

2ND
EDITION

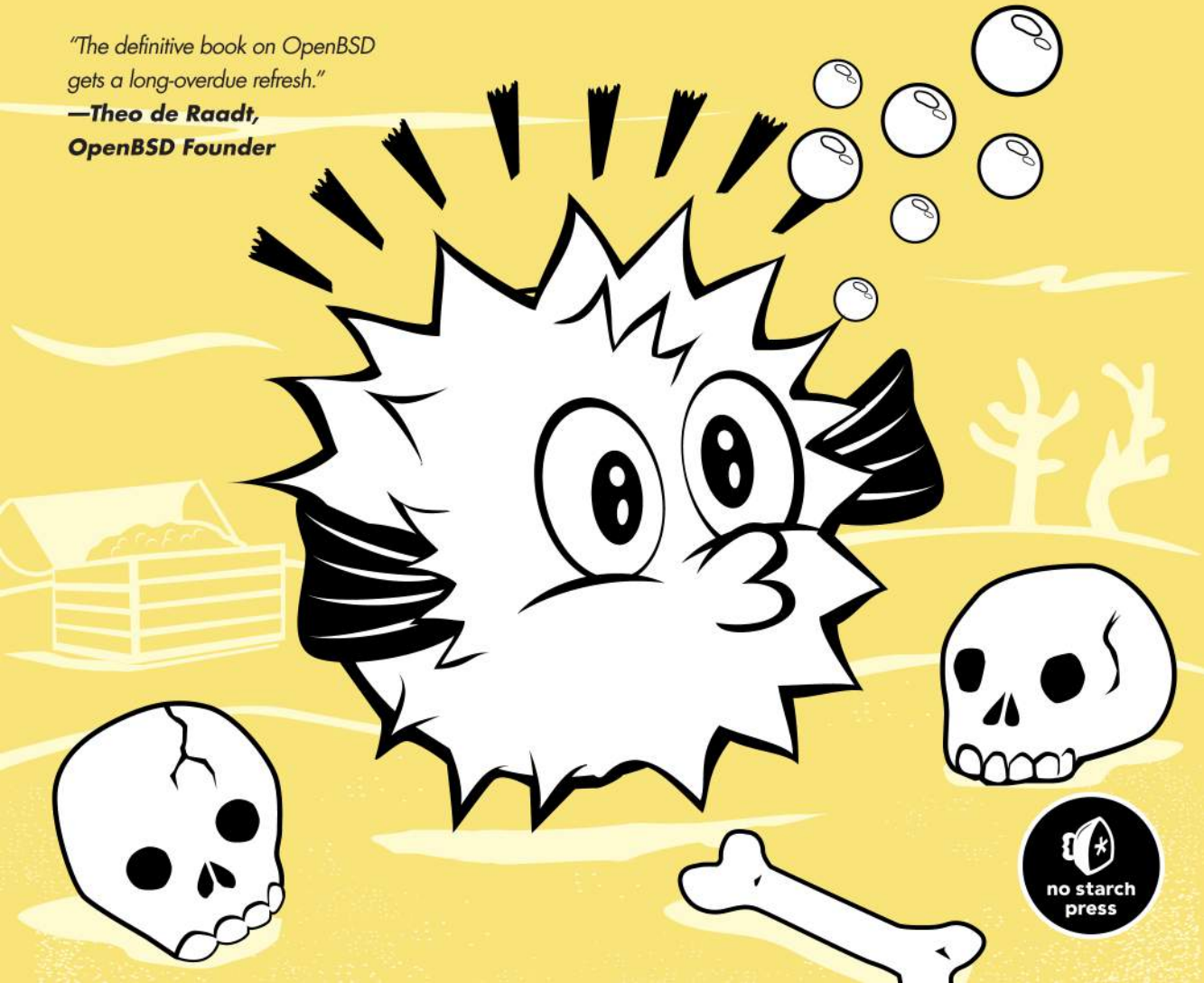
ABSOLUTE OPENBSD

UNIX FOR THE PRACTICAL PARANOID

MICHAEL W. LUCAS

*"The definitive book on OpenBSD
gets a long-overdue refresh."*

—Theo de Raadt,
OpenBSD Founder



CONTENTS IN DETAIL

FOREWORD by Henning Brauer

XXV

ACKNOWLEDGMENTS

XXVII

INTRODUCTION

XXIX

What Is Security?	xxx
What Is BSD?	xxxii
The BSD License	xxxii
AT&T vs. the World	xxxii
The Birth of OpenBSD	xxxiii
The OpenBSD Community	xxxiv
OpenBSD Users	xxxiv
OpenBSD Contributors	xxxiv
OpenBSD Committers	xxxv
OpenBSD Coordinator	xxxv
OpenBSD's Strengths	xxxv
Portability	xxxvi
Power	xxxvi
Documentation	xxxvi
Free	xxxvii
Correctness	xxxviii
Security	xxxviii
OpenBSD and Your Security	xxxix
OpenBSD's Uses	xl
Desktop	xl
Server	xl
Network Management	xl
About This Book	xl
Contents Overview	xli

1

GETTING ADDITIONAL HELP

1

OpenBSD's Support Model	2
The Code Is Fine. What's Wrong with You?	2
Sources of Information	3
Man Pages	3
The OpenBSD Website	7
OpenBSD Mailing Lists	8
Using OpenBSD Problem-Solving Resources	10
Using the OpenBSD Website	10
Using Man Pages	10
Using Internet Searches	11
Using Mailing Lists	11

2

INSTALLATION PREPARATIONS

15

OpenBSD Hardware	16
Supported Hardware.	17
Proprietary Hardware, Blobs, and Firmware.	17
Processors	18
Memory (RAM)	18
Hard Drives	18
Virtualization	19
Multiple Operating Systems	19
Getting OpenBSD	19
Official CDs	20
Internet Downloads	20
Mirror Site Layout	20
Release Directories	21
Boot Media	22
Choosing Install Media	22
Local Installation Servers	23
File Sets	23
Partitioning	25
Standard OpenBSD Partitions	26
Creating Other Partitions	29
Partition Filesystems	29
Multiple Hard Drives.	29
Understanding Partitions	30
MBR Partitions	30
Disklabel Partitions	31
Understanding Disklabels	31
Sectors and Lies	31
Sectors and Disklabels.	32
Other Information.	35

3

INSTALLATION WALK-THROUGH

37

Hardware Setup	38
BIOS Configuration	38
Making Boot Media	38
Making Boot Floppies	39
Making Boot CDs	40
Installing OpenBSD	41
Running the Installation Program	41
Multiple Network Cards.	43
Setting Up Services and the First User	44
Setting the Time Zone	45
Setting Up the Disk	46
Choosing File Sets.	47
Finishing the Installation.	49
Custom Disk Layout	49
Viewing Disklabels	50
Deleting Partitions	51
Erasing Existing Disklabels	51

Creating Disklabel Partitions	51
Writing the New Disklabel	53
Adding More Disks	54
Advanced Disklabel Commands.	54
Changing Basic Drive Parameters	54
Modifying Existing Partitions.	55
Entering Expert Mode	55
Getting More Help	55

4 POST-INSTALL SETUP 57

First Steps	58
Checking the System Errata	58
Setting the Root Password	58
Software Configuration.	59
Time and Date	60
Setting the Time Zone	60
Setting the Date and Time	60
Hostname	61
Networking.	62
Configuring Ethernet Interfaces	62
Setting a Default Gateway	64
Setting Name Service Servers.	65
Mail Aliases and Status Mail.	65
Keyboard Mapping	66
Installing Ports and Source Code	66
Booting to a Graphic Console	67
Onward!.	67

5 THE BOOT PROCESS 69

Power-On and the Boot Loader	70
Booting in Single-User Mode	71
Mounting Disks in Single-User Mode	71
Starting the Network in Single-User Mode	72
Booting an Alternate Kernel.	72
Booting a Different Kernel File	72
Booting from an Alternate Hard Disk	73
Making Boot Loader Settings Permanent	74
Serial Consoles	75
Other Platform Serial Consoles	75
Serial Console Physical Setup	75
Serial Console Configuration	76
Changing the Serial Console Speed	77
Changing the Client Serial Port.	78
Serial Logins.	79
Multiuser Startup	79
Startup System Scripts	80
Software Startup Scripts.	82
Third-Party rc.d Scripts.	83
Force-Starting Software	83

6	USER MANAGEMENT	85
The Root Account		86
Adding Users		86
Adding Users Interactively		87
Adding Users Noninteractively		89
User Account Restrictions		92
Removing User Accounts		92
Editing User Accounts		93
Login Classes		94
Login Class Definitions		94
Changing login.conf		95
Legal Values for login.conf Variables		95
Setting Resource Limits		96
Modifying the Shell Environment		97
Password and Login Options		98
Changing Authentication Methods		99
Using Login Classes for RADIUS Authentication		100
Unprivileged User Accounts		102
The nobody Account		103
_username		103
Creating Unprivileged Users		104
 7	 ROOT, AND HOW TO AVOID IT	 105
The Root Password		106
Using Groups		106
The /etc/group File		107
Creating Groups		107
Groups, Unprivileged Users, and Group Permissions		108
Hiding Root with sudo		109
Why Use sudo?		109
sudo Disadvantages		109
An Overview of the sudo Software		110
The visudo(8) Command		110
The /etc/sudoers File		111
/etc/sudoers Aliases		113
Changing sudo's Default Behavior		117
sudo and the Environment		119
Using sudo		120
sudo Password Caching		120
Running Commands Under sudo		121
Running Commands as Other Users		121
sudoedit		121
The Biggest sudo Mistake: Exclusions		122
sudo Logs		123

8

DISKS AND FILESYSTEMS

125

Device Nodes	126
Raw and Block Devices	126
Device Attachment vs. Device Name	127
DUIDs and /etc/fstab	128
MBR Partitions and fdisk(8)	129
Viewing MBR Partitions	130
Adding and Removing Partitions	130
Making a Partition Bootable	131
Exiting fdisk	131
Labeling Disks	132
Viewing Labels	132
Creating Disklabel Partitions	132
Backing Up and Restoring Disklabels	133
The Fast File System	133
FFS Versions	133
Blocks, Fragments, and Inodes	134
Creating FFS Filesystems	134
FFS Mount Options	135
Filesystem Integrity	138
What's Currently Mounted?	140
Mounting and Unmounting Partitions	140
Mounting Standard Filesystems	141
Mounting at Nonstandard Locations	141
Unmounting Partitions	141
Mounting with Options	142
How Full Is That Partition?	142
What's All That Stuff?	143
Setting \$BLOCKSIZE	143
Adding New Hard Disks	144
Creating an MBR Partition	144
Creating a Disklabel	144
Moving Partitions	145
Adding New Filesystems	146
Stackable Mounts	146

9

MORE FILESYSTEMS

147

Backing Up to the /altroot Partition	148
Memory Filesystems	148
Creating MFS Partitions	149
Mounting an MFS at Boot	149
Foreign Filesystems	150
Inodes vs. Vnodes	150
Common Foreign Filesystems	151
Foreign Filesystem Ownership	152

Removable Media	153
Mounting Filesystem Images	153
Attaching Vnode Devices to Disk Images	154
Detaching Vnode Devices from Images	154
Basic NFS Setup	154
The OpenBSD NFS Server	155
Exporting Filesystems	156
Read-Only Mounts	157
NFS and Users	157
Permitted Clients	158
Multiple Exports for One Partition	159
NFS Clients	159
Software RAID	160
RAID Types	161
Preparing Disks for softraid	162
Creating softraid Devices	163
softraid Status	164
Identifying Failed softraid Volumes	164
Rebuilding Failed softraid Volumes	164
Deleting softraid Devices	165
Reusing softraid Disks	166
Bootng from a softraid Device	166
Encrypted Disk Partitions	166
Creating Encrypted Partitions	166
Using Encrypted Partitions	167
Automatic Decryption	168

10

SECURING YOUR SYSTEM

169

Who Is the Enemy?	170
Script Kiddies	170
Botnets	170
Disaffected Users	171
Skilled Attackers	171
OpenBSD Security Announcements	172
OpenBSD Memory Protection	172
W^X	173
.rodata Segments	173
Guard Pages	174
Address Space Layout Randomization	174
ProPolice	174
And More!	174
File Flags	175
File Flag Types	175
Setting, Viewing, and Removing File Flags	176
Securelevels	177
Setting the System Securelevel	178
Securelevel Definitions	178

What Securelevel Do You Need?	180
Securelevel Weaknesses	180
Keeping Secure	181

11

OVERVIEW OF TCP/IP

183

Network Layers	184
The Physical Layer	184
The Datalink Layer	185
The Network Layer	185
The Transport Layer	186
Applications	186
The Life and Times of a Network Request	187
Network Stacks	188
IPv4 Addresses and Subnets	189
Calculating a Decimal IPv4 Netmask	190
Viewing IPv4 Addresses	191
Unusable IPv4 Addresses	191
Special IPv4 Addresses	192
IPv4 Addressing Pitfalls	192
IPv6 Addresses and Subnets	192
IPv6 Basics	193
Understanding IPv6 Addresses	193
Viewing IPv6 Addresses	194
IPv6 Subnets	194
Special IPv6 Addresses	194
Assigning IPv6 Addresses	195
Remedial TCP/IP	196
ICMP	196
UDP	196
TCP	197
How Protocols Fit Together	198
Transport Protocol Ports	198
Reserved Ports	199
Which Ports Are Open?	200
IP Routing	202
IPv4 Routed Network Example	203
Managing Routing with route(8)	204

12

CONNECTING TO THE NETWORK

209

DNS Resolution	210
The /etc/resolv.conf File	210
The /etc/hosts File	212
Resolver vs. Dynamic Configuration	212
Ethernet	213
Protocol and Hardware	213

Configuring Ethernet	215
Using ifconfig(8)	216
Configuring Default Routes	219
Using Dynamic Configuration	219
Configuring the Network at Boot	219
Trunking	221
Link Aggregation Protocols	221
Trunk Configuration	221
Trunks at Boot	222
VLANs	223
Configuring Switches	223
Configuring VLAN Devices	223
Configuring VLANs at Boot	224
IPv6 Over Tunnels	224

13

SOFTWARE MANAGEMENT

225

Making Software	226
Source Code and Software	226
The Ports and Packages System	227
Using Packages	228
Package Files and \$PKG_PATH	228
Finding Packages	229
Installing Packages	230
Identifying Where Files Originate	232
Uninstalling Packages	234
Package Limitations	235
Using Ports	235
The Ports Tree	236
Secondary Ports	237
Read-Only Ports Tree	238
Finding Software	239
Building Ports	241
What a Port Installation Does	242
Port Build Stages	243
Customizing Ports	246
Local Distfile Mirrors	246
Flavors	249
Subpackages	251
Packages and rc.d Scripts	252

14

EVERYTHING /ETC

255

/etc Across Unix Variants	256
The /etc Files	256
/etc/adduser.conf	256
/etc/amd	256
/etc/authpf	256

/etc/bgpd.conf	257
/etc/boot.conf	257
/etc/changelist	257
/etc/chio.conf	257
/etc/csh.*	257
/etc/daily and /etc/daily.local	257
/etc/dhclient.conf	257
/etc/dhcpd.conf	257
/etc/disklabels/	257
/etc/disktab	258
/etc/dumpdates	258
/etc/dvmrpd.conf	258
/etc/exports	258
/etc/fstab	258
/etc/firmware	258
/etc/fonts/	259
/etc/fstab	259
/etc/ftpchroot	259
/etc/ftpusers	259
/etc/gettytab	259
/etc/group	260
/etc/hostapd.conf	260
/etc/hostname.*	260
/etc/hosts	260
/etc/hosts.equiv	260
/etc/hosts.lpd	260
/etc/hotplug/	261
/etc/ifstated.conf	261
/etc/iked/, /etc/iked.conf, /etc/ipsec.conf, and /etc/isakmpd	261
/etc/inetd.conf	261
/etc/kbdtype	261
/etc/kerberosV/	262
/etc/ksh.kshrc	262
/etc/ldap/ and /etc/ldapd.conf	262
/etc/localtime	262
/etc/locate.rc	262
/etc/login.conf	262
/etc/lynx.cfg	262
/etc/magic	262
/etc/mail/	263
/etc/mail.rc	263
/etc/mailer.conf	263
/etc/man.conf	264
/etc/master.passwd, /etc/passwd, /etc/spwd.db, and /etc/pwd.db	265
/etc/mixerctl.conf	268
/etc/mk.conf	268
/etc/moduli	268
/etc/monthly and /etc/monthly.local	268
/etc/motd	269
/etc/mrouted.conf	269

/etc/mtree/	269
/etc/mygate.	269
/etc/myname.	269
/etc/netstart.	269
/etc/networks	269
/etc/newsyslog.conf	269
/etc/nginx/	269
/etc/nsd.conf.	270
/etc/ntpd.conf	270
/etc/ospf6d.conf and /etc/ospfd.conf	270
/etc/pf.conf and /etc/pf.os	270
/etc/ppp/	270
/etc/printcap	270
/etc/protocols	270
/etc/rbootd.conf.	271
/etc/rc.*	271
/etc/relayd.conf.	271
/etc/remote	271
/etc/resolv.conf and /etc/resolv.conf.tail	271
/etc/ripd.conf	271
/etc/rmt	271
/etc/rpc	272
/etc/sasyncd.conf.	272
/etc/sensorsd.conf	272
/etc/services	272
/etc/shells	272
/etc/skel/	272
/etc/sliphome/.	272
/etc/snmpd.conf.	273
/etc/ssh/.	273
/etc/ssl/	273
/etc/sudoers	273
/etc/sysctl.conf.	273
/etc/syslog.conf	273
/etc/systrace/	273
/etc/termcap	274
/etc/ttys	274
/etc/weekly and /etc/weekly.local.	276
/etc/wsconsctl.conf.	276
/etc/X11	276
/etc/ypldap.conf	276

15 SYSTEM MAINTENANCE

277

Scheduled Tasks	277
Daily Maintenance	278
Weekly Maintenance	282
Monthly Maintenance	282
Custom Maintenance Scripts.	282

System Logs	282
Facilities	283
Priority	284
Sorting Messages via syslogd(8)	284
Log Actions	287
Customizing syslogd	288
Syslog and Embedded Systems	289
Log File Maintenance	289
newsyslog.conf Fields	290
Monitoring Logs	293
Adding a PID File	293
Signal Name	293
Command to Execute	294
System Time	294
Configuring ntpd(8)	294
Using ntpd(8)	296
Hardware Sensors	296
Device Drivers	297
Sensor Configuration	298

16

NETWORK SERVERS

303

The inetd Small-Server Handler	304
Configuring inetd	304
Restricting Incoming Connections	305
The lpd Printing Daemon	306
The DHCP Server dhcpd	307
How DHCP Works	307
Configuring dhcpd(8)	308
Static IP Address Assignments	309
Enabling dhcpd	309
dhcpd and Firewalls	309
The TFTP Daemon tftpd	310
Specifying a tftpd Directory	310
tftpd and Files	311
tftpd Logging	311
Testing the TFTP Server	311
The SNMP Agent snmpd	312
SNMP MIBs	312
SNMP Security	314
Configuring snmpd	314
Debugging snmpd	315
Getting snmpd Information	316
The SSH Server sshd	317
Disabling sshd	318
SSH Host Keys	318
sshd Network Options	318
chrooting Users	319

17

DESKTOP OPENBSD 323

Configuring Your Console with wscons	324
Screen Blanking	324
Setting wscons Variables at Boot.	325
Running Virtual Terminals with tmux	325
The tmux Status Bar and Window Names	326
tmux Commands and Window Management	326
Getting Online Help	327
Disconnecting, Reconnecting, and Managing Sessions	327
Using tmux Commands	328
Setting tmux Options	329
Configuring tmux	329
Setting Up X	330
Configuring X.	330
Starting X Manually.	330
Booting into X.	330
Emulating a Three-Button Mouse	331
Using the cwm Window Manager	331
Configuring cwm	331
Creating cwm Windows	332
Managing Windows	333
Locking the Screen	333
Connecting to Other Machines with SSH	334
Creating an Application Menu	334
Using Keyboard Navigation.	335
Decorating cwm	335
Unmapping and Remapping Keys.	336

18

KERNEL CONFIGURATION 339

What Is the Kernel?	340
Kernel Messages.	340
Startup Messages	340
Device Attachments	341
Connections and Numbering	342
Using dmessage to View Installed Devices	343
Viewing and Adjusting Sysctls	343
Sysctl MIBs.	343
Viewing Sysctls.	344
Changing Sysctl Values	345
Types of Sysctl Values	345
Setting Sysctls at Boot	346
Altering the Kernel with config(8)	348
Making a Backup of the Default Kernel	349
Device Drivers and the Kernel.	349
Enabling Drivers	350
Editing the Kernel with config	350
Boot-Time Kernel Configuration	353

19	BUILDING CUSTOM KERNELS	355
Kernel Cautions		355
Don't Build Custom Kernels.		356
Why Build Custom Kernels?		356
Problems Building Custom Kernels.		357
Problems Running Custom Kernels.		358
Preparing for Kernel Customization		358
Kernel Configuration		359
Configuration Entries		359
Configuring GENERIC.		360
Your Kernel Configuration		362
Testing Your Kernel Configuration with config(8).		364
Building a Kernel		365
Kernel Build Errors.		365
Installing Your Kernel		366
Identifying the Running Kernel		366
 20		
UPGRADING		367
Why Upgrade?		368
OpenBSD Versions.		368
OpenBSD-current		368
OpenBSD Snapshots		369
OpenBSD Releases		369
OpenBSD-stable		370
Which Version Should You Use?		370
The OpenBSD Upgrade Process.		371
Following the Upgrade Guide.		371
Customizing Upgrades		373
Upgrading from Official Media		373
Upgrading Over the Network		374
Choosing File Sets.		375
Updating /etc		375
Mounting Filesystems.		376
Using sysmerge(8) to Compare /etc Files.		376
Updating Installed Packages		380
Updating the Package Repository		380
Using the Upgrade Command		381
Why Build Your Own OpenBSD?		382
Preparations for Building Your Own OpenBSD		383
Preparing the Base Operating System		383
Getting Source Code.		384
Updating Source Code		385
Building OpenBSD-stable		388
Upgrading the Kernel		388
Building the Userland		389
Building Xenocara.		389
Building a Release.		389
Using the Release		392

Building OpenBSD-current	392
Following -current	392
Merging /etc	393
Upgrading Ports	393

21

PACKET FILTERING 395

Firewalls	396
Enabling and Configuring PF	397
Packet-Filtering Basics	398
Packet-Filtering Concepts	398
“My Network Can Do No Wrong”	400
What Packet Filtering Doesn’t Do	400
PF Components	401
Packet Filter Control and Configuration	401
Interface Groups	401
PF Configuration	402
Filtering Rules	403
Default Permit or Default Deny	404
Packet Pattern Matching	404
A Complete Ruleset	409
Activating Rules	409
Viewing Active Rules	410
Filtering Rules and the State Table	411
TCP States	411
UDP States	412
ICMP States	413
Packet Filtering with Lists and Macros	413
Using Lists	413
Using Macros	414
A Common Error: List Exclusions and Negations	415
Sanitizing Traffic	415
Illegal Packets	415
Packet Reassembly	416
Packet Modification	416
Blocking Spoofed Packets	416
PF Options	417
The set block-policy Option	417
The set limit Option	417
The set optimization Option	419
The set skip Option	420

22

ADVANCED PF 421

Packet Filtering with Tables	422
Defining Tables	422
Using Tables	423
Viewing Tables	423
Searching Tables	424

Changing Tables	424
Tables and Automation	425
Using NAT	426
Private NAT Addresses	426
Configuring NAT	427
How NAT Works	427
Multiple or Specific Public Addresses	428
Bidirectional NAT	429
Redirection	431
Multiple Addresses and Interface Groups	432
Port Manipulation and Ranges	432
Transparent Interception	433
Anchors	434
Adding Rules to Anchors	434
Viewing and Flushing Anchors	436
Conditional Filtering	436
Nested Anchors: /*	436
FTP and PF	437
Configuring ftp-proxy(8)	438
PF Configuration and the FTP Proxy	438
Bandwidth Management	439
Queues for Bandwidth Management	440
Parent Queue Definitions	441
Child Queue Definitions	442
Queue Options	442
A CBQ Ruleset	443
Assigning Traffic to Queues	444
Using the match Keyword	444
Viewing Queues	445
PF Edges	445
Using Include Files	445
Skipping Matches with quick	446
Logging PF	446
Reading PF Logs	447
Real-Time Log Access	447
Filtering tcpdump	447
Ruleset Tracing	448

23 CUSTOMIZING OPENBSD 449

Virtualizing OpenBSD	450
Diskless Installation	450
Diskless Hardware	451
DHCP Server Setup	452
TFTP Server Setup	453
Completing Diskless Installation	454
Running Diskless	454
Using rarpd(8) for Reverse ARP	454
Running bootparamd(8)	455
Setting Up the NFS Root Directory	455
Power On!	456

USB Installation Media	457
Using a Virtual Machine	457
Running a Diskless Installation.	457
Converting ISO Images	457
Customizing OpenBSD Installations.	458
Custom File Sets	458
Post-Install Shell Scripts	459
Customizing Upgrades	460
 AFTERWORD	 461
 INDEX	 465