF,HTML和很少其他的能被更多读者接受的格式也是可以的。Microsoft Word (.doc) 格式是被邮件列表服务器拒绝的。

freebsd-kde (<http://freebsd.kde.org/mailman/listinfo/kde-freebsd>)

KDE

讨论关于在FreeBSD系统上使用KDE。这是一个纯技术的邮件列表。

freebsd-hackers (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-hackers>)

技术讨论

这是一个与FreeBSD相关的技术讨论论坛，是一个主要的技术性邮件列表。他是针对个别的工作在FreeBSD上的人来提出问题或讨论相关的解决方案, 也欢迎对这些问题感兴趣的个别的讨论者。这是一个纯技术的邮件列表。

freebsd-hardware (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-hardware>)

FreeBSD硬件的普通讨论

有关FreeBSD运行的硬件类型的普通讨论，包括是否该买的一些问题和建议。

freebsd-hubs (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-hubs>)

镜象站点

人们运行FreeBSD的镜象站点的公告和讨论。

freebsd-isp (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-isp>)

ISP供应商问题

这是一个讨论使用FreeBSD的ISP供应商的邮件列表。这是一个纯技术的邮件列表。

freebsd-openoffice (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-openoffice>)

OpenOffice.org

关于OpenOffice.org和StarOffice. 的移植和维护。

freebsd-performance (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-performance>)

讨论关于调整及高速运行FreeBSD

这个邮件列表提供了一个为黑客，管理员和有关的团体去讨论与FreeBSD性能相关的主题的空间。可以在这里进行讨论的包括在任意高负载下，体验版下或者是有限制的条件下安装FreeBSD。非常鼓励自愿地为了改进FreeBSD性能的相关团体去订阅这个列表。这是个高技术含量的列表理论上说适合有丰富经

验的FreeBSD用户，黑客，或对FreeBSD的速度、性能、升级感兴趣的管理员。这不是一个问答式的列表，关于这些应该去读相关文档，但他是一个可以投稿的地方，或者了解关于待解决的与性能相关的主题。

freebsd-pf (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-pf>)

关于**packet filter** 防火墙系统的问题和讨论

关于FreeBSD 环境下packet filter (pf) 防火墙系统的讨论。这里欢迎技术讨论，以及一般的应用问题。此外，这里也是讨论ALTQ QoS 框架的合适场所。

freebsd-platforms (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-platforms>)

移植到非**Intel** 平台上

跨平台的FreeBSD 问题，关于非Intel FreeBSD 移植版本的讨论和提议。这是一个纯技术性的邮件列表，其讨论内容严格限制为技术。

freebsd-policy (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-policy>)

核心团队策略的决定

这是一个很小的只读的有关核心团队策略决定的邮件列表。

freebsd-ports (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ports>)

“**ports**” 的讨论

关于FreeBSD的“ports collection” (/usr/ports)的讨论, ports的基础构造和调整过的ports结构。这是一个纯技术的邮件列表。

freebsd-ports-bugs (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-ports-bugs>)

“**ports**” bugs的讨论

讨论关于FreeBSD的“ports collection” (/usr/ports),问题报告ports建议，或者ports的修正。这是一个纯技术的邮件列表。

freebsd-proliant (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-proliant>)

关于**FreeBSD** 在**HP ProLiant** 服务器平台上的技术讨论

这个邮件列表用来讨论在HP ProLiant 服务器上使用FreeBSD，包括讨论ProLiant 专用的驱动、管理软件、配置工具，以及BIOS 更新等。同样地，这里也是讨论hpsamd、hpsmcli，以及hpacucli 模块的主要场所。

freebsd-python (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-python>)

FreeBSD 上的**Python**

这是一个讨论关于如何在FreeBSD 上改善Python 支持的邮件列表。这是一个纯技术的邮件列表。它是为那些移植Python、其第三方模块，以及**Zope** 相关软件到FreeBSD 上的人准备的。这里也欢迎参与技术讨论的人。

freebsd-questions (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-questions>)

用户问题

这是一个有关FreeBSD问题的邮件列表。您不应当发送“how to”问题给技术列表，除非您认为这个问题是非常可爱的技术问题。

freebsd-scsi (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-scsi>)

SCSI子系统

这是一个讨论FreeBSD的SCSI子系统的邮件列表。这是一个纯技术的列表。

freebsd-security (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-security>)

安全问题

FreeBSD的计算机安全问题（DES, Kerberos, 已知的安全漏洞和修复等）。这是一个纯技术的邮件列表。注意：这不是一个问和答的列表，但是同时给出问题和答案到FAQ是欢迎的。

freebsd-security-notifications (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-security-notifications>)

安全通知

FreeBSD安全问题和修复的通知。这不是一个讨论列表，讨论的列表应当是FreeBSD-security

freebsd-small (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-small>)

在嵌入式应用程序中使用FreeBSD

这个列表讨论了与极小的和嵌入的FreeBSD安装的讨论主题。这是一个纯技术的列表。

freebsd-stable (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-stable>)

讨论关于FreeBSD-STABLE版的使用

这是一个FreeBSD-STABLE用户的邮件列表。它包括-STABLE的新特性可能会影响用户的警告。任何运行“STABLE”的人应当经常关注这个列表。这是一个纯技术的列表。

freebsd-standards (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-standards>)

C99 & POSIX一致

这是关于FreeBSD顺应C99和POSIX标准的技术讨论论坛。

freebsd-usb (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-usb>)

讨论FreeBSD的USB支持

这个邮件列表是关于FreeBSD上的USB支持的技术性讨论。

freebsd-user-groups (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-user-groups>)

用户组调整列表

这个邮件列表为协调从各地的使用群体到彼此相互讨论问题和从核心团队中指定个人。这个邮件列表应被限制到大纲和协调用户组计划的范围之内。

freebsd-vendors (<http://lists.FreeBSD.org/mailman/listinfo/freebsd-vendors>)

商家

讨论FreeBSD计划和FreeBSD软硬件商家的协调。

C.1.4 过滤邮件列表

FreeBSD邮件列表是使用了多种过滤方法去消除垃圾邮件、病毒和其他没用的电子邮件。这部分所描述的并不包括所有常用的保护邮件列表的消除方法。

邮件列表只包含一些允许的附件类型。所有在列表中有MIME类型的附件的电子邮件在邮件列表中被转发之前将被过滤掉。

- application/octet-stream
- application/pdf
- application/pgp-signature
- application/x-pkcs7-signature
- message/rfc822
- multipart/alternative
- multipart/related
- multipart/signed
- text/html
- text/plain
- text/x-diff
- text/x-patch

注意: 一些邮件列表可以允许附件为其他MIME类型，但是以上列出的应该被多数的邮件列表所采用。

如果一个电子邮件包含HTML和纯文本形式，HTML的形式将被删除。如果一个电子邮件内容只是HTML形式，他将被转换为纯文本格式。

C.2 Usenet新闻组

除了FreeBSD两个特殊的新闻组，还有很多讨论FreeBSD或与FreeBSD用户相关的其他讨论组。一些新闻组的关键词搜索档案 (http://minnie.tuhs.org/BSD-info/bsdnews_search.html)是可以使用的，有什么问题可以与Warren Toomey <wkt@cs.adfa.edu.au>联系。

C.2.1 BSD特殊的新闻组

- comp.unix.bsd.freebsd.announce (news:comp.unix.bsd.freebsd.announce)
- comp.unix.bsd.freebsd.misc (news:comp.unix.bsd.freebsd.misc)
- de.comp.os.unix.bsd (news:de.comp.os.unix.bsd) (德语)
- fr.comp.os.bsd (news:fr.comp.os.bsd) (法语)
- it.comp.os.freebsd (news:it.comp.os.freebsd) (意大利语)

C.2.2 Internet上其他的UNIX新闻组

- comp.unix (news:comp.unix)
- comp.unix.questions (news:comp.unix.questions)
- comp.unix.admin (news:comp.unix.admin)
- comp.unix.programmer (news:comp.unix.programmer)
- comp.unix.shell (news:comp.unix.shell)
- comp.unix.user-friendly (news:comp.unix.user-friendly)
- comp.security.unix (news:comp.security.unix)
- comp.sources.unix (news:comp.sources.unix)
- comp.unix.advocacy (news:comp.unix.advocacy)
- comp.unix.misc (news:comp.unix.misc)
- comp.bugs.4bsd (news:comp.bugs.4bsd)
- comp.bugs.4bsd.ucb-fixes (news:comp.bugs.4bsd.ucb-fixes)
- comp.unix.bsd (news:comp.unix.bsd)

C.2.3 X Window系统

- comp.windows.x.i386unix (news:comp.windows.x.i386unix)
- comp.windows.x (news:comp.windows.x)
- comp.windows.x.apps (news:comp.windows.x.apps)
- comp.windows.x.announce (news:comp.windows.x.announce)
- comp.windows.x.intrinsics (news:comp.windows.x.intrinsics)
- comp.windows.x.motif (news:comp.windows.x.motif)
- comp.windows.x.pex (news:comp.windows.x.pex)
- comp.emulators.ms-windows.wine (news:comp.emulators.ms-windows.wine)

C.3 World Wide Web服务器

中央服务器, 阿根廷, 爱尔兰, 爱沙尼亚, 奥地利, 澳大利亚, 巴西, 保加利亚, 比利时, 冰岛, 波兰, 丹麦, 德国, 俄罗斯, 法国, 菲律宾, 芬兰, 哥斯达黎加, 韩国, 荷兰, 吉尔吉斯斯坦, 加拿大, 捷克共和国, 科威特, 拉脱维亚, 立陶宛, 罗马尼亚, 美国, 南非, 挪威, 葡萄牙, 日本, 瑞典, 瑞士, 圣马力诺, 斯洛伐克共和国, 斯洛文尼亚, 泰国, 土耳其, 乌克兰, 西班牙, 希腊, 新加坡, 新西兰, 匈牙利, 意大利, 印度尼西亚, 英国, 中国大陆, 中国台湾, 中国香港.

(2006/03/25 21:54:18 UTC 更新)

- 中央服务器
 - <http://www.FreeBSD.org/>
- 阿根廷
 - <http://www.ar.FreeBSD.org/>
- 爱尔兰
 - <http://www.ie.FreeBSD.org/>
 - <http://www2.ie.FreeBSD.org/>
- 爱沙尼亚
 - <http://www.ee.FreeBSD.org/>
- 奥地利
 - <http://www.at.FreeBSD.org/>
 - <http://www2.at.FreeBSD.org/> (IPv6)
- 澳大利亚
 - <http://www.au.FreeBSD.org/>
 - <http://www2.au.FreeBSD.org/>
- 巴西
 - <http://www.br.FreeBSD.org/>
 - <http://www2.br.FreeBSD.org/www.freebsd.org/>
 - <http://www3.br.FreeBSD.org/>
- 保加利亚

- <http://www.bg.FreeBSD.org/>
- <http://www2.bg.FreeBSD.org/>

•

比利时

- <http://freebsd.unixtech.be/>

•

冰岛

- <http://www.is.FreeBSD.org/>

•

波兰

- <http://www.pl.FreeBSD.org/>
- <http://www2.pl.FreeBSD.org/>

•

丹麦

- <http://www.dk.FreeBSD.org/> (IPv6)
- <http://www3.dk.FreeBSD.org/>

•

德国

- <http://www.de.FreeBSD.org/>
- <http://www1.de.FreeBSD.org/>
- <http://www2.de.FreeBSD.org/> (IPv6)

•

俄罗斯

- <http://www.ru.FreeBSD.org/>
- <http://www2.ru.FreeBSD.org/>
- <http://www3.ru.FreeBSD.org/>
- <http://www4.ru.FreeBSD.org/>
- <http://www5.ru.FreeBSD.org/>

- 法国
 - <http://www.fr.FreeBSD.org/>
- 菲律宾
 - <http://www.FreeBSD.org.ph/>
- 芬兰
 - <http://www.fi.FreeBSD.org/>
 - <http://www2.fi.FreeBSD.org/>
- 哥斯达黎加
 - <http://www1.cr.FreeBSD.org/>
- 韩国
 - <http://www.kr.FreeBSD.org/>
 - <http://www2.kr.FreeBSD.org/>
- 荷兰
 - <http://www.nl.FreeBSD.org/>
 - <http://www2.nl.FreeBSD.org/>
- 吉尔吉斯斯坦
 - <http://www.kg.FreeBSD.org/>
- 加拿大
 - <http://www.ca.FreeBSD.org/>
 - <http://www2.ca.FreeBSD.org/>

- 捷克共和国
 - <http://www.cz.FreeBSD.org/>
- 科威特
 - <http://www.kw.FreeBSD.org/>
- 拉脱维亚
 - <http://www.lv.FreeBSD.org/>
 - <http://www2.lv.FreeBSD.org/>
- 立陶宛
 - <http://www.lt.FreeBSD.org/>
- 罗马尼亚
 - <http://www.ro.FreeBSD.org/>
 - <http://www1.ro.FreeBSD.org/>
 - <http://www2.ro.FreeBSD.org/>
 - <http://www3.ro.FreeBSD.org/>
- 美国
 - <http://www2.us.FreeBSD.org/>
 - <http://www4.us.FreeBSD.org/> (IPv6)
 - <http://www5.us.FreeBSD.org/> (IPv6)
- 南非
 - <http://www.za.FreeBSD.org/>
 - <http://www2.za.FreeBSD.org/>

- 挪威
 - <http://www.no.FreeBSD.org/>
 - <http://www2.no.FreeBSD.org/> (IPv6)
- 葡萄牙
 - <http://www.pt.FreeBSD.org/>
 - <http://www1.pt.FreeBSD.org/>
 - <http://www4.pt.FreeBSD.org/>
 - <http://www5.pt.FreeBSD.org/>
- 日本
 - <http://www.jp.FreeBSD.org/www.FreeBSD.org/> (IPv6)
- 瑞典
 - <http://www.se.FreeBSD.org/>
 - <http://www2.se.FreeBSD.org/>
- 瑞士
 - <http://www.ch.FreeBSD.org/>
 - <http://www2.ch.FreeBSD.org/>
- 圣马力诺
 - <http://www.sm.FreeBSD.org/>
- 斯洛伐克共和国
 - <http://www.sk.FreeBSD.org/>
 - <http://www2.sk.FreeBSD.org/>

- 斯洛文尼亚
 - <http://www.si.FreeBSD.org/>
 - <http://www2.si.FreeBSD.org/>

- 泰国
 - <http://www.th.FreeBSD.org/>

- 土耳其
 - <http://www.tr.FreeBSD.org/>
 - <http://www2.tr.FreeBSD.org/>
 - <http://www.enderunix.org/freebsd/>

- 乌克兰
 - <http://www.ua.FreeBSD.org/>
 - <http://www2.ua.FreeBSD.org/>
 - <http://www5.ua.FreeBSD.org/>
 - <http://www4.ua.FreeBSD.org/>

- 西班牙
 - <http://www.es.FreeBSD.org/>
 - <http://www2.es.FreeBSD.org/>
 - <http://www3.es.FreeBSD.org/>

- 希腊
 - <http://www.gr.FreeBSD.org/>
 - <http://www.FreeBSD.gr/>

-

新加坡

- <http://www2.sg.FreeBSD.org/>

•

新西兰

- <http://www.nz.FreeBSD.org/>

•

匈牙利

- <http://www.hu.FreeBSD.org/>
- <http://www2.hu.FreeBSD.org/>

•

意大利

- <http://www.it.FreeBSD.org/>
- <http://www.gufi.org/mirrors/www.freebsd.org/data/>

•

印度尼西亚

- <http://www.id.FreeBSD.org/>

•

英国

- <http://www.uk.FreeBSD.org/>
- <http://www2.uk.FreeBSD.org/>
- <http://www3.uk.FreeBSD.org/>
- <http://www4.uk.FreeBSD.org/>
- <http://www1.uk.FreeBSD.org/> (IPv6)

•

中国大陆

- <http://www.cn.FreeBSD.org/>

•

中国台湾

- <http://www.tw.FreeBSD.org/>
- <http://www2.tw.FreeBSD.org/>
- <http://www3.tw.FreeBSD.org/>
- <http://www4.tw.FreeBSD.org/>
-
- 中国香港
- <http://www.hk.FreeBSD.org/>

C.4 Email地址

下面的用户组提供了与FreeBSD相关的邮件地址。如果他被滥用的话，这个列表的管理员有收回的权利。

域	工具	用户组	管理员
ukug.uk.FreeBSD.org	Forwarding only	<freebsd-users@uk.FreeBSD.org>	Lee Johnston <lee@uk.FreeBSD.org>

C.5 Shell账号

下面的用户组为积极支持FreeBSD的人们提供了shell账号。如果他被滥用的话，这个列表的管理员有撤销的权利。

主机	访问	工具	管理员
dogma.freebsd-uk.eu.org	Telnet/FTP/SSH	Email, Web space, Anonymous FTP	Lee Johnston <lee@uk.FreeBSD.org>

附录D.

PGP 公钥

有些时候，您可能需要校验签名或者发送加密的邮件给官员或者开发者，这里为了方便您而提供了一些密钥。完整的FreeBSD.org 用户密钥可以在<http://www.FreeBSD.org/doc/pgpkeyring.txt> 下载。

D.1 官员

D.1.1 Security Officer 团队<security-officer@FreeBSD.org>

```
pub 1024D/CA6CDFB2 2002-08-27 FreeBSD Security Officer <security-officer@FreeBSD.org>
    Key fingerprint = C374 0FC5 69A6 FBB1 4AED B131 15D6 8804 CA6C DFB2
sub 2048g/A3071809 2002-08-27
```

D.1.2 核心团队秘书<core-secretary@FreeBSD.org>

```
pub 1024R/FF8AE305 2002-01-08 core-secretary@FreeBSD.org
    Key fingerprint = CE EF 8A 48 70 00 B5 A9 55 69 DE 87 E3 9A E1 CD
```

D.1.3 Ports 管理团队秘书<portmgr-secretary@FreeBSD.org>

```
pub 1024D/7414629C 2005-11-30
    Key fingerprint = D50C BA61 8DC6 C42E 4C05 BF9A 79F6 E071 7414 629C
uid FreeBSD portmgr secretary <portmgr-secretary@FreeBSD.org>
sub 2048g/80B696E6 2005-11-30
```

D.2 核心团队成员

D.2.1 John Baldwin <jhb@FreeBSD.org>

```
pub 1024R/C10A874D 1999-01-13 John Baldwin <jbaldwin@weather.com>
    Key fingerprint = 43 33 1D 37 72 B1 EF 5B 9B 5F 39 F8 BD C1 7C B5
uid John Baldwin <john@baldwin.cx>
uid John Baldwin <jhb@FreeBSD.org>
uid John Baldwin <jobaldwi@vt.edu>
```

D.2.2 Jun Kuriyama <kuriyama@FreeBSD.org>

```
pub 1024D/FE3B59CD 1998-11-23 Jun Kuriyama <kuriyama@imgsrc.co.jp>
    Key fingerprint = 5219 55CE AC84 C296 3A3B B076 EE3C 4DBB FE3B 59CD
uid                                     Jun Kuriyama <kuriyama@FreeBSD.org>
uid                                     Jun Kuriyama <kuriyama@jp.FreeBSD.org>
sub 2048g/1CF20D27 1998-11-23
```

D.2.3 Warner Losh <imp@FreeBSD.org>

```
pub 1024D/E81F487F 2006-03-13 [expires: 2008-03-12]
    Key fingerprint = 5D5A F71F 20BE 38C9 93B5 CFCA 6E98 96C7 E81F 487F
uid                                     M. Warner Losh <imp@bsdimp.com>
sub 2048g/C35953D9 2006-03-13 [expires: 2008-03-12]
```

D.2.4 Wes Peters <wes@FreeBSD.org>

```
pub 1024D/AD10C6C4 2000-10-19 Wes Peters <wes@freebsd.org>
    Key fingerprint = 76C4 753C 83FF D982 C57D 3A2A 7387 E292 AD10 C6C4
uid                                     Wes Peters <wes@softweyr.com>
sub 1024g/237A5EF9 2000-10-19
```

D.2.5 Murray Stokely <murray@FreeBSD.org>

```
pub 1024D/0E451F7D 2001-02-12 Murray Stokely <murray@freebsd.org>
    Key fingerprint = E2CA 411D DD44 53FD BB4B 3CB5 B4D7 10A2 0E45 1F7D
sub 1024g/965A770C 2001-02-12
```

D.2.6 Peter Wemm <peter@FreeBSD.org>

```
pub 1024D/7277717F 2003-12-14 Peter Wemm <peter@wemm.org>
    Key fingerprint = 622B 2282 E92B 3BAB 57D1 A417 1512 AE52 7277 717F
uid                                     Peter Wemm <peter@FreeBSD.ORG>
sub 1024g/8B40D9D1 2003-12-14
pub 1024R/D89CE319 1995-04-02 Peter Wemm <peter@netplex.com.au>
    Key fingerprint = 47 05 04 CA 4C EE F8 93 F6 DB 02 92 6D F5 58 8A
uid                                     Peter Wemm <peter@perth.dialix.oz.au>
uid                                     Peter Wemm <peter@haywire.dialix.com>
```

D.3 开发者

D.3.1 Ariff Abdullah <ariff@FreeBSD.org>

```
pub 1024D/C5304CDA 2005-10-01
    Key fingerprint = 5C7C 6BF4 8293 DE76 27D9  FD57 96BF 9D78 C530 4CDA
uid      Ariff Abdullah <skywizard@MyBSD.org.my>
uid      Ariff Abdullah <ariff@MyBSD.org.my>
uid      Ariff Abdullah <ariff@FreeBSD.org>
sub 2048g/8958C1D3 2005-10-01
```

D.3.2 Will Andrews <will@FreeBSD.org>

```
pub 1024D/F81672C5 2000-05-22 Will Andrews (Key for official matters) <will@FreeBSD.org>
    Key fingerprint = 661F BBF7 9F5D 3D02 C862  5F6C 178E E274 F816 72C5
uid      Will Andrews <will@physics.purdue.edu>
uid      Will Andrews <will@puck.firepipe.net>
uid      Will Andrews <will@c-60.org>
uid      Will Andrews <will@csociety.org>
uid      Will Andrews <will@csociety.ecn.purdue.edu>
uid      Will Andrews <will@telperion.openpackages.org>
sub 1024g/55472804 2000-05-22
```

D.3.3 Eric Anholt <anholt@FreeBSD.org>

```
pub 1024D/6CF0EAF7 2003-09-08
    Key fingerprint = 76FE 2475 820B B75F DCA4  0F3E 1D47 6F60 6CF0 EAF7
uid      Eric Anholt <eta@lclark.edu>
uid      Eric Anholt <anholt@FreeBSD.org>
sub 1024g/80B404C1 2003-09-08
```

D.3.4 Mathieu Arnold <mat@FreeBSD.org>

```
pub 1024D/FE6D850F 2005-04-25
    Key fingerprint = 2771 11F4 0A7E 73F9 ADDD  A542 26A4 7C6A FE6D 850F
uid      Mathieu Arnold <mat@FreeBSD.org>
uid      Mathieu Arnold <m@absolight.fr>
uid      Mathieu Arnold <m@absolight.net>
uid      Mathieu Arnold <mat@mat.cc>
uid      Mathieu Arnold <arn_mat@club-internet.fr>
uid      Mathieu Arnold <mat@cpan.org>
uid      Mathieu Arnold <mathieu.arnold@t-online.fr>
uid      Mathieu Arnold <arn-mat@micronet.fr>
sub 2048g/EAD18BD9 2005-04-25
```

D.3.5 Satoshi Asami <asami@FreeBSD.org>

```
pub 1024R/1E08D889 1997-07-23 Satoshi Asami <asami@cs.berkeley.edu>
   Key fingerprint = EB 3C 68 9E FB 6C EB 3F DB 2E 0F 10 8F CE 79 CA
uid                               Satoshi Asami <asami@FreeBSD.ORG>
```

D.3.6 Simon Barner <barner@FreeBSD.org>

```
pub 1024D/EBADA82A 2000-11-10
   Key fingerprint = 67D1 3562 9A2F 3177 E46A 35ED 0A49 FEFD EBAD A82A
uid                               Simon Barner <barner@FreeBSD.org>
uid                               Simon Barner <barner@in.tum.de>
uid                               Simon Barner <barner@informatik.tu-muenchen.de>
uid                               Simon Barner <barner@gmx.de>
sub 2048g/F63052DE 2000-11-10
```

D.3.7 Doug Barton <DougB@FreeBSD.org>

```
pub 1024D/D5B2F0FB 2003-01-16
   Key fingerprint = 9DD1 E44C 8660 ADA6 580F 83B6 C886 A42B D5B2 F0FB
uid                               Doug Barton <DougB@DougBarton.us>
uid                               Doug Barton <DougB@DougBarton.net>
uid                               Doug Barton <DougB@FreeBSD.org>
sub 4096g/2DBB3F89 2003-01-16
```

D.3.8 Vitaly Bogdanov <bvs@FreeBSD.org>

```
pub 1024D/B32017F7 2005-10-02 Vitaly Bogdanov <gad@gad.glazov.net>
   Key fingerprint = 402E B8E4 53CB 22FF BE62 AE35 A0BF B077 B320 17F7
uid                               Vitaly Bogdanov <bvs@freebsd.org>
sub 1024g/0E88C62E 2005-10-02
```

D.3.9 Renato Botelho <garga@FreeBSD.org>

```
pub 1024D/2244EDA9 2003-12-16 [expires: 2010-03-22]
uid                               Renato Botelho <garga@FreeBSD.org>
uid                               Renato Botelho <renato@galle.com.br>
uid                               Renato Botelho <garga@brainsoft.com.br>
uid                               Renato Botelho <freebsd@galle.com.br>
sub 1024g/7B295760 2003-12-16
```

D.3.10 Anton Berezin <tobez@FreeBSD.org>

```
pub 1024D/7A7BA3C0 2000-05-25 Anton Berezin <tobez@catpipe.net>
    Key fingerprint = CDD8 560C 174B D8E5 0323 83CE 22CA 584C 7A7B A3C0
uid                                Anton Berezin <tobez@tobez.org>
uid                                Anton Berezin <tobez@FreeBSD.org>
sub 1024g/ADC71E87 2000-05-25
```

D.3.11 Damien Bergamini <damien@FreeBSD.org>

```
pub 2048R/D129F093 2005-03-02
    Key fingerprint = D3AB 28C3 1A4A E219 3145 54FE 220A 7486 D129 F093
uid                                Damien Bergamini <damien.bergamini@free.fr>
uid                                Damien Bergamini <damien@FreeBSD.org>
sub 2048R/9FBA73A4 2005-03-02
```

D.3.12 Tim Bishop <tdb@FreeBSD.org>

```
pub 1024D/5AE7D984 2000-10-07
    Key fingerprint = 1453 086E 9376 1A50 ECF6 AE05 7DCE D659 5AE7 D984
uid                                Tim Bishop <tim@bishnet.net>
uid                                Tim Bishop <T.D.Bishop@kent.ac.uk>
uid                                Tim Bishop <tdb@i-scream.org>
uid                                Tim Bishop <tdb@FreeBSD.org>
sub 4096g/7F886031 2000-10-07
```

D.3.13 Martin Blapp <mbr@FreeBSD.org>

```
pub 1024D/D300551E 2001-12-20 Martin Blapp <mb@imp.ch>
    Key fingerprint = B434 53FC C87C FE7B 0A18 B84C 8686 EF22 D300 551E
sub 1024g/998281C8 2001-12-20
```

D.3.14 Roman Bogorodskiy <novel@FreeBSD.org>

```
pub 1024R/1DAACA46 2004-05-25 [expires: 2007-01-06]
    Key fingerprint = AC27 CF29 5E51 E53F 8C8D DB90 8074 5B38 1DAA CA46
uid                                Roman Bogorodskiy <novel@FreeBSD.org>
uid                                Roman Bogorodskiy <bogorodskiy@gmail.com>
uid                                Roman Bogorodskiy <bogorodskiy@inbox.ru>
uid                                Roman Bogorodskiy <novel@clublife.ru>
```

D.3.15 Hartmut Brandt <harti@FreeBSD.org>

```
pub 1024D/5920099F 2003-01-29 Hartmut Brandt <brandt@fokus.fraunhofer.de>
   Key fingerprint = F60D 09A0 76B7 31EE 794B BB91 082F 291D 5920 099F
uid                               Hartmut Brandt <harti@freebsd.org>
sub 1024g/21D30205 2003-01-29
```

D.3.16 Oliver Braun <obraun@FreeBSD.org>

```
pub 1024D/EF25B1BA 2001-05-06 Oliver Braun <obraun@unsane.org>
   Key fingerprint = 6A3B 042A 732E 17E4 B6E7 3EAF C0B1 6B7D EF25 B1BA
uid                               Oliver Braun <obraun@obraun.net>
uid                               Oliver Braun <obraun@freebsd.org>
uid                               Oliver Braun <obraun@haskell.org>
sub 1024g/09D28582 2001-05-06
```

D.3.17 Jonathan M. Bresler <jmb@FreeBSD.org>

```
pub 1024R/97E638DD 1996-06-05 Jonathan M. Bresler <jmb@Bresler.org>
   Key fingerprint = 31 57 41 56 06 C1 40 13 C5 1C E3 E5 DC 62 0E FB
uid                               Jonathan M. Bresler <jmb@FreeBSD.ORG>
uid                               Jonathan M. Bresler
uid                               Jonathan M. Bresler <Jonathan.Bresler@USi.net>
uid                               Jonathan M. Bresler <jmb@Frb.GOV>
```

D.3.18 Christian Brueffer <brueffer@FreeBSD.org>

```
pub 1024D/A0ED982D 2002-10-14 Christian Brueffer <chris@unixpages.org>
   Key fingerprint = A5C8 2099 19FF AACA F41B B29B 6C76 178C A0ED 982D
uid                               Christian Brueffer <brueffer@hitnet.rwth-aachen.de>
uid                               Christian Brueffer <brueffer@FreeBSD.org>
sub 4096g/1DCC100F 2002-10-14
```

D.3.19 Markus Brueffer <markus@FreeBSD.org>

```
pub 1024D/78F8A8D4 2002-10-21 Markus Brueffer <brueffer@phoenix-systems.de>
   Key fingerprint = 3F9B EBE8 F290 E5CC 1447 8760 D48D 1072 78F8 A8D4
uid                               Markus Brueffer <buff@hitnet.rwth-aachen.de>
uid                               Markus Brueffer <mbrueffer@mi.rwth-aachen.de>
uid                               Markus Brueffer <markus@FreeBSD.org>
uid                               Markus Brueffer <markus@brueffer.de>
sub 4096g/B7E5C7B6 2002-10-21
```

D.3.20 Wilko Bulte <wilko@FreeBSD.org>

```
pub 1024D/B5F2C0E5 2005-01-26
uid Wilko Bulte <wilko@FreeBSD.org>
uid Wilko Bulte <wkb@xs4all.nl>
sub 1024D/CEE36724 2005-01-26
```

D.3.21 Oleg Bulyzhin <oleg@FreeBSD.org>

```
pub 1024D/78CE105F 2004-02-06
   Key fingerprint = 98CC 3E66 26DE 50A8 DBC4 EB27 AF22 DCEF 78CE 105F
uid Oleg Bulyzhin <oleg@FreeBSD.org>
uid Oleg Bulyzhin <oleg@rinet.ru>
sub 1024g/F747C159 2004-02-06
```

D.3.22 Jesus R. Camou <jcamou@FreeBSD.org>

```
pub 1024D/C2161947 2005-03-01
   Key fingerprint = 274C B265 48EC 42AE A2CA 47D9 7D98 588A C216 1947
uid Jesus R. Camou <jcamou@FreeBSD.org>
sub 2048g/F8D2A8DF 2005-03-01
```

D.3.23 Hye-Shik Chang <perky@FreeBSD.org>

```
pub 1024D/CFDB4BA4 1999-04-23 Hye-Shik Chang <perky@FreeBSD.org>
   Key fingerprint = 09D9 57D6 58BA 44DD CAEC 71CD 0D65 2C59 CFDB 4BA4
uid Hye-Shik Chang <hyeshik@gmail.com>
sub 1024g/A94A8ED1 1999-04-23
```

D.3.24 Jonathan Chen <jon@FreeBSD.org>

```
pub 1024D/2539468B 1999-10-11 Jonathan Chen <jon@spock.org>
   Key fingerprint = EE31 CDA1 A105 C8C9 5365 3DB5 C2FC 86AA 2539 468B
uid Jonathan Chen <jon@freebsd.org>
uid Jonathan Chen <chenj@rpi.edu>
uid Jonathan Chen <spock@acm.rpi.edu>
uid Jonathan Chen <jon@cs.rpi.edu>
sub 3072g/B81EF1DB 1999-10-11
```

D.3.25 陈洛祁<luoqi@FreeBSD.org>

```
pub 1024D/2926F3BE 2002-02-22 Luoqi Chen <luoqi@FreeBSD.org>
   Key fingerprint = B470 A815 5917 D9F4 37F3 CE2A 4D75 3BD1 2926 F3BE
uid Luoqi Chen <luoqi@bricore.com>
```



```
uid                               Luoqi Chen <lchen@onetta.com>
sub 1024g/5446EB72 2002-02-22
```

D.3.26 Andrey A. Chernov <ache@FreeBSD.org>

```
pub 1024R/D99D08EB 1992-08-20 Andrey A. Chernov <ache@FreeBSD.org>
   Key fingerprint = 33 03 9F 48 33 7B 4A 15 63 48 88 0A C4 97 FD 49
```

D.3.27 Sean Chittenden <seanc@FreeBSD.org>

```
pub 1024D/EE278A28 2004-02-08 Sean Chittenden <sean@chittenden.org>
   Key fingerprint = E41F F441 7E91 6CBA 1844 65CF B939 3C78 EE27 8A28
sub 2048g/55321853 2004-02-08
```

D.3.28 Junho CHOI <cjh@FreeBSD.org>

```
pub 1024D/E60260F5 2002-10-14 CHOI Junho (Work) <cjh@wdb.co.kr>
   Key fingerprint = 1369 7374 A45F F41A F3C0 07E3 4A01 C020 E602 60F5
uid                               CHOI Junho (Personal) <cjh@kr.FreeBSD.org>
uid                               CHOI Junho (FreeBSD) <cjh@FreeBSD.org>
sub 1024g/04A4FDD8 2002-10-14
```

D.3.29 Crist J. Clark <cjc@FreeBSD.org>

```
pub 1024D/FE886AD3 2002-01-25 Crist J. Clark <cjclark@jhu.edu>
   Key fingerprint = F04E CCD7 3834 72C2 707F 0A8F 259F 8F4B FE88 6AD3
uid                               Crist J. Clark <cjclark@alum.mit.edu>
uid                               Crist J. Clark <cjc@freebsd.org>
sub 1024g/9B6BAB99 2002-01-25
```

D.3.30 Joe Marcus Clarke <marcus@FreeBSD.org>

```
pub 1024D/FE14CF87 2002-03-04 Joe Marcus Clarke (FreeBSD committer address) <marcus@FreeBSD.org>
   Key fingerprint = CC89 6407 73CC 0286 28E4 AFB9 6F68 8F8A FE14 CF87
uid                               Joe Marcus Clarke <marcus@marcuscom.com>
sub 1024g/B9ACE4D2 2002-03-04
```

D.3.31 Nik Clayton <nik@FreeBSD.org>

```
pub 1024D/2C37E375 2000-11-09 Nik Clayton <nik@freebsd.org>
   Key fingerprint = 15B8 3FFC DDB4 34B0 AA5F 94B7 93A8 0764 2C37 E375
uid                               Nik Clayton <nik@slashdot.org>
```

```
uid          Nik Clayton <nik@crf-consulting.co.uk>
uid          Nik Clayton <nik@ngo.org.uk>
uid          Nik Clayton <nik@bsd1.com>
sub 1024g/769E298A 2000-11-09
```

D.3.32 Aaron Dalton <aaron@FreeBSD.org>

```
pub 1024D/56CBA70B 2005-10-23 [expires: 2006-10-23]
    Key fingerprint = CD8A DA9B B70F 94BB F2DA 76E6 0078 73C4 56CB A70B
uid          Aaron Dalton <aaron@daltons.ca>
sub 1024g/15661754 2005-10-23 [expires: 2006-10-23]
```

D.3.33 Ceri Davies <ceri@FreeBSD.org>

```
pub 1024D/34B7245F 2002-03-08 Ceri Davies <ceri@submonkey.net>
    Key fingerprint = 9C88 EB05 A908 1058 A4AE 9959 A1C7 DCC1 34B7 245F
uid          Ceri Davies <setantae@submonkey.net>
uid          Ceri Davies <ceri@FreeBSD.org>
sub 1024g/0C482CBC 2002-03-08
```

D.3.34 Brad Davis <brd@FreeBSD.org>

```
pub 1024D/ED0A754D 2005-05-14 [expires: 2007-05-14]
    Key fingerprint = 5DFD D1A6 BEEE A6D4 B3F5 4236 D362 3291 ED0A 754D
uid          Brad Davis <brd@FreeBSD.org>
uid          Brad Davis <so14k@so14k.com>
sub 2048g/1F29D404 2005-05-14 [expires: 2007-05-14]
```

D.3.35 Brooks Davis <brooks@FreeBSD.org>

```
pub 1024D/F2381AD4 2001-02-10 Brooks Davis (The Aerospace Corporation) <brooks@aero.org>
    Key fingerprint = 655D 519C 26A7 82E7 2529 9BF0 5D8E 8BE9 F238 1AD4
uid          Brooks Davis <brooks@one-eyed-alien.net>
uid          Brooks Davis <brooks@FreeBSD.org>
uid          Brooks Davis <brooks@aero.org>
sub 2048g/CFDACA7A 2003-01-25 [expires: 2008-01-24]
sub 1024g/42921194 2001-02-10 [expires: 2009-02-08]
```

D.3.36 George V. Neville-Neil <gnn@FreeBSD.org>

```
pub 1024D/440A33D2 2002-09-17
    Key fingerprint = AF66 410F CC8D 1FC9 17DB 6225 61D8 76C1 440A 33D2
uid          George V. Neville-Neil <gnn@freebsd.org>
uid          George V. Neville-Neil <gnn@neville-neil.com>
```

sub 2048g/95A74F6E 2002-09-17

D.3.37 Pawel Jakub Dawidek <pjd@FreeBSD.org>

```
pub 1024D/B1293F34 2004-02-02 Pawel Jakub Dawidek <Pawel@Dawidek.net>
   Key fingerprint = A3A3 5B4D 9CF9 2312 0783 1B1D 168A EF5D B129 3F34
uid                               Pawel Jakub Dawidek <pjd@FreeBSD.org>
uid                               Pawel Jakub Dawidek <pjd@FreeBSD.pl>
sub 2048g/3EEC50A7 2004-02-02 [expires: 2006-02-01]
```

D.3.38 Brian S. Dean <bsd@FreeBSD.org>

```
pub 1024D/723BDEE9 2002-01-23 Brian S. Dean <bsd@FreeBSD.org>
   Key fingerprint = EF49 7ABE 47ED 91B3 FC3D 7EA5 4D90 2FF7 723B DEE9
sub 1024g/4B02F876 2002-01-23
```

D.3.39 Vasil Dimov <vd@FreeBSD.org>

```
pub 1024D/F6C1A420 2004-12-08
   Key fingerprint = B1D5 04C6 26CC 0D20 9525 14B8 170E 923F F6C1 A420
uid                               Vasil Dimov <vd@FreeBSD.org>
uid                               Vasil Dimov <vd@datamax.bg>
sub 4096g/A0148C94 2004-12-08
```

D.3.40 Alexey Dokuchaev <danfe@FreeBSD.org>

```
pub 1024D/3C060B44 2004-08-23 Alexey Dokuchaev <danfe@FreeBSD.org>
   Key fingerprint = D970 08A4 922C 8D63 0C19 8D27 F421 76EE 3C06 0B44
sub 1024g/70BAE967 2004-08-23
```

D.3.41 Dima Dorfman <dd@FreeBSD.org>

```
pub 1024D/69FAE582 2001-09-04
   Key fingerprint = B340 8338 7DA3 4D61 7632 098E 0730 055B 69FA E582
uid                               Dima Dorfman <dima@trit.org>
uid                               Dima Dorfman <dima@unixfreak.org>
uid                               Dima Dorfman <dd@freebsd.org>
sub 2048g/65AF3B89 2003-08-19 [expires: 2005-08-18]
sub 2048g/8DB0CF2C 2005-05-29 [expires: 2007-05-29]
```

D.3.42 Bruno Ducrot <bruno@FreeBSD.org>

```
pub 1024D/7F463187 2000-12-29
    Key fingerprint = 7B79 E1D6 F5A1 6614 792F D906 899B 4D28 7F46 3187
uid          Ducrot Bruno (Poup Master) <ducrot@poupinou.org>
sub 1024g/40282874 2000-12-29
```

D.3.43 Alex Dupre <ale@FreeBSD.org>

```
pub 1024D/CE5F554D 1999-06-27 Alex Dupre <sysadmin@alexdupre.com>
    Key fingerprint = DE23 02EA 5927 D5A9 D793 2BA2 8115 E9D8 CE5F 554D
uid          Alex Dupre <ale@FreeBSD.org>
uid          [jpeg image of size 5544]
uid          Alex Dupre <ICQ:5431856>
sub 2048g/FD5E2D21 1999-06-27
```

D.3.44 Peter Edwards <peadar@FreeBSD.org>

```
pub 1024D/D80B4B3F 2004-03-01 Peter Edwards <peadar@FreeBSD.org>
    Key fingerprint = 7A8A 9756 903E BEF2 4D9E 3C94 EE52 52F7 D80B 4B3F
uid          Peter Edwards <pmedwards@eircom.net>
```

D.3.45 Josef El-Rayes <josef@FreeBSD.org>

```
pub 2048R/A79DB53C 2004-01-04 Josef El-Rayes <josef@FreeBSD.org>
    Key fingerprint = 58EB F5B7 2AB9 37FE 33C8 716B 59C5 22D9 A79D B53C
uid          Josef El-Rayes <josef@daemon.li>
```

D.3.46 Udo Erdelhoff <ue@FreeBSD.org>

```
pub 1024R/E74FA871 1994-07-19 Udo Erdelhoff <uer@de.uu.net>
    Key fingerprint = 8C B1 80 CA 2C 52 73 81 FB A7 B4 03 C5 32 C8 67
uid          Udo Erdelhoff <ue@nathan.ruhr.de>
uid          Udo Erdelhoff <ue@freebsd.org>
uid          Udo Erdelhoff <uerdelho@eu.uu.net>
uid          Udo Erdelhoff <uerdelho@uu.net>
```

D.3.47 Ruslan Ermilov <ru@FreeBSD.org>

```
pub 1024D/996E145E 2004-06-02 Ruslan Ermilov (FreeBSD) <ru@FreeBSD.org>
    Key fingerprint = 274E D201 71ED 11F6 9CCB 0194 A917 E9CC 996E 145E
uid          Ruslan Ermilov (FreeBSD Ukraine) <ru@FreeBSD.org.ua>
uid          Ruslan Ermilov (IPNet) <ru@ip.net.ua>
sub 1024g/557E3390 2004-06-02 [expires: 2007-06-02]
```

D.3.48 Lukas Ertl <le@FreeBSD.org>

```
pub 1024D/F10D06CB 2000-11-23 Lukas Ertl <le@FreeBSD.org>
    Key fingerprint = 20CD C5B3 3A1D 974E 065A B524 5588 79A9 F10D 06CB
uid                                     Lukas Ertl <a9404849@unet.univie.ac.at>
uid                                     Lukas Ertl <l.ertl@univie.ac.at>
uid                                     Lukas Ertl <le@univie.ac.at>
sub 1024g/5960CE8E 2000-11-23
```

D.3.49 Stefan Farfeleder <stefanf@FreeBSD.org>

```
pub 1024D/8BEFD15F 2004-03-14 Stefan Farfeleder <stefan@fafoe.narf.at>
    Key fingerprint = 4220 FE60 A4A1 A490 5213 27A6 319F 8B28 8BEF D15F
uid                                     Stefan Farfeleder <stefanf@comlang.tuwien.ac.at>
uid                                     Stefan Farfeleder <stefanf@FreeBSD.org>
uid                                     Stefan Farfeleder <stefanf@ten15.org>
sub 2048g/418753E9 2004-03-14 [expires: 2007-03-14]
```

D.3.50 Chris D. Faulhaber <jedgar@FreeBSD.org>

```
pub 1024D/FE817A50 2000-12-20 Chris D. Faulhaber <jedgar@FreeBSD.org>
    Key fingerprint = A47D A838 9216 F921 A456 54FF 39B6 86E0 FE81 7A50
uid                                     Chris D. Faulhaber <jedgar@fxp.org>
sub 2048g/93452698 2000-12-20
```

D.3.51 Brian F. Feldman <green@FreeBSD.org>

```
pub 1024D/41C13DE3 2000-01-11 Brian Fundakowski Feldman <green@FreeBSD.org>
    Key fingerprint = 6A32 733A 1BF6 E07B 5B8D AE14 CC9D DCA2 41C1 3DE3
sub 1024g/A98B9FCC 2000-01-11 [expires: 2001-01-10]

pub 1024D/773905D6 2000-09-02 Brian Fundakowski Feldman <green@FreeBSD.org>
    Key fingerprint = FE23 7481 91EA 5E58 45EA 6A01 B552 B043 7739 05D6
sub 2048g/D2009B98 2000-09-02
```

D.3.52 Mário Sérgio Fujikawa Ferreira <lioux@FreeBSD.org>

```
pub 1024D/75A63712 2006-02-23 [expires: 2007-02-23]
    Key fingerprint = 42F2 2F74 8EF9 5296 898F C981 E9CF 463B 75A6 3712
uid                                     Mario Sergio Fujikawa Ferreira (lioux) <lioux@FreeBSD.org>
uid                                     Mario Sergio Fujikawa Ferreira <lioux@uol.com.br>
sub 4096g/BB7D80F2 2006-02-23 [expires: 2007-02-23]
```

D.3.53 Tony Finch <fanf@FreeBSD.org>

```
pub 1024D/84C71B6E 2002-05-03 Tony Finch <dot@dotat.at>
    Key fingerprint = 199C F25B 2679 6D04 63C5 2159 FFC0 F14C 84C7 1B6E
uid                                     Tony Finch <fanf@FreeBSD.org>
uid                                     Tony Finch <fanf@apache.org>
uid                                     Tony Finch <fanf2@cam.ac.uk>
sub 2048g/FD101E8B 2002-05-03
```

D.3.54 Marc Fonvieille <blackend@FreeBSD.org>

```
pub 1024D/4F8E74E8 2004-12-25 Marc Fonvieille <blackend@FreeBSD.org>
    Key fingerprint = 55D3 4883 4A04 828A A139 A5CF CD0F 51C0 4F8E 74E8
uid                                     Marc Fonvieille <marc@blackend.org>
uid                                     Marc Fonvieille <marc@freebsd-fr.org>
sub 1024g/37AD4E7D 2004-12-25
```

D.3.55 Pete Fritchman <petef@FreeBSD.org>

```
pub 1024D/74B91CFD 2001-01-30 Pete Fritchman <petef@FreeBSD.org>
    Key fingerprint = 9A9F 8A13 DB0D 7777 8D8E 1CB2 C5C9 A08F 74B9 1CFD
uid                                     Pete Fritchman <petef@databits.net>
uid                                     Pete Fritchman <petef@csh.rit.edu>
sub 1024g/0C02AF0C 2001-01-30
```

D.3.56 Bill Fumerola <billf@FreeBSD.org>

```
pub 1024D/7F868268 2000-12-07 Bill Fumerola (FreeBSD Developer) <billf@FreeBSD.org>
    Key fingerprint = 5B2D 908E 4C2B F253 DAEB FC01 8436 B70B 7F86 8268
uid                                     Bill Fumerola (Security Yahoo) <fumerola@yahoo-inc.com>
sub 1024g/43980DA9 2000-12-07
```

D.3.57 Sebastien Gioria <gioria@FreeBSD.org>

```
pub 1024D/7C8DA4F4 2002-02-09 Sebastien Gioria <eagle@freebsd-fr.org>
    Key fingerprint = 41F4 4885 7C23 6ED3 CC24 97AA 6DDD B426 7C8D A4F4
uid                                     Sebastien Gioria <gioria@FreeBSD.ORG>
uid                                     Sebastien Gioria <gioria@Francenet.fr>
uid                                     Sebastien Gioria <gioria@fluxus.net>
sub 4096g/F147E4D3 2002-02-09
```

D.3.58 Marcus Alves Grando <mnag@FreeBSD.org>

```
pub 1024D/CDCC273F 2005-09-15 [expires: 2010-09-14]
    Key fingerprint = 57F9 DEC1 5BBF 06DE 44A5 9A4A 8BEE 5F3A CDCC 273F
uid          Marcus Alves Grando <marcus@sbh.eng.br>
uid          Marcus Alves Grando <marcus@corp.grupos.com.br>
uid          Marcus Alves Grando <mnag@FreeBSD.org>
sub 2048g/698AC00C 2005-09-15 [expires: 2010-09-14]
```

D.3.59 John-Mark Gurney <jmg@FreeBSD.org>

```
pub 1024R/3F9951F5 1997-02-11 John-Mark Gurney <johnmark@gladstone.uoregon.edu>
    Key fingerprint = B7 EC EF F8 AE ED A7 31 96 7A 22 B3 D8 56 36 F4
uid          John-Mark Gurney <gurney_j@efn.org>
uid          John-Mark Gurney <jmg@cs.uoregon.edu>
uid          John-Mark Gurney <gurney_j@resnet.uoregon.edu>
```

D.3.60 Daniel Harris <dannyboy@FreeBSD.org>

```
pub 1024D/84D0D7E7 2001-01-15 Daniel Harris <dannyboy@worksforfood.com>
    Key fingerprint = 3C61 B8A1 3F09 D194 3259 7173 6C63 DA04 84D0 D7E7
uid          Daniel Harris <dannyboy@freebsd.org>
uid          Daniel Harris <dh@askdh.com>
uid          Daniel Harris <dh@wordassault.com>
sub 1024g/9DF0231A 2001-01-15
```

D.3.61 Daniel Hartmeier <dhartmei@FreeBSD.org>

```
pub 1024R/6A3A7409 1994-08-15 Daniel Hartmeier <dhartmei@freebsd.org>
    Key fingerprint = 13 7E 9A F3 36 82 09 FE FD 57 B8 5C 2B 81 7E 1F
```

D.3.62 John Hay <jhay@FreeBSD.org>

```
pub 2048R/A9275B93 2000-05-10 John Hay <jhay@icomtek.csir.co.za>
    Key fingerprint = E7 95 F4 B9 D4 A7 49 6A 83 B9 77 49 28 9E 37 70
uid          John Hay <jhay@mikom.csir.co.za>
uid          Thawte Freemail Member <jhay@mikom.csir.co.za>
uid          John Hay <jhay@csir.co.za>
uid          John Hay <jhay@FreeBSD.ORG>
```

D.3.63 Sheldon Hearn <sheldonh@FreeBSD.org>

```
pub 1024D/74A06ACD 2002-06-20 Sheldon Hearn <sheldonh@starjuice.net>
    Key fingerprint = 01A3 EF91 9C5A 3633 4E01 8085 A462 57F1 74A0 6ACD
sub 1536g/C42F8AC8 2002-06-20
```

D.3.64 Mike Heffner <mikeh@FreeBSD.org>

```
pub 1024D/CDECBF99 2001-02-02 Michael Heffner <mheffner@novacoxmail.com>
    Key fingerprint = AFAB CCEB 68C7 573F 5110 9285 1689 1942 CDEC BF99
uid                               Michael Heffner <mheffner@vt.edu>
uid                               Michael Heffner <mikeh@FreeBSD.org>
uid                               Michael Heffner <spock@techfour.net>
uid                               Michael Heffner (ACM sysadmin) <mheffner@acm.vt.edu>
sub 1024g/3FE83FB5 2001-02-02
```

D.3.65 Martin Heinen <mheinen@FreeBSD.org>

```
pub 1024D/116C5C85 2002-06-17 Martin Heinen <mheinen@freebsd.org>
    Key fingerprint = C898 3FCD EEA0 17ED BEA9 564D E5A6 AFF2 116C 5C85
uid                               Martin Heinen <martin@sumuk.de>
sub 1024g/EA67506B 2002-06-17
```

D.3.66 Niels Heinen <niels@FreeBSD.org>

```
pub 1024D/5FE39B80 2004-12-06 Niels Heinen <niels.heinen@ubizen.com>
    Key fingerprint = 75D8 4100 CF5B 3280 543F 930C 613E 71AA 5FE3 9B80
uid                               Niels Heinen <niels@defaced.be>
uid                               Niels Heinen <niels@heinen.ws>
uid                               Niels Heinen <niels@FreeBSD.org>
sub 2048g/057F4DA7 2004-12-06
```

D.3.67 Guy Helmer <ghelmer@FreeBSD.org>

```
pub 1024R/35F4ED2D 1997-01-26 Guy G. Helmer <ghelmer@freebsd.org>
    Key fingerprint = A2 59 4B 92 02 5B 9E B1 B9 4E 2E 03 29 D5 DC 3A
uid                               Guy G. Helmer <ghelmer@cs.iastate.edu>
uid                               Guy G. Helmer <ghelmer@palisadesys.com>
```

D.3.68 Maxime Henrion <mux@FreeBSD.org>

```
pub 1024D/881D4806 2003-01-09 Maxime Henrion <mux@FreeBSD.org>
    Key fingerprint = 81F1 BE2D 12F1 184A 77E4 ACD0 5563 7614 881D 4806
sub 2048g/D0B510C0 2003-01-09
```


D.3.69 Michael L. Hostbaek <mich@FreeBSD.org>

```
pub 1024D/0F55F6BE 2001-08-07 Michael L. Hostbaek <mich@freebsdcluster.org>
   Key fingerprint = 4D62 9396 B19F 38D3 5C99 1663 7B0A 5212 0F55 F6BE
uid                               Michael L. Hostbaek <mich@freebsdcluster.dk>
uid                               Michael L. Hostbaek <mich@icommerce-france.com>
uid                               Micahel L. Hostbaek <mich@freebsd.dk>
uid                               Michael L. Hostbaek <mich@the-lab.org>
uid                               Michael L. Hostbaek <mich@freebsd.org>
sub 1024g/8BE4E30F 2001-08-07
```

D.3.70 胡庭豪<foxfair@FreeBSD.org>

```
pub 1024D/4E9BCA59 2003-09-01 Foxfair Hu <foxfair@FreeBSD.org>
   Key fingerprint = 280C A846 CA1B CAC9 DDCF F4CB D553 4BD5 4E9B CA59
uid                               Foxfair Hu <foxfair@drago.fomokka.net>
uid                               Howard Hu <howardhu@yahoo-inc.com>
sub 1024g/3356D8C1 2003-09-01
```

D.3.71 Jordan K. Hubbard <jkh@FreeBSD.org>

```
pub 1024R/8E542D5D 1996-04-04 Jordan K. Hubbard <jkh@FreeBSD.org>
   Key fingerprint = 3C F2 27 7E 4A 6C 09 0A 4B C9 47 CD 4F 4D 0B 20
```

D.3.72 Michael Johnson <ahze@FreeBSD.org>

```
pub 1024D/3C046FD6 2004-10-29 Michael Johnson (FreeBSD key) <ahze@FreeBSD.org>
   Key fingerprint = 363C 6ABA ED24 C23B 5F0C 3AB4 9F8B AA7D 3C04 6FD6
uid                               Michael Johnson (pgp key) <ahze@ahze.net>
sub 2048g/FA334AE3 2004-10-29
```

D.3.73 Trevor Johnson <trevor@FreeBSD.org>

```
pub 1024D/3A3EA137 2000-04-20 Trevor Johnson <trevor@jpj.net>
   Key fingerprint = 7ED1 5A92 76C1 FFCB E5E3 A998 F037 5A0B 3A3E A137
sub 1024g/46C24F1E 2000-04-20
```

D.3.74 Poul-Henning Kamp <phk@FreeBSD.org>

```
pub 1024R/0358FCBD 1995-08-01 Poul-Henning Kamp <phk@FreeBSD.org>
   Key fingerprint = A3 F3 88 28 2F 9B 99 A2 49 F4 E2 FA 5A 78 8B 3E
```

D.3.75 Josef Karthausser <joe@FreeBSD.org>

```

pub 1024D/E6B15016 2000-10-19 Josef Karthausser <joe@FreeBSD.org>
    Key fingerprint = 7266 8EAF 82C2 D439 5642 AC26 5D52 1C8C E6B1 5016
uid                                     Josef Karthausser <joe@tao.org.uk>
uid                                     Josef Karthausser <joe@uk.FreeBSD.org>
uid                                     [revoked] Josef Karthausser <josef@bsd1.com>
uid                                     [revoked] Josef Karthausser <joe@pavilion.net>
sub 2048g/1178B692 2000-10-19

```

D.3.76 Vinod Kashyap <vkashyap@FreeBSD.org>

```

pub 1024R/04FCCDD3 2004-02-19 Vinod Kashyap (gnupg key) <vkashyap@freebsd.org>
    Key fingerprint = 9B83 0B55 604F E491 B7D2 759D DF92 DAA0 04FC CDD3

```

D.3.77 Kris Kennaway <kris@FreeBSD.org>

```

pub 1024D/68E840A5 2000-01-14 Kris Kennaway <kris@citusc.usc.edu>
    Key fingerprint = E65D 0E7D 7E16 B212 1BD6 39EE 5ABC B405 68E8 40A5
uid                                     Kris Kennaway <kris@FreeBSD.org>
uid                                     Kris Kennaway <kris@obsecrity.org>
sub 2048g/03A41C45 2000-01-14 [expires: 2006-01-14]

```

D.3.78 Giorgos Keramidas <keramida@FreeBSD.org>

```

pub 1024D/318603B6 2001-09-21 Giorgos Keramidas <keramida@FreeBSD.org>
    Key fingerprint = C1EB 0653 DB8B A557 3829 00F9 D60F 941A 3186 03B6
uid                                     Giorgos Keramidas <charon@labs.gr>
uid                                     Giorgos Keramidas <keramida@ceid.upatras.gr>
uid                                     Giorgos Keramidas <keramida@hellug.gr>
uid                                     Giorgos Keramidas <keramida@linux.gr>
sub 1024g/50FDBAD1 2001-09-21

```

D.3.79 Max Khon <fjoe@FreeBSD.org>

```

pub 1024D/414420F4 2003-04-29 Max Khon <fjoe@freebsd.org>
    Key fingerprint = CE1F 29CA A6BF 2F26 13E8 1B61 62AE 6B8F 4144 20F4
uid                                     Max Khon <fjoe@iclub.nsu.ru>
sub 1024g/6585039B 2003-04-29

```

D.3.80 Jung-uk Kim <jkim@FreeBSD.org>

```
pub 1024D/BF6A9D53 2004-04-07
    Key fingerprint = F841 0339 93EF D27D 32AD 3261 9A56 B2D5 BF6A 9D53
uid      Jung-uk Kim <jkim@FreeBSD.org>
uid      Jung-uk Kim <jkim@niksun.com>
sub 4096g/B01CA5A0 2004-04-07
```

D.3.81 Andreas Klemm <andreas@FreeBSD.org>

```
pub 1024D/6C6F6CBA 2001-01-06 Andreas Klemm <andreas.klemm@eu.didata.com>
    Key fingerprint = F028 D51A 0D42 DD67 4109 19A3 777A 3E94 6C6F 6CBA
uid      Andreas Klemm <andreas@klemm.gtn.com>
uid      Andreas Klemm <andreas@FreeBSD.org>
uid      Andreas Klemm <andreas@apsfilter.org>
sub 2048g/FE23F866 2001-01-06
```

D.3.82 Johann Kois <jkois@FreeBSD.org>

```
pub 1024D/DD61C2D8 2004-06-27 Johann Kois <J.Kois@web.de>
    Key fingerprint = 8B70 03DB 3C45 E71D 0ED4 4825 FEB0 EBEF DD61 C2D8
uid      Johann Kois <jkois@freebsd.org>
sub 1024g/568307CB 2004-06-27
```

D.3.83 Sergei Kolobov <sergei@FreeBSD.org>

```
pub 1024D/3BA53401 2003-10-10 Sergei Kolobov <sergei@FreeBSD.org>
    Key fingerprint = A2F4 5F34 0586 CC9C 493A 347C 14EC 6E69 3BA5 3401
uid      Sergei Kolobov <sergei@kolobov.com>
sub 2048g/F8243671 2003-10-10
```

D.3.84 Maxim Konovalov <maxim@FreeBSD.org>

```
pub 1024D/2C172083 2002-05-21 Maxim Konovalov <maxim@FreeBSD.org>
    Key fingerprint = 6550 6C02 EFC2 50F1 B7A3 D694 ECF0 E90B 2C17 2083
uid      Maxim Konovalov <maxim@macomnet.ru>
sub 1024g/F305DDCA 2002-05-21
```

D.3.85 Joseph Koshy <jkoshy@FreeBSD.org>

```
pub 1024D/D93798B6 2001-12-21 Joseph Koshy (FreeBSD) <jkoshy@freebsd.org>
    Key fingerprint = 0DE3 62F3 EF24 939F 62AA 2E3D ABB8 6ED3 D937 98B6
sub 1024g/43FD68E9 2001-12-21
```

D.3.86 Wojciech A. Koszek <wkoszek@FreeBSD.org>

```
pub 1024D/C9F25145 2006-02-15
    Key fingerprint = 6E56 C571 9D33 D23E 9A61 8E50 623C AD62 C9F2 5145
uid      Wojciech A. Koszek <dunstan@FreeBSD.czyst.pl>
uid      Wojciech A. Koszek <wkoszek@FreeBSD.org>
sub 4096g/3BBD20A5 2006-02-15
```

D.3.87 Roman Kurakin <rik@FreeBSD.org>

```
pub 1024D/C8550F4C 2005-12-16 [expires: 2008-12-15]
    Key fingerprint = 25BB 789A 6E07 E654 8E59 0FA9 42B1 937C C855 0F4C
uid      Roman Kurakin <rik@FreeBSD.org>
sub 2048g/D15F2AB6 2005-12-16 [expires: 2008-12-15]
```

D.3.88 Hideyuki KURASHINA <rushani@FreeBSD.org>

```
pub 1024D/439ADC57 2002-03-22 Hideyuki KURASHINA <rushani@bl.mmtr.or.jp>
    Key fingerprint = A052 6F98 6146 6FE3 91E2 DA6B F2FA 2088 439A DC57
uid      Hideyuki KURASHINA <rushani@FreeBSD.org>
uid      Hideyuki KURASHINA <rushani@jp.FreeBSD.org>
sub 1024g/64764D16 2002-03-22
```

D.3.89 Clement Laforet <clement@FreeBSD.org>

```
pub 1024D/0723BA1D 2003-12-13 Clement Laforet (FreeBSD committer address) <clement@FreeBSD.org>
    Key fingerprint = 3638 4B14 8463 A67B DC7E 641C B118 5F8F 0723 BA1D
uid      Clement Laforet <sheepkiller@cultdeadsheep.org>
uid      Clement Laforet <clement.laforet@cotds.org>
sub 2048g/23D57658 2003-12-13
```

D.3.90 Max Laier <mlaier@FreeBSD.org>

```
pub 1024D/3EB6046D 2004-02-09 Max Laier <mlaier@freebsd.org>
    Key fingerprint = 917E 7F25 E90F 77A4 F746 2E8D 5F2C 84A1 3EB6 046D
uid      Max Laier <max@love2party.net>
```

D.3.91 Erwin Lansing <erwin@FreeBSD.org>

```
pub 1024D/15256990 1998-07-03 Erwin Lansing <erwin@lansing.dk>
    Key fingerprint = FB58 9797 299A F18E 2D3E 73D6 AB2F 5A5B 1525 6990
uid      Erwin Lansing <erwin@FreeBSD.org>
uid      Erwin Lansing <erwin@droso.dk>
uid      Erwin Lansing <erwin@droso.org>
```

sub 2048g/7C64013D 1998-07-03

D.3.92 Sam Lawrance <lawrance@FreeBSD.org>

pub 1024D/32708C59 2003-08-14
 Key fingerprint = 1056 2A02 5247 64D4 538D 6975 8851 7134 3270 8C59
 uid Sam Lawrance <lawrance@FreeBSD.org>
 uid Sam Lawrance <boris@brooknet.com.au>
 sub 2048g/0F9CCF92 2003-08-14

D.3.93 李彦明<leeym@FreeBSD.org>

pub 1024R/5EB52E51 1999-03-03 Yen-Ming Lee <leeym@FreeBSD.org>
 Key fingerprint = FE 7E 04 56 FC D7 24 21 B9 3B 53 06 E8 93 B5 81
 uid Yen-Ming Lee <leeym@civil.ncku.edu.tw>
 uid Yen-Ming Lee <leeym@cae.ce.ntu.edu.tw>
 uid Yen-Ming Lee <leeym@leeym.com>

D.3.94 Sam Leffler <sam@FreeBSD.org>

pub 1024D/BD147743 2005-03-28
 Key fingerprint = F618 F2FC 176B D201 D91C 67C6 2E33 A957 BD14 7743
 uid Samuel J. Leffler <sam@freebsd.org>
 sub 2048g/8BA91D05 2005-03-28

D.3.95 Jean-Yves Lefort <jylefort@FreeBSD.org>

pub 1024D/A3B8006A 2002-09-07
 Key fingerprint = CC99 D1B0 8E44 293D 32F7 D92E CB30 FB51 A3B8 006A
 uid Jean-Yves Lefort <jylefort@FreeBSD.org>
 uid Jean-Yves Lefort <jylefort@brutele.be>
 sub 4096g/C9271AFC 2002-09-07

D.3.96 Alexander Leidinger <netchild@FreeBSD.org>

pub 1024D/B0063FE7 1999-11-11
 Key fingerprint = C518 BC70 E67F 143F BE91 3365 79E2 9C60 B006 3FE7
 uid Alexander Leidinger (Privat) <Alexander@Leidinger.net>
 sub 1024g/263CAC76 1999-11-11
 pub 1024D/72077137 2002-01-31
 Key fingerprint = AA3A 8F69 B214 6BBD 5E73 C9A0 C604 3C56 7207 7137
 uid Alexander Leidinger <netchild@FreeBSD.org>
 sub 2048g/8C9828D3 2002-01-31

D.3.97 Dejan Lesjak <lesi@FreeBSD.org>

```
pub 1024D/96C5221F 2004-08-18 Dejan Lesjak <lesi@FreeBSD.org>
    Key fingerprint = 2C5C 02EA 1060 1D6D 9982 38C0 1DA7 DBC4 96C5 221F
uid                               Dejan Lesjak <dejan.lesjak@ijs.si>
sub 1024g/E0A69278 2004-08-18
```

D.3.98 Chuck Lever <cel@FreeBSD.org>

```
pub 1024D/8FFC2B87 2006-02-13
    Key fingerprint = 6872 923F 5012 F88B 394C 2F69 37B4 8171 8FFC 2B87
uid                               Charles E. Lever <cel@freebsd.org>
sub 2048g/9BCE0459 2006-02-13
```

D.3.99 Greg Lewis <glewis@FreeBSD.org>

```
pub 1024D/1BB6D9E0 2002-03-05 Greg Lewis (FreeBSD) <glewis@FreeBSD.org>
    Key fingerprint = 2410 DA6D 5A3C D801 65FE C8DB DEEA 9923 1BB6 D9E0
uid                               Greg Lewis <glewis@eyesbeyond.com>
sub 2048g/45E67D60 2002-03-05
```

D.3.100 李鑫 <delphij@FreeBSD.org>

```
pub 1024D/CAEEB8C0 2004-01-28
    Key fingerprint = 43B8 B703 B8DD 0231 B333 DC28 39FB 93A0 CAEE B8C0
uid                               Xin LI <delphij@FreeBSD.org>
uid                               Xin LI <delphij@frontfree.net>
uid                               Xin LI <delphij@delphij.net>
uid                               Xin LI <delphij@geekcn.org>

pub 1024D/42EA8A4B 2006-01-27 [expires: 2008-01-01]
    Key fingerprint = F19C 2616 FA97 9C13 2581 C6F3 85C5 1CCE 42EA 8A4B
uid                               Xin LI <delphij@geekcn.org>
uid                               Xin LI <delphij@FreeBSD.org>
uid                               Xin LI <delphij@delphij.net>
sub 4096g/11A94A02 2006-01-27 [expires: 2008-01-01]
```

D.3.101 Tai-hwa Liang <avatar@FreeBSD.org>

```
pub 1024R/F4013AB1 1998-05-13 Tai-hwa Liang <avatar@FreeBSD.org>
    Key fingerprint = 5B 05 1D 37 7F 35 31 4E 5D 38 BD 07 10 32 B9 D0
uid                               Tai-hwa Liang <avatar@mmlab.cse.yzu.edu.tw>
```

D.3.102 廖英杰<ijliao@FreeBSD.org>

```
pub 1024D/11C02382 2001-01-09 Ying-Chieh Liao <ijliao@CCCA.NCTU.edu.tw>
    Key fingerprint = 4E98 55CC 2866 7A90 EFD7 9DA5 ACC6 0165 11C0 2382
uid                                Ying-Chieh Liao <ijliao@FreeBSD.org>
uid                                Ying-Chieh Liao <ijliao@csie.nctu.edu.tw>
uid                                Ying-Chieh Liao <ijliao@dragon2.net>
uid                                Ying-Chieh Liao <ijliao@tw.FreeBSD.org>
sub 4096g/C1E16E89 2001-01-09
```

D.3.103 林东毅<clive@FreeBSD.org>

```
pub 1024D/A008C03E 2001-07-30 Clive Lin <clive@tongi.org>
    Key fingerprint = FA3F 20B6 A77A 6CEC 1856 09B0 7455 2805 A008 C03E
uid                                Clive Lin <clive@CirX.ORG>
uid                                Clive Lin <clive@FreeBSD.org>
sub 1024g/03C2DC87 2001-07-30 [expires: 2005-08-25]
```

D.3.104 Mark Linimon <linimon@FreeBSD.org>

```
pub 1024D/84C83473 2003-10-09
    Key fingerprint = 8D43 1B55 D127 0BFC 842E 1C96 803C 5A34 84C8 3473
uid                                Mark Linimon <linimon@FreeBSD.org>
uid                                Mark Linimon <linimon@lonesome.com>
sub 1024g/24BFF840 2003-10-09
```

D.3.105 Tilman Linneweh <arved@FreeBSD.org>

```
pub 1024D/807AC53A 2002-06-03 Tilman Linneweh <e0025974@student.tuwien.ac.at>
    Key fingerprint = A92F 344F 31A8 B8DE DDFA 7FB4 7C22 C39F 807A C53A
uid                                Tilman Linneweh <arved@arved.at>
uid                                Tilman Linneweh <arved@FreeBSD.org>
uid                                Tilman Linneweh <linneweh@zid.tuwien.ac.at>
sub 1024g/FA351986 2002-06-03 [expires: 2006-07-19]
```

D.3.106 Remko Lodder <remko@FreeBSD.org>

```
pub 1024D/8F494B77 2004-09-03 Remko Lodder (my FreeBSD.org uid) <remko@FreeBSD.org>
    Key fingerprint = 575D 8AD6 8646 E6D2 1226 0A8C D2A9 0DFF 8F49 4B77
uid                                Remko Lodder (Remko Lodder) <remko@elvandar.org>
sub 2048g/D843AEDD 2004-09-03 [expires: 2005-09-03]
```

D.3.107 Scott Long <scottl@FreeBSD.org>

```
pub 1024D/017C5EBF 2003-01-18 Scott A. Long (This is my official FreeBSD key) <scottl@freebsd.org>
    Key fingerprint = 34EA BD06 44F7 F8C3 22BC B52C 1D3A F6D1 017C 5EBF
sub 1024g/F61C8F91 2003-01-18
```

D.3.108 Pav Lucistnik <pav@FreeBSD.org>

```
pub 1024D/C14EB282 2003-08-25 Pav Lucistnik <pav@FreeBSD.org>
    Key fingerprint = 2622 B7E3 7DA5 5C53 2079 855B 9ED7 583F C14E B282
uid Pav Lucistnik <pav@oook.cz>
sub 1024g/7287A947 2003-08-25
```

D.3.109 Bruce A. Mah <bmah@FreeBSD.org>

```
pub 1024D/5BA052C3 1997-12-08
    Key fingerprint = F829 B805 207D 14C7 7197 7832 D8CA 3171 5BA0 52C3
uid Bruce A. Mah <bmah@acm.org>
uid Bruce A. Mah <bmah@ca.sandia.gov>
uid Bruce A. Mah <bmah@ieee.org>
uid Bruce A. Mah <bmah@cisco.com>
uid Bruce A. Mah <bmah@employees.org>
uid Bruce A. Mah <bmah@freebsd.org>
uid Bruce A. Mah <bmah@packetdesign.com>
uid Bruce A. Mah <bmah@kitchenlab.org>
sub 2048g/B4E60EA1 1997-12-08
```

D.3.110 Mike Makonnen <mtm@FreeBSD.org>

```
pub 1024D/7CD41F55 2004-02-06 Michael Telahun Makonnen <mtm@FreeBSD.Org>
    Key fingerprint = AC7B 5672 2D11 F4D0 EBF8 5279 5359 2B82 7CD4 1F55
uid Michael Telahun Makonnen <mtm@tmsa-inc.com>
uid Mike Makonnen <mtm@identd.net>
uid Michael Telahun Makonnen <mtm@acs-et.com>
sub 2048g/E7DC936B 2004-02-06
```

D.3.111 David Malone <dwmalone@FreeBSD.org>

```
pub 512/40378991 1994/04/21 David Malone <dwmalone@maths.tcd.ie>
    Key fingerprint = 86 A7 F4 86 39 2C 47 2C C1 C2 35 78 8E 2F B8 F5
```


D.3.112 Sergey Matveychuk <sem@FreeBSD.org>

```
pub 1024D/B71F605D 1999-10-13
    Key fingerprint = 4704 F374 DB28 BEC6 51C8 1322 4DC9 4BD8 B71F 605D
uid          Sergey Matveychuk <sem@FreeBSD.org>
uid          Sergey Matveychuk <sem@ciam.ru>
uid          Sergey Matveychuk <sem@core.inec.ru>
sub 2048g/DEAF9D91 1999-10-13
```

D.3.113 Emanuel Haupt <ehaupt@FreeBSD.org>

```
pub 1024D/55E67774 2005-07-08 [expires: 2007-12-19]
    Key fingerprint = 17B3 FD8F BA68 4AB4 10FD A9D1 AD52 6588 55E6 7774
uid          Emanuel Haupt <ehaupt@FreeBSD.org>
uid          Emanuel Haupt <ehaupt@critical.ch>
uid          Emanuel Haupt <haupt@critical.ch>
sub 4096g/CDEE5E7D 2005-07-08 [expires: 2006-01-04]
```

D.3.114 Koop Mast <kwm@FreeBSD.org>

```
pub 1024D/F95426DA 2004-09-10 Koop Mast <kwm@rainbow-runner.nl>
    Key fingerprint = C66F 1835 0548 3440 8576 0FFE 6879 B7CD F954 26DA
uid          Koop Mast <kwm@FreeBSD.org>
sub 1024g/A782EEDD 2004-09-10
```

D.3.115 Makoto Matsushita <matusita@FreeBSD.org>

```
pub 1024D/20544576 1999-04-18
    Key fingerprint = 71B6 13BF B262 2DD8 2B7C 6CD0 EB2D 4147 2054 4576
uid          Makoto Matsushita <matusita@matatabi.or.jp>
uid          Makoto Matsushita <matusita@FreeBSD.org>
uid          Makoto Matsushita <matusita@jp.FreeBSD.ORG>
uid          Makoto Matsushita <matusita@ist.osaka-u.ac.jp>
sub 1024g/F1F3C94D 1999-04-18
```

D.3.116 Tom McLaughlin <tmclaugh@FreeBSD.org>

```
pub 1024D/E2F7B3D8 2005-05-24
    Key fingerprint = 7692 B222 8D23 CF94 1993 0138 E339 E225 E2F7 B3D8
uid          Tom McLaughlin (Personal email address) <tmclaugh@sdf.lonestar.org>
uid          Tom McLaughlin (Work email address) <tmclaughlin@meditech.com>
uid          Tom McLaughlin (FreeBSD email address) <tmclaugh@FreeBSD.org>
sub 2048g/16838F62 2005-05-24
```

D.3.117 Jean Milanez Melo <jmelo@FreeBSD.org>

```
pub 1024D/AA5114BF 2006-03-03
    Key fingerprint = 826D C2AA 6CF2 E29A EBE7 4776 D38A AB83 AA51 14BF
uid          Jean Milanez Melo <jmelo@FreeBSD.org>
uid          Jean Milanez Melo <jmelo@freebsdbrasil.com.br>
sub 4096g/E9E1CBD9 2006-03-03
```

D.3.118 Kenneth D. Merry <ken@FreeBSD.org>

```
pub 1024D/54C745B5 2000-05-15 Kenneth D. Merry <ken@FreeBSD.org>
    Key fingerprint = D25E EBC5 F17A 9E52 84B4 BF14 9248 F0DA 54C7 45B5
uid          Kenneth D. Merry <ken@kdm.org>
sub 2048g/89D0F797 2000-05-15

pub 1024R/2FA0A505 1995-10-30 Kenneth D. Merry <ken@plutotech.com>
    Key fingerprint = FD FA 85 85 95 C4 8E E8 98 1A CA 18 56 F0 00 1F
```

D.3.119 Dirk Meyer <dinoex@FreeBSD.org>

```
pub 1024R/331CDA5D 1995-06-04 Dirk Meyer <dinoex@FreeBSD.org>
    Key fingerprint = 44 16 EC 0A D3 3A 4F 28 8A 8A 47 93 F1 CF 2F 12
uid          Dirk Meyer <dirk.meyer@dinoex.sub.org>
uid          Dirk Meyer <dirk.meyer@guug.de>
```

D.3.120 Yoshiro Sanpei MIHIRA <sanpei@FreeBSD.org>

```
pub 1024R/391C5D69 1996-11-21 sanpei@SEAPLE.ICC.NE.JP
    Key fingerprint = EC 04 30 24 B0 6C 1E 63 5F 5D 25 59 3E 83 64 51
uid          MIHIRA Yoshiro <sanpei@sanpei.org>
uid          Yoshiro MIHIRA <sanpei@FreeBSD.org>
uid          MIHIRA Yoshiro <sanpei@yy.cs.keio.ac.jp>
uid          MIHIRA Yoshiro <sanpei@cc.keio.ac.jp>
uid          MIHIRA Yoshiro <sanpei@educ.cc.keio.ac.jp>
uid          MIHIRA Yoshiro <sanpei@st.keio.ac.jp>
```

D.3.121 Marcel Moolenaar <marcel@FreeBSD.org>

```
pub 1024D/61EE89F6 2002-02-09 Marcel Moolenaar <marcel@xcllnt.net>
    Key fingerprint = 68BB E2B7 49AA FF69 CA3A DF71 A605 A52D 61EE 89F6
sub 1024g/6EAB456 2002-02-09
```

D.3.122 Dmitry Morozovsky <marck@FreeBSD.org>

```
pub 1024D/6B691B03 2001-07-20
    Key fingerprint = 39AC E336 F03D C0F8 5305 B725 85D4 5045 6B69 1B03
uid          Dmitry Morozovsky <marck@rinet.ru>
uid          Dmitry Morozovsky <marck@FreeBSD.org>
sub 2048g/44D656F8 2001-07-20
```

D.3.123 Thomas Möstl <tmml@FreeBSD.org>

```
pub 1024D/419C776C 2000-11-28 Thomas Moestl <tmml@FreeBSD.org>
    Key fingerprint = 1C97 A604 2BD0 E492 51D0 9C0F 1FE6 4F1D 419C 776C
uid          Thomas Moestl <tmoestl@gmx.net>
uid          Thomas Moestl <t.moestl@tu-bs.de>
sub 2048g/ECE63CE6 2000-11-28
```

D.3.124 Rich Murphey <rich@FreeBSD.org>

```
pub 1024R/583443A9 1995-03-31 Rich Murphey <rich@lamprey.utmb.edu>
    Key fingerprint = AF A0 60 C4 84 D6 0C 73 D1 EF C0 E9 9D 21 DB E4
```

D.3.125 Akinori MUSHASHA <knu@FreeBSD.org>

```
pub 1024D/9FD9E1EE 2000-03-21 Akinori MUSHASHA <knu@and.or.jp>
    Key fingerprint = 081D 099C 1705 861D 4B70 B04A 920B EFC7 9FD9 E1EE
uid          Akinori MUSHASHA <knu@FreeBSD.org>
uid          Akinori MUSHASHA <knu@idaemons.org>
uid          Akinori MUSHASHA <knu@ruby-lang.org>
sub 1024g/71BA9D45 2000-03-21
```

D.3.126 Masafumi NAKANE <max@FreeBSD.org>

```
pub 1024D/CE356B59 2000-02-19 Masafumi NAKANE <max@wide.ad.jp>
    Key fingerprint = EB40 BCAB 4CE5 0764 9942 378C 9596 159E CE35 6B59
uid          Masafumi NAKANE <max@FreeBSD.org>
uid          Masafumi NAKANE <max@accessibility.org>
uid          Masafumi NAKANE <kd5pdi@qsl.net>
sub 1024g/FA9BD48B 2000-02-19
```

D.3.127 Yoichi NAKAYAMA <yoichi@FreeBSD.org>

```
pub 1024D/E0788E46 2000-12-28 Yoichi NAKAYAMA <yoichi@assist.media.nagoya-u.ac.jp>
    Key fingerprint = 1550 2662 46B3 096C 0460 BC03 800D 0C8A E078 8E46
uid          Yoichi NAKAYAMA <yoichi@eken.phys.nagoya-u.ac.jp>
```

```
uid                               Yoichi NAKAYAMA <yoichi@FreeBSD.org>
sub 1024g/B987A394 2000-12-28
```

D.3.128 Alexander Nedotsukov <bland@FreeBSD.org>

```
pub 1024D/D004116C 2003-08-14 Alexander Nedotsukov <bland@FreeBSD.org>
   Key fingerprint = 35E2 5020 55FC 2071 4ADD 1A4A 86B6 8A5D D004 116C
sub 1024g/1CCA8D46 2003-08-14
```

D.3.129 Simon L. Nielsen <simon@FreeBSD.org>

```
pub 1024D/27359A51 2003-07-22 [expires: 2006-07-21]
   Key fingerprint = 912B F341 7E90 2049 05B4 3800 87DA 5C0D 2735 9A51
uid                               Simon L. Nielsen <simon@nitro.dk>
uid                               Simon L. Nielsen <simon@FreeBSD.org>
sub 2048g/C11D9097 2003-07-22 [expires: 2006-07-21]
```

D.3.130 Anders Nordby <anders@FreeBSD.org>

```
pub 1024D/00835956 2000-08-13 Anders Nordby <anders@fix.no>
   Key fingerprint = 1E0F C53C D8DF 6A8F EAAD 19C5 D12A BC9F 0083 5956
uid                               Anders Nordby <anders@FreeBSD.org>
sub 2048g/4B160901 2000-08-13
```

D.3.131 David O'Brien <obrien@FreeBSD.org>

```
pub 1024R/34F9F9D5 1995-04-23 David E. O'Brien <defunct - obrien@Sea.Legent.com>
   Key fingerprint = B7 4D 3E E9 11 39 5F A3 90 76 5D 69 58 D9 98 7A
uid                               David E. O'Brien <obrien@Nuxi.com>
uid                               deobrien@ucdavis.edu
uid                               David E. O'Brien <whois Do38>
uid                               David E. O'Brien <obrien@FreeBSD.org>
uid                               David E. O'Brien <dobrien@seas.gwu.edu>
uid                               David E. O'Brien <obrien@cs.ucdavis.edu>
uid                               David E. O'Brien <defunct - obrien@media.sra.com>
uid                               David E. O'Brien <obrien@elsewhere.roanoke.va.us>
uid                               David E. O'Brien <obrien@Nuxi.com>

pub 1024D/7F9A9BA2 1998-06-10 "David E. O'Brien" <obrien@cs.ucdavis.edu>
   Key fingerprint = 02FD 495F D03C 9AF2 5DB7 F496 6FC8 DABD 7F9A 9BA2
uid                               "David E. O'Brien" <obrien@Nuxi.com>
uid                               "David E. O'Brien" <obrien@FreeBSD.org>
sub 3072g/BA32C20D 1998-06-10
```

D.3.132 Philip Paeps <philip@FreeBSD.org>

```

pub 1024D/049DB879 2001-01-04 Philip Paeps <philip@paeps.cx>
    Key fingerprint = FA74 3C27 91A6 79D5 F6D3 FC53 BF4B D0E6 049D B879
uid                                     Philip Paeps <philip@pub.telenet.be>
uid                                     Philip Paeps <philip.paeps@pandora.be>
uid                                     Philip Paeps <philip@nixsys.be>
uid                                     Philip Paeps <philip@freebsd.org>
sub 2048g/476FFC94 2001-01-04

```

D.3.133 Hiten Pandya <hmp@FreeBSD.org>

```

pub 1024D/938CACA8 2004-02-13 Hiten Pandya (FreeBSD) <hmp@FreeBSD.org>
    Key fingerprint = 84EB C75E C75A 50ED 304E E446 D974 7842 938C ACA8
uid                                     Hiten Pandya <hmp@backplane.com>
sub 2048g/783874B5 2004-02-13

```

D.3.134 Mark Peek <mp@FreeBSD.org>

```

pub 1024D/330D4D01 2002-01-27 Mark Peek <mp@FreeBSD.org>
    Key fingerprint = 510C 96EE B4FB 1B0A 2CF8 A0AF 74B0 0B0E 330D 4D01
sub 1024g/9C6CAC09 2002-01-27

```

D.3.135 Peter Pentchev <roam@FreeBSD.org>

```

pub 1024D/16194553 2002-02-01
    Key fingerprint = FDBA FD79 C26F 3C51 C95E DF9E ED18 B68D 1619 4553
uid                                     Peter Pentchev <roam@ringlet.net>
uid                                     Peter Pentchev <roam@sbnd.net>
uid                                     Peter Pentchev <roam@FreeBSD.org>
uid                                     Peter Pentchev <roam@online.bg>
uid                                     Peter Pentchev <roam@orbitel.bg>
uid                                     Peter Pentchev <roam@techlab.office1.bg>
uid                                     Peter Pentchev <roam@cnsys.bg>
sub 1024g/7074473C 2002-02-01

```

D.3.136 Denis Peplin <den@FreeBSD.org>

```

pub 1024D/485DDDF5 2003-09-11 Denis Peplin <den@FreeBSD.org>
    Key fingerprint = 495D 158C 8EC9 C2C1 80F5 EA96 6F72 7C1C 485D DDF5
sub 1024g/E70BA158 2003-09-11

```

D.3.137 Gerald Pfeifer <gerald@FreeBSD.org>

```
pub 1024D/745C015A 1999-11-09 Gerald Pfeifer <gerald@pfeifer.com>
    Key fingerprint = B215 C163 3BCA 0477 615F 1B35 A5B3 A004 745C 015A
uid                                Gerald Pfeifer <Gerald.Pfeifer@vibe.at>
uid                                Gerald Pfeifer <pfeifer@dbai.tuwien.ac.at>
uid                                Gerald Pfeifer <gerald@pfeifer.at>
uid                                Gerald Pfeifer <gerald@FreeBSD.org>
sub 1536g/F0156927 1999-11-09
```

D.3.138 John Polstra <jdp@FreeBSD.org>

```
pub 1024R/BFBCF449 1997-02-14 John D. Polstra <jdp@polstra.com>
    Key fingerprint = 54 3A 90 59 6B A4 9D 61 BF 1D 03 09 35 8D F6 0D
```

D.3.139 Kirill Ponomarew <krion@FreeBSD.org>

```
pub 1024D/AEB426E5 2002-04-07
    Key fingerprint = 58E7 B953 57A2 D9DD 4960 2A2D 402D 46E9 AEB4 26E5
uid                                Kirill Ponomarew <krion@voodoo.bawue.com>
uid                                Kirill Ponomarew <krion@guug.de>
uid                                Kirill Ponomarew <krion@FreeBSD.org>
sub 1024D/05AC7CA0 2006-01-30 [expires: 2008-01-30]
sub 2048g/C3EE5537 2006-01-30 [expires: 2008-01-30]
```

D.3.140 Mark Pulford <markp@FreeBSD.org>

```
pub 1024D/182C368F 2000-05-10 Mark Pulford <markp@FreeBSD.org>
    Key fingerprint = 58C9 C9BF C758 D8D4 7022 8EF5 559F 7F7B 182C 368F
uid                                Mark Pulford <mark@kyne.com.au>
sub 2048g/380573E8 2000-05-10
```

D.3.141 Thomas Quinot <thomas@FreeBSD.org>

```
pub 1024D/393D2469 1999-09-23 Thomas Quinot <thomas@cuivre.fr.eu.org>
    Empreinte de la clé = 4737 A0AD E596 6D30 4356 29B8 004D 54B8 393D 2469
uid                                Thomas Quinot <thomas@debian.org>
uid                                Thomas Quinot <thomas@FreeBSD.org>
sub 1024g/8DE13BB2 1999-09-23
```

D.3.142 Herve Quiroz <hq@FreeBSD.org>

```
pub 1024D/85AC8A80 2004-07-22 Herve Quiroz <hq@FreeBSD.org>
    Key fingerprint = 14F5 BC56 D736 102D 41AF A07B 1D97 CE6C 85AC 8A80
uid                                     Herve Quiroz <herve.quiroz@esil.univ-mrs.fr>
sub 1024g/8ECCAFED 2004-07-22
```

D.3.143 Doug Rabson <dfr@FreeBSD.org>

```
pub 1024R/95C11771 2000-02-27 Doug Rabson <dfr@freebsd.org>
    Key fingerprint = 20 BB E4 38 5D 89 D2 D4 68 A6 2F DC 0A DE 10 3C
```

D.3.144 Jim Rees <rees@FreeBSD.org>

```
pub 512/B623C791 1995/02/21 Jim Rees <rees@umich.edu>
    Key fingerprint = 02 5F 1B 15 B4 6E F1 3E F1 C5 E0 1D EA CC 17 88
```

D.3.145 Tom Rhodes <trhodes@FreeBSD.org>

```
pub 1024D/1B9EBD43 2002-01-15 Tom Rhodes <trhodes@FreeBSD.org>
    Key fingerprint = 2D4D 1D31 A5C6 08AA 1075 C963 C0F9 A089 1B9E BD43
uid                                     Tom Rhodes <darklogik@pittgoth.com>
sub 3072g/F7A606E4 2002-01-15
```

D.3.146 Benno Rice <benno@FreeBSD.org>

```
pub 1024D/87C59909 2002-01-16 Benno Rice <benno@FreeBSD.org>
    Key fingerprint = CE27 DADA 08E3 FAA3 88F1 5B31 5E34 705A 87C5 9909
uid                                     Benno Rice <benno@jeamland.net>
sub 1024g/4F7C2BAD 2002-01-16 [expires: 2007-01-15]
```

D.3.147 Matteo Riondato <matteo@FreeBSD.org>

```
pub 1024D/1EC56BEC 2003-01-05
    Key fingerprint = F0F3 1B43 035D 65B1 08E9 4D66 D8CA 78A5 1EC5 6BEC
uid                                     Matteo Riondato (Rionda) <rionda@FreeSBIE.ORG>
uid                                     Matteo Riondato (Rionda) <rionda@riondabsd.net>
uid                                     Matteo Riondato (Rionda) <rionda@autistici.org>
uid                                     Matteo Riondato (Rionda) <rionda@gufi.org>
uid                                     Matteo Riondato (Rionda) <matteo@riondato.com>
uid                                     Matteo Riondato (Rionda) <rionda@riondato.com>
uid                                     Matteo Riondato (Rionda) <matteo@FreeBSD.ORG>
sub 1024g/A040570C 2003-01-05
```

D.3.148 Ollivier Robert <roberto@FreeBSD.org>

```
pub 1024D/7DCAE9D3 1997-08-21
    Key fingerprint = 2945 61E7 D4E5 1D32 C100 DBEC A04F FB1B 7DCA E9D3
uid      Ollivier Robert <roberto@keltia.freenix.fr>
uid      Ollivier Robert <roberto@FreeBSD.org>
sub 2048g/C267084D 1997-08-21
```

D.3.149 Craig Rodrigues <rodrigc@FreeBSD.org>

```
pub 1024D/3998479D 2005-05-20
    Key fingerprint = F01F EBE6 F5C8 6DC2 954F 098F D20A 8A2A 3998 479D
uid      Craig Rodrigues <rodrigc@freebsd.org>
uid      Craig Rodrigues <rodrigc@crodrigues.org>
sub 2048g/AA77E09B 2005-05-20
```

D.3.150 Guido van Rooij <guido@FreeBSD.org>

```
pub 1024R/599F323D 1996-05-18 Guido van Rooij <guido@gvr.org>
    Key fingerprint = 16 79 09 F3 C0 E4 28 A7 32 62 FA F6 60 31 C0 ED
uid      Guido van Rooij <guido@gvr.win.tue.nl>

pub 1024D/A95102C1 2000-10-25 Guido van Rooij <guido@madison-gurkha.nl>
    Key fingerprint = 5B3E 51B7 0E7A D170 0574 1E51 2471 117F A951 02C1
uid      Guido van Rooij <guido@madison-gurkha.com>
sub 1024g/A5F20553 2000-10-25
```

D.3.151 Niklas Saers <niklas@FreeBSD.org>

```
pub 1024D/C822A476 2004-03-09 Niklas Saers <niklas@saers.com>
    Key fingerprint = C41E F734 AF0E 3D21 7499 9EB1 9A31 2E7E C822 A476
sub 1024g/81E2FF36 2004-03-09
```

D.3.152 Mark Santcroos <marks@FreeBSD.org>

```
pub 1024D/DBE7EB8E 2005-03-08
    Key fingerprint = C0F0 44F3 3F15 520F 6E32 186B BE0A BA42 DBE7 EB8E
uid      Mark Santcroos <marks@ripe.net>
uid      Mark Santcroos <mark@santcroos.net>
uid      Mark Santcroos <marks@freebsd.org>
sub 2048g/FFF80F85 2005-03-08
```


D.3.153 Hiroki Sato <hrs@FreeBSD.org>

```

pub 1024D/2793CF2D 2001-06-12
    Key fingerprint = BDB3 443F A5DD B3D0 A530 FFD7 4F2C D3D8 2793 CF2D
uid      Hiroki Sato <hrs@allbsd.org>
uid      Hiroki Sato <hrs@eos.ocn.ne.jp>
uid      Hiroki Sato <hrs@ring.gr.jp>
uid      Hiroki Sato <hrs@FreeBSD.org>
uid      Hiroki Sato <hrs@jp.FreeBSD.org>
uid      Hiroki Sato <hrs@vlsi.ee.noda.tus.ac.jp>
uid      Hiroki Sato <hrs@jp.NetBSD.org>
uid      Hiroki Sato <hrs@NetBSD.org>
sub 1024g/8CD251FF 2001-06-12

```

D.3.154 Wolfram Schneider <wosch@FreeBSD.org>

```

Type Bits/KeyID   Date      User ID
pub 1024/2B7181AD 1997/08/09 Wolfram Schneider <wosch@FreeBSD.org>
    Key fingerprint = CA 16 91 D9 75 33 F1 07 1B F0 B4 9F 3E 95 B6 09

```

D.3.155 David Schultz <das@FreeBSD.org>

```

pub 1024D/BE848B57 2001-07-19 David Schultz <das@FreeBSD.ORG>
    Key fingerprint = 0C12 797B A9CB 19D9 FDAF 2A39 2D76 A2DB BE84 8B57
uid David Schultz <dschultz@uclink.Berkeley.EDU>
uid David Schultz <das@FreeBSD.ORG>
sub 2048g/69206E8E 2001-07-19

```

D.3.156 Jens Schweikhardt <schweikh@FreeBSD.org>

```

pub 1024D/0FF231FD 2002-01-27 Jens Schweikhardt <schweikh@FreeBSD.org>
    Key fingerprint = 3F35 E705 F02F 35A1 A23E 330E 16FE EA33 0FF2 31FD
uid      Jens Schweikhardt <schweikh@schweikhardt.net>
sub 1024g/6E93CACC 2002-01-27 [expires: 2005-01-26]

```

D.3.157 Johan van Selst <johans@FreeBSD.org>

```

pub 1024D/7DA5C53B 2001-03-03
    Key fingerprint = 3021 482B 52C1 3FFE 4752 4D57 68E1 252B 7DA5 C53B
uid      Johan van Selst <johans@stack.nl>
uid      Johan van Selst <johans@unix.nl>
uid      Johan van Selst <johans@gletsjer.net>
uid      Johan van Selst <johans@vrijschrift.org>
uid      Johan van Selst <johans@FreeBSD.org>
sub 2048g/EF1C75DD 2001-03-03
sub 1024R/355F8408 2005-11-05

```

sub 1024R/9AF7EE88 2005-11-05

D.3.158 Gregory Neil Shapiro <gshapiro@FreeBSD.org>

```
pub 1024R/4FBE2ADD 2000-10-13 Gregory Neil Shapiro <gshapiro@gshapiro.net>
   Key fingerprint = 56 D5 FF A7 A6 54 A6 B5 59 10 00 B9 5F 5F 20 09
uid                               Gregory Neil Shapiro <gshapiro@FreeBSD.org>

pub 1024D/F76A9BF5 2001-11-14 Gregory Neil Shapiro <gshapiro@FreeBSD.org>
   Key fingerprint = 3B5E DAF1 4B04 97BA EE20 F841 21F9 C5BC F76A 9BF5
uid                               Gregory Neil Shapiro <gshapiro@gshapiro.net>
sub 2048g/935657DC 2001-11-14

pub 1024D/FCE56561 2000-10-14 Gregory Neil Shapiro <gshapiro@FreeBSD.org>
   Key fingerprint = 42C4 A87A FD85 C34F E77F 5EA1 88E1 7B1D FCE5 6561
uid                               Gregory Neil Shapiro <gshapiro@gshapiro.net>
sub 1024g/285DC8A0 2000-10-14 [expires: 2001-10-14]
```

D.3.159 Arun Sharma <arun@FreeBSD.org>

```
pub 1024D/7D112181 2003-03-06 Arun Sharma <arun@sharma-home.net>
   Key fingerprint = A074 41D6 8537 C7D5 070E 0F78 0247 1AE2 7D11 2181
uid                               Arun Sharma <arun@freebsd.org>
uid                               Arun Sharma <arun.sharma@intel.com>
sub 1024g/ACAD98DA 2003-03-06 [expires: 2005-03-05]
```

D.3.160 Norikatsu Shigemura <nork@FreeBSD.org>

```
pub 1024D/7104EA4E 2005-02-14
   Key fingerprint = 9580 60A3 B58A 0864 79CB 779A 6FAE 229B 7104 EA4E
uid                               Norikatsu Shigemura <nork@cityfujisawa.ne.jp>
uid                               Norikatsu Shigemura <nork@ninth-nine.com>
uid                               Norikatsu Shigemura <nork@FreeBSD.org>
sub 4096g/EF56997E 2005-02-14
```

D.3.161 徐三泰 <vanilla@FreeBSD.org>

```
pub 1024D/ACE75853 2001-11-20 Vanilla I. Shu <vanilla@FreeBSD.org>
   Key fingerprint = 290F 9DB8 42A3 6257 5D9A 5585 B25A 909E ACE7 5853
sub 1024g/CE695D0E 2001-11-20
```

D.3.162 Dmitry Sivachenko <demon@FreeBSD.org>

```
pub 1024D/13D5DF80 2002-03-18 Dmitry Sivachenko <mitya@cavia.pp.ru>
    Key fingerprint = 72A9 12C9 BB02 46D4 4B13 E5FE 1194 9963 13D5 DF80
uid                                     Dmitry S. Sivachenko <demon@FreeBSD.org>
sub 1024g/060F6DBD 2002-03-18
```

D.3.163 Jesper Skriver <jesper@FreeBSD.org>

```
pub 1024D/F9561C31 2001-03-09 Jesper Skriver <jesper@FreeBSD.org>
    Key fingerprint = 6B88 9CE8 66E9 E631 C9C5 5EB4 22AB F0EC F956 1C31
uid                                     Jesper Skriver <jesper@skriver.dk>
uid                                     Jesper Skriver <jesper@wheel.dk>
sub 1024g/777C378C 2001-03-09
```

D.3.164 Ville Skyttä <scop@FreeBSD.org>

```
pub 1024D/BCD241CB 2002-04-07 Ville Skyttä <ville.skytta@iki.fi>
    Key fingerprint = 4E0D EBAB 3106 F1FA 3FA9 B875 D98C D635 BCD2 41CB
uid                                     Ville Skyttä <ville.skytta@xemacs.org>
uid                                     Ville Skyttä <scop@FreeBSD.org>
sub 2048g/9426F4D1 2002-04-07
```

D.3.165 Andrey Slusar <anray@FreeBSD.org>

```
pub 1024D/AE7B5418 2005-12-12
    Key fingerprint = DE70 C24B 55A0 4A06 68A1 D425 3C59 9A9B AE7B 5418
uid                                     Andrey Slusar <anray@ext.by>
uid                                     Andrey Slusar <anrays@gmail.com>
uid                                     Andrey Slusar <anray@FreeBSD.org>
sub 2048g/7D0EB77D 2005-12-12
```

D.3.166 Gleb Smirnoff <glebius@FreeBSD.org>

```
pub 1024D/1949DC80 2003-08-25
    Key fingerprint = 872C E14A 2F03 A3E8 D882 026E 5DE4 D7FE 1949 DC80
uid                                     Gleb Smirnoff <glebius@FreeBSD.org>
uid                                     Gleb Smirnoff <glebius@cell.sick.ru>
uid                                     Gleb Smirnoff <glebius@bestcom.ru>
uid                                     Gleb Smirnoff <glebius@rambler-co.ru>
uid                                     Gleb Smirnoff <glebius@freebsd.org>
uid                                     Gleb Smirnoff <glebius@freebsd.int.ru>
sub 1024g/A05118BD 2003-08-25
```

D.3.167 Ken Smith <kensmith@FreeBSD.org>

```
pub 1024D/29AEA7F6 2003-12-02 Ken Smith <kensmith@cse.buffalo.edu>
    Key fingerprint = 4AB7 D302 0753 8215 31E7 F1AD FC6D 7855 29AE A7F6
uid                                     Ken Smith <kensmith@freebsd.org>
sub 1024g/0D509C6C 2003-12-02
```

D.3.168 Ben Smithurst <ben@FreeBSD.org>

```
pub 1024D/2CEF442C 2001-07-11 Ben Smithurst <ben@LSRfm.com>
    Key fingerprint = 355D 0FFF B83A 90A9 D648 E409 6CFC C9FB 2CEF 442C
uid                                     Ben Smithurst <ben@vinosystems.com>
uid                                     Ben Smithurst <ben@smithurst.org>
uid                                     Ben Smithurst <ben@FreeBSD.org>
uid                                     Ben Smithurst <csxbscs@comp.leeds.ac.uk>
uid                                     Ben Smithurst <ben@scientia.demon.co.uk>
sub 1024g/347071FF 2001-07-11
```

D.3.169 Dag-Erling C. Smørgrav <des@FreeBSD.org>

```
pub 1024D/A0D39168 2004-08-21 [expires: 2006-08-21]
    Key fingerprint = 82B6 AED6 2F8B 1591 4A92 EE36 3FA0 DE08 A0D3 9168
uid                                     Dag-Erling Smørgrav <des@des.no>
uid                                     Dag-Erling Smørgrav <des@freebsd.org>
uid                                     [jpeg image of size 3868]
sub 1024g/E7611058 2004-08-21 [expires: 2006-08-21]
```

D.3.170 Maxim Sobolev <sobomax@FreeBSD.org>

```
pub 1024D/888205AF 2001-11-21 Maxim Sobolev <sobomax@FreeBSD.org>
    Key fingerprint = 85C9 DCB0 6828 087C C977 3034 A0DB B9B7 8882 05AF
uid                                     Maxim Sobolev <sobomax@mail.ru>
uid                                     Maxim Sobolev <sobomax@altavista.net>
uid                                     Maxim Sobolev <vegacap@i.com.ua>
```

```
pub 1024D/468EE6D8 2003-03-21 Maxim Sobolev <sobomax@portaone.com>
    Key fingerprint = 711B D315 3360 A58F 9A0E 89DB 6D40 2558 468E E6D8
uid                                     Maxim Sobolev <sobomax@FreeBSD.org>
uid                                     Maxim Sobolev <sobomax@mail.ru>
uid                                     Maxim Sobolev <vegacap@i.com.ua>
```

```
pub 1024D/6BEC980A 2004-02-13 Maxim Sobolev <sobomax@portaone.com>
    Key fingerprint = 09D5 47B4 8D23 626F B643 76EB DFEE 3794 6BEC 980A
uid                                     Maxim Sobolev <sobomax@FreeBSD.org>
uid                                     Maksym Sobolyev (It's how they call me in official documents. Pret
uid                                     Maksym Sobolyev (It's how they call me in official documents. Pret
sub 2048g/16D049AB 2004-02-13 [expires: 2005-02-12]
```

D.3.171 Brian Somers <brian@FreeBSD.org>

```
pub 1024R/666A7421 1997-04-30 Brian Somers <brian@freebsd-services.com>
    Key fingerprint = 2D 91 BD C2 94 2C 46 8F 8F 09 C4 FC AD 12 3B 21
uid          Brian Somers <brian@awfulhak.org>
uid          Brian Somers <brian@FreeBSD.org>
uid          Brian Somers <brian@OpenBSD.org>
uid          Brian Somers <brian@uk.FreeBSD.org>
uid          Brian Somers <brian@uk.OpenBSD.org>
```

D.3.172 Nicolas Souchu <nsouch@FreeBSD.org>

```
pub 1024D/C744F18B 2002-02-13 Nicholas Souchu <nsouch@freebsd.org>
    Key fingerprint = 992A 144F AC0F 40BA 55AE DE6D 752D 0A6C C744 F18B
sub 1024g/90BD3231 2002-02-13
```

D.3.173 Suleiman Souhlal <ssouhlal@FreeBSD.org>

```
pub 1024D/2EA50469 2004-07-24 Suleiman Souhlal <ssouhlal@FreeBSD.org>
    Key fingerprint = DACF 89DB 54C7 DA1D 37AF 9A94 EB55 E272 2EA5 0469
sub 2048g/0CDCC535 2004-07-24
```

D.3.174 Rink Springer <rink@FreeBSD.org>

```
pub 1024D/ECEDBFFF 2003-09-19
    Key fingerprint = A8BE 9C82 9B81 4289 A905 418D 6F73 BAD2 ECED BFFF
uid          Rink Springer <rink@il.fontys.nl>
uid          Rink Springer (FreeBSD Project) <rink@FreeBSD.org>
uid          Rink Springer <rink@stack.nl>
sub 2048g/3BC3E67E 2003-09-19
```

D.3.175 Vsevolod Stakhov <vsevolod@FreeBSD.org>

```
pub 1024D/213D0033 2005-03-14 [expires: 2008-03-13]
    Key fingerprint = B852 0010 761E 944A C76D D447 A25D C12C 213D 0033
uid          Vsevolod Stakhov <vsevolod@FreeBSD.org>
uid          Vsevolod Stakhov <cebka@jet.msk.su>
uid          Vsevolod Stakhov <vsevolod@highsecure.ru>
sub 2048g/786F2187 2005-03-14 [expires: 2008-03-13]
```

D.3.176 Volker Stolz <vs@FreeBSD.org>

```
pub 1024R/3FD1B6B5 1998-06-16 Volker Stolz <vs@freebsd.org>
    Key fingerprint = 69 6F BD A0 2E FE 19 66 CF B9 68 6E 41 7D F9 B9
uid Volker Stolz <stolz@i2.informatik.rwth-aachen.de> (LSK)
uid Volker Stolz <vs@foldr.org>
```

D.3.177 宋政隆<clsung@FreeBSD.org>

```
pub 1024D/956E8BC1 2003-09-12 Cheng-Lung Sung <clsung@FreeBSD.org>
    Key fingerprint = E0BC 57F9 F44B 46C6 DB53 8462 F807 89F3 956E 8BC1
uid Cheng-Lung Sung (Software Engineer) <clsung@dragon2.net>
uid Cheng-Lung Sung (Alumnus of CSIE, NCTU, Taiwan) <clsung@sungsung.c
uid Cheng-Lung Sung (AlanSung) <clsung@tiger2.net>
uid Cheng-Lung Sung (FreeBSD@Taiwan) <clsung@freebsd.csie.nctu.edu.tw>
uid Cheng-Lung Sung (Ph.D. Student of NTU.EECS) <d92921016@ntu.edu.tw>
uid Cheng-Lung Sung (FreeBSD Freshman) <clsung@tw.freebsd.org>
uid Cheng-Lung Sung (ports committer) <clsung@FreeBSD.org>
sub 1024g/1FB800C2 2003-09-12
```

D.3.178 Gregory Sutter <gsutter@FreeBSD.org>

```
pub 1024D/845DFEDD 2000-10-10 Gregory S. Sutter <gsutter@zer0.org>
    Key fingerprint = D161 E4EA 4BFA 2427 F3F9 5B1F 2015 31D5 845D FEDD
uid Gregory S. Sutter <gsutter@freebsd.org>
uid Gregory S. Sutter <gsutter@daemonnews.org>
uid Gregory S. Sutter <gsutter@pobox.com>
sub 2048g/0A37BBCE 2000-10-10
```

D.3.179 Koichi Suzuki <metal@FreeBSD.org>

```
pub 1024D/AE562682 2004-05-23 SUZUKI Koichi <metal@FreeBSD.org>
    Key fingerprint = 92B9 A202 B5AB 8CB6 89FC 6DD1 5737 C702 AE56 2682
sub 4096g/730E604B 2004-05-23
```

D.3.180 Gary W. Swearingen <garys@FreeBSD.org>

```
pub 1024D/FAA48AD5 2005-08-22 [expires: 2007-08-22]
    Key fingerprint = 8292 CC3E 81B5 E54F E3DD F987 FA52 E643 FAA4 8AD5
uid Gary W. Swearingen <garys@freebsd.org>
sub 2048g/E34C3CA0 2005-08-22 [expires: 2007-08-22]
```

D.3.181 Yoshihiro Takahashi <nyan@FreeBSD.org>

```
pub 1024D/8394B81F 2001-10-15 Yoshihiro TAKAHASHI <nyan@jp.FreeBSD.org>
    Key fingerprint = D4FA D8CA 2AED FCF4 90A3 3569 8666 0500 8394 B81F
uid                               Yoshihiro TAKAHASHI <nyan@furiru.org>
uid                               Yoshihiro TAKAHASHI <nyan@FreeBSD.org>
sub 1024g/B796F020 2001-10-15
```

D.3.182 Mikhail Teterin <mi@FreeBSD.org>

```
pub 1024R/3FC71479 1995-09-08 Mikhail Teterin <mi@aldan.star89.galstar.com>
    Key fingerprint = 5F 15 EA 78 A5 40 6A 0F 14 D7 D9 EA 6E 2B DA A4
```

D.3.183 Gordon Tetlow <gordon@FreeBSD.org>

```
pub 1024D/357D65FB 2002-05-14 Gordon Tetlow <gordont@gnf.org>
    Key fingerprint = 34EF AD12 10AF 560E C3AE CE55 46ED ADF4 357D 65FB
uid                               Gordon Tetlow <gordon@FreeBSD.org>
sub 1024g/243694AB 2002-05-14
```

D.3.184 Lars Thegler <lth@FreeBSD.org>

```
pub 1024D/56B0CA08 2004-05-31 Lars Thegler <lth@FreeBSD.org>
    Key fingerprint = ABAE F98C EA78 1C8D 6FDD CB27 1CA9 5A63 56B0 CA08
uid                               Lars Thegler <lars@thegler.dk>
sub 1024g/E8C58EF3 2004-05-31
```

D.3.185 Thierry Thomas <thierry@FreeBSD.org>

```
pub 1024D/C71405A2 1997-10-11 Thierry Thomas <thierry@pompo.net>
    Key fingerprint = 3BB8 F358 C2F1 776C 65C9 AE51 73DE 698C C714 05A2
uid                               Thierry Thomas <thierry@thomas.as>
uid                               Thierry Thomas <tthomas@mail.dotcom.fr>
uid                               Thierry Thomas (See <http://horde.org>.) <thierry@horde.org>
uid                               Thierry Thomas (FreeBSD committer) <thierry@FreeBSD.org>
sub 2048g/277D65DB 1997-10-11
sub 1024G/8866DD0F 2002-01-26
sub 1024g/36DA7AF9 2003-11-26 [expires: 2003-11-27]
sub 1024R/C5529925 2003-11-26
```

D.3.186 Andrew Thompson <thompsa@FreeBSD.org>

```
pub 1024D/BC6B839B 2005-05-05
    Key fingerprint = DE74 3F49 B97C A170 C8F1 8423 CAB6 9D57 BC6B 839B
uid      Andrew Thompson <thompsa@freebsd.org>
uid      Andrew Thompson <andy@fud.org.nz>
sub 2048g/92E370FB 2005-05-05
```

D.3.187 Florent Thoumie <flz@FreeBSD.org>

```
pub 1024D/5147DCF4 2004-12-04
    Key fingerprint = D203 AF5F F31A 63E2 BFD5 742B 3311 246D 5147 DCF4
uid      Florent Thoumie (FreeBSD committer address) <flz@FreeBSD.org>
uid      Florent Thoumie (flz) <florent@thoumie.net>
uid      Florent Thoumie (flz) <flz@xbsd.org>
uid      [jpeg image of size 1796]
sub 2048g/15D930B9 2004-12-04
```

D.3.188 Hajimu UMEMOTO <ume@FreeBSD.org>

```
pub 1024D/BF9071FE 2005-03-17
    Key fingerprint = 1F00 0B9E 2164 70FC 6DC5 BF5F 04E9 F086 BF90 71FE
uid      Hajimu UMEMOTO <ume@mahoroba.org>
uid      Hajimu UMEMOTO <ume@FreeBSD.org>
uid      Hajimu UMEMOTO <ume@jp.FreeBSD.org>
sub 2048g/748DB3B0 2005-03-17
```

D.3.189 Stephan Uphoff <ups@FreeBSD.org>

```
pub 2048R/D684B04A 2004-10-06 Stephan Uphoff <ups@freebsd.org>
    Key fingerprint = B5D2 04AE CA8F 7055 7474 3C85 F908 7F55 D684 B04A
uid      Stephan Uphoff <ups@tree.com>
sub 2048R/A15F921B 2004-10-06
```

D.3.190 Jacques Vidrine <nectar@FreeBSD.org>

```
pub 2048R/33C1627B 2001-07-05 Jacques A. Vidrine <nectar@celabo.org>
    Key fingerprint = CB CE 7D A0 6E 01 DC 61 E5 91 0A BE 79 17 D3 82
uid      Jacques A. Vidrine <jvidrine@verio.net>
uid      Jacques A. Vidrine <n@nectar.com>
uid      Jacques A. Vidrine <jacques@vidrine.cc>
uid      Jacques A. Vidrine <nectar@FreeBSD.org>
uid      Jacques A. Vidrine <n@nectar.cc>

pub 1024D/1606DB95 2001-07-05 Jacques A. Vidrine <nectar@celabo.org>
    Key fingerprint = 46BC EA5B F70A CC81 5332 0832 8C32 8CFF 1606 DB95
```



```
uid          Jacques A. Vidrine <jvidrine@verio.net>
uid          Jacques A. Vidrine <n@nectar.com>
uid          Jacques A. Vidrine <jacques@vidrine.cc>
uid          Jacques A. Vidrine <nectar@FreeBSD.org>
uid          Jacques A. Vidrine <n@nectar.cc>
sub 2048g/57EDEA6F 2001-07-05
```

D.3.191 Adam Weinberger <adamw@FreeBSD.org>

```
pub 1024D/42C743FD 2002-10-12 Adam Weinberger <adam@vectors.cx>
   Key fingerprint = A980 3F2E 80A8 9619 9D1C 82E8 A3C2 8CD9 42C7 43FD
sub 1024g/15D67628 2002-10-12
```

D.3.192 Nate Williams <nate@FreeBSD.org>

```
pub 1024D/C2AC6BA4 2002-01-28 Nate Williams (FreeBSD) <nate@FreeBSD.org>
   Key fingerprint = 8EE8 5E72 8A94 51FA EA68 E001 FFF9 8AA9 C2AC 6BA4
sub 1024g/03EE46D2 2002-01-28
```

D.3.193 Garrett Wollman <wollman@FreeBSD.org>

```
pub 1024D/0B92FAEA 2000-01-20 Garrett Wollman <wollman@FreeBSD.org>
   Key fingerprint = 4627 19AF 4649 31BF DE2E 3C66 3ECF 741B 0B92 FAEA
sub 1024g/90D5EBC2 2000-01-20
```

D.3.194 Jörg Wunsch <joerg@FreeBSD.org>

```
pub 1024D/69A85873 2001-12-11 Joerg Wunsch <j@uriah.heep.sax.de>
   Key fingerprint = 5E84 F980 C3CA FD4B B584 1070 F48C A81B 69A8 5873
pub 1024D/69A85873 2001-12-11 Joerg Wunsch <j@uriah.heep.sax.de>
uid          Joerg Wunsch <joerg_wunsch@interface-systems.de>
uid          Joerg Wunsch <joerg@FreeBSD.org>
uid          Joerg Wunsch <j@ida.interface-business.de>
sub 1024g/21DC9924 2001-12-11
```

D.3.195 Maksim Yevmenkin <emax@FreeBSD.org>

```
pub 1024D/F050D2DD 2003-10-01 Maksim Yevmenkin <m_evmenkin@yahoo.com>
   Key fingerprint = 8F3F D359 E318 5641 8C81 34AD 791D 53F5 F050 D2DD
```

D.3.196 Bjoern A. Zeeb <bz@FreeBSD.org>

```
pub 1024D/0E4A7875 2000-02-04 Bjoern A. Zeeb <bz@FreeBSD.org>
    Key fingerprint = 5E31 F886 E2EE BA7E 2AA5 DDD4 21C5 0916 0E4A 7875
uid                                     Bjoern A. Zeeb <bz@zabbadoz.net>
uid                                     Bjoern A. Zeeb <bzeeb@zabbadoz.net>
uid                                     Bjoern A. Zeeb <bzeeb-lists@lists.zabbadoz.net>
sub 1024g/6139751B 2000-02-04
```

D.3.197 Alexey Zelkin <phantom@FreeBSD.org>

```
pub 1024D/9196B7D9 2002-01-28 Alexey Zelkin <phantom@FreeBSD.org>
    Key fingerprint = 4465 F2A4 28C1 C2E4 BB95 1EA0 C70D 4964 9196 B7D9
sub 1024g/E590ABA4 2002-01-28
```

索引

Symbols

- .k5login, 353
- .k5users, 353
- .rhosts, 431
- /boot/kernel.old, 179
- /etc, 277
- /etc/gettytab, 515
- /etc/groups, 325
- /etc/login.conf, 323
- /etc/mail/access, 569
- /etc/mail/aliases, 569
- /etc/mail/local-host-names, 569
- /etc/mail/mailer.conf, 569
- /etc/mail/mailertable, 569
- /etc/mail/sendmail.cf, 569
- /etc/mail/virtusertable, 569
- /etc/remote, 521
- /etc/ttys, 517
- /usr, 277
- /usr/bin/login, 515
- /usr/local/etc, 279
- /usr/share/skel, 318
- /var, 277
- 10 base 2, 709
- 10 base T, 710
- 386BSD, 3, 6
- 386BSD Patchkit, 3
- 4.3BSD-Lite, 4
- 4.4BSD-Lite, 1, 2
- 802.11
 - (见无线网络)
- partitions, 408
- 安全
 - DoS 攻击
 - (见拒绝服务攻击(DoS))
 - OpenSSH, 368
 - OpenSSL, 356
 - 防火墙, 642
 - 密码, 334
 - 一次性口令, 335
- 安全事件审计
 - (见MAC)

- 安装
 - 常见问题, 81
- 办公套件
 - KOffice, 149
 - OpenOffice.org, 150
- 备份软件
 - dump / restore, 431
 - tar, 432
- 本地化, 263, 476, 478
 - 德语, 485
 - 俄语, 482
 - 繁体中文, 484
 - 韩语, 485
 - 日语, 485
- 编辑器, 108
 - emacs, 108
 - vi, 108
- 编码, 477
- 编译器
 - C, 2
 - C++, 2
 - FORTRAN, 2
- 并口电缆IP
 - (见PLIP)
- 并行版本系统
 - (见CVS)
- 拨入服务, 514
- 串口通讯, 505
- 垂直刷新率, 131
- 磁盘
 - file-backed (4.X), 437
 - 内存文件系统(4.X), 439
 - 添加, 408
 - 虚拟, 437
 - 移除内存盘, 440
- 磁盘的串连, 458
- 磁盘镜像, 454, 459
- 磁盘配额, 323
- 打印服务器
 - Windows 客户机, 637
- 打印机, 483
- 单用户模式, 492
- 单用户模式, 314, 495
- 当前
 - 使用CVSup 同步, 487
- 当前版
 - 编译, 488
 - 使用, 487

- 当前的
 - 使用CTM 同步, 487, 489
- 登入分类, 478, 479
- 地址重定向, 713
- 电视卡, 170
- 电子表格
 - Gnumeric, 153
- 电子邮件
 - (见email)
 - 接收, 567
- 调整
 - 内核限制, 296
 - 以sysctl, 293
- 调整内核, 253
- 动态主机配置协议
 - (见DHCP)
- 对称多处理器(SMP), 2
- 多播路由, 685
- 多用户模式, 314, 492
- 多用户设备, 1
- 二进制代码兼容性
 - BSD/OS, 2
 - Linux, 2
 - NetBSD, 2
 - SCO, 2
 - SVR4, 2
- 二进制兼容模式
 - Linux, 243
- 繁体中文
 - BIG-5编码, 478
- 反向DNS (reverse DNS), 619
- 防火墙, 2, 642, 699, 699
 - IPFILTER, 645
 - IPFW, 663
 - PF, 643
- 防火墙/primary>
 - 规则集, 642
- 分区规划, 277
- 符号链接, 245
- 服务, 279
- 根文件系统, 101
 - 无盘操作, 705
- 根域(root zone), 619
- 共享库, 244
- 国际化
 - (见本地化)
- 国家代码, 477
- 环境变量, 107
- 黄页(yellow pages)
 - (见NIS)
- 回环设备, 680
- 基本输入/输出系统
 - (见BIOS)
- 集权式访问控制
 - (见MAC)
- 计算机系统研究组(CSRG), 2
- 交换分区, 278
- 交换分区分配, 278
- 结对, 694
- 解析器(resolver), 619
- 进程记帐, 377
- 拒绝服务(DoS), 332
- 拒绝服务攻击(DoS), 328
- 可执行类加载器, 274
- 控制台, 89, 314
- 快照, 486
- 宽限期, 444
- 蓝牙, 691
- 联机手册, 111
- 路由, 3, 679
- 路由传播, 684
- 路由器, 682, 699
- 密码学, 635
- 命令行, 107
- 默认路由, 680, 681
- 目录, 92
- 目录层次, 94
- 内存保护, 1
- 内核, 309
 - NOTES, 179
 - 编译, 495
 - 建立/安装, 177
 - 建立一个定制的内核, 176
 - 配置, 157, 711
 - 配置文件, 179
 - 引导标志, 312
 - 引导交互, 312
- 内核调整, 263
- 内核选项
 - BRIDGE, 699
 - cpu, 180
 - CPU_ENABLE_SSE, 163
 - cpu类型, 180
 - device pf, 644
 - device pfbg, 644
 - device pfsync, 644

- FAST_IPSEC, 359
- ident, 180
- IPDIVERT, 664
- IPFILTER, 646
- IPFILTER_DEFAULT_BLOCK, 646
- IPFILTER_LOG, 646
- IPFIREWALL, 664
- IPFIREWALL_DEFAULT_TO_ACCEPT, 664
- IPFIREWALL_VERBOSE, 664
- IPFIREWALL_VERBOSE_LIMIT, 664
- IPSEC, 359, 364
- IPSEC_DEBUG, 359
- IPSEC_ESP, 359
- LINUX, 244
- MROUTING, 685
- MSDOSFS, 181
- NFS, 181
- NFS_ROOT, 181
- SMP, 183
- USER_LDT, 163
- 机器, 180
- 配额, 323
- 启动脚本, 90
- 抢占式多任务, 1
- 桥接, 698
- 权限, 92
 - 符号, 93
- 日志文件, 291
 - FTP, 637
 - named, 627
- 软性限制, 443
- 设备节点, 159, 191
- 声卡, 157
- 视频ports, 166
- 视频包, 166
- 水平刷新率, 131
- 添加用户, 318
- 条带, 452
- 条带盘, 458
- 图象扫描仪, 172
- 网关, 679
- 网卡
 - 测试, 287
 - 故障排除, 288
 - 配置, 285, 286
 - 驱动程序, 285
- 网络地址转换
 - (见NAT)
- 文本编辑器, 108
- 文件服务器
 - UNIX 客户机, 596
 - Windows 客户机, 637
- 文件权限, 92
- 文件系统
 - HFS, 417
 - ISO 9660, 416, 417
 - Joliet, 417
 - 挂接, 102
 - 快照, 441
 - 使用fstab的挂接, 102
 - 卸下, 103
- 稳定版, 488
 - 编译, 489
 - 使用, 488
 - 使用CVSup同步, 489
- 无盘操作, 700
 - 内核配置, 705
 - 只读的/usr, 707
- 无盘工作站, 700
- 无线网络, 685
 - 加密, 688
 - 接入点, 686
- 物理地址扩展(PAE)
 - 大内存, 191
- 系统配置, 277
- 系统优化, 277
- 限制TCP 带宽延迟积
 - net.inet.tcp.inflight.enable, 298
- 限制用户使用系统资源, 323
 - coredumpsize, 323
 - cputime, 323
 - fi lesize, 324
 - maxproc, 324
 - memorylocked, 324
 - memoryuse, 324
 - openfi les, 324
 - sbsize, 324
 - stacksize, 324
 - 配额, 323
- 信号11, 500
- 虚拟控制台, 89
- 虚拟内存, 2
- 虚拟主机, 288
- 虚拟专用网
 - (见VPN)
- 一次性口令, 335

- 以太网
 - MAC 地址, 680
 - MAC地址, 247
- 引导, 308
- 应用程序
 - Maple, 248
 - MATLAB, 250
 - Oracle, 252
 - SAP R/3, 256
- 硬性限制, 443
- 用户
 - 运行FreeBSD 的大型站点, 3
- 邮件
 - 改变mta, 571
 - 配置, 576
 - 疑难解答, 573
- 邮件服务程序
 - exim, 567
 - postfix, 567
 - qmail, 567
 - sendmail, 567
- 邮件服务器, 568
- 邮件列表, 490
- 邮件用户代理, 582
- 语言代码, 477
- 域
 - 例子, 619
- 源代码, 2
- 帐户
 - daemon, 318
 - nobody, 318
 - operator, 318
 - 超级用户(root), 317
 - 改变口令, 322
 - 删除, 320
 - 添加, 318
 - 系统, 318
 - 限制, 323
 - 修改, 318
 - 用户, 318
 - 组, 325
- 中断风暴, 304
- 终端, 89, 510
- 重宿主机, 682
- 重新编译world, 490
- 主机, 290
- 主机名, 290
- 主引导记录(MBR), 309

- 专用(dangerously dedicated), 99
- 子网, 679, 680
- 自动挂接服务, 599
- 组, 325
- 浏览器
 - web, 146

A

- Abacus, 154
- AbiWord, 150
- accounting
 - disk space, 442
 - printer, 217, 230
- ACL, 373
- ACPI, 301, 302
 - ASL, 304, 305
 - error messages, 305
 - problems, 302, 303
 - 调试, 306
 - 问题, 306
- Acrobat Reader, 152
- adduser, 479
- AIX, 601
- Alpha, 10, 15, 80, 82
- Alpha BIOS, 82
- Amanda, 433
- amd, 599
- anti-aliased fonts, 135
- Apache, 3, 632
 - 模块, 634
 - 配置文件, 633
 - 启动和停止, 633
- APIC
 - 禁用, 304
- APM, 186, 301
- applications
 - Mathematica, 246
- apsfilter, 216
- ARC, 82
- ASCII, 240, 477
- AT&T, 4
- AUDIT, 402
- AutoPPP, 538

B

- backup floppy, 429
- backup software
 - Amanda, 433
 - cpio, 432
 - pax, 432
- banner pages
 - (见header pages)
- baud rate, 197
- BGP, 682
- BIND, 573, 619
 - 缓存域名服务器, 626
 - 配置文件, 621
 - 启动, 621
 - 在沙盒中运行, 627
- bind9
 - 安装, 630
- BIOS, 27, 308
- bits-per-second, 201, 505
- Blue Mountain Arts, 3
- Boot Loader, 308
- Boot Manager, 308, 309
- boot-loader, 310
- BOOTP
 - 无盘操作, 703
- Bourne shells, 107
- BSD Copyright, 5
- BSD partitions, 409

C

- CD burner
 - ATAPI, 416
 - ATAPI/CAM driver, 416, 421
- CDROMs
 - burning, 417, 418
 - creating, 416
 - 创建启动光盘, 417
- centronics
 - (见parallel printers)
- CHAP, 532, 534, 539
- chpass, 321
- chroot, 627
- Cisco, 542
- Coda, 437
- committers, 5
- compression, 430

- Computer Systems Research Group (CSRG), 6
- comsat, 330
- contributors, 6
- core team, 6
- coredumpsize, 323
- cpio, 432
- cputime, 323
- cron, 487, 489
 - 配置, 282
- crypt, 334
- CTM, 178, 489, 738
- cu, 83
- cuad, 509
- CUPS, 239
- CURRENT, 486
- CVS
 - 代码库, 5
 - 匿名, 178, 489, 736
- cvsup, 178, 487, 489

D

- DCE, 505
- default route, 557
- DES, 334
- DEVFS, 498
- device.hints, 313
- DGA, 164
- DHCP
 - dhcpd.conf, 617
 - 安装, 617
 - 服务器, 616
 - 配置文件, 616, 618
 - 无盘操作, 702
 - 需求, 615
- dial-out service, 520
- disk quotas, 442
 - checking, 442, 443
 - limits, 442
- disklabel, 433, 437
- disks
 - encrypting, 444
 - memory, 437
- disks (磁盘)
 - fi le-backed (采用文件作为后端), 438
 - 内存文件系统, 440
- DNS, 290, 539, 566, 577, 619

- 记录, 624
- DNS 服务器, 3
- domain name, 558
- DOS, 13, 27, 82, 482
- DoS 攻击
 - (见拒绝服务攻击(DoS))
- DSL, 699
- DSP, 159
- DTE, 505
- dump, 431
- DVD
 - burning, 421
 - DVD+RW, 423
 - DVD-RW, 424
 - DVD-Video, 423

E

- editors
 - ee, 108
- ee, 108
- ELF, 275
 - 标记, 275
- emacs, 108
- email, 2, 566
- Etherboot, 703
- Ethernet, 562
 - MAC address, 562

F

- fdisk, 408
- fetchmail, 589
- fi lesize, 324
- fi nger, 330
- Firefox, 149
- fi x-it fbppies, 433
- fbppy disks, 429
- fbw control protocol, 197
- fonts, 248
 - anti-aliased, 135
 - LCD screen, 137
 - spacing, 136
 - TrueType, 134
- FORTTRAN, 212
- Free Software Foundation, 4, 6
- FreeBSD Project

- goals, 5
 - 开发模式, 5
- FreeBSD 安全公告, 375
- FreeBSD 项目
 - 历史, 3
- Free软件基金会, 112
- FreshMeat, 115
- FreshPorts, 115
- FTP
 - anonymous, 45, 58
 - passive mode, 40
 - via a HTTP proxy, 40
 - 匿名, 636, 637
- FTP 服务器, 2, 636

G

- GateD, 564
- GEOM, 452, 452, 454
- GEOM 磁盘框架
 - (见GEOM)
- getty, 515
- Ghostsript, 210
- GIMP, 150
- GNOME, 140
 - anti-aliased fonts, 141
- GNU Compiler Collection, 3
- GNU General Public License (GPL), 5
- GNU Lesser General Public License (LGPL), 5
- GnuCash, 153
- Gnumeric, 153
- GNU工具, 245
- GQview, 153
- Greenman, David, 4
- Grimes, Rod, 3
- gv, 152
- gzip, 430

H

- hardware, 81
- HCI, 692
- header pages, 202, 218
- HP-UX, 601
- Hubbard, Jordan, 3
- hw.ata.wc, 294

I

- I/O 端口, 159
- IEEE, 432
- ifconfig, 689
- IKE, 364
- IMAP, 566, 568
- init, 309, 314
- installation, 8
 - fbppies, 86
 - from MS-DOS, 87
 - from QIC/SCSI Tape, 87
 - headless (serial console), 83
 - network
 - Ethernet, 87
 - FTP, 40, 85
 - NFS, 88
 - parallel (PLIP), 87
 - serial (SLIP or PPP), 87
- Intel i810 显示芯片, 133
- Internet Software Consortium (ISC), 615
- Internet 连接共享, 711
- IP 别名, 288
- IP 伪装
 - (见NAT)
- IP 子网, 698
- IPCP, 535
- ipf, 647
- IPFILTER
 - 规则处理顺序, 652
 - 规则语法, 652
 - 记录日志, 648
 - 内核选项, 646
 - 启用, 646
 - 统计, 647
 - 有状态过滤, 654
- ipfstat, 647
- ipfw, 665
 - 带状态过滤, 668
 - 规则处理顺序, 666
 - 规则语法, 666
 - 记录日志, 669
 - 内核选项, 664
 - 启用, 664
- ipmon, 648
- ipnat, 659
- IPsec, 358
 - AH, 359

- ESP, 359
 - security policies, 364
- IPX/SPX, 710
- IRQ, 159
- ISA, 157
- ISDN, 699, 707
 - 单独的桥/路由器, 709
 - 卡, 708
- ISO 9660, 416
- ISP, 531, 534

J

- JMA Wired, 3
- Jolitz, Bill, 4

K

- KDE, 141
 - anti-aliased fonts, 143
 - display manager, 142
- Kerberos
 - Kerberos5
 - 故障排除, 353
 - 客户端配置, 353
 - 历史, 350
 - 密钥分发中心, 350
 - 启用服务, 352
 - 外部资源, 356
 - 限制和不足, 355
 - KerberosIV, 330, 334
 - 安装, 342
 - 初始配置, 344
- Kermit, 543
- kern.cam.scsi_delay, 295
- kern.ipc.somaxconn, 297
- kern.maxfiles, 296
- kernel
 - configuration, 560
 - LINT, 179
- kernel options
 - SCSI_DELAY, 295
- kernel.old, 312
- keymap, 480
- KLD (kernel loadable object), 243
- KLD (内核可加载对象), 690
- KOffice, 149
- Konqueror, 149

L

- L2CAP, 693
- LCD screen, 137
- LCP, 538
- LDAP, 638
- LINT, 179
- Linux, 601
 - ELF程序, 245
 - 安装Linux运行时库, 244
- Linux二进制兼容模式, 243
- LISA, 433
- loader, 310
- loader 配置, 310
- locale, 477, 479
- login name, 532
- LPD spooling system, 194
- LPRng, 239
- ls, 92

M

- MAC, 379
 - 文件系统防火墙策略, 387
- MAC Biba 完整性策略, 392
- MAC LOMAC, 393
- MAC Multi-Level 安全策略, 391
- MAC 端口访问控制表策略, 388
- MAC 故障排除, 400
- MAC 接口屏蔽策略, 388
- MAC 进程分区策略, 390
- MAC 配置测试, 396
- MAC 其他UID 可见策略, 386
- MAC 实现举例, 394
- MacOS, 338
- make, 493
- make.conf, 491
- MAKEDEV, 191, 498, 510
- Master Boot Record (MBR), 308
- maxproc, 324
- MD5, 334
- memorylocked, 324
- memoryuse, 324
- mencoder, 168
- mergemaster, 496
- mgetty, 538
- Microsoft Windows, 27, 637, 690
 - 设备驱动, 690

- MIME, 478, 479
- MIT, 342
- modem, 514, 543, 560, 708
- mod_perl
 - Perl, 635
- mod_php
 - PHP, 635
- mount, 83, 437
- mountd, 596
- moused, 481
- Mozilla, 147
 - disabling anti-aliased fonts, 137
- MPlayer
 - making, 167
 - 使用, 167
- MS-DOS, 240, 338
- MX record, 573
- MX 记录, 567, 576, 626
- MySQL, 482

N

- nameserver, 532, 558
- NAT, 2, 659, 699, 711
 - 以及IPFILTER, 659
 - 以及IPFW, 674
- natd, 711
- NDIS, 690
- NDISulator, 690
- net.inet.ip.portrange.*, 298
- Net/2, 4
- NetBIOS, 539, 638
- NetBSD, 6, 601
- Netcraft, 3
- netgroups, 609
- network printing, 223, 224
- newfs, 437
- newsyslog.conf, 292
- NFS, 437, 444, 596
 - configuration, 596
 - export examples, 597
 - mounting, 598
 - server, 596
 - uses, 598
 - 安装多台机器, 502
 - 无盘操作, 704
- nfsd, 596

- NIS, 601
 - 从服务器, 602, 605
 - 服务器配置, 603
 - 客户机, 602
 - 客户机配置, 607
 - 口令格式, 614
 - 映射, 604
 - 域, 601
 - 域名, 603
 - 主服务器, 602
- NIS+, 638
- NOTES, 179
- Novell, 4
- ntalk, 330
- NTP, 639
 - ntp.conf, 640
 - ntpd, 639
 - 配置, 640
 - 选择服务器, 639
- ntpdate, 640
- null modem cable, 83
- null-modem cable, 197, 506, 524

O

- OBEX, 697
- OpenBSD, 6, 601
- openfi les, 324
- OpenOffi ce.org, 150
- OpenSSH, 368
 - 安全复制, 369
 - 客户, 369
 - 配置, 369
 - 启用, 368
 - 隧道, 371
- OpenSSL
 - 生成证书, 356
- Opera, 148
- OS/2, 240, 409
- OSPF, 682

P

- packages, 113
 - deleting, 117
 - installing, 116
 - managing, 117

- page accounting, 217
- Pair Networks, 3
- PAP, 532, 534, 539
- parity, 197, 201
- partitions, 99
- passwd命令, 322
- password, 539
- password?/primary> , 532
- pax, 432
- PCI, 157
- PCL, 200, 241
- PDF
 - 查看器, 152, 152, 152
- pgp keys, 802
- pkg_add, 116
- pkg_delete, 117
- pkg_info, 117
- pkg_version, 117
- PLIP, 714
- POP, 566, 568
- Portaudit, 374
- portmanager, 124
- portmap, 596, 601
- ports, 113
 - disk-space, 124
 - 安装, 119
 - 升级, 123
 - 卸载, 123
- Ports Collection, 244
- portupgrade, 123
- POSIX, 432, 478
- PostScript, 196, 200
 - emulating, 210
 - 查看器, 152
- PPP, 531, 531, 573, 708
 - client, 542
 - confi guration, 532, 540
 - creating device nodes, 532
 - kernel PPP, 542
 - Microsoft extensions, 539
 - NAT, 540
 - over ATM, 554
 - over Ethernet, 552
 - PPPoE, 531
 - receiving incoming calls, 535
 - server, 542
 - troubleshooting, 549
 - user PPP, 533

- with dynamic IP addresses, 535
 - with static IP addresses, 533
 - 内核级PPP, 531
 - 用户级PPP, 531
- PPP shells, 536, 537
- PPPoA
 - (见基于ATM的PPP)
- PPPoE
 - (见PPP, over Ethernet)
- print jobs, 194, 203, 209, 228, 233
 - controlling, 228
- printer spool, 203
- printers
 - capabilities, 201
 - network, 223, 224
 - parallel, 196, 200
 - restricting access to, 226
 - serial, 196, 201, 204, 210
 - usage, 232
 - USB, 196
- printing, 194, 233
 - filters, 205, 207, 209
 - apsfilter, 216
 - header pages, 203
- procmail, 590
- pw, 479
- pw命令, 323

R

- racoona, 364
- RAID, 458
 - CCD, 410
 - hardware, 413
 - software, 410, 413, 457
 - Vinum, 413
- RAID-1, 459
- RAID-5, 459
- rc files
 - rc.serial, 510, 518
- rc 文件, 314
 - rc.conf, 278
- rebuilding world
 - timings, 495
- resolv.conf, 290
- restore, 431
- RFCOMM, 694

- RIP, 565, 682
- rlogind, 330
- rmuser, 320
- root partition, 437
- routed, 541
- rpcbind, 596, 601
- RPMs, 259
- RS-232C cables, 505, 507
- rshd, 330

S

- Samba 服务器, 637
- sandboxes, 330
- sbsize, 324
- scp, 369
- screenmap, 480
- SCSI, 27
- SDL, 164
- SDP, 695
- security, 327
 - 后门, 328
 - 窃取用户帐户, 328
 - 确保FreeBSD的安全, 329
- sendmail, 330, 541, 568
- serial console, 83, 523
- serial port, 201
- setkey, 364
- shells, 107
- shutdown, 315
- single-user mode, 312
- skeleton directory, 318
- slices, 99, 408
- SLIP, 531, 557, 560, 561
 - client, 557
 - connecting with, 558
 - routing, 564
 - server, 559
- SMTP, 541, 576
- Soft Updates, 295
 - 详细资料, 295
- Solaris, 275, 601
- Sony Japan, 3
- Sophos Anti-Virus, 3
- spreadsheet
 - Abacus, 154
- SQL 数据库, 638

SRM, 82
ssh, 334
sshd, 330
SSL, 635
STABLE, 486
stacksize, 324
static IP address, 532
static routes, 564
su, 329, 408
SunOS, 178, 603
Supervalu, 3
swap (交换区)
 encrypting (加密), 450
sysctl, 292, 293, 331
sysctl.conf, 292
sysinstall, 480, 615
 adding disks, 408
syslog, 627, 637
syslog.conf, 291
sysutils/cdrtools, 416

T

tape media, 427
 AIT, 429
 DDS (4mm) tapes, 427
 DLT, 428
 Exabyte (8mm) tapes, 428
 QIC tapes, 427
 QIC-150, 428
tar, 430, 432
TCP Wrappers, 340, 608
TCP/IP networking, 560, 561
TCP/IP 网络, 1
TELEHOUSE America, 3
telnetd, 330
TeX, 195, 235
 printing DVI files, 212
TFTP
 无盘操作, 704
timeout, 534
traceroute, 684
troff, 208
Tru64 UNIX, 604
TrueType Fonts, 134
ttyd, 509
tunefs, 295

U

U.C. Berkeley, 2, 4, 6
UDP, 615
Unicode, 482
UNIX, 92, 532
USB
 disks, 414
USENET, 2
UUCP, 574

V

vfs.hirunningspace, 294
vfs.vmiodirenable, 294
vfs.write_behind, 294
vi, 108
Vinum, 457
 串连, 458
 镜像, 459
 条带, 458
vipw, 479
virtual disks, 437
vm.swap_idle_enabled, 294
VPN, 359
 创建, 360

W

Walnut Creek CDROM, 4
Weathernews, 3
web 服务器, 2
 安全, 635
 配置, 632
WEP, 688
wheel, 329
Williams, Nate, 3
Windows, 338
Windows drivers, 690
Windows NT, 601

X

X Display Manager, 138

X Window 系统, 1

(参见XFree86)

Accelerated-X, 3

XFree86, 3

X11, 131

X11 True Type 字体服务器, 481

X11 调优, 132

X11输入方法(XIM), 482

XF86Config, 132

XFree86, 131

XFree86 4.X, 131

XML, 135

Xorg, 131

xorg.conf, 132

Xpdf, 152

XVideo, 164

Y

Yahoo!, 3

Z

zip drive, 187

Colophon

本书是数百名为“FreeBSD 文档计划”工作的志愿者合作的成果。这些文字使用符合DocBook DTD的SGML 撰写，并采用开放源代码的DSSSL 引擎，**Jade** 来转换为许多其他的表现形式。我们使用了Norm Walsh 的DSSSL 样式表用于为**Jade** 提供生成不同表现形式的指引，并增加了一组自定义的改动。高德纳(Donald Knuth)的 $\text{\TeX}$ 排版语言、Leslie Lamport 的 $\text{\LaTeX}$ ，以及Sebastian Rahtz 的**Jade $\text{\TeX}$** 宏集，为这份文档的印刷版本发挥了至关重要的作用。
