

- 297 – TIP Message Buffers
- 280 – A Draft of Host Names
- 274 – Establishing a local guide for network usage
- 273, 237 - More on standard host names
- 271 – IMP System change notifications
- 270 – Correction to BBN Report No
- 263 – "Very Distant" Host interface
- 254 – Scenarios for using ARPANET computers
- 247 – Proffered set of standard host names
- 241 – Connecting computers to MLC ports
- 239 – Host mnemonics proposed in RFC 226 (NIC 7625)
- 236 – Standard host names
- 233 – Standardization of host call letters
- 230 – Toward reliable operation of minicomputer-based terminals on a TIP
- 229 – Standard host names
- 228 – Clarification
- 226 – Standardization of host mnemonics
- 218 – Changing the IMP status reporting facility
- 213 – IMP System change notification
- 209 – Host/IMP interface documentation
- 208 – Address tables
- 73, 67 - Response to NWG/RFC 67
- 71 – Reallocation in Case of Input Error
- 70 – Note on Padding
- 64 – Getting rid of marking
- 41 – IMP-IMP Teletype Communication
- 25 – No High Link Numbers
- 19 – Two protocol suggestions to reduce congestion at swap bound nodes
- 17 – Some questions re: Host-IMP Protocol
- 12 – IMP-Host interface flow diagrams
- 7 – Host-IMP interface
- 6 – Conversation with Bob Kahn

#### **8b. Host Front End Protocols**

- 929, 928, 705, 647 - Proposed Host-Front End Protocol

#### **8c. ARPANET NCP (Obsolete Predecessor of TCP/IP)**

- 801 – NCP/TCP transition plan
- 773 – Comments on NCP/TCP mail service transition strategy
- 714 – Host-Host Protocol for an ARPANET-Type Network
- 689 – Tenex NCP finite state machine for connections
- 663 – Lost message detection and recovery protocol
- 636 – TIP/Tenex reliability improvements
- 635 – Assessment of ARPANET protocols
- 534, 516, 512 - Lost message detection
- 492, 467 - Response to RFC 467
- 489 – Comment on resynchronization of connection status proposal
- 425 – "But my NCP costs \$500 a day"
- 210 – Improvement of Flow Control
- 176 – Comments on "Byte size for connections"
- 165 – Proffered official Initial Connection Protocol
- 147 – Definition of a socket
- 142 – Time-Out Mechanism in the Host-Host Protocol
- 132, 124, 107, 102 - Typographical Error in RFC 107

- 129 – Request for comments on socket name structure
- 128 – Bytes
- 117 – Some comments on the official protocol
- 72 – Proposed Moratorium on Changes to Network Protocol
- 68 – Comments on Memory Allocation Control Commands: CEASE, ALL, GVB, RET, and RFNM
- 65 – Comments on Host/Host Protocol document #1
- 60 – Simplified NCP Protocol
- 59 – Flow Control - Fixed Versus Demand Allocation
- 58 – Logical Message Synchronization
- 57, 54 - Thoughts and Reflections on NWG/RFC 54
- 56 – Third Level Protocol: Logger Protocol
- 55 – Prototypical implementation of the NCP
- 50, 49, 47, 45, 44, 40, 39, 38, 36, 33 - Comments on the Meyer Proposal
- 42 – Message Data Types
- 23 – Transmission of Multiple Control Messages
- 22 – Host-host control message formats
- 18 – IMP-IMP and HOST-HOST Control Links
- 15 – Network subsystem for time sharing hosts
- 11 – Implementation of the Host-Host software procedures in GORDO
- 9, 1 - Host software
- 8 – Functional specifications for the ARPA Network
- 5 – Decode Encode Language (DEL)
- 2 – Host software

#### **8d. ARPANET Initial Connection Protocol**

- 202 – Possible Deadlock in ICP
- 197 – Initial Connection Protocol - Reviewed
- 161 – Solution to the race condition in the ICP
- 151, 148, 143, 127, 123 - Comments on a proffered official ICP: RFCs 123, 127
- 150 – Use of IPC Facilities: A Working Paper
- 145 – Initial Connection Protocol Control Commands
- 93 – Initial Connection Protocol
- 80 – Protocols and Data Formats
- 66 – NIC - third level ideas and other noise

#### **8e. USENET**

- 1036 – Standard for interchange of USENET messages
- 850 – Standard for interchange of USENET messages

#### **8f. Other**

- 1553 – Compressing IPX Headers Over WAN Media (CIPX)
- 1132 – Standard for the transmission of 802.2 packets over IPX networks
- 935 – Reliable link layer protocols
- 916 – Reliable Asynchronous Transfer Protocol (RATP)
- 914 – Thinwire protocol for connecting personal computers to the Internet
- 824 – CRONUS Virtual Local Network

### **9. Measurement**

#### **9a. General**

- 2724 – RTFM: New Attributes for Traffic Flow Measurement
- 2723 – SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups
- 2722 – Traffic Flow Measurement: Architecture

- 2721 –RTFM: Applicability Statement
- 2681 –A Round-trip Delay Metric for IPPM
- 2680 –A One-way Packet Loss Metric for IPPM
- 2679 –A One-way Delay Metric for IPPM
- 2678, 2498 - IPPM Metrics for Measuring Connectivity
- 2544, 1944 - Benchmarking Methodology for Network Interconnect Devices
- 2432 –Terminology for IP Multicast Benchmarking
- 2330 –Framework for IP Performance Metrics
- 2285 –Benchmarking Terminology for LAN Switching Devices
- 1857, 1404 - A Model for Common Operational Statistics
- 1273 –Measurement Study of Changes in Service-Level Reachability in the Global  
TCP/IP Internet: Goals, Experimental Design, Implementation, and Policy  
Considerations
- 1262 –Guidelines for Internet Measurement Activities
- 557 – Revelations in network host measurements
- 546 – Tenex load averages for July 1973
- 462 – Responding to user needs
- 415 – Tenex bandwidth
- 392 – Measurement of host costs for transmitting network data
- 352 – TIP Site Information Form
- 308 – ARPANET host availability data
- 286 – Network Library Information System
- 214, 193 - Network checkpoint
- 198 – Site Certification - Lincoln Labs 360/67
- 182 – Compilation of list of relevant site reports
- 180 – File system questionnaire
- 156 – Status of the Illinois site: Response to RFC 116
- 153 – SRI ARC-NIC status
- 152 – SRI Artificial Intelligence status report
- 126 – Graphics Facilities at Ames Research Center
- 112 – User/Server Site Protocol: Network host questionnaire responses
- 106 – User/Server Site Protocol Network Host Questionnaire
- 104 – Link 191

### 9b. Surveys

- 971 – Survey of data representation standards
- 876 – Survey of SMTP implementations
- 848 – Who provides the "little" TCP services?
- 847 – Summary of Smallberg surveys
- 846, 845, 843, 842, 839, 838, 837, 836, 835, 834, 833, 832 - Who talks TCP? -  
survey of 22 February 1983
- 844 – Who talks ICMP, too? - Survey of 18 February 1983
- 787 – Connectionless data transmission survey/tutorial
- 565 – Storing network survey data at the datacomputer
- 545 – Of what quality be the UCSB resources evaluators?
- 530 – Report on the Survey project
- 523 – SURVEY is in operation again
- 519 – Resource evaluation
- 514 – Network make-work
- 464 – Resource notebook framework
- 460 – NCP survey
- 459 – Network questionnaires
- 450 – MULTICS sampling timeout change
- 446 – Proposal to consider a network program resource notebook

- 96 – An Interactive Network Experiment to Study Modes of Access the Network Information Center
- 90 – CCN as a Network Service Center
- 81 – Request for Reference Information
- 78 – NCP Status Report: UCSB/Rand

### 9c. Statistics

- 1030 – On testing the NETBLT Protocol over diverse networks
- 996 – Statistics server
- 618 – Few observations on NCP statistics
- 612, 601, 586, 579, 566, 556, 538, 522, 509, 497, 482, 455, 443, 422, 413, 400, 391, 378 - Traffic statistics (December 1973)
- 603, 597, 376, 370, 367, 366, 362, 353, 344, 342, 332, 330, 326, 319, 315, 306, 298, 293, 288, 287, 267, 266 - Response to RFC 597: Host status
- 550 – NIC NCP experiment
- 388 – NCP statistics
- 255, 252, 240, 235 - Status of network hosts

## 10. Privacy, Security and Authentication

### 10a. General

- 2716 – PPP EAP TLS Authentication Protocol
- 2712 – Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)
- 2704 – The KeyNote Trust-Management System Version 2
- 2693 – SPKI Certificate Theory
- 2692 – SPKI Requirements
- 2630 – Cryptographic Message Syntax
- 2628 – Simple Cryptographic Program Interface (Crypto API)
- 2627 – Key Management for Multicast: Issues and Architectures
- 2538 – Storing Certificates in the Domain Name System (DNS)
- 2537 – RSA/MD5 KEYS and SIGs in the Domain Name System (DNS)
- 2536 – DSA KEYS and SIGs in the Domain Name System (DNS)
- 2523, 2522 - Photuris: Extended Schemes and Attributes
- 2504 – Users' Security Handbook
- 2479 – Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)
- 2478, 2078, 1508 - The Simple and Protected GSS-API Negotiation Mechanism
- 2444 – The One-Time-Password SASL Mechanism
- 2440 – OpenPGP Message Format
- 2437, 2313 - PKCS #1: RSA Cryptography Specifications Version 2.0
- 2367 – PF\_KEY Key Management API, Version 2
- 2315 – PKCS 7: Cryptographic Message Syntax Version 1.5
- 2314 – PKCS 10: Certification Request Syntax Version 1.5
- 2289, 2243, 1938 - A One-Time Password System
- 2267 – Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
- 2246 – The TLS Protocol Version 1.0
- 2245 – Anonymous SASL Mechanism
- 2222 – Simple Authentication and Security Layer (SASL)
- 2196, 1244 - Site Security Handbook
- 2179 – Network Security For Trade Shows
- 2094 – Group Key Management Protocol (GKMP) Architecture
- 2093 – Group Key Management Protocol (GKMP) Specification
- 2025 – The Simple Public-Key GSS-API Mechanism (SPKM)

- 1991 –PGP Message Exchange Formats
- 1964 –The Kerberos Version 5 GSS-API Mechanism
- 1949 –Scalable Multicast Key Distribution
- 1948 –Defending Against Sequence Number Attacks
- 1898 –CyberCash Credit Card Protocol Version 0.8
- 1824 –The Exponential Security System TESS: An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange (E.I.S.S.-Report 1995/4)
- 1805 –Location-Independent Data/Software Integrity Protocol
- 1760 –The S/KEY One-Time Password System
- 1751 –A Convention for Human-Readable 128-bit Keys
- 1750 –Randomness Recommendations for Security
- 1704 –On Internet Authentication
- 1511 –Common Authentication Technology Overview
- 1510 –The Kerberos Network Authentication Service (V5)
- 1509 –Generic Security Service API : C-bindings
- 1507 –DASS - Distributed Authentication Security Service
- 1457 –Security Label Framework for the Internet
- 1455 –Physical Link Security Type of Service
- 1424 –Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services
- 1423, 1115 - Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers
- 1422, 1114 - Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management
- 1421, 1113, 989 - Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures
- 1355 –Privacy and Accuracy Issues in Network Information Center Databases
- 1281 –Guidelines for the Secure Operation of the Internet
- 1170 –Public key standards and licenses
- 1135 –Helminthiasis of the Internet
- 1108 –US Department of Defense Security Options for the Internet Protocol
- 1040 –Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures
- 1038 –Draft revised IP security option
- 1004 –Distributed-protocol authentication scheme
- 972 – Password Generator Protocol

#### **10b. Encryption, Authentication and Key Exchange Algorithms**

- 2631 –Diffie-Hellman Key Agreement Method
- 2612 –The CAST-256 Encryption Algorithm
- 2286 –Test Cases for HMAC-RIPEMD160 and HMAC-RIPEMD128
- 2268 –A Description of the RC2(r) Encryption Algorithm
- 2202 –Test Cases for HMAC-MD5 and HMAC-SHA-1
- 2144 –The CAST-128 Encryption Algorithm
- 2040 –The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms
- 1810 –Report on MD5 Performance
- 1321 –The MD5 Message-Digest Algorithm
- 1320, 1186 - The MD4 Message-Digest Algorithm
- 1319 –The MD2 Message-Digest Algorithm

#### **10c. IP Security Protocol (IPSec)**

- 2709 –Security Model with Tunnel-mode IPsec for NAT Domains
- 2451 –The ESP CBC-Mode Cipher Algorithms
- 2412 –The OAKLEY Key Determination Protocol

- 2411 –IP Security Document Roadmap
- 2410 –The NULL Encryption Algorithm and Its Use With IPsec
- 2409 –The Internet Key Exchange (IKE)
- 2408 –Internet Security Association and Key Management Protocol (ISAKMP)
- 2407 –The Internet IP Security Domain of Interpretation for ISAKMP
- 2406, 1827 - IP Encapsulating Security Payload (ESP)
- 2405 –The ESP DES-CBC Cipher Algorithm With Explicit IV
- 2404 –The Use of HMAC-SHA-1-96 within ESP and AH
- 2403 –The Use of HMAC-MD5-96 within ESP and AH
- 2402, 1826 - IP Authentication Header
- 2401, 1825 - Security Architecture for the Internet Protocol
- 2104 –HMAC: Keyed-Hashing for Message Authentication
- 2085 –HMAC-MD5 IP Authentication with Replay Prevention
- 1852 –IP Authentication using Keyed SHA
- 1851 –The ESP Triple DES Transform
- 1829 –The ESP DES-CBC Transform
- 1828 –IP Authentication using Keyed MD5

## 11. Network Experience and Demonstrations

- 2123 –Traffic Flow Measurement: Experiences with NeTraMet
- 1435 –IESG Advice from Experience with Path MTU Discovery
- 1306 –Experiences Supporting By-Request Circuit-Switched T3 Networks
- 967 – All victims together
- 573 – Data and file transfer: Some measurement results
- 525 – MIT-MATHLAB meets UCSB-OLS -an example of resource sharing
- 439 – PARRY encounters the DOCTOR
- 420 – CCA ICCC weather demo
- 372 – Notes on a Conversation with Bob Kahn on the ICCC
- 364 – Serving remote users on the ARPANET
- 302 – Exercising The ARPANET
- 231 – Service center standards for remote usage: A user's view
- 227 – Data transfer rates (Rand/UCLA)
- 113 – Network activity report: UCSB Rand
- 89 – Some historic moments in networking
- 4 – Network timetable

## 12. Site Documentation

- 30, 27, 24, 10, 3 - Documentation Conventions

## 13. Protocol Standards By Other Groups Of Interest To The Internet

### 13a. ANSI

- 183 – EBCDIC codes and their mapping to ASCII
- 20 – ASCII format for network interchange

### 13b. NRC

- 942 – Transport protocols for Department of Defense data networks
- 939 – Executive summary of the NRC report on transport protocols for Department of Defense data networks

### 13c. ISO

- 1698 –Octet Sequences for Upper-Layer OSI to Support Basic Communications Applications
- 1629, 1237 - Guidelines for OSI NSAP Allocation in the Internet
- 1575, 1139 - An Echo Function for CLNP (ISO 8473)

- 1574 –Essential Tools for the OSI Internet
- 1561 –Use of ISO CLNP in TUBA Environments
- 1330 –Recommendations for the Phase I Deployment of OSI Directory Services (X.500) and OSI Message Handling Services (X.400) within the ESNET Community
- 1238, 1162 - CLNS MIB for use with Connectionless Network Protocol (ISO 8473) and End System to Intermediate System (ISO 9542)
- 1223 –OSI CLNS and LLC1 protocols on Network Systems HYPERchannel
- 1008 –Implementation guide for the ISO Transport Protocol
- 1007 –Military supplement to the ISO Transport Protocol
- 995 – End System to Intermediate System Routing Exchange Protocol for use in conjunction with ISO 8473
- 994 – Final text of DIS 8473, Protocol for Providing the Connectionless-mode Network Service
- 982 – Guidelines for the specification of the structure of the Domain Specific Part (DSP) of the ISO standard NSAP address
- 941 – Addendum to the network service definition covering network layer addressing
- 926 – Protocol for providing the connectionless mode network services
- 905 – ISO Transport Protocol specification ISO DP 8073
- 892 – ISO Transport Protocol specification
- 873 – Illusion of vendor support

## **14. Interoperability With Other Applications And Protocols**

### **14a. Protocol Translation and Bridges**

- 1086 –ISO-TP0 bridge between TCP and X.25
- 1029 –More fault tolerant approach to address resolution for a Multi-LAN system of Ethernets

### **14b. Tunneling and Layering**

- 2661 –Layer Two Tunneling Protocol "L2TP"
- 2556 –OSI connectionless transport services on top of UDP Applicability Statement for Historic Status
- 2353 –APPN/HPR in IP Networks APPN Implementers' Workshop Closed Pages Document
- 2166 –APPN Implementer's Workshop Closed Pages Document DLSw v2.0 Enhancements
- 2126, 1859, 1006 - ISO Transport Service on top of TCP (ITOT)
- 2114, 2106 - Data Link Switching Client Access Protocol
- 1795, 1434 - Data Link Switching: Switch-to-Switch Protocol AIW DLSw RIG: DLSw Closed Pages, DLSw Standard Version 1
- 1791 –TCP And UDP Over IPX Networks With Fixed Path MTU
- 1634, 1551, 1362 - Novell IPX Over Various WAN Media (IPXWAN)
- 1613 –cisco Systems X.25 over TCP (XOT)
- 1538 –Advanced SNA/IP : A Simple SNA Transport Protocol
- 1356 –Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode
- 1240 –OSI connectionless transport services on top of UDP: Version 1
- 1234 –Tunneling IPX traffic through IP networks
- 1085 –ISO presentation services on top of TCP/IP based internets
- 1070 –Use of the Internet as a subnetwork for experimentation with the OSI network layer
- 983 – ISO transport arrives on top of the TCP

#### **14c. Mapping of Names, Addresses, and Identifiers**

- 1439 –The Uniqueness of Unique Identifiers
- 1236 –IP to X.121 address mapping for DDN
- 1069 –Guidelines for the use of Internet-IP addresses in the ISO Connectionless-Mode Network Protocol

### **15. Miscellaneous**

#### **15a. General**

- 2664, 1594, 1325, 1206, 1177 - FYI on Questions and Answers - Answers to Commonly Asked "New Internet User" Questions
- 2636, 2604 - Wireless Device Configuration (OTASP/OTAPA) via ACAP
- 2635 –DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam\*)
- 2626 –The Internet and the Millennium Problem (Year 2000)
- 2555 –30 Years of RFCs
- 2468 –I REMEMBER IANA
- 2441 –Working with Jon, Tribute delivered at UCLA, October 30, 1998
- 2351 –Mapping of Airline Reservation, Ticketing, and Messaging Traffic over IP
- 2350 –Expectations for Computer Security Incident Response
- 2309 –Recommendations on Queue Management and Congestion Avoidance in the Internet
- 2235 –Hobbes' Internet Timeline
- 2234 –Augmented BNF for Syntax Specifications: ABNF
- 2151, 1739 - A Primer On Internet and TCP/IP Tools and Utilities
- 2150 –Humanities and Arts: Sharing Center Stage on the Internet
- 2057 –Source Directed Access Control on the Internet
- 1983, 1392 - Internet Users' Glossary
- 1958 –Architectural Principles of the Internet
- 1941, 1578 - Frequently Asked Questions for Schools
- 1935 –What is the Internet, Anyway?
- 1865 –EDI Meets the Internet Frequently Asked Questions about Electronic Data Interchange (EDI) on the Internet
- 1855 –Netiquette Guidelines
- 1775 –To Be "On" the Internet
- 1758, 1417, 1295 - NADF Standing Documents: A Brief Overview
- 1746 –Ways to Define User Expectations
- 1709 –K-12 Internetworking Guidelines
- 1691 –The Document Architecture for the Cornell Digital Library
- 1633 –Integrated Services in the Internet Architecture: an Overview
- 1580 –Guide to Network Resource Tools
- 1501 –OS/2 User Group
- 1498 –On the Naming and Binding of Network Destinations
- 1470, 1147 - FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices
- 1462 –FYI on "What is the Internet?"
- 1453 –A Comment on Packet Video Remote Conferencing and the Transport/Network Layers
- 1432 –Recent Internet Books
- 1402, 1290 - There's Gold in them thar Networks! or Searching for Treasure in all the Wrong Places
- 1400 –Transition and Modernization of the Internet Registration Service
- 1359 –Connecting to the Internet - What Connecting Institutions Should Anticipate
- 1345 –Character Mnemonics and Character Sets



- 1336, 1251 - Who's Who in the Internet: Biographies of IAB, IESG and IRSG Members
- 1324 -A Discussion on Computer Network Conferencing
- 1302 -Building a Network Information Services Infrastructure
- 1300 -Remembrances of Things Past
- 1296 -Internet Growth (1981-1991)
- 1291 -Mid-Level Networks Potential Technical Services
- 1259 -Building the open road: The NREN as test-bed for the national public network
- 1242 -Benchmarking terminology for network interconnection devices
- 1208 -Glossary of networking terms
- 1207 -FYI on Questions and Answers: Answers to commonly asked "experienced Internet user" questions
- 1199, 1099 - Request for Comments Summary Notes: 1100-1199
- 1192 -Commercialization of the Internet summary report
- 1181 -RIPE Terms of Reference
- 1180 -TCP/IP tutorial
- 1178 -Choosing a name for your computer
- 1173 -Responsibilities of host and network managers: A summary of the "oral tradition" of the Internet
- 1169 -Explaining the role of GOSIP
- 1167 -Thoughts on the National Research and Education Network
- 1118 -Hitchhikers guide to the Internet
- 1015 -Implementation plan for interagency research Internet
- 992 - On communication support for fault tolerant process groups
- 874 - Critique of X.25
- 531 - Feast or famine? A response to two recent RFC's about network information
- 473 - MIX and MIXAL?
- 472 - Illinois' reply to Maxwell's request for graphics information (NIC 14925)
- 429 - Character Generator Process
- 408 - NETBANK
- 361 - Deamon Processes on Host 106
- 313 - Computer based instruction
- 256 - IMPSYS change notification
- 225 - Rand/UCSB network graphics experiment
- 219 - User's view of the datacomputer
- 187 - Network/440 Protocol Concept
- 169 - Computer networks
- 146 - Views on issues relevant to data sharing on computer networks
- 13 - Zero Text Length EOF Message

#### **15b. Bibliographies**

- 2007 -Catalogue of Network Training Materials
- 1463 -FYI on Introducing the Internet-- A Short Bibliography of Introductory Internetworking Readings
- 1175 -FYI on where to start: A bibliography of internetworking information
- 1012 -Bibliography of Request For Comments 1 through 999
- 829 - Packet satellite technology reference sources
- 290 - Computer networks and data sharing: A bibliography
- 243 - Network and data sharing bibliography

#### **15c. Humorous RFCs**

- 2551 -The Roman Standards Process -- Revision III
- 2550 -Y10K and Beyond

2549 –IP over Avian Carriers with Quality of Service  
2325 –Definitions of Managed Objects for Drip-Type Heated Beverage Hardware  
Devices using SMIV2  
2324 –Hyper Text Coffee Pot Control Protocol (HTCPCP/1.0)  
2323 –IETF Identification and Security Guidelines  
2322 –Management of IP numbers by peg-dhcp  
2321 –RITA -- The Reliable Internetwork Troubleshooting Agent  
2100 –The Naming of Hosts  
1927 –Suggested Additional MIME Types for Associating Documents  
1926 –An Experimental Encapsulation of IP Datagrams on Top of ATM  
1925 –The Twelve Networking Truths  
1924 –A Compact Representation of IPv6 Addresses  
1882 –The 12-Days of Technology Before Christmas  
1776 –The Address is the Message  
1607 –A VIEW FROM THE 21ST CENTURY  
1606 –A Historical Perspective On The Usage Of IP Version 9  
1605 –SONET to Sonnet Translation  
1438 –Internet Engineering Task Force Statements Of Boredom (SOBs)  
1437 –The Extension of MIME Content-Types to a New Medium  
1313 –Today’s Programming for KRFC AM 1313 Internet Talk Radio  
1217 –Memo from the Consortium for Slow Commotion Research (CSCR)  
1216 –Gigabit network economics and paradigm shifts  
1149 –Standard for the transmission of IP datagrams on avian carriers  
1121 –Act one - the poems  
1097 –Telnet subliminal-message option  
968 – Twas the night before start-up  
748 – Telnet randomly-lose option  
527 – ARPAWOCKY

## 16. Unissued

2727, 2726, 2725, 2708, 2707, 2700, 2699, 2600, 2599, 2576, 1849, 1840, 1839,  
1260, 1182, 1061, 853, 723, 715, 711, 710, 709, 693, 682, 676, 673, 670, 668, 665,  
664, 650, 649, 648, 646, 641, 639, 605, 583, 575, 572, 564, 558, 554, 541, 540, 536,  
517, 507, 502, 484, 481, 465, 444, 428, 427, 424, 397, 383, 380, 375, 358, 341, 337,  
284, 279, 277, 275, 272, 262, 261, 260, 259, 258, 257, 248, 244, 220, 201, 159, 92,  
26, 14

# *Appendix 2*

## *Glossary Of Internetworking Terms And Abbreviations*

### **TCP/IP Terminology**

Like most large enterprises, TCP/IP has a language all its own. A curious blend of networking jargon, protocol names, and abbreviations, the language is both difficult to learn and difficult to remember. To outsiders, discussions among the cognoscenti sound like meaningless babble laced with acronyms at every possible opportunity. Even after a moderate amount of exposure, readers may find that specific terms are difficult to understand. The problem is compounded because some terminology is loosely defined and because the sheer volume is overwhelming.

This glossary helps solve the problem by providing short definitions for terms used throughout the Internet. It is not intended as a tutorial for beginners. Instead, we focus on providing a concise reference to make it easy for those who are generally knowledgeable about networking to look up the meaning of specific terms or acronyms quickly. Readers will find it substantially more useful as a reference after they have studied the text than before.

## A Glossary of Terms and Abbreviations In Alphabetical Order

### **10/100 hardware**

Applied to any Ethernet hardware that can operate at either 10 Mbps or 100 Mbps.

### **10Base2**

The technical name for the original thick Ethernet.

### **10Base5**

The technical name for thin Ethernet.

### **10Base-T**

The technical name for twisted pair Ethernet operating at 10 Mbps.

### **100Base-T**

The technical name for twisted pair Ethernet operating at 100 Mbps. The term *100Base-TX* is more specific.

### **1000Base-T**

The technical name for twisted pair Ethernet operating at 1000 Mbps (1 Gbps).

### **127.0.0.1**

The IP *loopback* address used for testing. Packets sent to this address are processed by the local protocol software without ever being sent across a network.

### **2X Problem**

An inefficient routing situation caused by mobile IP in which a datagram crosses the global Internet twice when traveling from a computer to a mobile that is visiting a nearby network.

### **576**

The minimum datagram size all hosts and routers must handle.

### **802.3**

The IEEE standard for Ethernet.

### **822**

The TCP/IP standard format for electronic mail messages. Mail experts often refer to ‘822 messages.’ The name comes from RFC 822 that contains the specification. 822 format was previously known as 733 format.

### **9180**

The default MTU size for sending IP datagrams over an ATM network.

### **AAL**

(*ATM Adaptation Layer*) Part of the ATM protocols. Several adaptation layers exist; AAL5 is used for data.

**ABR**

Either *Available Bit Rate*, an ATM designation for service that does not guarantee a rate, or *Area Border Router*, an OSPF designation for a router that communicates with another area.

**ACK**

Abbreviation for *acknowledgement*.

**ACK implosion**

A reference to a problem that can occur with a reliable multicast protocol in which many acknowledgements (ACKs) go back to the source. Most reliable multicast schemes use designated routers to aggregate ACKs.

**acknowledgement**

A response sent by a receiver to indicate successful reception of information. Acknowledgements may be implemented at any level including the physical level (using voltage on one or more wires to coordinate transfer), at the link level (to indicate successful transmission across a single hardware link), or at higher levels (e.g., to allow an application program at the final destination to respond to an application program at the source).

**acknowledgement aggregator**

Used in a reliable multicast scheme to avoid the ACK implosion problem.

**active open**

The operation that a client performs to establish a TCP connection with a server at a known address.

**adaptive retransmission**

The scheme TCP uses to make the retransmission timer track the mean round-trip time.

**address**

An integer value used to identify a particular computer that must appear in each packet sent to the computer.

**address binding**

The translation of a higher-layer address into an equivalent lower-layer address (e.g., translation of a computer's IP address to the computer's Ethernet address).

**address mask**

A synonym for *subnet mask*.

**address resolution**

Conversion of a protocol address into a corresponding physical address (e.g., conversion of an IP address into an Ethernet address). Depending on the underlying network, resolution may require broadcasting on a local network. See ARP.

**administrative scoping**

A scheme for limiting the propagation of multicast datagrams. Some addresses are reserved for use within a site or within an organization.

**ADSL**

(*Asymmetric Digital Subscriber Line*) A popular DSL variant.

**Advanced Networks and Services**

The company that owned and operated the Internet backbone in 1995.

**agent**

In network management, an agent is the server software that runs on a host or router being managed.

**AH**

(*Authentication Header*) A header used by IPsec to guarantee the authenticity of a datagram's source.

**all routers group**

The well-known IP multicast group that includes all routers on the local network.

**all systems group**

The well-known IP multicast group that includes all hosts and routers on the local network.

**anonymous FTP**

An FTP session that uses login name *anonymous* to access public files. A server that permits anonymous FTP often allows the password *guest*.

**anonymous network**

A synonym for *unnumbered network*.

**ANS**

Abbreviation for *Advanced Networks and Services*.

**ANSI**

(*American National Standards Institute*) A group that defines U.S. standards for the information processing industry. ANSI participates in defining network protocol standards.

**ANSNET**

The Wide Area Network that formed the Internet backbone until 1995.

**anycast**

An address form introduced with IPv6 in which a datagram sent to the address can be routed to any of a set of computers. An *anycast address* is called a *cluster address*.

**API**

(*Application Program Interface*) The specification of the operations an application program must invoke to communicate over a network. The socket API is the most popular for internet communication.

**application gateway**

An application program that connects two or more heterogeneous systems and translates among them. E-mail gateways are especially popular.

**application-server paradigm**

A synonym for *client-server* paradigm.

**area**

In OSPF, a group of routers that exchange routing information.

**area manager**

A person in charge of an IETF area. The set of area managers form the IESG.

**ARP**

(*Address Resolution Protocol*) The TCP/IP protocol used to dynamically bind a high-level IP Address to a low-level physical hardware address. ARP is used across a single physical network and is limited to networks that support hardware broadcast.

**ARPA**

(*Advanced Research Projects Agency*) The government agency that funded the ARPANET, and later, the global Internet. The group within ARPA with responsibility for the ARPANET was IPTO (*Information Processing Techniques Office*), later called ISTO (*Information Systems Technology Office*). ARPA was named *DARPA* for many years.

**ARPANET**

A pioneering long haul network funded by ARPA (later DARPA) and built by BBN. It served from 1969 through 1990 as the basis for early networking research and as a central backbone during development of the Internet. The ARPANET consisted of individual packet switching nodes interconnected by leased lines.

**ARQ**

(*Automatic Repeat reQuest*) Any protocol that uses positive and negative acknowledgements with retransmission techniques to ensure reliability. The sender automatically repeats the request if it does not receive an answer.

**AS**

(*Autonomous System*) A collection of routers and networks that fall under one administrative entity and cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice. Routers within an autonomous system have a high degree of trust. Before two autonomous systems can communicate, one router in each system sends reachability information to a router in the other.

**ASN.1**

(*Abstract Syntax Notation. 1*) The ISO presentation standard protocol used by SNMP to represent messages.

**Assigned Numbers**

The RFC document that specifies (usually numeric) values used by TCP/IP protocols.

**ATM**

(*Asynchronous Transfer Mode*) A connection-oriented network technology that uses small, fixed-size cells at the lowest layer. ATM has the potential advantage of being able to support voice, video, and data with a single underlying technology.

**ATM Adaptation Layer (AAL)**

One of several protocols defined for ATM that specifies how an application sends and receives information over an ATM network. Data transmissions use AAL5.

**ATMARP**

The protocol a host uses for address resolution when sending IP over an ATM network.

**AUI**

(*Attachment Unit Interface*) The connector used for thick-wire Ethernet.

**authority zone**

A part of the domain name hierarchy in which a single name server is the authority.

**backbone network**

Any network that forms the central interconnect for an internet. A national backbone is a WAN; a corporate backbone can be a LAN.

**base64**

An encoding used with MIME to send non-textual data such as a binary file through e-mail.

**base header**

In the proposed IPng, the required header found at the beginning of each datagram.

**baseband**

Characteristic of any network technology like Ethernet that uses a single carrier frequency and requires all stations attached to the network to participate in every transmission. Compare to *broadband*.

**bastion host**

A secure computer that forms part of a security firewall and runs applications that communicate with computers outside an organization.

**baud**

Literally, the number of times per second the signal can change on a transmission line. Commonly, the transmission line uses only two signal states (e.g., two voltages), making the baud rate equal to the number of bits per second that can be transferred. The underlying transmission technique may use some of the bandwidth, so it may not be the case that users experience data transfers at the line's specified bit rate. For example, because asynchronous lines require 10 bit-times to send an 8-bit character, a 9600 baud asynchronous transmission line can only send 960 characters per second.



**BCP**

(*Best Current Practice*) A label given to a subset of RFCs that contain recommendations from the IETF about the use, configuration, or deployment of internet technologies.

**Bellman-Ford**

A synonym for *distance-vector*.

**Berkeley broadcast**

A reference to a nonstandard IP broadcast address that uses all zeros in the host portion instead of all ones. The name arises because the technique was introduced and propagated in Berkeley's BSD UNIX.

**best-effort delivery**

Characteristic of network technologies that do not provide reliability at link levels. IP works well over best-effort delivery hardware because IP does not assume that the underlying network provides reliability. The UDP protocol provides best-effort delivery service to application programs.

**BGP**

(*Border Gateway Protocol*) The major exterior gateway protocol used in the Internet. Four major versions of BGP have appeared, with BGP-4 being the current.

**big endian**

A format for storage or transmission of binary data in which the most-significant byte (bit) comes first. The TCP/IP standard network byte order is big endian. Compare to *little endian*.

**binary exponential backoff**

A technique used to control network contention or congestion quickly. A sender doubles the amount of time it waits between each successive attempt to use the network.

**BISYNC**

(*BInary SYNchronous Communication*) An early, low-level protocol developed by IBM and used to transmit data across a synchronous communication link. Unlike most modern link level protocols, BISYNC is byte-oriented, meaning that it uses special characters to mark the beginning and end of frames. BISYNC is often called BSC, especially in commercial products.

**BNC**

The style of connector used with thin-wire Ethernet.

**BOOTP**

Abbreviation for *BOOTstrap Protocol*, a protocol a host uses to obtain startup information, including its IP address, from a server.

**bps**

(*bits per second*) A measure of the rate of data transmission.

**bridge**

A computer that connects two or more networks and forwards packets among them. Bridges operate at the physical network level. For example, an Ethernet bridge connects two physical Ethernet cables, and forwards from one cable to the other exactly the packets that are not local. Bridges differs from repeaters because bridges store and forward complete packets, while repeaters forward all electrical signals. Bridges differ from routers because bridges use physical addresses, while routers use IP addresses.

**broadband**

Characteristic of any network technology that multiplexes multiple, independent network carriers onto a single cable (usually using frequency division multiplexing). For example, a single 50 Mbps broadband cable can be divided into five 10 Mbps carriers, with each treated as an independent Ethernet. The advantage of broadband is less cable; the disadvantage is higher cost for equipment at connections. Compare to *baseband*.

**broadcast**

A packet delivery system that delivers a copy of a given packet to all hosts that attach to it is said to broadcast the packet. Broadcast may be implemented with hardware (e.g., as in Ethernet) or with software (e.g., IP broadcasting in the presence of subnets).

**broadcast and prune**

A technique used in data-driven multicast forwarding in which routers forward each datagram to each network until they learn that the network has no group members.

**router**

(*Bridging ROUTER*) A device that operates as a bridge for some protocols and as a router for others (e.g., a router can bridge DECNET protocols and route IP).

**BSC**

(*Binary Synchronous Communication*) See BISYNC.

**BSD UNIX**

(*Berkeley Software Distribution UNIX*) The version of UNIX released by U.C. Berkeley or one of the commercial systems derived from it. BSD UNIX was the first to include TCP/IP protocols.

**care-of address**

A temporary IP address used by a mobile while visiting a foreign network.

**category 5 cable**

A standard for wiring that is used with twisted pair Ethernet.

**CBT**

(*Core Based Trees*) A demand-driven multicast routing protocol that builds shared forwarding trees.

**CCIRN**

(*Coordinating Committee for Intercontinental Research Networking*) An international group that helps coordinate international cooperation on internetworking research and development.

**CCITT**

(*Consultative Committee on International Telephony and Telegraphy*) The former name of International Telecommunications Union.

**CDDI**

(*Copper Distributed Data Interface*) An adaptation of the FDDI network technology for use over copper wires.

**cell**

A small, fixed-size packet. The fixed size makes hardware optimization possible. Cells are often associated with ATM networks in which a cell contains 48 octets of data and 5 octets of header.

**cell tax**

A reference to the 10% header overhead imposed by ATM.

**CGI**

(*Common Gateway Interface*) A technology a server uses to create a Web page dynamically when the request arrives.

**checksum**

A small, integer value computed from a sequence of octets by treating them as integers and computing the sum. A checksum is used to detect errors that result when the sequence of octets is transmitted from one machine to another. Typically, protocol software computes a checksum and appends it to a packet when transmitting. Upon reception, the protocol software verifies the contents of the packet by recomputing the checksum and comparing to the value sent. Many TCP/IP protocols use a 16-bit checksum computed with one's complement arithmetic, with all integer fields in the packet stored in network byte order.

**CIDR**

(*Classless Inter-Domain Routing*) The standard that specifies the details of both classless addressing and an associated routing scheme.

**CL**

See *connectionless service*.

**class of address**

The category of an IP address. The class of an address determines the location of the boundary between network prefix and host suffix.

**classful addressing**

The original IPv4 addressing scheme in which host addresses were divided into three classes: A, B, and C.

**classless addressing**

An extension of the original IPv4 addressing scheme that ignores the original class boundaries. Classless addressing was motivated by the problem of address space exhaustion.

**client-server**

The model of interaction in a distributed system in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the program satisfying the request is called the server. It is usually easier to build client software than server software.

**closed window**

A situation in TCP where a receiver has sent a window advertisement of zero because no additional buffer space is available. The sending TCP cannot transmit additional data until the receiver opens the window.

**cluster address**

The term originally used for *anycast* address.

**CO**

See *connection-oriented service*.

**codec**

(*coder/decoder*) A hardware device used to convert between an analog audio signal and a stream of digital values.

**congestion**

A situation in which traffic (temporarily) exceeds the capacity of networks or routers. TCP includes a congestion control mechanism that allows it to back off when the internet becomes congested.

**connection**

An abstraction provided by protocol software. TCP provides a connection from an application on one computer to an application on another.

**connection-oriented service**

Characteristic of the service offered by any technology that requires communicating entities to establish a connection before sending data. TCP provides connection-oriented service as does ATM hardware.

**connectionless service**

Characteristic of any packet delivery service that treats each packet or datagram as a separate entity and allows communicating entities to transmit data before establishing communication. Each packet carries a destination address to identify the intended recipient. Most network hardware, the Internet Protocol (IP), and the User Datagram Protocol (UDP) provide connectionless service.

**COPS**

(*Common Open Policy Service*) A protocol used with RSVP to verify whether a request meets policy constraints.

**core architecture**

Characteristic of an internet architecture that has a central routing system surrounded by local routing systems. The original Internet had a single backbone network, and used a core architecture. As ISPs developed backbone systems, the Internet moved away from a single core.

**count to infinity**

A popular synonym for the *slow convergence* problem.

**CRC**

(*Cyclic Redundancy Code*) A small, integer value computed from a sequence of octets used to detect errors that result when the sequence of octets is transmitted from one machine to another. Typically, packet switching network hardware computes a CRC and appends it to a packet when transmitting. Upon reception, the hardware verifies the contents of the packet by recomputing the CRC and comparing it to the value sent. Although more expensive to compute, a CRC detects more errors than a checksum that uses additive methods.

**CR-LF**

(*Carriage Return - Line Feed*) A two-character sequence used to terminate text lines in application-layer protocols such as TELNET and SMTP.

**CSMA/CD**

(*Carrier Sense Multiple Access with Collision Detection*) A characteristic of network hardware that operates by allowing multiple stations to contend for access to a transmission medium by listening to see if the medium is idle, and a mechanism that allows the hardware to detect when two stations simultaneously attempt transmission. Ethernet uses CSMA/CD.

**CSU/DSU**

(*Channel Service Unit/Data Service Unit*) An electronic device that connects a computer or router to a digital circuit leased by the telephone company. Although the device fills two rolls, it usually consists of a single physical piece of hardware.

**cumulative acknowledgement**

An alternative to the selective acknowledgements used by TCP. A cumulative acknowledgement reports all data that has been received successfully rather than each piece of data that arrives.

**DARPA**

(*Defense Advanced Research Projects Agency*) Former name of ARPA.

**data-driven multicast**

A scheme for multicast forwarding that uses the broadcast and prune approach. See *demand-driven multicast*.

**datagram**

See *IP datagram*.

**DCE**

(*Data Communications Equipment*) Term ITU protocol standards apply to switching equipment that forms a packet switched network to distinguish it from the computers or terminals that connect to the network. Also see *DTE*.

**DDCMP**

(*Digital Data Communication Message Protocol*) The link level protocol used in the original NSFNET backbone.

**DDN**

(*Defense Data Network*) The part of the Internet associated with U.S. military sites.

**default route**

A single entry in a list of routes that covers all destinations which are not included explicitly. The routing tables in most routers and hosts contain an entry for a default route.

**delay**

One of the two primary measures of a network. Delay refers to the difference between the time a bit of data is injected into a network and the time the bit exits.

**delayed acknowledgement**

A heuristic employed by a receiving TCP to avoid silly window syndrome.

**demand-driven multicast**

A scheme for multicast forwarding that requires a router to join a shared forwarding tree before delivering packets. See *data-driven multicast*.

**demultiplex**

To separate from a common input into several outputs. Demultiplexing occurs at many levels. Hardware demultiplexes signals from a transmission line based on time or carrier frequency to allow multiple, simultaneous transmissions across a single physical cable. IP software demultiplexes incoming datagrams, sending each to the appropriate high-level protocol module or application program. See *multiplex*.

**DHCP**

(*Dynamic Host Configuration Protocol*) A protocol that a host uses to obtain all necessary configuration information including an IP address. DHCP is popular with ISPs because it allows a host to obtain a temporary IP address.

**DiffServe**

(*Differentiated Services*) A scheme adopted to replace the original IP type of service. DiffServe provides up to 64 possible types of service (e.g., priorities); each datagram carries a field in the header that specifies the type of service it desires.

**directed broadcast address**

An IP address that specifies "all hosts" on a specific network. A single copy of a directed broadcast is routed to the specified network where it is broadcast to all machines on that network.

**distance-vector**

A class of routing update protocols that use a distributed shortest path algorithm (SPF) in which each participating router sends its neighbors a list of networks it can reach and the distance to each network.

**DNS**

*(Domain Name System)* The on-line distributed database system used to map human-readable machine names into IP addresses. DNS servers throughout the connected Internet implement a hierarchical namespace that allows sites freedom in assigning machine names and addresses. DNS also supports separate mappings between mail destinations and IP addresses.

**domain**

A part of the DNS naming hierarchy. Syntactically, a domain name consists of a sequence of names (labels) separated by periods (dots).

**dotted decimal notation**

A syntactic form used to represent 32-bit binary integers that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. Many TCP/IP application programs accept dotted decimal notation in place of destination machine names.

**dotted hex notation**

A syntactic form used to represent binary values that consists of hexadecimal values for each 8-bit quantity with dots separating them.

**dotted quad notation**

A syntactic form used to represent binary values that consists of hexadecimal values for each 16-bit quantity with dots separating them.

**DS3**

A telephony classification of speed for leased lines equivalent to approximately 45 Mbps.

**DSL**

*(Digital Subscriber Line)* A set of technologies used to provide high-speed data service over the copper wires that connect between telephone offices, local residences or businesses.

**DTE**

*(Data Terminal Equipment)* Term ITU protocol standards apply to computers and/or terminals to distinguish them from the packet switching network to which they connect. Also see *DCE*.

**DVMRP**

*(Distance Vector Multicast Routing Protocol)* A protocol used to propagate multicast routes.

**E.164**

An address format specified by ITU and used with ATM.

**EACK**

(*Extended ACKnowledgement*) Synonym for *SACK*.

**echo request and reply**

A type of message that is used to test network connectivity. The ping program uses ICMP echo request and reply messages.

**EGP**

(*Exterior Gateway Protocol*) A term applied to any protocol used by a router in one autonomous system to advertise network reachability to a router in another autonomous system. BGP-4 is currently the most widely used exterior gateway protocol.

**EIA**

(*Electronics Industry Association*) A standards organization for the electronics industry. Known for RS232C and RS422 standards that specify the electrical characteristics of interconnections between terminals and computers or between two computers.

**encapsulation**

The technique used by layered protocols in which a lower level protocol accepts a message from a higher level protocol and places it in the data portion of the low-level frame. Encapsulation means that datagrams traveling across a physical network have a sequence of headers in which the first header comes from the physical network frame, the next from the Internet Protocol (IP), the next from the transport protocol, and so on.

**end-to-end**

Characteristic of any mechanism that operates only on the original source and final destination. Applications and transport protocols like TCP are classified as end-to-end.

**epoch date**

A point in history chosen as the date from which time is measured. TCP/IP uses January 1, 1900, Universal Time (formerly called Greenwich Mean Time) as its epoch date. When TCP/IP programs exchange date or time of day they express time as the number of seconds past the epoch date.

**ESP**

(*Encapsulating Security Payload*) A packet format used by IPsec to send encrypted information.

**Ethernet**

A popular local area network technology invented at the Xerox Corporation Palo Alto Research Center. An Ethernet is a passive coaxial cable; the interconnections contain all active components. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Xerox Corporation, Digital Equipment Corporation, and Intel Corporation developed and published the standard for 10 Mbps Ethernet. Originally, Ethernet used a coaxial cable. Later versions use a smaller coaxial cable (*thinner*) or twisted pair cable (10Base-T).



**Ethernet meltdown**

An event that causes saturation or near saturation on an Ethernet. It usually results from illegal or misrouted packets, and typically lasts only a short time.

**EUI-64**

A 64-bit IEEE layer-2 addressing standard.

**exponential backoff**

See *binary exponential backoff*.

**extension header**

Any of the optional IPv6 headers that follows the base header.

**eXternal Data Representation**

See *XDR*.

**extra hop problem**

A routing problem in which a datagram takes an extra, unnecessary trip across a network. The problem can be difficult to detect because communication appears to work.

**fair queueing**

A well-known technique for controlling congestion in routers. Called “fair” because it restricts every host to an equal share of router bandwidth. Fair queueing is not completely satisfactory because it does not distinguish between small and large hosts or between hosts with a few active connections and those with many.

**Fast Ethernet**

A popular term for 100Base-T Ethernet.

**FCCSET**

(*Federal Coordinating Council for Science, Engineering, and Technology*) A government group noted for its report that called for high-speed computing and high-speed networking research.

**FDDI**

(*Fiber Distribution Data Interface*) A token ring network technology based on fiber optics. FDDI specifies a 100 Mbps data rate using 1300 nanometer light wavelength, and limits networks to approximately 200 km in length, with repeaters every 2 km or less.

**FDM**

(*Frequency Division Multiplexing*) The method of passing multiple, independent signals across a single medium by assigning each a unique carrier frequency. Hardware to combine signals is called a multiplexor; hardware to separate them is called a demultiplexor. Also see *TDM*.

**file server**

A process running on a computer that provides access to files on that computer to programs running on remote machines. The term is often applied loosely to computers that run file server programs.

**FIN**

A special TCP segment used to close a connection. Each side must send a FIN.

**firewall**

A configuration of routers and networks placed between an organization's internal internet and a connection to an external internet to provide security.

**five-layer reference model**

The protocol layering model used by TCP/IP. Although originally controversial, the success of TCP/IP has led to wide acceptance.

**fixed-length subnetting**

A subnet address assignment scheme in which all physical nets in an organization use the same mask. The alternative is *variable-length subnetting*.

**flat namespace**

Characteristic of any naming in which object names are selected from a single set of strings (e.g., street names in a typical city). Flat naming contrasts with hierarchical naming in which names are divided into subsections that correspond to the hierarchy of authority that administers them.

**flow**

A general term used to characterize a sequence of packets sent from a source to a destination. Some technologies define a separate flow for each pair of communicating applications, while others define a single flow to include all packets between a pair of hosts.

**flow control**

Control of the rate at which hosts or routers inject packets into a network or internet, usually to avoid congestion.

**Ford-Fulkerson algorithm**

A synonym for the distance-vector algorithm that refers to the researchers who discovered it.

**forwarding**

The process of accepting an incoming packet, looking up a next hop in a routing table, and sending the packet on to the next hop. IP routers perform datagram forwarding.

**fragment extension header**

An optional header used by IPv6 to mark a datagram as a fragment.

**fragmentation**

The process of dividing an IP datagram into smaller pieces when they must travel across a network that cannot handle the original datagram size. Each fragment has the same format as a datagram: fields in the IP header specify whether a datagram is a fragment, and if so, the offset of the fragment in the original datagram. IP software at the receiving end must reassemble fragments to produce the original datagram.

**frame**

Literally, a packet as it is transmitted across a serial line. The term derives from character oriented protocols that added special start-of-frame and end-of-frame characters when transmitting packets. We use the term throughout this book to refer to the objects that physical networks transmit.

**Frame Relay**

The name of a connection-oriented network technology that is offered by telephone companies.

**FTP**

(*File Transfer Protocol*) The TCP/IP standard, high-level protocol for transferring files from one machine to another. FTP uses TCP.

**full duplex**

Characteristic of a technology that allows simultaneous transfer of data in two directions. TCP provides full duplex connections.

**FYI**

(*For Your Information*) A subset of the RFCs that contain tutorials or general information about topics related to TCP/IP or the connected Internet.

**gated**

(*GATEway Daemon*) A program run on a router that uses an IGP to collect routing information from within one autonomous system and EGP to advertise the information to another autonomous system.

**gateway**

Any mechanism that connects two or more heterogeneous systems and translates among them. Originally, researchers used the term *IP gateway* for dedicated computers that route IP datagrams; vendors have adopted the term *IP router*.

**gateway requirements**

See *router requirements*.

**Gbps**

(*Giga Bits Per Second*) A measure of the rate of data transmission equal to  $2^{30}$  bits per second. Also see *Kbps*, *Mbps*, and *baud*.

**GGP**

(*Gateway to Gateway Protocol*) The protocol originally used by core gateways to exchange routing information. GGP is now obsolete.

**gopher**

An early menu-driven information service used in the Internet.

**GOSIP**

(*Government Open Systems Interconnection Profile*) A U.S. government procurement document that specified agencies may use OSI protocols in new networks after August 1991. Although GOSIP was originally thought to eliminate the use of TCP/IP on government internets, clarifications have specified that government agencies can continue to use TCP/IP.

**graceful shutdown**

A protocol mechanism that allows two communicating parties to agree to terminate communication without confusion even if underlying packets are lost, delayed, or duplicated. TCP uses a 3-way handshake to guarantee graceful termination.

**graft**

An operation in which a multicast router joins a shared forwarding tree; the opposite of *prune*.

**GRE**

(*Generic Routing Encapsulation*) A scheme for encapsulating information in IP that includes IP-in-IP as one possibility.

**H.323**

An ITU recommendation for a suite of protocols used for IP telephony.

**half duplex**

Characteristic of a technology that only permits data transmission in one direction at a time. Compare to *full duplex*.

**hardware address**

The low-level addresses used by physical networks. Synonyms include *physical address* and *MAC address*. Each type of network hardware has its own addressing scheme (e.g., an Ethernet address is 48 bits).

**header**

Information at the beginning of a packet or message that describes the contents and specifies a destination.

**HELLO**

A protocol used on the original NSFNET backbone. Although obsolete, Hello is interesting because it uses delay as the routing metric and chooses a path with minimum delay.

**HELO**

The command on the initial exchange of the SMTP protocol.

**hierarchical addressing**

An addressing scheme in which an address can be subdivided into parts that each identify successively finer granularity. IP addresses use a two-level hierarchy in which the first part of the address identifies a network and the second part identifies a particular host on that network. Routers use the network portion to forward a datagram until the datagram reaches a router that can deliver it directly. Subnetting introduces additional levels of hierarchical routing.

**historic**

An IETF classification used to discourage the use of a protocol. In essence, a program that is declared historic is obsolete.

**hold down**

A short fixed time period following a change to a routing table during which no further changes are accepted. Hold down helps avoid routing loops.

**hop count**

A measure of distance between two points in an internet. A hop count of  $n$  means that  $n$  routers separate the source and destination.

**hop limit**

The IPv6 name for the datagram header field that IPv4 calls *time to live*. The hop limit, which prevents datagrams from following a routing loop forever, is decremented by each router along the path.

**host**

Any end-user computer system that connects to a network. Hosts include devices such as printers, small notebook computers, as well as large supercomputers. Compare to *router*.

**host requirements**

A long document that contains revisions and updates of many TCP/IP protocols. The host requirements document is published in a pair of RFCs. See *router requirements*.

**host-specific route**

An entry in a routing table that refers to a single host computer as opposed to routes that refer to a network, an IP subnet, or a default.

**HTML**

(*HyperText Markup Language*) The standard document format used for Web pages.

**HTTP**

(*Hypertext Transfer Protocol*) The protocol used to transfer Web documents from a server to a browser.

**hub**

An inexpensive electronic device to which multiple computers attach, usually using twisted pair wiring, to send and receive packets. A hub operates at layer 2 by replicating signals. Ethernet hubs are especially popular.

**IAB**

(*Internet Architecture Board*) A small group of people who set policy and direction for TCP/IP and the global Internet. The IAB was formerly known as the *Internet Activities Board*. See *IETF*.

**IAC**

(*Interpret As Command*) An escape used by TELNET to distinguish commands from normal data.

**IANA**

(*Internet Assigned Number Authority*) Essentially one individual (Jon Postel), IANA was originally responsible for assigning IP addresses and the constants used in TCP/IP protocols. Replaced by ICANN in 1999.

**ICANN**

(*Internet Corporation For Assigned Names and Numbers*) The organization that took over the IANA duties after Postel's death.

**ICCB**

*(Internet Control and Configuration Board)* A predecessor to the IAB.

**ICMP**

*(Internet Control Message Protocol)* An integral part of the Internet Protocol (IP) that handles error and control messages. Specifically, routers and hosts use ICMP to send reports of problems about datagrams back to the original source that sent the datagram. ICMP also includes an echo request/reply used to test whether a destination is reachable and responding.

**ICMPv6**

*(Internet Control Message Protocol version 6)* The version of ICMP that has been defined for use with IPv6.

**IEN**

*(Internet Engineering Notes)* A series of notes developed in parallel to RFCs. Although the series is obsolete, some IENs contain early discussion of TCP/IP and the Internet not found in RFCs.

**IESG**

*(Internet Engineering Steering Group)* A committee consisting of the IETF chairperson and the area managers. The IESG coordinates activities among the IETF working groups.

**IETF**

*(Internet Engineering Task Force)* A group of people under the IAB who work on the design and engineering of TCP/IP and the global Internet. The IETF is divided into areas, which each has an independent manager. Areas are further divided into working groups.

**IGMP**

*(Internet Group Management Protocol)* A protocol that hosts use to keep local routers apprised of their membership in multicast groups. When all hosts leave a group, routers no longer forward datagrams that arrive for the group.

**IGP**

*(Interior Gateway Protocol)* The generic term applied to any protocol used to propagate network reachability and routing information within an autonomous system. Although there is no single standard IGP, RIP is among the most popular.

**IMP**

*(Interface Message Processor)* The original term for packet switches in the ARPANET; now loosely applied to a switch in any packet network.

**InATMARP**

*(Inverse ATM ARP)* Part of the address resolution protocol needed for non-broadcast multiple access networks such as ATM.

**indirect delivery**

Delivery of a datagram through a router as opposed to a direct transmission from the source host to the destination host.

**INOC**

(*Internet Network Operations Center*) Originally, a group of people at BBN that monitored and controlled the Internet core gateway system. Now applied to any group that monitors an internet.

**inter-autonomous system routing**

Also known as exterior routing. BGP-4 is currently the most popular protocol for exterior routing.

**International Organization for Standardization**

See *ISO*.

**International Telecommunications Union (ITU)**

An international organization that sets standards for interconnection of telephone equipment. It defined the standards for X.25 network protocols. (Note: in Europe, *PTTs* offer both voice telephone services and X.25 network services).

**internet**

Physically, a collection of packet switching networks interconnected by routers along with TCP/IP protocols that allow them to function logically as a single, large, virtual network. When written in upper case, Internet refers specifically to the global Internet.

**Internet**

The collection of networks and routers that spans over 200 countries, and uses TCP/IP protocols to form a single, cooperative virtual network.

**Internet address**

See *IP address*.

**Internet Draft**

A draft document generated by the IETF; if approved, the document will become an RFC.

**Internet Protocol**

See *IP*.

**Internet Society**

The non-profit organization established to foster interest in the Internet. The Internet Society is the host organization of the IAB.

**Internet worm**

A program designed to travel across the Internet and replicate itself endlessly. When a student released the Internet worm, it made the Internet and many attached computers useless for hours.

**interoperability**

The ability of software and hardware on multiple machines from multiple vendors to communicate meaningfully. This term best describes the goal of internetworking, namely, to define an abstract, hardware independent networking environment that makes it possible to build distributed computations that interact at the network transport level without knowing the details of underlying technologies.

**Intranet**

A private corporate network consisting of hosts, routers, and networks that use TCP/IP technology. An intranet may or may not connect to the global Internet.

**IP**

*(Internet Protocol)* The TCP/IP standard protocol that defines the IP datagram as the unit of information passed across an internet and provides the basis for connectionless, best-effort packet delivery service. IP includes the ICMP control and error message protocol as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two fundamental protocols.

**IP address**

A 32-bit address assigned to each host that participates in a TCP/IP internet. IP addresses are the abstraction of physical hardware addresses just as an internet is an abstraction of physical networks. To make routing efficient, each IP address is divided into a network portion and a host portion.

**IP datagram**

The basic unit of information passed across a TCP/IP internet. An IP datagram is to an internet as a hardware packet is to a physical network — each datagram contains a source and destination address along with data.

**IP gateway**

A synonym for *IP router*.

**IP-in-IP**

The encapsulation of one IP datagram inside another for transmission through a tunnel. IP in IP is often used to send multicast datagrams across the Internet.

**IP multicast**

An addressing and forwarding scheme that allows transmission of IP datagrams to a subset of hosts. The Internet currently does not have extensive facilities for routing IP multicast.

**IP router**

A device that connects two or more (possibly heterogeneous) networks and passes IP traffic between them. As the name implies, a router looks up the datagram's destination address in a routing table to choose a next hop.

**IP switching**

Originally a high-speed IP forwarding technology developed by Ipsilon Corporation, now generally used in reference to any of several similar technologies.

**IP telephony**

A telephone system that uses IP to transport digitized voice.

**IPng**

*(Internet Protocol — the Next Generation)* A term applied to all the activities surrounding the specification and standardization of the next version of IP. Also see *IPv6*.



**IPsec**

(*IP SECURITY*) A security standard that allows the sender to choose to authenticate or encrypt a datagram. IPsec can be used with either IPv4 or IPv6.

**IPv4**

(*Internet Protocol version 4*). The official name of the current version of IP.

**IPv6**

(*Internet Protocol version 6*). The name of the next version of IP. Also see *IPng*.

**IRSG**

(*Internet Research Steering Group*) The group of people who head the IRTF.

**IRTF**

(*Internet Research Task Force*) A group of people working on research problems related to TCP/IP and the connected Internet. The IRTF is not as active as the IETF.

**ISDN**

(*Integrated Services Digital Network*) The name of the digital network service that telephone carriers provide.

**ISO**

(*International Organization for Standardization*) An international body that drafts, discusses, proposes, and specifies standards for network protocols. ISO is best known for its 7-layer reference model that describes the conceptual organization of protocols. Although it has proposed a suite of protocols for Open System Interconnection, the OSI protocols have not been widely accepted in the commercial market.

**ISOC**

Abbreviation for *Internet SOCIety*.

**isochronous**

Characteristic of a network system that does not introduce jitter. The conventional telephone system is isochronous.

**ISODE**

(*ISO Development Environment*) Software that provides an ISO transport level protocol interface on top of TCP/IP. ISODE was designed to allow researchers to experiment with ISO's higher-level OSI protocols without requiring an internet that supports the lower levels of the OSI suite.

**ISP**

(*Internet Service Provider*) Any organization that sells Internet access, either permanent connectivity or dialup access.

**ITU**

Abbreviation for the *International Telecommunication Union*, a standards organization.

**jitter**

A technical term used to describe unwanted variance in delay caused when one packet in a sequence must be delayed more than another. The typical cause of jitter is other traffic on a network.

**Karn's Algorithm**

An algorithm that allows transport protocols to distinguish between valid and invalid round-trip time samples, and thus improve round-trip estimations.

**Kbps**

(*Kilo Bits Per Second*) A measure of the rate of data transmission equal to  $2^{10}$  bits per second. Also see *Gbps*, *Mbps*, and *baud*.

**keepalive**

A small message sent periodically between two communicating entities to ensure that network connectivity remains intact and that both sides are still responding. BGP uses keepalives.

**LAN**

(*Local Area Network*) Any physical network technology designed to span short distances (up to a few thousand meters). Usually, LANs operate at tens of megabits per second through several gigabits per second. Examples include Ethernet and FDDI. See *MAN* and *WAN*.

**layer 1**

A reference to the hardware interface layer of communication. The name is derived from the ISO 7-layer reference model. Layer 1 specifications refer to physical connections, including connector configuration and voltages on wires. (Sometimes called *level 1*.)

**layer 2**

In the ISO 7-layer model, a reference to link level communication (e.g., frame format). In the TCP/IP 5-layer model, layer 2 refers to physical frame format and addressing. Thus, a layer 2 address is a MAC address (e.g., an Ethernet address).

**layer 3**

In the ISO 7-layer model, a reference to the network layer. In the TCP/IP 5-layer model, a reference to the internet layer (IP and the IP datagram format). Thus, an IP address is a layer 3 address.

**leaf**

A graph-theoretic term for a router or a network at the "edge" of an internet.

**link-local address**

An address used with IPv6 that has significance only on a single network.

**link state routing**

One of two approaches used by routing protocols in which routers broadcast status messages and use Dijkstra's SPF algorithm to compute shortest paths. See *distance vector routing*.

**link status routing**

A synonym for *link state routing*.

**LIS**

(*Logical IP Subnet*) A group of computers connected via ATM that use ATM as an isolated local network. A computer in one LIS cannot send a datagram directly to a computer in another LIS.

**little endian**

A format for storage or transmission of binary data in which the least-significant byte (bit) comes first. See *big endian*.

**LLC**

(*Logical Link Control*) One of the fields in an NSAP header.

**logical subnet**

An abbreviation of *Logical IP Subnet (LIS)*.

**long haul network**

Older term for *wide area network (WAN)*.

**longest-prefix matching**

The technique used by IP routers when searching a routing table. Among all entries that match the destination address, a router picks the one that has the longest subnet mask.

**loopback address**

A network address used for testing which causes outgoing data to be processed by the local protocol software without sending packets. IP uses 127.0.0.0 as the loopback prefix.

**LSR**

(*Loose Source Route*) An IP option that contains a list of router addresses that the datagram must visit in order. Unlike a strict source route, a loose source route allows the datagram to pass through additional routers not on the list. See *SSR*.

**MABR**

(*Multicast Area Border Router*) The MOSPF term for a multicast router that exchanges routing information with another area.

**MAC**

(*Media Access Control*) A general reference to the low-level hardware protocols used to access a particular network. The term *MAC address* is often used as a synonym for *physical address*.

**mail bridge**

Informal term used as a synonym for a *mail gateway*.

**mail exchanger**

A computer that accepts e-mail; some mail exchangers forward the mail to other computers. DNS has a separate address type for mail exchangers.

**mail exploder**

Part of an electronic mail system that accepts a piece of mail and a list of addresses as input and sends a copy of the message to each address on the list. Most electronic mail systems incorporate a mail exploder to allow users to define mailing lists locally.

**mail gateway**

A machine that connects to two or more electronic mail systems (especially dissimilar mail systems on two different networks) and transfers mail messages among them. Mail gateways usually capture an entire mail message, reformat it according to the rules of the destination mail system, and then forward the message.

**MAN**

(*Metropolitan Area Network*) Any physical network technology that operates at high speeds (usually hundreds of megabits per second through several gigabits per second) over distances sufficient for a metropolitan area. See *LAN* and *WAN*.

**Management Information Base**

See *MIB*.

**martians**

Humorous term applied to packets that turn up unexpectedly on the wrong network, often because of incorrect routing tables.

**mask**

See *subnet mask*.

**maximum transfer unit**

See *MTU*.

**MBONE**

(*Multicast BackBONE*). A cooperative agreement among sites to forward multicast datagrams across the Internet by use of IP tunneling.

**Mbps**

(*Millions of Bits Per Second*) A measure of the rate of data transmission equal to  $2^{20}$  bits per second. Also see *Gbps*, *Kbps*, and *baud*.

**MIB**

(*Management Information Base*) The set of variables (database) that a system running an SNMP agent maintains. Managers can fetch or store into these variables.

**MILNET**

(*MILitary NETwork*) Originally part of the ARPANET, MILNET was partitioned in 1984.

**MIME**

(*Multipurpose Internet Mail Extensions*) A standard used to encode data such as images as printable ASCII text for transmission through e-mail.

**mobile IP**

A technology developed by the IETF to permit a computer to travel to a new site while retaining its original IP address. The computer contacts a server to obtain a second, temporary address, and then arranges for all datagrams to be forwarded to it.

**Mosaic**

An early Web browser program.

**MOSPF**

(*Multicast Open Shortest Path First*) Multicast Extensions to the OSPF routing protocol.

**MPLS**

(*Multi-Protocol Label Switching*) A technology that uses high speed switching hardware to carry IP datagrams. MPLS is descended from IP switching and label switching.

**mrouted**

(*Multicast ROUTE Daemon*) A program used with a protocol stack that supports IP multicast to establish multicast routing.

**MSL**

(*Maximum Segment Lifetime*) The longest time a datagram can survive in the Internet. Protocols use the MSL to guarantee a bound on the time duplicate packets can survive.

**MSS**

(*Maximum Segment Size*) A term used with TCP. The MSS is the largest amount of data that can be transmitted in one segment. Sender and receiver negotiate maximum segment size at connection startup.

**MTU**

(*Maximum Transfer Unit* or *Maximum Transmission Unit*) The largest amount of data that can be transferred across a given physical network. The MTU is determined by the network hardware.

**multi-homed host**

A host using TCP/IP that has connections to two or more physical networks.

**multicast**

A technique that allows copies of a single packet to be passed to a selected subset of all possible destinations. Some hardware (e.g., Ethernet) supports multicast by allowing a network interface to belong to one or more multicast groups. IP supports an internet multicast facility.

**multiplex**

To combine data from several sources into a single stream in such a way that it can be separated again later. Multiplexing occurs at many levels. See *demultiplex*.

**multiplicative decrease**

A technique used by TCP to reduce transmission when congestion occurs. TCP decreases the size of the effective window by half each time a segment is lost.

**NACK**

*(Negative Acknowledgement)* A response from the recipient of data to the sender of that data to indicate that the transmission was unsuccessful (e.g., that the data was corrupted by transmission errors). Usually, a NACK triggers retransmission of the lost data.

**Nagle algorithm**

A self-clocking heuristic that clumps outgoing data to improve throughput and avoid silly window syndrome.

**NAK**

Synonym for *NACK*.

**name resolution**

The process of mapping a name into a corresponding address. The domain name system provides a mechanism for naming computers in which programs use remote name servers to resolve a machine name into an IP address.

**NAP**

*(Network Access Point)* One of several physical locations where ISPs interconnect their networks. A NAP also includes a route server that supplies each ISP with reachability information from the routing arbiter system. In addition to NAPs, many ISPs now have private peering arrangements.

**NAT**

*(Network Address Translation)* A technology that allows hosts with private addresses to communicate with an outside network such as the global Internet.

**NBMA**

*(Non-Broadcast Multi-Access)*. A characteristic of a network that connects multiple computers but does not supply hardware-level broadcast. ATM is the prime example of a NBMA network.

**Net 10 address**

A general reference to a nonroutable address (i.e., one that is reserved for use in an intranet and not used on the global Internet). The prefix 10.0.0.0 was formerly assigned to ARPANET; it was designated as a nonroutable address when the ARPANET ceased operation.

**NetBIOS**

*(Network Basic Input Output System)* NetBIOS is the standard interface to networks on IBM PC and compatible personal computers. TCP/IP includes guidelines that describe how to map NetBIOS operations into equivalent TCP/IP operations.

**network byte order**

The TCP/IP standard for transmission of integers that specifies the most significant byte appears first (big endian). Sending machines are required to translate from the local integer representation to network byte order, and receiving machines are required to translate from network byte order to the local machine representation.

**network management**

See *MIB* and *SNMP*.

**Next Header**

A field used in IPv6 to specify the type of the item that follows.

**NFS**

(*Network File System*) A protocol originally developed by SUN Microsystems, Incorporated that uses IP to allow a set of cooperating computers to access each other's file systems as if they were local.

**NIC**

(*Network Interface Card*) A hardware device that plugs into the bus on a computer and connects the computer to a network.

**NIST**

(*National Institute of Standards and Technology*) Formerly, the National Bureau of Standards. NIST is one standards organization within the US that establishes standards for network protocols.

**NLA**

(*Next Level Aggregation*) In IPv6 addressing, the third most significant set of bits in a unicast address. Also see *TLA*.

**NOC**

(*Network Operations Center*) Originally, the organization at BBN that monitored and controlled several networks that formed part of the global Internet. Now, used for any organization that manages a network.

**nonroutable address**

Any address that uses one of the network prefixes which are reserved for use in intranets. Routers in the global Internet will report an error if a datagram containing a nonroutable address accidentally reaches them. See *net-10 address*.

**NSAP**

(*Network Service Access Point*) An address format that can be encoded in 20 octets. The ATM Forum recommends using NSAP addresses.

**NSF**

(*National Science Foundation*) A U.S. government agency that funded some of the research and development of the Internet.

**NSFNET**

(*National Science Foundation NETwork*) Used to describe the Internet backbone in the U.S., which is supported by NSF.

**NVT**

(*Network Virtual Terminal*) The character-oriented protocol used by TELNET.

**OC series standards**

A series of standards for the transmission of data over optical fiber. For example, the popular OC3 standard has a bit rate of approximately 155 million bits per second.

**octet**

An 8-bit unit of data. Although engineers frequently use the term *byte* as a synonym for octet, a byte can be smaller or larger than 8 bits.

**one-armed router**

An IP router that understands two addressing domains, but only has one physical network connection. One-armed routers are typically used to add security or address translation rather than to forward packets between networks. Also called a *one-armed firewall*.

**OSI**

(*Open Systems Interconnection*) A reference to protocols developed by ISO as a competitor for TCP/IP. They are not widely deployed or supported.

**OSPF**

(*Open Shortest Path First*) A link state routing protocol design by the IETF.

**OUI**

(*Organizationally Unique Identifier*) Part of an address assigned to an organization that manufactures network hardware; the organization assigns a unique address to each device by using its OUI plus a suffix number.

**out of band data**

Data sent outside the normal delivery path, often used to carry abnormal or error indicators. TCP has an *urgent data* facility for sending out-of-band data.

**packet**

Used loosely to refer to any small block of data sent across a packet switching network.

**packet filter**

A mechanism in a router that can be configured to reject some types of packets and admit others. Packet filters are used to create a security firewall.

**path MTU**

The minimum MTU along a path from the source to destination, which specifies the largest datagram that can be sent along the path without fragmentation. The standard recommends that IP use Path MTU Discovery.

**PCM**

(*Pulse Code Modulation*) A standard for voice encoding used in digital telephony that produces 8000 8-bit samples per second.

**PDN**

(*Public Data Network*) A network service offered by a common carrier.

**PDU**

(*Packet Data Unit*) An ISO term used for either packet or message.

**peering arrangement**

An cooperative agreement between two ISPs to exchange both reachability information and data packets. In addition to peering at NAPs, large ISPs often have private peering arrangements.



**PEM**

(*Privacy Enhanced Mail*) A protocol for encrypting e-mail to prevent others from reading messages as they travel across an internet.

**perimeter security**

A network security mechanism that places a firewall at each connection between a site and outside networks.

**physical address**

A synonym for *MAC address* or *hardware address*.

**PIM-DM**

(*Protocol Independent Multicast Dense Mode*) A data-driven multicast routing protocol similar to DVMRP.

**PIM-SM**

(*Protocol Independent Multicast Sparse Mode*) A demand-driven multicast routing protocol that extends the ideas in CBT.

**PING**

(*Packet InterNet Groper*) The name of a program used with TCP/IP internets to test reachability of destinations by sending them an ICMP echo request and waiting for a reply. The term is now used like a verb as in, "please ping host A to see if it is alive."

**playback point**

The minimum amount of data required in a jitter buffer before playback can begin.

**point-to-point network**

Any network technology such as a serial line that connects exactly two machines. Point-to-point networks do not require attached computers to have a hardware address.

**poison reverse**

A heuristic used by distance-vector protocols such as RIP to avoid routing loops. When a route disappears, instead of simply removing the route from its advertisement, a router advertises that the destination is no longer reachable.

**POP**

(*Post Office Protocol*) The protocol used to access and extract e-mail from a mailbox.

**port**

See *protocol port*.

**positive acknowledgement**

Synonym for *acknowledgement*.

**POTS**

(*Plain Old Telephone Service*) A reference to the standard voice telephone system.

**PPP**

(*Point to Point Protocol*) A protocol for framing IP when sending across a serial line. Also see *SLIP*.

**promiscuous ARP**

See *proxy ARP*.

**promiscuous mode**

A feature of network interface hardware that allows a computer to receive all packets on the network.

**protocol**

A formal description of message formats and the rules two or more machines must follow to exchange those messages. Protocols can describe low-level details of machine to machine interfaces (e.g., the order in which the bits from a byte are sent across a wire), or high-level exchanges between application programs (e.g., the way in which two programs transfer a file across an internet). Most protocols include both intuitive descriptions of the expected interactions as well as more formal specifications using finite state machine models.

**protocol port**

The abstraction that TCP/IP transport protocols use to distinguish among multiple destinations within a given host computer. TCP/IP protocols identify ports using small positive integers. Usually, the operating system allows an application program to specify which port it wants to use. Some ports are reserved for standard services (e.g., electronic mail).

**provider prefix**

An addressing scheme in which an ISP owns a prefix of an address and assigns each customer addresses that begin with the prefix. IPv6 offers provider prefix addressing.

**provisioned service**

A service that is configured manually.

**proxy**

Any device or system that acts in place of another (e.g., a proxy Web server acts in place of another Web server).

**proxy ARP**

The technique in which one machine, usually a router, answers ARP requests intended for another by supplying its own physical address. By pretending to be another machine, the router accepts responsibility for forwarding packets. The purpose of proxy ARP is to allow a site to use a single IP network address with multiple physical networks.

**prune**

An operation in which a multicast router removes itself from a shared forwarding tree; the opposite of *graft*.

**pseudo header**

Source and destination IP address information sent in the IP header, but included in a TCP or UDP checksum.

**PSN**

(*Packet Switching Node*) The formal name of ARPANET packet switches that replaced the original term *IMP*.

**PSTN**

(*Public Switched Telephone Network*) The standard voice telephone system.

**public key encryption**

An encryption technique that generates encryption keys in pairs. One of the pair must be kept secret, and one is published.

**PUP**

(*Parc Universal Packet*) In the internet system developed by Xerox Corporation, a PUP is the fundamental unit of transfer, like an IP datagram is in a TCP/IP internet. The name was derived from the name of the laboratory at which the Xerox internet was developed, the Palo Alto Research Center (PARC).

**push**

The operation an application performs on a TCP connection to force data to be sent immediately. A bit in the segment header marks pushed data.

**PVC**

(*Permanent Virtual Circuit*) The type of virtual circuit established by an administrator rather than by software in a computer. Unlike an SVC, a PVC lasts a long time (e.g., weeks or months).

**QoS**

(*Quality of Service*) Bounds on the loss, delay, jitter, and minimum throughput that a network guarantees to deliver. Some proponents argue that QoS is necessary for real-time traffic.

**RA**

See *routing arbiter*.

**RARP**

(*Reverse Address Resolution Protocol*) A protocol that can be used at startup to find an IP address. Although once popular, most computers now use *BOOTP* or *DHCP* instead.

**RDP**

(*Reliable Datagram Protocol*) A protocol that provides reliable datagram service on top of the standard unreliable datagram service that IP provides. RDP is not among the most widely implemented TCP/IP protocols.

**reachability**

A network is "reachable" from a given host if a datagram can be sent from the host to a destination on the network. Exterior routing protocols exchange reachability information.

**reassembly**

The process of collecting all the fragments of an IP datagram and using them to create a copy of the original datagram. The ultimate destination performs reassembly.

**RED**

*(Random Early Discard)* A technique routers use instead of tail-drop when their queue overflows to improve TCP performance. As the queue fills, the router begins discarding datagrams at random.

**redirect**

An ICMP message sent from a router to a host on a local network to instruct the host to change a route.

**reference model**

A description of how layered protocols fit together. TCP/IP uses a 5-layer reference model; earlier protocols used the ISO 7-layer reference model.

**regional network**

A network that covers a medium-size geographical area such as a few cities or a state.

**reliable multicast**

A multicast delivery system that guarantees reliable transfer to every member.

**reliable transfer**

Characteristic of a mechanism that guarantees to deliver data without loss, without corruption, without duplication, and in the same order as it was sent, or to inform the sender that delivery is impossible.

**repeater**

A hardware device that extends a LAN. A repeater copies electrical signals from one physical network to another. No longer popular.

**replay**

An error situation in which packets from a previous session are erroneously accepted as part of a later session. Protocols that do not prevent replay are not secure.

**reserved address**

A synonym for *nonroutable address*.

**reset**

A segment sent by TCP to report an error.

**resolution**

See *address resolution*

**RFC**

*(Request For Comments)* The name of a series of notes that contain surveys, measurements, ideas, techniques, and observations, as well as proposed and accepted TCP/IP protocol standards. RFCs are available on-line.

**RIP**

(*Routing Information Protocol*) A protocol used to propagate routing information inside an autonomous system. RIP derives from an earlier protocol of the same name developed at Xerox.

**RJE**

(*Remote Job Entry*) A service that allows submission of a (batch) job from a remote site.

**rlogin**

(*Remote LOGIN*) The remote login protocol developed for UNIX by Berkeley. Rlogin offers essentially the same service as TELNET.

**ROADS**

(*Running Out of Address Space*) A reference to the possible exhaustion of the IPv4 address space.

**round trip time**

The total time required to traverse a network from a source computer to a destination and back to the source. TCP uses round trip times to compute a retransmission timer.

**route**

In general, a route is the path that network traffic takes from its source to its destination. In a TCP/IP internet, each IP datagram is routed independently; routes can change dynamically.

**route aggregation**

The technique used by routing protocols to combine multiple destinations that have the same next hop into a single entry. A default route provides the highest degree of aggregation.

**route server**

A server that operates at a NAP and uses BGP to communicate reachability information from the routing arbiter database.

**routed**

(*Route Daemon*) A program devised for UNIX that implements the RIP protocol. Pronounced "route-d."

**router**

A special purpose, dedicated computer that attaches to two or more networks and forwards packets from one to the other. In particular, an IP router forwards IP datagrams among the networks to which it connects. A router uses the destination address on a datagram to choose a next-hop to which it forwards the datagram. Researchers originally used the term *gateway*.

**router alert**

An IP option that causes each intermediate router to examine a datagram even if the datagram is not destined to the router.

**router requirements**

A document that contains updates to TCP/IP protocols used in routers. See *host requirements*.

**routing arbiter**

A replicated, authenticated database that contains all possible routes in the Internet. Each ISP that connects to a NAP uses BGP to communicate with a route server to obtain information.

**routing loop**

An error condition in which a cycle of routers each has the next router in the cycle as the shortest path to a given destination.

**RP**

(*Rendezvous Point*) The router used as a target for a join request in a demand-driven multicast scheme.

**RPB**

(*Reverse Path Broadcast*) A synonym for *RPF*.

**RPC**

(*Remote Procedure Call*) A technology in which a program invokes services across a network by making modified procedure calls. The NFS protocol uses a specific type of RPC.

**RPF**

(*Reverse Path Forwarding*) A technique used to propagate broadcast packets that ensures there are no routing loops. IP uses reverse path forwarding to propagate subnet broadcast and multicast datagrams.

**RPM**

(*Reverse Path Multicast*) A general approach to multicasting that uses the TRPB algorithm.

**RS**

See *route server*.

**RS232**

A standard by EIA that specifies the electrical characteristics of slow speed interconnections between terminals and computers or between two computers. Although the standard commonly used is RS232C, most people refer to it as RS232.

**RST**

(*ReSeT*) A common abbreviation for a TCP *reset* segment.

**RSVP**

(*Resource ReserVation Protocol*) The protocol that allows an endpoint to request a flow with specific QoS; routers along the path to the destination must agree before they approve the request.

**RTCP**

(*RTP Control Protocol*) The companion protocol to RTP used to control a session.

**RTO**

(*Round trip Time-Out*) The delay used before retransmission. TCP computes RTO as a function of the current round trip time and variance.

**RTP**

(*Real-time Transport Protocol*) The primary protocol used to transfer real-time data such as voice and video over IP.

**RTT**

(*Round Trip Time*) A measure of delay between two hosts. The round trip time consists of the total time taken for a single packet or datagram to leave one machine, reach the other, and return. In most packet switching networks, delays vary as a result of congestion. Thus, a measure of round trip time is an average, which can have high standard deviation.

**SA**

(*Security Association*) Used with IPsec to denote a binding between a set of security parameters and an identifier carried in a datagram header. A host chooses SA bindings; they are not globally standardized. See *SPI*.

**SACK**

(*Selective ACKnowledgement*) An acknowledgement mechanism used with sliding window protocols that allows the receiver to acknowledge packets received out of order, but within the current sliding window. Also called extended acknowledgement. Compare to the *cumulative acknowledgement* scheme used by TCP.

**SAR**

(*Segmentation And Reassembly*) The process of dividing a message into cells, sending them across an ATM network, and reforming the original message. AAL5 performs SAR when sending IP across an ATM network.

**segment**

The unit of transfer sent from TCP on one machine to TCP on another. Each segment contains part of a stream of bytes being sent between the machines as well as additional fields that identify the current position in the stream and a checksum to ensure validity of received data.

**selective acknowledgement**

See SACK.

**self clocking**

Characteristic of any system that operates periodically without requiring an external clock (e.g., uses the arrival of a packet to trigger an action).

**self-healing**

Characteristic of a mechanism that overcomes failure automatically. A dual FDDI ring is self-healing because it can accommodate failure of a station or a link.

**self-identifying frame**

Any network frame or packet that includes a field to identify the type of the data being carried. Ethernet uses self-identifying frames, but ATM does not.

**server**

A running program that supplies service to clients over a network. Examples include providing access to files or to World Wide Web pages.

**seven-layer reference model**

See *ISO*.

**SGMP**

(*Simple Gateway Monitoring Protocol*) A predecessor of SNMP.

**shared tree**

A forwarding scheme used by demand-driven multicast routing protocols. A shared tree is an alternative to a shortest path tree.

**shortest path routing**

Routing in which datagrams are directed over the shortest path; all routing protocols try to compute shortest paths. Also see *SPF*.

**shortest path tree**

The multicast forwarding tree that is optimal from a given source to all members of the group. A shortest path trees is an alternative to a shared tree.

**signaling**

A telephony term that refers to protocols which establish a circuit.

**silly window syndrome**

A condition that can arise in TCP in which the receiver repeatedly advertises a small window and the sender repeatedly sends a small segment to fill it. The resulting transmission of small segments makes inefficient use of network bandwidth.

**SIP**

(*Session Initiation Protocol*) A protocol devised by the IETF for signaling in IP telephony. (Note: SIP was formerly used to refer to *Simple IP*, a protocol that served as the basis for IPv6.)

**SIPP**

(*SIP Plus*) An extension of *Simple IP* that was proposed for IPv6. See *IPv6*.

**site-local address**

An address used with IPv6 that has significance only at a single site.

**sliding window**

Characteristic of protocols that allow a sender to transmit more than one packet of data before receiving an acknowledgement. After receiving an acknowledgement for the first packet sent, the sender "slides" the packet window and sends another. The number of outstanding packets or bytes is known as the window size; increasing the window size improves throughput.

**SLIP**

(*Serial Line IP*) A framing protocol used to send IP across a serial line. SLIP is popular when sending IP over dialup phone lines. See *PPP*.



**slow convergence**

A problem in distance-vector protocols in which two or more routers form a routing loop that persists until the routing protocols increment the distance to infinity.

**slow-start**

A congestion avoidance scheme in TCP in which TCP increases its window size as ACKs arrive. The term is a slight misnomer because slow-start achieves high throughput by using exponential increases.

**SMDS**

(*Switched Multimegabit Data Service*) A connectionless packet service developed by regional telephone companies.

**SMI**

(*Structure of Management Information*) Rules that describe the form of MIB variables.

**SMTP**

(*Simple Mail Transfer Protocol*) The TCP/IP standard protocol for transferring electronic mail messages from one machine to another. SMTP specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

**SNA**

(*System Network Architecture*) The name applied to an architecture and a class of network products offered by IBM Corporation. SNA does not interoperate with TCP/IP.

**SNAP**

(*SubNetwork Attachment Point*) An IEEE standard for a small header that is added to data when sending across a network that does not have self-identifying frames. The SNAP header specifies the type of the data.

**SNMP**

(*Simple Network Management Protocol*) A protocol used to manage devices such as hosts, routers, and printers. A specific version is denoted with a suffix (e.g., SNMPv3). Also see *MIB*.

**SOA**

(*Start Of Authority*) A keyword used with DNS to denote the beginning of the records for which a particular server is the authority. Other records in the server are reported as non-authoritative answers.

**socket API**

The set of procedures an application uses to communicate over a TCP/IP network. The name is derived from an abstraction offered by the Unix operating system.

**soft state**

A technique in which a receiver times out information rather than depending on the sender to maintain it. Soft state works well when the sender and receiver become disconnected.

**source quench**

A congestion control technique in which a machine experiencing congestion sends a message back to the source of the packets requesting that the source stop transmitting. In a TCP/IP internet, routers send an ICMP source quench message when a datagram overruns the input queue.

**source route**

A route that is determined by the source. In IP, a source route consists of a list of routers a datagram should visit; the route is specified as an IP option. Source routing is most often used for debugging. See *LSR* and *SSR*.

**source tree**

A synonym for *shortest path tree*.

**SPF**

(*Shortest Path First*) A class of routing update protocols that uses Dijkstra's algorithm to compute shortest paths. See *link state routing*.

**SPI**

(*Security Parameters Index*) The identifier IPsec uses to specify the Security Association that should be used to process a datagram.

**split horizon update**

A heuristic used by distance-vector protocols such as RIP to avoid routing loops. Routes are not advertised over the interface from which they were learned.

**SS7**

(*Signaling System 7*) The conventional telephone system standard used for signaling.

**SSL**

(*Secure Sockets Layer*) A de facto standard for secure communication created by Netscape, Inc. SSL was an Internet Draft, but did not become an RFC.

**SSR**

(*Strict Source Route*) An IP option that contains a list of router addresses that the datagram must visit in order. See *LSR*.

**standard byte order**

See *network byte order*.

**STD**

(*STanDard*) The designation used to classify a particular RFC as describing a standard protocol.

**store-and-forward**

The paradigm used by IP routers in which an incoming datagram is stored in memory until it can be forwarded on toward its destination.

**subnet addressing**

An extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks. Outside of the site using subnet addressing, routing continues as usual by dividing the destination address into a network portion and a local portion. Routers and hosts inside a site using subnet addressing interpret the local portion of the address by dividing it into a physical network portion and a host portion.

**subnet mask**

A bit mask used to select the bits from an IP address that correspond to the subnet. Each mask is 32 bits long, with one bits in the portion that identifies a network and zero bits in the portion that identifies a host.

**SubNetwork Attachment Point**

See *SNAP*.

**supernet addressing**

Another name for *CIDR*.

**SVC**

(*Switched Virtual Circuit*) The type of virtual circuit established dynamically and terminated when no longer needed; usually software in a computer requests an SVC. Unlike a PVC, an SVC can have a short duration.

**SWS**

See *silly window syndrome*.

**SYN**

(*SYNchronizing segment*) The first segment sent by the TCP protocol, it is used to synchronize the two ends of a connection in preparation for opening a connection.

**T3**

The telephony designation for a protocol used over DS3-speed lines. The term is often used (incorrectly) as a synonym for DS3.

**tail drop**

A policy routers use to manage queue overflow which simply discards all datagrams that arrive after the queue is full. More harmful to TCP throughput than RED.

**TCP**

(*Transmission Control Protocol*) The TCP/IP standard transport level protocol that provides the reliable, full duplex, stream service on which many application protocols depend. TCP allows a process on one machine to send a stream of data to a process on another. TCP is connection-oriented in the sense that before transmitting data, participants must establish a connection. All data travels in TCP segments, which each travel across the Internet in an IP datagram. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two fundamental protocols.

**TCP/IP Internet Protocol Suite**

The official name of the TCP/IP protocols.

**TDM**

(*Time Division Multiplexing*) A technique used to multiplex multiple signals onto a single hardware transmission channel by allowing each signal to use the channel for a short time before going on to the next one. Also see *FDM*.

**TDMA**

(*Time Division Multiple Access*) A method of network access in which time is divided into slots and each node on the network is assigned one of the slots. Because all nodes using TDMA must synchronize exactly (even though the network introduces propagation delays between them), TDMA technologies are difficult to design and the equipment is expensive.

**TELNET**

The TCP/IP standard protocol for remote terminal service. TELNET allows a user at one site to interact with a remote timesharing system at another site as if the user's keyboard and display connected directly to the remote machine.

**TFTP**

(*Trivial File Transfer Protocol*) The TCP/IP standard protocol for file transfer with minimal capability and minimal overhead. TFTP depends only on the unreliable, connectionless datagram delivery service (UDP), so it is designed for use on a local network.

**thicknet**

Used to refer to the original thick coaxial cable used with 10Base5 Ethernet. See *thinnet*, *10Base2*, and *10Base-T*.

**thinnet**

Used to refer to the thinner, more flexible coaxial cable used with 10Base2 Ethernet. See *thicknet*, *10Base5*, and *10Base-T*.

**three-way handshake**

The 3-segment exchange TCP uses to reliably start or gracefully terminate a connection.

**TLA**

(*Top Level Aggregation*) In IPv6 addressing, the second most significant set of bits in a unicast address. Also see *NLA*.

**TLI**

(*Transport Layer Interface*) An alternative to the socket interface defined for System V UNIX.

**TLV encoding**

Any representation format that encodes each item with three fields: a type, a length, and a value. IP options often use TLV encoding.

**tn3270**

A version of TELNET for use with IBM 3270 terminals.

**token ring**

When used in the generic sense, a type of network technology that controls media access by passing a distinguished packet, called a token, from machine to machine. A computer can only transmit a packet when holding the token. When used in a specific sense, it refers to the token ring network hardware produced by IBM.

**TOS**

(*Type Of Service*) A reference to the original interpretation of the field in an IPv4 header that allows the sender to specify the type of service desired. Now replaced by *DiffServe*.

**TP-4**

A protocol designed by ISO to be similar to TCP.

**traceroute**

A program that prints the path to a destination. Traceroute sends a sequence of datagrams with the Time-To-Live set to 1, 2, etc., and uses the ICMP TIME EXCEEDED messages that are returned to determine routers along the path.

**traffic class**

A reference to a set of services available in the *DiffServe* interpretation.

**traffic policing**

A reference to mechanisms used with systems that guarantee QoS. Incoming traffic is measured, and any traffic that exceeds the agreed bounds is discarded.

**traffic shaping**

A reference to mechanisms used with systems that guarantee QoS. Incoming traffic is placed in a buffer and clocked out at a fixed rate.

**trailer encapsulation**

A nonconventional method of encapsulating IP datagrams for transmission in which the "header" information is placed at the end of the packet. Trailers have been used with Ethernet to aid in aligning data on page boundaries. ATM's AAL5 uses trailers.

**transceiver**

A device that connects a host interface to a local area network (e.g., Ethernet). Ethernet transceivers contain analog electronics that apply signals to the cable and sense collisions.

**triggered updates**

A heuristic used with distance-vector protocols such as RIP. When a routing table changes, the router sends updates immediately without waiting for the next cycle.

**TRPB**

(*Truncated Reverse Path Broadcast*) A technique used in data-driven multicasting to forward multicast datagrams. See *broadcast* and *prune*.

**TRPF**

(*Truncated Reverse Path Forwarding*) A synonym for *TRPB*.

**TTL**

(*Time To Live*) A technique used in best-effort delivery systems to avoid endlessly looping packets. For example, each IP datagram is assigned an integer time to live when it is created. Each router decrements the time to live field when the datagram arrives, and a router discards any datagram if the time to live counter reaches zero.

**tunneling**

A technique in which a packet is encapsulated in a high-level protocol and passed across a transport system. The MBONE tunnels each IP multicast datagram inside a conventional IP datagram; a VPN uses tunneling to pass encrypted datagrams between sites. See *IP-in-IP*.

**twisted pair Ethernet**

The 10Base-T Ethernet wiring scheme that uses twisted pair wires from each computer to a hub. See *thicknet* and *thinnet*.

**type of service routing**

A routing scheme in which the choice of path depends on the characteristics of the underlying network technology as well as the shortest path to the destination.

**UART**

(*Universal Asynchronous Receiver and Transmitter*) An electronic device consisting of a single chip that can send or receive characters on asynchronous serial communication lines that use RS232. UARTs are flexible because they have control lines that allow the designer to select parameters like transmission speed, parity, number of stop bits, and modem control. UARTs appear in terminals, modems, and on the I/O boards in computers that connect the computer to terminal(s).

**UCBCAST**

See *Berkeley broadcast*.

**UDP**

(*User Datagram Protocol*) The protocol that allows an application program on one machine to send a datagram to an application program on another. UDP uses the Internet Protocol (IP) to deliver datagrams. Conceptually, the important difference between UDP datagrams and IP datagrams is that UDP includes a protocol port number, allowing the sender to distinguish among multiple application programs on a given remote machine.

**unicast**

A method of addressing and routing in which a packet is delivered to a single destination. Most IP datagrams are sent via unicast. See *multicast*.

**universal time**

The international standard time reference that was formerly called Greenwich Mean Time. It is also called universal coordinated time.

**unnumbered network**

A technique for conserving IP network prefixes that leaves a point to point connection between two routers unnumbered.

**unreliable delivery**

Characteristic of a mechanism that does not guarantee to deliver data without loss, corruption, duplication, or in the same order as it was sent. IP is unreliable.

**urgent data**

The method used in TCP to send data out of band. A receiver processes urgent data immediately upon receipt.

**URI**

(*Uniform Resource Identifier*) A generic term used to refer to a URN or a URL.

**URL**

(*Uniform Resource Locator*) A string that gives the location of a piece of information. The string begins with a protocol type (e.g., FTP) followed by the identification of specific information (e.g., the domain name of a server and the path name to a file on that server).

**URN**

(*Uniform Resource Name*) A string that gives the location of a piece of information. Unlike a URL, a URN is guaranteed to persist over long periods of time.

**UUCP**

(*Unix to Unix Copy Program*) An application program developed in the mid 1970s for version 7 UNIX that allows one UNIX timesharing system to copy files to or from another UNIX timesharing system over a single (usually dialup) link. Because UUCP is the basis for electronic mail transfer in UNIX, the term is often used loosely to refer to UNIX mail transfer.

**variable-length subnetting**

A subnet address assignment scheme in which each physical net in an organization can have a different mask. The alternative is *fixed-length subnetting*.

**vBNS**

(*very high speed Backbone Network Service*) The 155 Mbps backbone network that was deployed in 1995 and is now used for networking research.

**VC**

(*Virtual Circuit*) A path through a network from one application to another that is used to send data. The VC, established either by protocol software or manually, provides the illusion of a "connection". Although the concept is the same, ATM expands the term to *Virtual Channel*.

**vector-distance**

Now called *distance-vector*.

**very high speed Backbone Network Service**

See vBNS.

**virtual circuit**

The basic abstraction provided by a connection-oriented protocol like TCP. Once a virtual circuit has been created, it stays in effect until explicitly shut down.

**VLSM**

(*Variable Length Subnet Mask*) A subnet mask used with variable length subnetting.

**VPI/VCI**

(*Virtual Path Identifier plus Virtual Circuit Identifier*) A connection identifier used by ATM; each connection a host opens is assigned a unique VPI/VCI.

**VPN**

(*Virtual Private Network*) A technology that connects two or more separate sites over the Internet, but allows them to function as if they were a single, private network. VPN software guarantees that although packets travel across the Internet, the contents remains private.

**WAN**

(*Wide Area Network*) Any physical network technology that spans large geographic distances. Also called long-haul networks, WANs have significantly higher delays and higher costs than networks that operate over shorter distances. See *LAN* and *MAN*.

**well-known port**

Any of a set of protocol port numbers preassigned for specific uses by transport level protocols (i.e., TCP and UDP). Each server listens at a well-known port, so clients can locate it.

**window**

See *sliding window*.

**window advertisement**

A value used by TCP to allow a receiver to tell a sender the size of an available buffer.

**Windows Sockets Interface**

A variant of the socket API developed by Microsoft. Often called *WINSOCK*.

**working group**

A group of people in the IETF working on a particular protocol or design issue.

**World Wide Web**

The large hypermedia service available on the Internet that allows a user to browse information.

**WWW**

See *World Wide Web*.

**X**

See *X-Window System*.

**X.25**

An older protocol standardized by the ITU which was popular in Europe before TCP/IP.



**X25NET**

(*X.25 NETwork*) A service offered by CSNET that passed IP traffic between a subscriber site and the Internet using X.25.

**X.400**

The ITU protocol for electronic mail.

**XDR**

(*eXternal Data Representation*) The standard for a machine-independent data representation. To use XDR, a sender translates from the local machine representation to the standard external representation and a receiver translates from the external representation to the local machine representation.

**X-Window System**

A software system developed at MIT for presenting and managing output on bit-mapped displays. Each window consists of a rectangular region of the display that contains textual or graphical output from one remote program. A special program called a window manager allows the user to create, move, overlap, and destroy windows.

**zero window**

See *closed window*.

**zone of authority**

Term used in the domain name system to refer to the group of names for which a given name server is an authority. Each zone must be supplied by two name servers that have no common point of failure.

