# Table of Contents

## FOREWORD
- xlii

## PREFACE
- xliv

## ACKNOWLEDGMENTS
- xlvii

## SECTION ONE: BASIC ADMINISTRATION

### CHAPTER 1 WHERE TO START
- 3
  - Essential duties of the system administrator ................. 4
  - Account provisioning ........................................ 4
  - Adding and removing hardware ............................. 4
  - Performing backups .......................................... 5
  - Installing and upgrading software .......................... 5
  - Monitoring the system ....................................... 5
  - Troubleshooting ............................................. 5
  - Vigilantly monitoring security .............................. 6
  - Fire fighting ................................................ 6
  - Suggested background ....................................... 6
  - Friction between UNIX and Linux .......................... 7
  - Linux distributions ......................................... 9
  - Example systems used in this book ......................... 10
    - Example Linux distributions ............................. 11
    - Example UNIX distributions .............................. 12
System-specific administration tools .................................................... 13
Notation and typographical conventions ............................................. 13
Units ........................................................................................................ 14
Man pages and other on-line documentation ....................................... 16
  Organization of the man pages ............................................................... 16
  man: read man pages ............................................................................. 17
  Storage of man pages ........................................................................... 17
  GNU Texinfo ......................................................................................... 18
Other authoritative documentation ...................................................... 18
  System-specific guides ......................................................................... 18
  Package-specific documentation ........................................................... 19
  Books ...................................................................................................... 19
  RFCs and other Internet documents ..................................................... 20
  The Linux Documentation Project ......................................................... 20
Other sources of information ................................................................. 20
Ways to find and install software ............................................................ 21
  Determining whether software has already been installed ................. 22
  Adding new software ............................................................................ 23
  Building software from source code ..................................................... 25
System administration under duress ...................................................... 26
Recommended reading ......................................................................... 27
  System administration ......................................................................... 27
  Essential tools ..................................................................................... 27
Exercises ................................................................................................. 28

CHAPTER 2  SCRIPTING AND THE SHELL .................................................. 29
Shell basics .............................................................................................. 30
Command editing ................................................................................... 30
Pipes and redirection .............................................................................. 31
Variables and quoting ............................................................................ 32
Common filter commands ..................................................................... 33
  cut: separate lines into fields ................................................................. 34
  sort: sort lines ....................................................................................... 34
  uniq: print unique lines ........................................................................ 35
  wc: count lines, words, and characters ................................................ 35
  tee: copy input to two places ............................................................... 35
  head and tail: read the beginning or end of a file ............................. 36
  grep: search text ................................................................................... 36
# Table of Contents

**bash scripting** .......................................................... 37
  From commands to scripts .............................................. 38
  Input and output ....................................................... 40
  Command-line arguments and functions ............................ 40
  Variable scope .......................................................... 42
  Control flow ............................................................. 43
  Loops ........................................................................... 45
  Arrays and arithmetic ................................................... 47

**Regular expressions** .................................................... 48
  The matching process ..................................................... 49
  Literal characters ........................................................ 49
  Special characters ........................................................ 50
  Example regular expressions .......................................... 51
  Captures ....................................................................... 52
  Greediness, laziness, and catastrophic backtracking ........... 53

**Perl programming** .......................................................... 54
  Variables and arrays ....................................................... 55
  Array and string literals ................................................ 56
  Function calls ................................................................ 56
  Type conversions in expressions ...................................... 57
  String expansions and disambiguation of variable references . 57
  Hashes .......................................................................... 57
  References and autovivification ....................................... 59
  Regular expressions in Perl ............................................. 60
  Input and output ............................................................ 61
  Control flow .................................................................... 61
  Accepting and validating input ........................................ 63
  Perl as a filter ............................................................... 64
  Add-on modules for Perl .................................................. 65

**Python scripting** ............................................................. 66
  Python quick start .......................................................... 67
  Objects, strings, numbers, lists, dictionaries, tuples, and files . 69
  Input validation example ................................................ 70
  Loops ............................................................................ 71

**Scripting best practices** .................................................. 73

**Recommended reading** .................................................... 74
  Shell basics and __bash__ scripting ................................... 74
  Regular expressions ....................................................... 74
  Perl scripting ................................................................ 75
  Python scripting ............................................................ 75

**Exercises** .................................................................... 76
CHAPTER 3  BOOTING AND SHUTTING DOWN

Bootstrapping ................................................................. 78
  Recovery boot to a shell .............................................. 78
  Steps in the boot process ............................................ 78
  Kernel initialization .................................................. 79
  Hardware configuration .............................................. 79
  Creation of kernel processes ..................................... 79
  Operator intervention (recovery mode only) ..................... 80
  Execution of startup scripts ..................................... 81
  Boot process completion .......................................... 81
Booting PCs .............................................................. 82
  GRUB: The GRand Unified Boot loader ............................ 83
    Kernel options .................................................... 84
    Multibooting ...................................................... 85
Booting to single-user mode ......................................... 86
  Single-user mode with GRUB ....................................... 86
  Single-user mode on SPARC ........................................ 86
  HP-UX single-user mode ........................................... 87
  AIX single-user mode ............................................... 87
Working with startup scripts ........................................ 87
  init and its run levels ............................................. 88
  Overview of startup scripts ..................................... 89
  Red Hat startup scripts .......................................... 91
  SUSE startup scripts .............................................. 93
  Ubuntu startup scripts and the Upstart daemon .............. 94
  HP-UX startup scripts ............................................ 95
  AIX startup .......................................................... 95
Booting Solaris .......................................................... 97
  The Solaris Service Management Facility ........................ 97
  A brave new world: booting with SMF ........................... 99
Rebooting and shutting down ......................................... 100
  shutdown: the genteel way to halt the system ................. 100
  halt and reboot: simpler ways to shut down ................. 101
Exercises ................................................................. 102

CHAPTER 4  ACCESS CONTROL AND ROOTLY POWERS

Traditional UNIX access control .................................... 104
  Filesystem access control ......................................... 104
  Process ownership .................................................. 105
  The root account .................................................... 105
  Setuid and setgid execution ..................................... 106
# Table of Contents

Modern access control .............................................. 106  
Role-based access control ........................................ 108  
SELinux: security-enhanced Linux ............................... 109  
POSIX capabilities (Linux) ....................................... 109  
PAM: Pluggable Authentication Modules ....................... 109  
Kerberos: third-party cryptographic authentication .......... 110  
Access control lists .............................................. 110  
Real-world access control ....................................... 110  
Choosing a root password ....................................... 111  
Logging in to the root account ................................ 112  
su: substitute user identity .................................... 113  
sudo: limited su ................................................. 113  
Password vaults and password escrow ......................... 117  
Pseudo-users other than root .................................. 118  
Exercises .................................................................. 119

## Chapter 5  Controlling Processes  
120

Components of a process ......................................... 120  
PID: process ID number ......................................... 121  
PPID: parent PID ................................................ 121  
UID and EUID: real and effective user ID .................... 122  
GID and EGID: real and effective group ID .................. 122  
Niceness .............................................................. 123  
Control terminal .................................................... 123  
The life cycle of a process ...................................... 123  
Signals .................................................................... 124  
kill: send signals .................................................... 127  
Process states ......................................................... 128  
nice and renice: influence scheduling priority .............. 129  
ps: monitor processes ............................................. 130  
Dynamic monitoring with top, prstat, and topas ............ 133  
The /proc filesystem .............................................. 135  
strace, truss, and tusc: trace signals and system calls .... 136  
Runaway processes ............................................... 138  
Recommended reading ........................................... 139  
Exercises .................................................................. 139

## Chapter 6  The Filesystem  
140

Pathnames ............................................................. 142  
Absolute and relative paths ...................................... 142  
Spaces in filenames ............................................... 142  
Filesystem mounting and unmounting ......................... 143  
The organization of the file tree ............................... 145
Unix and Linux System Administration Handbook

File types .......................................................... 147
  Regular files .................................................... 149
  Directories ...................................................... 149
  Character and block device files ................................. 150
  Local domain sockets .......................................... 151
  Named pipes .................................................. 151
  Symbolic links ............................................... 151
File attributes .................................................. 152
  The permission bits .......................................... 152
  The setuid and setgid bits ................................... 153
  The sticky bit .............................................. 154
  ls: list and inspect files .................................... 154
  chmod: change permissions ................................... 156
  chown and chgrp: change ownership and group ............... 157
  umask: assign default permissions ................................ 158
  Linux bonus flags ........................................... 158
Access control lists ............................................. 159
  A short and brutal history of UNIX ACLs ................. 160
  ACL implementation ............................................ 161
  ACL support by system ....................................... 162
  POSIX ACLs ...................................................... 162
    Interaction between traditional modes and ACLs ........ 163
    Access determination ....................................... 165
    ACL inheritance ........................................... 166
  NFSv4 ACLs ...................................................... 166
    NFSv4 entities for which permissions can be specified ... 168
    Access determination ....................................... 168
    ACL inheritance ........................................... 169
    NFSv4 ACL viewing in Solaris ............................ 169
    Interactions between ACLs and modes ................... 171
    Modifying NFSv4 ACLs in Solaris ......................... 172
Exercises .......................................................... 173

Chapter 7 Adding New Users .................................... 174

The /etc/passwd file .............................................. 176
  Login name .................................................... 176
  Encrypted password ........................................... 179
  UID (user ID) number ........................................ 180
  Default GID number .......................................... 181
  GECOS field .................................................. 181
  Home directory ............................................... 182
  Login shell ................................................... 182
The /etc/shadow and /etc/security/passwd files .............. 183
The /etc/group file ............................................. 186
Table of Contents

Adding users: the basic steps ......................................... 187
  Editing the *passwd* and *group* files .......................... 188
  Setting a password ............................................... 188
  Creating the home directory and installing startup files .... 189
  Setting permissions and ownerships ............................. 190
  Setting a mail home ............................................. 190
  Configuring roles and administrative privileges ............... 190
  Final steps ...................................................... 191

Adding users with *useradd* ......................................... 191
  *useradd* on Ubuntu ............................................ 192
  *useradd* on SUSE .............................................. 193
  *useradd* on Red Hat .......................................... 193
  *useradd* on Solaris ........................................... 194
  *useradd* on HP-UX ............................................ 194
  *useradd* on AIX ................................................ 195
  *useradd* example ............................................... 197

Adding users in bulk with *newusers* (Linux) ..................... 197

Removing users ..................................................... 198

Disabling logins ................................................... 200

Managing users with system-specific tools ....................... 201

Reducing risk with PAM ........................................... 201

Centralizing account management ................................ 201
  LDAP and Active Directory .................................... 202
  Single sign-on systems ........................................ 202

Identity management systems ..................................... 203

Recommended reading ............................................... 204

Exercises ............................................................. 205

**CHAPTER 8 STORAGE** ........................................... 206

I just want to add a disk! .......................................... 207
  Linux recipe ..................................................... 207
  Solaris recipe .................................................. 208
  HP-UX recipe ................................................... 208
  AIX recipe ....................................................... 209

Storage hardware .................................................... 209
  Hard disks ....................................................... 210
  Solid state disks .............................................. 212

Storage hardware interfaces ...................................... 213
  The PATA interface ............................................. 215
  The SATA interface ............................................ 215
  Parallel SCSI .................................................... 216
  Serial SCSI ...................................................... 219

Which is better, SCSI or SATA? ................................... 219

Peeling the onion: the software side of storage ................ 220
## UNIX and Linux System Administration Handbook

- Attachment and low-level management of drives ........................................ 223
- Installation verification at the hardware level ........................................... 223
- Disk device files. ......................................................................................... 224
  - Disk devices for Linux ........................................................................... 224
  - Disk devices for Solaris .......................................................................... 225
  - Disk devices for HP-UX ......................................................................... 225
  - Disk devices for AIX ............................................................................. 226
- Formatting and bad block management ......................................................... 226
- ATA secure erase ......................................................................................... 227
- **hdparm**: set disk and interface parameters (Linux) .................................. 229
- Hard disk monitoring with SMART ............................................................. 230
- Disk partitioning. ......................................................................................... 231
  - Traditional partitioning. ......................................................................... 233
  - Windows-style partitioning ...................................................................... 234
  - GPT: GUID partition tables .................................................................... 235
  - Linux partitioning. .................................................................................. 236
  - Solaris partitioning. ................................................................................ 236
  - HP-UX partitioning. ............................................................................... 237
- RAID: redundant arrays of inexpensive disks .................................................. 237
  - Software vs. hardware RAID ................................................................. 237
  - RAID levels ............................................................................................. 238
  - Disk failure recovery ............................................................................. 241
  - Drawbacks of RAID 5 ............................................................................. 241
  - **mdadm**: Linux software RAID ............................................................ 242
- Logical volume management ........................................................................ 246
  - LVM implementations ............................................................................ 246
  - Linux logical volume management .......................................................... 247
    - Volume snapshots. ............................................................................... 249
    - Resizing filesystems ............................................................................ 250
  - HP-UX logical volume management ....................................................... 251
  - AIX logical volume management ............................................................ 253
- Filesystems ..................................................................................................... 254
  - Linux filesystems: the ext family ............................................................ 255
  - HP-UX filesystems: VxFS and HFS ......................................................... 256
  - AIX’s JFS2 ............................................................................................... 257
  - Filesystem terminology .......................................................................... 257
  - Filesystem polymorphism ........................................................................ 258
  - **mkfs**: format filesystems ..................................................................... 258
  - **fsck**: check and repair filesystems ....................................................... 259
  - Filesystem mounting ................................................................................ 260
  - Setup for automatic mounting ................................................................. 260
  - USB drive mounting ................................................................................ 263
  - Enabling swapping .................................................................................. 264
Table of Contents

ZFS: all your storage problems solved ............................................. 264
  ZFS architecture ........................................................................ 265
  Example: Solaris disk addition .................................................... 266
  Filesystems and properties .......................................................... 266
  Property inheritance ................................................................. 268
  One filesystem per user .............................................................. 269
  Snapshots and clones .................................................................. 269
  Raw volumes .............................................................................. 271
  Filesystem sharing filesystem through NFS, CIFS, and iSCSI ...... 271
  Storage pool management ......................................................... 272
  Storage area networking ........................................................... 274
  SAN networks ............................................................................ 275
  iSCSI: SCSI over IP .................................................................... 276
  Booting from an iSCSI volume ................................................... 277
  Vendor specifics for iSCSI initiators ............................................ 277
  Exercises .................................................................................... 281

Chapter 9 Periodic Processes ......................................................... 283
  cron: schedule commands .......................................................... 283
  The format of crontab files ........................................................ 284
  Crontab management ................................................................. 286
  Linux and Vixie-cron extensions ................................................ 287
  Some common uses for cron ....................................................... 288
    Simple reminders .................................................................. 288
    Filesystem cleanup ............................................................... 289
    Network distribution of configuration files ............................... 290
    Log file rotation .................................................................... 290
  Exercises .................................................................................... 291

Chapter 10 Backups ................................................................. 292
  Motherhood and apple pie .......................................................... 293
    Perform all backups from a central location ......................... 293
    Label your media ................................................................... 293
    Pick a reasonable backup interval ......................................... 294
    Choose filesystems carefully ............................................... 294
    Make daily dumps fit on one piece of media ....................... 294
    Keep media off-site ............................................................... 295
    Protect your backups ............................................................ 295
    Limit activity during backups ............................................... 296
    Verify your media ................................................................. 297
    Develop a media life cycle ...................................................... 297
    Design your data for backups ............................................... 298
    Prepare for the worst ............................................................. 298
Backup devices and media .................................................. 299
Optical media: CD-R/RW, DVD±R/RW, DVD-RAM, and Blu-ray .... 299
Portable and removable hard disks ........................................ 300
Magnetic tapes in general .................................................. 301
Small tape drives: 8mm and DDS/DAT ................................... 301
DLT/S-DLT ........................................................................... 301
AIT and SAIT ....................................................................... 302
VXA/VXA-X ......................................................................... 302
LTO ...................................................................................... 302
Jukeboxes, stackers, and tape libraries ................................... 302
Hard disks ............................................................................ 303
Internet and cloud backup services ........................................ 303
Summary of media types ...................................................... 304
What to buy ......................................................................... 304
Saving space and time with incremental backups .................... 305
A simple schedule ............................................................... 306
A moderate schedule ........................................................... 307
Setting up a backup regime with dump ................................. 307
Dumping filesystems ............................................................ 308
Restoring from dumps with restore ....................................... 310
Restoring entire filesystems .................................................. 313
Restoring to new hardware ................................................... 314
Dumping and restoring for upgrades ....................................... 314
Using other archiving programs ............................................ 315
tar: package files ................................................................. 315
dd: twiddle bits ..................................................................... 316
ZFS backups ....................................................................... 316
Using multiple files on a single tape ....................................... 317
Bacula ................................................................................. 318
The Bacula model ............................................................... 319
Setting up Bacula ............................................................... 320
Installing the database and Bacula daemons ......................... 320
Configuring the Bacula daemons .......................................... 321
Common configuration sections .......................................... 322
bacula-dir.conf: director configuration ................................. 324
Catalog resources .............................................................. 324
Storage resources .............................................................. 324
Pool resources .................................................................... 325
Schedule resources ........................................................... 325
Client resources ................................................................. 325
FileSet resources ............................................................... 326
Job resources ..................................................................... 326
Table of Contents

**bacula-sd.conf**: storage daemon configuration ........................................... 327
  The Director resource ................................................................. 327
  The Storage resource ................................................................. 327
  Device resources ............................................................................. 327
  Autochanger resources ...................................................................... 328
**bconsole.conf**: console configuration ......................................................... 328
  Installing and configuring the client file daemon .................................. 328
  Starting the Bacula daemons .............................................................. 329
  Adding media to pools ....................................................................... 329
  Running a manual backup .................................................................... 330
  Running a restore job ........................................................................ 330
  Backing up Windows clients .............................................................. 333
  Monitoring Bacula configurations ...................................................... 334
  Bacula tips and tricks ......................................................................... 334
  Alternatives to Bacula ....................................................................... 335
  Commercial backup products .............................................................. 335
    ADSM/TSM ...................................................................................... 336
    Veritas NetBackup ........................................................................... 336
    EMC NetWorker ............................................................................. 337
    Other alternatives ............................................................................ 337
  Recommended reading .......................................................................... 337
  Exercises ............................................................................................ 337

**CHAPTER 11** **SYSLOG AND LOG FILES** .............................................................. 340
  Finding log files ................................................................................... 341
    Files not to manage ........................................................................... 342
    Vendor specifics ................................................................................ 344
  Syslog: the system event logger ............................................................ 344
    Syslog architecture .......................................................................... 345
    Configuring **syslogd** ...................................................................... 345
    Config file examples ......................................................................... 349
      Stand-alone machine ...................................................................... 349
      Network logging client .................................................................. 349
      Central logging host ...................................................................... 350
    Syslog debugging .............................................................................. 351
    Alternatives to syslog ....................................................................... 351
    Linux kernel and boot-time logging ................................................. 352
    AIX logging and error handling ....................................................... 353
    Syslog configuration under AIX ....................................................... 355
  **logrotate**: manage log files .............................................................. 356
    Condensing log files to useful information ....................................... 358
    Logging policies .............................................................................. 359
  Exercises ............................................................................................ 361
CHAPTER 12  SOFTWARE INSTALLATION AND MANAGEMENT  362

Installing Linux and OpenSolaris ........................................ 363
Netbooting PCs ................................................................ 363
Setting up PXE for Linux .................................................. 364
Netbooting non-PCs .......................................................... 364
Using Kickstart: the automated installer for Red Hat Enterprise Linux ... 365
   Setting up a Kickstart configuration file ......................... 365
   Building a Kickstart server .......................................... 366
   Pointing Kickstart at your config file ............................ 367
Using AutoYaST: SUSE’s automated installation tool .................. 367
Automating installation with the Ubuntu installer ................... 368
Installing Solaris ................................................................ 370
Network installations with JumpStart .................................. 371
Network installations with the Automated Installer ............... 375
Installing HP-UX .............................................................. 377
Automating Ignite-UX installations .................................... 379
Installing AIX with the Network Installation Manager ........... 380
Managing packages ......................................................... 381
Managing Linux packages ................................................ 382
   rpm: manage RPM packages ....................................... 382
   dpkg: manage .deb packages in Ubuntu ......................... 383
Using high-level Linux package management systems ............ 384
   Package repositories .................................................. 385
   RHN: the Red Hat Network ....................................... 387
   APT: the Advanced Package Tool ................................. 387
   apt-get configuration ............................................... 388
   An example /etc/apt/sources.list file .......................... 389
   Creation of a local repository mirror ............................ 390
   apt-get automation .................................................... 391
   yum: release management for RPM ............................... 391
   Zypper package management for SUSE: now with more ZYpp! .. 392
Managing packages for UNIX ............................................. 393
   Solaris packaging ....................................................... 394
   HP-UX packaging ..................................................... 394
   Software management in AIX ...................................... 396
Revision control .............................................................. 397
   Backup file creation .................................................. 397
   Formal revision control systems .................................. 398
   Subversion .............................................................. 399
   Git ................................................................ 401
Software localization and configuration ............................... 404
   Organizing your localization ....................................... 405
   Testing ................................................................. 406
   Compiling locally ..................................................... 407
   Distributing localizations .......................................... 408
Table of Contents

Using configuration management tools ........................................... 408
  cfengine: computer immune system ........................................... 408
  LCFG: a large-scale configuration system ................................. 409
  Template Tree 2: cfengine helper ............................................ 410
  DMTF/CIM: the Common Information Model ................................ 410
Sharing software over NFS ..................................................... 411
  Package namespaces ......................................................... 411
  Dependency management ..................................................... 412
  Wrapper scripts ............................................................... 413
Recommended reading ......................................................... 413
Exercises ............................................................................ 414

CHAPTER 13 DRIVERS AND THE KERNEL 415

Kernel adaptation ..................................................................... 416
Drivers and device files .......................................................... 417
  Device files and device numbers ............................................. 418
  Device file creation ............................................................. 419
  Naming conventions for devices ............................................. 420
  Custom kernels versus loadable modules ................................. 420
Linux kernel configuration ...................................................... 421
  Tuning Linux kernel parameters ........................................... 421
  Building a Linux kernel ....................................................... 423
  If it ain’t broke, don’t fix it .................................................. 423
  Configuring kernel options .................................................. 423
  Building the kernel binary .................................................... 425
  Adding a Linux device driver ............................................... 425
Solaris kernel configuration ..................................................... 427
  The Solaris kernel area ......................................................... 427
  Configuring the kernel with /etc/system ................................ 428
  Adding a Solaris device driver .............................................. 430
  Debugging a Solaris configuration ........................................ 430
HP-UX kernel configuration .................................................... 431
Management of the AIX kernel ................................................ 432
  The Object Data Manager .................................................... 432
  Kernel tuning ................................................................... 434
Loadable kernel modules ......................................................... 434
  Loadable kernel modules in Linux ......................................... 435
  Loadable kernel modules in Solaris ....................................... 436
Linux udev for fun and profit ................................................... 437
  Linux sysfs: a window into the souls of devices ...................... 438
  Exploring devices with udevadm .......................................... 439
  Constructing rules and persistent names ............................... 439
Recommended reading ......................................................... 443
Exercises ............................................................................ 444
SECTION TWO: NETWORKING

CHAPTER 14 TCP/IP NETWORKING 447

TCP/IP and its relationship to the Internet ........................................... 447
Who runs the Internet? ........................................................................ 448
Network standards and documentation ................................................. 449
Networking road map .......................................................................... 450
IPv4 and IPv6 ....................................................................................... 451
Packets and encapsulation. ................................................................. 452
Ethernet framing. ................................................................................. 453
Maximum transfer unit ........................................................................ 453
Packet addressing ................................................................................ 454
Hardware (MAC) addressing ............................................................... 454
IP addressing ......................................................................................... 455
Hostname “addressing” ........................................................................ 456
Ports ....................................................................................................... 456
Address types. ......................................................................................... 456
IP addresses: the gory details ............................................................. 457
IPv4 address classes ............................................................................ 457
Subnetting ............................................................................................. 458
Tricks and tools for subnet arithmetic .................................................. 459
CIDR: Classless Inter-Domain Routing ................................................. 460
Address allocation ................................................................................ 461
Private addresses and network address translation (NAT) ................. 462
IPv6 addressing ..................................................................................... 464
Routing .................................................................................................... 465
Routing tables ....................................................................................... 466
ICMP redirects .................................................................................... 467
ARP: the Address Resolution Protocol ................................................. 468
DHCP: the Dynamic Host Configuration Protocol ............................... 469
DHCP software ..................................................................................... 470
How DHCP works ................................................................................ 470
ISC’s DHCP software .......................................................................... 471
Security issues ....................................................................................... 472
IP forwarding ......................................................................................... 472
ICMP redirects ..................................................................................... 473
Source routing ....................................................................................... 473
Broadcast pings and other directed broadcasts .................................... 473
IP spoofing, ............................................................................................ 473
Host-based firewalls ............................................................................. 474
Virtual private networks ....................................................................... 475
PPP: the Point-to-Point Protocol ......................................................... 476
# Table of Contents

Basic network configuration .................................................. 476
  Hostname and IP address assignment ..................................... 477
  `ifconfig`: configure network interfaces ............................... 478
  Network hardware options .................................................. 481
  `route`: configure static routes ......................................... 481
  DNS configuration .......................................................... 483
System-specific network configuration .................................... 484
  Linux networking .................................................................. 484
    NetworkManager ............................................................ 485
    Ubuntu network configuration .......................................... 486
    SUSE network configuration ............................................. 486
    Red Hat network configuration ...................................... 487
    Linux network hardware options .................................... 489
    Linux TCP/IP options ................................................... 490
    Security-related kernel variables .................................... 492
    Linux NAT and packet filtering ....................................... 493
  Solaris networking .......................................................... 494
    Solaris basic network configuration .................................. 494
    Solaris configuration examples ....................................... 496
    Solaris DHCP configuration ............................................ 497
    `ndd`: TCP/IP and interface tuning for Solaris ..................... 498
    Solaris security .......................................................... 499
    Solaris firewalls and filtering ....................................... 499
    Solaris NAT ............................................................... 500
    Solaris networking quirks .............................................. 501
  HP-UX networking .......................................................... 501
    Basic network configuration for HP-UX .............................. 501
    HP-UX configuration examples ......................................... 502
    HP-UX DHCP configuration ............................................ 504
    HP-UX dynamic reconfiguration and tuning .......................... 504
    HP-UX security, firewalls, filtering, and NAT ...................... 505
  AIX networking ................................................................ 506
    `no`: manage AIX network tuning parameters ....................... 507
Recommended reading .......................................................... 508
Exercises ............................................................................ 509

## Chapter 15 Routing

511

Packet forwarding: a closer look ............................................. 512
Routing daemons and routing protocols .................................. 515
  Distance-vector protocols .................................................. 515
  Link-state protocols ......................................................... 516
  Cost metrics ..................................................................... 517
  Interior and exterior protocols .......................................... 517
Protocols on parade .......................................................... 518
   RIP and RIPng: Routing Information Protocol .................. 518
   OSPF: Open Shortest Path First ................................ 519
   EIGRP: Enhanced Interior Gateway Routing Protocol ........ 519
   IS-IS: the ISO “standard” ........................................... 520
   Router Discovery Protocol and Neighbor Discovery Protocol 520
   BGP: the Border Gateway Protocol ............................... 520
Routing strategy selection criteria .................................... 521
Routing daemons ............................................................ 522
   routed: obsolete RIP implementation ............................ 522
   gated: first-generation multiprotocol routing daemon ....... 523
   Quagga: mainstream routing daemon ............................. 523
   ramd: multiprotocol routing system for HP-UX ............... 524
   XORP: router in a box ............................................. 524
   Vendor specifics .................................................... 525
Cisco routers .................................................................. 525
Recommended reading ..................................................... 528
Exercises ..................................................................... 530

CHAPTER 16 NETWORK HARDWARE 531

   Ethernet: the Swiss Army knife of networking ................ 532
   How Ethernet works .................................................... 532
   Ethernet topology ...................................................... 533
   Unshielded twisted pair cabling .................................. 534
   Optical fiber ............................................................... 536
   Connecting and expanding Ethernets ............................. 537
      Hubs ................................................................. 537
      Switches .............................................................. 538
      VLAN-capable switches .......................................... 539
      Routers ............................................................... 539
      Autonegotiation ..................................................... 539
      Power over Ethernet .............................................. 540
      Jumbo frames ....................................................... 541
   Wireless: ethernet for nomads ..................................... 541
      Wireless security .................................................. 543
      Wireless switches and lightweight access points ......... 543
   DSL and cable modems: the last mile ............................ 543
   Network testing and debugging .................................... 544
   Building wiring .......................................................... 545
      UTP cabling options .............................................. 545
      Connections to offices .......................................... 546
      Wiring standards ................................................ 546
**Table of Contents**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network design issues</td>
<td>547</td>
</tr>
<tr>
<td>Network architecture vs. building architecture</td>
<td>547</td>
</tr>
<tr>
<td>Expansion</td>
<td>548</td>
</tr>
<tr>
<td>Congestion</td>
<td>548</td>
</tr>
<tr>
<td>Maintenance and documentation</td>
<td>549</td>
</tr>
<tr>
<td>Management issues</td>
<td>549</td>
</tr>
<tr>
<td>Recommended vendors</td>
<td>550</td>
</tr>
<tr>
<td>Cables and connectors</td>
<td>550</td>
</tr>
<tr>
<td>Test equipment</td>
<td>550</td>
</tr>
<tr>
<td>Routers/switches</td>
<td>550</td>
</tr>
<tr>
<td>Recommended reading</td>
<td>550</td>
</tr>
<tr>
<td>Exercises</td>
<td>551</td>
</tr>
</tbody>
</table>

**CHAPTER 17  DNS: THE DOMAIN NAME SYSTEM  552**

Who needs DNS? .................................................. 554
Managing your DNS ............................................. 554
How DNS works ................................................... 555
Resource records ............................................... 555
Delegation ....................................................... 555
Caching and efficiency ....................................... 556
Multiple answers ............................................... 557
DNS for the impatient ......................................... 558
Adding a new machine to DNS ................................ 558
Configuring a DNS client ..................................... 561
Name servers .................................................... 563
Authoritative and caching-only servers .................. 563
Recursive and nonrecursive servers ....................... 565
The DNS namespace ............................................. 566
Registering a second-level domain name ................... 567
Creating your own subdomains ................................ 567
Designing your DNS environment ............................. 568
Namespace management ......................................... 568
Authoritative servers ......................................... 569
Caching servers ................................................ 569
Hardware requirements ........................................ 570
Security ........................................................ 571
Summing up ....................................................... 571
What’s new in DNS ............................................... 572
The DNS database ............................................... 574
Commands in zone files ....................................... 574
Resource records ............................................... 576
The SOA record .................................................. 579
NS records ....................................................... 581
A records ......................................................... 582
UNIX and Linux System Administration Handbook

PTR records ......................................................... 582
MX records ......................................................... 583
CNAME records ..................................................... 585
The CNAME hack .................................................. 585
SRV records ......................................................... 587
TXT records ........................................................ 588
IPv6 resource records ............................................. 589
   IPv6 forward records – AAAA .................................. 589
   IPv6 reverse records – PTR .................................... 589
SPF records ........................................................ 590
DKIM and ADSP records ......................................... 591
SSHFP resource records ......................................... 594
DNSSEC resource records ........................................ 595
Glue records: links between zones ............................... 596
The BIND software .................................................. 597
Version determination .............................................. 598
Components of BIND .............................................. 600
Configuration files .................................................. 600
The include statement ............................................ 602
The options statement ............................................ 602
The acl statement .................................................. 609
The (TSIG) key statement ....................................... 609
The trusted-keys statement ..................................... 610
The server statement .............................................. 610
The masters statement ............................................ 611
The logging statement ............................................ 612
The statistics-channels statement .............................. 612
The zone statement ................................................ 612
   Configuring the master server for a zone ................... 613
   Configuring a slave server for a zone ....................... 614
   Setting up the root server hints ............................ 614
   Setting up a forwarding zone ................................ 615
The controls statement for rndc ................................ 615
Split DNS and the view statement .............................. 617
BIND configuration examples ..................................... 618
The localhost zone ............................................... 619
A small security company ........................................ 620
The Internet Systems Consortium, isc.org ...................... 623
The NSD/Unbound software ....................................... 625
Installing and configuring NSD .................................... 625
   Fundamental differences from BIND ......................... 626
   NSD configuration example .................................. 627
   NSD key definitions ........................................... 628
   NSD global configuration options ......................... 629
   NSD zone-specific configuration options .................. 631
# Table of Contents

- **Running nsd** ................................................................. 632
- **Installing and configuring Unbound** ..................................... 632
- **Updating zone files** .......................................................... 638
- **Zone transfers** ............................................................... 639
- **BIND dynamic updates** ........................................................ 640
- **Security issues** ............................................................... 642
- **Access control lists in BIND, revisited** .................................... 643
- **Open resolvers** ............................................................... 644
- **Running in a chrooted jail** .................................................. 645
- **Secure server-to-server communication with TSIG and TKEY** ............... 645
- **Setting up TSIG for BIND** ................................................... 646
- **TSIG in NSD** ................................................................. 648
- **DNSSEC** ................................................................. 648
- **DNSSEC policy** .............................................................. 652
- **DNSSEC resource records** .................................................. 653
- **Turning on DNSSEC** .......................................................... 654
- **Key pair generation** .......................................................... 655
- **Zone signing** ................................................................. 657
- **The DNSSEC chain of trust** ................................................... 660
- **DLV: domain lookaside validation** ....................................... 661
- **DNSSEC key rollover** ........................................................ 662
- **DNSSEC tools** ............................................................... 663
  - ldns tools, nlnetlabs.nl/projects/ldns ........................................ 664
  - Sparta tools, dnssec-tools.org ............................................. 664
  - RIPE tools, ripe.net ........................................................... 665
  - Vantages tools, vantage-points.org ........................................ 665
- **Debugging DNSSEC** .......................................................... 665
- **Microsoft and DNS** .......................................................... 667
- **Testing and debugging** ..................................................... 667
- **Logging in BIND** ............................................................. 667
  - Channels ........................................................................... 668
  - Categories .......................................................................... 669
  - Log Messages ..................................................................... 669
  - Sample BIND logging configuration ....................................... 671
  - Debug levels in BIND .......................................................... 672
- **Logging in NSD/Unbound** .................................................... 673
- **Name server control programs** ............................................... 674
  - Using BIND’s rndc ............................................................. 674
  - Using NSD’s nsdc ............................................................... 675
  - Using unbound-control .......................................................... 675
- **Name server statistics** .......................................................... 676
- **Debugging with dig** ............................................................ 677
- **Lame delegations** .............................................................. 678
- **DNS sanity checking tools** ................................................... 679
- **Performance issues** ............................................................ 680
Vendor specifics ................................................................. 681
  Specifics for Linux .......................................................... 681
  Specifics for Solaris .......................................................... 684
  Specifics for HP-UX ........................................................... 684
  Specifics for AIX .............................................................. 685
Recommended reading .......................................................... 686
  Mailing lists and newsgroups ................................................ 686
  Books and other documentation .......................................... 687
  On-line resources .......................................................... 688
  The RFCs ................................................................. 688
Exercises ................................................................. 688

CHAPTER 18  THE NETWORK FILE SYSTEM 690
Introduction to network file services .............................................. 690
  Issues of state ............................................................... 691
  Performance concerns ..................................................... 691
  Security ................................................................. 691
The NFS approach .............................................................. 692
  Protocol versions and history ............................................. 692
  Transport protocols ........................................................ 693
  State ..................................................................... 693
  File system exports ........................................................ 693
  File locking ................................................................. 694
  Security concerns .......................................................... 695
  Identity mapping in version 4 ............................................ 696
  Root access and the nobody account .................................... 697
  Performance considerations in version 4 .............................. 698
  Disk quotas ................................................................. 698
Server-side NFS ................................................................. 698
  The share command and dfstab file (Solaris, HP-UX) ............... 700
  The exportfs command and the exports file (Linux, AIX) .......... 702
  Exports in AIX ............................................................. 702
  Exports in Linux .......................................................... 703
  nbsd: serve files .......................................................... 705
Client-side NFS ................................................................. 706
  Mounting remote filesystems at boot time ......................... 708
  Restricting exports to privileged ports ............................... 709
  Identity mapping for NFS version 4 ..................................... 709
  nfsstat: dump NFS statistics ............................................ 710
  Dedicated NFS file servers .............................................. 711
  Automatic mounting ....................................................... 711
  Indirect maps ............................................................. 713
  Direct maps ............................................................... 713
  Master maps .............................................................. 714
**Table of Contents**

Executable maps .................................................. 714
Automount visibility ............................................. 715
Replicated filesystems and automount ........................... 715
Automatic automounts (V3; all but Linux) ................. 716
Speciﬁcs for Linux .................................................. 717
Recommended reading ............................................... 717
Exercises .............................................................. 718

**CHAPTER 19 SHARING SYSTEM FILES** 719

What to share ...................................................... 720
Copying ﬁles around ............................................... 721
The NFS option ....................................................... 721
Push systems vs. pull systems ................................... 722
rdist: push ﬁles ....................................................... 722
rsync: transfer ﬁles more securely ............................ 725
Pulling ﬁles .......................................................... 727
The structure of LDAP data ....................................... 728
The point of LDAP .................................................. 730
LDAP documentation and speciﬁcations ....................... 731
OpenLDAP: the traditional open source LDAP server ...... 731
389 Directory Server: alternative open source LDAP server 732
LDAP instead of /etc/passwd and /etc/group ............... 733
LDAP querying ....................................................... 734
LDAP and security .................................................. 735
NIS: the Network Information Service ......................... 736
The NIS model ....................................................... 736
Understanding how NIS works ................................... 736
NIS security .......................................................... 738
Prioritizing sources of administrative information ........ 739
nscd: cache the results of lookups ............................. 740
Recommended reading .............................................. 741
Exercises .............................................................. 741

**CHAPTER 20 ELECTRONIC MAIL** 742

Mail systems ........................................................ 744
User agents .......................................................... 744
Submission agents .................................................. 745
Transport agents ..................................................... 746
Local delivery agents .............................................. 746
Message stores ....................................................... 746
Access agents ......................................................... 747
So many pieces, so little time ................................. 747
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The anatomy of a mail message</td>
<td>748</td>
</tr>
<tr>
<td>Reading mail headers</td>
<td>748</td>
</tr>
<tr>
<td>The SMTP protocol</td>
<td>750</td>
</tr>
<tr>
<td>You had me at EHLO</td>
<td>751</td>
</tr>
<tr>
<td>SMTP error codes</td>
<td>751</td>
</tr>
<tr>
<td>SMTP authentication</td>
<td>752</td>
</tr>
<tr>
<td>Mail system design</td>
<td>753</td>
</tr>
<tr>
<td>Using mail servers</td>
<td>754</td>
</tr>
<tr>
<td>Mail aliases</td>
<td>756</td>
</tr>
<tr>
<td>Getting aliases from files</td>
<td>758</td>
</tr>
<tr>
<td>Mailing to files</td>
<td>759</td>
</tr>
<tr>
<td>Mailing to programs</td>
<td>759</td>
</tr>
<tr>
<td>Aliasing by example</td>
<td>760</td>
</tr>
<tr>
<td>Building the hashed alias database</td>
<td>760</td>
</tr>
<tr>
<td>Using mailing lists and list wrangling software</td>
<td>760</td>
</tr>
<tr>
<td>Software packages for maintaining mailing lists</td>
<td>761</td>
</tr>
<tr>
<td>Content scanning: spam and malware</td>
<td>761</td>
</tr>
<tr>
<td>Spam</td>
<td>762</td>
</tr>
<tr>
<td>Forgeries</td>
<td>763</td>
</tr>
<tr>
<td>Message privacy</td>
<td>763</td>
</tr>
<tr>
<td>Spam filtering</td>
<td>764</td>
</tr>
<tr>
<td>When to filter</td>
<td>764</td>
</tr>
<tr>
<td>Greylisting/DCC</td>
<td>765</td>
</tr>
<tr>
<td>SpamAssassin</td>
<td>765</td>
</tr>
<tr>
<td>Blacklists</td>
<td>766</td>
</tr>
<tr>
<td>Whitelists</td>
<td>766</td>
</tr>
<tr>
<td>Miltering: mail filtering</td>
<td>767</td>
</tr>
<tr>
<td>SPF and Sender ID</td>
<td>767</td>
</tr>
<tr>
<td>DomainKeys, DKIM, and ADSP</td>
<td>768</td>
</tr>
<tr>
<td>MTA-specific antispam features</td>
<td>768</td>
</tr>
<tr>
<td>MailScanner</td>
<td>769</td>
</tr>
<tr>
<td><strong>amavisd-new</strong></td>
<td>769</td>
</tr>
<tr>
<td>How amavisd works</td>
<td>770</td>
</tr>
<tr>
<td>amavisd installation</td>
<td>771</td>
</tr>
<tr>
<td>Basic amavisd configuration</td>
<td>771</td>
</tr>
<tr>
<td>amavisd-new tools</td>
<td>772</td>
</tr>
<tr>
<td>Tests of your MTA’s scanning effectiveness</td>
<td>773</td>
</tr>
<tr>
<td>Email configuration</td>
<td>774</td>
</tr>
<tr>
<td><strong>sendmail</strong></td>
<td>775</td>
</tr>
<tr>
<td>The switch file</td>
<td>776</td>
</tr>
<tr>
<td>Starting sendmail</td>
<td>776</td>
</tr>
<tr>
<td>Mail queues</td>
<td>778</td>
</tr>
</tbody>
</table>
sendmail configuration ................................................................. 778
  The m4 preprocessor .................................................................. 779
  The sendmail configuration pieces ............................................. 779
  A configuration file built from a sample .mc file ......................... 781
sendmail configuration primitives .................................................. 782
Tables and databases ................................................................. 782
Generic macros and features ....................................................... 783
  OSTYPE macro ......................................................................... 783
  DOMAIN macro ....................................................................... 784
  MAILER macro ....................................................................... 784
  FEATURE macro ..................................................................... 784
  use_cw_file feature .................................................................. 784
  redirect feature ...................................................................... 785
  always_add_domain feature ..................................................... 785
  access_db feature .................................................................... 785
  virtusertable feature ............................................................... 786
  ldap_routing feature ................................................................ 786
  Masquerading features ............................................................. 787
  MAIL_HUB and SMART_HOST macros ...................................... 787
Client configuration ...................................................................... 788
Configuration options ................................................................. 789
Spam-related features in sendmail .................................................. 789
  Relay control ......................................................................... 791
  User or site blacklisting ........................................................... 792
  Throttles, rates, and connection limits ........................................ 792
Milter configuration in sendmail ..................................................... 794
amavisd and sendmail connection .................................................. 794
Security and sendmail ................................................................. 795
  Ownerships ............................................................................. 796
  Permissions ............................................................................ 797
  Safer mail to files and programs ............................................... 798
  Privacy options ....................................................................... 799
  Running a chrooted sendmail (for the truly paranoid) ................. 800
Denial of service attacks ............................................................... 800
SASL: the Simple Authentication and Security Layer ..................... 801
TLS: Transport Layer Security ..................................................... 801
sendmail performance ................................................................. 802
  Delivery modes ....................................................................... 802
  Queue groups and envelope splitting ....................................... 802
  Queue runners ...................................................................... 802
  Load average controls ............................................................ 803
  Undeliverable messages in the queue ....................................... 803
  Kernel tuning ........................................................................ 804
sendmail testing and debugging ......................................................... 805
  Queue monitoring ...................................................................... 806
  Logging .................................................................................... 806
Exim ............................................................................................... 807
  Exim installation ........................................................................ 808
  Exim startup .............................................................................. 810
  Exim utilities ............................................................................. 811
  Exim configuration language ...................................................... 811
  Exim configuration file ............................................................... 812
  Global options ........................................................................... 813
    Options .................................................................................... 813
    Lists ...................................................................................... 814
    Macros ................................................................................... 814
  ACLs (access control lists) ............................................................ 815
  Content scanning at ACL time ...................................................... 818
    Scanning for viruses ................................................................ 818
    Scanning for spam .................................................................. 819
  Authenticators ........................................................................... 820
  Routers ....................................................................................... 821
    The accept router .................................................................... 821
    The dnslookup router ............................................................... 822
    The manualroute router .......................................................... 822
    The redirect router .................................................................. 823
    Per-user filtering via .forward files ........................................... 823
  Transports ................................................................................... 824
    The appendfile transport .......................................................... 824
    The smtp transport .................................................................. 824
  Retry configuration .................................................................... 825
  Rewriting configuration ............................................................... 825
  Local scan function ................................................................... 825
  amavisd and Exim connection ....................................................... 826
  Logging ....................................................................................... 826
  Debugging ................................................................................... 827
Postfix ............................................................................................ 828
  Postfix architecture .................................................................... 828
  Receiving mail ........................................................................... 829
  Managing mail-waiting queues .................................................... 829
  Sending mail .............................................................................. 830
  Security ....................................................................................... 830
  Postfix commands and documentation ........................................ 830
  Postfix configuration ................................................................. 831
    What to put in main.cf .............................................................. 831
    Basic settings .......................................................................... 831
    Use of postconf ....................................................................... 832
Table of Contents

Lookup tables .................................................. 833
Local delivery .................................................. 834
Virtual domains ................................................. 835
Virtual alias domains ......................................... 835
Virtual mailbox domains ....................................... 836
Access control .................................................. 837
Access tables ................................................... 838
Authentication of clients and encryption .................... 839
Fighting spam and viruses ..................................... 840
Blacklists ......................................................... 840
Spam-fighting example ......................................... 841
SpamAssassin and procmail .................................... 841
Policy daemons .................................................. 841
Content filtering ............................................... 842
Content filtering with amavisd ................................. 842
Debugging ......................................................... 844
Looking at the queue ........................................... 844
Soft-bouncing .................................................... 845
Testing access control ......................................... 845
DKIM Configuration ............................................. 845
DKIM: DomainKeys Identified Mail ............................. 846
DKIM miltering ................................................... 846
DKIM configuration in amavisd-new ........................... 849
DKIM in sendmail ............................................... 850
DKIM in Exim ..................................................... 850
Signing outgoing messages ..................................... 850
Verifying incoming signed messages .......................... 851
A complete example ............................................. 851
DKIM in Postfix .................................................. 852
Integrated email solutions ..................................... 853
Recommended reading .......................................... 854
General spam references ....................................... 854
sendmail references ............................................ 854
Exim references .................................................. 855
Postfix references .............................................. 855
RFCs ............................................................... 855
Exercises .......................................................... 855
sendmail-specific exercises .................................... 857
Exim-specific exercises ......................................... 858
Postfix-specific exercises ....................................... 858

CHAPTER 21 NETWORK MANAGEMENT AND DEBUGGING 859
Network troubleshooting ....................................... 860
ping: check to see if a host is alive ........................... 861
SmokePing: gather ping statistics over time .......................... 864
traceroute: trace IP packets ................................................ 865
netstat: get network statistics ............................................. 868
   Inspecting interface configuration information .................... 868
   Monitoring the status of network connections ..................... 870
   Identifying listening network services .............................. 871
   Examining the routing table .......................................... 871
   Viewing operational statistics for network protocols ............ 872
Inspection of live interface activity .................................. 873
Packet sniffer .......................................................... 874
   tcpdump: industry-standard packet sniffer ......................... 875
   Wireshark and TShark: tcpdump on steroids ....................... 877
The ICSI Netalyzr ...................................................... 878
Network management protocols ......................................... 879
SNMP: the Simple Network Management Protocol .................... 880
   SNMP organization .................................................. 881
   SNMP protocol operations ......................................... 882
   RMON: remote monitoring MIB .................................... 883
The NET-SNMP agent ..................................................... 883
Network management applications ...................................... 884
   The NET-SNMP tools ................................................ 885
   SNMP data collection and graphing ................................. 886
   Nagios: event-based service monitoring ............................ 887
   The ultimate network monitoring package: still searching .... 888
   Commercial management platforms ................................. 889
NetFlow: connection-oriented monitoring ............................. 890
   Monitoring NetFlow data with nfldump and NfSen ............... 890
   Setting up NetFlow on a Cisco router ............................. 892
Recommended reading ................................................... 893
Exercises ............................................................ 894

CHAPTER 22 SECURITY 896

Is UNIX secure? .......................................................... 897
How security is compromised .......................................... 898
   Social engineering .................................................... 898
   Software vulnerabilities ............................................. 899
   Configuration errors ................................................ 900
Security tips and philosophy ........................................... 901
   Patches ............................................................... 901
   Unnecessary services ............................................... 902
   Remote event logging .............................................. 902
   Backups ............................................................... 903
   Viruses and worms .................................................. 903
   Trojan horses ......................................................... 903
# Table of Contents

Rootkits ................................................................. 904
Packet filtering ......................................................... 904
Passwords ................................................................. 905
Vigilance ................................................................. 905
General philosophy ..................................................... 905
Passwords and user accounts ........................................ 906
Password aging ......................................................... 906
Group logins and shared logins ..................................... 907
User shells ............................................................... 907
Rootly entries ........................................................... 907
PAM: cooking spray or authentication wonder? ................. 908
System support for PAM ............................................... 908
PAM configuration ...................................................... 908
A detailed Linux configuration example ......................... 911
Setuid programs ........................................................ 912
Effective use of \texttt{chroot} .......................................... 913
Security power tools .................................................. 914
Nmap: network port scanner ......................................... 914
Nessus: next-generation network scanner ......................... 916
John the Ripper: finder of insecure passwords ................... 916
\texttt{hosts\_access}: host access control ......................... 917
Bro: the programmable network intrusion detection system ... 918
Snort: the popular network intrusion detection system ......... 918
OSSEC: host-based intrusion detection ............................ 919
\hspace{1em} OSSEC basic concepts ................................ 920
\hspace{1em} OSSEC installation ........................................ 920
\hspace{1em} OSSEC configuration ..................................... 921
Mandatory Access Control (MAC) .................................. 922
Security-enhanced Linux (SELinux) ............................... 923
Cryptographic security tools ......................................... 924
Kerberos: a unified approach to network security ............... 924
PGP: Pretty Good Privacy ............................................ 925
SSH: the secure shell .................................................. 926
Stunnel ................................................................. 930
Firewalls ................................................................. 932
Packet-filtering firewalls ............................................. 932
How services are filtered .......................................... 933
Stateful inspection firewalls ....................................... 934
Firewalls: how safe are they? ...................................... 935
Linux firewall features ............................................... 935
Rules, chains, and tables .......................................... 935
Rule targets ............................................................. 936
\texttt{iptables} firewall setup ....................................... 937
A complete example .................................................. 937
IPFilter for UNIX systems ........................................... 939
Virtual private networks (VPNs) .......................................................... 942
IPsec tunnels .................................................. 943
All I need is a VPN, right? .................................................. 943
Certifications and standards .................................................. 944
Certifications .................................................. 945
Security standards .................................................. 945
ISO 27002 .................................................. 946
PCI DSS .................................................. 946
NIST 800 series .................................................. 947
Common Criteria .................................................. 947
OWASP .................................................. 947
Sources of security information .................................................. 947
CERT: a registered service mark of Carnegie Mellon University .... 948
SecurityFocus.com and the BugTraq mailing list .......................... 948
Schneier on Security .................................................. 948
SANS: the System Administration, Networking, and Security Institute . 948
Vendor-specific security resources .................................................. 949
Other mailing lists and web sites .................................................. 950
What to do when your site has been attacked .................................. 950
Recommended reading .................................................. 952
Exercises .................................................. 954

**CHAPTER 23  WEB HOSTING**  .................................................. 956
Web hosting basics .................................................. 957
Resource locations on the web .................................................. 957
Uniform resource locators .................................................. 957
How HTTP works .................................................. 958
Content generation on the fly .................................................. 959
Embedded interpreters .................................................. 959
FastCGI .................................................. 959
Script security .................................................. 960
Application servers .................................................. 960
Load balancing .................................................. 961
HTTP server installation .................................................. 963
Choosing a server .................................................. 963
Installing Apache .................................................. 964
Configuring Apache .................................................. 965
Running Apache .................................................. 966
Analyzing log files .................................................. 966
Optimizing for high-performance hosting of static content .............. 967
Virtual interfaces .................................................. 967
Using name-based virtual hosts .................................................. 968
Table of Contents

Configuring virtual interfaces ........................................... 968
   Linux virtual interfaces ............................................. 968
   Solaris virtual interfaces .......................................... 969
   HP-UX virtual interfaces .......................................... 970
   AIX virtual interfaces ............................................. 970
   Telling Apache about virtual interfaces ......................... 971
The Secure Sockets Layer (SSL) ........................................ 971
   Generating a Certificate Signing Request ......................... 972
   Configuring Apache to use SSL .................................... 973
Caching and proxy servers ............................................. 974
   Using the Squid cache and proxy server ......................... 975
   Setting up Squid .................................................... 975
   Reverse-proxying with Apache .................................... 976
Scaling beyond your limits ............................................. 977
   Cloud computing .................................................... 978
   Co-lo hosting ....................................................... 978
   Content distribution networks .................................... 978
Exercises .......................................................................... 979

SECTION THREE: BUNCH O' STUFF

CHAPTER 24  VIRTUALIZATION 983

Virtual vernacular .......................................................... 984
   Full virtualization ..................................................... 985
   Paravirtualization ..................................................... 986
   Operating system virtualization .................................... 986
   Native virtualization .................................................. 987
   Cloud computing ....................................................... 987
   Live migration ........................................................... 988
   Comparison of virtualization technologies ....................... 988
Benefits of virtualization ................................................. 988
A practical approach ........................................................ 989
Virtualization with Linux ................................................ 991
   Introduction to Xen ...................................................... 991
   Xen essentials ............................................................ 992
   Xen guest installation with virt-install ......................... 993
   Xen live migration ..................................................... 994
KVM ............................................................................. 995
   KVM installation and usage .......................................... 996
Solaris zones and containers ............................................ 997
   AIX workload partitions ............................................. 1001
Integrity Virtual Machines in HP-UX .................................................. 1003
Creating and installing virtual machines .................................. 1003
VMware: an operating system in its own right .......................... 1005
Amazon Web Services ............................................................... 1005
Recommended reading ............................................................. 1010
Exercises ................................................................................. 1010

CHAPTER 25 THE X WINDOW SYSTEM ........................................ 1011
The display manager ............................................................... 1013
Process for running an X application ....................................... 1014
The DISPLAY environment variable ....................................... 1015
Client authentication ............................................................... 1016
X connection forwarding with SSH ......................................... 1017
X server configuration ............................................................. 1019
Device sections ........................................................................ 1021
Monitor sections ....................................................................... 1021
Screen sections ......................................................................... 1022
InputDevice sections ............................................................... 1022
ServerLayout sections ............................................................. 1024
xrandr: not your father’s X server configurator ......................... 1025
Kernel mode setting ............................................................... 1025
X server troubleshooting and debugging ................................. 1026
Special keyboard combinations for X .................................... 1026
When X servers attack ............................................................ 1027
A brief note on desktop environments .................................... 1028
KDE ......................................................................................... 1029
GNOME ................................................................................... 1029
Which is better, GNOME or KDE? ......................................... 1030
Recommended reading ............................................................. 1030
Exercises ................................................................................. 1031

CHAPTER 26 PRINTING ................................................................. 1032
Printing-system architecture .................................................. 1033
Major printing systems .......................................................... 1033
Print spoolers .......................................................................... 1034
CUPS printing .......................................................................... 1034
Interfaces to the printing system .......................................... 1034
The print queue ........................................................................ 1035
Multiple printers and queues ................................................ 1036
Printer instances ...................................................................... 1036
Network printing ...................................................................... 1036
Filters ....................................................................................... 1037
CUPS server administration .................................................. 1038
Table of Contents

Network print server setup ........................................ 1039
Printer autoconfiguration ....................................... 1040
Network printer configuration ................................. 1040
Printer configuration examples ............................... 1041
Printer class setup ............................................... 1041
Service shutoff .................................................. 1041
Other configuration tasks ...................................... 1042
Printing from desktop environments .......................... 1043
   kprinter: print documents .................................. 1044
   Konqueror and printing ...................................... 1045
System V printing ................................................ 1045
   Overview ...................................................... 1045
   Destinations and classes ................................... 1046
   A brief description of lp .................................. 1047
   lpsched and lpshut: start and stop printing .......... 1047
   lpadmin: configure the printing environment ........... 1048
   lpadmin examples ........................................... 1050
   lpstat: get status information ............................ 1051
   cancel: remove print jobs .................................. 1051
   accept and reject: control spooling ...................... 1051
   enable and disable: control printing ..................... 1052
   lpmove: transfer jobs ....................................... 1052
   Interface programs .......................................... 1052
   What to do when the printing system is completely hosed ..... 1053
BSD and AIX printing .......................................... 1054
   An overview of the BSD printing architecture .......... 1054
   Printing environment control .............................. 1055
   lpd: spool print jobs ...................................... 1056
   lpr: submit print jobs ...................................... 1056
   lpq: view the printing queue ............................... 1056
   lprm: remove print jobs .................................... 1057
   lpc: make administrative changes ......................... 1057
   The /etc/printcap file ...................................... 1059
printcap variables .............................................. 1060
   sd: spool directory ....................................... 1061
   lf: error log file .......................................... 1061
   lp: device name ............................................ 1062
   rw: device open mode ..................................... 1062
   af: accounting file ....................................... 1062
   mx: file size limits ....................................... 1062
   rm and rp: remote access information ...................... 1062
   of, if: printing filters .................................... 1063
printcap variables for serial devices ....................... 1064
printcap extensions ........................................... 1064
What a long, strange trip it’s been ...................................................... 1065
  Printing history and the rise of print systems ................................. 1065
  Printer diversity ................................................................. 1066
Common printing software. .......................................................... 1067
  Printer diversity .................................................................... 1066
  Common printing software ....................................................... 1067
  Printer languages ................................................................... 1068
    PostScript ........................................................................ 1069
    PCL .............................................................................. 1069
    PDF ........................................................................... 1070
    XPS ........................................................................ 1070
    PJL............................................................................... 1070
  Printer drivers and their handling of PDLs ..................................... 1071
  PPD files ........................................................................... 1072
  Paper sizes ........................................................................... 1073
  Printer practicalities .................................................................. 1075
    Printer selection .................................................................. 1075
    GDI printers ...................................................................... 1076
    Double-sided printing ........................................................ 1076
    Other printer accessories .................................................... 1077
    Serial and parallel printers .................................................. 1077
    Network printers .................................................................. 1077
    Other printer advice ............................................................ 1077
      Use banner pages only if you have to .................................... 1078
      Fan your paper .................................................................. 1078
      Provide recycling bins ....................................................... 1078
      Use previewers .................................................................. 1078
      Buy cheap printers ........................................................... 1079
      Keep extra toner cartridges on hand ................................... 1079
      Pay attention to the cost per page ..................................... 1080
      Consider printer accounting ............................................. 1081
      Secure your printers ......................................................... 1081
    Troubleshooting tips ............................................................... 1081
      Restarting a print daemon .................................................. 1081
      Logging .......................................................................... 1082
      Problems with direct printing ............................................ 1082
      Network printing problems ............................................... 1082
      Distribution-specific problems ......................................... 1083
    Recommended reading ............................................................. 1083
    Exercises ........................................................................... 1084

CHAPTER 27 DATA CENTER BASICS .................................................. 1085
  Data center reliability tiers .......................................................... 1086
  Cooling .............................................................................. 1087
  Electronic gear ...................................................................... 1088
  Light fixtures ........................................................................ 1088
Table of Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators</td>
<td>1089</td>
</tr>
<tr>
<td>Total heat load</td>
<td>1089</td>
</tr>
<tr>
<td>Hot aisles and cold aisles</td>
<td>1089</td>
</tr>
<tr>
<td>Humidity</td>
<td>1091</td>
</tr>
<tr>
<td>Environmental monitoring</td>
<td>1091</td>
</tr>
<tr>
<td>Power</td>
<td>1091</td>
</tr>
<tr>
<td>Rack power requirements</td>
<td>1092</td>
</tr>
<tr>
<td>kVA vs. kW</td>
<td>1093</td>
</tr>
<tr>
<td>Remote control</td>
<td>1094</td>
</tr>
<tr>
<td>Racks</td>
<td>1094</td>
</tr>
<tr>
<td>Tools</td>
<td>1095</td>
</tr>
<tr>
<td>Recommended reading</td>
<td>1095</td>
</tr>
<tr>
<td>Exercises</td>
<td>1096</td>
</tr>
</tbody>
</table>

**CHAPTER 28** GREEN IT 1097

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green IT initiation</td>
<td>1098</td>
</tr>
<tr>
<td>The green IT eco-pyramid</td>
<td>1099</td>
</tr>
<tr>
<td>Green IT strategies: data center</td>
<td>1100</td>
</tr>
<tr>
<td>Application consolidation</td>
<td>1101</td>
</tr>
<tr>
<td>Server consolidation</td>
<td>1102</td>
</tr>
<tr>
<td>SAN storage</td>
<td>1103</td>
</tr>
<tr>
<td>Server virtualization</td>
<td>1103</td>
</tr>
<tr>
<td>Only-as-needed servers</td>
<td>1104</td>
</tr>
<tr>
<td>Granular utilization and capacity planning</td>
<td>1104</td>
</tr>
<tr>
<td>Energy-optimized server configuration</td>
<td>1104</td>
</tr>
<tr>
<td>Power-saving options for Linux</td>
<td>1104</td>
</tr>
<tr>
<td>Filesystem power savings</td>
<td>1105</td>
</tr>
<tr>
<td>Cloud computing</td>
<td>1106</td>
</tr>
<tr>
<td>Free cooling</td>
<td>1106</td>
</tr>
<tr>
<td>Efficient data center cooling</td>
<td>1106</td>
</tr>
<tr>
<td>Degraded mode for outages</td>
<td>1106</td>
</tr>
<tr>
<td>Equipment life extension</td>
<td>1107</td>
</tr>
<tr>
<td>Warmer temperature in the data center</td>
<td>1108</td>
</tr>
<tr>
<td>Low-power equipment</td>
<td>1108</td>
</tr>
<tr>
<td>Green IT strategies: user workspace</td>
<td>1108</td>
</tr>
<tr>
<td>Green IT friends</td>
<td>1110</td>
</tr>
<tr>
<td>Exercises</td>
<td>1111</td>
</tr>
</tbody>
</table>

**CHAPTER 29** PERFORMANCE ANALYSIS 1112

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What you can do to improve performance</td>
<td>1114</td>
</tr>
<tr>
<td>Factors that affect performance</td>
<td>1115</td>
</tr>
<tr>
<td>How to analyze performance problems</td>
<td>1117</td>
</tr>
</tbody>
</table>
System performance checkup .................................................. 1118
Taking stock of your hardware ................................................. 1118
Gathering performance data .................................................. 1121
Analyzing CPU usage .......................................................... 1121
How the system manages memory .......................................... 1124
Analyzing memory usage ...................................................... 1125
Analyzing disk I/O ............................................................... 1127
xdd: analyze disk subsystem performance ............................ 1129
sar: collect and report statistics over time ............................. 1129
nmon and nmon_analyser: monitor in AIX ............................... 1130
Choosing a Linux I/O scheduler ............................................. 1130
oprofile: profile Linux systems in detail ............................... 1131
Help! My system just got really slow! .................................... 1131
Recommended reading .......................................................... 1133
Exercises ............................................................................. 1134

CHAPTER 30 COOPERATING WITH WINDOWS 1135
Logging in to a UNIX system from Windows ......................... 1135
Accessing remote desktops ..................................................... 1136
X server running on a Windows computer ............................. 1136
VNC: Virtual Network Computing .......................................... 1138
Windows RDP: Remote Desktop Protocol ............................... 1138
Running Windows and Windows-like applications .................. 1139
Dual booting, or why you shouldn’t ....................................... 1140
Microsoft Office alternatives ................................................. 1140
Using command-line tools with Windows .............................. 1140
Windows compliance with email and web standards ............... 1141
Sharing files with Samba and CIFS ........................................ 1142
Samba: CIFS server for UNIX ............................................... 1142
Samba installation ............................................................... 1143
Filename encoding .............................................................. 1145
User authentication ............................................................. 1145
Basic file sharing ............................................................... 1146
Group shares ....................................................................... 1146
Transparent redirection with MS DFS .................................. 1147
smbclient: a simple CIFS client ............................................. 1148
Linux client-side support for CIFS ........................................ 1148
Sharing printers with Samba .................................................. 1149
Installing a printer driver from Windows .............................. 1151
Installing a printer driver from the command line ................. 1152
Debugging Samba ............................................................... 1152
Active Directory authentication ............................................. 1154
Getting ready for Active Directory integration ..................... 1155
Configuring Kerberos for Active Directory integration .......... 1156
Table of Contents

Samba as an Active Directory domain member ........................................ 1157
PAM configuration ................................................................. 1159
Alternatives to winbind ............................................................ 1160
Recommended reading ............................................................... 1160
Exercises ................................................................................. 1161

CHAPTER 31 SERIAL DEVICES AND TERMINALS 1162
The RS-232C standard ............................................................... 1163
Alternative connectors ............................................................... 1165
The DB-9 variant ....................................................................... 1166
The RJ-45 variant ....................................................................... 1166
Hard and soft carrier ................................................................. 1167
Hardware flow control .............................................................. 1168
Serial device files ...................................................................... 1168
setserial: set serial port parameters under Linux ......................... 1169
Pseudo-terminals ....................................................................... 1170
Configuration of terminals ......................................................... 1171
The login process ...................................................................... 1171
The /etc/ttytype file .................................................................... 1172
The /etc/gettytab file ............................................................... 1173
The /etc/gettydefs file ............................................................. 1173
The /etc/inittab file .................................................................... 1174
getty configuration for Linux ...................................................... 1175
Ubuntu Upstart .......................................................................... 1176
Solaris and sacadm ................................................................. 1176
Special characters and the terminal driver .................................. 1177
stty: set terminal options ......................................................... 1178
tset: set options automatically ................................................. 1178
Terminal unwedging ................................................................... 1179
Debugging a serial line ............................................................. 1180
Connecting to serial device consoles ........................................ 1180
Exercises ................................................................................. 1182

CHAPTER 32 MANAGEMENT, POLICY, AND POLITICS 1183
The purpose of IT ........................................................................ 1184
Budgeting and spending ............................................................ 1184
IT policy ..................................................................................... 1185
Service level agreements .......................................................... 1186
Scope and descriptions of services ............................................ 1187
Queue management policies ..................................................... 1188
Roles and responsibilities ........................................................ 1189
Conformance measurements ..................................................... 1189
The structure of an IT organization ........................................... 1190
The foundation: the ticketing and task management system ........... 1191
Common functions of ticketing systems .................................. 1191
Ticket ownership ................................................................... 1192
User acceptance of ticketing systems ....................................... 1192
Sample ticketing systems ....................................................... 1193
Ticket dispatching .................................................................. 1194
Skill sets within IT .................................................................. 1195
Time management .................................................................... 1196
The help desk ........................................................................ 1196
Scope of services ..................................................................... 1196
Help desk availability .............................................................. 1196
Help desk addiction ................................................................ 1196
The enterprise architects .......................................................... 1197
Make processes reproducible .................................................... 1197
Leave a trail of bread crumbs .................................................... 1198
Recognize the criticality of documentation ............................... 1198
Customize and write code ....................................................... 1198
Keep the system clean ............................................................. 1198
The operations group .............................................................. 1199
Aim for minimal downtime ...................................................... 1199
Document dependencies ......................................................... 1199
Repurpose or eliminate older hardware ..................................... 1200
Maintain local documentation ............................................... 1200
Standardized documentation .................................................. 1202
Hardware labeling .................................................................. 1203
Network documentation ......................................................... 1204
User documentation ............................................................... 1204
Keep environments separate .................................................. 1204
Automate, automate, automate ............................................... 1205
Management ......................................................................... 1206
Leadership ............................................................................. 1206
Personnel management ........................................................... 1207
Hiring .................................................................................... 1207
Firing ..................................................................................... 1208
Mechanics of personnel management ...................................... 1209
Quality control ....................................................................... 1209
Management without meddling .............................................. 1210
Community relations .............................................................. 1210
Management of upper management ....................................... 1211
Purchasing ............................................................................. 1212
Conflict resolution .................................................................. 1213
Mediation ............................................................................... 1213
Rogue users and departments ................................................ 1214
# Table of Contents

Policies and procedures .............................................. 1215
  The difference between policies and procedures ............. 1215
  Policy best practices ............................................ 1216
  Procedures .......................................................... 1216
Disaster recovery ..................................................... 1217
  Risk assessment .................................................... 1217
  Disaster management .............................................. 1218
  Staff for a disaster .............................................. 1220
  Power and HVAC .................................................. 1220
  Internet connection redundancy ................................. 1221
  Security incidents ............................................... 1222
Compliance: regulations and standards ............................ 1222
  ITIL: the Information Technology Infrastructure Library .... 1225
  NIST: the National Institute for Standards and Technology . 1225
Legal issues ............................................................ 1226
  Privacy ............................................................. 1226
  Policy enforcement ............................................... 1227
  Control = liability ............................................... 1228
  Software licenses ................................................. 1228
Organizations, conferences, and other resources ............... 1229
Recommended Reading ................................................ 1231
Exercises .............................................................. 1231

**INDEX** 1233
**A BRIEF HISTORY OF SYSTEM ADMINISTRATION** 1264
**IN DEFENSE OF AIX** 1274
**COLOPHON** 1277
**ABOUT THE CONTRIBUTORS** 1278
**ABOUT THE AUTHORS** 1279
Twenty-seven years ago, in 1983, I wrote what may have been the first system administrator's guide for the UNIX operating system. I'd been hired as a contractor to write documentation at a UNIX workstation company called Massachusetts Computer Company (MASSCOMP for short). When I finished the graphics programming manuals I'd been hired to write, I was casting around for something else to do there. "When any of us have system problems, we go to Tom Teixeira," I said. "What are our customers going to do?"

The answer was quick: "Uh, oh! We really need a manual." I was soon rehired to extract as much information as I could from Tom Teixeira's head and put it onto paper.

That book covered the basics: the root account, account addition, permission management, backup and restore, a bit about networking with UUCP, and so on. It was oriented toward System V, one of the two dominant flavors of UNIX at the time (the other being Berkeley UNIX).

All things considered, I did a pretty good job of extracting information from Tom and other members of the then rare caste of elite system administrators. But there was no question in my mind that when the *UNIX System Administration Handbook* (USAH) came out in 1989, the bible of the field had arrived—captured not by an amanuensis, but direct from the keyboards of the masters.

By then, O'Reilly had become a publisher. Recognizing that many of my technical writing customers were adopting UNIX, I had begun retaining the rights to the manuals I wrote so that I could resell them to other companies. In late 1985, we introduced our first books that were sold to the public rather than licensed to companies. We focused first on small books about individual topics such as vi,
sed and awk, termcap and terminfo, and the UUCP networking system. We called them “Nutshell Handbooks” because we wanted to capture everything “in a nutshell.”

We didn't really know anything about publishing. Our books had no spines (they were stapled), indexes, or ISBNs. We sold them by mail order, not through bookstores. But bit by bit, we learned. And eventually, we came into competition with the existing world of computer book publishers.

General UNIX administration was an obvious subject for us, but we didn't tackle it till years later. Why not? I am a big believer in filling unmet needs, not competing for the sake of it. And it was so clear that there was already a book on the topic that was not just good but GREAT! I could imagine neither the need to compete with such a comprehensive book nor the possibility of success in doing so.

Eventually, as our business matured and we entered the retail computer book market, we realized that competition can actually help grow the market. People see one book, and it's an outlier. They see more than one, and, to quote Arlo Guthrie, "they may think it's a movement." Besides, in that first edition of USAH, the authors had a clear bias toward BSD-based systems, and we thought there was room for a book with more of a System V bias.

In 1991, we published our own comprehensive book on UNIX system administration, Aileen Frisch's Essential System Administration.

As an author, editor, and publisher, I never paid much attention to the competition—except in a few cases. This is one of those cases. The UNIX System Administration Handbook is one of the few books we ever measured ourselves against. Could we be as good? Could we be better? Like the NBA duels of Magic Johnson and Larry Bird, the competition brought out the best in us.

Uh, oh again! Fourth edition? Aileen had better get back to work! :-)

Tim O'Reilly
June 2010
Preface

When we were writing the first edition of this book in the mid-1980s, we were eager to compare our manuscript with other books about system administration. To our delight, we could find only three. These days, you have your choice of hundreds. Here are the features that distinguish our book:

- We take a hands-on approach. You already have plenty of manuals; our purpose is to summarize our collective perspective on system administration and to recommend approaches that stand the test of time. This book contains numerous war stories and a wealth of pragmatic advice.
- This is not a book about how to run UNIX or Linux at home, in your garage, or on your PDA. We describe the management of production environments such as businesses, government offices, and universities.
- We cover networking in detail. It is the most difficult aspect of system administration and the area in which we think we can be of most help.
- We cover the major variants of UNIX and Linux.

The Organization of This Book

This book is divided into three large chunks: Basic Administration, Networking, and Bunch o’ Stuff.

Basic Administration presents a broad overview of UNIX and Linux from a system administrator’s perspective. The chapters in this section cover most of the facts and techniques needed to run a stand-alone system.

The Networking section describes the protocols used on UNIX systems and the techniques used to set up, extend, and maintain networks and Internet-facing
servers. High-level network software is also covered here. Among the featured
topics are the Domain Name System, the Network File System, electronic mail,
and network management.

Bunch o’ Stuff includes a variety of supplemental information. Some chapters dis-
cuss optional features such as those that support server virtualization. Others give
advice on topics ranging from eco-friendly computing to the politics of running a
system administration group.

Each chapter is followed by a set of practice exercises. Items are marked with our
estimate of the effort required to complete them, where “effort” is an indicator of
both the difficulty of the task and the time required. There are four levels:

no stars  Easy, should be straightforward
★         Harder or longer, may require lab work
★★        Hardest or longest, requires lab work and digging
★★★★★    Semester-long projects (only in a few chapters)

Some of the exercises require root or sudo access to the system; others require the
permission of the local sysadmin group. Both requirements are mentioned in the
text of the exercise.

OUR CONTRIBUTORS

We’re delighted that Ned McClain, David Schweikert, and Tobi Oetiker were able
to join us once again as contributing authors. With this edition, we also welcome
Terry Morreale and Ron Jachim as new contributors. These contributors’ deep
knowledge of a variety of areas has greatly enriched the content of this book.

CONTACT INFORMATION

Please send suggestions, comments, and bug reports to ulsah@book.admin.com.
We do answer mail, but please be patient; it is sometimes a few days before one of
us is able to respond. Because of the volume of email that this alias receives, we
regret that we are unable to answer technical questions.

To view a copy of our current bug list and other late-breaking information, visit
our web site, admin.com.

We hope you enjoy this book, and we wish you the best of luck with your adven-
tures in system administration!

Evi Nemeth
Garth Snyder
Trent R. Hein
Ben Whaley

June 2010
Acknowledgments

Many people contributed to this project, bestowing everything from technical reviews and suggested exercises to overall moral support. The following folks deserve special thanks for hanging in there with us:

Ron Aitchison  Peter Haag  Jeremy C. Reed
Eric Allman  Bryan Helvey  Andy Rudoff
Clay Baenziger  Matthijs Mekking  Michael Sinatra
Adam Boggs  Randall Munroe  Paul Vixie
Tom Christiansen  Eric Osterweil  Wouter Wijngaards
Dan Foster  Phil Pennock
Steve Gaede  William Putnam

Our editor at Prentice Hall, Mark Taub, deserves not only our thanks but also an award for dealing patiently with flaky authors and a supporting cast that sometimes seemed to run to thousands of contributors.

We’ve had outstanding technical reviewers. Two in particular, Jonathan Corbet and Pat Parseghian, deserve special mention not only for their diplomatic and detailed comments but also for their willingness to stick with us over the course of multiple editions.

Mary Lou Nohr once again did an exceptional job as copy editor. She is a car crushing plant and botanical garden rolled into one.

This edition’s awesome cartoons and cover were conceived and executed by Lisa Haney. Her portfolio is on-line at lisahaney.com.

Linda Grigoleit, Terry Hoffman, and John Sullivan helped us negotiate the IBM network and obtain equipment for evaluation.
Thanks also to Applied Trust (appliedtrust.com), which contributed laboratory space and a variety of logistical support.

Finally, we were unable to reach an agreement that would allow us to publicly acknowledge one of our distinguished contributing authors. His contributions and support throughout the project were nonetheless appreciated, and we send him this palindrome for his collection: “A man, a plan, a canoe, pasta, Hero's rajas, a coloratura, maps, snipe, percale, macaroni, a gag, a banana bag, a tan, a tag, a banana bag again (or a camel), a crepe, pins, Spam, a rut, a Rolo, cash, a jar, sore hats, a peon, a canal—Panama!”
An awful lot of UNIX and Linux information is available these days, so we’ve designed this book to occupy a specific niche in the ecosystem of man pages, blogs, magazines, books, and other reference materials that address the needs of system administrators.

First, it’s an orientation guide. It reviews the major administrative systems, identifies the different pieces of each, and explains how they work together. In the many cases where you must choose between various implementations of a concept, we describe the advantages and drawbacks of the major players.

Second, it’s a quick-reference handbook that summarizes what you need to know to perform common tasks on a variety of common UNIX and Linux systems. For example, the ps command, which shows the status of running processes, supports more than 80 command-line options on Linux systems. But a few combinations of options satisfy 99% of a system administrator’s needs; see them on page 130.

Finally, this book focuses on the administration of enterprise servers and networks. That is, serious system administration. It’s easy to set up a single desktop system; harder to keep a virtualized network running smoothly in the face of load spikes, disk failures, and intentional attacks. We describe techniques and rules of
Chapter 1  Where to Start

...thumb that help networks recover from adversity, and we help you choose solutions that scale as your site grows in size, complexity, and heterogeneity.

We don't claim to do all of this with perfect objectivity, but we think we've made our biases fairly clear throughout the text. One of the interesting things about system administration is that reasonable people can have dramatically different notions of what constitute the most appropriate policies and procedures. We offer our subjective opinions to you as raw data. You'll have to decide for yourself how much to accept and to what extent our comments apply to your environment.

1.1 ESSENTIAL DUTIES OF THE SYSTEM ADMINISTRATOR

The Wikipedia page for "system administrator" includes a nice discussion of the tasks that system administration is generally thought to include. This page currently draws a rather sharp distinction between administration and software development, but in our experience, professional administrators spend much of their time writing scripts. That doesn't make system administrators developers per se, but it does mean that they need many of the same analytical and architectural skills.

The sections below summarize some of the main tasks that administrators are expected to perform. These duties need not necessarily be carried out by a single person, and at many sites the work is distributed among a team. However, at least one person must understand all the components and make sure that every task is being done correctly.

**Account provisioning**

The system administrator adds accounts for new users, removes the accounts of users that are no longer active, and handles all the account-related issues that come up in between (e.g., forgotten passwords). The process of adding and removing users can be automated, but certain administrative decisions (where to put a user's home directory, which machines to create the account on, etc.) must still be made before a new user can be added.

When a user should no longer have access to the system, the user's account must be disabled. All the files owned by the account should be backed up and then disposed of so that the system does not accumulate unwanted baggage over time.

**Adding and removing hardware**

When new hardware is purchased or when hardware is moved from one machine to another, the system must be configured to recognize and use that hardware. Hardware-support chores can range from the simple task of adding a printer to the more complex job of adding a disk array.

Now that virtualization has arrived in the enterprise computing sphere, hardware configuration can be more complicated than ever. Devices may need installation
Maintaining local documentation

at several layers of the virtualization stack, and the system administrator may need to formulate policies that allow the hardware to be shared securely and fairly.

**Performing backups**

Performing backups is perhaps the most important job of the system administrator, and it is also the job that is most often ignored or sloppily done. Backups are time consuming and boring, but they are absolutely necessary. Backups can be automated and delegated to an underling, but it is still the system administrator’s job to make sure that backups are executed correctly and on schedule (and that the resulting media can actually be used to restore files).

**Installing and upgrading software**

When new software is acquired, it must be installed and tested, often under several operating systems and on several types of hardware. Once the software is working correctly, users must be informed of its availability and location. As patches and security updates are released, they must be incorporated smoothly into the local environment.

Local software and administrative scripts should be properly packaged and managed in a fashion that’s compatible with the native upgrade procedures used on systems at your site. As this software evolves, new releases should be staged for testing before being deployed to the entire site.

**Monitoring the system**

Large installations require vigilant supervision. Don’t expect users to report problems to you unless the issues are severe. Working around a problem is usually faster than taking the time to document and report it, so users often follow the path of least resistance.

Regularly ensure that email and web services are working correctly, watch log files for early signs of trouble, make sure that local networks are properly connected, and keep an eye on the availability of system resources such as disk space. All of these chores are excellent opportunities for automation, and a variety of off-the-shelf monitoring systems can help sysadmins with this task.

**Troubleshooting**

System failures are inevitable. It is the administrator’s job to play mechanic by diagnosing problems and calling in experts if needed. Finding the problem is often harder than fixing it.

**Maintaining local documentation**

As a system is changed to suit an organization’s needs, it begins to differ from the plain-vanilla system described by the documentation. Since the system administrator is responsible for making these customizations, it’s also the sysadmin’s duty to document the changes. This chore includes documenting where cables are run
and how they are constructed, keeping maintenance records for all hardware, re-
cording the status of backups, and documenting local procedures and policies.

**Vigilantly monitoring security**
The system administrator must implement a security policy and periodically
check to be sure that the security of the system has not been violated. On low-
security systems, this chore might involve only a few basic checks for unauthor-
ized access. On a high-security system, it can include an elaborate network of
traps and auditing programs.

**Fire fighting**
Although helping users with their various problems is rarely included in a system
administrator's job description, it claims a significant portion of most administra-
tors’ workdays. System administrators are bombarded with problems ranging
from “It worked yesterday and now it doesn't! What did you change?” to “I spilled
coffee on my keyboard! Should I pour water on it to wash it out?”

In most cases, your response to these issues affects your perceived value as an
administrator far more than does any actual technical skill you might possess. You
can either howl at the injustice of it all, or you can delight in the fact that a single
well-handled trouble ticket scores as many brownie points as five hours of mid-
night debugging. You pick!

1.2 **Suggested Background**

We assume in this book that you have a certain amount of Linux or UNIX experi-
ence. In particular, you should have a general concept of how the system looks
and feels from the user's perspective since we don't review this material. Several
good books can get you up to speed; see the reading list on page 27.

Even in these days of Compiz-powered 3D desktops, the GUI tools for system
administration on UNIX and Linux systems remain fairly simplified in compari-
son with the richness of the underlying software. In the real world, we still admin-
ister by editing configuration files and writing scripts, so you'll need to be com-
fortable with both a command-line shell and a text editor.

Your editor can be a GUI tool like **gedit** or a command-line tool such as **vi** or
**emacs**. Word processors such as Microsoft Word and OpenOffice Writer are quite
different from text editors and are nearly useless for administrative tasks. Com-
mand-line tools have an edge because they can run over simple SSH connections
and on ailing systems that won't boot; there's no need for a window system. They
are also much faster for the quick little edits that administrators often make.

We recommend learning **vi** (now seen most commonly in its rewritten form,
**vim**), which is standard on all UNIX and Linux systems. Although it may appear
a bit pallid when compared with glitzier offerings such as **emacs**, it is powerful
and complete. GNU's **nano** is a simple and low-impact "starter editor" that has
on-screen prompts. Be wary of nonstandard editors, though; if you become addicted to one, you may soon tire of dragging it along with you to install on every new system.

One of the mainstays of administration (and a theme that runs throughout this book) is the use of scripts to automate administrative tasks. To be an effective administrator, you must be able to read and modify Perl and bash/sh scripts.

For new scripting projects, we recommend Perl or Python. As a programming language, Perl is admittedly a bit strange. However, it does include many features that are indispensable for administrators. The O’Reilly book *Programming Perl* by Larry Wall et al. is the standard text; it’s also a model of good technical writing. A full citation is given on page 27.

Many administrators prefer Python to Perl, and we know of sites that are making a concerted effort to convert. Python is a more elegant language, and Python scripts are generally more readable and easier to maintain. (As Amazon’s Steve Yegge said, “The Python community has long been the refuge for folks who finally took the red pill and woke up from the Perl Matrix.”) A useful set of links that compare Python to other scripting languages (including Perl) can be found at python.org/doc/Comparisons.html.

Ruby is an up-and-coming language that maintains many of the strengths of Perl while avoiding some of Perl’s syntactic pitfalls and adding modern object-oriented features. It doesn’t yet have a strong tradition as a scripting language for system administrators, but that will likely change over the next few years.

We also suggest that you learn expect, which is not a programming language so much as a front end for driving interactive programs. It’s an efficient glue technology that can replace some complex scripting. expect is easy to learn.

Chapter 2, *Scripting and the Shell*, summarizes the most important things to know about scripting for bash, Perl, and Python. It also reviews regular expressions (text matching patterns) and some shell idioms that are useful for sysadmins.

### 1.3 FRICTION BETWEEN UNIX AND LINUX

Because they are similar, this book covers both UNIX and Linux systems. Unfortunately, mentioning UNIX and Linux together in the same sentence can sometimes be like stepping into a political minefield, or perhaps blundering into a large patch of quicksand. But since the relationship between UNIX and Linux seems to engender some confusion as well as animosity, it’s hard to avoid staking out a position. Here is our perspective and our short version of the facts.

Linux is a reimplementation and elaboration of the UNIX kernel. It conforms to the POSIX standard, runs on several hardware platforms, and is compatible with most existing UNIX software. It differs from many—but not all—variants of UNIX in that it is free, open source, and cooperatively developed. Linux includes
Chapter 1 Where to Start

technical advances that did not exist in UNIX, so it is more than just a UNIX clone. At the same time, traditional UNIX vendors have continued to refine their systems, so there are certainly areas in which commercial UNIX systems are superior to Linux.

Whatever the relative merits of the systems, Linux is a legally, developmentally, and historically distinct entity that cannot properly be referred to as "UNIX" or as a "version of UNIX." To do so is to slight the work and innovation of the Linux community. At the same time, it's somewhat misleading to insist that Linux is "not UNIX." If your creation walks like a duck and quacks like a duck, you may have invented a duck.

Schisms exist even within the Linux camp. It has been argued, with some justification, that referring to Linux distributions simply as "Linux" fails to acknowledge the work that went into the software that runs outside the kernel (which in fact constitutes the vast majority of software on an average system). Unfortunately, the most commonly suggested alternative, GNU/Linux, has its own political baggage and has been officially endorsed only by the Debian distribution. The Wikipedia entry for "GNU/Linux naming controversy" outlines the arguments on both sides. Interestingly, the use of open source software is now predominant even on most UNIX systems, but no one seems to be pushing for a GNU/UNIX designation just yet.

Linux software is UNIX software. Thanks largely to the GNU Project, most of the important software that gives UNIX systems their value has been developed under some form of open source model. The same code runs on Linux and non-Linux systems. The Apache web server, for example, doesn't much care whether it's running on Linux or Solaris. From the standpoint of applications and most administrative software, Linux is simply one of the best-supported and most widely available varieties of UNIX.

It's also worth noting that Linux is not the only free UNIX-like operating system in the world. OpenSolaris is free and open source, although its exact licensing terms have earned suspicious looks from some open source purists. FreeBSD, NetBSD, and OpenBSD—all offshoots of the Berkeley Software Distribution from UC Berkeley—have ardent followers of their own. These OSes are generally comparable to Linux in their features and reliability, although they enjoy somewhat less support from third-party software vendors.

1. Since Wikipedia contains Linux information and must therefore refer to Linux frequently, the debate has particular relevance to Wikipedia itself. The discussion page for the Wikipedia article is also well worth reading.
2. After all, "GNU's not UNIX!"
3. Several of our technical reviewers protested that we seem to be crediting GNU with the creation of most of the world's free software. We are not! However, GNU has certainly done more than any other group to promote the idea of free software as a social enterprise and to structure ongoing debate about licensing terms and interactions between free and nonfree software.
UNIX and Linux systems have both been used in production environments for many years, and they both work well. At this point, the choice between them has more to do with packaging, support, and institutional inertia than any real difference in quality or modernity.

In this book, comments about “Linux” generally apply to Linux distributions but not to traditional UNIX variants. The meaning of “UNIX” is a bit more fluid, as we occasionally apply it to attributes shared by all UNIX derivatives, including Linux (e.g., “UNIX file permissions”). To avoid ambiguity, we usually say “UNIX and Linux” when we mean both.

1.4 Linux Distributions

All Linux distributions share the same kernel lineage, but the ancillary materials that go along with that kernel can vary quite a bit. Distributions vary in their focus, support, and popularity. There continue to be hundreds of independent Linux distributions, but our sense is that distributions based on the Debian, Red Hat, and SUSE lineages will continue to predominate in production environments over the next five years.

The differences among Linux distributions are not cosmically significant. In fact, it is something of a mystery why there are so many different distributions, each claiming “easy installation” and “a massive software library” as its distinguishing features. It’s hard to avoid the conclusion that people just like to make new Linux distributions.

Many smaller distributions are surprisingly competitive in terms of fit and finish. All major distributions, including the second tier, include a relatively painless installation procedure, a well-tuned desktop environment, and some form of package management. Most distributions also allow you to boot from the distribution DVD, which can be handy for debugging and is also a nice way to take a quick look at a new distribution you are considering.

Since our focus in this book is the management of large-scale installations, we’re partial to distributions such as Red Hat Enterprise Linux that take into account the management of networks of machines. Some distributions are designed with production environments in mind, and others are not. The extra crumbs of assistance that the production-oriented systems toss out can make a significant difference in ease of administration.

When you adopt a distribution, you are making an investment in a particular vendor’s way of doing things. Instead of looking only at the features of the installed software, it’s wise to consider how your organization and that vendor are going to work with each other in the years to come.

4. We consider a “production” environment to be one that an organization relies on to accomplish real work (as opposed to testing, research, or development).
Some important questions to ask are

- Is this distribution going to be around in five years?
- Is this distribution going to stay on top of the latest security patches?
- Is this distribution going to release updated software promptly?
- If I have problems, will the vendor talk to me?

Viewed in this light, some of the more interesting, offbeat distributions don’t sound quite so appealing. But don’t count them out: E*Trade, for example, runs on Gentoo Linux.

The most viable distributions are not necessarily the most corporate. For example, we expect Debian Linux (OK, OK, Debian GNU/Linux!) to remain viable for a long time despite the fact that Debian is not a company, doesn’t sell anything, and offers no formal, on-demand support. Debian itself isn’t one of the most widely used distributions, but it benefits from a committed group of contributors and from the enormous popularity of the Ubuntu distribution, which is based on it.

Table 1.1 lists some of the most popular mainstream distributions.

<table>
<thead>
<tr>
<th>Distribution</th>
<th>Web site</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS</td>
<td>centos.org</td>
<td>Free analog of Red Hat Enterprise</td>
</tr>
<tr>
<td>Debian</td>
<td>debian.org</td>
<td>Closest to GNU</td>
</tr>
<tr>
<td>Fedora</td>
<td>fedoraproject.org</td>
<td>De-corporatized Red Hat Linux</td>
</tr>
<tr>
<td>Gentoo</td>
<td>gentoo.org</td>
<td>Compile-it-yourself, optimized</td>
</tr>
<tr>
<td>Linux Mint</td>
<td>linuxmint.com</td>
<td>Ubuntu-based, elegant apps</td>
</tr>
<tr>
<td>Mandriva</td>
<td>mandriva.com</td>
<td>Long history, “easy to try”</td>
</tr>
<tr>
<td>openSUSE</td>
<td>opensuse.org</td>
<td>Free analog of SUSE Linux Enterprise</td>
</tr>
<tr>
<td>Oracle Enterprise Linux</td>
<td>oracle.com</td>
<td>Oracle-supported version of RHEL</td>
</tr>
<tr>
<td>PCLinuxOS</td>
<td>pclinuxos.com</td>
<td>Fork of Mandriva, KDE-oriented</td>
</tr>
<tr>
<td>Red Flag</td>
<td>redflag-linux.com</td>
<td>Chinese distro, similar to Red Hat</td>
</tr>
<tr>
<td>Red Hat Enterprise</td>
<td>redhat.com</td>
<td>Reliable, slow-changing, commercial</td>
</tr>
<tr>
<td>Slackware</td>
<td>slackware.com</td>
<td>Grizzled, long-surviving distro</td>
</tr>
<tr>
<td>SUSE Linux Enterprise</td>
<td>novell.com/linux</td>
<td>Strong in Europe, multilingual</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>ubuntu.com</td>
<td>Cleaned-up version of Debian</td>
</tr>
</tbody>
</table>

A comprehensive list of distributions, including many non-English distributions, can be found at linux.org/dist, lwn.net/Distributions, or distrowatch.com.

1.5 **Example systems used in this book**

We have chosen three popular Linux distributions and three UNIX variants as our examples to discuss throughout this book: Ubuntu Linux, openSUSE, Red Hat Enterprise Linux, Solaris, HP-UX, and AIX. These systems are representative of
Example Linux distributions

the overall marketplace and account collectively for an overwhelming majority of the installations in use at large sites today.

Information in this book generally applies to all of our example systems unless a specific attribution is given. Details particular to one system are marked with the vendor’s logo:

- Ubuntu® 9.10 "Karmic Koala"
- openSUSE® 11.2
- Red Hat® Enterprise Linux® 5.5
- Solaris™ 11 and OpenSolaris™ 2009.06
- HP-UX® 11i v3
- AIX® 6.1

These logos are used with the kind permission of their respective owners. However, the vendors have not reviewed or endorsed the contents of this book. The paragraphs below provide a bit more detail about each of these example systems.

Example Linux distributions

Information that’s specific to Linux but not to any particular distribution is marked with the Tux penguin logo shown at left.

The Ubuntu distributions maintain an ideological commitment to community development and open access, so there’s never any question about which parts of the distribution are free or redistributable. Ubuntu currently enjoys philanthropic funding from South African entrepreneur Mark Shuttleworth.

Ubuntu is based on the Debian distribution and uses Debian’s packaging system. It comes in two main forms, a Desktop Edition and a Server Edition. They are essentially similar, but the Server Edition kernel comes pretuned for server use and does not install a GUI or GUI applications such as OpenOffice.

SUSE, now part of Novell, has taken the path of Red Hat and forked into two related distributions: one (openSUSE) that contains only free software; and another (SUSE Linux Enterprise) that costs money, includes a formal support path, and offers a few extra trinkets. Nothing in this book is specific to one SUSE distribution or the other, so we simply refer to them collectively as “SUSE.”

Red Hat has been a dominant force in the Linux world for most of the last decade, and its distributions are widely used in North America. In 2003, the original Red Hat Linux distribution was split into a production-centered line called Red Hat Enterprise Linux (which we refer to as RHEL or Red Hat in this book) and a
community-based development project called Fedora. The split was motivated by a variety of technical, economic, logistic, and legal reasons.

The distributions were initially similar, but Fedora has made some significant changes over the last five years and the two systems aren't currently synchronized in any meaningful way. RHEL offers great support and stability but is effectively impossible to use without paying licensing fees to Red Hat.

The CentOS Project (centos.org) collects source code that Red Hat is obliged to release under various licensing agreements (most notably, the GNU Public License) and assembles it into a complete distribution that is eerily similar to Red Hat Enterprise Linux, but free of charge. The distribution lacks Red Hat’s branding and a few proprietary tools, but is in other respects equivalent. CentOS aspires to full binary and bug-for-bug compatibility with RHEL.

CentOS is an excellent choice for sites that want to deploy a production-oriented distribution without paying tithes to Red Hat. A hybrid approach is also feasible: front-line servers can run Red Hat Enterprise Linux and avail themselves of Red Hat’s excellent support, while desktops run CentOS. This arrangement covers the important bases in terms of risk and support while also minimizing cost and administrative complexity.

Example UNIX distributions

Solaris is a System V derivative with many extensions from the company formerly known as Sun Microsystems, now part of Oracle. Solaris (as it was called in the mid-80s) was originally the progeny of Berkeley UNIX, but a (now historic) corporate partnership between Sun and AT&T forced a change of code base. Solaris runs on a variety of hardware platforms, most notably Intel x86 and SPARC.

In Sun’s hands, Solaris was free to download and use. However, Oracle has changed this policy, and current downloads are labeled as 90-day free trial editions. The existence of OpenSolaris, an explicitly free and open source version of Solaris, complicates the picture as well. At this point (mid-2010), Oracle’s exact plans for Solaris and OpenSolaris remain unclear.

The release of Solaris 11 is expected some time this year, and every indication so far is that it will hew closely to OpenSolaris. In this book, the composite system we refer to as “Solaris” is based on production Solaris 10 and OpenSolaris releases, adjusted with guidance from our network of deep-cover spies within Oracle. In a few cases, we note specifics for Solaris 10 or OpenSolaris.

HP-UX is based on System V and is tied to Hewlett-Packard’s hardware platforms. It’s closer to the ancestral source tree than either Solaris or AIX, but HP has kept pace with developments in the OS world and has added a variety of its own enhancements. Now that HP has begun supporting Linux as well, the future of HP-UX is somewhat less clear.

---

5. See page 1264 for some background on BSD, System V, and the general history of UNIX.
IBM's AIX started as a variant of Berkeley's 4.2BSD, but as of version 4 in 1994, most parts of the system migrated to System V. At this point, AIX has drifted rather far from both origins.

In general, we have the impression that AIX has enjoyed less cross-pollination from other systems than most UNIX variants. It also seems to have fallen under the Svengali-like influence of some of IBM's mainframe and AS/400 operating systems, from which it inherits conventions such as the Object Data Manager (see page 432), the use of configuration commands rather than configuration files, and the SMIT administrative interface. Over time, one might charitably say, it has grown to be more and more like itself.

IBM has been pursuing an interestingly OS-agnostic approach to marketing its hardware for most of the last decade. IBM continues to develop and promote AIX, but it's also engaged in partnerships with Red Hat and Novell to ensure that their respective Linux distributions run smoothly on IBM hardware. It will be interesting to see how this approach plays out in the years ahead.

1.6 SYSTEM-SPECIFIC ADMINISTRATION TOOLS

Modern systems include a variety of visually oriented tools and control panels (such as SUSE's YaST2 and IBM's SMIT) that help you configure or administer selected aspects of the system. These tools are useful, especially for novice administrators, but they also tend to be relatively incomplete reflections of the underlying software. They make many administrative tasks easier, but most fall short of being authoritative.

In this book, we cover the underlying mechanisms that the visual tools manipulate rather than the tools themselves, for several reasons. For one, the visual tools tend to be proprietary (or at least, system-specific). They introduce variation into processes that may actually be quite consistent among systems at a lower level. Second, we believe that it's important for administrators to have an accurate understanding of how their systems work. When the system breaks, the visual tools are often not helpful in tracking down and fixing problems. Finally, manual configuration is often faster, more flexible, more reliable, and easier to script.

1.7 NOTATION AND TYPOGRAPHICAL CONVENTIONS

In this book, filenames, commands, and literal arguments to commands are shown in boldface. Placeholders (e.g., command arguments that should not be taken literally) are in italics. For example, in the command

\texttt{cp} \texttt{file directory}

you're supposed to replace \texttt{file} and \texttt{directory} with the names of an actual file and an actual directory.
Chapter 1 Where to Start

Excerpts from configuration files and terminal sessions are shown in a fixed-width font.\footnote{It's not really a fixed-width font, but it looks like one. We liked it better than the real fixed-width fonts that we tried. That's why the columns in some examples may not all line up perfectly.} Sometimes, we annotate sessions with italic text. For example:

\$ grep Bob /pub/phonelist
# Look up Bob's phone number
Bob Knowles 555-2834
Bob Smith 555-2311

Outside of these specific cases, we have tried to keep special fonts and formatting conventions to a minimum as long as we could do so without compromising intelligibility. For example, we often talk about entities such as the daemon group or the printer anchor-lw with no special formatting at all.

We use the same conventions as the manual pages for command syntax:

- Anything between square brackets ("[" and "]") is optional.
- Anything followed by an ellipsis ("…") can be repeated.
- Curly braces ("{" and "}") mean that you should select one of the items separated by vertical bars ("|").

For example, the specification

\texttt{bork [-x] \{on|off\} filename …}

would match any of the following commands:

\begin{itemize}
  \item bork on /etc/passwd
  \item bork -x off /etc/passwd /etc/smartd.conf
  \item bork off /usr/lib/tmac
\end{itemize}

We use shell-style globbing characters for pattern matching:

- A star (*) matches zero or more characters.
- A question mark (?) matches one character.
- A tilde or “twiddle” (~) means the home directory of the current user.\footnote{Solaris 10's default shell for root is the original Bourne shell, which (rather surprisingly) does not understand – or –\texttt{user} notation.}
- \texttt{~user} means the home directory of \texttt{user}.

For example, we might refer to the startup script directories /etc/rc0.d, /etc/rc1.d, and so on with the shorthand pattern /etc/rc*.d.

Text within quotation marks often has a precise technical meaning. In these cases, we ignore the normal rules of U.S. English and put punctuation outside the quotes so that there can be no confusion about what's included and what's not.

1.8 Units

Metric prefixes such as kilo-, mega-, and giga- are defined as powers of 10: one megabuck is 1,000,000 dollars. However, computer types have long poached these prefixes and used them to refer to powers of 2. For example, one "megabyte" of...
memory is really \(2^{20}\) or 1,048,576 bytes. The stolen units have even made their way into formal standards such as the JEDEC Solid State Technology Association’s Standard 100B.01, which recognizes the prefixes as denoting powers of 2 (albeit with some misgivings).

In an attempt to restore clarity, the International Electrotechnical Commission has defined a set of numeric prefixes (kibi-, mebi-, gibi-, and so on, abbreviated Ki, Mi, and Gi) based explicitly on powers of 2. Those units are always unambiguous, but they are just starting to be widely used. The original kilo-series prefixes are still used in both senses.

Context helps with decoding. RAM is always denominated in powers of 2, but network bandwidth is always a power of 10. Storage space is usually quoted in power-of-10 units, but block and page sizes are in fact powers of 2.

In this book, we use IEC units for powers of 2, metric units for powers of 10, and metric units for rough values and cases in which the exact basis is unclear, undocumented, or impossible to determine. In command output and in excerpts from configuration files, we leave the original values and unit designators. We abbreviate bit as b and byte as B. Table 1.2 shows some examples.

### Table 1.2 Unit decoding examples

<table>
<thead>
<tr>
<th>Example</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>56 kb/s serial line</td>
<td>A serial line that transmits 56,000 bits per second</td>
</tr>
<tr>
<td>1kB file</td>
<td>A file that contains 1,000 bytes</td>
</tr>
<tr>
<td>4KiB SSD pages</td>
<td>SSD pages that contain 4,096 bytes</td>
</tr>
<tr>
<td>8KB of memory</td>
<td>Not used in this book; see note below</td>
</tr>
<tr>
<td>100MB file size limit</td>
<td>Nominally (10^8) bytes; in context, ambiguous</td>
</tr>
<tr>
<td>100MB disk partition</td>
<td>Nominally (10^8) bytes; in context, probably 99,999,744 bytes (^a)</td>
</tr>
<tr>
<td>1GiB of RAM</td>
<td>Exactly 1,073,741,824 bytes of memory (^b)</td>
</tr>
<tr>
<td>1 Gb/s Ethernet</td>
<td>A network that transmits 1,000,000,000 bits per second</td>
</tr>
<tr>
<td>1TB hard disk</td>
<td>A hard disk that stores 1,000,000,000 bytes</td>
</tr>
</tbody>
</table>

\(^a\) That is, \(10^8\) rounded down to the nearest whole multiple of the disk’s 512-byte block size  
\(^b\) But according to Microsoft, still not enough memory to run the 64-bit version of Windows 7

The abbreviation K, as in “8KB of RAM!”, is not part of any standard. It’s a computerese adaptation of the metric abbreviation k, for kilo-, and originally meant 1,024 as opposed to 1,000. But since the abbreviations for the larger metric prefixes are already uppercase, the analogy doesn’t scale. Later, people became confused about the distinction and started using K for factors of 1,000, too.

The Ubuntu Linux distribution is making a valiant attempt to bring rationality and consistency to this issue; see wiki.ubuntu.com/UnitsPolicy for some additional details.
1.9 **MAN PAGES AND OTHER ON-LINE DOCUMENTATION**

The manual pages, usually called “man pages” because they are read with the **man** command, constitute the traditional “on-line” documentation. (Of course, these days all the documentation is on-line in some form or another.) Man pages are typically installed with the system. Program-specific man pages come along for the ride when you install new software packages.

Man pages are concise descriptions of individual commands, drivers, file formats, or library routines. They do not address more general topics such as “How do I install a new device?” or “Why is this system so damn slow?” For those questions, consult your vendor’s administration guides (see page 18) or, for Linux systems, the documents available from the Linux Documentation Project.

**Organization of the man pages**

All systems divide the man pages into sections, but there are minor variations in the way some sections are defined. The basic schema used by our example systems is shown in Table 1.3.

<table>
<thead>
<tr>
<th>Linux</th>
<th>Solaris</th>
<th>HP-UX</th>
<th>AIX</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>User-level commands and applications</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>System calls and kernel error codes</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>Library calls</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>7</td>
<td>4</td>
<td>Device drivers and network protocols</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>Standard file formats</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>–</td>
<td>6</td>
<td>Games and demonstrations</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>5</td>
<td>7</td>
<td>Miscellaneous files and documents</td>
</tr>
<tr>
<td>8</td>
<td>1m</td>
<td>1m</td>
<td>8</td>
<td>System administration commands</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>–</td>
<td>–</td>
<td>Obscure kernel specs and interfaces</td>
</tr>
<tr>
<td>–</td>
<td>–</td>
<td>–</td>
<td>9</td>
<td>HP-UX general information</td>
</tr>
</tbody>
</table>

Some sections may be further subdivided. For example, Solaris’s section 3c contains man pages about the system’s standard C library. There is also considerable variation in the exact distribution of pages; some systems leave section 8 empty and lump the system administration commands into section 1. A lot of systems have discontinued games and demos, leaving nothing in section 6. Many systems have a section of the manuals called “1” (lowercase L) for local man pages.

The exact structure of the sections isn’t important for most topics because **man** finds the appropriate page wherever it is stored. You only need to be aware of the section definitions when a topic with the same name appears in multiple sections. For example, **passwd** is both a command and a configuration file, so it has entries in both section 1 and section 4 or 5.
Storage of man pages

**man:** read man pages

*man title* formats a specific manual page and sends it to your terminal through *more, less*, or whatever program is specified in your PAGER environment variable. *title* is usually a command, device, filename, or name of a library routine. The sections of the manual are searched in roughly numeric order, although sections that describe commands (sections 1, 8, and 6) are usually searched first.

The form *man section title* gets you a man page from a particular section. Thus, on most systems, *man sync* gets you the man page for the *sync* command, and *man 2 sync* gets you the man page for the *sync* system call.

Under Solaris, you must preface the section number with the *-s* flag, for example, *man -s 2 sync*.

*man -k keyword* or *apropos keyword* prints a list of man pages that have *keyword* in their one-line synopses. For example:

```bash
$ man -k translate
objcopry (1) - copy and translate object files
dcgettext (3) - translate message
tr (1) - translate or delete characters
snmptranslate (1) - translate SNMP OID values into more useful information
tr (1p) - translate characters
...
```

The keywords database can become out of date. If you add additional man pages to your system, you may need to rebuild this file with *mandb* (Ubuntu, SUSE), *makewhatis* (Red Hat), or *catman -w* (Solaris, HP-UX, AIX).

**Storage of man pages**

*nroff* input for man pages is usually kept in directories under */usr/share/man*. Linux systems compress them with *gzip* to save space. (The *man* command knows how to uncompress them on the fly.) The *man* command maintains a cache of formatted pages in */var/cache/man* or */usr/share/man* if the appropriate directories are writable, but this is a security risk. Most systems preformat the man pages once at installation time (see *catman*) or not at all.

Solaris understands man pages formatted with SGML in addition to the traditional *nroff*. The SGML pages have their own section directories underneath */usr/share/man*.

The *man* command can search several man page repositories to find the manual pages you request. On Linux systems, you can find out the current default search path with the *manpath* command. This path (from Ubuntu) is typical:

```bash
ubuntu$ manpath
/usr/local/man:/usr/local/share/man:/usr/share/man
```
Chapter 1 Where to Start

If necessary, you can set your MANPATH environment variable to override the default path:

    export MANPATH=/home/share/localman:/usr/share/man

Some systems let you set a custom system-wide default search path for man pages, which can be useful if you need to maintain a parallel tree of man pages such as those generated by OpenPKG. If you want to distribute local documentation in the form of man pages, however, it is simpler to use your system’s standard packaging mechanism and to put man pages in the standard man directories. See Chapter 12, Software Installation and Management, for more details.

GNU Texinfo

Linux systems include a sort of supplemental on-line man page system called Texinfo. It was invented long ago by the GNU folks in reaction to the fact that the nroff command to format man pages was proprietary to AT&T. These days we have GNU’s own groff to do this job for us and the nroff issue is no longer important, but Texinfo still lumbers along like a zombie in search of human brains.

Although the use of Texinfo seems to be gradually fading, a few GNU packages persist in documenting themselves with Texinfo files rather than man pages. You can pipe the output of the Texinfo reader, info, through less to evade info’s built-in navigation system.

Fortunately, packages that are documented with Texinfo usually install man page stubs that tell you to use the info command to read about those particular packages. You can safely stick to the man command for doing manual searches and delve into info land only when instructed to do so. info info initiates you into the dark mysteries of Texinfo.

1.10 OTHER AUTHORITY DOCUMENTATION

Man pages are just a small part of the official documentation. Most of the rest, unfortunately, is scattered about on the web.

System-specific guides

Major vendors have their own dedicated documentation projects, and many continue to produce useful book-length manuals. These days the manuals are usually found on-line rather than in the form of printed books. The extent and quality of the documentation vary widely, but most vendors produce at least an administration guide and an installation guide. Table 1.4 shows where to look for each of our example systems.

The standout in this crowd is IBM, which produces a raft of full-length books on a variety of administration topics. You can buy them as books, but they’re also available for free as downloads. The downside to IBM’s completeness is that many of the documents seem to lag a version or two behind the current release of AIX.
Where to Start

Red Hat is the unfortunate laggard in the documentation race. Most of its documents relate to its proprietary value-added systems rather than to Linux administration generally.

Package-specific documentation

Most of the important software packages in the UNIX and Linux world are maintained by individuals or by third parties such as the Internet Systems Consortium and the Apache Software Foundation. These groups write their own documentation. The quality runs the gamut from embarrassing to spectacular, but jewels such as *Version Control with Subversion* from svnbook.red-bean.com make the hunt worthwhile.

UNIX vendors and Linux distributors always include the appropriate man pages in their packages. Unfortunately, they tend to skimp on other documentation, mostly because there really isn’t a standard place to put it (check `/usr/share/doc`). It’s often useful to check the original source of the software to see if additional materials are available.

Supplemental documents include white papers (technical reports), design rationales, and book- or pamphlet-length treatments of particular topics. These supplemental materials are not limited to describing just one command, so they can adopt a tutorial or procedural approach. Many pieces of software have both a man page and an article. For example, the man page for `vi` tells you about the command-line arguments that `vi` understands, but you have to go to the in-depth treatment to learn how to actually edit a file.

Books

The best resources for system administrators in the printed realm (aside from this book :-) are the O’Reilly series of books. The series began with *UNIX in a Nutshell* over 20 years ago and now includes a separate volume on just about every important UNIX and Linux subsystem and command. The series also includes books on the Internet, Windows, and other non-UNIX topics. All the books are reasonably priced, timely, and focused.
Chapter 1  Where to Start

Tim O’Reilly has become quite interested in the open source movement and runs a conference, OSCON, on this topic as well as conferences on other trendy techie topics. OSCON occurs twice yearly, once in the United States and once in Europe. See oreilly.com for more information.

RFCs and other Internet documents
The Request for Comments document series describes the protocols and procedures used on the Internet. Most of these documents are relatively detailed and technical, but some are written as overviews. They are absolutely authoritative, and many are quite useful for system administrators. See page 449 for a more complete description of these documents.

The Linux Documentation Project
Linux systems have another major source of reference information: the Linux Documentation Project at tldp.org. This site hosts a huge array of user-contributed documentation ranging from FAQs to full-length guides. The LDP also centralizes efforts to translate Linux-related documents into additional languages.

Unfortunately, many of the LDP documents are not well maintained. Since Linux-years are a lot like dog-years in their relation to real time, untended documents are apt to go out of date quickly. Always check the time stamp on a HOWTO or guide and weigh its credibility accordingly.

1.11 OTHER SOURCES OF INFORMATION
The sources discussed in the previous section are generally the most reliable, but they’re hardly the last word in UNIX and Linux documentation. Countless blogs, discussion forums, and news feeds are available on the Internet.

It should go without saying, but Google is a system administrator’s best friend. Unless you’re looking up the details of a specific command or file format, Google should be the first resource you consult for any sysadmin question. Make it a habit; if nothing else, you’ll avoid the delay and humiliation of having your questions in an on-line forum answered with a link to Google.8 When stuck, Google.

We can’t enumerate every useful collection of UNIX and Linux information on the Internet, but a few of the most significant ones are shown in Table 1.5.

Another fun and useful resource is Bruce Hamilton’s “Rosetta Stone” page at bhami.com/rosetta.html. It contains pointers to the commands and tools used for various system administration tasks on many different operating systems.

If you’re a Linux site, don’t be shy about accessing general UNIX resources. Most information is directly applicable to Linux.

8. Or worse yet, a link to Google through lmgty.com
Ways to find and install software

1.12 WAYS TO FIND AND INSTALL SOFTWARE

Chapter 12, *Software Installation and Management*, addresses software provisioning in detail. But for the impatient, here’s a quick primer on how to find out what’s installed on your system and how to obtain and install new software.

Modern operating systems divide their contents into packages that can be installed independently of one another. The default installation includes a range of starter packages that you can expand according to your needs.

Add-on software is often provided in the form of precompiled packages as well, although the degree to which this is a mainstream approach varies widely among systems. Most software is developed by independent groups that release the software in the form of source code. Package repositories then pick up the source code, compile it appropriately for the conventions in use on the systems they serve, and package the resulting binaries. It’s usually easier to install a system-specific binary package than to fetch and compile the original source code. However, packagers are sometimes a release or two behind the current version.

The fact that two systems use the same package format doesn’t necessarily mean that packages for the two systems are interchangeable. Red Hat and SUSE both use RPM, for example, but their filesystem layouts are somewhat different. It’s best to use packages designed for your particular system if they are available.

Table 1.5 Sysadmin resources on the web

<table>
<thead>
<tr>
<th>Web site</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blogs.sun.com</td>
<td>Great collection of technical articles, many Solaris-related</td>
</tr>
<tr>
<td>cpan.org</td>
<td>Authoritative collection of Perl modules</td>
</tr>
<tr>
<td>freshmeat.net</td>
<td>Large index of Linux and UNIX software</td>
</tr>
<tr>
<td>kernel.org</td>
<td>Official Linux kernel site</td>
</tr>
<tr>
<td>linux.com</td>
<td>Linux forum, good for new users&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>linux.org</td>
<td>General Linux information clearing house</td>
</tr>
<tr>
<td>linux.slashdot.org</td>
<td>Linux-specific arm of tech news giant Slashdot</td>
</tr>
<tr>
<td>linuxhq.com</td>
<td>Compilation of kernel-related info and patches</td>
</tr>
<tr>
<td>lwn.net</td>
<td>Linux and open source news service</td>
</tr>
<tr>
<td>lxe.com</td>
<td>Linux news aggregator</td>
</tr>
<tr>
<td>rootvg.net</td>
<td>AIX-oriented site with lots of links and good forums</td>
</tr>
<tr>
<td>securityfocus.com</td>
<td>General computer security info</td>
</tr>
<tr>
<td>serverfault.com</td>
<td>Collaboratively edited database of sysadmin questions</td>
</tr>
<tr>
<td>ServerFiles.com</td>
<td>Directory of network admin software and hardware</td>
</tr>
<tr>
<td>slashdot.org</td>
<td>Tech news in a variety of categories</td>
</tr>
<tr>
<td>solariscentral.org</td>
<td>Open blog with Solaris-related news and articles</td>
</tr>
<tr>
<td>sun.com/bigadmin</td>
<td>Sun-specific aggregation site for admin info</td>
</tr>
<tr>
<td>sunhelp.org</td>
<td>Very nice collection of Sun-related material</td>
</tr>
<tr>
<td>ugu.com</td>
<td>UNIX Guru Universe – all things sysadmin</td>
</tr>
</tbody>
</table>

<sup>a</sup> This site is now run by the Linux Foundation.
Major Linux distributions provide excellent package management systems that include tools for accessing and searching Internet software repositories. Distributors aggressively maintain these repositories on behalf of the community, so there is rarely a need for Linux administrators to step outside the bounds of their systems’ default package manager. Life is good.

UNIX systems show more ambivalence about package management. Solaris, HP-UX, and AIX all provide packaging software that works at the level of individual machines. However, the vendors of these systems don’t maintain repositories of open source software, so the user communities are mostly left to fend for themselves. Unfortunately, one of the main pieces of glue that holds a packaging universe together is a way for packages to reliably refer to other packages in order to express dependency or compatibility information. Without some central coordination, the whole ecosystem can quickly fall apart.

In the real world, results have varied. Solaris has an add-on system (pkgutil from blastwave.org) that provides for easy software installation from an Internet repository, much like the native systems found on Linux distributions. HP-UX has a nice Internet repository in the form of the HP-UX Porting and Archiving Centre at hpux.connect.org.uk, but packages must be manually and individually downloaded. At the more dismal end of the spectrum, the availability of prepackaged software for AIX is somewhat scattershot.

Administrators without access to prepackaged binaries must install software the old-fashioned way: by downloading a tar archive of the source code and manually configuring, compiling, and installing it. Depending on the software and the operating system, this process can range from trivial to nightmarish.

In this book, we generally assume that optional software is already installed rather than torturing you with boilerplate instructions for installing every package. If there’s a potential for confusion, we sometimes mention the exact names of the packages needed to complete a particular project. For the most part, however, we don’t repeat installation instructions since they tend to be similar from one package to the next.

Determining whether software has already been installed

For a variety of reasons, it can be a bit tricky to determine which software package contains the component you actually need. Rather than starting at the package level, it’s easier to use the shell’s which command to find out if a relevant binary is already in your search path. For example, the following command reveals that the GNU C compiler has already been installed on this machine:

```
  aix$ which gcc
  /opt/pware/bin/gcc
```

9. OpenSolaris does offer a Linux-quality package management system and Internet repository. This feature does not exist in Solaris 10, but it’s likely to be featured in Solaris 11.
If **which** can’t find the command you’re looking for, try **whereis**; it searches a broader range of system directories and is independent of your shell’s search path.

Another alternative is the incredibly useful **locate** command, which consults a precompiled index of the filesystem to locate filenames that match a particular pattern. **locate** is part of the GNU **findutils** package, which is included by default on most Linux systems but must be installed by hand on UNIX.

**locate** is not specific to commands or packages but can find any type of file. For example, if you weren’t sure where to find the **signal.h** include file, you could try

```
ubuntu$ locate signal.h
/usr/include/signal.h
/usr/include/asm/signal.h
/usr/include/asm-generic/signal.h
/usr/include/linux/signal.h
...
```

**locate**’s database is updated periodically by the **updatedb** command, which runs out of **cron**. Therefore, the results of a **locate** don’t always reflect recent changes to the filesystem.

If you know the name of the package you’re looking for, you can also use your system’s packaging utilities to check directly for the package’s presence. For example, on a Red Hat or SUSE system, the following command checks for the presence (and installed version) of the Python scripting language:

```
redhat$ rpm -q python
python-2.4.3-21.el5
```

### Adding new software

Adding new software

If you do need to install additional software, you first need to determine the canonical name of the relevant software package. For example, you’d need to translate “I want to install **locate**” to “I need to install the **findutils** package,” or translate “I need **named**” to “I have to install BIND.” A variety of system-specific indexes on the web can help with this, but Google is usually just as effective. For example, a search for “locate command” takes you directly to several relevant discussions. If you’re on a UNIX system, throw in the name of the operating system as well.

Once you know the name of the relevant software, you can download and install it. The complete installation is usually a single command on Linux systems and on Solaris systems that have **pkgutil** installed. For HP-UX and AIX you’ll have to download either a prebuilt binary package or the project’s original source code. If the latter, try to locate the project’s official web page through Google and download the source code from one of the project’s mirrors.

The following examples show the installation of the **wget** command on each of our example systems. It’s a nifty GNU utility that turns HTTP and FTP downloads into atomic commands—very useful for scripting. **wget** is installed by
default on each of our example Linux systems, but the commands shown below can be used for both initial installation and later updates.

Ubuntu uses APT, the Debian Advanced Package Tool:

```
ubuntu# apt-get install wget
Reading package lists... Done
Building dependency tree
Reading state information... Done
wget is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

The SUSE version is

```
suse# yast --install wget
<runs in a terminal-based UI>
```

The Red Hat version is

```
redhat# yum install wget
Loaded plugins: fastestmirror
... Parsing package install arguments
Package wget-1.10.2-7.el5.i386 is already installed and latest version
Nothing to do
```

On a Solaris system with `pkutil` already installed (see blastwave.org for instructions on setting this up)

```
solaris# /opt/csw/bin/pkutil --install wget
<multiple pages of output as seven packages are installed>
```

For HP-UX, we found an appropriate binary package on hpux.connect.org.uk and downloaded it to the `/tmp` directory. The commands to unpack and install it were

```
hpux# gunzip /tmp/wget-1.11.4-hppa-11.31.depot.gz
hpux# swinstall -s /tmp/wget-1.11.4-hppa-11.31.depot wget
====== 05/27/09 13:01:31 EDT BEGIN swinstall SESSION (non-interactive) (jobid=hpux11-0030)
  * Session started for user "root@hpux11".
  * Beginning Selection
  * Target connection succeeded for "hpux11:/".
  * Source: /tmp/wget-1.11.4-hppa-11.31.depot
  * Targets: hpux11/
  * Software selections:
    wget.wget-RUN,r=1.11.4,a=HP-UX_B./800
  * Selection succeeded.
  * Beginning Analysis and Execution
  ...
  * Analysis and Execution succeeded.
  ...
```
Building software from source code

The package depot on the `swinstall` command line must be specified as a full path starting with `/`; otherwise, `swinstall` tries to find the file on the network. The `wget` at the end tells `swinstall` which package to install from within the depot file.

Unfortunately, the installation is not really as easy as it first appears. The installed version of `wget` won't actually run because several of the libraries on which it depends have not been installed:

```
hpux$ wget http://samba.org/samba/docs/Samba3-HOWTO.pdf
/usr/lib/dld.sl: Can’t open shared library: /usr/local/lib/libcrypto.sl
/usr/lib/dld.sl: No such file or directory
[HP ARIES32]: Core file for 32 bit PA-RISC application
[HP ARIES32]: /usr/local/bin/wget saved to /tmp/core.wget.
```

`swinstall` does have some dependency management built in, but its abilities unfortunately do not extend to Internet repositories. You’ll have to read the fine print and install all the appropriate prerequisite packages (in this case, six more) to make things right.

Building software from source code

There is in fact at least one binary `wget` package available for AIX in RPM format. A Google search for “aix wget rpm” should turn up some good leads. After downloading, the installation command would be a simple

```
aix# rpm --install wget-1.11.4-1.aix5.1.ppc.rpm
```

But just for illustration, let’s build the AIX version of `wget` from the original source code.

Our first chore is to find the code, but that’s easy: the first Google result for “wget” takes us right to the project page at GNU, and the source tarball is just a link away. After downloading the current version into the `/tmp` directory, we unpack, configure, build, and install it:

```
aix# cd /tmp; gunzip wget-1.11.4.tar.gz
aix# tar xfp wget-1.11.4.tar
aix# cd wget-1.11.4
aix# ./configure --disable-ssl --disable-nls       # See comments below
configure: configuring for GNU Wget 1.11.4
checking build system type... rs6000-ibm-aix

... config.status: creating src/config.h
config.status: executing default commands
generating po/POTFILES from /po/POTFILES.in
creating po/Makefile
aix# make
<several pages of compilation output>
aix# make install
<about a page of output>
```
Chapter 1 Where to Start

This configure/make/make install sequence is common to the majority of UNIX and Linux software and works on all systems as long as you have the development environment and any package-specific prerequisites installed. However, it's always a good idea to check the package's INSTALL or README file for specifics.

In this case, the --disable-ssl and --disable-nls options to configure omit some wget features that depend on other libraries that haven't been installed. In real life, you'd probably want to install the prerequisites. Use configure --help to see all the configuration options. Another useful configure option is --prefix=directory, which lets you put the software somewhere other than /usr/local.

1.13 System Administration Under Duress

System administrators wear many hats. In the real world, they are often people with other jobs who have been asked to look after a few computers on the side. If this is your situation, tread carefully and be aware of how this scenario tends to play out over the long term.

The more experienced you become at system management, the more the user community comes to depend on you. Networks invariably grow, and administrative work tends to accumulate over time as your administration system becomes more sophisticated and you add additional layers. You will soon find that you are the only person in your organization who knows how to perform a variety of important tasks.

Once coworkers come to think of you as the local system administrator, it is difficult to extricate yourself from this role. That is not necessarily a bad thing, but we know several people who have changed jobs to escape it. Since many administrative tasks are intangible, you may also find that you're expected to be both a full-time administrator and a full-time engineer, writer, or analyst.

There is a common tendency for unwilling administrators to fend off requests by adopting a surly attitude and providing poor service. This approach usually backfires; it makes you look bad and creates additional problems.

Instead, consider keeping detailed records of the time you spend on system administration. Your goal should be to keep the work at a manageable level and to assemble evidence that you can use when you ask to be relieved of administrative duties. In most organizations, you will need to lobby the management from six months to a year to get yourself replaced, so plan ahead.

On the other hand, you may find that you enjoy system administration and that you prefer it to real work. Employment prospects remain good. Unfortunately, your political problems will probably intensify. See Chapter 32, Management, Policy, and Politics, for a preview of the delights in store.

10. A tendency lovingly and sadistically documented in Simon Travaglia’s Bastard Operator from Hell stories; see bofh.ntk.net for the archive. (Look under BOFH.)
1.14 RECOMMENDED READING


SALUS, PETER H. *The Daemon, the GNU & the Penguin: How Free and Open Software is Changing the World*. Reed Media Services, 2008.

This fascinating history of the open source movement by UNIX’s best-known historian is also available at groklaw.com under the Creative Commons license. The URL for the book itself is quite long; look for a current link at groklaw.com or try this compressed equivalent: tinyurl.com/d6u7j.


System administration


This is a good book with particularly strong coverage of the policy and procedural aspects of system administration. The authors maintain a system administration blog at everythingsysadmin.com.


This is a classic all-around guide to UNIX system administration that is sadly somewhat out of date. We hope a new version is in the works!

Essential tools


Chapter 1 Where to Start


This book is also available for free on the web at diveintopython.org.


This book, optimistically subtitled Everything You Need to Know, is unfortunately a bit on the dry side. However, it covers the Ruby 1.9 release and includes a wealth of detail that only the language designer is really in a position to know. Best for those who already have a working knowledge of Perl or Python.

1.15 Exercises

E1.1 What command would you use to read about the terminal driver, tty (not the tty command)? How would you read a local tty man page that was kept in /usr/local/share/man?

E1.2 Does a system-wide config file control the behavior of the man command at your site? What lines would you add to this file if you wanted to store local material in /doc/man? What directory structure would you have to use in /doc/man to make it a full citizen of the man page hierarchy?

☆ E1.3 What is the current status of Linux kernel development? What are the hot issues? Who are the key players? How is the project managed?

☆ E1.4 Research several UNIX and Linux systems and recommend an operating system for each of the following applications. Explain your choices.
   a) A single user working in a home office
   b) A university computer science lab
   c) A corporate web server
   d) A server cluster that runs the database for a shipping company

☆ E1.5 Suppose you discover that a certain feature of Apache httpd does not appear to work as documented on Ubuntu.
   a) What should you do before reporting the bug?
   b) If you decide that the bug is real, whom should you notify and how?
   c) What information must be included to make the bug report useful?

★★ E1.6 Linux has made dramatic inroads into production environments. Is UNIX doomed? Why or why not?
You might think that a book about system administration would be the last place to find a chapter on environmental and social consciousness. But now that large IT installations have become commonplace, the environmental impact and resource consumption of the equipment we oversee have started to attract attention. Green IT is the art and science of reducing these hidden and not-so-hidden costs.

Although each of us can make a difference through small changes in our choices and behavior, most improvement comes from centrally driven efforts to effect change. For example, no amount of “Choose unleaded gasoline! It’s a whole lot better!” would have equalled the impact of the federal mandate to stop producing cars that required lead. Guess who can set similar mandates for your IT organization? You can!

But why bother? Bragging rights and the satisfaction of doing the right thing for the planet may be reason enough for some. But there are practical reasons to convince decision-makers in your organization to consider a green IT effort as well:

- **Lower initial costs** – by minimizing the equipment that your organization buys and uses, you reduce capital expenditures. By minimizing the size of the data center required, you can reduce real estate costs.
Chapter 28  Green IT

- **Lower operating costs** – power, management, and maintenance for equipment cost money over time. Efficient use of fewer pieces of equipment means that your organization spends less on the direct costs of operations.

- **Indirect cost savings** – you pay for electricity twice: once to power your equipment, and then again to cool down the equipment after it has converted that expensive power into heat. Less equipment means less cooling, less square footage for IT projects, and fewer people dedicated to IT operations. Fewer people means less spent on rent, office cooling, wages, benefits, and support.

This chapter focuses on some basic concepts you can use to reduce your IT organization's energy and resource consumption. We've targeted organizations that have from 1 to 500 servers in their data centers. If your environment is larger, you should consider hiring an expert in green data-center construction to achieve the most dramatic results.

### 28.1 Green IT Initiation

What exactly does it mean to be "green"? We define it as

- Lower power consumption
- Smaller physical plant requirements
- Lower consumption of consumables
- Recyclable outputs

There is no silver bullet or single path to a green IT environment. Despite some vendors' claims, you cannot purchase one product that makes all the greenness in the world shower down upon you. Specifically, green IT is a lot more than just server virtualization. And, like so many aspects of system administration, green IT is more a journey than a destination. You must first visualize where you want to go, map out a plan to get there, and chart your progress along the way. Ongoing measurement and monitoring must be key elements of your overall plan.

Start your green IT journey by assessing the eco-friendliness of your current environment. Take a comprehensive view of all IT within your organization, not only to maximize the project's impact but also to ensure that you don't ultimately end up playing the "squeeze the balloon" game. For example, it might seem eco-wonderful to remove *all* the servers from your environment until you discover that eliminating your 50 managed servers has resulted in users purchasing and deploying 600 rogue server-class systems in their cubicles as part of a "personal server deprivation revolt."

---

1. The informational work done by IT equipment is not significant in a thermodynamic sense. Computers are essentially 100% efficient at converting electricity into heat.
Here is some information to gather as you start your green IT assessment:

- **Equipment survey** – everything, including servers, laptops, workstations, monitors, printers, storage devices, network gear, backup devices, UPSs, and cooling units. Capture the location, model number, “size” (in units appropriate to the specific equipment), and age of each item. It’s helpful to have power consumption data for each item as well. Rated power consumption can be misleading—better to measure a device’s actual energy use with a Kill A Watt meter, which costs around $20.\(^2\) For devices that have both active and sleep states (e.g., printers), you may want to record average energy use over a one-day or one-week period.

- **Accounting of consumables** – paper, toner, storage media

- **Organizational metrics** – including gross revenue, number of employees, number of physical locations, total facility energy consumption, IT equipment energy consumption (in data centers), data center cooling energy consumption, total IT capital cost, total IT operations cost, and total facilities costs for data centers.

Once you’ve collected this baseline data, identify one to three targets for optimization. These targets should be tied to your organization’s overall strategy for success and growth, and if achieved, they should also demonstrate progress toward becoming a greener IT shop. We can’t tell you what targets will work best for your environment, but here are some appropriate examples:

- Data center energy consumption per dollar of gross revenue
- Number of employees per physical server
- Sheets of paper used per employee per month
- Average energy consumption of an employee’s workspace equipment
- Average life of a laptop computer
- Data center energy use as a proportion of total facility use\(^3\)

Plan to reassess your green IT status at least yearly, but review energy consumption monthly.

### 28.2 The Green IT Eco-Pyramid

It’s easy to see how eco-unfriendly your organization is. The hard part is making (and monitoring) progress toward the goal of being green. To help you navigate the sea of choices presented in this chapter, we map green IT strategies into three divisions, as shown in Exhibit A on the next page.

\(^2\) This product is designed for the North American market, but similar products exist for other markets. A version made for the UK can be found at reuk.co.uk/Buy-UK-Power-Meter.htm.

\(^3\) This metric multiplied by 100 yields the percentage of facility power delivered to IT equipment and is known in the industry as “DCiE.” It is a standard metric that can be used to compare organizations. Power usage effectiveness (PUE) is the reciprocal of DCiE and is a common benchmark for very large data centers.
Chapter 28 Green IT

Exhibit A  Approaches to green IT

We show these categories in the form of a pyramid because the strategies at the bottom have the most significant impact and are most likely to provide secondary benefits. As you go up the pyramid, the strategies involve more cost and effort and tend to be less effective.

Reducing direct consumption should always be your first-choice strategy; less is more. If you can achieve your mission with less effort and fewer resources, that eliminates both capital and operational costs.

Mitigation of secondary consumption is the next best strategy. For example, the cooling needed to support a server counts as secondary consumption since it only occurs because the server exists in the first place. Optimizing the HVAC system to minimize cooling expenses saves money, but it doesn’t save as much as eliminating the server entirely.

Perhaps somewhat nonintuitively, choosing products and technologies that have been designed to be “green” is our lowest-value strategy. Think of it this way: we first reduce the number of cars on the road as much as possible, and only then do we replace the remaining cars with fuel efficient models.

28.3 Green IT strategies: data center

Data centers are excellent targets for green IT initiatives because they typically operate $7 \times 24 \times 365$ and are under the direct control of the IT group. A study by Lawrence Berkeley Laboratories showed that data centers can be as many as 40 times more energy-intensive than conventional office space.4

At this level of consumption, special strategies are required. As shown in Exhibit B, the strategies to reduce direct consumption at the bottom of the pyramid are

---

the most effective approaches. You don’t need to use every strategy in a given environment, but every little bit counts.

**Exhibit B  Green IT strategies for data centers**

Application consolidation

Over time, organizations and IT departments tend to accumulate applications. New applications come onboard to support specific business initiatives and the CEO’s pet projects, but old applications rarely die. More commonly, they linger “on the road to retirement” for a decade with no one being willing to take the risk of pulling the plug. Whatever the reason, the number one opportunity for progress in an established organization is to consolidate applications to the minimum set that meets current business needs.

Let’s consider an example organization that has three applications: EmployeeLinq, AccountAwesome, and ElectricClockster. Although this is a simplified example, it’s loosely based on real-world applications used by one organization that we examined. Each of the applications had a back-end database server, an application server, and a web front-end server. That’s a total of nine servers to support these three applications.

The first step toward consolidation is to map out the functions provided by each application. Table 28.1 on the next page shows the features of our example apps. As you can see, there’s quite a bit of overlap.

This organization had three systems that could be (and were!) used to track time, two systems that could do payroll (though only one was currently in use), and many other overlapping functions.

This situation came to pass because three different departments—Finance, Human Resources, and Operations—had each chosen their own application. Not only does this lack of coordination waste energy and computing resources, but it
also complicates or forestalls integration of data among departments. In this case, moving the organization to a single application trimmed software, hardware, and energy costs by over 60% and resulted in smoother data flow within the company.

Your situation is probably not this dramatic, but if you take the time to map out your application domains, chances are that you’ll find some significant overlap. The business case for consolidating applications is easy to make because the projected results can (at least in part) be expressed in dollars saved. Data integration and operational improvements are just icing on the cake.

**Server consolidation**

Most organizations have at least a few “single purpose” servers that operate at 10% utilization or less. For example, we’ve seen many organizations that have dedicated NTP (network time protocol) servers. NTP is a low-overhead protocol that requires very little computational effort. Reserving a server for NTP is like flying a Boeing 767 cross-country with only one passenger.

Server consolidation is a close cousin of application consolidation and is equally effective. Instead of bundling multiple functions into one application, you bundle multiple services onto one server machine.

Unlike Windows, UNIX and Linux excel at preemptive multitasking. A good solution in the NTP case is to run the NTP daemon on the same servers that provide common infrastructural services such as DNS and Kerberos.5

Another common opportunity for server consolidation is presented by database servers that are dedicated to a single application. If you have competent sysadmins and DBAs (and good monitoring), a single database server should be able to host the databases for many applications. Once again, this consolidation reduces license fees, capital costs, and energy consumption.

---

5. NTP is a special case in that its response latency must be kept low. However, that doesn’t mean you can’t run other services on the same machine. NTP server daemons are commonly **nice**d to give them ready access to the CPU whenever they want it (see page 129). You can achieve similar ends—perhaps even a bit more reliably—through server virtualization.
In some cases, you may be able to reduce the number of servers you need by replacing old, less powerful servers with a smaller number of new, more powerful, and more energy-efficient servers.

**SAN storage**

One common indicator of IT gluttony is a fleet of servers that are loaded up with hard disks. For example, imagine a data center that has 100 servers, each with six 1TB disks. That’s 600 disks that must be manufactured, maintained, powered, and eventually scrubbed and disposed of. The likelihood that these drives’ average utilization exceeds 50% is virtually nil.

This approach results in excessive waste because it chops the storage into discrete chunks that cannot be efficiently managed to make “just the right amount” of storage available to each server or application. Some servers may have less than 1TB of actual data in play while others are underprovisioned at 6TB and unable to benefit from the idle drives in their neighbor’s chassis. The reality is that it’s hard to push much above 30% storage utilization in a typical data center that has discrete storage for each server.

A good alternative to this approach is a storage area network or SAN; see page 274 for more details. SAN technology provides highly reliable storage that is also eco-friendly because sysadmins can allocate the centralized storage space efficiently. Many organizations exceed 90% utilization on their SANs. That’s triple the efficiency of discrete storage. Now that SANs can run on Ethernet, there is no longer any major hardware hurdle to deploying this wonderful tool.

**Server virtualization**

Server virtualization seems to be everyone’s favorite topic in the green IT arena, although some of the current buzz is probably fueled by the marketing dollars of the companies selling virtualization platforms.

Server virtualization (covered in detail in Chapter 24) is in fact a fantastic tool. Its eco-impact is similar to that of server consolidation. In both approaches, several applications or services end up running on a single computer. Virtualization reduces energy consumption by reducing the number of chassis in production and achieving higher utilization of the remaining units.

Virtualization offers some additional features that are not provided by consolidation, such as the ability to easily scale out identical systems, the ability to reserve a portion of the hardware’s capacity for a given server, and the ability to migrate virtual servers among physical chassis. Those aspects of virtualization are a win.

Virtualization also has a dark side. Applications that are I/O intensive typically do not virtualize well and tend to be more sluggish in a virtualized environment. The virtualization process itself consumes resources, so virtualized systems have overhead that physical systems do not. The additional layers of abstraction introduced by virtualization require constant vigilance on the part of system administrators,
both because the virtualization itself must be actively managed and because virtualization may affect the operation of the hosted systems.

Virtualization is best employed in environments that have adequate IT staff and mature processes. At this point, we don't really recommend server virtualization for beginning sysadmins. However, the technology is rapidly becoming more reliable and easier to use. Soon, it will be inescapable.

**Only-as-needed servers**

Only-as-needed servers are powered down when not in use. This approach works best in cases where the demand for computing power is predictably cyclical; for example, when the server is linked to the accounting cycle or to work that is only done in the wee hours of the morning. This isn't a common technique, but every once in a while there's a green IT savings opportunity so special that only this trick fits.

You can roll your own implementation with some scripts and Ethernet-connected (managed) power strips. Platforms such as RightScale (rightscale.com) extend the concept into demand-based territory. Using systems such as this, you can set thresholds at which additional servers are automatically spun up (or spun down) according to metrics such as CPU load or transaction volume.

**Granular utilization and capacity planning**

In green IT, as in other areas, you can only manage what you can measure. Careful data collection is an essential tool for optimizing your environment.

If you track your site's use of resources such as CPU and memory (see Chapter 29, *Performance Analysis*), you can plan your hardware deployments so that you don't have to buy overprovisioned servers "just to make sure" your capacity is sufficient. Monitoring and analysis take time, but they're an excellent basis for "lean and mean" data center management.

Buy only what you need; use only what you must.

**Energy-optimized server configuration**

Some systems give you the opportunity to save energy by altering the behavior of the system itself.

*Power-saving options for Linux*

CPUs and CPU cores can be idled to reduce their power consumption. To achieve the lowest possible power consumption, you pack as many threads as possible onto one core or CPU and do not activate additional cores or CPUs until they are needed. Conversely, to achieve the best possible performance, you distribute threads as widely as possible among cores and CPUs to minimize the time-costs of context switching and cache contention. In theory, you must trade away some performance to reduce power consumption.
In practice, the opportunity to idle parts of the CPU only arises when the system isn’t busy. In those circumstances, the additional overhead of packing threads onto one core may have no detectable effect. Experiment to see if you can discern any difference with your specific workload.

The process scheduler’s power management system consults two control variables, both of which are set through files in the /sys/devices/system/cpu directory. The sched_mc_power_savings variable controls whether all cores on a CPU are used before activating another CPU, and the sched_smt_power_savings variable controls whether all thread slots on a core are used before activating another core. In both cases, a value of 0 turns power saving off and a 1 turns it on.

For example, to turn on both power-saving modes, you could use the commands

```bash
$ sudo sh -c 'echo 1 > /sys/devices/system/cpu/sched_mc_power_savings'
$ sudo sh -c 'echo 1 > /sys/devices/system/cpu/sched_smt_power_savings'
```

To make these changes persistent across reboots, check out the sysctl command or add the lines to a startup script such as /etc/init.d/local on Ubuntu or SUSE (create it if necessary) or /etc/rc.local on Red Hat.

A computer’s CPU is one of its most profligate consumers of energy (just look at those heat sinks!), so aggressive power management can significantly reduce the system’s power use.

**Filesystem power savings**

You can save power and increase performance by preventing filesystems from maintaining a “last access” time (st_atime) for every file. This information isn’t very useful, and it theoretically adds a tax of one seek and one write to every file operation. (The real-world impact is harder to quantify because of block caching.)

Zedlewski et al. analyzed hard disk power consumption in a 2003 paper and concluded that seeks cost about 4 millijoules each on an IBM Microdrive; the cost is probably at least double that for a standard drive with its larger armature. Combining the cost of seeks with the cost of writes, we calculate the benefit of disabling last access times to be up to several kWh per drive per year. Not a huge savings, but probably worthwhile for the performance benefits alone; the energy savings are just gravy.

On most filesystems, you can turn off maintenance of the last access time with the noatime option to mount:

```bash
$ sudo mount -o remount,noatime  /
```

Some Linux systems also support the relatime mount option, which provides hybrid functionality. Under this option, last access time is only updated if the previous value is earlier than the file’s modification time. This mode allows tools such as mail readers to correctly identify cases in which an interesting file has been changed but not yet read.
Cloud computing

Take a deep breath, and think outside the box—outside the box of your data center, that is. The recent availability of "cloud computing" has brought many benefits, but one worth mentioning here is energy efficiency. In their quest to provide low-cost, high-reliability services, providers like Amazon have constructed ultra-high-efficiency data centers and utilization management processes. These cloud providers can supply compute cycles that are more eco-friendly than you could ever achieve in your own data center.

If you have applications (especially web applications) that don't absolutely have to live under your own roof, consider outsourcing their infrastructure to a cloud data center. You still have complete administrative control of the virtual systems that run in this environment. You just never get to physically "hug" them.

Free cooling

Nothing is more disturbing on a cold winter's day than to walk outside a data center and see the compressor pad whirling away at full speed. It's 10 degrees outside, but the HVAC engineer apparently designed a system that uses mechanical cooling (and an amazing amount of energy) to pull heat out of the data center regardless of the ambient temperature.

Fortunately, some modern HVAC engineers specialize in data centers and have a better solution to this problem: use outside air for cooling when the temperature is low enough.

Of course, this solution isn't available everywhere or in every season. The Green Grid, a consortium of technology companies dedicated to advancing energy efficiency in data centers, now produces "free cooling" maps for North America and Europe that illustrate how many hours a year a center can be cooled by outside air in a given area. A more detailed on-line cooling calculator is also available—check it out at thegreengrid.org.

Efficient data center cooling

Various tricks of data center design can be used to reduce the amount of energy used for cooling. For example, the hot aisle/cold aisle layout described on page 1089 concentrates cooling where it is most needed and allows other parts of the data center to operate at higher temperatures.

See Chapter 27, Data Center Basics, for a broader discussion of some of these tips.

Degraded mode for outages

Many organizations are obsessed with availability (aka uptime). What often aren't considered are the additional energy and resources used to ensure a particular level of availability.
Equipment life extension

Internal customers are accustomed to thinking of services as being either up or down. Consider offering degraded service as an additional choice for fault management, and ask whether that might meet the customers’ availability needs.

For example, instead of running a fully redundant set of equipment for every production environment, you could use server virtualization to deploy several applications to a single chassis in the event of an outage. This configuration might supply all the standard functionality, but at slower speed than normal. In some cases, this tradeoff can reduce the organization’s capital costs by 50% or more.

Equipment life extension

Electronics manufacturing consumes energy and generates toxic waste, so purchases of new equipment entail an environmental cost that isn’t necessarily reflected in the price tag. Unfortunately, the technology industry has become so accustomed to rapid innovation and product development that manufacturers often discontinue support for equipment after just a few years.

If your current equipment meets your business needs and is reasonably energy efficient, you may want to consider a life extension strategy. Such a scheme typically involves scouring eBay and other sources of salvage equipment for similar systems you can acquire cheaply and bring to your site as a source of vintage spare parts. This approach typically extends system life by two to three years, though in at least one case we have kept a system running eight extra years this way.

If older equipment is not meeting performance requirements or cannot be supplemented by on-site spares, another option is to buy new equipment for the production environment and reassign the current equipment to a development environment, where performance and reliability are not as important. This approach doesn’t avoid new purchases entirely, but it may delay purchases for the development environment for a year or two.

If equipment simply must be retired, make sure that you turn it over to a legitimate computer recycler who will break it down into component pieces and recycle each piece appropriately. Make sure the recycler has a certified data destruction program so that your data doesn’t later show up in someone else’s hands.

Computers contain a surprising amount of toxic waste. Whatever you do, don’t just throw old equipment into the dumpster—that waste typically goes to a landfill not designed to handle electronics.

Some regions have organizations that provide computer recycling services for free. In the Portland, Oregon, area, freegeek.org is a model recycling program.

---

6. If your current equipment is not energy efficient, you may be better off replacing it immediately to achieve operational energy savings, even when disposal and replacement costs are considered.
Warmer temperature in the data center
Approximately one-third of the energy consumed in a traditional data center goes to support cooling. Historically, data centers have maintained temperatures in the range of 68–77 degrees Fahrenheit. These values are now seen as conservative.

In early 2009, the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) issued guidance that an expanded range of 64.4–80.6 degrees Fahrenheit is acceptable for data centers. Raising the data center temperature by three degrees typically saves an estimated 12% in cooling costs.

See Chapter 27, *Data Center Basics*, for additional cooling tips.

Low-power equipment
When procuring new equipment, take the time to select products that have minimal environmental impact.

The IEEE has standardized the criteria for environmental assessment of electronics in IEEE publication 1680. One evaluation system based on IEEE P1680, the Electronic Products Environmental Assessment Tool (EPEAT), considers a wide range of potential impacts that might be involved in a product's manufacture. It can help you compare products uniformly. The system currently covers desktop and laptop computers, thin clients, workstations, and computer monitors. It is required for U.S. federal government purchases. Visit EPEAT at epeat.net.

Note that EPEAT compliance requires conformance to Energy Star standards (in version 5.0 as of July 1, 2009) for energy consumption during use.

Some server manufacturers (including Dell, Sun, IBM, and HP) offer environmentally focused product families. But even eco-friendly servers have an environmental impact and consume power. The existence of these product lines should not be viewed as a license to add equipment in the name of being green. Focus first on reducing the number of servers that you need, then pick the most eco-friendly option for meeting that need.

28.4 Green IT strategies: user workspace
Staff work areas present another set of opportunities to green up your operations. Exhibit C summarizes some improvements to consider.

Below are listed workspace arenas in which green IT can be a player. Most of the accompanying suggestions are straightforward, and you'll find many of them familiar from other sources. (Chances are that you're already doing some of them.)

- User education – encourage users to power off equipment that's not needed, to think before they print documents, and to let desktop equipment go into a power-saving mode instead of running a screen saver (or, better yet, turn it off).
Green IT strategies: user workspace

Exhibit C  Green IT strategies for the workspace

- **Monitors** – replace CRTs with LCD monitors. They use significantly less power and contain fewer toxic elements.

- **Workstation idle** – centrally configure workstations to “sleep” or power-off when idle for a given period (e.g., 30 minutes).

- **Workstation count** – limit desktop workstations to one per user. Users who claim to need more than one workstation should be encouraged to use a desktop virtualization client.

- **Task-based sizing** – don’t buy “one size fits all” workstations. Have three or four tiers of workstation specifications so that users have the appropriate configuration for their task mix.

- **Personal heaters** – this is not really an IT topic per se, but it’s a pet peeve of ours, and the IT department is usually the one to notice. Do not allow the use of personal space heaters in users’ offices or cubicles. Explain to users that such heaters feed a vicious cycle in which the office HVAC and the heater fight in an effort to enforce different temperature targets. If the user’s work area is truly the wrong temperature, escalate the issue with the appropriate HVAC support team. (Maybe you can offer them some VIP IT support in exchange for their assistance.)

- **Print duplexing** – configure printers to default to double-sided, two-up printing. This works fine for most routine printing, and users can always select something other than the default for special cases.

- **eDocument campaign** – launch a campaign or contest within your organization to find ways to eliminate the use of printed documents.

- **Office temperature** – since office computing equipment is designed to work at much higher temperatures than humans are, raise that office cooling setting to 78°F or higher.
• **Equipment recycling** – once or twice a year, hold equipment recycling days during which staff can pile up their unwanted, unused, or underutilized equipment for your favorite recycling company to haul off. If you’re really eco-friendly, let staff add equipment from home to the pile.

• **Equipment life extension** – once a workstation has become too old or too slow to be used by staff with the most intense computing demands, cycle it down to staff who have lower requirements. They’ll see it as an upgrade, and you’ll squeeze another year or two of life out of it.

• **Workplace recycling** – start a workplace recycling program for used paper. Many recycling companies also accept office plastics (soda bottles, etc.) in the same stream.

• **Recycled paper and printer cartridges** – become a consumer of recycled goods. Purchase 100% recycled paper for your printers and copiers, and buy recycled toner cartridges as well. We’ve had outstanding luck with Boise Aspen 100 as general-purpose recycled printer paper that’s inexpensive and has outstanding ecological characteristics.

• **Telecommuting** – encourage staff to telecommute one or more days per week by installing and supporting technologies that facilitate remote access, such as VPNs, VOIP service at home, and web-available applications. In addition to the benefits for the staff involved, telecommuting reduces the use of transportation and office support services. Make sure, though, that telecommuters turn off their equipment at whichever site they’re not occupying on a given day. Otherwise, this policy can backfire, at least from an energy conservation perspective.

### 28.5 Green IT Friends

If you’re looking to do even more in the green IT space, you can find both camaraderie and guidance from a variety of organizations and resources. Table 28.2 lists some of the groups that we’re familiar with and recommend.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Web site</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy Star</td>
<td>energystar.gov</td>
<td>Consumer product standards</td>
</tr>
<tr>
<td>EPEAT</td>
<td>epeat.net</td>
<td>Green electronics manufacturing</td>
</tr>
<tr>
<td>French Green IT</td>
<td>greenit.fr</td>
<td>French Green IT blog</td>
</tr>
<tr>
<td>Green IT Observatory</td>
<td>greenit.bf.rmit.edu.au</td>
<td>Australian green IT research</td>
</tr>
<tr>
<td>Green IT Promo Council</td>
<td>greenit-pc.jp</td>
<td>Green IT for Japan and Asia</td>
</tr>
<tr>
<td>Green Standards Trust</td>
<td>greenstandards.org</td>
<td>Office equipment recycling</td>
</tr>
<tr>
<td>IT Industry Council</td>
<td>itic.org</td>
<td>General best practices for IT</td>
</tr>
<tr>
<td>Less Watts</td>
<td>lesswatts.org</td>
<td>Saving power with Linux</td>
</tr>
<tr>
<td>The Green Grid</td>
<td>thegreengrid.org</td>
<td>Data center focus</td>
</tr>
</tbody>
</table>
In addition to stockpiling green ideas, many of these organizations have their own sets of benchmark data that you can use to find out how your organization compares with others of similar size and activity.

28.6 Exercises

E28.1 Use a Kill A Watt meter to measure the power consumption of your desktop workstation under various load conditions, including sleep mode or power-save mode. How much power would be saved if you turned your workstation off every night?

E28.2 Write a script that emails the system administrator when CPU load indicates that a new server should be spun up.

E28.3 Make a list of the main applications that your organization uses today. Which ones have overlapping functionality?

E28.4 Visit thegreengrid.org and determine if your location could benefit by using outside air for cooling.

★ E28.5 Organizations such as TerraPass and Carbonfund.org sell CO2 "offsets" through which organizations can compensate for their carbon emissions. For example, one common strategy used by offsetters is to subsidize the development of carbon-neutral energy sources (e.g., solar and wind power), with the goal of reducing future emissions.

These programs have proved controversial. Some observers doubt the reality of the claimed emission reductions, while others question the programs on philosophical grounds.7

Select a specific carbon offset provider and assess the plausibility of the strategies it is pursuing. Are the programs sufficiently well documented that you could make your own evaluation of their quality? Has any impartial group evaluated this provider, and if so, what were their conclusions?

7. WordPress developer Mark Jaquith wrote, “It’s like killing a person, and then convincing a murderer to kill one less person. You didn’t negate your murder. You still killed the person. Convincing someone else to reduce their emissions doesn’t make up for your emissions.” We don’t necessarily endorse this view, but it is representative the anti-offset perspective.
We have alphabetized files under their last components. And in most cases, only the last component is listed. For example, to find index entries relating to the /etc/mail/aliases file, look under aliases. Our friendly vendors have forced our hand by hiding standard files in new and inventive directories on each system.
aliases, email continued
file format 757
hashed database 760
loops 758
and mailing lists 760–761
network distribution 290
for new users 178
postmaster 757
aliases.db file 760
alien command 382
Allman, Eric 344, 779
allow-update clause, DNS 613, 641
Alpine mail client 745
always_add_domain feature, sendmail 785
Amanda backup system 335
amavisd.conf file 771
amavisd-agent command 772
amavisd-nanny command 772
amavisd-new 769–773
configuration 771–772
DKIM 489
use with Exim 826
installation 771
monitoring 772
use with Postfix 842–843
use with sendmail 794–795
tools 772–773
Amazon web services 978, 1005–1009, 1106
additional features 1009
Elastic Block Store 1006
Elastic Compute Cloud (EC2) 1005
ElasticFox 1009
installation and configuration 1006
instance termination 1009
Simple Storage Service (S3) 1006
AME backup tapes 302
American Power Conversion (APC) 1094
American Registry for Internet Numbers (ARIN) 461–462, 549
Anaconda 365
Analog Apache log analyzer 967
Anderson, Paul 409
annual failure rate (AFR) 211
Anvin, H. Peter 364
anycast 457, 603
Apache Software Foundation 19, 964
APC (American Power Conversion) 1094
APNIC 462
AppArmor 924
applications consolidating 1101
servers 960
virtualization 987
appropriate use policy (AUP) 1228
apropos command 17
APT (Advanced Package Tool) 24, 387–391
apt-get command 387–391
ARIN (American Registry for Internet Numbers) 461–462, 549
ARP (Address Resolution Protocol) 450, 455, 468–469, 491
arp command 469
ARPANET 448, 509
ASHRAE temperature range 1087, 1108
AT&T 12
AT&T UNIX System V 268
ATA interface 213–215
cables 215
power connector 215
secure erase 227–228
SMART reporting 230–231
TRIM command 228
ATA-over-Ethernet (AoE) 276
Athena, Project 1011
atime option, turning off 1105
Atkins, Todd 358
auditing 107
AUP (appropriate use policy) 1228
/etc/security/auth_attr file 108
authadmin command 108
Author Domain Signing Practice (ADSP) 572, 768
authorization, Solaris 108
authors, contacting xlvf
/etc/rbac/author file 108
auto_master file 712
auto.direct file 713, 716
Automated Installer, Solaris 375–376
automount direct maps 713
Linux 717
master maps 714
replicated filesystems 715
automount command 712–713
automounters
configuration 712–715
NFS and 711–715
replicated filesystems 715
Windows 1147
autonegotiation, Ethernet 539–540
autonomous systems 517–518
tools 772–773
Amazon web services 978, 1005–1009, 1106
additional features 1009
Elastic Block Store 1006
Elastic Compute Cloud (EC2) 1005
ElasticFox 1009
installation and configuration 1006
instance termination 1009
Simple Storage Service (S3) 1006
AME backup tapes 302
American Power Conversion (APC) 1094
American Registry for Internet Numbers (ARIN) 461–462, 549
Anaconda 365
Analog Apache log analyzer 967
Anderson, Paul 409
annual failure rate (AFR) 211
Anvin, H. Peter 364
anycast 457, 603
Apache Software Foundation 19, 964
302
see also Bacula
ADSM/TSM 336
Amanda 335
Bacula 318–335
commercial systems 335
dd command 316
dump restore command 308–314
EMC NetWorker 337
tar command 315–316
Veritas 336
backups 292–337
see also Bacula
see also media, backup
centralized 293
cloud services 303
compression 299
designing data for 298
encryption 295, 304
fitting on media 294
full restore 313–314
hints 293–298
Internet 303
interval between 294
off-site storage 295
programs 315–335
to removable disks 300
restoring 293, 310–315
schedules 305–307
security 295
setting up 307–314
Index

backups continued
snaps 296
for upgrades 314–315
when to make 296
for Windows 333
for ZFS filesystems 316

Bacula 318–335
architecture 319
bacula-dir.conf file 324–327
bacula-sd.conf file 327
bconsole.conf file 328
client file daemon 328
configuration files 321–329
installation 330
monitoring 334
restoring files 330–333
terms 322
Tips 334
troubleshooting 334–335
Windows clients 333
bad blocks, disk 227
Baretta, Anne 1177
bash shell 29
argument processing 40–42
arithmetic 47
basic use 30–33
best practices 73–74
command editing 30–31
file test operators 44
loops 45–46
pipes and redirection 31–32
scripting 37–48
search path 113
variables and quoting 32–33,
42–43
~/.bash_profile file 42, 189
.bashrc file 189
bastion hosts 796
BATV (bounce address tag validation) 756, 765
baud rate, tricks for determining 1181
BCP documents 450
BCPL (Basic Combined Programming Language) 1266
Berkeley DB library 308, 760, 782, 833
Berkeley Fast File System 254–255
Berkeley Internet Name Domain system see BIND
Berkeley see University of California at Berkeley
Berkeley Software Design, Inc. (BSDI) 1270
Bernstein, Dan 809
BGP protocol 516, 520–521, 523
bgpd daemon 523
/bin directory 146
BIND see also DNS
see also name servers
see also named
ACLs 643–644
address match lists 601
AIX 685–686
client configuration 561–563
components 600
configuration examples 618–624
configuration files 600–624
control programs 674
debugging 667–681
distribution-specific information 681–683
DNSSEC 573, 648–667
.key DNSSEC key file 646
dnssec-keygen command 646–647, 655
dnssec-signzone command 657, 660
dnssec-signzone command
657, 660
doc (domain obscenity control) 679–680
documentation 686, 688
forwarding zone, configuring 615
HP-UX 684–685
keys, generating 654
KSK (key signing key) 653
localhost zone configuration example 619
logging 612, 667–672
loopback address 616
master server, configuring 613
/etc/named directory 603
/etc/named.conf file 600–624,
643, 671
named-checkconf command 600, 648, 679
named-checkzone command 600, 679
notification options 603
differences from NSD 626
nsupdate command 641
performance 680
.private DNSSEC key file 646
query forwarding 606
BIND continued
/etc/resolv.conf file 561–562
RIPE DNSSEC tools 665
rndc command 638, 672, 674
/etc/rndc.conf file 616
/etc/rndc.key file 616
rndc-confgen command 616
root server hints 614
root.cache file 615
security 571
shell interfaces see dig and
nslookup
slave server, configuring 614
Solaris 684
split DNS 617–618, 620–623
statistics 676
stub zones, configuring 614
/etc/syslog.conf file 668
updating zone files 640–642
versions 597–599
zone transfers 564, 639–640
BIOSes 82
blackhole option, DNS 606
blacklists 766
in Exim 817–818
in Postfix 840–841
in sendmail 792
block device files 148, 150, 418
blocking factor, tape 315
bogus directive, DNS 611
boot command 429
boot loaders 79, 82–85
GRUB 85–86
multibooting 85
bootstrapping 78–81
device probing 79
directly to bash 92
from the network, non-PCs 364
from the network, PCs 363
fscck and 81
kernel initialization 79
kernel options 84
kernel threads 79
mounting NFS filesystems 708
multibooting 85
PC-specific issues 82
single-user mode 80–81, 88
startup scripts 87–100
/etc/sysconfig directory 92–93
Bostic, Keith 1270
Bourne shell 14
Bourne, Steve 1266
Bourne-again shell see bash
breakout boxes 1180
Bro network intrusion detection system 918
broadcast
addresses 480
directed 473, 508
domain 534
storms 480, 538
Bryant, Bill 925
BSD printing 1054–1065
see also printing
architecture 1054–1055
configuration 1059–1065
lpc command 1057–1059
lpd daemon 1056
lpq command 1056–1057
lpr command 1056
lprm command 1057
printcap file 1059–1065
PRINTER environment variable 1054
BSD UNIX 8, 12, 1268–1273
budgeting 1184
BugTraq 948
Burgess, Mark 408
bus errors 126
BUS signal 125
byte swapping 316
C
C language 1266
CA (Certificate Authority) 972
cable modems 544
cables
see also serial cables
10*Base* 533–535
Category 5 545
Ethernet 534–536
labeling 549
PATA/IDE 215
SATA 216
Cacti performance monitor 886
CAIDA (Cooperative Association for Internet Data Analysis) 463
Canaday, Rudd 1265
canonical name (CNAME) DNS records 585
capabilities (POSIX) 109
capacity planning 1104
capital cost reduction 1098–1110
carbon offsets 1111
Card, Rémy 255
catman command 17
CBK (common body of knowledge) 945
CD backups 299
CDNs (content distribution networks) 978–979
CentOS Linux 10, 12
CERT 948, 952
Certificate Authority (CA) 972
Certificate Signing Request (CSR) 972
Certified Information Systems Auditor (CISA) 945
Challenge Handshake Authentication Protocol (CHAP) 276
change management 1197–1198, 1205, 1225
ChaosNet 577
CHAP (Challenge Handshake Authentication Protocol) 276
character device files 148, 150, 418
Chatworth Products 1094
chattr command 159
cdev command 178
Check Point 475
chfn command 182
chgrp command 157–158
chkconfig command 91, 94
chkrootkit script 904
chmod command 152, 156–157, 165, 167, 169–170, 172
chown command 157–158
Christiansen, Tom 49, 66, 74
chrole command 108
chroot 913–914
for named 643, 645
for Postfix 830
for sendmail 800
chsh command 182
chuser command 195
CIA triad 944
CIDR (Classless Inter-Domain Routing) 458, 460–461
CIFS see Samba
CIM (Common Information Module) system configuration 410
CIP (Critical Infrastructure Protection) 1224
CISA (Certified Information Systems Auditor) 945
Cisco 475, 963
Cisco routers 525–528, 950
CiscoWorks 889
CISSP (Certified Information Systems Security Professional) 945
Citadel 853
CJIS (Criminal Justice Information Systems) 1223
ClamAV virus scanner 819, 903
Classless Inter-Domain Routing (CIDR) 458, 460–461
ClearEmail 755
Clearswift email appliance 853
clock synchronization 288
clogin command 1002
cloud computing 987, 1005, 1106
backups 303
hosting 978
cmdprivadm command 108
CNAME DNS records 585
COBIT 1223
code promotion 1204–1205
Coker, Russell 924
colocation web hosting 978
common body of knowledge (CBK) 945
Common Criteria 947
Common UNIX Printing System see CUPS
Communigate Pro 853
community relations 1210
Computer Systems Research Group (CSRG) 1268
concentrators see Ethernet, hubs
.config file for Linux kernel 424–425
configuration files
copying 721–727
network distribution 290
pulling 727
pushing 722–727
configuration management 1225
configure command 26
/usr/exim/configure file 812
conflict resolution 1213
ConnectionRateThrottle option, sendmail 800
Index

connectors
DB-25 1163–1165
DB-9 1166
PATA 215
RJ-45 1166
SATA 216
SCSI 217
consoles, serial 1180
console-setup file 1172
CONT signal 125–126, 128
contacting the authors xlv
Content Control 755
content distribution networks (CDNs) 978–979
content scanning 761–773
using Exim 818–820
control characters 1177–1178
control terminal 123
controls
statement, DNS 615–616
cookies, NFS 693
cooling
calculating load 1088–1089
data center 1087–1091, 1106, 1108
hot aisle/cold aisle 1106
in-row 1090
office temperature 1109
using outside air 1106
Cooper, Mendel 48
COPPA (Children’s Online Privacy Protection Act) 1223
Corbato, Fernando 1265
core files 289
Courier IMAP server 747
CPAN 65–66
CPU
load averages 1123
statistics 1122
usage, analyzing 1116–1123
CRAC (computer room air conditioner) 1089
crfs command 209, 254, 259
cron daemon 283–291
common uses 288–290
configuration (crontab) files 284–287
logging 284, 288
cron.allow and cron.deny files 286–287
/etc/cron.d directory 287–288
crontab command 286–287
/etc/crontab file 287
crontab files 284–287
CRT 1109
/etc/security/crypt.conf file 194
cryptography
backups, encryption of 295, 304
Diffie-Hellman key exchange 648
in DNS 573, 645–667
in LDAP 735
MD5 algorithm 646
password encryption 176, 179, 1144
public key 927
in sendmail 795–801
SSL 972
tools 924
.cshrc file 189
CSMA/CD (Ethernet) 532
CSR (Certificate Signing Request) 972
cftime file attribute 154
CTS (clear to send) signal 1168
cu command 1181
Cummins Onan 1092
CUPS 1032, 1034–1043
see also printing
autoconfiguration 1040
configuration 1038–1043
cupsd daemon 1038
cupsd.conf file 1039
cupsdisable command 1042
cupsenable command 1042
filters 1037–1038
lpadmin command 1041
lpoptions command 1036
lpr command 1035
MIME types 1037
network printers 1040
network printing 1036–1037
print queue 1035–1036
printer classes 1041
PRINTER environment variable 1036
cupsd.conf file 1039
cut command 34
Cygwin X server tools 1137, 1141
cylinders, disk 210
Cyrus IMAP server 747
DAT backup tapes 301
data center
see also cooling
availability 1086
components 1086
cooling load 1088–1089
energy use 1100
generators, standby 1086, 1091
green IT strategies for 1100–1108
hot aisle 1089–1091
humidity 1091
HVAC 1086
in-row cooling 1090
monitoring 1091
power 1091
preventative maintenance 1092
rack density 1092
rack power requirements 1092–1093
racks 1094
raised floor 1089, 1094
redundant power 1086
reliability tiers 1086–1087
remote power control 1094
temperature 1108
temperature range 1087
tool box 1095
UPSs 1086, 1091
wiring tracks 1094
zones 1093
data leak prevention (DLP) 754–755
databases
administrative 721, 736
DNS 555, 574–597
NIS 736
Postfix 833–837
sendmail 782–783
/etc/datemsk file 185
DB-25 connectors 1163–1165
DB-9 connectors 1165–1166
dbm/db library 782
DCC (Distributed Checksum Clearinghouses) 765
DCD (data carrier detect) signal 1167–1168
DCE (Data Communications Equipment) interface 1164–1165
DG1 1099
dd command 316, 992
DDS backup tapes 301
.deb software package format 382
**debconf** 368
Debian GNU/Linux 8–11
debugging see troubleshooting
DEC VT100 terminal 1175
default routes 466, 501, 513, 521
defaultdomain file 494
defaultrouter file 496
DefaultUser option, *sendmail* 759, 796
degraded mode 1106
DELAY_LA option, *sendmail* 801, 803
delgroup command 193
deluser command 193
/etc/deluser.conf file 199
deluser.local script 199
denial of service (DOS) attacks 349, 583, 727, 800–801, 1132
Dennis, Jack 1265
deraison, Renaud 916
desktop environments 1028–1030
Desktop Management Interface (DMI) 1119
deutsch, L. Peter 1068
/dev directory 150, 417
devfs, Solaris 419
devfsadm command 419
devfsadm daemon 225, 419
device drivers 150–151, 415–418
adding to Linux kernel 425–427
device awareness 427
loadable 431, 434–437
loadable modules 434–436
MODULE_DEVICE_TABLE macro 427
for PC hardware 417
serial 420
Solaris 430
terminal and control characters 1177–1178
Windows printer 1151–1152
device files 148, 150–151, 414
creating 419
device numbers 418
for disks 207, 224–226
for filesystems 420
for serial ports 420, 1168–1170
Solaris 429
for tape drives 309, 420
devices, pseudo 419
df command 260
NFS and 708
DFStab file 700
DHCP (Dynamic Host Configuration Protocol) 469–472, 477, 480, 484, 497–498, 504, 510
BIND and 640
HP-UX 504
Solaris 480, 497–498
/etc/dhcp.* files 497
dhcpagent program 497
dhcpd.conf file 471–472
dhcpdb2conf program 504
dhcrelay daemon 472
Diffie-Hellman key exchange 648
dig command 597–598, 615, 677–679
Dihu, Habeeb 765
directories 147–150
copying 315
directory statement, DNS 603
disaster recovery 1217–1222
from a security incident 950–952
internet connectivity 1221
planning 298, 1217
power and HVAC 1220
risk assessment 1217
staffing 1220
standards 1226
test plans 1220
/dev/disk directory 224–225
disks
see also filesystems
acoustic management 229–230
addition 207–209
AIX management 209, 224, 226, 253–255, 257, 280–281
ATA/PATA/IDE interface 213–215
as backup media 303
configuration 220–227
device files 207, 224–226
elevator algorithm 1130
failure rates 211, 213, 231
Fibre Channel 214, 275
formatting 226–227
hardware installation 223–230
hardware interfaces 213–220
hardware overview 209–213
hot-plugging 223
HP-UX management 208, 224–226, 237, 251–253, 256–257, 280
hybrid 209
I/O analysis 1127–1130
labeling 233
Linux management see Linux load balancing 1114, 1129
logical volume management 221–222, 246–254
partitioning 221–223, 231–237
performance 210, 212, 219–220, 1116–1130
quotas 698
RAID arrays 221–222, 234, 237–245, 1115
RAM 1129
removable 300
SATA interface 214–216
secure erase 227–228
SMART monitoring 230–231
software overview 220–223
solid state 206, 209–210, 212–213, 228, 300
traditional vs. SSD 210
USB 300
utilization of 1103
DISPLAY environment variable 1015, 1019
distance-vector routing protocols 515
Distfile file 723–725
Distributed Checksum Clearing-houses (DCC) 765
Distributed Management Task Force (DMTF) 410
DIX Ethernet II 453
DKIM (DomainKeys Identified Mail) 572, 768, 845–853
and *amavisd-new* 849
and Exim 850–852
and Postfix 852–853
and *sendmail* 850
DNS records for 846
miltering 846–848
DKIM DNS records 591–594
DMS records for 846
miltering 846–848
DKIM DNS records 591–594
DIX Ethernet II 453
DIX Ethernet II 453
DLT backup tapes 301
DMI (Desktop Management Interface) 1119
dmidecode command 1119
DMTF (Distributed Management Task Force) 410
Index

DNS 554–688

see also BIND

see also domain names, DNS

see also name servers

see also resource records, DNS

see also zones, DNS

adding a new machine 558–560

ADSP records 768, 846

anycast routing 603

architecture 568–572

authoritative servers 564, 569

caching 556–557

caching servers 564, 569

use with CIDR 585–587

client configuration 483–484

CNAME hack 585–587

cryptography in 573, 645–667

database 555, 574–597

delegation 555

denial of service (DOS) attacks 583

design 568–572

doc (domain obscenity control) 679–680

domain names see domain names, DNS

dynamic updates 640–642

EDNS0 protocol 574

efficiency 556–557

email security 571

forward mapping 554

internationalization 574

IP addresses 582–583

IPv6 support 573, 589

lame delegations 670, 678–679

master name server 564

Microsoft and 667

namespace 568

nonauthoritative servers 564

nonrecursive servers 565

Punycode 574

record types 578

recursive servers 565

referrals 565

resolver configuration 561–563

resource records see resource records, DNS

reverse mapping 554, 582–583, 623

RFCs 688

root servers configuration file 555

round-robin 962

security 571

DNS continued

server architecture 571

server hints 566

service switch file 776

setup 568–572

slave server 564

SOA record serial number 580

SOA record timeout values 580

Sparta DNSSEC tools 664

split view DNS 569, 617–618

SSHFP record 928

stub servers 564

stub zones 597

TKEY 645–648

traceroute and 867

TSIG (transaction signatures) 623, 645–648

TTL settings 680

Vantages DNSSEC framework 665

ZSKs (zone-signing keys) 653

DNSKEY DNS records 650

dnslookup router, Exim 822

DNSSEC 573, 648–667

DNSSEC-KEYGEN command 646–647, 655

dnssec-signzone command 657, 660

doc (domain obscenity control), DNS 679–680

DOCSIS standard 544

documentation 18–20

BCPs 450

FYIs 450

importance of 1200

man pages 16–18

network 1204

package-specific 19

passwords 112, 117–118

RFCs 449–450

standardization 1202

STDs 450

system-specific 18–19

tools for 1185

white papers 19

Doering, Gert 1171

domain directive, DNS 562

DOMAIN macro, sendmail 784

domain names, DNS 566–568

domain name length 567

internationalization 574

registration 549, 567

second-level 567

domain obscenity control 679–680

DomainKeys Identified Mail see

DKIM 768

DontBlameSendmail option 796, 798

DOS (denial of service) attacks 349, 583, 727, 800–801, 1132

dot files 189–190

Double Choco Latte 1193

double-sided printing 1076

Dovecot IMAP server 747

dpkg command 383

DR see disaster recovery

drill command 625, 677

drivers directory, Linux kernel

source tree 426

drivers see device drivers

DrWeb virus scanner 819

/dsk directory 226

DSL networks 543–544

DSR (data set ready) signal 1168

DTE (Data Terminal Equipment) interface 1164–1165

DTR (data terminal ready) signal 1168

dual booting 85, 1140

dump command 305–310

/etc/dumpdates file 309

dumps see backups

duplex printing 1076, 1109

DVD backups 299

dynamic servers 1104

E

E*Trade 10

e2fsck command 251

eco-pyramid 1099–1100

EdgeCast 978

editors, text 6–7

eeprom command 1168

EFF (Electronic Frontier Founda-
tion) 1231

effective user IDs (EUIDs) 122

EFI (Extensible Firmware Interface) 235

EFI partitioning 235–236

EIA-232-E standard 1163

EIA-606 standard 543–544

DTI (Data Terminal Equipment) interface 1164–1165

dual booting 85, 1140

dump command 305–310

/etc/dumpdates file 309

dumps see backups
duplex printing 1076, 1109

DVD backups 299
dynamic servers 1104
email
see also Exim
see also MX DNS records
see also Postfix
see also sendmail
aliases see aliases, email
appliances 853
architecture 753–756, 828–830
blacklists 766, 792, 817–818, 840–841
clients 745
components 744–746
content scanning 761–773
delivery status codes 752
denial of service (DOS) attacks 800–801
DNS security 572
DNS SPF records 590–591
envelope 748
fallback MX 803
filtering 767
forgery 763
headers 748–750
home mailbox 190
IMAP protocol 747
integrated solutions 853
Local delivery agents (LDA) 746
loops 758
mailing lists 760–761
managed services 743
market share 774
message checks 762
message stores 746–747
message structure 748–750
MX records 583–584
POP protocol 747
privacy 763
relaying 791–792
SASL 801
secure messaging appliances 853
security 572, 759, 795–801
server setup 754–756
spam see spam
submission agents (MSAs) 743–746
system components 744–746
system design 753–756
testing bulk mail 773
to files 759
to programs 759, 798–799
transport agents 746
email continued
transport layer security (TLS) 801
undeliverable messages 803
user agents 744
virus scanning 769–773
whitelists 766–767
embedded interpreters 959
EMC Ionix (Infra) 1194
EMC, backup tool 337
encryption see also cryptography
of backups 295, 304
of passwords 176, 179, 1144
system components 744–746
system design 753–756
tests bulk mail 773
to files 759
to programs 759, 798–799
transport agents 746
ethtool command 489–490
EUIDs (effective user IDs) 122
European Expert Group for IT-Security 773
event correlation 359
/etc/event.d files 1172, 1176
/etc/event.d directory 94
eXamples systems 10–13
logos 11
exec system call 123
executable maps, NFS auto-
mounter 714
execute bit 153
exicyclog command 811
exigrep command 811
exilog command 811
Exim 807–828
see also email
access control lists (ACLs) 815–818
aliases file 823
authentication 820
blacklists 817–818
command line flags for 810
configuration language 811–827
classification content scanning 818–820
decomposition debugging 827–828
DKIM 850–852
design issues 808–810
installation of 808–810
logging 826–827
macros 814
monitoring status of 811
retry configuration file section 825
rewrite configuration file section 825
transports 824–825
utilities 811
virus scanning 825–826
exim_checkaccess command 811
exim_dbmbuild command 811
exim_dumpdb command 811
exim_fixdb command 811
exim_lock command 811
exim_tidydb command 811
eximon application 811
eximstats command 811
exinext command 811
exipick command 811
exigrep command 811
exiqsumm command 811
exiwhat command 811
Index

expect command 7, 1171
export shell command 33
exports command 699
exports file 699, 702–705
ext filesystems 158–159, 255–256
extended partitions 235
extendvg command 254
Extensible Firmware Interface (EFI) 235

F

F5 Networks 963
Fabry, Robert 1268
FALLBACK_MX option, sendmail 803
FastCGI 959–960
fasterase command 228
fax server 1171
faxgetty process 1171
FC-AL (Fibre Channel arbitrated loop) 214
fcntl system call 694
fdisk command 207, 235–237
FEATURE macro, sendmail 784
Fedora Directory Server 728
Fedora Linux 10, 12
FERPA (Family Educational Rights and Privacy Act) 1223
Ferraiolo, David 108
FHS (Filesystem Hierarchy Standard) 146
fiber 536–537
colors of 537
connectors 537
diameters of 537
multimode 536
single mode 537
Fibre Channel interface 214, 275
Fibre-Channel-over-Ethernet (FCoE) 276
Field, Julian 769
file attributes continued
link count 155
on ext filesystems 158–159
owner 155
permission bits 152–155
setuid/setgid bits 106, 153–154, 912–913
sticky bit 154–155
file descriptors 31–32
file statement, DNS 614
filenames
control characters in 148
encoding under Samba 1145
length restrictions 142
pathnames 142–143
pattern matching 14, 51, 148
spaces in 142–143
files
see also device files
see also directories
see also file attributes
see also filenames
access control 104–105
default permissions 158
deleting 148–151
links vs. original files 149
modes see file attributes
NFS locking 694
ownership 155
permissions 105, 110, 152–159, 164–172
removing temporary 289
servers, dedicated NFS 711
servers, system files 727
sharing with Samba 1146
types of 147–152
Filesystem Hierarchy Standard
(FHS) 146
filesystems 254–263
see also partitions
backing up 294
 caching 257–258
checking and repairing 81
cleaning with cron 289–290
copying 316
defined 222
disabling setuid execution 912
enabling ACLs 162
exporting through NFS 698–705
ext (Linux) 158–159, 255–256
JFS (AIX) 255, 257
journaling 255–256
lazy unmounting 144
filesystems continued
load balancing 1114, 1129
loopback 143
mounting 143, 260–263, 1148
mounting at boot time, NFS 708
organization 145–146
overview 140–172
page clusters 213
quotas 698
repairing 81, 258–261
replicated 715
resizing 250–251
root 81, 146, 232
snapshots 249, 259, 269–271
spaces in 142–143
types 141
unmounting 144–145
VxFS (HP-UX) 256–257
ZFS (Solaris) 161, 166–172,
208, 222, 232, 240, 242, 264–274,
274, 316
/etc/filesystems file 143, 254, 259–
260, 263
filter commands 33
find command 31, 143, 289
findutils package 23, 143
finger command 181
firewalls 474–475, 499–500, 932–942
ICMP blocking 862, 867
Linux IP tables 935–942
Netfilter 935–939
packet-filtering 932–933
stateful 934
trace route and 867
FISMA (Federal Information Security Management Act) 947, 1223
flash memory disks (SSDs) 206,
209–210, 212–213, 228
flock system call 694
flow control, serial line 1168
flow down liability 1228
Fluke meter 1090, 1094
fork system call 123
format command 208, 227, 236, 266
.forward file, email 797
forward mapping, DNS 554
forwarders option, DNS 606
fragmentation, of packets 454
FreeBSD 8
freegeek.org 1107
French Green IT 1110
/etc/default/fs file 258
fsck command 81, 258–261
F-Secure virus scanner 819
FSF (Free Software Foundation) 1229
/etc/fstab file 143, 208, 259–262, 708, 711, 1149
FSUID process parameter 122
FTP
  active vs. passive 933
  through firewalls 933–934
fully qualified hostnames 566
FUSE (Linux user-space filesystems) 258
fuser command 144–145, 902, 1129
FYI documents 450
gated routing daemon 502, 523
gconf tool 190
gdm display manager 1013
GECOS information 181
Gentoo Linux 10
gethostbyname routine 739
gethostent routine 1133
getpwent routine 721
getpwnam routine 721
getpwuid routine 721
getty process 1171–1177
  configuration file 1173
gettydefs file 1173–1175
gettytab file 1173
Ghostscript 1068
GIAC (Global Information Assurance Certification) 945
gbi prefix 15
GIDs see group IDs
Git 401–404
git command 401
GlassFish application server 961
GLBA (Gramm-Leach-Bliley Act) 1224
globbing 14, 51, 148
Gmail 743
GNOME 1029–1030
  see also X Window System
Gnu PG (GPG) 925
GNU Software Foundation 8
GNU Texinfo 18
GNU/Linux controversy 8
Google 20, 963
parted command 207, 236, 243
GPG (GNU Privacy Guard) 763
GPT partitioning 235–236
Green Grid 1106
green IT
  approaches 1100
  assessment 1099
  benefits of 1097
  consumables 1099
  equipment survey 1099
  metrics 1099
  organizations 1110
  pyramid 1100–1101, 1109
  strategies 1100–1110
  suggested measurements 1099
  user education 1108
Green IT Observatory 1110
Green IT Promo Council 1110
Green Standards Trust 1110
greet_pause feature, sendmail 793
grep command 36
groff command 18
/etc/group file 104, 181, 186–187
  group IDs 186
  see also groups
  in ls output 155
  mapping to names 105
  real, effective, and saved 105, 122
  substitution 106–107
groupadd command 187
groupdel command 187
groupmod command 187
groups
  see also /etc/group file
  default 181
  effective 122
  GIDs (group IDs) 105, 186
  vs. RBAC 108
  wheel or system 181
grepc command 187
GRUB boot loader
  multiboot configuration 85
  single-user mode 86
grof file 83, 85
/etc/gshadow file 186
GTUBE 773
halt command 101
halting the system 100–101
Hamilton, Bruce 20
hard carrier 1167
hard links 149–150, 155
hardware
  see also cables
  see also connectors
  see also Ethernet
  see also networks
  see also PC hardware
  cooling 1087–1091
  environment 1087–1091
  equipment racks 1094
  hubs 537
  kernel adaptation 416, 964
  memory 79, 1114
  power supplies 1091
  probing 79
  routers 539
  switches 534, 538–539, 543
  temperature monitoring 1091
  tools 1095
  wiring 545–547
hardware flow control 1168
Hazel, Philip 49, 807
hbvm command suite 1003
hdparm command 228–230
head command 36
HEAT 1194
heaters, personal 1109
Hein, Trent R. 1270, 1279
help desk 1196–1197, 1225
Hesiod 577
HIDS (Host Intrusion Detection System) 904, 919
HIPAA (Health Insurance Portability and Accountability Act) 1224
history
  of BSD 1268–1273
  of Linux 1271–1273
  of Sun Microsystems (now Oracle America) 1268
  of system administrators 1264–1273
  of UNIX 1265–1273
Index

I/O channels 31–32
I/O schedulers 1130–1131
IANA (Internet Assigned Numbers Authority) 451, 567
IBM 701 computer 1264
IBM BladeCenter HS20 1093
ICANN (Internet Corporation for Assigned Names and Numbers) 448, 461, 549, 567
ICMP 450
error messages 454
firewall blocking 862, 867
netstat output 872
packets 938
ping and 861
redirects 467–468, 473, 493, 499, 505, 508–509, 514–515
sequence numbers 862
traceroute and 866
TTL and 865
IDE interface 213–215
cables 215
power connector 215
secure erase 227–228
SMART reporting 230–231
TRIM command 228
idisk command 237
idle timeout, workstation 1109
IEEE 802.* standards (Ethernet) 502, 533, 539–540, 542
IEEE P1680 1108
IETF (Internet Engineering Task Force) 448
ifconfig command 458, 478–482, 495–497, 501–502, 513, 969–970
ifdown command 485–486
ifup command 485–486
IGF (Internet Governance Forum) 448
IGMP (Internet Group Management Protocol) 456
IIS web server 1141
Image Packaging System 394
IMAP (Internet Message Access Protocol) 747
incident handling, security 950–952
incident management 1225
$INCLUDE directive, DNS 575
include directive, for email aliases 758
include statement, DNS 602
indirect maps, NFS automounter 713
inetd daemon 506
info command 18
information technology (IT) management automation 1205
budgeting 1184–1185
community relations 1210
disaster recovery 1217–1222
documentation, tools for 1185
enterprise architecture (EA) 1197–1199
firing 1208
help desk 1196–1197
hiring 1207
management, role of 1206–1215
operations 1199–1206
organizational structure 1190–1196
personnel management 1207
policies and procedures 1215–1217
policy 1185
prioritization of work 1188–1189
purchasing 1212
purpose of 1184
quality control 1209
rogue users 1214
service level agreement 1186–1190
skill sets 1195
ticketing systems and processes 1191–1196
init process 78, 80–81, 88–89, 123, 1171–1175
AIX and 96
bootstrapping and 81
run levels and 88–91
Solaris and 97
startup scripts and 87, 93
Ubuntu and 94
zombie processes and 124, 128, 130
/etc/init.d directory 87, 89–91, 93
initlog 353
inittab file 89, 96, 1171, 1174–1175
inodes 155, 257
in-row cooling 1090
insmod command 435–436

Index

home directories 146, 182, 189, 233
creating 189
logging in to 182
missing 182
removing 198
Host Intrusion Detection System (HIDS) 904, 919
HOST_STATUS_DIRECTORY option, sendmail 803
hostname command 478
/etc/hostname file 486
/etc/hostname.* files 495
hostnames
fully qualified 566
mapping to IP addresses 456, 477
/etc/hosts file 456, 477–478, 494, 502
/etc/hosts.allow file 917–918
/etc/hosts.deny file 917–918
hot aisle cooling 1089–1091
Hotmail 743
hot-pluggable disks 223
HP 303
HP-UX 12
disk addition recipe 208
disk device files 224–226
disk partitions 237
documentation 19
filesystems 256–257
installation 377–379
iSCSI support 280
kernel configuration 431–432
log files 344
logical volume management 251–253
named 684–685
network configuration 501–506
NFS (Network File System) 700–701
security 505–506
single-user mode 87
startup scripts 95
HTTP protocol 957–959
httpd.conf file 965–974
hubs, Ethernet 537
humidity 1091
hung terminals 1179
HUP signal 125–126
HVAC air cooling
HylaFAX 1171

1243
installation
of AIX 380
of HPUX 377–379
of Linux see Linux installation
of Solaris 370–376
installp command 397
INT signal 125–126
Integrity virtual machines 1003–1004
intent logs 255–256
/etc/interfaces file 486
interfaces, network see networks
International Computer Science Institute (ICSI) 918
International Organization for Standardization (ISO) 534
Internet
Cache Protocol (ICP) 975
governance 448–450
history 447
protocol security (IPsec) 475
registries 448, 461, 549, 567
standards and documentation 449–450
system administration resources 20
Worm 896
Internet Corporation for Assigned Names and Numbers (ICANN) 448, 461, 549, 567
Internet Engineering Task Force (IETF) 448
Internet Governance Forum (IGF) 448
Internet protocol see IP
Internet Society (ISOC) 448, 957
Interop 1230
iosc1 1173
IOS (Cisco router OS) 525–528
ioscan command 208, 225–226, 280, 1169
iostat command 1127
IP 447–508
IP continued
forwarding 472, 482, 493, 499, 505, 508, 511–515
fragmentation 863
IPV4 vs. IPV6 451–452
kernel options 490, 492–493, 498–499
loopback interface 457, 467, 513, 583
masquerading see NAT
netmasks 458–461, 479, 495
packet fragmentation 454
ports 456
protocol stack 450–452
routing 465–468, 511–528
source routing 473, 493, 499, 505, 508
spoofing 473–474
subnetting 458–461, 479, 495
IP addresses 454–465
IP Calculator program 460
ipcalc command 460
ipf command 500, 942
ipf.conf file 940
IPFilter 499, 506, 939–942
host and port filtering 940
ipf command 942
keep state keywords 941
NAT 941
quick keyword 940
ipfstat command 500
ipnat command 500–501
IPSec 277, 943
IPSec protocol 475
iptables 935–939
iptables commands 475
IPv4 451–452, 464–465, 509
DNS support 573, 589
routing protocols 518–520
IQNs (iSCSI Qualified Names) 277
IronPort email appliance 753, 853
ISC (Internet Software Consortium) 470
ISC cron 287–288
ISCSI 276–281
AIX 280–281
HP-UX 280
Linux 277–279
Solaris 279–280
iSCSI Qualified Names (IQNs) 277
iscsiadm command 278–279
iscsid daemon 278
/etc/iscsi/iscsi.conf file 278
iscsiutil command 280
IS-IS protocol 518–520
ISOC (Internet Society) 448, 957
iscal id 1171
IT Industry Council 1110
ITIL (Information Technology Infrastructure Library) 1224–1225
J
Jachim, Ron 1278
Jacobson, Van 865, 875
jail, chroot 913
Jaquist, Mark 1111
JBOD RAID mode 238
JBoss application server 961
Jetmore, John 773
Jetty application server 961
JFS filesystem 255, 257
John the Ripper 916
Jolitz, Bill 1270
Jolitz, Bill 1270
journals (filesystem) 255–256
Joy, Bill 1268
JSON (JavaScript Object Notation) 960
jukeboxes, tape media 303
jumbo frames 541
Jumpstart, Solaris 371–375
Justman, Ian 765

K
Karels, Mike 1270
Kaspersky virus scanner 819
kcweb command 431
KDE 1029–1030
see also X Window System
KDEPrint framework 1043–1045
kdm display manager 1013
Kerberos 110, 924–925
/kernel directory 427
kernel 415–417
AIX configuration 432–434
and NFS 705
ARP cache 469
boot time options 84
building, Linux 423–425
.config file, customizing 424–425
device drivers 150–151, 415–418
device numbers 418
HP-UX configuration 431–432
initialization 79
IP options 490, 492–493, 498–499
Linux configuration 421–423
loadable modules 434–436
location 146
logging 352
monolithic vs micro 416
options, Linux 421, 423–425
saved group IDs 122
Solaris configuration 427–431
source tree, Linux 424–425
swappiness parameter 1125
threads 79
tuning, AIX 434
tuning, Linux 421–423
udev system 437
KEY DNS records 647
.key DNSSEC key file, DNS 646
key remapping
backspace key 1177
delete key 1177
devices
key statement, DNS 609
keymap file, corrupted 92
keys, generating BIND 654
keys, SSH 926
kibi-prefix 15
Kickstart 365–367
Kill A Watt meter 1088, 1099
kill command 127, 1132
KILL signal 125–127
kinit command 1157
ldbg daemon 352
KMS (kernel mode setting) 1025–1026
Kojim, Tomasz 903
Kolstad, Rob 1270
konqueror browser 1044
kprinter command 1044
kprinter tool 1044
ks.cfg file 365–367
Kuhn, Rick 108
kVA unit conversion 1093–1094
KVM 995–997
guest installation 996
live migration 997
virsh command 997
virt-install command 996
kW unit conversion 1093–1094
LDAP (Lightweight Directory Access Protocol) 728–735
and Active Directory 202
administration tools 730
attribute names 729
documentation 731
mail routing architecture 754
OpenLDAP 731
query example 734
security 735
setup 731–732
structure of data 728
use with Exim 809
use with Postfix 833
use with sendmail 759, 786–787
and user IDs 181
uses of 730–731, 733
ldap_routing feature, sendmail 786–787
ldap.conf file 732–733
ldapsearch command 734
LDIF (LDAP Data Interchange Format) 729
ldns DNSSEC routines 664
leadership 1206
legacy systems 1162, 1180
Less Watts 1110
Levy, Stephen 924
lifespan, equipment 1107, 1110
Lightweight Directory Access Protocol see LDAP
Lightweight Wireless Access Point Protocol (LWAPP) 543
Limelight 978
limit shell built-in 1133
links
hard 149–150, 155
symbolic 148, 151
link-state routing protocols 516
Linux
disk addition recipe 207–208
disk device files 224–225
disk partitions 236
distributions 9–10
filesystems 158–159, 255–256
iSCSI support 277–279
kernel configuration 421–423
kernel tuning 421–423
loadable drivers 432–423
log files 344
Linux continued

logical volume management 247–251
logo 11
mandatory access control (MAC) 109, 923–924
named 681–684
network configuration 484–494
NFS (Network File System) 702–705
RAID 240, 242–245
reasons to choose 1113
security 492
security-enhanced 109, 923–924
single-user mode 86
startup scripts, Red Hat 91–93
startup scripts, SUSE 93–94
startup scripts, Ubuntu 94–95
vendor logos 11
volume snapshots 249
vs. UNIX 7–9

LINUX Documentation Project 20
Linux installation
see also system administration
see also system configuration
automating with AutoYaST 367–368
automating with debconf 368
automating with debian-installer 368–370
automating with Kickstart 365–367
ks.cfg file 365–367
netbooting 363–364
PXE protocol 363–364
PXELINUX 364
TFTP protocol 364
Linux Mint 10
Linux package management 382–393
alien conversion tool 382
APT 387–391
.deb format 382
dpkg/APT 382–383
Red Hat Network 387
repositories 385
RPM format 382
rpm/yum 382–383
yum 391
yum/Red Hat Network 382
Zypper 392
Linux Virtual Server 963

Lions, John 1268
LISA (Large Installation System Administration) conference 1230
LMTT protocol 830
ln command 149, 151–152
load average, sendmail 803
load averages 1123
load balancing
disks and filesystems 1114, 1129
servers 1114
web server 961–963
loadable drivers 431, 434–437
Linux 435–436
Solaris 436–437
loadable modules 434–437
Local Area Network (LAN) 532–539
local delivery agents (LDA), email 746
local domain sockets 148, 151
localhost 457, 467
localhost zone configuration example, BIND 619
localization
compilation 407
distribution 408
/usr/local hierarchy 407
wrapper scripts 413
locate command 23
lockd daemon 694
lockf system call 694
log files 341–344
see also logging
see also syslog
AIX 344
analyzing and searching 358–359
for Apache 966
finding 341–342
for cron 284
HP-UX 344
Linux 344
lists of 343
monitoring 358–359
rotating 290, 356–358
Solaris 344
web hosting 966
/dev/log socket 345
logcheck 358
logger command 351
logging
see also log files
see also syslog
for BIND 612, 667–672
boot-time 352–353
to central server 350
for cron 288
enterprise strategy and policy 359
for Exim 826–827
kernel 352–353
for NSD 673–674
for sendmail 806–807
storage considerations 360
for sudo 114
logging in from Windows 1135
logging statement, DNS 612, 667
logical unit numbers (SCSI) 218
logical volume management 221–222, 246–254
see also ZFS filesystem
AIX 253–254
HP-UX 251–253
inter-system comparison 247
Linux 247–251
login command 1171
.login file 189
/etc/default/login file 194, 907
login process 1171
/etc/security/login.cfg file 182, 185, 195–196, 1172
/etc/login.defs file 182, 185, 193, 198–199
logins see user accounts
logos, vendor 11
logrotate 356–358
/etc/logrotate.cnf file 357
/etc/logrotate.d directory 357
loopback
address 457, 467
address, BIND 616
filesystem 143
interface 457, 467, 513, 583
LOPSA (League of Professional System Administrators) 1230
lost+found directory 260, 290
low-power equipment 1108
ls command 152, 154–155, 167, 169–171
lsattr command 159, 178
lscfg command 1120
lsdev command 209, 226
lsmod command 435
lssof command 145, 708, 902, 1129
<table>
<thead>
<tr>
<th>Command/Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lsusb</code> command</td>
<td>441</td>
</tr>
<tr>
<td><code>lsvg</code> command</td>
<td>1002</td>
</tr>
<tr>
<td><code>lswpar</code> command</td>
<td>209</td>
</tr>
<tr>
<td><code>lvchange</code> command</td>
<td>250</td>
</tr>
<tr>
<td><code>lvcreate</code> command</td>
<td>207–208, 248–249, 252–253</td>
</tr>
<tr>
<td><code>lvdisplay</code> command</td>
<td>249</td>
</tr>
<tr>
<td><code>lvextend</code> command</td>
<td>253</td>
</tr>
<tr>
<td><code>lvlnboot</code> command</td>
<td>253</td>
</tr>
<tr>
<td><code>lvm</code> command</td>
<td>247</td>
</tr>
<tr>
<td><code>LVM</code></td>
<td>see logical volume management</td>
</tr>
<tr>
<td><code>lvmadm</code> command</td>
<td>252</td>
</tr>
<tr>
<td><code>lvresize</code> command</td>
<td>250</td>
</tr>
<tr>
<td><code>LWAPP</code> (Lightweight Wireless Access Point Protocol)</td>
<td>543</td>
</tr>
<tr>
<td><code>m4</code> command</td>
<td>779–782, 789</td>
</tr>
<tr>
<td><code>MAC</code> (Mandatory Access Control)</td>
<td>109</td>
</tr>
<tr>
<td><code>MAC addresses</code></td>
<td>454–455, 464</td>
</tr>
<tr>
<td><code>machinfo</code> command</td>
<td>1120</td>
</tr>
<tr>
<td>Mackerras, Paul</td>
<td>725</td>
</tr>
<tr>
<td><code>macros, sendmail</code></td>
<td>782–795</td>
</tr>
<tr>
<td><code>magic cookies, NFS</code></td>
<td>693</td>
</tr>
<tr>
<td><code>magic cookies, X Windows</code></td>
<td>1016</td>
</tr>
<tr>
<td><code>mail</code> command</td>
<td>744</td>
</tr>
<tr>
<td>Mail eXchanger (MX) DNS records</td>
<td>583–584</td>
</tr>
<tr>
<td>mail see email</td>
<td>745</td>
</tr>
<tr>
<td>mail submission agents (MSAs)</td>
<td>745</td>
</tr>
<tr>
<td><code>mail transport agents (MTAs)</code></td>
<td>746</td>
</tr>
<tr>
<td><code>mail user agents (MUAs)</code></td>
<td>744</td>
</tr>
<tr>
<td><code>MAIL_HUB</code> macro</td>
<td>828</td>
</tr>
<tr>
<td>Maildrop</td>
<td>828</td>
</tr>
<tr>
<td><code>MAILER</code> macro</td>
<td>828</td>
</tr>
<tr>
<td>gmail</td>
<td>828</td>
</tr>
<tr>
<td><code>MAIL_LOCAL</code> delivery agent</td>
<td>798</td>
</tr>
<tr>
<td>Maildir format</td>
<td>798</td>
</tr>
<tr>
<td>Maildrop</td>
<td>798</td>
</tr>
<tr>
<td><code>MAILER</code> macro</td>
<td>798</td>
</tr>
<tr>
<td>mailing lists</td>
<td>798, 760–761</td>
</tr>
<tr>
<td>Mailman</td>
<td>761</td>
</tr>
<tr>
<td><code>mailq</code> command</td>
<td>806, 830</td>
</tr>
<tr>
<td><code>.mailrc</code> file</td>
<td>819</td>
</tr>
<tr>
<td>MailScanner</td>
<td>819</td>
</tr>
<tr>
<td><code>main.cf</code> file</td>
<td>831</td>
</tr>
<tr>
<td>major device numbers</td>
<td>150</td>
</tr>
<tr>
<td>make command</td>
<td>25</td>
</tr>
<tr>
<td><code>makedbm</code> command</td>
<td>737</td>
</tr>
<tr>
<td><code>makemap</code></td>
<td>737</td>
</tr>
<tr>
<td><code>mkfile</code></td>
<td>737</td>
</tr>
<tr>
<td><code>main</code> function</td>
<td>737</td>
</tr>
<tr>
<td><code>main</code> file</td>
<td>737</td>
</tr>
<tr>
<td><code>makefile</code></td>
<td>737</td>
</tr>
<tr>
<td><code>make</code> command</td>
<td>737</td>
</tr>
<tr>
<td><code>makefile</code></td>
<td>737</td>
</tr>
<tr>
<td><code>make</code> command</td>
<td>737</td>
</tr>
<tr>
<td><code>make</code> command</td>
<td>737</td>
</tr>
<tr>
<td><code>make</code> command</td>
<td>737</td>
</tr>
<tr>
<td><code>make</code> command</td>
<td>737</td>
</tr>
<tr>
<td>mean time between failures (MTBF)</td>
<td>211</td>
</tr>
<tr>
<td><code>mebi</code>-prefix</td>
<td>299–305</td>
</tr>
<tr>
<td>media, backup</td>
<td>299–305</td>
</tr>
<tr>
<td><code>see also tapes</code></td>
<td>299–305</td>
</tr>
<tr>
<td><code>CD and DVD</code></td>
<td>299</td>
</tr>
<tr>
<td><code>comparison of</code></td>
<td>299</td>
</tr>
<tr>
<td><code>jukeboxes</code></td>
<td>299</td>
</tr>
<tr>
<td><code>labeling</code></td>
<td>299</td>
</tr>
<tr>
<td><code>life of</code></td>
<td>299</td>
</tr>
<tr>
<td><code>magnetc tape</code></td>
<td>299</td>
</tr>
<tr>
<td><code>optical</code></td>
<td>299</td>
</tr>
<tr>
<td>SSD</td>
<td>300</td>
</tr>
<tr>
<td><code>summary of types</code></td>
<td>304</td>
</tr>
<tr>
<td>verifying</td>
<td>297</td>
</tr>
<tr>
<td><code>mediainit</code> command</td>
<td>227</td>
</tr>
<tr>
<td>MediaWiki</td>
<td>1185</td>
</tr>
<tr>
<td><code>memory</code></td>
<td>1185</td>
</tr>
<tr>
<td>effect on performance</td>
<td>138, 1114, 1116, 1125–1127</td>
</tr>
<tr>
<td>kernel initialization and</td>
<td>79</td>
</tr>
<tr>
<td>paging</td>
<td>1129, 1132</td>
</tr>
<tr>
<td>RAM disks</td>
<td>1129</td>
</tr>
<tr>
<td>usage, analyzing</td>
<td>1125–1127</td>
</tr>
<tr>
<td>memory management</td>
<td>1124–1125</td>
</tr>
<tr>
<td>Message Labs</td>
<td>763</td>
</tr>
<tr>
<td><code>message of the day</code></td>
<td>763</td>
</tr>
<tr>
<td>message stores, email</td>
<td>763</td>
</tr>
<tr>
<td><code>/var/log/messages</code> file</td>
<td>349, 352</td>
</tr>
<tr>
<td>Metcalfe, Bob</td>
<td>532</td>
</tr>
<tr>
<td>meter, power</td>
<td>1099</td>
</tr>
<tr>
<td><code>ngetty</code> process</td>
<td>1171–1176</td>
</tr>
<tr>
<td>Microsoft Exchange, replacements for</td>
<td>853</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td>745</td>
</tr>
<tr>
<td>Microsoft Windows see Windows</td>
<td>745</td>
</tr>
<tr>
<td><code>mii-tool</code> command</td>
<td>489</td>
</tr>
<tr>
<td>Miller, Todd</td>
<td>114</td>
</tr>
<tr>
<td><code>miltering, email</code></td>
<td>767</td>
</tr>
<tr>
<td>MIME (Multipurpose Internet Mail Extensions)</td>
<td>744</td>
</tr>
<tr>
<td><code>mingetty</code> process</td>
<td>1171–1176</td>
</tr>
<tr>
<td>Microsoft Exchange, replacements for</td>
<td>853</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td>745</td>
</tr>
<tr>
<td>Microsoft Windows see Windows</td>
<td>745</td>
</tr>
<tr>
<td><code>mii-tool</code> command</td>
<td>489</td>
</tr>
<tr>
<td>Miller, Todd</td>
<td>114</td>
</tr>
<tr>
<td><code>miltering, email</code></td>
<td>767</td>
</tr>
<tr>
<td>MIME (Multipurpose Internet Mail Extensions)</td>
<td>744</td>
</tr>
<tr>
<td><code>mingetty</code> process</td>
<td>1171–1176</td>
</tr>
<tr>
<td>Microsoft Exchange, replacements for</td>
<td>853</td>
</tr>
<tr>
<td>Microsoft Outlook</td>
<td>745</td>
</tr>
<tr>
<td>Microsoft Windows see Windows</td>
<td>745</td>
</tr>
</tbody>
</table>
mksf command 1169
mkswp command 264
mkuser command 195
/etc/security/mkuser.default file 195
mkvg command 209, 246, 254
mkwpar command 1002
mod_perl interpreter 960
mod_php interpreter 960
mod_python interpreter 960
modems 1167
modinfo command 431, 436–437
modload command 437
/etc/modprobe.conf file 436
MODULE_DEVICE_TABLE macro 427
modunload command 437
Mondo Rescue 335
monitoring
environmental 1091
log files 358–359
processes 130–135
temperature 1091
Morreale, Terry 1278
Morris worm 896
Morris, Robert, Jr. 896
motd file 1172
mount command 143–145, 258, 260–262, 706–709
mount points, filesystem 143
mount.smbfs 1149
mountd daemon 699
mountpoint ZFS property 268
mpstat command 1122
/var/spool/mqueue directory 806
MRTG (Multi-Router Traffic Grapher) 886
MSA (mail submission agent) 745
MSN Hotmail 743
mt command 317
MTA (mail transport agent) 746
MTBF (mean time between failures) 211
MTU (Maximum Transfer Unit) 453–454
mtx package 318
MUAs (mail user agents) 744
multibooting 85
multicast addresses 456–457
multicores processors 990
Multics 1265
multimode fiber 536
multiprocessor machines, analyzing performance 1122
Multipurpose Internet Mail Extensions (MIME) 744
multiuser mode 81
MX DNS records 583–584
MySQL 318, 320–321, 956, 1193

N

Nagios SNMP monitoring tool 887
name servers
see also DNS
see also BIND
see also named
authorized 564, 569
caching 556–557, 569
caching-only 564
delegation 555
dynamic updates 640–642
forwarding 606
hints 566
lame delegations 670, 678–679
master 564
nonauthoritative 564
recursion 565
resolver 561–563
slave 564
stub 564
switch file 682
zone delegation 596–597
name service switch 494
named
see also BIND
see also DNS
see also name servers
acl statement 609
ACLs 609, 643–644
AIX 685–686
allow-update clause 613, 641
avoid-notify-ports option 605
blackhole option 606
bogus directive 611
chrooted 643, 645
command-line interface see named, rndc
compiling with OpenSSL 655
configuration examples 618–624
directory statement 603
named continued
domain directive 562
error messages 670
file statement 614
forwarders option 606
forwarding zone, configuring 615
$GENERATE directive 587
HP-UX 684–685
$INCLUDE directive 575
include statement 602
init scripts 681
ISC configuration example 623
key statement 609
Linux 681–684
localhost zone configuration example 619
logging 667–672
logging statement 612, 667
master server, configuring 613
masters statement 611, 614
match-clients clause 617
/etc/named.conf file 600–624, 643, 671
named.run file 672
named-checkconf command 600, 648, 679
named-checkzone command 600, 679
notify option 604
options directive 561
options statement 602–609
$ORIGIN directive 575
provide-ixfr option 639
recursion option 604
request-ixfr option 639
RHEL 684
rndc command 638, 672, 674
root server hints 614
root.cache file 615
search directive 561
server statement 610, 639
slave server, configuring 614
Solaris 684
starting 640
statements, list of 601
stub zones, configuring 614
SUSE 683
testing 667–681
transfer-source option 623
$TTL directive 575–576, 581
Ubuntu 682
update-policy clause 641
updating zone files 640–642
Index 1249

named continued
  versions 599
  view statement 617
  zone commands 574–575
  zone statement 612–615
  zone-statistics option 613

named daemon 563
named pipes 148, 151
named_dump.db file 674
/etc/named.conf file 600–624, 643, 671
named.run file 672
named-checkconf command 600, 648, 679
named-checkzone command 600, 679
nano editor 6
ncftp command 727
ndbm library 308
ndd command 468, 498–499, 504–505, 970
nddconf file 95
neigh directory 491
Neighbor Discovery Protocol 520
Nelson, T.J. 847
Nemeth, Evi 1269, 1279
NERC (North American Electric Reliability Corporation) 1224
Nessus 916
net command 1158
NetBIOS 1142
netbooting
  non-PCs 364
  PCs 363
NetBSD 8
netconf file 95, 501, 504
netdaemon file 95
Netfilter 935–939
netmasks 458–461, 479, 495
netmasks file 495
NeTraverse 1140
Netscape Directory Server 728
NET-SNMP 885–886
netstat command 466, 483, 503, 512–514, 868–873
  interfaces 868
  monitoring connections 870
  network statistics 868–873
  and NFS UDP overflows 705
  open ports 871
  routing table 871
Network Address Translation (NAT) 462–464, 493–494, 500–501
Network Appliance, Inc. 711
Network Auto-Magic 494
network booting 363–364
network documentation 1204
/etc/sysconfig/network file 487
Network Intrusion Detection System (NIDS) 918
network printers 1040
network unreachable error 482
network wiring
  building 545–547
  cable analyzer 545
  cable choices 533–536, 545
  maintenance and documentation 549
  for offices 546
  Wireshark network sniffer 545
  NetworkManager 485–486
networks
  see also Ethernet
  see also IP addresses
  see also network wiring
  see also routing
  see also TCP/IP addresses
  454–455, 457, 464, 467
  administrative databases 721, 736
  AIX configuration 506–508
  broadcast storms 538
  connecting and expanding 537–539
  design issues 547–549
  firewalls 932–942
  hardware options 481
  host addition 476–484
  HP-UX configuration 501–506
  interface activity reports 873
  interface configuration 478–481
  IPFilter firewall 939–942
  Linux configuration 484–494
  load balancing 1114
  loopback 457, 467, 513, 583
  management issues 549–550, 859
  management protocols 879–883
  management standards 879–880
  monitoring 869–870
networks continued
  MTU 453–454
  ping and 861–863
  port scanning 914–916
  RHEL configuration 487–489
  routing tables 871
  scanner, Nessus 916
  Solaris configuration 494–501
  statistics 868–873
  SUSE configuration 486–487
  tools 860
  troubleshooting 544–545, 860–873
  Ubuntu configuration 486
  unreachable 482
  virtual interfaces 481
  VLANs 539
  VPNs 475–476
  wireless 541–543
  Wireshark 877
/etc/networks file 483
network-scripts directory 92, 488
Neumann, Peter 1266
newaliases command 290, 760, 830
newgrp command 186
newusers command 197
NFS (Network File System) 690–717
ACLs 161, 166–172
AIX 702–703
all_squash option 698, 704
anongid option 704
anonuid option 704
as a configuration file distribution method 721
buffer sizes 708
client 706–709
common options, Linux 704
configuration, server 698–705
cookies 693
dedicated file servers 711
disk quotas 698
and dump 309
entities 168
export configuration files 700
exporting filesystems 698–705
exports 693
file locking 694
firewall configuration 696
hard vs. soft mounts 707
history of 692
HP-UX 700–701
identity mapping 696, 709–710
NFS continued

insecure option 704
Linux 702–705
maintaining state 693
mount command 706–709
mounting filesystems at boot time 708
nfsd daemon 705
no_root_squash option 704
noaccess option 703
nobody account 118, 697
performance on wide area networks 698
protocol versions 692
Red Hat 717
root access 697
secure option 704
secure.locks option 704–705
security 695–698, 700, 709
Solaris 700–701, 708
statistix 710
subtree_check option 704
subtree_check option 708
using to export email 756
version 4 features 692
and ZFS 271–272
nfsd daemon 699, 705
nfsstat command 710
nice command 129–130, 1123
nice value 123
NIDS (Network Intrusion Detection System 918
NIS (Network Information Service) 494, 736–738
architecture 736–738
commands 738
database files 736
directories 736
files to share 720
map files 736
master server 736–737
slave servers 736–737
NIST (National Institute for Standards and Technology) 1225–1226
NIST 800-34 standard 1226
NIST 800-53 standard 1226
nmap port scanner 914–916
nmbd daemon 1143
nmon tool 1130
no command 468, 507–508
nobody 118, 697
node filename 494
/etc/iscsi/nodes directory 278

nohup command 127
Nortel 963
notify option, DNS 604
Novell 13
NS DNS records 596
nscd daemon 740
nscd.conf file 740
NSD
architecture 625
configuration 625
configuration examples 625, 627–638
diffrences from BIND 626
DNSSEC performance 625
drill command 625
logging 673–674
ns name server daemon 625
nscd command 675
starting the daemon 632
unbound configuration 632–633
unbound performance tuning 636
unbound server 625
unbound.conf file 633
unbound-control command 675
nscd command 675
NSEC DNS records 659
nsswitch command 677
nsswitch.conf file 494, 733, 739, 776
nsupdate command 641
NTP protocol 288
null modem serial cable 1165, 1180
nullclient feature, sendmail 788
nwamd daemon 494

O

O'Reilly Media 1270
O'Reilly series (books) 19
O'Reilly, Tim 20, 1270
IBM Object Data Manager 432
Object Data Manager (ODM) 115, 280, 506
OC4j application server 961
ODM (Object Data Manager) 115, 280, 506
ODMDIR environment variable 115
Oetiker, Tobias 410, 886, 1278
office temperature 1109
office wiring 546
off-site backup storage 295
OM1 fiber 537
OM2 fiber 537
OM3 fiber 537
on-demand servers 1104
open source software 8
Open Web Application Security Project 947
OpenBSD 8
Open-iSCSI 277–279
OpenLDAP 731
OpenOffice 11, 1140
openprom prompt 429
OpenSolaris 8, 12
OpenSSL 972–973
openSUSE 10–11
OpenVPN 475
operating cost reduction 1098–1110
operating system installation see installation
oprofile tool 1131
options directive, DNS 561
options statement, DNS 602–609
Oracle 12
Oracle Enterprise Linux 10
$ORIGIN directive, DNS 575
orphaned processes 124, 128, 130
OSI fiber 537
OSI network protocols 520
OSPF protocol 519–521, 523
ospfd daemon 523
ospf daemon 523
OSTYPE macro, sendmail 783–784
OTRS 1193
ownership
of files 155, 157
of processes 105

P

pacadm command 1177
package management 21–26, 381–387
repositories 387
packages see software packages
packet forwarding 472, 482, 493, 499, 505, 508, 511–515
packets 452
dropped 862
filtering 904, 932
packets continued
handling with Netfilter 935–939
ICMP 938
round trip time 863
sniffers 545, 874–878
tracing 865–867
PAGER environment variable 17
paging 1129, 1132
PAM (Pluggable Authentication Modules) 109–110, 201, 721, 908–912, 1159
paper sizes 1073–1075
paper, recycled 1110
parted command 207, 225, 236
partitions 221–223, 231–237
see also filesystems
alignment 212
GPT (EFI) style 235–236
guidelines 232–233
HP-UX 237
Linux 236
load balancing 1129
Solaris 232–233, 236–237
Windows-style 233–235
passphrases 112
/etc/default/passwd file 194
/etc/security/passwd file 185
passwd command 106, 188
/etc/passwd file 176–183
editing 179, 188
group ID numbers 155
security 906–908
user ID numbers 105, 155
/etc/default/password file 907
passwords
aging 906
boot loader 900
 cracking 916
cryptography 176, 179, 1144
cryptosand 176, 179, 1144
cesw 117–118
forcing users to change 185
group 186
initial 188
root 111
Samba 1144
security 906–908
selection 111–112, 188
shadow 183–185
strength 916
when to change 112
PAT (Port Address Translation) 493
PATA interface 213–215
cables 215
power connector 215
secure erase 227–228
SMART reporting 230–231
TRIM command 228
patching 901
path MTU discovery 454
pathnames 36, 48–54
pattern matching 36, 48–54
Paxson, Vern 918
PC hardware
see also hardware
BIOSes 82
boot device priority 82
bootstrapping 82
boot device priority 82
bootstrapping 82
multibooting 85
vs. UNIX hardware 82
PCI DSS (Payment Card Industry Data Security Standard) 295, 946, 1224
PCL 1069
PCLinuxOS 10
PCRE library 49
PDF 1070
Pennock, Phil 851
Pen-pals 756
performance 1112–1133
see also performance analysis tools
analysis methodology 1117
application 1113
BIND 680
common issues 1114
CPU 1116, 1118, 1121–1123
disks 210, 212, 219–220, 1116, 1127, 1129–1131
disk typing 1115–1116
factors affecting 1115–1116
improving 1112–1117
load averages 1123
magic 1113
measuring and monitoring 886
memory 138, 1114, 1116, 1124–1127
monitoring 1115
NFS 708
nice command 129
SDSC Secure Syslog 352
sendmail 802–805
Squid web cache 975–976
SSD 1115
st_atime flag 159
syncing log files 348
troubleshooting 1131–1133
performance continued
tuning rules 1113
web server 959–963, 967
performance analysis tools
iostat command 1127
mpstat command 1122
oprofile command 1131
sar command 1129
top command 1123
uptime command 1123
vmstat command 1121
Perl 7, 54–66, 956
add-on modules 65–66
best practices 73–74
example scripts 733
file test operators 62
as a filter 64–65
generating passwords 732
hashes 57–59
I/O 61
insecure example 900
regular expressions in 49, 60
scripting 54–66
and swatch 358
variable types 55–59
wrapping cron jobs 727
permissions
on files 105, 110, 152–159, 164–172
sendmail 797–798
umask and 158
PGP (Pretty Good Privacy) 763, 925
phishing 899, 1226
phpLDAPadmin 730
Phusion Passenger 960
physical volumes eological volume management
picocom command 1181
PIDS 121
Pilgrim, Mark 67
ping command 473, 861–863
pinout, connector
DB-25 1164–1165
DB-9 1166
RJ-45 1167
pipes, named 148, 151
PJL 1070
pkgadd command 430
pkgutil command 23
pkutil command 24
/platform directory 427
Pluggable Authentication Modules (PAM) 109–110, 201, 721, 908–912
pmadm command 1177
PoE (Power over Ethernet) 540
policy 1215–1217
flow down 1228
Postfix policy daemons 841
user agreement 1227–1228
/etc/security/policy.conf file 194
pooladm command 999
poolcfg command 999
POP (Post Office Protocol) 747, 1141
ports, network 456
privileged 456, 914, 933
scanning 914–916
well known 914, 933
ports, serial 1163–1165
POSIX 7
ACLs 160–166
APIs under Windows 1141
capabilities 109
Post Office Protocol (POP) 747, 1141
postalias command 830
postcat command 830
postconf command 830, 832
Postfix 828–845
see also email
access control 837–839, 845
architecture 828
authentication 839
blacklists 840–841
chrooted 830
command-line utilities 830
configuring 831–839
content filtering 842
debugging 844–845
DKIM 852–853
local delivery 834
lookup tables 833
policy daemons 841
queues 829–830
security 830
sending email 830
spam control 840–843
virtual domains 835–837
virus scanning 842–843
postfix command 830
Postini 762
postmap command 830
PostScript 1069
postsuper command 830
posture assessment 1215
power consumption 1099
power factor 1093
power management 1091
of hard disks 229–230
power meter 1099
Power over Ethernet 540
power saving, Linux 1104
power use, measurement of 1099
PPD (PostScript Printer Description) files 1035, 1072–1073
PPIDs 121
PPP protocol 476
PPPoE 476
Pratt, Ian 991
Preston, W. Curtis 337
Pretty Good Privacy (PGP) 763, 925
preventative maintenance 1092
printcap file 1059–1065
printer cartridges, recycled 1110
PRINTER environment variable 1036, 1054
printing 1032–1083
see also BSD printing
see also CUPS
see also System V printing
architecture 1033–1034
BSD printing 1054–1065
choosing a printer 1075
CUPS 1034–1043
duplex 1076
eDocument campaign 1109
from desktop environment 1043–1045
GDI printers 1076
history 1065–1066
languages 1068–1072
major printing systems 1033–1034
network printers 1077
page description languages (PDL) 1068–1072
paper sizes 1073–1075
paper, recycled 1110
parallel printers 1077
PCL 1069
PDF 1070
PJL 1070
PostScript 1069
PPD files 1072–1073
serial printers 1077
sharing printers using Samba 1149–1152
printing continued
spooler 1033–1034
system identification 1034
System V printing 1045–1054
tips 1077–1081
tools 1067–1068
troubleshooting 1053–1054, 1081–1083
Windows driver installation 1151–1152
WinPrinters 1076
XPS 1070
priority, processes 123, 129–130
privacy 1226
/private DNSSEC key file 646
private IP addresses 462, 569, 597, 617
privedit command 108
privileged ports 456, 914, 933
privrun command 108
problem management 1225
PROC filesystem 135–136, 262, 439, 490, 1118
procedures 1215–1217
processes
control terminal 123
EGID (effective group ID) 122
EUID (effective user ID) 122
execution states 128
FSUID parameter 122
GID (group ID) 122
IDs 121
init see init process
monitoring 130–135
nicing 129–130
orphaned 124, 128, 130
ownership 105, 122
PPID (parent PID) 121
priority 123, 129–130
runaway 138–139
scheduling 105
sending signals to 127
spontaneous 79
standard I/O channels 123
stopping and starting 128
tracing 136–137
UID (user ID) 122
zombie 124, 128, 130
procmail command 746, 841
/etc/security/prof_attr file 108
/etc/profile file 190
profiler, system 1131
Project Athena 1011
provide-ixfr option, DNS 639
Index

proxies, web 974
printf command 430, 1120
ps command 130–133, 1123, 1132
pseudo-devices 419
pseudo-terminals 1162, 1170
psinfo command 1120
psstat command 1125
PTR DNS records 582, 623
public key cryptography 927
PUE 1099
Punycode 574
purchasing 1212
Purdue 1269
PuTTY 1135
P-UX Security Containment 922
pvcreate command 207–208, 246, 248, 251
pwdadm command 185, 200
PXELINUX 364
pyramid, green IT 1100–1101, 1109
Python 7, 66–73
quad A DNS records 589
Quagga routing daemon 523–524
quaggaadm command 524
quality control 1209
queue groups, sendmail 802
QUIT signal 125, 127
quota ZFS property 267
quotas, disk 698
RAID continued
RAID 5 write hole 238, 241–242
software vs. hardware 237–238
RAID-Z see ZFS filesystem
RAM disks 1129
ramd routing daemon 524
RANCID router config tool 528
RBAC (Role Based Access Control) 108–109, 190
RB (Realtime Black Lists) see blacklists
/etc/rc.boot script 95
/etc/rc.config.d directory 95
/etc/rc.log file 95
/etc/rc.serial file 1170
/etc/event.d/rc-default file 95
RCPT command, SMTP 763
rdc command 524
rdesktop command 1139
rdist command 290, 722–725
RDP (Remote Desktop Protocol) 1138
/redisk directory 226
read errors, disk 227
real-time scheduling 123
RealVNC 1138
reboot command 101
rebooting 100–101
Recovery Point Objective (RPO) 299
Recovery Time Objective (RTO) 299
recursion option, DNS 604
recycling
equipment 1107, 1110
in the workplace 1110
paper 1110
Red Flag Linux 10
red flag rule 1224
Red Hat Enterprise Linux see RHEL
redirect feature, sendmail 785
redirect router, Exim 823
redirects (ICMP) 467–468, 473, 493, 499, 505, 508–509, 514–515
redundant arrays of inexpensive disks see RAID
Reed, Darren 939
refquota ZFS property 267
refreservation ZFS property 267
refresh command 345
REFUSE_LA option, sendmail 800
regexes see regular expressions
registration of domain names see domain names, registration
regular expressions 36, 48–54
capture groups 52–53
examples 51–52
failure modes 53–54
lazy operators 53
matching process 49
in Perl 49, 60
special characters in 50–51
regulations, compliance with 1222–1229
reltime option 1105
/etc/mail/relay-domains file 791
release management 1225
rem_drv command 437
remapping
backspace key 1177
delete key 1177
Remedy 1194
Remote Desktop Protocol (RDP) 1138
remote power control 1094
renice command 129–130, 1132
replicated filesystems 715
repositories, software 385
reproducible processes 1197
request-ixfr option, DNS 639
reservation ZFS property 267
reset command 1180
resize2fs command 251
/etc/resolv.conf file 561–484
resolver configuration 483–484
resource records, DNS 555, 576–596
A 582, 596
AAAA 589
ADSP 591–594
CNAME 585
DKIM 591–594
DNSKEY 650
format 576
glue 596–597
KEY 647
MX 583–584
NS 596
NSEC 659
PTR 582, 623
quad A 589
RRSIG 649, 659
SOA 579–581, 638
special characters in 576
SRV 590–591
SPF 590–591
rack density 1092
rack power 1092–1093
racks, equipment 1094
RAID 221–222, 234, 237–245, 1115
failure recovery 241
levels 238–241
Linux 240, 242–245
Q
qmgr command 830
qshape command 844
quad A DNS records 589
Quagga routing daemon 523–524
quaggaadm command 524
quality control 1209
queue groups, sendmail 802
QUIT signal 125, 127
quota ZFS property 267
quotas, disk 698
R
rack density 1092
rack power 1092–1093
racks, equipment 1094
RAID 221–222, 234, 237–245, 1115
failure recovery 241
levels 238–241
Linux 240, 242–245
resource records, DNS continued
  SSHFP 594–595
time to live 576
  trailing dot in names 576
  TXT 588, 603
  WKS 588
restore command 310–314
retiring equipment 1107
reverse mapping, DNS 554, 582–583, 623
revision control 397–404
  Git 401–404
  Subversion 399–401
RFCs 20, 449–450
  DNS-related 688
  email-related 746
  LDAP-related 731
  NFS-related 449–450
  private address space 462
  SNMP-related 893
RHEL 11–12
  documentation 19
  named 684
  network configuration 487–489
Richards, Martin 1266
RightScale 978, 1104
RIP protocol 516, 518, 521–523
  ripd daemon 523
  RIPE DNSSEC tools 665
  RIPng protocol 518
  ripngd daemon 523
Ritchie, Dennis 1265
RJ-45 connectors 1166–1167
rm command 149–151
  rmmod command 435
  rmrole command 108
  rmuser command 195
  rndc command 638, 672, 674
    /etc/rndc.conf file 616
    /etc/rndc.key file 616
  rndc-config command 616
  roesch, Marty 918
  rogue users 1214
roleadd command 108
roleadm command 108
rolelist command 108
rolemod command 108
root account 105–106, 907
  see also RBAC
    accessing 112–118
root account continued
  accessing via NFS 697
  password 111
  user ID 105
  root filesystem 81, 146, 232
    backup copy 232
  rootkits 904
  rotating log files 356–358
  route command 466, 481–483
  routed daemon 496, 522
  Router Discovery Protocol 520
  routers 539
  routes file 487
  routing, network 465–468, 511–528
    architecture design 521–522
    autonomous systems 517–518
    CIDR (Classless Inter-Domain Routing) 458, 460–461
    Cisco routers 525–528
    cost metrics 517
demons 522–525
default routes 466, 501, 513, 521
  forwarding 472, 482, 505, 512–515
  ICMP redirects 467–468, 473, 493, 499, 505, 508–509, 514–515
  multi-ISP 518
  netmasks 458
  protocols 515–516, 518–523
  source routing 473, 493, 499, 505, 508
  static routes 466, 481–483, 521
  subnetting 458
  tables 465–467, 511–515, 871
  unreachable networks 482
  XORP (eXtensible Open Router Platform) 524
Rowland, Craig 358
  rpc.mount daemon 699
  rpc.nfsd daemon 699
  rpm command 382–383
  RPM software package format 382
  RPO (Recovery Point Objective) 299
  quotad daemon 698
  RRSIG DNS records 649, 659
  RS-232 standard 1163–1165
  rsync command 290, 335, 725–727
  rsyncd.conf file 726
  rsyncd.secrets file 727
  RT (Request Tracker) 1193
RTO (Recovery Time Objective) 299
RTS (request to send) signal 1168
Ruby 7, 66
Ruby on Rails 960
run levels 1174
  changing 89
  init and 88–91, 1174
  RunAsUser sendmail user account 796
runaway processes 138–139
running Linux programs from
  Windows 1136–1137
  rxvt command 1141
  s
  S/MIME 763
  SAAS (Software as a Service) 987
  sacadm command 1176–1177
  Safe Harbor 1224
  SafeFileEnvironment option, sendmail 799
  SAGE (System Administrators Guild) 1230
  SAIT backup tapes 302
  sam sysadmin tool (now smh) 201
  Samba 166, 1142–1160
    see also Windows
    Active Directory integration 1154–1160
    CIFS 1142
    command-line file transfer
      program 1148
    compiling for Active Directory
      integration 1156
    configuration 1143
daemons 1143
    debugging 1152–1154
    displaying active connections
      and locked files 1153
    file sharing 1146
    filename encoding 1145
    group shares 1146
    installation 1143–1144
    Kerberos configuration 1156
    listing configuration options 1144
    log files 1152
    net command 1158
    password encryption 1144
    printer sharing 1149–1152
    security 1143
Index

Samba continued
setting up passwords 1144
sharing files 1142
troubleshooting 1152–1154
user authentication 1145
UTF-8 encoding 1145
winbind 1155
SAN see storage area networks
SANS Institute 945, 948, 1230, 1270
sar command 873, 1125, 1129
Sarbanes-Oxley Act (SOX) 946, 1223, 1225
SAS interface see SCSI interface
SASL (Simple Authentication and Security Layer) 801
SATA interface 214–216
cables 216
secure erase 227–228
SMART reporting 230–231
TRIM command 228
vs. SCSI 219–220
savelog 358
/sbin directory 146
SCA-2 connector (SCSI) 217
Scarab 1193
sched_mc_power_savings kernel parameter 1105
sched_smt_power_savings kernel parameter 1105
schedulers, I/O 1130–1131
scheduling classes 123
Schneier, Bruce 948
Schweikert, David 1278
scientific method 1117
scp command 926
scripting 29–74
see also bash
see also Perl
best practices 73–74
SCSI interface 214
addressing 218
connector diagrams 217
connectors 217
parallel 216–218
termination 217
troubleshooting 218
vs. SATA 219–220
S-DLT backup tapes 301
SDSC Secure Syslog 352
search directive, DNS 561
search path 22
SEC (Simple Event Correlator) 359
secondary partitions 235
secure erase 227–228
Secure Sockets Layer (SSL) 475, 801
secure tunnel 942
/etc/default/security file 195
security
see also cryptography
access control 103–118
AIX 507–508
of backups 295, 903
BIND 571
Bro network intrusion detection system 918
buffer overflows 899
CBK (common body of knowledge) 945
certifications 944–945
CGI scripts 960
chroot and 913
CISA (Certified Information Systems Auditor) 945
CISSP (Certified Information Systems Security Professional) 945
Common Criteria 947
configuration issues 900
of credit cards see PCI DSS
(Payment Card Industry Data Security Standard)
cryptography 176, 179, 924, 1144
denial of service (DOS) attacks 583, 727, 800–801, 1132
of discarded disks 227–228
DNS 571
DNSSEC 573, 648–667
DOS attack via syslog 349
email 763
email to files 759
email to programs 759, 798–799
encryption see cryptography
firewalls 932–942
flaws in UNIX and Linux 897
GIAC (Global Information Assurance Certification) 945
handling attacks 950–952
hardening practices 901
HIDS 904, 919
hints 905
HP-UX 505–506
identifying open ports 871, 902
identity theft 1224
Security continued
information sources 947–950
IP firewalls 474–475, 499–500, 932–942
IPFilter 939–942
iptables 935–939
Kerberos 110, 924–925
LDAP and 735
Linux 492
login names, uniqueness 178
loss from breach 897
mandatory access control (MAC) 922
monitoring 904–905, 935
of named 643–645
NFS 695–698, 700, 709
NIDS 918
NIST 800 security standards 947
of Exim 810
of networks 107
of passwords 906–908
OSSEC host intrusion detection system 919–922
overview 896–901
OWASP 947
packet sniffers 874–878
PAM 109–110, 201, 721, 908–912
of passwd file 906–908
password encryption algorithms 179
of passwords 111, 176, 179, 905, 916
PCI Data Security Standard 946
phishing 899
port scanning 914–916
of Postfix 830
removing unnecessary services 902
reporting break-ins 952
root account 907
rootkits 904
Samba 1143
SDSC Secure Syslog 352
of search paths 113
secure tunnel 942
SELinux 923–924
of sendmail 795–801
setuid programs 912–913
/etc/shadow file 906–908
shadow passwords 183–185
SNMP 882
**security continued**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snort network intrusion detection system</td>
<td>918</td>
</tr>
<tr>
<td>Solaris</td>
<td>499</td>
</tr>
<tr>
<td>SSH</td>
<td>926–930</td>
</tr>
<tr>
<td>SSHP DNS records</td>
<td>594–595</td>
</tr>
<tr>
<td>SSL</td>
<td>971–974</td>
</tr>
<tr>
<td>standards</td>
<td>945–947</td>
</tr>
<tr>
<td><strong>stunnel</strong></td>
<td>930–932</td>
</tr>
<tr>
<td><strong>sudo</strong> command</td>
<td>113–116</td>
</tr>
<tr>
<td>tools</td>
<td>914–932</td>
</tr>
<tr>
<td>Trojan horses</td>
<td>903</td>
</tr>
<tr>
<td>TSIG (transaction signatures)</td>
<td>623, 645–648</td>
</tr>
<tr>
<td>user account hygiene</td>
<td>175</td>
</tr>
<tr>
<td>vigilance</td>
<td>175</td>
</tr>
<tr>
<td>viruses</td>
<td>825–826, 842–843, 903</td>
</tr>
<tr>
<td>of VPNs</td>
<td>475–476, 942–944</td>
</tr>
<tr>
<td>vs. convenience</td>
<td>898, 900</td>
</tr>
<tr>
<td>web script</td>
<td>960</td>
</tr>
<tr>
<td>of wireless networks</td>
<td>543</td>
</tr>
<tr>
<td>X Window System</td>
<td>1015–1019, 1137</td>
</tr>
<tr>
<td><strong>sendmail continued</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Installation and Operation Guide</strong></td>
<td>854</td>
</tr>
<tr>
<td>logging</td>
<td>806–807</td>
</tr>
<tr>
<td><strong>m4</strong> and</td>
<td>779–782, 789</td>
</tr>
<tr>
<td>masquerading</td>
<td>787</td>
</tr>
<tr>
<td>ownership, files</td>
<td>796–797</td>
</tr>
<tr>
<td>performance</td>
<td>802–804</td>
</tr>
<tr>
<td>permissions</td>
<td>797–798</td>
</tr>
<tr>
<td>privacy options</td>
<td>799–800</td>
</tr>
<tr>
<td>queue groups</td>
<td>802</td>
</tr>
<tr>
<td>queue runners</td>
<td>802</td>
</tr>
<tr>
<td>queues</td>
<td>777–778, 802, 806</td>
</tr>
<tr>
<td>rate and connection limits</td>
<td>793</td>
</tr>
<tr>
<td>Red Hat</td>
<td>92</td>
</tr>
<tr>
<td>relaying</td>
<td>791–792</td>
</tr>
<tr>
<td>security</td>
<td>795–801</td>
</tr>
<tr>
<td>and the service switch file</td>
<td>776</td>
</tr>
<tr>
<td>slamming</td>
<td>793</td>
</tr>
<tr>
<td>using SMTP to debug</td>
<td>750</td>
</tr>
<tr>
<td>spam control features</td>
<td>789–795</td>
</tr>
<tr>
<td>startup script</td>
<td>93</td>
</tr>
<tr>
<td>statistics</td>
<td>805</td>
</tr>
<tr>
<td>version of 775</td>
<td>775</td>
</tr>
<tr>
<td><strong>virtuersetable feature</strong></td>
<td>786</td>
</tr>
<tr>
<td>Sendmail, Inc.</td>
<td>801</td>
</tr>
<tr>
<td><strong>sendmail.cf</strong> file</td>
<td>777–778</td>
</tr>
<tr>
<td><strong>serial</strong> file</td>
<td>1170</td>
</tr>
<tr>
<td>serial cables</td>
<td>1163–1168</td>
</tr>
<tr>
<td>DB-9 to DB-25</td>
<td>1166</td>
</tr>
<tr>
<td>modem</td>
<td>1165</td>
</tr>
<tr>
<td>null modem</td>
<td>1165</td>
</tr>
<tr>
<td>RJ-45 to DB-25</td>
<td>1167</td>
</tr>
<tr>
<td>straight-through</td>
<td>1164–1165</td>
</tr>
<tr>
<td><strong>serial connectors</strong></td>
<td></td>
</tr>
<tr>
<td>DB-25</td>
<td>1163–1165</td>
</tr>
<tr>
<td>DB-9</td>
<td>1166</td>
</tr>
<tr>
<td>RJ-45</td>
<td>1166</td>
</tr>
<tr>
<td>serial drivers</td>
<td>420</td>
</tr>
<tr>
<td>serial ports</td>
<td>1163–1165</td>
</tr>
<tr>
<td>bidirectional</td>
<td>1169</td>
</tr>
<tr>
<td>breakout boxes</td>
<td>1180</td>
</tr>
<tr>
<td>consoles</td>
<td>1180</td>
</tr>
<tr>
<td>DCE vs. DTE</td>
<td>1164–1165</td>
</tr>
<tr>
<td>debugging</td>
<td>1180</td>
</tr>
<tr>
<td>device files</td>
<td>1168–1170</td>
</tr>
<tr>
<td>drivers, special characters</td>
<td>1177–1180</td>
</tr>
<tr>
<td>flow control</td>
<td>1168</td>
</tr>
<tr>
<td>HP-UX</td>
<td>1169</td>
</tr>
<tr>
<td>parameters, setting</td>
<td>1169–1170</td>
</tr>
<tr>
<td>resetting</td>
<td>1179–1180</td>
</tr>
<tr>
<td>setting options</td>
<td>1178–1180</td>
</tr>
<tr>
<td>Solaris</td>
<td>1176–1177</td>
</tr>
<tr>
<td><strong>Server Name Indication (SNI)</strong></td>
<td>968</td>
</tr>
<tr>
<td><strong>server statement, DNS</strong></td>
<td>610, 639</td>
</tr>
<tr>
<td><strong>server utilization</strong></td>
<td>983</td>
</tr>
<tr>
<td><strong>servers</strong></td>
<td></td>
</tr>
<tr>
<td>consolidation</td>
<td>1102</td>
</tr>
<tr>
<td>DNS/BIND</td>
<td>563–566</td>
</tr>
<tr>
<td>energy optimization of</td>
<td>1104–1105</td>
</tr>
<tr>
<td>HTTP</td>
<td>963</td>
</tr>
<tr>
<td>load balancing</td>
<td>1114</td>
</tr>
<tr>
<td>master NIS</td>
<td>736–737</td>
</tr>
<tr>
<td><strong>name see BIND, DNS, and</strong></td>
<td></td>
</tr>
<tr>
<td><strong>named</strong></td>
<td></td>
</tr>
<tr>
<td><strong>NFS</strong></td>
<td>698–705, 711</td>
</tr>
<tr>
<td><strong>NIS slave</strong></td>
<td>736–737</td>
</tr>
<tr>
<td>Squid</td>
<td>974–976</td>
</tr>
<tr>
<td>system files</td>
<td>727</td>
</tr>
<tr>
<td>virtualization</td>
<td>1103</td>
</tr>
<tr>
<td>VNC</td>
<td>1138</td>
</tr>
<tr>
<td>web proxy</td>
<td>974</td>
</tr>
<tr>
<td>X Window System for Windows</td>
<td>1137, 1141</td>
</tr>
<tr>
<td><strong>servers on demand</strong></td>
<td>1104</td>
</tr>
<tr>
<td>Service Access Facility</td>
<td>1176</td>
</tr>
<tr>
<td>service level agreements</td>
<td>1186–1190</td>
</tr>
<tr>
<td>measurement of 1189–1190</td>
<td>1187</td>
</tr>
<tr>
<td>service management facility</td>
<td>97</td>
</tr>
<tr>
<td>fault management resource identifiers</td>
<td>97</td>
</tr>
<tr>
<td>manifests and profiles</td>
<td>98</td>
</tr>
<tr>
<td>predictive self-healing</td>
<td>99</td>
</tr>
<tr>
<td>service switch file</td>
<td>776</td>
</tr>
<tr>
<td>ServiceDesk</td>
<td>1194</td>
</tr>
<tr>
<td><strong>/etc/services</strong> file</td>
<td>456, 933</td>
</tr>
<tr>
<td><strong>setfacil</strong> command</td>
<td>165</td>
</tr>
<tr>
<td>setrlimit system call</td>
<td>1133</td>
</tr>
<tr>
<td><strong>/etc/init.d/setserial</strong> script</td>
<td>1170</td>
</tr>
<tr>
<td>setserial command</td>
<td>1169</td>
</tr>
<tr>
<td>setuid/setgid bits</td>
<td>106–107, 153–154, 912–913</td>
</tr>
<tr>
<td><strong>sfdisk</strong> command</td>
<td>207</td>
</tr>
<tr>
<td><strong>sh</strong> see <strong>bash</strong></td>
<td></td>
</tr>
<tr>
<td><strong>/etc/shadow</strong> file</td>
<td>183–185, 906–908, 1171</td>
</tr>
<tr>
<td>shadow passwords</td>
<td>183–185</td>
</tr>
<tr>
<td>Shaprio, Gregory</td>
<td>801</td>
</tr>
<tr>
<td>share (Samba)</td>
<td>1142</td>
</tr>
<tr>
<td><strong>share command</strong></td>
<td>271, 699–700</td>
</tr>
<tr>
<td>SHARE user group</td>
<td>1265</td>
</tr>
<tr>
<td>shareall command</td>
<td>699</td>
</tr>
<tr>
<td><strong>shareiscsi</strong> ZFS property</td>
<td>272</td>
</tr>
<tr>
<td><strong>sharens</strong> ZFS property</td>
<td>271</td>
</tr>
</tbody>
</table>
Index

sharesmb ZFS property  271
sharing a filesystem see NFS sharing a filesystem
shebang  37
shell
  see also bash
globbing 14, 51
login 182
startup files 189
SHELL variable 1179
/etc/shells file 182–183
Shimpi, Anand 213
shocking nonsense 111
showmount command 706
shred utility  228
shutdown command 100–101, 349
  signals  124–127
  see also individual signal names
called, blocked, or ignored 125
CONT 125–126, 128
HUP 125–126
INT 125–126
KILL 125–127
list of important 125
QUIT 125, 127
sending to a process 127
STOP 125–126, 128
TERM 125–127
TSTOP 125–126, 128
WINCH 125–126
Simple Mail Transport Protocol see SMB protocol
single mode fiber  537
single sign-on systems 202
CAS 203
JOSSO 203
Likewise Open 203
single-user mode
AIX 87
booting to 80, 86
bypassing 80
HP-UX 87
Linux 86
manual booting 80
remounting the root filesystem 81
Solaris 86
/etc/skel directory 190
SLA see service level agreement
Slackware Linux 10
slamming, controlling in sendmail 793
slapd daemon 731
slave servers, NIS 736–737
slurpd daemon 731
SMART monitoring 230–231
SMART_HOST macro, sendmail 787
smartctl command 231
smartd daemon 231
/etc/smbd.conf file 231
SMB protocol see Samba
smb.conf file 1143, 1149, 1153
smbclient 1148
smbcontrol 1153
smbd daemon 1143
smbfs filesystem 1148
smbpasswd 1144
smbstatus 1153
smsh sysadmin tool (HP-UX) 201
SMP (symmetric multiprocessing) 1122
snmpd daemon 731
SNMP 879–889
agents 883–886
using Cacti 886
CiscoWorks and 889
community string 882
data collection 886
data organization 881
HP-UX 96
MIBs (Management Information Bases) 881
using Nagios 887
OIDs (object identifiers) 881–882
RMON MIB 883
security 882
tools 885–888
traps 882
software
  see also software package tools
  see also software packages
  compilation 25–26
  installation 21–26
  open source 8
  package management 21–26
  sharing over NFS 411
  vulnerabilities 899
software as a service (SAAS) 987
software flow control 1168
software licenses 1228–1229
software package tools
  see also package management
  see also software
  see also software packages
  alien 382
  APT 387–391
  apt-get 387–391
  dpkg 383
  high level, Linux 384–387
  rpm 382–383
  /etc/apt/sources.list file 388
  yum 391
Solaris 12
ACI management 172
disk addition recipe 208
disk device files 224–225
disk partitions (slices) 232–233, 236–237
documentation 19
installation 370–376
iSCSI support 279–280
kernel configuration 427–431
loadable drivers 436–437
log files 344
mandatory access control (MAC) 922
named 684
network configuration 494–501
NFS (Network File System) 700–701, 708
Solaris continued

security 499
service management facility see service management facility
single-user mode 86
startup scripts 97–100
trusted extensions 922
volume manager 246
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316

solid state disks 206, 209–210, 212–213, 228
Solaris continued

service management facility see service management facility
single-user mode 86
startup scripts 97–100
trusted extensions 922
volume manager 246
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316

solid state disks 206, 209–210, 212–213, 228
Solaris continued

service management facility see service management facility
single-user mode 86
startup scripts 97–100
trusted extensions 922
volume manager 246
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316

solid state disks 206, 209–210, 212–213, 228
Solaris continued

service management facility see service management facility
single-user mode 86
startup scripts 97–100
trusted extensions 922
volume manager 246
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316

solid state disks 206, 209–210, 212–213, 228
Solaris continued

service management facility see service management facility
single-user mode 86
startup scripts 97–100
trusted extensions 922
volume manager 246
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316

solid state disks 206, 209–210, 212–213, 228
Solaris continued

service management facility see service management facility
single-user mode 86
startup scripts 97–100
trusted extensions 922
volume manager 246
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316

solid state disks 206, 209–210, 212–213, 228
Solaris continued

service management facility see service management facility
single-user mode 86
startup scripts 97–100
trusted extensions 922
volume manager 246
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316

solid state disks 206, 209–210, 212–213, 228
Solaris continued

service management facility see service management facility
single-user mode 86
startup scripts 97–100
trusted extensions 922
volume manager 246
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316

solid state disks 206, 209–210, 212–213, 228
Index

State University of New York (SUNY) Buffalo 1269
stateful inspection firewalls 934
static routes 466, 481–483, 521
static_routes file 483
static-routes file 488–489
statistics
    BIND 676
    CPU 1122
    network 868–873
    NFS 710
sendmail 805
STD documents 450
sticky bit 154–155
STOP signal 125–126, 128
storage area networks 274–281
    AIX 280–281
    benefits of 1103
    HP-UX 280
    iSCSI 276–281
    Linux 277–279
    Solaris 279–280
    utilization 1103
storage management see disks
Storage Technology 303
strace command 136
straight-through serial cables 1164–1165
STREAMS 509
striping (RAID 0) 239–240, 248, 253
stty command 1167, 1178, 1180
stunnel 930–932
su command 113
submission agents, email (MSA) 745
subnetting 458–461, 479, 495
Subversion 399–401
superblocks (filesystem) 257
superuser see root account
SUSE Linux 9, 11
    documentation 19
    named 683
    network configuration 486–487
svcadm command 98
svcfg command 99
svcs command 97, 494
svn command 400
svnserve daemon, Subversion 399
svnserve.conf file 399
swaks command 773, 828
swap command 264, 1125
swap space 222, 264
swapinfo command 264, 1125
swapon command 261, 264, 1125
/etc/swapspaces file 264
swatch 358
swininstall command 25, 377, 395
switch file 682
switches 534, 538–539, 543
swrole command 108
symbolic links 148, 151
symmetric multiprocessing (SMP) 1122
Sympa 761
sync command 101
sync system call 101, 258
synchronizing files
    copying 721
    rdist 722–725
    rsync 725–727
    wget 727
/sys directory 438
/proc/sys directory 421
/etc/sysconfig directory 92–93, 487–488
sysctl command 348
/etc/syslog.conf file 345–351
syslog 344–351
    see also log files
    see also logging
    actions 348
    alternatives 351
    architecture 345
    central server 350
    configuring 345–351, 355
    debugging 351
    and DNS logging 667–672
    and network logging 673–674
    and logging 667–672
    and DNS attack via 349
    facilities and severity levels 346
    facility names 346
    m4 preprocessor on Solaris 348
    network logging configuration 349
    restarting 345
    security 349, 352
    severity levels 347
    /etc/syslog.conf file 345–351
    syslogd daemon 345
    time stamps 347
    /etc/syslog.conf file 345–351, 807
    syslogd daemon 345
    syslog-ng replacement for syslog 351
/etc/system file 428–429
system administration 26
    disaster recovery 298
    essential tasks 4–6
    GUI tools 6, 13
    Internet resources 20
    toolbox 1095
system administrator
    conferences 1229–1231
    exit checklist 1209
    firing 1208
    happiness 1186
    hiring 1207
    history 1264–1273
    interviewing 1208
    legal considerations 1226–1229
    priorities 1188–1189
    roles and responsibilities 1189
    skill sets 1195
    time management 1196
    training resources 1229–1231
system administrator management see information technology (IT) management
system configuration 404–411
    see also hardware
    see also Linux installation
    see also system administration
cfengine 408
CIM (Common Information Model) 410
LCFG (large-scale configuration system) 409
management 408–411
Template Tree 2 410
System V printing 1045–1054
    see also printing
accept command 1051
cancel command 1051
classes 1046
configuration 1048–1051
destinations 1046
disable command 1052
enable command 1052
interface programs 1052–1053
lp command 1047
lpadmin command 1048–1050
lpmove command 1052
lpchid command 1046
lpsched daemon 1047
lpshut command 1048
lpstat command 1051
reject command 1051
troubleshooting 1053–1054
System V UNIX 13
system-config-network command 487

T

tail command 36
tape drives, device names 420
tapes, backup
see also media, backup
4mm 301
8mm 301
AIT 302
AME 302
and multiple files 317
blocking factor 315
copying 316
DDS/DAT 301
device files 309
DLT/S-DLT 301
library, robotic 318
LTO 302
SAIT 302
stackers 303
VXA 302
tar command 315–316
target numbers (SCSI) 218
/etc/iscsi/targets file 280
TCP connection states 870
TCP wrappers 506
TCP/IP see IP
tcpdump command 875
tee command 35
telnetting 1110
telinit command 89, 1175
temperature
data center 1087, 1108
effect on hard disks 211
office 1109
Template Tree 2 410
temporary files, removing 289
TERM environment variable 1178
TERM signal 125–127
termcap file 1172
terminals Terminal Server service, Windows 1139
terminals continued Ubuntu 1176
unwedging 1179–1180
terminators (SCSI) 217
terminfo file 1172
testing, system 406
testparm 1144
Texinfo 18
text editors 6–7
The Green Grid 1110
Third Brigade 919
Thompson, Ken 1265
threads, kernel 79
Thunderbird mail client 745
TIA (Telecommunications Industry Association) 534
TIA/EIA-568A standard 536	
ticketing systems 1191–1196
TightVNC 1138
Time Slider widget 269–270
time to live (TTL), packets 865
tip command 1181
TLS (Transport Layer Security) 475, 801
TLT/S-DLT tapes 301
/tmp directory 146, 232
TO_ICONNECT option, sendmail 803
Tomcat application server 961
tools, hardware 1095
top command 133–135, 1123, 1132
Torvalds, Linus 1271
trace route command 865–867
Track-It! 1194
transfer-source option, DNS 623
transport agents, email 746
Transport Layer Security (TLS) 475, 801
Tridgell, Andrew 725, 1142
TRIM command (disks) 228
Trojan, Erik 356
Troy horses 903
Troxmar, Michal 930
Trouble Ticket Express 1193
troubleshooting
see also performance
Bacula 334–335
BIND 667–681
disk hardware 226–227
Exim 827–828
named 667–681
network hardware, cable analyzers 545
network hardware, sniffers 545
troubleshooting continued
network hardware, T-BERD
line analyzer 545
networks 544–545, 860–873
Postfix 844–845
printing 1053–1054, 1081–1083
runaway processes 138–139
Samba 1152–1154
SCSI problems 218
sendmail 805–807
serial line 1180
sluggish system 1131–1133
Solaris kernel 430
ssl log 351
wedged terminal 1179
X Window System 1026–1028
Xorg X server 1026–1028
Trusted AIX 922
TrustedUser sendmail user account 796
Ts’o, Theodore 255
tset command 1178, 1180
TSIG (transaction signatures) 623, 645–648
TSM (Tivoli Storage Manager) 336
TSTP signal 125–126, 128
TTL (time to live), packets 865
$TTL directive, DNS 575–576, 581
TTL for DNS resource records 576
/dev/tty device 35
ttyadm command 1177
ttydefs file 1176
ttmym command 1177
ttytype file 1172
tune2fs command 256, 259
tuning
AIX kernel 434
Linux kernel 421–423
NFS 708
Tux logo 11
Tweedie, Stephen 255
TXT DNS records 588, 603
typeglobs, Perl 64
typographic conventions 13–14

U

Ubuntu Linux 10–11
documentation 19
named 682
network configuration 486
udev system 419, 437, 439
Index

udevadm command 438–439
udevd daemon 150, 419
UDP (User Datagram Protocol) 450
UFS filesystem 254
UIDs see user IDs
Ultrasound project 1138
umask command 158, 190
umount command 144–145, 261, 708
uname command 435
unbound-control commands 675
undeliverable messages, sendmail 803
uninterruptible power supplies (UPSs) 1086, 1091, 1220
uniq command 35
units 14–15
University of California at Berkeley 1268
University of Colorado 1269
University of Maryland 1269
University of Utah 1269
UNIX
- history of 1265–1273
- origin of name 1266
- reasons to choose 1113
- vs. Linux 7–9
UNIX File System (UFS) 254
UNIX package management 393–397
AIX 396
HP-UX 394
Image Packaging System 394
installp command 397
pkg tool for Solaris 394
Solaris 394
swinstall command for HP-UX 395
unlink system call 151
unshare command 271
unshielded twisted pair see UTP cables
unsolicited commercial email see spam
unwedging terminals 1179
updatedb command 23
update-policy clause, DNS 641
update-rc.d command 94
updating zone files, DNS 640–642
upgrades 314–315
UPPUs (uninterruptible power supplies) 1086, 1091, 1220
Upstart daemon 94, 1176
uptime command 1123, 1132
Uptime Institute, The 1086
URI (Uniform Resource Identifier) 957
URL (Uniform Resource Locator) 957–958
protocols 958
URN (Uniform Resource Name) 957
USB disks 263, 300
US-CERT 948
use_cv_file feature, sendmail 784
USENIX Association 1229–1230, 1270
/etc/security/user file 185, 195
user accounts
- adding by hand 187–191
- adding in bulk (Linux) 197
- adding with useradd 191–197
- AIX options 196
- aliases, global (email) 178
- authentication under Samba 1145
- centralized management 201
- daemon 118
- disabling 200
- email home 190
- GECOS information 181
- GIDs (group ID) 181
- home directories 146, 182, 189, 233
- hygiene 175
- LDAP and AD 202
- locking and unlocking 200
- login names 176–178
- login shell 182
- managing with GUI tools 201
- nobody (NFS) 118, 697
- password encryption 179
- passwords 188
- policy agreements 191
- pseudo-users 118, 180
- RBAC 190
- removing 198–199
- roles and administrative privileges 190
- sendmail use of 796
- shared 907
- single sign-on systems 202
- startup files 189
- sys 118
- testing 191
- UIDs (user IDs) 180–181
- user accounts continued
  - user management config files 192
  - user management tools 175, 192
- vipw command 188
- user agents, email 744
- user IDs 105
  - in ls output 155
  - real, effective, and saved 105
- user management tools 175
- user policy agreement 1227–1228
- user workspaces, green strategies for 1108–1110
- /etc/user_attr file 108
- /etc/default/useradd file 193, 195
- useradd command 175, 187, 191
  - example 197
  - on AIX 195
  - on HP-UX 194
  - on Red Hat 193
  - on Solaris 194
  - on SUSE 193
  - on Ubuntu 192
- useradd.local script 193
- userdel command 175
- userdel.local script 199
- usermod command 184
- usernames see user accounts
- /usr directory 146
- UTP cables 534–536, 545
- UUIDs, for partitions 262
- UW imapd IMAP server 747

V

van Rossum, Guido 67
Vantages DNSSEC framework 665
/var directory 146, 233
VAX 1268
vendor logos 11
vendors we like 550
Venema, Wietse 828, 1171
Veritas 246, 251, 256, 336
/etc/vfstab file 143, 259–260, 263, 708, 711
vgcreate command 207–208, 248, 252
vgdisplay command 208, 248, 250
vgextend command 252
vi editor 6, 30
view statement, DNS 617
.vimrc file 189
vipw command 188
virsh command 997
virt-install command 993, 996
virt-manager application 993
virtual domains, Postfix 835–837
virtual hosts, web 967–971
virtual memory 1124–1125
Virtual Network Computing see VNC protocol
virtual network interfaces 481
virtual terminals and X 1026
VirtualHost clause, Apache 971
virtualization see also KVM
see also Xen
see also zones and containers
AIX workload partitions 1001–1002
Amazon web services 1005–1009
benefits of 988–989, 1103
challenges 1103
cloud computing 987
definition 983
hardware suggestions 990
history of 984
hypervisor 985
Integrity virtual machines 1003–1004
Linux 991–997
live migration 988
paravirtualization 986
types of 984–988
virtuseretable feature, sendmail 786
virus scanning 761–773, 903
see also email
amavisd-new 769–773
testing 773
using Exim 818–819
using Postfix 840–843
using sendmail 794–795
visudo command 116
Vixie, Paul 287
Vixie-cron 287–288
VLANS 539
vmstat command 1121–1122,
1126–1127, 1132
VMware 1005, 1139
VNC protocol 1138
vncserver command 1138
volume groups see logical volume management
volume snapshots 249, 259, 269–271
VPNs (virtual private networks) 475–476, 942–944
IPsec tunnels 943
SSH tunnels 943
VRFY command 763
VT100 terminal 1175
vtysh command 524
VXA backup tapes 302
VxFS filesystem 256–257

W

wait system call 124
Wall, Larry 7, 54
Ward, Grady 111
WBEEM (Web-Based Enterprise Management) standard 880
wc command 35
Web 2.0 956
web hosting 957–976
Apache 963–974
Apache configuration 965–974
Apache installation 964–966
application servers 960
caching server 974–976
CDN (content distribution network) 978–979
certificates 972–974
CGI scripting 959
and cloud computing 978
c-o-locatio-ration 978
content distribution network (CDN) 978–979
embedded interpreters 959
IIS (Windows) 1141
load balancing 961–963
log files 966
performance 961–963, 967
proxy servers 974–976
security 960, 971–974
Squid cache 974–976
SSL 971–974
static content 967
virtual interfaces 967–971
WebLogic application server 961
WebSense 755
WebSphere application server 961
well-known ports 914, 933
WEP (Wired Equivalent Privacy) 543
wget command 23, 727
Whaley, Ben 1279
wheel group 113, 181
whereis command 23
which command 22
Wi-Fi Protected Access 543
Wikipedia 8
Win4Lin 1140
winbind Samba component 925, 1155
WINCH signal 125–126
Windows see also Samba
accessing remote desktops 1136
ACLs 1146
Active Directory authentication 1154–1160
automounter 1147
backups 335
DFS (Distributed File System) 1147
dual booting 1140
email and web standards compliance 1141
IMAP 1141
logging in from 1135
mounting Windows filesystems 1148
multibooting with LINUX 85
POP (Post Office Protocol) 1141
printing 1151–1152
RDP (Remote Desktop Protocol) 1138
running Linux programs from 1136–1137
running under VMware 1139
running Windows programs under Linux 1139
sharing files 1142
SMTP 1141
Terminal Server service 1139
UNIX software running on 1141
VNC servers 1138
Wine project 1139
X forwarding 1137
X Window System servers 1137, 1141
xterm for 1141
Windows MBR 82, 233–235
Wine project 1139
WinSCP 1136
Wired Equivalent Privacy 543
Index

wireless networks 541–543
wireless networks see networks, wireless
wireless standards 542
Wireshark packet sniffer 545, 877
wiring see network wiring
wiring standards 546–547
WKS DNS records 588
workload partitions 1001–1002
workstation
  count per user 1109
  sizing 1109
  timeout 1109
World Wide Web
  HTTP protocol 957–959
  URIs 957
  URLs 957
  URNs 957
WPA see Wi-Fi Protected Access
WPAR see workload partitions
wrapper scripts for localization 413
write errors, disk 227
write hole (RAID 5) 238, 241–242

X

X display manager 1013–1014
X Window System 1011–1030
see also Xorg
  X server architecture 1012
  client authentication 1016–1017
  client/server model 1012
  desktop environments 1028–1030
  DISPLAY environment variable 1015, 1019
  display manager 1013–1014
  history 1011–1012
  killing the X server 1026
  magic cookies 1016
  running an application 1014–1019
  security 1015–1019
  security under Windows 1137
  SSH and 1017–1019
  startup files 189
  troubleshooting 1026–1028
  virtual terminals 1026
  Windows servers 1137, 1141
  X forwarding 1137
  X server output 1027–1028
X11 see X Window System

xargs command 143
xauth command 1016
xdd tool 1129
.Xdefaults file 189
xdm directory 1013
xdpyinfo command 1028
Xen 991–995
see also virtualization
  configuration files 992
  distribution support 991
donut 991
  live migration 994
  virt-install command 993
  virtual block devices 992
  xend daemon 992
  xm command 991, 994
  xend daemon 992
  XFree86 X Server 1011
  xhost command 1016–1017
  xinit command 1013
  .xinitrc file 189
  xkcd.com 1087
  xm command 991
  xntpd command 130
  XON/XOFF 1168
  Xorg
    X server 1019–1024
    configuring 1019–1024
    debugging 1026–1028
    logging 1027–1028
  xdpyinfo command 1028
  xorg.conf file 1019–1024
  xorgconfig tool 1019
  xrandr command 1025
  xorg.conf file 1019–1024
  xorgconfig tool 1019
  XRORP (eXtensible Open Router Platform) 524
  XPS 1070
  xrandr command 1025
  xsession file 1014
  ~/.xsessions file 1014
  xtab file 699
  xterm console emulator 1141
  /var/yp file 736–737
  yp* commands 737–738
  ypupdated daemon 738
  yum command 24, 391

Y

Yahoo! Mail, 743
YaST 486
yast command 24
Yegge, Steve 7
Ylönen, Tatu 926
Yost wiring standard 1167
Yost, Dave 1167
Z

Zebra routing daemon 523
Zend server 960
Zeus 963
zfs command 266–272
  ~/.zfs directory 269
ZFS filesystem 161, 166–172, 208, 222, 232, 240, 242, 264–274, 316
  architecture diagram 265
  properties 267–269
  RAID-Z implementation 265–266
  raw volumes 271
  snapshots and clones 269–271
  storage pools 265, 272–274
Zimbra 745, 747, 853
Zimmermann, Phil 763, 925
zombie processes 124, 128, 130
zone statement, DNS 612–615
zoneadm command 999
zonecfg command 999
zones and containers 997–1001
see also virtualization
  advanced features 1001
  global zone 998
  sparse 998
  whole-root 998
zones, DNS 563
  commands 574–575
  files 574
  linkage 596–597
  transfers 564, 639–640
  updating files 640–642
zone-statistics option, DNS 613
zpool command 208, 266, 272–274
zypper command 392