The Practice of System and Network Administration

Second Edition
This page intentionally left blank
## Contents at a Glance

### Part I  Getting Started  
1  
Chapter 1  What to Do When . . .  
Chapter 2  Climb Out of the Hole  

### Part II  Foundation Elements  
39  
Chapter 3  Workstations  
Chapter 4  Servers  
Chapter 5  Services  
Chapter 6  Data Centers  
Chapter 7  Networks  
Chapter 8  Namespaces  
Chapter 9  Documentation  
Chapter 10  Disaster Recovery and Data Integrity  
Chapter 11  Security Policy  
Chapter 12  Ethics  
Chapter 13  Helpdesks  
Chapter 14  Customer Care  

### Part III  Change Processes  
389  
Chapter 15  Debugging  
Chapter 16  Fixing Things Once  
Chapter 17  Change Management  
Chapter 18  Server Upgrades  
Chapter 19  Service Conversions  
Chapter 20  Maintenance Windows  
Chapter 21  Centralization and Decentralization
### Contents at a Glance

#### Part IV Providing Services 521
- Chapter 22 Service Monitoring 523
- Chapter 23 Email Service 543
- Chapter 24 Print Service 565
- Chapter 25 Data Storage 583
- Chapter 26 Backup and Restore 619
- Chapter 27 Remote Access Service 653
- Chapter 28 Software Depot Service 667
- Chapter 29 Web Services 689

#### Part V Management Practices 725
- Chapter 30 Organizational Structures 727
- Chapter 31 Perception and Visibility 751
- Chapter 32 Being Happy 777
- Chapter 33 A Guide for Technical Managers 819
- Chapter 34 A Guide for Nontechnical Managers 853
- Chapter 35 Hiring System Administrators 871
- Chapter 36 Firing System Administrators 899
- Epilogue 909

#### Appendixes 911
- Appendix A The Many Roles of a System Administrator 913
- Appendix B Acronyms 939
- Bibliography 945
- Index 955
1.20 Keeping Management Happy 15
1.21 Keeping SAs Happy 16
1.22 Keeping Systems from Being Too Slow 16
1.23 Coping with a Big Influx of Computers 16
1.24 Coping with a Big Influx of New Users 17
1.25 Coping with a Big Influx of New SAs 17
1.26 Handling a High SA Team Attrition Rate 18
1.27 Handling a High User-Base Attrition Rate 18
1.28 Being New to a Group 18
1.29 Being the New Manager of a Group 19
1.30 Looking for a New Job 19
1.31 Hiring Many New SAs Quickly 20
1.32 Increasing Total System Reliability 20
1.33 Decreasing Costs 21
1.34 Adding Features 21
1.35 Stopping the Hurt When Doing “This” 22
1.36 Building Customer Confidence 22
1.37 Building the Team’s Self-Confidence 22
1.38 Improving the Team’s Follow-Through 22
1.39 Handling Ethics Issues 23
1.40 My Dishwasher Leaves Spots on My Glasses 23
1.41 Protecting Your Job 23
1.42 Getting More Training 24
1.43 Setting Your Priorities 24
1.44 Getting All the Work Done 25
1.45 Avoiding Stress 25
1.46 What Should SAs Expect from Their Managers? 26
1.47 What Should SA Managers Expect from Their SAs? 26
1.48 What Should SA Managers Provide to Their Boss? 26

2 Climb Out of the Hole 27

2.1 Tips for Improving System Administration 28
  2.1.1 Use a Trouble-Ticket System 28
  2.1.2 Manage Quick Requests Right 29
  2.1.3 Adopt Three Time-Saving Policies 30
  2.1.4 Start Every New Host in a Known State 32
  2.1.5 Follow Our Other Tips 33
2.2 Conclusion 36
Part II  Foundation Elements

3  Workstations

3.1  The Basics
    3.1.1  Loading the OS
    3.1.2  Updating the System Software and Applications
    3.1.3  Network Configuration
    3.1.4  Avoid Using Dynamic DNS with DHCP

3.2  The Icing
    3.2.1  High Confidence in Completion
    3.2.2  Involve Customers in the Standardization Process
    3.2.3  A Variety of Standard Configurations

3.3  Conclusion

4  Servers

4.1  The Basics
    4.1.1  Buy Server Hardware for Servers
    4.1.2  Choose Vendors Known for Reliable Products
    4.1.3  Understand the Cost of Server Hardware
    4.1.4  Consider Maintenance Contracts and Spare Parts
    4.1.5  Maintaining Data Integrity
    4.1.6  Put Servers in the Data Center
    4.1.7  Client Server OS Configuration
    4.1.8  Provide Remote Console Access
    4.1.9  Mirror Boot Disks

4.2  The Icing
    4.2.1  Enhancing Reliability and Service Ability
    4.2.2  An Alternative: Many Inexpensive Servers

4.3  Conclusion

5  Services

5.1  The Basics
    5.1.1  Customer Requirements
    5.1.2  Operational Requirements
    5.1.3  Open Architecture
    5.1.4  Simplicity
    5.1.5  Vendor Relations
6 Data Centers

6.1 The Basics
   6.1.1 Location
   6.1.2 Access
   6.1.3 Security
   6.1.4 Power and Cooling
   6.1.5 Fire Suppression
   6.1.6 Racks
   6.1.7 Wiring
   6.1.8 Labeling
   6.1.9 Communication
   6.1.10 Console Access
   6.1.11 Workbench
   6.1.12 Tools and Supplies
   6.1.13 Parking Spaces

6.2 The Icing
   6.2.1 Greater Redundancy
   6.2.2 More Space

6.3 Ideal Data Centers
   6.3.1 Tom’s Dream Data Center
   6.3.2 Christine’s Dream Data Center

6.4 Conclusion
7 Networks 187

7.1 The Basics 188
  7.1.1 The OSI Model 188
  7.1.2 Clean Architecture 190
  7.1.3 Network Topologies 191
  7.1.4 Intermediate Distribution Frame 197
  7.1.5 Main Distribution Frame 203
  7.1.6 Demarcation Points 205
  7.1.7 Documentation 205
  7.1.8 Simple Host Routing 207
  7.1.9 Network Devices 209
  7.1.10 Overlay Networks 212
  7.1.11 Number of Vendors 213
  7.1.12 Standards-Based Protocols 214
  7.1.13 Monitoring 214
  7.1.14 Single Administrative Domain 216

7.2 The Icing 217
  7.2.1 Leading Edge versus Reliability 217
  7.2.2 Multiple Administrative Domains 219

7.3 Conclusion 219
  7.3.1 Constants in Networking 219
  7.3.2 Things That Change in Network Design 220

8 Namespaces 223

8.1 The Basics 224
  8.1.1 Namespace Policies 224
  8.1.2 Namespace Change Procedures 236
  8.1.3 Centralizing Namespace Management 236

8.2 The Icing 237
  8.2.1 One Huge Database 238
  8.2.2 Further Automation 238
  8.2.3 Customer-Based Updating 239
  8.2.4 Leveraging Namespaces 239

8.3 Conclusion 239

9 Documentation 241

9.1 The Basics 242
  9.1.1 What to Document 242
9.1.2 A Simple Template for Getting Started 243
9.1.3 Easy Sources for Documentation 244
9.1.4 The Power of Checklists 246
9.1.5 Storage Documentation 247
9.1.6 Wiki Systems 249
9.1.7 A Search Facility 250
9.1.8 Rollout Issues 251
9.1.9 Self-Management versus Explicit Management 251

9.2 The Icing 252
9.2.1 A Dynamic Documentation Repository 252
9.2.2 A Content-Management System 253
9.2.3 A Culture of Respect 253
9.2.4 Taxonomy and Structure 254
9.2.5 Additional Documentation Uses 255
9.2.6 Off-Site Links 258

9.3 Conclusion 258

10 Disaster Recovery and Data Integrity 261
10.1 The Basics 261
10.1.1 Definition of a Disaster 262
10.1.2 Risk Analysis 262
10.1.3 Legal Obligations 263
10.1.4 Damage Limitation 264
10.1.5 Preparation 265
10.1.6 Data Integrity 267

10.2 The Icing 268
10.2.1 Redundant Site 268
10.2.2 Security Disasters 268
10.2.3 Media Relations 269

10.3 Conclusion 269

11 Security Policy 271
11.1 The Basics 272
11.1.1 Ask the Right Questions 273
11.1.2 Document the Company’s Security Policies 276
11.1.3 Basics for the Technical Staff 283
11.1.4 Management and Organizational Issues 300
11.2 The Icing
   11.2.1 Make Security Pervasive 315
   11.2.2 Stay Current: Contacts and Technologies 316
   11.2.3 Produce Metrics 317
11.3 Organization Profiles 317
   11.3.1 Small Company 318
   11.3.2 Medium-Size Company 318
   11.3.3 Large Company 319
   11.3.4 E-Commerce Site 319
   11.3.5 University 320
11.4 Conclusion 321

12 Ethics 323
   12.1 The Basics 323
      12.1.1 Informed Consent 324
      12.1.2 Professional Code of Conduct 324
      12.1.3 Customer Usage Guidelines 326
      12.1.4 Privileged-Access Code of Conduct 327
      12.1.5 Copyright Adherence 330
      12.1.6 Working with Law Enforcement 332
   12.2 The Icing 336
      12.2.1 Setting Expectations on Privacy and Monitoring 336
      12.2.2 Being Told to Do Something Illegal/Unethical 338
   12.3 Conclusion 340

13 Helpdesks 343
   13.1 The Basics 343
      13.1.1 Have a Helpdesk 344
      13.1.2 Offer a Friendly Face 346
      13.1.3 Reflect Corporate Culture 346
      13.1.4 Have Enough Staff 347
      13.1.5 Define Scope of Support 348
      13.1.6 Specify How to Get Help 351
      13.1.7 Define Processes for Staff 352
      13.1.8 Establish an Escalation Process 352
      13.1.9 Define “Emergency” in Writing 353
      13.1.10 Supply Request-Tracking Software 354
13.2 The Icing

13.2.1 Statistical Improvements

13.2.2 Out-of-Hours and 24/7 Coverage

13.2.3 Better Advertising for the Helpdesk

13.2.4 Different Helpdesks for Service Provision and Problem Resolution

13.3 Conclusion

14 Customer Care

14.1 The Basics

14.1.1 Phase A/Step 1: The Greeting

14.1.2 Phase B: Problem Identification

14.1.3 Phase C: Planning and Execution

14.1.4 Phase D: Verification

14.1.5 Perils of Skipping a Step

14.1.6 Team of One

14.2 The Icing

14.2.1 Based Model-Training

14.2.2 Holistic Improvement

14.2.3 Increased Customer Familiarity

14.2.4 Special Announcements for Major Outages

14.2.5 Trend Analysis

14.2.6 Customers Who Know the Process

14.2.7 Architectural Decisions That Match the Process

14.3 Conclusion

Part III Change Processes

15 Debugging

15.1 The Basics

15.1.1 Learn the Customer’s Problem

15.1.2 Fix the Cause, Not the Symptom

15.1.3 Be Systematic

15.1.4 Have the Right Tools

15.2 The Icing

15.2.1 Better Tools

15.2.2 Formal Training on the Tools

15.2.3 End-to-End Understanding of the System

15.3 Conclusion
16 Fixing Things Once

16.1 The Basics
   16.1.1 Don’t Waste Time
   16.1.2 Avoid Temporary Fixes
   16.1.3 Learn from Carpenters

16.2 The Icing

16.3 Conclusion

17 Change Management

17.1 The Basics
   17.1.1 Risk Management
   17.1.2 Communications Structure
   17.1.3 Scheduling
   17.1.4 Process and Documentation
   17.1.5 Technical Aspects

17.2 The Icing
   17.2.1 Automated Front Ends
   17.2.2 Change-Management Meetings
   17.2.3 Streamline the Process

17.3 Conclusion

18 Server Upgrades

18.1 The Basics
   18.1.1 Step 1: Develop a Service Checklist
   18.1.2 Step 2: Verify Software Compatibility
   18.1.3 Step 3: Verification Tests
   18.1.4 Step 4: Write a Back-Out Plan
   18.1.5 Step 5: Select a Maintenance Window
   18.1.6 Step 6: Announce the Upgrade as Appropriate
   18.1.7 Step 7: Execute the Tests
   18.1.8 Step 8: Lock out Customers
   18.1.9 Step 9: Do the Upgrade with Someone Watching
   18.1.10 Step 10: Test Your Work
   18.1.11 Step 11: If All Else Fails, Rely on the Back-Out Plan
   18.1.12 Step 12: Restore Access to Customers
   18.1.13 Step 13: Communicate Completion/Back-Out
## Contents

18.2 The Icing
   18.2.1 Add and Remove Services at the Same Time
   18.2.2 Fresh Installs
   18.2.3 Reuse of Tests
   18.2.4 Logging System Changes
   18.2.5 A Dress Rehearsal
   18.2.6 Installation of Old and New Versions on the Same Machine
   18.2.7 Minimal Changes from the Base
18.3 Conclusion

19 Service Conversions
   19.1 The Basics
      19.1.1 Minimize Intrusiveness
      19.1.2 Layers versus Pillars
      19.1.3 Communication
      19.1.4 Training
      19.1.5 Small Groups First
      19.1.6 Flash-Cuts: Doing It All at Once
      19.1.7 Back-Out Plan
   19.2 The Icing
      19.2.1 Instant Rollback
      19.2.2 Avoiding Conversions
      19.2.3 Web Service Conversions
      19.2.4 Vendor Support
   19.3 Conclusion

20 Maintenance Windows
   20.1 The Basics
      20.1.1 Scheduling
      20.1.2 Planning
      20.1.3 Directing
      20.1.4 Managing Change Proposals
      20.1.5 Developing the Master Plan
      20.1.6 Disabling Access
      20.1.7 Ensuring Mechanics and Coordination
      20.1.8 Deadlines for Change Completion
      20.1.9 Comprehensive System Testing
23 Email Service 543

23.1 The Basics 543
  23.1.1 Privacy Policy 544
  23.1.2 Namespaces 544
  23.1.3 Reliability 546
  23.1.4 Simplicity 547
  23.1.5 Spam and Virus Blocking 549
  23.1.6 Generality 550
  23.1.7 Automation 552
  23.1.8 Basic Monitoring 552
  23.1.9 Redundancy 553
  23.1.10 Scaling 554
  23.1.11 Security Issues 556
  23.1.12 Communication 557

23.2 The Icing 558
  23.2.1 Encryption 559
  23.2.2 Email Retention Policy 559
  23.2.3 Advanced Monitoring 560
  23.2.4 High-Volume List Processing 561

23.3 Conclusion 562

24 Print Service 565

24.1 The Basics 566
  24.1.1 Level of Centralization 566
  24.1.2 Print Architecture Policy 568
  24.1.3 System Design 572
  24.1.4 Documentation 573
  24.1.5 Monitoring 574
  24.1.6 Environmental Issues 575

24.2 The Icing 576
  24.2.1 Automatic Failover and Load Balancing 577
  24.2.2 Dedicated Clerical Support 578
  24.2.3 Shredding 578
  24.2.4 Dealing with Printer Abuse 579

24.3 Conclusion 580

25 Data Storage 583

25.1 The Basics 584
  25.1.1 Terminology 584
25.1.2 Managing Storage 588  
25.1.3 Storage as a Service 596  
25.1.4 Performance 604  
25.1.5 Evaluating New Storage Solutions 608  
25.1.6 Common Problems 609  

25.2 The Icing 611  
25.2.1 Optimizing RAID Usage by Applications 611  
25.2.2 Storage Limits: Disk Access Density Gap 613  
25.2.3 Continuous Data Protection 614  

25.3 Conclusion 615  

26 Backup and Restore 619  
26.1 The Basics 620  
26.1.1 Reasons for Restores 621  
26.1.2 Types of Restores 624  
26.1.3 Corporate Guidelines 625  
26.1.4 A Data-Recovery SLA and Policy 626  
26.1.5 The Backup Schedule 627  
26.1.6 Time and Capacity Planning 633  
26.1.7 Consumables Planning 635  
26.1.8 Restore-Process Issues 637  
26.1.9 Backup Automation 639  
26.1.10 Centralization 641  
26.1.11 Tape Inventory 642  

26.2 The Icing 643  
26.2.1 Fire Drills 643  
26.2.2 Backup Media and Off-Site Storage 644  
26.2.3 High-Availability Databases 647  
26.2.4 Technology Changes 648  

26.3 Conclusion 649  

27 Remote Access Service 653  
27.1 The Basics 654  
27.1.1 Requirements for Remote Access 654  
27.1.2 Policy for Remote Access 656  
27.1.3 Definition of Service Levels 656  
27.1.4 Centralization 658  
27.1.5 Outsourcing 658
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.1.6</td>
<td>Authentication</td>
<td>661</td>
</tr>
<tr>
<td>27.1.7</td>
<td>Perimeter Security</td>
<td>661</td>
</tr>
<tr>
<td>27.2</td>
<td>The Icing</td>
<td>662</td>
</tr>
<tr>
<td>27.2.1</td>
<td>Home Office</td>
<td>662</td>
</tr>
<tr>
<td>27.2.2</td>
<td>Cost Analysis and Reduction</td>
<td>663</td>
</tr>
<tr>
<td>27.2.3</td>
<td>New Technologies</td>
<td>664</td>
</tr>
<tr>
<td>27.3</td>
<td>Conclusion</td>
<td>665</td>
</tr>
<tr>
<td>28</td>
<td>Software Depot Service</td>
<td>667</td>
</tr>
<tr>
<td>28.1</td>
<td>The Basics</td>
<td>669</td>
</tr>
<tr>
<td>28.1.1</td>
<td>Understand the Justification</td>
<td>669</td>
</tr>
<tr>
<td>28.1.2</td>
<td>Understand the Technical Expectations</td>
<td>670</td>
</tr>
<tr>
<td>28.1.3</td>
<td>Set the Policy</td>
<td>671</td>
</tr>
<tr>
<td>28.1.4</td>
<td>Select Depot Software</td>
<td>672</td>
</tr>
<tr>
<td>28.1.5</td>
<td>Create the Process Manual</td>
<td>672</td>
</tr>
<tr>
<td>28.1.6</td>
<td>Examples</td>
<td>673</td>
</tr>
<tr>
<td>28.2</td>
<td>The Icing</td>
<td>682</td>
</tr>
<tr>
<td>28.2.1</td>
<td>Different Configurations for Different Hosts</td>
<td>682</td>
</tr>
<tr>
<td>28.2.2</td>
<td>Local Replication</td>
<td>683</td>
</tr>
<tr>
<td>28.2.3</td>
<td>Commercial Software in the Depot</td>
<td>684</td>
</tr>
<tr>
<td>28.2.4</td>
<td>Second-Class Citizens</td>
<td>684</td>
</tr>
<tr>
<td>28.3</td>
<td>Conclusion</td>
<td>686</td>
</tr>
<tr>
<td>29</td>
<td>Web Services</td>
<td>689</td>
</tr>
<tr>
<td>29.1</td>
<td>The Basics</td>
<td>690</td>
</tr>
<tr>
<td>29.1.1</td>
<td>Web Service Building Blocks</td>
<td>690</td>
</tr>
<tr>
<td>29.1.2</td>
<td>The Webmaster Role</td>
<td>693</td>
</tr>
<tr>
<td>29.1.3</td>
<td>Service-Level Agreements</td>
<td>694</td>
</tr>
<tr>
<td>29.1.4</td>
<td>Web Service Architectures</td>
<td>694</td>
</tr>
<tr>
<td>29.1.5</td>
<td>Monitoring</td>
<td>698</td>
</tr>
<tr>
<td>29.1.6</td>
<td>Scaling for Web Services</td>
<td>699</td>
</tr>
<tr>
<td>29.1.7</td>
<td>Web Service Security</td>
<td>703</td>
</tr>
<tr>
<td>29.1.8</td>
<td>Content Management</td>
<td>710</td>
</tr>
<tr>
<td>29.1.9</td>
<td>Building the Manageable Generic Web Server</td>
<td>714</td>
</tr>
<tr>
<td>29.2</td>
<td>The Icing</td>
<td>718</td>
</tr>
<tr>
<td>29.2.1</td>
<td>Third-Party Web Hosting</td>
<td>718</td>
</tr>
<tr>
<td>29.2.2</td>
<td>Mashup Applications</td>
<td>721</td>
</tr>
<tr>
<td>29.3</td>
<td>Conclusion</td>
<td>722</td>
</tr>
</tbody>
</table>
Part V  A Management Practices

30 Organizational Structures

30.1 The Basics

30.1.1 Sizing
30.1.2 Funding Models
30.1.3 Management Chain’s Influence
30.1.4 Skill Selection
30.1.5 Infrastructure Teams
30.1.6 Customer Support
30.1.7 Helpdesk
30.1.8 Outsourcing

30.2 The Icing

30.2.1 Consultants and Contractors

30.3 Sample Organizational Structures

30.3.1 Small Company
30.3.2 Medium-Size Company
30.3.3 Large Company
30.3.4 E-Commerce Site
30.3.5 Universities and Nonprofit Organizations

30.4 Conclusion

31 Perception and Visibility

31.1 The Basics

31.1.1 A Good First Impression
31.1.2 Attitude, Perception, and Customers
31.1.3 Priorities Aligned with Customer Expectations
31.1.4 The System Advocate

31.2 The Icing

31.2.1 The System Status Web Page
31.2.2 Management Meetings
31.2.3 Physical Visibility
31.2.4 Town Hall Meetings
31.2.5 Newsletters
31.2.6 Mail to All Customers
31.2.7 Lunch

31.3 Conclusion
32 Being Happy

32.1 The Basics
- 32.1.1 Follow-Through
- 32.1.2 Time Management
- 32.1.3 Communication Skills
- 32.1.4 Professional Development
- 32.1.5 Staying Technical

32.2 The Icing
- 32.2.1 Learn to Negotiate
- 32.2.2 Love Your Job
- 32.2.3 Managing Your Manager

32.3 Further Reading
32.4 Conclusion

33 A Guide for Technical Managers

33.1 The Basics
- 33.1.1 Responsibilities
- 33.1.2 Working with Nontechnical Managers
- 33.1.3 Working with Your Employees
- 33.1.4 Decisions

33.2 The Icing
- 33.2.1 Make Your Team Even Stronger
- 33.2.2 Sell Your Department to Senior Management
- 33.2.3 Work on Your Own Career Growth
- 33.2.4 Do Something You Enjoy

33.3 Conclusion

34 A Guide for Nontechnical Managers

34.1 The Basics
- 34.1.1 Priorities and Resources
- 34.1.2 Morale
- 34.1.3 Communication
- 34.1.4 Staff Meetings
- 34.1.5 One-Year Plans
- 34.1.6 Technical Staff and the Budget Process
- 34.1.7 Professional Development
### 34.2 The Icing
- 34.2.1 A Five-Year Vision
- 34.2.2 Meetings with Single Point of Contact
- 34.2.3 Understanding the Technical Staff’s Work

### 34.3 Conclusion

### 35 Hiring System Administrators

#### 35.1 The Basics
- 35.1.1 Job Description
- 35.1.2 Skill Level
- 35.1.3 Recruiting
- 35.1.4 Timing
- 35.1.5 Team Considerations
- 35.1.6 The Interview Team
- 35.1.7 Interview Process
- 35.1.8 Technical Interviewing
- 35.1.9 Nontechnical Interviewing
- 35.1.10 Selling the Position
- 35.1.11 Employee Retention

#### 35.2 The Icing
- 35.2.1 Get Noticed

### 35.3 Conclusion

### 36 Firing System Administrators

#### 36.1 The Basics
- 36.1.1 Follow Your Corporate HR Policy
- 36.1.2 Have a Termination Checklist
- 36.1.3 Remove Physical Access
- 36.1.4 Remove Remote Access
- 36.1.5 Remove Service Access
- 36.1.6 Have Fewer Access Databases

#### 36.2 The Icing
- 36.2.1 Have a Single Authentication Database
- 36.2.2 System File Changes

### 36.3 Conclusion
Our goal for this book has been to write down everything we’ve learned from our mentors and to add our real-world experiences. These things are beyond what the manuals and the usual system administration books teach.

This book was born from our experiences as SAs in a variety of organizations. We have started new companies. We have helped sites to grow. We have worked at small start-ups and universities, where lack of funding was an issue. We have worked at midsize and large multinationals, where mergers and spin-offs gave rise to strange challenges. We have worked at fast-paced companies that do business on the Internet and where high-availability, high-performance, and scaling issues were the norm. We’ve worked at slow-paced companies at which high tech meant cordless phones. On the surface, these are very different environments with diverse challenges; underneath, they have the same building blocks, and the same fundamental principles apply.

This book gives you a framework—a way of thinking about system administration problems—rather than narrow how-to solutions to particular problems. Given a solid framework, you can solve problems every time they appear, regardless of the operating system (OS), brand of computer, or type of environment. This book is unique because it looks at system administration from this holistic point of view; whereas most other books for SAs focus on how to maintain one particular product. With experience, however, all SAs learn that the big-picture problems and solutions are largely independent of the platform. This book will change the way you approach your work as an SA.

The principles in this book apply to all environments. The approaches described may need to be scaled up or down, depending on your environment, but the basic principles still apply. Where we felt that it might not be obvious how to implement certain concepts, we have included sections that illustrate how to apply the principles at organizations of various sizes.
This book is not about how to configure or debug a particular OS and will not tell you how to recover the shared libraries or DLLs when someone accidentally moves them. Some excellent books cover those topics, and we refer you to many of them throughout. Instead, we discuss the principles, both basic and advanced, of good system administration that we have learned through our own and others’ experiences. These principles apply to all OSs. Following them well can make your life a lot easier. If you improve the way you approach problems, the benefit will be multiplied. Get the fundamentals right, and everything else falls into place. If they aren’t done well, you will waste time repeatedly fixing the same things, and your customers\textsuperscript{1} will be unhappy because they can’t work effectively with broken machines.

**Who Should Read This Book**

This book is written for system administrators at all levels. It gives junior SAs insight into the bigger picture of how sites work, their roles in the organizations, and how their careers can progress. Intermediate SAs will learn how to approach more complex problems and how to improve their sites and make their jobs easier and their customers happier. Whatever level you are at, this book will help you to understand what is behind your day-to-day work, to learn the things that you can do now to save time in the future, to decide policy, to be architects and designers, to plan far into the future, to negotiate with vendors, and to interface with management. These are the things that concern senior SAs. None of them are listed in an OS’s manual. Even senior SAs and systems architects can learn from our experiences and those of our colleagues, just as we have learned from each other in writing this book. We also cover several management topics for SA trying to understand their managers, for SAs who aspire to move into management, and for SAs finding themselves doing more and more management without the benefit of the title.

Throughout the book, we use examples to illustrate our points. The examples are mostly from medium or large sites, where scale adds its own problems. Typically, the examples are generic rather than specific to a particular OS; where they are OS-specific, it is usually UNIX or Windows.

One of the strongest motivations we had for writing this book is the understanding that the problems SAs face are the same across all OSs. A new

\textsuperscript{1} Throughout the book, we refer to the end users of our systems as *customers* rather than *users*. A detailed explanation of why we do this is in Section 31.1.2.
OS that is significantly different from what we are used to can seem like a black box, a nuisance, or even a threat. However, despite the unfamiliar interface, as we get used to the new technology, we eventually realize that we face the same set of problems in deploying, scaling, and maintaining the new OS. Recognizing that fact, knowing what problems need solving, and understanding how to approach the solutions by building on experience with other OSs lets us master the new challenges more easily.

We want this book to change your life. We want you to become so successful that if you see us on the street, you’ll give us a great big hug.

Basic Principles

If we’ve learned anything over the years, it is the importance of simplicity, clarity, generality, automation, communication, and doing the basics first. These six principles are recurring themes in this book.

1. **Simplicity** means that the smallest solution that solves the entire problem is the best solution. It keeps the systems easy to understand and reduces complex component interactions that can cause debugging nightmares.

2. **Clarity** means that the solution is straightforward. It can be easily explained to someone on the project or even outside the project. Clarity makes it easier to change the system, as well as to maintain and debug it. In the system administration world, it’s better to write five lines of understandable code than one line that’s incomprehensible to anyone else.

3. **Generality** means that the solutions aren’t inherently limited to a particular case. Solutions can be reused. Using vendor-independent open standard protocols makes systems more flexible and makes it easier to link software packages together for better services.

4. **Automation** means using software to replace human effort. Automation is critical. Automation improves repeatability and scalability, is key to easing the system administration burden, and eliminates tedious repetitive tasks, giving SAs more time to improve services.

5. **Communication** between the right people can solve more problems than hardware or software can. You need to communicate well with other SAs and with your customers. It is your responsibility to initiate communication. Communication ensures that everyone is working
toward the same goals. Lack of communication leaves people concerned and annoyed. Communication also includes documentation. Documentation makes systems easier to support, maintain, and upgrade. Good communication and proper documentation also make it easier to hand off projects and maintenance when you leave or take on a new role.

6. *Basics first* means that you build the site on strong foundations by identifying and solving the basic problems before trying to attack more advanced ones. Doing the basics first makes adding advanced features considerably easier and makes services more robust. A good basic infrastructure can be repeatedly leveraged to improve the site with relatively little effort. Sometimes, we see SAs making a huge effort to solve a problem that wouldn’t exist or would be a simple enhancement if the site had a basic infrastructure in place. This book will help you identify what the basics are and show you how the other five principles apply. Each chapter looks at the basics of a given area. Get the fundamentals right, and everything else will fall into place.

These principles are universal. They apply at all levels of the system. They apply to physical networks and to computer hardware. They apply to all operating systems running at a site, all protocols used, all software, and all services provided. They apply at universities, nonprofit institutions, government sites, businesses, and Internet service sites.

**What Is an SA?**

If you asked six system administrators to define their jobs, you would get seven different answers. The job is difficult to define because system administrators do so many things. An SA looks after computers, networks, and the people who use them. An SA may look after hardware, operating systems, software, configurations, applications, or security. A system administrator influences how effectively other people can or do use their computers and networks.

A system administrator sometimes needs to be a business-process consultant, corporate visionary, janitor, software engineer, electrical engineer, economist, psychiatrist, mindreader, and, occasionally, a bartender.

As a result, companies call SAs different names. Sometimes, they are called network administrators, system architects, system engineers, system programmers, operators and so on.
This book is for “all of the above.”

We have a very general definition of system administrator: one who manages computer and network systems on behalf of another, such as an employer or a client. SAs are the people who make things work and keep it all running.

Explaining What System Administration Entails

It’s difficult to define system administration, but trying to explain it to a nontechnical person is even more difficult, especially if that person is your mom. Moms have the right to know how their offspring are paying their rent. A friend of Christine Hogan’s always had trouble explaining to his mother what he did for a living and ended up giving a different answer every time she asked. Therefore, she kept repeating the question every couple of months, waiting for an answer that would be meaningful to her. Then he started working for WebTV. When the product became available, he bought one for his mom. From then on, he told her that he made sure that her WebTV service was working and was as fast as possible. She was very happy that she could now show her friends something and say, “That’s what my son does!”

System Administration Matters

System administration matters because computers and networks matter. Computers are a lot more important than they were years ago. What happened?

The widespread use of the Internet, intranets, and the move to a web-centric world has redefined the way companies depend on computers. The Internet is a 24/7 operation, and sloppy operations can no longer be tolerated. Paper purchase orders can be processed daily, in batches, with no one the wiser. However, there is an expectation that the web-based system that does the process will be available all the time, from anywhere. Nightly maintenance windows have become an unheard-of luxury. That unreliable machine room power system that caused occasional but bearable problems now prevents sales from being recorded.

Management now has a more realistic view of computers. Before they had PCs on their desktops, most people’s impressions of computers were based on how they were portrayed in film: big, all-knowing, self-sufficient, miracle machines. The more people had direct contact with computers, the more realistic people’s expectations became. Now even system administration itself is portrayed in films. The 1993 classic *Jurassic Park* was the first mainstream movie to portray the key role that system administrators play in large systems.
The movie also showed how depending on one person is a disaster waiting to happen. IT is a team sport. If only Dennis Nedry had read this book.

In business, nothing is important unless the CEO feels that it is important. The CEO controls funding and sets priorities. CEOs now consider IT to be important. Email was previously for nerds; now CEOs depend on email and notice even brief outages. The massive preparations for Y2K also brought home to CEOs how dependent their organizations have become on computers, how expensive it can be to maintain them, and how quickly a purely technical issue can become a serious threat. Most people do not think that they simply “missed the bullet” during the Y2K change but that problems were avoided thanks to tireless efforts by many people. A CBS Poll shows 63 percent of Americans believe that the time and effort spent fixing potential problems was worth it. A look at the news lineups of all three major network news broadcasts from Monday, January 3, 2000, reflects the same feeling.

Previously, people did not grow up with computers and had to cautiously learn about them and their uses. Now more and more people grow up using computers, which means that they have higher expectations of them when they are in positions of power. The CEOs who were impressed by automatic payroll processing are soon to be replaced by people who grew up sending instant messages and want to know why they can’t do all their business via text messaging.

Computers matter more than ever. If computers are to work and work well, system administration matters. We matter.

**Organization of This Book**

This book has the following major parts:

- **Part I: Getting Started.** This is a long book, so we start with an overview of what to expect (Chapter 1) and some tips to help you find enough time to read the rest of the book (Chapter 2).
- **Part II: Foundation Elements.** Chapters 3–14 focus on the foundations of IT infrastructure, the hardware and software that everything else depends on.
- **Part III: Change Processes.** Chapters 15–21 look at how to make changes to systems, starting with fixing the smallest bug to massive reorganizations.
• Part IV: Providing Services. Chapters 22–29 offer our advice on building seven basic services, such as email, printing, storage, and web services.

• Part V: Management Practices. Chapters 30–36 provide guidance—whether or not you have “manager” in your title.

• The two appendixes provide an overview of the positive and negative roles that SAs play and a list of acronyms used in the book.

Each chapter discusses a separate topic; some topics are technical, and some are nontechnical. If one chapter doesn’t apply to you, feel free to skip it. The chapters are linked, so you may find yourself returning to a chapter that you previously thought was boring. We won’t be offended.

Each chapter has two major sections. The Basics discusses the essentials that you simply have to get right. Skipping any of these items will simply create more work for you in the future. Consider them investments that pay off in efficiency later on. The Icing deals with the cool things that you can do to be spectacular. Don’t spend your time with these things until you are done with the basics. We have tried to drive the points home through anecdotes and case studies from personal experience. We hope that this makes the advice here more “real” for you. Never trust salespeople who don’t use their own products.

What’s New in the Second Edition

We received a lot of feedback from our readers about the first edition. We spoke at conferences and computer user groups around the world. We received a lot of email. We listened. We took a lot of notes. We’ve smoothed the rough edges and filled some of the major holes.

The first edition garnered a lot of positive reviews and buzz. We were very honored. However, the passing of time made certain chapters look passé.

The first edition, in bookstores August 2001, was written mostly in 2000. Things were very different then. At the time, things were looking pretty grim as the dot-com boom had gone bust. Windows 2000 was still new, Solaris was king, and Linux was popular only with geeks. Spam was a nuisance, not an industry. Outsourcing had lost its luster and had gone from being the corporate savior to a late-night comedy punch line. Wikis were a research idea, not the basis for the world’s largest free encyclopedia. Google was neither a household name nor a verb. Web farms were rare, and “big sites” served millions of hits per day, not per hour. In fact, we didn’t have a chapter
on running web servers, because we felt that all one needed to know could
be inferred by reading the right combination of the chapters: Data Centers,
Servers, Services, and Service Monitoring. What more could people need?

My, how things have changed!

Linux is no longer considered a risky proposition, Google is on the rise,
and offshoring is the new buzzword. The rise of India and China as economic
superpowers has changed the way we think about the world. AJAX and other
Web 2.0 technologies have made the web applications exciting again.

Here’s what’s new in the book:

• Updated chapters: Every chapter has been updated and modernized and
new anecdotes added. We clarified many, many points. We’ve learned a
lot in the past five years, and all the chapters reflect this. References to
old technologies have been replaced with more relevant ones.

• New chapters:
  – Chapter 9: Documentation
  – Chapter 25: Data Storage
  – Chapter 29: Web Services

• Expanded chapters:
  – The first edition’s Appendix B, which had been missed by many read-
er s who didn’t read to the end of the book, is now Chapter 1: What
to Do When . . .
  – The first edition’s Do These First section in the front matter has ex-
  panded to become Chapter 2: Climb Out of the Hole.

• Reordered table of contents:
  – Part I: Getting Started: introductory and overview material
  – Part II: Foundation Elements: the foundations of any IT system
  – Part III: Change Processes: how to make changes from the smallest
to the biggest
  – Part IV: Providing Services: a catalog of common service offerings
  – Part V: Management Practices: organizational issues
What’s Next

Each chapter is self-contained. Feel free to jump around. However, we have carefully ordered the chapters so that they make the most sense if you read the book from start to finish. Either way, we hope that you enjoy the book. We have learned a lot and had a lot of fun writing it. Let’s begin.

Thomas A. Limoncelli
Google, Inc.
tom@limoncelli.org

Christina J. Hogan
BMW Sauber F1 Team
chogan@chogan.com

Strata R. Chalup
Virtual.Net, Inc.
strata@virtual.net

P.S. Books, like software, always have bugs. For a list of updates, along with news and notes, and even a mailing list you can join, please visit our web site: www.EverythingSysAdmin.com.
This page intentionally left blank
Acknowledgments

Acknowledgments for the First Edition

We can’t possibly thank everyone who helped us in some way or another, but that isn’t going to stop us from trying. Much of this book was inspired by Kernighan and Pike’s *The Practice of Programming* (Kernighan and Pike 1999) and John Bentley’s second edition of *Programming Pearls* (Bentley 1999).

We are grateful to Global Networking and Computing (GNAC), Synopsys, and Eircom for permitting us to use photographs of their data center facilities to illustrate real-life examples of the good practices that we talk about.

We are indebted to the following people for their helpful editing: Valerie Natale, Anne Marie Quint, Josh Simon, and Amara Willey.

The people we have met through USENIX and SAGE and the LISA conferences have been major influences in our lives and careers. We would not be qualified to write this book if we hadn’t met the people we did and learned so much from them.

Dozens of people helped us as we wrote this book—some by supplying anecdotes, some by reviewing parts of or the entire book, others by mentoring us during our careers. The only fair way to thank them all is alphabetically and to apologize in advance to anyone that we left out: Rajeev Agrawala, Al Aho, Jeff Allen, Eric Anderson, Ann Benninger, Eric Berglund, Melissa Binde, Steven Branigan, Sheila Brown-Klinger, Brent Chapman, Bill Cheswick, Lee Damon, Tina Darmohray, Bach Thuoc (Daisy) Davis, R. Drew Davis, Ingo Dean, Arnold de Leon, Jim Dennis, Barbara Dijker, Viktor Dukhovni, Chelle-Marie Ehlers, Michael Erlinger, Paul Evans, Rémy Evard, Lookman Fazal, Robert Fulmer, Carson Gaspar, Paul Glick, David “Zonker” Harris, Katherine “Cappy” Harrison, Jim Hickstein, Sandra Henry-Stocker, Mark Horton, Bill “Whump” Humphries, Tim Hunter, Jeff Jensen, Jennifer Joy, Alan Judge, Christophe Kalt, Scott C. Kennedy, Brian Kernighan, Jim Lambert, Eliot Lear,

Thanks also to Lumeta Corporation and Lucent Technologies/Bell Labs for their support in writing this book.

Last but not least, the people at Addison-Wesley made this a particularly great experience for us. In particular, our gratitude extends to Karen Gettman, Mary Hart, and Emily Frey.

Acknowledgments for the Second Edition

In addition to everyone who helped us with the first edition, the second edition could not have happened without the help and support of Lee Damon, Nathan Dietsch, Benjamin Feen, Stephen Harris, Christine E. Polk, Glenn E. Sieb, Juhani Tali, and many people at the League of Professional System Administrators (LOPSA). Special 73s and 88s to Mike Chalup for love, loyalty, and support, and especially for the mountains of laundry done and oceans of dishes washed so Strata could write. And many cuddles and kisses for baby Joanna Lear for her patience.

Thanks to Lumeta Corporation for giving us permission to publish a second edition.

Thanks to Wingfoot for letting us use its server for our bug-tracking database.

Thanks to Anne Marie Quint for data entry, copyediting, and a lot of great suggestions.

And last but not least, a big heaping bowl of “couldn’t have done it without you” to Mark Taub, Catherine Nolan, Raina Chrobak, and Lara Wysong at Addison-Wesley.
About the Authors

Tom, Christine, and Strata know one another through attending USENIX conferences and being actively involved in the system administration community. It was at one of these conferences that Tom and Christine first spoke about collaborating on this book. Strata and Christine were coworkers at Synopsys and GNAC, and coauthored Chalup, Hogan et al. (1998).

Thomas A. Limoncelli

Tom is an internationally recognized author and speaker on system administration, time management, and grass-roots political organizing techniques. A system administrator since 1988, he has worked for small and large companies, including Google, Cibernet Corp, Dean for America, Lumeta, AT&T, Lucent/Bell Labs, and Mentor Graphics. At Google, he is involved in improving how IT infrastructure is deployed at new offices. When AT&T trivested into AT&T, Lucent, and NCR, Tom led the team that split the Bell Labs computing and network infrastructure into the three new companies.

In addition to the first and second editions of this book, his published works include Time Management for System Administration (2005), and papers on security, networking, project management, and personal career management. He travels to conferences and user groups frequently, often teaching tutorials, facilitating workshops, presenting papers, or giving invited talks and keynote speeches.

Outside of work, Tom is a grassroots civil-rights activist who has received awards and recognition on both state and national levels. Tom’s first published paper (Limoncelli 1997) extolled the lessons SAs can learn from activists. Tom doesn’t see much difference between his work and activism careers—both are about helping people.

He holds a B.A. in computer science from Drew University. He lives in Bloomfield, New Jersey.
For their community involvement, Tom and Christine shared the 2005 Outstanding Achievement Award from USENIX/SAGE.

Christina J. Hogan

Christine’s system administration career started at the Department of Mathematics in Trinity College, Dublin, where she worked for almost 5 years. After that, she went in search of sunshine and moved to Sicily, working for a year in a research company, and followed that with 5 years in California.

She was the security architect at Synopsys for a couple of years before joining some friends at GNAC a few months after it was founded. While there, she worked with start-ups, e-commerce sites, biotech companies, and large multinational hardware and software companies. On the technical side, she focused on security and networking, working with customers and helping GNAC establish its data center and Internet connectivity. She also became involved with project management, customer management, and people management. After almost 3 years at GNAC, she went out on her own as an independent security consultant, working primarily at e-commerce sites.

Since then, she has become a mother and made a career change: she now works as an aerodynamicist for the BMW Sauber Formula 1 Racing Team. She has a Ph.D. in aeronautical engineering from Imperial College, London; a B.A. in mathematics and an M.Sc. in computer science from Trinity College, Dublin; and a Diploma in legal studies from the Dublin Institute of Technology.

Strata R. Chalup

Strata is the owner and senior consultant of Virtual.Net, Inc., a strategic and best-practices IT consulting firm specializing in helping small to midsize firms scale their IT practices as they grow. During the first dot-com boom, Strata architected scalable infrastructures and managed some of the teams that built them for such projects as talkway.net, the Palm VII, and mac.com. Founded as a sole proprietorship in 1993, Virtual.Net was incorporated in 2005. Clients have included such firms as Apple, Sun, Cimflex Teknowledge, Cisco, McAfee, and Micronas USA.

Strata joined the computing world on TOPS-20 on DEC mainframes in 1981, then got well and truly sidetracked onto administering UNIX by 1983, with Ultrix on the VAX 11-780, Unisys on Motorola 68K micro systems, and a dash of Minix on Intel thrown in for good measure. She has the
unusual perspective of someone who has been both a user and an administrator of Internet services since 1981 and has seen much of what we consider the modern Net evolve, sometimes from a front-row seat. An early adopter and connector, she was involved with the early National Telecommunications Infrastructure Administration (NTIA) hearings and grant reviews from 1993–1995 and demonstrated the emerging possibilities of the Internet in 1994, creating NTIA’s groundbreaking virtual conference. A committed futurist, Strata avidly tracks new technologies for collaboration and leverages them for IT and management.

Always a New Englander at heart, but marooned in California with a snow-hating spouse, Strata is an active gardener, reader of science fiction/fantasy, and emergency services volunteer in amateur radio (KF6NBZ). She is SCUBA-certified but mostly free dives and snorkles. Strata has spent a couple of years as a technomad crossing the country by RV, first in 1990 and again in 2002, consulting from the road. She has made a major hobby of studying energy-efficient building construction and design, including taking owner-builder classes, and really did grow up on a goat farm.

Unlike her illustrious coauthors, she is an unrepentant college dropout, having left MIT during her sophomore year. She returned to manage the Center for Cognitive Science for several years, and to consult with the EECS Computing Services group, including a year as postmaster@mit-eddie, before heading to Silicon Valley.
In this chapter, we pull together the various elements from the rest of the book to provide an overview of how they can be used to deal with everyday situations or to answer common questions system administrators (SAs) and managers often have.

1.1 Building a Site from Scratch

- Think about the organizational structure you need—Chapter 30.
- Check in with management on the business priorities that will drive implementation priorities.
- Plan your namespaces carefully—Chapter 8.
- Build a rock-solid data center—Chapter 6.
- Build a rock-solid network designed to grow—Chapter 7.
- Build services that will scale—Chapter 5.
- Build a software depot, or at least plan a small directory hierarchy that can grow into a software depot—Chapter 28.
- Establish your initial core application services:
  - Authentication and authorization—Section 3.1.3
  - Desktop life-cycle management—Chapter 3
  - Email—Chapter 23
  - File service, backups—Chapter 26
  - Network configuration—Section 3.1.3
  - Printing—Chapter 24
  - Remote access—Chapter 27
1.2 Growing a Small Site

- Provide a helpdesk—Chapter 13.
- Establish checklists for new hires, new desktops/laptops, and new servers—Section 3.1.1.5.
- Consider the benefits of a network operations center (NOC) dedicated to monitoring and coordinating network operations—Chapter 22.
- Think about your organization and whom you need to hire, and provide service statistics showing open and resolved problems—Chapter 30.
- Monitor services for both capacity and availability so that you can predict when to scale them—Chapter 22.
- Be ready for an influx of new computers, employees, and SAs—See Sections 1.23, 1.24, and 1.25.

1.3 Going Global

- Design your wide area network (WAN) architecture—Chapter 7.
- Follow three cardinal rules: scale, scale, and scale.
- Standardize server times on Greenwich Mean Time (GMT) to maximize log analysis capabilities.
- Make sure that your helpdesk really is 24/7. Look at ways to leverage SAs in other time zones—Chapter 13.
- Architect services to take account of long-distance links—usually lower bandwidth and less reliable—Chapter 5.
- Qualify applications for use over high-latency links—Section 5.1.2.
- Ensure that your security and permissions structures are still adequate under global operations.

1.4 Replacing Services

- Be conscious of the process—Chapter 18.
- Factor in both network dependencies and service dependencies in transition planning.
- Manage your Dynamic Host Configuration Protocol (DHCP) lease times to aid the transition—Section 3.1.4.1.
1.6 Moving to/Opening a New Building

- Don’t hard-code server names into configurations, instead, hard-code aliases that move with the service—Section 5.1.6.
- Manage your DNS time-to-live (TTL) values to switch to new servers—Section 19.2.1.

1.5 Moving a Data Center

- Schedule windows unless everything is fully redundant and you can move first half of a redundant pair and then the other—Chapter 20.
- Make sure that the new data center is properly designed for both current use and future expansion—Chapter 6.
- Back up every file system of any machine before it is moved.
- Perform a fire drill on your data backup system—Section 26.2.1.
- Develop test cases before you move, and test, test, test everything after the move is complete—Chapter 18.
- Label every cable before it is disconnected—Section 6.1.7.
- Establish minimal services—redundant hardware—at a new location with new equipment.
- Test the new environment—networking, power, uninterruptable power supply (UPS), heating, ventilation, air conditioning (HVAC), and so on—before the move begins—Chapter 6, especially Section 6.1.4.
- Identify a small group of customers to test business operations with the newly moved minimal services, then test sample scenarios before moving everything else.
- Run cooling for 48–72 hours, and then replace all filters before occupying the space.
- Perform a dress rehearsal—Section 18.2.5.

1.6 Moving to/Opening a New Building

- Four weeks or more in advance, get access to the new space to build the infrastructure.
- Use radios or walkie-talkies for communicating inside the building—Chapter 6 and Section 20.1.7.3.
• Use a personal digital assistant (PDA) or nonelectronic organizer—Section 32.1.2.

• Order WAN and Internet service provider (ISP) network connections 2–3 months in advance.

• Communicate to the powers that be that WAN and ISP connections will take months to order and must be done soon.

• Prewire the offices with network jacks during, not after, construction—Section 7.1.4.

• Work with a moving company that can help plan the move.

• Designate one person to keep and maintain a master list of everyone who is moving and his or her new office number, cubicle designation, or other location.

• Pick a day on which to freeze the master list. Give copies of the frozen list to the moving company, use the list for printing labels, and so on. If someone’s location is to be changed after this date, don’t try to chase down and update all the list copies that have been distributed. Move the person as the master list dictates, and schedule a second move for that person after the main move.

• Give each person a sheet of 12 labels preprinted with his or her name and new location for labeling boxes, bags, and personal computer (PC). (If you don’t want to do this, at least give people specific instructions as to what to write on each box so it reaches the right destination.)

• Give each person a plastic bag big enough for all the PC cables. Technical people can decable and reconnect their PCs on arrival; technicians can do so for nontechnical people.

• Always order more boxes than you think you’ll be moving.

• Don’t use cardboard boxes; instead, use plastic crates that can be reused.

1.7 Handling a High Rate of Office Moves

• Work with facilities to allocate only one move day each week. Develop a routine around this schedule.

• Establish a procedure and a form that will get you all the information you need about each person’s equipment, number of network and telephone connections, and special needs. Have SAs check out nonstandard equipment in advance and make notes.
• Connect and test network connections ahead of time.
• Have customers power down their machines before the move and put all cables, mice, keyboards, and other bits that might get lost into a marked box.
• Brainstorm all the ways that some of the work can be done by the people moving. Be careful to assess their skill level; maybe certain people shouldn’t do anything themselves.
• Have a moving company move the equipment, and have a designated SA move team do the unpacking, reconnecting, and testing. Take care in selecting the moving company.
• Train the helpdesk to check with customers who report problems to see whether they have just moved and didn’t have the problem before the move; then pass those requests to the move team rather than the usual escalation path.
• Formalize the process, limiting it to one day a week, doing the prep work, and having a move team makes it go more smoothly with less downtime for the customers and fewer move-related problems for the SAs to check out.

1.8 Assessing a Site (Due Diligence)

• Use the chapters and subheadings in this book to create a preliminary list of areas to investigate, taking the items in the Basics section as a rough baseline for a well-run site.
• Reassure existing SA staff and management that you are here not to pass judgment but to discover how this site works, in order to understand its similarities to and differences from sites with which you are already familiar. This is key in both consulting assignments and in potential acquisition due-diligence assessments.
• Have a private document repository, such as a wiki, for your team. The amount of information you will collect will overwhelm your ability to remember it: document, document, document.
• Create or request physical-equipment lists of workstations and servers, as well as network diagrams and service workflows. The goal is to generate multiple views of the infrastructure.
• Review domains of authentication, and pay attention to compartmentalization and security of information.
• Analyze the ticket-system statistics by opened-to-close ratios month to month. Watch for a growing gap between total opened and closed tickets, indicating an overloaded staff or an infrastructure system with chronic difficulties.

1.9 Dealing with Mergers and Acquisitions

• If mergers and acquisitions will be frequent, make arrangements to get information as early as possible, even if this means that designated people will have information that prevents them from being able to trade stock for certain windows of time.

• Some mergers require instant connectivity to the new business unit. Others are forbidden from having full connectivity for a month or so until certain papers are signed. In the first case, set expectations that this will not be possible without some prior warning (see previous item). In the latter case, you have some breathing room, but act quickly!

• If you are the chief executive officer (CEO), you should involve your chief information officer (CIO) before the merger is even announced.

• If you are an SA, try to find out who at the other company has the authority to make the big decisions.

• Establish clear, final decision processes.

• Have one designated go-to lead per company.

• Start a dialogue with the SAs at the other company. Understand their support structure, service levels, network architecture, security model, and policies. Determine what the new model is going to look like.

• Have at least one initial face-to-face meeting with the SAs at the other company. It’s easier to get angry at someone you haven’t met.

• Move on to technical details. Are there namespace conflicts? If so, determine how are you going to resolve them—Chapter 8.

• Adopt the best processes of the two companies; don’t blindly select the processes of the bigger company.

• Be sensitive to cultural differences between the two groups. Diverse opinions can be a good thing if people can learn to respect one another—Sections 32.2.2.2 and 35.1.5.

• Make sure that both SA teams have a high-level overview diagram of both networks, as well as a detailed map of each site’s local area network (LAN)—Chapter 7.
• Determine what the new network architecture should look like—Chapter 7. How will the two networks be connected? Are some remote offices likely to merge? What does the new security model or security perimeter look like?—Chapter 11.

• Ask senior management about corporate-identity issues, such as account names, email address format, and domain name. Do the corporate identities need to merge or stay separate? What implications does this have on the email infrastructure and Internet-facing services?

• Learn whether any customers or business partners of either company will be sensitive to the merger and/or want their intellectual property protected from the other company—Chapter 7.

• Compare the security policies, mentioned in Chapter 11—looking in particular for differences in privacy policy, security policy, and how they interconnect with business partners.

• Check router tables of both companies, and verify that the Internet Protocol (IP) address space in use doesn’t overlap. (This is particularly a problem if you both use RFC 1918 address space [Lear et al. 1994, Rekhler et al. 1996].)

• Consider putting a firewall between the two companies until both have compatible security policies—Chapter 11.

1.10 Coping with Frequent Machine Crashes

• Establish a temporary workaround, and communicate to customers that it is temporary.

• Find the real cause—Chapter 15.

• Fix the real cause, not the symptoms—Chapter 16.

• If the root cause is hardware, buy better hardware—Chapter 4.

• If the root cause is environmental, provide a better physical environment for your hardware—Chapter 6.

• Replace the system—Chapter 18.

• Give your SAs better training on diagnostic tools—Chapter 15.

• Get production systems back into production quickly. Don’t play diagnostic games on production systems. That’s what labs and preannounced maintenance windows—usually weekends or late nights—are for.
1.11 Surviving a Major Outage or Work Stoppage

- Consider modeling your outage response on the Incident Command System (ICS). This ad hoc emergency response system has been refined over many years by public safety departments to create a flexible response to adverse situations. Defining escalation procedures before an issue arises is the best strategy.

- Notify customers that you are aware of the problem on the communication channels they would use to contact you: intranet help desk “outages” section, outgoing message for SA phone, and so on.

- Form a “tiger team” of SAs, management, and key stakeholders; have a brief 15- to 30-minute meeting to establish the specific goals of a solution, such as “get developers working again,” “restore customer access to support site” and so on. Make sure that you are working toward a goal, not simply replicating functionality whose value is non-specific.

- Establish the costs of a workaround or fallback position versus downtime owing to the problem, and let the businesspeople and stakeholders determine how much time is worth spending on attempting a fix. If information is insufficient to estimate this, do not end the meeting without setting the time for the next attempt.

- Spend no more than an hour gathering information. Then hold a team meeting to present management and key stakeholders with options. The team should do hourly updates of the passive notification message with status.

- If the team chooses fix or workaround attempts, specify an order in which fixes are to be applied, and get assistance from stakeholders on verifying that the each procedure did or did not work. Document this, even in brief, to prevent duplication of effort if you are still working on the issue hours or days from now.

- Implement fix or workaround attempts in small blocks of two or three, taking no more than an hour to implement total. Collect error message or log data that may be relevant, and report on it in the next meeting.

- Don’t allow a team member, even a highly skilled one, to go off to try to pull a rabbit out of his or her hat. Since you can’t predict the length of the outage, you must apply a strict process in order to keep everyone in the loop.
Appoint a team member who will ensure that meals are brought in, notes taken, and people gently but firmly disengaged from the problem if they become too tired or upset to work.

1.12 What Tools Should Every SA Team Member Have?

- A laptop with network diagnostic tools, such as network sniffer, DHCP client in verbose mode, encrypted TELNET/SSH client, TFTP server, and so on, as well as both wired and wireless Ethernet.
- Terminal emulator software and a serial cable. The laptop can be an emergency serial console if the console server dies or the data center console breaks or a rogue server outside the data center needs console access.
- A spare PC or server for experimenting with new configurations—Section 19.2.1.
- A portable label printer—Section 6.1.12.
- A PDA or nonelectronic organizer—Section 32.1.2.
- A set of screwdrivers in all the sizes computers use.
- A cable tester.
- A pair of splicing scissors.
- Access to patch cables of various lengths. Include one or two 100-foot (30-meter) cables. These come in handy in the strangest emergencies.
- A small digital camera. (Sending a snapshot to technical support can be useful for deciphering strange console messages, identifying model numbers, and proving damage.)
- A portable (USB)/firewire hard drive.
- Radios or walkie-talkies for communicating inside the building—Chapter 6 and Section 20.1.7.3.
- A cabinet stocked with tools and spare parts—Section 6.1.12.
- High-speed connectivity to team members’ home and the necessary tools for telecommuting.
- A library of the standard reference books for the technologies the team members are involved in—Sections 33.1.1, 34.1.7, and bibliography.
- Membership to professional societies such as USENIX and LOPSA—Section 32.1.4.
• A variety of headache medicines. It’s really difficult to solve big problems when you have a headache.
• Printed, framed, copies of the SA Code of Ethics—Section 12.1.2.
• Shelf-stable emergency-only snacky bits.
• A copy of this book!

1.13 Ensuring the Return of Tools

• Make it easier to return tools: Affix each with a label that reads, “Return to [your name here] when done.”
• When someone borrows something, open a helpdesk ticket that is closed only when the item is returned.
• Accept that tools won’t be returned. Why stress out about things you can’t control?
• Create a team toolbox and rotate responsibility for keeping it up to date and tracking down loaners.
• Keep a stash of PC screwdriver kits. When asked to borrow a single screw driver, smile and reply, “No, but you can have this kit as a gift.” Don’t accept it back.
• Don’t let a software person have a screwdriver. Politely find out what the person is trying to do, and do it. This is faster than fixing the person’s mistakes.
• If you are a software person, use a screwdriver only with adult super-vision.
• Keep a few inexpensive eyeglass repair kits in your spares area.

1.14 Why Document Systems and Procedures?

• Good documentation describes the why and the how to.
• When you do things right and they “just work,” even you will have forgotten the details when they break or need upgrading.
• You get to go on vacation—Section 32.2.2.
• You get to move on to more interesting projects rather than being stuck doing the same stuff because you are the only one who knows how it works—Section 22.2.1.
• You will get a reputation as being a real asset to the company: raises, bonuses, and promotions, or at least fame and fortune.
• You will save yourself a mad scramble to gather information when investors or auditors demand it on short notice.

1.15 Why Document Policies?

• To comply with federal health and business regulations.
• To avoid appearing arbitrary, “making it up as you go along,” and senior management doing things that would get other employees into trouble.
• Because other people can’t read your mind—Section A.1.17.
• To communicate expectations for your own team, not only your customers—Section 11.1.2 and Chapter 12.
• To avoid being unethical by enforcing a policy that isn’t communicated to the people that it governs—Section 12.2.1.
• To avoid punishing people for not reading your mind—Section A.1.17.
• To offer the organization a chance to change their ways or push back in a constructive manner.

1.16 Identifying the Fundamental Problems in the Environment

• Look at the Basics section of each chapter.
• Survey the management chain that funds you—Chapter 30.
• Survey two or three customers who use your services—Section 26.2.2.
• Survey all customers.
• Identify what kinds of problems consume your time the most—Section 26.1.3.
• Ask the helpdesk employees what problems they see the most—Sections 15.1.6 and 25.1.4.
• Ask the people configuring the devices in the field what problems they see the most and what customers complain about the most.
• Determine whether your architecture is simple enough to draw by hand on a whiteboard; if its not, maybe it’s too complicated to manage—Section 18.1.2.
1.17 Getting More Money for Projects

- Establish the need in the minds of your managers.
- Find out what management wants, and communicate how the projects you need money for will serve that goal.
- Become part of the budget process—Sections 33.1.1.12 and 34.1.6.
- Do more with less: Make sure that your staff has good time-management skills—Section 32.1.2.
- Manage your boss better—Section 32.2.3.
- Learn how your management communicates with you, and communicate in a compatible way—Chapters 33 and 34.
- Don’t overwork or manage by crisis. Show management the “real cost” of policies and decisions.

1.18 Getting Projects Done

- Usually, projects don’t get done because the SAs are required to put out new fires while trying to do projects. Solve this problem first.
- Get a management sponsor. Is the project something that the business needs, or is it something the SAs want to implement on their own? If the former, use the sponsor to gather resources and deflect conflicting demands. If a project isn’t tied to true business needs, it is doubtful whether it should succeed.
- Make sure that the SAs have the resources to succeed. (Don’t guess; ask them!)
- Hold your staff accountable for meeting milestones and deadlines.
- Communicate priorities to the SAs; move resources to high-impact projects—Section 33.1.4.2.
- Make sure that the people involved have good time-management skills—Section 32.1.2.
- Designate project time when some staff will work on nothing but projects, and the remaining staff will shield them from interruptions—Section 31.1.3.
- Reduce the number of projects.
- Don’t spend time on the projects that don’t matter—Figure 33.1.
- Prioritize → Focus → Win.
• Use an external consultant with direct experience in that area to achieve the highest-impact projects—Sections 21.2.2, 27.1.5, and 30.1.8.
• Hire junior or clerical staff to take on mundane tasks, such as PC desktop support, daily backups, and so on, so that SAs have more time to achieve the highest-impact projects.
• Hire short-term contract programmers to write code to spec.

1.19 Keeping Customers Happy

• Make sure that you make a good impression on new customers—Section 31.1.1.
• Make sure that you communicate more with existing customers—Section 31.2.4 and Chapter 31.
• Go to lunch with them and listen—Section 31.2.7.
• Create a System Status web page—Section 31.2.1.
• Create a local Enterprise Portal for your site—Section 31.2.1.
• Terminate the worst performers, especially if their mistakes create more work for others—See Chapter 36.
• See whether a specific customer or customer group generates an unusual proportion of complaints or tickets compared to the norm. If so, arrange a meeting with the customer’s manager and your manager to acknowledge the situation. Follow this with a solution-oriented meeting with the customer’s manager and the stakeholders that manager appoints. Work out priorities and an action plan to address the issues.

1.20 Keeping Management Happy

• Meet with the managers in person to listen to the complaints: don’t try to do it via email.
• Find out your manager’s priorities, and adopt them as your own—Section 32.2.3.
• Be sure that you know how management communicates with you, and communicate in a compatible way—Chapters 33 and 34.
• Make sure that the people in specialized roles understand their roles—Appendix A.
1.21 Keeping SAs Happy

- Make sure that their direct manager knows how to manage them well—Chapter 33.
- Make sure that executive management supports the management of SAs—Chapter 34.
- Make sure that the SAs are taking care of themselves—Chapter 32.
- Make sure that the SAs are in roles that they want and understand—Appendix A.
- If SAs are overloaded, make sure that they manage their time well—Section 32.1.2; or hire more people and divide the work—Chapter 35.
- Fire any SAs who are fomenting discontent—Chapter 36.
- Make sure that all new hires have positive dispositions—Section 13.1.2.

1.22 Keeping Systems from Being Too Slow

- Define slow.
- Use your monitoring systems to establish where the bottlenecks are—Chapter 22.
- Look at performance-tuning information that is specific to each architecture so that you know what to monitor and how to do it.
- Recommend a solution based on your findings.
- Know what the real problem is before you try to fix it—Chapter 15.
- Make sure that you understand the difference between latency and bandwidth—Section 5.1.2.

1.23 Coping with a Big Influx of Computers

- Make sure that you understand the economic difference between desktop and server hardware. Educate your boss or chief financial officer (CFO) about the difference or they will balk at high-priced servers—Section 4.1.3.
- Make sure that you understand the physical differences between desktop and server hardware—Section 4.1.1.
- Establish a small number of standard hardware configurations, and purchase them in bulk—Section 3.2.3.
• Make sure that you have automated host installation, configuration, and updates—Chapter 3.

• Check power, space, and heating, ventilating, and air conditioning (HVAC) capacity for your data center—Chapter 6.

• Ensure that even small computer rooms or closets have a cooling unit—Section 2.1.5.5.

• If new machines are for new employees, see Section 1.24.

### 1.24 Coping with a Big Influx of New Users

• Make sure that the hiring process includes ensuring that new computers and accounts are set up before the new hires arrive—Section 31.1.1.

• Have a stockpile of standard desktops preconfigured and ready to deploy.

• Have automated host installation, configuration, and updates—Chapter 3.

• Have proper new-user documentation and adequate staff to do orientation—Section 31.1.1.

• Make sure that every computer has at least one simple game and a CD/DVD player. It makes new computer users feel good about their machines.

• Ensure that the building can withstand the increase in power utilization.

• If dozens of people are starting each week, encourage the human resources department to have them all start on a particular day of the week, such as Mondays, so that all tasks related to information technology (IT) can be done in batches and therefore assembly-lined.

### 1.25 Coping with a Big Influx of New SAs

• Assign mentors to junior SAs—Sections 33.1.1.9 and 35.1.5.

• Have an orientation for each SA level to make sure the new hires understand the key processes and policies; make sure that it is clear whom they should go to for help.

• Have documentation, especially a wiki—Chapter 9.

• Purchase proper reference books, both technical and nontechnical—time management, communication, and people skills—Chapter 32.

• Bulk-order the items in Section 1.12.
1.26 Handling a High SA Team Attrition Rate

- When an SA leaves, completely lock them out of all systems—Chapter 36.
- Be sure that the human resources department performs exit interviews.
- Make the group aware that you are willing to listen to complaints in private.
- Have an “upward feedback session” at which your staff reviews your performance.
- Have an anonymous “upward feedback session” so that your staff can review your performance.
- Determine what you, as a manager, might be doing wrong—Chapters 33 and 34.
- Do things that increase morale: Have the team design and produce a T-shirt together—a dozen dollars spent on T-shirts can induce a morale improvement that thousands of dollars in raises can't.
- Encourage everyone in the group to read Chapter 32.
- If everyone is leaving because of one bad apple, get rid of him or her.

1.27 Handling a High User-Base Attrition Rate

- Make sure that management signals the SA team to disable accounts, remote access, and so on, in a timely manner—Chapter 36.
- Make sure that exiting employees return all company-owned equipment and software they have at home.
- Take measures against theft as people leave.
- Take measures against theft of intellectual property, possibly restricting remote access.

1.28 Being New to a Group

- Before you comment, ask questions to make sure that you understand the situation.
- Meet all your coworkers one on one.
- Meet with customers both informally and formally—Chapter 31.
- Be sure to make a good first impression, especially with customers—Section 31.1.1.
• Give credence to your coworkers when they tell you what the problems in the group are. Don’t reject them out of hand.
• Don’t blindly believe your coworkers when they tell you what the problems in the group are. Verify them first.

1.29 Being the New Manager of a Group

• That new system or conversion that’s about to go live? Stop it until you’ve verified that it meets your high expectations. Don’t let your predecessor’s incompetence become your first big mistake.
• Meet all your employees one on one. Ask them what they do, what role they would like to be in, and where they see themselves in a year. Ask them how they feel you can work with them best. The purpose of this meeting is to listen to them, not to talk.
• Establish weekly group staff meetings.
• Meet your manager and your peers one on one to get their views.
• From day one, show the team members that you have faith in them all—Chapter 33.
• Meet with customers informally and formally—Chapter 31.
• Ask everyone to tell you what the problems facing the group are, listen carefully to everyone, and then look at the evidence and make up your own mind.
• Before you comment, ask questions to make sure that you understand the situation.
• If you’ve been hired to reform an underperforming group, postpone major high-risk projects, such as replacing a global email system, until you’ve reformed/replaced the team.

1.30 Looking for a New Job

• Determine why you are looking for a new job; understand your motivation.
• Determine what role you want to play in the new group—Appendix A.
• Determine which kind of organization you enjoy working in the most—Section 30.3.
• Meet as many of your potential future coworkers as possible to find out what the group is like—Chapter 35.

• Never accept the first offer right off the bat. The first offer is just a proposal. Negotiate! But remember that there usually isn’t a third offer—Section 32.2.1.5.

• Negotiate in writing the things that are important to you: conferences, training, vacation.

• Don’t work for a company that doesn’t let you interview your future boss.

• If someone says, “You don’t need to have a lawyer review this contract” and isn’t joking, you should have a lawyer review that contract. We’re not joking.

1.31 Hiring Many New SAs Quickly

• Review the advice in Chapter 35.

• Use as many recruiting methods as possible: Organize fun events at the appropriate conferences, use online boards, sponsor local user groups, hire famous people to speak at your company and invite the public, get referrals from SAs and customers—Chapter 35.

• Make sure that you have a good recruiter and human resources contact who knows what a good SA is.

• Determine how many SAs of what level and what skills you need. Use the SAGE level classifications—Section 35.1.2.

• Move quickly when you find a good candidate.

• After you’ve hired one person, refine the other job descriptions to fill in the gaps—Section 30.1.4.

1.32 Increasing Total System Reliability

• Figure out what your target is and how far you are from it.

• Set up monitoring to pinpoint uptime problems—Chapter 22.

• Deploy end-to-end monitoring for key applications—Section 24.2.4.

• Reduce dependencies. Nothing in the data center should rely on anything outside the data center—Sections 5.1.7 and 20.1.7.1.
1.33 Decreasing Costs

- Decrease costs by centralizing some services—Chapter 21.
- Review your maintenance contracts. Are you still paying for machines that are no longer critical servers? Are you paying high maintenance on old equipment that would be cheaper to replace?—Section 4.1.4.
- Reduce running costs, such as remote access, through outsourcing—Chapter 27 and Section 21.2.2.
- Determine whether you can reduce the support burden through standards and/or automation?—Chapter 3.
- Try to reduce support overhead through applications training for customers or better documentation.
- Try to distribute costs more directly to the groups that incur them, such as maintenance charges, remote access charges, special hardware, high-bandwidth use of wide-area links—Section 30.1.2.
- Determine whether people are not paying for the services you provide. If people aren’t willing to pay for the service, it isn’t important.
- Take control of the ordering process and inventory for incidental equipment such as replacement mice, minihubs, and similar. Do not let customers simply take what they need or direct your staff to order it.

1.34 Adding Features

- Interview customers to understand their needs and to prioritize features.
- Know the requirements—Chapter 5.
- Make sure that you maintain at least existing service and availability levels.
- If altering an existing service, have a back-out plan.
- Look into building an entirely new system and cutting over rather than altering the running one.
- If it’s a really big infrastructure change, consider a maintenance window—Chapter 20.
- Decentralize so that local features can be catered to.
- Test! Test! Test!
- Document! Document! Document!
1.35 Stopping the Hurt When Doing “This”

- Don’t do “that.”
- Automate “that.”

If It Hurts, Don’t Do It

A small field office of a multinational company had a visit from a new SA supporting the international field offices. The local person who performed the SA tasks when there was no SA had told him over the telephone that the network was “painful.” He assumed that she meant painfully slow until he got there and got a powerful electrical shock from the 10Base-2 network. He closed the office and sent everyone home immediately while he called an electrician to trace and fix the problem.

1.36 Building Customer Confidence

- Improve follow-through—Section 32.1.1.
- Focus on projects that matter to the customers and will have the biggest impact—Figure 33.1.
- Until you have enough time to complete the ones you need to, discard projects that you haven’t been able to achieve.
- Communicate more—Chapter 31.
- Go to lunch with customers and listen—Section 31.2.7.
- Create a good first impression on the people entering your organization—Section 31.1.1.

1.37 Building the Team’s Self-Confidence

- Start with a few simple, achievable projects; only then should you involve the team in more difficult projects.
- Ask team members what training they feel they need, and provide it.
- Coach the team. Get coaching on how to coach!

1.38 Improving the Team’s Follow-Through

- Find out why team members are not following through.
- Make sure that your trouble-ticket system assists them in tracking customer requests and that it isn’t simply for tracking short-term requests.
Be sure that the system isn’t so cumbersome that people avoid using it—Section 13.1.10.

- Encourage team members to have a single place to list all their requests—Section 32.1.1.
- Discourage team members from trying to keep to-do lists in their heads—Section 32.1.1.
- Purchase PDAs for all team members who want them and promise to use them—Section 32.1.1.

1.39 Handling an Unethical or Worrisome Request

- See Section 12.2.2.
- Log all requests, events, and actions.
- Get the request in writing or email. Try a a soft approach, such as “Hey, could you email me exactly what you want, and I’ll look at it after lunch?” Someone who knows that the request is unethical will resist leaving a trail.
- Check for a written policy about the situation—Chapter 12.
- If there is no written policy, absolutely get the request in writing.
- Consult with your manager before doing anything.
- If you have any questions about the request, escalate it to appropriate management.

1.40 My Dishwasher Leaves Spots on My Glasses

- Spots are usually the result of not using hot enough water rather than finding a special soap or even using a special cycle on the machine.
- Check for problems with the hot water going to your dishwasher.
- Have the temperature of your hot water adjusted.
- Before starting the dishwasher, run the water in the adjacent sink until it’s hot.

1.41 Protecting Your Job

- Look at your most recent performance review and improve in the areas that “need improvement”—whether or not you think that you have those failings.
• Get more training in areas in which your performance review has indicated you need improvement.
• Be the best SA in the group: Have positive visibility—Chapter 31.
• Document everything—policies and technical and configuration information and procedures.
• Have good follow-through.
• Help everyone as much as possible.
• Be a good mentor.
• Use your time effectively—Section 32.1.2.
• Automate as much as you can—Chapter 3 and Sections 16.2, 26.1.9, and 31.1.4.3.
• Always keep the customers’ needs in mind—Sections 31.1.3 and 32.2.3.
• Don’t speak ill of coworkers. It just makes you look bad. Silence is golden. A closed mouth gathers no feet.

1.42 Getting More Training
• Go to training conferences like LISA.
• Attend vendor training to gain specific knowledge and to get the inside story on products.
• Find a mentor.
• Attend local SA group meetings
• Present at local SA group meetings. You learn a lot by teaching.
• Find the online forums or communities for items you need training on, read the archives, and participate in the forums.

1.43 Setting Your Priorities
• Depending on what stage you are in, certain infrastructure issues should be happening.
  – Basic services, such as email, printing, remote access, and security, need to be there from the outset.
  – Automation of common tasks, such as machine installations, configuration, maintenance, and account creation and deletion, should happen early; so should basic policies.
  – Documentation should be written as things are implemented, or it will never happen.
1.45 Avoiding Stress

- Build a software depot and deployment system.
- Monitor before you think about improvements and scaling, which are issues for a more mature site.
- Think about setting up a helpdesk—Section 13.1.1.

• Get more in touch with your customers to find out what their priorities are.
• Improve your trouble-ticket system—Chapter 13.
• Review the top 10 percent of the ticket generators—Section 13.2.1.
• Adopt better revision control of configuration files—Chapter 17, particularly Section 17.1.5.1.

1.44 Getting All the Work Done

• Climb out of the hole—Chapter 2.
• Improve your time management; take a time-management class—Sections 32.1.2 and 32.1.2.11.
• Use a console server so that you aren’t spending so much time running back and forth to the machine room—Sections 6.1.10 and 4.1.8 and 20.1.7.2.
• Batch up similar requests; do as a group all tasks that require being in a certain part of the building.
• Start each day with project work, not by reading email.
• Make informal arrangements with your coworkers to trade being available versus finding an empty conference room and getting uninterrupted work done for a couple of hours.

1.45 Avoiding Stress

• Take those vacations! (Three-day weekends are not a vacation.)
• Take a vacation long enough to learn what hasn’t been documented well. Better to find those issues when you are returning in a few days than when you’re (heaven forbid) hit by a bus.
• Take walks; get out of the area for a while.
• Don’t eat lunch at your desk.
• Don’t forget to have a life outside of work.
• Get weekly or monthly massages.
• Sign up for a class on either yoga or meditation.
1.46 What Should SAs Expect from Their Managers?

- Clearly communicated priorities—Section 33.1.1.1
- Enough budget to meet goals—Section 33.1.1.12
- Feedback that is timely and specific—Section 33.1.3.2
- Permission to speak freely in private in exchange for using decorum in public—Section 31.1.2

1.47 What Should SA Managers Expect from Their SAs?

- To do their jobs—Section 33.1.1.5
- To treat customers well—Chapter 31
- To get things done on time, under budget
- To learn from mistakes
- To ask for help—Section 32.2.2.7
- To give pessimistic time estimates for requested projects—Section 33.1.2
- To set honest status of milestones as projects progress—Section 33.1.1.8
- To participate in budget planning—Section 33.1.1.12
- To have high ethical standards—Section 12.1.2
- To set at least one long vacation per year—Section 32.2.2.8
- To keep on top of technology changes—Section 32.1.4

1.48 What Should SA Managers Provide to Their Boss?

- Access to monitoring and reports so that the boss can update himself or herself on status at will
- Budget information in a timely manner—Section 33.1.1.12
- Pessimistic time estimates for requested projects—Section 33.1.2
- Honest status of milestones as projects progress—Section 33.1.1.8
- A reasonable amount of stability
This page intentionally left blank
Index

10 Gigabit Ethernet standard, 198
19-inch racks, 152, 155
802.3 Spanning Tree Protocol bridge, 45

A
Acceptable-use policy, 318, 320, 579
Access
data centers, 134
databases, 904–905
monitoring, 534–535
Access control policy, 229–230
Accidental file deletion, 621–623
Account names, 223
Accountability and shared accounts, 290, 292
Accounting policy, 568–569
Accounts, longevity policy, 230–231
Acquisitions overview, 8–9
Active Directory lookups, 720
Active listening, 376
mirroring, 792–794
reflection, 795–796
standardizing on phrases, 793–794
summary statements, 794–795
Active monitoring systems, 532–534
Active Server Pages, 691
ActiveDirectory, 237, 332
Ad hoc solution finder, 921–922
Add-ons and preloaded operating systems, 53
Administration
centralization, 507
Administrative functions, separate networks for, 89
Administrator access, 327
Administrator account, 291
AJAX, 691–692
Alerting to failure, 524
Alerts, 530–532
real-time monitoring, 527
Algorithms and high-latency networks, 102–103
Aliases, 231
e-mail servers, 549
Always make backups, 786
Always-on Internet technology, 664
“An Analysis of UNIX System Configuration” (Evard), 41–42
Anonymizer service, 335
Anonymizing redirection service, 258
ANS.1 format, 529
Antispam software, 550
Anti-virus software, 550
AOLServer, 691
Apache, 691, 720
AppleTalk, 569
Appliances, 84–85
Application servers, upgrading, 211
Applications
centralizing, 116
configuring properly, 32–33
critical servers lists, 34
high latency, 101
new configuration information and, 426–428
Applications (continued)
  optimizing RAID usage, 611–612
  response-time monitoring, 537
  security, 709–710
  streamlining write path, 612
  updating, 54–57
Architects, 401, 736
Archival backups, 624–625
Archival restores, 624
Archive tapes
  obsolescence, 624
  separating from other backups, 624
Archives, 624, 627
Archiving
  email, 784
  logs, 299
Asking for help, 808–809
Assessing sites overview, 7–8
Asset management, 513
Assumer, 379
Asynchronous JavaScript, 692
ATM (Asynchronous Transfer Mode), 187, 212
ATS, 139–140, 177
Attackers
  contacts in industry, 301
  logs, 299
  mail relay hosts, 556–557
  mean time to, 289
  responding to, 303–307
  site used to launch, 307
  spoofing real-time monitoring system, 525
Audio latency, 103
Audit trail, 415
Auditing, 298, 318–319
  security consultants, 308–309
Auditor, 302
AUP (acceptable-use policy), 276–277, 326–327
AUSCERT (Australian Computer Emergency Response Team), 289
Authentication, 290, 318
  Apache, 720
  biometric mechanism, 291
  CGI-based applications, 720–721
  handheld token-based system, 291
  inflexibility, 292
  information used for, 292
  over phone, 292
  remote access service, 661
  shared accounts, 290–291
  strong system of, 291
  web server software, 720
Authentication and authorization service, 97
Authentication services
  customer requirements, 96
  full redundancy, 122
Authorization, 290–293
Authorization matrix, 293–295, 320
AutoLoad, 47, 50
Automated front ends, 428
Automated installation, 43, 47–49, 53–54
Automated inventory, 238
Automated operating system installation, 32–33
Automated services, 737
Automated update system, 57
Automatic failover, 573, 577
Automatic network configuration, 469
Automating
  backups, 639–641
  combining with cloning, 51
  completely automated, 47–49
  done a little at a time, 413
  email service, 552
  fixing root problem, 413
  fixing symptoms and alerting SA, 412
  fixing symptoms without fixing root cause, 412
  hidden costs, 46
  manual steps and, 764–765
  monitoring, 535
  operating system, 46–47
  testing, 764
  updating servers, 463
  verification tests, 441
AutoPatch system, 54, 56
Availability monitoring, 527
Awards wall, 810–811
B

Back door, 906

Back-out plans, 417
  backups, 443
  relying on, 448
  service conversions, 465–466
  testing after use, 448–449
  when initiated, 444
  when to execute, 466
  writing, 443

Backup and restore system, 621
  basics, 620–643
  speed of interconnections, 635

Backup media, 622

Backup policies, 230

Backup software
  automation, 628
  homegrown, 641
  installation, 744–745
  scheduling algorithms, 639

Backup tapes
  changing M-W-F, 786
  file-by-file inventory of, 642–643
  passing cost to customer, 625
  tracking reuse, 643

Backups, 583, 619
  always making, 786
  automating, 639–641
  back-out plan, 443
  bubble-up dynamic schedule, 632
  centralization, 641–642
  commands, 639
  consumables planning, 635–637
  corporate guidelines, 625–626
  D2D2T (disk-to-disk-to-tape), 635
  data storage service, 598–601
  data-recovery SLA and policy, 626
  delegating, 641
  disk drive as buffer, 635
  DLTs (digital linear tapes), 635–637
  email, 559–560
  fire drills, 643–644
  full backups, 620, 627–628
  high-availability databases, 647–648
  homegrown backup software, 641
  incremental backups, 620, 627–628, 633
  Internet-based systems, 647
  jukeboxes, 639, 642
  length of cycle, 628–631
  locally replicated software, 683
  manual backups, 639, 641
  media, 644–647
  minimal tape index, 642
  mirrored disks, 84
  mirrors, 599–600
  mistimed, 626
  NAS, 600
  network-based backups, 641
  networked off-site, 646–647
  nine-track tape drives, 649
  no substitute for, 598–599
  off-site storage, 644–647
  RAID mirrors to speed, 600
  risks, 417
  SANs, 600–601
  scheduling, 627–633, 639
  SLAs, 625–626
  speed of, 633–634
  tape inventory, 639, 642–643
  tape usage, 628–633
  technology changes, 648–649
  thinking aspect of, 640–641
  time and capacity planning,
    633–635
  true incrementals or differentials,
    633

Balancing work and personal life,
  809–810

Bandwidth
  addictiveness of increases, 657
  hijacked, 703–704
  versus latency, 101–103

Bell Labs, 45–46, 234, 244
  AutoPatch system, 56
  Computer Science Research
    group, 65
  demo schedule, 419
  laptop subnet, 65
  network-split project, 461
  pillars versus layers approach, 461
  Rioting-Mob Technique, 459–460
  UNIX Room, 412
BGP (Border Gateway Protocol), 187
Biometric mechanism, 291
Blade servers, 91–92
Bleeding edge, 218
bleeding edger, 932
Blind guessing, 604
Bonuses, 825
Boot disks, mirroring, 83
Boot server, 121
Booting critical systems, 483
Boss philosophy, 811
Bot farms, 704
Bounced email, 409
Break, 599
Brick, 205
“Bring me a rock” management technique, 843
British Telecom, 465
Broadcast domain, 197
Browsers, 689
Budget administrator, 926–927
Budgets
nontechnical manager, 860–862
technical managers, 834–835
technical staff, 860–862
Bugtraq, 289
Build licenses, administrating, 332
Building
generator backups, 143
rewiring, 202
Bulk-license popular packages, 331
Business applications support team, 312
Business desktop computers, 73
Business partners relationship, 757
Businesses
constraints, 476
security meeting needs, 285–287
security through infrastructure, 288
Business-specific services, 95
Buy-versus-build decision, 845–848
Buzzword-compliant tools, 399
Buzzwords, 376

C

Cable bundling, 165
Cables
categories, 198
color coding, 161
hiding, 159
labeling, 167–169, 182, 206
lengths, 163
managing in racks, 156–158
networks, 163
organizing, 157–158
patch cables, 161–163
prelabeled, 168
raised floor, 159–160
slack in, 163
testing after installation, 202
value of test printouts, 203
Cage nut, 153
calendar command, 419
calendar global alias, 98
Calendar program, 33–34
Calendar server, 109, 231
CamelCase, 249
Canned solutions, 845
CAP (Columbia Appletalk Protocol) server, 121
Capacity monitoring, 527–528
Capacity planner, 926
Capacity planning, 524
Capturing command line, 245
Capturing screen shots, 244–245
Career goals, 812–813
Career paths, 833–834
Careful planner, 925–926
Carpenters, 410–412
The Case of the 500-Mile Email, 402
Cat-5 cable, 161
Cat-6 cable, 161–162
CDP (continuous data protection), 598, 614–615
Cellphones, 488
Center-of-the-universe host, 122
Central funnel architecture, 572–573
Central host, 210
Central machine, 121
Centralization, 501–502
110 percent, 504
access, 504
administration, 507
asset management, 513
backups, 641–642
balance, 504
basics, 502–512
candidates, 505–510
commodity, 509–510
consolidating purchasing, 513–515
consolidation, 506–507
cost savings, 505
distributed systems, 506
easier-to manage architecture, 505
experience counts, 503
giving up control, 505
guiding principles, 502–505
helpdesk, 741
impediment management decisions or politics, 505
improving efficiency, 501
increased purchasing power, 509
introducing new economies of scale, 505
involvement, 503
issues similar to new service, 504
left hand, right hand, 508–509
motivation, 502–503
outsourcing, 515–518
printing, 566–568
problem-solving, 502
remote access service, 658
single points of failure, 512
specialization, 508
tape changes, 641
veto power, 505
Centralized file servers, 509
Centralized funnel, 573
Centralized group for services, 508
Centralized model for customer support, 740–741
Centralized storage, 597–598
Centralizing network management, 738
services, 98, 737
CERT/CC, 289
Certificates, 704–706
CFO (chief financial officer), 734
CGI (Common Gateway Interface), 691
programs, 701–702
scripts, 691
servers, 695
CGI-based applications and authentication, 720–721
Change advisory board, 417
Change completion deadlines, 488–489
Change control namespace, 230
Change log, 451
Change management
audit trail, 415
automated checks, 426–428
automated front ends, 428
basics, 416–428
categories of systems changed, 416
communication and scheduling, 416
communications structure, 418–419
documentation, 422, 424
e-commerce companies, 415
ITIL (Infrastructure Library), 417
locking, 424–426
managing risk, 415
Nagano Olympics, 430–431
planning and testing, 416
process and documentation, 416
processes, 422, 424
reboot test, 427–428
revision control and automation, 416
revision history, 424–426
risk management, 417–418
scheduling, 419–422
specific procedures for each combination, 416
streamline processing, 431–432
successful large-scale events, 431
technical aspects, 424–428
types of changes made, 416
Change procedures, 236
Change proposals, managing, 479–481
Change-control forms, 422
Change-freeze times, 422, 423
CHANGELOG file, 453
Change-management meetings, 428–431
Change-proposal forms, 422
Chaos topology, 195
Checklists, 246–247, 821
Christine’s dream data center, 183–184
CIAC (Computer Incident Advisory Capability), 289
Cisco
   NetAid, 431
   routers, 395
Classifier role, 368
Classifying problems, 368–369
Clean Desk Policy, 315
Clean network architecture, 190–191
Clean state, 42
Clear directions, 842–843
Clerks
   installing software, 761–762
   managed by SAs versus by customers, 761
   simple automation, 763–764
   solving performance problem, 762–763
Client servers and OS configuration, 79–80
Clients
   email, 553
   moving away from resources, 64
   redundancy, 553–554
   services, 97
Clones, upgrading, 443
Cloning hard disks, 50–51
Closed cable management, 158
Closed services, 104
Closed source security-sensitive products, 296
Cluster file systems, 588
Clusters and namespace databases, 232
CMS (content-management system), 253
Code control systems, 425
Code red emergencies, 32
Code yellow emergencies, 32
Colocation (colo) center, 71, 743
Colocation facility, 129–130
Color coding
   cables, 161
   network cables, 167–168
   network jacks, 200
Commands, listing last executed, 245
Commercial encryption packages, 559
Commercial software, 684
Commodity centralization, 509–510
Commodity service, 510
Communicating service priorities, 820–821
Communication
   within company, 551
   company culture, 419
   customers, 837
   data centers, 170
   email service, 557–558
   emergencies, 488
   mail user agents, 551
   maintenance windows, 495
   nontechnical managers, 857–858
   plan updates, 57
   post maintenance, 490–491
   radios or mobile phones, 170
   scheduling and, 416
   sensitive updates, 420–421
   service conversions, 461–462
   stalled processes, 822
   technical issues, 791
Communication change, 418–419
Communication policy, 307
Communication skills
   active listening, 792–796
   happy SAs (system administrators), 790–796
   I statements, 791–792
   my problems, 791
   other people’s problems, 791
   our problems, 791
   your problems, 791
Communications closets, 300
Community strings, 529
CommVault, 622
Companies
   culture and communication, 419
   defending right to information, 310
   security, 314
Company policy, enforcing, 828–829
Company-confidential information, 274
Compensation (comp) time, 358
Competitive advantage, 847–848
Complete restores, 625
Complexity of networks, 190
Components
  failure, 597
  hot-swap, 86–87
  used by other applications, 115
Compression, 189
Computer closets, 35–36, 129
Computer room, 129
Computers
  building and initializing processes, 42
  centralizing purchasing process, 513–514
  clean desktop, 785
  clean state, 42
  configured state, 42
  coping with big influx of, 16–17
  debug process, 42
  early delivery to customer, 515
  entropy, 42
  function-based primary name, 109
  life cycle, 41–44
  new state, 42
  off state, 42
  preloading operating system, 51–53
  rebuild process, 42
  retiring, 44
  reviewing software on, 437
  service-based aliases, 469
  solid infrastructure, 287–288
  standardizing components, 514
  states and transitions exist, 43
  support time, 730
  tying services to, 98
  unknown state, 42
  updating, 42
  usable only in configured state, 43
  warranties, 76
Concurrent Versions System, 425
Condensing data, 525–526
Configuration files
  automated checks, 426–428
  locking, 424–426
  manually modified, 426–428
  master copies, 237
  separate for web site, 715
  tracking changes to, 453
Configuration fixes, 704
Configured state, 42–43
conf.v file, 425
ConServer, 80
Consistency policy, 233–234
Console access in data centers, 171
Console servers, 121, 171
Console window programs, 245
Consolidation
  centralization, 506–507
  purchasing, 513–515
Constraints, 476
Consultants, 743–745, 756
Consumables, 621
  planning and backups, 635–637
Contacts and security, 316–317
Containment, 63–64
Content scanning, 557
Contractors, 743–745
Contributing software policy, 671–672
Conversions, 465, 468
COO (chief operating officer), 734
Cooling
  air output from ceiling, 137
  computer closets, 35–36
  costs, 146
  data centers, 136–148
  humidity control, 137–138
  IDF closets, 201
  network devices, 201
  providing sufficient, 35–36
  racks, 151
  raised floors, 137
  rules, 137
  smaller solutions, 146
  spot coolers, 146
  UPS, 139
Coordination, ensuring, 483–488
CopyExact, 411
Copyright-adherence policy, 330–332
Corporate culture
  help desks reflecting, 346
  maintenance windows, 477
Corporate guidelines and backups, 625–626
Corporate namespaces, 543
Corporate network and third-party access, 279
Corporations
application response time, 537
ethical policies and controls, 323
helpdesks, 368
staffing helpdesks, 347
Cost/benefit analysis, 823
Costs, decreasing, 21
CPU
chip sets and L2 cache, 606–607
monitoring and, 524–525
monitoring usage, 601–602
servers, 70
Craft worker, 376–377
Crashes
coping with, 9
monitoring system, 36
Critical DNS server, upgrading, 453–454
Critical host maintenance contracts, 75–76
Critical inner voice, 805–807
Critical servers
dependencies, 483
lists of, 34
stringent change-management processes, 424
Critical services, 122
Critical systems, booting, 483
Criticism, 807–808
Crontabs, 78
Cross-functional teams, 310–313
Cross-shipping, 77
Cryptographic certificates, 705–706
CTO (chief technical officer), 733–734
CTRL-ALT-DEL, 81
The Cuckoo’s Egg (Stoll), 402
Customer advocate, 927
Customer dependency check, 437
Customer requests
basics, 364–380
frequent time-consuming requests, 383
greeting to, 364–367
Customer support, 735–736, 739–741, 931
centralized model, 740–741
decentralized model, 740
dedicated personnel, 739
hybrid models, 740
marketing-driven, 369
solutions, 847
Customers, 756
aligning priorities with expectations, 758–760
announcing upgrade to, 445–446
attitude of SAs, 756–758
becoming craft worker, 376
building confidence, 22
classifying problems, 368–369
communicating change to, 418–419
communicating conversion plan to, 461–462
communicating upgrade or back-out plan, 448–449
communication, 837
compelled to lie, 370
consultants, 756
cconversion having little impact on, 458–459
decentralization and, 511–512
defining emergencies for, 31
digging into problem before reporting it, 392–394
feature creep, 837
generating most tickets, 382
giving up control, 505
good first impression, 752–755
group statistics, 601
high and small things, 758–759
ignored requests, 28
ignoring messages from system administrators, 449
importance of printing, 565
incorrect jargon, 392
increased familiarity with, 381
inexperienced, 375
involving in standardization process, 66
keeping happy, 15
listening to concerns of, 503
locking out for server upgrade, 446–447
meeting with groups, 766–767
meeting with single point of contact, 866–868
opportunities to interact with, 757
perceptions, 751, 760
physical access to data center, 135
policies associated with email service, 558
prioritizing solutions, 375
processes to help themselves, 347–348
questions in particular category, 383
relationship with support team, 740–741
relying on services, 438
reporting same issue, 382–383
requirements, 837
restoring access after upgrade, 448
SA email to, 770–773
self-service requests, 383
service requirements, 98–100
service rollout, 120
setting hostnames, 62–63
standards, 66
task-length perception, 29–30
town hall meetings, 768–770
training, 462
usage guidelines, 326–327
useful feedback, 375
verifying repair of problem, 378
weekly meetings with, 867
Customer/SA, 931
Customization and decentralization, 511
Customizing striping, 611–612
Cutting edge, 218
Cylinders, 584

Data
backups, 619–620
block optimization, 607
condensing, 525–526
corruption, 267
expiring, 526
length of time to keep, 526
protection, 614
restoring, 619–620
security, 271–272
Data cables, 166
Data centers, 129
access, 134
basics, 130–176
biometric locks, 135–136
booting machines, 483
cleaned power, 138
communication, 170
communication backups, 131
console access, 171
cooling, 136–148
costs, 129
directing airflow, 137
duplicating critical services across, 268
dust and, 173
earthquake zone, 132
equipment, 130
extra electrical capacity, 144–145
extra space in, 179
extrawide doors, 134
fire suppression, 149–150
flooding, 132
heat sensors, 142
heating, 137
high security requirements, 135
high-reliability, 177–178
hot spots, 142
humidity control, 137–138
HVAC system, 142
ideal, 179–185
interruption of service, 473
keyboards, 171
keys, 135
labeling, 166–169
lightning protection, 132–133
locating servers in, 110
location, 131–132
Data centers (continued)
locking, 135
maintenance window, 130
MDF (main distribution frame), 204
minimum aisle width, 154
mobile items, 175–176
monitoring temperature, 143
monitors, 171
moving overview, 5
natural disasters, 131–132
physical checks, 300
planning for future, 130
political boundary, 131–132
power, 136–148
proximity badges, 135
racks, 150–159
raised floor, 134
redundancy, 176–177
redundant locations, 133–134
reliability, 110
restricting access, 135
security, 134–136
servers, 78–79
tools and supplies, 173–175
visitor policy, 136
wasted space, 156
wiring, 159–166
workbench, 172–173
working in, 173
Data flow analysis and scaling, 124–125
Data format, 189
Data integrity, 78, 267
Data pipeline optimization, 606–608
Data storage, 583, 864
basics, 584–611
CDP (continuous data protection), 614–615
cost, 589
current usage, 590
DAS (directly attached storage), 587
departments and groups assessment, 589
evaluating new solutions, 608–609
filesystems, 587
inventory and spares policy, 593
key individual disk components, 584–585
less-desirable hardware, 608
limits, 613–614
managing, 588–596
mapping groups onto storage infrastructure, 592–593
NAS (network-attached storage), 587–588
performance, 604–608
physical infrastructure, 609–610
pipeline optimization, 606–608
planning for future, 593–594
problems, 609–611
quotas, 592–593
RAID (Redundant Array of Independent Disks), 585–587
reframing as community resource, 588–589
resource difficulties, 592
SAN (storage area networks), 588
saturation behavior, 610–611
standards, 594–596
storage-needs assessment, 590–591
terminology, 584–588
testing new system, 608
timeouts, 610
unexpected events, 591
usage model, 608
volumes, 587
Data storage service, 596
backups, 598–601
historical monitoring, 601
monitoring, 601–603
reliability, 597–598
storage SLA, 596–597
Data transfer path saturation, 610–611
Data writes, 607
Database-driven web sites, 695–696, 716
Databases
automating data access, 710
high-availability and backups, 647–648
preparation function, 710
read-only views, 702
read-write views, 702
scaling usage, 702
tuning block size, 611–612
web sites, 701
Dataflow analysis example, 126
Dataflow model, 124–125
Data-recovery SLA and policy, 626
dbadmin account, 291
dbadmin group, 291
Deadlines for change completion, 488–489
Debug process, 42
Debugging
active monitoring systems, 533
basics, 391–398
better tools for, 399–400
email, 553
end-to-end understanding of system, 400–402
fixing cause, not symptom, 393–394
follow-the-path, 395
learn customer's problem, 392–393
Microsoft Windows, 396
networks, 190
right tools for, 395–398
Sun RPC-based protocols, 397–398
systematic about finding cause, 394–395
TCP-based protocols, 397–398
turning as, 399
UNIX systems, 396
Decentralization, 501
110 percent, 504
access, 504
balance, 504
basics, 502–512
candidates, 510–512
customization, 511
democratizing control, 510
diversity in systems, 512
fault tolerance, 510–511
guiding principles, 502–505
issues similar to building new service, 504
many single points of failure, 512
meeting customers' needs, 511–512
motivation, 502–503
opportunity to improve response times, 510
problem-solving, 502
veto power, 505
Decentralized model, 501, 740
Decision point, 417–418
Decisions
precompiling, 785–787
technical manager, 843–848
Decreasing costs, 21
Dedicated machines services, 120–122
Dedicated network router, 84
Deexecutioner, 379
Defense in depth, 272
Defining emergencies, 31
Defining scope of SA team's responsibility policy, 31
Definition of emergency policy, 821
Defragmenting hard disks, 614
Delegation, 831
Deleting files and UNIX shells, 410–411
Deletion policy, 671–672
Demarcation points, 205
Dependency chains, 539
Depots, 672
Descriptive names, 225–226
Desk location and visibility, 767
Desktop computers
cost in early 1990s, 90
eyear, 130
Desktops, rolling out new software to, 120
Developer's tool chain, 685
Device discovery, 535
Device drivers, 53
Devices
labeling, 34
monitoring discovery, 535
naming standards, 206
networks, 209–211
parts not hot swappable, 88
SNMP requests, 529
UPS (uninterruptible power supply), 35
Devices Control Panel, 410
DHCP
  automatically generating configuration, 59
  dynamic DNS servers, 61–65
dynamic leases, 60–61
hidden costs, 58
lease times, 64–65
moving clients away from resources, 64
network configuration, 58
public networks, 61
templates rather than per-host configuration, 58–60
DHCP: A Guide to Dynamic TCP/IP Network Configuration (Kercheval), 65
The DHCP Handbook (Lemon and Droms), 65
DHCP servers, 58
Diagnostic services and maintenance contracts, 75
Diagnostic tools, 395–398
Diameter, 232
diff command, 377, 440
Disaster worrier, 925
Disaster-recovery plan
  archives, 624
  basics, 261–267
damage limitation, 264–265
data integrity, 267
lack and risk-taking, 262
legal obligations, 263–264
media relations, 269
preparation, 265–267
recreating system, 266
redundant site, 268
requirements for, 264
risk analysis, 262–263
security disasters, 268–269
Disasters
  being prepared for, 265–266
damage limitation, 264–265
damage prevention, 263
  defining, 262
restoring services after, 265–266
risk analysis, 262–263
Disconnection policy, 306–307
  Disk failures, 602, 623
  Disk-cloning system, 32
  Disposable servers, 91
Distributed network support, 738
Distributed parity, 586
Distributed systems and centralization, 506
Distribution-server model, 668–669
Diversity in systems, 512
DLTs (digital linear tapes), 635–637
DNS, 96–97
  appliances, 84
  authenticating updates, 63
  hosts with static leases, 62
  MX (Mail eXchanger) records, 553
  no customer requirements, 98
  round-robin name server records, 699–700
  updates and TTL (time to live) field, 467
  zones and subzones, 233
DNS hosting, 717
DNS master, 121
DNS names, 225
Document repository, 247–248
  dynamic, 252
  important documents and, 266
  rollout issues, 251
  rules or policies, 248
  self-management versus explicit management, 251–252
  source code control, 248
Document retention policy, 560
Document root, 695
Document storage area, 247–248
Documentation, 241, 253
  accounts requiring special handling, 763
  basics, 242–252
  capturing command line, 245
  capturing screen shots, 244–245
  change management, 422, 424
  change procedures, 236
  checklists, 34, 246–247
  creation as you work, 34
  culture of respect, 253–254
device names, 206
document repository, 247–248
dynamic repository, 252
e-mail, 245–246
e-mail service, 557–558
enabling comments, 254
feedback, 243–244
labeling, 206
LAN connections, 207
making work easier, 241
maps of physical and logical
    networks, 205–206
metadata, 243
monitoring, 534–535
networks, 205–207
online, 206
partially automated installation, 49
print service, 573–574
QA (quality assurance), 243
quick guide, 244
redundancy, 241
request-tracking system, 246
restores, 638
revision control, 254
rollout issues, 251
routers, 207
search facility, 250–251
shared directory, 248
software depots, 672–673
sources for, 244–246
storage, 247–248
template, 243–244
title, 243
trouble-ticket system, 246
WAN connections, 207
what to document, 242–243
wikis, 249–250
Documentation repository, web-based,
    249–250
Documenting
    disliked processes, 242–243
    job description, 243
    security policies, 276–283
Doers of repetitive tasks, 936
DokuWiki, 253
Domain registration, 717
DOS, 587
DoS (denial-of-service) attack, 273,
    309, 320
Double component failure, 87
Draft server, 717
Dress rehearsal, 451–452
Drive controller, 585
Drive protocol, 585
Drivers and preloaded operating
    systems, 53
Drupal, 253
Dual-boot updates, 56
Due-diligence assessments, 7–8
Dumb pipelining algorithm, 7, 8
Dumpster diving, 229, 334
Duplex printing, 576
Duplexing units, 569
Dynamic DNS servers and DHCP,
    61–65
Dynamic leases, 60–62
Dynamic routing, 208
Dynamic to-do lists, 779
Dynamically generated web pages,
    691
E
EAP (employee assistance program),
    807
echo command, 410–411
ECMAScript, 691
E-commerce sites
    application response time, 537
    authorization matrix, 320
    backups, 625
    change management, 415
    end-to-end testing, 537
    helpdesks, 347, 368
    IT and system administration, 742
    layers and pillars conversions, 461
    maintenance windows, 475
    namespaces, 233
    pervasive monitoring, 535
    privacy laws, 337
    SA function of maintaining site, 742
    SA (system administrators) team,
        746–747
    security programs, 319–320
    verifying problems, 373
EDA, 311
Educating customers, 384
Educator, 923
EIGRP (Enhanced Interior Gateway Routing Protocol), 187
Eircom, 169
Electronic accomplishment wall, 811
Email, 543
    as alerting mechanism, 530
    all customers, 770–773
    archiving, 784
    arriving in unexpected place, 548
    backups, 559–560
    bounced, 409
    company-confidential information, 544
    consistent look and feel, 739
    content scanning, 557
    debugging, 553
    documentation, 245–246
    filtering, 284
    forwarding policy, 338, 552
    handling only once, 784
    internal and external email addresses, 545
    message sizes, 555
    message storage, 543
    monitoring, 337
    namespace, 544
    privacy policy, 544
    reading someone else’s, 339–340
    reliability, 543
    remote access service, 654
    retention policy, 559–560
    risks associated with, 558
    saving copy, 245
    scalability, 543
    SEC violations, 337
    traffic levels, 554
    working well, 33–34
Email access servers, 547
Email accounts, 552
Email addresses, 545
    name conflicts, 226–227
    reuse policy, 235
Email appliances, 84
Email clients
    checking for email at predefined interval, 555
    encryption, 559
    protocols, 551
Email machines and hot spares, 547
Email servers, 121, 503, 547
    aliases, 549
    monitoring, 552–553
Email service
    advanced monitoring, 560–561
    automation, 552
    bad mail-delivery scheme, 548–549
    basic monitoring, 552–553
    basics, 543–558
    beta test, 546
    communication, 557–558
    documentation, 557–558
    encryption, 559
    gateways and email translation devices, 549
    generality, 550–551
    high-volume list processing, 561–562
    lack of standardization, 549
    large bursts of traffic, 554
    machines involved in, 547–548
    message size limits, 556
    namespaces, 544–546
    policies, 558
    redundancy, 553–554
    reliability, 123, 546–547
    scaling, 554–556
    security, 544, 556–557
    simplicity, 547–549
    spam, 549–550
    spare spool space, 556
    virus blocking, 549–550
Email software, 106
Email system
    architecture, 543
    costs of malfunctioning, 546
    failure, 546
    namespace management system, 543
    open protocols, 543, 550–551
    proprietary, 107
    viruses, 557
Emergencies, 29, 31–32
  communication during, 488
  defining in writing, 353–354
  planning and, 354
Emergency facility, 266–267
Emergency lighting, 143
Employees
  explaining failure to, 839
  feedback, 839
  in-person orientation, 755–756
  listening to, 840–841
  publicly acknowledging, 838
  recognition, 838–839
  reprimands, 839–840
  respecting, 838–841
  retention, 401, 893–894
Encrypted tunnels, 212
Encryption, 189, 559, 656
Encryption system, 559
End-to-end expert, 937
End-to-end monitoring, 561
End-to-end testing, 536–537
End-to-end understanding of system, 400–402
Enjoying what you do, 804
Entropy, 42
Environment
  identifying fundamental problems in, 13
  services, 110–111
Environment variables, 406
Environmental issues and printers, 575–576
EPO (emergency power off) procedure, 485
Equipment
  height in rack units (U), 152
  labeling, 166
  reusing internally, 596
Error messages, real-time monitoring, 531
Escalation
  establishing process, 352–353
  monitoring rate of, 356
  Escalation policy, 353, 531–532
  Escalation procedure, 532
  ESMTP (extended SMTP), 550
Etherreal, 395
Ethernet, 101, 187, 198
Ethics, 323
  basics, 323–336
  copyright adherence, 330–332
  customer usage guidelines, 326–327
  hiding evidence, 336
  informed consent, 324
  issues, 23
  law enforcement and, 332–335
  people harming your company, 335
  privacy and monitoring policy, 336–337
  privileged-access code of conduct, 327–330
  professional code of conduct, 324–326
  something illegal/unethical, 338–340
ETR (estimated time to repair), 656
ETSI (European Telecommunication Standards Institute) standard, 177–178
Exchange mail server, 107
Executing solutions, 375–376
Exit process, 287
Experience counts, 503
Expertise, 508
Expiring data, 526
Extensibility and servers, 70
External audits, 308–309, 317
External sites and security, 717
F
Facilitator, 930–931
Failed disk, mirroring, 83
Failover, 86
Failures
  alerting to, 524
  corruption of arrays or scrambled data, 609
  hot-swap components, 87
  reporting, 530
  single points of, 510, 512
Family Educational Rights and Privacy Act, 323
Family time, 810
FAQ (Frequently Asked Questions), 256
Fast (100MB) Ethernet, 188, 198
FAT, 587
FAT32, 587
Fault tolerance and decentralization, 510–511
FC (fibre channel), 606
FCC (Federal Communications Commission), 330
FDDI (Fiber-Distributed Data Interface), 188
Feature creep, 837
Features, adding, 21
The Feeling Good Handbook (Burns), 806
Fiber termination, 202
Field offices security team, 312–313
File formats, 104
File Motel, 622
File servers, 121
appliances, 84
centralized, 509
File systems fragmentation, 614
Filer line of file appliance, 622
Files
accidentally deleting, 410–411, 621–623
automated checks, 426–428
capturing session to, 245
listing to be deleted, 410
mystery-deletes, 401–402
rebuilding, 413
Filesystems
journaling, 587
snapshots of, 622
Filtering email servers, 547
FIN packet, 700
Fire drills and backups, 643–644
Fire suppression in data centers, 149–150
Fire-prevention systems, 265
Firewalls, 271, 284, 289, 702
email protection, 557
general-purpose machines as, 211
inbound rules, 123
OS-based, 210–211
permitting only outbound email (SMTP) traffic, 123
remote access service, 655–656
Firing SAs (system administrators)
access databases, 904–905
corporate policies for, 900
physical access, 901
remote access, 901–902
service access, 901–904
single authentication database, 905
system file changes, 906
termination checklist, 900–901
First offer, 802–803
First tier of support, 352–353
First-class citizens, 45
First.last-style email addresses, 545
Five-year vision, 864–866
Fixing
biggest time-drain, 34–35
problems, 373–376
real problem, 413
same small things time after time, 408
things once, 405–412
Flash-cuts, 463–465
Flat namespaces, 223
Flat network topology, 197
Flat physical topology, 212
Flexibility, improving, 501
Flight director, 478
change completion deadlines, 488–489
developing master plan, 481–482
mentoring new, 492–493
performance level of SA team, 489
technique, 473–474
Floor puller game, 183
Follow-the-path debugging, 395
Follow-through, 28–29, 778–780
Formal documents and legal issues, 560
Formal training on tools, 400
Form-field corruption, 708
Formulaic names, 225
Four-post racks, 153–154
Fragmentation and multiuser systems, 614
Frame Relay, 212
Free software licenses and copying, 331
FreeBSD system, 211
Fresh installs, 450–451
Front-line support group, 119
Front-mountable servers, 153
FTP (File Transfer Protocol), 189, 296, 398
Full backups, 620, 624, 627–628
Full mesh, 212
Full redundancy, 86–87, 122
Full-disclosure mailing lists, 289
Functional group-based topology, 197
Functional names, 225–227
Functionality and security-sensitive products, 297
Fundamental services, 95, 111
Fuzzy match algorithm, 440

G
Gateways, 106–107, 549
General printer architecture policy, 568
General-purpose machines, 234
Generators, 139–140, 265
  backup building circuits, 143
distributing, 177
failure, 177
maintenance, 141
Generic services, 95
GET request, 528–529, 691
Getting Things Done, 815
Gigabit Ethernet, 198
Globalization overview, 4
Globally flat namespaces, 233
GNAC, Inc., 148, 157
GNU Stow, 672, 675–677
GNU/Cfengine, 237
Goal setting, 781–782
Goals, 830
  nontechnical managers, 836
  structure to achieve, 821
Golden host, 50
Golden master server, 718
Good first impressions, 752–755
Google, 90
  definition of emergencies, 32
gmail service, 784
IT teams, 747
mass email, 772
printer maps, 574
updating servers, 463
Google Maps, 721
Go-to person, 916–917
Graphical programs, 441
Graphs and historical monitoring, 527
Grouped power cords, 114
Groups
  mapping onto storage structure, 592–593
  new manager, 19
  new members, 18–19

H
The Hagglers Handbook (Koren and Goodman), 803
Halt key sequence, 121
Halt message, 121
Handheld token-based system, 291
Handles, 232–233
Handling paper once, 783–784
Happiness, 806–807
Happy SAs (system administrators), 777
  awards wall, 810–811
  basics, 778–797
  communication skills, 790–796
  follow-through, 778–780
  loving your job, 804–811
  managing your manager, 811–814
  negotiation, 798–803
  organizing, 778
  professional development, 796–797
  staying technical, 797
  time management, 780–790
to-do lists and appointment calendars, 778–780
Hard disk controllers, 83
Hard disks
  blocks, 584
  cloning, 50–51, 443
  cyclinders, 584
  DAD (disk access density), 613
defragmenting, 614
density, 613
discarding, 595
Hard disks (continued)
  drive controller, 585
  drive protocol, 585
  fragmentation, 613–614
  HBA (host bus adapter), 585
  heads, 584–585
  increasing size, 613
  key individual components, 584–585
  performance, 613
  platters, 584–585
  price per gigabyte, 583
  price per megabyte, 583
  sectors, 584
  spindle, 584–585
  tracks, 584
Hard emotions, 791–792
Hard outages, 114
Hardware, 81
  buying for servers, 69–71
  cost of, 72–74
  failure, 597
  grouped power cords, 114
  servers, 69
Hardware cards and remote console
  access, 81
HavenCo, 133
HBA (host bus adapter), 585
Head hunters, 875
Heating and data centers, 137
Hello. World program, 440–442
Help, specifying how to get, 351–352
Helpdesk, 343
  basics, 343–356
  better advertising for, 358–359
  call hand-off procedures, 347
  call-volume ratios, 347
  centralization, 741
  classifier role, 368
  communicating procedures, 344–345
  corporate culture, 346
  corporations, 368
  critically examining metrics, 517
  customer-to-attendant ratios, 347
  defining emergency in writing, 353–354
  defining processes for staff, 352
  defining scope of support, 348–351
  division of labor, 360
  e-commerce sites, 368
  emailing new policies, 359
  escalation procedures, 352–353, 741
  formal and informal, 344–345
  friendly face, 346
  greeters, 367
  having enough staff, 347
  home phone number of supervisor, 358
  identifying top 10 requesters, 357
  installing new service, 359–360
  metrics, 347
  multiple, 741
  multiyear trends, 356
  out-of-hours and 24/7 coverage, 357–358
  out-of-scope technologies, 350–351
  permitting tickets creation by email, 408
  portal Web site gateway, 359
  problems with service, 119
  recorder, 369–372
  as referral service, 350
  reporting problems, 359–360
  requesting new services, 359–360
  request-tracking software, 354–356
  SA (system administrators) teams, 741
  SAs (system administrators), 736–737
  scripts, 352
  SLAs (service-level agreements), 32
  specifying how to get help, 351–352
  statistics, 354–357
  time management, 351–352
  time-to-call completion, 347
  virtual, 345
  web site for documentation and FAQs, 348
Helping someone, 804–805
HHA (handheld authenticators), 278, 905
Hidden infrastructure, 491
High consistency, 233–234
High-availability data service, 598
High-availability databases backups, 647–648
High-availability sites, 495–497 availability, 497
High-latency links, 101
High-latency networks, 102–103
High-level management support for network policies, 280–282
Highly critical host maintenance contracts, 75
High-performing salespeople, 363
High-port-density network equipment, 168
High-reliability data centers, 177–178
High-volume list processing, 561–562
High-volume list services, 562
Hijacked web sites, 703–704
HIPAA (Health Insurance Portability and Accountability Act), 323
Hiring SAs (system administrators) basics, 871–894
diversity, 880–881
employee retention, 893–894
getting company noticed, 894–895
identifying people to hire, 871–872
interview process, 884–886
interview team, 882–883
job description, 872–874
knowing what you are looking for, 879–880
nontechnical interviewing, 891–892
persuading them to work for you, 871–872
recruiting, 875–877
rushing hiring decision, 878
selling position, 892–893
skill level, 874–875
team considerations, 878–882
technical interviewing, 886–890
timing, 877–878
Hiring System Administrators (Phillips and LeFebvre), 879
Hiring the person, 873, 876
Hiring the skill, 873, 876
Historical data
collection, 215–216, 523
trending, 493
Historical metamonitoring, 540
Historical monitoring, 523–527
data storage service, 601
scaling problems, 538
history command, 245
Hit-and-run sysadmin, 379
Home network routers, 211
Home office, 662–663
/home/adm/docs directory, 248
Homegrown off-site backup storage, 646
/home/src directory, 673
Horizontal cable management, 158
Horizontal scaling, 699–700
Hostnames, 62–63, 228
Hosts
broadcasting incorrect routing information, 208
center-of-the-universe, 122
complex routing problems, 209
consolidating services onto fewer, 506
determining hostname, 62
dynamic leases, 62
intruders breaking into, 703–704
IP addresses, 60–61
labeling, 182
MAC (media access control) address, 48
multihomed, 208
multiple servers on one, 697–698
names, 228
requiring to perform routing, 209
securing before going live, 290
simple routing, 207–209
single-homed, 208
starting in known state, 32–33
static leases, 62
Hot spares, 547, 587
Hot spots, 142
Hot-plug components versus hot-swap components, 88–89
Hot-swap components, 87–89
HousingMaps, 721
How to get help policy, 31, 820
How to print document, 573–574
How-to docs, 255–256
HP OpenView, 367
HP-UX, 46, 54
HTML (Hypertext Markup Language) and wikis, 249
HTTP (HyperText Transfer Protocol), 189
   error and status codes, 692–693
   web based products, 297
HTTP over SSL (Secure Sockets Layer), 704–705
HVAC systems, 141–142, 176–177

I
I statements, 791–792
IBM
   Clean Desk Policy, 315
   FDA division, 311
   Nagano Olympics, 430–431
ICMP (Internet control message protocol), 526–527
Ideal data centers, 179–185
IDF (intermediate distribution frame), 212–213
   aligning vertically in building, 199
   allocating space for, 198–199
   arranging, 205
   closet numbers, 200
   connecting, 203–205
   connecting cable, 198
   connecting to another IDF, 198
   connections with MDF, 199
   installing jacks, 201–202
   laying out, 198–199
   locking, 200
   numbering, 200
   punch block, 198
   remote console access, 200
   restricted access, 200
   RJ-45 connectors, 198
   running fiber, 202
   security, 200
   wiring, 198
IDF closets, 201
IDS (intrusion detection systems), 299
IEEE (Institute of Electrical and Electronic Engineers), 107
IEEE 802.1q VLAN protocols, 212
IEEE 802.1x, 61
IETF (Internet Engineering Task Force), 107, 562, 689
IETF standards, 214
Ignite-UX, 46
Illegal or unethical actions, 338–340
IMAP (Internet Message Access Protocol) server, 109
IMAP4, 189, 556
Implementers, 302, 737
Improving system administration
   biggest time-drain, 34–35
   calendaring, 33–34
   documenting as you go, 34
   email, 33–34
   host starting in known state, 32–33
   power and cooling, 35–36
   quick fixes, 35
   quick requests, 29–30
   simple monitoring, 36
   time-saving policies, 30–32
   trouble-ticket system, 28–29
Incident response, 303–307, 319
Incident-reporting mechanism, 305
Incident-response team, 303–304
Incremental backups, 620, 622, 627–628, 633
Independent services, 115
In-depth attacks, 308
Individual file restores, 624
Industrial espionage, 267
Informal documents and legal issues, 560
Informal off-site backup storage, 645
Information
   malicious alteration, 274
   protection, 271
   security, 313–314
Information-protection group, 318
Information-protection program, 315
Informed consent, 324
Infrastructure
   maintaining services, 730
   services, 97
   standards, 508–509
Infrastructure builder, 917–918
Infrastructure teams, 737–739
Input, validating, 709
Insecurity, 806
Insider trading, 337
Install room, 55
Installation, 43
  partially automated, 49–50
  pervasive monitoring, 535
  UNIX software, 668
  well-documented process, 49
Installer, 914
Installing new service, 359–360
Instant rollback of service conversion, 467–468
Integration and security-sensitive products, 297
Integrators, 736
Intel, 411
Intellectual property, protecting, 310
Intelligent queuing mechanisms, 118
Interactive web pages, 691–692
Intercompany security focus groups, 301
Interfaces, labeling, 167
Internal auditing, 298–300
Internal auditing team, 308
Internal mail servers, 123
Internal sites publishing model, 716
Internal verification, 299
Internal web services and security, 704
International business sites privacy laws, 337
Internet, 195
  gateway and law enforcement, 335
  mobile phone access, 692
  security, 271
  SMTP-based protocol, 550–551
  transmission of unencrypted information, 656
Internet-based backup systems, 647
Interpersonal communication, 376
Interpersonal effectiveness, 376
Interruption of service, 473
Interruptions, handling, 29–30
Interview process, 884–886
Interview team, 882–883
Intranets and privileged information, 704
Intrusion incident-response team, 303
Inventory, automated, 238
Inventory and spares policy, 593
Involvement, 503
I/O servers, 70
IP addresses, 60–61
  dependencies, 121
  longevity policy, 230–231
IP (intellectual property) manager, 310
IP-KVMs, 80–81
IRIX RoboInst, 54
Irrevocable key, 136
iSCSI, 606
ISDN (Integrated Services Digital Network), 196
ISO (International Organization for Standardization) standards, 257
ISPs maintenance windows, 475
ITIL (Infrastructure Library), 417
JavaScript, 691–692, 692
Job Descriptions for System Administrators (Darmohray), 874
Jobs
  advertisement, 872
  description, 243, 872–874
  looking for, 19–20
  protecting, 23–24
Journaling, 587
Jukeboxes, 639, 642
JumpStart, 46, 48–49, 51, 65, 406
Kerberos authentication system, 105
Kernel and packet routing, 210
Key escrow, 705
Keyboards in data centers, 171
Kick-off meetings, 100
KickStart, 46
Known state, 52, 55
KVM switches, 80–81, 486
L
L1-A, 81
L2 cache, 606–607
Lab technician, 919–920
Labeling
cables, 167–169, 182, 206
data centers, 166–169
equipment, 166
high-port-density network
equipment, 168
hosts, 182
interfaces, 167
keeping up to date, 168
network equipment connecting to
WANs, 168
network jacks, 200
networks, 205–206
policy for enforcing standards, 169
ports in software, 168
printers, 574
racks, 160
Labeling devices, 34
LAMP (Linux, Apache, MySQL, and
Perl), 697
LAMP (Linux, Apache, MySQL, and
PHP), 697
LAMP (Linux, Apache, MySQL, and
Python), 697
LANs, 188
connections documentation, 207
dynamically assigned leases, 60
large using VLANs, 212–213
network bandwidth, 524
not sent routing protocols on, 208
star topology, 191–192
Laptops and critical device drivers, 53
Large companies
SA (system administrators) team, 746
security program, 319
Latency
versus bandwidth, 101–103
finding problem, 398
recording information, 526
storage SLA, 596
Law enforcement, working with,
332–335
Layers approach, 460–461
Layers versus pillars, 460–461
LDAP (Lightweight Directory Access
Protocol), 115, 239, 720
LDP (Line Printer Daemon) Protocol
over TCP/IP, 569
Leading edge versus reliability,
217–218
Leaf node, 193
Learning
from carpenters, 410–412
from mistakes, 832
new skills, 796
Lease times and DHCP, 64–65
Legal department, 310–311, 313
Legal issues, 560
Level 0 backup, 620
Level 1 backup, 620
Level-focused person, 935
Levels, 585
Leveraging namespaces, 239
License servers, 761
Lights-out operation, 147
Line-of-sight radio communications,
487
Linux Documentation Project, 258
Linux system, 211
Linux tools, 667
LISA (Large Installation System
Administration) conference, 797,
848
List of printers, 574
List processing, 547
high-volume, 561–562
redundancy, 553
scaling, 554–555
List servers, 562
Live audio and video, streaming, 692
Live equipment, 150
Load balancers, 89, 554, 700, 702
Load balancing print service, 577
Load sharing, 87
Load testing, 117
Loading operating system, 46–54
Locally replicated software backups,
683
Location numbers, 200
Location-based topology, 197
Locking, 424–426
Log files, rotating, 533
Logging, 451, 710
Logic bomb, 906
Logical networks
  maps of, 205–206
  topology, 195–197
Logical-network topology, 205
Logins and name conflicts, 226
Log-retention policy, 277
Logs, 299
  detailed and timestamped, 306
  storing in nonstandard space, 710
Longevity policy, 230–231
Long-term motivators, 804–806
Long-term solution, 822–823
LOPSA (League of Professional System Administrators), 72, 324, 796
Lose-lose situation, 798
Lose-win situation, 798
Loving your job
  accepting criticism, 807–808
  asking for help, 808–809
  bad boss, 807
  balancing work and personal life, 809–810
  being motivated, 804–806
  enjoying what you do, 804
  great boss, 807
  happiness, 806–807
  support structure, 808
Low-latency environment, 102
Loyalty, 838
Lucent Technologies, 232–233, 457
LUDE, 672
Lumeta, 151, 477

M
MAC (media access control)
  address, 48
Mac OS X, 237
Mac OS X server, 211
Machine independence services, 109
Machine room, 82, 129
Mail delivery systems, 554–555
mail global alias, 98
Mail relay hosts, 553, 556–557
Mail transport systems, 554–555
Mail user agents communications, 551
Mail-filtering software, 788
Mailing lists, 399, 409, 552, 561–562, 788
Mailping, 536
Mainframes, 130
Maintainer, 915
Maintenance, 735–736
  generators, 141
  selecting window for, 443–445
  UPS, 140–141
Maintenance contracts, 74–78, 731
Maintenance patches, 297
Maintenance windows, 130
  basics, 475–492
  benefiting company, 474–475
  communications, 495
  comprehensive system testing, 489–490
  corporate culture, 477
  deadlines for change completion, 488–489
  developing master plan, 481–482
  direct console access, 486
  directing, 478
  disabling access, 482–483
  e-commerce sites, 475
  ensuring mechanics and coordination, 483–488
  flight director, 473–474, 478, 492–493
  handheld radios, 486–488
  hidden infrastructure, 491
  high availability for systems, 475
  high-availability sites, 495–497
  interruption of service, 473
  ISPs, 475
  KVM switches, 486
  limited service ability, 493–494
  managing change proposals, 479–481
  planning, 477
  postmaintenance communication, 490–491
  postmortem, 492
  reducing complexity and making testing easier, 474
  redundancy, 496
  reenabling remote access, 491
Maintenance windows (continued)
SA group visibility after, 491–492
scheduling, 474–476, 495
serial console servers, 486
shutdown/boot sequence, 483–485
testing console servers and tools, 482–483
trending historical data, 493
undetected problems, 492
weekly reminders, 476
Major outage, surviving overview, 10–11
Major updates, 420, 422
Majordomo mailing lists, 409
make account command, 237
make command, 236
make newuser command, 237
Makefiles, 237, 413
automating tasks, 677
VPATH facility, 673
Malicious alteration, 274
Malware
blocking, 550
protection, 284
Managed hosting, 718
Management
keeping happy overview, 15
security officer, 281
security policy issues, 300–314
tasks, 797
telling you to break the law, 331
time-saving policies, 31
Management chain, 733–734
Managers
career goals and, 812–813
grooming SAs for positions, 813
information provided for boss of, 26
making success of, 811–812
making your needs known to, 812
managing, 811–814
non-work-related requests, 814
raises and, 811
time management, 813
understanding security job, 282
upward delegation, 813–814
what system administrators expect from, 26
Managing quick requests correctly, 29–30
Managing risk, 415
Managing your manager, 811–814
Manual backups, 639, 641
Manual installation, 43
Manual processes, 46
Manual steps and automation, 764–765
Mashup applications, 721–722
Mass email, 770–773
Master images, 50
Master plan, 481–482
Master station, 538
MDA (mail delivery agents), 547
MDF (main distribution frame), 198–199, 203–205, 212–213
Mean time to attack, 289
Measuring, 604
Measuring twice, 410–411
Mechanics, ensuring, 483–488
Media
disasters and, 269
off-site backup storage, 644–647
Media servers, 696–697
MediaWiki, 253
Medium-sized company
SA (system administrators) team, 745–746
security program, 318–319
Memory and monitoring, 524–525
Mentor Graphics, 248, 445
Mentoring new flight director, 492–493
Mentors, 881–882
Mergers overview, 8–9
Merging existing namespaces, 226–227
Metamonitoring, 539–540
Metrics
helpdesks, 347
SAs (system administrators), 384
security, 317
MIBs, 528
Microformats, 692
Micromanagement, 855–856
Micromanaging, 841
Microsoft
  ActiveDirectory, 64, 237, 332
  DHCP servers, 60
  Exchange mail server, 107
  Kerberos authentication system, 105
  preventing interoperating with non-Microsoft Kerberos systems, 105
Microsoft Exchange, 551
Microsoft IIS, 691
Microsoft OSs, 438
Microsoft Windows, 410
  automating software updates, 54
  debugging, 396
  Remote Installation Service, 46
Microsoft Windows NT 4.0, 50
MIL-SPEC requirements, 72
Minicomputers, 130
Mirrored disks
  backups, 84
  break, 599
  reattached, 599
Mirroring, 83, 585–586, 587, 599–600, 792–794
MIS, 312
Misdelegator, 379
Mobile phones, 170–171, 692
Model-based training, 380, 381
Modem pools, 664
Modems and backward compatibility, 664
Modules, 672
MONET (multiwavelength optical network), 188
monitor, 930
Monitoring, 523
  accessibility, 534–535
  active systems for, 532–534
  alerting, 215
  application response time, 537
  automation, 535
  availability, 527
  basics, 523–534
  capacity, 527–528
  clogging network links, 538
  CPU and memory, 524–525
  CPU usage, 601–602
  crashes, 36
data storage service, 601–603
dependency chains, 539
device discovery, 535
disk failures, 602
documentation, 534–535
duplicating, 540
e-mail, 337
e-mail servers, 552–553
e-mail service, 552–553
end-to-end testing, 536–537, 561
file service operations, 603
granular priority system, 538
high-volume list services, 562
historical, 215–216, 523–524, 525–527
individual resource usage, 603
I/O local usage, 602
lack of usage, 603
master station, 538
metamonitoring, 539–540
multiple variables in SNMP, 528
network bandwidth, 524
network local interface, 602
networking bandwidth usage, 602–603
network-interface state transitions, 215
networks, 214–215
nonredundant network component, 539
notification scripts, 602
outages, 602
performance problems, 524
pervasive, 535
postmaster address, 553
print service, 574–575
problems failed to catch, 536
RAID for disk failures, 597
rate of change, 602
real-time, 215, 523–524, 527–534
remote probes, 538
routing problems, 215
scaling problems, 537–539
security, 525
services, 119
setting expectations, 336–337
Monitoring (continued)
- space used/space free, 602
- spikes or troughs, 601
- spoolers, 574–575
- status of printers, 575
- storage volume utilization, 601
- storage-access traffic, 601
- storage-to-server networks, 603
- tasks, 524
- web server errors, 698
- web services, 698–699

Monitoring and privacy policy, 277, 318, 321
Monitors in data centers, 171
Morale, 838, 855–857
Motivation, 502–503
Motivators, 804–805
Motorola, 316
mountd, 397

Moving data center overview, 5
MPLS (Mail Protocol Label Switching), 187
MRTGs (multirouter traffic graphics), 255, 538
MS-SMS (Microsoft’s System Management Service), 668
MTA (mail transport agent), 547
MTTR (mean time to repair), 73
MUA (mail user agent), 547
Multicast, 187
Multihomed hosts, 208, 210
Multimedia files, 692
Multimedia servers, 696–697
Multiple administrative domains, 219
Multiple inexpensive servers, 89–92
Multiple servers on one host, 697–698
Multiple-star topology, 192, 196
Multiply-redundant spoolers, 573
Multiuser systems and fragmentation, 614
Multiyear maintenance contracts, 800–801
My SQL, 238
Mystery file deletes, 401–402

N
- N + 1 redundancy, 85–87
- Name conflicts, 226–227
- Name services, 96, 122
- Name tokens, 545–550

Names
- aliases, 231
- corporate culture, 227–228
- descriptive, 225–226
- difficult-to-type, 228
- formulaic, 225, 227
- functional, 225–227
- hosts, 228
- longevity, 231
- no method for choosing, 225
- obscuring, 231
- security implications, 228
- sequential, 227
- thematic, 225, 227

Namespace databases, 232
Namespace management system, 543

Namespaces
- abstract or concrete thing, 223
- access control policy, 229–230
- adding software packages into, 244
- attributes, 223
- backup policies, 230
- basics, 224–237
- centralizing into SQL database, 238
- centralizing management, 236–237
- change control, 230
- change procedures, 236
- changes, 230
- cleanup, 236–237
- conflicts, 226
- consistency policy, 233–234
- corporate, 543
- customer-based updating, 239
- diameter, 232
- email service, 544–546
- flat, 223
- functional aliases, 227
- further automation, 238
- globally flat, 233
- inventory of all systems, 238
leverage, 239
longevity policy, 230–231
managed formally, 223–224
master copies, 237
merging existing, 226–227
name tokens, 545–550
naming policy, 224–228
policies, 224–236
protecting from modification, 230
reuse policy, 235
scope policy, 231–233
single, global, 232–233
thickness, 232
unique corporation-wide, 545
wide and thick e-commerce, 233
Naming conflicts, 715
Naming conventions, 207
Naming policy, 224–228
Naming standards, 234
NAS (network-attached storage), 587–588
backups, 600
configuration changes of underlying networks, 610
file-sharing services, 605
performance, 605
NAS servers, 598, 600
NAT (network address translation) gateways, 702
Natural disasters, 131–132, 645
NEBS (Network Equipment Building System) standard, 155, 177–178
Negative behavior, 824
Negotiations
after making request or offer, 802
always refusing first offer, 802–803
asking for what you honestly want, 801–802
being careful what you say, 803
developing positive relationship, 800
doing your homework, 800
format of meeting, 801
information not leaked, 798
knowing vendor’s competition, 799
multiyear maintenance contracts, 800–801
nebulous requests, 799
not revealing strategy to opponent, 802
planning, 799
power dynamic, 799
recognizing negotiating situation, 798–799
rehearsing situation, 800
silence as negotiating tool, 803
variety of techniques, 801
working toward win-win situation, 798
NetAid, 431
NetApp, 121, 622
NetApp Filers, 85
Network access control, 61
Network addressing architectures, 187
Network Administrator, 291
Network Appliance’s file server, 586
Network cables, 167–168
Network components outage and monitoring, 539
Network configuration, 57–61, 610
Network connectivity policy, 277
Network devices, 209–211
automating weekly audit, 529
cooling, 201
firewalls, 210–211
hardware or MAC address, 188
hot-swappable interface cards, 88
IP (or AppleTalk or DECnet), 188
moving packets quickly, 209–210
path data travels, 188
routers, 209–210
software upgrades and configuration changes, 211
switches, 209
transport information, 188
UPS (uninterruptible power supply), 35
Network disk, 668
Network equipment connecting to WANs, 168
protected power, 201
Network Information Service, 232
Network jacks, 200
Network Notes, 690
Network policies
  centralizing authority, 282–283
  high-level management support, 280–282
Network racks, 204
Network router, 84
Network row, 204
Network services
  design of, 196
  modern computing infrastructures, 739
  scripted tests, 441
Network vendors, 213–214
Network-based backups, 641
Network-based software push system, 668
Networked off-site backups, 646–647
Networking
  constants, 219–220
  TCP/IP, 188–189
Networking devices, 81
Networking printers, 568
Networks, 187
  administrative functions, 89
  assigned based on physical location, 197
  bandwidth and local area network, 524
  basics, 188–217
  cables, 163
  centralizing management, 738
  changes in design, 220
  clean architecture, 190–191
  complexity, 190
  connection to world-wide governments, 279–280
  debugging, 190
  demarcation points, 205
  direct cabling, 606
  documentation, 205–207
  IDF (intermediate distribution frame), 197–203
  inconsistent architecture, 196
  installing jacks, 201–203
  labeling, 205–206
  lack of single administrative group, 216–217
  leading edge versus reliability, 217–218
  lunch-related traffic, 215
  massive, disruptive cleaning, 473
  MDF (main distribution frame), 203–205
  modern computing infrastructures, 739
  monitoring, 214–215
  multiple administrative domains, 219
  naming conventions, 207
  network administrators support, 190
  network devices, 209–211
  OSI (Open Systems Interconnection) model, 188–189
  overlay networks, 212–213
  parameter updates, 57–61
  real-time monitoring, 215
  running fiber, 202
  security measures, 272
  simple host routing, 207–209
  single administrative domain, 216–217
  single set of policies and practices, 216
  solid infrastructure, 287–288
  standards-based protocols, 214
  topologies, 191–197
  tracking software licences, 332
  unsecured, 289
  vendor support, 190
  wiring, 198
Newsletters, 770
NFS, 397
  badcall, 603
  caches, 683
  dependencies outside data centers, 110–111
  mounting problems tools, 397
NFS server, 112
Nine-track tape drives, 649
NIS (Network Information Service) master, 121
NNTP, 398
Nonconstructive criticism, 808
Non-critical server, 74
Nonprofit organizations and SA
(system administrators) team, 747
Nonstandard protocols, 551
Nontechnical interviewing, 891–892
Nontechnical manager
analogy for, 835
basics, 853–863
budgets, 860–862
communication, 837, 857–858
customer requirements, 836
deadlines, 836
five-year vision, 864–866
goals, 836
morale, 855–857
one-year plans, 860
overriding technical decision, 856
priorities, 854–855
professional development, 862–863
rehearsing executive visits, 858–859
requirements tasks, 836–837
resources, 854–855
single point of contact meetings, 866–868
staff meetings, 858–859
supporting team, 857
technical managers and, 835–837
understanding technical staff's work, 868–869
Nonuniform operating system, 46–47
Nonverifier, 379
Non-work-related requests, 814
NTFS, 587
Nuclear power plants, 411

O
Off state, 42
Office location and visibility, 767
Office moves, 6–7
Off-shoring, 518
Off-site backup storage, 644–647
Off-site links, 258
Off-site records-storage service, 645–646
On-call expert, 923
One, some, many technique, 56–57, 120

The One Minute Manager (Blanchard), 815
The One Minute Sales Person
(Johnson), 815
One spooler per building, 573
One-day workshops and training
programs, 796, 862
One-year plans, 860
Online documentation, 206
Open architecture services, 104–107
Open architectures, 96
Open cable management, 158
Open file formats, 104, 106
Open protocols, 96, 104–106
Open source software
 licenses and copying, 331
security-sensitive products, 296
Open standards, 690
Open systems and gateways, 106
OpenDirectory, 237
OpenSSL, 705
Operational requirements services, 100–103
Optimization, 604, 607
Organizational structures
 basics, 727–743
examples, 745
Organizations
 ethics-related policies, 323
security policy issues, 300–314
Organizing from the Inside Out
(Morgenstern), 815
OS-based firewalls, 210–211
OSHA (Occupational Safety and
Health Administration) regulations, 257
OSI (Open Systems Interconnection) model, 188–189
OSPF (Open Shortest Path First), 187
OSs (operating systems)
 add-ons, 43
automated loading, 46–47
automating installation, 32–33,
763–764
caching algorithms, 701
checklists, 32, 53–54
client server configuration, 79–80
OSs (operating systems) (continued)
consistent method of loading, 32–33
degrading slowly, 43
disk-cloning system, 32
inconsistent configuration problems, 33
integrity, 43
known state, 52
less dependent on hardware, 53
life cycle, 41–42
loading, 41, 46–54
loading files, 43
maintaining, 44–65
manually loading, 763
nonuniformity, 46–47
preloaded, 51–53
promoting, 45
RAID 1, 83
reloading from scratch, 52
scripts or programs to bring machine up, 409
second-class-citizens, 684–685
single-function network appliances, 79
upgrading servers, 435–454
vendor loaded, 52
verifying software compatibility, 438–439
web servers, 79
workstations, 41
OTP (one-time password), 278
Outages, 382, 597
Out-of-hours and 24/7 helpdesk coverage, 357–358
Out-of-scope technologies, 350–351
Outsider, 934–935
Outsourcing
centralization, 515–518
colocation (colo) center, 743
printing, 577
remote access service, 658–661
SA (system administrators) teams, 741–743
security, 638, 742
Overhead power bus, 146–147
Overlay networks, 212–213

P
Packages, 673–675, 677–678
services and, 438
source code, 673
Packet routing, 210
Pages, 689
Paging, 530
PAM (pluggable authentication module), 720
Parallel/USB cable connection, 569
PARIS (Programmable Automatic Remote Installation Service), 51
Parking spaces for mobile items, 175–176
Partially automated installation, 49–50
Passive mode, 209
Passwords, 273, 528–529, 705
Patch cables, 161–163, 203
Patch panels, 160–161, 204
Patches, 33, 54, 56–57, 161
PCL, 569
PDA, taking along, 786–787
PDUs (power distribution units), 147–149
power supplies, 86
racks, 151
Peer programming, 447
Peer-to-peer print architecture, 572–573
Peer-to-peer services, 62
Penetration testing, 309
Per group spoolers, 573
Per project verification, 299
Perception, 751–765
Performance
changes in, 116–117
data storage, 604–608
intelligent queuing mechanisms, 118
NAS, 605
optimizing, 604
QoS (quality of service), 118
RAID, 604–605
RAM, 604
remote sites, 118–119
SANs, 606
services, 116–119
spindles, 604
Performance review, 834
Perimeter security, 272
Permanent fixes, 407–409
Permanent lease, 60
Permissions, 678, 710
Personal life, balancing with work, 809–810
Personal problems, 805
Pervasive monitoring, 535
Phone number conversion, 465
Phone-screening candidates, 877
PHP, 691
Physical access, 901
Physical issues and scripted tests, 441
Physical networks, maps of, 205–206
Physical security breaches, 300
Physical topology, 212
Physical visibility, 767
Physical-network conversion, 464
Physics, knowledge of, 402
Pillars approach, 460–461
ping, 397–398
Pipelining algorithms, 607
Pirated software, 330–332
pkginfo package, 438
Plaintext and wikis, 249
Planning
  maintenance windows, 477
  testing and, 416
Platforms, 44–45
  controlled by management or by SA team, 66
  standards, 508–509
Platters, 584–585
Policies, documenting overview, 13
Policy conformance, 319
Policy enforcer, 923–925
Policy navigator, 932
Policy writer, 301, 918
Polling systems, 525
POP (Post Office Protocol) server, 109
POP3, 556
POPI (Protection of Proprietary Information) program, 316
Port 80, 297
Portable serial consoles, 171
portmap traceroute function, 397
Positive behavior, 824
Positive roles, 914–932
Positive visibility, 752–765
POST requests, 691–692
Postgres, 238
Postinstall scripts, 54
Postmaintenance communication, 490–491
Postmaster address, monitoring, 553
Posts, 153–154
PostScript, 569
Potential security incidents, 304
Power
  ATS, 139–140
  available from several sources, 177
  cleaned, 138
  data centers, 136–148
  distributing to racks, 146–148
  emergency lighting, 143
  extra electrical capacity, 144–145
  generators, 139–140
  loss of, 265
  maximum load, 143–144
  overhead power bus, 146–147
  PDUs (power-distribution units), 147–148
  providing sufficient, 35–36
  redundancy, 176–177
  UPS, 138–141
Power cables, separating from data cables, 166
Power supplies, 85–86
PowerUser permissions, 291
The Practice of Programming
  (Kernighan and Pike), 440, 765
Precompiling decisions, 785–787
Preloaded operating systems, 51–53
Premade patch cables, 203
Preparation function, 710
Prewiring racks, 160
Prewiring trade-offs, 166
Price per gigabyte-month, 583
Price per megabyte, 583
print global alias, 98
Print jobs, 572
Print server, 121, 577
Print service
- accounting policy, 568–569
- automatic failover, 577
- basics, 566–567
- central funnel architecture, 572–573
- dedicated clerical support, 578
- documentation, 573–574
- general printer architecture policy, 568
- how to print document, 573–574
- level of centralization, 566–567
- list of printers, 574
- load balancing, 577
- minimizing waste, 575
- monitoring, 574–575
- peer-to-peer print architecture, 572–573
- printer access policy, 570
- printer equipment standard, 569–570
- printer label, 574
- printer naming policy, 571–572
- redundant systems, 577
- system design, 572–573

Print system
- installing new, 54–55
- spoolers, 573

Printer abuse, 579
- Printer access policy, 570
- Printer label, 574
- Printer naming policy, 571–572

Printers
- access to, 570
- canceling print jobs, 570–571
- confidentiality, 567
- consistent tray scheme, 574
- convenience, 567
- cost, 567
- dedicated clerical support, 578
- environmental issues, 575–576
- equipment standard, 569–570
- list of, 574
- maintenance, 568
- monitoring status, 575
- naming, 571–572
- no standards for, 567
- nonbusiness use, 579
- protocols, 569
- recommended configuration, 570
- sharing, 566–567
- special, 567
- supplies, 569
- test print, 575
- toner cartridges, 569

Printing
- architecture policies, 568
- centralization, 566–568
- commodity service, 510
- duplex, 576
- /etc/passwd file, 229
- importance of, 565
- outsourced, 577
- printer abuse, 579
- shredding, 578–579

Priorities
- nontechnical managers, 854–855
- setting, 24–25
- technical manager, 820–821, 843–845

Prioritizing
- problems, 27
- tasks, 781
- trouble tickets, 354

Privacy and monitoring policy, 336–337
- Privacy policies, 337, 544
- private password, 529
- Privileged access, 327–330
- Privileged users, 323
- Privileged-access code of conduct, 327–330
- Privileges and web servers, 710
- Proactive solutions, 76
- Problem preventer, 915–916
- Problem reports, tracking, 366
- Problem statements, 369–372
- Problem-reporting mechanisms, 304
- Problem-reporting procedures, 304
- Problems
  - architectural decisions, 384–385
  - classifying, 368–369
  - educating customers, 384
  - encapsulating test in script or batch file, 372
finding real, 393
fixing, 373–376
fixing cause, no symptom, 393–394
fixing once, 405–413
fixing upstream, 823
flexible solutions, 371
formal decision tree, 368
helping customer save face, 371
identifying, 367–373
Internet routing, 370
knowledge of physics, 402
learning about customer’s, 392–393
more accurate method to reproduce, 378
prioritizing, 27
process of elimination, 394
reproducing, 372–373
short-term solutions, 35
skipping steps, 378–380
solutions, 373–376
successive refinement, 394–395
support groups, 369
systematic about finding cause, 394–395
unreported or not affecting users, 372
verifying, 372–373
verifying repair, 376–378
Problem-solving, 502
Procedures documenting overview, 12–13
Process and documentation, 416
Process of elimination, 394
Processes
  centralization, 505
  change management, 422, 424
  high confidence in completion, 65–66
  recording knowledge about, 413
proclmail, 784, 788
Procrastination, 787
Product finder, 920–921
Product-development group, 312
Production server, 717
Products
  gluing together several, 846
  integrating or customizing, 845–846
  versus protocols, 104–105
  security-sensitive purposes, 295–298
  standardizing on, 509
  volume purchasing deals, 513
Professional code of conduct, 324–326
Professional development, 796–797, 862–863
Professional organizations, 796
Profiles, managing, 720
Program Files directory, 438
Programming Pearls (Bentley), 765
Projects
  design documents for larger, 841
  finishing overview, 14–15
  kick-off meetings, 100
  Promotions, asking for, 812
  Proprietary email software, 106
  Proprietary email system, 107
  Proprietary file formats, 104
  Proprietary protocols, 104
  Prosecution policy, 306
Protocols
  based on TCP, 397–398
  embedding communications into, 297
  limiting on WAN, 191
  open, 104
  versus products, 104–105
  proprietary, 104
  standards-based, 214
  Sun RPC-based, 397
  TCP-based, 398
  vendor-proprietary, 107, 214
Provisioning new services, 360
Proximity badge readers, 135
Public information, 274
Public networks, 61
public password, 529
Punch block, 198
Purchasing, consolidating, 513–515
Push-to-talk features, 488
PUT, 528–529
Q
QA server, 717
QoS (quality of service), 118, 187
QPS (queries per second), 89–90, 694
Quick fixes, 35
Quick requests, 29–30

R
Rack frame, 90
Rack unit (U), 152
Racks
  19-inch racks, 152, 155
  air circulation, 156
  boltless, 153
  cable management, 152, 156–158
  cage nut, 153
  cooling system, 151
  data centers, 150–159
  depth, 155
  with doors, 156
  environment, 159
  extra floor space, 159
  first of each group of holes, 152
  four-post, 153, 154
  height, 154–155
  hole size, 153
  keeping power cables away from
    network cables, 151
  labeling, 160
  mounting servers, 153–154
  NEBS (Network Equipment Building
    System) compliant, 155
  numbering holes, 152–153
  organizing equipment, 151
  overview, 152–153
  patch panel, 160–161
  PDUs (power-distribution units), 151
  posts, 153–154
  prewiring, 160
  rack-mount units, 159
  rails, 152
  server wiring, 163
  shelves, 159
  specific purpose, 151
  strength, 158
  threaded, round holes for bolting
    equipment, 153
  too much prewiring, 163–164
  two-post, 154
  vertical power distribution units, 166
  width, 155
  wiring infrastructure, 151
Rack-unit, 90
Radical print solutions, 374
Radios, 170
RADIUS authentication protocol, 232
RAID (Redundant Array of
  Independent Disks), 87–88, 585–587
  customizing striping, 611–612
  file snapshots, 599
  hardware failure, 83
  hot spare, 587
  levels, 585
  monitoring for disk failures, 597
  not substitute for backup, 598–599
  optimizing usage by applications,
    611–612
  performance, 604–605
  reliability, 597
  triple-mirror configuration, 600
RAID 0, 585–586, 604–605
RAID 1, 83, 585–586, 605
RAID 2, 586
RAID 3, 586, 605
RAID 4, 586, 605
RAID 5, 586, 605
RAID 10, 586–587, 605
RAID mirrors to speed backups, 600
RAIDs 6-9, 586
Rails, 152
Raised floors, 137, 147, 159–160
RAM, 604
Ramanujan, 228
RAS devices, 211
Raw storage, 589–590
RCS, 237, 453
RDF (Resource Description
  Framework) Site Summary, 251
Reactive solutions, 76–77
Reading, 796
README file, 248
“Ready to eat” systems, 503
Real-time availability monitoring,
  215
Real-time monitoring, 523–524, 527–534
acknowledging, 532
active monitoring systems, 532–534
alert policy, 530
alerts, 527, 530–531
availability monitoring, 527
capacity monitoring, 527–528
critical outage, 530–531
error messages, 531
escalation policy, 531–532
escalation procedure, 532
flexibility, 528
handling problems, 539
indicating condition of monitored item, 538
scaling problems, 538
SNMP (Simple Network Monitoring Protocol), 528–529
standard mechanisms, 527
storage requirements, 527
test modules, 528
Reboot test, 427–428
Rebuild process, 42–43
Rebuilding files, 413
Recorder, 369–372
Recording requests, 786
Recruiting, 875–877
Recycling, 575–576
RedHat Linux, 46, 54
Redirect, 715
Redundancy
centralized funnel, 573
clients, 553–554
data centers, 176–177
data integrity, 122
data synchronization, 122
email service, 553–554
full, 86–87
high-availability sites, 496–497
HVAC systems, 176–177
list processing hosts, 553
load sharing, 87
mail relay hosts, 553
maintenance windows, 496
\(n+1\), 86–87
physical-network design, 205
power, 176–177
spoolers, 568
upgrades, 123
Redundant multiple-star topology, 193–194
Redundant power supplies, 85–86
Redundant servers, 89
Redundant site, 268
Reference lists, 256–257
Reflection, 795–796
Refresh period, 467
Registry, 410
Regression testing, 440
Reigning in partner network connections, 279–280
Relational Junction, 702
Reliability
choosing affordable amount, 598
data centers, 110
data storage service, 597–598
e-mail service, 123, 546–547
grouping, 113–115
versus leading-edge networks, 217
NAS servers, 598
RAID, 597
remote access service, 656
security and, 273
servers, 112–115
services, 101, 112–115
software depots, 670
web hosting, 719
web servers, 704
Remote access
aspects not to outsource, 659
authentication database, 659
connecting to Internet, 653
cost analysis and reduction, 663–664
directly connecting computer to network, 653
home office, 662–663
problems lumped together as, 653
reenabling, 491
removing, 901–902
Remote access outsourcing companies, 658–661
Remote access policy, 277
Remote access service, 653
acceptable use, 656
always-on connections, 656
from another company’s site, 656
authentication, 661
basics, 654–662
centralization, 658
common customers, 654
coverage area, 654
customers for trial services, 657
email, 654
encryption, 656
ETR (estimated time to repair), 656
firewalls, 655–656
helpdesk staff, 657
high-speed access, 656
home use of, 654–655
low-cost, convenient solution, 654–656
new technologies, 664–665
outsourcing, 658–661
perimeter security, 661–662
policy, 656
reliability, 656
requirements, 654–656
responsibilities for access, 656
security and, 655–656
security policies, 656
service levels, 656–658
short-duration connections, 654
in trial phase, 657
Remote console access, 80–83, 200
Remote email access, 557
Remote Installation Service, 46
Remote power management, 147
Remote sites, 118–119
Removable media, 337
Removing roadblocks, 821–823
Rensselaer Polytechnic Institute, 238
Repair person, 914–915
Repeatability, 32
Repeaters, 488
Replacing services overview, 4–5
Replication, 676
Reporting problems, 359–360
Reproducer role, 372–373
Reproducing problems, 372–373
Reputation as can-do person, 760–761
Request management, 28–29
Request Tracker, 29
Requesting new services, 359–360
Requests, 759, 786
Request-tracking software, 354–356
Request-tracking system, 246
Resources
security team, 300–303
servers, 125
Respecting employees, 838–841
Response policy, 305–306
Restores, 619
accidental file deletion, 621–623
archival backups, 624–625
complete restores, 625
data-recovery SLA and policy, 626
disk failure, 623
documentation, 638
fire drills for, 644
individual file, 624
process issues, 637–638
reasons for, 621–624
security implications, 637–638
self-service, 622–623
setting expectations with customers, 637
speed of, 634
tape inventory, 642–643
technology changes, 648–649
time and capacity planning, 633–635
training system administrators, 638
types, 624–625, 627
Retention policy of email, 559–560
Reuse policy, 235
Revenue-generating Internet presence, 742
Revision control and automation, 416
Revision Control System, 425
Revision history, 424–426
Rewards, 824–825
Rewiring building, 202
RFCs, static assignment, 60–61
Ring topologies, 192–193, 196
Rioting-Mob Technique, 459–460
RIP, RIPv2 (Routing Information Protocol), 207
Risk analysis, 262–263
Risk manager, 303
Risks, 415, 417–418
Risk-taking, 262
RJ-45 connectors, 198
Roaming profiles, 78
Robolnst, 46, 54
Role accounts, 290–291, 293
Rolling upgrade, 123
Root access, 327
Root account, 291
Round-robin DNS name server records, 699–700
Routers, 86, 187, 207, 209–211
Routine updates, 420, 422
Routing, 208
Routing hosts, 123
Routing protocol, 209
Routing protocols, 187
RPMs, 54
RSS feed, 692
RT wiki, 253
RTT (round-trip time), 101

S
SA (system administration) team
attitude of, 756–758
becoming system advocate, 760–765
blatant disrespect for people, 756
building self-confidence, 22
business applications support team, 312
business partners relationship, 757
centralized models, 732–733
centralizing, 507
clear directions, 842
clerk role, 761
coaching, 831–833
communicating change to, 418–419
consultants, 743–745
contractors, 743–745
customer support, 735–736, 739–741
customers, 756
customer-to-SA ratio, 729–730
decentralized models, 732–733
deployment of new services, 736
designing new service architectures, 736
Dilbert check, 879
distributed network support, 738
division of labor, 759
e-commerce sites, 746–747
eliminating redundancy, 732
fixing quick requests, 759
funding models, 730–733
goals, 830
helpdesk, 741
helping customer help himself, 756
high support costs, 729
hiring considerations, 878–882
improving follow-through, 22–23
infrastructure teams, 737–739
in-person orientation, 755–756
large company, 746
long-term solution, 822–823
maintenance, 735–736
maintenance contracts, 731
management chain’s influence, 733–735
manager keeping track of, 825–827
medium-sized company, 745–746
morale, 821
more customized service, 732
nonprofit organizations, 747
opportunities for growth on, 881
outsourcing, 741–743
overstaffing, 728
perception of, 756–758
personality clashes, 878–879
priorities and customer expectations, 758–760
promoting from within, 737
reduced duplication of services, 732
requests against policy, 756
resentment toward customers, 757
restricting size and growth, 730
rewarding, 824–825
roles, 735–737, 934–937
saying no when appropriate, 756
security as cooperative effort, 311–312
SA (system administration) team (continued)

- senior generalists, 736
- short-term solution, 822–823
- sizing, 728–730
- skill selection, 735–737
- small company, 745
- specializing, 745–746
- standardization, 732
- strengthening, 849
- strengths and weaknesses, 732
- structure, 727–743
- system clerk, 760
- town hall meeting, 768–770
- understaffing, 731
- universities, 747
- users, 756
- venting about customers, 757–758
- viewed as cost center, 730–731
- vision for, 830–831
- written policies to guide, 820

Safe-delete programs, 383

SAGE (System Administrators’ Guild), 72, 324, 399

SANs (storage area networks), 180, 588
- AoE (ATA over Ethernet), 606
- backups, 600–601
- caveats, 603–604
- cluster file systems, 588
- components from different vendors, 603
- configuration of underlying networks, 610
- generating snapshots of LUNs, 601
- moving backup traffic off primary network, 635
- moving file traffic off main network, 606
- performance, 606
- reducing isolated storage, 588
- tape backup units, 588

SANS Computer Security Incident Handling: Step-by-Step booklet, 307

Sarbanes-Oxley Act, 323

Sarbanes-Oxley compliance, 746

Sarbanes-Oxley governing-practice regulations, 257

SAs (system administrators)
- assumer, 379
- attire, 753
- basics, 364–380
- boundaries between areas of responsibility, 285–286
- career crisis, 834
- career goals, 812–813
- career paths, 833–834
- Carte Blanche Night, 445
- checklists, 821
- closer, 380
- craft worker, 376
- deexecutioner, 379
- dress rehearsal for paper presentations, 768
- firing, 899–908
- fixing problems, 533
- flexibility, 371
- good first impression, 752–755
- greeting customer, 364–367
- helpdesk, 736–737
- high-quality handoffs, 381
- high-stress work life, 855
- hiring, 20, 871–896
- hit-and-run sysadmin, 379
- holistic improvement, 381
- increased customer familiarity, 381
- informed consent, 324
- interaction with customer at appointment, 753
- interesting projects, 744, 824
- involved in hiring process, 760
- isolation, 27
- job description, 872–874
- law enforcement and, 332–335
- learning from mistakes, 832
- lunch with customers, 773
- management expectations, 26
- management meetings, 766–767
- meetings with single point of contact, 866–868
- metrics, 384
- misdelegator, 379
model-based training, 380–381
monitoring system, 534
morale, 855–857
negative roles, 932–934
new hire’s first day, 754–755
nonverifier, 379
ogre, 378
outsourcing remote access, 658–659
PC delivery, 755
physical visibility, 767
positive roles, 914–932
positive visibility, 755
problem identification, 367–373
professional development, 862–863
promoting to management, 797
reproducer role, 372–373
selling security to, 314
setting priorities for, 734
shared responsibilities for machines, 285–286
special announcements for major outages, 382
standards, 66
stereotypes, 378–380
system status web page, 765–766
technical development, 833
trend analysis, 382–384
understanding customers expectations, 99
visibility paradox, 765
working alone, 380
wrong fixer, 379
yelling at people, 753–754
SAS-70 (Statement of Auditing Standards No. 70), 178

Scaling
CGI programs, 702
challenges, 702–703
choosing method, 701–702
data flow analysis, 124–125
database usage, 702
email service, 554–556
gradual, 701–702
horizontal, 699–700
IMAP4, 556
importance of, 703
load balancers, 702
POP3, 556
problems and monitoring, 537–539
pulling data from several sources, 702
services, 100
subsystems and common resources, 702
vertical, 699, 700–701
web services, 699–703
SCCS (Source Code Control System), 237

Scheduling
change management, 419–422
change-freeze times, 422, 423
maintenance windows, 475–476, 495
major updates, 420
no changes on Friday, 421
routine update, 420
sensitive updates, 420, 422
SCM (Software Configuration Management), 67
Scope of responsibility, 350
Scope of support, 348–351
Scope of work policy, 821
Scope policy, 231–233
Scope-of-support policy, 348–350
script command, 245
Scripting languages, 710
Scripts
to bring machine up, 409
helpdesks, 352
OK or FAIL message, 440
outputting commands to do task, 763
sharing, 411
software verification tests, 439–442
Search engines web repository, 250–251
Search facility, 250–251
SEC (Securities and Exchange Commission), 329–330
Second tier of support, 352–353
Second-best situation, 798
Second-class-citizens, 684–685
Secure connections, 704–706
Securing hosts before going live, 290
Security, 271
  applications, 709–710
  asking right questions, 273–275
  authentication, 290–293
  authorization, 290–293
  authorization matrix, 293–295
  automating data access, 710
  bulk emails, 338
  certificates, 704–706
  companies, 314
  competitive advantage, 314
  contacts, 316–317
  containment, 63–64
  cooperative effort, 311–312
  data, 271–272
  data centers, 134–136
  defeating or finding way around, 285
  directory traversal, 707–708
  effectively selling, 313–314
  email filtering, 284
  email service, 544, 556–557
  enabling people to work effectively, 285–286
  external sites, 717
  features consistently enabled, 33
  firewalls, 284
  form-field corruption, 708
  hosts determining hostname, 62
  IDF (intermediate distribution frame), 200
  implications of restores, 637–638
  information, 313–314
  information protection, 274
  internal auditing, 298–300
  internal web services, 704
  Internet, 271
  known, standard configurations, 287
  limiting potential damage, 709
  logging, 710
  logs, 299
  malware protection, 284
  mean time to attack, 289
  meeting business needs, 285–287
  metrics, 317
  monitoring, 525
  names, 228
  off-site backup storage, 646
  only as good as weakest link, 283
  outsourcing, 742
  passwords, 273
  permissions and privileges, 710
  pervasive, 315–316
  physical breaches, 300
  process for someone leaving company, 287
  projects verification, 299
  protecting important data, 275–276
  protecting service availability, 274–275
  protecting web server application, 706–707
  protecting web server content, 707–708
  raising awareness, 316
  reliability, 273
  remote access outsourcing
    companies, 660
  remote access service, 655–656
  remote console, 82–83
  remote email access, 557
  secure connections, 704–706
  secure perimeter, 661–662
  security-sensitive products, 296
  selecting right products and vendors, 295–298
  servers, 97
  shared development environment, 286–287
  single administrative domain, 217
  sites without, 284–285
  SNMP problems, 529
  solid infrastructure, 287–288
  spotlighting bad behavior, 291
  SQL injection, 708
  staff disagreeing with management decisions, 281
  state of, 284
  statically assigned IP addresses, 61
  technologies, 316–317
  theft of resources, 275
  through obscurity, 296
  UNIX, 271
  validating input, 709
AUP (acceptable-use policy), 276–277
basics, 272–277
better technology means less, 278
communication policy, 307
cooperation from other departments, 276
defense in depth, 272
disconnection policy, 306–307
documenting, 276–283
external audits, 308–309
HHA (handheld authenticators), 278
lack hampering security team, 278–279
log-retention policy, 277
management and organizational issues, 300–314
monitoring and privacy policy, 277
network connectivity policy, 277
outside auditing company, 300
partner network connections, 279–280
perimeter security, 272
remote access policy, 277
response policy, 305–306
technical staff, 283–300
without management support, 281–282
Security policy council, 282–283
Security professionals, 316
Security programs
e-commerce sites, 319–320
large companies, 319
medium-size company, 318–319
organization profiles, 317–321
small company, 318
universities, 320–321
Security Symposium, 797
Security system, 273
Security team
advisories, 289
auditor, 302
benchmarking company, 301
business applications support team, 312
contacts in industry, 300–301
cross-functional teams, 310–313
effectively selling security, 313–314
field offices, 312–313
full-disclosure mailing lists, 289
implementer, 302
incident response, 303–307
incident-response team, 303
independent feedback, 308
intercompany security focus groups, 301
involved at outset, 311
knowing latest attacks, 289
legal department, 310
points of contact, 304
policy writer, 301
product-development group, 312
reasonable staffing levels, 300
resources, 300–303
risk manager, 303
security architect, 301–302
security bulletins, 289
security operations staff, 302
variety of skills, 301–303
Security-awareness program, 318
Security-sensitive logs, 299
Security-sensitive products, 295–298
Self-help books, 815
Self-help desk, 255
Self-help systems, 345
Self-service restores, 622–623
Selling position, 892–893
Sendmail, 545
Senior generalists, 736
Senior management, 308, 313
Sensitive updates, 420, 422
SEPP, 672
Sequential names, 227
Sequential reads, 586
Serial console concentrators, 80–81
Serial console servers, 486
Serial consoles, 81
Serial port-based devices, 80
Serial ports, monitoring, 81
Server appliances, 84–85
Server computers, 73
Server upgrades, 448–449
Server virtualization, 506–507
Servers
access to, 97
buying hardware for, 69–71
colocation centers, 71
connected to multiple networks, 110
controlled introduction, 74–75
cooling and ventilation, 71
cost, 73, 90
cost of hardware, 72–74
CPUs, 70
data center, 78–79
data integrity, 78
disposable, 91
downtime, 74
extensibility, 70
front-mountable, 153
full redundancy, 122
full versus N + 1 redundancy, 86–87
growing number of customers, 117
hardware, 69
heterogeneous environments, 72
high availability options, 71
high availability requirements, 135
high performance throughput, 70
homogeneous environments, 72
hot-swap components, 87–88
hot-swap hardware, 74
I/O, 70
KVM switches, 80–81
lack of similar configurations on, 506
large groups of similar, 74
listing contents of directories, 248
load balancers, 89
load sharing, 87
locating in data center, 110
location of, 78–79
LUN (logical unit number), 588
maintenance contracts, 71, 74–78
management options, 71
MIL-SPEC requirements, 72
mirroring boot disks, 83
mounting in racks, 153–154
MTTR (mean time to repair), 73
multiple inexpensive, 89–92
name conflicts, 226
no side-access needs, 71
operating system configuration, 79–80
OS configuration, 79–80
peak utilization, 117
rack mounting, 78–79
rack-mountable, 70–71
redundant hardware, 74
redundant power supplies, 85–86
reliability, 110, 112–115
reliability and service ability, 84–89
remote console access, 80–83
required software, 79
resources, 125
restricting direct login access, 111
security, 97
separate networks for administrative functions, 89
server appliances, 84–85
services, 95, 118
simplicity, 97
spare parts, 74–78
terminals, 80
upgrade options, 70
upgrading, 435–454
UPS (uninterruptible power supply), 35
usage patterns, 125
vendors, 72
versatility, 70
wiring, 163
Service
conversions, 457
protection, 614
Service access, 901–904
Service checklist, 436–438, 453
Service conversions
adoption period, 464
avoiding, 468–469
back-out plan, 465–466
basics, 458
communication, 461–462
dividing into tasks, 460–461
doing it all at once, 463–465
failure, 466
flash-cuts, 463–465
future directions for product, 468
gradual, 463
instant rollback, 467–468
invisible change, 457
layers versus pillars, 460–461
minimizing intrusiveness, 458–460
old and new services available
simultaneously, 464
physical-network conversion, 464
Rioting-Mob Technique, 459–460
simultaneously for everyone,
464–465
slowly rolling out, 463
solid infrastructure in place, 458
test group, 463
training, 462
vendor support, 470
without service interruption, 459
Services, 95
adding and removing at same time,
450
additional requirements, 96
administrative interface, 100
adversely affecting, 112
associated with service-based name,
121
authentication and authorization
service, 97
average size of data loaded, 125
bad first impression, 117
basic requirements, 95
basics, 96–120
budget, 103
business-specific, 95
capacity planning, 119
cascading failures, 97
catch-22 dependencies, 111
centralization, 98, 116, 505, 508
client systems, 97
closed, 104
complexity, 107–108
consolidating, 506
critical, 122
customer requirements, 96, 98–100
customers relying on, 438
data storage, 596–604
dataflow analysis for scaling,
124–125
dedicated machines, 120–122
default responsible entity, 532
depending on few components, 113
desired features, 101
disabling, 450
equipment, 96, 110–111
escalation procedure, 532
failover system, 122
features wanted in, 98–99
first impressions, 120
five-year vision, 864–866
full redundancy, 122–123
function-based names, 109
fundamental, 95
generic, 95
hard outages, 114
hardware and software for, 108–109
high level of availability, 110
independent, 98, 115
infrastructure, 97
integrated into helpdesk process, 116
kick-off meetings, 100
latency, 103
listing, 453
lists of critical servers, 34
load testing, 117
machine independence, 109
machines and software part of, 97
mashup applications, 721–722
Microsoft Windows, 410
modeling transactions, 124
Services (continued)
monitoring, 103, 119
more supportable, 98
moving, 109
network performance issues, 101
network topology, 113–114
no customer requirements, 98
no direct or indirect customers, 438
open architecture, 96, 104–107
open protocols, 96
operational requirements, 100–103
packages and, 438
performance, 96, 116–119
potential economies of scale, 501
protecting availability, 274–275
prototyping phase, 657–658
providing limited availability, 493–494
redundancy, 112
reliability, 96, 97, 101, 112–115
relying on email, 96
relying on network, 96
relying on other services, 96–97
remote sites, 118–119
reorganizing, 501
restricted access, 111–112
restricting direct login access, 111
rolled out to customers, 120
scaling, 100
server-class machines, 96
servers, 118
simple text-based protocols, 441
simplicity, 107–108, 113
single or multiple servers, 115
single points of failure, 113
SLA (service-level agreement), 99
soft outages, 114
splitting, 121–122
stand-alone machines providing, 96
standards, 116
talking directly to clients, 62
testing, 469
tied to global alias, 98
tied to IP addresses, 109, 121
transaction based, 124
trouble tickets, 103
ty ing to machine, 98
upgrade path, 100–101
usability trials, 99
vendor relations, 108
virtual address, 109
Web-based, 469
Services Control Panel, 410
Shared accounts, 290–292
Shared development environment, 286–287
Shared directory, 248
Shared role accounts, 293
Shared voicemail, 292–293
Shoe-shining effect, 634
Short-term solution, 822–823
Shredding, 578–579
Shutdown sequence, 485
Shutdown/boot sequence, 483–485
SIDs (Windows), 223
Simple host routing, 207–209
Single, global namespaces, 232–233
Single administrative domain, 216–217
Single authentication database, 905
Single points of failure, 510, 512
Single-function network appliances, 79
Single-homed hosts, 208
Sites
assessing overview, 7–8
used to launch new attacks, 307
virtual connections between, 212
without security, 284–285
Skill level, 874–875
SLAs (service-level agreements), 32
backup and restore system, 621
backups, 625–626
monitoring conformance, 525
remote access outsourcing
companies, 660
services, 99
web service, 694
Slow bureaucrats, 789–790
Small company
SA (system administrators) team, 745
security program, 318
Smart pipelining algorithm, 607
SMB (Server Message Block) print
protocol, 569
SME (subject matter expert), 374, 375
SMS and automating software updates, 54
SMTP (Simple Mail Transfer Protocol), 104, 189, 398, 548
smtp global alias, 98
SMTP server, 109
Snake Oil Warning Signs: Encryption Software to Avoid (Curtin), 316
Snake Oil Warning Signs: Encryption Software to Avoid (Curtin), 559
Snapshots of filesystems, 622
SNMP (Simple Network Monitoring Protocol), 528–529
SNMP packets, 529
SNMPv2, 526
SNMPv2 polling, 527
SNMPv2 traps, 527
Social engineering, 303, 308–309, 333–334
Social engineers, 334
SOCKS relay, 121
Soft emotions, 791–792
Soft outages, 114
Software
collection policy, 671–672
installation test suite, 440
labeling ports, 168
management approval for downloading, 331
no longer supported, 439
old and new versions on same machine, 452
regression testing, 440
reuse policy, 235
selecting for support depot, 672
single place for customers to look for, 669
tracking licenses, 672
upgrade available but works only on new OS, 439
upgrading to release supported on both OSs, 439
verification tests, 439–442
verifying compatibility, 438–439
Software depots, 667
bug fixes, 670
bugs and debugging, 671
building and installing packages, 671
commercial software, 684
contributing software policy, 671–672
customer wants from, 670
deletion policy, 671–672
different configurations for different hosts, 682
documenting local procedure for injecting new software packages, 672–673
justification for, 669–670
librarians, 669
local replication, 683
managing UNIX symbolic links, 672
new versions of package, 670
OSs supported, 671
packages maintained by particular person, 671
reliability requirements, 670
requests for software, 669–670, 672
same software on all hosts, 670
scope of distribution, 672
second-class-citizens, 684–685
Solaris, 667–668
technical expectations, 670
tracking licenses, 672
UNIX, 668, 673–679
upgrades, 671
Windows, 668, 679–682
Software Distributor (SD-UX), 54
Software licenses, 332
Software piracy, 330–332
Software updates, 54–57
Solaris
automating software updates, 54
JumpStart, 46, 48, 65, 406
software depot, 667–668
solution designer, 921
Solutions, 373–376
building from scratch, 846–847
executing, 375–376
expensive, 374
proposals, 374
radical print, 374
radical print solutions, 374
selecting, 374–375
Solutions database, 246
SONET (synchronous optical network), 188
Source Code Control System, 425
SOURCENAME script, 673–674
SourceSafe, 425
Spam, 703
  blocking, 550
  email service, 549–550
Spammers, 338
Spare parts, 74–78
  cross-shipped, 77
  valuable, 175
Spare-parts kit, 77–78
Spare parts, organizing, 174
Special applications, 53
Specialization and centralization, 508
Special-purpose formats, 692
Special-purpose machines, 234
Spindles, 584–585, 604
Splitting
  center-of-the-universe host, 122
Splitting central machine, 121
Splitting services, 121–122
Spoolers
  monitoring, 574–575
  print system, 573
  redundancy, 568
Spot coolers, 146
Spreadsheets
  service checklist, 436–438
Spyware, 284
SQL injection, 708
SQL lookups, 720
SQL (Structured Query Language) request, 103
SSH package, 80
SSL (Secure Sockets Layer)
  cryptographic certificates, 705
Staff
  defining processes for, 352
Staff meetings
  knowledge transfer, 859
  nontechnical managers, 858–859
Staffing helpdesks, 347
Stakeholders, 100, 429
  hardware standards, 595
  signing off on each change, 429
Stalled processes
  being a good listener, 822
  being good listener, 822
  communication, 822
  restarting, 821–823
Standard configuration
  customers involved in, 66
Standard configurations
  multiple, 66–67
Standard protocols, 107, 468
Standardization
  data storage, 594–596
Standardizing on certain phrases, 793–794
Standardizing on products, 509
Standards-based protocols, 214
Star topology, 191–192, 196
  multiple stars variant, 192
  single-point-of-failure problem, 191–192
Start-up scripts, 409
Static documents, 694–695
Static files, 701
Static leases
  hosts, 62
Static web server, 694–695
Static web sites
  document root, 695
  status, 397
Status messages, 766
Stop-gap measures
  preventing from becoming permanent solutions, 50
Storage
  documentation, 247–248
Storage consolidation, 506
Storage devices
  confusing speed onf, 610
  other ways of networking, 606
Storage servers
  allocating on group-by-group basis, 588
  serving many groups, 589
Storage SLA, 596–597
- availability, 596
- latency, 596
- response time, 596

Storage standards, 594–596

Storage subsystems
- discarding, 595

Storage-needs assessment, 590–591

Streaming, 692

Streaming video
- latency, 103

Streaming-media, 696–697

Stress
- avoiding, 25

Strictly confidential information, 274

Striping, 585, 586
- customizing, 611–612

StudlyCaps, 249

SubVersion, 248, 425

Subzones, 233

Successive refinement, 394–395

sudo, 383

sudo command, 714

sudo program, 329

SUID (set user ID) programs, 383

Summary statements, 794–795

Sun Microsystems, 799

Sun OS 5.x
- JumpStart, 51

Sun RPC-based protocols, 397

SunOS 4.x
- PARIS (Programmable Automatic Remote Installation Service), 51
- unable to automate, 51

Supercomputers, 130

Superuser account
- access from unknown machine, 293

Supplies
- organizing, 174

Support
- customer solutions, 847
- defining scope of, 348–351
- first tier of, 352–353
- how long should average request take to complete, 349
- second tier of, 352–353
- what is being supported, 348
- when provided, 348–349
- who will be supported, 348

Support groups
- problems, 369

Support structure, 808

/sw/contrib directory, 678

/sw/default/bin directory, 674

Switches, 187, 209

swlist package, 438

Symbolic links
- managing, 675

Symptoms
- fixing, 393–394
- fixing without fixing root cause, 412

System
- balancing stress on, 591–592
- end-to-end understanding, 400–402
- increasing total reliability, 20

System Administrator’s Code of Ethics, 324–3267

System administration, 364
- accountability for actions, 29
- as cost center, 734
- tips for improving, 28–36

System Administrator team
- defining scope of responsibility policy, 31
- emergencies, 29
- handling day-to-day interruptions, 29–30
- specialization, 29

System Administrator team member tools, 11–12

System advocates, 760–765

System boot scripts, 427

System clerk, 760

system clerk, 918–919

System configuration files, 424–426

System file changes, 906

System files, 428

System Management Service, 55–56

System software, updating, 54–57

System status web page, 765–766
Systems
diversity in, 512
documenting overview, 12–13
polling, 525
speeding up overview, 16
Systems administrators
coping with big influx, 17
keeping happy overview, 16
Systems administrators team, 18

Tape backup units, 588
Tape drives, 642
nine-track, 649
shoe-shining effect, 634
speeds, 634
Tape inventory, 642–643
tar files, 673
Tasks
automating, 763–764
checklists of, 34
daily, 785
domino effect, 759
intrusive, 460
layers approach, 460–461
monitoring, 524
not intrusive, 460
order performed, 30
outsourcing, 515
pillars approach, 460–461
prioritizing, 30, 781
TCP, 527, 700
TCP connections, 526
TCP-based protocols, 397–398, 398
tcpdump, 395
TCP/IP, 191
TCP/IP (Transmission Control Protocol/Internet Protocol), 187
TCP/IP Illustrated, Volume 1 (Stevens), 398
TCP/IP networking, 188–189
TDD (Test-Driven Development), 442
Tech rehearsal, 452
Technical development, 833
technical interviewing, 886–890
Technical lead, 797

Technical library or scrapbook, 257–258
Technical manager
as bad guy, 828
buy-versus-build decision, 845–848
clear directions, 842–843
coaching, 831–833
decisions, 843–848
decisions that appear contrary to direction, 830–831
employees, 838–843
informing SAs of important events, 840
involved with staff and projects, 841
listening to employees, 840–841
micromanaging, 841
positive about abilities and direction, 841–842
priorities, 843–845
recognition for your accomplishments, 850
respecting employees, 838–841
responsibilities, 843
role model, 838
roles, 843
satisfied in role of, 850
selling department to senior management, 849–850
strengthening SA team, 849
vision leader, 830–831
Technical managers
automated reports, 826
basics, 819–848
blame for failures, 827
brainstorming solutions, 822–823
budgets, 834–835
bureaucratic tasks, 822
career paths, 833–834
communicating priorities, 820–821
contract negotiations and bureaucratic tasks, 827–828
enforcing company policy, 828–829
keeping track of team, 825–827
knowledgeable about new technology, 835
meetings with staff, 825–826
nontechnical managers and, 835–837
Index 1003

pessimistic estimates, 836
recognizing and rewarding successes, 827
removing roadblocks, 821–823
reports and, 825
responsibilities, 820–835
rewards, 824–825
SLAs, 820
soft issues, 822
structure to achieve goals, 821
supporting role for team, 827–830
team morale, 821
technical development, 833
tracking group metrics, 827
written policies to guide SA team, 820–821
Technical staff
budgets, 860–862
security policies, 283–300
technocrat, 927–928
Technologies
security, 316–317
Technology platforms, 697
technology staller, 932
tee command, 395
Telecommunications industry
high-reliability data centers, 177–178
TELNET, 80, 398
Templates
announcing upgrade to customers, 445–446
database-driven web sites, 695
DHCP systems, 58–60
Temporary fix, 412
Temporary fixes
avoiding, 407–409
TERM variable, 406
Terminal
capture-to-file feature, 245
Terminal servers, 171
Terminals, 80
termination checklist, 900–901
Test plan, 417
Test print, 575
Testing
alert system, 531
comprehensive system, 489–490
finding problems, 490
server upgrade, 447
Tests integrated into real-time monitoring system, 451
TFTP (Trivial File Transfer Protocol) server, 59
Theft of intellectual property, 267
Theft of resources, 275
Thematic names, 225, 227
Third-party spying
wireless communication, 530
Third-party web hosting, 718–721
Ticket system
knowledge base flag, 246
Tickets
email creation, 408
Time management, 780–790
daily planning, 782–783
daily tasks, 785
difficulty of, 780–781
finding free time, 788
goal setting, 781–782
handling paper once, 783–784
human time wasters, 789
interruptions, 780–781
managers, 813
precompiling decisions, 785–787
slow bureaucrats, 789–790
staying focused, 785
training, 790
Time Management for System Administrators (Limoncelli), 815
Time saving policies
defining emergencies, 31
defining scope of SA team’s responsibility policy, 31
how people get help policy, 31
Time server, 121
Time-drain
fixing biggest, 34–35
Timeouts
data storage, 610
Time-saving policies, 30–32
written, 31
timing
hiring SAs (system administrators), 877–878
Index

Tivoli, 367
TLS (Transport Layer Security), 704
/tmp directory, 56
Token-card authentication server, 121
Tom’s dream data center, 179–182
Tool chain, 685
Tools
    better for debugging, 399–400
    buzzword-compliant, 399
    centralizing, 116
    characteristics of good, 397
    debugging, 395–398
    ensuring return, 12
    evaluating, 399
    evaluation, 400
    formal training on, 400
    knowing why it draws conclusion, 396–397
    NFS mounting tools, 397
    System Administrator team member, 11–12
Tools and supplies
    data centers, 173–175
Topologies, 191–197
    chaos topology, 195
    flat network topology, 197
    functional group-based topology, 197
    location-based topology, 197
    logical network topology, 195–197
    multiple-star topology, 192
    multistar topology, 196
    redundant multiple-star topology, 193–194
    ring topologies, 192–193, 196
    star topology, 191–192, 196
Town hall meetings, 768–770
    customers, 768–770
    dress rehearsal for paper presentations, 768
    feedback from customers, 769
    introductions, 769
    meeting review, 770
    planning, 768
    presentations, 768
    question-and-answer sessions, 768
    review, 769
    show and tell, 769–770
    welcome, 768
Trac wiki, 253
traceroute, 397, 398
Tracking changes, 319
Tracking problem reports, 366
Tracks, 584
Training
    customers, 462
    service conversions, 462
Transactions
    modeling, 124
    successfully completing, 537
Transparent failover, 553–554
Traps
    SNMP (Simple Network Monitoring Protocol), 528
Trend analysis
    SAs (System administrators), 382–384
Trending historical data, 493
Triple-mirror configuration, 600
Trojan horse, 671
Trouble reports
    enlightened attitude toward, 758
Trouble tickets
    enlightened attitude toward, 758
    prioritizing, 354
Trouble-ticket system, 28–29
    documentation, 246
Trouble-tracking software, 366
Turning as debugging, 399
Two-post posts, 153
Two-post racks, 154

U
UCE (unsolicited commercial email), 549–550
UID
    all-accounts usage, 234
    UID ranges, 234
UIDs (UNIX), 223
Universities
    acceptable-use policy, 320
    codes of conduct, 327
constraints, 476
monitoring and privacy policy, 321
no budget for centralized services, 747–748
SA (system administrators) team, 747
security programs, 320–321
staffing helpdesks, 347
UNIX
add-on packages for, 452–453
automounter, 231
boot-time scripts, 438
calendar command, 419
at cmd, 65
code control systems, 425
crontab files, 438
customized version, 52
diff command, 377, 440
/etc/ethers file, 59
/etc/hosts file, 59–60
/etc/passwd file, 578
history command, 245
level 0 backup, 620
level 1 backup, 620
listing TCP/IP and UDP/IP ports, 438
login IDs, 225
maintaining revision history, 425–426
make command, 236
reviewing installed software, 438
root account, 291
script command, 245
security, 271
set of UIDs, 223
software depot, 668
strict permissions on directories, 43
sudo command, 714
SUID (set user ID) programs, 383
syncing write buffers to disk before halting system, 608
system bot scripts modified by hand, 427
tee command, 395
tools, 667
/usr/local/bin, 667
/var/log directory, 710
Web server Apache, 452
wrapper scripts, 671
UNIX Backup and Recovery (Preston), 620
UNIX desktops
configured email servers, 547
UNIX kernels, 396
UNIX printers
names, 571–572
UNIX servers
later users for tests, 442
UNIX shells
deleting files, 410–411
UNIX software
installation, 668
UNIX software depot
archiving installation media, 678
area where customers can install software, 678
automating tasks, 677
automounter map, 675–677
commercial software, 684
control over who can add packages, 678
defining standard way of specifying OSs, 677
deleting packages, 677
/home/src directory, 673
managing disk space, 677–678
managing symbolic links and automounter maps, 676–677
master file, 677
network of hosts, 675–677
NFS access, 681
obsolete packages, 676
packages, 673
policies to support older OSs, 676
programs in package, 675
reliability requirements, 676
replication, 676
SOURCENAME script, 673–674
/sw/contrib directory, 678
/sw/default/bin directory, 674
symbolic links, 674–675
wrappers, 679
UNIX software depots
   different configurations for different
   hosts, 682
   local replication, 683
   NFS caches, 683
UNIX systems
   NFS, 110–111
UNIX system
   /etc/passwd file, 229
   /etc/shadow file, 229
   login IDs, 229
   /var/adm/CHANGES file, 451
UNIX systems
   assembly-line approach to
   processing, 395
   configuring to send email from
   command line, 408
   crontabs, 78
   debugging, 396
   distributing printcap information, 572
   mail-processing utilities, 784
   Network Information Service, 232
   no root access for user, 78
   simple host routing, 207–208
   sudo program, 329
   tcpdump, 395
   /var directory, 78
UNIX workstations, 130
UNIX/Linux
   filesystem, 587
Unknown state, 42
Unproductive workplace, 806
Unrealistic promises, 503–504
unrequested solution person, 922
Unsafe workplace, 806
Unsecured networks, 289
Updates
   absolute cutoff conditions, 418
   authentication DNS, 63
   back-out plan, 418
   communication plan, 57
   differences from installations,
   55–56
   distributed to all hosts, 57
   dual-boot, 56
   host already in use, 55
   host in usable state, 55
   host not connected, 56
   known state, 55
   lease times aiding in propagating, 64–65
   live users, 55–56
   major, 420, 422
   network parameters, 57–61
   performing on native network of
   host, 55
   physical access not required, 55
   routine, 420, 422
   security-sensitive products, 297
   sensitive, 420–421, 422
   system software and applications,
   54–57
Updating applications, 54–57
Updating system software, 54–57
Upgrades
   advanced planning reducing need,
   468
   automating, 33
   redundancy, 123
Upgrading
   application servers, 211
   clones, 443
   critical DNS server, 453–454
Upgrading servers
   adding and removing services at
   same time, 450
   announcing upgrade to customers,
   445–446
   basics, 435–449
   customer dependency check, 437
   dress rehearsal, 451–452
   exaggerating time estimates, 444
   executing tests, 446
   fresh installs, 450–451
   installing of old and new versions on
   same machine, 452
   length of time, 444
   locking out customers, 446–447
   logging system changes, 451
   minimal changes from base,
   452–453
   multiple system administrators,
   447
review meeting with key representatives, 437
selecting maintenance window, 443–445
service checklist, 436–438
tech rehearsal, 452
testing your work, 447
tests integrated into real-time monitoring system, 451
verification tests, 439–442
verifying software compatibility, 438–439
when, 444
writing back-out plan, 443
UPS (uninterruptible power supply), 35, 138–141, 265
cooling, 139
environmental requirements, 140–141
failure, 177
lasting longer than hour, 139
maintenance, 140–141
notifying staff in case of failure or other problems, 138
power outages, 138
switch to bypass, 140
trickle-charge batteries, 141
Upward delegation, 813–814
URL (uniform resource locator), 690
changing, 715
inconsistent, 715
messy, 715
URL namespace planning, 715
Usability
security-sensitive products, 296–297
Usable storage, 589–590
USENIX, 399, 848
USENIX (Advanced Computing Systems Association), 796
USENIX Annual Technical Conference, 796–797
USENIX LISA conference, 562
User base
high attrition rate, 18
Users, 756
balance between full access and restricting, 43
ethics-related policies, 323
USS (user code of conduct), 326
Utilization data, 524
V
Variables
SNMP (Simple Network Monitoring Protocol), 528
VAX/VMS operating system, 622
vendor liaison, 928–929
Vendor loaded operating systems, 52
Vendor relations
services, 108
Vendor support networks, 190
Vendor-proprietary protocols, 107, 214
Vendors
business computers, 70–72
configurations tuned for particular applications, 108
home computers, 70–72
network, 213–214
product lines computers, 70–72
proprietary protocols, 104
RMA (returned merchandise authorization), 77
security bulletins, 289
security-sensitive purposes, 295–298
server computers, 70–72
support for service conversions, 470
Vendor-specific security, 707
Verification tests
automating, 441
Hello. World program, 440–442
manual, 441–442
OK or FAIL message, 440
Verifying
problem repair, 376–378
problems, 372–373
Version control system, 453
Versions
storing differences, 425
Vertical cable management, 158
Vertical scaling, 699, 700–701
Veto power, 505
vir shell script, 425
Virtual connections between sites, 212
Virtual helpdesks, 345
  welcoming, 346
Virtual hosts, 506–507
Virtual machines
  defining state, 507
  migrating onto spare machine, 507
  rebalancing workload, 507
Virtual servers, 91
Virtualization cluster, 507
Virus blocking
  email service, 549–550
Viruses, 284
  email system, 557
  introduced through pirated software, 330
  web sites, 704
Visibility, 751
  desk location and, 767
  newsletters, 770
  office location and, 767
  status messages, 766
  town meetings, 768–770
Visibility paradox, 765
Vision leader, 830–831
visionary, 929
VLAN, 212
  large LANs using, 212–213
  network topology diagrams, 213
Voicemail
  confidential information, 292
  shared, 292–293
Volumes, 587
  filesystem, 587
VPATH facility, 673
VPN service, 664
VPNs, 187, 284
VT-100 terminal, 80

W
W3C (World Wide Web Consortium), 689
WAFL file system, 586
WAN (wide area network), 102
WAN connections
  documentation, 207
WANs, 187, 188
  limiting protocols, 191
  redundant multiple-star topology, 194
  Ring topologies, 193
  star topology, 191–192
Wattage monitor, 610
Web
  data formats, 692
  open standards, 689
  security, 271
  special-purpose formats, 692
Web applications, 690
  managing profiles, 720
  standard formats for exchanging data between, 721–722
Web browser
  system status web page, 766
Web browsers, 690, 691
  multimedia files, 692
Web client, 691
Web content, 717
  accessing, 689
Web council, 711–712
  change control, 712–713
Web farms
  redundant servers, 89
Web forms
  intruder modification, 708
Web hosting, 717
  advantages, 718
  managing profiles, 719–721
  reliability, 719
  security, 719
  third-party, 718–721
  unified login, 719–721
Web outsourcing
  advantages, 718–719
  disadvantages, 719
  hosted backups, 719
  web dashboard, 719
Web pages
  dynamically generated, 691
  HTML or HTML derivative, 692
  interactive, 691–692
Web proxies
   layers approach, 461
Web repository
   search engines, 250–251
Web server Apache
   UNIX, 452
Web server appliances, 84
Web server software
   authentication, 720
Web servers, 691
   adding modules or configuration directives, 716
   alternative ports, 697–698
   building manageable generic, 714–718
   directory traversal, 707–708
   Horizontal scaling, 699–700
   letting others run web programs, 716
   limiting potential damage, 709
   logging, 698, 710
   managing profiles, 720
   monitoring errors, 698
   multimedia servers, 696–697
   multiple network interfaces, 698
   OS (operating system), 79
   overloaded by requests, 699
   pages, 689
   permissions, 710
   privileges, 710
   protecting application, 706–707
   protecting content, 707–708
   questions to ask about, 714
   redirect, 715
   reliability, 704
   round-robin DNS name server records, 699–700
   security, 703–710
   server-specific information, 699
   static documents, 694–695
   validating input, 709
   vertical scaling, 700–701
   web-specific vulnerabilities, 707
Web service
   architectures, 694–698
   basics, 690–718
   building blocks, 690–693
   CGI servers, 695
   database-driven web sites, 695–696
   multimedia servers, 696–697
   SLAs (service level agreements), 694
   static web server, 694–695
   URL (uniform resource locator), 690
Web services
   AJAX, 691–692
   centralizing, 506
   content management, 710–714
   Horizontal scaling, 699–700
   load balancers, 700
   monitoring, 698–699
   multiple servers on one host, 697–698
   scaling, 699–703
   security, 703–710
   vertical scaling, 700–701
   web client, 691
Web sites, 399, 689
   basic principles for planning, 715–716
   building from scratch overview, 3
   certificates, 704–706
   CGI programs, 701
   CGI servers, 695
   change control, 712–716
   changes, 713
   compromised, 704
   content updates, 712
   database-driven, 695–696
   databases, 701
   deployment process for new releases, 717–718
   DNS hosting, 717
   document repository, 248
   domain registration, 717
   fixes, 713
   form-field corruption, 708
   growing overview, 4
   hijacked, 703–704
   HTTP over SSL (Secure Sockets Layer), 704–705
   political issue, 713–714
   publication system, 253
   secure connections, 704–706
   separate configuration files, 715
   setting policy, 693–694
Web sites (continued)
SQL injection, 708
static, 694–695
static files, 701
updates, 713
updating content, 716
viruses, 704
visitors, 704
web content, 717
web hosting, 717
web system administrator, 693
web team, 711–712
webmaster, 693–694
Web system administrator, 693
Web team, 711–712
Web-based documentation repository, 249–250
Web-based request system
provisioning new services, 360
Web-based service
surfing web anonymously, 335
Web-Based Services, 469
Webmaster, 693–694, 711, 712
Week-long conferences, 796, 862
WiFi networks
network access control, 61
Wiki Encyclopedia, 252
Wiki sites, 692
Wikipedia, 252, 258
Wikis, 249–250, 252
ease of use, 251
enabling comments, 254
FAQ (Frequently Asked Questions), 256
formatting commands, 249
help picking, 250
how-to docs, 255–256
HTML (Hypertext Markup Language), 249
internal group-specific documents, 255
low barrier to entry, 254
naming pages, 249
off-site links, 258
placeholder pages, 249
plaintext, 249
procedures, 257
reference lists, 256–257
requests through ticket system, 255
revision control, 254
self-help desk, 255
source-code control system, 249
structure, 254
taxonomy, 254
technical library or scrapbook, 257–258
wiki-specific embedded formatting tags or commands, 249
WikiWikiWeb, 249
WikiWords, 249
Windows
Administrator account, 291
code control systems, 425
distribution-server model, 668–669
filesystem, 587
loading files into various system directories, 43
login scripts, 115
network disk, 668
network-based software push system, 668
PowerUser permissions, 291
security, 271
software depot, 668
WINS directory, 223
Windows NT
automating installation, 47
listing TCP/IP and UDP/IP ports, 438
Services console, 438
SMB (Server Message Block) print protocol, 569
unique SID (security ID), 51
Windows NT Backup and Restore (Leber), 620
Windows platforms
roaming profiles, 78
storing data on local machines, 78
Windows software depot, 669
commercial software, 684
selecting software for, 672
Windows software depots, 679
Admin directory, 680–681
certain products approved for all systems, 680–681
directory for each package, 681
  disk images directory, 680
  Experimental directory, 680
  notes about software, 681
  Preinstalled directory, 680
  replicating, 681–682
  self-installed software, 680
  special installation prohibitions and
  controls, 680–681
  Standard directory, 680
  version-specific packages, 681
WINS directory, 223
Wireless communication
  as alerting mechanism, 530
  third-party spying, 530
Wiring
  data centers, 159–166
  good cable-management
  practices, 151
  higher-quality copper or fiber, 198
  IDF (intermediate distribution
  frame), 198
  networks, 198
  payoff for good, 164–165
  servers, 163
Wiring closet, 197–203
Wiring closets
  access to, 201
  floorplan for area served, 200
  protected power, 201
  training classes, 200
Work
  balancing with personal life, 809–810
  Work stoppage
    surviving overview, 10–11
Workbench
  data centers, 172–173
Worksations
  maintenance contracts, 74
Workstations, 41
  automated installation, 43
  bulk-license popular packages, 331
  defining, 41
  disk failure, 78
  long life cycles, 41
  maintaining operating systems, 44–65
  managing operating systems, 41
  manual installation, 43
  network configuration, 57–61
  reinstallation, 43–44
  spareparts, 74
  storing data on servers, 78
  updating system software and
  applications, 54–57
Worms, 284
Wrapper scripts, 671
Wrappers, 679
Write streams
  streamlining, 612

X
xed shell script, 425
XML, 692
XSRF (Cross-Site Reverse Forgery), 710

Y
Yahoo!, 90