Index

10 Gigabit Ethernet standard, 19819-inch racks, 152, 155802.3 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 email 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 - 54Automated 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 local area networks, 524 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

С

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 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 opperating 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, 741 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 conversion 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

D

D2D2T (disk-to-disk-to-tape), 635 DAD (disk access density), 613 Daemons, 115 Daily planning, 782–783 Daily tasks, 785 DAS (directly attached storage), 587 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 - 125Data 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 sysem, 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 - 122Dedicated 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 - 411Deletion 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 early, 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 worrrier, 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 email, 245-246 email 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, 607 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

Ethereal, 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 - 330professional code of conduct, 324-326 something illegal/unethical, 338-340 ETR (estimated time to repair), 656 ETSI (European Telecommunication Standards Institute) standard, 177 - 178Exchange 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

Η

The Haggler's 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, 741 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 adminstrators), 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 Protability 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, 223 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 - 213aligning 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 802.1 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

J

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

K

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 - 218Leaf 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

Μ

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-availabiilty 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 - 11Major 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 - 30Managing 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 email, 337 email servers, 552-553 email 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

leveraging, 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 - 282Network 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 - 218lunch-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 - 111mounting 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 analogies 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

0

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 - 103Optimization, 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 - 176Partially 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 - 148providing 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, 566-576 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 confidentaility, 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 - 13Process and documentation, 416 Process of elimination, 394 Processes centralization, 505 change management, 422, 424 high confidence in completion, 65-66 recording knowledge about, 413 procmail, 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 snaphots, 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 - 87physical-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 email 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 RoboInst, 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 snaphots 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 - 286special 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 - 251Search 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 - 275protecting 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 - 287single 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

vendor-specific, 707 VPNs, 284 Web, 271 web hosting, 719 web servers, 703-710 web services, 703-710 Windows, 271 Security architect, 301–302, 318 Security bulletins, 289 Security conferences, 316 Security consultants, 308–309 Security disasters, 268–269 Security incidents, 303–307 Security industry contacts, 316 Security operations staff, 302 Security patches, 704 Security perimeter, 317 Security policies, 271 AUP (acceptable-use policy), 276 - 277basics, 272-315 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 - 279log-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 - 280perimeter 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 - 80OS 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, 450additional 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 environment, 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 tying 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 Sings: 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 contribution 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 Spares, 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 - 30specialization, 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

Т

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 - 258Technical 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

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 Administators (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

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 - 12Tools 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 - 194ring 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 Universal client, 690, 691 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 sysems 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 - 65live 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 derivitive, 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 servers, 691 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 - 250Web-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 - 65managing 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