

## Symbols

---

/etc/ipsec.secrets file, 433–435  
 /etc/mrtg.cfg file, 282  
     example, 280–281  
     keywords, 282–286  
     templates, 286–288  
     testing, 290  
 /etc/nagios/contactgroups.cfg file, editing, 255  
 /etc/nagios/contacts.cfg file, editing, 255–256  
 /etc/nagios/hostgroups.cfg file, editing, 254  
 /etc/nagios/hosts.cfg file, editing, 250–252  
 /etc/nagios/services.cfg file, editing, 252–254  
 /etc/raddb/acct\_users configuration file  
     (FreeRADIUS), 154  
 /etc/raddb/clients.conf configuration file  
     (FreeRADIUS), 151  
 /etc/raddb/dictionary configuration file  
     (FreeRADIUS), 154  
 /etc/raddb/radiusd.conf configuration file  
     (FreeRADIUS), 153  
 /etc/raddb/users configuration file (FreeRADIUS),  
     152–153  
 /etc/syslog.conf file  
     reloading, 190  
     rules, adding, 188  
     syslog daemon, configuring, 187

## A

---

AAA (authentication, authorization, and  
     accounting), 115–116  
     RADIUS, 118–120  
         Cisco PIX Firewall configuration, 177–178  
         Cisco router configuration, 175  
         Cisco switch configuration, 176  
         comparing with TACACS+, 120–121  
         deploying on Linux-based server,  
             148–158  
         messages, 120  
         Microsoft IAS-based servers, configuring,  
             159–161, 164, 169, 172–174

TACACS+, 117, 121  
     Cisco PIX Firewalls configuration,  
         145–146  
     Cisco router configuration, 136–140  
     Cisco switch configuration, 141–144  
     Cisco VPN concentrator configuration,  
         146–147  
     configuration file, 123–125, 132  
     Linux-based servers, deploying, 121–122  
     server installation, 122–123  
 absolute timeouts, 135  
 ACCEPT messages (TACACS+), 118  
 access control, RADIUS, 118–120  
     comparing with TACACS+, 120–121  
 accessing router home page, 29  
 accounting, configuring  
     on Linux-based TACACS+, 132  
     on Cisco routers, 139–140  
     on Cisco switches, 144  
     on Microsoft IAS-based servers, 173–174  
 ACID (Analysis Console for Intrusion  
     Databases), 399  
 active connections, displaying with netstat  
     command, 98  
 active versus passive packet analyzers, 316  
 adding  
     icons to Dia stencils, 501  
     redundancy to network monitoring systems, 267  
     rules to /etc/syslog.conf file, 188  
 advanced architecture of Windows-based Snort,  
     399–401  
 advanced Nagios features, 266–267  
 AES (Advanced Encryption Standard), 421  
 agentless monitoring, 231  
 AH (Authentication Header), 421  
 Allen, Jeff, 293  
 Allman, Eric, 181  
 analyzing Tcpdump output, 341  
 anomaly-based IDSs, 388  
 apt-get command (Linux), 278  
 arp command, 109  
     verifying Layer 2 connectivity, 109–110  
 audit trails, 116  
 auditing  
     Cisco routers with RAT, 367  
     live routers with RAT, 375–376

- multiple configurations with RAT, 374
- with SDM, 377

- authentication, configuring
  - on Cisco routers, 137–138
  - on Cisco switches, 142
  - on Linux-based TACACS+ servers, 125
- authorization, configuring
  - on Cisco routers, 138–139
  - on Cisco switches, 143–144
- autocommand feature (TACACS+ Daemon), 131
- automating Rancid, 405
- availability, 231
- Availability Manager, 268
- Availability page (Nagios), 264

## B

- BGP meltdown emergencies, troubleshooting, 87–90
- Big Brother
  - change notification interval, configuring, 239
  - configuring, 235–236
  - deploying, 233
  - e-mail notification, sending, 239
  - for Windows
    - configuring, 242–245
    - deploying, 242
    - installing, 242
    - server, starting, 245–246
  - hyperlinks, creating for node information, 241
  - installing, 233–235
  - performance, increasing, 240
  - scalability, improving, 241
  - server, starting, 237–239
  - services, monitoring, 240–241
  - source code files, 234
- bootable CD-based toolkits, 316
  - Linux live CD-ROMs, 317–319
- browser-based GUI, 28

## C

- Cacti
  - configuring, 295, 299–301
  - deploying, 294–295
  - features of, 294
  - graphs, viewing, 302
  - installing, 295
  - monitoring Cisco devices, 297–299
  - poller.php script, 301–303
  - templates, importing, 300
- Cain & Abel, 357
- Capture Text, 9
- capturing data with Minicom, 13
- CAs (certificate authorities), 422
- CatOS-based switches
  - configuration files, saving, 39
  - RADIUS, configuring, 176
  - SNMP, configuring, 306
  - SPAN ports, configuring, 337
  - syslog server functionality, configuring, 214–216
  - TACACS+. configuring, 141–142
    - accounting, 144
    - authentication, 142
    - authorization, 143–144
- cfgmaker tool, 278–279
  - /etc/mrtg.cfg file, 280–282
  - keywords, 282–286
  - templates, 286–288
- chmod command, 125
- Cisco Configmaker, 32
- Cisco devices
  - monitoring with Cacti, 297–299
  - performance monitoring configuration, 304
  - SNMP, configuring, 304–307
  - SSH, configuring, 24
- Cisco IDS products, 415
- Cisco IOS configuration files, saving, 38–39
- Cisco PIX Firewall,
  - PDM access, enabling, 31
  - RADIUS configuration, 177–178
  - TACACS+ configuration, 145–146

- Cisco routers
  - configuration files
    - auditing with RAT, 371
    - multiple configurations, auditing with RAT, 374
  - IDS functionality, 407
    - configuring, 408–409
    - network monitoring, 410
    - verifying configuration, 410
  - passwords, 356
    - decrypting, 357
    - Type 5, decrypting, 359–361
    - Type 7, decrypting, 357–359
  - port scans, performing, 363
  - RADIUS configuration, 175
  - SDM
    - configuring, 377
    - deploying, 377
    - launching, 378
    - One-Step Lockdown, 382–383
    - Security Audit Wizard, 380–382
  - securing, 355–356
    - best practices, 383–384
    - RAT, 367
  - TACACS+ configuration, 136–137
    - accounting, 139–140
    - authentication, 137–138
    - authorization, 138–139
  - unnneeded services, disabling, 362–363
  - vulnerabilities, discovering, 364–367
- Cisco SDM, 376–377
  - configuring on Cisco routers, 377
  - deploying on Cisco routers, 377
  - launching, 378
  - One-Step Lockdown, 382–383
  - Security Audit Wizard, 380–382
- Cisco switches
  - RADIUS configuration, 176
  - TACACS+ configuration, 141–142
    - accounting, 144
    - authentication, 142
    - authorization, 143–144
- Cisco Threat Response, 415
- Cisco VPN 3000 Series concentrators
  - SNMP, configuring, 307
  - syslog, configuring, 222
  - TACACS+, configuring, 146–147
- CiscoWorks, 310, 415
- clear-text passwords, 128
- CLI (command-line interface), 7
- client/server (Nessus), running, 329–330
- command authorization, configuring for Linux-based TACACS+ user accounts, 130–131
- commands
  - arp, 109–110
  - chmod, 125
  - config net, 38
  - copy config tftp, 38
  - copy ftp, 43–45
  - copy running-config tftp, 38
  - copy startup-config tftp, 38
  - copy tftp config, 38
  - copy tftp runing-config, 38
  - copy tftp startup-config, 38
  - crypto key generate rsa, 24
  - dig, 96
  - enable secret, 356
  - exit, 95
  - grep, 190
  - ip scp server enable, 46
  - ipconfig, 51
  - kill, 190
  - Linux, apt-get, 278
  - nbstat, 107–108
  - netstat, 96, 190
    - active connections, displaying, 98
    - all connections, displaying, 98–99
    - Linux-based, 102–104
    - routing tables, displaying, 101–102
    - Windows-based, 97
  - nslookup, 92
    - Linux-based, 94–96
    - Windows-based, 93–94
  - ping, 53
    - BGP meltdown emergencies, troubleshooting, 87–90
    - DNS name resolution, 58–59
    - inaccurate results of, 53
    - IOS-based, 63–72
    - Linux-based, 59–62
    - network connectivity, troubleshooting, 73
    - running continuously, 57–58
    - timeout value, 53
    - Windows-based, 50–51

- service password-encryption, 356
- show arp, 108
- show interface ethernet0, 111
- show proc cpu, 90
- tee, 16
- traceroute, 74
  - BGP meltdown emergencies, troubleshooting, 87–90
  - interpreting results of, 80
  - IOS-based, 82–86
  - Linux-based, 77–80
- tracert, 75
  - inaccurate results of, 77
- whois, 90–92
- write net, 38
- commercial Cisco products, configuring syslog server functionality, 222
- common ports, scanning, 325–326
- community string (SNMP), 273
- comparing RADIUS and TACACS+, 120–121
- components of SNMP, 272
- config net command, 38
- configuration files
  - /etc/nagios/contactgroups.cfg, editing, 255
  - /etc/nagios/contacts.cfg, editing, 255–256
  - /etc/nagios/hostgroups.cfg, editing, 254
  - /etc/nagios/hosts.cfg, editing, 250–252
  - /etc/nagios/services.cfgm, editing, 252–254
  - /etc/syslog.conf
    - rules, adding, 188
    - syslog daemon, configuring, 187
  - /etc/syslog-ng.conf, Syslog-ng daemon, configuring, 193
  - auditing with RAT, 371
  - Catalyst, saving, 39
  - Cisco IOS, saving, 38–39
  - for Linux-based TACACS+ server, templates, 134–136
  - for TACACS+, 123–125
    - encryption key, 125
    - verifying, 132
  - multiple configurations, auditing with RAT, 374
  - PIX, saving, 39
  - running configuration, copying to
    - FTP server, 45
  - syslog.conf., reloading, 190
  - syslog-ng.conf
    - destination parameter, 195–197
    - filter parameter, 197–198
    - log parameter, 198–203
    - options parameter, 193–194
    - source parameter, 194
  - TFTP, creating, 37
- configuring
  - Big Brother, 235–236
    - change notification interval, 239
    - Windows-based, 242–245
  - Cisco devices
    - with Cisco Configmaker, 32
  - Cisco devices for syslog server
    - functionality, 212
      - CatOS-based switches, 214–216
      - Cisco routers, 212–214
      - commercial Cisco products, 222
      - PIX Firewalls, 216–220
      - VPN concentrators, 220–222
  - cu, 13
  - HTPE macros, 18–20
  - IIS servers, FTP services, 41–43
  - IOS-based HTTP servers, 29
  - IOS-based IDS sensors, 408–409
  - Linux-based FTP servers, 43–44
  - Linux-based macros
    - GtkTerm, 21–23
    - Minicom, 20–21
  - Linux-based Snort, 392
  - Microsoft IAS-based RADIUS server, 160–161
    - accounting parameters, 173–174
    - remote-access policies, 164, 169, 172–173
  - Minicom, 11–13
  - Nagios for Linux, 248–249
  - passwords (TACACS+), 127–129
  - performance monitoring, 304
    - MRTG, 278
  - PIX IDSs, 411–413
  - PuTTY, 25
  - RADIUS
    - FreeRADIUS, 150–154
      - on Cisco PIX Firewalls, 177–178
      - on Cisco routers, 175
      - on Cisco switches, 176
  - Rancid, 402–405
  - RAT, 369–370

- SDM on Cisco routers, 377
  - SNMP
    - on Cisco routers, 304–306
    - on Cisco switches, 306
    - on Cisco VPN 3000 Concentrators, 307
    - on PIX Firewalls, 306–307
  - SPAN ports
    - for CatOS switches, 337
    - for IOS-based switches, 337–338
  - SSH
    - client, 26
    - for Cisco devices, 24
  - syslog daemon, 185–187
  - Syslog-ng daemon, 192–193
    - destination parameter, 195–197
    - filter parameter, 197–198
    - log parameter, 198–203
    - options parameter, 193–194
    - source parameter, 194
  - TACACS+
    - accounting, 132
    - command authorization, 130–131
    - default authentication for Linux-based
      - TACACS+ servers, 125
    - expiration date, 129
    - groups, 126
    - on Cisco PIX Firewalls, 145–146
    - on Cisco routers, 136–140
    - on Cisco switches, 141–144
    - on Cisco VPN concentrators, 146–147
    - service authorization, 129–130
    - usernames, 127
  - Windows-based FTP servers, 39–40
  - Windows-based performance monitoring
    - systems
      - Cacti, 295, 299–303
  - Windows-based Snort, 395
  - Windows-based Syslog server
    - Kiwi Syslogd Server, 204, 207
  - connecting icons
    - in Dia diagrams, 500
    - in Network Notepad diagrams, 507
  - connections
    - displaying with Linux-based netstat
      - command, 104
    - removing from Network Notepad diagrams, 507
  - connectivity
    - troubleshooting
      - MTU-related problems, 54–57
      - with ping command, 73
      - verifying with ping command, 51–53
  - console port, 6
  - console tools (Windows-based), HyperTerminal, 8–9
  - CONTINUE messages (TACACS+), 118
  - continuous ping command
    - executing, 57–58
    - IOS-based, 70–71
    - Linux-based, 60–61
  - copy config tftp command, 38
  - copy ftp command, 43–45
  - copy running-config tftp command, 38
  - copy startup-config tftp command, 38
  - copy tftp config command, 38
  - copy tftp running-config command, 38
  - copy tftp startup-config command, 38
  - copying running configuration to FTP server, 45
  - CPU utilization, 271
  - creating
    - Big Brother hyperlinks for node
      - information, 241
    - live CD-ROMs, 318
    - network diagrams
      - Dia, 498–501
      - graphic design tool requirements, 496–497
      - with Network Notepad, 505–509
  - Cricket, 293
  - cron, 290
  - crontab, 290
  - crypto key generate rsa command, 24
  - CSACS (Cisco Secure Access Control Server), 178
  - CS-MARS (Cisco Security Monitoring, Analysis and Response System), 415
  - cu, configuring, 13
- ## D
- 
- debug messages for Linux-based TACACS+
    - daemon, viewing, 133–134
  - decrypting Cisco IOS passwords, 357
    - Type 5, 359–361
    - Type 7, 357–359

- default authentication, configuring on Linux-based TACACS+ servers, 125
- default syslog severity level logging, overriding, 188
- defining macros for HTPE, 18–20
- delay, 271
- depicting topologies in network diagrams, 495
- deploying
  - Big Brother, 233
  - for Windows, 242–246
  - Dia, 498
  - Linux-based RADIUS servers, 148–149
    - FreeRADIUS, 149–158
  - Linux-based Snort, 392
  - Linux-based Syslog-ng daemon, 191–203
  - Linux-based TACACS+ server, 121
    - configuration file, 123–125, 132
    - installation files, downloading, 122
  - Nagios for Linux, 246–247
  - Network Notepad, 505
  - OpenSWAN, 427
  - performance monitoring tools
    - Cacti, Windows-based, 294–295
    - MRTG, Linux-based, 274–290
    - MRTG, Windows-based, 290–292
  - SDM on Cisco routers, 377
  - syslog servers, 185
  - Windows-based Snort, 394
  - Windows-based Syslog daemon, Kiwi Syslogd Server, 203
- DES (Data Encryption Standard), 421
- destination parameter, syslog-ng.conf, 195–197
- destination-drivers, 195
- D-H (Diffie-Hellman), 422
- Dia, 497
  - adding text boxes in diagrams, 500
  - creating diagrams, 498–501
  - deploying, 498
  - exporting diagrams as JPEGs, 501
  - icons, inserting, 500
  - inserting Ethernet backbone in diagrams, 500
  - shapes, 498
  - sheets, 498
  - stencils, adding new icons to, 501
  - viewing sample diagrams, 501
- dig command, 96
- digital signatures, 423

- disabling unneeded services on Cisco routers, 362–363
- discovering vulnerabilities on Cisco routers, 364–367
- displaying
  - connections with netstat command
    - active connections, 98
    - all connections, 98–99
    - Linux-based, 104
  - Ethernet statistics, 104
  - logs from Syslog-ng daemon, 203
  - network statistics, 105–106
  - protocol statistics summary, 100–101
  - syslog messages on Linux OS, 190
  - TCP/IP statistics, netstat command, 96–97
  - UDP connection statistics, 98
- DNS names, resolving, 58–59
- documentation, 510
- domain names
  - mail servers, identifying, 93–94
  - nslookup command, 92
    - Linux-based, 94–96
    - Windows-based, 93–94
  - whois command, 90–92
- downloading installation files for Linux-based TACACS+ server deployment, 122
- Downtime page (Nagios), 260
- Dsniff, 338
- dynamic connections between network diagram icons, 497

---

## E

- editing
  - configuration files
    - /etc/nagios/contactgroups.cfg file, 255
    - /etc/nagios/contacts.cfg file, 255–256
    - /etc/nagios/hostgroups.cfg file, 254
    - /etc/nagios/hosts.cfg file, 250–252
    - /etc/nagios/services.cfg file, 252–254
    - OpenSWAN configuration file, 429–435
  - syslogd daemon, 189
- enable secret command, 356
- enabling
  - IOS HTTP server, 29
  - SCP, 46

- syslog servers on Cisco devices, 212
  - CatOS-based switches, 214–216
  - Cisco routers, 212–214
  - commercial Cisco products, 222
  - PIX Firewalls, 216–220
  - VPN concentrators, 220–222
- encrypted passwords, 128
- encryption, Vigenere algorithm, 356
- encryption key for Linux-based TACACS+ server configuration file, 125
- enhancing Big Brother performance, 240
- ERROR messages (TACACS+), 118
- ESP (Encapsulating Security Payload), 421
- establishing Telnet sessions with HTPE, 17
- Ethereal, 343–344
  - capture sessions, 345
  - output, filtering, 347
  - root password, setting, 345
  - TCP packets, re-assembling, 350
- Ethernet
  - statistics, displaying, 104
  - backbone. inserting in diagrams
    - Dia diagrams, 500
    - Network Notepad diagrams, 508
- Event Viewer, 203
- examples of Tcpdump, 342–343
- exit command, 95
- exiting Minicom, 13
- expiration dates, configuring for Linux-based TACACS+ user accounts, 129
- exporting
  - Dia diagrams as JPEGs, 501
  - Network Notepad diagrams as .bmp files, 509

## F

- facility parameter (syslog packets), 182–183
- false negatives, 388
- features
  - of Cacti, 294
  - of dig command, 96
- file format of network diagrams, selecting, 496

- file management, 33
  - with TFTP server, 33
    - IOS-based, 37
    - Linux-based, 35–37
    - Windows-based, 34
- filter parameter for syslog-ng.conf, 197–198
- filtering Ethereal output, 347
- filters (Tcpdump), 340
- five nines, 231
- format of syslog messages, differences among Cisco devices, 185
- fping command, 73
- FreeRADIUS
  - configuration files, 151–154
  - configuring, 150–151
  - installing, 149
  - running, 154–158
- FTP services
  - IIS servers configuring, 41–43
  - Linux-based, configuring, 43–44
  - Windows-based, configuring, 39–40

## G

- generate\_passwd utility, 128
- generating Nessus reports, 332
- GetPass utility, 359
- graphic design tools
  - Linux-based, Dia, 497–501
    - adding text boxes in diagrams, 500
    - creating diagrams, 498–501
    - deploying, 498
    - exporting diagrams as JPEGs, 501
    - icons, inserting, 500
    - inserting Ethernet backbone in diagrams, 500
    - shapes, 498
    - sheets, 498
    - stencils, adding new icons to, 501
    - viewing sample diagrams, 501
  - requirements for network diagram creation, 496–497
  - Windows-based, Network Notepad, 504–509
    - creating network diagrams, 505–509
    - deploying, 505
    - exporting diagrams as .bmp files, 509

- icons, adding to libraries, 509
- inserting Ethernet backbone in diagrams, 508
- viewing sample diagrams, 509
- graphing utilities, RRDTool, 292
- graphs (Cacti), viewing, 302
- grep command, 190
- groups, configuring for Linux-based TACACS+ servers, 126
- GtkTerm
  - configurations, saving, 14
  - Linux-based macros, configuring, 21–23
- GUI-based configuration tools, 28
- GUIs, browser-based, 28

## H

---

- hardening Debian Linux, website, 267
- HIDSs (host-based IDSs), 388
  - Rancid, 401–402
    - automating, 405
    - configuring, 402–405
    - e-mail output, obtaining, 405
    - installing, 402
    - testing, 405
- HIPAA (Health Insurance Portability and Accountability Act), 116
- histograms generated by MRTG, 276
- hostname parameter (syslog packets), 184
- hping, 73
- HTPE (HyperTerminal Private Edition)
  - establishing Telnet sessions, 17
  - macro feature, 18–20
- hyperlinks (Big Brother), creating for node information, 241
- HyperTerminal, 8–9

## I

---

- ICMP (Internet Control Message Protocol), network monitoring, 232
- icons
  - connecting in Network Notepad diagrams, 507
  - dynamic connections between, 497

- inserting
  - in Dia diagrams, 500
  - in Dia stencils, 501
  - in Network Notepad diagrams, 507
  - in Network Notepad libraries, 509
- idle timeouts, 135
- IDSs (Intrusion Detection Systems), 388
  - Cisco products, 415
  - HIDSs, Rancid, 401–405
  - PIX IDSs
    - configuring, 411–413
    - network monitoring, 413–414
    - verifying configuration, 413
  - placement of, 388–389
  - router IDSs, 407
    - configuring, 408–409
    - network monitoring, 410
    - verifying configuration, 410
  - signature-based, Snort, 391–401
- IIS servers
  - FTP services, configuring, 41–43
  - installing, 40
- IKE (Internet Key Exchange), 421–423
- importing Cacti templates, 300
- improving Big Brother scalability, 241
- inaccurate results of ping command, 53
- in-band management methods, 6
- indexmaker tool, 288
- inserting
  - icons
    - in Dia diagrams, 500
    - in Dia stencils, 501
    - in Network Notepad diagrams, 507
    - in Network Notepad libraries, 509
    - text in Network Notepad diagrams, 508
- installation files, downloading for Linux-based TACACS+ server deployment, 122
- installing
  - Big Brother
    - on Linux systems, 233–235
    - on Windows systems, 242
  - FreeRADIUS, 149
  - IIS servers, 40
  - Linux-based Snort, 392
  - Microsoft IAS-based RADIUS server, 159
  - Nagios, 249
    - for Linux, 247–248



- OpenSWAN, 428
  - performance monitoring tools, MRTG, 277
- Rancid, 402
- RAT, 368
- Syslog-ng daemon, 191–192
- TACACS+ daemon, 122–123
- Windows-based performance monitoring systems, Cacti, 295
- Windows-based Snort, 394–395
- Windows-based Syslog server, Kiwi Syslogd Server, 204
- interesting traffic, 423
- interoperability
  - of OpenSWAN
    - with Cisco IOS, 439–450
    - with Cisco PIX Firewall, 450–461
    - with Cisco VPN 3000 Series concentrators, 461–470
  - of Windows-based VPNs with Cisco products, 472–482, 486–489
- interpreting results of traceroute command, 80
- interval option (netstat command), 101
- intranet web portals, 511
- invoking
  - macros with predefined shortcut keys, 23
  - Nmap, 320
- IOS HTTP servers, enabling, 29
- IOS-based ping command, 63
  - MTU testing, 72
  - privileged mode, 65–70
  - running continuously, 70–71
  - user mode, 63–65
- IOS-based switches, configuring SPAN ports, 337–338
- IOS-based traceroute command, 82
  - options, 85–86
  - privileged mode, 84–86
  - user mode, 82–84
- IP packets, TTL field, 74
- ip scp server enable command, 46
- ipconfig command, 51
- IPM (Internet Performance Monitor), 310

- IPSec, 420
  - components of, 422
  - digital signatures, 423
- IKE
  - preshared keys, 423
  - SAs, 423
- interesting traffic, 423
- key management, 422
- OpenSWAN. *See* OpenSWAN
- VPNs, Windows-based, 470–482, 486–489
- ISO image files, 318

---

## J-K

- Jacobson, Van, 74
- jitter, 271
- keywords, /etc/mrtg.cfg file, 282–286
- kill command, 190
- Kiwi Syslogd Server
  - configuring, 204, 207
  - deploying, 203
  - graphical statistics summary, viewing, 210–211
  - installing, 204
  - messages, viewing, 209–210
  - starting, 209
- Knoppix, 318

---

## L

- latency, 271
- launching SDM, 378
- Layer 2 connectivity, verifying with arp command, 109–110
- libraries, 505. *See also* stencils
  - adding icons to, 509
- limitations of MRTG, 292
- Linux
  - apt-get command, 278
  - Big Brother
    - change notification interval, configuring, 239
    - configuring, 235–236
    - deploying, 233
    - e-mail notification, sending, 239

- installing, 233–235
  - performance, increasing, 240
  - server, starting, 237–239
  - services, monitoring, 240–241
- FreeRADIUS
- configuring, 150–154
  - deploying, 149
  - running, 154–158
- FTP servers, configuring, 43–44
- graphic design tools, Dia, 497
- adding new icons to stencil, 501
  - creating diagrams with, 498–501
  - deploying, 498
  - exporting diagrams as JPEGs, 501
  - icons, 500
  - inserting Ethernet backbone, 500
  - shapes, 498
  - sheets, 498
  - text boxes, adding, 500
  - viewing sample diagrams, 501
- macros
- GtkTerm, configuring, 21–23
  - Minicom, configuring, 20–21
- Nagios
- advanced feature, 266–267
  - configuring, 248–249
  - deploying, 246–247
  - Downtime page, 260
  - installing, 247–248
  - Process Info page, 262
  - scalability, improving, 241
  - status, viewing, 258
  - verifying configuration, 256–257
- netstat command, 102–103
- active connections, displaying, 104
  - routing tables, displaying, 106
- network monitoring, creating hyperlinks for
- node information, 241
- nslookup command, 94–96
- OpenSWAN
- configuration files, editing, 429–435
  - installing, 428
  - interoperability with Cisco IOS, 439–450
  - interoperability with Cisco PIX Firewall, 450–461
  - interoperability with Cisco VPN 3000 Series concentrators, 461–463, 468–470
  - troubleshooting, 436–438
- performance-monitoring systems, MRTG, 275–276
- configuring, 278
  - histograms, 276
  - indexmaker tool, 288
  - installing, 277
  - limitations of, 292
- ping command, 59
- limiting packets sent, 61
  - running continuously, 60–61
- RADIUS servers, deploying, 148–149
- Snort
- alerts, viewing, 393
  - configuring, 392
  - deploying, 392
  - installing, 392
  - starting, 392
- syslog messages, viewing, 190
- Syslog-ng daemon
- configuring, 192–193
  - deploying, 191–203
  - installing, 191–192
- TACACS+ server deployment, 121
- accounting, configuring, 132
  - command authorization, configuring, 130–131
  - configuration files, 123–125, 134–136
  - debug messages, viewing, 133–134
  - default authentication, configuring, 125
  - expiration dates, configuring, 129
  - groups, configuring, 126
  - installation files, downloading, 122
  - passwords, configuring, 127–129
  - service authorization, configuring, 129–130
  - starting, 132–133
  - users, configuring, 127
- terminal emulation
- cu, configuring, 13
  - Minicom, configuring, 11–13
- traceroute command, 77–78
- options, 79–80
  - tracing path with ICMP probes, 82
- Linux live CD-ROMs, 317–319

- listing active connections with netstat command, 97
- live CD-ROMs, 317, 319
  - creating, 318
  - Knoppix, 318
- localizing (RAT), 369
- log parameter (syslog-ng.conf), 198–203
- logging Telnet sessions, 16
- logical topology, 496
- Loose option (traceroute command), 85

## M

- MAC addresses, tracing with nbstat command, 107–108
- macros
  - defining for HTPE, 18, 20
  - for destination-driver file, 195–196
  - invoking with predefined shortcut keys, 23
  - Linux-based
    - GtkTerm, configuring, 21–23
    - Minicom, configuring, 20–21
- mail servers, identifying for domain names, 93–94
- managing system files with TFTP server, 33
  - IOS-based, 37
  - Linux-based, 35–37
  - Windows-based, 34
- MD5 (Message Digest 5), 421
- mean time to respond, 230
- memory utilization, 271
- message parameter (syslog packets), 184–185
- messages
  - RADIUS, 120
  - syslog
    - differences among Cisco devices, 185
    - severity, 183–184
  - TACACS+, 118
- MIBs (Management Information Bases), 272
- Microsoft IAS-based RADIUS servers
  - accounting parameters, configuring, 173–174
  - configuring, 160–161
  - installing, 159
  - remote-access policies, configuring, 164, 169, 172–173
- Mills, Dr. Dave, 50

- Minicom, 11
  - configuring, 11–13
  - exiting, 13
  - Linux-based macros, 20–21
- monitoring
  - Big Brother services, 240–241
  - Cisco devices with Cacti, 297–299
- MRTG (Multi-Router Traffic Grapher)
  - /etc/mrtg.cfg file, testing, 290
  - configuring, cfgmaker tool, 278–288
  - deploying, 275–276
  - histograms, 276
  - indexmaker tool, 288
  - installing, 277
  - limitations of, 292
  - Linux-based, deploying, 275–290
  - Windows-based, deploying, 290–292
- MS-DOS, traceroute command, 75
  - inaccurate results of, 77
- MTBF (mean time between failure), 230
- MTTR (mean time to repair), 230
- MTU (maximum transmission unit)
  - connectivity, troubleshooting, 54–57
  - testing with Linux-based ping command, 62
- Muuss, Mike, 50

## N

- Nagios
  - /etc/nagios/hosts.cfg file, editing, 250–252
  - advanced features, 266–267
  - Availability page, 264
  - Downtime page, 260
  - installing, 247–249
  - Linux-based
    - configuring, 248–249
    - deploying, 246–247
    - installing, 247–248
  - Process Info page, 262
  - product documentation, viewing, 258
  - starting, 256–257
  - status, viewing, 258
  - Trends page, 262
  - viewing network status, 258
- nbstat command, 107–108

- Nessus, 328
  - caveats, 335
  - discovering Cisco router vulnerabilities, 364–367
  - reports, generating, 332
  - running client/server, 329–330
  - setup options, 329, 332
- netstat command, 96, 190
  - active connections, displaying, 98
  - all connections, displaying, 98–99
  - interval option, 101
  - Linux-based, 102–103
    - active connections, displaying, 104
    - routing tables, displaying, 106
  - routing tables, displaying, 101–102
  - Windows-based, 97
- network diagrams
  - creating, design tool requirements, 496–497
  - Dia
    - creating, 498–501
    - Ethernet backbone, inserting, 500
    - exporting as JPEGs, 501
    - icons, inserting, 500
    - samples, viewing, 501
    - text boxes, inserting, 500
  - file format, 496
  - icons, dynamic connections, 497
  - Network Notepad
    - creating, 505–509
    - exporting as .bmp files, 509
    - inserting Ethernet backbone, 508
    - samples, viewing, 509
  - topology, depicting, 495
- network monitoring systems, adding
  - redundancy to, 267
- Network Notepad
  - deploying, 505
  - diagrams, exporting as .bmp files, 509
  - icons, adding to libraries, 509
  - inserting Ethernet backbone in diagrams, 508
  - network diagrams, creating, 505–509
  - sample diagrams, viewing, 509
- network scanners, 319
  - Nessus, 328
    - caveats, 335
    - reports, generating, 332
    - running client/server, 329–330
    - setup options, 329, 332
  - Nmap, 319–320
    - common ports, scanning, 325–326
    - options, 321–322
    - remote OS detection, 326–327
    - special characters, 321–322
    - TCP ports, scanning, 323–324
    - UDP ports, scanning, 324–325
    - verbose option, 327–328
  - network statistics, displaying, 105–106
  - NIDSs (Network-Based IDS), 388
  - Nmap, 319–320, 363
    - common ports, scanning, 325–326
    - invoking, 320
    - options, 321–322
    - remote OS detection, 326–327
    - special characters, 321–322
    - TCP ports, scanning, 323–324
    - UDP ports, scanning, 324–325
    - verbose option, 327–328
  - NMSs (network management systems), 274
  - ns, 240
  - nslookup command, 92
    - Linux-based, 94–96
    - Windows-based, 93–94
  - NTP (Network Time Protocol), importance of event correlation, 212

---

## O

- obtaining Rancid e-mail output, 405
- OE (Opportunistic Encryption), 432
- Oetiker, Tobias, 275, 292
- OIDs (object identifiers), 272
- One-Step Lockdown, 377
- One-Step Lockdown (SDM), 382–383
- open source network scanners, 319
- OpenSWAN, 426–427
  - configuration file, editing, 429–435
  - deploying, 427
  - installing, 428
  - interoperability
    - with Cisco IOS, 439–450
    - with Cisco PIX Firewall, 450–461
    - with Cisco VPN 3000 Series concentrators, 461–463, 468–470

- OE, 432
- troubleshooting, 436–438
- options
  - for arp command, 109
  - for IOS-based traceroute command, 85–86
  - for syslog-ng.conf, 193–194
- OS fingerprinting, 326–327
- out-of-band management interfaces, 6
- out-of-band signaling, 6
- output (Tcpdump), analyzing, 341
- overriding
  - default syslog severity level logging, 188
  - destination-driver file global options, 196

## P

- packet analyzers, 316, 335, 338–339
  - Ethereal, 343–344
    - capture sessions, 345
    - captured packets, viewing, 345
    - output, filtering, 347
    - re-assembling TCP packets, 350
    - root password, setting, 345
  - preparing network for, 336
  - Tcpdump, 339–340
    - examples, 342–343
    - filters, 340
    - output, analyzing, 341
- packet loss, 271
- parameters
  - for network performance monitoring, 271
  - for syslog packets
    - facility, 182–183
    - hostname, 184
    - message, 184–185
    - severity, 183–184
    - timestamp, 184
- passwords
  - clear-text, 128
  - configuring for Linux-based TACACS+ servers, 127–129
  - for Cisco routers, 356
    - decrypting, 357
    - Type 5, decrypting, 359–361
    - Type 7, decrypting, 357–359
- PDM, enabling access on Cisco PIX Firewall, 31
- Percival, 293
- performance monitoring
  - Cisco device configuration, 304
  - MRTG, 275–276
    - configuring, 278
    - histograms, 276
    - indexmaker tool, 288
    - installing, 277
    - Linux-based, deploying, 275–290
    - Windows-based, deploying, 290–292
  - parameters, 271
  - RRDTool, 292
  - SNMP, 272
    - Cisco device configuration, 304–307
    - community string, 273
    - components of, 272
    - security, configuring, 309
    - versions of, 273
    - tools, deploying, 274
- per-node keywords, /etc/mrtg.cfg file, 283–286
- PFS (Perfect Forward Secrecy), 422
- Phase 1 (IKE), 421
- Phase 2 (IKE), 421
- physical topology, 496
- ping command, 53
  - BGP meltdown emergencies, troubleshooting, 87–90
  - DNS name resolution, 58–59
  - inaccurate results of, 53
  - IOS-based, 63
    - privileged mode, 65–70
    - running continuously, 70–71
    - user mode, 63–65
  - Linux-based, 59
    - limiting packets sent, 61
    - MTU, testing, 62
    - running continuously, 60–61
  - network connectivity, troubleshooting, 73
  - running continuously, 57–58
  - timeout value, 53
  - Windows-based, 50–51
- PIX Firewalls
  - configuration files, saving, 39
  - SNMP, configuring, 306–307
  - syslog server functionality, configuring, 216–220

**PIX IDSs**

- configuring, 411–413
- network monitoring, 413–414
- verifying configuration, 413
- placement of IDSs, 388–389
- poller.php script (Cacti), 301–302
- port mirroring, 336
- port scans, performing on Cisco routers, 363
- preparing network for packet analyzers, 336
- presared keys, 423
- privileged mode (Cisco IOS)
  - ping command, 65–70
  - traceroute command, 84–86
- Process Info page (Nagios), 262
- ProFTP, 43
- protocol statistics summary, viewing, 100–101
- public key encryption, 424
- PuTTY, 25

---

**Q-R**

---

Quick Mode, 423

RADIUS (Remote-Access Dial-In User Service), 118–120

- comparing with TACACS+, 120–121
- Linux-based server deployment, 148–149
  - FreeRADIUS, 149–158
- messages, 120
- Microsoft IAS-based servers
  - configuring, 160–161, 164, 169, 172–174
  - installing, 159

Rancid (Really Awesome New Cisco confIg Differ), 401–402

- automating, 405
- configuring, 402–405
- e-mail output, obtaining, 405
- installing, 402
- testing, 405

RAT (Router Audit Tool), 367

- configuration files, auditing, 371
  - multiple configurations, 374
- configuring, 369–370
- installing, 368
- live routers, auditing, 375–376
- reports, 372–374

- record option (traceroute command), 85
- redundancy, adding to network monitoring systems, 267
- REJECT messages (TACACS+), 118
- reloading syslog.conf file, 190
- remote OS detection, 326–327
- remote-access policies, configuring on Microsoft IAS-based servers, 164, 169, 172–173
- removing connections from Network Notepad diagrams, 507
- reports
  - Nessus, generating, 332
  - RAT, 372
- requirements for creating network diagrams, 496–497
- restarting syslog daemon, 190
- restoring PIX configurations, 38
- RME (Resource Manager Essentials), 268
- Roesch, Martin, 391
- root password (Ethereal), setting, 345
- router home page, accessing, 29
- router IDSs, 407
  - configuring, 408–409
  - network monitoring, 410
- routers
  - configuration files, auditing with RAT, 371
  - passwords, 356
    - decrypting, 357
    - Type 5, decrypting, 359–361
    - Type 7, decrypting, 357–359
  - port scans, performing, 363
  - securing, 355–356
    - best practices, 383–384
    - RAT, 367
  - unneded services, disabling, 362–363
  - vulnerabilities, discovering, 364–367
- routing tables, displaying with netstat command, 101–102
- RRDTool, 292
- RTT (round-trip time) delay, 231
- rules, 391
  - adding to /etc/syslog.conf file, 188
- rules test reports (RAT), 372–374
- running
  - FreeRADIUS, 154–158
  - Nagios, 256–257
- running configuration, copying to ftp server, 45

## S

- SAA (Service Assurance Agent), 310
- sample diagrams, viewing
  - Dia diagrams, 501
  - Network Notepad diagrams, 509
- SARA (Security Auditor's Research Assistant), 319
- SAs (security associations), 422
- SATAN (Security Administrator's Tool for Analyzing Networks), 319
- saving
  - Catalyst configuration files, 39
  - Cisco IOS configuration files, 38–39
  - GtkTerm configurations, 14
  - PIX configuration files, 39
- scalability of Big Brother, improving, 241
- scanners, 316
- scanning
  - common ports, 325–326
  - TCP ports, 323–324
  - UDP ports, 324–325
- Scheidler, Balazs, 191
- SCP (Secure Copy Protocol), 46
- SDM (Cisco Router and Security Device Manager), 32, 376–377
  - configuring on Cisco routers, 377
  - deploying on Cisco routers, 377
  - launching, 378
  - One-Step Lockdown, 382–383
  - Security Audit Wizard, 380–382
- security
  - AAA, 115–116
    - RADIUS, 118–120
    - TACACS+, 117, 121–125, 132
  - Cisco routers, 355–356
    - best practices, 383–384
    - disabling unneeded services, 362–363
    - passwords, 356–357
    - RAT, 367–370
    - Type 5 passwords, decrypting, 359–361
    - Type 7 passwords, decrypting, 357–359
    - vulnerabilities, discovering, 364–367
  - configuring on SNMP, 309
  - switches, 355
  - syslog servers, 211
  - testing, 316
    - bootableCD-ROM–based toolkits, 316–319
    - Nessus, 328–332, 335
    - network scanners, 319
    - Nmap, 319–328
      - packet analyzers, 335–347, 350
  - Security Audit Wizard (SDM), 377, 380–382
  - security wheel, 315
  - selecting file format of network diagrams, 496
  - sensors, 389
  - service authorization, configuring for Linux-based TACACS+ user accounts, 129–130
  - service password-encryption command, 356
  - session timeouts, Linux-based TACACS+ server configuration, 135
  - setup options (Nessus), 329, 332
  - severity levels, overriding default logging, 188
  - severity parameter (syslog packets), 183–184
  - SHA (Security Hash Algorithm), 421
  - shapes, 498
  - sheets, 498
  - show arp command, 108
  - show interface ethernet0 command, 111
  - show proc cpu command, 90
  - signature-based IDSs, 388
  - Snort, 391
    - Linux-based, deploying, 392–393
    - Windows-based, 398–401
      - Windows-based, configuring, 395
      - Windows-based, deploying, 394
      - Windows-based, installing, 394–395
      - Windows-based, starting, 395–397
  - SLAs (service-level agreements), 230
  - SmokePing, 73
  - sniffers, 23. *See also* packet analyzers
  - SNMP (Simple Network Management Protocol), 272
    - community string, 273
    - components of, 272
    - configuring
      - on Cisco routers, 304–306
      - on Cisco switches, 306
      - on Cisco VPN 3000 Concentrators, 307
      - on PIX Firewalls, 306–307
    - NMSs, 274

- securing, 309
- versions of, 273
- Snort, 391
  - Linux-based
    - alerts, viewing, 393
    - configuring, 392
    - deploying, 392
    - installing, 392
    - starting, 392
  - Windows-based
    - advanced architecture, 399–401
    - alerts, viewing, 398
    - configuring, 395
    - deploying, 394
    - installing, 394–395
    - starting, 395–397
- source code files, Big Brother, 234
- source parameter, syslog-ng.conf, 194
- source-drivers, 194
- SPAN (Switched Port Analyzer), 336
  - for CatOS switches, port configuration, 337
  - for IOS-based switches, port configuration, 337–338
- SSH (Secure Shell)
  - Cisco SSH Security Advisory web page, 23
  - clients
    - configuring, 26
    - PuTTY, 25
  - configuring for Cisco devices, 24
  - connecting PCs to Cisco devices, 24
- starting
  - Big Brother server, 237–239
    - on Windows, 245–246
  - GtkTerm, 14
  - Linux-based Snort, 392
  - Linux-based TACACS server, 132–133
  - Nagios, 256–257
  - Syslog-ng daemon, 203
  - Windows Component Wizard, 40
  - Windows-based Snort, 395–397
  - Windows-based Syslog server, Kiwi Syslogd Server, 209
- stencils, Dia, 497
  - adding new icons to, 501
- Storner, Henrik, 241
- strict option (traceroute command), 85
- summarizing protocol statistics, 100–101
- switches, securing, 355
  - RAT, 367
- syntax, Syslog-ng.conf statements
  - destination, 195
  - filter, 197
  - log, 198
  - options, 193
  - source, 194
- syslog
  - /etc/syslog.conf file, adding rules, 188
  - configuring for Cisco devices, 212
    - CatOS-based switches, 214–216
    - Cisco routers, 212–214
    - commercial Cisco products, 222
    - PIX Firewalls, 216–220
    - VPN concentrators, 220–222
  - daemon
    - configuring, 187
    - restarting, 190
    - verifying operation, 190
  - deploying, 185
  - packet parameters
    - facility, 182–183
    - hostname, 184
    - message, 184–185
    - severity, 183–184
    - timestamp, 184
  - securing, 211
  - varying formats among Cisco devices, 185
- syslog.conf file, reloading, 190
- Syslogd daemon, 181
  - editing, 189
  - limitations of, 191
  - permitting remote syslog messages, 189
  - versus Syslog-ng daemon, 191
- Syslog-ng daemon
  - configuring, 192–193
  - destination-driver file, overriding global options, 196
  - destination-drivers, 195
  - implementing as central syslog server, 200
  - installing, 191–192
  - logs, viewing, 203
  - source-drivers, 194
  - starting, 203
  - versus syslogd daemon, 191



- syslog-ng.conf file
  - destination parameter, 195–197
  - filter parameter, 197–198
  - log parameter, 198–203
  - options parameter, 193–194
  - source parameter, 194
- system file management with TFTP server, 33
  - IOS-based, 37
  - Linux-based, 35–37
  - Windows-based, 34

## T

- TACACS+ (Terminal Access Controller Access Control System plus), 117, 121
  - comparing with RADIUS, 120–121
  - configuration file, 123–125
    - encryption key, 125
    - verifying, 132
  - configuring
    - on Cisco PIX Firewall, 145–146
    - on Cisco routers, 136–140
    - on Cisco switches, 141–144
    - on Cisco VPN concentrators, 146–147
  - Linux-based servers, 121
    - accounting, configuring, 132
    - command authorization, configuring, 130–131
    - debug messages, viewing, 133–134
    - default authentication, configuring, 125
    - expiration dates, configuring, 129
    - groups, configuring, 126
    - installation files, downloading, 122
    - passwords, configuring, 127–129
    - service authorization, configuring, 129–130
    - starting, 132–133
    - usernames, configuring, 127
  - messages, 118
  - server installation, 122–123
- TCP
  - connection statistics, displaying, 98
  - port scanning, 323–324
- TCP/IP, netstat command, 96–97
- Tcpdump, 339–340
  - examples, 342–343
  - filters, 340
  - output, analyzing, 341
- tee command, 16
- Telnet
  - auditing live routers with RAT, 375–376
  - connecting with HTPE, 17
  - logging sessions, 16
- templates
  - for /etc/mrtg.cfg file, 286–288
  - for Cacti, importing, 300
  - for Linux-based TACACS+ server
    - configuration file, 134–136
- terminal emulation software, 7
  - Linux-based
    - cu, 13
    - Minicom, 11–13
  - Windows-based, HyperTerminal, 8–9
- testing
  - /etc/mrtg.cfg file, 290
  - bootable CD-ROM–based toolkits, 316–319
  - Ethereal, 343–347, 350
  - MTU with ping command
    - IOS-based, 72
    - Linux-based, 62
  - Nessus, 328–332, 335
  - Nmap, 319–328
  - packet analyzers, 335–339
  - Rancid, 405
  - Tcpdump, 339–343
- text, adding to Network Notepad diagrams, 508
- text boxes, inserting in Dia diagrams, 500
- TFTP (Trivial File Transfer Protocol)
  - configuration files, creating, 37
  - file management, 33
    - IOS-based, 37
    - Linux-based, 35–37
    - Windows-based, 34
  - inherent weaknesses of, 39–40
- ftftpd (TFTP Daemon), 35
- throughput, 271
- timeout value, ping command, 53
- timestamp option (traceroute command), 85
- timestamp parameter (syslog packets), 184
- topology, depicting in network diagrams, 495

- traceroute command, 74
  - interpreting results of, 80
  - IOS-based, 82
    - options, 85–86
    - privileged mode, 84–86
    - user mode, 82–84
  - Linux-based, 77, 79–80
    - options, 79–80
    - tracing path with ICMP probes, 82
  - troubleshooting BGP meltdown emergencies, 87–90
- tracert command, 75
  - inaccurate results of, 77
- tracing MAC addresses with nbstat command, 107–108
- Trends page (Nagios), 262
- troubleshooting
  - BGP meltdown emergencies, 87–90
  - connectivity
    - MTU-related problems, 54–57
    - with ping command, 73
  - OpenSWAN, 436–438
- TTL field (IP packets), 74
- Type 5 encryption, 356
  - passwords, decrypting, 359–361
- Type 7 encryption, 356
  - passwords, decrypting, 357–359

## U

---

- UDP (User Datagram Protocol)
  - connection statistics, displaying, 98
  - port scanning, 324–325
- unneeded services, disabling on Cisco routers, 362–363
- user mode ping command, 63–65
- user mode traceroute command, 82–84
- usernames, configuring for Linux-based TACACS+ servers, 127
- utilities, GUI-based configuration tools, 28

## V

---

- verbose option (Nmap), 327–328
- verbose option (traceroute command), 85
- verifying
  - /etc/mrtg.cfg file, 290
  - Cacti configuration, 301–303
  - connectivity with ping command, 51–53
  - IOS-based IDS sensor configuration, 410
  - Layer 2 connectivity with arp command, 109–110
  - Linux-based TACACS+ configuration file, 132
  - Nagios configuration, 256–257
  - PIX IDS configuration, 413
  - syslog daemon operation, 190
- versions of SNMP, 273
- viewing
  - alerts (Linux-based Snort), 393
  - Cacti graphs, 302
  - captured packets (Ethereal), 345
  - Kiwi Syslogd Server
    - graphical statistics summary, 210–211
    - messages, 209–210
  - Linux-based TACACS server debug messages, 133–134
  - logs from Syslog-ng daemon, 203
  - Nagios product documentation, 258
  - network status with Nagios, 258
  - sample Dia diagrams, 501
  - sample Network Notepad diagrams, 509
  - syslog messages on Linux OS, 190
  - Windows-based Snort alerts, 398
- Vigenere algorithm, 356
- VPN concentrators, configuring syslog server functionality, 220–222
- VPNs, Windows-based, 470–471
  - interoperability with Cisco products, 472–482, 486–489
- VSAs (vendor-specific attributes), 119
- vsFTP (Very Secure FTP), 43
- vulnerabilities, discovering on Cisco routers, 363, 366–367

## W

### web pages

- Cisco Security Advisory, SSH Security Advisory page, 23
- router home page, accessing, 29

### web-based GUIs, 28

websites, hardening Debian Linux, 267

whois command, 90–92

### Windows

#### Cacti

- configuring, 295, 299–301
- deploying, 294–295
- graphs, viewing, 302
- installing, 295
- poller.php script, 301–303

FTP servers, configuring, 39–40

graphic design tools, Network Notepad, 504

- creating network diagrams, 505–509
- deploying, 505
- exporting diagrams as .bmp files, 509
- inserting Ethernet backbone, 508
- viewing sample diagrams, 509

#### Kiwi Syslogd Server

- configuring, 204, 207
- deploying, 203
- installing, 204
- starting, 209
- viewing graphical statistics summary, 210–211
- viewing messages, 209–210

MRTG, 290–292

netstat command, 97

network monitoring systems, Big Brother

- deployment, 242–246

nslookup command, 93–94

ping command, 50–51

#### Snort

- advanced architecture, 399–401
- alerts, viewing, 398
- configuring, 395
- deploying, 394
- installing, 394–395
- starting, 395–397

terminal emulation, HyperTerminal, 8–9

tracert command, 75

- inaccurate results of, 77

VPNs, 470–471

- interoperability with Cisco products, 472–482, 486–489

Windows Component Wizard, starting, 40

Windump, 350

write net command, 38

WUFTP, 43