

# Practical TCP/IP

**Designing, using, and troubleshooting  
TCP/IP networks on Linux® and Windows®**

---

Niall Mansfield



Addison-Wesley

*An imprint of* Pearson Education

---

London • Boston • Indianapolis • New York • Mexico City • Toronto  
Sydney • Tokyo • Singapore • Hong Kong • Cape Town • New Delhi  
Madrid • Paris • Amsterdam • Munich • Milan • Stockholm



---

# Index

---

- “WN” refers to Windows Networking;  
DUN refers to dial-up networking.
- 0.0.0.0 (address) 106, 117  
<00> (NetBIOS) 497, 510–11, 519  
\000 string (DHCP) 774  
<01><02> (NetBIOS) 573  
<03> (NetBIOS) 538  
\0xHH notation 511  
5-4-3 rule 732  
10.0.0.0 (address) 102, 110  
16th-byte suffix characters *see* NetBIOS suffix  
<20> (NetBIOS) 510  
*30 Years of RFCs* 727  
40-bit keys 537  
56-bit keys 537  
127.0.0.1 (address) 107, 508  
128-bit keys 537  
169.254.0.0 (address) 103  
172.16.0.0 (address) 102  
192.0.2 (address) 110  
192.168.0.0 (address) 102  
220 code (SMTP) 296  
221 code (SMTP) 299  
224.0.0.0 (address) 106  
250 code (SMTP) 297  
255 (broadcast address) 104  
255.255.255.255 (limited broadcast address) 104  
304 status code (HTTP) 384  
354 code (SMTP) 297  
401 status code (HTTP) 386  
802.x standards 55, 493  
*1984* (novel) 727
- A records (DNS) 192, 219  
A tags (HTML) 355  
access control 544  
ACK flag (TCP) 274  
acknowledgements (TCP) 263  
ACL (access control list, Windows) 544  
Active Directory 186, 204, 205, 228, 438, 460, 468, 581  
Active Server Pages *see* ASP  
ActiveX programs 394
- adapter status, NetBIOS 495  
ADDALTCOMP (Browstat) 824  
address classes *see* IP addresses  
Address Resolution Protocol *see* ARP  
ADSL 608, 627  
advertisements, filtering 653–4  
aggressive mode (IKE, VPN) 703  
AH (Authentication Header, VPN) 694  
ALG *see* application-level gateways  
aliases (DNS) 195  
“always on” access 598, 663  
AND operator (Netmon) 481  
ANNOUNCE (Browstat) 825  
announcements, Windows browsing 558, 569  
anti-virus scanning 652  
ANY GROUP address (Netmon) 482, 491  
APIPA (Automatic Private IP Addressing) 110  
<applet> tag (HTML) 394  
application layer 405, 724  
application-level gateways (ALG) 634–5  
APT (Advanced Package Tool, Debian) 389  
ARC4 encryption 694  
“areas” (of IETF working groups) 728  
ARP (Address Resolution Protocol) 34–7, 56, 74–5  
    bridging 647  
ARPANET 110  
ASCII, commands sent in 273, 294–5, 302–3, 326–7,  
    358–9, 434–5, 359  
ASN.1 (Abstract Syntax Notation 1) 461  
ASP (Active Server Pages) 375, 394  
AT modem commands 662, 678–9  
attachments to e-mail 319–21  
attack signatures 651  
audio and visual status indicators (DUN) 676  
authentication 386, 395, 446, 472, 536, 639  
authentication package (Windows) 528  
*authoritative* servers (DNS) 209, 220  
*authority* concept (DNS) 208  
**Authorization:** header (HTTP) 386–7  
automated keying (VPN) 702  
Automatic Private IP Addressing *see* APIPA  
auto-negotiation, hubs/switches 732  
Avian Carriers 56

- b-node 512, 514, 819
- Back** button in a browser 385
- “backbone” cable 731
- “backdoors”
  - around firewalls 640
  - around security systems 490
- backup browsers (WN) 557, 566
- backup Internet connections 598
- backup domain controller *see* BDC
- backup mail servers 291
- bandwidth 281, 599, 655
- banner advertisements 653, 659
- base64 encoding 320, 324, 386, 395, 792–3
- Basic-type authentication (HTTP) 386
- bcc (blind carbon copy) 298
- BDC (backup domain controller) 525, 546–7
- Bellovin, Steven 464
- Berferd 646
- Berkeley sockets 281
- Best Current Practice RFCs 726
- “best effort” systems and protocols 33, 260, 399
- BGP (Border Gateway Protocol) 135
- Bigfoot 442
- BIND (Berkeley Internet Name Domain) 240–1
- bind** nameserver 203
- bindings (WN) 471, 477, 688
- blackholes.mail-abuse.org** 657
- BOG (Basic Operations Guide, **bind**) 240
- Bootstrap Protocol (BOOTP) 412, 423
- bounced e-mail messages 309
- boundary delimiters (e-mail) 320
- boundary=** parameter (MIME) 323
- BREAK (Browstat) 826
- broadcast addresses 104–5, 111, 517, 766, 770
- broadcast media 663
- broadcast name resolution (WN) 472, 499
- broadcast node 512
- broadcast packets 34, 471, 494–5
- broadcast storms 105
- browse election (WN) 568
- browse lists (WN) 557, 562, 575
- browse masters (WN) 557
- BROWSER protocol (WN) 558
- browser servers, locating of (WN) 560–1
- browser service (WN) 556
- browsing (WN) 588
  - definitions of 473, 556
  - problems with 579
  - in several domains 564–5
  - temporary inconsistencies 572
  - and VPN 709
  - white paper on 578, 581
  - see also* Web browsers
- browsing a packet list 339
- BROWSTAT command 824–7
- Brutus** 659
- BSD Packet Filter 25
- BSD sockets 281
- bugs in software 58
- building blocks of TCP/IP 8
- bulletin boards 270
- “bump in the stack” (BITS, VPN) 693
- “bump in the wire” (BITW, VPN) 693
- bus networks 16
- bus topology 731
- cable modems 608
- cabling 40–3, 70–1, 613, 776–7
- cached account information 533
- cached credentials 532, 549
- caching 378
  - in DNS 224–5
  - in Web browsers 378, 384–5, 394
  - see also* NetBIOS: name cache
- caching servers (DNS) 224
- caching-only servers (DNS) 224, 226
- cacls** command 584
- .cap files 487
- Capture > Filter (Netmon) 688
- “Capture child process died” error 334
- capture files 334, 345, 486–7
- capture filters 480, 482
- cardctl**, PCMCIA 774
- carrier pigeons 56
- catch-all security rules 629
- ccTLDs 208
- CDE (Common Desktop Environment) 437
- Centrex 684
- CERT 241, 645
- CGI programs 375
- CGI scripts 375
- challenge/response 536, 538
- character generator *see* **chargen**
- character-based browsers 357
- chargen** service 426, 476
- charset** parameter (MIME) 323
- chat 652
- checksums, UDP 399, 401
- chess, analogy with 4
- Cheswick, William 464
- CIDR (Classless Inter-Domain Routing) 91, 109–11, 179
  - notation 801
- CIFS (Common Interface File System) 490
- circuit-switching networks 10
- Classes A, B, C, D and E (IP addresses) 88
- Classless Inter-Domain Routing *see* CIDR
- client access license (CAL) 593
- client-to-client configuration (VPN) 693
- Client for Microsoft Networks 582
- client-to-site VPN 693
- CNAME records (DNS) 194
- coaxial cabling 17

- Code Red 627, 645, 650, 716
- collision domains 735
- Colorize Display (etherreal) 342
- .com domain and .com zone 210
- COM1 Properties 678
- Comer, Doug xviii
- command-line tools xvii
- Comment field in Windows Explorer 563
- Common Gateway Interface *see* CGI
- common names (LDAP) 440
- community string (SNMP) 446
- compression in software (DUN) 671–2
- computer account (WN) 534–5, 537
- concurrent servers 808
- congestion control (TCP) 281
- Connect As 543
- “connect failed” error message 81, 278
- connection, *direct* or *local* 60
- connection-oriented protocols 261
- “connection refused” error message 278
- connectionless transmission 261, 399
- connectoids, Windows 9x 689
- Content-Description header (MIME) 324
- Content-Disposition header (MIME) 325
- content filtering 653
- Content-Transfer-Encoding header (MIME) 324
- contingency planning 617
- Control Panel > Hardware profile 683
- Control Panel > Modems 666–7
- Control Panel > Network 44
- Control Panel > Network > Services 427, 502, 813
- Control Panel > RAS > Properties 669
- Control Panel > Service 476
- Control Panel > Service > Bindings 477
- control port (FTP) 428
- corrupted packets 399, 401
- country code top-level domains *see* ccTLDs
- cr.yy.to (Web site) 240
- credentials (WN) 551
- cross-over cabling (UTP) 41, 71, 734, 776
- cryptography 715
- Ctrl-Alt-Del 526, 530, 538, 814
- The Cuckoo’s Egg* 646
  
- daemons 808
- DATA (by e-mail) 297
- data port (FTP) 428
- data transfer process (FTP) 429
- database synchronization (WN) 547
- datagrams 398
- daytime 426, 476, 614, 641, 813
- DB9 serial cable connector 777
- DB25 serial cable connector 777
- DCE endpoint locator 474
- DCHP 769
- dead gateways, detection of 146
  
- Debian Linux xvii, 766
- DEBUG (Browstat) 825
- debugging 4–5, 642
  - output for failed name resolution 248–9
  - See also* Troubleshooting
- DEC Pathworks 470
- DECnet 470
- dedicated servers 373
- default gateways 64
  - allocation of addresses 612
  - creating routes for 128–9
  - for dial-up 680
  - error reporting 80–1
  - made permanent 69
  - multiple 130–1, 146
  - not belonging to a configured interface 67
  - not specific to an interface 131
  - on remote networks 672
  - setting on Linux 68–9
  - setting on Windows 66–7
- default.ida 650
- delegation (DNS) 212–19
  - concept of 208
  - at different levels 213
- delegation entries 212
- demilitarized zone (DMZ) 223, 229, 551, 599, 636, 650;
  - see also* DMZ ports; DMZ servers
- demultiplexing 267, 398, 402–3
- DEN (Directory-Enabled Network) 439, 461
- denial of service (DoS) attacks 632
- “deny” rules 629
- Department of Defense 725
- DES encryption 694, 698
- “destination host unreachable” error message 64, 81
- destination ports 265, 402
- \\Device\Packet 75
- dhclient 418, 769, 774–5
- DHCP (Dynamic Host Configuration Protocol) 179, 401
  - configuration 416–19, 773
  - implementations 424
  - leases 414–19
  - link with DNS 424
  - motivation 410–11
  - relay 420
  - servers 424, 639
  - troubleshooting 417
  - working of 412–15
- DHCP Failover Protocol 424
- DHCPACK 412
- dhcpcd 416, 774
- DHCPDISCOVERY 412
- DHCPOFFER 412, 414
- DHCPREQUEST 412
- diagnostic techniques *see* Troubleshooting
- Dialing Properties 667
- dial-up accounts 666

- dial-up networking 662–79
  - error numbers 679
  - on Linux 688
  - monitoring of connection status 676
  - problems with 618
  - testing 613, 685
  - troubleshooting 678–9, 687
  - on Windows 9x 689
- Dial-Up Networking Monitor 676–89
- dial-up VPN, protection of 706
- Diffie-Hellman key agreement method 703
- dig** (domain information groper) 205
- digital certificates 388
- direct serial cable 684–5
- directly-connected networks
  - creating routes for 128–9
  - netmasks for 30–1
- directories, definition of (LDAP) 440
- Directory Access Protocol (DAP) 438
- directory information tree (DIT, LDAP) 440
- Directory-Enabled Network *see* DEN
- “disable all” (Netmon) 485
- discard** service 426, 476
- discovery of domain controller 532
- disinfecting viruses 652
- display filters (Netmon) 484, 801
- display filters (**ethereal**) 340–1, 343
- display server (X window system) 436
- distinguished name* (DN) 440
- Distributed Management Task Force (DMTF) 439
- DIX Ethernet 491
- DMZ *see* demilitarized zone
- DMZ ports 638
- DMZ servers 637
- DNR (domain name resolver) 242
- DNS (domain name system) 182, 614, 624
  - configuration 54
  - caching 224–5, 507
  - concepts 183
  - configuration 186–91, 228–35
  - contents 194–5
  - and DHCP 424
  - distributed nature of database 208–9
  - dynamic 622
  - e-mail filtering 657
  - and **ethereal** 203
  - glossary 237
  - identifier field 197
  - internal motivation 228
  - interrogation of 192–3, 198–200
  - names 191, 494, 496, 513
  - and NetBIOS name resolution order 818–20
  - packet flow 216–17
  - packet formats 196–7
  - packet tracing 214–15
  - port numbers 182, 243
  - primary and secondary configuring servers 241
  - problems and causes 250–1
  - query types 195
  - resolving of names 184–5
  - server addresses 672
  - Service Search Order 190
  - servers 184, 222–4, 637
  - settings 773
  - tcpdump** output 196–7
  - troubleshooting 246–7
  - used as NetBIOS name server 506–7
  - using WINS on Windows 522
  - and Windows 2000 241
- DNS Planning* 242
- DNS\_1 and DNS\_2 773
- DNS.EXE process 240
- document root directory (HTTP) 374
- domain
  - computer added to (WN) 534
  - definition of 207, 524
  - Windows *see* NT-domain
- Domain Announcement (WN) 573
- domain controller (DC) 439, 525, 532–3, 536, 546–7, 557
  - and dial-up 682
- Domain and Domain Suffix Search Order (DNS) 242
- Domain Enum** (WN) 573
- Domain Manager (WN) 537
- domain master browser (WN) 566, 572
- Domain Monitor (WN) 537
- domain name resolver (DNS) 821
- domain name system *see* DNS
- domain names (DNS) 206–7
  - definition of 207
  - setting of 232–3
- Domain Suffix Search Order (DNS) 235, 506
- domainname<1d>* and *<1b>* 560, 566–8, 571–3, 581
- domainname<1e>* 567–8
- domainname<20>* 562
- domains
  - compared with zones (DNS) 211
  - learning from other domains (WN) 573
  - tree structure (DNS) 206
  - Windows Networking 472
- dommon** (WN) 537, 547
- dots in searchlist queries 235
- dotted decimal notation 29
- “down” keyword, **interfaces** file 768
- Draft Standard RFCs 729
- dropped packets 262, 399
- DUL (Dial-Up List) 657, 659
- dumb-terminal browsers 357
- dumb terminals 270
- DUMPNET (Browstat) 826
- DUN *see* Dial-up Networking
- duplicate packets 262
- dynamic addresses used by ISPs 420–1

- dynamic DNS 424, 622
- Dynamic Host Configuration Protocol *see* DHCP
- dynamic IP addresses 410, 605, 608
- dynamic Web pages 375, 393–4
  
- echo** service 426, 475
- eDirectory (Novell) 439, 461
- egrep** 349
- EHLO SMTP command 296–7, 316
- Einstein, Albert 469
- ELECT (Browstat) 827
- election (WN)
  - criteria for 568
  - Force 569, 671
  - tracing of 570–1
- e-mail
  - addresses found using LDAP 442
  - filtering 657
  - headers 298–301
  - log files 310–11
  - non-text messages 318–19
  - open relays 656
  - receipt of 310
  - security 312, 316
  - servers, internal 637
  - troubleshooting 308
  - viruses 652
  - Web-based 308, 329
  - see also* attachments; SMTP; MIME
- Encapsulating Security Payload (ESP, VPN) 713
- encapsulation 33, 699, 804
- encryption 692, 694
- end-to-end protocols 261
- enterprises** subtree (SNMP) 445
- Entire Network (WN) 587
- entries* in LDAP directories 440
- “enumerate servers” request (WN) 562
- envelope (SMTP) 296–7
- ephemeral ports 266, 402, 455
- equal cost multipath routing 146
- error 720 (WN) 490
- error 2550 (WN) 582
- error reporting from a LAN PC 80–1
- errors, deliberate 51
- escape characters, **telnet** 282
- ESMTP (extended SMTP) 316
- ESP (Encapsulating Security Payload, VPN) 694
- /etc/dhclient.conf* 419
- /etc/dhcpd.conf* 419
- /etc/dhcpd/config* 769
- /etc/ethers* 137, 157, 423
- /etc/exports* 454
- /etc/hostname* 769
- /etc/hosts* 253, 769
- /etc/hosts.allow* 659
- /etc/hosts.deny* 659
- /etc/inetd.conf* 427, 811
- /etc/init.d/network* 774
- /etc/modules* 767
- /etc/network/interfaces* 419, 768–770
- /etc/network/options* 766
- /etc/networks* 145, 241
- /etc/nsswitch.conf* 769
- /etc/passwd* 529
- /etc/pcmcia/network* 770
- /etc/pump.conf* 419
- /etc/resolv.conf* 188, 255, 768
- /etc/services* 279, 400, 402, 427, 458, 810–11
- /etc/shadow* 529
- eth0** interface 48, 156
- eth0:1** and **eth0:2** 768
- eth1** and **eth2** 767
- eth1:2** and **eth0:3** 772
- etherreal** 203, 334–5
  - compared with Network Monitor 478
  - on dial-up connections 687
  - display filters 340–1
  - example session 338–9
  - exchanging capture files 487
  - features and options 342–3
  - field names 798–801
  - installation 798
  - selection of packets 336–7
  - tips and tricks 344–5
  - versions 344
- Etherfind** 26
- Ethernet 16–17, 32–5, 55
  - addresses 32–5; *see also* MAC addresses
  - bridges 733
  - broadcasts 34
  - eth0** and **lo** interfaces 48
  - hubs and switches 731–5
  - and Network Monitor 487
  - packet type 800 (IP) 33
  - packet type 806 (ARP) 35
  - payload 32–3
  - repeater 732
  - transceivers 731
  - transmission of data 32–3
  - types of 17, 480
  - see also* Thick Ethernet; Thin Net; UTP
- ETRN command (SMTP) 292, 316
- ETYPE (Netmon) 491
- Eudora 442
- event IDs, Windows 553, 588
- Event Viewer, Windows 590
- Exim** mail server 315
- experimental** subtree (SNMP) 445
- Expires:** (HTTP response header) 365, 374
  
- FAT files 545
- File and Print Sharing 582
- File Transfer Protocol *see* FTP
- filehandles (NFS) 453, 455

- filtering attachment types 653
- filtering of e-mail 657
- FIN flag (TCP) 277
- Find > Computer 576–7
- FINDMASTER (Browstat) 825
- finger** service 458
- firewalls 431, 551, 607, 615, 626–45, 693
  - added to existing live networks 651
  - choice of 638
  - definition of 626
  - hybrid 635
  - implementation of 640–1
  - internal 646
  - motivation for 627
  - operation of 628–31
  - packet-filtering 628
  - troubleshooting 642
- Flack, Marjorie 57
- flags in routing tables 117, 134–5
- flags: rd** (recursion desired, DNS) 219
- Follow TCP stream (**ethereal**) 345
- FORCEANNOUNCE (Browstat) 825
- forged e-mail messages 312
- fork** system call 808, 811
- Forward** button in a browser 385
- forwarders, purpose of (DNS) 228–9
- forwarding IP packets 61–3
- Fport** tool, like **netstat** 407
- FQDN (fully-qualified domain name) 207, 248, 293, 820
- frames 55
- FreeS/WAN project 713
- From: (e-mail header) 298
- FTP (File Transfer Protocol) 428–9
  - active* and *passive* modes 431, 434–5
  - establishment of connections 430–1
  - example session 434–5
  - viruses 652
- full requests (HTTP) 362
- full-duplex switches 42
- fully-qualified domain name *see* FQDN
- “Gateway” implementation, VPN 693
- GD** option (**winscl.exe**) 573
- generic top-level domains *see* gTLDs
- Genmask 116
- GET command (HTTP) 358, 391
- GetBackupList** (WN) 561–2, 566
- GETBLIST (Browstat) 827
- GETDOMAIN (Browstat) 824
- getif** SNMP tool 462
- GETMASTER (Browstat) 827
- GETNETBIOS (Browstat) 824
- get.get-next** (SNMP) 462
- GETPDC (Browstat) 826
- GETWINS (Browstat) 824
- GIF, disabling animation of 653
- GNOME 437
- Gnutella 490
- Google search engine *xix*
- GPS (Global Positioning System) 451
- Grant dialin permission to user (DUN) 682
- grep** 345
- group addresses (Netmon) 482
- group name registration (WN) 499
- group names (WN), 472, 497, 815
- “group” in MAC addresses 491
- groups of users (WN) 547
- gTLDs 208
- Guest account (WN) 545, 594
- GUI-based tools *xvii*
- H.323 602
- h-node (NetBIOS) 512, 514, 819
- hacking 627, 646
- “hand symbols” in Windows Explorer 584
- Hang Up (DUN) 674
- hardening of operating systems 639
- hardware packets *see* frames
- hardware problems 58
- hardware profiles, Windows 683
- hashed passwords 529, 538, 544
- Hayes modem commands 678
- header fields, IP packets 33
- header lines (e-mail) 298
- Helminthiasis of the Internet* 283
- HELO command (SMTP) 297
- Hess, Joey 807
- “Hide file extension for known file types” 508, 510
- high-availability firewalls 638
- Historic RFCs 726
- history mechanism in Web browser 385
- Hobbit, the 807
- home pages, Web 374
- hop count, IP routing 76
- hop-by-hop communication 28
- host address component of a URL 372–3
- host** command 192–5
- Host: header (HTTP) 364, 367
- host-to-host layer 724–5
- host IDs in IP addresses 180
- host** manpage summary 788–91
- host** options 221, 225
- “host unreachable” error message 81
- hostname 232–3, 769, 818
- hosts
  - definition of 148
  - see also* **hosts** file
- hosts\_access(5)** 660
- hosts** file 239, 252–3, 508, 510–11, 589, 659
- Hotmail 308, 389
- HTML (HyperText Markup Language) 355, 359
- HTTP (Hypertext Transfer Protocol) 354–5, 359, 366–7

- binary data not encoded 368
- example session 358–9
- history 393
- and MIME 368–9
- persistent connections 360, 370–1
- protocol 393
- requests and response headers 362–5
- security 386–7
- troubleshooting connections 390–1
- used instead of FTP 428
- versions of 360–1
- HTTP/1.1 server response codes 802–3
- “hub and spoke” routing 716, 731
- hubs 17, 40–3, 731–5
  - dual-speed 735
  - stackable 735
  - see also* Ethernet; switches
- hum 729
- HUP signal 427, 813
- hybrid node (NetBIOS) *see* h-node
- HyperTerminal** 270, 678
- HyperText Markup Language *see* HTML
- Hypertext Transfer Protocol *see* HTTP
  
- ICMP (Internet Control Message Protocol) 38
  - “host unreachable” error message 64, 81
  - source quench* messages 281
  - time exceeded 76
- ICMP redirects 132–7, 146–7, 153
- identification of networks 86–7
- IDs for networks, sub-nets and hosts 180
- IEEE (Institute of Electrical and Electronic Engineers) 32
  - networking standards 55
- IEEE 802.x *see* 802.x standards
- IESG *see* Internet Engineering Steering Group
- IETF 716, 728
- If-Modified-Since: header (HTTP) 374
- IF\_PORT, PCMCIA 770
- ifconfig** 48–9, 57–8
  - options 72, 156
  - in routing tables 128
- ifup** 769
- IKE 695, 702–3, 713–14
  - problems with 709
- ILLEGAL (Browstat) 825
- IMAP (Internet Message Access Protocol) 326–7
  - example session 796
  - motivation for 326
- IMG tag (HTML) 355
- Import LMHOSTS** 510
- in.named** process 240
- individual names (NetBIOS) 815
- inetd** 660, 811
- inode number 453
- in-office-on-Ethernet** 683
- instance values (SNMP) 447
  
- instant messaging 654
- Institute of Electrical and Electronic Engineers *see* IEEE
- integers, specification of (**etereal**) 801
- inter-networks 8, 70
- interactive logon (WN) 540
- interdomain trust accounts (WN) 547
- interfaces
  - multiple 83
  - netmasks specific to 99
  - speed of 639
  - see also* Ethernet: **eth0** and **lo** interfaces
- interfaces** file *see* **/etc/network/interfaces**
- intermediate routers 20
- intermittent connection 292, 663
- internal addresses, mapping of 601
- internal firewalls 715
- internal names, DNS servers for 228
- internal servers 616, 637
- Internet connection
  - alternatives 618
  - back-up 620–1
  - cost 599
  - testing of 828–9
- Internet Connection Sharing (ICS) 618, 684
- Internet Control Message Protocol *see* ICMP
- Internet daemon *see* **inetd**, **xinetd**
- Internet drafts RFCs 728
- Internet Engineering Steering Group (IESG) 728
- Internet Engineering Task Force (IETF) 728
- Internet Explorer 246, 380–1, 385
- Internet group names (NetBIOS) 815
- Internet group type (WN) 497
- Internet history 12
- Internet Key Exchange (VPN) 695
- Internet layer 725
- Internet Message Access Protocol *see* IMAP
- Internet Research Task Force (IRTF) 730
- Internet Security Association and Key Management Protocol *see* ISAKMP
- Internet service provider (ISP)
  - changing 624
  - choice of 606
  - compared with direct dial-up 663
  - mail servers at 287
  - phone numbers 670
  - relay backup by 291
  - use of dynamic addresses 420–1
- Internet standards 726–30
- Interplanetary Internet 730
- intrusion detection systems (IDSs) 651, 658
- IP (internet protocol) 8
- IP addresses 28–31, 49
  - allocation of 415, 612
  - calculation of ranges 100–1
  - checking of 44
  - classes of 88–91

- IP addresses (Continued)
  - configuration of 768
  - dynamic and static 410, 598, 605, 608, 672
  - fixed 672
  - multiple 154–7
  - network part* and *host part* of 88
  - of networks 106
  - ranges and range sizes of 92–5
  - setting on Linux 48
  - setting on Windows 44–5
  - specification of 801
  - troubleshooting 140
  - uniqueness of 29
- IP aliasing 57, 178
- IP forwarding 71, 711, 767
- IP header compression 672
- IP layer 723
- IP masquerading *see* NAT
- IP Next Generation (version 6) 110
- IP numbers
  - for small self-configured networks 103
  - for use in documentation 102–3
  - special 102–7
- IP protocol numbers 701, 804
- IP ranges and netmasks 164
- IP routing *see* routers; routing
- IP security protocol *see* IPsec
- IPADDR 770, 774
- ipconfig** 46, 66–7, 155, 416
- ipconfig/all** node type 512
- ipconfig/displaydns** 506
- iPlanet 439
- IProute2 146
- IPsec (IP security protocol) 694, 698, 709
  - see also* VPN
- IPX 640
- IRQ setting 58
- ISAKMP (Internet Security Association and Key Management Protocol) 703, 713
- ISDN 608, 662
- ISO-8859-1 parameter (MIME) 323
- ISP *see* Internet service provider
- iterative queries (DNS) 218–19
- iterative servers 808
  
- Java 394
- JavaScript 394, 653
- JSPNRMPTGSBSSDIR 817
- junk e-mail *see* spam
- Just Fast Keying (JFK) 714
  
- Kaufman, Charlie xviii
- KaZaA 490
- KDE 437
- key lifetime (VPN) 703
- key management (VPN) 694
- keywords, filtering of 653
- kill -HUP 813
  
- L0phtcrack 659
- LAN 612
- LAN Manager 470, 529
- LAN Server 470
- LAN test networks 158–9
- LAST command (POP3) 303
- Last-Modified: (HTTP response header) 365
- layer-1, layer-2 and layer-3 switches 735
- Layer 2 Tunneling Protocol (L2TP) 714
- layers 8–9, 724
- <1c> group-name 534
- <1c> group 511
- LDAP (Lightweight Directory Access Protocol) 438–9, 460, 707
  - directories and databases 440–1
  - referrals 441
  - replication 441
  - used to find e-mail addresses 442
- LDAP Data Interchange Format (LDIF) 441
- learning bridges 733
- leased lines 610
- leases *see* DHCP
- “Leave message on server” (POP3) 303
- libcap** 24–5, 350, 487
- licensing of networks 593
- lifetime of NetBIOS cache entries 508, 509, 511
- Lightweight Directory Access Protocol *see* LDAP
- limited broadcast address 104
- “lineprinter” 449
- “link” indicator lights 40
- link integrity 732
- link layer 404, 722
- link layer encryption 694
- link numbers 180
- Linux
  - Debian xvii
  - Documentation Project xix
  - Red-Hat xvii
- Linux Advanced Routing 146
- listening* for connection requests 264, 267–8
- LISTWFWD 826
- LM authentication 538
- LM challenge/response 538
- Lmhosts** 239, 252, 510–11, 549, 572, 584, 589, 682, 709, 819
- Lmshvc.exe** 813
- lo interface 48
- load balancing 372
- Local Echo, **telnet** 272
- local logon (WLN) 528–9
- Local Security Authority *see* LSA
- localhost** 508
- LOCALLIST (Browstat) 825
- lockd** 464
- log files (e-mail) 310–11
- logger** tool 448

- logging to a file (DUN) 667
- loghost** (syslog) 448
- logical operators (**etherreal**) 800
- logon (DUN) 682, 689
- logon (WN)
  - and access to network resources 544–5
  - to a different domain 540
  - encryption of traffic 531
  - over a network 530–9
  - types 540–3, 551
- logon messages (WN) 527, 533
- logon** process (WN) 526
- logon prompt 526–7
- logon servers (WN) 546
- logs (NT) 590
- Lone Ranger mask 92
- loopback address 107
- Lotus 286, 490
- LPR printing 449
- lpr** system 462
- LSA (Local Security Authority) 528, 539, 544
- LSASS.EXE** 528
- lynx** browser 357, 388–9
  
- m-node 512, 515, 819
- MAC addresses 32
  - allocated to manufacturers by IEEE 32, 55
  - and IP forwarding 62
  - names used instead of 137
  - see also* Ethernet addresses
- machine names xxi
- machines, definition of 148
- mail-abuse.org** 657
- MAIL FROM (SMTP) 297
- mail headers *see* e-mail headers
- mail servers
  - backup relays 291
  - locating of 288–9
  - vulnerability of 650
- mail systems 328–9; *see also* e-mail
- mailbox servers 302, 315
- main mode (IKE, VPN) 703
- malicious requests 650
- managed hubs 735
- managed objects (SNMP) 444
- managed switches 17, 43
- management stations (SNMP) 444
- man-in-the-middle attacks 694
- manual address allocation (DHCP) 415
- manual keying (VPN) 695–8
- Map Network Drive (WN) 575
- mapping
  - of IP addresses 605
  - of a network drive 545
  - of networks 640
- MAPS (Mail Abuse Prevention System) 656
  
- “Martian” packets 110
- masquerading *see* NAT
- master browsers (WN) 557
- master servers (DNS) 220
- MASTERANNOUNCE (Browstat) 825
- MASTERNAME (Browstat) 826
- MD5 697–8
- Media Access Control (MAC) addresses *see* MAC addresses
- message stores, e-mail 315
- message transfer agents (MTAs) 315
- message user agents (MUAs) 315
- mget** command 459
- mgmt subtree (SNMP) 445
- MIB (Management Information Base) 445
- Microsoft Authentication Package 528
- Microsoft Exchange 286, 328
- Microsoft Knowledgebase xix, 489
  - see also* MS-KB-\*
- Microsoft Operations Manager 350
- Microsoft Resource Kits xviii
- Microsoft TechNet 489
- Microsoft Windows Network 587
- Mills, David 461
- MIME (Multipurpose Internet Mail Extension) 299, 319
  - attachments, nested 794–5
  - headers 322–5
  - and HTTP 368–9
  - optional parameters 323
- mimencode** 395
- minus (–) sign (**tcpdump**) 219
- missing packets 262
- mixed* node (NetBIOS) *see* m-node
- modem log files 679
- modem properties 673
- modem speakers 667, 670
- ModemDet.txt** 679
- ModemLogmodemnames.txt** 679
- modems
  - combined with routers 618
  - configuration 667–9
  - on firewalls 640
  - installation 666
  - troubleshooting 678, 687
- Morris Internet worm 283
- Motif 437
- mountd** daemon 454
- MP3 654
- MS-KB-Q102716 549
- MS-KB-Q102878 582
- MS-KB-Q102908 82
- MS-KB-Q106211 552
- MS-KB-Q119495 519
- MS-KB-Q119495 817
- MS-KB-Q120642 146
- MS-KB-Q121004 519
- MS-KB-Q121005 423

- MS-KB-Q121005 519
- MS-KB-Q122422 550
- MS-KB-Q126449 594
- MS-KB-Q137565 820
- MS-KB-Q139270 519, 821
- MS-KB-Q140064 519
- MS-KB-Q140064 817
- MS-KB-142309 821
- MS-KB-Q147706 550
- MS-KB-Q149664 550
- MS-KB-Q150518 550
- MS-KB-Q150737 519
- MS-KB-Q150820 817
- MS-KB-Q151795 82
- MS-KB-Q158148 550
- MS-KB-Q160177 519
- MS-KB-Q160177 519
- MS-KB-Q160699 424
- MS-KB-Q161431 820
- MS-KB-Q163409 519
- MS-KB-Q163409 817
- MS-KB-Q163949 519
- MS-KB-Q164765 519
- MS-KB-Q167248 550
- MS-KB-Q167640 519
- MS-KB-Q168076 519
- MS-KB-Q168821 580
- MS-KB-Q171564 146
- MS-KB-Q171567 519
- MS-KB-Q172218 519
- MS-KB-Q172218 820
- MS-KB-Q172227 623
- MS-KB-Q172931 549
- MS-KB-Q173199 552
- MS-KB-Q173525 519
- MS-KB-Q173882 550
- MS-KB-Q173941 519
- MS-KB-Q175024 550
- MS-KB-Q180094 550
- MS-KB-Q181171 519
- MS-KB-Q181171 550
- MS-KB-Q183859 550
- MS-KB-Q185786 519
- MS-KB-Q187709 519
- MS-KB-Q187742 423
- MS-KB-Q188305 582
- MS-KB-Q193819 424
- MS-KB-Q195611 242
- MS-KB-Q195686 147
- MS-KB-Q198550 242, 821
- MS-KB-Q198550 519
- MS-KB-Q201535 394
- MS-KB-Q214467 242
- MS-KB-Q220874 110
- MS-KB-Q227410 241
- MS-KB-Q230744 242
- MS-KB-Q230744 519, 821
- MS-KB-Q234815 624
- MS-KB-Q236901 519
- MS-KB-Q259240 645
- MS-KB-Q262655 550
- MS-KB-Q263070 394
- MS-KB-Q266729 550
- MS-KB-Q314104 519
- MS-KB-Q314108 549
- MS-Outlook 389
- MSBROWSE 573, 591, 816
- MSV1\_0 528, 530, 544, 549
- MTAs, message transfer agent 317
- MUA, message user agent 317
- multi-boot 780
- multicasting 106, 111, 474
- multiple DMZ ports 638
- multiple networks
  - configuration of 771
  - on one wire 154–7
- multiple routers 150–3
- multiplexed NetBIOS sessions 475
- Multipurpose Internet Mail Extension *see* MIME
- Muuss, Mike 57
- MX records 195, 288–93, 652
  - for subdomains 293
- name claim *see* name registration
- name discovery (WN) 518
- name query (WN) 499
- name registration (WN) 498–9
- name resolution (WN) 494–5, 507, 519, 588
  - order of (WN) 513, 521
  - systems, DNS and other 252
  - troubleshooting (WN) 516–17
- name service switch 769
- name table (WN) 495
- name=** parameter (MIME) 323
- named** process 240
- nameserver** keyword, DNS resolver 188
- Napster 490
- NAT (Network Address Translation) 600–11, 623, 638, 693, 696, 699
  - benefits of 600
  - configuring 612
  - default gateways 601
  - dynamic IP addresses 605
  - need for 608
  - NetBIOS 602
  - one-to-one 605, 779
  - problems with 602
  - public servers 605
  - renumbering a network 603
  - security 602
  - static 605
  - and VPN 602
  - working of 601

- nbstat** 475, 512, 519, 591, 817
  - options 497, 510–11
- NBT** *see* **NetBT** 471
- NdisWan** adapters 688
- NDS** (Novell Directory Services) 439
- Nemeth, Evi** xix
- Nessus** 659
- net help** 475
- net helpmsg** 475
- net share** 584
- net time** 464
- net use** 454, 513, 543, 583, 681
- net view** 496, 517, 556, 563–4, 574, 578
- NetBEUI** 470, 490, 517, 579, 589, 640
- NetBIOS** 404, 470, 472–3, 490, 538, 557, 588, 640
  - caching 507–10, 521
  - default node type 513
  - name resolution 252, 499, 682, 818–21
  - name server 500–1
  - names 494–7, 815–17
    - and NAT 602
  - node types 512–13, 521
    - over TCP/IP 471
    - and VPN 709
  - see also* name registration; Windows Net-working
- NetBIOS Datagram Distribution (NBDD)** 489
- NetBIOS Extended User Interface** 490
- NetBIOS Interface** service 490
- NetBIOS Protocol** 519
- NetBIOS Session Service (NBSS)** 475, 531, 562
  - multiplexed over TCP 475
- NetBIOS suffix** 496, 503, 506, 511, 815
- NetBT** 471
  - Destination Name in packet 558
  - messages 23
  - see also* **NetBIOS**
- netcat** 282, 432–3, 641
  - manpage 805–7
  - for troubleshooting UDP 407
  - as TCP client or server 432–3, 435
    - u option 448
  - as UDP client or server 433
- netdom** 537, 542, 545
- Netlogon** 526, 530–1, 534, 539, 623
- Netlogon channel, secure** 536
- netmasks** 28, 109
  - 255.0.0.0 94
  - 255.255.255.0 and 255.255.0.0 30, 92–3
  - and address classes 90–1
  - calculations 100–1, 108–9
  - checking of 44
  - and CIDR 91
  - compared with sub-net masks 87, 109
  - for directly-connected networks 30–1
  - examples of use of 98–9
  - and IP address ranges 94–5, 164
  - Lone Ranger type 92
  - multiple 98
  - reasons for use of 86–7
  - semiconductor mask analogy 92
  - specific to interfaces 99
  - specifying ranges of IP addresses 92–3
  - stored on machines 31
  - table of 96–7
  - troubleshooting 140–1
- NetMeeting** 602
- Netmon** *see* **Network Monitor**
- Netmon Agent Service** 486
- Netscape** 287, 301, 306, 382–3, 439, 442
- NetServerEnum2** 562, 564, 566–7
- netstat** 268–9, 278, 402, 407, 430
- netstat** service 458
- network access layer** 725
- network address and port translation (NAPT)** 604
- Network Address Translation** *see* **NAT**
- network addresses** 102, 110
- network card, broken** 684
- network cards, configuring of** 72–3
- network diagrams** 779
- network-directed broadcast address** 104, 111
- Network-disabled hardware profile** 683
- network drive mapping** 583
- network elements (SNMP)** 444
- Network File System** *see* **NFS** network IDs 180
- network interface card (NIC)** 16
- Network Intrusion Detection systems (IDSs)** 651
- network layer** 404, 723
- network logon** 530
- Network Monitor** 475, 478–87
  - compared with **ethernet** and **tcpdump** 487
  - tips 486
  - tutorial 491
- Network Monitor Agent** 478
- Network Neighborhood** 496, 556, 574, 587
- network port translation (NPT)** 604
- network range, different sizes of** 94–5
- network reference models** 722–5
- network services, control of** 808–14
- network size and IP address classes** 88
- Network Time Protocol** *see* **NTP**
- “network unreachable” error 64, 69, 81
- network.opts** 773
- networks** file *see* **/etc/networks**
- networks compared with stand-alone machines** 6–7
- NFS (Network File System)** 401, 452–3, 464, 830
  - compared with **Windows Networking** 470
  - implementation 454–5
  - lock manager 464
  - mounting 454
  - sniffing 456–7
  - Version 4 407
- ngrep** 346–50
- NIC** *see* **network interface card**
- Nimda** worms 627, 645
- NIS (Network Information Service)** 253
- NIS+** 253

- nltest** 545 **nltest.exe /SC-QUERY** 537
- nltest.exe /SC-RESET** 537
- Nmap** 659
- nmblookup** 517, 591, 815
- NO CARRIER reply 679
- “no route to host” error message 81, 143
- node numbers (SNMP) 461
- node types, choice of 514–15; *see also* NetBIOS
- nodns** 775
- non-browsers (WN) 566
- nonce 538
- non-routable IP numbers 102
- Non-standards track RFCs 726
- normal group (NetBIOS) 497, 815
- notation *xx*
  - for routing 151
- Novell 404, 470
- Novell Directory Services (NDS) 461
- NS (name server) records (DNS) 195
- nslookup** 192–5, 198–9, 202–3, 248
  - manpage 781–7
  - TTL 227
  - v output 219
  - vc option 243
- NT – domains 524–5, 552
  - naming 549, 589
- NT FAQ 489
- NT Service Browser 574
- NT Services 476
- NTFS filesystems 545
- NTLM
  - challenge/response 538
  - hash 529
  - v2 538
- NTP (Network Time Protocol) 450–1, 463–4
- null-modem 685, 777
  
- Oakley groups 703
- object ID (OID, SNMP) 445
- <object> tag (HTML) 394
- /octet-stream (MIME) 322
- octets* 273
- OH** indicator 678
- on-site toolkit 780
- open relays 313
- OpenLook 437
- operating systems, hardening of 639
- “operation not supported by device” error message 69
- option numbers (DHCP) 413
- OR** operator (Netmon) 481
- ORBS (Open Relay Behavior-modification System) 657
- origin servers (HTTP) 376–8
- Orwell, George 727
- OSI
  - e-mail system 329
  - network reference model 8
    - seven-layer model 725
- OSPF (Open Shortest Path First) 135
- OTHERDOMAIN (Browstat) 824
- Outlook Express 287, 301, 307, 442, 794
  
- p-node (NetBIOS) 512, 514, 819
- P (push) flag (TCP) 275
- packet.dll** 350
- packet filtering 144
- packet sniffers 4–5, 16, 25–6, 343
- packet-switching 10
- packets 10–11
  - dropped 23
  - flow in DNS 216–17
  - forwarding of 61–3
  - selection of 20–1
  - tracing of 4–5, 74–5, 214–15
  - see also* frames
- parameter request lists (DHCP) 413
- parameters for networking 31
  - setting of 48–9, 72
- pass-through authentication (WN) 540
- passwords 528–9, 674
- PASV** command (FTP) 434–5
- patch cables, UTP 731
- pattern-recognition engines 652
- PCMCIA card 58, 666, 683, 770–3
- PDC (primary domain controller) 525, 546, 550, 566
- peer-to-peer networking 468, 490, 594
- penetration testing 651, 659
- perfect forward secrecy *see* PFS
- Perlman, Radia xviii
- Permissions 582
- “permit/deny” rules 629
- /persistent:yes drive mapping 585
- persistent connections 360, 370–1
- personal firewalls 707, 715
- PFS (perfect forward secrecy, VPN) 702
- PGP 694
- Phase 1 and Phase 2 exchanges (VPN) 703
- phonebook entries (DUN) 670, 673
- phonebook wizard (DUN) 671
- physical layer 722
- ping** 4
  - a option 57
  - applications 470
  - broadcast storms 105
  - command options 39
  - disabled 39, 766
  - firewall blocks 39
  - and NetBIOS 507
  - options 182
  - origin of name 38–9
  - story of 57
- pipeline requests (HTTP) 370
- plain-text commands *see* ASCII

- playboy.com 654
- plus (+) sign (DNS identifier) 197
- plus (+) sign (**tcpdump**) 219
- POP3 (Post Office Protocol, version 3) 286
  - configuration of servers settings 306–7
  - functions of server 302–3
  - and mail clients 316
  - messages retrieved by **telnet** 304–5
  - motivation for 302
  - ports 303
  - troubleshooting 310–11
- POPDOMAIN (Browstat) 824
- POPSERVER(Browstat) 824
- pop-up windows 653
- port address translation (PAT) 604
- PORT command (FTP) 430, 435
- port names 279, 810
- port numbers 182, 373, 804
  - link with UDP 402–3
  - specification of 480
- portmapper 454, 456, 474
- ports 264–5, 724
  - and security servers 278
- Post Office protocol, version 3 *see* POP3
- postal service, analogies with 11, 135, 262
- Postel, Jon 727
- potential browsers 566
- PPP (Point-to-Point Protocol) 624, 663, 686
  - settings 673
- PPP adapter **NdisWan4** 681
- PPTP (Point-to-Point Tunneling Protocol) 715
- preference values, DNS MX records 290
- primary domain controller *see* PDC
- primary servers, DNS 220–3
  - at ISPs 223
- primary servers, WINS 501
- printers 574
- private addresses 102, 110, 600
- private DNS servers 616
- private leased lines 176–7
- private** subtree (SNMP) 445
- /proc** pseudo-file 71
- process/application layer 725
- promiscuous mode 16, 478
- Proposed Standard 729
- protocol analyzers 334
- Protocol Hierarchy Statistics, **ethereal** 342
- protocol interpreter (PI) (FTP) 429
- protocol stack 404, 722–5
- protocols 8, 273
  - relationships between 404–5
  - proxies, use of 378–9, 394
    - application* and *application-level* 634
- Proxomitron 379, 384, 653
- Proxy ARP 56, 641, 647, 685
- proxy servers 650
- proxy systems, virus-scanning 652
- pseudo adapters (DUN) 688
- PTR records (DNS) 194
- public-key encryption 388
- public servers 599, 605, 616, 636–7
- pulist** (process and user list) 814
- pull partners (WINS) 505
- pump** 418, 769, 774
- pump.conf** 775
- push partners* (WINS) 505
- qotd** service 458
- “quarantine” 652
- QUIT command (SMTP) 299
- quoted-printable* input (MIME) 324
- r-commands 282
- RADIUS 706–7, 715
- RARP (Reverse ARP) 423
- RAS (Remote Access Service) 668, 684–8
- rasphone.exe** 669, 689
- RBL (Real-time Blackhole List) 656, 659
- rcode** (response code, DNS) 198
- RCPT TO (SMTP) 297, 313
- Rdr.sys** 476, 574
- read-only UTP cable 777
- read-uit.txt** 830
- reality TV 654
- realms 386
- reason phrases, HTTP codes 802
- Received: (e-mail header) 299–300
- Reconnect at Logon (WN) 585
- recursive queries (DNS) 220–1
- Red-Hat Linux xvii
- redirector (WN) 476
- redirects *see* ICMP redirects
- redundancy, mail servers 290
- reference clocks 451
- rekeying (VPN) 702
- relay backup (SMTP) 291
- relay servers (SMTP) 288
- relays, open (SMTP) 656
- reliable* and *unreliable* protocols 260
- reloading of NetBIOS cache 509
- remote* commands (**telnet**) 282
- remote login 270
- remote machines, installation of Netmon Agent Service
  - on 486
- remote sites, connection to 176
- renewal time (DHCP) 414
- replication from master to backup servers (WN) 567
- replication partners (WINS) 505
- Request Announcement** (WN) 569
- request headers (HTTP) 362
- requests for comments *see* RFCs
- RequireSignOrSeal** 537
- res\_mkquery** (**nslookup**) 198
- re-sending packets (Netmon) 491

- Resolver library 203–4
- resolving of names (DNS) 184–5
- resource records (RRs, DNS) 194
- response codes (FTP) 434
- response headers (HTTP) 312–5
- RETR (POP3) 281
- RETR (FTP) 434
- reverse lookup (DNS) 236–7
- RFCs 9, 726
- RFC-768 400, 406
- RFC-805 239
- RFC-816 146
- RFC-819 239
- RFC-821 297, 315
- RFC-822 727
- RFC-830 239
- RFC-883 239
- RFC-894 55
- RFC-917 179, 109
- RFC-940 109
- RFC-942 725
- RFC-959 428, 459
- RFC-973 315
- RFC-1001 488, 515, 519, 581
- RFC-1002 489
- RFC-1034 239
- RFC-1035 239
- RFC-1042 55
- RFC-1081 316
- RFC-1095 464
- RFC-1101 239
- RFC-1122 130, 146
- RFC-1135 283
- RFC-1144 686
- RFC-1149 56, 726
- RFC-1157 461
- RFC-1166 239
- RFC-1213 445, 461
- RFC-1305 463
- RFC-1335 623
- RFC-1345 319
- RFC-1367 109
- RFC-1481 109
- RFC-1517 109
- RFC-1518 109
- RFC-1519 109
- RFC-1541 422
- RFC-1597 110
- RFC-1631 623
- RFC-1661 686
- RFC-1812 146
- RFC-1822 727
- RFC-1825 713
- RFC-1869 316
- RFC-1918 110
- RFC-1919 645
- RFC-1939 316
- RFC-1945 360, 393
- RFC-1984 727
- RFC-1985 316
- RFC-2026 728
- RFC-2030 463
- RFC-2046 794
- RFC-2058 406, 715
- RFC-2131 422
- RFC-2223 730
- RFC-2251 460
- RFC-2396 393
- RFC-2401 713
- RFC-2402 713
- RFC-2403 713
- RFC-2404 713
- RFC-2405 713
- RFC-2406 713
- RFC-2407 713
- RFC-2408 713
- RFC-2409 713
- RFC-2504 644
- RFC-2507 687
- RFC-2508 687
- RFC-2509 687
- RFC-2555 727
- RFC-2578 446, 461
- RFC-2616 393, 802
- RFC-2821 218, 297, 299, 315
- RFC-2822 315, 727
- RFC-2828 644
- RFC-2870 241
- RFC-2916 644
- RFC-3010 407, 464
- RFC-3160 728
- RFC-3164 462
- RFC-3195 462
- RFCs 726–30
- RIP (Routing Information Protocol) 135
- RJ45 plug pin numbers 776
- root domains (DNS) 207, 210
- root servers (DNS) 208, 220–1
- root zones (DNS) 210, 240
- roots of domain tree structures (DNS) 207
- “rough consensus and running code” 729
- round-trip time 39, 290, 372
- route** command
  - metrics 145
  - options 68–9, 126, 134
- route add** 68
- route print** 67, 124
- routed networks 586–7
- routers 8, 28, 60–5
  - code in 115
  - combined with modems 618
  - configuration 71, 623

- definition of 64, 148
- intermediate 20
- with multiple interfaces 64, 620
- with multiple netmasks 98
- for test networks 158, 160
- routes, configuring on 612
- routing
  - for directly-connected networks 128–9
  - fundamental decision on 60–1
    - IP layer only used in 725
    - with multiple interfaces 86
    - to remote sites 176
    - troubleshooting 142–3
- routing daemons 135
- routing loops 76
- routing protocols, automatic 134–5
- routing tables 114–16
  - adding routes 118–21, 124–7
  - automatically-created entries 128
  - cache 134
  - common problems with 121, 127
  - definition of 114
  - deleting routes 120–1, 126–7
  - dial-up 681
  - display of 116, 122
  - entries for default settings 128
  - and ICMP redirects 132–3
  - Linux format 117–21
  - made permanent 119
  - Windows format 122–7
- RPC 573–4
- rpc.lockd** 464
- RPCCMP (Browstat) 825
- rpcinfo** 457
- RPCLIST (Browstat) 826
- RSS (Relay Spam Stopper) 657, 659
- RST (reset) (TCP) 278, 281
- “running code” 729
  
- SA (Security Association) (VPN) 697
- Salus, Peter 12
- SAM (Security Account Manager) (WN) 528–9, 538, 544, 546, 549
- Samba 517, 519, 582, 590–1, 830
- Samba TNG 593
- Sam Spade** 203
- SANS Institute 645
- SAP 491
- SAP/ETYPE 480
- Satan** security scanner 659
- sc** (service controller) (WN) 813
- sc qc** sub-command 489, 813
- scanning, security, 658
- “scavenging” (WINS) 522
- sclist** (service controller list) 491, 813
- <script> tag (HTML) 394
- SD... (Browstat) 824
- SealSecureChannel** 537
- searchlists (DNS resolver) 231–5
- secondary servers (DNS) 220–3, 501
- secret keys (HTML) 388
- secure attention sequence (SAS) 526
- secure channel (WN) 527, 530, 536–7, 539
- Secure DNS 242, 715
- secure login 283
- Security Account Manager *see* SAM
- Security Association *see* SA
- security in depth 636
- security gateways 694
- security glossary 644
- security guidelines 644
- security holes 275, 536
- security ID (SID) (WN) 544
- Security Parameter Index *see* SPI
- security policy 640, 653
- Security Policy Database *see* SPD
- Security Reference Monitor (WN) 544
- security servers 278
- security sub-systems 526
- Security Templates, Windows 637, 644
- security tools 645
- segment master browser 560, 566
- segments, network 32
- semiconductor masks 92
- sendmail** server 315, 635
- sequence numbers, TCP 263, 273, 275
- serial connection 270, 777
- server descriptions (WN) 563
- server hosting at ISPs 599
- Server Manager (WN) 534
- Server NT Service 562, 584
- server trust accounts (WN) 547
- server architecture 808
- servers, DNS
  - for internal names 228
  - location of 222–3
  - types 220–1, 226–8
- Service Control Manager, Windows 476
- Service Controller, Windows 813
- Service** file *see* */etc/services* file
- Service Pack, Windows 678
- Services.exe** 476, 574, 813
- session keys 536
- settings
  - display of 46, 48
  - preservation across reboots 49
- shadow DNS servers 229
- share dealing 654
- share-level security, (WN) 545
- shared secrets (VPN) 703
- shares 452, 545, 574–5, 584
- shopping 654
- “Show all files”, Windows Explorer 508

- SignSecureChannel 537
- simple domain names (DNS) 207
- Simple Mail Transfer Protocol *see* SMTP
- Simple Network Management Protocol *see* SNMP
- simple requests (HTTP) 362
- Simple TCP/IP Services 476
- simultaneous connections, firewall capacity 633, 639
- single-DES encryption 694, 697
- single sign-on (WN) 472, 524
- SIOCADDRT error message 69
- Sircam worm 651
- site security handbook RFC 644
- site-to-site VPN 693
- sites, planning of 598–9
- slave servers, DNS 220
- slaves and forwarders (DNS) 226
- SLIP (Serial Line IP) 624, 686
- Small Business Server 618
- smart hosts (SMTP) 288
- SMB (Server Message Block) 23, 470
- \*SMBSERVER 577, 820
- SMS version of Netmon 486, 491
- SMTP (Simple Mail Transfer Protocol) 288, 285-316,318
  - components of a session 296–9
  - configuration of servers settings 306–7
  - messages passed to POP3 server 302
  - response codes 296
  - telnet as client 294–5
  - viruses 652
- sniffers *see* packet sniffers
- SNMP (Simple Network Management Protocol) 444–5, 461, 735
  - managed switches 43
  - utilities 446–7
- snmpget 445
- snmpmon 462
- snmputil get 447
- snmpwalk 462
- snoop 26
- Snort 658
- socket pairs 282
- sockets 281
- software downloads 830
- Son-of-IKE (VPN) 714
- source ports 265, 402
- source quench ICMP messages 281
- spam 312–13, 316, 650, 656
- spanning tree algorithm 735
- spanning, server architecture 808
- SPD (Security Policy Database) (VPN) 697–700
- Speciner, Mike xviii
- SPI *see* stateful packet inspection
- SPI (Security Parameter Index) 697
- split DNS servers 229
- spoofed messages (SMTP) 312
- SPX protocol 404
- Srv.sys 476
- sscan 659
- SSH (secure shell) 283
- SSL (Secure Sockets Layer) 388, 395
- stackable hubs 735
- stand-alone machines compared with networks 6–7
- Standards track RFCs 726
- standards for networking 55
- star topology network 731
- Start > Dial-Up Networking 670
- start\_fn 772
- stateful packet inspection (SPI) 632, 650
- static mapping (WINS) 504
- static Web pages 375
- status lights on modem (DUN) 676
- Stevens, Richard xviii
- Stoll, Clifford 646
- stop\_fn 772
- store and forward e-mail system 291
- straight-through UTP cables 734
- strata (NTP) 451
- stratum-0 clocks (NTP) 451
- streaming audio/video 654
- subdomains (DNS) 207
  - creation of 219
  - and delegation 219
- Subject: (e-mail header) 298
- sub-net IDs 180
- sub-net masks 31, 87, 109, 161, 179
  - see also* netmasks
- sub-nets 179
  - assigning IP numbers 170–3
  - correct method of creation 164–5
  - example 174–5
  - incorrect method of creation 162–3
  - motivation for 160–1
  - in operation 161
  - planning of 166–7
  - size calculations 168–9
- Sun Microsystems 452
- supersede statement 775
- super-servers 811
- switched hubs *see* switches
- switches 17, 42–3, 731–5
  - problems with tcpdump 42
  - SNMP 43
- symmetric encryption 388
- SYN (synchronize) flag (TCP) 274
- SYN Flood 632
- syslog 401, 448–9, 462–3, 639, 658
- sysstat service 458
- Systems Management Server 478
- T-pieces 731
- tags, HTML 355
- tar archives 653
- Task Manager, Windows 589, 814
- TCP (Transmission Control Protocol) 8, 260–1

- acknowledgements 276
- connections and ports 264–8
- establishing a connection 274–5
- and HTTP 358
- life-cycle of a connection 274–5
- listening on multiple addresses 279
- reliable connection provided by 262–3
- sockets 281–2
- special features 281
- supporting NetBIOS connections 475
- termination of a connection 277
- and UDP 452
- unique identifier for connections 266
- used for long queries 400
- used for zone transfer 400
- TCP client, **netcat** as 432
- TCP server, **netcat** as 432–3
- TCP Wrappers 659, 812
- tcpd** 660, 812
- tcpdump** 4–7, 16–19, 41, 56, 216, 225, 278
  - alias for quick typing 24
  - command summary 736–40
  - compared with Network Monitor 487
  - display options 19
  - DNS packet display format 196–7
  - and **ethereal** 343
  - exchanging capture files 487
  - filter options 20
  - manpage 741–65
  - N and -f options 358
  - and NetBIOS 475
  - NFS packet display format 456
  - “operation not permitted” message 23
  - options 22, 137, 157
  - output format 18
  - problems with 22–5, 42, 734
  - S and F flags in output 371
  - tracing packets across a router 74–5
  - X option 57, 275, 280, 294
  - see also* Appendix 4
- telcos 10–11
- telnet** (telecommunications network protocol) 81, 270–1, 282, 614
  - applications 470
  - connection 390
  - as POP client 302–3
  - security 293
  - servers 271
  - as STMP client 294–5
  - terminal emulators 270
  - title-bar in window 272
  - URL type 354
  - used as universal TCP client 272–3, 293
- terminators, Ethernet 731
- text strings, specification of (**ethereal**) 801
- TFTP (Trivial File Transfer Protocol) 401
- Thick Ethernet 17, 160, 731
- “thin client” architecture 437
- Thin-net 17, 160, 731
- third-party transfers, FTP 429
- 3Com 470
- 3+Open 470
- three-way handshakes 632, 274–5, 588–9, 632–3
- throughput of firewalls 639
- TICKLE (Browstat) 826
- time exceeded (ICMP) 76
- time-to-live *see* TTL
- timestamps (SMTP) 300
- tlst** (task list) 814
- To: (e-mail header) 298
- tombstoning* 520
- top-level domains (TLDs) 208
- top-level media type (MIME) 322
- traceroute** 76–8, 203
  - and firewalls 148
  - mapping 83
  - problems with 147–8
  - showing varying paths 138–9
- tracing of election 570–1
- tracing of packets 4–5, 74–5, 214–15
- Transmission Control Protocol *see* TCP
- transport layer 405, 724
- transport protocols 260, 398
  - see also* TCP, UDP
- traps (SNMP) 444, 462
- tree structure, LDAP 445
- tree structure, DNS 206–207
- triple-DES encryption 694
- “Trojan horse” programs 526, 626
- Troubleshooting
  - basic network configuration 52–53
  - DNS – 246–7
  - Dial-up networking 678–87
  - e-mail send/receive, 308
  - firewalls 642
  - general techniques 51–3
  - HTTP 390–1
  - IP addresses 138–9
  - name resolution, NetBIOS 516–7
  - netmasks 140–1
  - network browsing, Windows 578–9
  - routing 140–1
  - Windows Networking 588–9
  - VPN 708–9
- TRUNCLOG (Browstat) 825
- trust relationships (WN) 541, 551
- trusted domains (WN) 537, 551
- TTL (time-to-live) 76, 198, 247, 624
  - caching and DNS 225
  - values 147
- TURN command (SMTP) 292, 316
- two-factor authentication (VPN) 706

- UC Davis SNMP 446
- UCE (unsolicited commercial e-mail) *see* spam
- UDP (User Datagram Protocol) 398–9, 474, 695, 810
  - applications making use of 400–1, 406–7
  - datagram-oriented 396
  - and DHCP 412
  - and NFS 452
  - ports 402–3
  - services available for 427
  - and SNMP 444
  - and TCP 452
  - troubleshooting 407
  - use instead of TCP 406
- UDP client, **netcat** as 433
- UDP server, **netcat** as 433
- “unable to connect to remote host” error message 81, 278
- UNC notation, Windows 585
- unique names (NetBIOS) 497
- unshielded twisted pair *see* UTP
- unsolicited commercial e-mail (UCE) *see* spam
- “up” keyword, **interfaces** file 767
- “uplink” ports hubs/switches 734
- URLs
  - blocking 638, 659
  - filtering 654
  - host address component of 372–3
  - syntax 354, 372–3
  - and Web page names 374
- User Datagram Protocol *see* UDP
- User Identifier (UID) (WN) 545
- User Manager for Domains 541, 547, 551, 682
- User Rights Policy 547
- user **root** and user **administrator** 18
- usernames 519
- UTP (unshielded twisted pair) 17, 40–1, 732, 776–7
  - hubs and switches 17
- UUCP network 318
- uencode** program 318
  
- Van Jacobson header compression 686
- /var/log/sys-info** 448
- /var/log/syslog** 773
- videoconferencing 602
- VIEW (Browstat) 826
- virtual IP 605
- virtual private networking *see* VPN
- Virtual Router Redundancy Protocol *see* VRRP
- virtual servers 605
- virus scanning 638, 652
- viruses 650
- VPN (virtual private networking) 501, 638, 692–710, 804
  - compared with private leased lines 177
  - default gateway 693
  - definition of 692
  - devices 694
  - implementation 700
  - and NAT 602
  - protocols for 701–2
  - testing 708, 710–11
  - troubleshooting 708
  - wireless networking 707
- VRRP (Virtual Router Redundancy Protocol) 620
- vulnerability testing and scanning, 651, 659
- vvv** (very very verbose) **tcpdump** 216
  
- war-driving 712
- Web appendices xxiii
- Web-based e-mail 308, 329
- Web browsers 356–7
  - caching in 384–5
  - for character screens 357
  - checking of settings 391
  - configuration, of 380–3
  - multiple connections in 371
- Web pages
  - dynamic 375, 393–4
  - links within 355
  - miscellaneous topics 388–9
  - specification of addresses 354–5
  - static 375
  - and URLs 374
  - viruses 652
- Web proxy servers 376–7
  - configuration of browsers 380–3
- Web servers 637
- webster** service 458
- well-known ports 265, 278, 286, 358, 373, 388, 402, 412, 428, 438, 444, 449, 455, 468, 474, 558, 701, 703
- wget** 388
- wildcards 124, 577
- Windows, versions of xviii
- Windows-1252** parameter (MIME) 323
- Windows 2000 xvii, 58, 186, 204, 241, 424, 438, 460, 468–9, 581, 637
- Windows 9x 469, 582
- Windows DNS client 522
- Windows Explorer 454, 563, 584–5, 594
- Windows Help 475
- Windows Internet Name Service *see* WINS
- Windows name resolution 822–3
- Windows Network Monitor *see* Network Monitor
- Windows Networking
  - architecture 470–1
  - on different networking systems 494
  - implementation 472–7
  - origins 468, 471
  - over a routed network 505, 586–7
  - over TCP/IP 474
  - security 471–2
  - separate from TCP/IP 471
  - sniffing 469, 531

- troubleshooting 552, 578–9, 588–9
  - see also* NetBIOS; NetBT
- Windows Registry 589
- Windows for Workgroups 470
- Windows XP 496, 581
- WindowsKey-F 577
- windump** 18, 24, 75, 350, 798
  - on dial-up connections 687
  - error opening adapter 26
  - installation problems 25
- winipcfg** 46
- WinLogon** 526, 528, 530–1, 544
- Winpcap** 798
- WINS (Windows Internet Name Service) 252, 472, 500, 561, 572, 586, 589
  - architecture and implementation 519
  - client configuration 501
  - database replication 505, 520
  - and dial-up 682
  - and discovery 532
  - integrating clients 504
  - multiple servers 505
  - proxy agents 504
  - server configuration 502–3
  - for VPN 709
  - white paper on 519
- WINS Manager 520
- winsadm.exe** 502
- winschk** 519
- winscl** 503, 519, 573
- winsdmp** 503, 519
- wireless LANs 712
- wiring hubs 40
- WIZ wizard command (SMTP) 635
- WKSTADOM 826
- wntipcfg** 46–7, 416, 512
- Woodcock, Robert 807
- WORKGROUP domain 564
- workgroups 471, 494, 499, 525, 552, 556
  - self-contained 515
- working groups 728
- Workstation Service 476
- workstation trust account 534
- WPAD (Web Proxy Autodiscovery Protocol) 394
- www convention 373
- WWW-Authenticate:** header 386
- X11TransSocketINETConnect error 334
- X.400 system 329
- X.500 protocol 438
- X terminals 437
- X Window system 334, 436–7, 458, 460
- xinetd** 459, 814
- zone transfers (DNS) 221
- zones in DNS 208–13