



# Absolute OpenBSD: UNIX for the Practical Paranoid

by *Michael W. Lucas*  
ISBN:1886411999

No Starch Press © 2003



Back Cover .....	- 17 -
ACKNOWLEDGMENTS .....	- 20 -
Chapter 0: Introduction.....	- 21 -
Overview .....	- 21 -
What Is BSD? .....	- 21 -
BSD Goes Public .....	- 22 -
AT&T UNIX .....	- 22 -
What Is OpenBSD? .....	- 23 -
Other BSDs.....	- 24 -
NetBSD.....	- 24 -
FreeBSD .....	- 24 -
Mac OS X.....	- 24 -
BSD/OS .....	- 25 -
OpenBSD Users.....	- 25 -
OpenBSD Developers .....	- 25 -
Contributors .....	- 26 -
Committers .....	- 26 -
Coordinator.....	- 26 -
OpenBSD's Strengths .....	- 27 -
Portability .....	- 27 -
Power.....	- 27 -
Documented.....	- 28 -
Free .....	- 28 -
Correctness .....	- 29 -
Security.....	- 29 -
OpenBSD Security .....	- 30 -
OpenBSD's Uses.....	- 30 -
Desktop.....	- 31 -
Server.....	- 31 -
Network Management .....	- 31 -
Who Should Read This Book? .....	- 31 -
Contents Overview .....	- 32 -
Chapter 1: Additional Help .....	- 35 -
Overview .....	- 35 -
OpenBSD Community Support.....	- 35 -
"The Code Is Fine; What's Wrong with You?" .....	- 36 -
Man Pages .....	- 37 -
Manual Sections .....	- 38 -
Navigating Man Pages.....	- 39 -
Finding Man Pages .....	- 40 -
Section Numbers and Man .....	- 40 -
Man Page Contents.....	- 41 -
Man Pages on the Web .....	- 42 -
www.OpenBSD.org.....	- 42 -
Website Mirrors.....	- 42 -
The OpenBSD FAQ .....	- 42 -
Other Websites .....	- 43 -
Mailing Lists.....	- 44 -
The Main Mailing Lists .....	- 44 -
Subscribing to a Mailing List .....	- 44 -
Other Official Lists.....	- 45 -
Non @OpenBSD.org Mailing Lists .....	- 45 -

Using the Mailing Lists .....	- 45 -
Using OpenBSD Problem-Solving Resources.....	- 46 -
www.OpenBSD.org .....	- 46 -
Man Pages.....	- 46 -
Checking the Internet.....	- 47 -
Mailing for Help .....	- 48 -
Discussion Topics.....	- 48 -
Contents of Help Requests.....	- 49 -
Formatting Help Requests .....	- 49 -
Sending Your Email .....	- 50 -
Responding to Email.....	- 51 -
Chapter 2: Installation Preparations.....	- 52 -
Overview.....	- 52 -
OpenBSD Hardware .....	- 52 -
Proprietary Hardware.....	- 53 -
Processor.....	- 53 -
Memory (RAM).....	- 54 -
Hard Drives.....	- 54 -
Getting OpenBSD.....	- 55 -
CD-ROMs.....	- 55 -
Finding OpenBSD on the Net.....	- 56 -
The OpenBSD Release .....	- 58 -
Choosing Your Install Method .....	- 59 -
Local Installation Servers .....	- 59 -
Distribution Sets .....	- 60 -
bsd.....	- 60 -
baseXX.tgz.....	- 60 -
etcXX.tgz .....	- 61 -
manXX.tgz.....	- 61 -
compXX.tgz.....	- 61 -
gameXX.tgz .....	- 61 -
miscXX.tgz .....	- 61 -
xbaseXX.tgz.....	- 62 -
xbaseXX.tgz.....	- 62 -
xservXX.tgz.....	- 62 -
xshareXX.tgz .....	- 62 -
Partitioning .....	- 62 -
Why Partition?.....	- 63 -
Standalone OpenBSD Partitioning .....	- 63 -
Root.....	- 64 -
Swap Space .....	- 65 -
/tmp .....	- 66 -
/var .....	- 66 -
/usr .....	- 66 -
/home .....	- 67 -
Multiple Hard Drives.....	- 67 -
Multiple OS Partitioning.....	- 68 -
Disk Sectors .....	- 68 -
Decisions Complete!.....	- 69 -
Chapter 3: Dedicated Installation .....	- 70 -
Overview.....	- 70 -
Hardware Setup .....	- 70 -

BIOS Setup .....	- 71 -
Making a Boot Floppy .....	- 71 -
Creating Floppies on UNIX.....	- 72 -
Creating Floppies on Windows 9x .....	- 72 -
Creating Boot Floppies on Modern Microsoft Systems .....	- 73 -
Booting .....	- 73 -
The Install Program .....	- 74 -
Disk Setup .....	- 75 -
Creating OpenBSD Partitions.....	- 76 -
Understanding a Disklabel .....	- 77 -
Adding Partitions.....	- 79 -
Subsequent Disks.....	- 82 -
Other Disklabel Operations .....	- 83 -
Expert Mode .....	- 83 -
Changing Basic Drive Parameters.....	- 83 -
Deleting Existing Partitions.....	- 84 -
Modifying Existing Partitions .....	- 84 -
Deleting Existing Disklabels .....	- 85 -
Online Help .....	- 85 -
Final Disk Configuration.....	- 85 -
Network Setup .....	- 86 -
If Your System Has Multiple Network Cards .....	- 87 -
Testing Network Connectivity .....	- 89 -
Root Password .....	- 89 -
Installation Media.....	- 90 -
CD-ROM Installs.....	- 90 -
Network Installs.....	- 91 -
Distribution Sets .....	- 92 -
Custom Installation Sets and Scripts .....	- 94 -
Final Installation Steps .....	- 94 -
Chapter 4: Multiboot Installation .....	- 96 -
Highlights .....	- 96 -
Dual-Boot Install Overview .....	- 96 -
MBR Partitions .....	- 97 -
A Dozen Different fdisk.....	- 98 -
Dual-Boot Installation Restrictions .....	- 98 -
Windows NT/2000/XP Installs.....	- 99 -
Windows 9x installs .....	- 100 -
Linux/FreeBSD Installs .....	- 100 -
Hard Disk Geometry.....	- 100 -
Using fdisk During an Install .....	- 102 -
Reading MBR Partitions.....	- 102 -
Creating MBR Partitions .....	- 103 -
Editing a MBR Partition.....	- 104 -
Set Active Partition.....	- 105 -
Completing fdisk .....	- 106 -
Other fdisk Options .....	- 106 -
Starting Over .....	- 106 -
Disable a Partition .....	- 106 -
Disklabel on Multiboot Systems .....	- 107 -
Installing from a Foreign File System Partition .....	- 109 -
Boot Managers.....	- 110 -

Finding GAG .....	- 110 -
Chapter 5: Post-Install Setup .....	- 112 -
Overview.....	- 112 -
Basic Configuration .....	- 112 -
Time Zone.....	- 112 -
Date.....	- 113 -
Set Host Name .....	- 114 -
Ethernet Interface Configuration .....	- 114 -
DHCP.....	- 115 -
Default Gateway .....	- 115 -
Nameservice .....	- 115 -
Mail Aliases.....	- 116 -
Testing your Work.....	- 116 -
Integrated Program Configuration.....	- 117 -
/etc/rc Daemon Configuration .....	- 117 -
Common /etc/rc.conf Assignments.....	- 118 -
Routing Options.....	- 118 -
Packet Filtering.....	- 119 -
Diskless Clients .....	- 119 -
Time Management.....	- 120 -
Daemons .....	- 121 -
IPv6 features .....	- 123 -
NFS .....	- 124 -
AFS configuration .....	- 125 -
Kerberos Setup.....	- 125 -
Miscellaneous Variables .....	- 126 -
Installing the Source Code.....	- 127 -
Installing the Ports Collection .....	- 127 -
Further Setup .....	- 127 -
Chapter 6: Startup and Booting .....	- 128 -
Overview.....	- 128 -
Boot Configuration .....	- 129 -
Boot Prompt.....	- 129 -
Booting Single-User .....	- 130 -
Booting in Kernel Configuration Mode.....	- 131 -
Booting Alternate Kernels .....	- 131 -
Booting from an Alternate Hard Disk .....	- 131 -
Other Useful Boot Commands.....	- 132 -
/etc/boot.conf .....	- 132 -
Serial Consoles .....	- 133 -
Hardware Serial Console .....	- 133 -
Software Serial Console .....	- 134 -
Non-i386 Serial Consoles.....	- 134 -
Serial Console Physical Setup .....	- 134 -
Serial Console Client .....	- 135 -
Configuring the Serial Console .....	- 136 -
Multiuser Startup .....	- 137 -
/etc/rc .....	- 137 -
/etc/rc.conf .....	- 137 -
/etc/netstart.....	- 138 -
/etc/rc.securelevel .....	- 138 -
/etc/rc.local.....	- 138 -

/etc/rc.conf.local .....	- 138 -
/etc/rc.shutdown.....	- 139 -
Editing /etc/rc Scripts .....	- 139 -
Port-Based Software Startup .....	- 139 -
Custom Software Startup.....	- 140 -
Chapter 7: Managing Users .....	- 142 -
Overview .....	- 142 -
Single-User Systems.....	- 142 -
Adding Users .....	- 143 -
Adding Users Interactively.....	- 143 -
/etc/adduser.conf.....	- 145 -
Adding Users Non-Interactively.....	- 148 -
Account Limitations .....	- 150 -
Removing User Accounts.....	- 150 -
Editing Users .....	- 151 -
Groups of Users .....	- 152 -
What Groups Are You In?.....	- 152 -
/etc/group.....	- 153 -
Primary Group.....	- 153 -
Creating Groups.....	- 154 -
User Classes.....	- 155 -
The Default Login Class.....	- 155 -
Legal Values for /etc/login.conf Variables.....	- 156 -
Resource Limits.....	- 157 -
Default Environment Setting.....	- 158 -
FTP Options.....	- 159 -
Controlling Password and Login Options .....	- 159 -
Authentication Methods .....	- 160 -
The Root Password.....	- 162 -
Using the Root Password.....	- 163 -
Who May Use the Root Password? .....	- 163 -
Using Groups to Avoid Using Root .....	- 164 -
Hiding Root with Sudo .....	- 166 -
Why Use Sudo? .....	- 167 -
Disadvantages to Sudo .....	- 167 -
Overview of Sudo.....	- 168 -
visudo .....	- 168 -
/etc/sudoers .....	- 169 -
Using Aliases in /etc/sudoers.....	- 173 -
Nesting Aliases.....	- 173 -
Using System Groups as User Aliases .....	- 174 -
Duplicating Alias Names.....	- 174 -
Using Sudo .....	- 174 -
Excluding Commands from ALL.....	- 176 -
Sudo Logs.....	- 177 -
Chapter 8: Networking .....	- 179 -
Overview .....	- 179 -
Network Layers .....	- 179 -
The Physical Layer.....	- 180 -
The Physical Protocol Layer.....	- 180 -
The Logical Protocol Layer.....	- 181 -
Applications.....	- 181 -

The Life and Times of a Network Request.....	181 -
Networking Basics.....	183 -
Mbufs.....	183 -
Bits.....	185 -
IP Addresses and Netmasks.....	186 -
Basic TCP/IP.....	190 -
IP.....	190 -
ICMP.....	191 -
UDP.....	191 -
TCP.....	191 -
How Protocols Fit Together.....	192 -
Network Ports.....	192 -
What Ports Are Open?.....	193 -
What's Listening on Ports?.....	195 -
Configuring Interfaces.....	196 -
IP Routing.....	198 -
Routed Internal Network Example.....	198 -
Routing Commands.....	200 -
Chapter 9: Internet Connections.....	203 -
Dial-up Internet Connections.....	203 -
Modems.....	204 -
Configuring PPP.....	204 -
Default Entry.....	205 -
Connection Configuration.....	206 -
Example ISP Configuration.....	207 -
Running PPP.....	207 -
Connection Types.....	208 -
Ethernet.....	210 -
Prerequisites.....	211 -
Ethernet Physical Protocol.....	211 -
MAC Addresses.....	212 -
Hubs, Switches, and Bridges.....	212 -
Configuring Your Ethernet Card.....	213 -
Multiple IP Addresses on One Ethernet Card.....	213 -
IP Aliases on a Loopback Interface.....	214 -
Blocks of Alias IPs.....	215 -
Chapter 10: Additional Security Features.....	216 -
Overview.....	216 -
Who Is the Enemy?.....	217 -
Script Kiddies.....	217 -
Disaffected Users.....	217 -
Skilled Attackers.....	218 -
Hackers.....	218 -
OpenBSD Security Announcements.....	218 -
Checksums.....	219 -
Using Checksums.....	219 -
Non-Matching Checksums.....	220 -
File Flags.....	220 -
Viewing a File's Flags.....	221 -
Flag Types.....	221 -
Setting and Removing File Flags.....	222 -
Securelevels.....	223 -



Setting Securelevels.....	- 223 -
Securelevel -1 .....	- 224 -
Securelevel 0 .....	- 224 -
Securelevel 1 .....	- 224 -
Securelevel 2 .....	- 225 -
Which Securelevel Do You Need? .....	- 225 -
Living with Securelevels .....	- 226 -
Systrace.....	- 226 -
System Calls .....	- 226 -
Systrace Policies .....	- 227 -
Sample Systrace Policy Rules .....	- 228 -
Permitting System Calls .....	- 228 -
Making a Systrace Policy File .....	- 231 -
Creating Systrace Policies .....	- 231 -
Public Systrace Policies.....	- 232 -
Policy Generation with systrace(1).....	- 232 -
Using Systrace Policies .....	- 233 -
Real-Time Systrace Monitoring .....	- 234 -
Software Security Features .....	- 235 -
Non-Executable Stack .....	- 235 -
PROT_purity .....	- 235 -
WorX .....	- 236 -
Read-Only Segments .....	- 236 -
Propolice.....	- 237 -
Chapter 11: Basic Kernel Configuration .....	- 238 -
Overview .....	- 238 -
What Is the Kernel? .....	- 238 -
Startup Messages .....	- 239 -
Device Attachments.....	- 240 -
Device Numbering.....	- 242 -
Sysctl(8).....	- 242 -
Sysctl Values .....	- 243 -
Viewing Available Sysctls.....	- 243 -
Changing Sysctl Values.....	- 245 -
Setting Sysctls at Boot.....	- 246 -
Table Sysctls.....	- 248 -
Kernel Alteration with config(8) .....	- 248 -
What Is Config(8)? .....	- 248 -
Preparation.....	- 249 -
Device Drivers and Config .....	- 249 -
Editing the Kernel with config .....	- 250 -
What Entries Mean .....	- 250 -
Configuring Existing Device Drivers .....	- 251 -
Adding Devices .....	- 254 -
Finding Conflicts .....	- 255 -
Changing Non-Device Driver Information.....	- 256 -
Completing Config .....	- 258 -
Installing Your Edited Kernel .....	- 258 -
Boot-Time Kernel Configuration .....	- 259 -
Chapter 12: Building Custom Kernels .....	- 261 -
The Culture of Kernel Compilation.....	- 261 -
Why Build a Custom Kernel?.....	- 262 -

Problems Building Custom Kernels .....	- 263 -
Problems Running Custom Kernels.....	- 263 -
Preparations .....	- 264 -
Configuration File Format .....	- 265 -
Configuration Files .....	- 266 -
Machine-Independent Configuration.....	- 266 -
Machine-Dependent Configuration .....	- 267 -
Your Kernel Configuration File.....	- 268 -
Busses and Attachments .....	- 269 -
mainbus0.....	- 269 -
Connection Configuration .....	- 269 -
Stripping Down the Kernel.....	- 270 -
Dmessage and Kernel Configuration.....	- 271 -
Enhancing the Kernel .....	- 272 -
Changing the Kernel.....	- 272 -
config(8) .....	- 273 -
Config Errors .....	- 273 -
Building a Kernel.....	- 274 -
Build Errors .....	- 275 -
Installing Your Kernel .....	- 275 -
Identifying Your Booted Kernel.....	- 275 -
Chapter 13: Add-On Software .....	- 277 -
Overview.....	- 277 -
Making Software .....	- 278 -
Source Code.....	- 278 -
Crossing Platforms.....	- 279 -
The Ports and Packages System .....	- 279 -
The Ports Tree.....	- 280 -
Ports Subcategories.....	- 281 -
Finding Software .....	- 282 -
Using Packages.....	- 284 -
Package Files .....	- 285 -
Installing Packages .....	- 285 -
Installing from CD-ROM .....	- 286 -
Installing from FTP.....	- 286 -
Package Architectures .....	- 289 -
Package Contents.....	- 289 -
Uninstalling Packages.....	- 291 -
Packaging Problems.....	- 291 -
Using Ports.....	- 292 -
Installing a Port.....	- 294 -
What the Port Install Does .....	- 294 -
Port Build Stages .....	- 296 -
Port Flavors.....	- 300 -
Uninstalling and Reinstalling .....	- 302 -
Customizing Download Sources.....	- 302 -
Running Foreign Software.....	- 304 -
Chapter 14: /ETC.....	- 305 -
Overview.....	- 305 -
/etc/adduser.conf.....	- 306 -
/etc/afs/.....	- 306 -
/etc/amd/ .....	- 306 -

/etc/authpf/ .....	- 306 -
/etc/boot.conf .....	- 306 -
/etc/bootptab .....	- 306 -
/etc/ccd.conf .....	- 307 -
/etc/changelist .....	- 307 -
/etc/csh.* .....	- 307 -
/etc/daily .....	- 307 -
Root Filesystem Backups .....	- 308 -
Daily Filesystem Integrity Check .....	- 308 -
/etc/daily.local .....	- 308 -
/etc/dhclient.conf .....	- 309 -
Prolonging Lease Requests .....	- 309 -
Rejecting Bad DHCP Servers .....	- 309 -
Announcing Host Information .....	- 310 -
/etc/dhcpd.conf .....	- 310 -
/etc/disklabels/ .....	- 311 -
/etc/exports .....	- 311 -
/etc/fstab .....	- 311 -
/etc/ftpchroot .....	- 311 -
/etc/ftpusers .....	- 311 -
/etc/groups .....	- 311 -
/etc/hostname .....	- 312 -
/etc/hosts .....	- 312 -
/etc/hosts.equiv .....	- 312 -
/etc/inetd.conf .....	- 313 -
/etc/hosts.lpd .....	- 315 -
/etc/kerberosIV .....	- 315 -
/etc/kerberosV .....	- 315 -
/etc/ksh.kshrc .....	- 315 -
/etc/localtime .....	- 316 -
/etc/locate.rc .....	- 316 -
/etc/login.conf .....	- 317 -
/etc/lynx.cfg .....	- 317 -
/etc/magic .....	- 317 -
/etc/mail/ .....	- 317 -
/etc/mail.rc .....	- 317 -
/etc/mailer.conf .....	- 318 -
/etc/man.conf .....	- 318 -
Search Index .....	- 318 -
Manual Page Location .....	- 319 -
Displaying Manual Pages .....	- 319 -
Section Names .....	- 320 -
/etc/master.passwd .....	- 320 -
Fields .....	- 321 -
/etc/mk.conf .....	- 323 -
/etc/moduli .....	- 323 -
/etc/monthly .....	- 323 -
/etc/monthly.local .....	- 323 -
/etc/motd .....	- 324 -
/etc/mtree .....	- 324 -
/etc/myname .....	- 324 -
/etc/netstart .....	- 324 -

/etc/newsyslog.conf .....	324 -
/etc/passwd.....	327 -
/etc/pf.conf.....	328 -
/etc/phones .....	328 -
/etc/portal.conf.....	328 -
/etc/ppp/ .....	329 -
/etc/printcap .....	329 -
/etc/protocols.....	329 -
/etc/pwd.db.....	330 -
/etc/rbootd.conf.....	330 -
/etc/rc.* .....	330 -
/etc/remote .....	330 -
/etc/resolv.conf.....	331 -
Domain or Domain Search Settings .....	331 -
The Nameserver List.....	332 -
/etc/rpc .....	332 -
/etc/security.....	332 -
/etc/services.....	333 -
/etc/shells .....	333 -
/etc/skel/ .....	333 -
/etc/skeykeys.....	333 -
/etc/sliphome/.....	333 -
/etc/spwd.db.....	334 -
/etc/ssh/ .....	334 -
/etc/ssl/ .....	334 -
/etc/sudoers .....	334 -
/etc/sysctl.conf.....	334 -
/etc/syslog.conf.....	334 -
Facilities.....	335 -
Levels.....	336 -
Actions.....	337 -
Creating syslog.conf Entries .....	337 -
Logging by Program Name .....	338 -
/etc/systrace/ .....	339 -
/etc/termcap.....	339 -
/etc/ttys.....	339 -
Terminal Types.....	339 -
Configuring /etc/ttys .....	340 -
/etc/weekly .....	341 -
/etc/weekly.local .....	341 -
/etc/wsconsctl.conf.....	341 -
Change Keyboard Encoding .....	342 -
Idle Screen Blank.....	342 -
Chapter 15: Disk and File System Management .....	344 -
Device Nodes.....	344 -
Raw and Block Devices.....	345 -
The File System Table: /etc/fstab .....	346 -
The Fast File System .....	347 -
FFS Mount Options .....	347 -
Using FFS Mount Options.....	350 -
What's Mounted Now? .....	350 -
Corrupt FFS Partitions.....	350 -

Failed Automatic Fscks .....	- 351 -
Mount(8) and FFS .....	- 352 -
Mounting Standard File Systems.....	- 352 -
Mounting with Options.....	- 353 -
Forcing Read-Write Mounts .....	- 353 -
Mounting All Standard File Systems .....	- 353 -
Mounting Partitions at Other Mount Points .....	- 354 -
Unmounting FFS File Systems.....	- 354 -
Mounting Foreign File Systems .....	- 354 -
Using Foreign Mounts .....	- 355 -
Vnodes, Foreign File Systems, and FFS .....	- 355 -
Foreign File System Types .....	- 356 -
File System Permissions .....	- 357 -
Removable Media.....	- 357 -
Removable Disks and /etc/fstab .....	- 358 -
Formatting Floppies.....	- 358 -
Adding New Hard Disks .....	- 360 -
fdisk .....	- 360 -
Partitioning .....	- 361 -
Creating File Systems.....	- 362 -
Mounting Your New Drive .....	- 362 -
Moving Data to a New Partition.....	- 362 -
Memory File Systems.....	- 363 -
MFS and Swap .....	- 364 -
Creating an MFS Partition.....	- 364 -
Mounting MFS Partitions at Boot .....	- 364 -
Mounting Disk Images .....	- 365 -
Vnode Device Nodes .....	- 365 -
Running vnconfig(8) and mount(8).....	- 366 -
Disconnecting Disk Images .....	- 366 -
Encrypted Partitions .....	- 367 -
Creating a Partition File.....	- 367 -
Partition File Setup .....	- 368 -
Unclean Shutdowns .....	- 369 -
Incorrect and Changing Keys .....	- 369 -
Chapter 16: Upgrading OpenBSD.....	- 371 -
Overview .....	- 371 -
Why Upgrade?.....	- 371 -
Versions of OpenBSD .....	- 372 -
Current.....	- 372 -
Snapshots.....	- 373 -
Releases .....	- 373 -
Which Version Should You Use?.....	- 374 -
Errata .....	- 375 -
Errata Prerequisites.....	- 376 -
Applying Errata .....	- 376 -
Compiling Kernel Errata .....	- 377 -
Compiling Userland Errata.....	- 377 -
Upgrading OpenBSD.....	- 378 -
Upgrade Prerequisites.....	- 378 -
Upgrading Base Software.....	- 378 -
The Upgrading Mini-FAQ.....	- 378 -

Customized Upgrades .....	- 380 -
Installing Updated Base Software .....	- 380 -
Merging /etc .....	- 383 -
Preparations .....	- 383 -
Installing Mergemaster .....	- 384 -
Running Mergemaster .....	- 385 -
Updating Ports and Packages.....	- 388 -
Updating the Ports Tree .....	- 389 -
Updating Installed Packages.....	- 389 -
Finding Obsolete Packages.....	- 390 -
Dependencies in Updated Packages .....	- 390 -
Upgrades from Source .....	- 391 -
Source Code Distribution .....	- 391 -
Source Code Repositories.....	- 392 -
Tags.....	- 392 -
Mixing Repository Versions.....	- 393 -
Source-changes@OpenBSD.org.....	- 393 -
CVS Setup .....	- 394 -
Running CVS.....	- 395 -
CVSup Setup .....	- 396 -
Running CVSup.....	- 398 -
Standard Source Build Process .....	- 398 -
The Build Commands .....	- 399 -
Source Upgrade Problems .....	- 401 -
Chapter 17: Basic Packet Filtering .....	- 402 -
Overview.....	- 402 -
Firewalls .....	- 402 -
Enabling PF .....	- 403 -
What Is Packet Filtering?.....	- 404 -
Basic Packet Filtering Concepts .....	- 404 -
Packet Filter Control Program .....	- 406 -
/etc/pf.conf .....	- 406 -
In and Out .....	- 407 -
"My Network Can Do No Wrong" .....	- 407 -
Logical Operators .....	- 408 -
Combining Entries with Braces .....	- 410 -
Macros .....	- 411 -
Tables.....	- 412 -
Defining Tables .....	- 413 -
Table Attributes .....	- 414 -
Exclusions.....	- 414 -
Using Tables in Rules .....	- 415 -
Options.....	- 416 -
Timing Options .....	- 416 -
Enabling Logging .....	- 417 -
PF Memory Limits.....	- 417 -
Blocked Packet Policy .....	- 418 -
Packet Normalization.....	- 418 -
Avoiding Fragment Processing.....	- 420 -
Packet Filtering .....	- 421 -
What Packet Filtering Doesn't Do .....	- 421 -
Packet Filtering Rule Design .....	- 422 -

Pass and Block.....	- 422 -
Additional Actions in Rules .....	- 425 -
Packet Pattern Matching.....	- 426 -
Labels .....	- 432 -
Anchors and Named Rulesets.....	- 434 -
Rules, Interfaces, and DHCP.....	- 435 -
Using Stateful Inspection .....	- 435 -
State Modulation .....	- 437 -
Filtering Spoofed Packets.....	- 438 -
Chapter 18: More Packet Filtering .....	- 440 -
Overview .....	- 440 -
Network Address Translation.....	- 440 -
NAT Rule Order.....	- 441 -
Private NAT Addresses .....	- 442 -
Exclusions from NAT.....	- 442 -
Bi-directional NAT.....	- 442 -
Packet Filtering and NAT.....	- 443 -
Connection Redirection .....	- 444 -
Redirecting Ranges of Ports .....	- 445 -
Redirection and Proxies.....	- 446 -
Redirection and Packet Filtering .....	- 446 -
FTP and Firewalls.....	- 447 -
Configuring the FTP Proxy Application .....	- 447 -
Load Balancing.....	- 449 -
Types of Load Balancing.....	- 450 -
Outbound Load Balancing.....	- 451 -
Inbound Load Balancing .....	- 452 -
Bandwidth Management.....	- 453 -
Queues .....	- 454 -
Queue Types .....	- 454 -
Queue Options .....	- 455 -
ALTQ Parent Queue Setup.....	- 456 -
Defining Priority Queues.....	- 457 -
Defining Class-Based Queues .....	- 458 -
Subdividing a CBQ Queue .....	- 459 -
Assigning Traffic to Queues.....	- 461 -
Queuing by Type of Service.....	- 461 -
Rule Optimization .....	- 462 -
Chapter 19: Managing PF.....	- 464 -
pfctl(8).....	- 464 -
General Commands .....	- 464 -
Loading Rules.....	- 465 -
Flushing Rules .....	- 466 -
Viewing PF Information.....	- 467 -
Clearing PF Statistics .....	- 470 -
Managing Tables .....	- 471 -
Table Statistics.....	- 473 -
Managing State Tables .....	- 473 -
Viewing the State Table .....	- 474 -
Removing States.....	- 474 -
Killing States .....	- 475 -
Authenticating PF.....	- 475 -

User Account Setup .....	- 476 -
Server Setup.....	- 476 -
PF Setup.....	- 477 -
Creating authpf(8) Rules.....	- 478 -
Per-User Authpf Rules.....	- 478 -
Authpf Access Lists.....	- 479 -
PF Logging .....	- 479 -
Reading PF Logs.....	- 480 -
Real-Time Log Access .....	- 480 -
Appendix A: i386 Kernel Configuration Choices .....	- 482 -
Overview.....	- 482 -
CPU Configuration .....	- 482 -
Miscellaneous Options.....	- 483 -
Common Device Drivers .....	- 485 -
Busses .....	- 485 -
i386 Core Hardware.....	- 487 -
Bridges.....	- 488 -
Non-SCSI Controllers.....	- 489 -
SCSI Controllers .....	- 491 -
RAID Controllers.....	- 492 -
SCSI Interface Devices.....	- 492 -
Non-SCSI Storage Devices.....	- 493 -
MII Network Cards.....	- 494 -
Non-MII Network Cards.....	- 496 -
Gigabit Ethernet Cards .....	- 497 -
Wireless Network Cards .....	- 498 -
Non-Ethernet Network Cards .....	- 498 -
CardBus Devices .....	- 499 -
BIOS Devices .....	- 500 -
Serial Ports.....	- 500 -
Console Drivers .....	- 502 -
USB Devices.....	- 503 -
Multimedia Hardware.....	- 507 -
Radio Support .....	- 510 -
Hardware Crypto Cards .....	- 510 -
i386 Kernel Options.....	- 511 -
Bus Options .....	- 511 -
Debugging Options .....	- 512 -
Security Options .....	- 513 -
Userland Syscall Options.....	- 513 -
Filesystem Options .....	- 514 -
Networking Options.....	- 517 -
Console Options.....	- 519 -
Binary Compatibility Options.....	- 520 -
Misc Options.....	- 521 -
Pseudo-Devices.....	- 522 -
Disk-Like Pseudo-Devices .....	- 522 -
Networking Pseudo-Devices .....	- 522 -
IPv6 Pseudo-Devices .....	- 524 -
Miscellaneous Pseudo-Devices .....	- 525 -
Appendix B: PF Example Configurations .....	- 526 -
Overview.....	- 526 -



---

Home Firewall .....	- 526 -
Small Office Usage.....	- 527 -
3-Tier Architecture .....	- 529 -
Afterword .....	- 532 -



Absolute OpenBSD: UNIX for the Practical Paranoid

by Michael W. Lucas

ISBN:1886411999

No Starch Press © 2003

This book takes readers through the intricacies of the OpenBSD platform, and teaches them how to manage the system with friendly explanations, background information, troubleshooting suggestions, and copious examples.

Table of Contents

[Absolute OpenBSD UNIX for the Practical Paranoid](#)

[Chapter 0](#) - Introduction

[Chapter 1](#) - Additional Help

[Chapter 2](#) - Installation Preparations

[Chapter 3](#) - Dedicated Installation

[Chapter 4](#) - Multiboot Installation

[Chapter 5](#) - Post-Install Setup

[Chapter 6](#) - Startup and Booting

[Chapter 7](#) - Managing Users

[Chapter 8](#) - Networking

[Chapter 9](#) - Internet Connections

[Chapter 10](#) - Additional Security Features

[Chapter 11](#) - Basic Kernel Configuration

[Chapter 12](#) - Building Custom Kernels

[Chapter 13](#) - Add-On Software

[Chapter 14](#) - /ETC

[Chapter 15](#) - Disk and File System Management

[Chapter 16](#) - Upgrading OpenBSD

[Chapter 17](#) - Basic Packet Filtering

[Chapter 18](#) - More Packet Filtering

[Chapter 19](#) - Managing PF

[Appendix A](#) - i386 Kernel Configuration Choices

[Appendix B](#) - PF Example Configurations

[Afterword](#)

[Index](#)

[List of Tables](#)

---

## Back Cover

This straightforward, practical, and complete guide to mastering the powerful and complex OpenBSD operating system, is for the experienced UNIX user who wants to add OpenBSD to his or her repertoire. The author assumes a knowledge of basic UNIX commands, design, and permissions. The book takes you through the intricacies of the platform and teaches how to manage your system, offering friendly explanations, background information, troubleshooting suggestions, and copious examples throughout.

### About the Author

Michael W. Lucas, author of *Absolute BSD*, has been working with BSD-based operating systems since the late 1980s. His column, *Big Scary Daemons*, for the O'Reilly Report is in its third year. He has worked for several years as a consultant specializing in security, intrusion response, and network management.

---

# Absolute OpenBSD UNIX for the Practical Paranoid



by Michael W. Lucas

San Francisco

Copyright © 2003 by Michael W. Lucas.

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.



Printed on recycled paper in the United States of America

1 2 3 4 5 6 7 8 9 10 - 06 05 04 03

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

**Publisher:** William Pollock  
**Managing Editor:** Karol Jurado  
**Cover and Interior Design:** Octopod Studios  
**Copyeditor:** Kenyon Brown  
**Compositor:** Wedobooks  
**Proofreader:** Stephanie Provines

Distributed to the book trade in the United States by Publishers Group West, 1700 Fourth Street, Berkeley, CA 94710; phone: 800-788-3123; fax: 510-658-1834.

Distributed to the book trade in Canada by Jacqueline Gross & Associates, Inc., One Atlantic Avenue, Suite 105, Toronto, Ontario M6K 3E7 Canada; phone: 416-531-6737; fax 416-531-4259.

---

For information on translations or book distributors outside the United States, please contact No Starch Press, Inc. directly:

No Starch Press, Inc.

555 De Haro Street, Suite 250, San Francisco, CA 94107

phone: 415-863-9900; fax: 415-863-9950; <[info@nostarch.com](mailto:info@nostarch.com)>; <http://www.nostarch.com>

The information in this book is distributed on an "As Is" basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

*Library of Congress Cataloguing-in-Publication Data*

Lucas, Michael W., 1967- Absolute OpenBSD: UNIX for the practical paranoid /  
Michael W. Lucas  
Includes index.

ISBN 1-886411-99-9

1. OpenBSD (Electronic resource)
2. Operating systems (Computers)
3. UNIX (Computer file) I. Title.

QA76.9.O63L835 2003

005.4'32--dc21

2003000473

*For Elizabeth, who brings spring's rich warm sunlight into darkest night*

---

## ACKNOWLEDGMENTS

OpenBSD is quite a trip, and the OpenBSD community even more so. Since starting this book, I've talked with more practical and professional paranoids than I knew existed outside of politics. It's been my privilege to work with some of the best computer security people in the world. Best of all, these people care about their work, and the impact it has on average people such as our parents and friends.

The following people all provided feedback on one or more chapters of this book, or answered specific questions on frequently-misunderstood aspects of OpenBSD, and as such deserve my heartfelt thanks. Some of them are OpenBSD crown princes, and others are just users who were trying to figure out what their computer was actually doing. What I've done right is thanks to them, and what I've done wrong is my own fault. They are, in alphabetical order: Shawn Carroll, Chris Cappuccio, Dave Feustel, Thorsten Glaser, Daniel Hartmeier, Jason Houx, Volker Kindermann, Anil Madhavapeddy, U.N. Owen (aka dreamwvr), Francisco Luis Roque, Srebrenko Sehic, Matt Simonsen, Sam Smith, Duncan Matthew Stirling, Peter Werner, and Jason Wright.

A special thanks goes out to Theo de Raadt, for taking time out of his fiendishly busy schedule to provide special insight into the innards of OpenBSD, for not holding back when I goofed, and especially for sticking to his standards of freedom, despite everything the world has to say on that subject.

When an author says something like, "Hold the presses! OpenBSD just added a whole slew of functionality and I have to rewrite huge sections of the book you were planning to ship out tomorrow," the editor is supposed to respond with dire threats involving chainsaws. The folks at No Starch just say, "Well, get to work then." I have been forced to report to the Secret Author Cabal that Bill and Karol are patient, kind, and thoughtful enough to resist our best techniques for driving publishers into Lovecraftian madness.

Then there's Sifu Brown and the fine staff and volunteers of the School of Chinese Martial Arts in Berkley, Michigan (<http://www.ZenMartialArts.com>). They have absolutely nothing to do with computers, but they have an awful lot to do with me not making dire threats involving chainsaws. Somehow, the Five Ways to Become a Great Martial Artist turned out to be the same as the Five Ways to Write a Great Computer Book. I just never knew it before.

And finally, for Liz, and not just for catching the pet rats before they can stash seeds in server cases.

**Michael Lucas**  
**Saint Clair Shores, MI**  
**May 2003**

---

# Chapter 0: Introduction

## *Overview*

*The very quick path to a quiescent pager? OpenBSD.*

Welcome to *Absolute OpenBSD*! This book is an introductory text to general management of the OpenBSD server operating system. OpenBSD is a member of the BSD family of operating systems and is widely regarded as the most secure operating system available anywhere, under any licensing terms. It's widely used by Internet service providers, embedded systems manufacturers, and anyone who needs security and stability. If you're an experienced UNIX systems administrator who wants to add OpenBSD to your repertoire, this book is for you!

By the time you finish this book you should be comfortable on an OpenBSD system. You will understand how to manage, upgrade, and patch computers running OpenBSD. You'll also have a basic understanding of OpenBSD's software, security, and network management features.

## *What Is BSD?*

AT&T employees created UNIX in the early 1970s. At the time, the monster telephone company was forbidden to compete in the computer industry. The telecommunications company used UNIX internally, but could not transform it into a commercial product. As such, AT&T was willing to license the UNIX software and its source code to universities for a nominal fee. This worked well for all parties: AT&T got a few pennies and a generation of computer scientists who cut their teeth on AT&T technology, the universities avoided high operating system license fees, and the students were able to dig around inside the source code and see how computers really worked.

Compared to some of the other operating systems of the time, the original UNIX wasn't very good. But all these students had the source code for it and could improve the parts that they didn't like. If an instructor found a certain bug particularly vexing, he could assign his students the job of fixing it. If a university network engineer, professor, or student needed a feature, he could use the source code to quickly implement it. As the Internet grew in the early 1980s, these additions and features were exchanged between universities in the form of patches. The Computer Science Research Group (CSRG) at the University of California, Berkeley, acted as a central clearinghouse for these patches. The CSRG distributed these patches to anyone with a valid AT&T source code license. The resulting collection of patches became known as the

---

Berkeley Software Distribution, or BSD.

This continued for a long, long time. If you look at the copyright for any BSD-derived code, you will see the following text.

```
Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.
```

Fifteen years of continuous development by the brightest students of the best computer science programs in the world, moderated by the faculty of one of the top technical schools in the country. That's more than a lifetime in software development. As you might imagine, the result was pretty darn good – almost everyone who used UNIX was really using BSD. The CSRG was quite surprised, near the end of these years, when it found that it had replaced almost all of the original AT&T code!

## ***BSD Goes Public***

In the early 1990s, the CSRG's funding started to run out. The University of California had to decide what to do with all this wonderful source code it owned. The simplest thing would have been to drop the original tapes down a well and pretend that the CSRG had never happened. In keeping with the spirit of academic freedom, however, it released the entire BSD collection to the public under an extremely liberal license. The license can be summarized like this:

- Don't claim you wrote this.
- Don't sue us if it breaks.
- Don't use our name to promote your product.

Compare this with the software license found on almost any commercial operating system. The BSD license is much easier to understand and unobjectionable to almost anyone. Anyone in the world can take the BSD code and use it for any purpose they like, from desktop computers to self-guided lawnmowers. Not surprisingly, many computer manufacturers jumped right on BSD. Not only was the code free, but also every computer science graduate for the last 15 years was familiar with it.

## ***AT&T UNIX***

As the CSRG was merrily improving AT&T's product, AT&T was doing its own UNIX development work to meet its internal needs. As AT&T developers implemented features, they



- [\*India: A Sacred Geography online\*](#)
- [\*read online The Mammoth Book of Best New Erotica 5 book\*](#)
- [\*Peter Pan: Peter and Wendy and Peter Pan in Kensington Gardens here\*](#)
- [\*read Coincidence Engine pdf, azw \(kindle\), epub\*](#)
- [\*download online Miscarriages of Justice: Famous London Cases\*](#)
  
- <http://creativebeard.ru/freebooks/India--A-Sacred-Geography.pdf>
- <http://serazard.com/lib/The-Mammoth-Book-of-Best-New-Erotica-5.pdf>
- <http://deltaphenomics.nl/?library/Secure-the-Soul--Christian-Piety-and-Gang-Prevention-in-Guatemala.pdf>
- <http://hasanetmekci.com/ebooks/Coincidence-Engine.pdf>
- <http://studystategically.com/freebooks/Miscarriages-of-Justice--Famous-London-Cases.pdf>